Antecedentes: bitcoin y ethereum

Blockchain y computación cuántica

CONTENIDO

Objetivos

- Comprender los principales acontecimientos, la operativa y las características de *bitcoin*.
- Entender las características y los distintos tipos de *wallets*.
- Profundizar en el funcionamiento y características de *ethereum*.
- Comparar *bitcoin* y *ethereum*.
- Conocer otras soluciones DLT.

Introducción

La tecnología *blockchain* cuenta con un recorrido de poco más de 10 años. Con el lanzamiento de *bitcoin* en 2009 se establece la primera generación de la tecnología, conocida como *blockchain* 1.0, esta primera generación está orientada a ofrecer soluciones de monedas digitales o criptomonedas.

La aparición de los *smart contracts* en 2015 con el lanzamiento de ethereum, establece una nueva generación denominada *blockchain* 2.0, donde la tecnología *blockchain* permite la ejecución de programas que almacenan información y pueden proporcionar servicios, situando a *blockchain* más allá de las monedas digitales.

Blockchain 1.0: bitcoin

Bitcoin marca el comienzo de la tecnología *blockchain* y forma parte de un primer conjunto de soluciones centradas en las criptomonedas, asociadas a lo que se conoce como *blockchain* 1.0.

Creador

Satoshi Nakamoto es el seudónimo del creador o creadores de *bitcoin*, red que comenzó a funcionar en 2009. El objetivo de *bitcoin* es proporcionar un **sistema de pago distribuido** que no requiere la intervención de instituciones financieras. Se basa en la **criptografía** para generar firmas digitales y en **funciones** *hash* que permiten generar identificadores únicos para los bloques que almacenan las transacciones ejecutadas y que componen la cadena de bloques. Estas funciones hash se utilizan como parte fundamental del reto que establece el algoritmo de prueba de trabajo.

La identidad de Satoshi Nakamoto es desconocida. En alguna ocasión afirmó ser un varón japonés de 37 años, pero siempre se ha especulado con que es poco probable debido a su perfecto inglés y al hecho de que el software de bitcoin no está ni documentado ni etiquetado en japonés.

El especialista en seguridad Dan Kaminsky [1] analizó el código de *bitcoin* y afirmó que Satoshi o era un genio o un grupo de personas con altísimos conocimientos de seguridad y criptografía.

El código de *bitcoin* se considera un desarrollo genial que difícilmente podría haber desarrollado una sola persona.

Satoshi [2] [3] colaboró con otros programadores que se unieron al proyecto hasta mediados de 2010, cuando entrega el control del repositorio del código fuente y la clave de alerta de la red a Gavin Andresen. Satoshi transfiere los dominios relacionados a miembros destacados de la comunidad *bitcoin* y pone fin a su actividad en el proyecto.

Características

Bitcoin [4] establece en **21 millones el número máximo de BTC** en circulación. La recompensa por generar un bloque se divide por la mitad aproximadamente cada 4 años, este hecho se conoce como halving event y representa un cambio de era.

- **Era 1:** 2009 – 2012 recompensa 50 BTC
- **Era 2:** 2012 – 2016 recompensa 25 BTC
- **Era 3:** 2016 – 2020 recompensa 12,5
- **Era 4:** 2020 – 2024 recompensa 6,25

Bitcoin está programado para tener 32 *halving*, el último año en que se recibirá recompensa por el minado de un bloque será 2140. Hay que tener en cuenta que al final de la era 3 se habrá generado cerca del 88 % de los BTC totales.

- Número máximo en circulación posible: 21 000 000 BTC
- Fracciones: hasta 8 decimales. Último decimal Satoshi
- Fecha del último BTC: 2140
- Se encuentra en el *halving* # 2 que termina en 2020.
- En 2020 se entrará *halving* # 3 (2020-2024).
- 32 posibles *halving* llevan a 2140.
- A partir de 2140 no es posible plantear más producción porque se exceden los 8 decimales.

