ÍNDICE

PRÓLOGO

SOBRE EL LIBRO

En este libro el lector aprenderá los conceptos fundamentales de la tecnología Blockchain, su historia, su arquitectura, protocolos y aplicaciones. Se analizarán los principales proyectos Blockchain que permiten el desarrollo de aplicaciones descentralizadas y se estudiarán los principales protocolos de consenso, las tecnologías utilizadas y sus aplicaciones.

OBJETIVOS

Los objetivos de este trabajo pueden ser definidos en los siguientes puntos:

- Conocer y explicar los fundamentos de las tecnologías Blockchain.
- Describir el funcionamiento de la cadena de bloques de Bitcoin, la cual asienta las bases de muchas de las funcionalidades de las cadenas de bloques que coexisten en la actualidad.
- Comprender las ventajas y características de la descentralización estudiando el minado de criptomonedas.
- Comprender las bases técnicas de las aplicaciones descentralizadas basadas en Ethereum/Blockchain.

- Describir el funcionamiento de la cadena de bloques de Ethereum comparándolo respecto a la tecnología de Bitcoin. A su vez, desarrollar algunas características más distinguibles de la tecnología Ethereum.
- Conocer los principales tipos de billeteras para almacenar criptomonedas.
- Comprender cómo Ethereum puede ser usado para la generación de contratos inteligentes.
- Dar a conocer los conceptos de tokenomics y Finanzas descentralizadas (DEFI).
- Describir las principales amenazas de ciberseguridad a tener en cuenta en los proyectos basados en Blockchain.

EL AUTOR

José Manuel Ortega es ingeniero de software e investigador de ciberseguridad con interés en nuevas tecnologías, open source, seguridad y testing. En los últimos años ha mostrado interés en proyectos de innovación utilizando tecnologías Big Data y lenguajes de programación como Python.

Actualmente se encuentra trabajando como ingeniero de software en proyectos de investigación relacionados con Big Data, Ciberseguridad y Blockchain. Ha impartido docencia a nivel universitario y colaborado con el colegio oficial de ingenieros informáticos. También ha sido ponente en varias conferencias orientadas a desarrolladores a nivel nacional e internacional. Más información acerca de las conferencias impartidas y otros trabajos publicados se puede consultar en su sitio personal https://josemanuelortegablog.com

