Módulo 1. Un viaje por la historia del dinero e introducción a la tecnología blockchain

BARÇA INNOVATION HUB
Universitas

Te damos la bienvenida al primer módulo de nuestro curso sobre blockchain y criptomonedas. En este módulo, recorreremos la fascinante evolución del dinero, desde los primeros días del trueque hasta el surgimiento de la economía clásica. Es clave comprender cómo ha cambiado el dinero a lo largo del tiempo para entender el impacto revolucionario que las monedas digitales, como Bitcoin, están teniendo en la economía actual.

Para aprovechar al máximo este curso, te recomendamos que te registres en el intercambio de criptomonedas WhiteBIT y participes activamente en cada tema.

- Para registrarte, accede a la plataforma de intercambio WhiteBIT y crea tu cuenta. Ingresa tu correo electrónico, elige una contraseña segura, acepta los términos de uso y sigue los pasos para completar el registro.
- Verifica tu identidad (KYC) para poder operar en la plataforma de intercambio. Puedes seguir una guía paso a paso en el video (WhiteBIT, 2023a) o consultar el blog de WhiteBIT (WhiteBIT, 2023b).

Unidad 1

Unidad 1

Capítulo 1. La historia del dinero: del trueque a la economía clásica

Al comienzo de la civilización, las comunidades intercambiaban bienes y servicios a través de un sistema primitivo llamado trueque.

El **trueque** es un sistema en el cual los bienes y servicios se intercambian directamente sin usar un medio común de cambio, como el dinero. En una transacción de trueque, dos personas intercambian mercancías, donde cada una recibe lo que la otra desea. El valor de los bienes o servicios que se intercambian depende de las preferencias y necesidades de las personas involucradas. El trueque fue el método predominante de comercio en las primeras sociedades, antes de que existieran sistemas de moneda más formales.

Este tipo de intercambio fue común en diversas civilizaciones antiguas y sociedades primitivas durante miles de años. Se utilizó como la forma principal de intercambio hasta que se desarrollaron sistemas de

comercio más avanzados. El trueque predominó en las transacciones económicas desde la aparición de las primeras comunidades humanas, hasta que se desarrollaron sistemas de intercambio más sofisticados.

La transición del trueque comenzó cuando las sociedades enfrentaron el "problema de la doble coincidencia de necesidades". A medida que este problema se volvía más evidente, las comunidades buscaron soluciones, lo que llevó al surgimiento del protodinero y medios de intercambio más eficientes.

Figura 1. Trueque (M1-U1-1)

Fuente: Creada por el autor para este módulo.

Complejidades de las transacciones por trueque

Las transacciones por trueque presentaban complicaciones, ya que era necesario que ambas partes coincidieran exactamente en lo que querían. Si un agricultor quería cambiar trigo por herramientas, tenía que encontrar un herrero que no solo necesitara trigo, sino que también ofreciera las herramientas necesarias en cantidad y calidad. Esta situación tan poco práctica limitaba el alcance y la eficiencia del comercio, lo que frenaba el desarrollo económico de las primeras sociedades.

Limitaciones geográficas

El problema de la doble coincidencia de necesidades se agravaba debido a la distancia geográfica. En un mundo donde la comunicación y el transporte eran limitados, encontrar a alguien con necesidades que coincidieran perfectamente era aún más difícil. Esto restringía el comercio a nivel local e impedía interacciones económicas más amplias como las que hoy son comunes.

Surgimiento de alternativas al trueque

Al notar las limitaciones del trueque, las sociedades comenzaron a explorar medios alternativos para facilitar el intercambio. Esta búsqueda de métodos más eficientes marcó los primeros pasos hacia

la evolución del dinero, al tratar de superar los desafíos que planteaba el trueque con la doble coincidencia de necesidades.

Impacto en el crecimiento económico

El problema de la doble coincidencia no solo dificultaba el comercio, sino que también frenaba el crecimiento económico. Al no existir un medio de intercambio estandarizado, las transacciones eran complicadas, lo que impedía la especialización del trabajo, clave para el progreso económico.

Surgimiento del protodinero y el dilema de los bienes valiosos

A medida que las sociedades evolucionaban, también lo hacían sus métodos de comercio y acumulación de riqueza. Este capítulo aborda cómo surgió el protodinero y el complejo proceso de decisión que enfrentaban las personas al intentar predecir la demanda y obtener ventajas comerciales.

El nacimiento del protodinero

El desarrollo del protodinero representó un cambio crucial en la manera en que las personas percibían y usaban ciertos bienes valiosos. Esta evolución, impulsada por la rareza y el valor simbólico de ciertos objetos, también estuvo influenciada por los contextos culturales, sociales y económicos de las diversas comunidades.

El protodinero no se limitaba a un conjunto específico de objetos; por el contrario, las distintas culturas de todo el mundo emplearon una gran variedad de bienes con valor intrínseco. Algunos ejemplos notables son las conchas, los dientes de animales y el pedernal; otras sociedades utilizaron piedras preciosas, plumas raras o artefactos intrincadamente elaborados como protodinero, lo que muestra la diversidad cultural en la evolución de las primeras formas de moneda.

La transición de los bienes valiosos al protodinero estuvo profundamente entrelazada con las prácticas y creencias culturales, como una forma de sumar capas de complejidad. Estos objetos a menudo tenían un significado cultural que iba más allá de su utilidad o valor económico, convirtiéndose en símbolos de estatus, espiritualidad o identidad comunitaria.

De reservas de valor a medios de intercambio

Los objetos de protodinero no solo servían como reservas de valor, sino también como medios de intercambio dentro de las sociedades paleolíticas. Esto permitía a las personas realizar transacciones, promoviendo un método de comercio más eficiente y estandarizado. Esta transición sentó las bases para la eventual aparición de sistemas monetarios más sofisticados.

A medida que los bienes valiosos adquirían importancia, los primeros humanos se enfrentaron a un dilema crucial: ¿qué objetos desearían

otros para el intercambio? Predecir correctamente la demanda futura de ciertos bienes valiosos se convirtió en una ventaja estratégica; esto transformó a algunas sociedades e individuos en centros económicos capaces de proporcionar consistentemente objetos deseados para el intercambio.

Especialización y ventaja comercial

Como ejemplo de la naturaleza adaptable de las sociedades humanas, algunas tribus nativas americanas, como los Narragansett, se especializaron en crear bienes valiosos específicamente para su valor comercial. La capacidad de producir objetos con demanda anticipada les otorgaba una ventaja significativa en las interacciones económicas. Cuanto antes pudieran predecir la demanda de estos bienes, mayor era la ventaja económica que sus propietarios obtenían.

