



UNIVERSIDAD DE
GUADALAJARA
Red Universitaria de Jalisco

2ª. Edición del Encuentro ANUIES-TIC 2017



ellucian.





Blockchain y sus aplicaciones

Acerca de mi

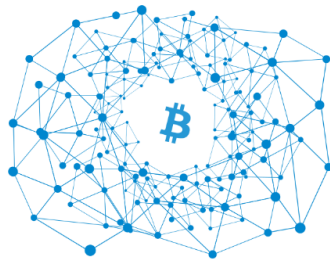
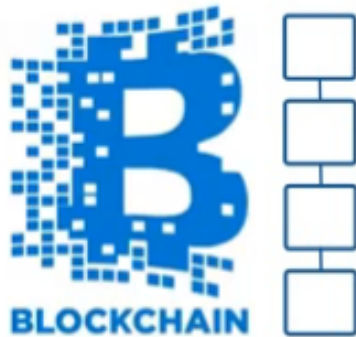
- Juan Carlos Campuzano Ramírez
 - Experiencia.
 - Atención a incidentes cibernéticos/mandamientos ministeriales.
 - Actividades adicionales como:
 - Capacitación y concientización en temas relacionados con la ciberseguridad.
 - Forense digital.
 - Pruebas de penetración.
 - Creación de equipos de respuesta cibernética.
 - Gestión de crisis cibernéticas.
 - Egresado de la Facultad de Ingeniería de la UNAM.
 - Unidad de Cómputo Académico, FI.
 - Administrador de la red y centro de datos de la DGCCH.
 - Subdirector de fuentes de información, CERT-MX Policía Federal.
 - **Mnemo-CERT.**

Mnemo

- Compañía de origen Española creada en el año 2000.
- Presencia en España, Arabia Saudita, Colombia y México.
- Proyectos en mas de 11 países.
- Servicios principales enfocados en ciberseguridad.
- Personal con amplia experiencia en la creación y gestión de Equipos de respuesta cibernéticos y sector financiero.
 - UNAM-CERT (2001)
 - CERT-MX (2010)
 - Mnemo-CERT (2014)

Agenda

- Definición de blockchain.
- Bitcoin, un ejemplo del uso de blockchain.
- Implicaciones en ciberseguridad.
- Futuras aplicaciones.
- Conclusiones.



Algunas definiciones

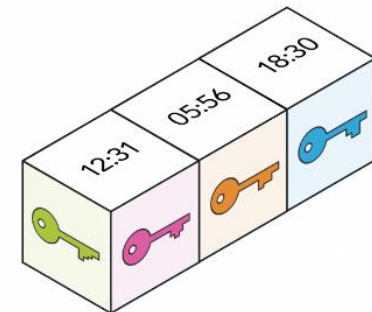


Definición inicial

- Blockchain o cadena de bloques, concebido en 2008 y aplicado por primera vez en el año 2009.

Definición

- Es una base de datos distribuida que mantiene una lista de crecimiento continua de registros llamados bloques seguros de



Características de blockchain



Aparición 2009.

Bases de datos abiertas y **descentralizadas**.

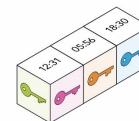
Transacciones **seguras y confiables**.

Existe un libro maestro de transacciones.

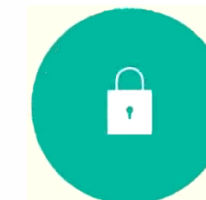
Uso de algoritmos criptográficos.

Cadenas de bloque.

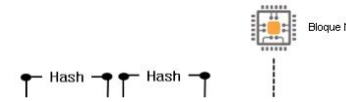
- Cada bloque hace referencia al anterior.
- No puede ser borrado o modificado.
- **Se puede realizar con cualquier tipo de información.**



Se puede implementar en entornos públicos y privados.



¿Qué es blockchain?



Sus aplicaciones van mas allá de las criptomonedas.



Surgió como el soporte tecnológico del Bitcoin.

Promete transformar la forma en que se intercambia un valor.

Esta construido con 3 tecnologías

- Criptografía de llave pública
- Redes P2P
- Protocolo de Blockchain

Plantea la siguiente revolución industrial.

