Universitat Oberta de Catalunya

Estudio de tecnologías Bitcoin y Blockchain

BENITO LOPEZ RODRIGUEZ
11 Junio 2018

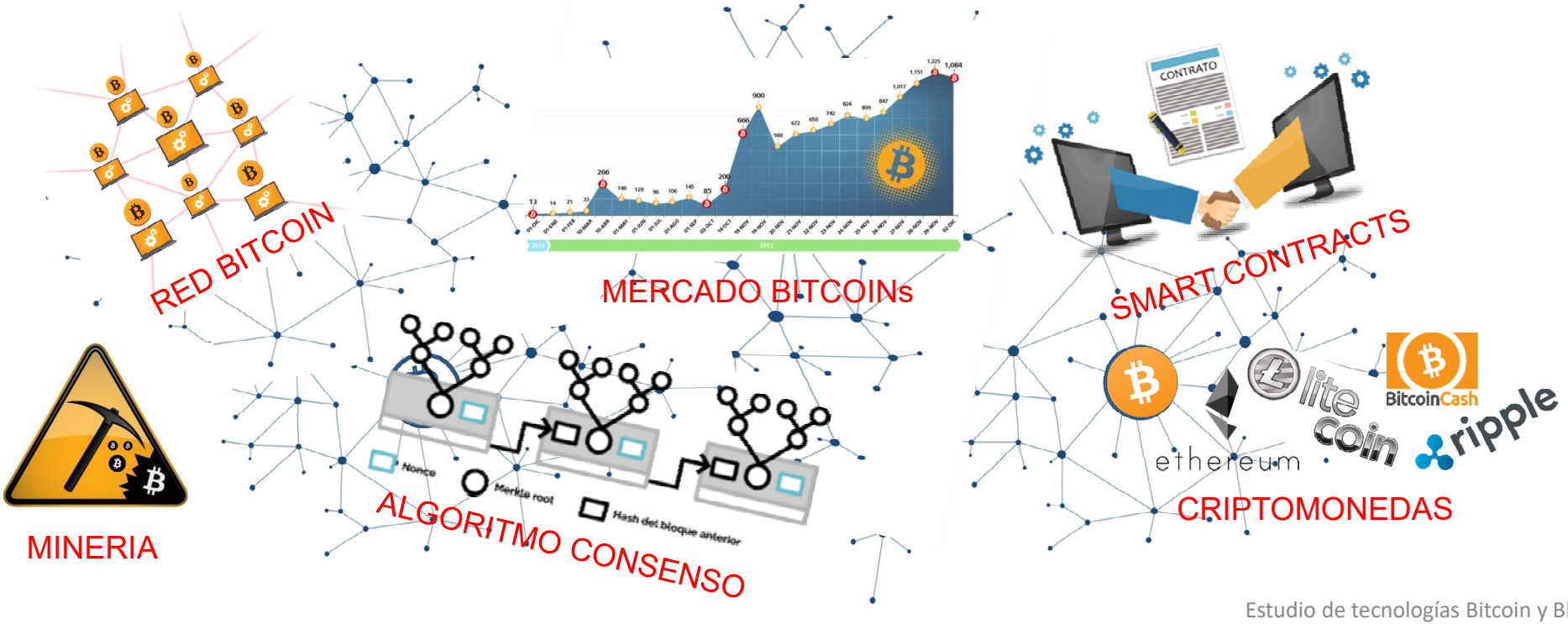
Universitat Oberta de Catalunya

AGENDA

- Objetivos.
- Bitcoin.
- Blockchain.
- Aplicativos de Blockchain.
- Otras criptodivisas.
- Conclusiones.

Objetivos

- Estudiar las tecnologías Bitcoin y Blockchain para comprender sus beneficios en aplicaciones presentes y futuras.



