

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
- Algoritmos 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
- ...

[1] Es computacionalmente y socialmente muy caro e improbable

Introducción a Bitcoin

[Bitcoin: A Peer-to-Peer Electronic Cash System \(Satoshi Nakamoto\)](#)

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

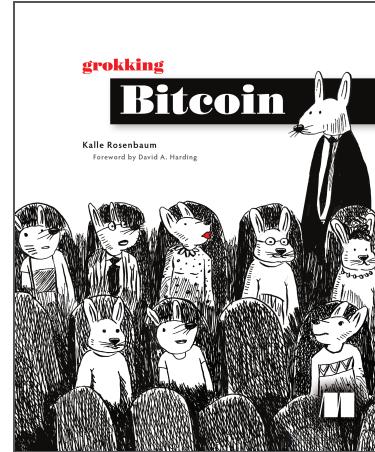
¿Qué es Bitcoin?

Grokking bitcoin (Kalle Rosenbaum, 2019):

[GitHub](#)

[Biblioteca EHU](#)

[Manning](#)



¿Qué es Bitcoin?

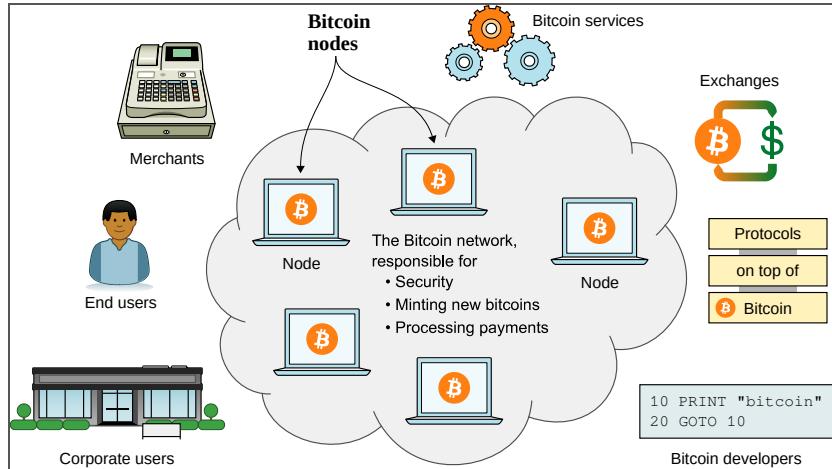
Un sistema de dinero digital

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

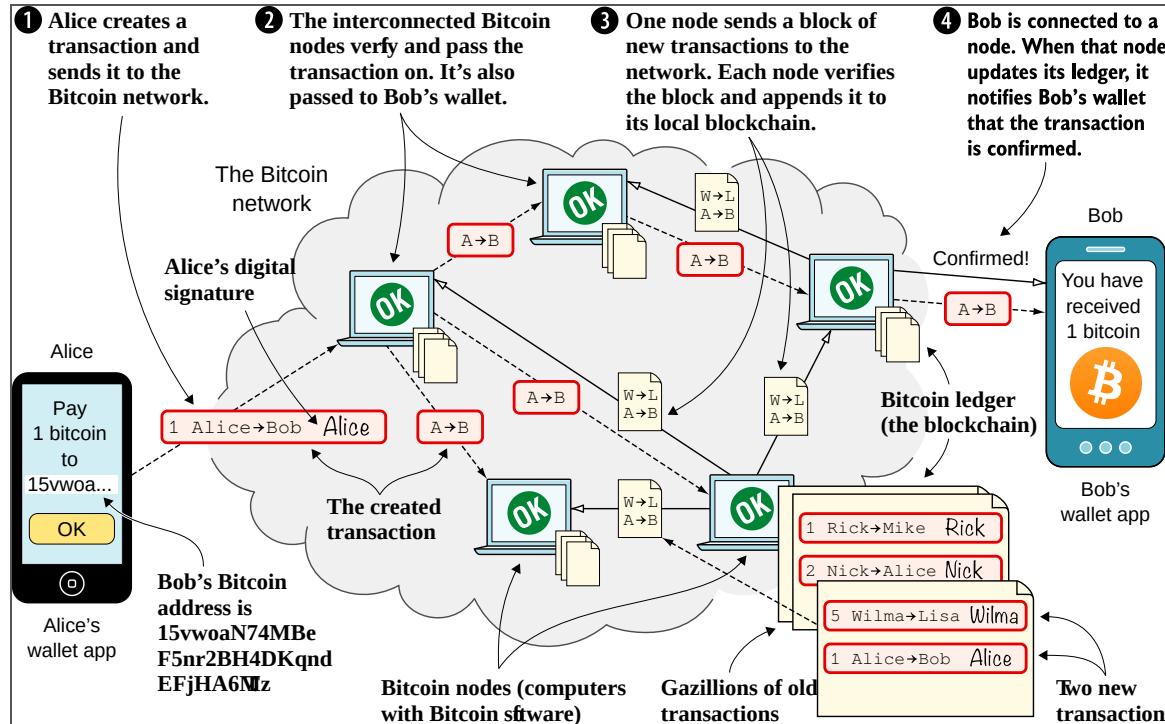
Poner bitcoins nuevos en circulación a una velocidad predeterminada

