Hash, Blockchain y Bitcoin

Antonio J. Di Scala

con la ayuda de Andrea Gangemi

Politecnico di Torino

https://crypto.polito.it/

Dedicada al recuerdo de Daniel Hernán Fuentes (⋆1962 - †2018)

Diciembre 2021

Abstract: Inicio contando de la criptografia en el Politecnico di Torino. Despues les explico que son las funciones de hash y dos modos de construirlas. Luego les hablare del primer bloque de la Bitcoin Blockchain, genesis Block, y del modo que Satoshi Nakamoto creo la Bitcoin Address 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. Durante la charla pienso crear algunas claves privadas/publicas de Bitcoin y ver su balance. En la parte final de la charla dare una breve explicacion de la idea de Blockchain, Proof of Work, el problema y la matematica involucrada en el asunto e.g. aritmetica modular, curvas elipticas.

Argomenti svolti:

1 Criptografia en el Politecnico di Torino (DISMA & DAUIN).

https://didattica.polito.it/laurea_magistrale/ingegneria_matematica/it/home
https://crypto.polito.it/
Que enseño?

-Criptografia & Criptoanalisis.

Objetivos? : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
-Criptografia Simetrica & Asimetrica

Ideas: Kerckhoffs principle, Shannon's approach/ideas, Computacionalmente infactible, IND , Probabilistic Encryption...

https://didattica.polito.it/pls/portal30/gap.pkg_guide.viewGap?p_cod_ins=03SOFNG&p_a_acc=2021&p_header=S

https://didattica.polito.it/pls/portal30/gap.pkg_guide.viewGap?p_cod_ins=03LPYOV&p_a_acc=2021&p_header=S&p_lang=IT

Era	Data	Dove	Evento/Persona
Pre Computer	∼ 2000 a.C.	Egitto	Geroglifici speciali
	∼ 625 a.C.	Bibbia, Geremia	Cifrario Atbash
	∼ 440 a.C.	Grecia	Scitala di Sparta
	∼ 150 a.C.	Grecia	Scacchiera di Polibio
	∼ 50 a.C.	Roma	Cifrario di Cesare
	∼ 850	Iraq	Al Kindi, analisi di frequenze
	1400	Europa	Nomenclator
	1466	Venezia	De Cifris, Leon B. Alberti
	1510	Venezia	Giovanni Soro, crittanalisi
	1518	Germania	Trithemius, Polygraphia
	1564	Brescia	Giovan B. Bellaso
	1586	Paris	Blaise de Vigenère
	1600	Paris	Antoine Rossignol
	1844	USA	Morse: Telegrafo elettrico
	1854/1863	Londra/Prussia	Charles Babbage / Friedrich Kasiski
	1883	Paris	Auguste Kerckhoffs
	1896	Londra	Marconi: Miglioramenti nella telegrafia
	∼ 1900	USA & Europa	Rotor Machines
	1919	USA	Vernam's OTP
	1920	USA	Friedman's IC
	1923	Germania	Enigma
	1928	Germania	Hilbert Entscheidungsproblem
	1935	England	Turing Machine
	1945	USA	Von Neumann Architecture
	1949	USA	Shannon's Perfect Secrecy
Computer	1951	USA	UNIVAC I: Primo Computer Commerciale
	1955	Italia	Inizia Olivetti ELEA
	1967	USA	Kahn's : The Codebreakers
	1969	USA	ARPANET
	1971	USA	Intel 4004: Primo microprocessore
	1975	USA	DES: Data Encryption Standard
	1976	USA	DH: New Directions in Cryptography
	1978	USA	RSA: Public-Key Cryptosystems
	1981	USA	MS-DOS
	1982	USA	GM: Probabilistic Public-Key Cryptosystems
	1991	CERN, Svizzera	www: World Wide Web
	1992	USA	Proof of Work
	1994	Europa	Smart Cards: EMV specifications
	1995	USA	Netscape IPO: "the web is for everyone"
	2001	USA	AES: Advanced Encryption Standard
	2007	Europa	Keccak: Permutations & Sponge
	2008		Blockchain & Bitcoin

2 Funciones Hash

Hash functions-such as MD5, SHA-1, SHA-256, SHA-3, and BLAKE2 -comprise the cryptographer's Swiss Army Knife: they are used in digital signatures, public-key encryption, integrity verification, message authentication, password protection, key agreement protocols, and many other cryptographic protocols.

