

OFICINA
Acelera
pyme

Cámara
Zaragoza

Blockchain en la Industria 4.0

Procesos más eficientes y seguros

28/09/2021



red.es

Cámara
de Comercio de España



Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Índice

1. ¿Qué es?
2. ¿Cómo funciona?
3. Criptomonedas
4. Contratos inteligentes
5. Estado del arte
6. Casos de uso



¿Qué es?

¿Qué no es?

BLOCKCHAIN

NO ES

BITCOIN

¿Qué es?

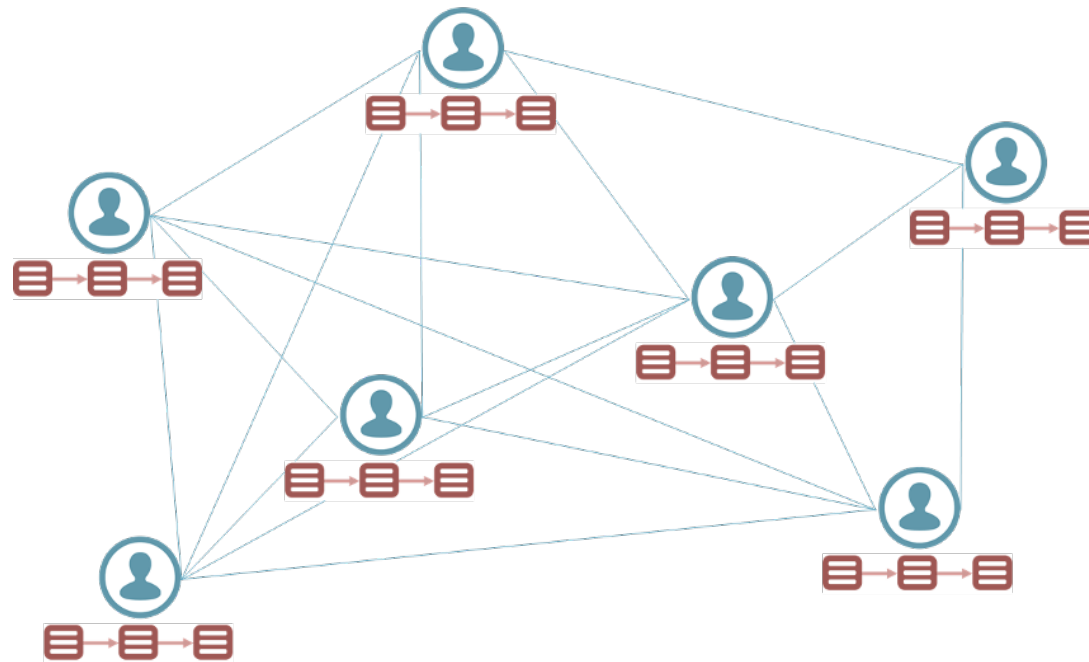
Base de datos

Pero muy especial ;-]



¿Qué es?

Distributed Ledger Technology (DLT)



¿Qué es?

Blockchain es una **tecnología** que permite que tú y yo estemos de **acuerdo** en algo, incluso cuando no hay **confianza** entre nosotros y sin necesitar de una **autoridad**

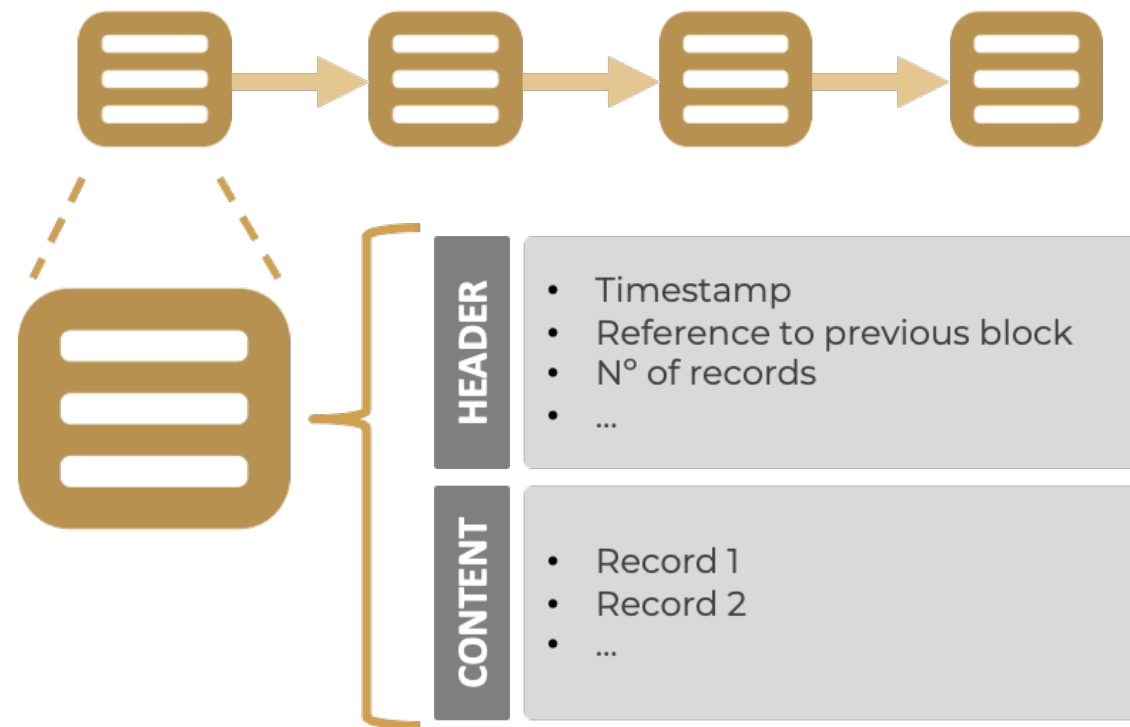
¿Qué es?

- Distribuida
- Descentralizada
- Segura
- Trazable
- Inmutable
- Confiable

¿Cómo funciona?

¿Cómo funciona?

Cadena de bloques



¿Cómo funciona?

Prueba de trabajo (PoW)

- **Protocolo de consenso basado en problema matemático**
- Toma un tiempo considerable resolverlo
- La dificultad de resolución se incrementa con el tiempo
- El minero tiene un gasto computacional de recursos (electricidad, dinero...)
- **Difícil de resolver, pero fácil de comprobar**



¿Cómo funciona?



