Herramientas de desarrollo Blockchain

ASPECTOS TÉCNICOS

Índice Temático

- Smart contract o contrato inteligente
- Oracles (Oráculos)
- Solidity
- Herramientas para trabajar con Solidity
- Marcos de desarrollo Nodos y clientes
- Librerías de desarrollo con Ethereum
- Revisión de bloques en Ethereum

Smart contract o contrato inteligente

Programa informático que ejecuta acuerdos establecidos entre dos o más partes haciendo que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas.

1. Se programan las condiciones,
2. Se 'coloca' en una blockchain para que no pueda modificarse.
3. Generalmente el código está disponible para ofrecer transparencia

Aplicaciones innumerables:

- Automatización en compra de productos (maquina expendedora)
- Alquiler o compra de propiedades
- Otros servicios: SLAs

Smart contract o contrato inteligente

Características avanzadas:

Función multifirma:

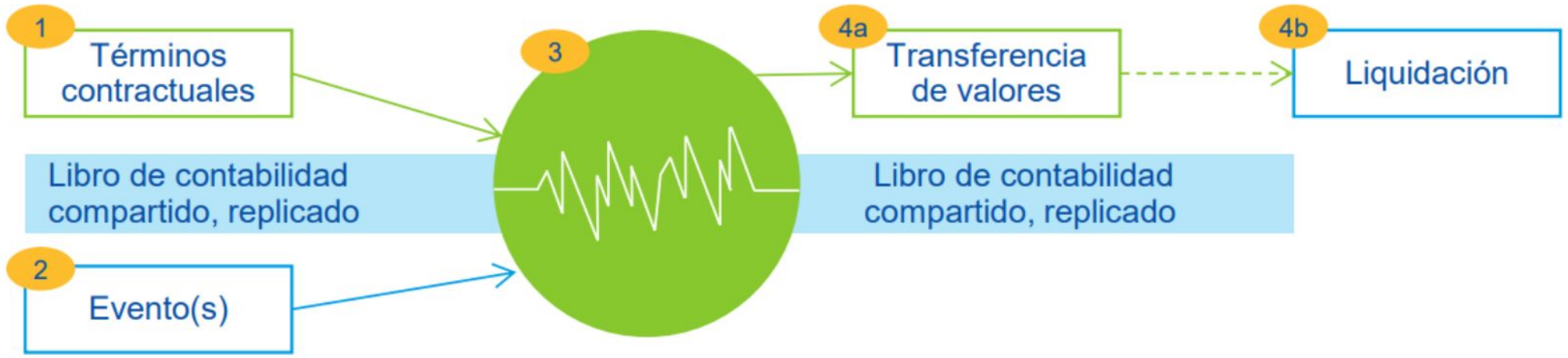
- Dos o más personas se deben de poner de acuerdo para hacer cumplir las condiciones de un contrato.
- El contrato bloquea los fondos de todo el mundo hasta que se dan las condiciones, por ejemplo que
  todos los usuarios hayan aportado.

Dobles depósitos:

- Permite a dos o más partes que no se conocen entre sí y que carecen de confianza el uno en el otro, realizar una transacción segura para ambos a través de un contrato inteligente.
- El contrato fuerza a cumplir el trato o destruye el dinero de ambos.

Smart contract o contrato inteligente

Aplicación de la lógica empresarial con los *smart contracts*



1

- Las contrapartidas establecen las obligaciones y las instrucciones de liquidación
- Activos puestos bajo la custodia del contrato inteligente
- Condiciones de ejecución ("Si... entonces...")

