Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Blockchain – the technology

mquiroga@cyte.co
mquiroga@uniandes.edu.co
m@cypherpunks.co

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Representación y transferencia de valor

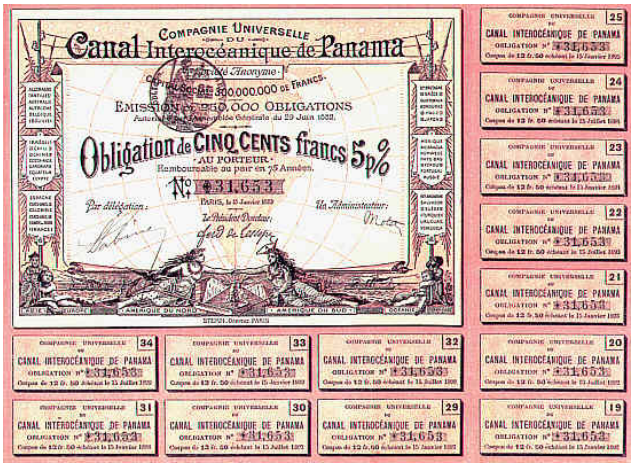
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Representación y transferencia de valor



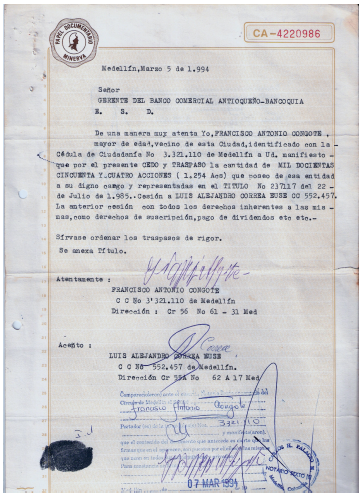
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Representación y transferencia de valor



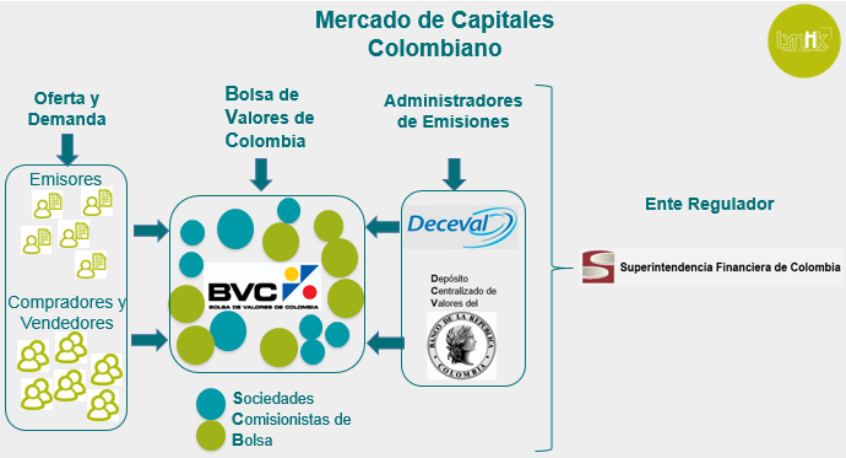
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Depósito Centralizado de Valores



1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Depósito Distribuido de Valores

- No Double-Spend:
- Immutability:
- Neutrality:
- Authorization:
- Auditability:
- Accounting:
- Non-expiration:
- Integrity:
- Transaction Atomicity:
- Discrete (Indivisible) Units of Value:
- Quorum of Control:
- Timelock/Aging:
- Replication:
- Forgery Protection:
- Consistency:
- Predictable Issuance:

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Funciones de hashing

- Sea una función *hashing* que tome un texto de tamaño arbitrario y encuentre un *digest* de tamaño fijo, tal que:
  - Dado M, sea sencillo calcular $h(M)$,
  - Dado $h(M)$, es computacionalmente imposible encontrar M,
  - Es computacionalmente imposible encontrar dos mensajes M_1 y M_2, tal que $h(M_1)=h(M_2)$,
  - Dado M_1 es computacionalmente imposible encontrar otro mensaje M_2, tal que $M_1 \neq M_2$ y $h(M_1)=h(M_2)$.

