OFICINA Acelera pyme

Cámara Zaragoza

Blockchain en la Industria 4.0

Procesos más eficientes y seguros

28/09/2021

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

Cámara de Comercio de España

UNIÓN EUROPEA

Fondo Europeo de Desarrollo Regional

Una manera de hacer Europa

Índice

¿Qué es?

¿Qué es?


digital
finance
money
exchange
ledger
data
financial
bitcoin
virtual
internet
transaction
cryptocurrency
crypto
contract
smart
finance
litecoin
cash
protocol
Blockchain
payments
network
node
internet
currency
coin
data
bitcoin
business
market
exchange
concept

¿Qué no es?

BLOCKCHAIN

NO ES

BITCOIN

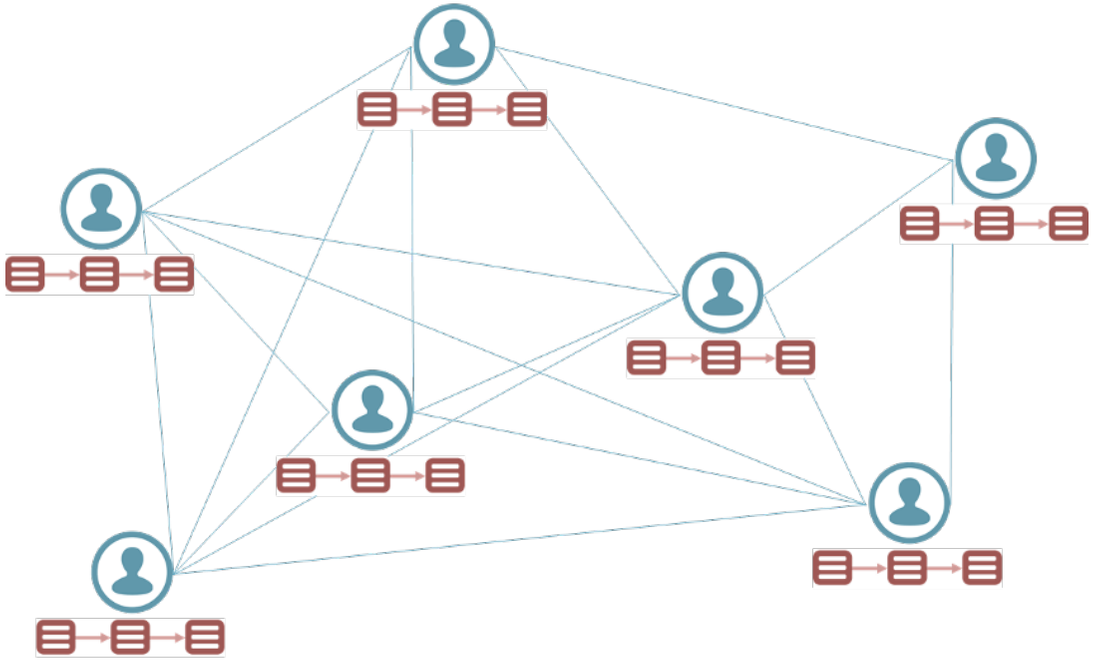
¿Qué es?

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**

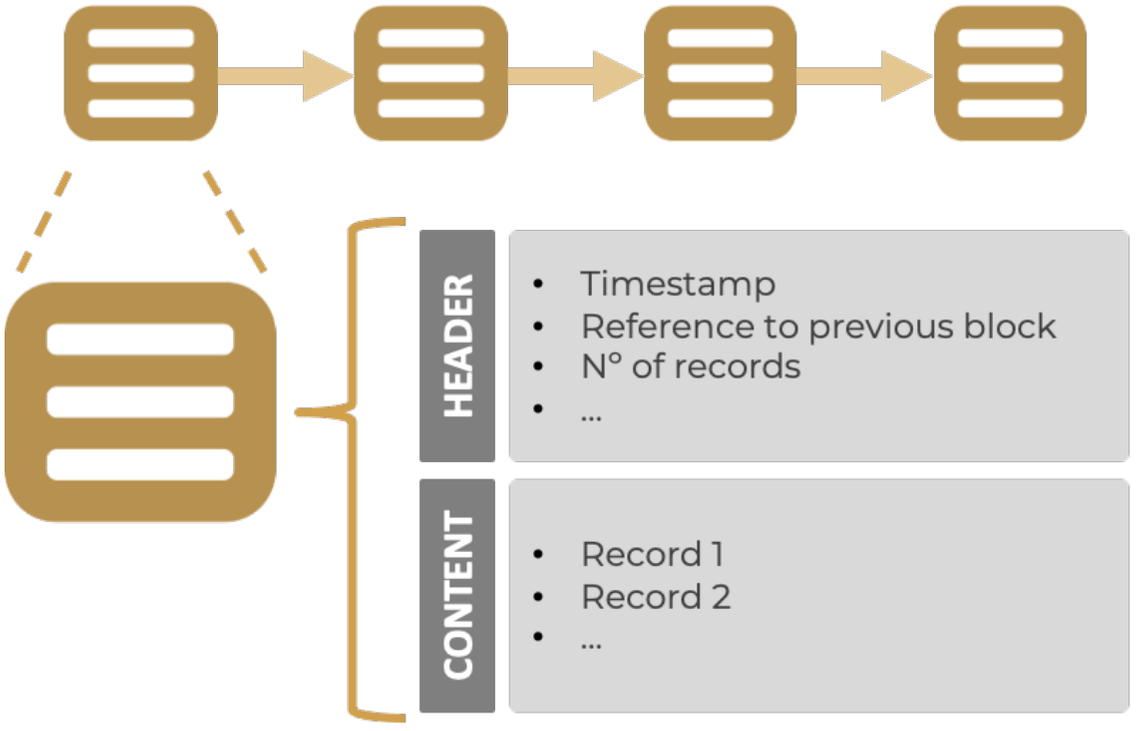
¿Qué es?

- 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?