Bitcoin

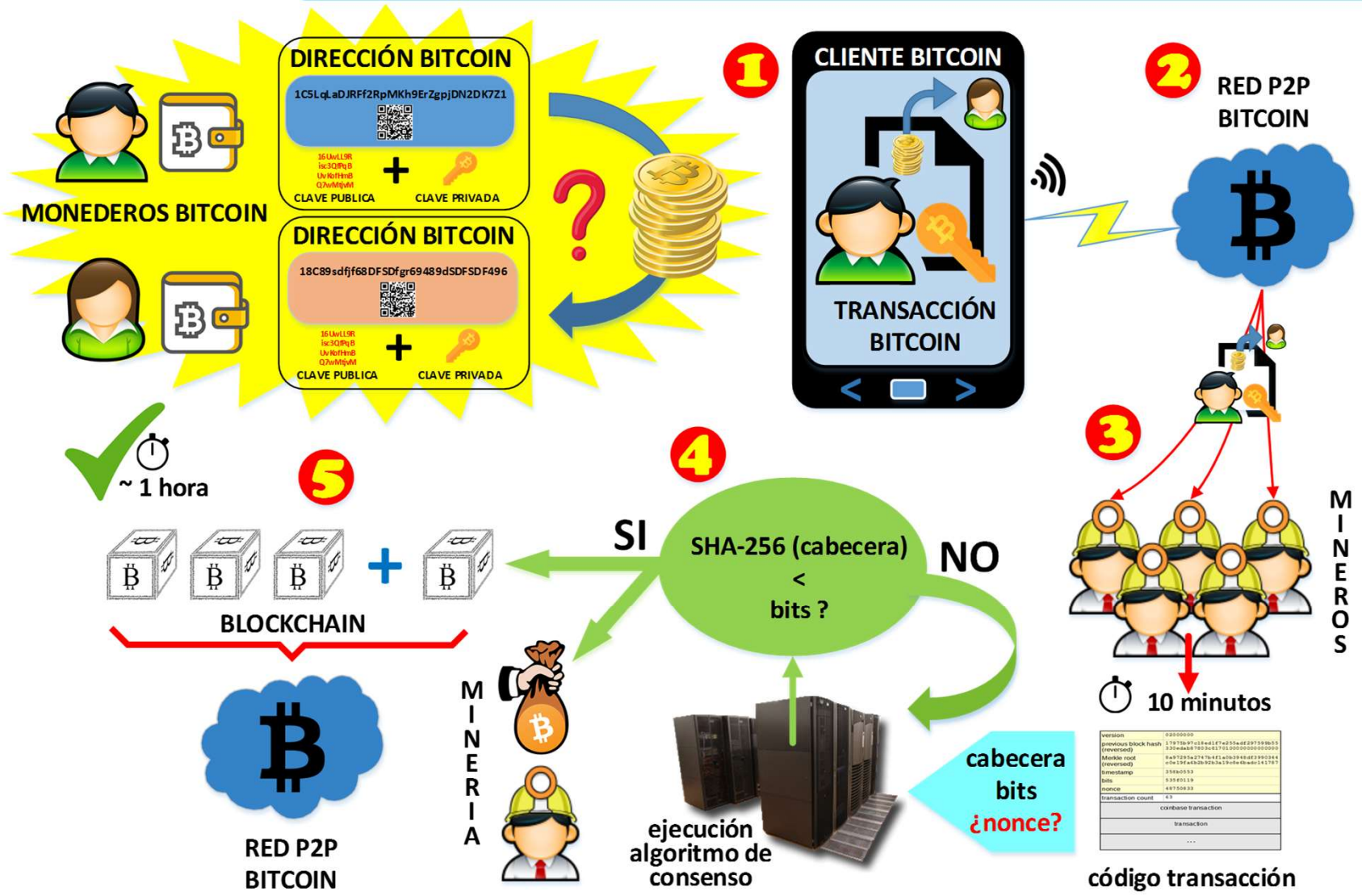
Bitcoin nace tras la crisis económica de 2008 como alternativa a la moneda tradicional, para evitar inflación y el control gubernamental

