ETSIT UPM

dit UPM

Blockchain: Desarrollo de Aplicaciones

Repaso Ethereum

BCDA 2018

Versión: 2018-10-03

¿Qué es Blockchain?

- Blockchain es como una base de datos replicada en muchos nodos.
  - La base de datos es un libro de contabilidad, y cada nodo tiene una copia.
- Características:
  - Descentralizado, transparente, sin censura, inmutabilidad (no puede alterarse el pasado), solo pueden añadirse nuevos apuntes, seguridad, no hay que confiar en un tercero, funcionamiento ininterrumpido, puedes actualizarte en cualquier momento, seguridad por consenso, cada nodo es una copia de seguridad, ...
- Los nodos de esta red están distribuidos por todo el planeta.

Cadena de Bloques

- Blockchain es una Cadena de Bloques.
- En cada bloque se añaden las nuevas transacciones que se han realizado desde el bloque anterior.

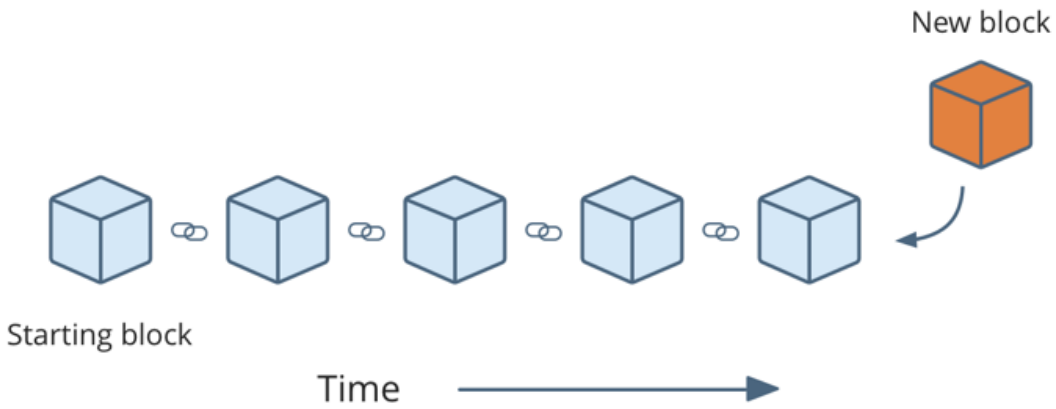
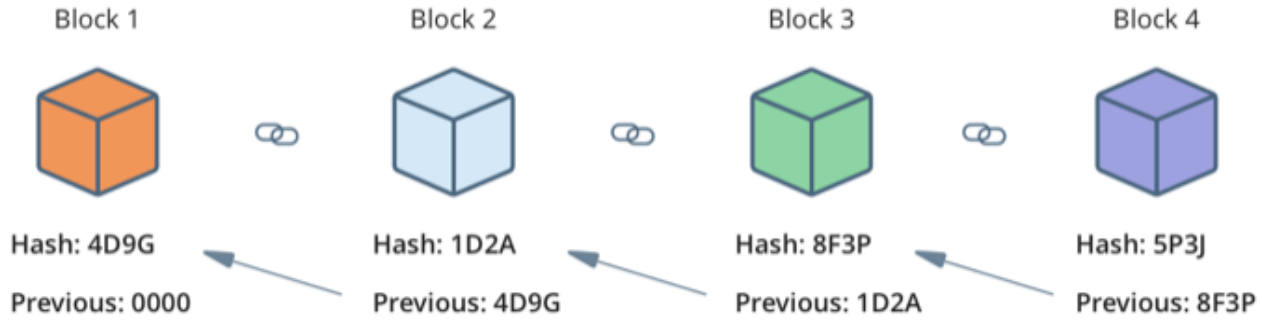


Imagen de https://blog.goodaudience.com/blockchain-explained-in-1000-words-6bb83020b036

- Cada bloque contiene:
  - sus transacciones.
  - el hash del bloque.
  - el hash del bloque anterior.