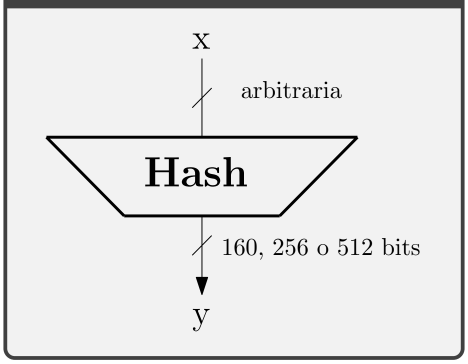
[Aumasson18, Chapter 6]

Una funzione **Hash** ha come dominio $\mathbb{Z}_2^*$ e come codominio $\mathbb{Z}_2^n$, dove di solito $n = 160, 256, 512$:

$$\textbf{Hash} : \mathbb{Z}_2^* \to \mathbb{Z}_2^n$$

dunque l'argomento x puo avere lunghezza arbitraria ma il valore $y = \textbf{Hash}(x)$, anche detto *digest, hash value, hash code* ha un numero finito di bits. Questo hash value è spesso pensato e usato come una "impronta digitale" del input x e.g.

Figura 2.0.1: Hash function



Una funzione **Hash** deve essere computazionalmente efficente e inoltre:

one-way
Collision Resistance
Second Preimage resistance or weak collision

https://en.wikipedia.org/wiki/SHA-2

https://en.wikipedia.org/wiki/RIPEMD

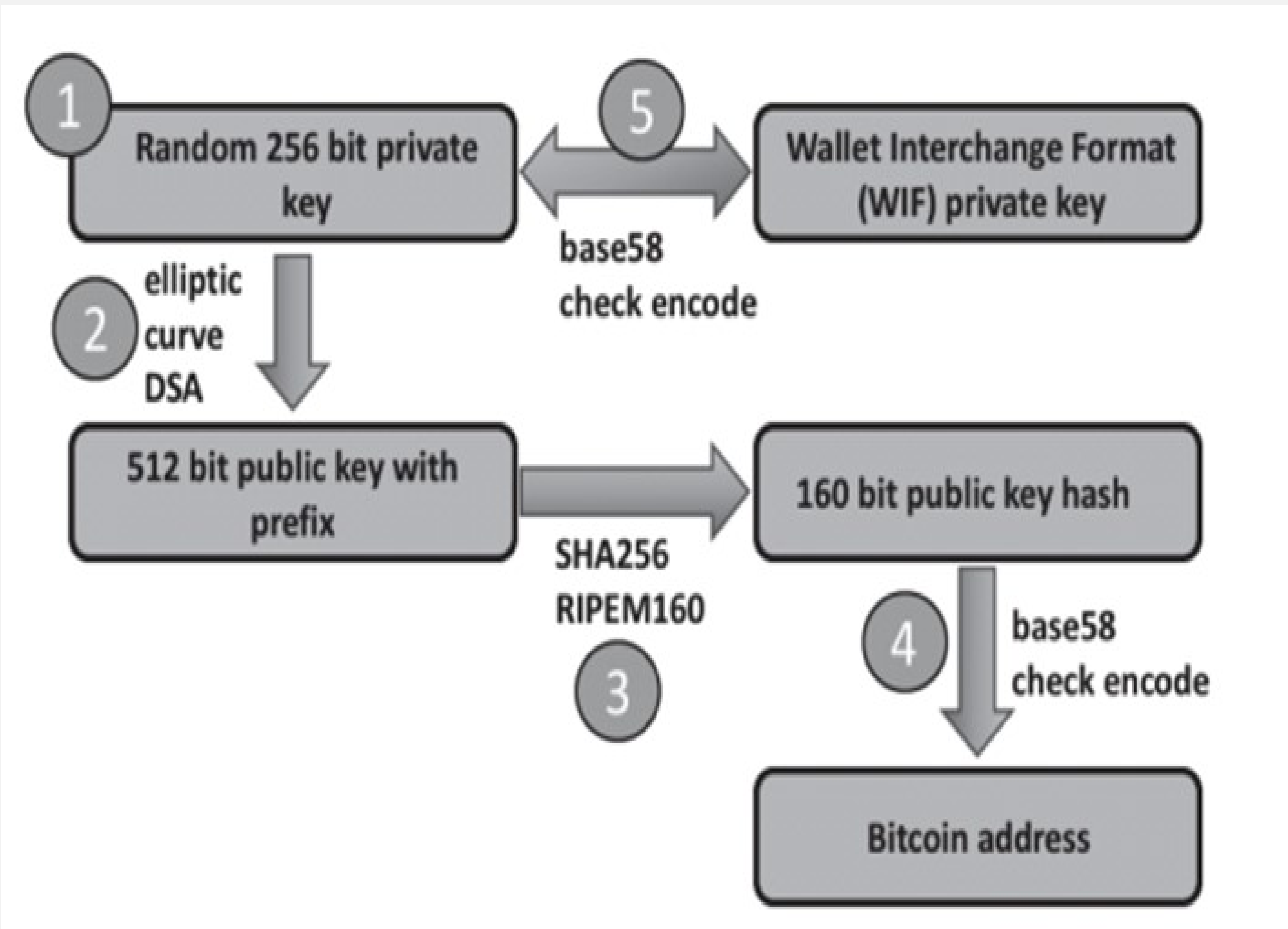
2.1 Construccion: Merkle-Damgård & Permutation-Sponge

