

IX Jornada de Seguridad y Protección de Datos de Carácter Personal

Escuela Universitaria de Ingeniería de Vitoria-Gasteiz
UPV/EHU



Tecnología *Blockchain* Caso de estudio: el *Bitcoin*



Ismael Etxeberria Agiriano
ismael.etxeberria@ehu.eus

Lenguajes y Sistemas Informáticos

29 de noviembre de 2017

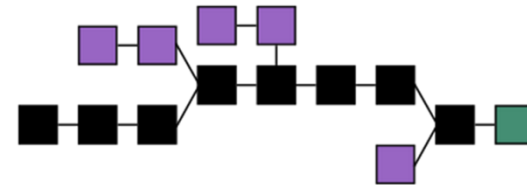


¿Qué es el bitcoin?

- 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, bitc  in, bitcoins, 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?

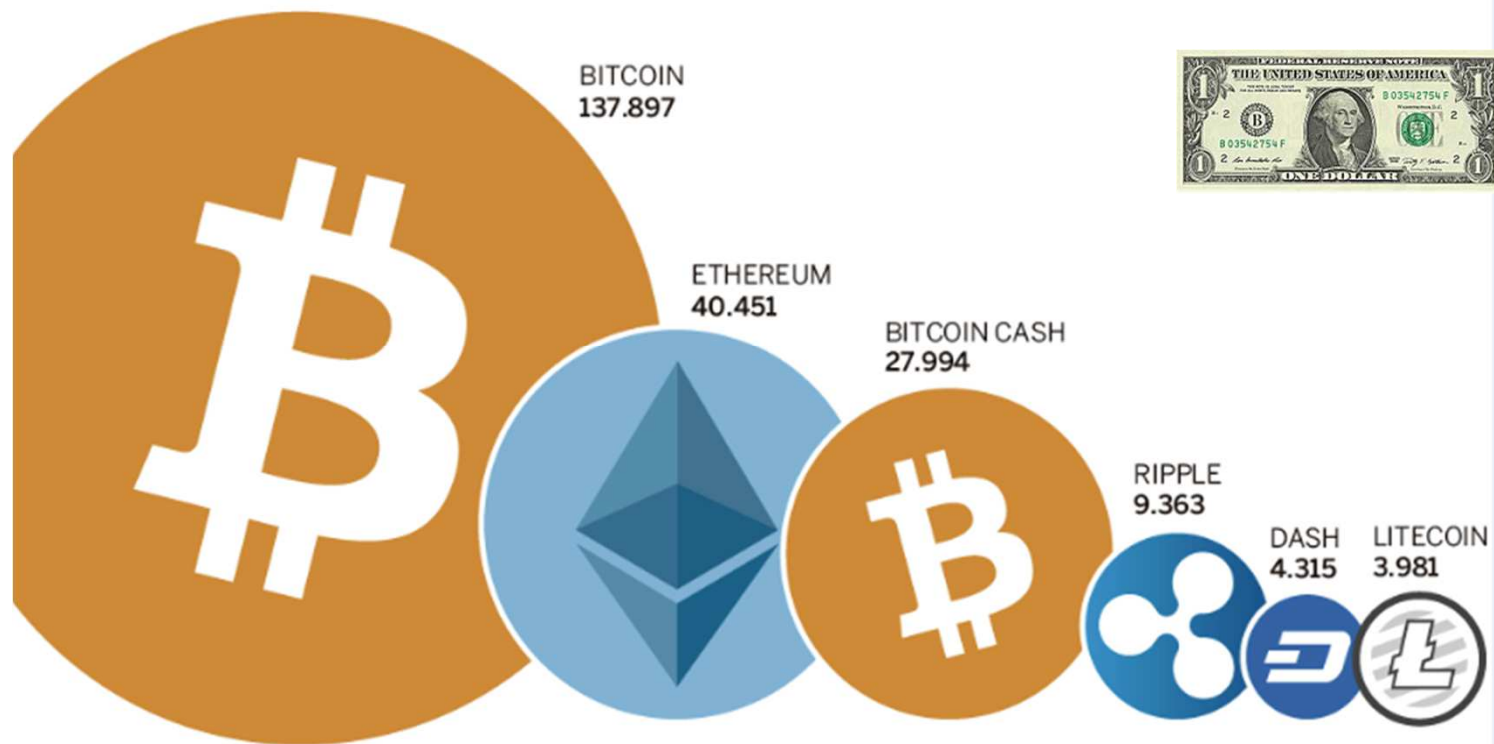
- A la sombra de bitcoin surgen otras monedas criptográficas



