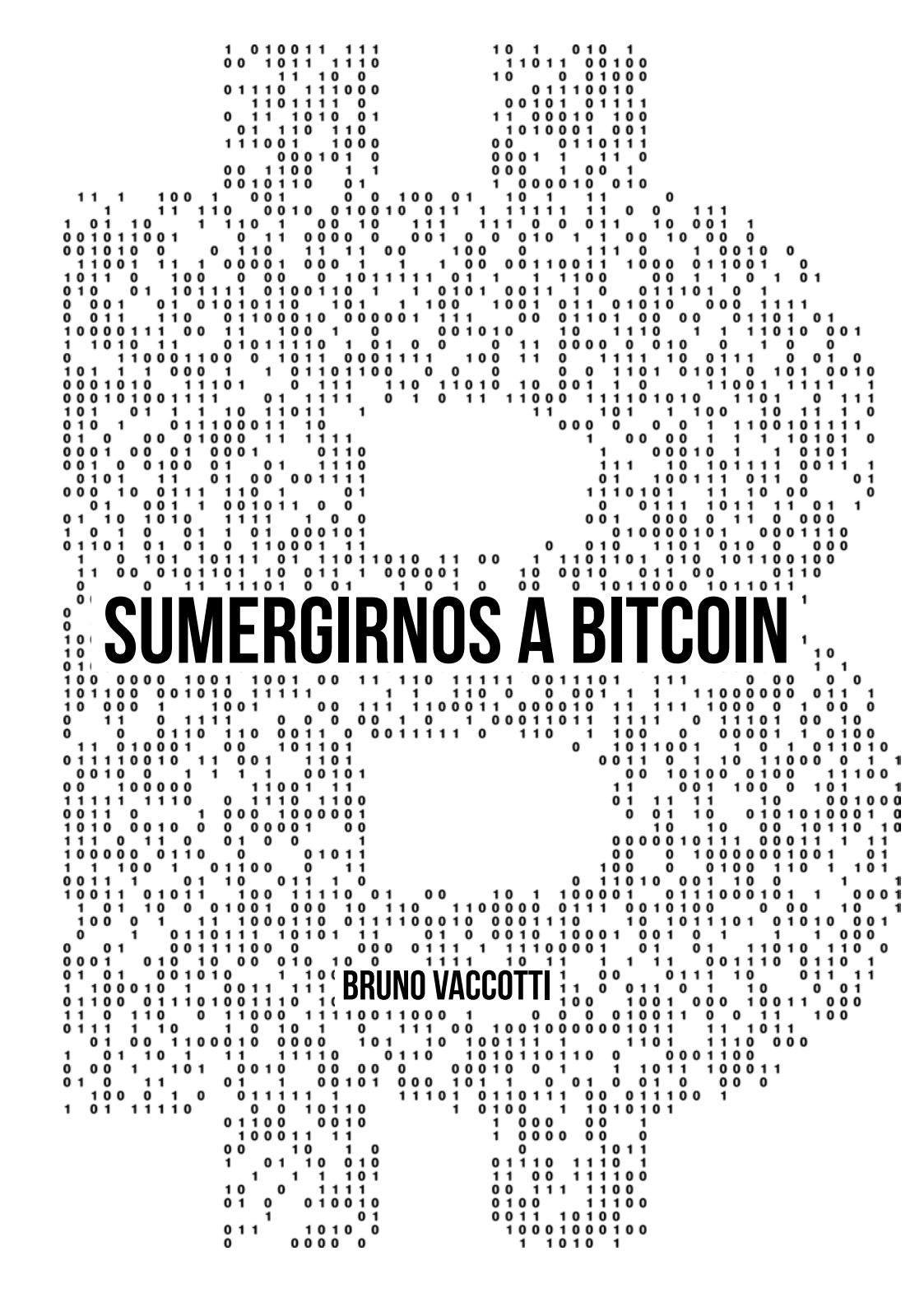
SUMERGIRNOS A BITCOIN
BRUNO VACCOTTI

UNAS PRIMERAS PALABRAS

Bitcoin no es más que una idea a la que le ha llegado su hora. La pregunta no es por qué, sino de qué manera podemos sumergirnos en este viaje hacia la comprensión de Bitcoin, Blockchain, finanzas descentralizadas y las oportunidades que tienen para el presente inmediato.

He tenido que trabajar en educación tanto en mi país como en otros de la región. Incluso antes de ser entusiasta del mundo de los activos digitales, en mi mente ya estaban presentes las dos aristas a las que creo que debemos volcar nuestra energía para mejorar las oportunidades de las generaciones venideras: la educación en tecnología y la educación financiera. Bitcoin es un camino fantástico para sentar bases sólidas en ambas. Un activo que convierte energía en medio de intercambio, en reserva de valor, a través de fuerza computacional y sus mecanismos para luchar con algo que parece inherente a la humanidad: la inflación.

Durante los últimos veinte años, hemos sido testigos de una revolución tecnológica que ha comenzado a redefinir los principios de la economía y el comercio global: la aparición de activos digitales. Algunos han tenido un fracaso estrepitoso, pero han sido las raíces para lo que hoy es Bitcoin. Vamos a recorrer juntos un poco de esa historia. Estos fenómenos no solamente han capturado la atención de los entusiastas de la tecnología y los inversores, sino que también han empezado a influir en los gobiernos, instituciones financieras y empresas de todo el mundo. Aprender sobre Bitcoin y Blockchain es crucial para entender cómo estas innovaciones moldean el presente y construyen un futuro prometedor.

Bitcoin representa un cambio de paradigma en la forma en que entendemos el dinero. Al ser descentralizado, no está controlado por ninguna entidad gubernamental o institución financiera, lo que reduce el riesgo de inflación y manipulación política. En regiones donde el acceso a servicios bancarios es limitado, ofrece una solución viable para la inclusión financiera. Cualquier persona con acceso a Internet puede participar en la economía digital sin necesidad de una cuenta bancaria tradicional.

Otro mundo de posibilidades que se abre gracias a Bitcoin es la Blockchain, la tecnología que sostiene toda la red de este activo y muchos otros servicios seguros y descentralizados, cuyo potencial va mucho más allá de las finanzas digitales. Actúa como un libro de contabilidad distribuido e inmutable que puede registrar transacciones de manera segura y transparente.

El impacto de ambas tecnologías, Bitcoin y Blockchain, se siente en varias industrias, y las oportunidades para el futuro son inmensas. Desde la creación de nuevas formas de comercio hasta la digitalización de activos físicos, su capacidad es inabarcable, y recién estamos dando los primeros pasos.

Aprender es avanzar e integrar es evolucionar. Por este motivo, es esencial dominar el uso de Bitcoin y Blockchain no solamente para los profesionales de la tecnología o las finanzas, sino para cualquier persona que quiera

construir el futuro y formar parte activa del mundo de oportunidades que esto significa. Bitcoin y Blockchain están redefiniendo cómo interactuamos con el dinero, la tecnología y la información, lo que proporciona nuevas oportunidades para la inclusión, la transparencia y la eficiencia. Bitcoin es educación para la libertad.

EL DINERO

EL DINERO

EL DINERO

EL DINERO

EL DINERO

EL DINERO

Recorrer rápidamente la historia del dinero nos permitirá ver la lógica del por qué los activos digitales tienen sentido y ya están presentes en nuestro día a día. Ya pagamos las cuentas con el celular o el reloj inteligente. Cada vez utilizamos menos dinero físico, aunque este sigue actuando como la unidad de valor.

Bitcoin tiene el potencial de reemplazar el dinero convencional. Si nos centramos en la naturaleza del dinero, las ventajas y limitaciones de las monedas fiat o convencionales y las características distintivas de Bitcoin que lo posicionan como una alternativa viable, comenzaremos a prestar cada vez mayor atención a un mundo que ya forma parte de nuestra cotidianidad y evoluciona a diario, el mundo de Bitcoin, Blockchain y los activos digitales.

Desde tiempos inmemoriales, el ser humano ha utilizado diversos bienes como medio de intercambio equivalente. En sus inicios de la historia de la humanidad, el trueque fue la forma más común de obtener diferentes recursos, pero pronto se hizo evidente que requería una coincidencia de deseos que no siempre era posible. Hoy sería inviable intercambiar manzanas por una motocicleta. Así, surgieron los metales preciosos, como el oro y la plata, con características ideales para el dinero: divisibilidad, durabilidad, portabilidad y escasez. Estos metales no solo eran valorados por sus propiedades intrínsecas, sino también por su aceptación general en las transacciones. Sin embargo, con el tiempo, las sociedades comenzaron a adoptar monedas fiat, es decir, monedas emitidas por un gobierno, que no estaban respaldadas por un objeto físico.

Las monedas fiat, aunque prácticas, tienen importantes limitaciones. Una de las más críticas es su vulnerabilidad a la inflación. Los gobiernos pueden imprimir dinero a voluntad; esto puede llevar a una devaluación significativa del poder adquisitivo. Las autoridades monetarias siguen teniendo mucho poder a la hora de manipular la oferta de dinero, y eso ha generado crisis económicas en la historia. La inflación erosiona los ahorros de las personas

y crea incertidumbre económica, lo que puede desincentivar la inversión y el crecimiento a largo plazo.

Además, las monedas fiat dependen de la confianza en las instituciones que las emiten. Esta confianza puede ser frágil, especialmente en tiempos de crisis política o económica. Cuando la confianza se pierde, el valor de la moneda puede desplomarse, como se ha visto en varias hiperinflaciones en el siglo XX.