3 Tener bitcoins ...

Tener bitcoins es tener la llave privada de un ”address” con balance positivo

Por ejemplo:
Bitcoin Address: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Bitcoin Address: 12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX

Figura 3.0.1: Private-Public-Address

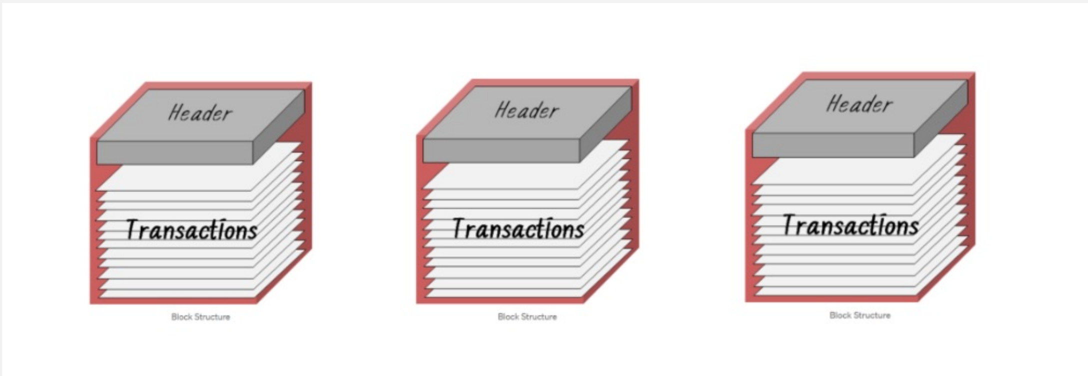


3.1 claves privadas/publicas de Bitcoin y ver su balance.

https://www.blockchain.com/explorer
https://btc.com/btc/block/0
https://en.bitcoin.it/wiki/Difficulty
https://btc.com/stats/diff

4 Blockchain

Figura 4.0.1: Block Chain



https://medium.com/@dongha.sohn/bitcoin-5-pool-merkle-root-272a9c83dec7
https://ldapwiki.com/wiki/Bitcoin%20network%20genesis%20block
https://chainquery.com/bitcoin-cli/getrawtransaction
https://chainquery.com/bitcoin-cli/getblock

4.1 Proof of Work (PoW)

https://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf
https://en.bitcoin.it/wiki/Nonce

5 Matematica

5.1 Aritmetica modular: Kuttaka & Teorema Chino del Resto

Figura 5.1.1: Aritmetica Modular

§IV.

Indeterminate equations of the first degree, to be solved in integers, must have occurred quite early in various cultures, either as puzzles (as exemplified by various epigrams in the Greek *Anthology*; cf. *Dioph.*, vol. II, pp. 43–72), or, more interestingly for the mathematician, as calendar problems. A typical problem of this kind may be formulated as a double congruence

$$x \equiv p \ (\text{mod } a), \ x \equiv q \ (\text{mod } b),$$

Protohistory 7

or as the linear congruence $ax \equiv m$ (mod b), or as an equation $ax - by = m$ in integers. The general method of solution for this is essentially identical with the "Euclidean algorithm" for finding the g.c.d. of a and b (*Eucl.*VII.2) or also (in modern terms) with the calculation of the continued fraction for a/b; the relation between the two problems is indeed so close that whoever knows how to solve the one can hardly fail to solve the other if the need for it arises. Nevertheless, if we leave China aside, the first explicit description of the general solution occurs in the mathematical portion of the Sanskrit astronomical work *Āryabhaṭīya*, of the fifth–sixth century A.D. (cf. e.g. Datta and Singh, *History of Hindu Mathematics*, Lahore 1938, vol. II, pp. 93–99). In later Sanskrit texts this became known as the *kuṭṭaka* (= "pulverizer") method; a fitting name, recalling to our mind Fermat's "infinite descent". As Indian astronomy of that period is largely based on Greek sources, one is tempted to ascribe the same origin to the *kuṭṭaka*, but of course proofs are lacking.