- Origen anónimo
- Código abierto en C++
- Funciona sobre Blockchain
- Criptomoneda descentralizada
- Deflacionaria. (hasta 21m.BTC)
- Infalsificable
- No legislada
- Volátil
- Permutable
- Intercambiable
- 100% del usuario
- Uso no requiere permiso
- Pseudoanónima
- Sin censura
- Sin intermediarios
- Transacciones irreversibles

ELEMENTOS BITCOIN

- USUARIO BITCOIN
- DIRECCIÓN BITCOIN
  - Clave privada
  - Clave pública
- BITCOIN / SATOSHI
- MONEDERO
- TRANSACCIÓN

- RED P2P BITCOIN
- MINERIA
- CONSENSO
- BLOQUE
- CADENA DE BLOQUES



1.- CREAR TRANSACCION

2.- PUBLICACION RED P2P

3.- EXTRACCIÓN MINERIA

4.- MINERÍA

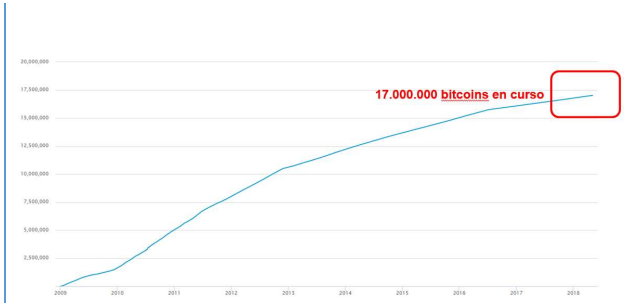
5.- RECOMPENSA MINERIA
AGREGAR BLOQUE

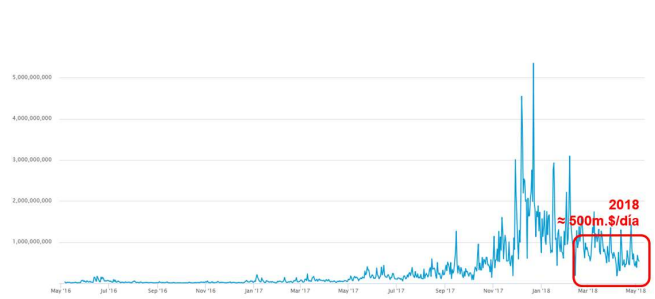
VENTAJAS / DESVENTAJAS FRENTE A MONEDA TRADICIONAL

- Global: No pertenece a gobiernos
- Independiente; no intervenible
- Transacciones baratas
- Transparente (Blockchain)
- No falsificable
- 24x7x365
- Satoshi beneficia micropagos
- Anonimato: beneficia su uso

- No permite comprar cualquier bien
- No todos los comercios lo aceptan
- La ausencia de un regulador incomoda mercados
- Muy volátil
- Límite (21 m.) deprime la economía
- Anonimato= actividades ilícitas

IMPACTO EN LOS MERCADOS



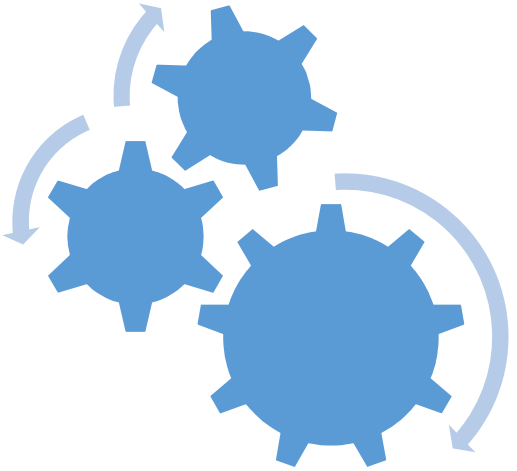


PRECIO BITCOIN	BITCOINS EN CURSO	TRANSACCIONES / DÍA
7.600$ (17.549$ en dic 2017)	17.000 BTC	500 millones $ /día

- Se prevé alcanzar 21 millones BTC en 2040.
- Volátil: no regulada, valor intrínseco nulo, noticias sobre violaciones de seguridad.
- Cada vez más empresas trabajan con BTC, salvo …
- Grandes inversores aún son cautos con el BTC