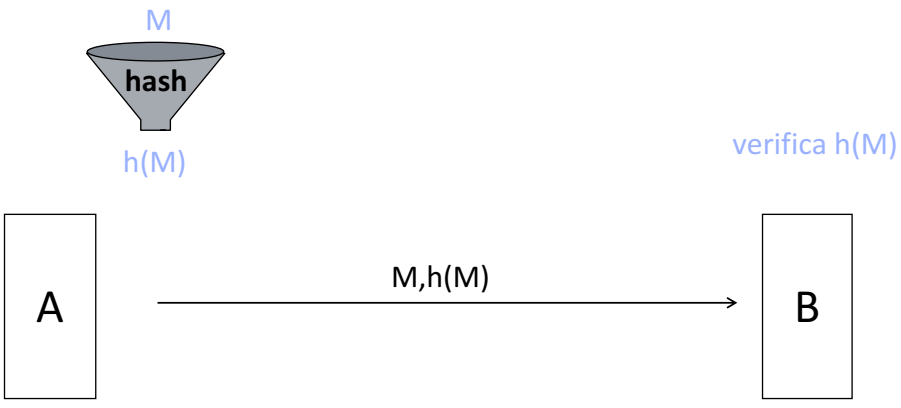
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Funciones de hashing



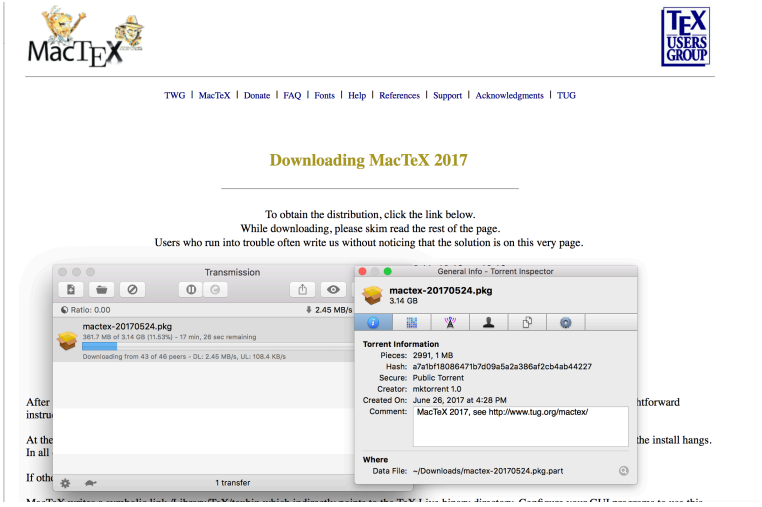
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Usos…



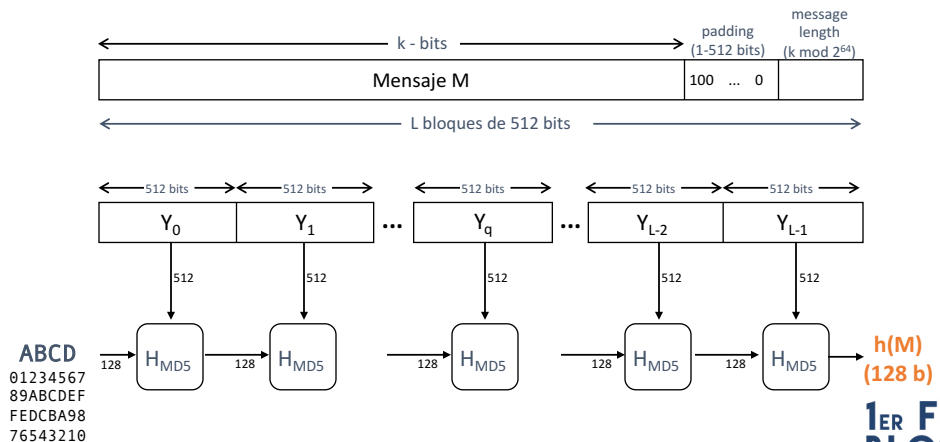
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Funciones de hashing (MD5)



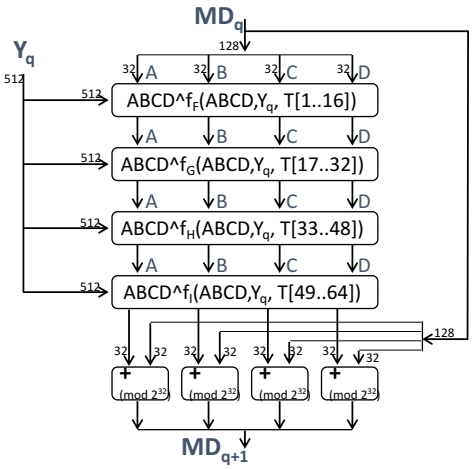
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Funciones de hashing (MD5 – un bloque)



