eman ta zabal zazu

Universidad del País Vasco | Euskal Herriko Unibertsitatea

GASTEIZKO INGENIARITZA ESKOLA

ESCUELA DE INGENIERÍA DE VITORIA-GASTEIZ

X Jornada de Seguridad y Protección de Datos de Carácter Personal

Escuela de Ingeniería de Vitoria-Gasteiz – UPV/EHU

Tecnología *Blockchain*

Fundamentos criptográficos

Denis Ionut Stefanescu – GIIGSI

dstefanescu001@ikasle.ehu.eus

Ismael Etxeberria Agiriano – LSI

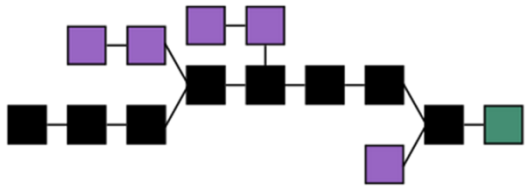
ismael.etxeberria@ehu.eus

31 de octubre de 2018

¿Qué es el bitcoin?

- Una criptomoneda, criptodivisa o **moneda digital**
  - Es un conjunto de anotaciones contables
  - Medio digital de intercambio
- La primera criptodivisa en operar
  - Desde el 3 de enero de 2009
  - Bitcoin, bitcóin, bitcoines, BTC
- Un protocolo
- Una red peer-to-peer (P2P)

¿Qué es una blockchain?



- Una blockchain, **cadena de bloques** o cadena articulada
  - Base de datos distribuida
  - Mecanismos para evitar la modificación de un dato publicado
  - Sellado temporal confiable y enlazando a un bloque anterior
  - Almacenar de forma creciente datos ordenados en el tiempo
- Aspectos relevantes
  - Almacenamiento de datos mediante replicación
  - Transmisión de datos mediante peer-to-peer
  - Confirmación de datos mediante un proceso de **consenso**
    - El tipo de algoritmo más utilizado es el de PoW **prueba de trabajo** en el que hay un proceso abierto competitivo y transparente de validación de las nuevas entradas llamada **minería**

¿Hay otras criptomonedas?

– A la sombra de bitcoin surgen otras monedas criptográficas

https://criptotendencia.com/2017/10/01/7-criptomonedas-para-invertir-en-octubre/

¿De dónde surge el bitcoin?

- En 2008, **Satoshi Nakamoto** publicó un artículo en la lista de criptografía de metzdowd.com

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

¿Quién creó el bitcoin?

- Satoshi Nakamoto

Satoshi Nakamoto goes public and denies he's bitcoin founder
https://www.youtube.com/watch?v=BoboO6QPGow

¿Quién creó el bitcoin (II)?

- El empresario australiano Craig Wright fue identificado públicamente como el creador del bitcoin Satoshi Nakamoto en diciembre de 2015
- La NSA afirma conocer quién es el multimillonario más elusivo del mundo (con un valor de más de 7B$ en noviembre de 2017) utilizando técnicas de **estilometría**

https://medium.com/cryptomuse/how-the-nsa-caught-satoshi-nakamoto-868affcef595

¿Qué es el bitcoin (II)?

- No es dinero fiduciario (fiat) como el dólar o el euro
  - Utiliza un sistema de Prueba de Trabajo (PoW)
- No tiene referentes de confianza
  - La criptografía desempeña ese papel
- No requiere permisos
  - Nadie puede impedir la participación en la red
- Permutable
  - Cada unidad es cambiable
- Por diseño la cantidad de unidades nunca podrá exceder los 21 millones de bitcoins
  - Ya se han extraído 16,7 millones
  - Se extraen actualmente a un ritmo de 25 bitcoins cada diez minutos

¿Qué es el bitcoin (III)?

- Es de código abierto
  - El código fuente de Bitcoin es accesible para todos
- Es descentralizado
  - No pertenece a ningún estado
  - Puede utilizarse libremente en todo el mundo
- Programable
  - Bitcoin Core proporciona una API en JSON-RPC para acceder a la red Bitcoin
- Pseudoanónimo – privacidad
  - No se requiere identificación para participar en la red bitcoin
  - Podemos realizar transacciones a través de la red Tor

¿Qué es el bitcoin (IV)?

- Es inviable su falsificación o duplicación gracias a un sofisticado sistema criptográfico
- Las transacciones son irreversibles
  - Todo el mundo conoce las transacciones que se realizan
- El dinero te pertenece al 100%
  - No puede ser intervenido por nadie ni las cuentas pueden ser congeladas

¿Qué aportan otras criptodivisas?