Acontecimientos destacados

- Mayo 2010. Se produce la **primera operación en el mundo real** con la compra de dos pizzas por 10 000 *bitcoins* [5].
- Octubre del 2010. Se produce el primer intercambio de dinero por *bitcoins*.
- Junio 2011. *Mt.Gox* [6] sufre un ataque de un *hacker*, afectando a 60 000 clientes.
- Julio 2011. Desaparece *mybitcoin*.com [7].
- Noviembre 2013. El banco central de China (5/12/13) emite una norma por la que excluye a *bitcoin* del sistema financiero.
- Marzo 2017. Se producen las primeras ETFs de *bitcoin* (Winklevoss y SolidX) que son denegadas por la SEC americana repetidamente.
- 2017. China prohíbe las casa de cambio de criptomonedas y *binance* [8] deja de operar en China por las restricciones.
- Enero 2018. El precio *(figura 1)* de *bitcoin* cae por debajo de los 8000 dólares después de haber llegado a rozar los 20 000 dólares en diciembre de 2017. Esta caída se debe al anuncio de varios países de medidas para controlar las actividades de financiación realizadas sobre *blockchain*.
- En mayo de 2018 la capitalización total de *bitcoin* llega a los 100 000 millones de dólares [9].
- En mayo de 2019 *binance* sufre un robo de 40 000 000 de dólares en criptomonedas.
- *Bitcoin* es la criptomoneda más importante y la que más capitalización tiene en la actualidad.

Comunidad

La comunidad de *bitcoin* ha permitido la divulgación del funcionamiento de *bitcoin* y extender su uso a nivel global [11].

Todas las comunidades tienen un papel **muy importante en** *blockchain*, las comunidades suelen ser de dos tipos, la **de mineros** y la de **desarrolladores**.

Ambas comunidades son importantes para la toma de decisiones sobre el presente y el futuro de un *blockchain*. En marzo de 2013 [12] la comunidad de *bitcoin* debatió sobre la necesidad de volver a una versión anterior del software por los nuevos parámetros introducidos al minado en la nueva versión. La comunidad de *bitcoin* decidió, finalmente, volver a la versión anterior, lo que obligó a deshacer la cadena y volver a ejecutar las transacciones de nuevo. Este hecho proporciona una visión clara del poder de la comunidad para definir el futuro de *bitcoin*, pero también establece un precedente de modificación de la cadena que volvió a sugerirse cuando en mayo de 2019 *binance* fue víctima de un ataque. En este caso la comunidad desestimó la opción de rehacer la cadena por lo que *binance* no pudo recuperar las criptomonedas robadas.

¿Cómo se pueden obtener *bitcoins*?

- Se pueden obtener como pago por un bien o un servicio.
- Se pueden comprar en una casa de cambio (*exchange*).
- **Intercambiándolos** con alguien cercano.
- Como resultado de la participación del **proceso de minería**.

¿Cómo se realiza un traspaso de *bitcoins*?

Actualmente, existen multitud de aplicaciones para realizar pagos con *bitcoin*, estas e pueden realizar desde un ordenador o un dispositivo móvil. Los datos que han de rellenarse para enviar una transacción son los se indican en la figura 2.

Wallets

Una *wallet* es la cartera digital donde se **almacenan las claves** que permiten controlar las direcciones *blockchain*. Las *wallet* no almacenan criptomonedas, solo las claves que permiten controlar las direcciones *blockchain*.