<https://anders.com/blockchain/blockchain.html>



UNIVERSIDAD DE
GUADALAJARA
Red Universitaria de Jalisco

Plataformas para desarrollar sobre blockchain



- Hyperledger



HYPERLEDGER

- IBM Blockchain



- Proyectos github

GitHub

- R3



- Entre otros

<https://anders.com/blockchain/blockchain.html>

<https://bitcoin.org/es/descargar>

Tokens

Peer A

Block:	#	1
Name:	13058	
To:	\$16.40	From: Jerry → Kingly
	\$4.27	From: Elinabeth → Jane
	\$9.22	From: Woshan → Lydia
	\$8.44	From: Lady Catherine de → Collins
	\$6.52	From: Charlotte → Elizabeth
From:	XX	
Hash:	8000c1c1200e6d6f1ac4b017d0ef47d073670d367fc7b8116a3c9d5	
	View	

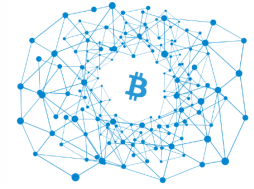
[illegible]

Peer B

[illegible]

Diebst	#	2	
Monat	19007		
Tät		From	to
\$ 97.87	From	valley	→ Lombard
\$ 48.61	From	case	→ Ash
\$ 6.15	From	partier	→ Dallas
\$ 16.04	From	scots	→ smc
\$ 86.12	From	slitshop	→ Burke
\$ 42.88	From	hushen	→ German
\$ 92.89	From	venisquet	→ Agone

Bitcoin, como un caso de ejemplo



Liberado en 2009 por un programador bajo el seudónimo de “Satoshis Nakamoto”.

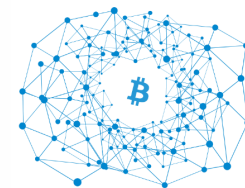
Transmitir dinero sin necesidad de un intermediario.

Es utilizada en actividades licitas e ilícitas.

Que no es.

- Una aplicación.
- Una compañía.

Bitcoin, como un caso de ejemplo



Transacciones en un día, últimas 24 horas.

TRANSACTIONS PER DAY

The number of bitcoin transactions in the last 24 hours.

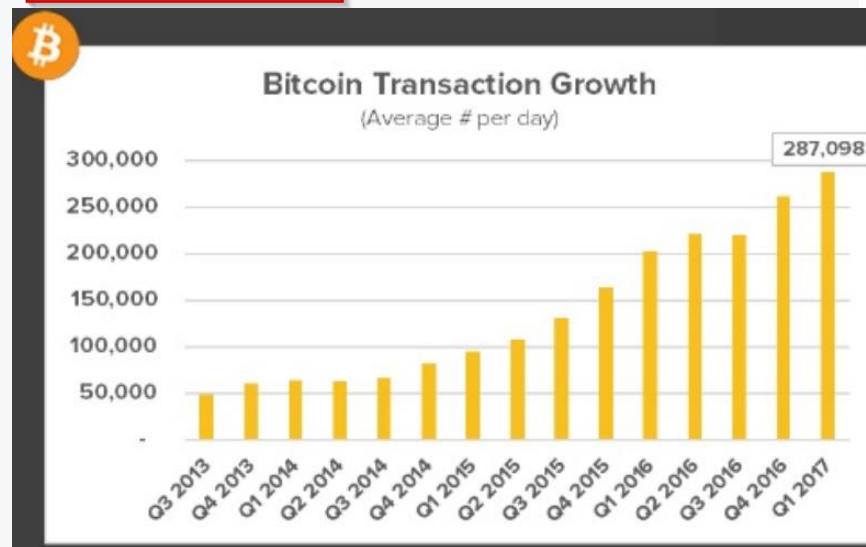
2 8 3 7 0 9

Transactions since Mon Oct 02 2017 19:46:49.

MARKET CAP: \$71,279,730,159.00

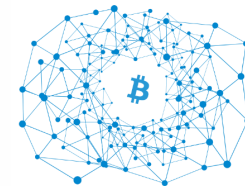
HASH RATE: 10,223,761.08 TH/s

1 BTC = \$4288.69



<https://blockchain.info/>

Bitcoin, como un caso de ejemplo



Comparativa de las características del dinero.



Características del dinero

	Oro	Efectivo (Euro)	Crypto (Bitcoin)
Fungible (Intercambiable)	Alto	Alto	Alto
No Desgastable	Moderado	Bajo	Alto
Portabilidad	Moderado	Alto	Alto
Durabilidad	Alto	Moderado	Alto
Divisibilidad	Moderado	Moderado	Alto
Seguro (No puede ser falsificado)	Moderado	Moderado	Alto
Fácilmente Manejable	Bajo	Alto	Alto
Escaso (Suministro Predecible)	Moderado	Bajo	Alto
Soberano (Emitido por el Gobierno)	Bajo	Alto	Bajo
Descentralizado	Bajo	Bajo	Alto
Inteligente (Programable)	Bajo	Bajo	Alto

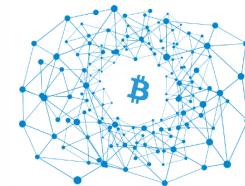


<http://blog.bit2me.com/es/precio-bitcoin/>



UNIVERSIDAD DE
GUADALAJARA
Red Universitaria de Jalisco

Bitcoin, como un caso de ejemplo



- Minería de Bitcoin.