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

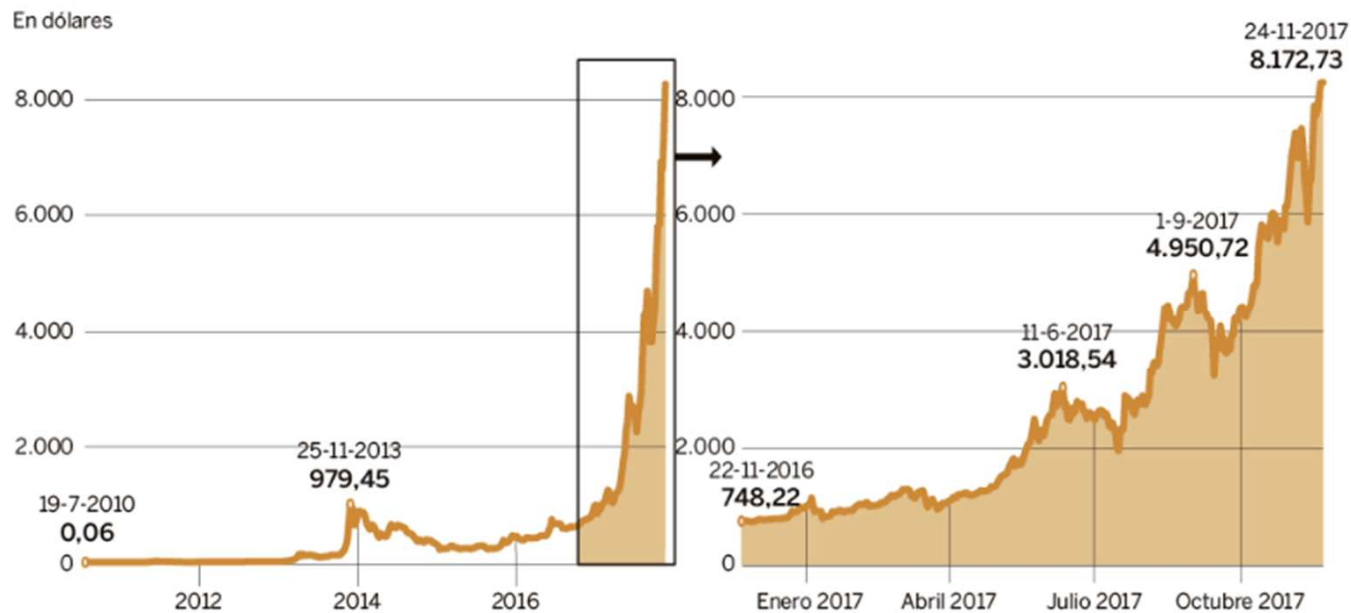
¿Cuánto dinero capitalizan?

A 24 de noviembre de 2017. Cifras en millones de dólares.



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

Cotización del bitcoin frente al dólar USD



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

¿Cuánto vale actualmente un bitcoin, BTC?

- A 25 de noviembre de 2017
- Contra el Euro (EUR)
 - 1 BTC = 7.357,44 €
 - 1 milibitcoins (mBTC 10^{-3} BTC) = 7,36 €
 - 1 microbitcoins (uBTC 10^{-6} BTC), bit = 0,74 c€
 - 1 Satoshi (10^{-9} BTC) = 0,0074 c€
- Contra el Dólar (USD)
 - 1 BTC = 8.644,26 \$
 - 1 milibitcoins (mBTC 10^{-3} BTC) = 8,64 \$
 - 1 microbitcoins (uBTC 10^{-6} BTC), bit = 0,86 c\$
 - 1 Satoshi (10^{-9} BTC) = 0,00086 c\$



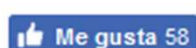
https://es.coinmill.com/BTC_EUR.html

¿Cuánto vale un bitcoin, BTC?