- *Ethereum* ofrece los llamados contratos inteligentes (*smart contracts*)
  - Tienen capacidad de cumplirse automáticamente una vez que las partes han acordado los términos
  - Como los contratos de papel son acuerdos en los que dos o más partes se comprometen a cumplir una serie de condiciones
    - El consentimiento voluntario
    - El objeto del contrato (bien o servicio)
    - Una causa justa, verdadera y lícita
  - Difieren en tres factores
    - El modo de escritura
    - Su implicación legal
    - El modo de cumplimiento

Fundamentos de criptografía

- Criptografía asimétrica
- Función trampa
- Función de resumen digital o *hash*
- Codificación base 64
- Codificación base 58

Criptografía asimétrica

- Dos claves: una pública y otra privada
  - Lo que se cifra con la **pública** puede ser descifrado con la **privada**
  - Lo que se cifra con la **privada** puede ser descifrado con la **pública**
- ECDSA. *Elliptic Curve Digital Signature Algorithm*
  - Emplea operaciones sobre puntos de curvas elípticas
  - Claves privadas de 256 bits
- DSA. *Digital Signature Algorithm*
  - Emplea exponenciaciones que (problema del logaritmo discreto)

Criptografía asimétrica

$Kr = C(M, r)$

$M = D(Kr, u)$

$Ku = C(M, u)$

$M = D(Ku, r)$

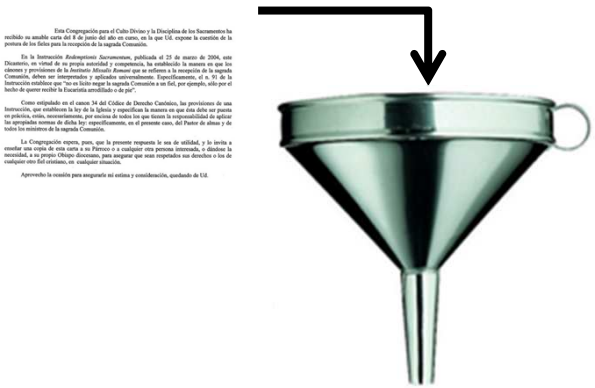
Función trampa

- Función matemática cuyo cálculo directo es sencillo, pero el cálculo de su función inversa es muy complejo
  - Involucra un elevado número (exponencial) de operaciones
- Ejemplo: factorización
  - Dados dos números primos (**p**, **q**) obtener **m = p·q**
  - Dado **m** la complejidad de obtener **(p, q)** es exponencial
  - Si **m** tiene 100 dígitos decimales se necesitan del orden de 10^{50} operaciones para factorizar m
  - Un ordenador convencional que realice 1.000.000 pruebas por segundo tardaría del orden de 10^{36} años de media

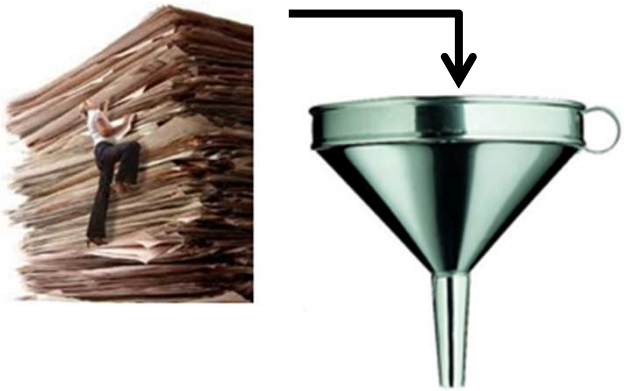
https://es.wikipedia.org/wiki/Funci%C3%B3n_trampa

Función de resumen digital o hash

- Reciben de entrada una cadena de longitud arbitraria
  - Puede ser muy corta o muy larga
  - Cambiando **un bit** cambia del orden de la mitad del resultado
- Devuelven una cadena de longitud fija
- Sirve como representación compacta del original