T[1..16]: $\sin\left(0, \frac{\pi}{2}\right)$

T[17..32]: $\sin\left(\frac{\pi}{2}, \pi\right)$

T[33..48]: $\sin\left(\pi, \frac{3\pi}{2}\right)$

T[49..64]: $\sin\left(\frac{3\pi}{2}, 2\pi\right)$

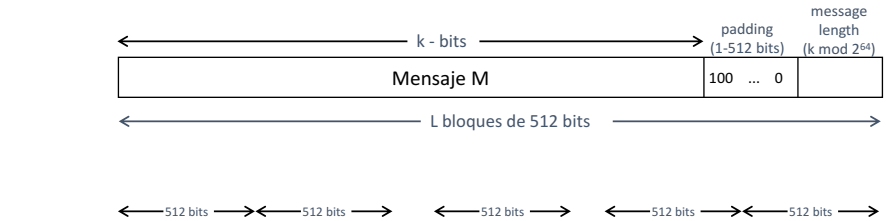
1ER FORO DE BLOCKCHAIN

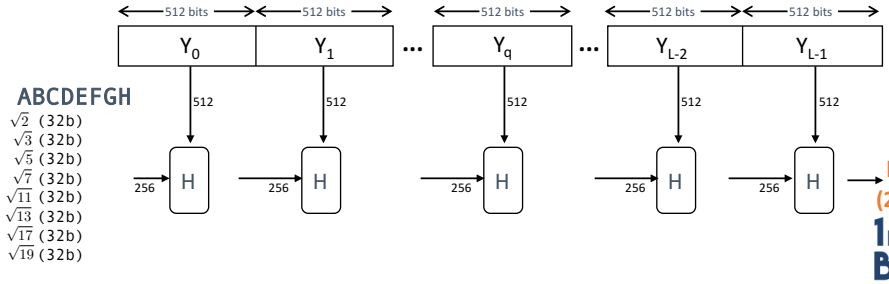
Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Funciones de hashing (SHA-256)





ABCDEFGH
$\sqrt{2}$ (32b)
$\sqrt{3}$ (32b)
$\sqrt{5}$ (32b)
$\sqrt{7}$ (32b)
$\sqrt{11}$ (32b)
$\sqrt{13}$ (32b)
$\sqrt{17}$ (32b)
$\sqrt{19}$ (32b)

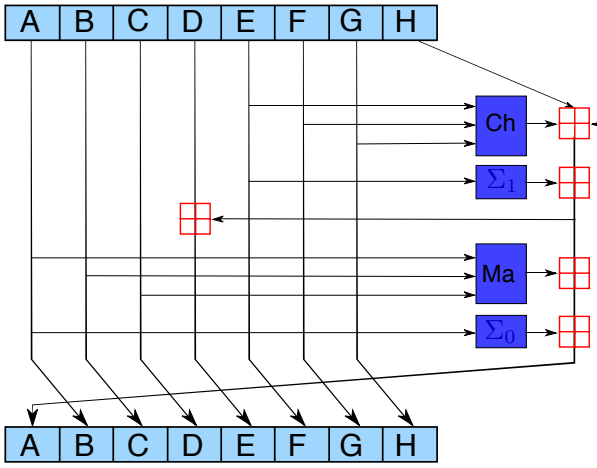
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Funciones de hashing (SHA-256 – un bloque)



W_t 64 words of 32b

K_t 64 words of 32b $\sqrt[3]{2}, \quad \sqrt[3]{2}, \quad \ldots \sqrt[3]{311}$

$\boxtimes$: Addition modulo 2^{32}

$$Ch(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$$
$$Ma(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$
$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Funciones de hashing (árboles de Merkle)