— A 27 de noviembre de 2017



BTCEUR



Resumen

Noticias

Precio	Variación	Hora
8098,66 €/	+0,00% ▲ +8098,66	10:00:06

CAMBIO		PRECIOS	
1 Euro =	0,00	Precio de compra 1 Bitcoin =	8102,16 Euros
1 Bitcoin =	8098,66 Euros	Precio de venta de 1 Bitcoin =	8095,16 Euros

<http://www.eleconomista.es/cruce/BTCEUR>

Cotización bitcoin BTC frente al dólar USD

- A 28 de noviembre de 2017



- Bitcoin nears \$10,000 mark as hedge funds plough in

<https://www.theguardian.com/technology/2017/nov/27/bitcoin-nears-10000-dollar-mark-as-hedge-funds-plough-in>

GDAX

BTC/EUR

Select product

BITCOIN

BTC/USD

\$9964.99

3.86%

▲

BTC/EUR

€8365.50

2.77%

▲

BTC/GBP

£7571.72

4.40%

▲

ETHER

ETH/USD

\$468.20

0.69%

▼

ETH/BTC

฿0.04686

4.64%

▼

ETH/EUR

€392.93

1.78%

▼

LITECOIN

LTC/USD

\$92.83

4.19%

▲

LTC/BTC

฿0.00930

0.11%

▲

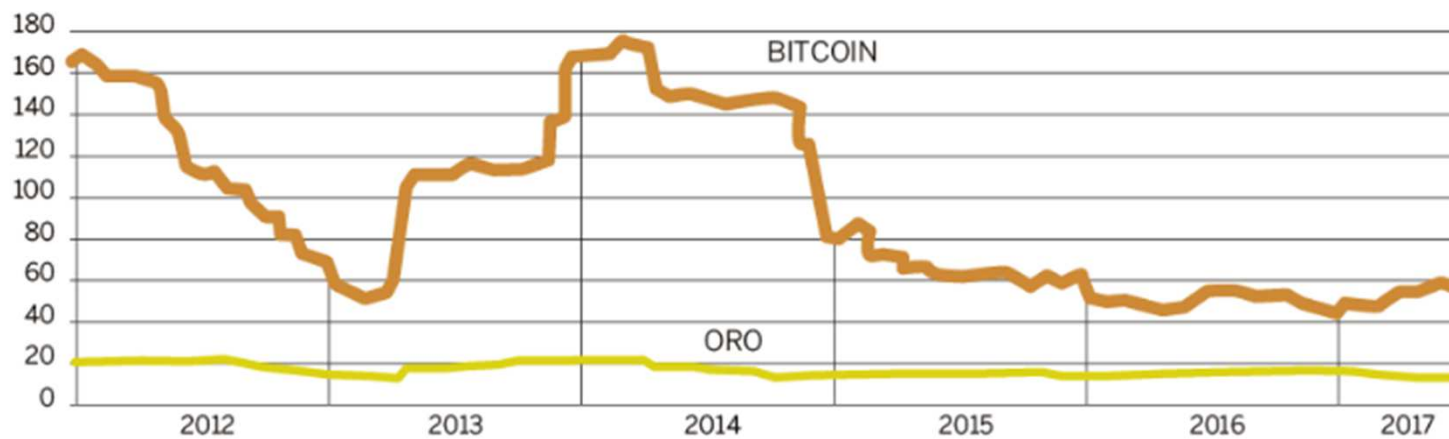
LTC/EUR

€77.38

2.10%

▲

Volatilidad del bitcoin frente al oro



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

Volatilidad diaria del bitcoin

— A 27 de noviembre de 2017



HISTÓRICO BTCEUR		
Fecha	Precio	Variación
26/11/17	0,0000	7708,1300
25/11/17	0,0000	7242,5600
24/11/17	0,0000	6946,5400
23/11/17	0,0000	6896,2600
22/11/17	0,0000	7021,7800
21/11/17	0,0000	6899,3800
20/11/17	0,0000	7013,5300
19/11/17	0,0000	6729,3200
18/11/17	0,0000	6602,4300
17/11/17	0,0000	6641,2200
16/11/17	0,0000	6634,2600
15/11/17	0,0000	6232,0800
14/11/17	0,0000	5678,5500
13/11/17	0,0000	5599,2500
12/11/17	0,0000	4904,3900
11/11/17	0,0000	5441,4300
10/11/17	0,0000	5759,3500
9/11/17	0,0000	6197,9800
8/11/17	0,0000	6425,4200

<http://www.eleconomista.es/cruce/BTCEUR>

Ya anda por los 10.000 USD

- **Bitcoin Guns for \$10,000 as Cryptocurrency Mania Defies Skeptics** 27 de noviembre de 2017



<https://www.bloomberg.com/news/articles/2017-11-26/bitcoin-surges-past-9-000-as-euphoria-reaches-a-fever-pitch>

¿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



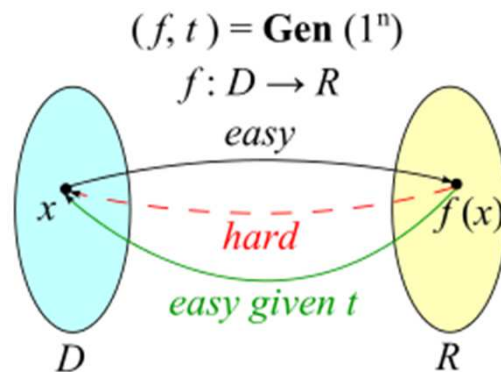
Fundamentos de criptografía

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



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



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)



