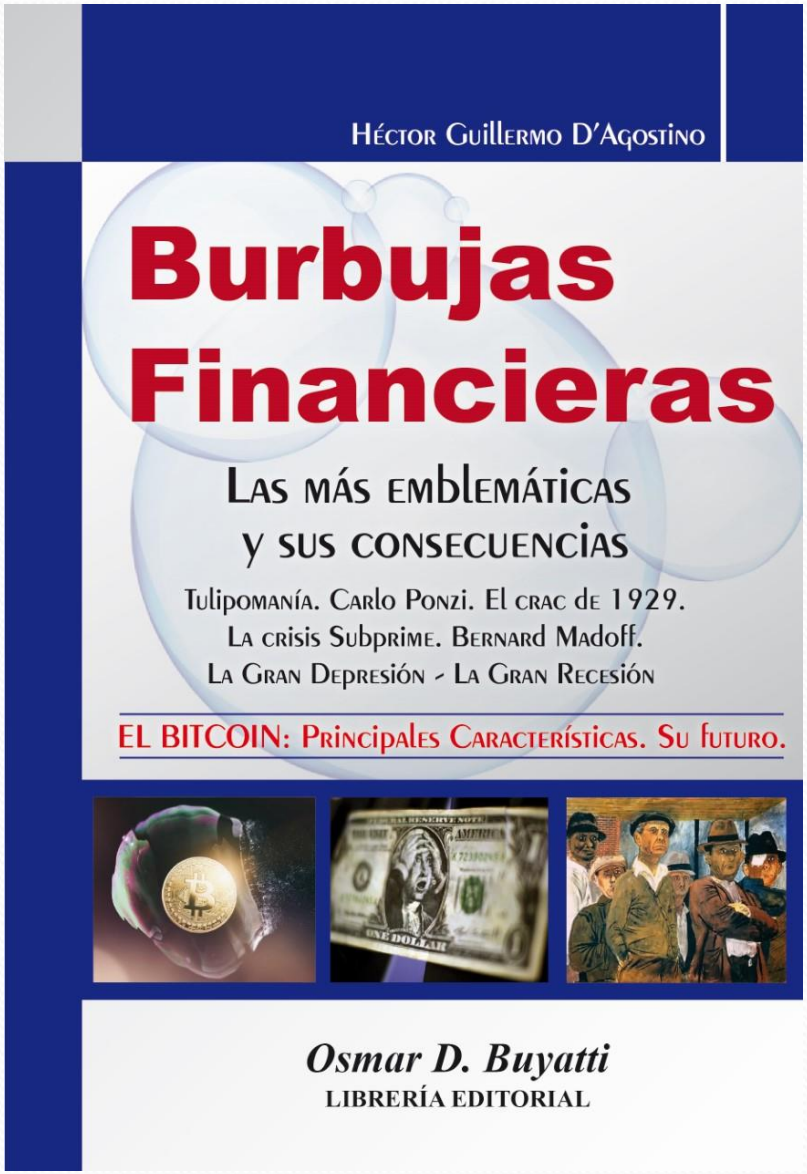
CRIPTOMONEDAS: BITCOIN


Héctor Guillermo D'Agostino
Burbujas Financieras
Las más emblemáticas y sus consecuencias
Tulipomanía. Carlo Ponzi. El crac de 1929.
La crisis Subprime. Bernard Madoff.
La Gran Depresión - La Gran Recesión
EL BITCOIN: Principales Características. Su futuro.
Osmar D. Buyatti
LIBRERÍA EDITORIAL

PAPER ORIGINAL: Satoshi Sakamoto

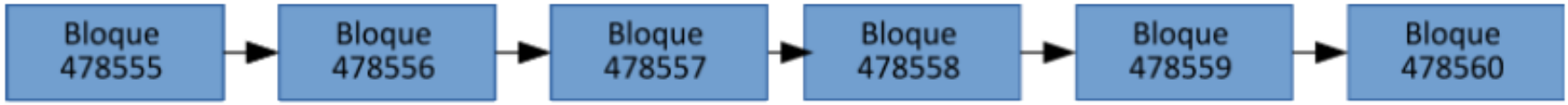
"Bitcoin: Un sistema efectivo electrónico peer-to-peer"

Publicado: 31-Octubre-2008

Solución problema "Doble Gasto", utilizando una red "Usuario-a-Usuario", con funciones criptográficas, sin Autoridad Central, etc.

