Bitcoin: Un Nuevo Mundo

- **Introducción Personal**
- **El Empoderamiento del Individuo**
- **Que es Bitcoin?**
- **Que resuelve? Que cambia?**
- **Situación Actual**
- **Como afectará al Mundo?**

sistemas edenia

Club de Investigación Tecnológica

Presentado por:
Rodrigo Fernández Castro
B.A. Filosofía – Ingenieria Mecánica
Tulane University

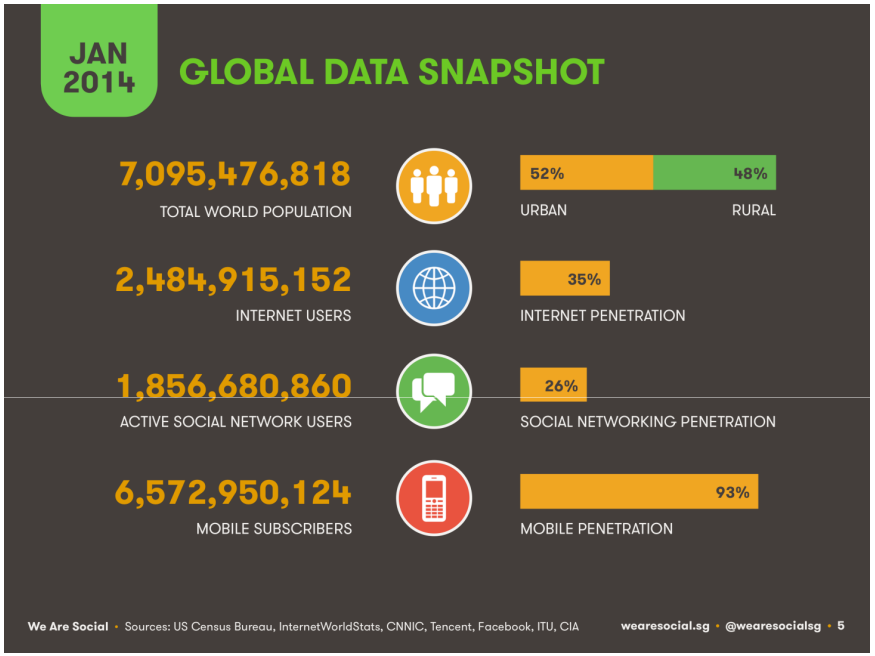
El Empoderamiento del Individuo

“Big Brother”

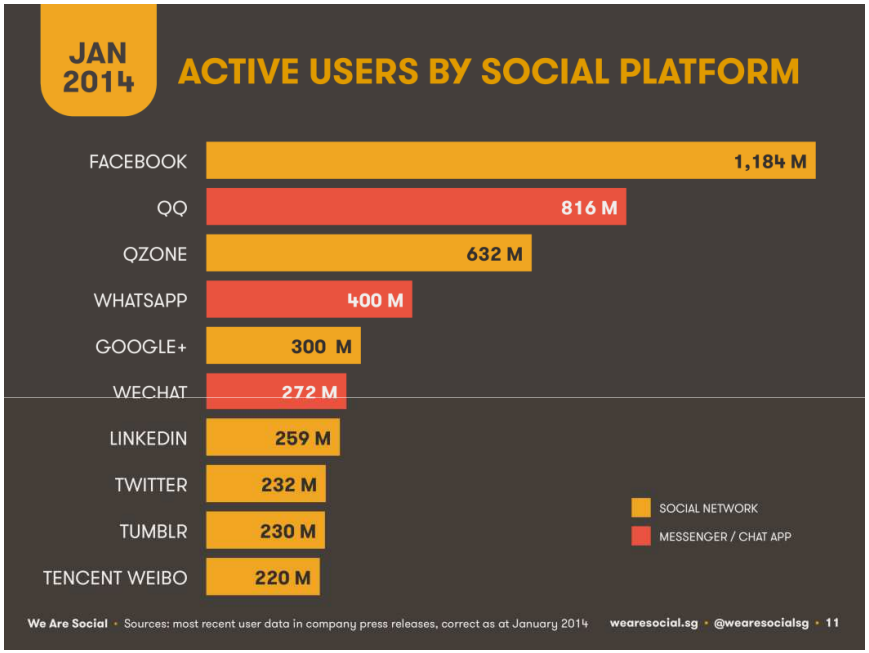
Comercial introduciendo la Apple Macintosh durante el Super Bowl de 1984
Basado en la novela “1984” de George Orwell, 1949

Datos Demográficos Internet 2014

Datos Globales



Usuarios por Plataforma Social

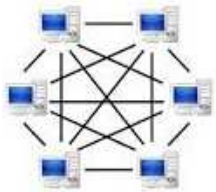


Que es Bitcoin?