Puede ejecutar



Puede ejecutar
Puede leer



Puede ejecutar
Puede leer
Puede escribir

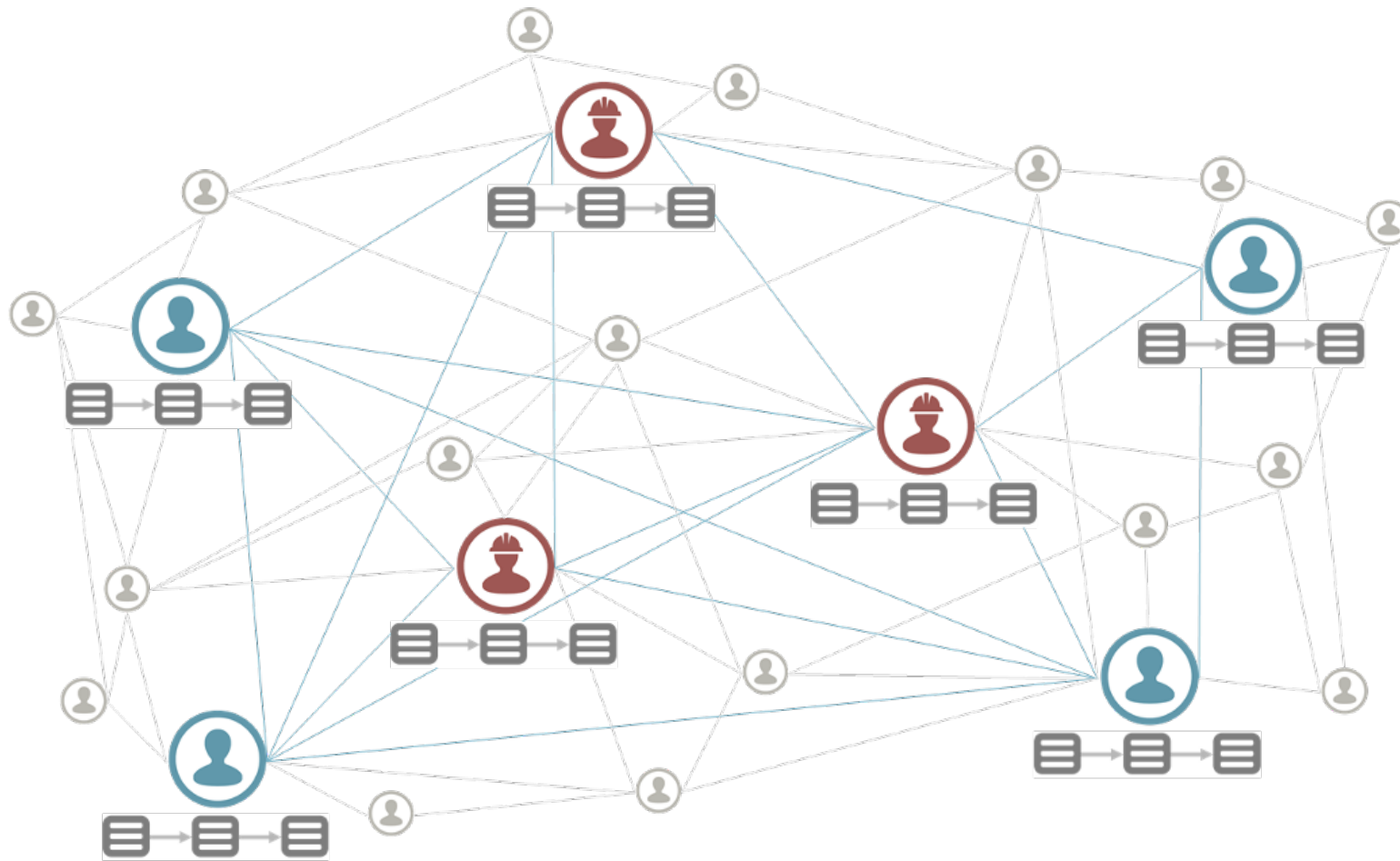
Miembros

Ejecutar = Enviar nuevos registros u operaciones

