

BITCOIN, PROTOCOLO Y CRIPTOGRAFÍA QUE LO HACE SEGURO

CARLOS RODRIGO GUZMÁN DURÁN
JORGE MARTÍNEZ ORTEGA

BITCOIN Y LIGHTNING
GUADALAJARA

22 de mayo, 2025

Bitcoin: un Sistema de Dinero Efectivo Electrónico entre Pares

El 1 de noviembre de 2008, un programador informático con seudónimo Satoshi Nakamoto envió el marco teórico (White paper) de Bitcoin a una lista de correo de criptografía titulado “Bitcoin: A Peer to Peer Electronic Cash System”.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshiin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

BITCOIN es un conjunto de conceptos y tecnologías que forman la base de un ecosistema de dinero digital

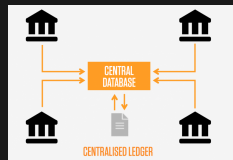
- 1 Funciones *hash* y árboles de Merkle tienen su origen en los años 50's hasta los diseños de la NSA (Agencia de seguridad Nacional de EU) en los años 90's.
- 2 Criptografía de clave pública y firmas digitales: inventadas en los 70's por Whitfield Diffie y Martin Hellman.
- 3 Blockchain: fue inventada por Stuart Haber y W. Scott Stornetta a principios de los 90's para proteger documentos mediante sellos de tiempo.

Tipos de “dineros”

- Tokens (objetos): conchas marinas, plumas, cuentas de cristal, monedas, billetes...



- Ledgers (libros contables):



Lyn Alden: «los tokens también pueden ser pensados como ledgers a los que no se tiene acceso completo y que se actualizan por posesión física.»

EVOLUCIÓN DEL DINERO

- 1 *Commodity money.*
- 2 Patrón oro.
- 3 Dinero fiat: patrón dolar.
- 4 Dinero criptográfico (dinero emergente)



Link ref.: Lyn Alden

ALGUNAS CARACTERÍSTICAS

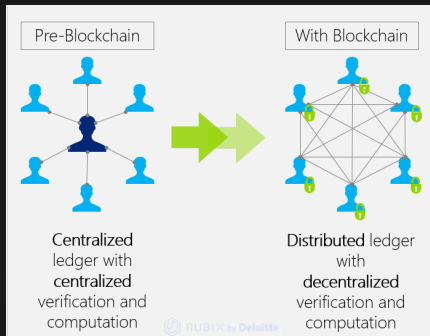
- Fungible.
- No consumible.
- Transportable.
- Duradero.
- Divisible.
- Verificable/autenticable.
- Escaso.

Traits of Money	Gold	Fiat (US Dollar)	Crypto (Bitcoin)
Fungible (<i>Interchangeable</i>)	High	High	High
Non-Consumable	High	High	High
Portability	Moderate	High	High
Durable	High	Moderate	High
Highly Divisible	Moderate	Moderate	High
Secure (<i>Cannot be counterfeited</i>)	Moderate	Moderate	High
Easily Transactable	Low	High	High
Scarce (<i>Predictable Supply</i>)	Moderate	Low	High
Sovereign (<i>Government Issued</i>)	Low	High	Low
Decentralized	Low	Low	High
Smart (<i>Programmable</i>)	Low	Low	High

Con estas características el dinero es el bien más vendible y su valor es principalmente de intercambio (en el tiempo y el espacio).

DINERO DIGITAL

Bitcoin es 100% digital... pero el dinero *fiat* también lo es en gran medida: el papel moneda es $< 8\%$ del dinero. El dinero *fiat* funciona principalmente con libros contables centralizados: Visa, Mastercard, Paypal, etc.



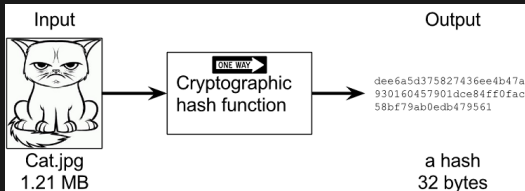
Pero ¿cómo se genera un consenso sobre el libro contable?

