Bitcoin

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Bitcoin

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

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

Material reciclado de Miguel Vidal: https://speakerdeck.com/mvidal/

Indice

- ¿Por qué Bitcoin en SGSSI?
- Introducción a Bitcoin
- Teoría monetaria básica
- ¿Qué es Bitcoin?
- Futuro de Bitcoin

¿Por qúe 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 qúe Bitcoin en SGSSI?

Es una aplicación muy exitosa de:

- Cifrado asimétrico
- Cifrado resumen

¿Por qúe Bitcoin en SGSSI?

Asegura:

- No repudio: no se puede[1] deshacer una transacción
- Integridad: no se puede[1] modificar la historia del blockchain
- Autenticididad
- 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

Teoría monetaria básica

Primer mecanismo de transferencia de valor: el trueque

Yo produzco manzanas, tu ovejas

Si me arreglas el tejado, te doy manzanas

… Pero tu no necesitas manzanas, necesitas naranjas (Ya tienes manzanas)

… Si te arreglo el tejado, me das ovejas, pero no tengo sitio para todas

El dinero surge como una abstracción más conveniente que el trueque

Teoría monetaria básica

El buen dinero (Sound money) es:

- Portable (Fácil de transportar)
- Homogéneo (Es lo mismo en todas partes)
- Divisible (En unidades más pequeñas)
- Durable (Retiene su valor en el tiempo)

Teoría monetaria básica

El buen dinero (Sound money) es:

- Escaso y difícil de conseguir/generar:
  - Evitar falsificaciones
  - Representación más fiel posible de la riqueza real en la economía (Por ejemplo cuesta mucho conseguir oro, dejando un margen de beneficio muy pequeño)

Teoría monetaria básica

A lo largo de la historia el buen dinero se ha implementado de diferentes maneras, sobretodo mediante el oro

El dinero era respaldado por las reservas de oro de cada gobierno (dinero **fiduciario** -fidare: confiar-)

Teoría monetaria básica

En los 70 se abandonó el patrón oro, y el dinero pasó a ser **fiat** ("Que así sea")

El dinero ahora se produce mediante deuda que adquieren los bancos con el banco central (BCE, Reserva Federal): como no está respaldado por nada, el gobierno puede "imprimir" todo el dinero que considere (No hay que minar oro, simplemente cambiar la tasa de interés)

Teoría monetaria básica

Según la escuela Austriaca el dinero fiat resulta en inflación y "Robo de salarios"

Satoshi Nakamoto creó Bitcoin como una manera de implementar el buen dinero, en contraposición al dinero fiat, y sin control de ninguna institución (¿En contra del sistema financiero y la crisis del 2008?)

Bloque génesis : "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

Teoría monetaria básica

Además, Bitcoin es mejor dinero que el oro, ya que su escasez está formalmente demostrada:

Si cayese un meteorito gigante lleno de oro en la tierra, el oro ya no serviría

Origen de Bitcoin

- 31 octubre 2008: Satoshi publica el whitepaper
- 17 noviembre 2008: envía bajo pedido el código fuente (en el que dice que lleva año y medio trabajando)
- 3 enero 2009: se mina el bloque génesis
- 8 enero 2009: primer tarball (rar) del código (0.1 alpha) en Spourceforge
- 12 enero 2009: 1ª transacción (de Satoshi a Hal Finney, bloque 170)

Origen de Bitcoin

- 5 octubre 2009: primer exchange que cotiza el precio calculando el coste eléctrico en producirlo (1$ -> 1309 btcs)
- 22 mayo 2010: Pizza day (Laszlo, 2 pizzas por 10k btcs)
- Diciembre 2010: Satoshi abandona el proyecto

¿Qué es Bitcoin?

- Un libro de cuentas (Ledger):
  - Compartido en una red P2P a la que cualquiera se puede sumar como nodo
  - Cualquier nodo puede validar su contenido
  - Imposible* modificar páginas del una vez validadas (blockchain)

¿Qué es Bitcoin?

- Un sistema de transferencia de valor basado en el libro de cuentas
- Un sistema monetario descentralizado no-infacionario, con alicientes para los nodos para emitir moneda y validar transacciones (**A la vez**). Se basa en el coste de la electricidad consumida para emitir la moneda.

Otros posibles usos de Bitcoin

- Acciones, opciones y otros instrumentos financieros y mercados bursátiles
- Contratos
- Elecciones
- Autoridades certificadoras
- Notarios, abogados…

¿Qué es Bitcoin?

- Protocolo: Bitcoin (con B)
- Moneda: bitcoin (con b). Simbolo: BTC o XTC. Satoshi: 0,00000001 BTC
- API programable

¿Qué es Bitcoin?