Competencia entre reservas de valor

A medida que las sociedades humanas se expandieron y se desarrollaron rutas comerciales, las reservas de valor dentro de las comunidades comenzaron a competir entre sí. Los comerciantes se encontraban en una encrucijada: decidir si almacenar sus ganancias comerciales en el medio de su propia sociedad, en el medio de la sociedad con la que comerciaban o en una combinación de ambas.

Beneficios de las reservas de valor extranjeras

Los comerciantes descubrieron las ventajas de mantener ahorros en fondos extranjeros, lo que facilitaba el comercio con otras comunidades y aceleraba la aceptación de estas reservas de valor en sus propias sociedades. La adopción de diversas reservas de valor incrementaba el poder adquisitivo de sus activos y esto fomentaba el crecimiento económico.

Aceptación global del oro

El culmen de estos desarrollos ocurrió en el siglo XIX, cuando la mayor parte del mundo adoptó un solo valor de reserva: el oro. Esto marcó el auge del mayor boom comercial de la historia. En los asentamientos que utilizaban el mismo valor de reserva, los costos de comerciar entre sí se redujeron significativamente y el potencial de comercio dio un gran salto.

A medida que avanzamos por el recorrido histórico del dinero, estas primeras adaptaciones y decisiones sentaron las bases para los conceptos de valor e intercambio, que evolucionaron hasta llegar a la era moderna, en la que las monedas digitales y la tecnología blockchain están transformando la manera en que entendemos y usamos el dinero.

Capítulo 2: La evolución de la economía clásica a las monedas digitales

La transición de la economía clásica a la era de las monedas digitales representa una evolución profunda en la forma en que las sociedades conceptualizan y se relacionan con los sistemas económicos. Este capítulo explora las raíces históricas de la economía clásica y los desafíos contemporáneos que han allanado el camino para el surgimiento de las monedas digitales.

La transición de un sistema económico basado en el oro a la economía clásica fue un proceso histórico y económico complejo. Aquí se presenta una visión simplificada de las fases clave.

Era del patrón oro

- El oro como moneda: en el siglo XIX y principios del siglo XX, muchos países adoptaron el patrón oro, en el cual el valor de su moneda estaba vinculado a una cantidad específica de oro.
- Estabilidad y comercio: el patrón oro se consideraba una fuerza estabilizadora para las economías, proporcionando un tipo de cambio fijo y fomentando el comercio internacional.

Desafíos y cambios económicos

- Después de la Primera Guerra Mundial: el impacto devastador de la Primera Guerra Mundial trajo consigo desafíos económicos y los países encontraron difícil mantener el patrón oro.

- Gran Depresión: la recesión global de los años treinta, conocida como la Gran Depresión, llevó a las naciones a reconsiderar sus políticas económicas.

Abandono del patrón oro

- Acuerdo de Bretton Woods (1944): el acuerdo de Bretton Woods estableció un nuevo sistema monetario internacional, en el cual las monedas estaban vinculadas al dólar estadounidense y este a su vez era convertible en oro.

- Shocks de Nixon (1971): en 1971, el presidente de EE.UU., Richard Nixon, suspendió la convertibilidad del dólar en oro, poniendo fin oficialmente al sistema de Bretton Woods y rompiendo el vínculo entre las principales monedas mundiales y el oro.

Surgimiento de la economía clásica

- Transición al dinero fíat: con el abandono del patrón oro, los países adoptaron monedas fíat, cuyo valor no está respaldado por bienes físicos, sino que depende de la confianza en los gobiernos emisores.

- Política monetaria: los bancos centrales ganaron mayor control sobre la política monetaria, utilizando herramientas como las tasas de interés para gestionar la inflación y la estabilidad económica.

Sistemas económicos modernos

- Globalización: la segunda mitad del siglo XX y el siglo XXI fueron testigos de un aumento de la globalización, avances tecnológicos y el surgimiento de las monedas digitales.

- Sistemas monetarios diversos: los distintos países adoptaron diferentes sistemas monetarios, como la flotación administrada, los tipos de cambio fijos y las monedas de flotación independiente.

La transición del patrón oro a la economía clásica fue un proceso dinámico moldeado por eventos históricos, desafíos económicos y

cambios en las políticas monetarias globales. Marcó un movimiento hacia sistemas económicos más flexibles y adaptables en respuesta a las necesidades cambiantes del mundo moderno.

Sin embargo, con el tiempo, la sociedad comenzó a reconocer las limitaciones de la economía clásica para abordar los escenarios económicos emergentes. La aparición de nuevos desafíos exigió una reevaluación de los modelos económicos tradicionales. En particular, las formas físicas de dinero, como las monedas y los billetes, comenzaron a revelar sus desventajas y limitaciones en la era digital.

La era digital trajo consigo tecnologías modernas y oportunidades asociadas con internet y los sistemas de pago electrónicos. Este cambio impulsó el desarrollo de la idea de las monedas digitales. Estas monedas, como Bitcoin y otras criptomonedas, han introducido posibilidades transformadoras en la manera en que interactuamos con el dinero y realizamos transacciones financieras.

El dinero fíat y el surgimiento de las monedas digitales

En el ámbito de la evolución monetaria, el término "dinero fíat" cobra protagonismo. La palabra "fíat" proviene del latín y se traduce como "que sea" o "hágase". En el contexto de las monedas, fíat se refiere al dinero cuyo valor proviene únicamente de la regulación y el decreto gubernamental. A diferencia de las monedas históricas, que estaban vinculadas a bienes físicos valiosos como el oro o la plata, el dinero

fíat carece de valor intrínseco y no puede intercambiarse por un bien subyacente específico.

En la era prefíat, los gobiernos acuñaban monedas de metales preciosos o emitían billetes que podían ser canjeados por una cantidad fija de dichos bienes. Sin embargo, la moneda fíat es distinta en el sentido de que es inconvertible; no está respaldada por un bien tangible. El valor del dinero fíat depende completamente de la confianza y la fe que el público deposita en el gobierno emisor, marcando una ruptura con los modelos monetarios tradicionales basados en activos físicos.

El dinero fíat, al no estar atado a reservas físicas como un acopio nacional de oro o plata, enfrenta el riesgo inherente de perder valor a través de la inflación y, en casos extremos, volverse completamente inútil durante una hiperinflación. Momentos históricos, como la hiperinflación en Hungría después de la Segunda Guerra Mundial, revelan el potencial devastador de que las tasas de inflación se dupliquen en un solo día.