CONSENSO DE SATOSHI

- 1 El libro contable es público (actualmente 752 GB).

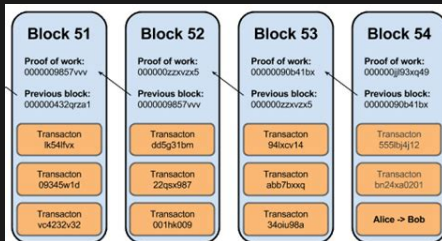


- 2 Para actualizar el libro contable es necesario invertir energía (proof of work) y la actualización debe contener transacciones "válidas". Hacer trampa no es rentable pues la red no toma en cuenta actualizaciones (bloques) con transacciones inválidas.



CONSENSO DE SATOSHI

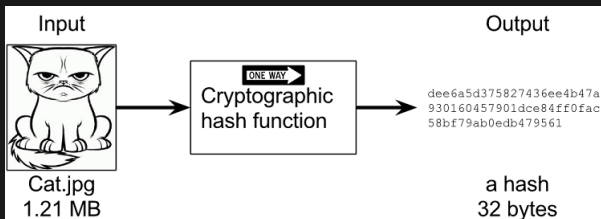
- 1 El libro contable es público (actualmente 743 GB).
- 2 Para actualizar el libro contable es necesario invertir energía (proof of work) y la actualización debe contener transacciones "válidas". Hacer trampa no es rentable pues la red no toma en cuenta actualizaciones (bloques) con transacciones inválidas.
- 3 Para asegurarse de que efectivamente todos poseen el mismo registro se "encadena" el bloque con el siguiente, de modo que toda modificación de un elemento de la cadena modifica el aspecto general del registro (cadena de *hashes*): **blockchain**.



FUNCIONES HASH CRIPTOGRÁFICAS

Son un elemento de las firmas digitales y de la prueba de trabajo.

- Es una función calculable mediante un algoritmo que tiene como entrada un archivo y lo convierte en una cadena fija y pequeña de bits.
- Barata: se calcula fácilmente. Compresión (digest). Uniforme (equi-probabilidad). Determinista (pseudo-aleatoria). No reversible.
- Sirven como identificadores de documentos, difícilmente corruptibles.



FUNCIONES HASH CRIPTOGRÁFICAS

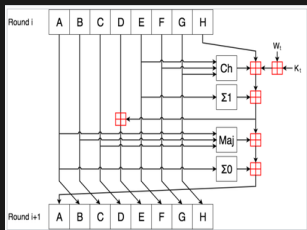


Figure: Wikipedia: SHA-2

Los componentes lila representan las siguientes operaciones:

$$\text{Ch}(E, F, G) = (E \wedge F) \oplus (\neg E \wedge G)$$

$$\text{Ma}(A, B, C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$

$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$

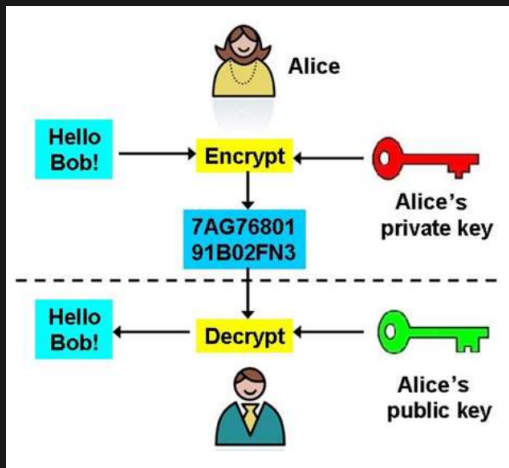
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

$\boxplus$ significa suma módulo 2^{32} .