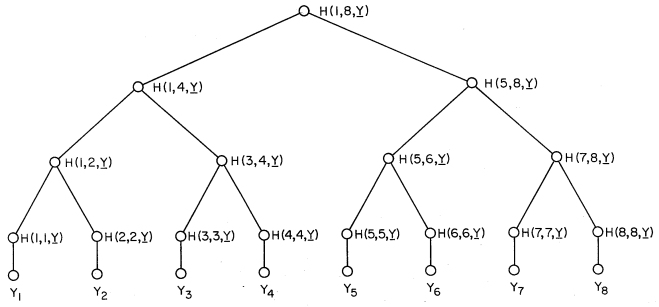


FIG__1

U.S. Patent Jan. 5, 1982 4,309,569

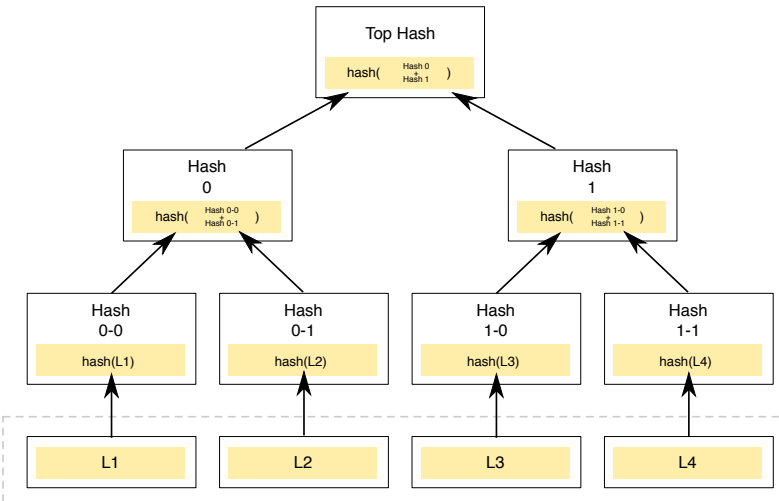
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Funciones de hashing (árboles de Merkle)



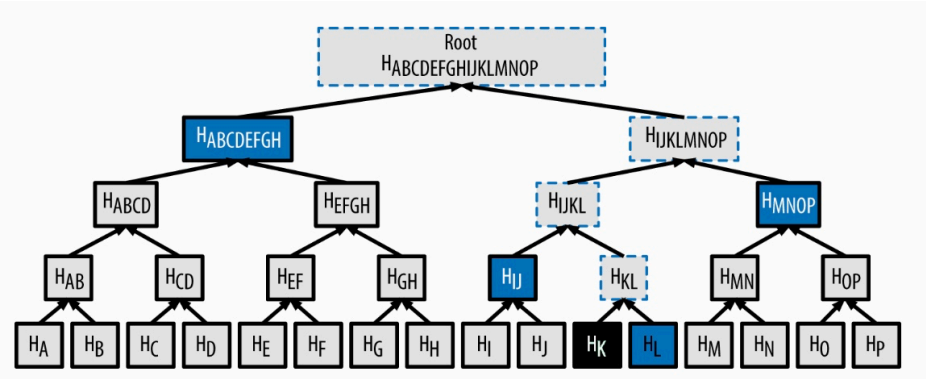
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Funciones de hashing (árboles de Merkle)



Para mostrar que la transacción K está en el bloque, basta con mostrar un "Merkle path" de sólo 4 hashes de 32b (128 bits total)

$$\log_2 N$$

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

•DISEÑADOR GRÁFICO• •OFREZCOME, precios bajos,• •trabajos profesionales estéti-• •cos, 3008385257, 4634950.• •CL25648984

¿E5CF2 016b7 65696 714b7 cb2be b528c 0e299 187db 2dfdc 51669 b435b d26c02bca? 95cc7b7412a552ab14ed51c2763 8fabb6f0d63554866b3f6e3e83 b74c42f094f.com m@cipher-punks.co 3208309045 CL88124

•ENTRENADOR personaliza-• •do, OFREZCOME, entrena-•

FONISTA, sin experiencia. 2553954, 3108093708. serviciodetalento@hotmail.com CL25647024

AUXILIAR CONTABLE ADMINISTRATIVA EXPERIENCIA, HELISA, LABORAL, OFFICE, REFERENCIAS COMPROBABLES. ZONA NORTE. HOJA VIDA FOTO decoracion14@gmail.com CL25649337

AUXILIAR CONTABLE CON EXPERIENCIA, vincula-

ASEADORAS TODEROS PRESA DE PROPIEDAD ho tal, para edificios, 2877668. gestiohumana@incolpro CL25649004

ASEADORES PERSONAL FEMENINO oficios varios, hoja de 10-03 Calle 128 No. 4 2582326. CL2564935

OFICIOS VARIOS, Hombr ven BACHILLER, conocimi sistemas, Carrera 28 No. 63A- CL25648809

OFICIOS VARIOS MU CHO 18 a 23 AÑOS 361

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Proof of Work

- ¿Cómo le muestro a un interlocutor que he hecho algún esfuerzo?
- *M* = “Muchos años después, frente al pelotón de fusilamiento, el Coronel Aureliano Buendía había de recordar aquella tarde remota en que su padre lo llevó a conocer el hielo. Macondo era entonces una aldea de *nonce* casas de barro y cañabrava...”