$$M = D(Ku, r)$$

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

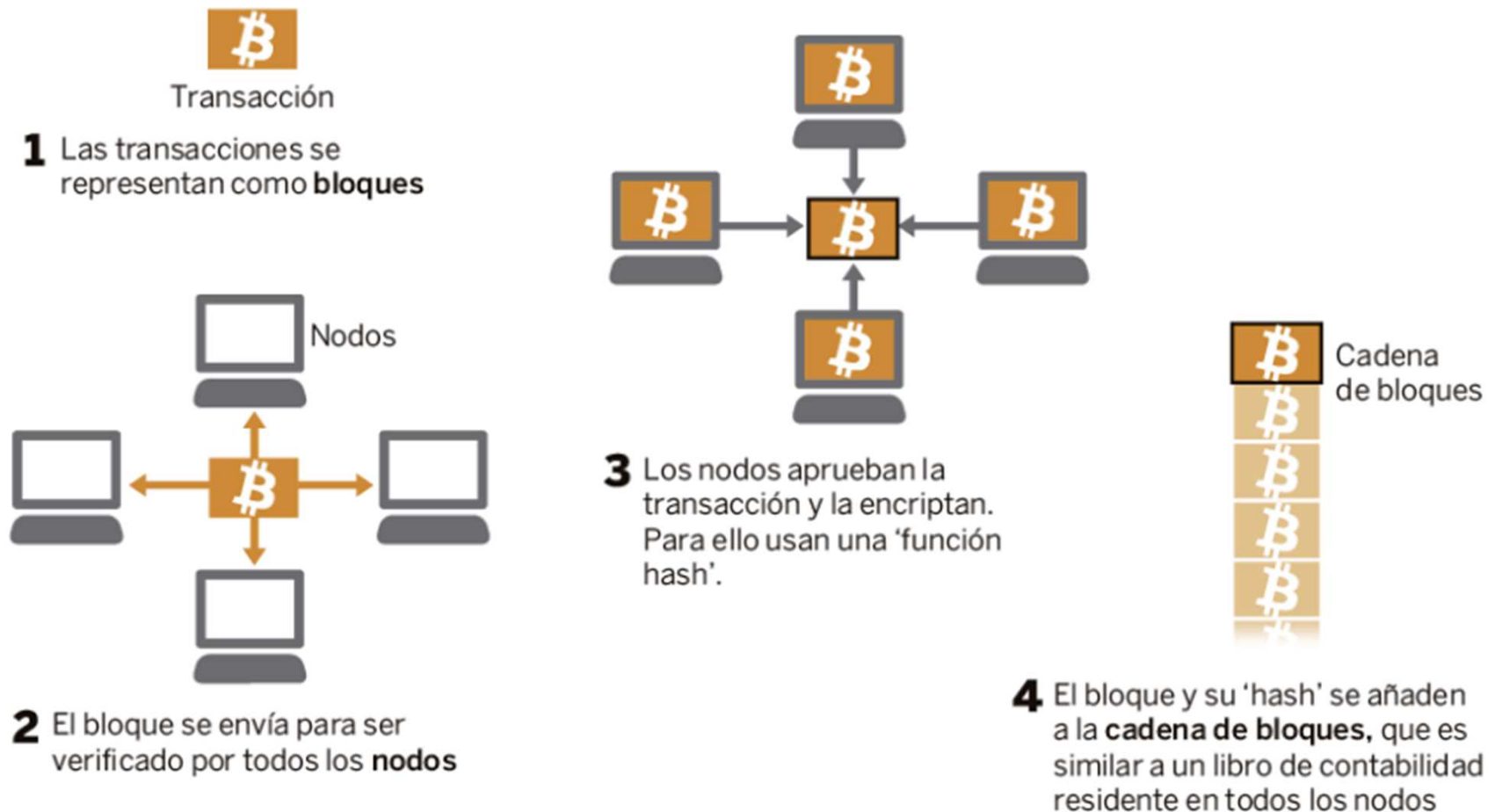
```
MC05XSpcLiIKc3luIG1hdGNoIEtsYXNpICJew0EtTE4tWl1bMC05XSpcLiIKCnN5biBtYXRjaCBC  
ZWdWZXJkZSAiXiAqXCogIiBuZXh0Z3JvdXA9VmVyZGUsVmVyZDEKc3luIG1hdGNoIFZlcmRlICAg  
ICJbXjAtOV0uKiIgY29udGFpbmVkc3luIG1hdGNoIEtsYXNpICJew0EtTE4tWl1bMC05XSpcLiIKCnN5biBtYXRjaCBCWZXJkMSAgICAiWzAtOV0uKiIgY29udGFp  
bmVkc3luIG1hdGNoIEtsYXNpICJew0EtTE4tWl1bMC05XSpcLiIKCnN5biBtYXRjaCBCWZXJkMSAgICAiWzAtOV0uKiIgY29udGFpbmVkc3luIG1hdGNo
```

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	O	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