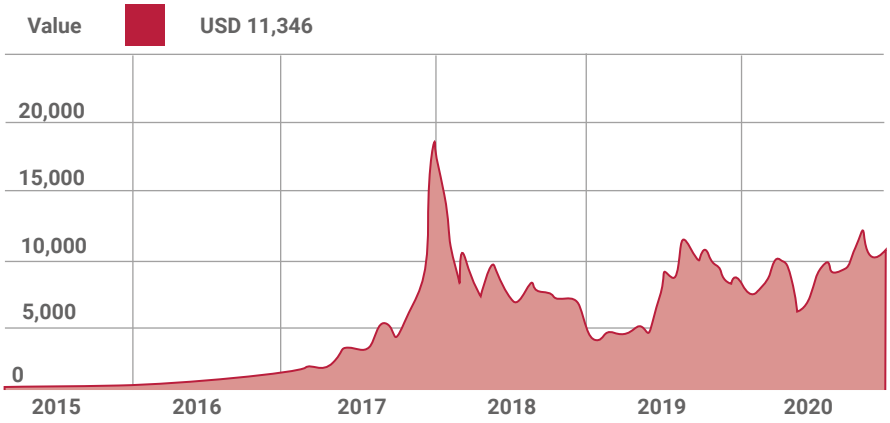


Figura 1. Histórico cotización *bitcoin* [10].

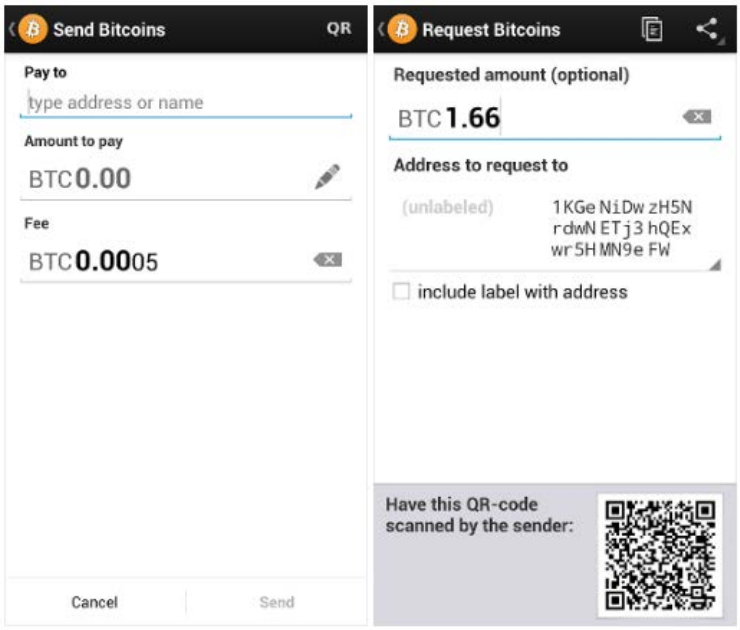


Figura 2. Imagen envío de *bitcoins* [13].

Por motivos de seguridad las criptomonedas se separan en dos *wallet*:

- ***Hot wallet:*** es aquel monedero conectado a internet.
- ***Cold wallet:*** es el monedero que no está conectado a internet, por lo tanto, es más difícil para los atacantes poder sustraer las claves. Puede ser un dispositivo físico que solo se utiliza en momentos puntuales.

Desventajas de *bitcoin*

Bitcoin es una moneda digital que está expuesta a una gran volatilidad, aunque se espera que a medida que tenga más participantes esta volatilidad se reduzca.

El consumo de energía que requiere el minado es otra de las desventajas. Según el estudio [14] del consumo de energía anual equivale al que realiza Austria.

Aunque esta red permite el intercambio de bienes y servicios, el tiempo que hay que esperar para la confirmación de las transacciones genera problemas a la hora de implantar *bitcoin* como medio de pago de masas.

Blockchain 2.0: *ethereum*

El término de *blockchain* 2.0 hace referencia a la evolución de *blockchain* 1.0 al incorporar la funcionalidad de *smart contracts*. El primer *blockchain* considerado 2.0 es *ethereum*.

Creador

Vitálik Buterin [15] se interesó por bitcoin en 2011 y poco más tarde fue cofundador y editor en jefe de *Bitcoin Magazine*.