Software

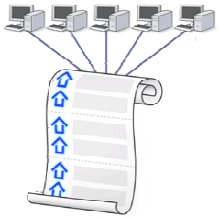
"Efectivo Programable"

- Código Abierto
- Criptografía asimétrica
- Autenticación SHA-256
- Prueba-de-trabajo



Red Descentralizada

Registro Público



Nueva Tecnología (Blockchain)

Moneda Digital

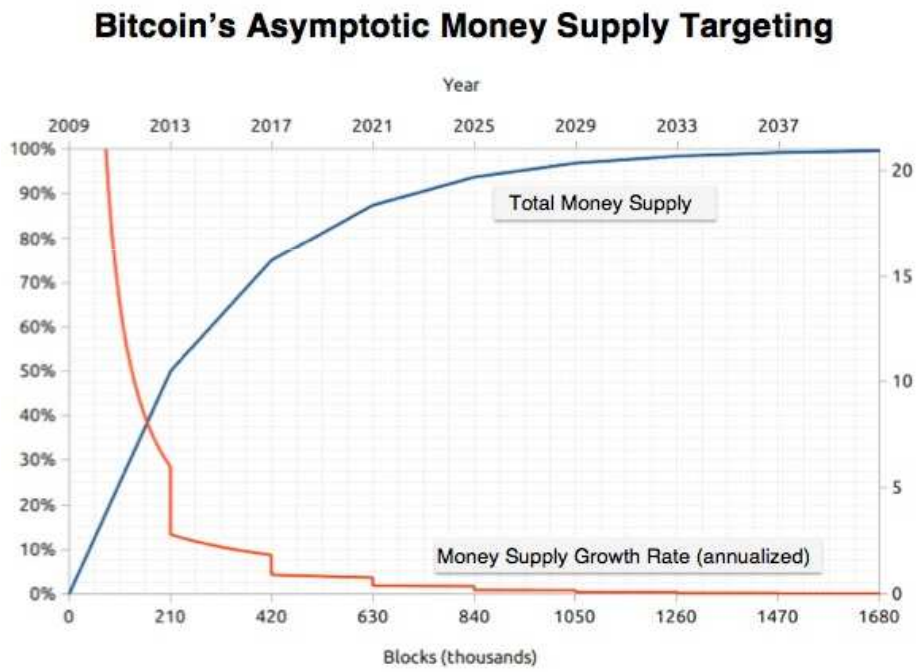
"Efectivo Digital"

Bitcoin: La Moneda

Ente cibernético autónomo y descentralizado programado para realizar un sistema de pagos

Programación de la Moneda:

- Habrán 21 millones de Bitcoin máximo en el año 2140
- La emisión/incentivo disminuye a la mitad cada 4 años.
- La unidad de moneda es divisible en 100 millones de fracciones. Dicha fraccion se le da en nombre “satoshi” en honor a su creador Satoshi Nakamoto.
- Se realiza una emisión monetaria por cada bloque completado como incentivo por ayudar a mantener y asegurar el registro.
- La prueba-de-trabajo tendrá una dificultad computacional variable para resolver cada 10 minutos en promedio.



Criptografía Usada

Criptografía Asimétrica

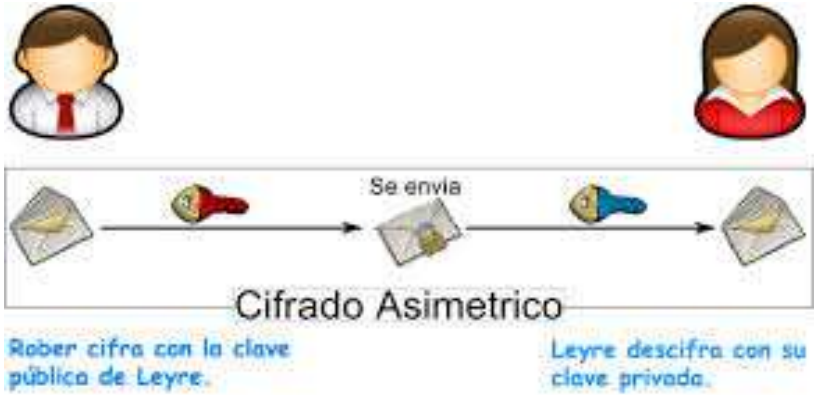
Acceso sin intercambio de contraseña (llave / candado)