Then, in 1621, Bachet, blissfully unaware (of course) of his Indian predecessors, but also of the connection with the seventh book of Euclid, claimed the same method emphatically as his own in his comments on *Dioph.*IV.41_b (= IV, lemma to 36), announcing that it was to be published in a book of arithmetical "elements"; as this never appeared, he inserted it in the second edition of his *Problèmes plaisants et délectables* (Lyon 1624), which is where Fermat and Wallis found it; both of them, surely, knew their Euclid too well not to recognize the Euclidean algorithm there.

5.2 Isomorfismos Hard y Hard Homogeneous Spaces

5.3 Curvas Elipticas

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

https://graui.de/code/elliptic2/

Links:
https://github.com/Gangi94/BlockchainAddress

https://www.cabling-wireless.com/tecnologienews-dalla-macchina-di-babbage-alla-ethereum

[Aumasson18] Jean-Philippe Aumasson,
Serious Cryptography: A Practical Introduction to Modern Encryption,
No Starch Press, 2018.

[Co06] Couveignes J-M.
Hard Homogeneous Spaces,
https://eprint.iacr.org/2006/291.pdf

[DH76] Diffie, W.; Hellman, M.
New directions in cryptography,
(1976). IEEE Transactions on Information Theory. 22 (6): 644-654.

[Na08] Nakamoto, S.
Bitcoin: A Peer-to-Peer Electronic Cash System,
https://bitcoin.org/bitcoin.pdf (2008). https://satoshi.nakamotoinstitute.org/emails/cryptography/1/

[We84] Weil, A.
Number Theory, *An approach through history from Hammurapi to Legendre* ,
Birkhauser, Boston (2007).

Antonio J. Di Scala
Dipartimento di Scienze Matematiche, "G.L. Lagrange"
Politecnico di Torino,
Corso Duca degli Abruzzi 24, 10129 Torino, Italy.
antonio.discala@polito.it
https://crypto.polito.it/

Hash,Blockchain y Bitcoin

giovedì 16 dicembre 2021 10:05

Hash, Blockchain y Bitcoin

Antonio J. Di Scala

con la ayuda de Andrea Gangemi

Politecnico di Torino

https://crypto.polito.it/

Dedicada al recuerdo de Daniel Hernán Fuentes (⋆1962 - †2018)

Diciembre 2021

Abstract: Inicio contando de la criptografia en el Politecnico di Torino. Despues les explico que son las funciones de hash y dos modos de construirlas. Luego les hablare del primer bloque de la Bitcoin Blockchain, genesis Block, y del modo que Satoshi Nakamoto creo la Bitcoin Address 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. Durante la charla pienso crear algunas claves privadas/publicas de Bitcoin y ver su balance. En la parte final de la charla dare una breve explicacion de la idea de Blockchain, Proof of Work, el problema y la matematica involucrada en el asunto e.g. aritmetica modular, curvas elipticas.

-Criptografia Simetrica & Asimetrica + CRIPTOANALISIS

Ideas: Kerckhoffs principle, Shannon's approach/ideas, Computacionalmente infactible, IND , Probabilistic Encryption...

claves

(Gen , Enc , Dec)