BLOCKHAIN O CADENAS DE BLOQUES.

CADENA DE BLOQUES



BLOCKCHAIN o CADENA DE BLOQUES:
Tecnología que sostiene a bitcoin

- Libro Contable digital
- Bloque - Registro transacciones
- Bloques encadenados
- Distribuido
- Público
- Situado en la Nube
- Archivo histórico distribuido
- No lleva saldos, sino transacciones

LA BLOCKCHAIN DE BITCOIN ES SOLO UNA, HAY VARIAS

1ra. Transacción, bloque Génesis: 03-Enero-2009

*Registro: 50 bitcoin; Premio

Prueba: Título del Diario The Times de ese día

"CHANCELLOR ON BRINK OF SECOND BAILOUT FOR BANK"

"CANCILLER AL BORDE DEL SEGUNDO RESCATE DE BANCOS"

THE TIMES

Max 5C, min -5C | Saturday January 3 2009 timesonline.co.uk No 69523 | £1.50

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

99p

Pub chain cuts the price of a pint from £1.09 to 1989 levels
Business, page 47

Continued on page 6, col 1
Leading article, page 2

Michael Sheen
Frost, Nixon and me
Magazine

Working mums
So that's how she does it
Body&Soul

Detox in style
The best spas on the planet
Travel

Salmon Rushdie
I Won't Marry Again
Pages 22, 23

Giant Killing?
Guide to the FA Cup Third Round
Sport

THE TIMES

Max 5C, min -5C

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today **Pullout Inside**

Participantes de la blockchain

- Usuarios
- Nodos Completos
- Mineros
- Desarrolladores

USUARIOS

- Compran y venden Bitcoin
- Crean una **BILLETERA DIGITAL** donde se encuentran Registradas sus transacciones
- Cuentan con una clave Pública y otra Privada
- Clave Privada: Es su firma digital
- Pueden ofrecer pagar una comisión (fee) al Minero para que registre antes sus transacciones
- Pérdida billetera y/o clave Privada: NO hay Reclamos
- Exchanges: Cobran Comisión por operar

NODOS COMPLETOS

- Cada uno contiene:
  * Alto poder de Cómputos
  * Una copia de la Blockchain
  * Lista de transacciones pendientes
- Pueden:
  * MINAR eficazmente
  * Brindar servicios a nodos con menos peso

MINEROS

- Validan las transacciones, controlando el “doble gasto” y datos criptográficos de los usuarios
- Ninguno tiene autoridad sobre otro: **Democratización**
- Premio y Comisiones: El que registra el bloque cobra un premio en bitcoins además de las comisiones al usuario
- Premios: 2018: 12,5 bitcoins. Comenzó con 50, luego 25. A partir Mayo 2020 de 6,25. Cada 210.000 bloques se reduce a/mitad.
- En teoría cualquiera puede ser minero. Al inicio con PC hogareña, **hoy con Gran Poder de Cómputos**
- **Conspira con la democratización.**
- **Además existe Centralización**

DESARROLLADORES

- Son **PROGRAMADORES** que confeccionan y actualizan (modifican) el software
- Ninguno tiene autoridad sobre otro **DEMOCRATIZACIÓN**
  - ¿Quienes son?
  - ¿Cuántos son?
  - ¿Están cartelizados?
  - ¿Operan otras criptomenedas?