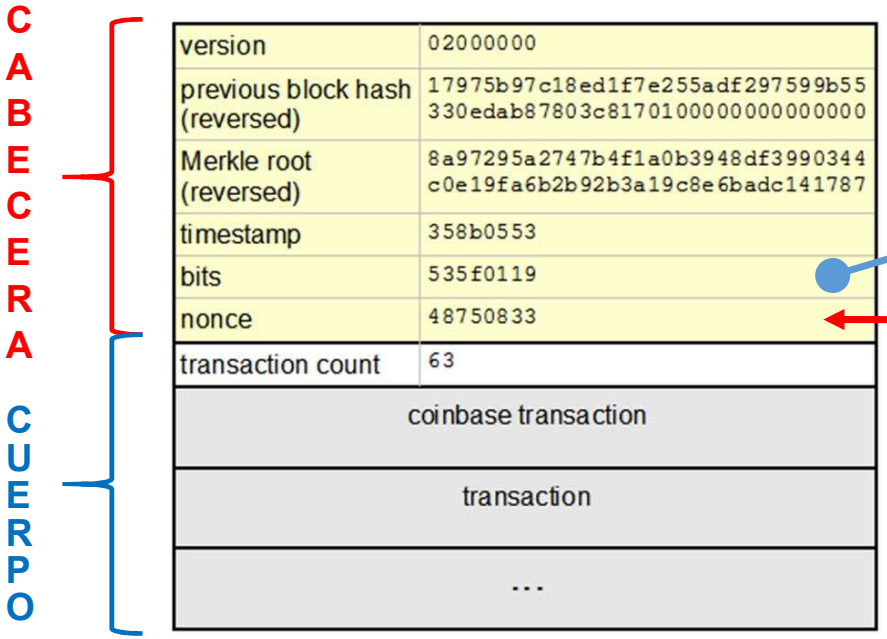
Tecnología de base de datos distribuida, formada por registros (bloques) enlazados y cifrados

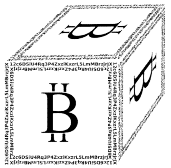
- **INMUTABLE e INTEGRO**: Los bloques de registros no se pueden modificar
- **CONFIABLE**: Su base de datos distribuida en nodos de una red P2P la hace escalable, y su información siempre disponible
- **TRAZABLE**: El propio protocolo crea los registros limpios, que son públicos y auditables
- **AGIL**: Transacciones en tiempo real, sin auditorías
- **AHORRA COSTES Y TIEMPO**: Se reducen tareas de registro y control



ALGORITMO DE CONSENSO

ARQUITECTURA

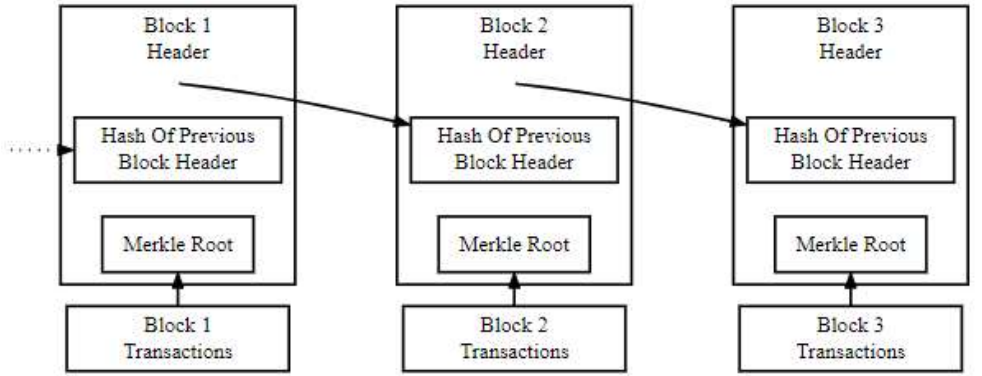




BLOQUE DE CADENA

SHA-256 (cabecera) < bits ?