En contraste, Bitcoin está diseñado para operar fuera del control de cualquier entidad centralizada. Su protocolo es transparente y su suministro está limitado a 21 millones de monedas, lo que lo convierte en un activo escaso. Esta escasez es imprescindible, ya que establece un valor intrínseco basado en la oferta y la demanda, en lugar de la manipulación gubernamental. Al momento de escribir estas líneas, 19,5 millones de Bitcoins han sido minados.

Cada usuario tiene el mismo acceso y control sobre su dinero, sin necesidad de intermediarios. Tal descentralización no solo aumenta la seguridad de las transacciones, sino que también reduce el riesgo de censura. Ningún Banco Central o ente regulador puede congelar o secuestrar una billetera de activos digitales, salvo excepciones vinculadas a terrorismo y crímenes de lesa humanidad. En un mundo donde las decisiones políticas pueden influir en el acceso a los recursos financieros, Bitcoin ofrece una alternativa que garantiza la libertad económica a los individuos.

La tecnología detrás de Bitcoin, la Blockchain, también juega un papel fundamental en su capacidad para reemplazar el dinero convencional. La Blockchain es un libro de contabilidad distribuido, inmutable e inalienable que registra todas las transacciones de manera segura y transparente. Cada transacción es verificada por nodos en la red, lo que elimina la necesidad de confianza en un tercero. Esta característica no solo asegura la integridad de las transacciones, sino que también proporciona un nivel de transparencia

que las monedas fiat no pueden igualar. En un sistema donde la corrupción y la manipulación son comunes, la Blockchain representa un avance hacia un sistema monetario más justo y equitativo.

Además, Bitcoin se adapta mejor a las necesidades de una economía globalizada y digital. A medida que el comercio internacional y las transacciones en línea se vuelven más comunes, las limitaciones del dinero convencional se hacen más evidentes. Las transferencias de dinero entre fronteras suelen implican costos elevados y tiempos de espera prolongados debido a la intermediación bancaria. Bitcoin permite transacciones instantáneas y de bajo costo, lo que lo convierte en una opción atractiva para individuos y empresas que operan a nivel global. Esto no solo mejora la eficiencia, sino que también democratiza el acceso a servicios financieros en regiones donde el sistema bancario tradicional es ineficaz o inexistente.

ANTECE-
DENTES

Ya hemos dicho que Bitcoin ha sido una idea a la que le ha llegado su hora. La propuesta de Satoshi Nakamoto no fue ni de cerca el primer intento de dinero digital sobre la faz de la Tierra; de hecho, varios aspectos de proyectos anteriores a Bitcoin se ven reflejados en él. Entonces, ¿por qué otros proyectos fracasaron y Bitcoin no? Repasaremos un poco la historia de cada uno de estos intentos previos que prepararon el camino a Bitcoin. Así permitiremos que el lector saque sus propias conclusiones.

DIGICASH

El primer caso al que haremos referencia es DigiCash, el primer intento, podríamos decir, relevante de crear una forma de dinero digital. Fundada en 1989 por el criptógrafo David Chaum, DigiCash fue una de las primeras empresas en explorar la posibilidad de realizar transacciones electrónicas de manera segura y anónima. En 1982, Chaum presentó un trabajo llamado *Blind Signatures for Untraceable Payments*, que se podría traducir como «Firmas a ciegas para pagos irrastreables». Muchas de las ideas presentadas en este trabajo nutren lo que luego conoceríamos como Blockchain. Sin lugar a dudas, su tesis en la Universidad de Berkeley (California) sobre «Sistemas informáticos establecidos, mantenidos y confiados mutuamente por grupos sospechosos» (*Cooperation of Mutually Suspicious Subsystems in a Computer Utility*) se considera un prototipo de Blockchain.

David Chaum, conocido en el campo de la criptografía, propuso un sistema que permitiera a los usuarios realizar transacciones en línea sin revelar su identidad. La idea era que el dinero digital debía ser tan seguro y privado como el efectivo en el mundo físico. Chaum desarrolló un protocolo llamado eCash, que utilizaba técnicas avanzadas de criptografía para garantizar la privacidad del usuario. Este sistema permitía a los usuarios retirar «monedas digitales» de un banco y realizar pagos sin que el banco pudiera rastrear las transacciones individuales.

En 1994, DigiCash lanzó su primer producto, eCash, un sistema de dinero digital basado en la criptografía. Funcionaba utilizando monedas digitales que podían ser enviadas de un usuario a otro, y cada transacción era verificada por el banco emisor. El enfoque de Chaum en la privacidad y el anonimato fue innovador, ya que ofrecía a los usuarios un nivel de confidencialidad que no estaba disponible en las transacciones electrónicas convencionales de la época.

A pesar de su innovación, DigiCash enfrentó varios desafíos. Uno de los principales obstáculos fue la falta de infraestructura y aceptación general por parte de los comerciantes. A finales de los años 90, la adopción de pagos electrónicos aún estaba en su etapa inicial, y muchos consumidores y comerciantes eran reacios a confiar en un sistema sin un respaldo tangible como el efectivo o las tarjetas de crédito.

Si DigiCash hubiera podido asociarse con una o más instituciones financieras importantes, probablemente habría tenido una mejor oportunidad de sobrevivir en el mundo financiero que se digitalizaba rápidamente. Una de las asociaciones potenciales más prometedoras fue con Citibank. El banco participó en negociaciones a largo plazo con DigiCash sobre la posibilidad de integración, solo para finalmente ir tras otros proyectos.

En 1998, DigiCash se declaró en quiebra. A pesar de su fracaso comercial, el legado de DigiCash perduró. Las ideas y tecnologías desarrolladas por Chaum influyeron en futuros proyectos en el campo de las criptomonedas.

E-GOLD

Casi en paralelo, aparece e-gold, que también representa un capítulo importante en la evolución del dinero digital, pues dio un paso hacia la creación de sistemas de pago en línea respaldados por activos tangibles. Fundada en 1996, la idea principal detrás de ella era ofrecer un medio de

intercambio en línea respaldado por oro físico, lo que proporcionaba una alternativa al dinero fiduciario y a las monedas digitales no respaldadas. Es decir, una manera primitiva de lo que hoy conocemos como tokenización.

El funcionamiento de e-gold era relativamente sencillo: los usuarios podían comprar e-gold a través de una plataforma en línea, donde cada unidad de e-gold representaba una cantidad específica de oro almacenado en bóvedas. Esto permitía a los usuarios realizar transacciones electrónicas entre cuentas de manera rápida y eficiente utilizando su saldo de e-gold. A diferencia de otros sistemas de pago en ese momento, e-gold ofrecía la posibilidad de realizar transacciones que, en teoría, eran más seguras y resistentes a la inflación, ya que estaban respaldadas por un activo tangible.

Durante su apogeo en la década de 1990 y principios de 2000, e-gold ganó popularidad y se convirtió en una de las plataformas de pago digital más utilizadas. Llegó a movilizar más de dos mil millones de dólares en un año. Atraía a una amplia variedad de usuarios, desde individuos que buscaban una forma de realizar transacciones en línea hasta comerciantes que recibían e-gold como forma de pago. Esta aceptación creciente ayudó a establecer una comunidad activa y un ecosistema de servicios relacionados, como intercambios y billeteras digitales.

Sin embargo, el éxito de e-gold también atrajo la atención de las autoridades. En la década de 2000, el sistema comenzó a ser utilizado por personas involucradas en actividades ilegales, como el comercio de bienes y servicios en la Deep Web. En 2008, las autoridades estadounidenses comenzaron a investigar a e-gold y sus fundadores por la falta de regulación y el uso del sistema en actividades ilícitas. Esto resultó en el arresto de Douglas Jackson y su socio, y en 2008, e-gold se declaró en quiebra.

A pesar de su caída, el legado de e-gold perdura. Fue uno de los primeros ejemplos de una moneda digital respaldada por un activo real y sentó las bases para futuros adelantos en el ámbito de las criptomonedas. Su historia

también destaca la importancia de la regulación en el espacio de los activos digitales, un tema que sigue siendo relevante debido a la aparición de nuevas criptomonedas y plataformas de pago.

B-MONEY

B-Money aparece en 1998 como una propuesta del criptógrafo Wei Dai, quien planteó un sistema de dinero electrónico que permitía transacciones anónimas y descentralizadas. B-Money se presentó en un documento que delineaba un sistema que, si bien no fue implementado en su momento, sirvió como antecedente para el desarrollo posterior de las criptomonedas.

B-Money se basaba en la idea de que el dinero digital debía ser capaz de funcionar de manera similar al efectivo, es decir, permitir a los usuarios realizar transacciones sin necesidad de un intermediario, como un banco. Wei Dai propuso un sistema que utilizaba una red de nodos para validar y verificar transacciones, así, las transacciones serían resistentes a la censura y anónimas. Este enfoque se anticipó a muchos de los principios fundamentales en el diseño de Bitcoin y otras criptomonedas.

Una de las características distintivas de B-Money era su énfasis en la privacidad. El sistema propuesto permitía que los usuarios generaran claves digitales que podían ser utilizadas para realizar transacciones sin revelar su identidad. Además, B-Money contemplaba la posibilidad de que se llevaran a cabo transacciones sin la necesidad de que un banco central o una entidad reguladora controlara el sistema.

A pesar de que B-Money era innovador, no llegó a ser implementado como una plataforma funcional. Sin embargo, influyó en la creación de otros sistemas de dinero digital y criptomonedas. En particular, muchos de los conceptos que se encuentran en B-Money están presentes en el diseño de Bitcoin.