La red Bitcoin

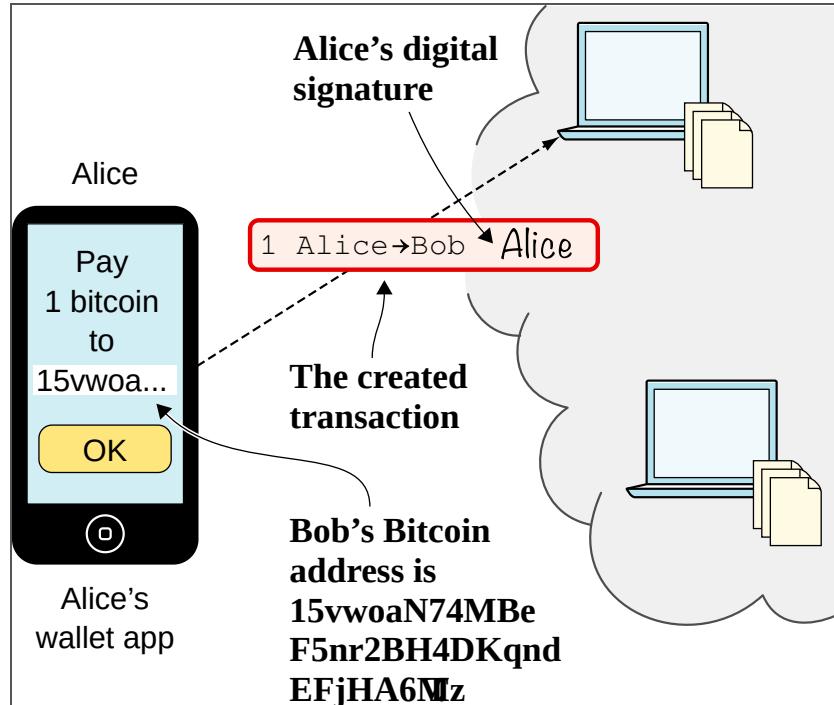
Un libro de contabilidad compartido (Todos los nodos tienen una copia)