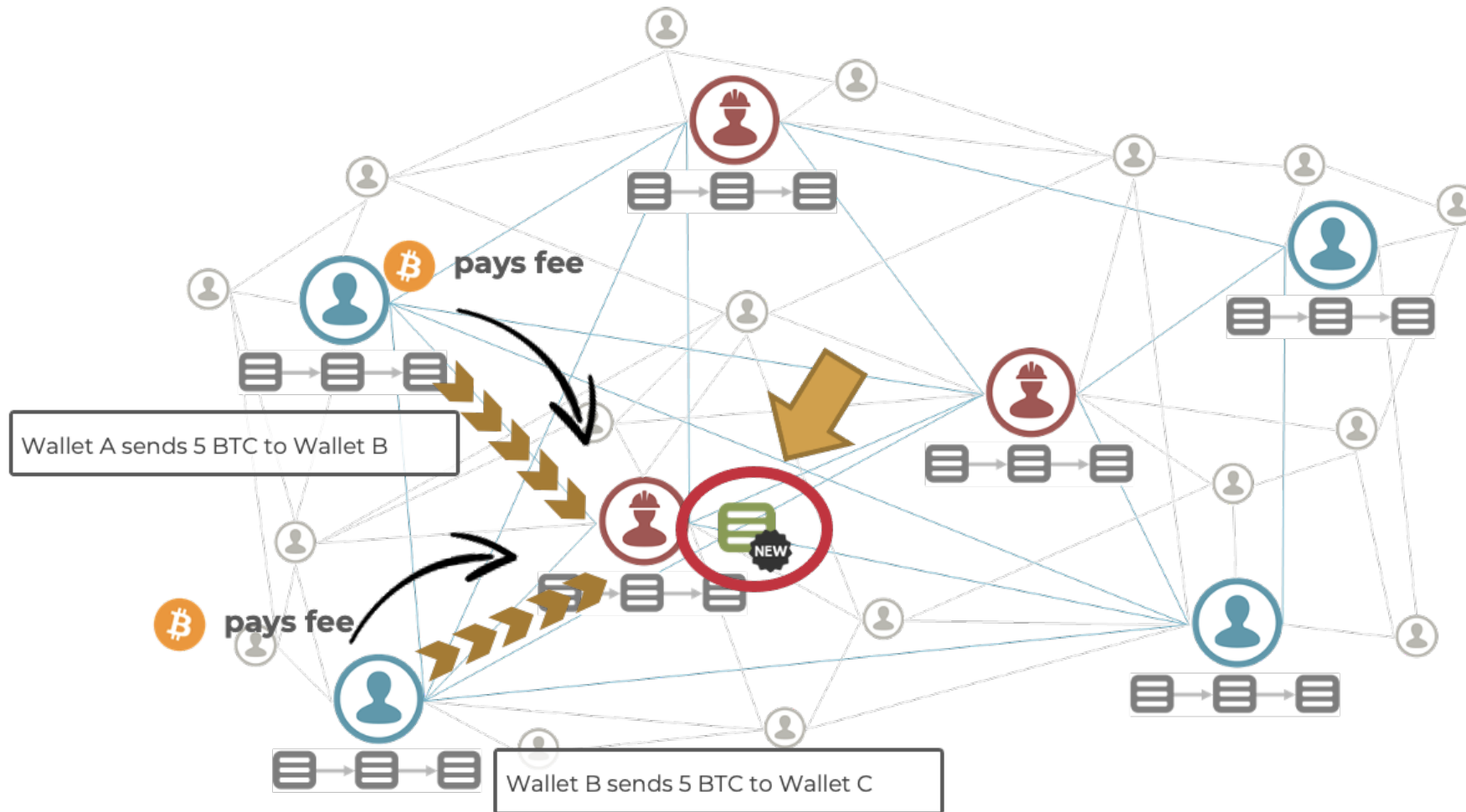


Participantes del consenso

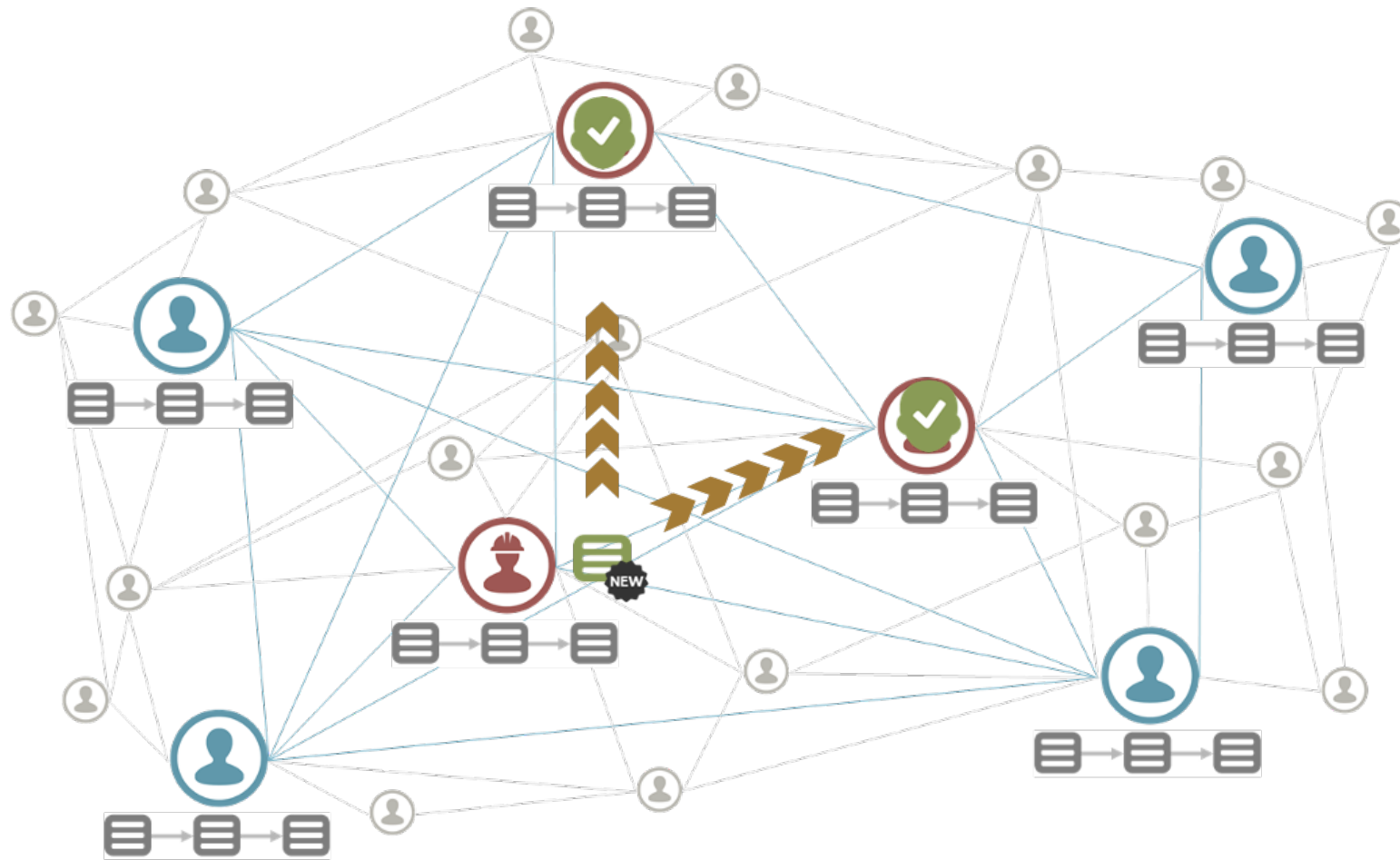
¿Cómo funciona?



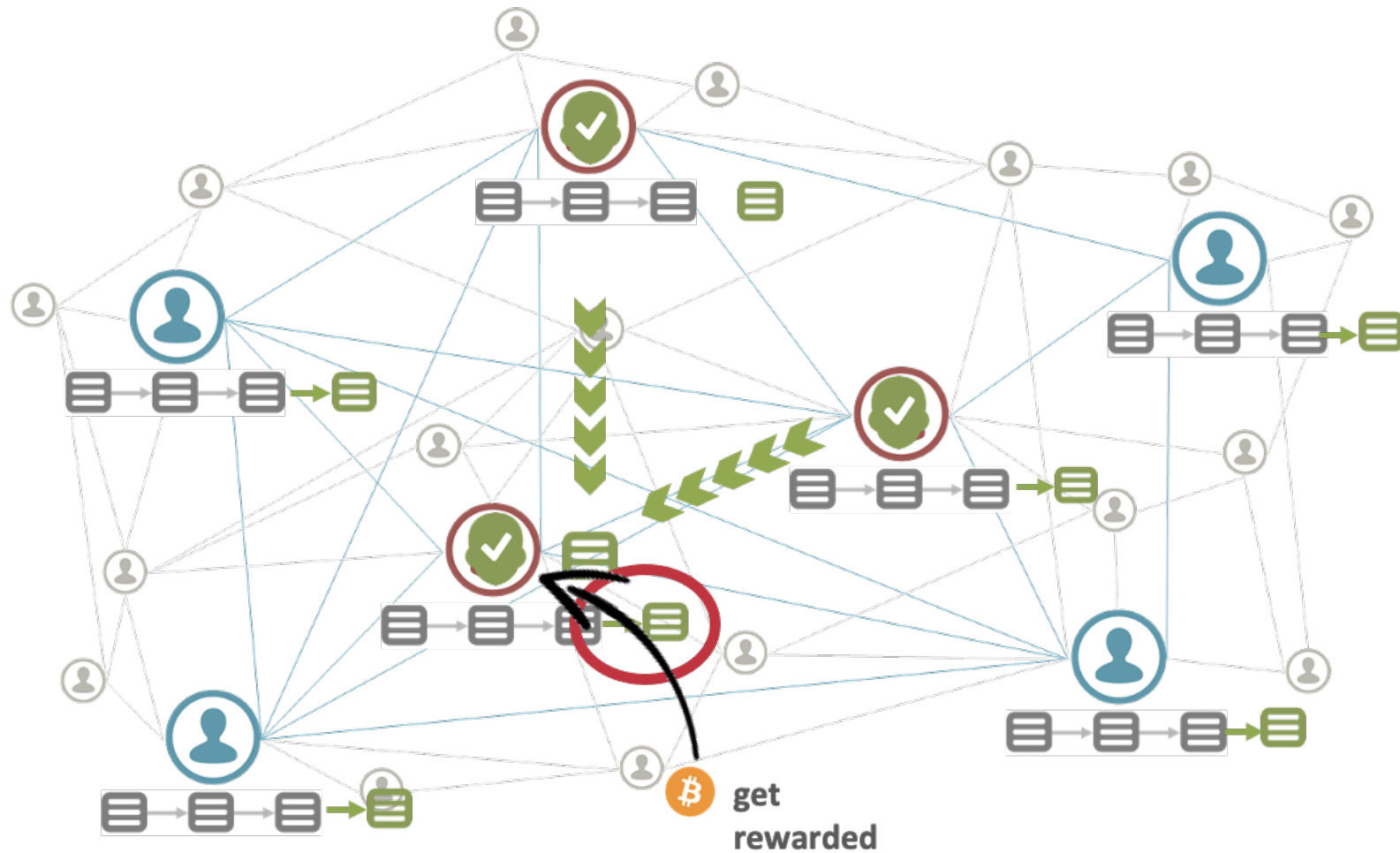
¿Cómo funciona?