Miembros

Puede ejecutar

Ejecutar = Enviar nuevos registros u operaciones

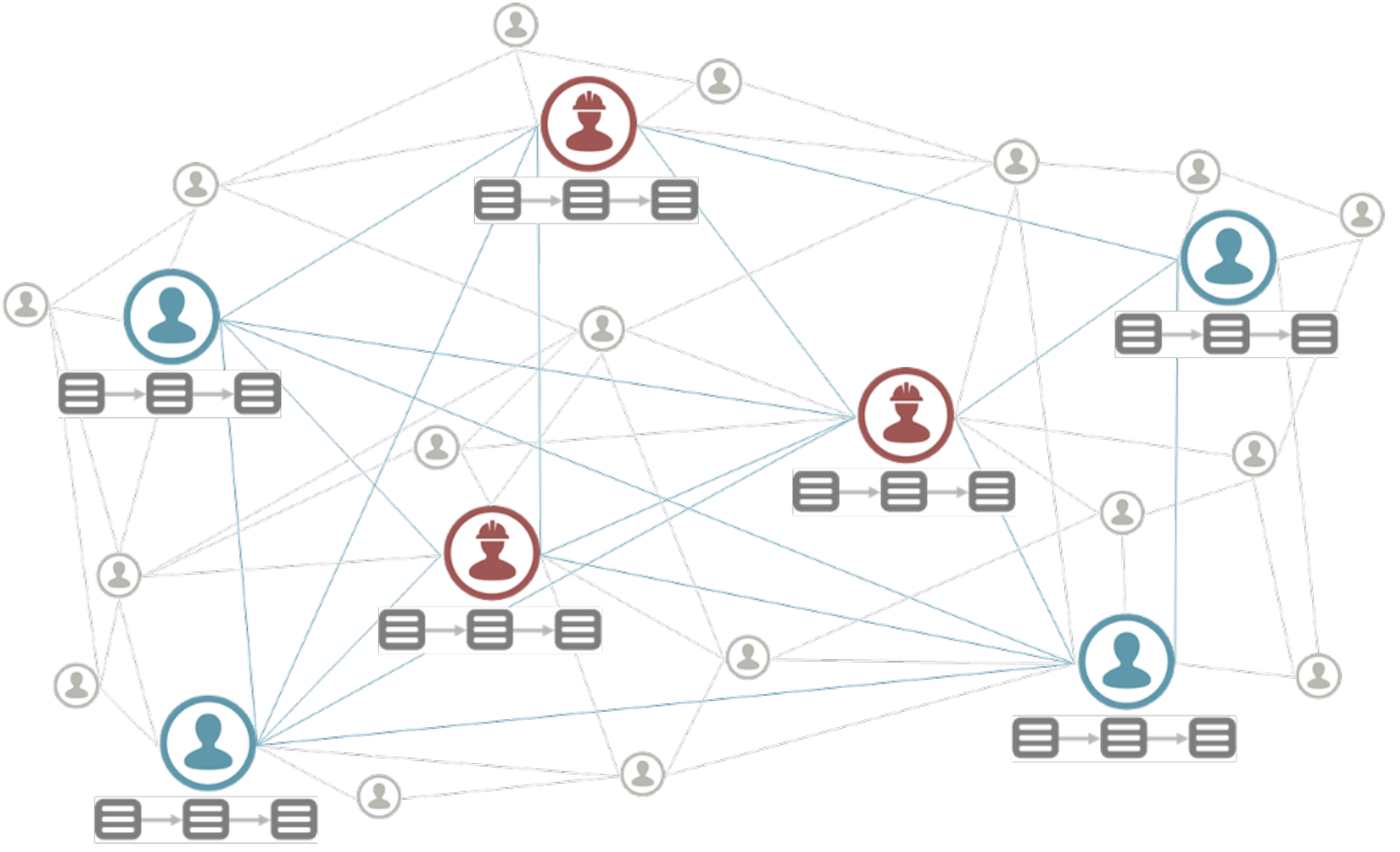
Puede ejecutar
Puede leer

Puede ejecutar