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

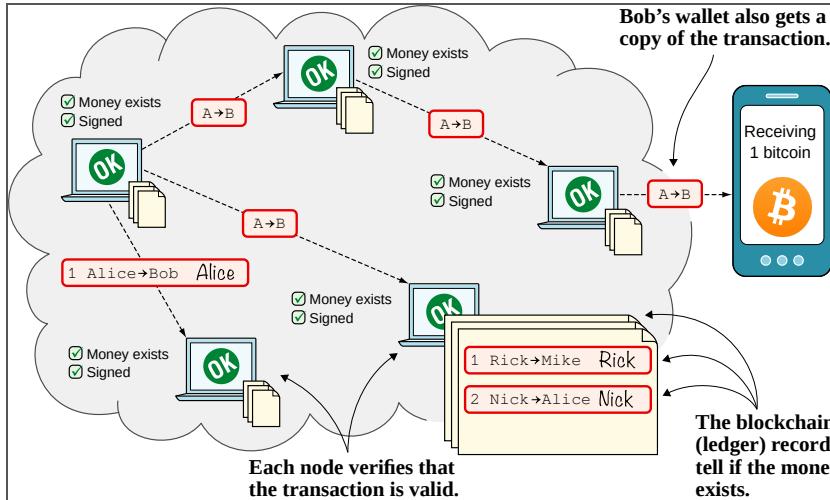
Pago



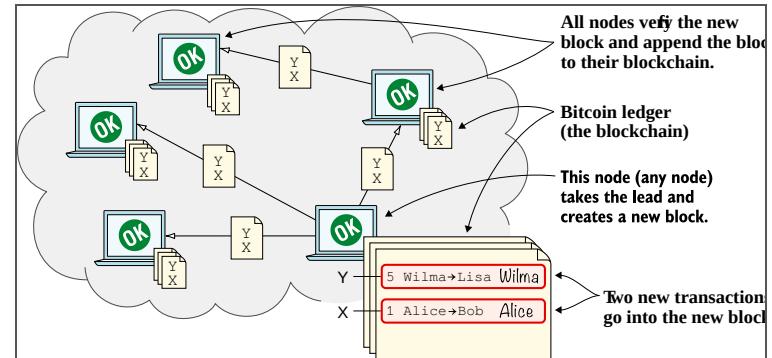
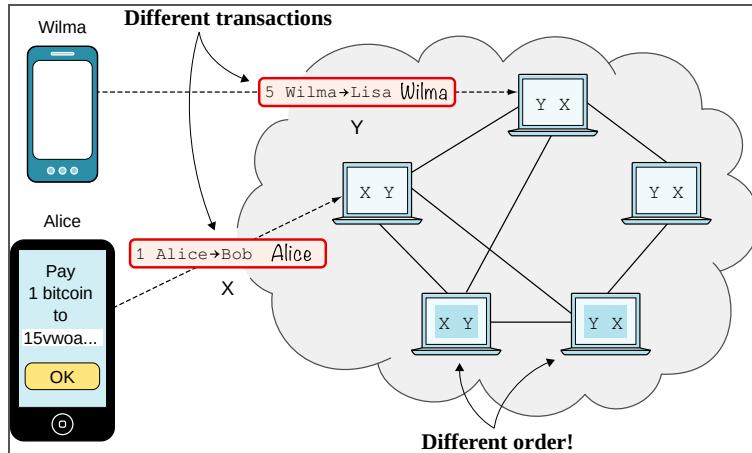
(1) Transacciones



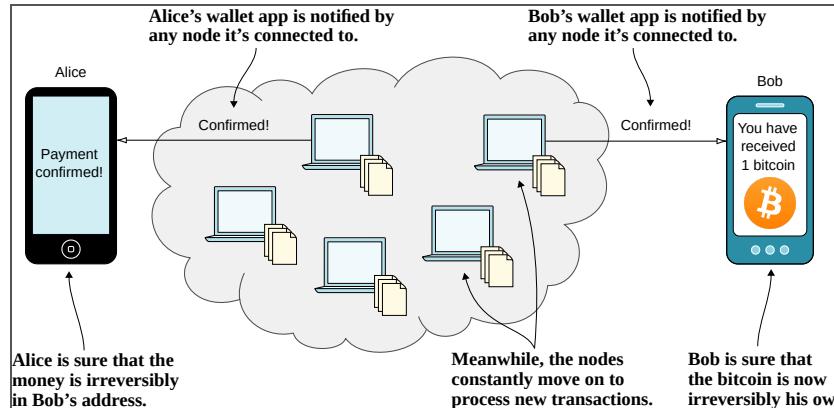
(2) Red



(3) Blockchain



(4) Carteras



¿Cómo se generan los Bitcoins?

- Mediante un proceso denominado minería, basado en una prueba de trabajo (PoW)
- Prueba de trabajo: resolución de cierto problema criptográfico por fuerza bruta
- Nadie puede controlar ni manipular el proceso de generación de la masa monetaria (No se puede "imprimir dinero")

Minería

- Dos funciones fundamentales:
 - Oferta monetaria: los mineros crean la nueva moneda (de forma matemáticamente controlada)
 - Seguridad: Mantienen la integridad de la cadena de bloques donde se incluyen las transacciones

