Revista Ciencias Económicas

https://revistas.ues.edu.sv/index.php/rce

El Bitcoin, aspectos generales para su comprensión

Bitcoin, general aspects for its understanding

Balmore Enrique López Ramírez

Docente de la Escuela de Economía, Facultad de Ciencias Económicas, Universidad de El Salvador

Revista de Ciencias Económicas (2023)
Vol. 1, Núm 1 · pp. 37-44

DOI: 10.5281/zenodo.10627311

Palabras clave
Criptomonedas
Bitcoin
dinero

Keywords:
Cryptocurrencies
Bitcoin
money

Correspondencia:
balmore.lopez@ues.edu.sv

Presentado: mayo *de 2023*
Aceptado: *junio de 2023*

RESUMEN

La disrupción tecnológica ha permitido la implementación de las criptomonedas y su rol como "dinero". Este artículo estudia las implicaciones de la criptomoneda Bitcoin y los aspectos generales para su comprensión.

ABSTRACT

Technological disruption has enabled the implementation of cryptocurrencies and their role as "money". This paper studies the implications of the Bitcoin cryptocurrency and general aspects for its understanding.

Las nuevas tecnologías, han permitido crear métodos de pago diferentes a los tradicionales, uno de estos nuevos métodos son las criptomonedas, de las cuales el más importante, por capitalización de mercado, es el bitcoin (García-Corral et al., 2022), que se define como una unidad de valor digital que puede intercambiarse electrónicamente y que no existe en forma física, sin una única autoridad u organización, en su lugar una red de ordenadores crea y rastrea los bitcoins utilizando fórmulas matemáticas complejas"(Bank, 2021).

El presente artículo inicia con la revisión de las razones de la importancia del fenómeno de las criptomonedas, en particular del bitcoin y expone aspectos generales de su operación, para iniciar la comprensión del mundo de la criptoeconomía. Diferenciaremos que Bitcoin, con "B" mayúscula,

se refiere a dos cosas: la primera a la red de Bitcoin y la segunda al protocolo Bitcoin. En el caso de la primera o sea la red Bitcoin, es la infraestructura global que almacena todas las transacciones Bitcoin en una base de datos pública conocida como la cadena de bloques o blockchain; la segunda o sea el protocolo Bitcoin, es el conjunto de reglas y estándares que definen cómo funcionan las transacciones Bitcoin en la red Bitcoin. Esto incluye cómo se crean los nuevos Bitcoins, cómo se verifican las transacciones, cómo se mantiene la cadena de bloques y muchas otras reglas técnicas. Mientras que bitcoin, con "b" minúscula, se refiere a la criptomoneda en sí. Es una unidad de moneda digital que las personas pueden comprar, vender y usar para realizar transacciones en la red Bitcoin.

Antecedentes

De 2008, en sus inicios, hasta el 29 de mayo del presente año, la capitalización del Bitcoin (significa el # de bitcoins por el precio de mercado), ascendía a los US$538.58 billones de dólares, con una emisión de 19.38 millones de unidades, a un precio de US$27.86 mil por unidad, representando el 47.8% de las principales 100 criptomonedas que en total sumaban una capitalización de mercado de 1,125.3 billones de dólares (CoinMarketCap, 2022), lo que permite dimensionar el impacto de la innovación financiera en los mercados (Figura 1).

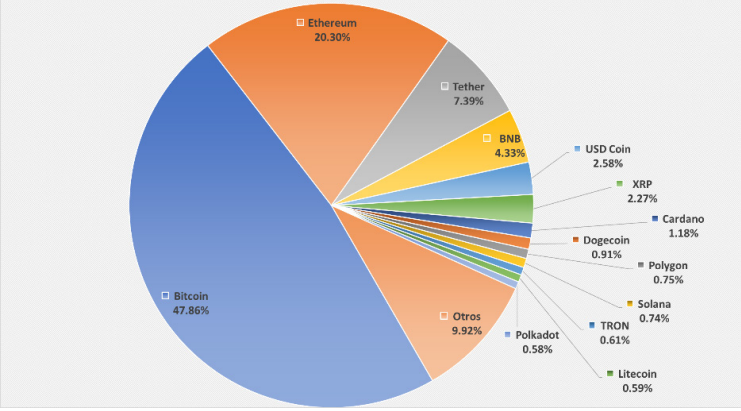
Parte de la implementación del bitcoin en El Salvador (Figura 2), implicó la creación de una app denominada "chivowallet", diseñada según el sitio web de ella: "para ser sencilla e intuitiva, dándote la funcionalidad que necesitas para tu uso diario, para consumo, remesas y finanzas personales en general" (GOES, 2021), colocando como incentivo de uso la recepción de US$30 en bitcoins para consumo, al momento del registro. (El salario mínimo en el país, es aproximadamente US$360 mensuales), además de no cobrar comisiones, sin embargo, esta wallet no traslada las claves al usuario, lo mantiene centralizado el registro, por lo que, en caso de extraviar el celular, la persona puede trasladar el saldo con una llamada telefónica. Para enero de 2022, 4 millones de personas han descargado la aplicación (Jha, 2022).