1 BITCOIN: ORIGEN DE LA CADENA DE BLOQUES

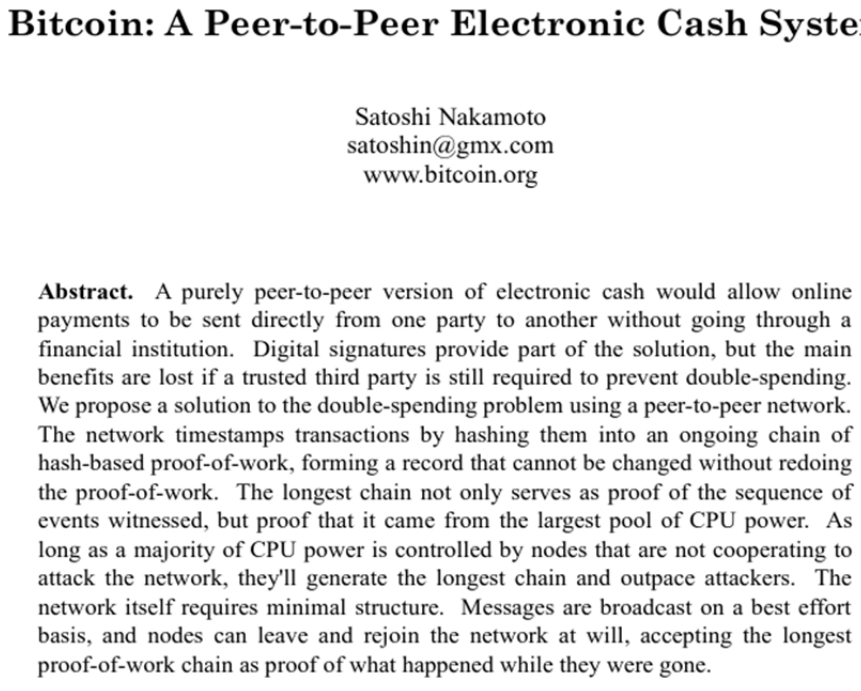
1.1 INTRODUCCIÓN

En octubre de 2008, una persona o grupo de personas bajo el pseudónimo de Satoshi Nakamoto presenta un documento académico denominado "**Bitcoin: a peer-to-peer electronic cash system**" en una lista de correo electrónico sobre criptografía. Este texto introdujo las bases de un sistema de efectivo electrónico descentralizado entre pares, llamado Bitcoin. El documento se puede consultar de forma abierta en https://bitcoin.org/bitcoin.pdf.

El objetivo de este documento es crear un nuevo mecanismo de pagos en internet, ya que el sistema de pagos en internet se basa mayoritariamente en un sistema de confianza en terceros, ya sean bancos o cualquier otra entidad, que tienen como cometido mover el dinero y generar transacciones a petición de sus clientes, lo cual requiere de un cierto nivel de confianza en estas entidades para registrar y gestionar el dinero de cada usuario, siendo en su mayoría, de una forma bastante opaca y con total desconocimiento de lo que sucede realmente con el dinero.

El documento comienza con una introducción explicando el problema que trata de resolver. Hoy en día, las aplicaciones de comercio electrónico dependen en su mayoría de instituciones financieras que actúan como terceros de confianza.

Por ejemplo, cuando yo realizo una compra en una tienda y pago con tarjeta de crédito o débito, el dinero no va desde mi cuenta a la cuenta del proveedor de forma directa, sino que en su lugar hay un intermediario o tercero de confianza, normalmente el banco, que verifica la transacción y la aprueba.



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.

Figura 1.1: Abstract del documento que dio a conocer el Bitcoin

Este documento propone el uso de una nueva tecnología totalmente descentralizada, que permita realizar pagos entre pares sin la necesidad de una entidad intermediaria en un medio electrónico, todo ello, gracias a la criptografía y a la capacidad de cómputo de los dispositivos electrónicos, que garantizará la seguridad del sistema en sí mismo y de las transacciones que se lleven en ella.

En el documento, se define la tecnología como “Bitcoin”, pero a su vez, también se asientan las bases del funcionamiento de un sistema público y descentralizado que registra globalmente las transacciones realizadas en el sistema, la cadena de bloques descentralizada o “Blockchain”, que, con el paso del tiempo, ha ido evolucionando hasta la creación de nuevas cadenas de bloques más complejas y añadiendo más utilidades a estas. Hasta tal punto, que hoy por hoy se estima que existen miles de cadenas de bloques con distintas implementaciones, o incluso algunas de ellas de uso privado.

El propósito de Bitcoin es ser un medio de efectivo electrónico entre pares. Para ello, se apoya en un sistema de pagos electrónicos basados en pruebas criptográficas en lugar de emplear un tercero de confianza para validar ese pago.

Bitcoin es un protocolo de código abierto, que se caracteriza por ser descentralizado en su diseño, ya que no requiere de un nodo central que almacene y procese toda la información, sino un conjunto de nodos distribuidos alrededor del mundo que se comunican entre sí y todos tienen la misma información actualizada.

Bitcoin se creó para prescindir de una entidad centralizada que pudiera manipular la información o censurar el uso de Bitcoin. **Bitcoin** con mayúscula hace referencia al **protocolo**, a la red. Mientras que **bitcoin** con minúscula hace referencia a la **unidad monetaria**, la cual puede dividirse hasta 8 decimales. Esto significa que la mínima cantidad de bitcoins que se puede poseer es 0.00000001 BTC, que como homenaje al creador se conoce como un Satoshi.