Además, si la confianza pública en la moneda se debilita, el valor fiduciario de esa moneda podría colapsar rápidamente. Distinto es el caso de una moneda respaldada por oro, cuyo valor proviene de su demanda en sectores como la joyería, la decoración y la tecnología, como dispositivos electrónicos y vehículos aeroespaciales. El uso tangible del oro ofrece un factor de estabilidad que no poseen las

monedas fíat, las cuales dependen de la confianza pública y las condiciones económicas para mantener su valor.

Puntos clave sobre las monedas fíat

- El dinero fíat es una moneda emitida por el gobierno que no está respaldada por bienes como el oro.
- Este tipo de dinero permite a los bancos centrales tener más control sobre la economía, ya que pueden decidir cuánto dinero imprimir.
- Hoy en día, la mayoría de las monedas en papel, como el dólar estadounidense, son ejemplos de dinero fíat.
- Uno de los riesgos del dinero fíat es que los gobiernos pueden imprimir en exceso, lo que podría generar hiperinflación.

El paso de las finanzas tradicionales hacia las monedas digitales representa un cambio importante, lo que presenta conceptos y tecnologías novedosas y revolucionarias. Esta transición está marcada por desarrollos y tendencias clave.

Surgimiento de las monedas digitales

La llegada de criptomonedas como Bitcoin dio inicio a esta transformación en el mundo financiero. Estas criptomonedas, basadas en tecnología blockchain, permiten realizar transacciones seguras y transparentes sin intermediarios.

Tecnología blockchain

Blockchain, la tecnología detrás de muchas monedas digitales, cambió la manera en que se registran y verifican las transacciones financieras. Su estructura descentralizada y resistente a manipulaciones aumenta la seguridad y transparencia, reduciendo el riesgo de fraude.

Finanzas descentralizadas (DeFi)

Las plataformas DeFi introdujeron servicios financieros como préstamos, créditos y comercio sin depender de los bancos tradicionales. DeFi utiliza contratos inteligentes en blockchain para automatizar procesos financieros.

Monedas digitales de bancos centrales (CBDC)

Algunos gobiernos y bancos centrales están explorando las CBDC (por su sigla en inglés), monedas digitales emitidas como una versión digital de las monedas tradicionales. Las CBDC buscan combinar las

ventajas de las monedas digitales con la estabilidad de las monedas fíat nacionales.

Tokenización de activos

Muchos activos tradicionales como inmuebles, arte y valores están siendo tokenizados en plataformas blockchain. Esto convierte activos físicos en tokens digitales, haciéndolos más accesibles, divisibles y negociables.

Sistemas de pago digitales

Los sistemas de pago digitales, impulsados por innovaciones fintech, se han vuelto muy comunes y ofrecen alternativas eficientes a los métodos de pago tradicionales. Las billeteras móviles, los pagos sin contacto y las transferencias entre personas están ganando cada vez más popularidad.

Un ejemplo destacado es WhiteBIT, una plataforma de intercambio de criptomonedas que permite comprar entradas para partidos de fútbol con monedas digitales. Esto es posible gracias a Whitepay, una empresa SaaS que proporciona soluciones para pagos con criptomonedas. Esta innovación permite a los fans comprar entradas con criptomonedas antes de que comience la venta oficial, lo que demuestra la creciente integración de estas monedas en transacciones cotidianas.

Adopción institucional

Existen instituciones como bancos y firmas de inversión que están reconociendo el potencial de las monedas digitales. Algunas incluso ofrecen servicios relacionados con criptomonedas, dando a sus clientes acceso a esta nueva clase de activos.

Desarrollos regulatorios

Los gobiernos y los organismos reguladores están trabajando en marcos legales para regular el uso de las monedas digitales. Es crucial tener claridad en las normativas para fomentar una innovación responsable y mitigar los riesgos.

Conciencia pública y aceptación

El aumento en la conciencia y aceptación pública está impulsando la adopción de las monedas digitales. Cada vez son más las personas que se benefician de las transacciones rápidas, transfronterizas y a bajo costo que estas monedas ofrecen.

La transición de las finanzas tradicionales a las digitales es dinámica y continúa evolucionando rápidamente. Con el avance tecnológico, la integración de las monedas digitales está transformando cómo las personas y las instituciones interactúan con los sistemas financieros.

El origen y la importancia de Bitcoin

Bitcoin nació como un sistema de pago digital descentralizado y de código abierto, buscando resolver las debilidades de las estructuras centralizadas como los bancos. La dependencia de estas entidades para gestionar el dinero a menudo carece de transparencia y no permite un control efectivo sobre sus operaciones.

En contraste, Bitcoin es un sistema descentralizado que no está controlado ni regulado por bancos centrales. Los usuarios de la red la construyen y mantienen colectivamente, con balances públicos y las identidades ocultas. La blockchain, que es un registro público y distribuido, almacena todas las transacciones, y la liquidación se realiza en Bitcoin o Satoshis.

La principal fortaleza de Bitcoin es su autosuficiencia, confiabilidad y carácter descentralizado. Aunque se le conoce como una moneda digital, su valor real va más allá, actuando como la moneda nativa de la red. La seguridad y el funcionamiento de Bitcoin están garantizados por la criptografía.

La criptografía es la ciencia que protege la información, asegurando su confidencialidad, integridad y autenticidad. Codifica los mensajes de tal manera que solo el remitente y el destinatario puedan entenderlos. La criptografía tiene raíces en civilizaciones antiguas, pero dio un gran salto con las comunicaciones por radio en el siglo XX.

Durante la Segunda Guerra Mundial, la máquina Enigma marcó un punto clave en la historia de la criptografía, cuando Alan Turing logró descifrarla. Este logro sentó las bases para que la criptografía moderna se consolidara como una ciencia. Hoy en día, los criptógrafos emplean funciones matemáticas complejas para resistir varios tipos de ataques, utilizando la estadística y otras ramas de las matemáticas.

La criptografía ha evolucionado para abarcar no solo la transmisión secreta de información, sino también la verificación de la integridad de mensajes y firmas digitales, y como base de las criptomonedas. En el caso de Bitcoin, la criptografía garantiza la seguridad y la inmutabilidad de las transacciones, lo que la convierte en un pilar clave en la revolución de las criptomonedas.

El origen de Bitcoin es el resultado de décadas de investigación en criptografía e informática. Marc Andreessen, pionero del primer navegador gráfico de internet, ve a Bitcoin como el producto de veinte años de investigación en criptomonedas y cuarenta años de avances en criptografía.