2

- Un evento desencadena la ejecución del contrato
- El evento puede hacer referencia a:
  - Una transacción iniciada
  - Información recibida

3

- Condiciones de contrato (Business Logic) dictadas en función de las condiciones que se encuentran

4a

- Valor transferido al destinatario al que va dirigido tal como lo estipulan los términos del contrato
- En el caso de los valores digitales de la cadena (ej. Bitcoin) las cuentas se liquidan atómicamente

4b

- En el caso de activos representados fuera de la cadena (p. ej. valores, activos inmobiliarios), las cuentas fuera de la cadena se ajustan a las instrucciones de liquidación
- Los cambios efectuados en las cuentas se reflejarán en el libro de contabilidad

Fuente: BBVA Research

Oracles (Oráculos)

Oracles (Oráculos)

Herramientas que permiten actualizar el estado de los contratos inteligentes con información externa

- Ejemplo: Apuestas deportivas.

Decisiones en el contrato pueden depender de información externa a blockchain

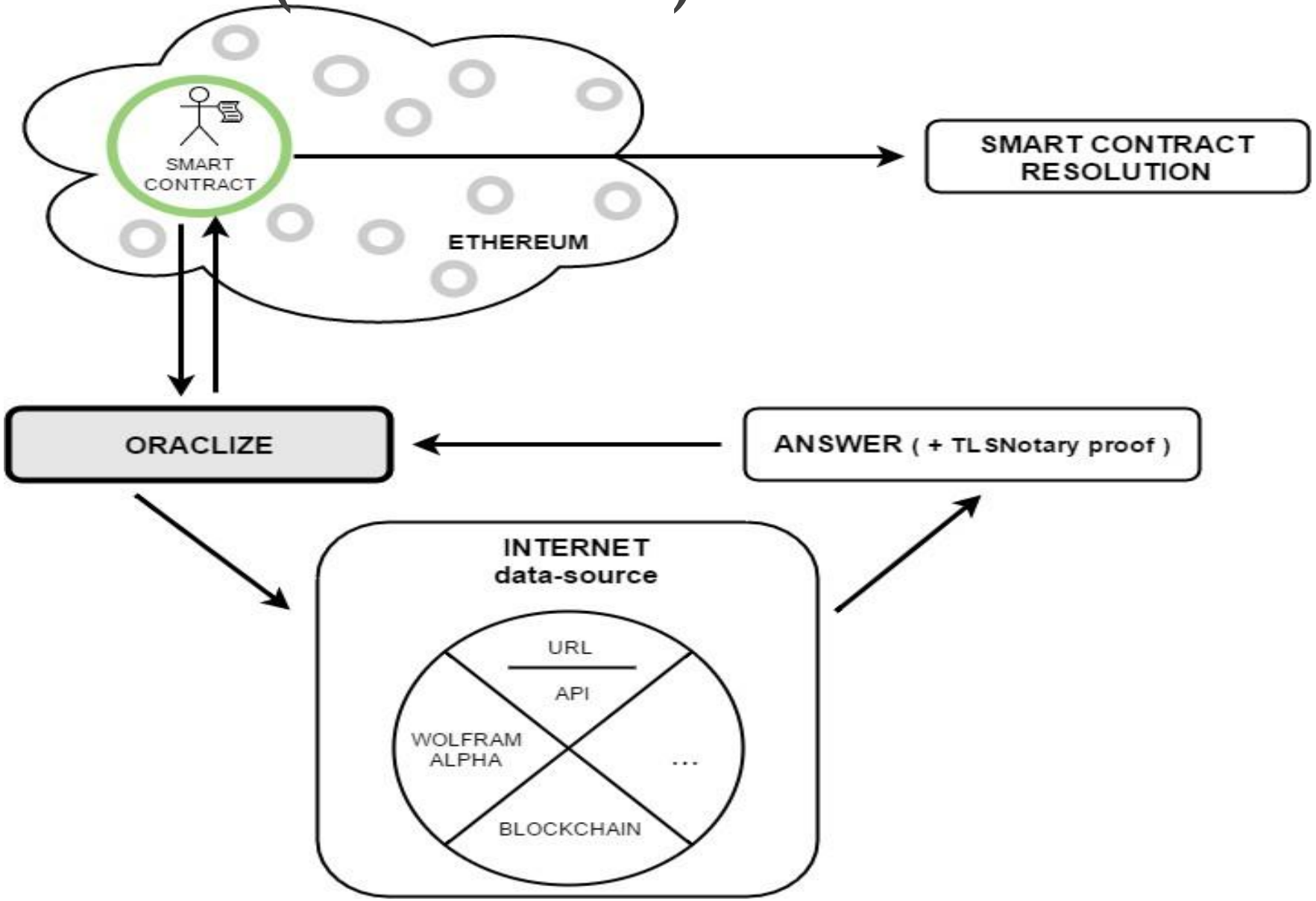
Al oráculo se le proporciona la dirección donde se va a encontrar la información determinante para ejecutar correctamente el contrato (resultado de un partido).