¿Cómo funciona?

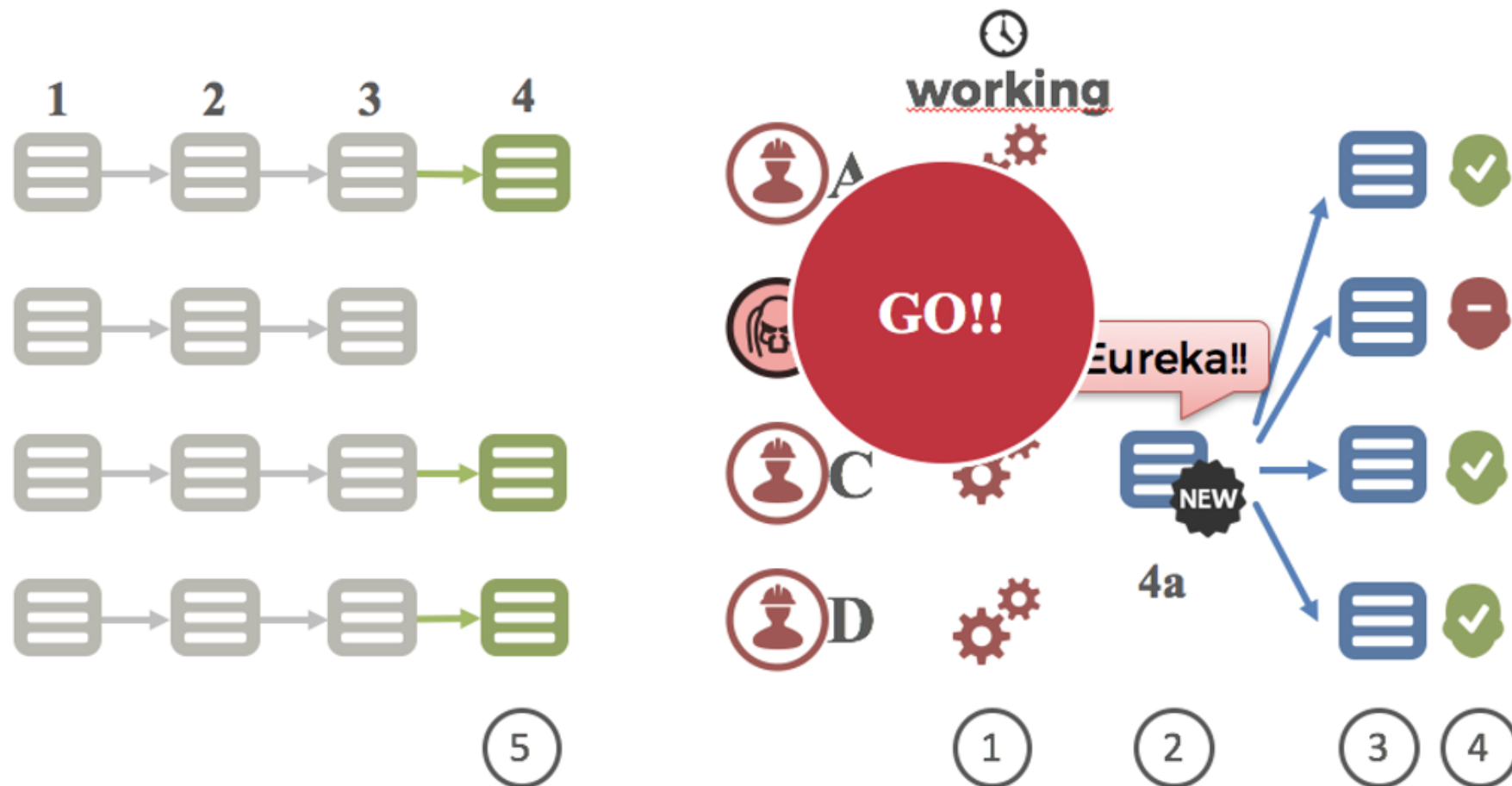


¿Cómo funciona?