- Empleada para verificar las transacciones, brindar seguridad y distribuir nuevas monedas en la red.
- Actualiza la blockchain con las últimas transacciones. Nadie tiene el control de la minería.
- Esta programado para que la recompensa se reduzca cada 4 años.
 - Comenzaron brindando 50 bitcoins.
 - Actualmente la recompensa es de 12.5 bitcoins.
- Se predice que todos los bitcoins serán extraídos en el 2140, con un total de 21 millones.
- Cada Bitcoin se puede dividir en 100 millones de partes.
- Conforme pasa el tiempo se requiere mayor poder de cómputo para la minería.

1 BTC	0.01 BTC	0.001 BTC	0.000001 BTC	0.00000001 BTC
A bitcoin	A bitcent	An mbit	A ubit	A satoshi

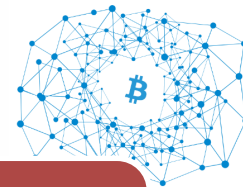


BITCOIN MINER



UNIVERSIDAD DE
GUADALAJARA
Red Universitaria de Jalisco

Bitcoin, como un caso de ejemplo



Busca resolver el problemas de compromiso de seguridad de instituciones centralizadas.

- Instituciones bancarias/Banco c
- 2014.
 - Ene, Neiman Marcus.
 - Jun, P.F. Chang's.
 - Ago, SuperVau.
 - Sep, Home Depot.
 - Oct, Dairy Queen.
- Target.

Another SWIFT Hack Stole \$12 Million

Heists Highlight Real-Time Payment Risks, Security Experts Warn

Mathew J. Schwartz (@euroinfosec) May 20, 2016

Wells Fargo accidentally leaks 50,000 clients' records

The bank accidentally sent thousands of sensitive documents to a former employee.



Mariella Moon, @mariella_moon
07.22.17 in Security

27
Comments

1704
Shares



Implicaciones en ciberseguridad

- Mercados negros

EEUU, Europol y Holanda anuncian el cierre de AlphaBay y Hansa, los mercados ilícitos más importantes de la Dark Web

- Silk road
- Alpha bay
- Hasa
- Evolution
- Entre otros

The screenshot shows the Evolution marketplace website. At the top, a blue navigation bar includes a welcome message for 'OldManRivers', notification icons, and a Bitcoin balance of 0.0000. Below this is a search bar with the word 'evolution' and a search button. A left sidebar lists various categories with their respective item counts. The main content area features a green success message, a welcome message, a notice about the buyer's guide, and a news section.

Categories	Count
Drugs	16802
Fraud Related	2391
Guides & Tutorials	3293
Services	1586
Counterfeits	1024
Digital Goods	2821
Drug Paraphernalia	369
Electronics	184
Erotica	387
Jewellery	176
Lab Supplies	37
Miscellaneous	207
Weapons	257

Implicaciones en ciberseguridad

Venta de productos ilegales.

The screenshot shows the AlphaBay Market website, a dark web marketplace. The browser address bar displays a .onion URL. The website header includes the AlphaBay Market logo and navigation links. A sidebar on the left lists various categories for sale, such as Fraud, Drugs & Chemicals, and Digital Products. The main content area features a listing for 'UBER Account Login Profiles - Worldwide Taxi Service'. The listing includes a description of the product, its features (Digital goods, Unlimited, Never), and a table of listing feedback from buyers. The feedback table shows three entries with dates, times, and comments.

Buyer	Date	Time	Comment
17y	March 26, 2015	21:50	Fast and reliable as always
in'm	March 26, 2015	06:58	quick and pro thanks mate
d7y	March 26, 2015	00:47	

Implicaciones en ciberseguridad

Exploits/Vulnerabilidades de día 0.

Exploits

Hello , I am selling privates FUD expls this topic will be always updated

There is now office FUD (**Not Macro**) , bypass aslr/dep , the office does NOT crash and the content showing up

cve2015-2545 - cve2015-1770

<https://www.cve.mitre.org/cgi-bin/cv...=cve-2015-2545>

<https://www.cve.mitre.org/cgi-bin/cv...=cve-2015-1770>

Output size : 47kb

detection rate : <http://nodistribute.com/result/2zio7OqjsynqPBCEeHZbkcWA>

price : 550USD

Payment : btc/pm

Jabber : [REDACTED]

mail : [REDACTED]

PS : i will add more expls here in the topic for other products you can pm me as well

regards



UNIVERSIDAD DE
GUADALAJARA
Red Universitaria de Jalisco

Implicaciones en ciberseguridad

Malware.



Summary	
Address	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Hash 160	17b4bd9a139158614e8f54c6b800a1822609436a
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	131
Total Received	19.83510304 BTC
Final Balance	0.09 BTC

<https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94>

Request Payment

Donation Button

Implicaciones en ciberseguridad

- Desaparición de compañías de intercambio.