HASHCASH

Hashcash es un concepto y un sistema que se originó en 1997, ideado por el criptógrafo Adam Back. Su propósito inicial era actuar como una forma de prueba de trabajo (*proof-of-work*) para combatir el *spam* en correos electrónicos. La idea detrás de Hashcash era que, para enviar un correo electrónico, el remitente tendría que realizar un cálculo computacional que requiriera tiempo y recursos. Esto significaba que sería costoso enviar grandes volúmenes de correos electrónicos no deseados, lo que haría al *spam* menos atractivo para los *spammers*.

El sistema de Hashcash utiliza un algoritmo que implica la generación de un «token» que contiene una marca de tiempo y un número de serie. Este token se crea mediante un proceso de *hashing*, y su validación requiere que el remitente realice un esfuerzo computacional significativo. Como resultado, cada correo enviado con un token de Hashcash incluye un costo computacional asociado, lo que desincentiva el envío masivo de correos electrónicos no solicitados.

Con el tiempo, la idea de Hashcash y su enfoque en la «prueba de trabajo» influyó en el desarrollo de sistemas de criptomonedas. Satoshi Nakamoto, el creador de Bitcoin, incorporó principios similares de prueba de trabajo en el diseño de la red Bitcoin, lanzada en 2009. En Bitcoin, el proceso de minería no solo asegura las transacciones, sino que también crea nuevos bitcoins. Esto convierte la prueba de trabajo en un componente esencial del sistema.

Aparte de su aplicación en la lucha contra el *spam*, el concepto de Hashcash ha sido utilizado en varios contextos dentro del mundo de la Blockchain y las criptomonedas. Su legado perdura en la forma en que se diseñan y operan las redes de criptomonedas, donde la seguridad y la integridad de las transacciones dependen de la capacidad computacional de los participantes.

SATOSHI NAKAMOTO Y LA NUEVA ERA DE LAS FINANZAS DESCENTRALIZADAS

El 31 de octubre de 2008, una persona autodenominada como Satoshi Nakamoto inicia un hilo de correos dentro de lo que se conocía como «una comunidad *cyberpunk*». Hagamos un paréntesis para entender un poco más sobre el submundo de los foros y los movimientos de Internet de décadas pasadas.

El *cyberpunk* es un subgénero de la ciencia ficción que surgió en la década de 1980 y se caracteriza por su enfoque en la interacción entre la tecnología avanzada y la sociedad. Se centra en un futuro distópico donde la tecnología, especialmente la informática y las redes, coexiste con un entorno social desolado, a menudo dominado por corporaciones poderosas y un gobierno opresivo.

Los relatos *cyberpunk* suelen presentar protagonistas hackers, rebeldes o antihéroes que operan al margen de la ley y utilizan la tecnología para desafiar el orden establecido. Temas como la identidad, la realidad virtual, la inteligencia artificial y la biotecnología son recurrentes en ellos. A menudo, estos mundos ficcionales están marcados por una estética oscura y urbana, donde la tecnología de punta contrasta con la decadencia social.

Autoras y autores destacados del género incluyen a William Gibson, cuyo libro *Neuromante* es considerado uno de los pilares del *cyberpunk*, y Bruce Sterling, entre otros. El *cyberpunk* también ha influido diversos medios, incluyendo películas como *Blade Runner* y *The Matrix*, así como la cultura de los videojuegos y el arte digital. El *cyberpunk* ha dejado una huella profunda en la forma en que se percibe la relación entre la humanidad y la tecnología en la actualidad.

Satoshi Nakamoto, esta persona o grupo de personas quien aún hoy se sigue manteniendo en anonimato, envió lo que se conoce como el «whitepaper de Bitcoin» a un grupo de usuarios que pertenecía a uno de estos foros, y la historia cambió para siempre. De Satoshi solamente sabemos que su

legado, gracias a Bitcoin y Blockchain, ha traspasado el mundo distópico del *cyberpunk*. Podemos decir que la ficción superó a la realidad.

El documento titulado Bitcoin: *Un sistema de efectivo electrónico de transacciones entre pares* describe cómo se puede llevar a cabo un sistema de dinero electrónico que funcione sin la necesidad de un intermediario. Este concepto es esencial para la funcionalidad de Bitcoin y tiene implicaciones significativas para el futuro de las transacciones financieras.

En un sistema financiero tradicional, las transacciones son procesadas por instituciones centrales, como bancos. Estos intermediarios son necesarios para verificar la autenticidad de las transacciones. Sin embargo, este enfoque tiene sus desventajas, como la dependencia de un tercero de confianza, las tarifas asociadas con las transacciones y la posibilidad de censura.

Nakamoto propone un sistema de transacciones entre pares (*peer-to-peer*) donde los participantes en la red pueden interactuar directamente sin necesidad de un intermediario. En este modelo, cada usuario actúa como un nodo en la red, lo que permite que las transacciones sean verificadas y registradas de manera descentralizada. Cualquier persona puede enviar y recibir pagos de forma directa. Esto simplifica el proceso y reduce costos de transacción.

El papel de la criptografía es fundamental en este sistema. Nakamoto utiliza técnicas criptográficas para asegurar que las transacciones sean seguras y que los usuarios puedan comprobar la validez de las mismas. Cada transacción se firma digitalmente, lo que garantiza que solo el propietario de una unidad de Bitcoin pueda gastarla. Además, se establece un protocolo que permite a los nodos de la red comunicarse entre sí intercambiando información sobre las transacciones y su estado.

CRIPTOGRAFÍA, LLAVE DE ACCESO A LA SEGURIDAD

Entonces, ¿qué es la criptografía? Es la disciplina que se encarga del estudio y la práctica de técnicas para proteger la comunicación y la información, de manera que solo las partes autorizadas puedan acceder a ella. Su objetivo principal es garantizar la confidencialidad, integridad y autenticidad de los datos. La criptografía se basa en la utilización de algoritmos matemáticos y claves secretas para codificar y decodificar información.

Existen varios tipos de criptografía, entre los cuales destacan:

1. Criptografía simétrica. Utiliza la misma clave tanto para cifrar como para descifrar la información. La seguridad depende de mantener la clave en secreto.

2. Criptografía asimétrica. También conocida como criptografía de clave pública, utiliza un par de claves: una pública, que puede ser compartida, y una privada, que se mantiene en secreto. Lo que se cifra con la clave pública solo puede ser descifrado con la clave privada correspondiente.

3. Funciones hash. Algoritmos que transforman datos de entrada de cualquier tamaño en una salida de tamaño fijo, generalmente utilizada para asegurar la integridad de los datos.

La criptografía es inherente en muchas áreas, incluyendo la seguridad en Internet, las comunicaciones, la protección de datos personales y la creación de criptomonedas, donde se utiliza para asegurar las transacciones y proteger la identidad de los usuarios.

Una de las innovaciones clave presentadas en esta sección es el concepto de la cadena de bloques (Blockchain). Cada vez que se realiza una transacción, se agrupa con otras en un bloque. Este bloque es luego agregado a la

cadena existente de bloques, lo que forma un registro cronológico de todas las transacciones que han tenido lugar en la red. Este enfoque no solo proporciona un historial de transacciones, sino que también asegura que la información sea inmutable, ya que modificar un bloque requeriría alterar todos los bloques posteriores, algo que es prácticamente imposible sin el consenso de la mayoría de la red.

LA PRUEBA DE TRABAJO COMO UNA SOLUCIÓN AL DOBLE GASTO

Nakamoto también presenta el mecanismo de «prueba de trabajo» (*proof-of-work*) como una forma de proteger la red. El proceso implica que los nodos deben resolver complejos problemas matemáticos para validar y añadir nuevos bloques a la cadena. Esto no solo ayuda a prevenir el doble gasto, sino que también incentiva a los participantes a contribuir con su poder de cómputo, ya que son recompensados con nuevas unidades de Bitcoin por su trabajo.

El doble gasto se refiere a la posibilidad de que un mismo activo digital sea gastado más de una vez, lo que podría socavar la confianza en el sistema y su funcionalidad. Solucionar el doble gasto aborda uno de los desafíos fundamentales que enfrenta cualquier sistema de dinero digital. Nakamoto reconoce que, sin una autoridad central, es vital encontrar una solución efectiva para este problema.

El enfoque tradicional para evitar el doble gasto en sistemas centralizados implica la supervisión de una entidad confiable, como un banco, que verifica y valida cada transacción antes de permitir su procesamiento. En un sistema descentralizado como Bitcoin, en el que no existe una autoridad central, se necesita un mecanismo que garantice la validez de las transacciones sin depender de un tercero.

Nakamoto propone utilizar una red de nodos interconectados que operan de manera independiente pero colaborativa. Cada nodo en la red tiene una copia del libro mayor, o blockchain, que contiene un registro completo de todas las transacciones realizadas. Cuando un usuario realiza una transacción, esta se transmite a la red y es recibida por todos los nodos. Cada nodo verifica la transacción asegurándose de que el remitente tenga suficientes fondos y que la transacción no esté intentando gastar monedas que ya han sido utilizadas en otra operación.

La solución presentada por Nakamoto es la implementación de un mecanismo de consenso basado en la prueba de trabajo (*proof-of-work*). Este método no solo facilita la validación de las transacciones, sino que también introduce un componente de competencia entre los nodos. Para agregar un nuevo bloque de transacciones a la cadena, los nodos deben resolver un complejo problema matemático, un proceso que requiere tiempo y recursos computacionales. Este esfuerzo es lo que asegura la integridad del sistema. Al tener que competir para resolver el problema, los nodos son incentivados a actuar honestamente. Cualquier intento de fraude, como el doble gasto, sería rápidamente detectado por la red.