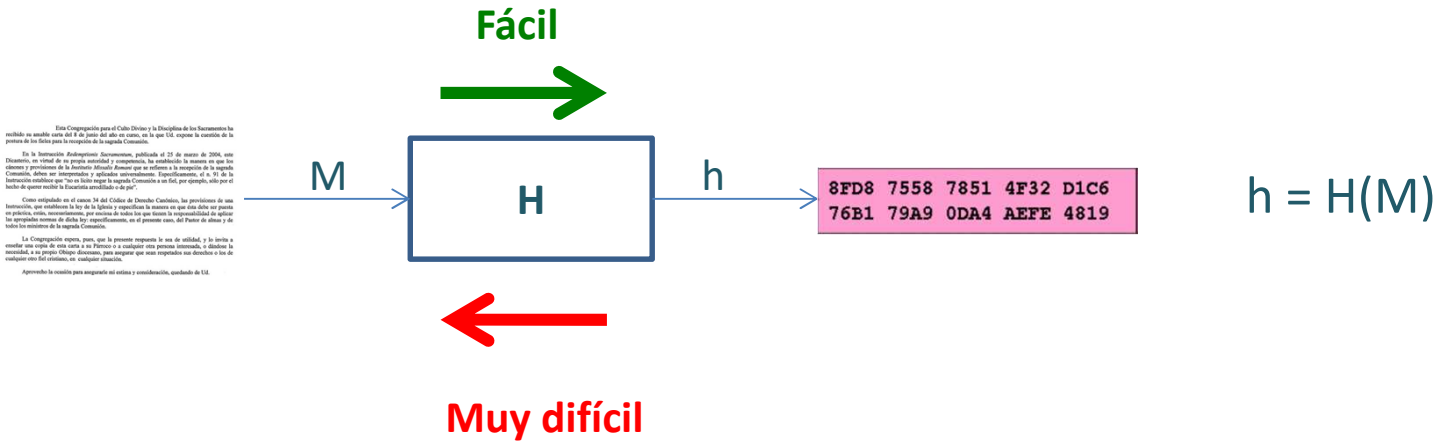
3b93cf8f1f095708d720fc5fe976eda4d38ee3d



b3b93cf8f1f095708d720fc5fe976eda4d38ee3d

Función de resumen digital o hash

- Suponen una función trampa



Codificación base 64

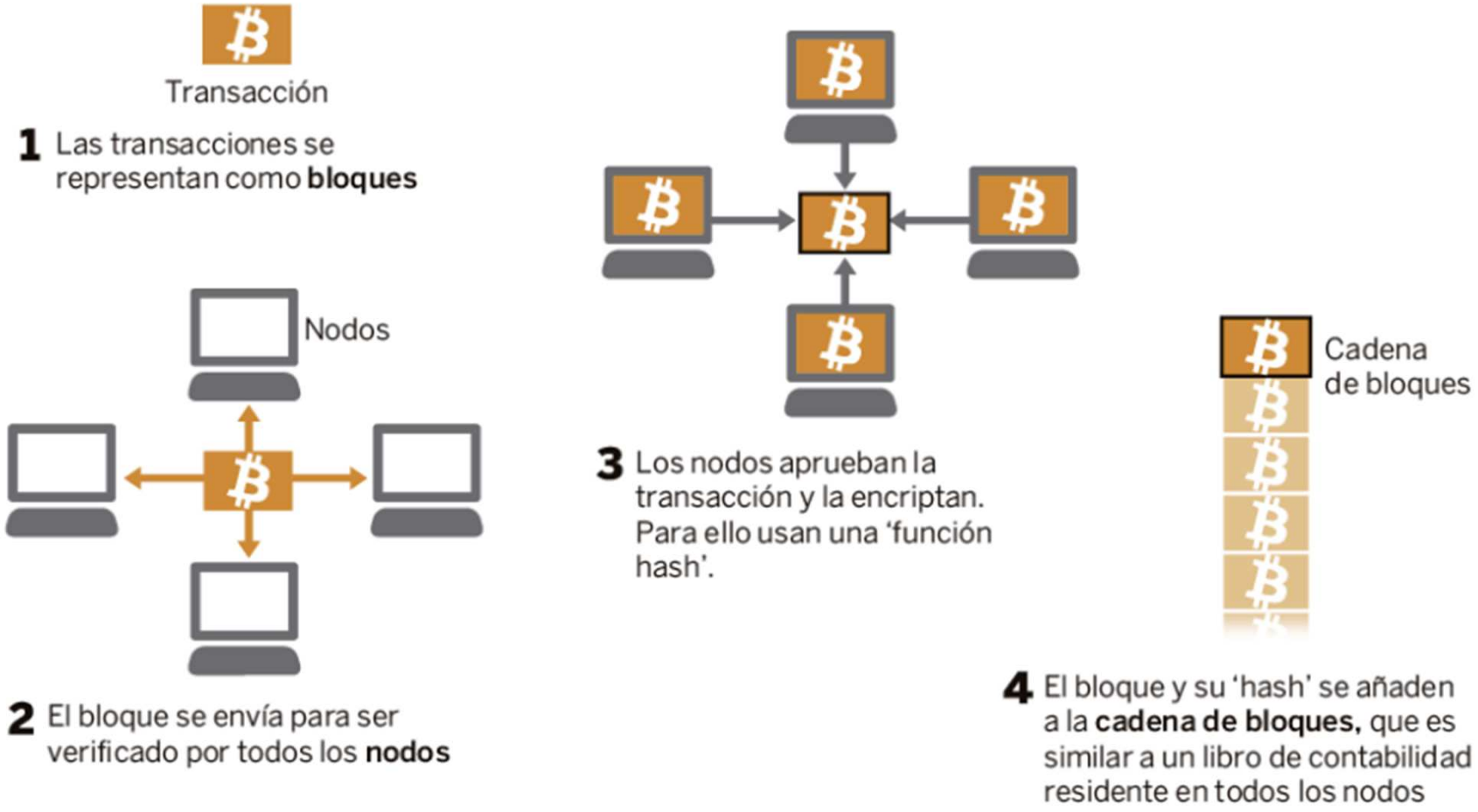
- Es una codificación de binario a texto que utiliza 64 dígitos (e.g. A-Z, a-z, 0-9 y +/) más uno de relleno (=)
- Permiten expresar números binarios de 6 bits