Llave Privada:

5J3KcFq3KEGrepxFYf8gttMnzx5fS3rRWykDdNMjWsMQnmuRTZP

Llave Pública:

1DCKjtHCvvcUfAhhFZASYh6FD81UtPFQK7



Criptografia SHA-256

Produce una firma de autenticidad (Hash) **única** para cualquier texto o contenido digital

Los pollitos dicen pio pio pio → **SHA-256 hash** →

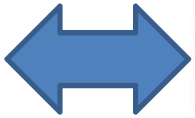
0bfc822a2e33137c2bbe7014848d49cc9e3875bf53f0576bf4dd01e37c5698ce

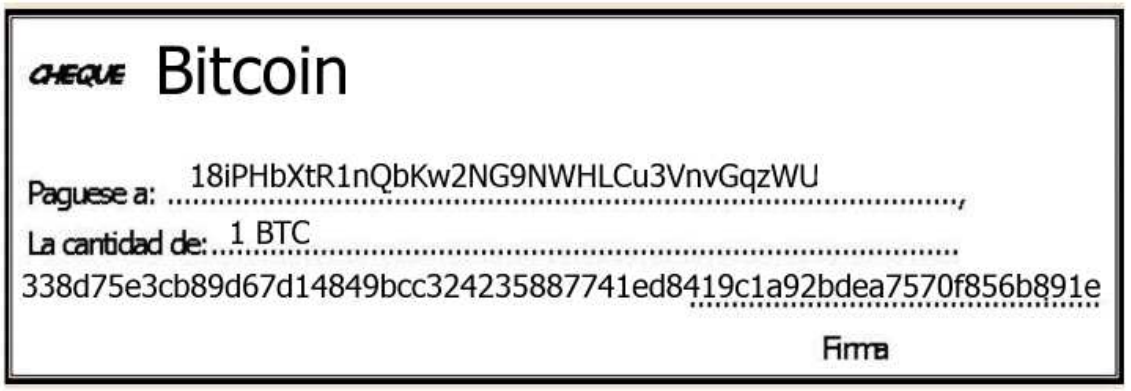
Los pollitos dicen pio pio pio. → **SHA-256 hash** →