A mediados de 2014 **propuso crear** *ethereum*, un sistema distribuido de pagos donde **se pudieran ejecutar** aplicaciones, añadiendo, de esta manera, una nueva característica a *blockchain*. Tras conseguir la financiación de su proyecto, *ethereum* empezó a funcionar en julio de 2015, siendo el primer *blockchain* que permitía la ejecución de código almacenado en la cadena de bloques. Esta nueva funcionalidad de *ethereum* se denominó *smart contracts*.

Características

Ethereum [16] dispone de su propia **criptomoneda llama** *ether* (ETH) y a diferencia de bitcoin la cantidad de ethers no está limitada.

El minado de bloques se realiza de media cada **15 segundos** y el mecanismo de consenso con el que nació es el de prueba de trabajo.

Inicialmente la recompensa que recibía el minero ganador era de 5 ETH, con el tiempo esta recompensa se ha ido reduciendo de manera progresiva.

Ethereum cuenta con una máquina virtual (**EVM**) que se encarga de **ejecutar el código de los** *smart contracts*.

Solidity es un lenguaje de programación de alto nivel desarrollado por el equipo de *ethereum* para el desarrollo de *smart contracts*.

Ethereum funciona como una máquina de estados. Las cuentas tienen asociado un saldo o estado que se va actualizando con la ejecución de las transacciones.

Funcionalidades

Permite realizar transacciones de ETH, lo que significa que es una plataforma de pagos con su moneda digital.

Se pueden **ejecutar** *smart contracts* que se almacenan dentro de *blockchain*, permitiendo establecer **reglas que determinan el comportamiento de la información recibida o guarda por el** *smart contract* en *blockchain*. De esta manera, una empresa puede registrar en *blockchain* la fabricación y entrega de un producto, haciendo que un *smart contract* almacene la trazabilidad del producto.

Se pueden realizar transacciones entre *smart contracts*, de esta manera, se pueden establecer servicios en *smart contracts* que sean utilizados por otros *smart contracts*.

La red de **nodos puede almacenar ficheros** que se trocean y se distribuyen utilizando *swarm*. Estos ficheros no se guardan en *blockchain*, pero el identificador que permite recuperar el fichero puede almacenarse en *blockchain*. Esto permite registrar un fichero a una dirección de *blockchain*.

Operaciones

Ethereum al contar con *smart contracts*, dispone de tres **tipos de transacciones** que permiten realizar las siguiente operativas:

- **Envío** de una cantidad de *ether* de una cuenta origen a otra cuenta destino.
- **Despliegue del código** de un *smart contracts*.
- Ejecución de un *smart contract* con una serie de argumentos.

Estas son las transacciones que ofrece *ethereum* para realizar las operativas que permiten transferir *ethers* y desplegar y operar con *smart contracts*.

Acontecimientos destacados

En julio de 2016 *ethereum* **se divide** generando dos líneas activas:

- *Ethereum* (ETH)
- *Ethereum Classic* (ETC)

Estas dos líneas aparecen como consecuencia de un fallo de programación encontrado en un *smart contract* denominado *The DAO* [17], donde un hacker consiguió robar 3 600 000 de ETH equivalente a 70 000 000 de dólares. La decisión de generar dos líneas se debe a la división que se generó en la comunidad de *ethereum* entre los que querían restaurar la cadena de bloques parar arreglar el bloqueo producido en el *smart contract* '*The DAO*'. Los partidarios de no modificar a cadena defendiendo que *blockchain* no se altera para corregir problemas derivados de la mala programación de un smart contract.

'*The DAO*' condicionó el *blockchain* de *ethereum* y propicio una caída considerable en la cotización *(figura 3)* del ETH.

En 2017 las *Initial Coin Offering* (ICO) se hacen muy populares, como instrumento de financiación para proyectos. Una ICO no es más que un conjunto de *smart contracts* que permiten recibir pagos en ETH y asignan un número de tokens a la dirección que realiza el pago. La idea es que estos tokens puedan ser intercambiados por un bien o servicio cuando el proyecto que se completa.