Codificación base 58

- Codificación para representar enteros largos
- Parecida a la base64 pero se ha modificado para eliminar caracteres no alfanuméricos y letras que pueden presentar ambigüedades al ser impresas
  - Caracteres eliminados: **0** (cero), **O** (o mayúscula), **I** (i mayúscula), **l** (L minúscula), **+** (más) y **/** (barra oblicua)

Decimal	Base58	Decimal	Base58	Decimal	Base58
0	1	20	M	40	h
1	2	21	N	41	i
2	3	22	P	42	j
3	4	23	Q	43	k
4	5	24	R	44	m
5	6	25	S	45	n
6	7	26	T	46	o
7	8	27	U	47	p
8	9	28	V	48	q
9	A	29	W	49	r
10	B	30	X	50	s
11	C	31	Y	51	t
12	D	32	Z	52	u
13	E	33	a	53	v
14	F	34	b	54	w
15	G	35	c	55	x
16	H	36	d	56	y
17	J	37	e	57	z
18	K	38	f		
19	L	39	g		

¿Cómo funciona bitcoin? Esquema general



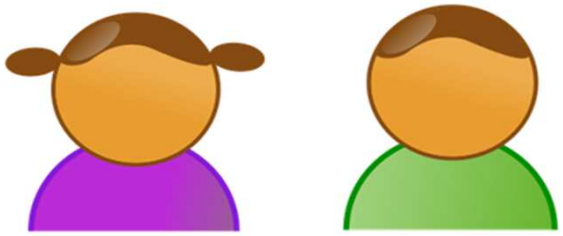
https://elpais.com/elpais/2017/11/24/media/1511547361_942588.html

¿Cómo funciona bitcoin? Monedero

- Para formar parte en la red bitcoin necesitamos una cartera o monedero de bitcoins (***wallet***)
  - Almacena toda la información necesaria para funcionar con bitcoins
  - Es el lugar virtual donde se guardan los bitcoins
  - En ella se guardan nuestras credenciales
  - En realidad contiene una colección de claves criptográficas con las que operar (públicas y privadas)

¿Cómo funciona bitcoin? Transacciones

- En el nivel más sencillo están las **transacciones**
  - Registran cambios atómicos del estado del sistema
- Todos/as conocen las transacciones de todos/as
- Cuando Alice quiere enviar 5,00 BTC a Bob simplemente difunde un mensaje:



Alice → Bob 5,00 BTC

- Todo el mundo recibe la notificación, actualiza su libro contable y transmite el mensaje

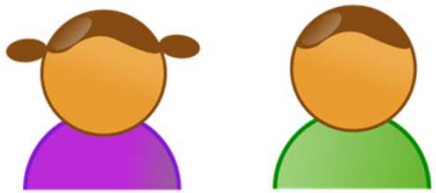
¿Cómo funciona? Libro contable distribuido

Libro contable			
Alice	฿19,467747723	Mallory	฿0,080031204
Bob	฿0,065536569	Oscar	฿0,709811526
Carlos	฿0,747131887	Pat	฿0,631617514
Carol	฿0,704195108	Peggy	฿0,888410385
Charlie	฿63,840082960	Sally	฿0,907425022
Chuck	฿0,454028458	Sam	฿20,089719008
Craig	฿0,326928742	Sybil	฿0,900167076
Dan	฿0,106105719	Trent	฿0,903675908
Dave	฿0,338227092	Trudy	฿0,601323693
Erin	฿0,129582161	Vanna	฿0,522074165
Eva	฿12,927510827	Víctor	฿0,111363242
Faythe	฿0,581819273	Walter	฿0,083730309
Frank	฿0,691601458	Wendy	฿0,217015319
Mallet	฿0,681967717		