Como dato curioso destacar que el 3 de enero de 2009, nació el primer bloque de transacciones de la red Bitcoin. Un bloque minado por Satoshi Nakamoto, con una recompensa utilizando el mecanismo de prueba de trabajo. Este bloque luego es verificado por todos los nodos de la red descentralizada de Bitcoin para darle veracidad al dato.

El protocolo Bitcoin posee mecanismos de consenso que hacen posible que la red funcione de forma descentralizada y tenga incentivos para validar las transacciones y añadir bloques a la cadena.

Las **transacciones** quedan registradas de forma pública en una base de datos y basándose en las transacciones procesadas en la red, el sistema determina el saldo que tiene cada dirección Bitcoin. Esta base de datos donde se registran todos los movimientos producidos es la llamada Cadena de Bloques, o Blockchain, que explicaremos más adelante.

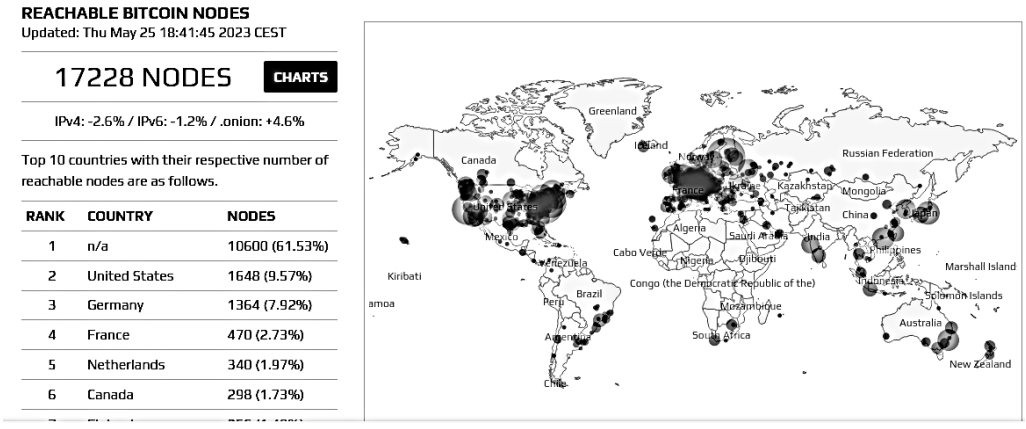
En Bitcoin no es posible la falsificación ya que, al ser una secuencia de datos encadenados y una combinación de transacciones, la única forma de realizar una transacción fraudulenta sería cambiando una transacción, y la anterior, y la anterior, hasta el bloque cero, lo cual es imposible.

La red Bitcoin está compuesta por miles de nodos alrededor de todo el mundo, cada uno de los cuales contiene la copia exacta y actualizada de toda la cadena de bloques, y en cada bloque se almacenan transacciones, información de ese bloque y su vinculación con el bloque anterior. De manera que si un nodo dejase de funcionar

la red no se vería afectada, y a su vez no hay un nodo central que sea más importante que el resto de la red. En resumen, Bitcoin consiste de:

- Una red entre pares distribuida (el protocolo Bitcoin).
- Un libro contable público (la cadena de bloques, o Blockchain)
- Un sistema distribuido, matemático y determinístico de emisión de moneda (minería distribuida)

Actualmente existen unos 13.000 nodos como se puede ver en la página https://bitnodes.io



REACHABLE BITCOIN NODES
Updated: Thu May 25 18:41:45 2023 CEST

17228 NODES **CHARTS**

IPv4: -2.6% / IPv6: -1.2% / .onion: +4.6%

Top 10 countries with their respective number of reachable nodes are as follows.

RANK	COUNTRY	NODES
1	n/a	10600 (61.53%)
2	United States	1648 (9.57%)
3	Germany	1364 (7.92%)
4	France	470 (2.73%)
5	Netherlands	340 (1.97%)
6	Canada	298 (1.73%)

Figura 1.2: Distribución de los nodos por país

1.2 TRANSACCIONES EN BITCOIN

Una transacción se produce cuando un individuo, el propietario, le envía una cantidad de monedas electrónicas a otro, el beneficiario. Cada una de estas transacciones conlleva una serie de operaciones. En concreto, cada transacción contiene la clave pública del beneficiario, un hash y la firma del propietario. De esta manera, una moneda electrónica se define en este contexto como una cadena de firmas digitales.