- Se puede transferir arbitrariamente entre nodos de la red
- Las transacciones son irreversibles
- Las transacciones se transmiten en segundos y se confirman en minutos
- Las transacciones se pueden recibir en cualquier momento esté o no el ordenador encendido
- La comisión por transacción es voluntaria y muy barata
- Hay un límite duro de 21M, pero son divisibles por 8 decimales

Máxima transparencia

- Todo el mundo ve todo
- Todo el mundo puede ejecutar código
- Todo el mundo puede validar transacciones

Máxima transparencia

- Todas las transacciones pasadas y presentes son públicas, pero no se vinculan a ninguna identidad, sino a una dirección (un hash)
- El anonimato y la trazabilidad dependen del propio usuario
- En la base de datos se añaden cada diez minutos los bloques de las transacciones que se han producido en ese periodo de tiempo con una serie de propiedades que las hacen aceptables

Máxima fiabilidad

- Integridad: No puede ser falsificado ni alterado
- No repudio
- Es fiable porque no necesitas fiarte de nadie

¿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

Libro "Grokking bitcoin":

GitHub (Ejemplo)

Manning

Red Bitcoin

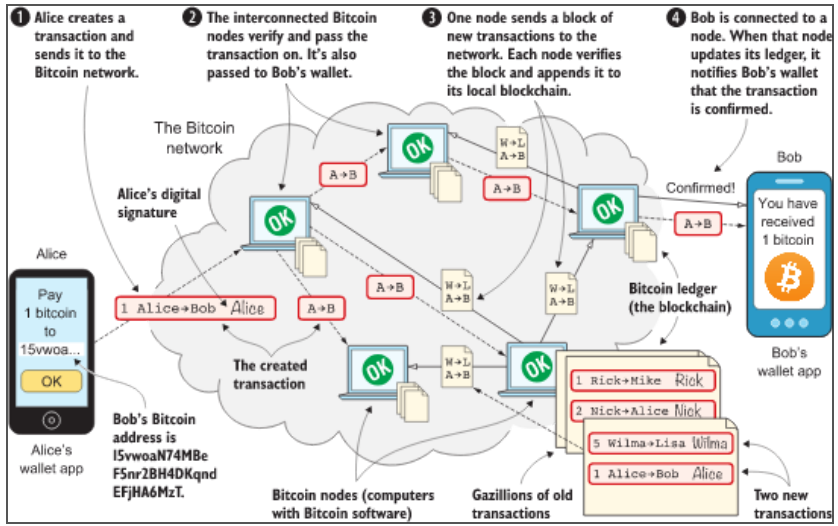
8.5.1. Bitcoin at a glance

The Bitcoin peer-to-peer network is huge. As of this writing:

- There are about 10,000 publicly accessible full nodes.
- Bitcoin's money supply is about 17,400,000 BTC.
- Each bitcoin is worth around $6,500.
- Bitcoin processes about 250,000 transactions per day.
- An estimate of 100,000 BTC, valued at $630 million, is moved daily.
- The total mining hashrate is about 50 Ehash/s, or 50×10^{18} hash/s. A typical desktop computer can do about 25 Mhash/s.
- The transaction fees paid each day total around 17 BTC. This averages to 6,800 satoshis per transaction, or about $0.40 per transaction.
- People in all corners of the world use Bitcoin to get around problems in their day-to-day lives.

bitnodes.io

Red Bitcoin


1 Alice creates a transaction and sends it to the Bitcoin network.
2 The interconnected Bitcoin nodes verify and pass the transaction on. It's also passed to Bob's wallet.
3 One node sends a block of new transactions to the network. Each node verifies the block and appends it to its local blockchain.
4 Bob is connected to a node. When that node updates its ledger, it notifies Bob's wallet that the transaction is confirmed.
The Bitcoin network
Alice's digital signature
Alice
Pay 1 bitcoin to 15vwoa...
OK
1 Alice→Bob Alice
A→B
W→L
A→B
Alice's wallet app
Bob's Bitcoin address is 15vwoaN74MBeF5nr2BH4DKqndEFjHA6MzT.
The created transaction
Bitcoin nodes (computers with Bitcoin software)
Gazillions of old transactions
Bitcoin ledger (the blockchain)
Confirmed!
Bob
You have received 1 bitcoin
Bob's wallet app
1 Rick→Mike Rick
2 Nick→Alice Nick
5 Wilma→Lisa Wilma
1 Alice→Bob Alice
Two new transactions