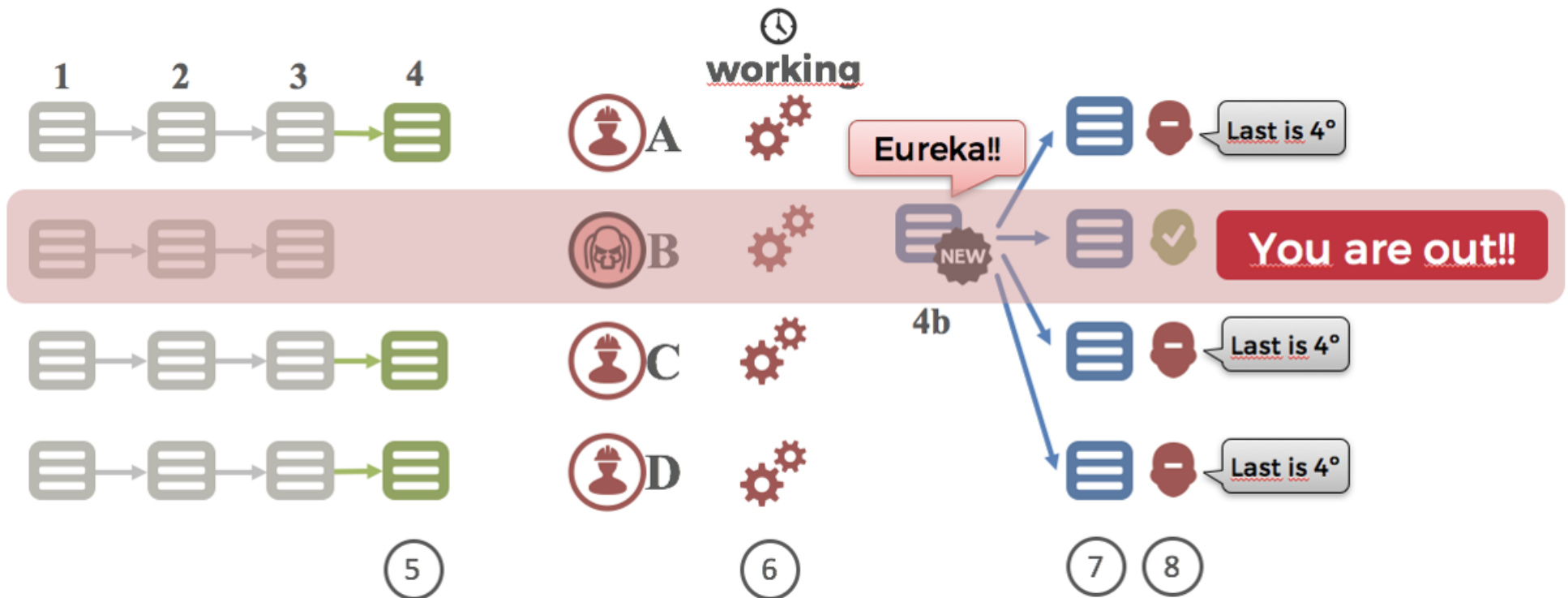
¿Cómo funciona?

Miembros honestos



¿Cómo funciona?

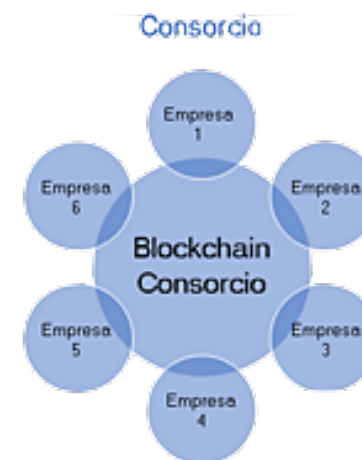
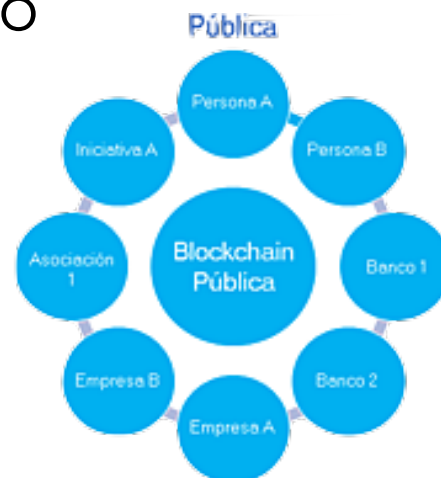
Miembros deshonestos



¿Cómo funciona?

Tipos de Acceso

- Público
- Privado
- Permisionado



Criptomonedas

Criptomonedas

Bitcoin

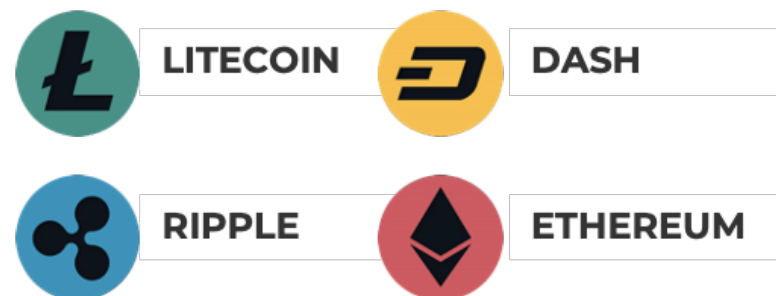
- Satoshi Nakamoto
- Creada en 2008
- Pagos entre iguales P2P
- Sin autoridades de terceros



Criptomonedas

AltCoins

- Litecoin -> Procesamiento rápido de transacciones
- Ripple -> Intercambio de dinero entre bancos
- Dash -> Centrada en la velocidad y el anonimato
- Ethereum -> Contratos inteligentes



Criptomonedas

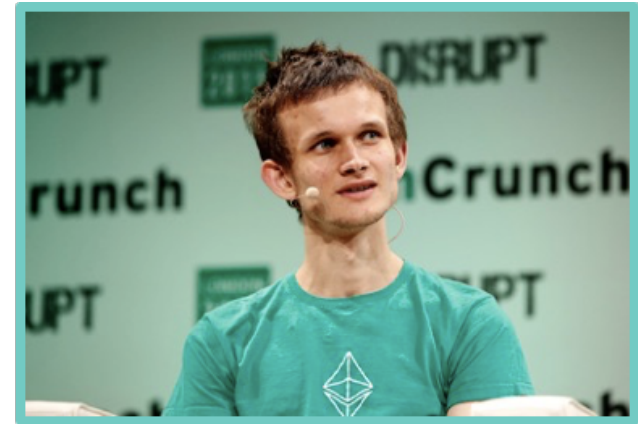
Parámetros

| Attribute | Value |
|----------------------------------|--------------------------|
| Name | Zcash |
| Launch Date | 28/10/16 |
| Main purpose | Currency |
| Currency code | ZEC |
| Maximum coins | 21 million |
| Block time | 10 minutes |
| Consensus facilitation algorithm | Proof of Work (equihash) |
| Difficulty adjustment algorithm | DigiShield V3 (modified) |
| Mining hardware | CPU, GPU |
| Difficulty adjustment period | 1 block |

Criptomonedas

Ethereum

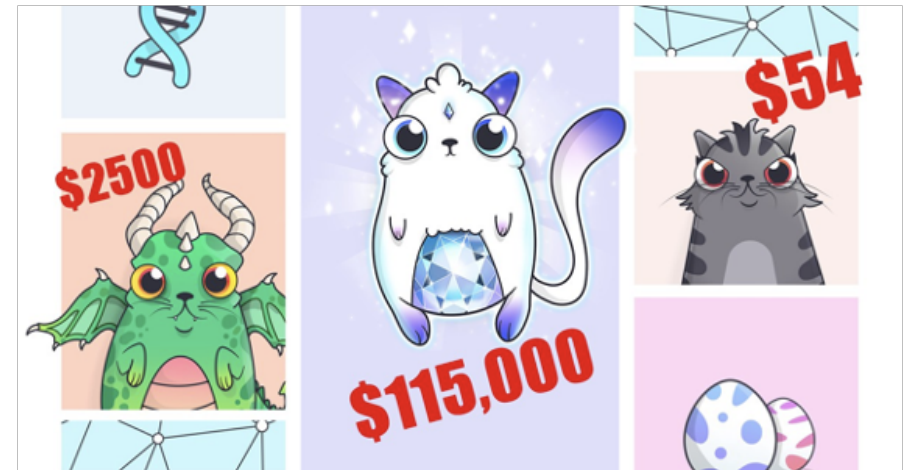
- Vitalik Buterin
- Creada en 2014
- No es una criptomoneda (ether) si no toda una **plataforma blockchain**
- **Contratos inteligentes**