La popularidad de las ICO hace que el precio *(figura 4)* del ETH crezca rápidamente en 2017. Este auge en el uso de la criptomoneda hace que el número de nodos activos crezca por encima de 25000 (*ethernodes*).

En 2017 se empieza a cuestionar la escalabilidad de *ethereum* y se critica el gran consumo energético que produce la red de nodos de *ethereum*. La organización de *ethereum* busca soluciones a los retos de *blockchain* y plantea un cambio de algoritmo de consenso con la finalidad de permitir mayor escalabilidad y reducir el coste energético del minado de bloques.

En 2018 las ICO empiezan a hacer frente a las diferentes regulaciones que imponen la mayoría de los países. Esto hace que muchos de los proyectos que empezaron con una ICO fracasen. La cotización *(figura 4)* de *ethereum* y el resto de monedas baja considerablemente en el primer cuarto de 2018.

Figura 3. Cotización *ethereum* 2016 [18].

Figura 4. Cotización *ethereum* 2017 – 2018 [19].

En 2018 el rumbo de *ethereum* se ve modificado, debido al rechazo de la comunidad al cambio que supone pasar de *proof of work* (PoW) a *proof of stake* (PoS).

En 2019 *ethereum* afronta una situación complicada, el volumen de transacciones se reduce notablemente y el foco regulatorio afecta al precio del ETH. La consecuencia es que el número de nodos disminuye considerablemente, al no ser rentable la actividad de los mineros y pone en riesgo la continuidad del proyecto.

En 2020 se espera que se implante definitivamente *ethereum* 2.0, momento en que el algoritmo de consenso de la red de *ethereum* pasará a ser PoS.

Comunidad

La comunidad de ethereum es la más grande de blockchain, cuenta con un gran número de desarrolladores que no solo actualizan el software de ethereum, sino que realizan sus propias aplicaciones distribuidas (DApp) [20].

Una *DApp* es una aplicación distribuida, lo que quiere decir que no se conecta a un servidor central y que la lógica de la aplicación se incluye en *smart contracts* desplegados en la red *blockchain (figura 5)*.

Comparativa

La comparación de los dos blockchain más representativos permite comprender mejor las características de cada uno de ellos y lo que es más importante entender la diferencias que existen entre *bitcoin* y *ethereum (tabla 1)*.

	Bitcoin	*Ethereum*
Comienzo	2009	2015
Criptomoneda	BTC	ETH
Propósito	Sistema de monedas digitales	Plataforma descentralizada para desarrolladores
Límite de criptomoneda	21 millones	Sin límite
Algoritmo de consenso	PoW	PoW -> PoS (2021)
Smart contracts	No	SI

Tabla 1. Tabla comparativa *bitcoin* / *ethereum*.