K

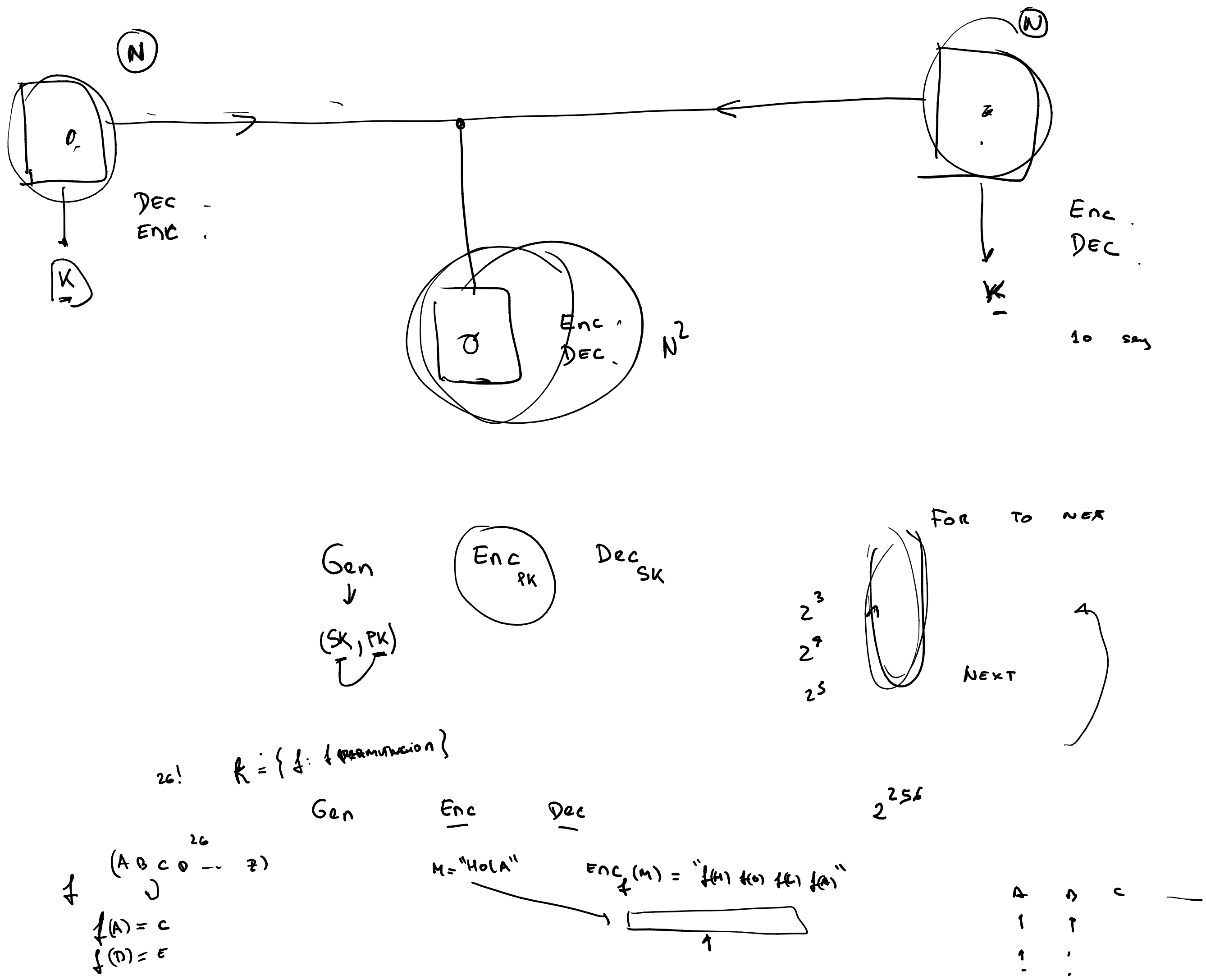
$Enc_K(M) = C$

M

$Dec_K(C) = M$

"(M,C)"

MERKLE



2 Funciones Hash

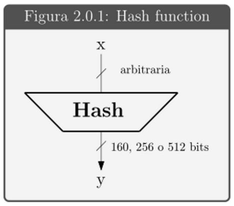
> Hash functions-such as MD5, SHA-1, SHA-256, SHA-3, and BLAKE2 -comprise the cryptographer's Swiss Army Knife: they are used in digital signatures, public-key encryption, integrity verification, message authentication, password protection, key agreement protocols, and many other cryptographic protocols.
>
> [Aumasson18, Chapter 6]

Una **funzione Hash** ha come dominio $\mathbb{Z}_2^*$ e come codominio $\mathbb{Z}_2^n$, dove di solito $n = 160, 256, 512$:

$$\textbf{Hash} : \mathbb{Z}_2^* \to \mathbb{Z}_2^n$$

dunque l'argomento x puo avere lunghezza arbitraria ma il valore $y = \textbf{Hash}(x)$, anche detto *digest*, *hash value*, *hash code* ha un numero finito di bits. Questo hash value è spesso pensato e usato come una "impronta digitale" del input x e.g.

