

Bitcoin

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



Bitcoin

<https://doi.org/10.5281/zenodo.4302267>

<https://github.com/mikel-egana-aranguren/EHU-SGSSI-01>



¿Por qué Bitcoin en SGSSI?

Es la criptomoneda más extendida, y muchos de sus conceptos también se usan en otras criptomonedas

Estas clases ...

... no son una apología de Bitcoin

... no son es una serie de consejos financieros

¿Por qué Bitcoin en SGSSI?

Es una aplicación muy exitosa de:

- Cifrado asimétrico
- Cifrado resumen

¿Por qué Bitcoin en SGSSI?

Asegura:

- No repudio: no se puede¹ deshacer una transacción
- Integridad: no se puede¹ modificar la historia del blockchain
- Autenticidad
- Pseudo-anonimato
- Etc.

[1] Es computacionalmente y socialmente muy caro e improbable

Introducción a Bitcoin

Bitcoin es a la vez:

- (Técnico) Un libro de contabilidad descentralizado y transparente
- (Político) Un sistema monetario:
 - Basado en el buen dinero ("sound money") según la [Escuela Austriaca](#) de economía
 - Que consume mucha energía eléctrica para emitir nueva moneda

Introducción a Bitcoin

No hay una división clara entre lo político y lo técnico (No hay nada más político que lo técnico)

Nos interesa más lo técnico pero no podemos obviar lo político

Introducción a Bitcoin

Bitcoin, como cualquier bien escaso, es susceptible de inversión (y especulación)

Eso hace que en las noticias siempre se hable de cuando sube y baja, pero eso no es lo más importante de Bitcoin

Lo más importante es cómo funciona para hacer transacciones monetarias, no como valor de inversión

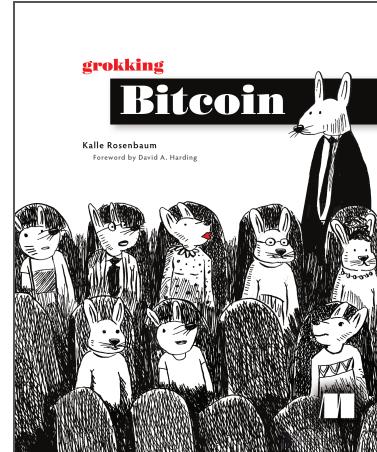
¿Qué es Bitcoin?

Grokking bitcoin (Kalle Rosenbaum, 2019):

[GitHub](#)

[Biblioteca EHU](#)

[Manning](#)



¿Qué es Bitcoin?

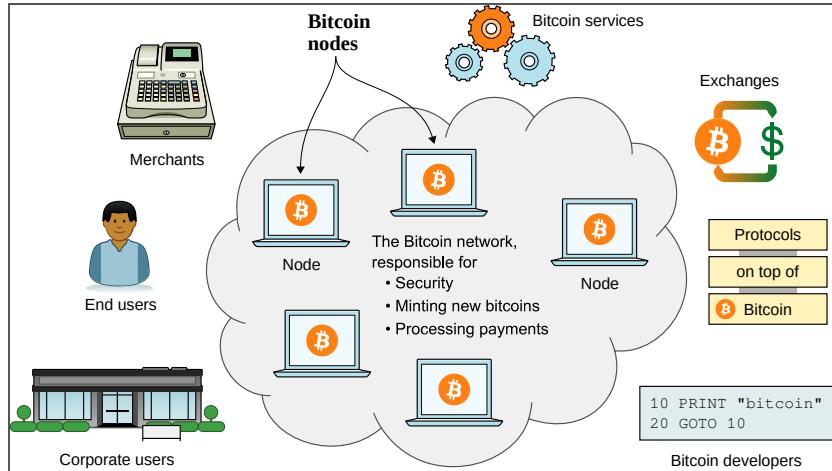
Un sistema de dinero digital

Basado en una red a la que cualquiera puede unirse a través de un nodo, y no gobernada por bancos ni gobiernos