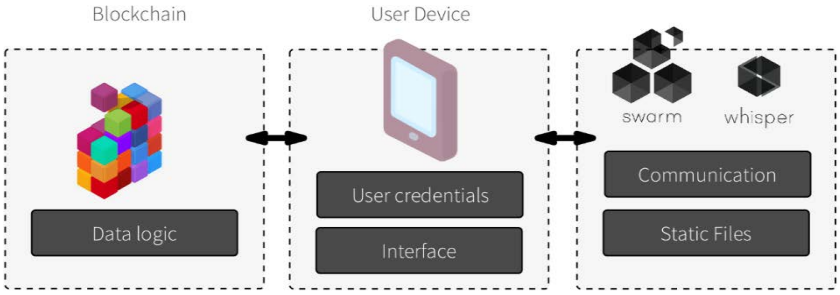
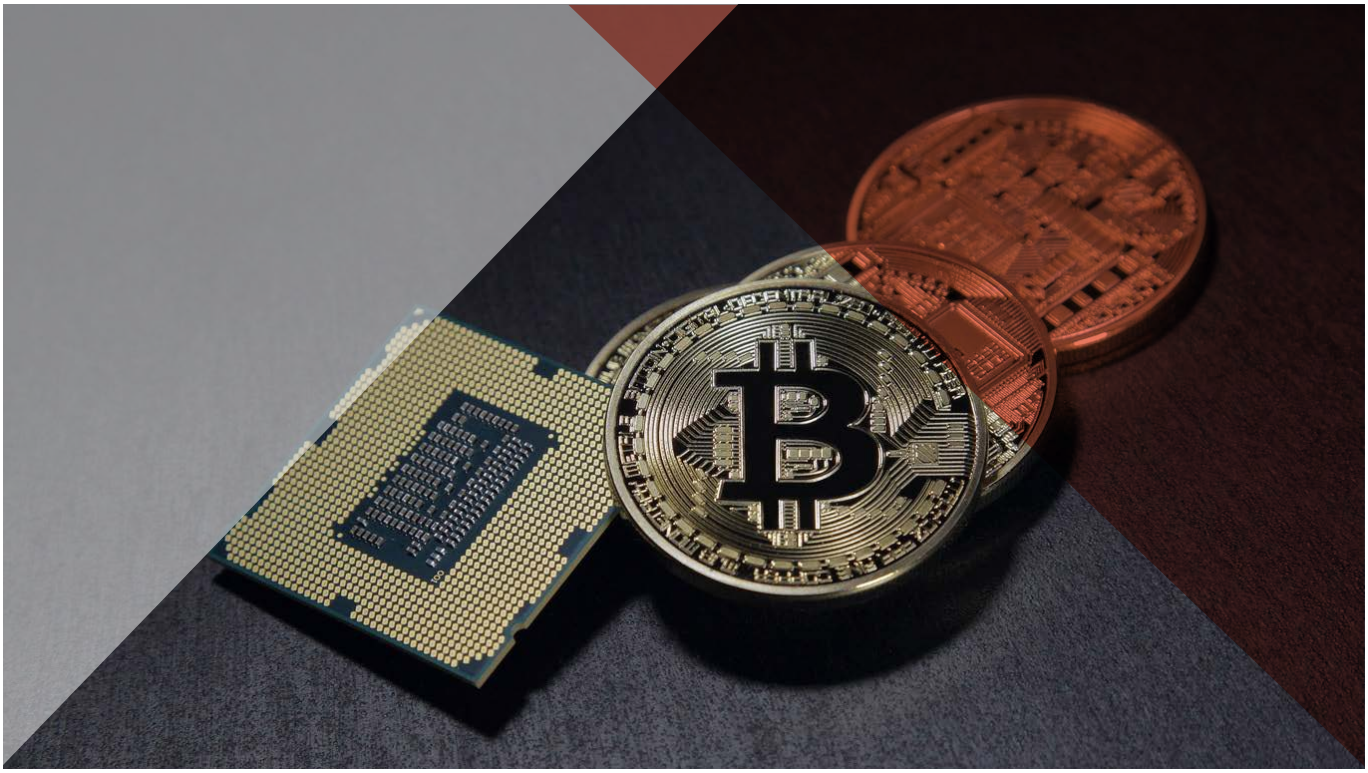


Figura 5. Imagen aplicación distribuida *ethereum* [21].



Aunque ambos *blockchain* comparten características, *ethereum* proporciona un entorno mucho más completo con el soporte de *smart contracts*. Actualmente, *ethereum* está inmerso en un proceso de cambio de algoritmo de consenso lo que va a permitir alcanzar las 10 000 transacciones por segundo.

Futuro de *blockchain* y DLT

Tras la aparición de *ethereum* han surgido un gran número de *blockchain* que ofrecen mayor número de transacciones por minuto, más escalabilidad, múltiples lenguajes de programación para *smart contracts* y otras muchas características como parte de la evolución de la tecnología *blockchain*.