El recorrido de Bitcoin incluye hitos importantes.

- **Primeros protocolos de dinero electrónico (1983)**. En 1983, los criptógrafos David Chaum y Stefan Brands crearon los primeros protocolos de dinero electrónico

en un intento de imaginar una moneda digital. Chaum proponía un sistema que garantizara la privacidad en las transacciones, un principio fundamental en las criptomonedas actuales.

- **Hashcash y la prueba de trabajo (1997)**. En 1997, Adam Back introdujo Hashcash, un sistema diseñado para prevenir el spam y los ataques DoS. Hashcash introdujo el concepto de prueba de trabajo, un mecanismo que requiere esfuerzo computacional para prevenir abusos. Este concepto luego se convertiría en una pieza central del algoritmo de consenso de Bitcoin para proteger la seguridad e integridad de la red.

- **B-money y bit-gold (1998)**. En 1998, Wei Dai propuso "b-money", un sistema de dinero electrónico anónimo y descentralizado. Al mismo tiempo, Nick Szabo desarrolló "bit-gold", una propuesta de moneda digital descentralizada y escasa. Estas ideas sentaron las bases teóricas para las criptomonedas, abordando temas como el consenso, la privacidad y la escasez.

- **El movimiento cypherpunk**. Durante estos años surge el movimiento cypherpunk, compuesto por criptógrafos y defensores de la privacidad, fue clave en la formación de los ideales detrás de las criptomonedas. Este grupo promovía la privacidad y

el uso de herramientas criptográficas para resistir el control centralizado.

- **El navegador Mosaic y el auge de las puntocom**. En los 90, el navegador Mosaic desarrollado por Marc Andreessen fue fundamental para la expansión de internet. Este avance tecnológico fue clave para el crecimiento de las puntocom, lo que a su vez impulsó la adopción de innovaciones digitales.

- **El génesis de Bitcoin (2009)**. La convergencia de estas ideas y avances tecnológicos culminó en el lanzamiento de Bitcoin en 2009 por una persona o grupo que usó el seudónimo Satoshi Nakamoto. Bitcoin combinó principios criptográficos, consenso descentralizado a través de la prueba de trabajo y la visión de una moneda sin fronteras y resistente a la censura. Su naturaleza descentralizada y el uso de una blockchain para un historial de transacciones transparente e inmutable lo distinguen de las formas tradicionales de dinero. El 3 de enero de 2009, se creó el primer bloque y se generaron cincuenta Bitcoins, lo que marcó el génesis de Bitcoin. Solo nueve días después, el 12 de enero, Satoshi Nakamoto envió diez Bitcoins a Hal Finney; fue la primera transferencia de Bitcoin registrada. El intercambio pionero de Bitcoins por moneda nacional ocurrió en septiembre de 2009, cuando Martti Malmi envió 5050 Bitcoins a un usuario llamado NewLibertyStandard, quien recibió

> $5.02 en su cuenta de PayPal. Cabe destacar que NewLibertyStandard propuso utilizar el costo de la electricidad para la generación de Bitcoin como métrica de valoración; se dotó así de una perspectiva única a la economía de las criptomonedas. Estos eventos iniciales sentaron las bases para la evolución disruptiva de las monedas digitales.

En abril de 2011, Satoshi Nakamoto desapareció, pero antes dejó un mensaje final en el foro principal de Bitcoin, Bitcointalk.org. Desde esta desaparición, la búsqueda por desvelar la identidad del creador ha persistido. Cada año surgen nuevas versiones y teorías, pero la comunidad no está tan cerca de desentrañar el misterio detrás del seudónimo.

Muchos rumores sugieren que el criptógrafo y programador Hal Finney podría ser el escurridizo creador. Notablemente, Finney fue el destinatario de la primera transacción de Bitcoin de Satoshi Nakamoto, lo que suma intriga a la especulación sobre su posible papel en la creación de Bitcoin. Sin embargo, a pesar de la especulación continua, la identidad detrás del seudónimo sigue eludiendo a la comunidad, con un aire de misterio alrededor de la figura enigmática que dio vida a la revolucionaria criptomoneda.

Monedas digitales vs. medios financieros tradicionales

Las monedas digitales representan dinero electrónico que opera exclusivamente dentro del ámbito digital, sin contrapartes físicas como billetes o monedas. Existen únicamente en forma electrónica y aprovechan la tecnología blockchain, un sistema descentralizado de registro de transacciones. El uso de blockchain asegura tanto la seguridad como la transparencia de las transacciones y, a su vez, afirma su autenticidad sin depender de una entidad central, ya sea un banco o un gobierno.

En la competencia entre diversos métodos de ahorro, se destacan las propiedades distintivas y valiosas, lo que permite un aumento en la demanda a lo largo del tiempo. A lo largo de la historia, diversos elementos han funcionado como formas de ahorro o "protodinero", pero algunos atributos se han destacado como especialmente deseables, lo que da a ciertos objetos una ventaja sobre los demás.

Tabla 1. Oro vs. Monedas fíat vs. Bitcoin

Características	Oro	Monedas fíat	Bitcoin
Durabilidad	El oro se posiciona como el líder indiscutido en durabilidad. La	En el mundo de las monedas fíat, la historia revela que muchos gobiernos han	Los Bitcoins, al no tener un emisor central, tienen una durabilidad que depende del

	mayoría del oro extraído o acuñado, incluidos los tesoros de civilizaciones antiguas como los faraones, no solo ha perdurado a lo largo de los siglos, sino que se espera que siga existiendo durante mucho más tiempo. Las monedas de oro, que alguna vez fueron usadas como moneda en tiempos antiguos, mantienen un valor considerable en la actualidad, lo que resalta la naturaleza	surgido y caído a lo largo de los siglos, y sus respectivas monedas han desaparecido junto con ellos. Hay ejemplos como los sellos de papel y de alquiler, o los Reichsmarks de la República de Weimar, que han perdido su valor porque las instituciones emisoras ya no existen. A partir de estos hechos históricos, sería imprudente ver las monedas fíat como activos intrínsecamente duraderos, con el dólar estadounidense y la libra esterlina	funcionamiento de la red de soporte. Aunque Bitcoin aún se encuentra en sus primeras etapas, hacer afirmaciones definitivas sobre su durabilidad es prematuro, aunque hay indicios prometedores. A pesar de los intentos de regulación gubernamental y de numerosos ataques de hackers, la red sigue funcionando, lo que destaca su notable nivel de "antifragilidad".

