Aspectos practicos y teoricos de Bitcoin

Antonio J. Di Scala

Politecnico di Torino
Dipartimento di Scienze Matematiche
https://crypto.polito.it/

Diciembre 2022

Abstract: Que es Bitcoin ? que significa **tener bitcoins (o satoshis)** ? Como obtenerlos i.e. como comprarlos? Como se usan (Lightning Network) ? Como se venden? Que es un "wallet" ? Que tienen estas preguntas que ver con criptografia ? El contenido de mi charla es principalmente hacer mas precisas estas preguntas e intentar dar algunas respuestas.

Sobre el orador: Actualmente Professore Ordinario di Matematica (Professore Ordinario es el cargo mas alto de la universidad en Italia). Doctor en Matemática, Fa.M.A.F, Universidad Nacional de Córdoba (2000). Licenciado en Matemática, Universidad de La Plata (1995). Técnico en Computación , ENET N3, Mar del Plata (1990). Más información : https://antoniojdiscala.ddns.net/

1 Que es Bitcoin ?

Es la red (de nodos https://bitnodes.io/) que siguiendo un protocolo implementa la "moneda" bitcoin (BTC) descrita nel white paper de 'Satoshi Nakamoto' en 2008.

El codigo del protocolo es open source y la primera version fue publicada en un repositorio (sourceforge) en 2009.

El protocolo gestiona la creacion, las transacciones de BTC y mantiene sincronizado el "libro diario" (Blockchain) en los nodos.

Como cualquier moneda, bitcoin es un objeto cuya finalidad es ser utilizado como medio de pago e intermediario de cambios y que cumple las funciones de:

- medida de valor (dinero como unidad de cuenta);
- medios de cambio en la venta de bienes y servicios y en las transacciones comerciales en general (moneda como instrumento de pago);
- fondo de valor (moneda como reserva de valor);

1.1 Caracteristicas principales del protocolo Bitcoin

- Primera moneda cuya implementacion depende de primitivas criptograficas.
- Peer to Peer. Libro diario distribuido en todos los nodos de la red.
- Bloques de transacciones : se agregan cada 10 minutos en promedio al "libro diario" desde el 3 de Enero de 2009 : https://mempool.space/
- Emite 900 BTC por dia hasta hasta Enero 2025, luego 450 por dia por 4 años, etc (i.e. reduciendo a mitad cada 4 años)
- Se emitiran 21000000 BTC $= 21 * 10^{14}$ sats .

2 Not you keys, Not your coins but ...

Billetera, monedero, llavero ?

Clients: apps o software .

bitcoin.org/en/choose-your-wallet
Wallets no custodial. Phoenix, Blue Wallet,... https://wasabiwallet.io/index.html#download
Wallets custodial. Wallet of Satoshi.

Frase seed

Dos claves: 256 bits Clave Privada
Clave Publica

BTC Address:

1tRkMBDDMGDLLcyh13eqP3WtUdcPxg66X

que seria el equivalente a un CBU (o un IBAN de la red SEPA en Europa).

Nota: numero total de claves privadas $\approx 10^{77}$. Numero de atomos en el universo visible 10^{80} ....

2.1 Elliptic curve : Secp256k1

$$y^2 = x^3 + 7 \pmod{p}$$

https://en.bitcoin.it/wiki/Secp256k1

2.2 Comprar, Usar , Vender

Plataformas KYC , exchanges ... , Bitkipi

CryptoAvisos, Bitrefill

Empresas que dan servicios de soporte : Bitcoin People, Ibex,

2.3 Que es Lightning Network ?

3 Don't Trust, Verify !

Mastering Bitcoin: Programming the Open Blockchain by Andreas Antonopoulos

Bitcoin Internals by Chris Clark.

Instalar un nodo?

Leer white paper.

https://en.bitcoin.it/wiki/Protocol_documentation
Github Andrea Gangemi https://github.com/Gangi94/BlockchainAddress
Escuchar y leer programas, revistas especilizadas e.g. BIP, ArXiv Cryptography

4 Doble utilizo y creación de BTC : Proof of Work

Generales Bizantinos: problema de consenso/sincronización :

- coordinarse (nodos) para estar todos de acuerdo en el orden cronologico de las transacciones.
- Emición de BTC.

Solución : problema matematico

$$\text{hash(Bloque)} < \text{target}$$

https://emn178.github.io/online-tools/sha256.html
Ejemplo programa Python.

https://andersbrownworth.com/blockchain/block

Se puede pensar en el valor intrinseco de poseer BTC como el valor de haber resuelto la desigualdad anterior.

4.1 Algunos hechos historicos

- Dwork and Naor in 1993.
- Adam Back's 1997 Hashcash.
- Nick Szabos in his digital currency proposal called Bit Gold, which was released between 1998 and 2005.

Henry Ford y Muscle Shoals.

5 Notas/Links:

- Unidad de cuenta: https://es.wikipedia.org/wiki/Unidad_de_cuenta
- Red SEPA: https://www.ecb.europa.eu/paym/integration/retail/sepa/html/index.en.html
- Wallet of Satoshi https://www.walletofsatoshi.com/
- Wallet Electrum: https://electrum.org/#home
- Wallet Bitkipi: https://bitkipi.com/
- Wallet Phoenix Tutorial: https://www.youtube.com/watch?v=Cx5PK1H5OR0
- Bitcoin Network Full Nodes: https://bitnodes.io/
- Bitcoin original code: http://btc.yt/lxr/satoshi/source/src/main.cpp?v=0.4.00rc1
- Sobre implementaciones distintas: https://bitcoinmagazine.com/technical/multiple-bitco
- Bitcoin White Paper: https://bitcoin.org/bitcoin.pdf
- Guia Bitcoin Full Node: https://github.com/BlockchainCommons/Learning-Bitcoin-from-the-C blob/master/A2_0_Compiling_Bitcoin_from_Source.md
- Explorador Block Chain: https://www.blockchain.com/explorer
- Henry Ford y Muscle Shoals: https://urbanutopias.net/2019/02/01/henry-ford-muscle-shoal
- Polar para empezar con LN: https://lightningpolar.com/
- Submarine Swaps: https://docs.lightning.engineering/the-lightning-network/multihop-paymen understanding-submarine-swaps
- ArXiv Cryptography and Security: https://arxiv.org/list/cs.CR/recent
- Cryptology ePrint Archive: https://eprint.iacr.org/days/7
- Datos, transcripciones Bitcoin y LN: https://btctranscripts.com/
- Bitcoin Italia Podcast: https://bitcoinitaliapodcast.it/
- Dos tanos en El Salvador: https://www.youtube.com/@bitcoinexplorers
- Rikky entrevista a un argentino: https://www.youtube.com/watch?v=pZ1Gv_q_bgM&t=914s
- Bitrefill: https://www.bitrefill.com/
- Ibex: https://www.poweredbyibex.io/