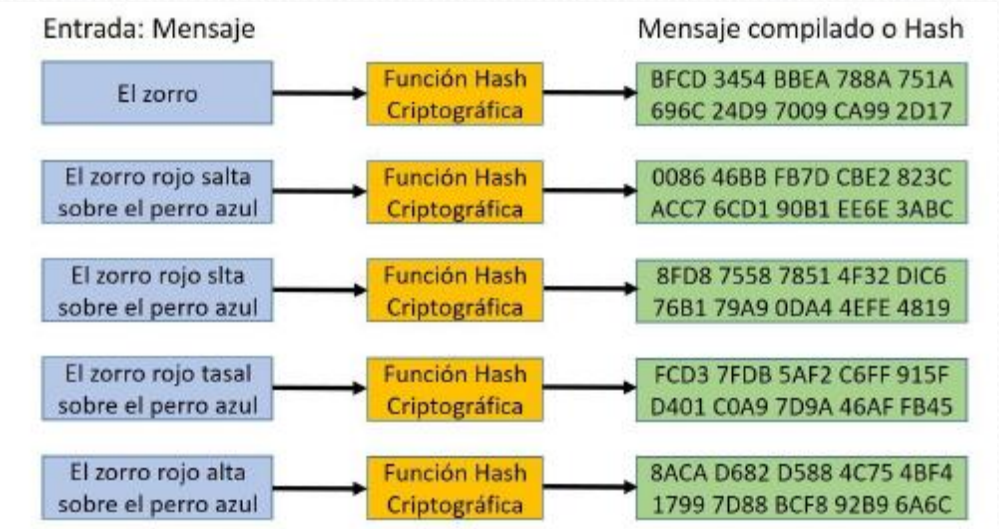
TRANSACCIONES

- Se registran en cada bloque
- Cronológicas
- No modificables
- Anónimas en cuanto a los Usuarios
- Visibles en cuanto al intercambio
- Verificables
- Funciones Criptográficas
- Prueba de Trabajo
- Validación por Consenso colectivo

- Cuando surgen transacciones entre los usuarios; todos los mineros crean inmediatamente un nuevo bloque y registran en su cabecera el **hash** del bloque anterior; luego deberán verificar las transacciones y finalmente anotar una respuesta a un problema matemático *que le envía el sistema*,

- El primero que resuelva el problema escribe al final del bloque el resultado obtenido, registra las transacciones y obtiene con toda esa información el **hash**[6] del bloque. Al mismo tiempo comunica al resto de los mineros que ha creado un nuevo bloque; éstos deberán validar la totalidad de los datos, y si no existe ningún inconveniente, el minero en cuestión -además de la comisión (fee) que pueda pagar el usuario- se gana un premio,

HASH


Entrada: Mensaje
Mensaje compilado o Hash
El zorro
Función Hash Criptográfica
BFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
El zorro rojo salta sobre el perro azul
Función Hash Criptográfica
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
El zorro rojo slta sobre el perro azul
Función Hash Criptográfica
8FD8 7558 7851 4F32 DIC6 76B1 79A9 0DA4 4EFE 4819
El zorro rojo tasal sobre el perro azul
Función Hash Criptográfica
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
El zorro rojo alta sobre el perro azul
Función Hash Criptográfica
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

CREACIÓN - EMISIÓN DE BITCOINS

- El Minero que registra un bloque puede cobrar una comisión (fee) al usuario,
- Además, en todos los casos gana un premio en bitcoins,
- En la actualidad el mismo es de 6,25 bitcons por bloque,
- El sistema prevé registrar un bloque cada 10 minutos,
- Es decir, se EMITEN desde Mayo 2020 6,25 bitcoins cada 10 minutos promedio,

Este régimen de premios es esencial para que el sistema funcione

Para registrar un bloque deberán antes resolver un problema matemático que les envía el sistema

Pero, la particularidad que presenta el problema matemático a resolver, es que no existe una fórmula para solucionar el mismo,

La solución se encuentra mediante el método “ir probando”, es decir al azar,

No hay otra manera de encontrar el resultado que mediante ésta técnica,

Como el número de bits sobre el cual van probando los mineros es muy grande, cuanto más potente sea la computadora más pruebas se podrán realizar en un determinado período,