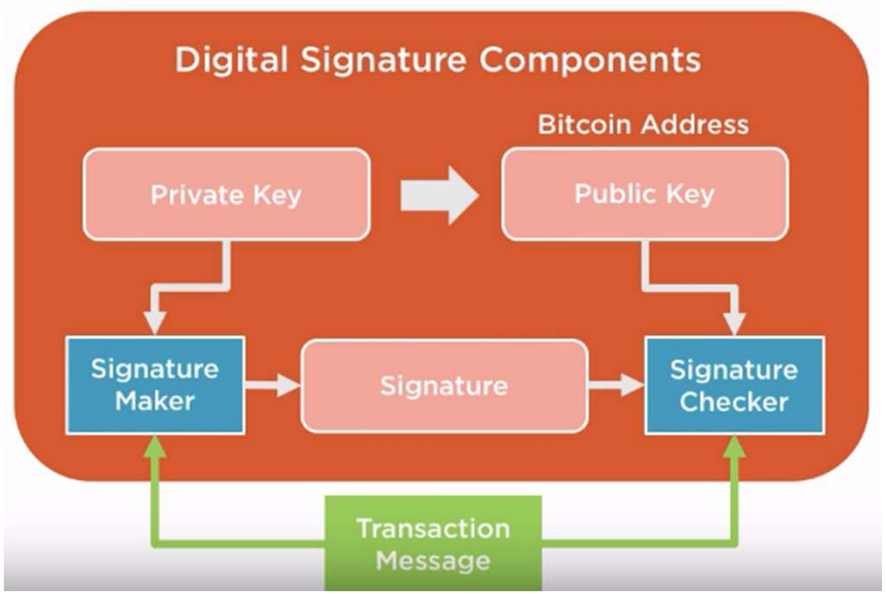
- Todo el mundo recibe la notificación, actualiza su libro contable y transmite el mensaje

¿Cómo sabemos que es Alice la que efectúa el pago?

- La transacción se firma con la clave privada de Alice
- Todo el mundo sabe su clave pública y puede/debe comprobarlo



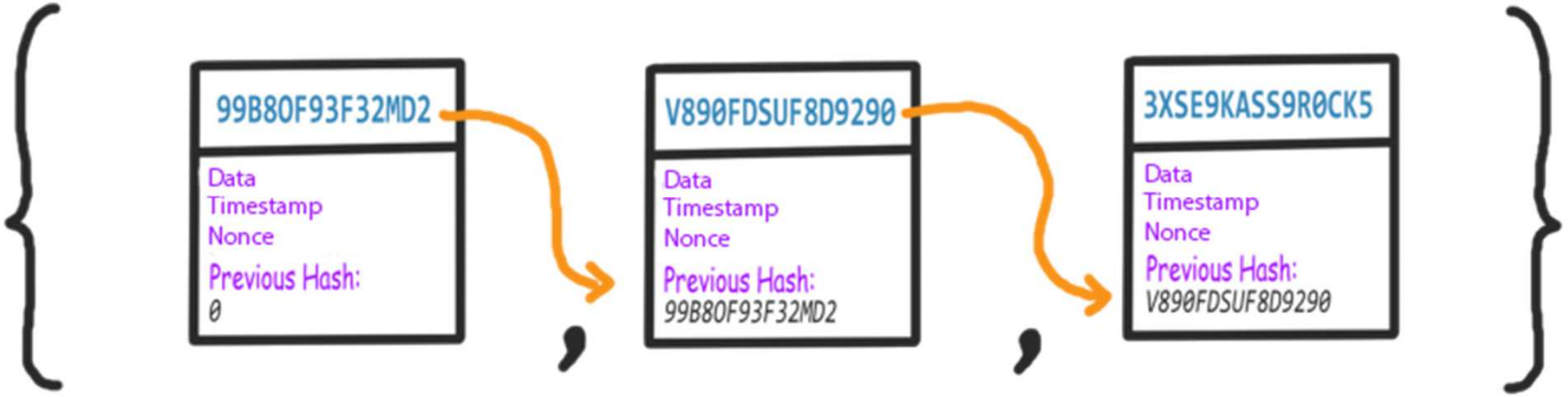
Alice → Bob 5,00 BTC



¿Cómo sabemos que Alice no gasta dos veces el mismo dinero?