Una vez que un bloque es añadido a la blockchain, se vuelve parte del registro público y es extremadamente difícil de alterar. Para cambiar una transacción anteriormente confirmada, un atacante tendría que rehacer todos los bloques posteriores a ese punto y superar a la mayoría de los nodos en la red, lo que es prácticamente inviable en una red lo bastante grande y distribuida. Este diseño asegura que, mientras más confirmaciones tenga una transacción, más segura se vuelve, pues el costo de revertirla aumenta exponencialmente.

Además, Nakamoto presenta la idea de que los usuarios deben esperar a que una transacción tenga suficientes confirmaciones antes de considerarla finalizada. Esto significa que, aunque una transacción puede ser vista por todos en la red inmediatamente, la verdadera seguridad de que no se haya

producido un doble gasto se establece a medida que más bloques se añaden a la cadena.

La prueba de trabajo (*proof-of-work*) es un componente fundamental del sistema que permite la creación de un consenso distribuido en la red Bitcoin. Además de asegurar la integridad de las transacciones, previene fraudes creando un entorno en el cual los participantes pueden confiar en que las transacciones son válidas sin necesidad de una autoridad central.

La idea detrás de la prueba de trabajo se basa en la necesidad de que los nodos de la red realicen un trabajo computacional significativo para validar y agregar transacciones a la blockchain. Este trabajo se manifiesta en la resolución de problemas matemáticos complejos que requieren una considerable cantidad de recursos computacionales y tiempo. El proceso implica que los mineros, que son nodos que compiten por validar transacciones, deben encontrar un valor de nonce (un número que solo se utiliza una vez) el cual, al ser combinado con los datos del bloque y procesado a través de una función hash criptográfica, produce un hash que cumple con ciertos criterios de dificultad.

La complejidad de los problemas matemáticos se ajustan periódicamente para garantizar que se fabriquen nuevos bloques de forma constante, aproximadamente cada diez minutos. Mientras más mineros se unen a la red y aumenta la potencia de cómputo total, la complejidad de los problemas también aumenta, lo que mantiene la estabilidad y la previsibilidad en la creación de bloques.

La prueba de trabajo tiene varios beneficios. Primero, actúa como un mecanismo de defensa contra ataques maliciosos. Dado que la creación de un bloque requiere una inversión significativa de recursos, un atacante tendría que controlar más del 50 % de la potencia de cómputo de la red para tener éxito en revertir transacciones previas o para realizar un doble

gasto. Esto hace que sea económicamente poco viable intentar manipular el sistema.

Además, la prueba de trabajo fomenta un entorno competitivo entre los mineros que hace más segura a la red. Cada minero busca resolver el problema antes que el otro, lo cual crea un incentivo para que cada uno contribuya con su poder computacional. Esta competencia asegura la integridad de la cadena de bloques y recompensa a los mineros con nuevas monedas generadas y tarifas de transacción. Así, se proporciona un modelo económico sostenible.

DESCENTRALIZACIÓN

La descentralización es un concepto clave en el diseño del sistema Bitcoin propuesto por Satoshi Nakamoto en su famoso «whitepaper». La descentralización se logra a través de una arquitectura distribuida que involucra múltiples nodos, todos los cuales pueden participar en el proceso de validación y verificación de transacciones.

En el contexto de Bitcoin, la descentralización significa que no hay un único punto de control o fallo. En lugar de depender de una autoridad central, como un banco o un gobierno, la red está compuesta por miles de nodos distribuidos por todo el mundo. Cada uno de estos nodos posee una copia de la blockchain, que es el libro mayor público en el que se registran todas las transacciones. Este enfoque reduce el riesgo de censura y manipulación, ya que no hay una entidad que pueda alterar el registro sin el consenso de la mayoría de los nodos.

La descentralización también fomenta la confianza entre los usuarios. En un sistema centralizado, los usuarios deben confiar en la autoridad que gestiona sus transacciones. En una red descentralizada, la confianza se distribuye entre todos los participantes. Cada nodo verifica las transacciones

y el algoritmo de consenso asegura que solo las transacciones válidas sean aceptadas. Esto crea un ambiente donde los usuarios pueden interactuar sin necesidad de conocer o confiar en los demás, lo que es especialmente valioso en un entorno digital donde las identidades pueden ser anónimas.

Asimismo, la descentralización promueve la innovación y la competencia. Al eliminar la necesidad de intermediarios, se abre la puerta a nuevos modelos de negocio y aplicaciones que pueden surgir sobre la red Bitcoin. Los desarrolladores pueden crear soluciones y servicios que operen sobre la Blockchain sin tener que obtener permisos o licencias de una autoridad central. Esto no solo impulsa la creatividad, sino que también permite que la tecnología evolucione de manera más rápida y eficiente.

Sin embargo, la descentralización también presenta desafíos. Uno de los principales es el problema de la escalabilidad. A medida que más usuarios se unen a la red y el volumen de transacciones aumenta, mantener una infraestructura descentralizada que pueda manejar esta carga se vuelve más complicado. Además, la diversidad de nodos y su distribución geográfica pueden llevar a problemas de latencia y sincronización.

VOCACIÓN POR LA PRIVACIDAD

Otro aspecto central que motivó el éxito de Bitcoin es su vocación por la privacidad. Aunque hablamos de un sistema de dinero digital que opera de manera transparente, con un libro mayor público llamado Blockchain, la privacidad de los usuarios es una preocupación importante que se aborda de manera cuidadosa. Nakamoto entiende que la capacidad de realizar transacciones sin revelar la identidad de los participantes es esencial para fomentar la adopción y el uso generalizado de la criptomoneda.

En el modelo de Bitcoin, las transacciones son visibles para todos los nodos en la red. Cualquier persona puede ver las transacciones y los saldos

asociados a las direcciones de Bitcoin. Sin embargo, la identidad de los propietarios de estas direcciones no está explícitamente vinculada a su nombre o información personal, lo que proporciona un nivel de anonimato. Cada usuario opera con una dirección única, que actúa como un seudónimo en la red. Esto permite a los usuarios realizar transacciones sin revelar su identidad real, aunque sus transacciones sean accesibles públicamente.

El enfoque de Nakamoto hacia la privacidad se basa en la idea de que, aunque las transacciones son transparentes, la privacidad debe ser respetada.

CONDUCTA DEFLACIONARIA

Otro tema interesante que plantea Bitcoin son sus medidas antiinflacionarias, fundamentales para el diseño del sistema monetario propuesto. La inflación es un fenómeno económico tras el aumento generalizado de precios y la disminución del poder adquisitivo de una moneda. Nakamoto reconoce que, para que Bitcoin funcione como una reserva de valor y un medio de intercambio efectivo, es necesario implementar mecanismos que limiten la inflación y fomenten la confianza de los usuarios en la moneda.

Uno de los aspectos más destacados de las medidas antiinflacionarias en Bitcoin es su suministro limitado. Nakamoto establece que el total de bitcoins que se pueden crear está fijado en 21 millones. Este límite contrasta con las monedas tradicionales, que pueden ser emitidas en cantidades ilimitadas por los bancos centrales.

Inicialmente, los mineros reciben una recompensa importante por cada bloque que añaden a la cadena de bloques, pero esta recompensa se reduce a la mitad aproximadamente cada cuatro años en un evento conocido como «halving». Esto no solo limita la cantidad de bitcoins que se introducen en circulación, sino que también crea una disminución predecible en la tasa de inflación a largo plazo. A medida que el número de bitcoins en circulación

se acerca al límite de 21 millones, se espera que la inflación se reduzca significativamente, lo que puede conducir a una apreciación del valor de la moneda. Esta estructura ofrece a los usuarios una forma de proteger su inversión contra la inflación, ya que el suministro escaso puede generar una demanda creciente siempre que más personas se interesan en utilizar y mantener bitcoins.

Además, Nakamoto implementa un sistema de ajuste de dificultad en el proceso de minería. Esta medida asegura que, independientemente de cuántos mineros participen en la red, los bloques se añaden a la cadena aproximadamente cada diez minutos. Si más mineros se unen y la tasa de generación de bloques aumenta, el sistema ajusta la dificultad para mantener constante ese intervalo de tiempo. Este ajuste evita la sobreproducción de bitcoins y estabiliza la tasa de inflación.

Otro aspecto importante de las medidas antiinflacionarias es la forma en que Bitcoin permite a los usuarios realizar transacciones sin intermediarios. Al eliminar la necesidad de un banco central o de instituciones financieras que controlen la emisión de dinero, Bitcoin se convierte en una forma de dinero más resistente a la manipulación inflacionaria. Los usuarios tienen un mayor control sobre sus activos y pueden decidir cuándo y cómo gastar sus bitcoins, lo que limita la influencia de políticas monetarias inflacionarias.

Sin embargo, Nakamoto también es consciente de que el éxito de estas medidas antiinflacionarias depende de la confianza de los usuarios en el sistema. Para que Bitcoin sea efectivo como una reserva de valor, las personas deben creer en su escasez y en la integridad del protocolo. La comunidad de usuarios y desarrolladores juega un papel crucial en la vigilancia y el mantenimiento del sistema, pues aseguran que las reglas predefinidas se respeten y que no se produzcan cambios arbitrarios en el suministro de bitcoins.

MINERÍA DE BITCOIN

La minería de Bitcoin es un proceso fundamental en el ecosistema de los activos digitales. Permite validar transacciones y asegurar la red. Sin embargo, este proceso requiere muchos recursos y genera una cantidad considerable de calor, lo que plantea un desafío significativo en términos de gestión térmica. Para abordar este problema, se han desarrollado diversas técnicas de enfriamiento en los centros de datos de gran volumen, entre las cuales destacan el *aircooling*, *hydrocooling* e *immersion cooling*.