- Seguridad:
  - Si se altera algo, se rompe la cadena de hashes.
  - Recalcular los hashes es muy costoso.
    - No hay un algoritmo, es a base de fuerza bruta.
  - Habría que corromper la mitad + 1 de los nodos de la red.
  - Es decir, se necesita hacer muchos cálculos, se tardaría mucho tiempo, y se detectaría fácilmente.

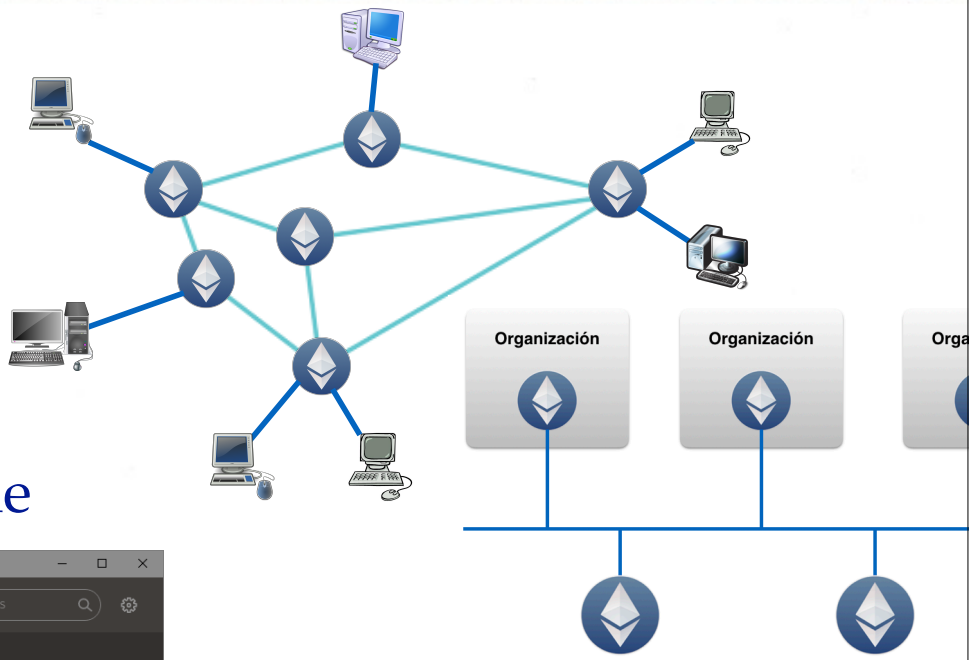
Imagen de https://blog.goodaudience.com/blockchain-explained-in-1000-words-6bb83020b036