- Efectivamente, hay una **carrera**
- Alice puede intentar realizar dos pagos en el tiempo que se actualiza el libro contable distribuido de todo el planeta
- Los **mineros** se encargan de competir para ver quién es el que decide cuál es el apunte contable que vence
- Buscan hashes con una forma determinada

Blockchain – ejemplo práctico



- Cada bloque contiene
  - Los datos del mismo (una cadena de caracteres)
  - Una marca temporal (tiempo en ms desde el 01/01/1970)
  - Un número aleatorio llamado ‘nonce’ (*number used once*)
  - El hash del bloque anterior (0 en caso del bloque génesis)
  - Su propio hash, calculado a partir de los datos anteriores

El proceso de minado

- Se trata de un proceso competitivo para validar nuevos bloques
- Se define un nivel de dificultad de minado (ej. d=5)
- Este proceso es cada vez más costoso conforme aumenta la dificultad de minado
- Se busca un 'nonce' que haga que la función hash empiece por un número de ceros igual a la dificultad
- Una vez encontrada la solución, el bloque se convertirá en una parte de la cadena una vez que los demás mineros den el visto bueno

Minado de dificultad 3

…
9617e132409a41027ea9422ab3e95e1e245885151a03803a7a668504e26c4385
61272dc9eb5210fb7f91d9522c282c0bb25b5710563b2c60e0b417228b56fa96
44da075310df25a4dd64fbd0b7ee39bf7a081509600fcb4efa20e5cda5d21cb7
fae824d228b516c43634b49c635c0a5d0df3ee11b589eb2377adfde8a309c903
710e84d7cc3ee03ea5d4d1aa6c9006653aa852d7232aefe42aca2649678010f9
b0fa0e7a09bf3018edd9247375e448809c7ff23f38e67bb3087b334efdb8e1e8
e4c3bba064fc4c609505db24f1b267d81fc9f2bad395d03e383cf9cf18d636da
b1453fffa4e615b5a35623c8970eb908cdd2891e75486e95b43af0d4c8a8610a
d15f10bc8a06c466765e7c29ef71352566db6728dcd937a04bc0bf0add06b522
5a489e7afdf980e5c9c34270f002d99fb47f167e4217142372ed663931b39ca9
19b257a3d4f4421970beaac62ccb0e2df8238e065343deea046ebec9b12924cf
6fb7d1c5f63cab2e3511c2a341213cebb40c29e6992557c03ced888fb77d5479
185f506b4620c377907c02d496010addc346214988d8d5beaeb023577c44c7a4
0003ec35de399452d78459a4c3deafc7a6c1115a49447f54436436ae09e3d17f 2470
…
15038742d6f9106c1e0758b40d3a5b86a7d56ad3d91311956e39f6fc9c58e7cc
000e469959b21be4b61627476cbe30bd99b2efc4b1f7217bafaadca95cb944a2 5117

Series de resultados con dificultad d=5

000000597407ea4ab0092483c7547ea6d8e2231015755b3b9d949f75a1eb9039
0000007186c411eda9936166a40d43dd08b4d3727dce4fc5cc0577c14f768bf1
000000c02e083f2bec5e3fb1e4e6f1f74bd030627703ce602c3a3872cd8f4394
0000010d1059acae8c8376662227b634efae6549204213311298dd633603e86a
00000149d94793adc64a8ed9447f8fd46e3662bb9f67d6e6604b2a5a986b152f
000001657289fdd16c7ee91e7b2cab56aa0676107ec56cd62ffba1db4fe4032e
0000025ca2238fb79eaf8b86e2c145729471660a16cf341d0e92450f3c4ce060
0000029cae64edcdef6deca4fedb51c873588e38f4f565cbfc68ba9d06439c27
000002cf4431261801f81092a4044359e76a77bba39c7c6dde85dc16caea8aab
0000030130a4e5fdcc3a3007f922d96f0b35b5e5960f3b68983e5b1bad3c8485
0000030b607c4e2ed0e3ce6c14bedc7bbd34ffd464847c2bba7a92fa0e204a4a
0000031aeeafde9b0b2311f6d9daf9bd6443e592390424c973e7db4e62fe156f
00000334634b1cddd70aa0b40388d6a9fb6b56e049611853a726484a30168edf
0000043d632d47c1ea6d31750482c7c38b94a4905247f3340721de748b88fda4
0000044ada38e58dba8f5556fe1b2c56ffb8e65b3275110aa6f43469712f0114
00000484566be5c1bede80371f191484cc4c3fefd1ac75d1acbdb3b38cef1de3
00000518550abba71de8f80a63b44a982c73a2d72536a0dbac339ea5c05bb584
0000071c9786491039ff2ff9fd7ea6f397634402dfa97913b68271c7e55151d4
0000076533e7a0f40c427a3c769bbba0b9721b592b08e95e2c5e6813e9c4e1cc