Protocolo: Bitcoin (con B)

Moneda: bitcoin (con b). Símbolo: BTC o XTC. Satoshi: 0,00000001 BTC

La red Bitcoin



La red Bitcoin

Procesar pagos

Asegurar que el libro de contabilidad compartido no se modifica

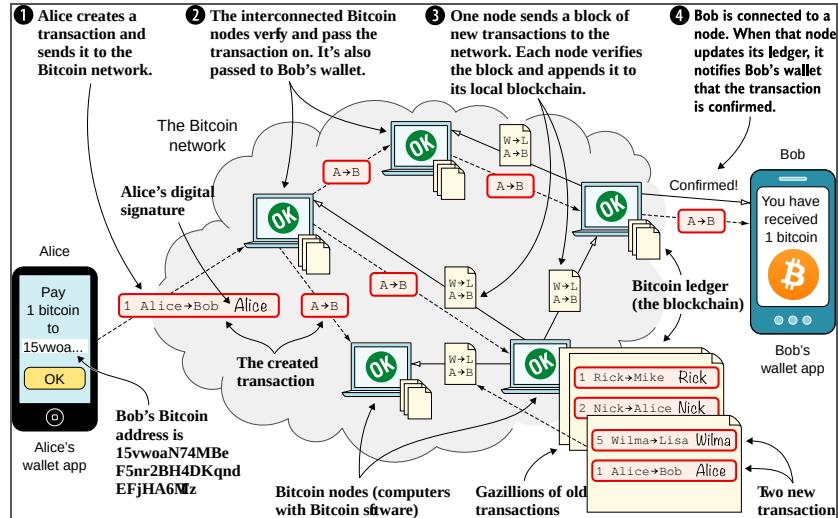
Poner bitcoins nuevos en circulación a una velocidad predeterminada

La red Bitcoin

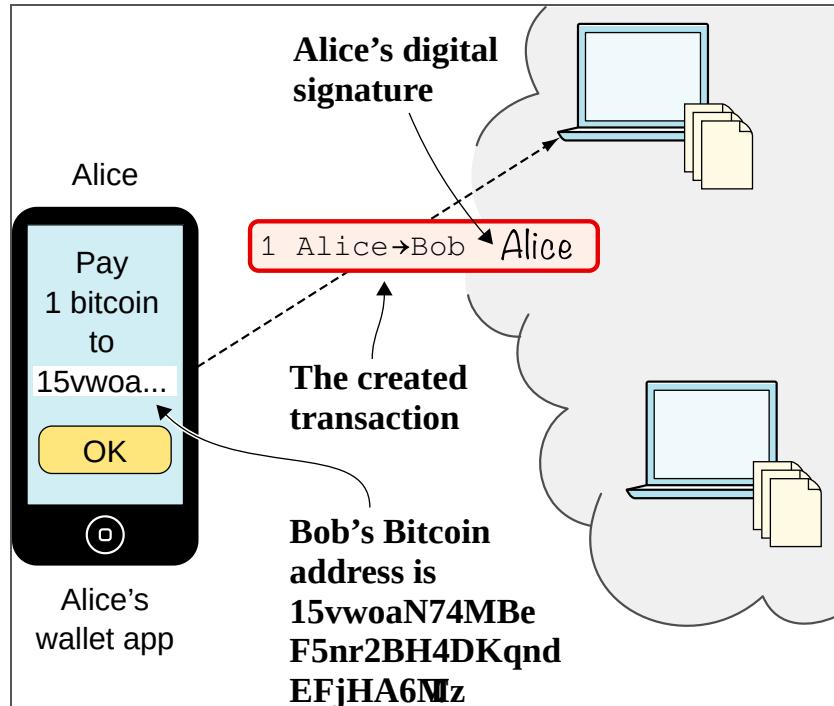
Un libro de contabilidad compartido (Todos los nodos tienen una copia)