Las empresas cada vez disponen de una oferta de soluciones *blockchain* más amplia, que se une a la necesidad de las empresas de ser más transparentes y ofrecer servicios donde el usuario tenga un mayor control sobre su información. En este aspecto existen varias iniciativas para generar identidades digitales basadas en *blockchain* que permiten a los ciudadanos tener un mayor control de la información que los ciudadanos proporcionan a empresas y organismos.

Se espera que *blockchain* llegue a dispositivos pequeños dotándolos de una identidad dentro de la red *blockchain*, lo que abre la puerta a un mundo mucho más independiente y a la necesidad de establecer reglas de comportamiento no vinculadas a fabricantes o proveedores. Es en este punto donde los *smart contracts* tienen un gran potencial para desarrollar tecnologías como el internet de las cosas (IOT).

El futuro de *blockchain* no está asociado a una única solución de *blockchain*. Actualmente, existen decenas de soluciones *blockchain* y el tiempo determinará cuales de estas propuestas se ha adaptado mejor a las necesidades de los usuarios. En el futuro existirán diferentes *blockchain* que tendrán que comunicarse entre ellos generando un conjunto de ecosistemas de información basados en las principales características de *blockchain*. También se utilizarán herramientas que permitan interconectar la información entre diferentes *blockchain* con la finalidad de proporcionar unos ecosistemas más abiertos y flexibles.

La tecnología *Distrubuted Ledger Tecnology* (DLT) [22], que se puede traducir como tecnología de libro mayor distribuido es un sistema que permite registrar información de manera distribuida. *Blockchain* es una solución DLT, pero existen otras, como las soluciones basadas en *Directed Acyclic Graph* (DAG) o grafos acíclicos dirigidos que organizan la información en forma de grafo, donde cada nueva transacción ha de validar al menos dos transacciones previas, generando un sistema que permite el intercambio de información sin el concepto de nodos mineros y con una gran capacidad para procesar mayores volúmenes de información. Esta propuesta está pensada para entornos donde se requiera procesar un gran volumen de transacciones. Esta es una solución que está en pleno desarrollo y, actualmente, existen pocas soluciones completamente operativas, pero ofrecen un nuevo camino dentro de las soluciones DLT que puede ser muy interesante en ciertos sectores relacionados con IOT. Un ejemplo de una solución basada en DAG es COTI [23] que se basa en un algoritmo de consenso que utiliza *machine learning*, que permite reducir considerablemente el costo de las transacciones a la par que ofrece mayor velocidad de procesado.

Resumen

La evolución de la tecnología *blockchain* es imparable, desde el comienzo de bitcoin que surge con el objetivo de ofrecer una plataforma de pagos sin la necesidad de organismos financieros, han aparecido numerosas soluciones *blockchain* que han ido mejorando las capacidades ofrecidas por *bitcoin*.

Con la aparición de *ethereum*, *blockchain* se trasforma en una tecnología capaz de ofrecer soluciones de negocio más allá del entorno financiero. Los *smart contracts* proporcionan una nueva funcionalidad que cambia el rumbo de *blockchain*.

La aparición en 2016 de mecanismos de financiación (ICO) basados en *smart contract* acelera el interés por la tecnología y aumentan considerablemente el uso y la capitalización de las diferentes plataformas de *blockchain*.

El 2017 los gobiernos comienzan a controlar las operaciones que realizan las empresas en *blockchain* y en 2018 muchos gobiernos establecen restricciones para llevar a cabo operaciones económicas en *blockchain*. Las consecuencias de estas decisiones se trasladan en una gran caída de cotización de todas la criptomonedas.

El futuro de *blockchain* depende de la capacidad de la tecnología para adaptarse a las necesidades de las empresas y usuarios. En este sentido has surgido otras soluciones DLT que permiten plantear soluciones en otras tecnologías como el internet de las cosas.