e0e6a205e71c7b896faf61f3197fb0f4f48f395e1326bba79eb35f5517988612

Ejemplo de Transacción

Llave Publica:
1P9sAMoBwbQWp4xHt31WGXLj4bBsbhGrA7

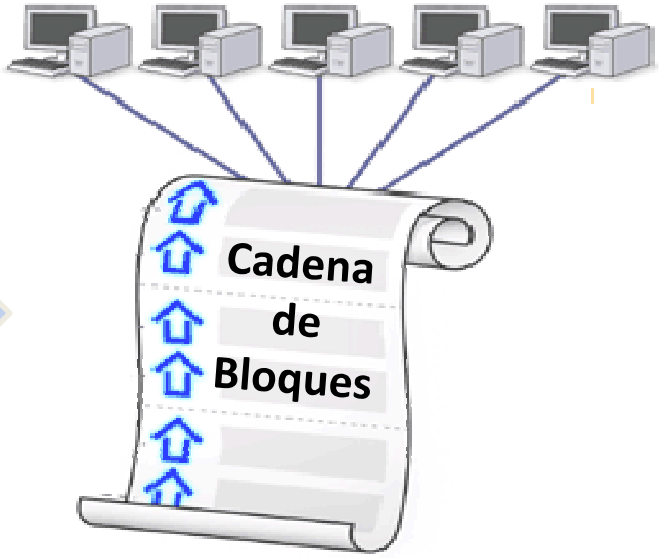




Llave Privada:
5J2pUqKkccyW7Hyhb8AWtDE7N7p4QQzvhprZvVTwS6NuNLXcYiv

Llave Publica:
18iPHbXtR1nQbKw2NG9NWHLCu3VnvGqzWU

Llave Privada:
5KAJmabNUBfP4tWt1ecD9untdnJiyAbeYTCjqqrKWdLUCUoD4bX



Registro Público

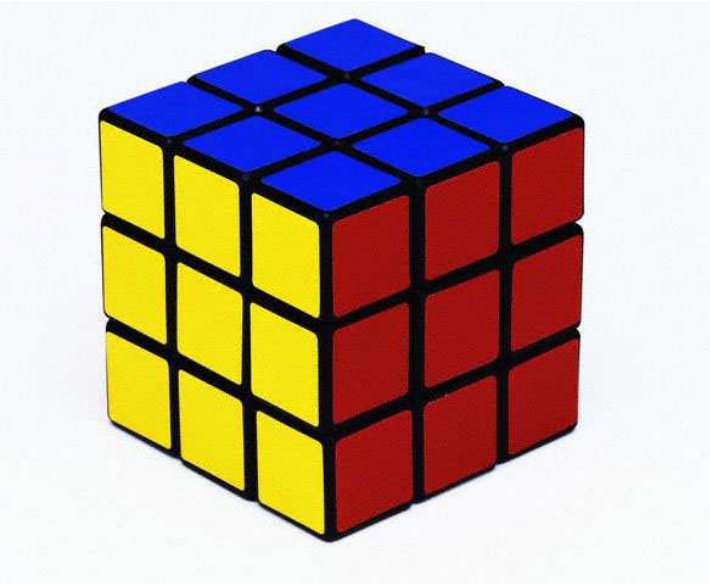
Prueba-de-Trabajo

Condicionar el acceso a un servicio determinado exigiendo que un trabajo sea realizado previamente.

Usos: Mitigación de ataques (DDoS) y SPAM

Bitcoin requiere de solventar problemas matemáticos de dificultad variable y de comprobación fácil.

Cubo Rubik – Fácil de comprobar



Sudoku – Dificultad variable

9	6	3	1	7	4	2	5	8
1	7	8	3	2	5	6	4	9
2	5	4	6	8	9	7	3	1
8	2	1	4	3	7	5	9	6
4	9	6	8	5	2	3	1	7
7	3	5	9	6	1	8	2	4
5	8	9	7	1	3	4	6	2
3	1	7	2	4	6	9	8	5
6	4	2	5	9	8	1	7	3

Mecánica del Registro Público de Transacciones

Transacción nueva

Marca de tiempo

Prueba-de-Trabajo

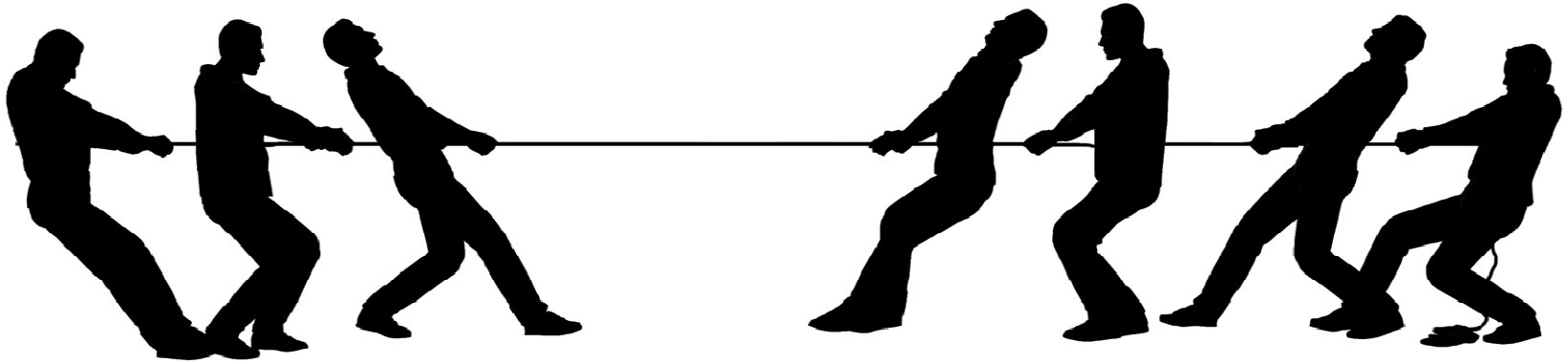
Nuevo Bloque! Hash!