Aspectos generales

En su papel seminal Nakamoto (2008), propuso un sistema de transacciones electrónicas, que eliminaba la confianza entre partes, sustituyéndola por pruebas criptográficas entre ellas, sin pasar por una institución financiera, mediante una red peer-to-peer, solución propuesta por el avance del comercio en internet (Nakamoto, 2008), representó un desafío al sistema monetario actual, que en el 2008 se hallaba en plena crisis.(Weber, 2016)

Figura 1

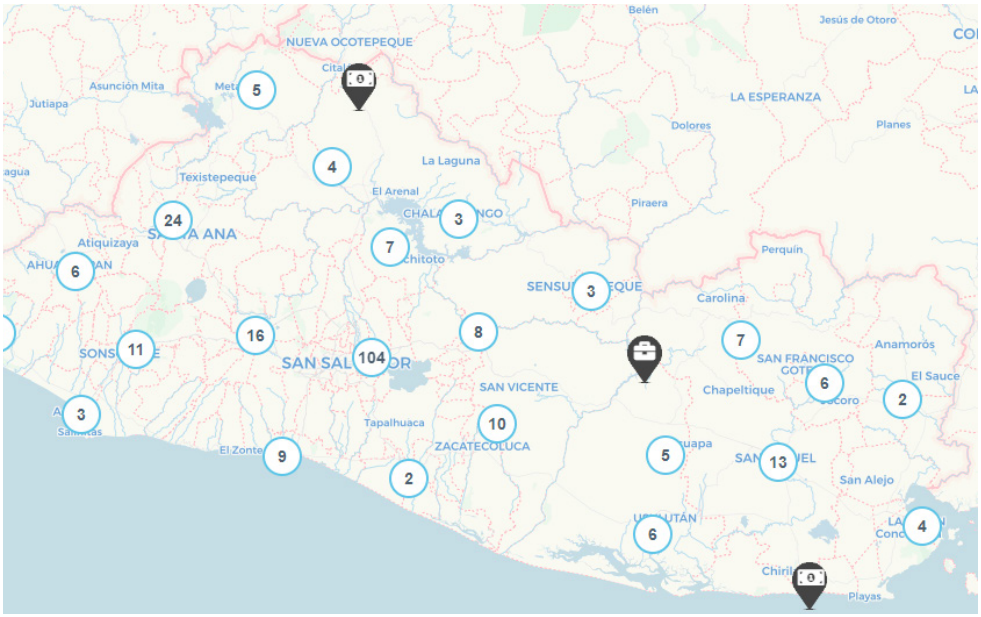
Participación de criptomonedas por capitalización al 29-05-2023



Nota. Presenta el porcentaje de participación en la capitalización de mercado de las principales criptomonedas. Fuente: (CoinMarketCap, 2022)

Figura 2

Número de establecimientos y negocios que aceptan transacciones bitcoin en El Salvador



Nota. Tomado de Coinmap.org

El bitcoin en términos monetarios se considera como un dinero sin mercancía, sin oro, fiduciario, sin estado o gobierno que lo respalde, y sin deuda, supone un desafío a las formas convencionales de moneda, sin embargo, no logra la credibilidad y aceptación por los consumidores y comerciantes, en un número suficientemente grande, como para generar el impulso, que lo haga superar su estado de curiosidad monetaria y de activo especulativo. (Bjerg, 2016).