Puede leer
Puede escribir

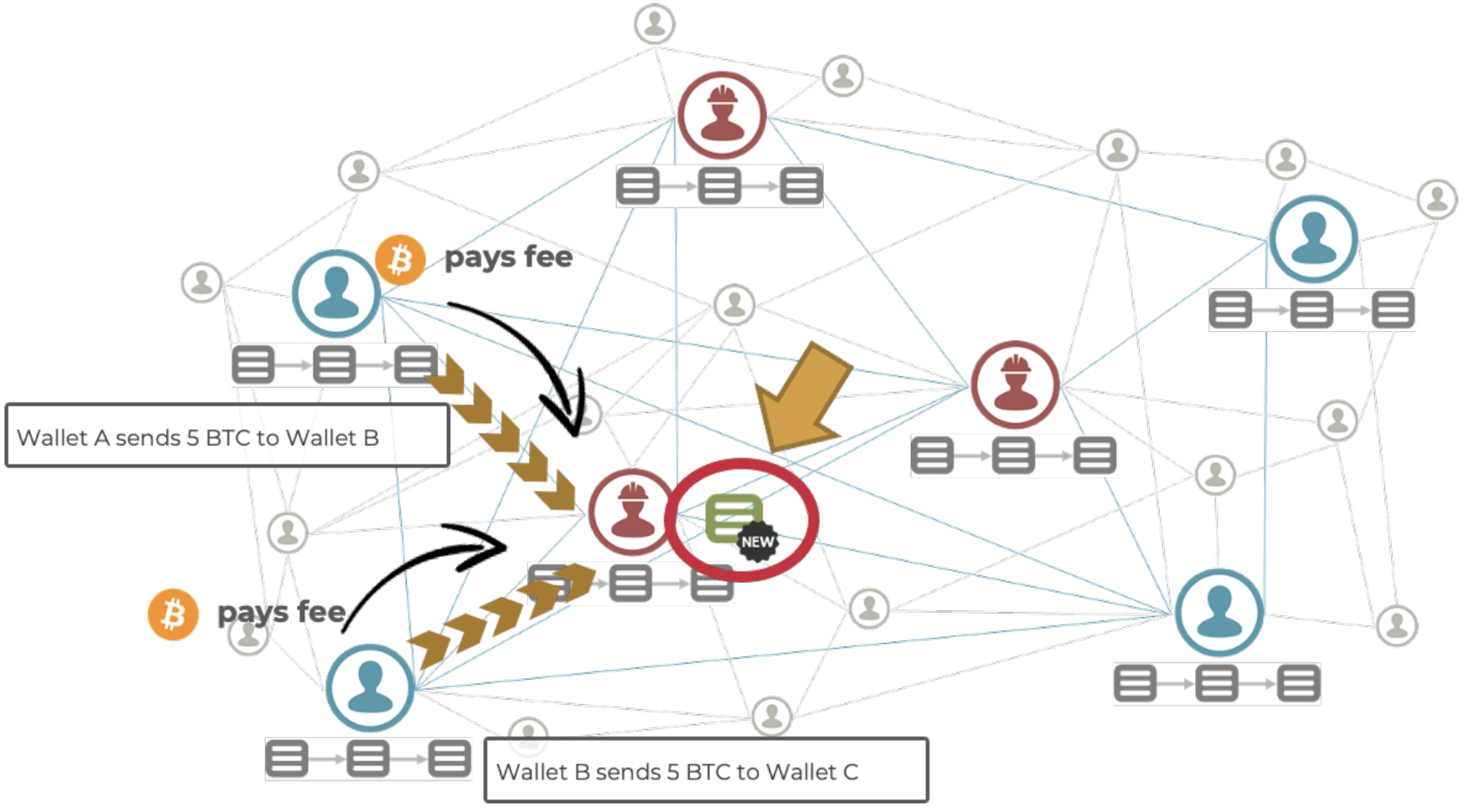
MINER

Participantes del consenso

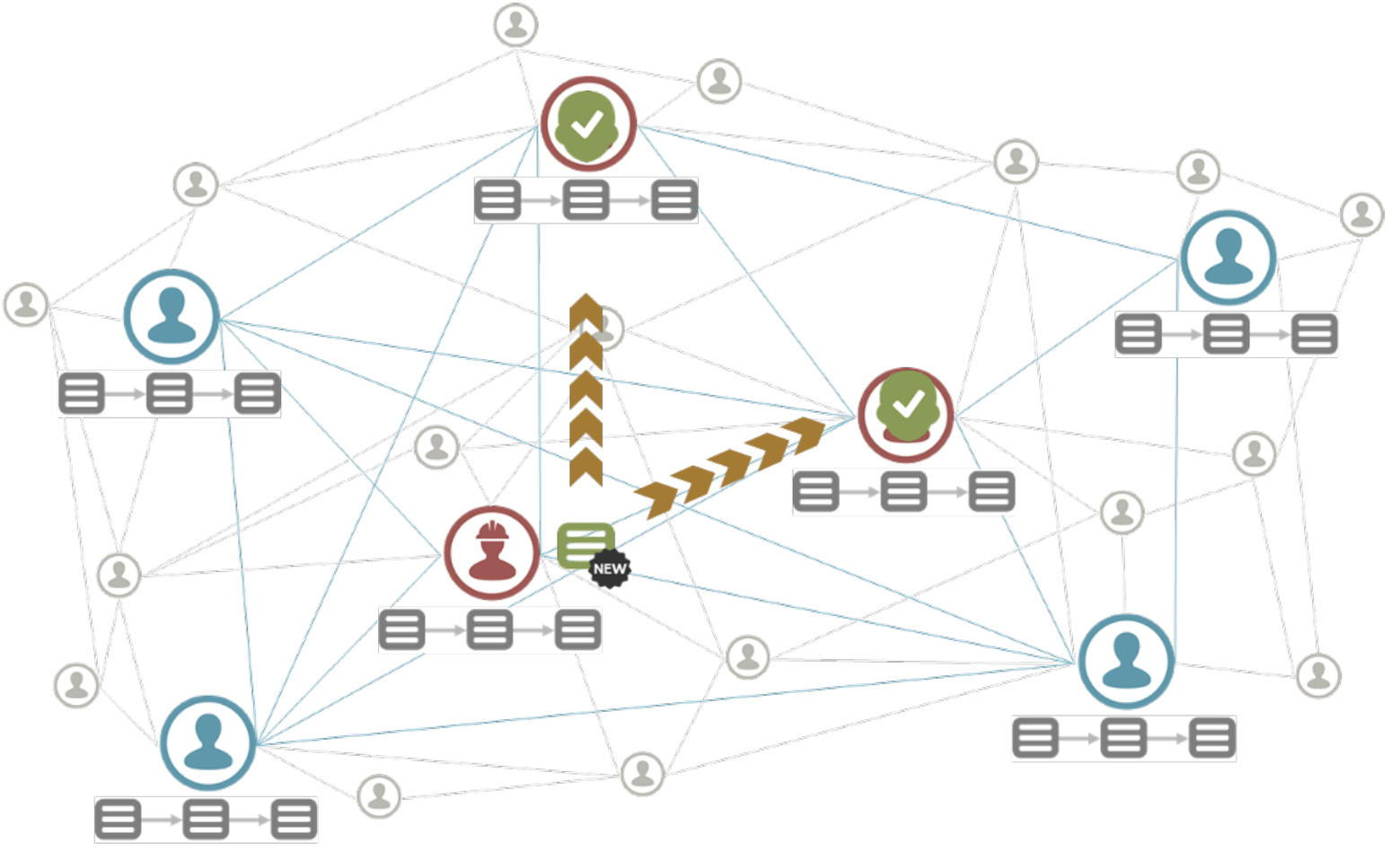
¿Cómo funciona?