FIRMA DIGITAL

- Cada usuario (A) genera una clave pública (PU-A) y una clave privada (PR-A).
- La clave privada sirve para encriptar mensajes. La clave pública sirve para desencriptarlos.
- Cada usuario envía su clave pública a aquellos con quien quiera comunicarse (en Bitcoin a toda la red).
- Alicia quiere enviar un mensaje M a otro usuario, o bien a toda la red. Encripta $m = \text{Enc}(M, \text{PR-A})$.
- El receptor puede leer el mensaje. Desencripta $M = \text{Des}(m, \text{PU-A})$, además sabe que proviene de A (firma digital).
- Para evitar suplantaciones debe ser imposible adivinar PR-A si conocemos PU-A.

FIRMA DIGITAL

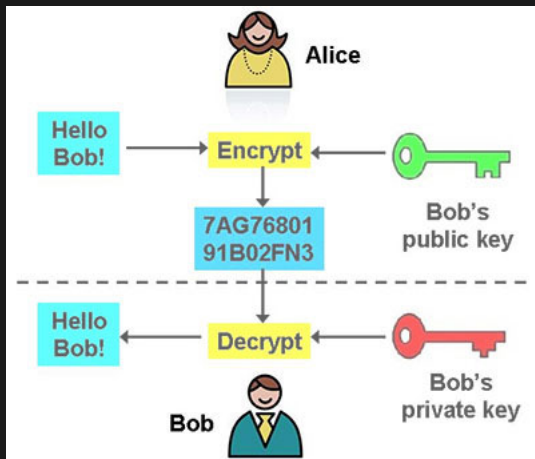


Se usa el Digital Signature Algorithm (DSA).

Criptografía de clave pública:

- Cada computadora (A) genera una clave pública (PU-A) y una clave privada (PR-A).
- La clave privada sirve para encriptar mensajes. La clave pública sirve para desencriptarlos.
- Cada usuario envía su clave pública a la red para que todas las computadoras en red la oigan.
- Alicia quiere enviar un mensaje M a Bob. Toma la clave pública de Bob y encripta $m = \text{Enc}(M, \text{PU-B})$.
- Envía el mensaje m a Bob por internet.
- Bob lee el mensaje y lo desencripta $\text{Des}(m, \text{PR-B}) = M$ usando su clave privada.
- Sólo Bob podrá desencriptar y leer ese mensaje.
- Para evitar ataques (hackers) debe ser casi imposible averiguar PR-B

CRIPTOGRAFÍA DE CLAVE PÚBLICA:



TRANSACCIONES

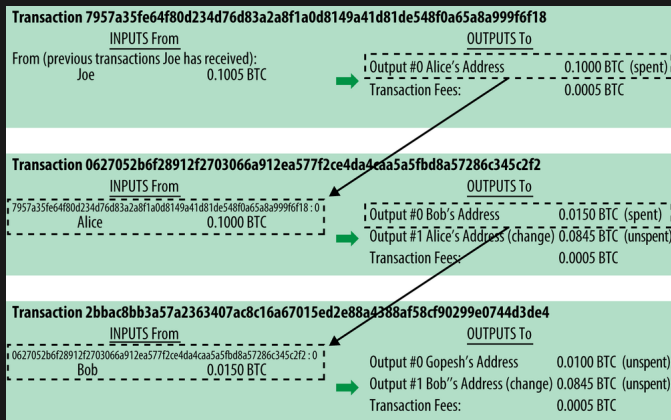


Figure: A. Antonopoulos, *Mastering Bitcoin*

MATEMÁTICAS

Criptografía: La criptografía ha servido, desde la antigüedad, para transmitir mensajes sin que puedan ser leídos, incluso si caen en manos del enemigo.

- Clave del César: desplazar el alfabeto k unidades
ABCDEFGHIJKLMNOPQRSTUVWXYZ
KLMNOPQRSTUVWXYZABCDEFGHIJ
- Alfabeto: $\mathbb{Z}_n = \{0, \dots, n-1\}$.
- Operación: $+$
- Clave: k
- Encriptación: $x \rightarrow x + k$
- Desencriptación: $x \rightarrow x - k$