El más famoso es Chailink:

- https://chain.link/

Oracles (Oráculos)

Oracles (Oráculos)



Solidity

Solidity es un lenguaje de programación de alto nivel cuya síntesis es similar a otro de los lenguajes de programación más usados hoy en día: Javascript.

crear y desarrollar contratos inteligentes que se ejecuten en la Máquina Virtual Ethereum (EVM de sus siglas en inglés).

Es de tipo ‘Turing completo’. Ejecutar cualquier código definido por el desarrollador, siguiente el

modelo de máquina de Turing.

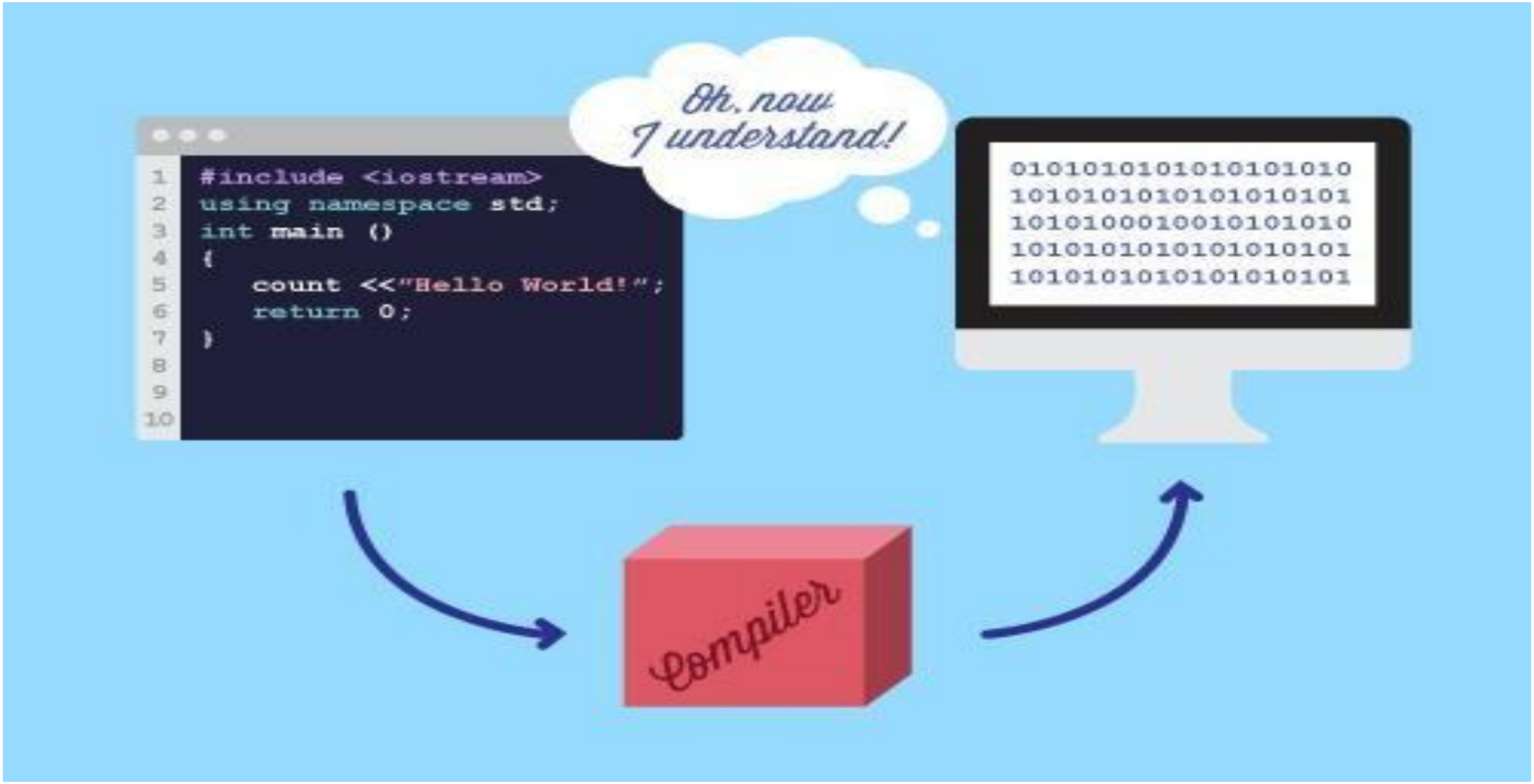
Bitcoin no tiene esta propiedad.