Red Bitcoin

"Enviar dinero": Clave pública --> clave privada

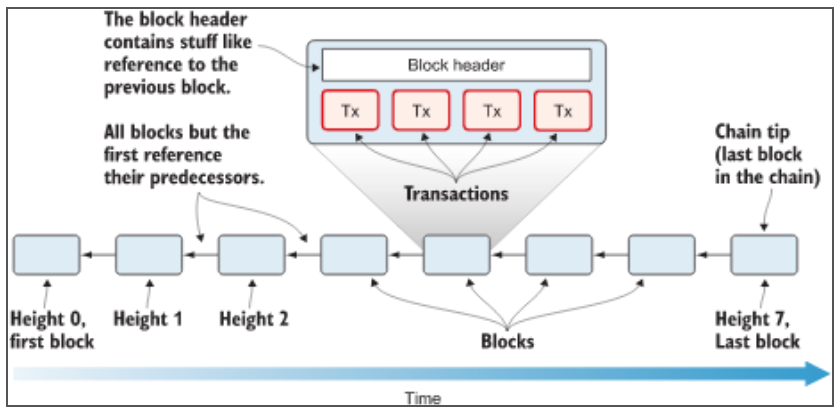
"Firmar transacciones": Clave privada --> Clave pública

Red Bitcoin

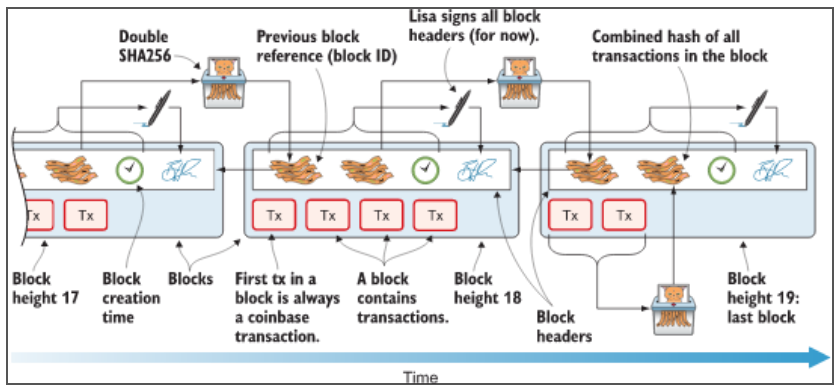
Cifrado resumen (Hash):

- **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

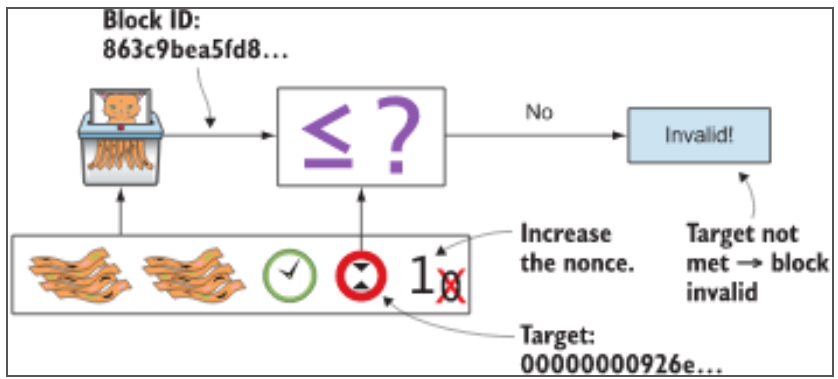
Validar: evitar doble gasto, timestamp adecuado, etc. --> generar hash

Ese hash tiene todos los anteriores

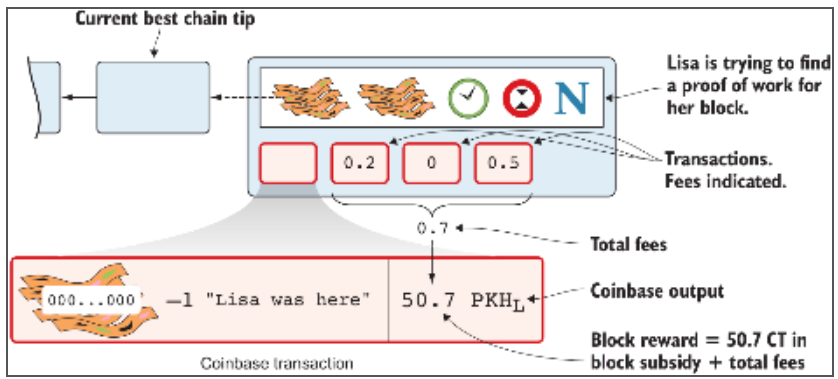
Pero hash debe ser un numero menor que **target**

Target va cambiando, para cambiar dificultad

Red Bitcoin (Proof of work)



Red Bitcoin (Proof of work)



Bitcoin Core

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

https://github.com/bitcoin/bitcoin/

BIPs

BitCoin improvement proposal

https://github.com/bitcoin/bips

Aprobación por "mayoría económica"

Futuro de Bitcoin

- Reserva de valor que respalda sistemas de transacción más rápidos (Por ejemplo VISA tarda 90 días en validar transacciones)
- Por ejemplo proyecto lightning "empaqueta" muchas transacciones que luego se dan a la vez