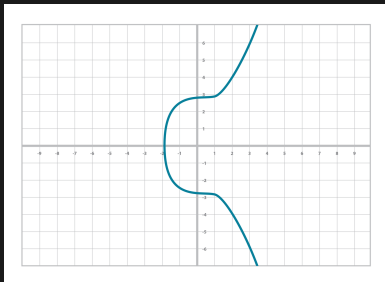
ARITMÉTICA MODULAR

- Aritmética del reloj: aritmética módulo 12, o módulo 24.
- $7 + 11 = 6 \pmod{12}$.
- Se puede restar, de hecho hay números negativos: $-1 = 11 \pmod{12}$.
- $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ tiene 12 elementos.
- $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ tiene n elementos.
- También hay producto: $7 \cdot 11 = 77 = 12 \cdot 6 + 5 = 5 \pmod{12}$

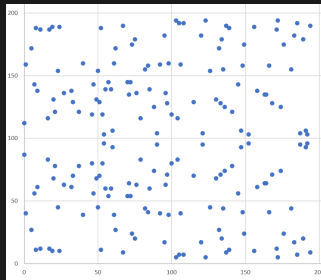


CURVAS ELÍPTICAS

- Curva elíptica: son las soluciones a la ecuación $y^2 = x^3 + ax + b$, con a, b enteros. Por ejemplo $y^2 = x^3 + 7$



(a) Soluciones en $\mathbb{R}$



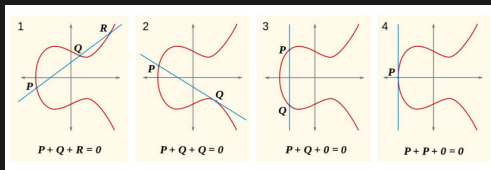
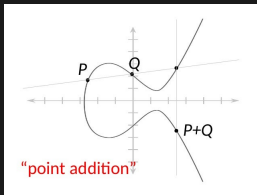
(b) Soluciones en $\mathbb{Z}_p$

Figure: J. Song, *Programming Bitcoin*

CURVAS ELÍPTICAS

- Hay una suma geométrica: Si P, Q son dos puntos en la curva, la recta que pasa por P y Q corta a la curva en un tercer punto $-R$. Sea R el punto simétrico. Se declara

$$P + Q = R$$



CRIPTOGRAFÍA DE CURVAS ELÍPTICAS

- Sean $P = (x_1, y_1)$, $Q = (x_2, y_2)$ y $R = P + Q = (x_3, y_3)$.
 - $x_3 = \lambda^2 - x_1 - x_2$
 - $y_3 = \lambda \cdot (x_1 - x_3) - y_1$
 - $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$
- Los puntos (x, y) de la curva con x, y en $\mathbb{Z}_p$ tienen la operación suma de puntos.
- $kP = P + P + \dots + P$ (k veces).
- Generación de claves:
 - Se elige una curva elíptica y un primo p . Se elige un punto base G en la curva.
 - El orden $n > 0$ es el mínimo que verifica $nG = 0$.
 - Clave privada: un número k entre 1 y $n - 1$
 - Clave pública: el punto $K = kG$.

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

- En Bitcoin se elige la curva elíptica

$$y^2 = x^3 + 7$$

- Sobre $\mathbb{Z}_p$, con el primo
 $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ (de 255 bits)
- Punto base $G = (g_x, g_y)$ con
 - $g_x = 55066263022277343669578718895168534326250603453777594175500187360389116729240$
 - $g_y = 32670510020758816978083085130507043184471273380659243275938904335757337482424$
- Clave privada: k , número de 256 bits, 32 bytes, 64 hex.
 - Se elige de forma aleatoria.
 - El número claves privadas es de 1.158×10^{77} poco menor que 2^{256} (hay 2^{270} átomos en el universo).
- Clave pública: se toma $kG = (x, y)$. Se concatena para formar $K = 04xy$, número de 520 bits, 65 bytes, 130 hex.