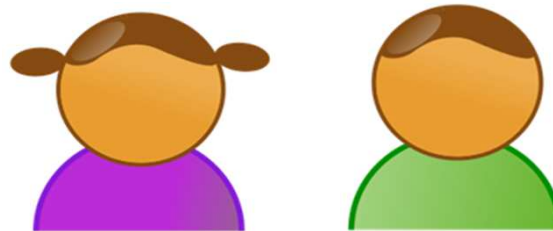
¿Cómo funciona bitcoin? Monedero

- 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

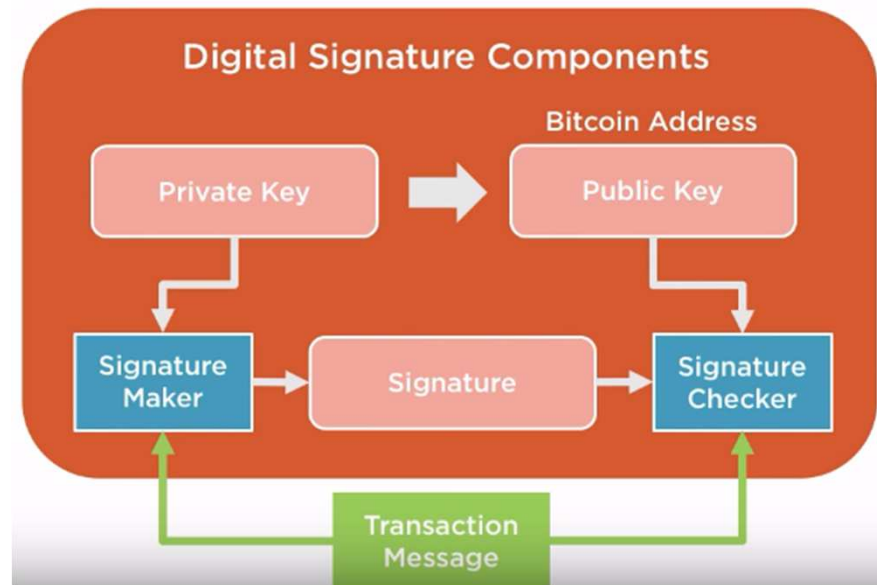
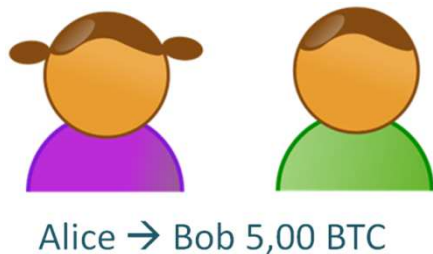
¿Cómo funciona? Libro contable distribuido