Criptomonedas

Cryptokitties

- **Non Fungible Tokens (NFT)**
- **Únicos**
- ERC-721
- \$\$\$



Contratos inteligentes

Contratos inteligentes

Smart contracts

- **Piezas de código incrustadas en la cadena de bloques (ERC-20)**
- Se ejecutan de manera autónoma cuando las condiciones de entrada se cumplen
- Auditable sin la necesidad de que terceros interfieran en el proceso
- Ofrece un nuevo **ecosistema lleno de posibilidades**



Contratos inteligentes

Flujo automatizado



Contratos inteligentes

Contrato codificado

```
mapping (bytes32 => uint8) public voterCount;
mapping (bytes32 => bytes32) public voterCandidate;
mapping (bytes32 => bool) public HasVoterVoted;

bytes32[] public candidateList;

function Voting(bytes32[] _candidateList, bytes32 _hashFile, bool _isInfinite) {
    candidateList = _candidateList;
    hashFile = _hashFile;
    fechaFinVotacion = now + 86400;
    isInfinite = _isInfinite;
    votationEnded = false;
}

function setFechaFinVotacion(uint _fechaFinVotacion) {
    fechaFinVotacion = _fechaFinVotacion;
}

function getFechaFinVotacion() public view returns (uint) {
    return fechaFinVotacion;
}

function getIsInfinite() public view returns (bool) {
    return isInfinite;
}

function getCandidates() public view returns (bytes32[]) {
    return candidateList;
}

// This function returns the total votes a candidate has received so far
function totalVotesFor(bytes32 candidate) view public returns (uint8) {
    require(validCandidate(candidate));
    return voterCount[candidate];
}

// This function returns the total votes a candidate has received so far
function getVotedCandidate(bytes32 candidate) view public returns (bytes32) {
    require(validCandidate(candidate));
    return voterCandidate[candidate];
}

// This function increments the vote count for the specified candidate. This
// is equivalent to casting a vote
function voteForCandidate(bytes32 voter, bytes32 candidate) public {
    require(validCandidate(candidate));
    require(votationEnded == false);
    if (validVoter(voter))
    {
        voterCandidate[candidate] = voter;
        HasVoterVoted[voter] = true;
        voterCount[candidate] += 1;
    }
}
```

Contratos inteligentes

Explorador de contratos

The screenshot shows a web interface for a blockchain explorer. On the left is a dark sidebar with navigation options: 'LATEST BLOCKS', 'LATEST TRANSACTIONS', 'LATEST CONTRACTS', and 'CONTACT'. The main area has a search bar at the top with the text 'Search for Block, Account or Transaction' and a 'status: UP' indicator. Below the search bar, the heading 'Latest contracts' is followed by '133 contracts found'. A pagination control shows page 1 selected. A table lists the latest contracts with columns for 'TIMESTAMP', 'ADDRESS', 'CREATION TRANSACTION', and 'TRANSACTIONS'.

| TIMESTAMP | ADDRESS | CREATION TRANSACTION | TRANSACTIONS |
|---------------------|-------------------------------------|--------------------------------------|--------------|
| 2018-09-30 06:57:41 | 0xc6cf5cc31196070b77113982c7dc7... | 0x64ae7a40c5519ea665dd1669b94d... | 3 |
| 2018-09-30 05:49:44 | 0x7c84ef0d1d1a3e6108378787cd356... | 0x8f6c36c1eca7478651bdc0a265886... | 3 |
| 2018-09-30 05:41:59 | 0xb217eea09801b09cf4202cf30a5fd7... | 0xd3a69570960564faa965430f548b8... | 3 |
| 2018-09-30 05:37:44 | 0x98365ae860648b96ed378061fad40... | 0x932aa567dfc9970ff320aeaeef3b54f... | 4 |
| 2018-09-30 05:33:29 | 0xe35d090536a3d9f3530b6f1ecca14... | 0x4bff7be8c896d97234e1e0638ceec... | 1 |
| 2018-09-30 05:25:29 | 0xda7290405a5c91e1bb8519dfda747... | 0x2b077a3f84a4a5924af9a0636bec7... | 5 |
| 2018-09-30 05:22:59 | 0xaf67df08d49754935360ad265f6c3d... | 0x2079afe9882776dd9f76710a930b2f... | 2 |
| 2018-09-30 05:20:59 | 0x85ce5a1aeea4f6b178b14ced84c24... | 0x9e156c878e5825ba9d4dead46be3f... | 1 |
| 2018-09-30 05:19:14 | 0x29f4c00a659f0e900b3926e240f9b1... | 0x3c31c020cbb3ec27850203cd8585... | 1 |

Contratos inteligentes

Red Ethereum

The dashboard displays the following metrics:

- BEST BLOCK:** #6,619
- UNCLES (CURRENT / LAST 50):** 0/0
- LAST BLOCK:** 1s ago
- AVG BLOCK TIME:** 16.66s
- AVG NETWORK:** 0.1H
- ACTIVE NODES:** 3/3
- GAS PRICE:** 1 gwei
- GAS LIMIT:** 8000000 gas
- PAGE LATENCY:** 2 ms
- UPTIME:** (represented by a lightbulb icon)

Visualizations include a **BLOCK TIME** bar chart, a **DIFFICULTY** line graph, a **BLOCK PROPAGATION** graph showing a 50% threshold, and a **LAST BLOCKS MINERS** bar chart with a value of 40. A **TRANSACTIONS** and **GAS SPENDING** section is also present but currently empty.