	perdurable de este metal precioso.	como casos relativamente excepcionales en este contexto.	
Movilidad	El oro, al ser una sustancia densa y tangible, es uno de los activos menos móviles. No sorprende que la mayor parte de este metal precioso permanezca en un solo lugar, ya que la propiedad cambia de manos con frecuencia sin necesidad de mover el metal físico. La transferencia de oro físico a largas	Las monedas fíat, en su mayoría digitales en la actualidad, tienen cierto grado de movilidad. Sin embargo, esta movilidad se ve limitada por regulaciones gubernamentales y controles de capital, lo que a menudo implica largos tiempos de procesamiento para transferencias grandes o, en algunos casos, las hace imposibles. Aunque el efectivo físico	Los Bitcoins destacan como el medio de almacenamiento de valor más portátil que se haya utilizado. Las claves privadas, que representan cantidades significativas de dinero, pueden guardarse de manera segura en una pequeña unidad USB para un fácil transporte. Además, se pueden transferir grandes sumas instantáneamente entre personas ubicadas en extremos opuestos del planeta.

	distancias implica costos elevados, riesgos considerables y una gran inversión de tiempo.	puede usarse para eludir ciertos controles, este enfoque conlleva altos riesgos asociados al almacenamiento y a los crecientes costos de transporte.	Mientras que las monedas fíat, predominantemente digitales ahora, comparten cierta movilidad, la facilidad incomparable para transportar y transferir un valor significativo distingue a los Bitcoins en términos de portabilidad.
Fungibilidad	El oro ha establecido el estándar de fungibilidad. Una onza de oro fundido es idéntica a cualquier otra y esta uniformidad ha sido durante mucho tiempo la base de su comercio en el	Aunque los billetes fíat son generalmente considerados de igual valor por los comerciantes, ha habido casos en los que los billetes de grandes y pequeñas denominaciones han sido tratados de manera	Los Bitcoins son fungibles a nivel de red. Esto significa que cada moneda transferida es tratada de manera equitativa a lo largo de toda la red. Sin embargo, dado que todo el recorrido de los Bitcoins puede ser rastreado en la blockchain, una sola moneda puede ser

	mercado. En contraste, la fungibilidad de las monedas fíat depende del grado permitido por las instituciones emisoras.	desigual. Por ejemplo, el gobierno indio, con el objetivo de eliminar el mercado negro, llevó a cabo una desmonetización total de los billetes de 500 y 1000 rupias. Como resultado, esos billetes han sido negociados por debajo de su valor nominal.	"denigrada" debido a su uso en actividades ilegales, lo que puede hacer que comerciantes o intercambios se nieguen a aceptarla. Sin mejoras en la privacidad y el anonimato del protocolo de red, Bitcoin no puede ser considerado tan fungible como el oro.
Corroborabilidad	En la mayoría de los casos, es sencillo verificar la autenticidad del oro. Sin embargo, el oro no es inmune a la falsificación. En el pasado, ha habido	Por su parte, la moneda fíat cuenta con características antifalsificación en los billetes, lo que facilita su verificación, aunque siempre existe el riesgo de que aparezcan billetes	En contraste, los Bitcoins pueden ser verificados con certeza matemática. A través de firmas criptográficas, el propietario de Bitcoins puede demostrar públicamente que posee las monedas reclamadas.

	criminales astutos que han utilizado tungsteno bañado en oro para engañar a los consumidores.	falsificados, lo cual representa una amenaza para los estados y sus ciudadanos.	
Patribilidad	Aunque el oro puede ser separado físicamente, lo que teóricamente permite su división, esta característica lo vuelve menos conveniente y práctico para el uso diario.	Las monedas fíat pueden dividirse hasta convertirse en monedas de bolsillo, lo que ofrece flexibilidad en la práctica. Sin embargo, el poder adquisitivo de las denominaciones pequeñas suele ser limitado.	Un Bitcoin puede dividirse en cien millones de partes, permitiendo transferencias en cantidades muy pequeñas. No obstante, es importante tener en cuenta que las tarifas de red pueden hacer que la transferencia de cantidades menores a través de Bitcoin sea extremadamente ineficiente.

Oferta	Si bien el oro ha mantenido su escasez durante muchos siglos, no está a salvo de un aumento en su oferta. El descubrimiento de nuevos métodos rentables para extraer o adquirir oro, como la minería en el lecho marino o la minería de asteroides, podría resultar en un incremento significativo en la disponibilidad de este metal valioso.	Las monedas fíat, a pesar de ser una invención relativamente reciente, han mostrado una tendencia hacia un suministro en constante expansión. Los estados han demostrado una inclinación consistente a aumentar la oferta monetaria para enfrentar desafíos políticos inmediatos. Las tendencias inflacionarias que implementan los gobiernos a nivel mundial han generado una sensación de desconfianza entre los	Lo que distingue a Bitcoin de las monedas fíat y del oro es su suministro extremadamente limitado. Según el concepto original, el número total de monedas que pueden ser creadas está limitado a veintiún millones. Esta característica única permite a los tenedores de Bitcoin conocer de antemano su porcentaje del suministro total de monedas en el mercado. Por ejemplo, una persona que posee diez Bitcoins podría saber que no más de 2,1 millones de personas en el mundo (menos del

		tenedores de monedas fíat, quienes permanecen atentos a posibles caídas en el valor de sus activos.	0,03% de la población global) podrían tener un número equivalente de monedas.
Resistencia a la censura	Aunque no es emitido por gobiernos, la naturaleza física del oro dificulta su movimiento, lo que lo hace más susceptible a la regulación gubernamental en comparación con Bitcoin. Un ejemplo de esto es la ley de control del oro en India.	En un sistema económico regulado, los gobiernos supervisan los bancos y las instituciones financieras para prevenir usos ilícitos de productos monetarios, ejemplificados por los controles de capital. Este marco regulatorio puede dificultar que los individuos, como	Bitcoin ganó una demanda temprana, en parte, debido a su uso en el comercio ilegal de drogas y eso generó una concepción errónea de que su principal atractivo era el anonimato. Sin embargo, las transacciones de Bitcoin se registran de forma permanente en la blockchain pública, lo que permite el análisis forense para rastrear el flujo de fondos. La

		un millonario, transfieran su riqueza a otro país para escapar de un régimen opresivo.	popularidad de la moneda en actividades ilícitas no se debe a un anonimato absoluto, sino a su resistencia a la censura. En la red de Bitcoin, las transacciones ocurren sin intervención humana, con un diseño distribuido de pares que es inherentemente resistente a la censura.

Fuente: Elaboración propia.