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



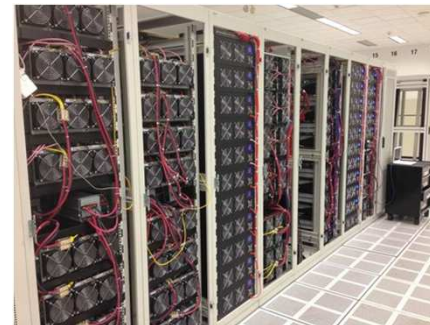
¿Cómo sabemos que Alice no gasta dos veces el mismo dinero?

- 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



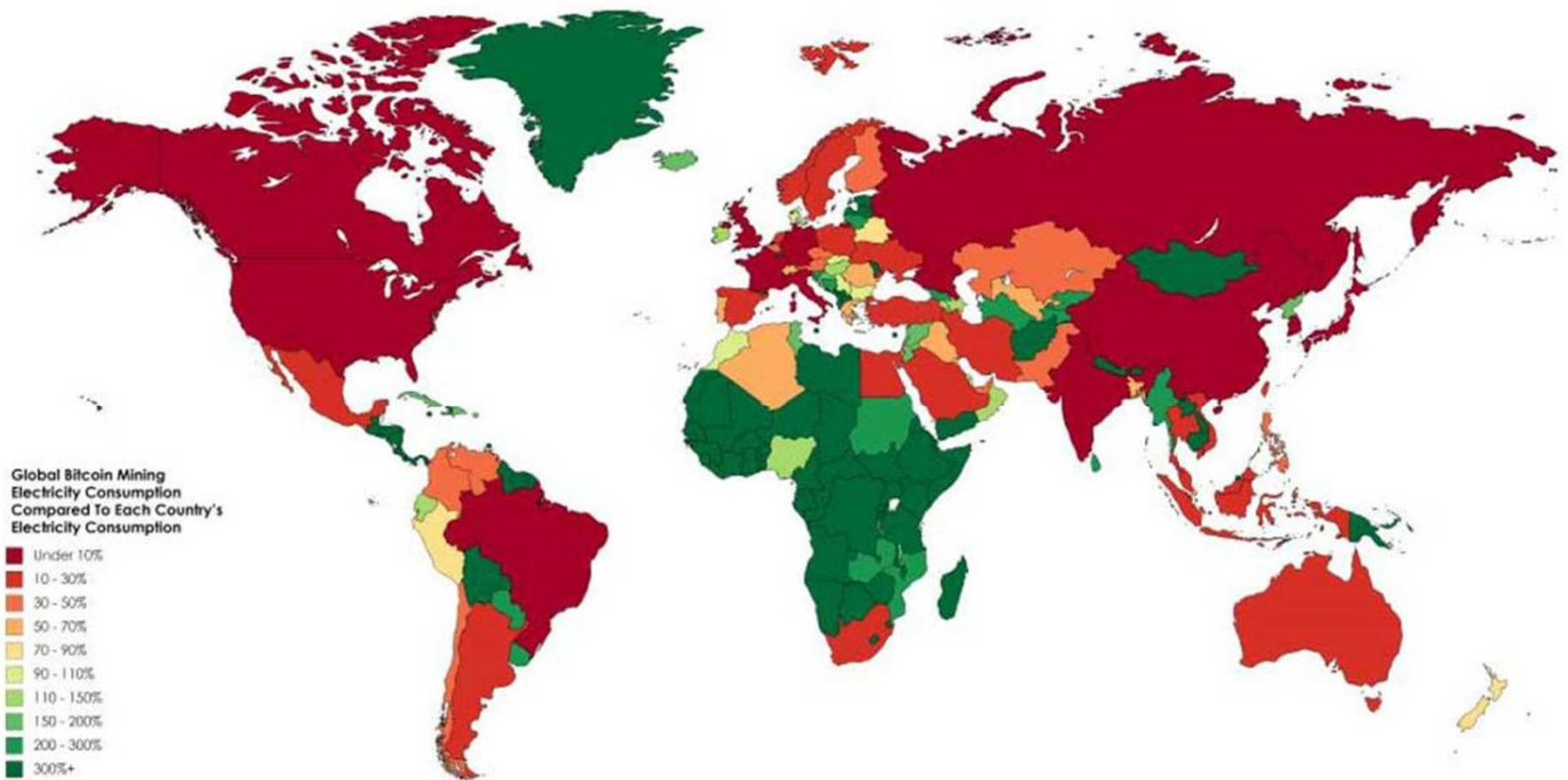
¿Cuesta mucho minar bitcoins?