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Proof of Work (.)

- h("Muchos años después, … Macondo era entonces una aldea de 241,848 casas de barro y cañabrava...")= 00000044194edf481fd55eba5c4a59fe09d31b7b6606526dd302b2db170b7ee6 — 25 bits (hasta 2^{25}=33'554,432 intentos)
- h("Muchos años después, … Macondo era entonces una aldea de 57'589,887 casas de barro y cañabrava...")= 000000368a10eb45f6a13eb44051909afe21b82843f29da747e0615751824591 — 26 bits (hasta 2^{26}=67'108,864 intentos)
- h("Muchos años después, … Macondo era entonces una aldea de 110'533,342 casas de barro y cañabrava...")= 0000001f7748ebe95ef5b9fea53df335f6b6f1192d2e9e4c50284fc3b6d2a31d — 27 bits (hasta 2^{27}=134'217,728 intentos)
- h("Muchos años después, … Macondo era entonces una aldea de 229'136,723 casas de barro y cañabrava...")= 000000072dbfb118b0bd850ee62f5fdde09465ebedd9db427c7ff3f7ffbce38b — 28 bits (hasta 2^{28}=268'435,456 intentos)

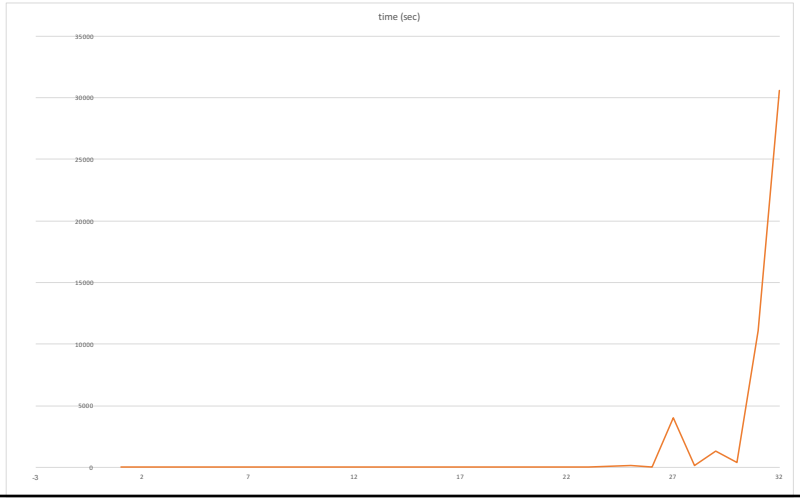
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Proof of Work (..)



31 bits en 30,566.5 seg = 8.49 horas

173.4 Kh/s

1ER FORO DE BLOCKCHAIN

Universidad de los Andes Facultad de Ingeniería | FOROS ISIS | Departamento de Ingeniería de Sistemas y Computación

Proof of Work (...)

- Es un esquema intrínsecamente asimétrico:
- Difícil cumplir la "*proof-of-work*"
  - Para encontrar un hash de 28 bits en cero utilicé como nonce 229'136,723
    - A falta de mejor estrategia hay que calcular 229'136,723 hashs
- Para verificar la "*proof-of-work*" sólo necesito ____ hashs

1ER FORO DE BLOCKCHAIN

Universidad de los Andes Facultad de Ingeniería | FOROS ISIS | Departamento de Ingeniería de Sistemas y Computación