Bibliografía

[1] J. Elias, *The unsolved mystery of Satoshi Nakamoto, the creator of Bitcoin*. 2017 [En línea]. Disponible en: https://in.pcmag.com/bitcoin/118113/the-unsolved-mystery-of-satoshi-nakamoto-the-creator-of-bitcoin?p=2&=1

[2] Satoshi Nakamoto. 2020 [En línea]. Disponible en: https://es.wikipedia.org/wiki/Satoshi_Nakamoto

[3] B. Bosker, *Gavin Andresen, bitcoin architect: meet the man bringing you bitcoin (and getting paid in it)*. 2013 [En línea]. Disponible en: https://www.huffpost.com/entry/gavin-andresen

[4] IG, *¿Qué es un halving de bitcoin?*. 2020 [En línea]. Disponible en: https://www.ig.com/es/bitcoin/bitcoin-halving

[5] Cos, *A Selection of Key Events in Bitcoin's History*. 2019 [En línea]. Disponible en: https://medium.com/coinmonks/a-selection-of-key-events-in-bitcoins-history-65a982c76ebf

[6] Trading Education, *Mt. Gox: the story of the biggest ever bitcoin hack*. 2020 [En línea]. Disponible en: https://trading-education.com/mt-gox-the-story-of-the-biggest-ever-bitcoin-hack

[7] *MyBitcoin*. 2017 [En línea]. Disponible en: https://en.bitcoin.it/wiki/MyBitcoin

[8] H. Partz, *China Didn't Ban Bitcoin Entirely, Says Beijing Arbitration Commission*. 2020 [En línea]. Disponible en: https://cointelegraph.com/news/china-didnt-ban-bitcoin-entirely-says-beijing-arbitration-commission

[9] Bitcoin, *Frequently asked questions*. 2020 [En línea]. Disponible en: https://bitcoin.org/en/faq#is-bitcoin-really-used-by-people

[10] Histórico cotización *Bitcoin*. [En línea]. Disponible en: https://es.cointelegraph.com/bitcoin-price-index

[11] Bitcoin, *frequently asked questions*. 2020 [En línea]. Disponible en: https://bitcoin.org/es/faq#general

[12] Bitcoin.com, *Bitcoin's software has been rolled back before*. 2019 [En línea]. Disponible en: https://news.bitcoin.com/bitcoins-software-has-been-rolled-back-before/

[13] Imagen envio de bitcoins. [En línea]. Disponible en: https://bitcoin.org/es/faq#como-de-dificil-es-realizar-un-pago-con-bitcoin

[14] J. Redman, *Bitcoin's software has been rolled back before*. 2019 [En línea]. Disponible en: https://digiconomist.net/bitcoin-energy-consumption

[15] Vitálik Buterin. 2020 [En línea]. Disponible en: https://es.wikipedia.org/wiki/Vit%C3%A1lik_Buterin

[16] Ethereum.org, *Ethereum*. 2020 [En línea]. Disponible en: https://ethereum.org/en/

[17] S. Falkon, *The story of the dao* - its history and consequences. 2019 [En línea]. Disponible en: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

[18] *Cotización Ethereum*. 2016 [En línea]. Disponible en: https://es.cointelegraph.com/ethereum-price-index

[19] *Cotización Ethereum*. 2017-2018. [En línea]. Disponible en: https://es.cointelegraph.com/ethereum-price-index

[20] *Ethereum Community*. 2020 [En línea]. Disponible en: https://ethereum.org/en/community/

[21] Decentralised Server models https://blog.ethereum.org/2016/07/12/build-server-less-applications-mist/

[22] Intelligent HQ, *DAG (Blockchain 3.0): a new hope for the emerging markets*. 2019 [En línea]. Disponible en: https://www.intelligenthq.com/dag-blockchain-3-0-a-new-hope-for-the-emerging-markets/

[23] Coti.io, *Coti*. 2020 [En línea]. Disponible en: https://coti.io/technology