Ninguna moneda tiene una historia tan extensa y duradera como el oro, que ha sido reverenciado a lo largo de los anales de la civilización humana. Las monedas acuñadas en la antigüedad continúan reteniendo un valor significativo en la era contemporánea.

Esto contrasta marcadamente con las monedas fíat, una anomalía reciente en la historia. Desde su introducción, han mostrado una

propensión a la depreciación. El uso de la inflación como una forma encubierta de tributación ha demostrado ser una tentación que pocos estados en la historia han resistido.

Las lecciones del siglo XX, durante el cual las monedas fíat comenzaron a dominar el sistema monetario global, subrayan la falta de fiabilidad de las monedas fíat a largo o incluso a medio plazo.

Por otro lado, Bitcoin, a pesar de su breve existencia, ha resistido ensayos sustanciales en el mercado. Esta resiliencia sugiere una alta probabilidad de que Bitcoin persista como almacenamiento de valor en el futuro cercano.

Capítulo 3: Alcanzando el consenso. El problema de los generales bizantinos en el núcleo de las soluciones blockchain.

El problema de los dos generales

Este es un experimento mental y un concepto en informática que ilustra los desafíos de alcanzar consenso y coordinarse entre dos entidades distribuidas en un contexto de incertidumbre y comunicación poco confiable.

En esta situación, hay dos generales, cada uno al mando de su ejército, que planean lanzar un ataque coordinado contra un enemigo común que se encuentra en una ciudad. Para que tengan éxito, los

generales deben sincronizar sus acciones y acordar un momento específico para atacar. Sin embargo, el desafío surge debido a la incertidumbre en la comunicación: los generales solo pueden comunicarse a través de mensajeros y existe el riesgo de que estos se pierdan, se retrasen o sean interceptados por el enemigo.

El problema se plantea de la siguiente manera:

- Los dos generales, A y B, se encuentran en lados opuestos de la ciudad enemiga con sus ejércitos.
- Necesitan decidir un momento común para atacar y que el asalto sea efectivo.
- La comunicación solo puede llevarse a cabo a través de mensajeros y estos pueden ser capturados o retrasados por el enemigo.

El problema fundamental es que no hay una forma segura de que los generales aseguren que ambos estén de acuerdo en el momento del ataque. Aunque un general envíe un mensaje al otro proponiendo un momento específico, no hay certeza de que el mensaje sea recibido, lo que puede resultar en que un general ataque mientras el otro se contenga, lo que llevaría al fracaso.

En el campo de la informática, el problema de los dos generales se utiliza frecuentemente como analogía para los desafíos en el diseño de sistemas distribuidos, especialmente en situaciones donde lograr consenso y comunicación confiable entre distintos componentes o nodos es crucial. Resalta las dificultades de garantizar un acuerdo entre entidades distribuidas cuando enfrentan incertidumbres en la comunicación y el riesgo de fallas.

El problema de los generales bizantinos

En 1982, Lamport, Szostak y Pease introdujeron un problema que involucra a múltiples generales, algunos de los cuales podrían ser traidores. Esta situación amplía el clásico problema de los dos generales y requiere que un número mayor de generales acuerden el momento del ataque. Un factor que complica esto es la posibilidad de que haya traidores entre los generales, capaces de dar información falsa sobre sus intenciones.

El paradigma de líder-seguidor del problema de los dos generales se transforma en una dinámica de comandante-subordinado. Para lograr consenso en este contexto, el comandante y cada subordinado deben alinearse en la misma decisión, ya sea atacar o retirarse.

Esta situación es conocida como el problema de los generales bizantinos. El general al mando debe emitir una orden a sus n-1 subordinados siguiendo los siguientes criterios:

- Todos los generales subordinados leales deben obedecer la misma orden.
- Si el general al mando es leal, todos los subordinados que le sean leales seguirán sus órdenes.

Es importante destacar que, incluso si el general al mando es un traidor, aún debe alcanzarse el consenso. Por lo tanto, todos los tenientes deben llegar a una mayoría de votos.

El algoritmo de consenso en este caso se basa en el concepto de la mayoría de decisiones percibidas por los subordinados.

Esto implica que el algoritmo puede alcanzar consenso siempre y cuando dos tercios de los participantes sean honestos. Si más de un tercio de los generales son traidores, el consenso se vuelve inalcanzable, lo que impide la coordinación de ataques entre ejércitos y resulta en la victoria del enemigo.

En resumen, mientras que el problema de los dos generales se centra en los desafíos de alcanzar consenso entre dos entidades con comunicación poco confiable, el problema de los generales bizantinos extiende el escenario para incluir a múltiples generales e introduce la complicación de posibles traidores entre ellos.

¿Cómo se relaciona esto con las blockchain? Las blockchain, al ser libros contables descentralizados, inherentemente carecen de una autoridad central, lo que las hace vulnerables a ataques impulsados por incentivos económicos para explotar debilidades. El valor almacenado en las blockchain las vuelve un objetivo atractivo para los atacantes que buscan manipular o interrumpir el sistema. Sin embargo, para garantizar la integridad y confiabilidad de una blockchain, es fundamental abordar el problema de los generales bizantinos mediante la tolerancia a fallos bizantinos.

Sin la tolerancia a fallos bizantinos, los pares maliciosos dentro de una red blockchain pueden propagar y validar transacciones falsas; esto socava la confianza en todo el libro contable. Además, la ausencia de una autoridad central que asuma la responsabilidad y corrija el daño resultante complica aún más el desafío.

La innovación revolucionaria que trajo la creación de Bitcoin radica en su ingeniosa solución al problema de los generales bizantinos, principalmente mediante la implementación de un mecanismo de consenso probabilístico de prueba de trabajo. Este enfoque, meticulosamente detallado por Satoshi Nakamoto (2008a) en un correo electrónico fundamental, marcó un momento clave en el desarrollo de sistemas descentralizados.

Al integrar la tolerancia a fallos bizantinos, las blockchain mejoran su resistencia frente a actores maliciosos que intentan comprometer el

sistema. El mecanismo de prueba de trabajo, como se ilustra en Bitcoin, ofrece una solución probabilística que aborda el problema de los generales bizantinos y establece un consenso descentralizado que resiste intentos de manipulación o desinformación. Esta solución innovadora sentó las bases para el funcionamiento seguro y confiable de las redes blockchain; demostró la aplicación práctica de la tolerancia a fallos bizantinos en el ámbito de la tecnología de libros contables distribuidos.