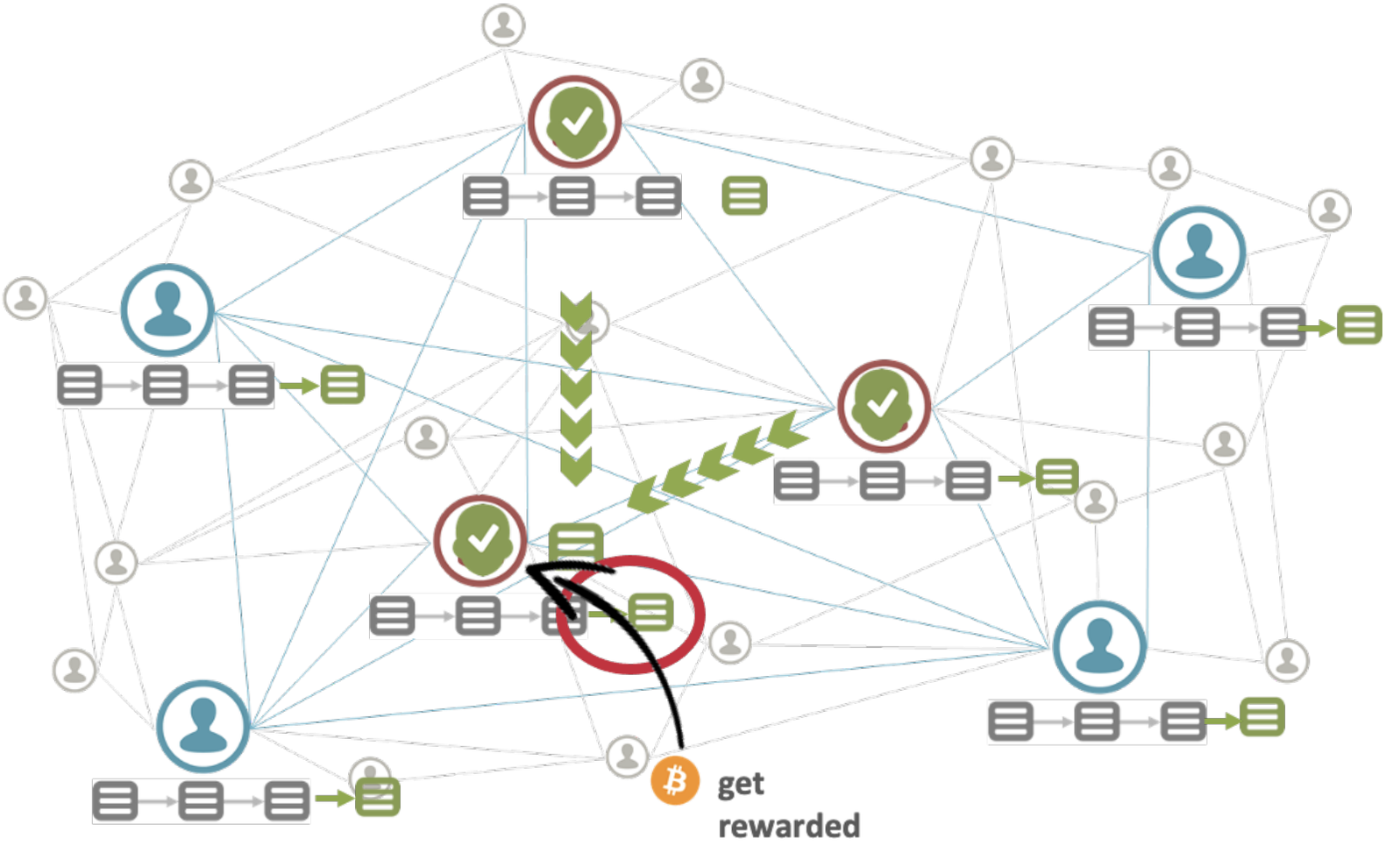
¿Cómo funciona?



¿Cómo funciona?



¿Cómo funciona?

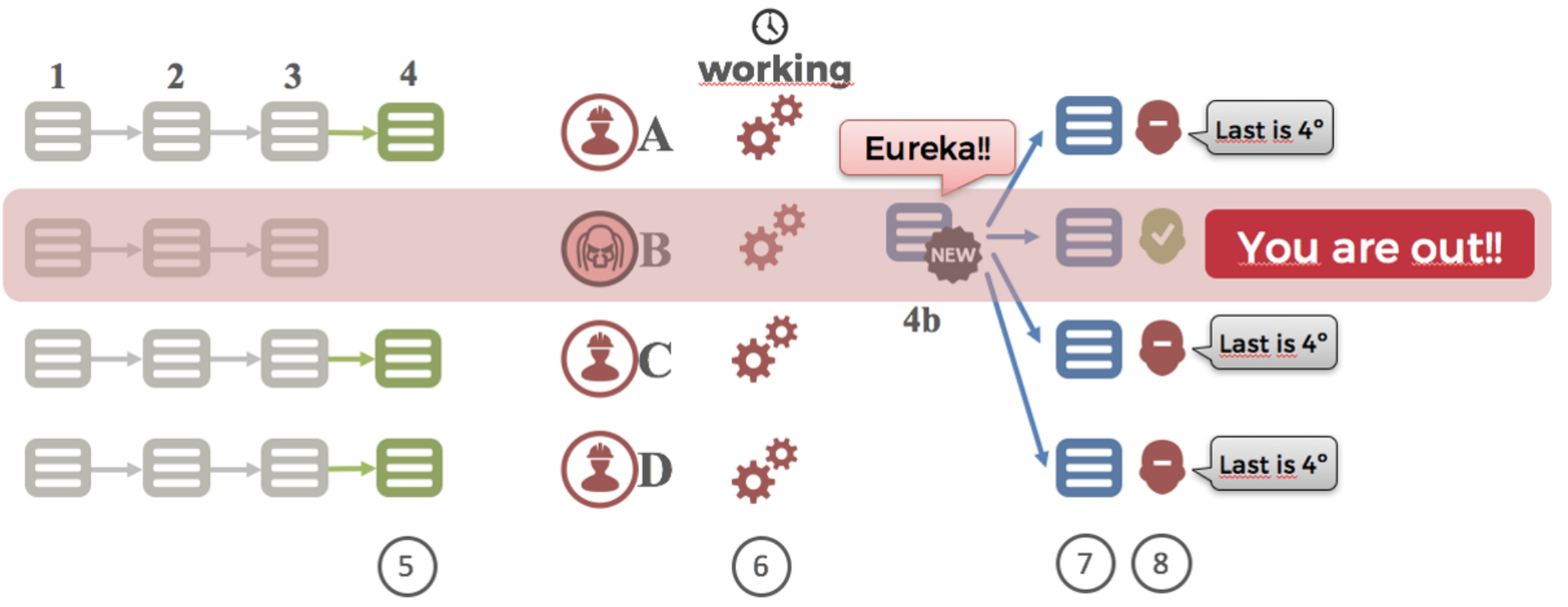


¿Cómo funciona?