Aircooling

El *aircooling* es la técnica de enfriamiento más utilizada en la minería de Bitcoin. Consiste en el uso de ventiladores y disipadores de calor que permiten la circulación de aire fresco y, así, enfriar los componentes de los equipos mineros. Es relativamente económica y fácil de implementar, lo que la convierte en una opción popular entre los mineros a pequeña escala. Sin embargo, su eficiencia se ve limitada en condiciones de alta temperatura y puede resultar en un consumo energético elevado debido al uso constante de ventiladores.

Hydrocooling

El *hydrocooling* utiliza agua como medio de enfriamiento. Implica la circulación de agua a través de un sistema de tuberías que absorbe el calor generado por los equipos mineros. La ventaja de esta técnica radica en su capacidad para mantener temperaturas más bajas de manera más eficiente que el *aircooling*, lo que puede traducirse en un mejor rendimiento de los mineros. No obstante, el *hydrocooling* requiere una infraestructura más compleja y puede presentar riesgos asociados con la gestión del agua y la posibilidad de fugas.

Immersion Cooling

El *immersion cooling* es una técnica innovadora que ha ganado popularidad en los últimos años. Los dispositivos mineros se sumergen en un líquido dieléctrico que disipa el calor de manera más efectiva. La inmersión total permite que el calor se elimine de forma más rápida y eficiente, lo que resulta en un mejor rendimiento y una mayor longevidad de los equipos. A pesar de sus beneficios, la inmersión presenta desafíos en términos de costos iniciales y la necesidad de un manejo especializado del líquido.

La minería o procesamiento de datos, en este caso de Bitcoin, es un proceso importante que permite la creación de nuevas monedas y la verificación de transacciones dentro de la red de Bitcoin. Este proceso se lleva a cabo utilizando equipos informáticos que resuelven complejos problemas matemáticos. Cada vez que se realiza una transacción dentro de la red, esta debe ser agrupada en un bloque. Los mineros compiten para ser los primeros en resolver un problema matemático asociado a ese bloque. Este problema, que implica encontrar un número específico llamado «nonce», es extremadamente difícil de resolver, pero fácil de verificar una vez encontrado. El primer minero que resuelve el problema tiene el derecho de agregar el bloque a la cadena de bloques, que es un registro público y compartido de todas las transacciones realizadas.

Una vez que un bloque es añadido a la cadena de bloques, o Blockchain, el minero es recompensado con los bitcoins recién generados, así como con las tarifas de transacción asociadas a las transacciones incluidas en ese bloque. Esta recompensa sirve como un incentivo para que los mineros continúen participando en el proceso, lo que a su vez mantiene la red segura y funcional.

POOL DE MINERÍA

Entonces, ¿de qué manera aumento las chances de generar Bitcoins? A través de un pool de minería, que es un grupo de mineros que se juntan para combinar su poder de procesamiento y aumentar las probabilidades de resolver bloques de transacciones. Al unirse en un pool, los mineros comparten los recursos de hardware y, por tanto, la capacidad de resolver problemas matemáticos complejos que permiten validar transacciones y crear nuevos bloques en la Blockchain de Bitcoin. Este enfoque colaborativo permite a los participantes del pool trabajar juntos para encontrar soluciones más rápido, lo que resulta en una mayor frecuencia de recompensas por bloque minado.

La distribución de las recompensas en un pool de minería se realiza de manera proporcional al poder de procesamiento que cada miembro aporta. Esto significa que, si un minero contribuye con un porcentaje determinado del total de poder de procesamiento del pool, recibirá una parte proporcional de las recompensas obtenidas. Esta metodología brinda a los mineros individuales una fuente más predecible de ingresos, en contraposición a la naturaleza aleatoria de la minería en solitario. Aquí es muy visual el ejemplo literal de la minería de antaño. Si en una mina, donde varios mineros se encontraban picando piedras de manera individual y uno encontraba una piedra preciosa, la recompensa de ese día se repartía entre todos los mineros presentes. El mismo concepto aplica para el pool de minería.

QUÉ LE DA SU VALOR A BITCOIN?

Son varios los factores que le otorgan su valor a Bitcoin.

ESCASEZ Y OFERTA LIMITADA

Uno de los factores primordiales que otorgan valor a Bitcoin es su naturaleza escasa. A diferencia de las monedas fiduciarias, que pueden ser emitidas sin límite por los bancos centrales, Bitcoin tiene un suministro máximo de 21 millones de monedas. Este modelo de escasez digital, análogo a los recursos naturales limitados, crea una sensación de valor intrínseco. A medida que se acerca el límite de suministro, la presión de la oferta y la demanda puede hacer que el precio de Bitcoin se aprecie, lo que atrae a inversores que buscan un activo con potencial de apreciación a largo plazo.

DESCENTRALIZACIÓN Y RESISTENCIA A LA CENSURA

Otro aspecto crucial que otorga valor a Bitcoin es su estructura descentralizada. A diferencia de los sistemas financieros tradicionales, Bitcoin opera en una red blockchain que no está controlada por ninguna entidad central. Esta descentralización no solo minimiza el riesgo de manipulación por parte de gobiernos o instituciones financieras, sino que también otorga a los usuarios un mayor control sobre sus activos. La resistencia a la censura es un atractivo significativo en contextos donde los sistemas financieros tradicionales son ineficaces o restrictivos, pues permite a las personas preservar su riqueza y realizar transacciones sin interferencias.

TECNOLOGÍA Y SEGURIDAD

La tecnología subyacente de Bitcoin, conocida como Blockchain, es otro componente importante que contribuye a su valor. Permite la creación de

un libro de contabilidad distribuido, donde cada transacción es registrada de manera transparente y permanente. La seguridad que ofrece Bitcoin, a través de complejos algoritmos criptográficos, disminuye considerablemente el riesgo de fraude y manipulación. La confianza en esta tecnología sustenta su valor, ya que los usuarios deben creer en la integridad del sistema para adoptar Bitcoin como un activo viable.

ACEPTACIÓN Y ADOPCIÓN CRECIENTE

El valor de Bitcoin también está influenciado por su aceptación y adopción en el mercado. Mientras más comerciantes y empresas comiencen a aceptar Bitcoin como forma de pago, su utilidad como medio de intercambio se incrementa. Esta creciente adopción legitima a Bitcoin como una alternativa viable a las monedas tradicionales, y a su vez puede contribuir a su valoración. Además, la inclusión de Bitcoin en plataformas de inversión y fondos institucionales ha aumentado su visibilidad y accesibilidad, lo que ha atraído a un público más amplio.

PERSPECTIVAS ECONÓMICAS Y DE INVERSIÓN

Desde una perspectiva económica, Bitcoin ha sido visto por muchos como una cobertura contra la inflación y la devaluación de las monedas tradicionales. En entornos económicos inciertos, donde las políticas monetarias pueden llevar a la depreciación de las divisas, los inversores han comenzado a considerar a Bitcoin como una reserva de valor. Este fenómeno ha llevado a un aumento en la demanda de Bitcoin y, con ello, ha contribuido a su apreciación en el mercado. Además, la volatilidad inherente de Bitcoin ha atraído a los especuladores que buscan aprovechar las fluctuaciones de precios, lo que a su vez alimenta su valor.

FACTORES PSICOLÓGICOS Y SOCIOCULTURALES

El valor de Bitcoin también está influenciado por factores psicológicos y socioculturales. La narrativa en torno a Bitcoin como un «activo del futuro» y su asociación con movimientos de innovación y disrupción tecnológica han generado un fervor que impulsa la demanda. La comunidad de entusiastas de Bitcoin, así como la cobertura mediática, han creado una especie de «efecto de manada» que puede llevar a movimientos de precios significativos. La creencia en el potencial de Bitcoin para transformar el sistema financiero global también juega un papel importante en su valoración.

Podemos decir entonces que el valor de Bitcoin es el resultado de una combinación compleja de factores. Su escasez inherente, la descentralización, la tecnología de seguridad, la creciente aceptación, las perspectivas económicas y los factores psicológicos son componentes interrelacionados que contribuyen a su valoración. A medida que Bitcoin continúa evolucionando, es fundamental que los inversores y usuarios comprendan estos elementos para tomar decisiones informadas.

VALOR DEL BITCOIN EN EL TIEMPO

El Bitcoin, la criptomoneda pionera y más reconocida a nivel mundial, ha experimentado una montaña rusa de valores desde su creación en 2009. Este artículo ofrece un resumen detallado de los mínimos y máximos históricos del Bitcoin año por año más una breve explicación de los factores que han influido en sus fluctuaciones de precios.

Inicia una revolución financiera

Mínimo y máximo de 2009: USD 0.0008 - USD 0.09.

El Bitcoin fue lanzado en enero de 2009 por Satoshi Nakamoto. Durante este año, Bitcoin no tenía valor de mercado real y se intercambiaba

entre entusiastas por precios simbólicos. La falta de una infraestructura de negociación sólida y el escaso conocimiento del público sobre las criptomonedas influyeron en su bajo valor inicial.

La primera transacción comercial

Mínimo y máximo de 2010: USD 0.0008 - USD 0.39.

El hito más notable de 2010 fue la primera transacción comercial de Bitcoin, en la que se pagaron 10 000 Bitcoin por dos pizzas, valoradas en aproximadamente USD 25. Este evento histórico ayudó a establecer un valor de mercado inicial para Bitcoin, aunque la moneda seguía siendo extremadamente volátil y poco conocida.

Primer aumento significativo

Mínimo y máximo de 2011: USD 0.30 - USD 31.91.