Los mecanismos de consenso forman la columna vertebral de las redes blockchain, ya aseguran que los participantes estén de acuerdo sobre la validez de las transacciones y el estado del libro mayor distribuido. Profundizaremos más en este tema en las siguientes unidades, pero queríamos mencionar los mecanismos de consenso más prominentes y originales que sirven como base para la evolución de la tecnología.

Capítulo 4: Emisión y valor de las criptomonedas

La emisión de moneda implica la creación y la introducción de nuevas unidades de una moneda en circulación. Este proceso es normalmente realizado por el banco central u otras entidades autorizadas, y puede darse mediante la impresión de billetes o el establecimiento de registros contables electrónicos.

El valor de una moneda está estrechamente relacionado con la interacción entre la oferta y la demanda en el mercado. Son diversos

los factores que influyen en el valor de una moneda, como las condiciones económicas de un país, las tasas de inflación, las tasas de interés, la estabilidad política y las relaciones internacionales. Cuando la demanda de una moneda excede su oferta, su precio tiende a aumentar. En cambio, si la oferta supera la demanda, el precio puede disminuir.

La dinámica del valor de una moneda se ve afectada por el delicado equilibrio entre oferta y demanda, así como por múltiples factores económicos y geopolíticos que influyen en la percepción del valor de una moneda en el mercado global.

¿Cómo se determina el valor de las monedas digitales? Para evaluar los riesgos asociados con las monedas digitales, es fundamental examinar los factores que influyen en su valor. El precio de cualquier activo, incluidas las monedas digitales como Bitcoin, se basa principalmente en la interacción entre la oferta y la demanda: un activo se valora según lo que las personas están dispuestas a pagar por él. Sin embargo, la complejidad radica en comprender los diversos factores que afectan esta demanda.

La demanda de monedas digitales está relacionada con diferentes variables, como la confianza de los inversores, el crecimiento de la infraestructura de apoyo, la expansión de la base de participantes y el volumen total del mercado. Por lo tanto, las dinámicas de oferta y demanda están sujetas a una gran cantidad de factores.

Un principio clave que sostiene el valor de cualquier activo es que no caerá a cero si al menos dos partes están interesadas en él. En el caso de Bitcoin, el interés y la participación global de millones de personas y miles de empresas hacen que la pérdida repentina de interés sea muy poco probable.

Además, la posible depreciación de un activo suele ocurrir cuando está frente a su destrucción o eliminación. Por ejemplo, si se borra la base de datos que contiene todas las transacciones del banco central, el valor de la moneda no física se reduciría a cero. Sin embargo, las criptomonedas descentralizadas, como Bitcoin, plantean un desafío diferente a esta situación. Si al menos una copia de la blockchain existe en algún nodo del mundo, Bitcoin sigue existiendo, aunque con menor liquidez.

Teniendo en cuenta estos principios básicos, discutir la depreciación teórica de Bitcoin en el contexto actual parece inútil. La fortaleza de Bitcoin proviene de su amplia adopción y de la naturaleza descentralizada de su blockchain.

Sin embargo, no hay falta de valor en analizar escenarios hipotéticos. Un colapso teórico de Bitcoin tendría repercusiones que irían más allá de su impacto inmediato en las monedas digitales. Como líder de tendencias y proveedor principal de liquidez en el comercio de intercambio, la caída de Bitcoin podría tener efectos en cadena y afectar potencialmente al 99% de otras criptomonedas. Esta caída se

extendería a la industria en general de criptomonedas; esto interrumpiría la minería, la participación, el préstamo e incluso afectaría a los emisores de stablecoins (criptomonedas estables). La depreciación hipotética de Bitcoin podría significar el colapso de un sector completo dentro de la economía emergente global.

¿Qué es el *halving* y cuándo se minarán todos los Bitcoins?

Figura 2. Bitcoin (M1-U1-2)

Fuente: Creada por el autor para este curso.

Bitcoin

El halving de Bitcoin es un evento programado en el protocolo de Bitcoin que ocurre cada cuatro años, o después de minar 210.000 bloques. Durante el halving, la recompensa que reciben los mineros

por añadir un nuevo bloque a la blockchain se reduce a la mitad. Esta reducción en la tasa de creación de nuevos Bitcoins actúa como un mecanismo para controlar la oferta total de Bitcoin.

El halving de Bitcoin impacta significativamente la economía de la minería de Bitcoin. En los inicios de Bitcoin, la recompensa por bloque era de cincuenta Bitcoins. El primer halving en 2012 la redujo a veinticinco Bitcoins, el segundo halving en 2016 la disminuyó a 12.5 Bitcoins y el tercer halving en 2020 la bajó a 6.25 Bitcoins.

El próximo halving de Bitcoin ocurrirá cuando el número de bloques alcance 840.000. Se espera que esto suceda en abril de 2024.

Esta disminución en la recompensa por bloque tiene implicaciones para la oferta total de Bitcoin. La oferta máxima de Bitcoin está limitada a 21 millones y los eventos de halving son cruciales para acercarse y eventualmente alcanzar este límite.

La comunidad sigue de cerca los eventos de halving de Bitcoin, ya que suelen tener un impacto considerable en la dinámica del mercado y afectan factores como la rentabilidad de los mineros, las dinámicas de oferta y demanda, y el sentimiento general del mercado.

¿Qué sucederá cuando se mine el último Bitcoin? Cuando se mine el último Bitcoin, se completará la oferta predeterminada y limitada de Bitcoin. La oferta máxima de Bitcoin está fijada en veintiún millones

de monedas, una decisión de diseño incluida en el protocolo de Bitcoin por su creador seudónimo, Satoshi Nakamoto. Se anticipa que el último Bitcoin se mine en el año 2140.

Figura 3. Minería de Bitcoin (M1-U1-3)

Fuente: [imagen sin título de minería de Bitcoin], (s.f.), https://bit.ly/49443SW.

Se esperan varias consecuencias y cambios en el ecosistema de Bitcoin cuando se produzca este evento.

- Recompensas por minería: en la actualidad, los mineros son recompensados con nuevos Bitcoins por agregar exitosamente un bloque a la blockchain. A medida que la oferta se acerque a su límite, la recompensa por bloque disminuirá y los mineros

dependerán cada vez más de las tarifas de transacción para sus ingresos.

- Dinámicas económicas: la transición de depender de las recompensas por bloque a las tarifas de transacción podría modificar los incentivos económicos para los mineros. Esto podría dar lugar a cambios en la estructura de costos de las transacciones de Bitcoin y en las dinámicas de los mercados de tarifas de transacción.