Miembros honestos

¿Cómo funciona?

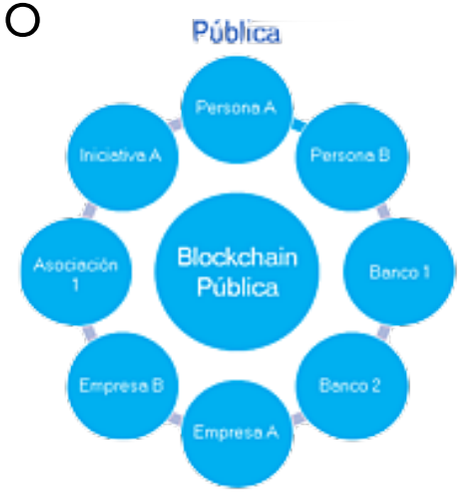
Miembros deshonestos



¿Cómo funciona?

Tipos de Acceso

- Público
- Privado
- Permisionado



Criptomonedas

Criptomonedas

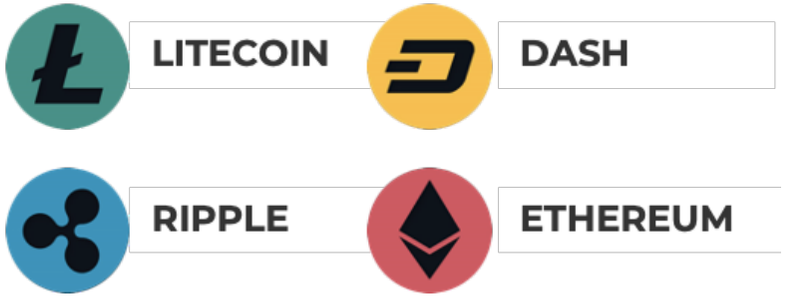
Bitcoin

- 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

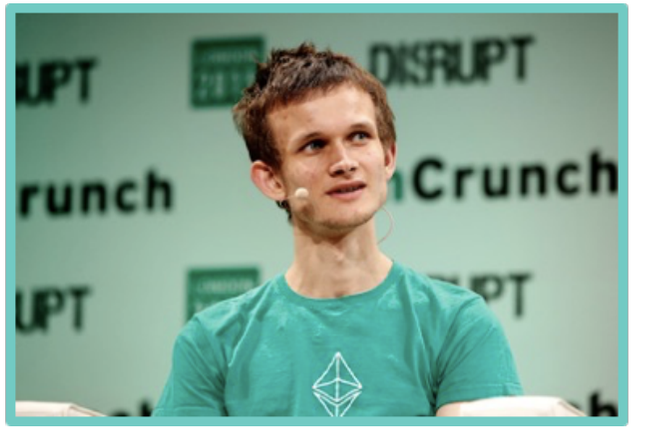
Parámetros

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

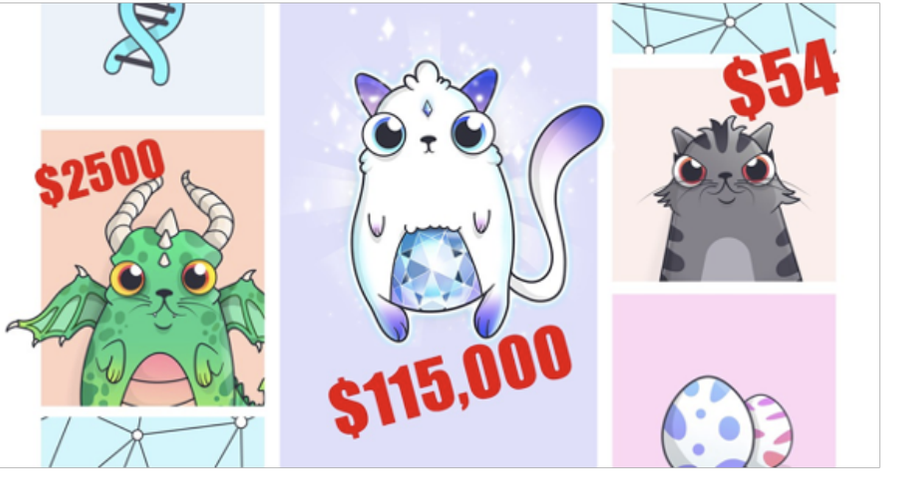
- Vitalik Buterin
- Creada en 2014
- No es una criptomoneda (ether) si no toda una **plataforma blockchain**
- **Contratos inteligentes**