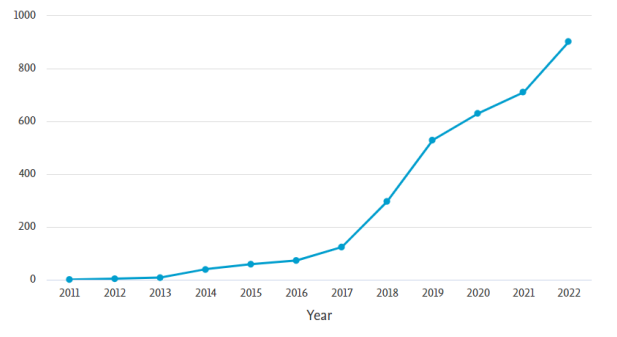
Como fenómeno, el bitcoin ha generado miles de investigaciones, por ejemplo, en la base de datos científica Scopus, la búsqueda mediante la palabra bitcoin y criptomoneda, generaba más de 5,395 publicaciones en el período 2011 al 2022, en todos los campos de investigación, desde economía, hasta física y matemática (Figura 3).

El Bitcoin comenzó a funcionar el 3 de enero de 2009, entre los entusiastas de la criptografía que realizaban transacciones y extraían intermitentemente tokens que entonces no valían nada hasta que se incluyeron en una bolsa en octubre de 2009 por un precio de 0,000764 dólares por bitcoin y el 22 de mayo de 2010 se registró la primera transacción real en la que Bitcoin cumplió la función de medio de cambio, a una tasa de $0,0025 por bitcoin (Ammous, 2018), el bitcoin como tal, presentó como fundamentos:

- *Descentralización:* Mediante el algoritmo de consenso, se mantiene la consistencia

Figura 3

Publicación de artículos científicos sobre bitcoin y criptomonedas



Nota. Presenta la cantidad de publicación científicas revisadas por pares registradas en Scopus (2023).

de la base de datos distribuida, evitando una agencia central.

- *Persistencia:* Las transacciones se validan rápidamente, es casi imposible revertir transacciones, una vez incluidas en la cadena de bloques.
- *Anonimato:* Las direcciones con que interactúan los usuarios no revela la identidad.
- *Auditabilidad:* Toda transacción hace referencia a las transacciones pasadas, cuando una transacción se incorpora a la cadena de bloques, pasa a no estar ya disponible (gastada)(Zheng et al., 2017).

La innovación que han introducido las criptomonedas, ha hecho que se considere su rol como "dinero", para lo cual, se requiere cumplir las tres funciones tradicionales del dinero: medio de intercambio, depósito de valor y unidad de cuenta; en particular la función de medio de intercambio, en principio por ser monedas electrónicas operativas desde cualquier dispositivo conectado a Internet, lo pueden cumplir fácilmente, pero esto requiere hallar la demanda para ser utilizada como medio de intercambio (Ammous, 2018), crear la demanda del bitcoin como medio de intercambio, supone la aceptación de los consumidores de la tecnología implícita.

El uso de los consumidores, como medio de intercambio, implica que han adquirido bitcoins, el cual lo depositan en una aplicación de software denominada wallet, esta mantiene las claves privadas, que le conceden acceso al registro de la moneda; y puede enviarse a otro usuario, en el momento del intercambio (Mattke et al., 2018).

¿Qué problemas pretende resolver el bitcoin?

El bloque inicial de bitcoin contiene el texto: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", que es interpretado como el recordatorio de la crisis monetaria, sin precedentes, del 2008 (Antonopoulos, 2020), un sistema monetario que la moneda virtual del Bitcoin trata de desafiar (Weber, 2016). Entonces como participa el bitcoin.

En una transacción personal, pagada con efectivo, el vendedor no necesita mayores datos del comprador, excepto asegurarse que el dinero físico sea auténtico; al no existir datos no existe el problema de que se robe el dinero del comprador, pero el dinero metálico entregado es emitido por un banco central, de tipo fiat, es decir basado en la confianza, pero justamente esto hace que esa entidad centralizada pueda abusar del poder de creación que reduzca su valor vía devaluación o inflación.(Pritzker, 2019), debe notarse que la operación tiene anonimidad (en el sentido que se requieren mínimos datos), la confianza proviene de poder verificar en físico el dinero, aunque se depende de un banco central para la gobernanza del mismo, así como su emisión y control.