Transacciones Validas!

Incentivo a seguir

Algoritmo de Consenso

Poder de Procesamiento



Reglas para resolución de disputas:

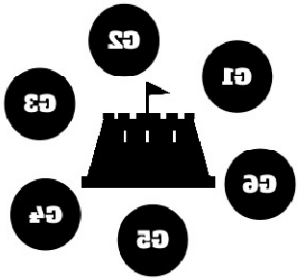
1- Los nodos trabajarán en la primera version del bloque que reciban

2- De haber dos versiones, el empate se rompe cuando la próxima prueba-de-trabajo es encontrada y una cadena se vuelve mas larga .

3- Los nodos se cambiarán a trabajar en la cadena mas larga.

Que resuelve? Que cambia?

El problema del Doble-Gasto sin ningun intermediario



El enigma informático del *“Problema de los generales bizantinos”*

Un nuevo organismo cibernético, autónomo y descentralizado que realiza una misión específica codificada en su software.
(DAO - Decentralized Autonomous Organization)

…. Pero hay algo mas…

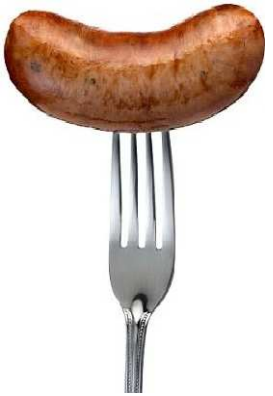
Un nuevo depósito de Confianza

ANTES:

Mejor confiar en Dios que confiar en el hombre

Mejor confiar en Dios que confiar en grandes hombres

Salmos 118:8-9



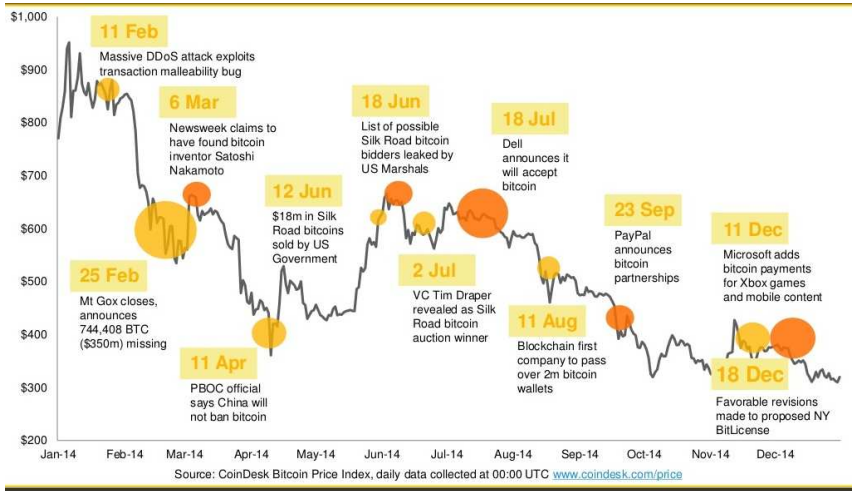
Y COMO COMPLEMENTO DESPUES:

Mejor confiar en Prueba Matemática que confiar en el hombre

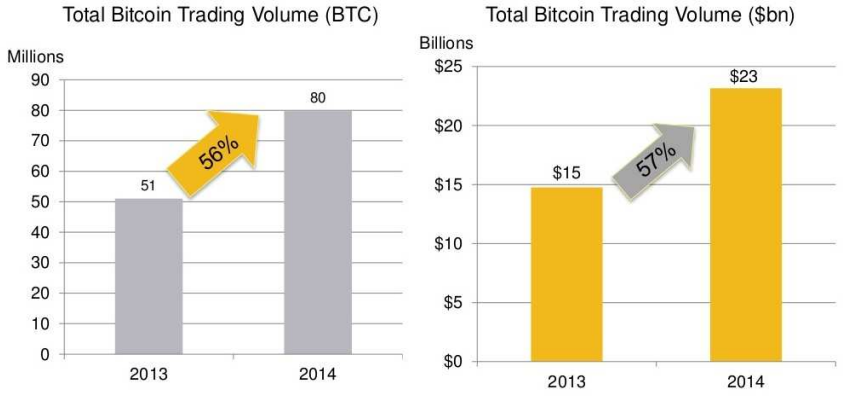
Mejor confiar en Prueba Matemática que confiar en grandes hombres