Por tanto, cada vez que se realiza una transacción se genera un hash con la clave pública del beneficiario y la transacción previa, después con este hash y la clave privada del propietario se firma la transacción en curso; por último, se incluye la clave pública del beneficiario y con todo esto ya se tendría una transacción. Con todas estas operaciones se puede verificar cada transacción de forma sencilla. Para seguir de forma gráfica el proceso, se incluye el siguiente diagrama.

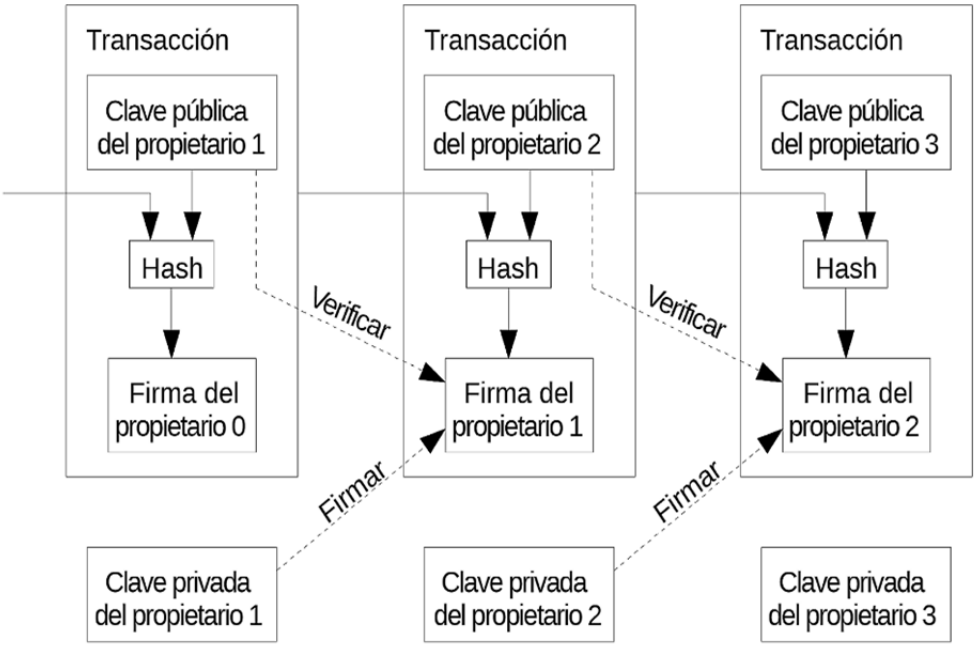


Figura 1.3: Diagrama de transacciones

Esta forma de trabajar no resuelve el problema antes mencionado, y no hay forma de verificar que uno de los propietarios no haya gastado dos veces la misma moneda. De esto se encarga la autoridad central de confianza, o casa de la moneda, que va comprobando cada una de esas transacciones para que eso no sea un problema. Con esta forma de trabajar, cada moneda debe regresar a la casa de la moneda para que esta distribuya una nueva, ya que solamente estas monedas son las que estarían libres de cualquier sospecha del doble gasto. El problema de esta solución centralizada es el que se ha comentado varias veces, todo depende de este sistema centralizado, como en un banco.

Para solucionar esto, Bitcoin propone que las transacciones sean públicas. De esta forma se puede tener un sistema en el que cualquiera pueda tener un historial de todas las transacciones y, al ser muchos, que el historial real sea aquel en el que la mayoría de los participantes estén de acuerdo. Así, el beneficiario tendría la certeza de que los propietarios previos no han firmado transacciones anteriores a la suya. En este sistema, la última transacción es la que cuenta y no se fija en el intento o no de dobles gastos posteriores.