El cambio a una sociedad digital obliga a que los pagos se realicen mediante internet, usando de un intermediario (generalmente el agente de pago es un banco, un emisor de tarjetas de crédito, etc.), lo que conlleva la necesidad de confiar en el intermediario en que apruebe y verifique el pago, esto para ambas partes de la operación, al vendedor le implica esperar que el intermediario haga que no sea posible la reversión de la transacción y que el cliente tenga fondos (Pritzker, 2019); además, la sociedad digital cambia la forma de emisión monetaria, ilustrado en las palabras de Bernanke, Presidente de la Reserva Federal al momento de la crisis del 2008, al explicar el dinero que uso la Fed, expresó: "Los bancos tienen cuenta en la Fed, casi de igual manera a la que usted tiene una cuenta en un banco comercial. Por tanto, para prestar dinero nos limitamos a usar el ordenador para aumentar el tamaño de la cuenta que tiene en la Fed" (Wray et al., 2015), el dinero se convierte en bits y bytes que son verificados por un tercero que administra la transferencia.

Por tanto, la propuesta de un sistema de dinero en efectivo electrónico peer-to-peer trata de resolver los problemas del sistema monetario actual, una propuesta en que los bancos son reemplazados por ese sistema de pares, descentralizados, para emitir y transferir dinero digital (Huibers, 2021).

Funcionamiento del Bitcoin

El bitcoin es efectivo digital (dinero electrónico o como posteriormente se denominaron criptomoneda) de persona a persona (Figura 4), que es gestionado por el protocolo Bitcoin mediante la tecnología blockchain, creando un sistema de pagos electrónicos que utiliza pruebas criptográficas en vez de confianza (Nakamoto, 2008); el protocolo Bitcoin es descrito como un libro digital de transacciones monetarias, en la forma de blockchain y su principal innovación es combinar la tecnología blockchain con firmas digitales en una red peer-to-peer con sellado de tiempo (Arjaliès, 2021), esta tecnología de contabilidad distribuida, popularizada por Bitcoin, con su mecanismo de consenso descentralizado, ha evolucionado a los contratos inteligentes (Cong & He, 2019).

En las transacciones en e-commerce, se genera el problema del doble gasto, porque las transacciones digitales pueden ser copiadas, como cualquier archivo digital, lo que da la posibilidad de gastar el dinero dos veces (equivale a falsificar dinero físico); cuando hay un intermediario (un banco, PayPal, etc.), él tiene los controles para que el dinero no pueda gastarse dos veces, la solución de Satoshi es que todas las transacciones sean públicas, así el beneficiario (receptor del dinero), puede confirmar que el dinero no ha sido gastado previamente, pero esto genera el problema de que todos los participantes estén de acuerdo con el historial al no estar en una base centralizada, llamado el problema del consenso en las versiones de la base (Cong & He, 2019).

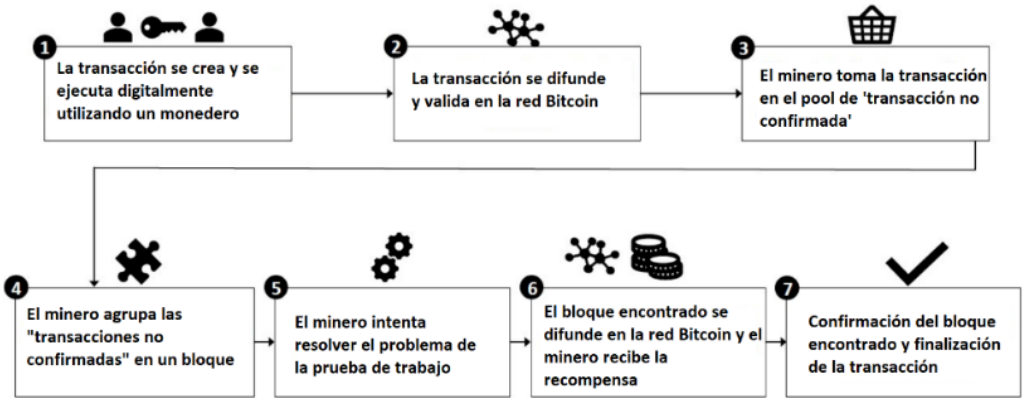
Una red peer-to-peer

Una red peer-to-peer(p2p), es definida como una colección de computadoras que reservan recursos para servir contenidos unas a otras, sin servidores aprovisionados por separado y sin un punto central de control, a las computadoras se les llama iguales debido a que cada una de ellas puede actuar de manera alternativa como cliente para otro igual y obtener su contenido, lo que hace interesantes a los sistemas de igual a igual es que no hay una infraestructura dedicada (Tanenbaum, 2013).