Criptomonedas

Cryptokitties

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



Contratos inteligentes

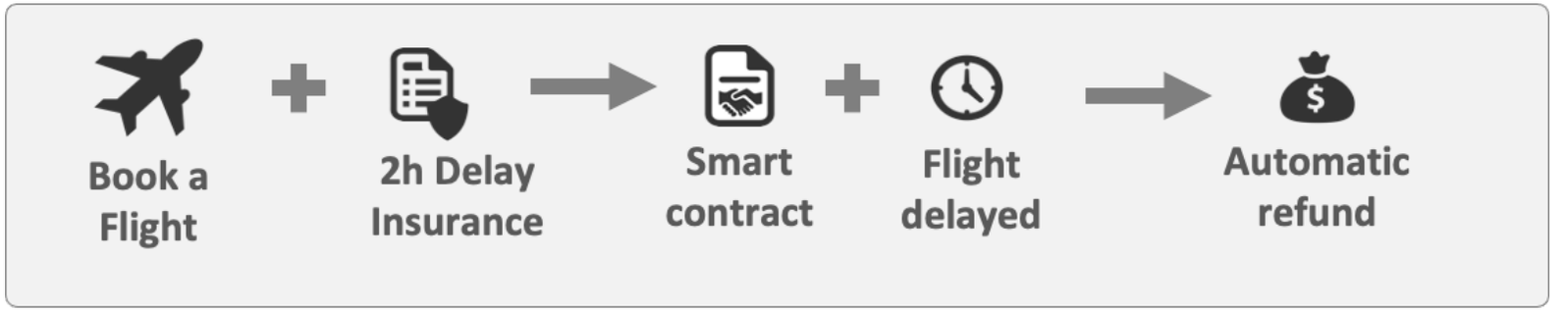
Contratos inteligentes

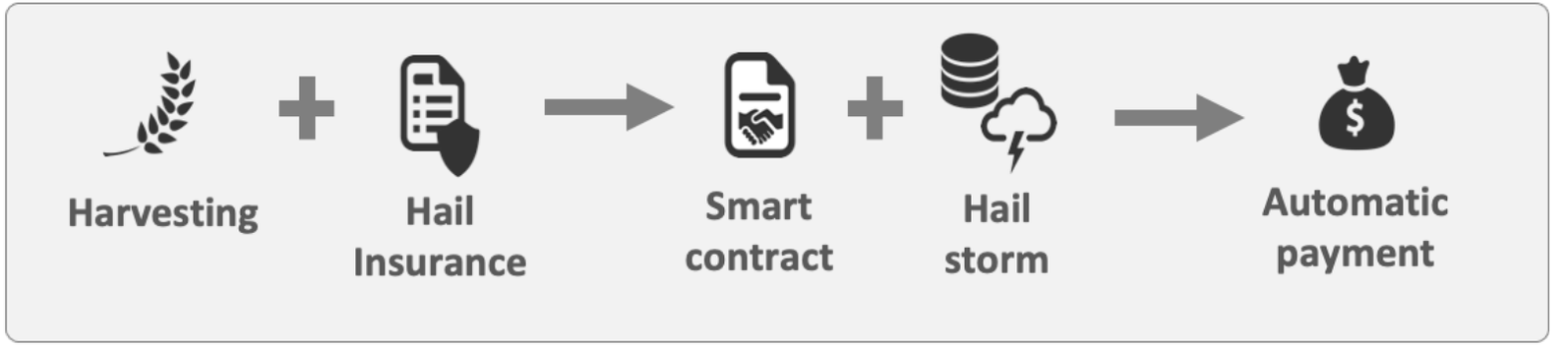
Smart contracts

- **Piezas de código incrustradas 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