- ‘Turing Complete’ fue una de las razones que motivaron a Vitalik Buterin a crear el proyecto Ethereum

Problemas: Pueden haber bucles infinitos. Debemos limitar la ejecución mediante Gas (en bitcoin no hace falta).

Solidity

Requiere un compilador y un intérprete



Herramientas para trabajar con Solidity

Remix

- Anteriormente conocido como Browser Solidity, proporciona un entorno de desarrollo integrado (IDE) que permite escribir contratos inteligentes basados en Solidity

Se puede utilizar de manera online, o instalarlo en nuestro ordenador

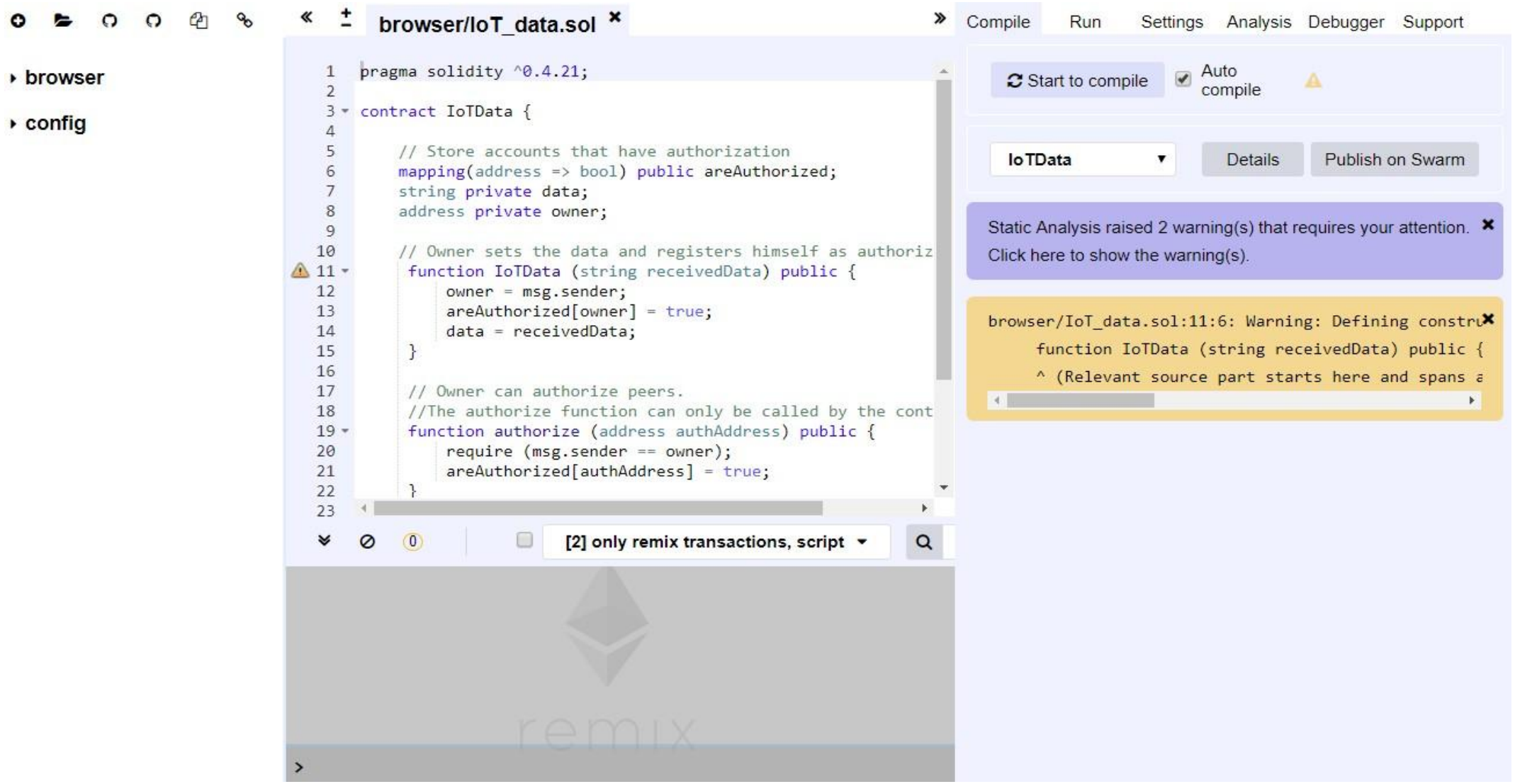
remix.ethereum.org.

Un guía muy buena:

https://miethereum.com/wp-content/uploads/2018/01/REMIX-EL-IDE-DE-ETHEREUM-TRADUCCI%C3%93N-AL-ESPA%C3%91OL.pdf

Herramientas para trabajar con Solidity

Remix



Marcos de desarrollo

Truffle: Framework autodenominado “la navaja suiza del ejército” para Ethereum. Un marco de desarrollo muy completo y muy utilizado entre los programadores de contratos inteligentes de Ethereum.

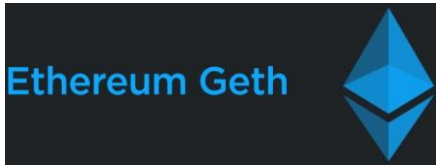
- http://truffleframework.com/

Hardhat es una de las herramientas más usadas para el desarrollo blockchain. Desde la compilación, testing, despliegue y el debugging de los contratos.
https://hardhat.org/

Nodos y clientes

Metamask: La Wallet oficial de Consensys. Con ella se puede implementar contratos inteligentes, pero además también sirve, entre otras cosas, para almacenar Ether, enviar/recibir transacciones e interactuar con la blockchain, ya sea en la red principal (mainnet) o en las redes de prueba (testnets).

Geth: Es una herramienta de línea de comandos multipropósito que ejecuta un cliente Ethereum completo y está implementado en Go.



Parity: Es otro cliente Ethereum, parecido a Geth, aunque los que lo han usado dicen que es mejor y más fácil de usar que éste, eso sí, más complejo en su instalación.