Es decir, los mineros que quieran tener más probabilidades de solucionar los problemas que el sistema les envía, deberán invertir en este tipo de equipos,

Y ello le genera gastos adicionales: el más elevado precio de la computadora y además pagar por la mayor cantidad de energía que consume,

No obstante, esta situación conspira contra la "democratización" de la minería, ya que todos los mineros no están en igualdad de condiciones. Además, se observa una creciente centralización de los mismos que favorece la manipulación del sistema,

Bitcoin - Minerías

Los pedidos de actualización del software lo pueden hacer los usuarios, los mineros y los desarrolladores. Así, la *comunidad bitcoin*, entre otros temas, debatió en su momento, si el bitcoin debería ser una moneda de reserva reemplazando al oro, y/o un medio de pago como el dinero,

Los desarrolladores y mineros trabajan por consenso,

Como el sistema es abierto y no existe jerarquía entre los mismos, puede llegar a ser muy difícil lograr consenso,

Hay dos maneras diferentes de modificar las normas, y por lo tanto generar una cadena de bloques alternativa a la actual, a saber: **a) Bifurcación suave o soft fork, y b) bifurcación dura o hard fork**,

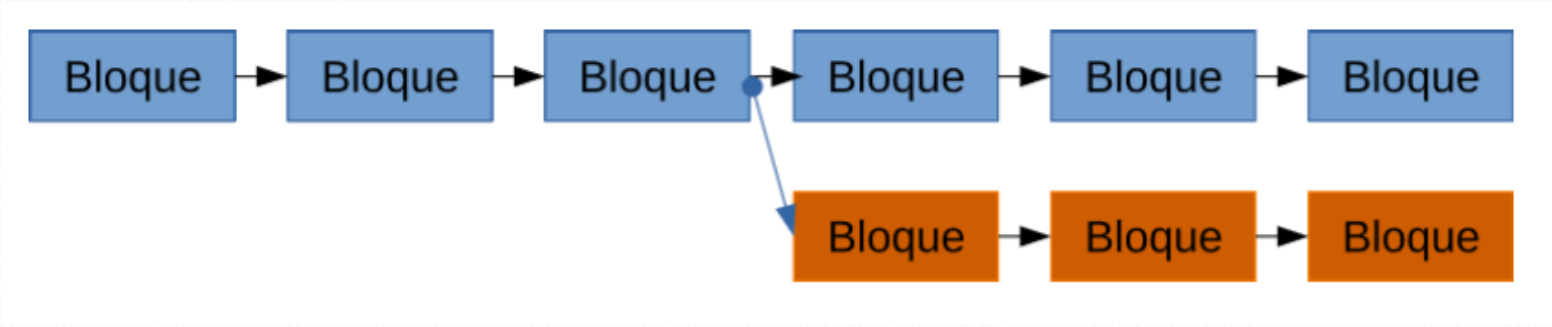
Hubo momentos que los desarrolladores tuvieron discrepancias en como actualizar los programas, es decir existieron dos versiones de software y presentaron las mismas a los mineros,

Los mineros también tuvieron diferencias sobre que software utilizar, así un grupo aceptó una versión y otro la versión diferente,

De esta manera, con una versión de software se construyó una cadena de bloques y surgió así, el 01 de agosto de 2017, el *bitcoin cash*; manteniendo -la otra cadena- el *bitcoin* tradicional. **Ocurrió un hard fork,**

SOFT FORK: Bifurcación Suave

HARD FORD: Bifurcación Dura



Pero, la novedad fue que los usuarios duplicaron sus unidades. Es decir, quien tenía por ejemplo 100 unidades de *bitcoin*, ahora se le sumaban a las mismas otras 100 unidades de *bitcoin cash,*

Las consecuencias fueron que el *bitcoin* disminuyó ligeramente su valor y *el bitcoin cash* comenzó a cotizar -en relación- con un precio muy bajo. Pero, por esos días, sumando los valores que tenían los *bitcoin más los bitcoin cash*, los usuarios habían ganado unos pocos dólares con relación al precio unitario que tenía el bitcoin antes del 01-08-2017,

Luego de ésta última fecha los *bitcoin* y los *bitcoin cash*, comenzaron a competir con las demás criptomonedas,

El o los autores del sistema han decidido que no se crearán más de 21(veintiún) millones de bitcoin.