Dificultad media de minado

- 16^1 = 16 iteraciones 3,91 milisegundos (1 cero)
- 16^2 = 256 iteraciones 62,50 milisegundos
- 16^3 = 4.096 1,00 segundo
- 16^4 = 65.536 16 segundos
- 16^5 = 1.048.576 4,27 minutos
- 16^6 = 16.777.216 68,27 minutos
- 16^7 = 268.435.456 18,20 horas
- 16^8 = 4.294.967.296 12,14 días
- $16^9 = 6{,}87 \cdot 10^{10}$ 194,18 días
- $16^{10} = 1{,}01 \cdot 10^{12}$ 8,51 años
- $16^{11} = 1{,}76 \cdot 10^{13}$ 136,10 años

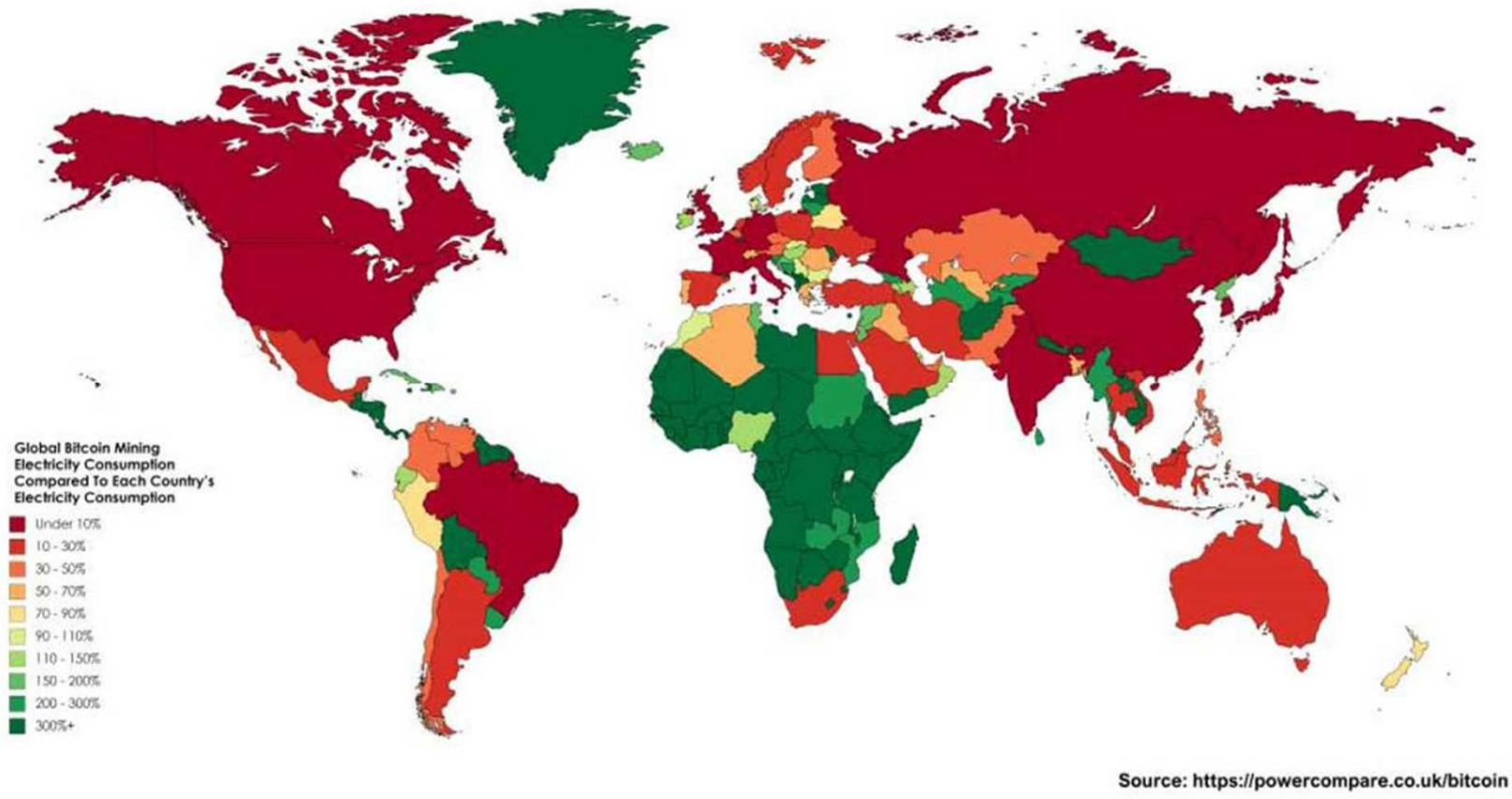
```
Intentando minar el bloque 1...
El bloque se ha minado!!! : 00000da3dc2b09a95d0ef73b153b1877d67f5dc37d9df99d6fde5b683371707e

Intentando minar el bloque 2...
El bloque se ha minado!!! : 0000077acfb12e3291a9b13945af5dfba32fdeea398a7f73debd58a3534b26af

Intentando minar el bloque 3...
El bloque se ha minado!!! : 0000082e4177c7c43cf764636ba8ca0055ee57ba53ccf6578e55bf4b2008cdeb


La cadena es válida: SÍ

El blockchain
[
  {
    "hash": "00000da3dc2b09a95d0ef73b153b1877d67f5dc37d9df99d6fde5b683371707e",
    "hashAnterior": "0",
    "datos": "El primer bloque (bloque génesis)",
    "marcaTemporal": 1538313210541,
    "nonce": 976901
  },
  {
    "hash": "0000077acfb12e3291a9b13945af5dfba32fdeea398a7f73debd58a3534b26af",
    "hashAnterior": "00000da3dc2b09a95d0ef73b153b1877d67f5dc37d9df99d6fde5b683371707e",
    "datos": "El segundo bloque",
    "marcaTemporal": 1538313212239,
    "nonce": 381641
  },
  {
    "hash": "0000082e4177c7c43cf764636ba8ca0055ee57ba53ccf6578e55bf4b2008cdeb",
    "hashAnterior": "0000077acfb12e3291a9b13945af5dfba32fdeea398a7f73debd58a3534b26af",
    "datos": "El tercer bloque",
    "marcaTemporal": 1538313212995,
    "nonce": 1484943
  }
]
```