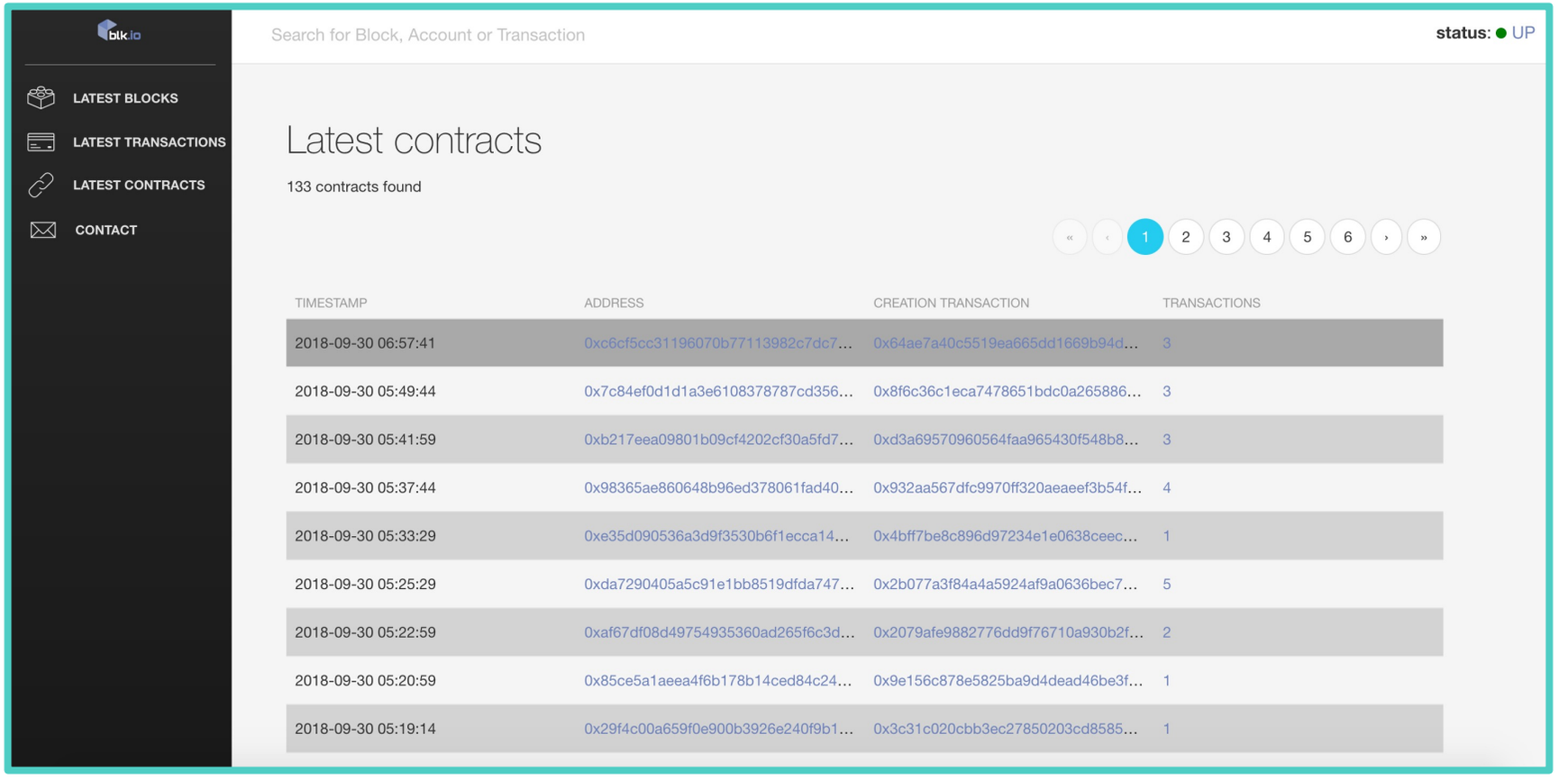
Contratos inteligentes

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



Contratos inteligentes

Red Ethereum

Contratos inteligentes

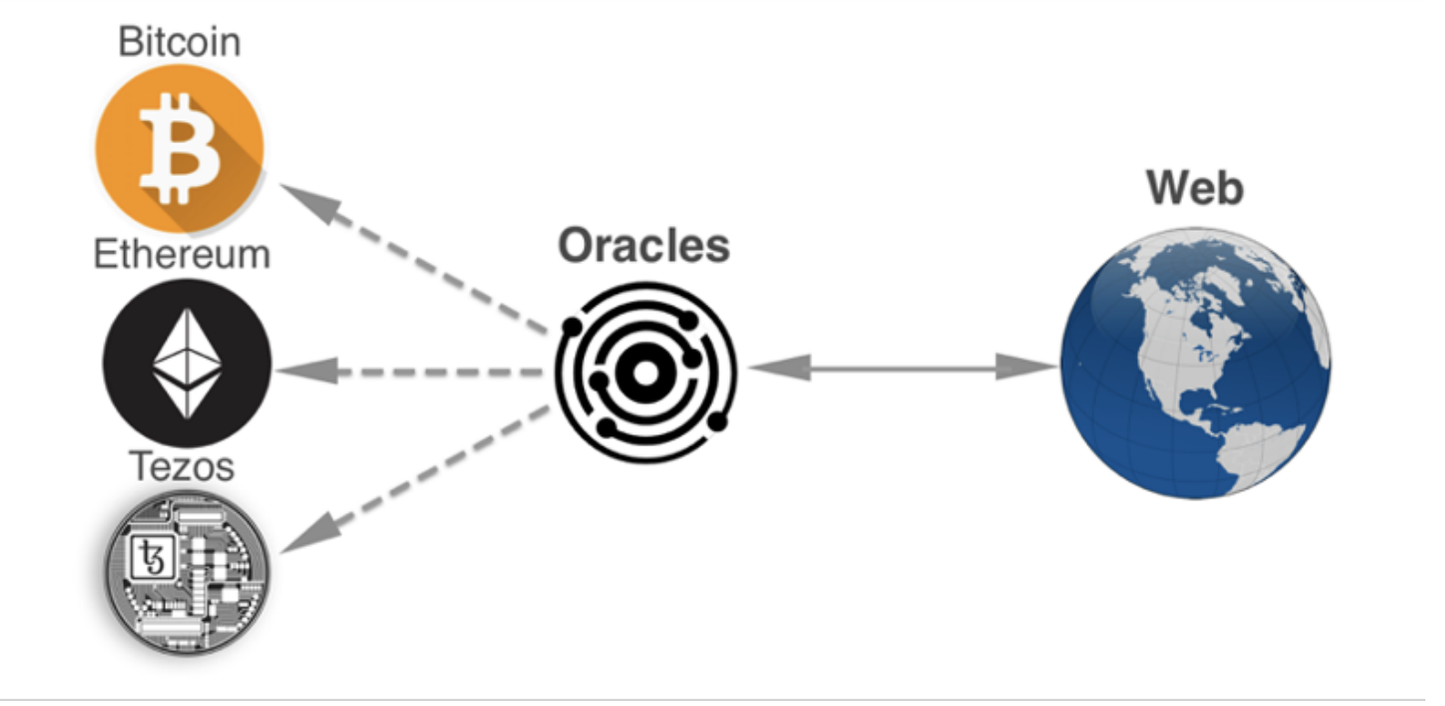
Beneficios

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

Contratos inteligentes

Oráculos

- MakerDAO
- Chainlink

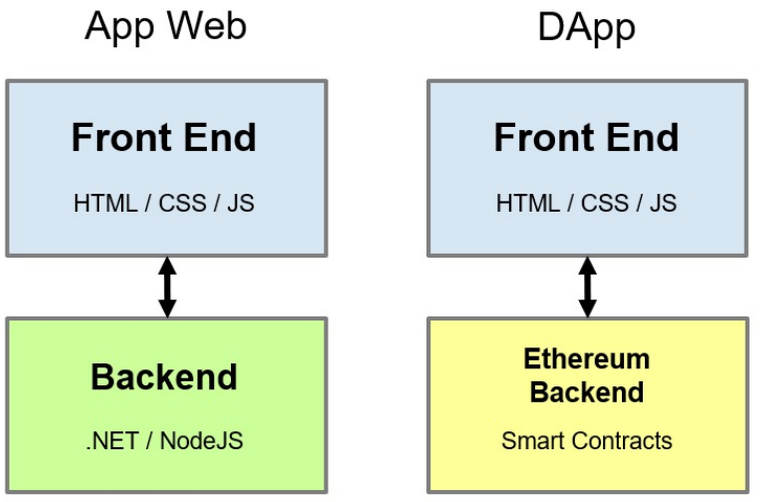


Estado del arte

Estado del arte

DApps

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



Estado del arte

- Velocidad
- Autonomía
- **Red IOTA**

IOT

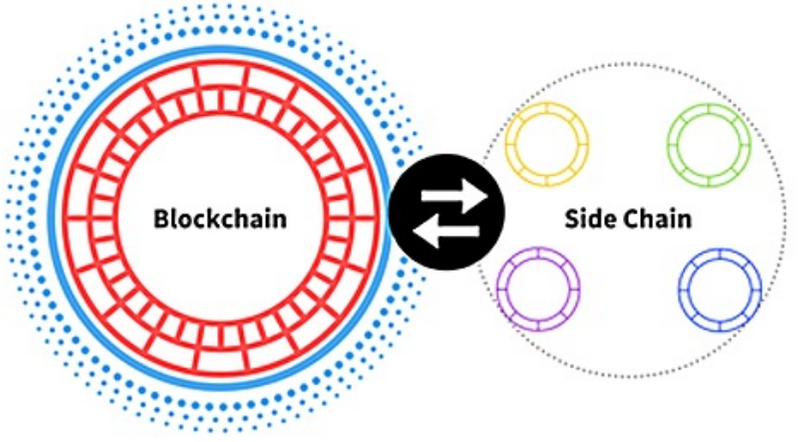
USUAL/NORMAL IOT MODEL VS BLOCKCHAIN BASE IOT MODEL