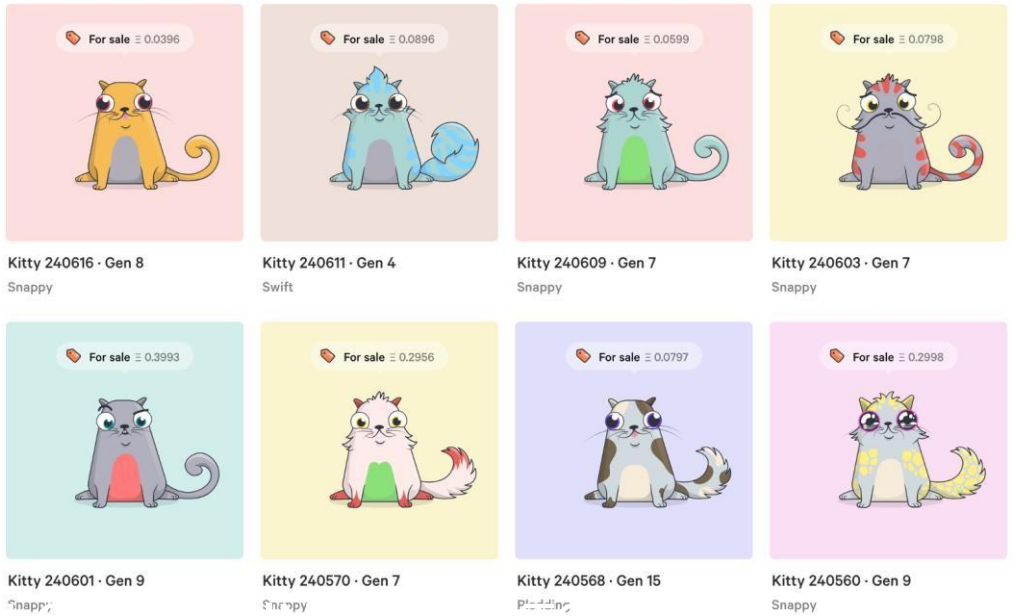
Nodos y clientes

Metamask: Extensión para los navegadores Google Chome, Opera, Firefox y Brave que integra gestión de wallets y capacidad para interactuar con Aplicaciones sobre blockchain o Dapps.

Hace las funciones de Wallet a la que poder pasar nuestros Ether e interactuar

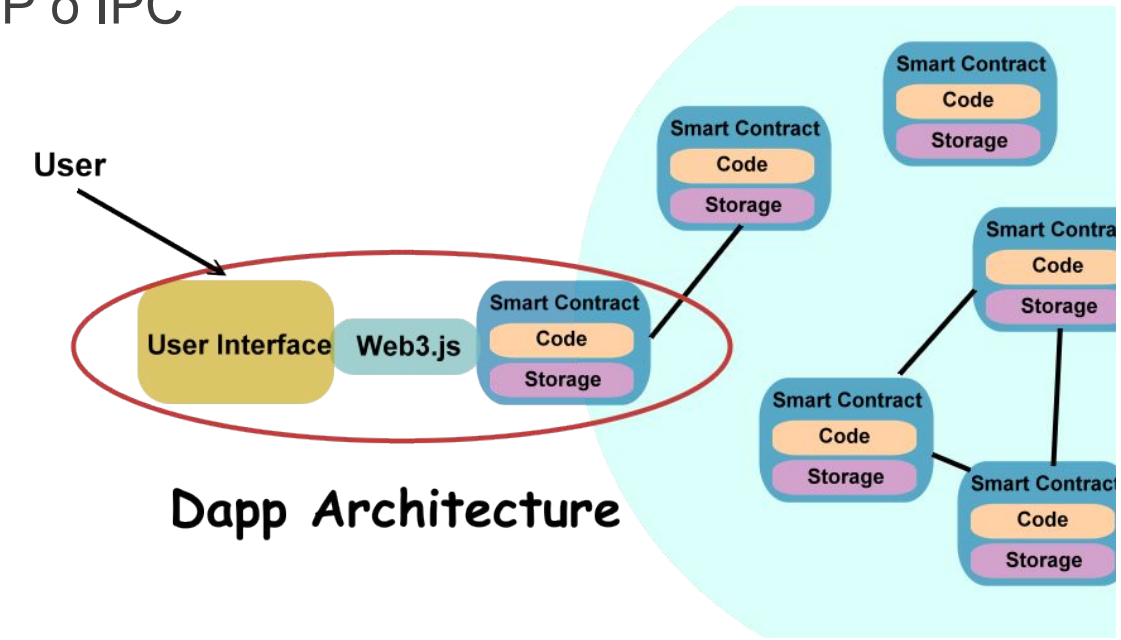
con Dapps. Ejemplo de Daap:

- https://www.cryptokitties.co/



Librerías de desarrollo con Ethereum

Web3.js: es una colección de librerías que nos permite interactuar con los clientes Ethereum mencionados anteriormente, ya sea de forma local (teniendo el cliente en nuestro propio ordenador) o de forma remota (estando el cliente instalado en otro ordenador) usando los protocolos HTTP o IPC



Revisión de bloques en Ethereum

Revisamos bloque 4588225

- Varias páginas:
- https://etherscan.io/
- https://etherchain.org/

Revisamos

- Height: Número de bloque
- Timestamp: Marca temporal
- Transactions: Transacciones
- Hash
- Parent Hash: Hash Padre

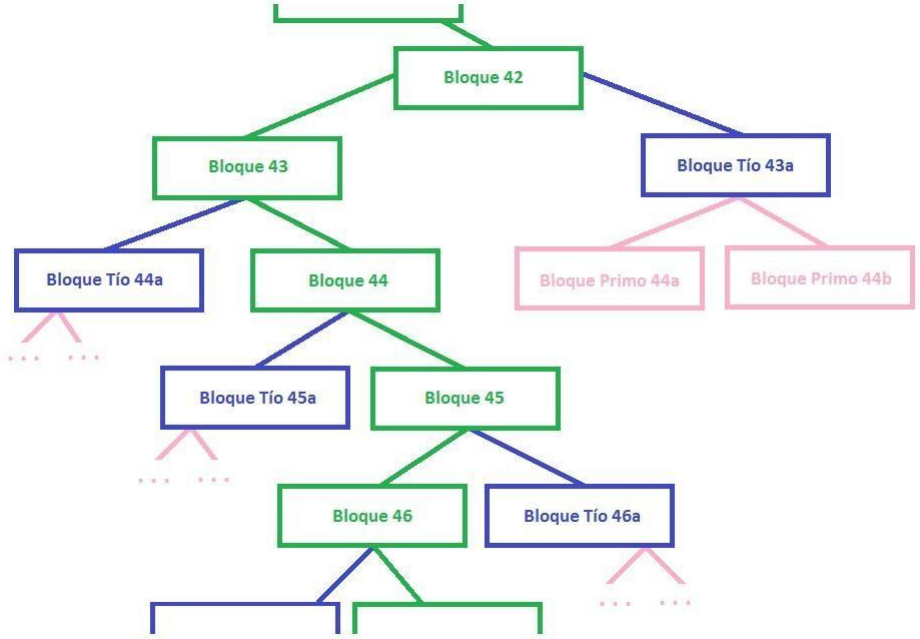
Revisión de bloques en Ethereum

Revisamos bloque 4588225

- Varias páginas:
- https://etherscan.io/
- https://etherchain.org/

Revisamos

- Sha3 Uncles / Uncle Hash: Hash tío
- Mined by / Miner: Minado por / Minero
- Difficulty: Dificultad
- Total difficulty: Dificultad total
- Size: Tamaño
- Gas used y Gas limit