Para que la cifra indicada anteriormente no resulte una limitación, los bitcoins pueden dividirse hasta en 8 (ocho) cifras decimales, es decir: 0,00000001. A cada uno de estos dígitos se los conoce popularmente como “satoshis”, en referencia al pseudónimo de él o los creadores. Por lo tanto,1 bitcoin es igual a 100 millones de satoshis (0,00000001 x 100.000.000 = 1),

Dicha cantidad de dígitos puede aumentar en el futuro, si las necesidades del sistema así lo requieren,

PRECIO DEL BITCOIN

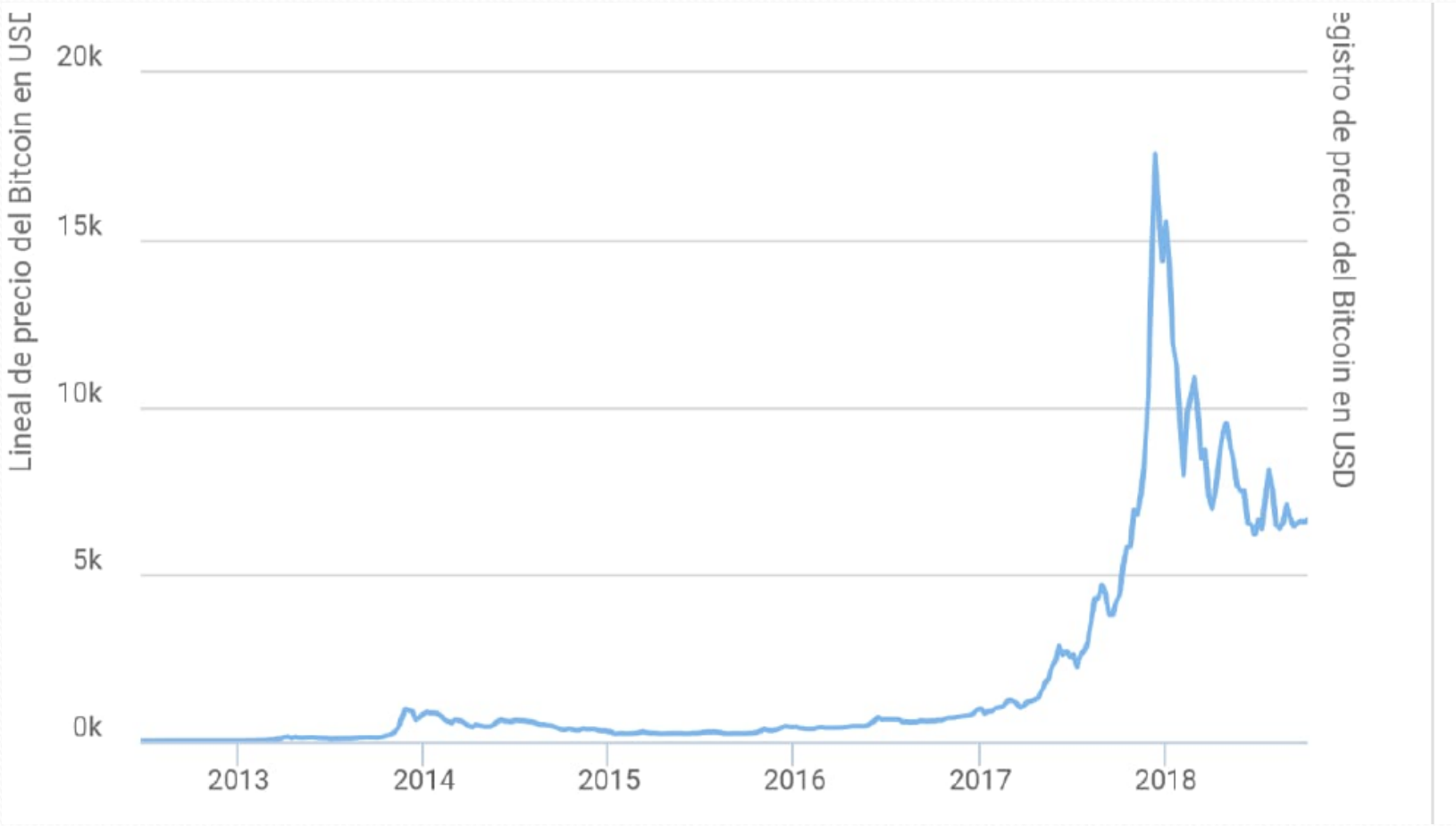
- En teoría: lo determina la evolución que tenga la oferta y demanda de los mismos,