ATTENTION! This page does not represent the entire state of the et

| Node | Client | Latency | Sync | Gas | Block | Hash | Gas Price | Gas Limit | Uptime | Age | |
|------------|---|---------|--------|-----|-------|--------|---------------------|-----------|--------|-----|---------|
| geth-dev-1 | Geth/v1.8.15-stable-89451f7c/linux-amd64/go1.10.4 | 3 ms | 0 KH/s | 2 | 0 | #6,619 | 99c20f4d...c1b001da | 13,239 | 0 | 0 | 1 s ago |
| geth-dev-0 | Geth/v1.8.15-stable-89451f7c/linux-amd64/go1.10.4 | 2 ms | 0 KH/s | 2 | 0 | #6,619 | 99c20f4d...c1b001da | 13,239 | 0 | 0 | 1 s ago |
| geth-dev-2 | Geth/v1.8.15-stable-89451f7c/linux-amd64/go1.10.4 | 30 ms | ⊗ | 2 | 0 | #6,619 | 99c20f4d...c1b001da | 13,239 | 0 | 0 | 1 s ago |

Contratos inteligentes

Beneficios

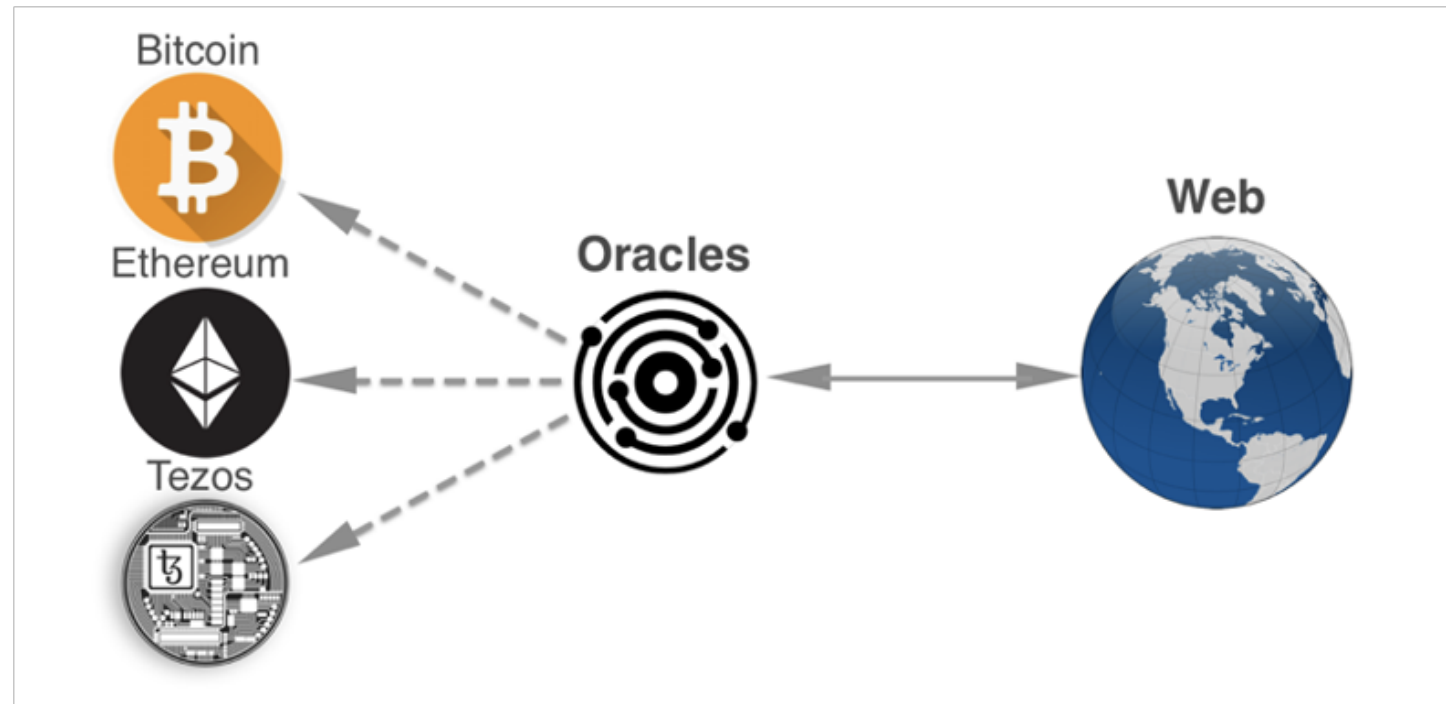
- Confianza
- Respaldo
- Seguridad
- Ahorro en costes
- Velocidad
- Precisión -> Oráculos



Contratos inteligentes

Oráculos

- MakerDAO
- Chainlink

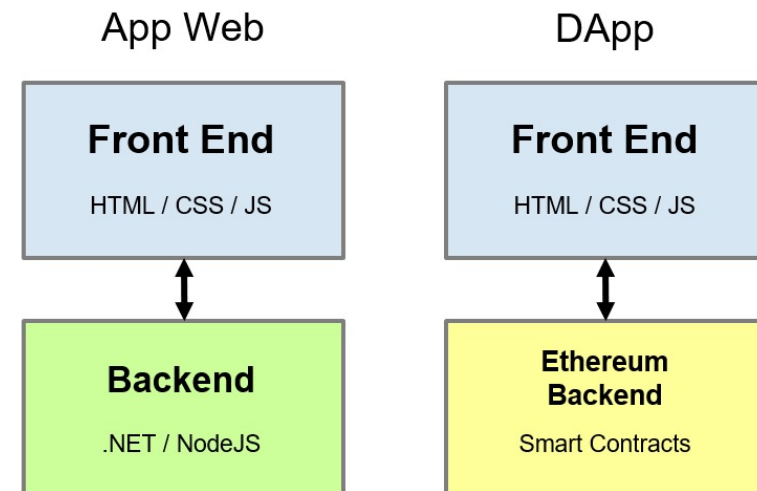


Estado del arte

Estado del arte

DApps

- Aplicaciones Descentralizadas
- Sin servidores centrales
- Blockchain para almacenar información



Estado del arte

IOT

- Velocidad
- Autonomía
- **Red IOTA**

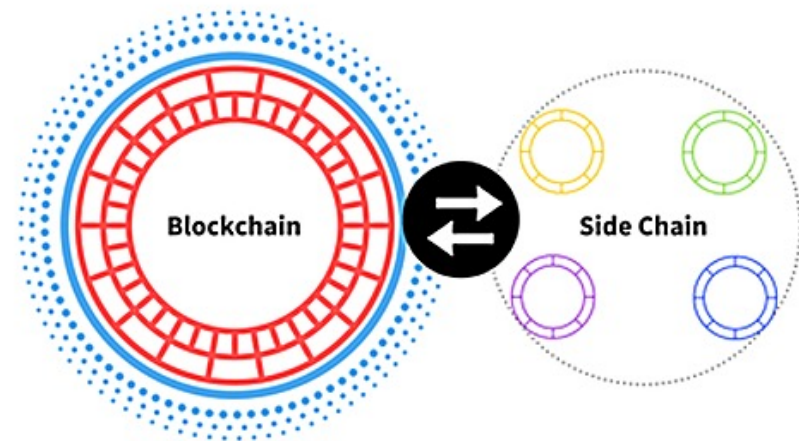
USUAL/NORMAL IOT MODEL VS BLOCKCHAIN BASE IOT MODEL

| USUAL/NORMAL IOT MODEL | BLOCKCHAIN BASE IOT MODEL |
|---|---|
| <p>Application Layer Transportation, financial, insurance and many others</p> | <p>Application Layer Transportation, financial, insurance and many others</p> |
| <p>Management Layer Data processing, analytics, security management</p> | <p>Management Layer Data processing, analytics</p> |
| <p>Network Layer LAN, WAN, PAN, Routers</p> | <p>Blockchain Layer Security, P2P (M2M) autonomous transactions, decentralization, smart contracts</p> |
| <p>Device Layer Sensors, Actuators, smart devices</p> | <p>Network Layer LAN, WAN, PAN, Routers</p> |
| <p>Physical Objects People, cars, homes, etc.</p> | <p>Device Layer Sensors, Actuators, smart devices</p> |
| | <p>Physical Objects People, cars, homes, etc.</p> |