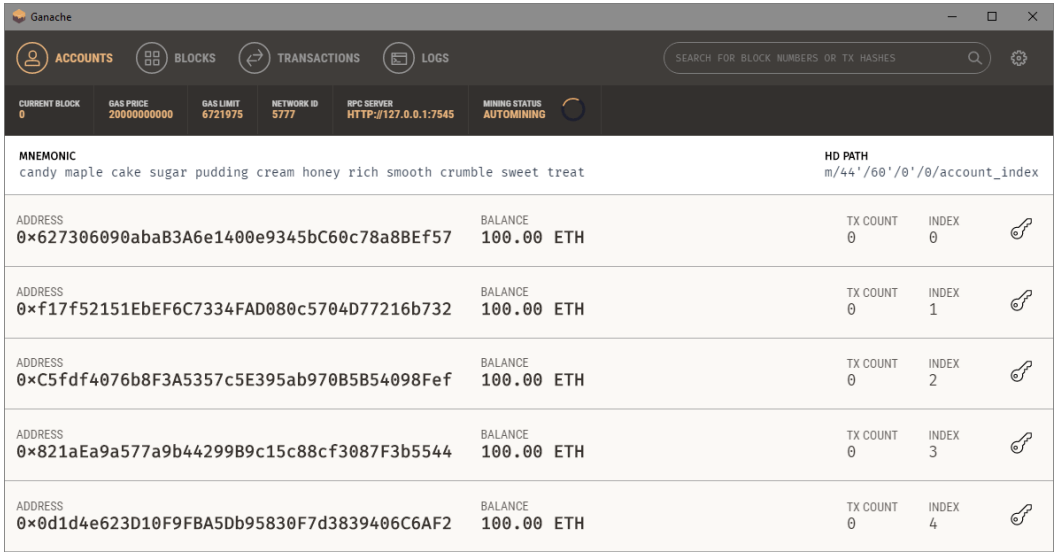
Redes Existentes

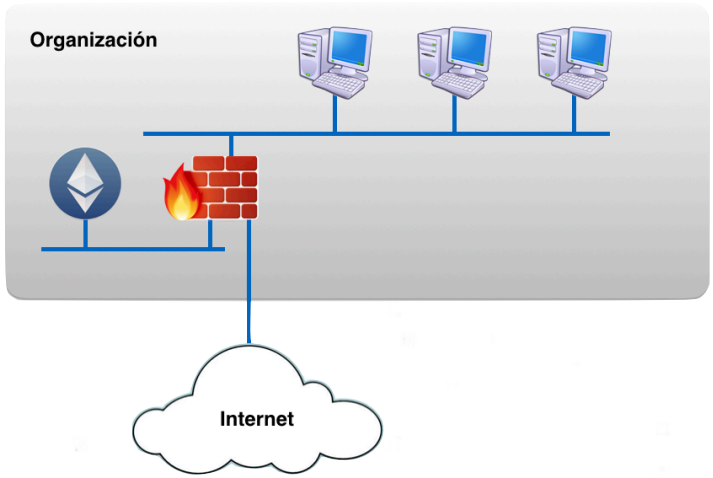
- Sabores:
  - Bitcoins, Ethereum, Quorum, Hyperledger, ...
- Diferencias:
  - Manejo de dinero (crypto monedas).
  - Soporte de Contratos Inteligentes.
  - Públicas, privadas, permisionadas o no, ...
- Ethereum:
  - https://www.ethereum.org

Redes Desplegadas

- Ethereum:
  - Main Net y redes privadas.
  - Redes de prueba.
    - Ropsten, Rinkeby
  - Redes ligeras de desarrollo.
    - ethereumjs-testrpc, Ganache







Cuentas Ethereum

- Dos tipos de cuentas:
  - Externally Owned Accounts (EOA).
    - Son principalmente las cuentas que usa un usuario para crear transacciones.
    - Tienen un balance.
    - ...
  - Contract Accounts.
    - Donde se ha desplegado un contrato (el programa).
    - Tienen un balance.
    - Tienen el estado del contrato.
    - ...

Cuentas EOA (de Usuario)

- Las cuentas de usuario:
  - Tienen una clave pública y privada.
    - Protegidas por una contraseña.
  - Mantienen un balance (dinero).
- El acceso a la clave privada es necesario para realizar transacciones.
- La gestión de nuestras cuentas y el uso de la clave privada se hace en:
  - Los propios nodos con los que nos conectamos a la red (públicas o privadas)
    - Geth (go-ethereum) - más usado, go.
    - WebThree (cpp-ethereum) - cpp
    - Parity - más rápido y ligero, Rust.
    - ...
  - Plugins que se conectan a nodos de terceros.
    - MetaMask - extensión de Chrome y Firefox - Usa Infura
  - Nodos no conectados a la red.
    - Mantienen las cuentas, se crean y firman las transacciones en ellos, y se envían a la red usando servicios como Etherscan o Infura.
  - Wallet Hardware
    - Almacenan las clases y el proceso de firmado se hace en hardware, conectándose a la red solo para enviar las transacciones firmadas.
    - Ledger, Trezor

Ciclo de Vida de una Transacción

- En un contrato se ejecuta el siguiente código para hacer una transacción:

```
Voting.deployed().then(function(instance) {
  instance.voteForCandidate('Nick', {gas: 140000, from:
web3.eth.accounts[0]}).then(function(r) {
    console.log("Voted successfully!")
  })
})
```

Ejemplo: https://medium.com/blockchannel/life-cycle-of-an-ethereum-transaction-e5c66bae0f6e

- Se crea el objeto con la transacción a enviar:

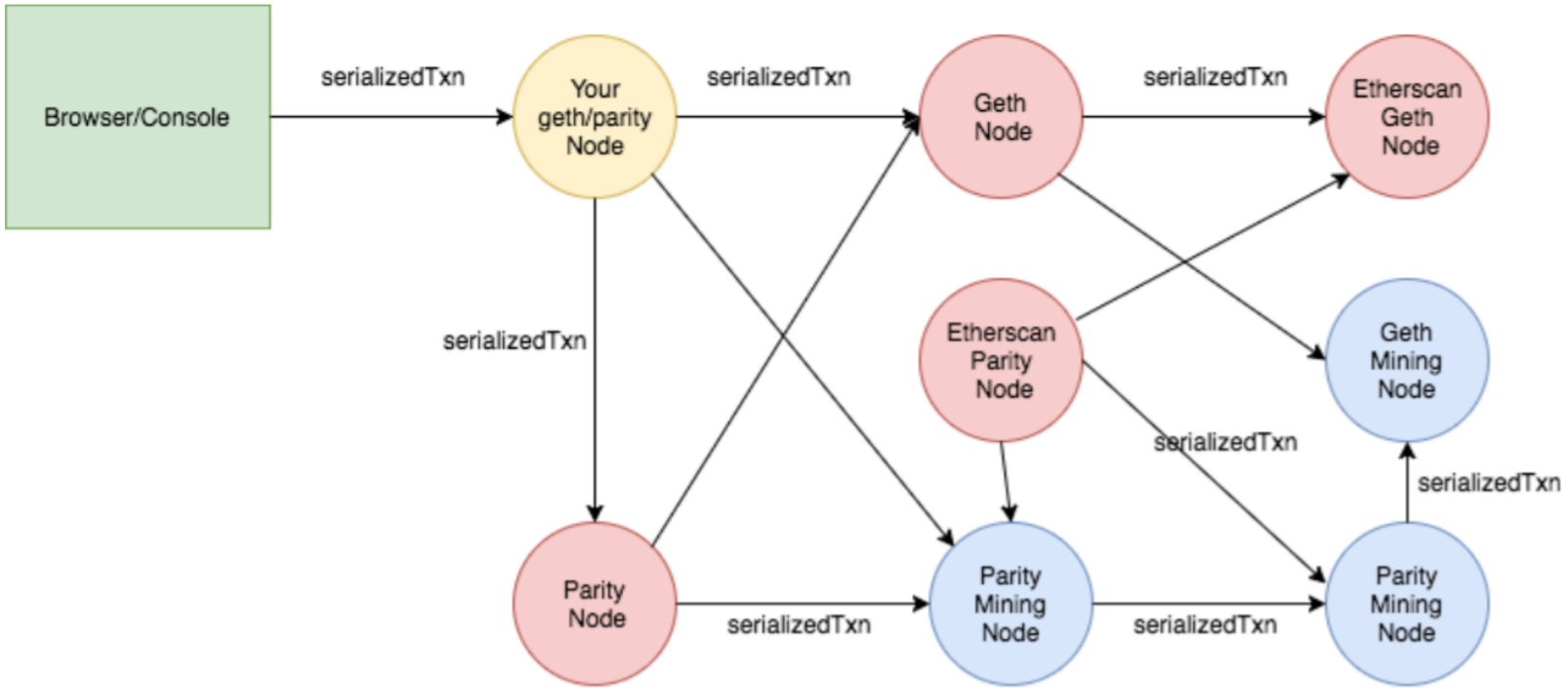
```
txnCount = web3.eth.getTransactionCount(web3.eth.accounts[0])
var rawTxn = {
    nonce: web3.toHex(txnCount),
    gasPrice: web3.toHex(100000000000),
    gasLimit: web3.toHex(140000),
    to: '0x633296baebc20f33ac2e1c1b105d7cd1f6a0718b',
    value: web3.toHex(0),
    data:
'0xcc9ab24952616d6100000000000000000000000000000000000000000000000000
0000000'
};
```

- Se firma y se serializa:

```
const privateKey =
Buffer.from('e331b6d69882b4ab4ea581s88e0b6s4039a3de5967d88dfdcffdd22
70c0fd109', 'hex')

const txn = new EthereumTx(rawTxn)
txn.sign(privateKey)
const serializedTxn = txn.serialize()
```

- Se valida en el nodo local.
- Se difunde la transacción por la red:



- Nodo minero incluye la transacción en un bloque y difunde el bloque por la red.
- Los nodos reciben el bloque y sincronizan su cadena.
  - Ejecutan las transacciones del nuevo bloque.