La red Bitcoin la forman un conjunto de usuarios que pueden entrar y salir de ella libremente, cada uno tiene la capacidad de crear de forma ilimitada pares de claves, una pública y otra privada, la primera se puede identificar con la dirección o el número de cuenta del usuario, todo aquel que quiera enviarle fondos necesitará conocerla, en tanto que la segunda, la clave privada, permite a un usuario hacer uso de los fondos asignados a una determinada clave pública (Llases, 2021).

Figura 4

Proceso de transacción de un bitcoin



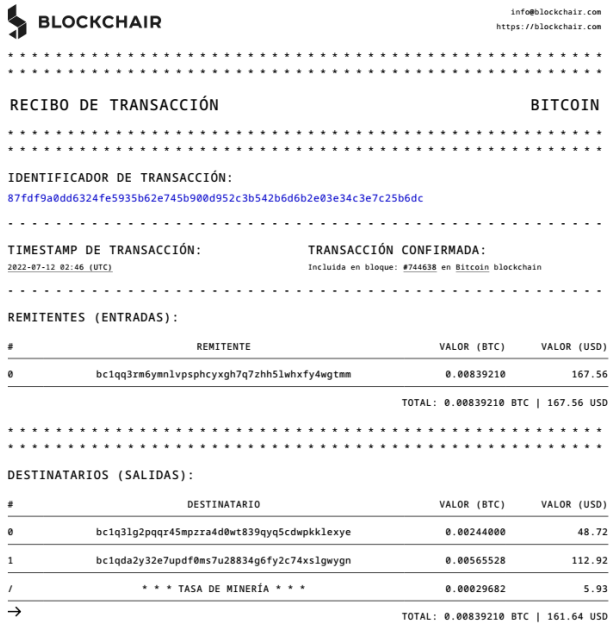
Nota. Tomado de Mattke et al., 2018

Por ser una red entre pares, cada nodo bitcoin se conecta a unos pocos nodos bitcoin, que son descubiertos al inicializarse mediante el protocolo entre pares, no hay una topología rígida, ni estructurada, los datos llamados transacciones y bloques en forma de mensajes, son propagados de cada nodo a todos los pares con conexión, en el proceso denominado "flooding", de tal manera que en pocos segundos se propaguen a toda la red (Antonopoulos, 2020). Los nodos de la red Bitcoin pueden ser: nodos normales, que realizan compras y ventas de bienes y servicios, empleando al bitcoin como moneda en transacciones; nodos mineros que además de realizar lo comentado, dedican su potencia de cómputo al validar la red, mediante los bloques de transacciones, el usuario, se identifica en la red por una o más direcciones Bitcoin, que son gestionadas en un monedero virtual denominado wallet (Gallardo et al., 2019).

Las wallet o carteras, tienen una colección de direcciones y claves que permiten gastar los bitcoin depositados en ella, mediante transacciones (Figura 5), son un tipo de software que guarda las direcciones de bitcoin y las claves privadas, empleadas para enviar y recibir los bitcoin (Antonopoulos, 2020).

Figura 5

Ejemplo de transacción de bitcoin



BLOCKCHAIR

info@blockchair.com
https://blockchair.com

RECIBO DE TRANSACCIÓN — BITCOIN

IDENTIFICADOR DE TRANSACCIÓN:
87fdf9a0dd6324fe5935b62e745b900d952c3b542b6d6b2e03e34c3e7c25b6dc

TIMESTAMP DE TRANSACCIÓN: 2022-07-12 02:46 (UTC)

TRANSACCIÓN CONFIRMADA: Incluida en bloque: #744638 en Bitcoin blockchain

REMITENTES (ENTRADAS):

#	REMITENTE	VALOR (BTC)	VALOR (USD)
0	bc1qq3rm6ymnlvpsphcyxgh7q7zhh5lwhxfy4wgtmm	0.00839210	167.56

TOTAL: 0.00839210 BTC | 167.56 USD

DESTINATARIOS (SALIDAS):

#	DESTINATARIO	VALOR (BTC)	VALOR (USD)
0	bc1q3lg2pqqr45mpzra4d0wt839qyq5cdwpkklexye	0.00244000	48.72
1	bc1qda2y32e7updf0ms7u28834g6fy2c74xslgwygn	0.00565528	112.92
/	* * * TASA DE MINERÍA * * *	0.00029682	5.93
→		TOTAL: 0.00839210 BTC | 161.64 USD	

Nota. Transacción de Bitcoin realizada en 2022.