CLAVE PÚBLICA Y CLAVE PRIVADA

- Ejemplo: clave privada

$$k = 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD$$

- Clave pública es $K = kG$

$$K = 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD * G$$

- $K = (x, y)$

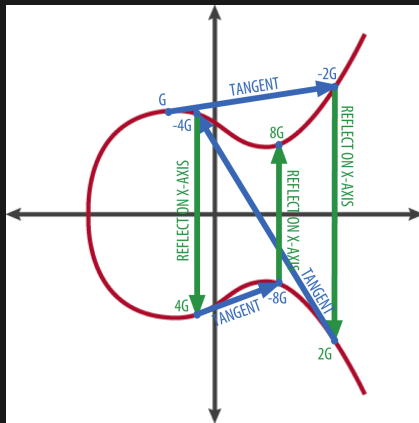
$$x = F028892BAD7ED57D2FB57BF33081D5CFCF6F9ED3D3D7F159C2E2FFF579DC341A$$

$$y = 07CF33DA18BD734C600B96A72BBC4749D5141C90EC8AC328AE52DDFE2E505BDB$$

- $K = 04F028892BAD7ED57D2FB57BF33081D5CFCF6F9ED3D3D7F159C2E2FFF579DC341A07CF33DA18BD734C600B96A72BBC4749D5141C90EC8AC328AE52DDFE2E505BDB$

CLAVE PÚBLICA

Para hacer el cálculo de $K = kG$, el algoritmo de exponenciación se traslada al algoritmo de duplicación (calcular $2G, 4G, 8G, 16G$, etc.)



VERIFICACIÓN DE FIRMAS: ÁLGEBRA DEL GRUPO

- **ECDSA:**

- Firma: (r, s) , mensaje m , hash $e = \text{SHA256}(m)$
- Verificar: $u_1G + u_2P = R$, donde:
 - $u_1 = e \cdot s^{-1} \mod n$, $u_2 = r \cdot s^{-1} \mod n$
 - R tiene $x = r \mod n$
- Usa suma de puntos y multiplicación escalar

- **Schnorr (BIP-340):**

- Firma: (R, s) , mensaje m , hash $e = H(R||P||m)$
- Verificar: $sG = R + eP$
 - R : punto, s : escalar, P : clave pública
- Linealidad: Simplifica y permite agregación
- **Grupo:** Abelian, orden $n \approx 2^{256}$, operaciones idénticas

COMPARACIÓN: ECDSA vs. SCHNORR

Aspecto	ECDSA	Schnorr (BIP-340)
Curva	secp256k1	secp256k1
Clave pública	(x, y) , 65 bytes (33 comprimida)	x , 32 bytes
Firma	(r, s) , ≈ 71 bytes	(R, s) , 64 bytes
Verificación	No lineal: $u_1G + u_2P = R$	Lineal: $sG = R + eP$
Agregación	No soportada	Soportada (multisig)
Uso	Legacy	Taproot (P2TR)

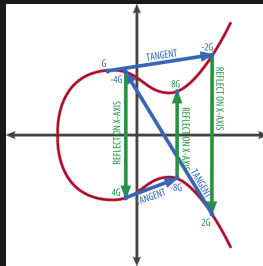
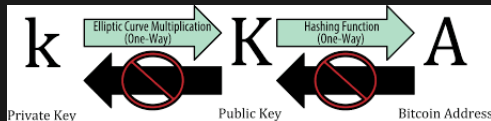


Figure: Operaciones en secp256k1

Bitcoin address

- La dirección Bitcoin de hecho es una forma comprimida de hasheado K .
- Dirección Bitcoin = RIPEMD160(SHA256(K)).



- RIPEMD160 (RACE Integrity Primitives Evaluation Message Digest) es una función HASH similar a SHA1 pero desarrollada por la comunidad académica. Tiene una salida de 160 bits (20 bytes, 40 hex).
- Para la mejor lectura humana, se usa el alfabeto (codificación) Base58Check, de 58 caracteres y con un código detector de errores.
- El alfabeto es 123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz (números, mayúsculas y minúsculas, quitando 0, O, l, I)

Transacción básica

- La transacción básica es:
 - Output: Bitcoin address (Public key hash)
 - Input (redeem): Public key + firma.