El libro de contabilidad tiene todas las transacciones que se han hecho

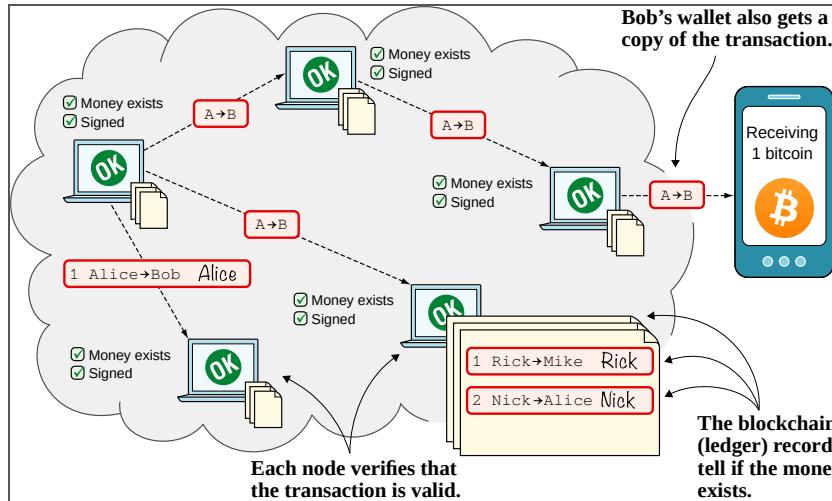
Pago



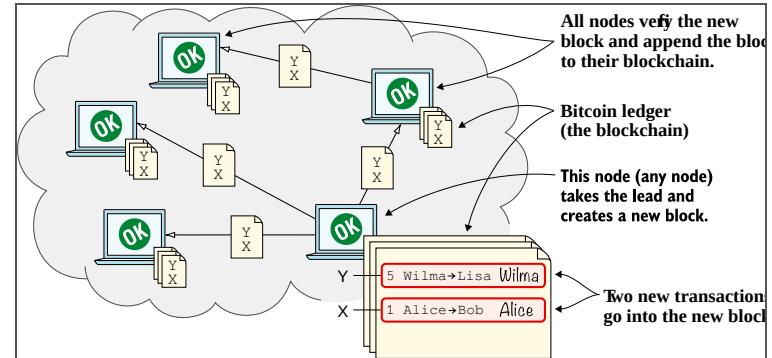
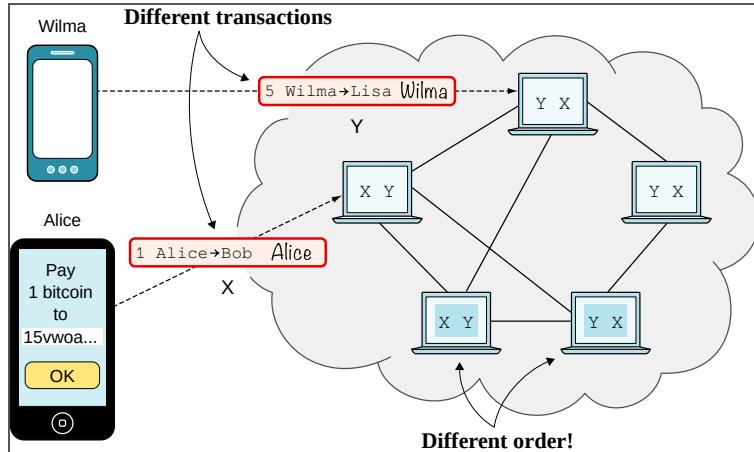
(1) Transacciones