Figura 2.0.1: Hash function



one-way

Collision Resistance

Second Preimage resistance or weak collision

Second Preimage resistance or weak collision

Hash $(x_0) = Y_0$

Hash $(x_1) = Y_0$

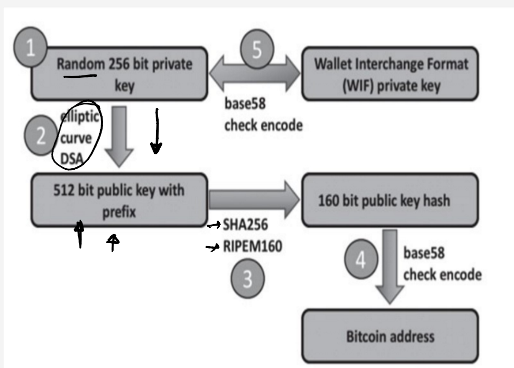
3 Tener bitcoins ...

Tener bitcoins es tener la llave privada de un "address" con balance positivo

Por ejemplo:
Bitcoin Address: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Bitcoin Address: 12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX

$0 \leq N < 2^{256}$

Figura 3.0.1: Private-Public-Address



$g \in G \quad + \;, \times$

$N \quad N \cdot g = g + \cdots + g$

clave Publica

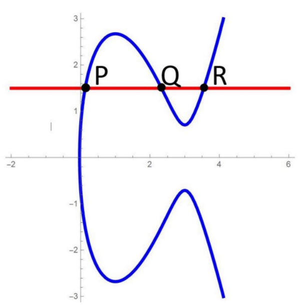
$(\mathbb{Z}, +)$

$\mathbb{Z} \xrightarrow{f} G$

$N \longrightarrow N \cdot g$

$\mathbb{Z}/N_0\mathbb{Z} \overset{f}{\cong} \langle g \rangle$

f one way



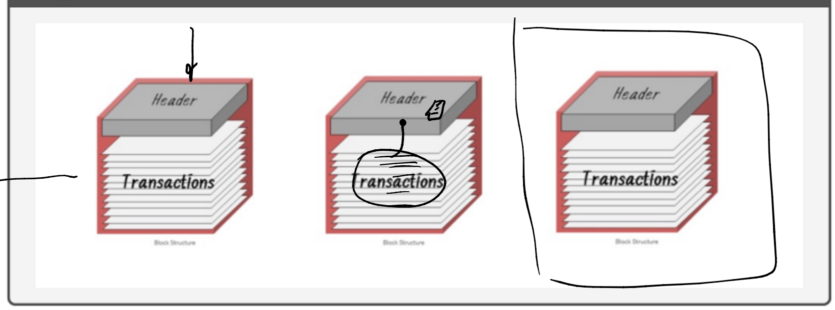
P+Q+R=0

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

"ARITMETICA MODULAR"

$x, y \in \mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$

Figura 4.0.1: Block Chain

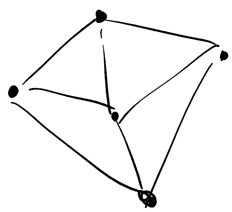


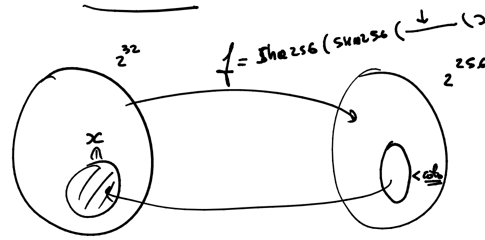
SHA256(SHA256(Header [32 bits])) = < Numero