En 2011, Bitcoin comenzó a ganar popularidad, y su precio se disparó a casi USD 32 en junio. Sin embargo, el mercado aún era muy volátil y el precio retrocedió rápidamente. Este aumento se debió en parte a la creciente cobertura mediática y al interés de los primeros inversores.

Consolidación y estabilidad relativa

Mínimo y máximo de 2012: USD 4.22 - USD 13.51.

El año 2012 vio una mayor estabilidad en el precio, con un rango de valores significativamente más estrecho. La comunidad de usuarios y desarrolladores continuó creciendo, y se implementaron mejoras técnicas que aumentaron la credibilidad y funcionalidad de la criptomoneda.

El primer gran rally

Mínimo y máximo de 2013: USD 13.30 - USD 1 156.

2013 fue un año crucial para todos los entusiastas del Bitcoin. El precio comenzó a dispararse en la primera mitad del año, alcanzó un máximo de USD 266 en abril y luego cayó. Posteriormente, en noviembre, Bitcoin alcanzó un nuevo máximo histórico de USD 1 156. Este auge fue impulsado por el aumento del interés institucional y la cobertura mediática global, aunque también hubo preocupaciones sobre burbujas especulativas.

Colapso de Mt. Gox

Mínimo y máximo de 2014: USD 309.87 - USD 951.

El colapso del *exchange* de criptomonedas Mt. Gox en febrero de 2014 tuvo un impacto significativo en el precio de Bitcoin, que cayó drásticamente. Este evento subrayó la importancia de la seguridad y la regulación en el mercado de criptomonedas. A pesar de estos desafíos, el precio se mantuvo relativamente estable en comparación con años anteriores.

Recuperación y crecimiento

Mínimo y máximo de 2015: USD 177.28 - USD 465.50.

Tras el colapso de Mt. Gox, el precio comenzó a recuperarse en 2015. La comunidad continuó trabajando en mejoras técnicas y de seguridad, y el interés en la tecnología Blockchain aumentó. Estos factores contribuyeron a una recuperación gradual del precio.

El halving y mayor adopción

Mínimo y máximo de 2016: USD 358.77 - USD 978.62.

El segundo *halving* de Bitcoin, que redujo la recompensa por bloque minado de 25 a 12.5 BTC, ocurrió en julio de 2016. Este evento redujo la oferta de nuevos Bitcoins y en él se anticipó que la moneda aumentaría su valor. Además, la adopción de Bitcoin como medio de pago y su reconocimiento como una reserva de valor contribuyeron a la apreciación del precio.

La explosión del mercado

Mínimo y máximo de 2017: USD 775.98 - USD 19 783.06.

En el año 2017 hubo un crecimiento exponencial. Desde un precio de aproximadamente USD 775 a principios de año, Bitcoin alcanzó un máximo histórico de casi USD 20 000 en diciembre. Este auge fue impulsado por un frenesí especulativo, el lanzamiento de futuros de Bitcoin y un aumento masivo en el interés de los inversores minoristas e institucionales.

La gran corrección

Mínimo y máximo de 2018: USD 3 191 - USD 17 527.

Después del espectacular aumento de 2017, el precio de Bitcoin sufrió una corrección importante en 2018. Aunque comenzó el año en niveles elevados, el precio cayó a aproximadamente USD 3 191 en diciembre. La corrección fue atribuida a la toma de ganancias, el aumento de la regulación y las preocupaciones sobre la viabilidad a largo plazo de las criptomonedas.

Estabilidad y recuperación moderada

Mínimo y máximo de 2019: USD 3 360.58 - USD 13 796.49.

En 2019, Bitcoin mostró signos de recuperación tras la corrección del año anterior. El precio fluctuó entre USD 3 360 y casi USD 14 000. El aumento del interés institucional y la adopción de la tecnología Blockchain por parte de grandes corporaciones contribuyeron a esta tendencia positiva.

Pandemia y resiliencia

Mínimo y máximo de 2020 USD 4 106.98 - USD 29 244.49.

La pandemia de COVID-19 afectó a los mercados financieros, incluido Bitcoin, que cayó a alrededor de USD 4 100 en marzo. Sin embargo, la criptomoneda mostró una notable resiliencia recuperándose y alcanzando un nuevo

máximo histórico de USD 29 244 en diciembre. La creciente percepción de Bitcoin como una reserva de valor y la adopción por parte de grandes inversores institucionales fueron factores clave.

Nuevos máximos históricos

Mínimo y máximo de 2021: USD 27 734 - USD 68 789.

En el año 2021, el Bitcoin pasó por un aumento sin precedentes en el precio, que alcanzó un máximo histórico de casi USD 69 000 en noviembre. Numerosas empresas de Wall Street, como Tesla, MicroStrategy o Block, se lanzaron a la compra de Bitcoin y lo incluyen en sus balances y operaciones de tesorería.

En España, los bancos dieron luz verde para la comercialización de criptomonedas. El Banco de España anunció en octubre de ese año un registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos. Ese año, El Salvador también entra al juego de manera sorprendentemente audaz anunciando que el Bitcoin será una moneda de curso legal en ese país y que todos los días el Estado comprará Bitcoin por concepto de reserva.

Correcciones y adopción

Mínimo y máximo de 2022: USD 16 283 - USD 48 086.

El 2022 no fue un año precisamente bueno para quien ingresó a Bitcoin entusiasmado por su máximo histórico de 2021, pero no dejó de ser un año interesante para los entusiastas veteranos y para aquellos que supieron perseverar a pesar de las correcciones.

En abril, la República Centroafricana adoptó al Bitcoin como moneda de curso legal en ese país.

En términos de regulación, el 2022 fue un año de creciente atención por parte de los gobiernos y organismos reguladores hacia Bitcoin y las criptomonedas en general. Estados Unidos y la Unión Europea avanzaron en la creación de marcos regulatorios destinados a brindar mayor claridad y protección a los inversores en criptomonedas.

Uno de los avances más destacados fue la creciente adopción de la red Lightning, una solución de segunda capa diseñada para mejorar la escalabilidad al permitir transacciones rápidas y de bajo costo. Su rápida adopción facilitó microtransacciones y promovió el uso de Bitcoin en el comercio diario.

Estabilización y meseta

Mínimo y máximo de 2023: USD 16 759 - USD 44 706.

Este año presentó altibajos en el espacio de las criptomonedas y, definitivamente, trajo algunas sorpresas consigo.

La aprobación de nuevas regulaciones alrededor del mundo y el interés de jugadores de alto perfil de la industria financiera por un ETF Bitcoin fueron algunos de los eventos notables durante el 2023.

A un año de la implosión del ecosistema Terra y el infame quiebre del intercambio FTX, el mercado de criptomonedas se recuperó mientras algunos afectados encontraron justicia en la detención de los creadores de ambos proyectos. Sam Bankman-Fried fue dictado culpable del colapso de FTX. El año se mostró más conservador que otros años *pre-halving*.

Nuevo halving y promesas

Mínimo y máximo de 2024: USD 40 127 - USD 73 750 (hasta octubre).

La masiva adopción de ETF y las agresivas compras por parte de Blackrock en año de *halving* vaticinaban un aumento en el precio. Sin embargo,

excluyendo un éxtasis *pre-halving* en marzo, en el cual se alcanzó el máximo registrado en el año, luego del *halving,* a Bitcoin le ha costado mantenerse sobre los USD 60 000, pues ha oscilado durante meses entre los USD 59 000 y USD 56 000 con cierta estabilidad. De todas maneras, al ser un año con poco movimiento con respecto a los *halving* anteriores, la rentabilidad para quien compró el primer día del año con respecto al precio actual supera un 50 %. La aparente meseta del año es simplemente un juego de ansiedades.

¿DÓNDE SE GUARDAN LOS BIT-COINS?

HARDWARE WALLETS

Las *hardware wallets,* o billeteras de *hardware,* son dispositivos físicos diseñados específicamente para el almacenamiento seguro de criptomonedas. Contrario a las billeteras de software, que almacenan las claves privadas en un dispositivo conectado a Internet, las billeteras de hardware almacenan estas claves en un entorno aislado, lo que las hace menos vulnerables a ataques cibernéticos.

El funcionamiento de una hardware wallet se basa en la generación y almacenamiento de claves criptográficas. Cuando un usuario crea una billetera de hardware, se genera una clave privada única adherida al dispositivo. Las transacciones se firman dentro de la billetera. La clave privada nunca se expone a Internet, incluso durante la transacción. Esto proporciona una capa adicional de seguridad, ya que reduce el riesgo de que los *hackers* accedan a las claves privadas.

Ventajas de las hardware wallets

1. Seguridad: La principal ventaja de las billeteras de *hardware* es su alta seguridad. Al almacenar las claves privadas fuera de Internet, se minimiza el riesgo de robo por parte de *hackers* y *malware*. Además, la mayoría cuentan con medidas adicionales de seguridad, como autenticación de dos factores y protección mediante un código PIN.

2. Control total: A diferencia de las plataformas de intercambio de criptomonedas, en las que los usuarios confían en terceros para almacenar sus activos, las billeteras de *hardware* permiten a los usuarios tener el control total de sus claves privadas. Esto significa que el usuario es el único responsable de su seguridad y gestión de activos.

3. Compatibilidad: La mayoría de las *hardware wallets* son compatibles con múltiples criptomonedas y se pueden utilizar con diversas aplicaciones de

software de billetera, lo que facilita la gestión de diferentes tipos de activos digitales en un solo dispositivo.