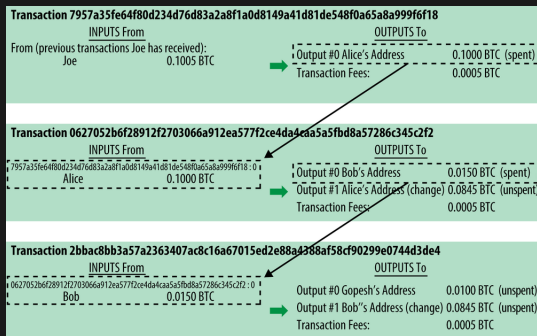
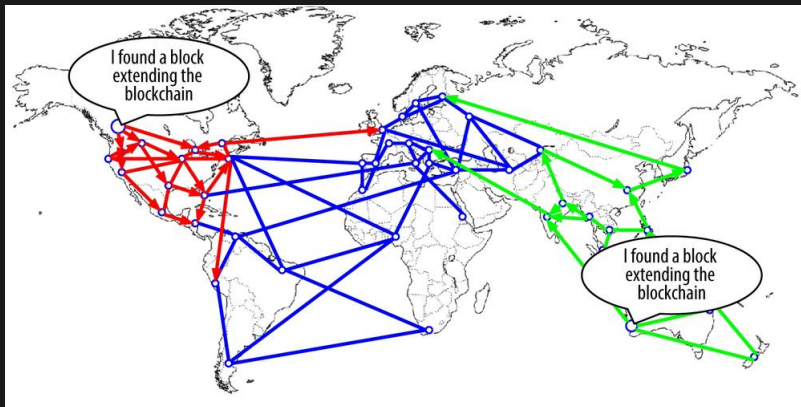


Figure: A. Antonopoulos, *Mastering Bitcoin*

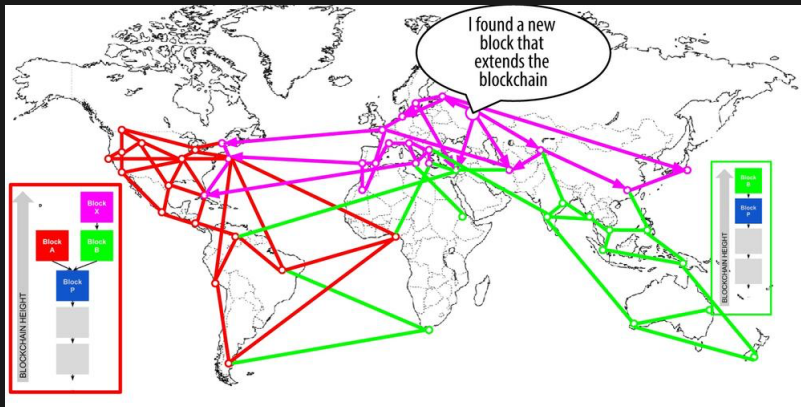
Blockchain

- Las nuevas transacciones flotan en la red y son recogidas por los mineros, para formar un nuevo bloque y añadirlo a la blockchain.
- El minero exitoso transmite el bloque a la red, y los demás lo copian a su blockchain.
- 10 minutos es el tiempo medio de distribución de una información enviada a la red, y que se distribuye nodo a nodo por internet.
- Es improbable que varios mineros encuentren un bloque a la vez o casi a la vez, si varios grupos de mineros se encuentran trabajando con cadenas distintas, produce un fork.

Resolviendo forks



Resolviendo forks



ALGUNAS REFERENCIAS

- ANDREAS ANTONOPOULOS, *Mastering Bitcoin*. O'Reilly Media (2017).
- SATOSHI NAKAMOTO, *Bitcoin: A Peer to Peer Electronic Cash System*. bitcoin.org (2009).
- RICARDO PEREZ-MARCO, *Bitcoin and Decentralized Trust Protocols*. Newsletter of the European Math. Soc., 100 p.32 (2016).
- JIMMY SONG, *Programming Bitcoin*. O'Reilly Media (2019).
- SAIFEDEAN AMMOUS, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* Wiley (2018).

¡Gracias!