Minería

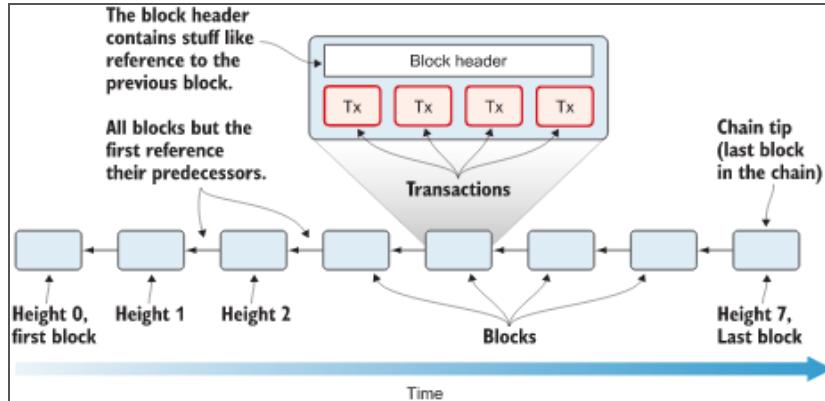
- Los mineros reciben una recompensa, que es la forma de crearse nuevos bitcoins
- Los mineros también se quedan con las pequeñas comisiones de cada transacción
- En total se crearán aproximadamente 21 millones de bitcoins

Red Bitcoin

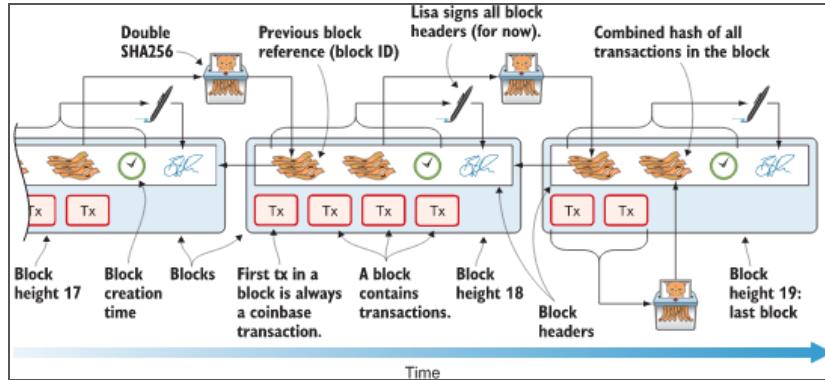
Cifrado resumen (Hash):

- **Para crear btcs, los mineros tienen que conseguir un hash**
- Resumir claves públicas
- Resumir transacciones
- Etc.

Red Bitcoin (Blockchain)



Red Bitcoin (Blockchain)



Red Bitcoin (Proof of work)

Validar bloques >> Generar bitcoins

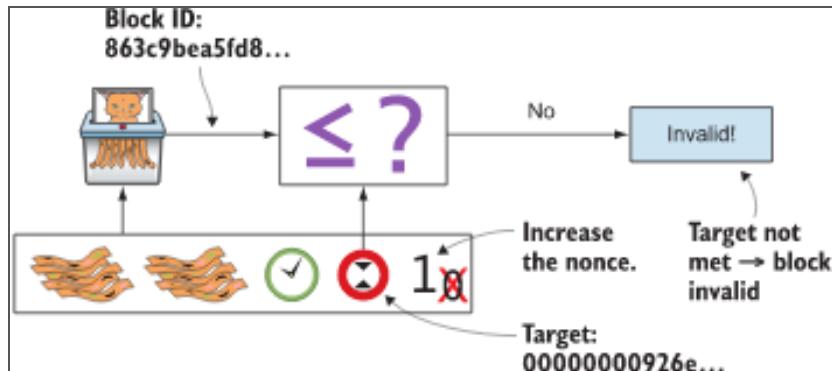
Validar: evitar doble gasto, timestamp adecuado, etc. >> generar hash

Ese hash tiene todos los anteriores

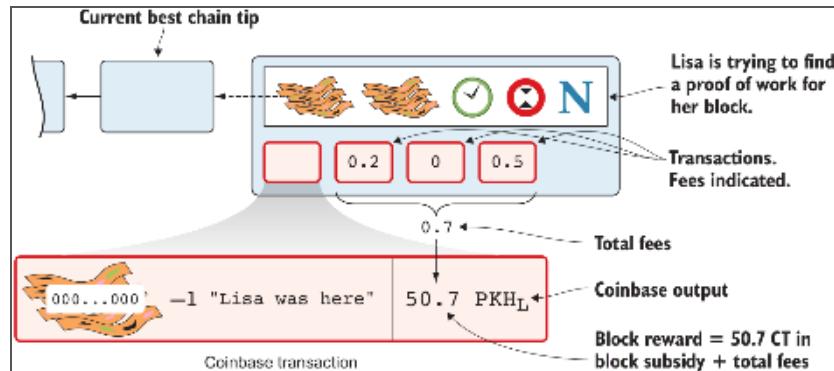
Pero hash debe ser un número menor que **target**