000 ··· 0

Proof of Work

Bitcoin Red C Red Internet





10 minutos

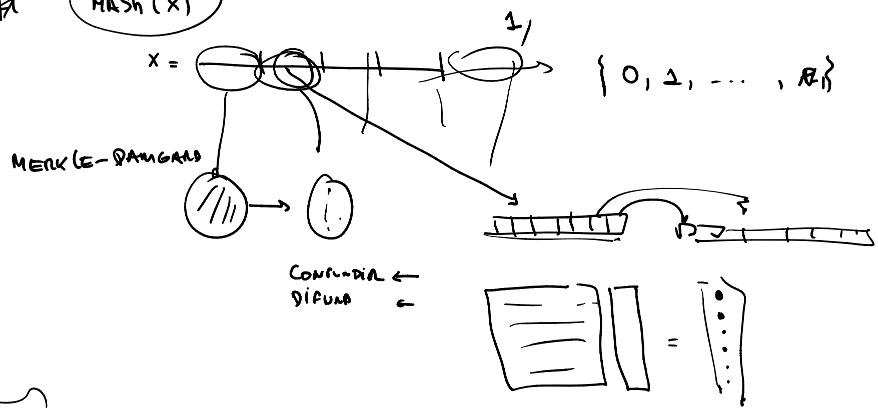
ℤ ℚ ℕ ℝ ℂ

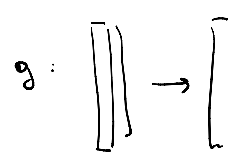
$a x + b = 0$

$a \cdot x = 1$ N

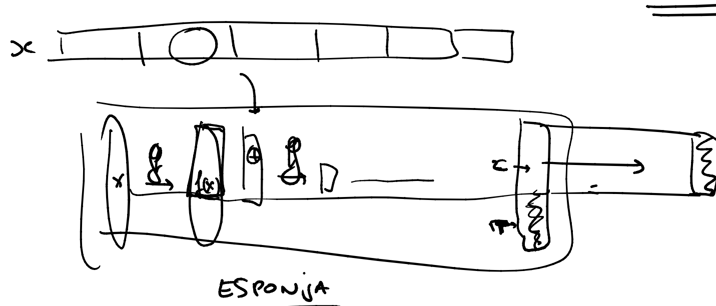
$a \cdot x$ < N

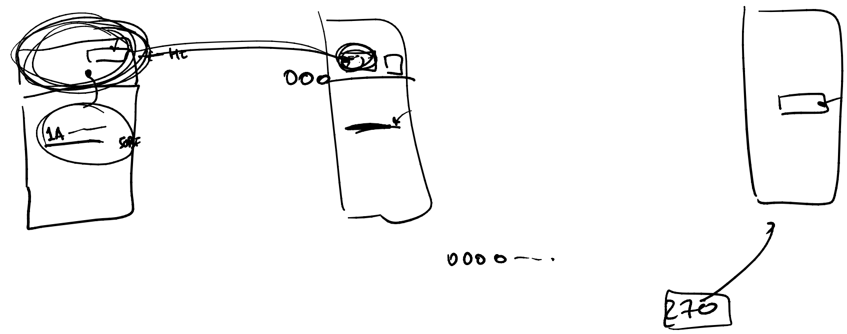
HASH(x)





KECCAK





0000 ...

$$y^2 = x^3 + ax + b$$

$$G = \langle g \rangle^*$$

$$\mathbb{Z}_N \xrightarrow{f} \langle g \rangle$$

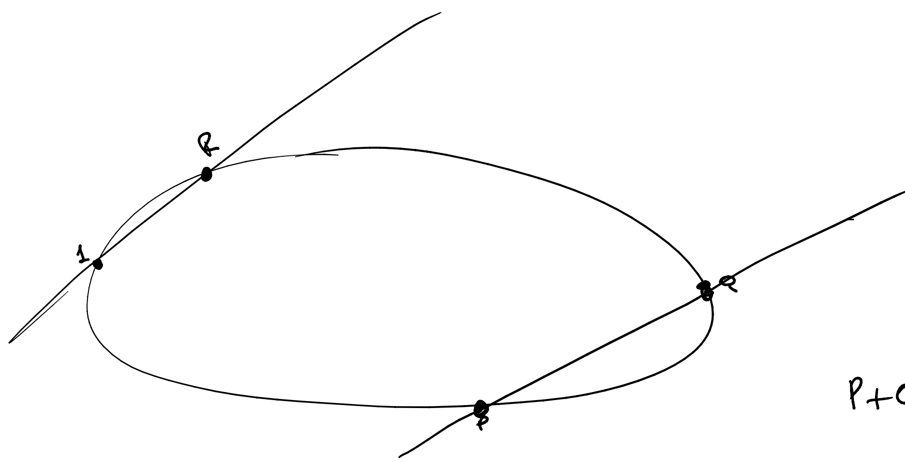
$$n \longrightarrow g^n = \underbrace{g \cdot \ldots \cdot g}_{n}$$

$$f^{-1}$$

Koblitz

≈ 85

Miller



$$P + Q = R$$

Cliente — Servidore