Block-chain en Bitcoin

Con las renuncias y descargas legales de responsabilidad del caso…

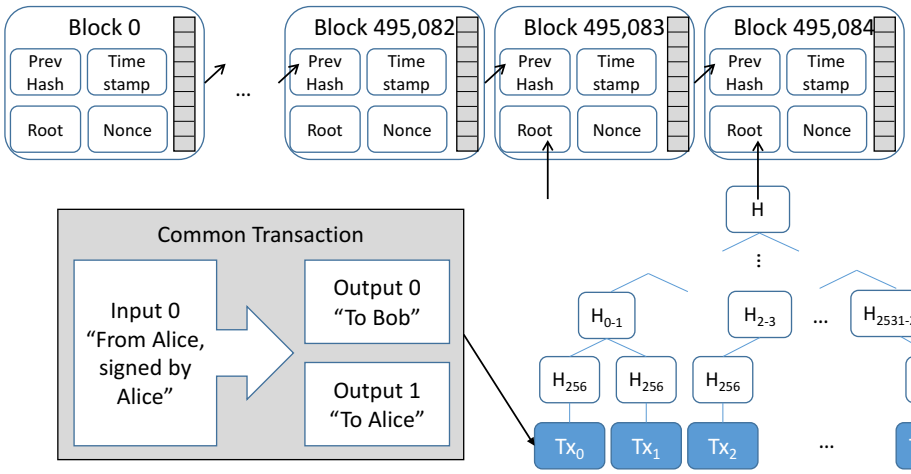
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

La block-chain bitcoin



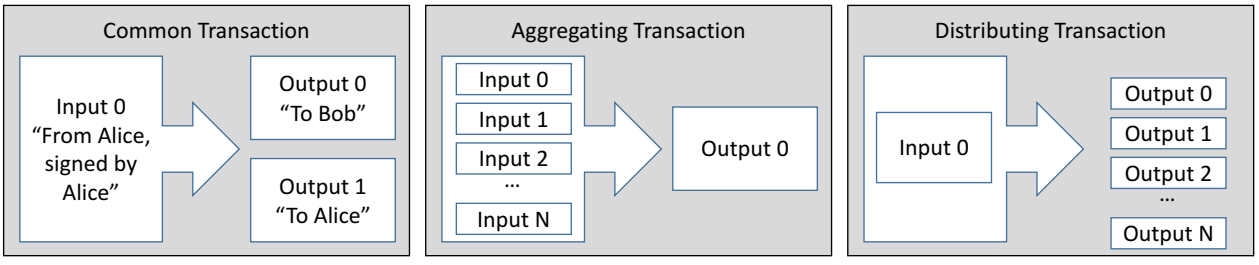
1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Types of transactions



1ER FORO DE BLOCKCHAIN

Universidad de los Andes Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

La block-chain bitcoin

- Viernes 23 de noviembre:
  - 495,804 bloques
    - Aproximadamente 2,400 transacciones por bloque
      - ~12 hashs en el árbol de Merkle
    - Aproximadamente 1.06 MBytes por bloque
  - 10,457 nodos
    - Más de 10,000 copias de la block-chain repartidas por todo el mundo
  - Código contribuido por ~ 400 programadores
    - Open-source, licencia MIT
- Sólo agregar
  - NO es una base de datos
  - Inmutable…

1ER FORO DE BLOCKCHAIN

Universidad de los Andes Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

v.g. el bloque 495,084

- Hash:
  00000000000000000401a0cd2e174d86ce94bbe5fdd0f1174fc3806c528f888
  18*4+1=73 bits (hasta 2^{73}=9.44x10^{21} intentos)
  = 1,726 millones de años
- Merkle root:
  811d7629f39cdd518aafa8bcc9e691857422e1b8b6a59e630d10427870742842
- Nonce: 2,233’172,667
- Block reward: 12.5 BTC
- Transaction fees: 2.20732412 BTC
- Number of transactions: 2532
- Previous block:
  00000000000000000001669c9903c7ee0db739d1f7f58c8454b02a8e7120d5c4

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

La block-chain bitcoin

- Es un esquema intrínsecamente asimétrico:
  - Difícil cumplir la "*proof-of-work*"
  - Alterar la block-chain requiere re-calcular varias "*proof-of-work*"
    - Sólo se puede agregar
      - Imposible de modificar
    - Hay más de 10,000 copias de la block-chain repartidas por todo el mundo
      - Completamente fault-tolerant
  - Cada nuevo bloque "apilado" hace más difícil revertir / alterar una transacción
    - Cada nuevo bloque es un "voto"
    - Incluye una estampilla de tiempo
  - *"A distributed ledger used by bitcoin for recording payments into a currency"*