Target va cambiando, para cambiar dificultad

Red Bitcoin (Proof of work)



Red Bitcoin (Proof of work)



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

One of your critiques of Bitcoin as a currency (which you clearly state it is not and cannot be) is that it limits policy space available, such that, when there is a pandemic, it won't be possible to increase the money supply. I suppose this also covers 'printing money', with all of the perverse consequences of QE that you yourself have documented elsewhere. Wouldn't the Bitcoin maximalists be at least coherent in arguing that this inability to print money is a feature, not a bug, of the system?

When 'Bitcoin maximalists', as you call them, wax lyrical about the inability to print money (and celebrate this inability as Bitcoin's feature, rather than its bug), they are being terribly unoriginal – banal, I dare say. Capitalism nearly died in 1929, and tens of millions *did* die in the war that ensued, because of this toxic fallacy that underpinned the Gold Standard then and Bitcoin now. Which fallacy? The fallacy of composition, as John Maynard Keynes called it.

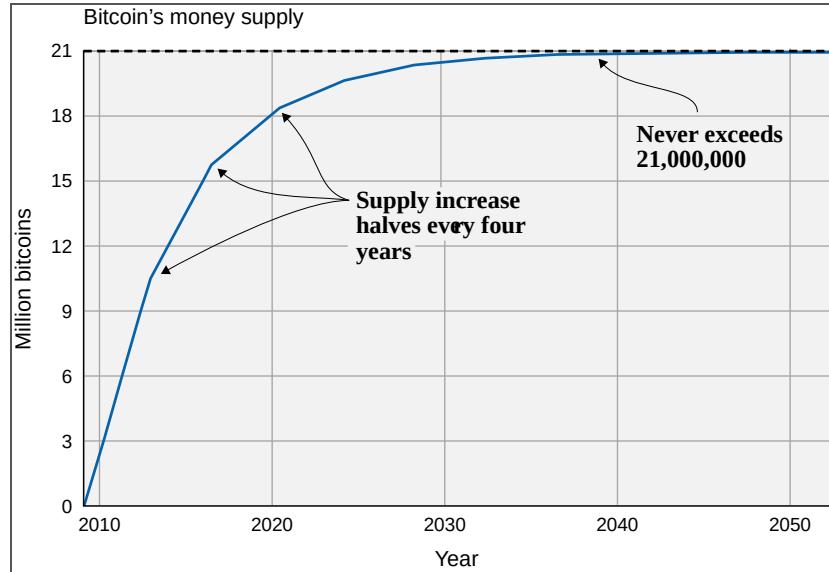
Its essence is a tendency to extrapolate from the personal realm to the macroeconomic one. To say that if something is good for me – if a practice is sound at the level of my family, business, etc. – it must also be good for the state, government, humanity at large. For example, yes, parsimony is a good thing for me, personally. If I can't make ends meet, I need to tighten my belt; otherwise, I shall sink more and more into debt. However, the exact opposite holds for a macroeconomy. If, in the midst of a recession, the government tries to tighten its belt as a means of eliminating its budget deficit, then public expenditure will decline at a time of falling private expenditure. And since the sum of private and public expenditure equals aggregate income, the government will be – inadvertently – magnifying the recession and, yes, its own deficit (as government revenues fall). This is an example of one thing (belt-tightening) being good at the micro-level and catastrophic at the macro level.

Similarly with gold, Bitcoin, and all other 'things' of exchange value: If you have gold, it is good for you if its supply is limited, fixed if possible. Same with Bitcoin, silver, dollars. (Nb. It is why the rich and powerful traditionally opposed expansionary monetary policy, crying 'hyperinflation' at the drop of a hat.) So, yes, if you are invested in Bitcoin, or for some reason you are elated every time its dollar exchange rate rises, you have

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)

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