Estado del arte

Sidechains

- Cadenas de bloques alternativas
- Complementan la cadena de bloque tradicional
- Solucionan problemas de escalabilidad: saturación, velocidad, tamaño



Estado del arte

Inter Planetary File system (IPFS)

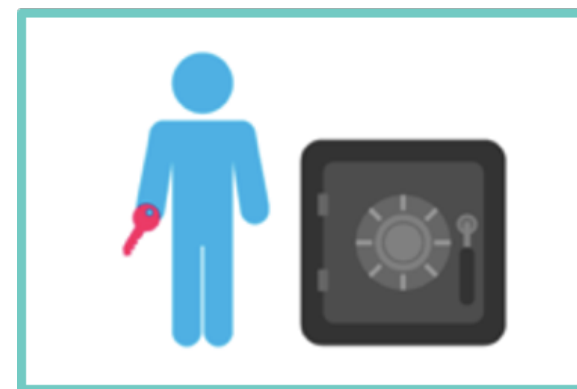
- Registrar datos de gran tamaño
- Sistema de archivos P2P
- En la cadena de bloques se guardan los enlaces y hashes de los ficheros compartidos



Estado del arte

Prueba de participación (PoS)

- Protocolo de consenso basado en el poder de adquisición del “minero” (stake)
- Mientras más criptomonedas tenga en su poder, más podrá validar
- No es necesario gastar recursos
- Se alcanza antes el consenso
- No hay recompensa de bloque, solo tasas de transacción



Estado del arte

Retos

- Tecnología nueva -> Escasez de personal cualificado
- Adopción -> Sistemas antiguos legados y costes iniciales
- Percepción pública errónea -> Bitcoin y especulación
- Teórico -> Pruebas de concepto
- **Escalabilidad -> Energía, velocidades, tamaños**
- **Consenso -> Investigación de otras pruebas de consenso**

Casos de uso

Casos de uso

Blockchain está aquí

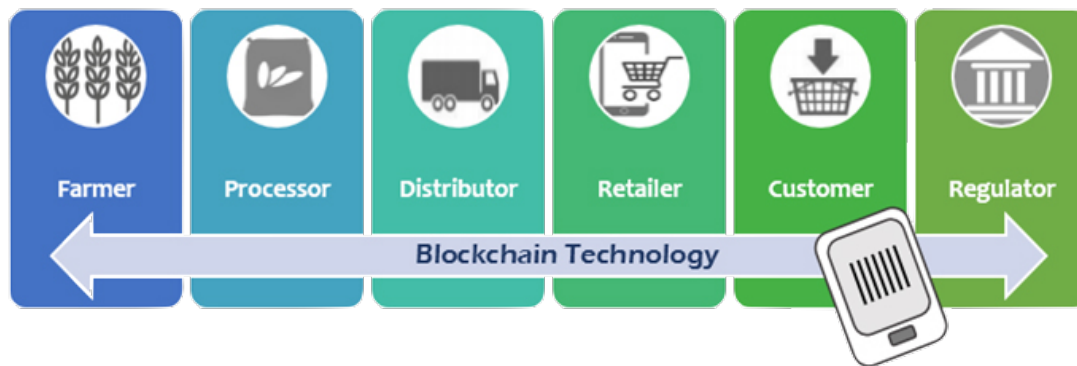
- Compartir información
- Confianza unificada
- Contratos autónomos
- Aplicable a todos los sectores



Casos de uso

Trazabilidad

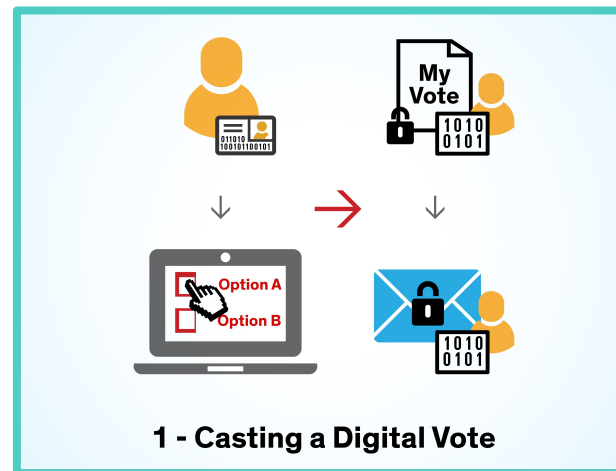
- Cadena de suministro
- + Registros en la Blockchain
- = **ripe.io**



Casos de uso

Identidad digital

- Inicio de sesión
- + ID Blockchain
- = **KeyBase**



Casos de uso

Fidelización de clientes

- Burger King
- + Criptomoneda
- = **Whopper Coin**



Casos de uso

Tokenomics

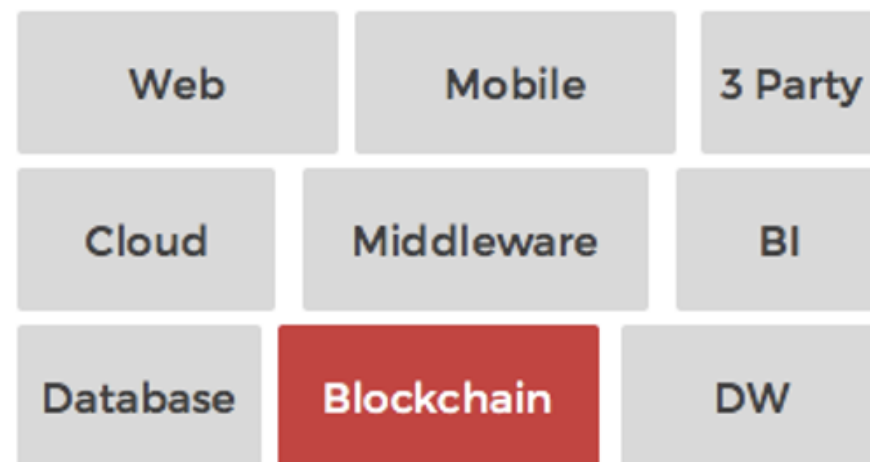
- Initial Coin Offering (ICO)
- + Criptomonedas
- = **Financiación**



Casos de uso

Herramienta general

- Cada caso de uso tiene una blockchain diferente
- Cada blockchain es distinta e independiente
- Blockchain as a Service (BaaS)



¿Tú qué vas a hacer con ella?



Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa