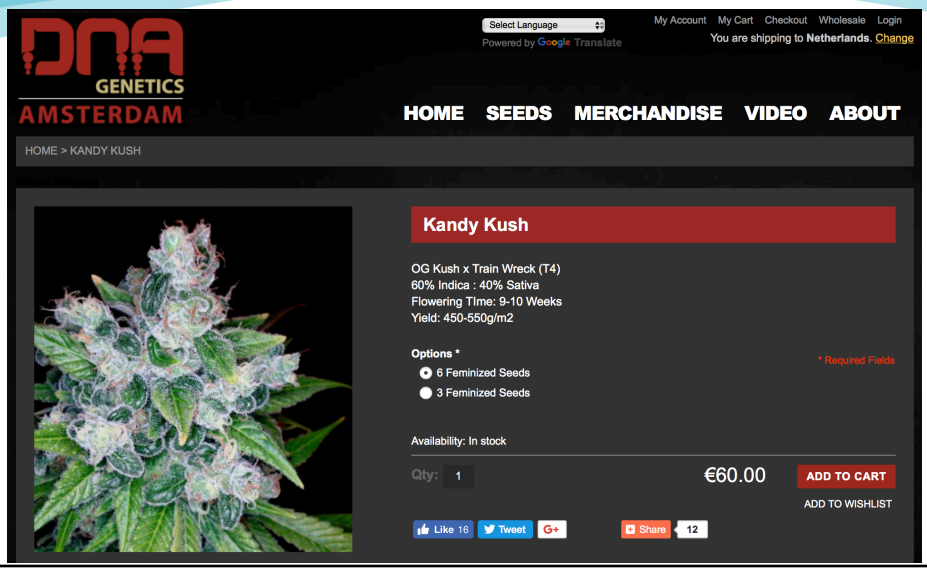
- La transacción `08654f9dc9d673b3527b48ad06ab1b199ad47b61fd54033af30c2ee975c588bd` contiene un enlace a un "número primo ilegal"

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación



1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

DEMOCRACY ON A BLOCKCHAIN

Brazil may write new laws with data stored on the ethereum blockchain

How to collect and verify signatures from 145 million voters across a landmass larger than the mainland United States?

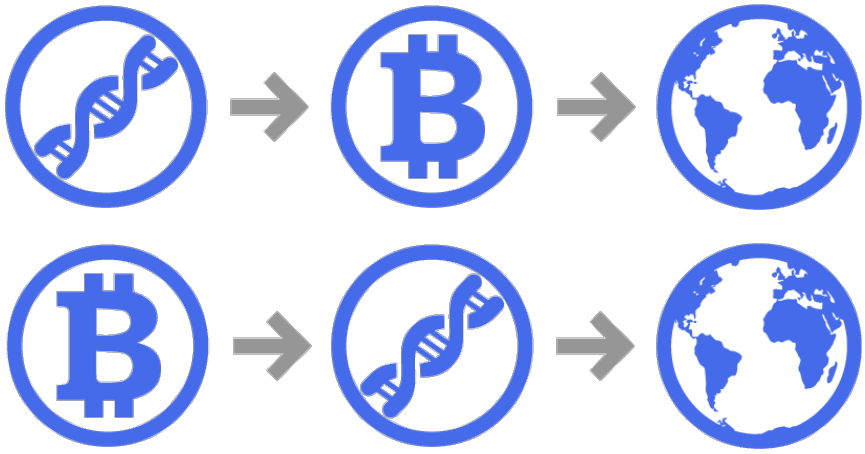
https://qz.com/1163660/brazil-may-write-new-laws-based-on-data-stored-on-the-ethereum-blockchain/

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación



The record for storage of non-living DNA is now 700,000 years

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

AntMiner S7	AntMiner S9	Avalon6
		
Advertised Capacity: 4.73 Th/s	**Advertised Capacity:** 13.5 Th/s	**Advertised Capacity:** 3.5 Th/s
Power Efficiency: 0.25 W/Gh	**Power Efficiency:** 0.098 W/Gh	**Power Efficiency:** 0.29 W/Gh
Weight: 8.8 pounds	**Weight:** 8.1 pounds	**Weight:** 9.5 pounds
Guide: Yes	**Guide:** Yes	**Guide:** No
Price: $479.95	**Price:** $1,987.95	**Price:** $499.95
Buy from amazon.com	Buy from amazon.com	Buy from amazon.com
Appx. BTC Earned Per Month: 0.1645	**Appx. BTC Earned Per Month:** 0.3603	**Appx. BTC Earned Per Month:** 0.1232