nonce



ALGORITMOS DE CONSENSO

- **PROOF OF WORK**: Algoritmo de “prueba de trabajo”, en el que se recompensa por un coste de capacidad de computo criptográfico (Ej.:Bitcoin)
- **PROOF OF STAKE**: Algoritmo de “prueba de participación” en el que se recompensa con comisiones de transacción por cantidad de toquens resueltos de que se disponga

TIPOS DE BLOCKCHAIN

- **PÚBLICO**: BBDD distribuida masivamente, y de acceso y modificación para cualquier entidad. El incentivo de mantenimiento es económico-criptográfico
- **PRIVADO**: BBDD centralizada en nodos. Su acceso y modificación es pre-asignado a entidades. Se mantiene por interés propio
- **HIBRIDO**: Los participantes son preseleccionados pero las transacciones son publicas

Aplicativos Blockchain

ACTUALES

- Criptomonedas
- Smart Contracts
- Navegadores
- Almacenamiento
- Donaciones
- Registros médicos
- Registros académicos
- Comercio on-line
- Informática colaborativa

FUTUROS

- Entidades gubernamentales
- Industria 4.0
- Logística
- Votaciones

Aplicativos Blockchain

SMART CONTRACTS: código informático almacenado en Blockchain que hace cumplir un contrato y verifica sus firmantes de forma transparente y segura

1 

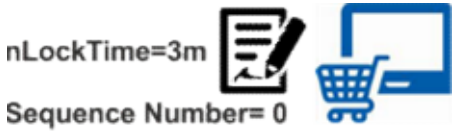
Intercambio de credenciales

2 

Usuario crea transacción

3 

Usuario envía HASP de la transacción

4 

Web comercial crea contrato agregando código con condiciones

5 

Web comercial envía contrato a Usuario

6 

Usuario firma contrato con clave privada, y se ejecuta contrato

Ejecución inmediata de clausulas, sector seguros, compraventa de mercancías, control de gasto, etc.

Universitat Oberta de Catalunya

Otras criptomonedas

	BITCOIN	ETHERUM	BITCOIN-CASH	RIPPLE	LITECOIN
LANZAMIENTO	2009	2015	2017	2012	2012
CREADOR	Satoshi Nakamoto	G. Wood, J.Wilcke,	Comunidades Bitcoin	Chris Larsen	Charlie Lee
TECNOLOGÍA	BlockChain	BlockChain	BlockChain	BlockChain	Blockchain
ALGORITMO	SHA-256	Ethash	SHA-256	ECDSA	Scrypt
VELOCIDAD TRANSACCION	Lenta	Lenta	Rápida	Muy rápida	Rápida
TIPO	Moneda	Moneda	Moneda	Red	Moneda
PRECIO ACTUAL	7.487$	591$	1101$	0,6525$	119$
CAPITALIZACIÓN	77.000m	36.000m	10.000m	9.000m	3.000m
MAX.CANTIDAD	21m	100m	21m	100 mil m	84m

FUTURO DE LA CRIPTOMONEDA

- Resurgimiento de la criptomoneda tras la alza y baja de 2017
- Posible regularización: Reducir volatilidad y transacciones opacas
- Se prevé Inversión de instituciones occidentales y especuladores
- Participación activa fondos de inversión y gestores activos
- Auge de “Alcoins” (criptomonedas derivadas del código fuente de Bitcoin)

Universitat Oberta de Catalunya

Conclusiones

- Bitcoin y otras criptodivisas ya están implantadas en los mercados
- Gobiernos y grandes inversores son aún cautos a su reconocimiento por no estar regulada, por su volatilidad y por el anonimato en sus transacciones
- El enorme potencial de la tecnología Blockchain y ya es la base de muchos aplicativos y de muchas soluciones futuras por su arquitectura segura, transparente y fiable

Universitat Oberta de Catalunya

MUCHAS GRACIAS

POR

SU ATENCIÓN