Situación Actual 2014

Precio 2014

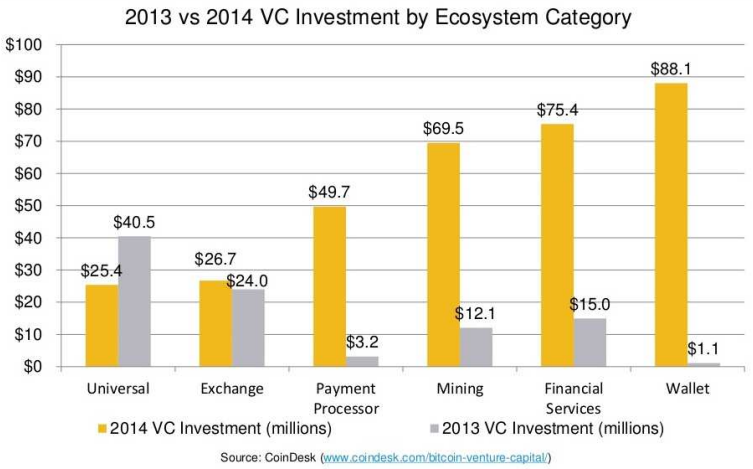


Volumen del Canje 2014



Sources: CoinDesk, Blockchain.info, Bitcoinity

Inversion por Categorías 2013-2014



Source: CoinDesk (www.coindesk.com/bitcoin-venture-capital/)

Top 10 Largest Bitcoin-Accepting Retailers

Rank	Company	Annual Revenue ($bn)
1	Microsoft	86.8
2	Dell	56.9
3	Dish Network	13.9
4	Expedia	5.0
5	Intuit	4.5
6	Monprix*	4.3
7	Time Inc.**	3.4
8	NewEgg	2.8
9	Overstock	1.3
10	TigerDirect*	1.0
	Total	**$179.9**

*Monprix is a private company; most recent revenue data is from 2005. TigerDirect estimate provided by parent company investor relations. Other divisions that are part of a larger parent organization, but do not break out individual divisional revenues, are excluded.

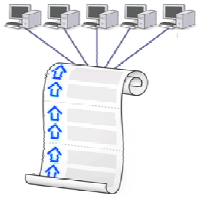
**The revenue is Time Inc. FY 2013 revenue

Sources: CoinDesk, Coinbase, BitPay, companies' annual reports

Que Esta Pasando Ahora?

Bitcoin

Blockchain 2.0



- **Infraestructura Básica**

  ARMORY bitpay BITSTAMP

  Monederos, Procesadores de Pago, Casas Cambio, Seguridad

- **Sector Financiero**

  litecoin R←BIT BTCjam

  Cripto-monedas, Micro-pagos, Remesas, Micro-prestamos.

Contratos Inteligentes

ethereum

Gobernanza

BITNATION GOVERNANCE 2.0

Internet de las Cosas

IBM Internet of Things

Plataformas de Desarrollo

NXT GENERATION

Como afectará al Mundo?

Ejercicio Especulativo

"Me sorprendería si dentro de diez años no estemos utilizando moneda electrónica - ahora que sabemos una manera de hacerlo ..."
—Satoshi Nakamoto

Costa Rican Bitcoin Painting

Recently sighted in a Hotel in Costa Rica - Seeking Identity Of Artist

"Bitcoin is a technological tour de force."
Bill Gates, Microsoft co-founder

"I do think Bitcoin ... has the potential to do something like change the world."
- Peter Thiel, Co-Founder of Paypal

Bitcoin may be the TCP/IP of money."
- Paul Buchheit, Creator of Gmail

"I own Bitcoins ... It's a great place to put assets, especially in places like Argentina"
- David Marcus, CEO of Paypal

"Bitcoin is a remarkable cryptographic achievement ..."
– Eric Schmidt, CEO of Google

"I'm a big fan of Bitcoin ... Regulation of money supply needs to be depoliticized."
Al Gore, US vice president and Nobel Peace winner