Application Layer Transportation, financial, insurance and many others	Application Layer Transportation, financial, insurance and many others
Management Layer Data processing, analytics, security management	Management Layer Data processing, analytics
Network Layer LAN, WAN, PAN, Routers	Blockchain Layer Security, P2P (M2M) autonomous transactions, decentralization, smart contracts
Device Layer Sensors, Actuators, smart devices	Network Layer LAN, WAN, PAN, Routers
Physical Objects People, cars, homes, etc.	Device Layer Sensors, Actuators, smart devices
	Physical Objects People, cars, homes, etc.

Estado del arte

Sidechains

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



Estado del arte

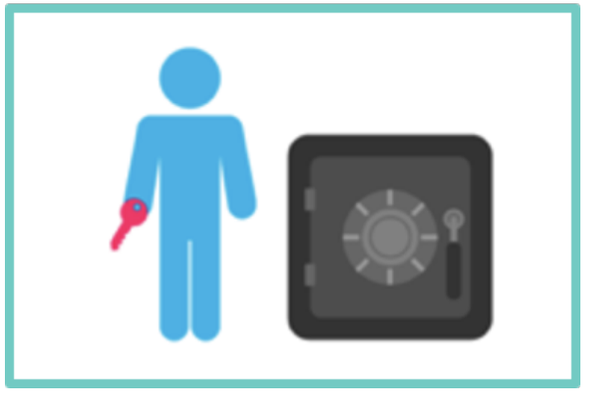
Inter Planetary File system (IPFS)

- 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 antigüos 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

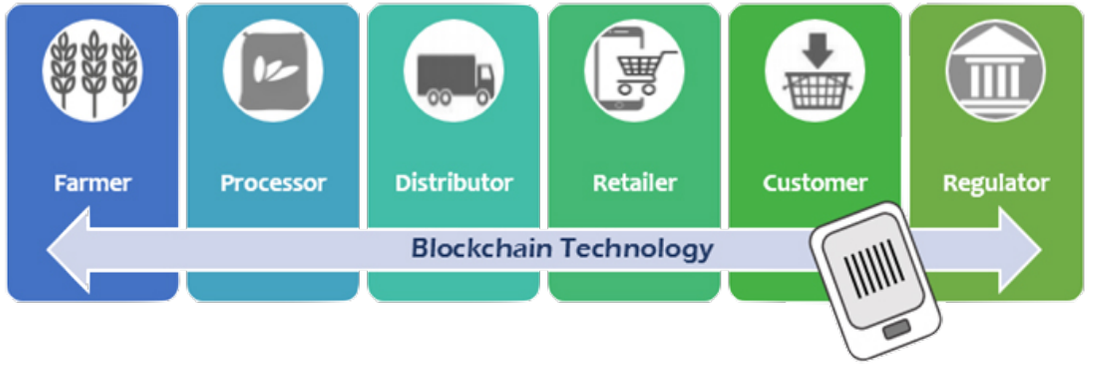
Blockchain está aquí

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

Casos de uso

Trazabilidad

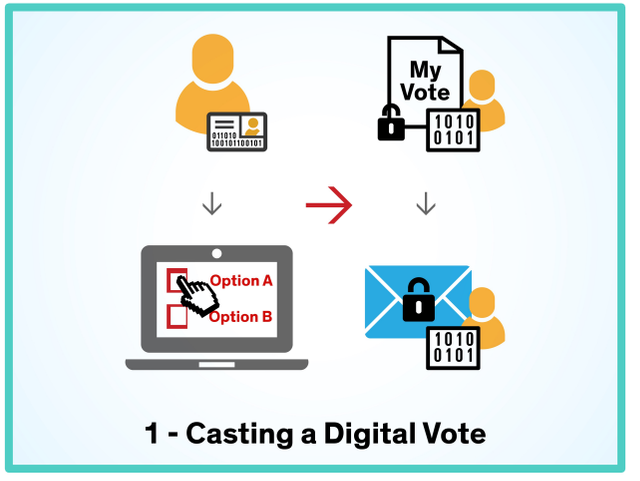
- Cadena de suministro
- + Registros en la Blockchain
- = **ripe.io**



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

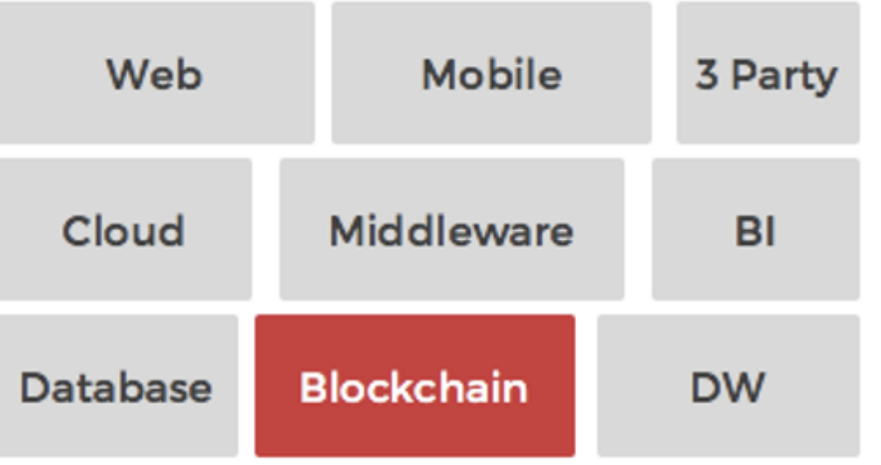
Tokenomics

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

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?

OFICINA Acelera pyme

Cámara Zaragoza

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

Cámara de Comercio de España

UNIÓN EUROPEA

Fondo Europeo de Desarrollo Regional

Una manera de hacer Europa