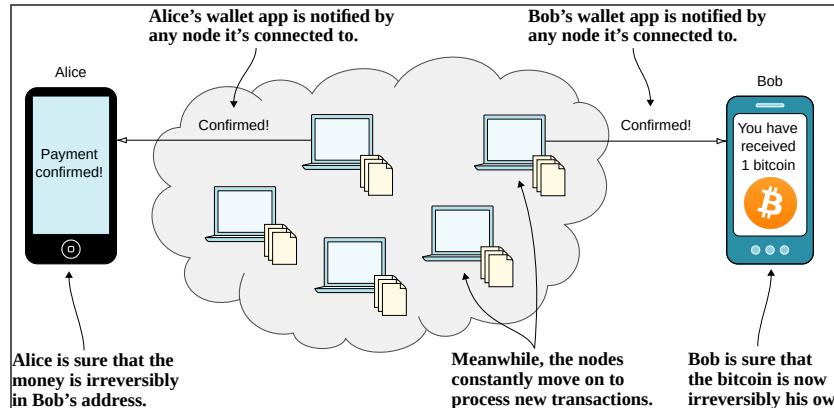
(2) Red



(3) Blockchain



(4) Carteras



Problemas que Bitcoin soluciona

- Falta de acceso a cuenta bancaria
- Falta de privacidad
- Transferencias entre países
- Hiper-inflación (*)

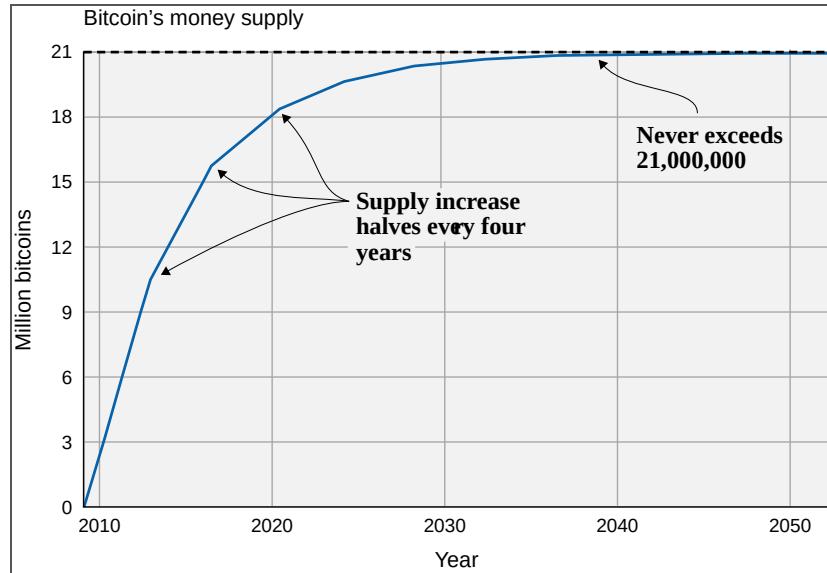
(*) La falacia de la composición (JM Keynes)

Discussing Crypto, the Left & Technofeudalism with Evgeny Morozov -
CRYPTO SYLLABUS long interview

Bitcoin vs instituciones financieras tradicionales

- Descentralizado
- Suministro limitado: 21 millones de bitcoins
- Sin fronteras

Suministro de bitcoins



Usos actuales de Bitcoin

- Ahorro
- Transferencias internacionales
- Compras
- Especulación financiera
- Certificado de propiedad
- Certificado de existencia
- ...

Cómo no usar Bitcoin

- Pagos pequeños (Lightning Network?)
- Pagos instantáneos (Lightning Network?)
- Inversión de todos nuestros ahorros (En realidad aplicable a cualquier actividad financiera)

?????

reward halves every 4 years bitcoin solo usa hashes (para firmar, para resumir las claves publicas,) y la clave privada para firmar (no para enviar a alguien confidencialmente, la clave publica se usa como "direccion", no como cifrador)? PKH Usar varios PKH mejora la privacidad Funciones Wallets 86-87

Bitcoin Core

<https://bitcoincore.org/en/about/>

<https://github.com/bitcoin/bitcoin/>

BIPs

BitCoin Improvement Proposal

<https://github.com/bitcoin/bips>

Economic majority

Futuro de Bitcoin

- Reserva de valor que respalda sistemas de transacción más rápidos (Como las tarjetas de crédito)
- Por ejemplo proyecto lightning "empaqueta" muchas transacciones que luego se dan a la vez