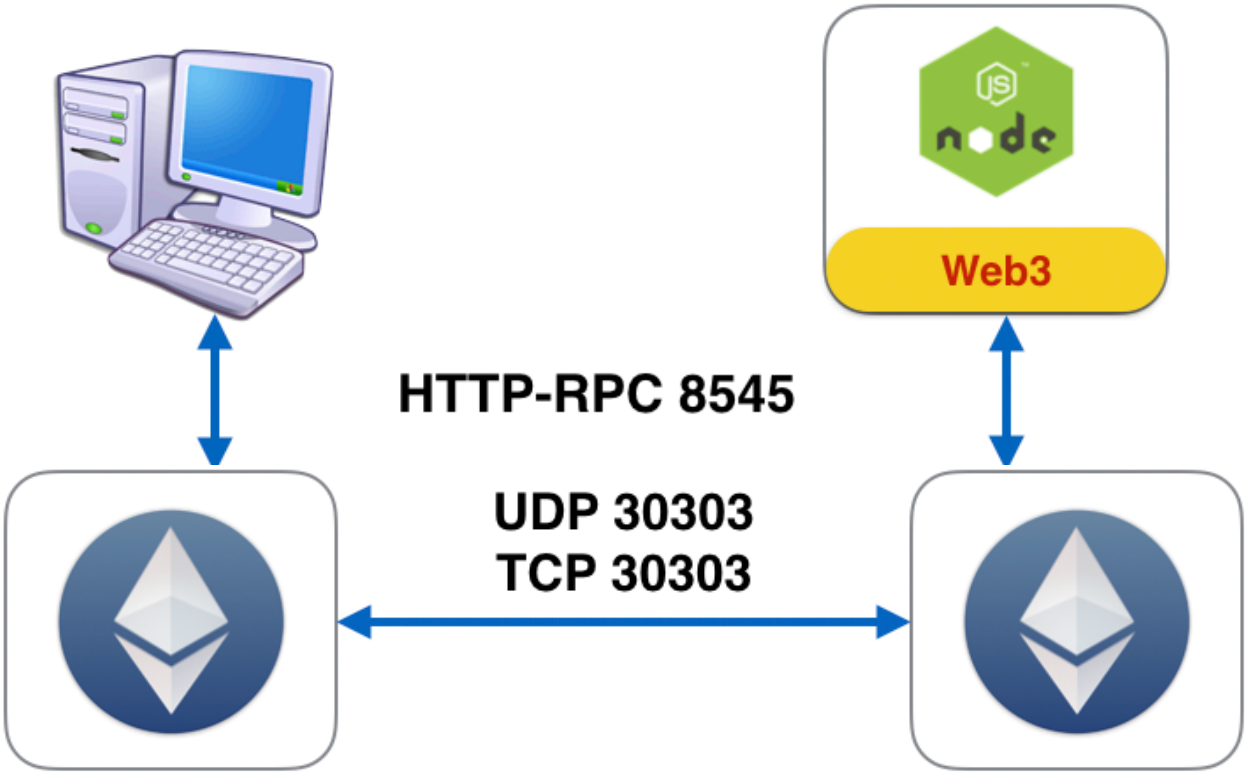
Coste de una Transacción

- Transacción
- Gas
- Precio del Gas
- Límite de Gas
- Gas usado
- Minería, fees (cuota)