- 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



Source: <https://powercompare.co.uk/bitcoin>

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

Aplicaciones blockchain

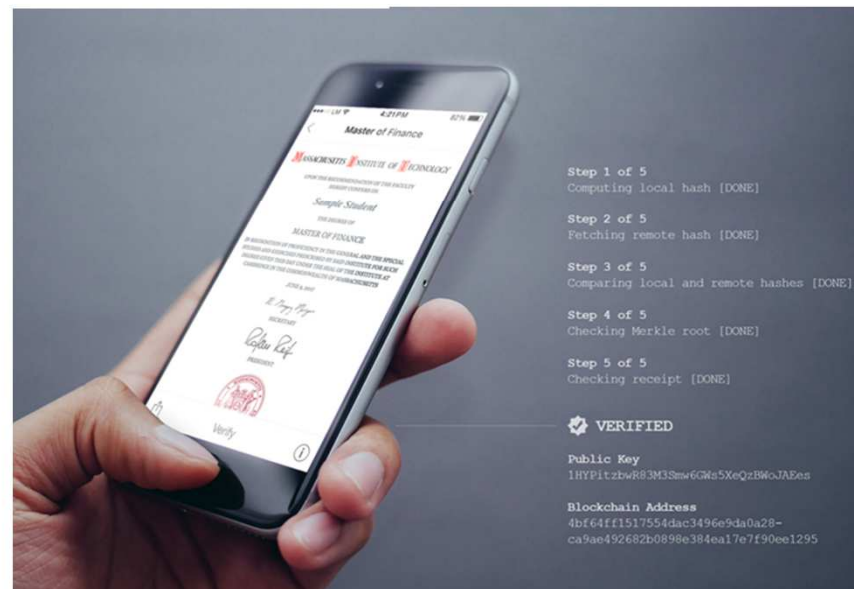
- Registro distribuido y verificación de datos
 - Historial médico de pacientes
 - Registro de la propiedad
 - Registro de vehículos
 - Protección de la propiedad intelectual
 - Creaciones digitales: autoría y fecha. *Proof of existence*
 - Registros de nacimientos y defunciones, matrimonios y divorcios, ...
 - 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>

Expedición de diplomas digitales

NOVEMBER 2017 – NEWSLETTER #3

- [Blockchain](#). MIT has successfully started to use blockchain technology to issue digital certificates. This way students securely own and share with employers their diplomas.