Las transacciones

Una transacción representa la asignación de una dirección Bitcoin a otra, una tarea atómica usando los protocolos Bitcoin, son estructuras de datos firmadas digitalmente que se forman por versión, entradas, salidas y tiempo de bloqueo, para la transferencia de dinero individuales, que se intercambian entre pares de la red (Praveen et al. 2021). Las entradas de la transacción especifican qué salidas (UTXO: "Unspent transaction output", transacción de salida no gastada) de una transacción anterior, se gastarán, utilizando el hash de la transacción que fueron creadas, llamado TXID (Transaction ID), es básicamente el número de identificación de la transacción) (Rosenbaum, 2019).

El hash del TXID, identifica de manera única a la transacción, se crea por una secuencia de texto compuesto por:

- La versión del protocolo bitcoin, expresado en 32 bit (hay dos versiones),
- Una bandera llamada "SegWit marker" (bandera de 'testigo agregado'), indica la presencia de datos de testigo,
- vin de entrada,
- vout, que identifica la lista de todas las salidas de una transacción,
- el tiempo de cierre, nLockTime (Bashir, 2023).

Los datos anteriores, concatenados, son introducidos en el algoritmo SHA265 y el resultado es nuevamente introducido al algoritmo SHA256, para obtener el TXID o hash de la transacción(Rosenbaum, 2019). El vin de entradas a su vez se compone por:

- El contador de entrada que indica la cantidad de entradas incluida en la transacción.
- El hash de la transacción anterior (en la que se adquirieron los bitcoins).
- Índice de salida que son 4 bytes, es el

índice de salida de la transacción anterior, como UTXO a gastar.
- La longitud del script de desbloqueo que puede ser de 1 a 9 bytes.
- El script de desbloqueo (ScriptSig), que debe llenar requisitos de formación.
- Una secuencia de números de 4 bytes, que normalmente desactiva mediante el hexadecimal 0xFFFFFFFF.

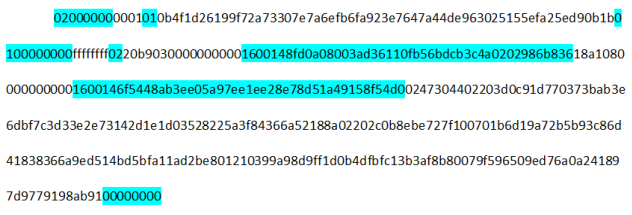
El vout, contiene tres campos: el de valor o cantidad a transferir en satoshis, en espacio de 8 bytes, el tamaño del script de bloqueo que puede ser de 1 a 9 bytes, y el Script de bloqueo,ScriptPubKey.

La transacción serializada (Figura 6), es utilizada para mediante el algoritmo sha256 genere un hash que es nuevamente introducido a la función, para generar el ID de la transacción (denominado doble SHA256), se emplea esta función porque la misma entrada produce la misma salida (concepto de función matemática), cualquier cambio en la entrada, produce hashes totalmente diferentes, tiene un tamaño fijo de 256 bits, es imposible con base a la salida, el calcular el valor de entrada (Rosenbaum, 2019).

Las transacciones deben llevar la firma digital, es el equivalente de la firma manuscrita, salvo que está vinculada a un número aleatorio denominado clave privada, tiene 3 propósitos, sirve como prueba que el propietario de ella es el dueño de los fondos, que autoriza el gasto de los fondos, es la prueba para la no reversibilidad de la transacción y sirve para que la operación no sea modificada, una vez firmada (Antonopoulos, 2020).

Figura 6

Serialización de transacción



Nota. Tomado Learn me a bitcoin (https://learnmeabitcoin.com/)

Las transacciones tienen total transparencia, se puede consultar el histórico de cada operación, mediante las direcciones bitcoin, se puede usar para trazar otras direcciones relacionadas, lo que hace que no sea completamente anónima, el anonimato del bitcoin se refiere a que las claves que se emplean, no contienen una identidad real en ellas (Gallardo et al., 2019). Es este proceso el que crea la cadena del protocolo Bitcoin, une una transacción con otra.