- En la práctica: Precio promedio de los principales EXCHANGES

- También, el precio está sujeto a manipulación

HISTORIAL PRECIO DEL BITCOIN - VOLATILIDAD

2017: En: 750 -1.150 - - - My-Jn: 2.000 - 3.000 - - -02/Nov: 7.000 - - - 21/Nov: 8.100 - - **- 17/Dic: 19.798** - - - **Enero 2018**: 8.148 -11.494



EXCHANGES: Bolsas de Cambios

- COINBASE: Muy popular, Americana, Sencilla, 10 millones usuarios, 35 millones monederos. Sigue creciendo, tiene pocas criptomonedas y altos costos.
- BITTREX: Se pueden comprar y vender cerca de 200 criptomonedas diferentes.
- BINANCE: También muy popular, china.
- Otras: BITFINEX, CEO.IO (europea), etc.
- LOCALES: RIPIO, SATOSHI TANGO, BITEX.
- Hoy exigen: Identificación de los compradores.

  Ello ocasiona demoras.

MONEDEROS: WALLETS

- Dos claves: Privada y Pública
- Envío de bitcoins: solo necesito saber la clave pública, luego el receptor la acepta con su clave privada.
- Perdida de la clave privada: Pérdida de los bitcoin.
- Desde 2009 hasta mediados de 2018: Existen cerca de 5 millones btc inaccesibles, sobre 16,5 m. emitidos a esa fecha.
- Monedero: no tiene el saldo de btc, sino a través de la clave privada permite visualizar en la red todas las transacciones.
- Populares: Electrum, Jaxx, Rippex, Exadus, etc.
- Custodia de Monederos: Se puede tercerizar.

SEGURIDAD QUE PRESENTA LA RED BITCOIN:

La seguridad informática es uno de los aspectos menos confiables que exhibe el sistema bitcoin y en general todas las criptomonedas. Así, podemos nombrar como ejemplos, los ataques por parte de hackers que sufrió Corea del Sur en 2017; en enero de 2018 ocurrió en Japón otro ataque en el que desaparecieron monedas virtuales por un valor cercano a los 453 millones de dólares[10], etc.

EL BITCOIN ¿ES UNA MONEDA?:

Las principales funciones que debe tener una moneda son (deben ser):

- **Medio de Cambio**: Es aceptada por toda la sociedad para realizar negocios y cancelar deudas. Es ésta la más importante función,
- **Unidad de Cuenta:** Sirve para determinar precios, es decir, cuánto valen los bienes y servicios que se comercian en el mercado, y
- **Depósito de Valor Estable:** Permite conservar riqueza a través del tiempo proporcionando liquidez plena.