Revisión de bloques en Ethereum

Revisamos bloque 4588225

- Varias páginas:
- https://etherscan.io/
- https://etherchain.org/

Revisamos

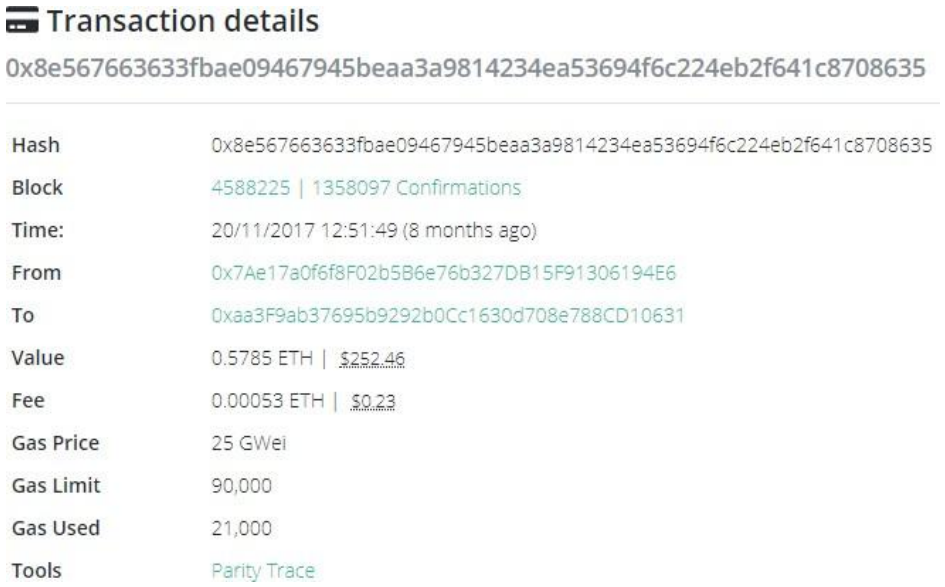
- Nonce / Poof of Work Nonce: Nonce de la prueba de trabajo
- Block reward: Recompensa del bloque
- Uncles reward: Recompensa tío
- Exta data: Datos extra
- *Lowest Gas price: Precio mínimo del Gas. 1 Gwei: 1.000.000.000 Wei (10^-9 ETH)*
- *Root / State root: Ruta / Ruta del estado: almacena el estado de todo el sistema al momento en el que el bloque fue generado.*
- *Tx Hash: Hash de todos los hashes de transacciones del bloque*

Revisión de bloques en Ethereum

Revisamos transacción (elegimos una del bloque)

Revisamos

- Hash / Tx Hash: Hash / Hash de la transacción
- *Tx Receipt Status: Estado del recibo de la transacción*
- *Block Height: Bloque donde se guarda*
- *Timestamp: Marca temporal*
- *From: Desde dónde o por quién fue realizada la transacción*
- *To: Hacia quién se realiza la transacción*



Revisión de bloques en Ethereum

Revisamos transacción (elegimos una del bloque)

Revisamos

- Gas limit and Gas used by Tx: Límite de Gas y Gas usado
- *Gas price: Precio del Gas*
- *Actual Tx Cost / Fee: Coste actual de la transacción / Com*
- *Cumulative Gas used: Acumulación de Gas usado: es la su transacción y todas las transacciones anteriores del mism*
- *Nonce*
- *Input data: Datos de entrada*

Transaction details

0x8e567663633fbae09467945beaa3a9814234ea53694f6c224eb2f641c8708635

Hash	0x8e567663633fbae09467945beaa3a9814234ea53694f6c224eb2f641c8708635
Block	4588225 | 1358097 Confirmations
Time:	20/11/2017 12:51:49 (8 months ago)
From	0x7Ae17a0f6f8F02b5B6e76b327DB15F91306194E6
To	0xaa3F9ab37695b9292b0Cc1630d708e788CD10631
Value	0.5785 ETH | $252.46
Fee	0.00053 ETH | $0.23
Gas Price	25 GWei
Gas Limit	90,000
Gas Used	21,000
Tools	Parity Trace