4. Durabilidad y portabilidad: Las billeteras de *hardware* están pensadas para ser robustas y duraderas. Además, su tamaño compacto las hace fáciles de transportar, lo que permite a los usuarios llevar sus criptomonedas de manera segura a cualquier lugar.

Desventajas de las hardware wallets

1. Costo: En contraste con las billeteras de software, que son gratuitas, las *hardware wallets* requieren una inversión inicial. Los precios pueden variar según la marca y las características del dispositivo.

2. Riesgo de pérdida o daño: Si el usuario pierde su billetera o sufre daños irreparables en el dispositivo, puede perder el acceso a sus criptomonedas de manera permanente, a menos que haya realizado copias de seguridad adecuadas de sus claves privadas.

3. Complejidad en el uso: Para los nuevos usuarios, la configuración y el uso de una *hardware wallet* pueden parecer complicados. Requiere cierta familiaridad con el manejo de criptomonedas y la comprensión de conceptos como claves públicas y privadas.

Importancia de las hardware wallets en el ecosistema de las criptomonedas

Las hardware wallets juegan un papel decisivo en el ecosistema de las criptomonedas, especialmente en un contexto donde la seguridad es una preocupación constante. A medida que más personas adoptan criptomonedas como medio de inversión, la necesidad de soluciones seguras para el almacenamiento de activos digitales se vuelve fundamental. Las billeteras de hardware no solo proporcionan un medio seguro para almacenar criptomonedas, sino que también fomentan la educación del usuario sobre la importancia de la seguridad en el mundo digital.

Además, en un entorno donde las regulaciones sobre criptomonedas están en constante evolución, contar con una *hardware wallet* permite a los usuarios mantener la soberanía sobre sus activos. Esto evita la dependencia de plataformas de intercambio que pueden estar sujetas a restricciones legales.

MOBILE WALLETS

Una *mobile wallet,* o billetera móvil*,* es una aplicación que permite a los usuarios almacenar información de sus tarjetas de crédito, débito y otros datos financieros en sus dispositivos móviles. Esta información puede ser utilizada para realizar compras en línea o en establecimientos físicos, así como para enviar y recibir dinero entre usuarios. Las billeteras móviles suelen funcionar a través de tecnologías como NFC (Comunicación de campo cercano, en español) y códigos QR, lo que facilita la realización de transacciones rápidas y seguras.

Para utilizar una *mobile wallet*, el usuario debe descargar la aplicación en su teléfono inteligente y vincularla a su cuenta bancaria o tarjetas de crédito. Una vez configurada, el usuario puede realizar pagos de forma sencilla, ya sea acercando su dispositivo a un terminal de pago compatible o escaneando un código QR. Las billeteras móviles también ofrecen la posibilidad de llevar un registro de las transacciones. Esto contribuye a una mejor gestión financiera.

Ventajas de las mobile wallets

Las *mobile wallets* ofrecen una serie de ventajas que han contribuido a su creciente popularidad:

1. Comodidad: La posibilidad de llevar todas las tarjetas e información financiera en un solo dispositivo simplifica el proceso de pago. Los usuarios no necesitan llevar efectivo ni múltiples tarjetas, lo que reduce el riesgo de pérdida o robo.

2. Seguridad: Las *mobile wallets* implementan diversas medidas de seguridad para proteger la información del usuario. Esto incluye encriptación de datos, autenticación biométrica (como huellas dactilares o reconocimiento facial) y la generación de códigos únicos para cada transacción. Tales características hacen que estas billeteras sean generalmente más seguras que los pagos con tarjetas de plástico.

3. Rapidez: Las transacciones realizadas a través de *mobile wallets* suelen ser más rápidas que los métodos tradicionales. Esto es beneficioso en entornos de alta demanda, como tiendas o eventos, donde la eficiencia en el proceso de pago es crucial.

4. Ofertas y recompensas: Muchas aplicaciones de billeteras móviles ofrecen programas de lealtad, descuentos y promociones exclusivas, lo que puede resultar en ahorros significativos para los usuarios.

5. Facilidad para enviar y recibir dinero: Las *mobile wallets* permiten transferencias de dinero entre usuarios de manera instantánea y sin complicaciones, algo útil para dividir cuentas o enviar regalos monetarios.

Desventajas de las mobile wallets

A pesar de sus numerosas ventajas, estas billeteras también presentan algunos inconvenientes, lo cual es importante considerar:

1. Dependencia de la tecnología: Para utilizar una *mobile wallet*, es necesario contar con un teléfono compatible y acceso a Internet. Esto puede ser un obstáculo en áreas con infraestructuras tecnológicas limitadas.

2. Preocupaciones de privacidad: El almacenamiento de información financiera en dispositivos móviles plantea preocupaciones sobre la privacidad y el uso indebido de datos. Los usuarios deben ser cautelosos al elegir aplicaciones y asegurarse de que cumplen con los estándares de seguridad.

3. Falta de aceptación: Aunque la aceptación de las billeteras móviles está en aumento, no todos los comercios están equipados para aceptar pagos a través de estas plataformas. Tal cosa puede limitar su utilidad en ciertas situaciones.

4. Riesgo de pérdida del dispositivo: Si un usuario pierde o le roban su dispositivo móvil, existe el riesgo de que su información financiera esté comprometida. Sin embargo, muchas aplicaciones ofrecen opciones de bloqueo remoto y eliminación de datos para mitigar este riesgo.

Impacto de las mobile wallets en la economía global

El crecimiento de las *mobile wallets* ha tenido un impacto significativo en la economía global. A medida que más personas adoptan esta tecnología, el uso de efectivo y tarjetas de crédito tradicionales ha disminuido en muchas regiones. Esto ha llevado a un cambio en la forma en que los comerciantes y las instituciones financieras operan, pues impulsa la innovación en servicios de pago y la creación de nuevas soluciones financieras.

Además, el auge de las billeteras móviles ha facilitado la inclusión financiera permitiendo que personas sin acceso a servicios bancarios tradicionales puedan realizar transacciones, ahorrar y participar en la economía digital. Esto es especialmente relevante en países en desarrollo, donde el acceso a la tecnología móvil es más común que el acceso a bancos físicos.

Desktop Wallets

Las *desktop wallets,* o billeteras de escritorio*,* son programas que se instalan en computadoras de escritorio o portátiles, los cuales proporcionan a los usuarios un medio para interactuar con diferentes redes de criptomonedas. Estas billeteras permite almacenar las claves privadas y públicas de forma local en el dispositivo, lo que significa que el usuario tiene control total sobre sus activos digitales. A diferencia de las billeteras en línea, en las que

las claves son gestionadas por un tercero, las *desktop wallets* ofrecen un mayor nivel de seguridad, ya que las claves privadas quedan ancladas en el dispositivo del usuario.

El funcionamiento de una *desktop wallet* se basa en la generación y gestión de pares de claves criptográficas. Al crear una billetera de escritorio, el *software* genera una clave privada que permite al usuario acceder a sus fondos y una clave pública que se utiliza para recibir criptomonedas. Cuando un usuario desea realizar una transacción, la billetera utiliza la clave privada para firmar la transacción, que luego se envía a la red de la criptomoneda correspondiente para su verificación.

Ventajas de las desktop wallets

1. Seguridad: Una de las principales ventajas de utilizar una *desktop wallet* es su nivel de seguridad. Almacenar las claves privadas en un dispositivo local reduce el riesgo de hackeos en plataformas en línea. Además, muchas billeteras de escritorio ofrecen características adicionales de seguridad, como cifrado y autenticación de dos factores.

2. Control total: Las *desktop wallets* permiten a los usuarios tener un control total sobre sus fondos. Los usuarios son responsables de la gestión de sus claves privadas, lo que les otorga un mayor sentido de propiedad y autonomía sobre sus activos.

3. Interfaz amigable: La mayoría de las billeteras de escritorio tienen interfaces intuitivas que facilitan la navegación y la gestión de criptomonedas. Esto las hace accesibles tanto para principiantes como para usuarios experimentados.

4. Compatibilidad: Las *desktop wallets* son compatibles con una amplia variedad de criptomonedas, lo que permite a los usuarios gestionar múltiples activos desde una sola aplicación.

Desventajas de las desktop wallets

1. Vulnerabilidad a *malware*: Aunque ofrecen un alto nivel de seguridad, las *desktop wallets* pueden ser vulnerables a *malware* y virus que puedan infectar el dispositivo. Es importante que los usuarios mantengan su *software* actualizado y utilicen programas de seguridad confiables.

2. Dependencia del *hardware:* Dado que las claves privadas se almacenan localmente, si el dispositivo se daña o se pierde, los usuarios pueden perder el acceso a sus fondos de manera irreversible, a menos que hayan realizado copias de seguridad adecuadas.

3. Conexión a Internet: Para realizar transacciones, las *desktop wallets* requieren una conexión a Internet. Esto las hace menos seguras en comparación con las *cold wallets*, o billeteras frías, que almacenan las claves privadas sin conexión.

4. Complejas para principiantes: Aunque la interfaz puede ser amigable, la configuración inicial y la gestión de claves privadas pueden resultar complicadas para aquellos que son nuevos en el mundo de las criptomonedas.

¿QUÉ SON LOS EXCHANGES Y CUÁL ES SU RELEVANCIA?

Los *exchanges* de criptomonedas son plataformas que permiten a los usuarios intercambiar criptomonedas por otras criptomonedas o por dinero fiat, como el dólar o el euro. Existen diversos tipos de *exchanges*, que se pueden clasificar en dos categorías principales: *exchanges* centralizados (CEX) y *exchanges* descentralizados (DEX).