ARGUMENTOS DE LA COMUNIDAD BITCOIN:

- ¿Cuál es el respaldo que tiene la principal moneda del mundo, el dólar estadounidense, a partir de 1971, cuando el Presidente Richard Nixon suspendió su convertibilidad con el oro?,

- ¿Cuál es la confiabilidad que tiene una moneda que emerge como consecuencia de la emisión sin respaldo de los Bancos Centrales?,

- Cuando los bancos efectúan préstamos con los depósitos a la vista de sus clientes; también están creando dinero,

- Continúan expresando: Es decir, estamos en presencia de *dinero fiat,* que es aquel cuya validez emana de una ley,

- En consecuencia, cuando los usuarios del bitcoin vayan adquiriendo más confianza en el mismo, se parecerá bastante a una *moneda fiat,*

- El algoritmo del sistema bitcoin representa al Banco Central de las monedas tradicionales, con la ventaja de que sus normas se determinan en forma descentralizada y por consenso. No existe un ente superior que fije de manera forzosa las reglas, etc..

ALGUNAS CONSIDERACIONES FINALES (I)

* Algoritmo (certeza matemática) *Vs* Normas de BC
* **Quienes realizan el algoritmo *Vs* Funcionarios BC**
* Anonimato con inseguridad Jurídica *Vs* Visibilidad c/relativa SJ
* Manipulación-Volatilidad *Vs* Default-Inflación (Países en VD)
* **OLIGOPOLIO Desarrolladores/Mineros *Vs* MONOPOLIO BC**
* COMPUTADORAS: ¿Podrían salir con mas capacidad para manipular o destruir la blockchain?

ALGUNAS CONSIDERACIONES FINALES (II)

- No se puede analizar con certeza al emisor
- No existe un contrato "Emisor - Usuario"
- REGULACIÓN: Impredecible, Limitar o Prohibir

¿SERÁ VIABLE EL SISTEMA LUEGO DE LOS 21 MILLONES?

FALTA DE REGULACIÓN

- Positivo: Favorece la innovación tecnológica.
- Negativo: No ingresa el dinero institucional. Si pierdo o me roban btc, no hay a quien reclamar.
- Bueno: lograr una regulación razonable que permita la innovación.

CONCLUSIÓN:

Por último, resulta obvio explicitar que aún no está todo dicho con las criptomonedas (también denominadas criptoactivos). Es evidente y preocupante la elevada inseguridad que presentan en los temas informáticos, jurídicos y la volatilidad de sus precios. Además, al ser técnicamente un sistema en permanente evolución no garantiza cuál será su final. Sabemos también que no es una moneda, por lo tanto; dejando de lado las operaciones que se realizan fuera de la ley y **las manipulaciones que puedan efectuarse al sistema**: ¿Qué razones tendría una persona o entidad para cambiar dinero real por una criptomoneda? La respuesta es sencilla, la ilusión de ganar mucho dinero en un determinado período de tiempo. Es decir, **estamos en presencia de una burbuja financiera.** Que tamaño llegará tener ésta burbuja, cuando estallará, o si contrariamente, se desinflará poco a poco; si las entidades financieras crearán sus propias criptomonedas, etc.; son cuestiones que nadie sabe con certeza.

ALGUNAS PÁGINAS WEB

http://elbitcoin.org

Información general sobre finanzas y bitcoin (publicidad)

http://bitcoinblockhalf.com

Como comprar bitcoin.

Estadísticas:

- *Total de bitcoins en circulación (1)*
- *Total de bitcoins que restan emitir: 21.000.000 menos (1)*
- *Precios*
- *Cantidad de Bloques Registrados*
- *Tiempo aproximado para la creación de un bloque, etc.*

Https://www.buybitcoinworldwide.com/es/precio/

Gráfico de historial del precio de Bitcoin

http://btcbitcoin.blogspot.com

Refleja los usuarios que se encuentran infectados

http://coinmarketcap.com

Precios de las 100 principales criptomonedas

https://deadcoins.com

Criptomonedas que desaparecieron de circulación

GRACIAS POR V/TIEMPO