- Mt. Gox feb 2014.
- BitInstant 2014.
- My Coin feb 2015.



El mercado de Bitcoins MyCoin desaparece con 387 millones de dólares



Carlos Zahumenszky
2/09/15 2:45pm • Archivar en: BITCOIN

9.0K 13 2



Implicaciones en ciberseguridad

Extorsiones.

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

In past, we launched one of the largest attacks in Switzerland's history. Use Google.

All network of [victim's name] will be DDoS-ed starting [date], if you don't pay 10 Bitcoins @ [bit coin address]

When we say all, we mean all - users will not be able to use any of your services.

Right now we will start 15 minutes attack on one of your IPs ([victim's IP address]). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by [date], attack will start, price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Our attacks are extremely powerful - our Mirai botnet can reach over 1 Tbps per second. So, no protection will help.

Prevent it all with just 10 BTC @ [bit coin address]

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

Futuras aplicaciones en el sector financiero

Criptomonedas.

<https://coinmarketcap.com/#MXN>

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$1,298,750,308,258	\$78227.37	16,602,250 BTC	\$23,139,130,677	-2.35%	
2	 Ethereum	\$503,341,762,282	\$5301.77	94,938,515 ETH	\$5,796,240,388	-1.87%	
3	 Ripple	\$141,380,062,174	\$3.69	38,343,841,883 XRP *	\$941,988,260	-0.89%	
4	 Bitcoin Cash	\$121,085,739,764	\$7272.71	16,649,325 BCH	\$2,379,328,540	-3.49%	
5	 Litecoin	\$50,416,397,392	\$947.38	53,216,482 LTC	\$1,620,216,021	-2.60%	
6	 Dash	\$40,583,505,724	\$5340.13	7,599,717 DASH	\$660,142,950	-5.48%	
7	 NEM	\$36,520,344,206	\$4.06	8,999,999,999 XEM *	\$61,574,270	-3.65%	
8	 NEO	\$29,797,166,217	\$595.94	50,000,000 NEO *	\$1,361,193,321	-9.77%	
9	 IOTA	\$27,671,541,616	\$9.96	2,779,530,283 MIOTA *	\$238,830,178	-4.31%	
10	 Monero	\$25,623,095,377	\$1689.15	15,169,242 XMR	\$713,982,395	1.00%	

Futuras aplicaciones en el sector financiero

- **Crear o redefinir modelos de negocio.**

1. Criptomonedas con respaldo bancario.
2. **Voto por Internet [Partido político danés 2014].**
3. Salud.
4. Otros usos dentro del sector financiero.
 - Productos de Ahorro.
 - Mecanismos de autenticación y seguridad.
 - Contabilidad.
 - Productos de crédito.
 - Mercados capitales e inversión.
5. Procesos de cumplimiento.
6. **Contratos inteligentes.**
7. Gestión de identidades. [Onename, keybase, shocard]
8. Registro y verificación de datos. [Tierion, Proof of Existence, Suecia]
9. Servicios de notaria. [stampery blockverify]
10. Alquiler de propiedades y economía colaborativa.
11. Aplicaciones militares. [DARPA mensajería segura]
12. **Descentralización del IoT / Almacenamiento [Storj].**
13. Registro de nombres de dominio.
14. Propiedad intelectual.



Futuras aplicaciones en el sector financiero

Estudian como desarrollar aplicaciones sobre blockchain.



Fuente: R3 consortium.

Futuras aplicaciones en el sector financiero

Estudian como desarrollar aplicaciones sobre blockchain.



UNIVERSIDAD DE
GUADALAJARA
Red Universitaria de Jalisco

Conclusiones

- Blockchain es la base para muchos proyectos que vendrán.
 - Brinda confianza, transparencia y escalabilidad.
- Permite invertir en soluciones alternativas a Bitcoin.
- Su uso se esta trabajando ampliamente a nivel mundial.
- Blockchain es un nuevo paradigma respecto a como se llevan a cabo nuevas actividades a nivel mundial.
- Requiere el trabajo conjunto.
 - Bancos, empresas, innovadores y reguladores.
- Discusiones jurídicas entorno al tema.
- Los usuarios serán 100% responsable de lo que sucede con tus cuentas, no habrá a quien reclamar.
- Manejo de vulnerabilidades en estos sistemas.
- Se deberán desarrollar capacidades de investigación para casos que involucren bitcoins.



UNIVERSIDAD DE
GUADALAJARA
Red Universitaria de Jalisco

Mnemo-CERT

Juan Carlos Campuzano Ramírez

jc.campuzano@mnemo.com

GRACIAS POR SU **ATENCIÓN**



ellucian®