~ US$142= / Th/s

This macbook pro: 173.42 Kh/s

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

https://qz.com/1055126/photos-china-has-one-of-worlds-largest-bitcoin-mines/
https://qz.com/1026605/photos-chinas-bitcoin-mines-and-miners/

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

https://qz.com/1055126/photos-china-has-one-of-worlds-largest-bitcoin-mines/
https://qz.com/1026605/photos-chinas-bitcoin-mines-and-miners/

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

https://qz.com/1055126/photos-china-has-one-of-worlds-largest-bitcoin-mines/
https://qz.com/1026605/photos-chinas-bitcoin-mines-and-miners/

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

https://qz.com/1055126/photos-china-has-one-of-worlds-largest-bitcoin-mines/
https://qz.com/1026605/photos-chinas-bitcoin-mines-and-miners/

1ER FORO DE BLOCKCHAIN

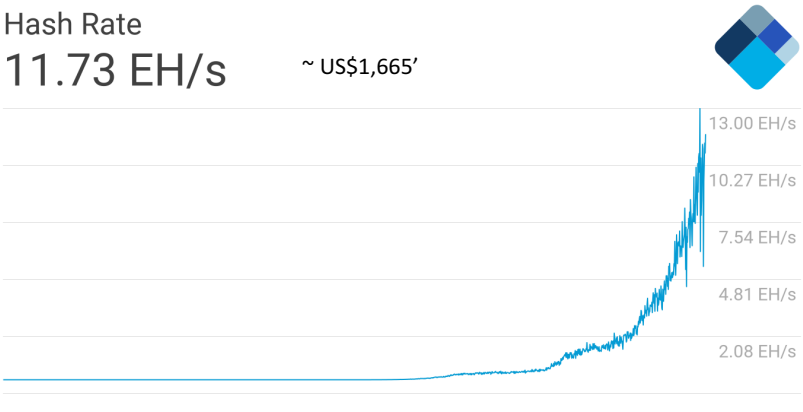
Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Hash Rate

11.73 EH/s ~ US$1,665'



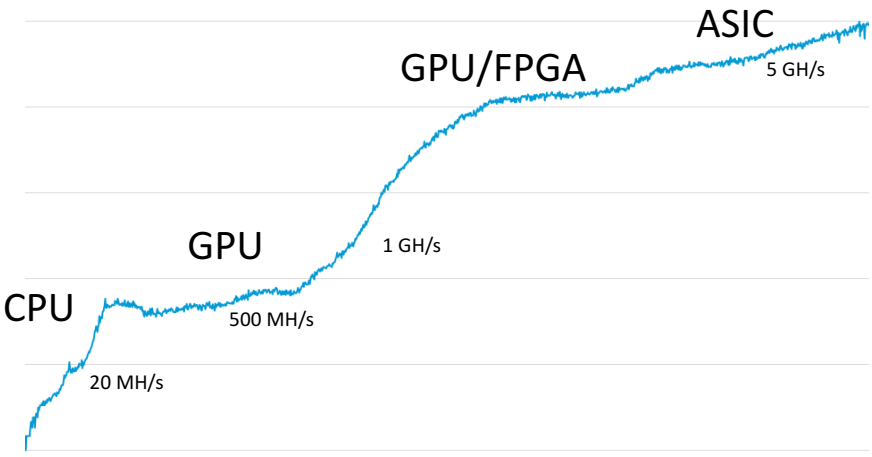
Exa: $1000^6 = 10^{18}$

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación



Escala logarítmica (https://blockchain.info/charts/hash-rate?timespan=all&scale=1)

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

Realidad del mining en Colombia

- Codensa: Valor Unitario kWh Col$454.07
- El hardware consume 1375 watts (1.3 kW), 31.2 kWh / día o 936 kWh/mes o Col$425,009.52
  - Solo es rentable con un precio de Col$30= kWh
  - Y con economías de escala en compra de hardware

- Mining is not minting

1ER FORO DE BLOCKCHAIN

Universidad de los Andes
Facultad de Ingeniería

FOROS ISIS

Departamento de Ingeniería de Sistemas y Computación

A futuro…

- Funciones de hashing intensivas en memoria
  - No ASIC
- ZKP (v.g. zerocash)

1ER FORO DE BLOCKCHAIN