CONCLUSIÓN

El protocolo Bitcoin, la cadena blockchain ha sido estudiado por sus posibles aplicaciones, el bitcoin representa una de ellas, que implementa soluciones para la descentralización de operaciones. En futuros artículos profundizaremos en otros elementos del funcionamiento.

REFERENCIAS

Ammous, S. (2018). Can cryptocurrencies fulfil the functions of money? *The Quarterly Review of Economics and Finance*, *70*, 38–51. https://doi.org/10.1016/j.qref.2018.05.010

Antonopoulos, A. (2020). *Dominando el Bitcoin: Todo lo que querías saber sobre bitcoin, criptomonedas y blockchain*.

Arjaliès, D.-L. (2021). The Role of Utopia in the Workings of Local and Cryptocurrencies. En R. Rau, R. Wardrop, & L. Zingales (Eds.), *The Palgrave Handbook of Technological Finance* (pp. 95–137). Springer International Publishing. https://doi.org/10.1007/978-3-030-65117-6_5

Bank, E. C. (2021, noviembre 18). *¿Qué es el bitcóin?* European Central Bank. https://www.ecb.europa.eu/ecb/educational/explainers/tell-me/html/what-is-bitcoin.es.html

Bashir, I. (2023). *Mastering Blockchain—Fourth Edition*. Packt Publishing. https://learning.oreilly.com/library/view/mastering-blockchain/9781803241067/

Bjerg, O. (2016). How is Bitcoin Money? *Theory,*

Culture & Society, *33*(1), 53–72. https://doi.org/10.1177/0263276415619015

CoinMarketCap. (2022, febrero 20). *Cryptocurrency Prices, Charts And Market Capitalizations*. CoinMarketCap. https://coinmarketcap.com/

Cong, L. W., & He, Z. (2019). Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*, *32*(5), 1754–1797. https://doi.org/10.1093/rfs/hhz007

Gallardo, I., Bazan, P., & Venosa, P. (2019). *Análisis del anonimato aplicado a criptomonedas*. 17.

García-Corral, F. J., Cordero-García, J. A., de Pablo-Valenciano, J., & Uribe-Toril, J. (2022). A bibliometric review of cryptocurrencies: How have they grown? *Financial Innovation*, *8*(1), 2. https://doi.org/10.1186/s40854-021-00306-5

GOES, G. de E. S. (2021, septiembre 1). *Inicio*. Chivo Wallet. https://chivowallet.com/chivowallet.com

Huibers, F. (2021). Distributed Ledger Technology and the Future of Money and Banking: Banking is Necessary, Banks Are Not. Bill Gates 1994. *Accounting, Economics, and Law: A Convivium*. https://doi.org/10.1515/ael-2019-0095

Jha, P. (2022, enero 18). *La billetera de Bitcoin de El Salvador incorpora a 4 millones de usuarios a través de una asociación con Netki*. Cointelegraph. https://es.cointelegraph.com/news/el-salvador-s-bitcoin-wallet-onboards-4m-users-with-netki-partnership

Llases, L. (2021). Breve análisis de la concentración de la potencia de minado en Bitcoin. *Papeles de Europa*, *34*, 29–39. https://doi.org/10.5209/pade.73881

Mattke, J., Maier, C., Müller, L., & Weitzel, T. (2018). Bitcoin Resistance Behavior: A QCA Study Explaining Why Individuals Resist Bitcoin as a Means of Payment. *ICIS 2018 Proceedings*. https://aisel.aisnet.org/icis2018/crypto/Presentations/4

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 9.

Praveen, G., Anand, M., Singh, P. K., & Ranjan, P. (2021). An Overview of Blockchain Consensus and Vulnerability. En T. Senjyu, P. N. Mahalle, T. Perumal, & A. Joshi (Eds.), *Information and Communication Technology for Intelligent Systems* (pp. 459–468). Springer. https://doi.org/10.1007/978-981-15-7078-0_44

Pritzker, Y. (2019). *Inventemos Bitcoin: La explicación sobre el primer dinero verdaderamente escaso y descentralizado* (Edición Kindle). https://www.amazon.com/-/es/Yan-Pritzker-ebook/dp/B07X1FLY22/ref=sr_1_1?__mk_es_