Los *exchanges* centralizados son gestionados por una entidad o empresa específica que actúa como intermediario en las transacciones. Suelen ofrecer una interfaz de usuario más amigable y varios servicios adicionales, como almacenamiento de criptomonedas y herramientas de *trading* avanzadas. Sin embargo, su centralización también los hace vulnerables a ataques cibernéticos y a problemas de seguridad, como el robo de fondos.

Por otro lado, los *exchanges* descentralizados operan sin un intermediario central. Utilizan contratos inteligentes en la blockchain para facilitar las transacciones. Esto aporta a los usuarios mayor control sobre sus fondos y más privacidad, ya que no es necesario proporcionar información personal. No obstante, los DEX pueden ser más complejos de usar y carecen de algunas funcionalidades que ofrecen sus contrapartes centralizadas.

FUNCIONAMIENTO DE LOS EXCHANGES

El funcionamiento de los *exchanges* implica varios procesos clave. Primero, los usuarios crean una cuenta en la plataforma y realizan un depósito, ya sea de criptomonedas o de dinero fiat. A partir de este momento, pueden hacer órdenes de compra o venta en el libro de órdenes del *exchange*. Estas órdenes se emparejan según los precios establecidos, lo cual permite que las transacciones se realicen de manera eficiente.

Los *exchanges* también proporcionan gráficos en tiempo real, información sobre las tendencias del mercado y herramientas para el análisis técnico,

así los *traders* son capaces de tomar decisiones informadas. Además, muchos *exchanges* ofrecen funciones adicionales, como la posibilidad de realizar *trading* con margen y participar en programas de *staking* y *lending* que pueden generar ingresos pasivos.

RELEVANCIA DE LOS EXCHANGE EN EL MUNDO DE LOS ACTIVOS DIGITALES

La relevancia de los *exchanges* en el mundo de las criptomonedas es innegable. En primer lugar, actúan como el puente entre el mundo fiat y el mundo cripto permitiendo a los usuarios convertir dinero tradicional en activos digitales y viceversa. Esto es especialmente importante para la adopción masiva de criptomonedas, pues facilita la entrada de nuevos usuarios al ecosistema.

Además, los *exchanges* son un indicador clave de la salud y actividad del mercado. Las fluctuaciones en los volúmenes de *trading* y en los precios de las criptomonedas que se observan en los *exchanges* son reflejo de la demanda y el interés de los inversores. A través de estas plataformas, los usuarios pueden participar en la formación de precios y en la liquidez del mercado, algo fundamental para el crecimiento de un ecosistema financiero sostenible.

Otro aspecto relevante es el papel de los *exchanges* en la innovación y el desarrollo de nuevas tecnologías. Muchos *exchanges* están a la vanguardia de la adopción de nuevas soluciones blockchain, mediante servicios como la integración de protocolos DeFi (finanzas descentralizadas) y la emisión de *tokens* a través de *Initial Exchange Offerings* (IEO). Esto no solo amplía las oportunidades para los inversores, sino que también fomenta la creación de nuevos proyectos criptográficos.

Sin embargo, la relevancia de los *exchanges* también viene acompañada de desafíos significativos. La regulación es un tema candente. Muchos gobiernos están trabajando para establecer marcos legales que regulen las operaciones de estas plataformas, lo que puede impactar su funcionamiento y crecimiento. Además, la seguridad sigue siendo una preocupación primordial. Con el tiempo, ha habido numerosos casos de *hackeos* y fraudes en *exchanges* centralizados. Esto ha llevado a una pérdida de confianza entre los usuarios.

¿DE QUÉ MANERA SE GANA DINERO CON BITCOIN?

Esta sección no ofrece consejos financieros ni busca impulsar al lector a realizar ningún tipo de inversión. Simplemente es algo que debemos incluir por el simple hecho de que, desde su aparición en 2009, Bitcoin ha capturado la atención de inversores, personas afines a la tecnología y al público en general. Su naturaleza descentralizada y su potencial para revolucionar el sistema financiero global han sido temas de discusión constante. A todos los entusiastas de este rubro nos hacen repetidamente la pregunta: ¿de qué manera se puede ganar dinero con Bitcoin?

COMPRA Y VENTA

El *trading* de Bitcoin es una de las formas más comunes de ganar dinero. Las personas compran Bitcoin a un precio bajo y lo venden a un precio más alto. Este método requiere un buen entendimiento del mercado y de sus fluctuaciones. Existen varios tipos de *trading*:

***Trading* Diario:** Implica comprar y vender Bitcoin en un solo día. Este método se basa en aprovechar pequeñas fluctuaciones de precio para obtener ganancias rápidas.

Swing Trading: Se centra en capturar tendencias a corto y mediano plazo mientras se mantiene la inversión durante días o semanas.

***Trading* a largo plazo (Hold):** Los inversores compran Bitcoin y lo mantienen durante un período prolongado esperando que su valor aumente con el tiempo.

MINERÍA

La minería es el proceso de validar y registrar transacciones en la cadena de bloques de Bitcoin. Los mineros utilizan computadoras para resolver complejas ecuaciones matemáticas. A cambio, reciben nuevas monedas

como recompensa. Dados los niveles de *hashrate* en el mundo y de dificultad de minado, la minería particular o casera no es el camino más eficiente para dedicarse a esto.

STAKING Y PRÉSTAMOS DE BITCOIN

Aunque el *staking*[1] es más común en criptomonedas que usan el protocolo *proof-of-stake*, algunos servicios permiten a los usuarios «prestar» sus Bitcoin a cambio de un interés. Plataformas de préstamos de criptomonedas ofrecen la posibilidad de ganar intereses al depositar Bitcoin en sus cuentas. Este método ofrece una forma pasiva de generar ingresos.

FAUCETS Y MICRO TAREAS

Existen sitios web llamados «faucets» que ofrecen pequeñas cantidades de Bitcoin a cambio de completar tareas sencillas, como ver anuncios o resolver captchas. Aunque no es la forma más rápida de acumular grandes cantidades, puede ser una entrada útil para principiantes al mundo de las criptomonedas.

PARTICIPACIÓN EN PROGRAMAS DE AFILIADOS

Muchas plataformas de intercambio y servicios de criptomonedas ofrecen programas de afiliados. Al referir nuevos usuarios, es posible ganar comisiones en Bitcoin. Esta estrategia es efectiva si se tiene acceso a una amplia audiencia interesada en las criptomonedas.

---

[1] *Staking* es el proceso mediante el cual los poseedores de criptomonedas participan en la validación de transacciones y la seguridad de una red blockchain al mantener y «bloquear» sus activos en una billetera. A cambio de esta contribución, los participantes reciben recompensas en forma de nuevas monedas o *tokens*, lo que les permite generar ingresos pasivos. Este método es común en blockchains que utilizan el mecanismo de consenso de prueba de participación (*proof-of-stake*, o PoS).

INVERSIONES EN FONDOS O ÍNDICES

Para aquellos que prefieren una inversión más diversificada, existen fondos e índices de criptomonedas que incluyen Bitcoin. Estos fondos permiten a los inversores obtener exposición al mercado de criptomonedas sin tener que gestionar directamente su compra y venta.

MAGIA

Lastimosamente, esta no es una forma de ganar dinero o satoshis. Tanto las maneras detalladas antes como otras deben estar respaldadas. Así como Bitcoin no ha podido ser hackeado, recordamos al lector que las plataformas, sistemas y modelos de negocio que prometen cosas increíbles basados en que utilizan Bitcoin pueden estar ligados a una estafa.

Blockchain es segura y transparente, pero siempre hay personas malintencionadas que crean modelos paralegales que la pueden incluir o incluso simular. Esto no quiere decir que tengan respaldo de la red o de algún organismo serio. Nuestro consejo es siempre mantenerse informado. Si algo o alguien promete cosas que suenan increíbles, como un porcentaje de ingresos fijos por mes o algo maravillosamente poético, dado que hemos analizado la volatilidad ascendente y la conducta de Bitcoin en toda su historia, podremos inferir que es, cuando menos, digno de sospecha.

LLEGAMOS HASTA AQUÍ.

Quiero agradecer y felicitar la valentía de recorrer estas páginas. El mundo cambia a una velocidad alarmante. Estoy seguro de que este material es perfectible, tanto que me niego a releerlo varias veces porque entonces nunca verá la luz. Espero que haya sido una herramienta para esclarecer un poco más este fascinante mundo y las oportunidades infinitas que la tecnología y las finanzas descentralizadas tienen para nosotros.

Por favor, no dudes en escribirme tus comentarios, correcciones, opiniones o lo que quieras; estaré más que agradecido. Y si este material te animó a realizar un cambio en algún aspecto de tu vida, también será una alegría que lo compartas conmigo.

¡Hasta pronto!

BIBLIOGRAFÍA

Mougayar, W. (2016). "The Business Blockchain: Promise, Practice, and the Application of the Next Internet Internet Internet".

Chaum, D. (1992). "Achieving Electronic Privacy." Scientific American, 267(3), 96-101.

Baur, D. G., & Lee, S. (2019). "Bitcoin: Medium of exchange or speculative assets?" Journal of International Financial Markets, Institutions and Money, 54, 1-19.

Zohar, A. (2015). "Bitcoin: Under the hood." Communications of the ACM, 58(9), 104-113. **Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.** https://bitcoin.org/bitcoin.pdf

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. Princeton University Press.

Franco, Pedro. "Understanding Bitcoin: Cryptography, Engineering and Economics." Wiley, 2014.

Popper, Nathaniel. "Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money." HarperCollins, 2015.

Szmigiera, M. (2021). "Bitcoin Trading: A Comprehensive Guide".

Decker, C., & Wattenhofer, R. (2013). "Information Propagation in Bitcoin".