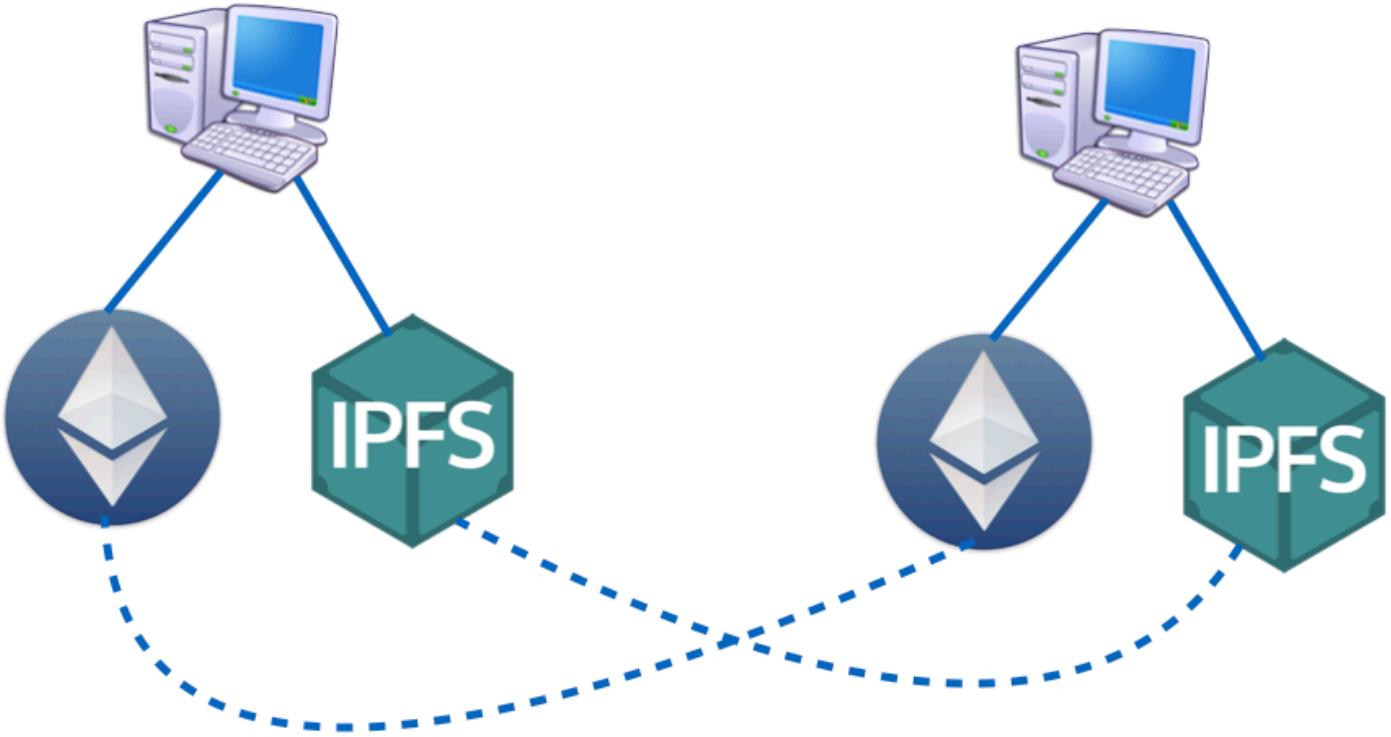
Dos Perspectivas

- Nivel Bajo: *(tripas)*
  - **Funcionamiento interno de la red blockchain**.
    - Protocolos, descubrimiento de nodos, consenso, minería, estructura de la cadena de bloques, algoritmos internos, ...
- Nivel Alto: *(dapps)*
  - **Desarrollo de Aplicaciones y Servicios sobre la red blockchain**.
    - Hay que desarrollar de los contratos inteligentes que se despliegan en la EVM.
      - La red se ve como un único ordenador en el que se despliegan y ejecutan los contratos inteligentes.
      - Idealmente se oculta la complejidad y los detalles de la red.
    - Y sobre esto se desarrollan las aplicaciones y servicios que corren en nuestros ordenadores/móviles y que usan los contratos inteligentes.

Protocolos Nodos



Persistencia



Cosas Pendientes de Repasar

- Remix, Wallet, MetaMask, ...
- Dapps , Tokens, ICOs, ERC, ...
- Prueba de trabajo, prueba de esfuerzo, ...
- Dificultad.
- Solidity.
- Seguridad.