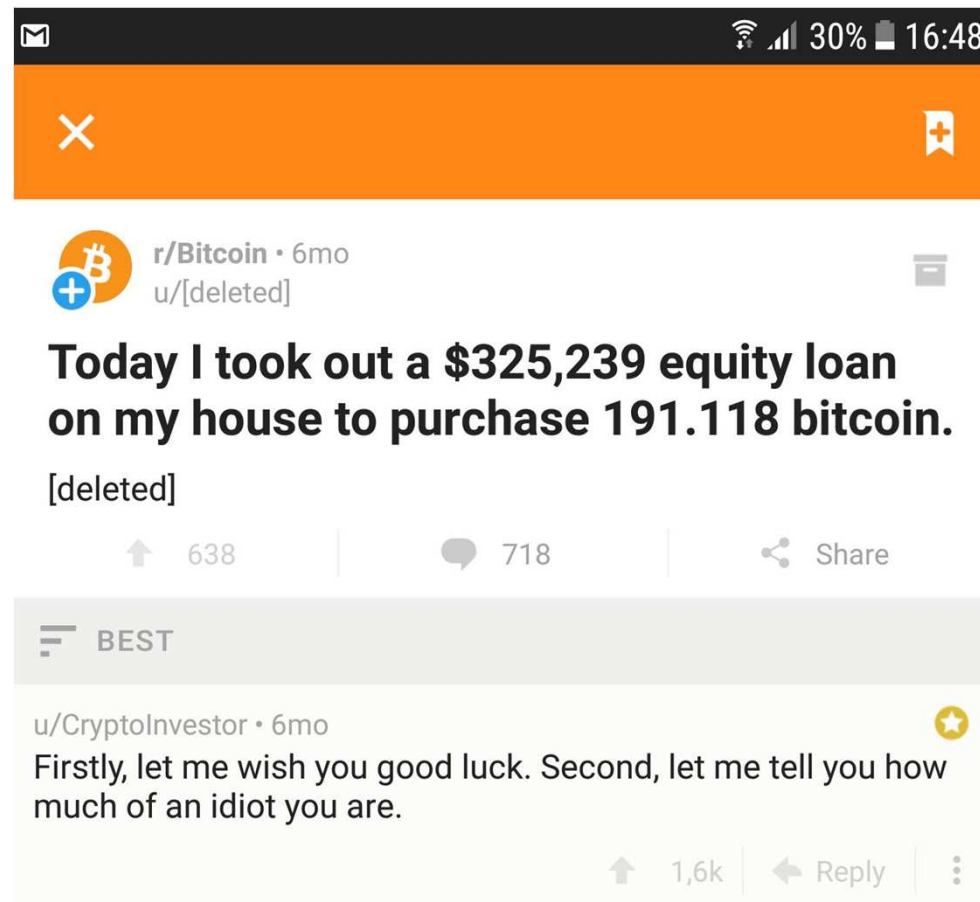


<http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017>

Conclusiones

- Bitcoin, Ethereum, ... criptodivisas
- Libro contable distribuido
- Firma digital
- Funciones hash
- Anonimato
- No trust
- Sistema piramidal / Burbuja

Tengan cuidado ahí fuera



“El precio del bitcoin es cercano a cero”

- El profesor en la Universidad de Harvard, augura el colapso de la cotización de las criptomonedas



https://elpais.com/economia/2017/11/23/actualidad/1511451344_178346.html



- La especulación acuña las ‘criptomonedas’
 - Diez millones de personas arriesgan su dinero en divisas digitales tan volátiles como el bitcoin o el ethereum seducidos por sus exponenciales ganancias a corto plazo

https://elpais.com/economia/2017/11/23/actualidad/1511450574_320432.html



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/>