¿Cuesta mucho minar bitcoins?

- Según un informe, en la actualidad el minado de Bitcoin es capaz de consumir la misma energía que 159 países de todo el mundo, entre los que se encuentran Irlanda, Hungría, Croacia, Serbia, Eslovaquia, Islandia o Corea del Norte
- Se estima que en el año 2020 el consumo del minado de monedas virtuales igualará al de todos los países del planeta juntos

https://cincodias.elpais.com/cincodias/2017/11/23/lifestyle/1511464481_564794.html

Consumo energético del bitcoin



https://powercompare.co.uk/bitcoin/

Alternativa al Proof of Work (PoW)

- Gasto económico y energético muy elevado
- Los mineros compiten entre sí y no tienen nada que perder
- Los actos maliciosos no tienen consecuencias
- Alternativa: **Prueba de Participación (*Proof of Stake*)**
  - Ya no habrá difíciles problemas matemáticos que los mineros deban resolver
  - Tendrán que poner sus propios fondos en juego para certificar que un bloque es válido
  - Si hay un comportamiento malicioso, el validador perderá su criptomoneda

https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Aplicaciones blockchain

- Registro distribuido y verificación de datos
  - Historial médico de pacientes
  - Registro de la propiedad
  - Registro de vehículos
  - Protección de la propiedad intelectual
  - Creaciones digitales: autoría y fecha. *Proof of existence*
  - Registros de nacimientos y defunciones, matrimonios y divorcios, ...
  - Registro internacional de antecedentes penales
  - Seguimiento de pedidos desde la compra hasta la recepción
  - Registro de auditoría verificable de las reclamaciones de seguros
- Seguimiento de la cadena de suministros y prueba de procedencia
- Expedición de certificados académicos
- Proteger derechos de autor
- Coches autodirigidos
- Almacenamiento distribuido en la nube
- Gestión de identidades digitales

https://www.fin-tech.es/2016/10/aplicaciones-de-la-tecnologia-blockchain.html

Conclusiones

- Bitcoin, Ethereum, … criptodivisas
- Libro contable distribuido
- Funciones hash, PoW – ¡Complejidad exponencial!
- Anonimato
- No trust

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
GASTEIZKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE VITORIA-GASTEIZ

Gracias

Otras Referencias

- Wikipedia - https://es.wikipedia.org/wiki/
  - Alice y Bob, Base58, Base64, Bitcoin, Cadena de bloques, Criptomoneda, *Cryptocurrency wallet*, ECDSA, Ethereum, *Stylometry*
- Bitcoin: A Peer-to-Peer Electronic Cash System
  - http://www.bitcoin.org/bitcoin.pdf
- Morgen E. Peck, *Blockchains: How they work and why they'll change the world*, IEEE Spectrum, Vol. 54, Issue 10. October 2017
- El País – Moneda Electrónica
  - https://elpais.com/tag/moneda_electronica/a
- ¿Cuánto vale un bitcoin? ¿Cómo y quién determina su precio?
  - http://blog.bit2me.com/es/precio-bitcoin/
- Proof of Work – Analogía para principiantes
  - http://www.criptomania.com/proof-of-work-vs-proof-of-stake/proof-of-work/proof-of-work-analogia-principiantes/