- Escasez y demanda: con una oferta fija y sin posibilidad de minería adicional, la escasez de Bitcoin se vuelve absoluta. Esta característica podría reforzar su percepción como un refugio de valor, similar a los metales preciosos como el oro, donde el principio de escasez impulsa la demanda.

- Impacto en el mercado: la culminación de la minería y la oferta fija podrían tener implicaciones para el mercado de criptomonedas en general. Los inversores, los comerciantes y las partes interesadas en el ámbito de las criptomonedas probablemente estén atentos a este hito por sus posibles efectos en la dinámica del mercado y el sentimiento.

Es importante señalar que estas predicciones son especulativas y el impacto real dependerá de diversos factores, como el estado del ecosistema financiero general, los avances tecnológicos, las consideraciones regulatorias y la evolución continua del espacio de criptomonedas.

Resumiendo

En conclusión, nuestro recorrido por la historia del dinero, desde los inicios del trueque hasta el establecimiento de principios económicos clásicos, ha establecido las bases para entender la evolución dinámica hacia las monedas digitales. En el segundo capítulo, revivimos la transición de la economía clásica a la era de las monedas digitales, explorando la naturaleza autorreguladora de las economías clásicas, el surgimiento del dinero fiduciario y la trascendental importancia de Bitcoin en la transformación de los paisajes financieros. Luego, el tercer capítulo se centró en el desafío fundamental de lograr consenso en sistemas descentralizados, desentrañando las complejidades del problema de los generales bizantinos y su relevancia directa para el concepto revolucionario de la tecnología blockchain. Finalmente, nuestro viaje concluyó con un enfoque en la emisión y el valor de las criptomonedas, con preguntas clave sobre la formación de los valores de las monedas digitales, las complejidades de los eventos de halving y las implicaciones futuras cuando se mine el último Bitcoin. Esta unidad educativa nos ha proporcionado una comprensión integral de los aspectos históricos, tecnológicos y

económicos que configuran el mundo del dinero, tanto tradicional como digital.

CONTINUAR

Unidad 2

Unidad 2

Capítulo 1: Introducción a los fundamentos de blockchain

En 2008, el panorama financiero global sufrió un cambio radical cuando Lehman Brothers Holdings Inc. se declaró en quiebra. Este acontecimiento, sumado a la creciente desconfianza del público en las instituciones bancarias tradicionales, abrió la puerta a la aparición de una nueva categoría de activos que operan de manera independiente a las estructuras bancarias convencionales. Fue en este contexto de agitación financiera que se presentó la primera criptomoneda, Bitcoin.

Bitcoin, lanzado en 2008 por una figura o grupo enigmático que usa el seudónimo Satoshi Nakamoto, representó una ruptura revolucionaria con las monedas tradicionales. El objetivo principal era crear una moneda digital descentralizada y de código abierto que funcionara sin la necesidad de un banco central o autoridad administrativa. El documento original que describe el concepto y los mecanismos de Bitcoin se encuentra disponible aquí (Nakamoto, 2008b).

En esta sección del módulo 1, exploraremos los principios fundamentales que rigen las criptomonedas para desglosar lo básico de la tecnología blockchain.

Bitcoin ≠ blockchain

Blockchain es un libro de contabilidad digital único y descentralizado que actúa como una base de datos especial distribuida en múltiples computadoras a nivel mundial. Esta tecnología innovadora garantiza el almacenamiento seguro de datos a través de una serie de bloques cronológicos, cada uno protegido por mecanismos criptográficos sólidos.

El concepto de blockchain tiene sus raíces en la década de 1990, fruto de la colaboración entre el científico informático Stuart Haber y el físico W. Scott Stornetta. Su visión consistía en aplicar la criptografía al blockchain para proteger los documentos digitales contra manipulaciones: esto marcó un momento clave en la evolución de la gestión segura de datos.

La influencia de Haber y Stornetta resonó en las comunidades de programación y criptografía, lo que inspiró el desarrollo de Bitcoin. Como la primera criptomoneda que utiliza la tecnología blockchain, Bitcoin se presentó como una moneda digital descentralizada y sin confianza, desafiando los paradigmas financieros tradicionales.

Desde esos primeros días, la blockchain ha ido más allá de su aplicación inicial en transacciones de criptomonedas. Su versatilidad abarca el registro de varios tipos de datos digitales y la realización de diversas tareas, lo que los convierte en un actor poderoso en el ámbito tecnológico. La adopción generalizada de la tecnología blockchain es evidente en el creciente número de usuarios de criptomonedas en todo el mundo.

Más allá de su conexión con las criptomonedas, la naturaleza descentralizada de la blockchain y su seguridad criptográfica lo hacen apto para diversas aplicaciones. Ya sea para registrar transacciones financieras, asegurar la integridad de documentos digitales o facilitar tareas complejas, la blockchain continúa evolucionando como una fuerza transformadora que promete innovación y seguridad en múltiples industrias.

Aunque a menudo se utilizan de manera intercambiable, Bitcoin y blockchain son conceptos distintos, y es fundamental entender sus diferencias. Bitcoin no es solo una moneda; es un protocolo completo construido sobre la tecnología blockchain. Un protocolo define las reglas que rigen la comunicación entre los participantes de la red. En el caso de Bitcoin, estas reglas regulan diversos aspectos, como la gestión de claves privadas y públicas, el proceso de minería para confirmar transacciones y más. Es importante destacar que otras criptomonedas como Ethereum, Waves, NEO, Ripple y varias más comparten un protocolo similar al de Bitcoin.

¿Qué es la descentralización en blockchain? La descentralización en el marco de la blockchain se refiere a la distribución del control y la toma de decisiones entre los usuarios de la red, en lugar de estar concentrada en una sola entidad, como un gobierno o una corporación. Este enfoque descentralizado resulta beneficioso en situaciones donde los usuarios desean coordinar con personas desconocidas o priorizan la seguridad y la integridad de sus datos.

En una red de blockchain descentralizada, no existe una autoridad central o intermediario que dicte el flujo de datos o transacciones. En su lugar, la verificación y el registro de las transacciones se confían a una red de computadoras ampliamente dispersas. Este esfuerzo colaborativo asegura la integridad general de la red.

Es fundamental reconocer que la blockchain va más allá de ser una simple base de datos. Además de su función básica, permite una variedad de servicios, incluidas criptomonedas y tokens no fungibles (NFT). Esta versatilidad permite a los usuarios participar en transacciones colaborativas sin depender de una autoridad centralizada. La naturaleza descentralizada de la blockchain no solo garantiza la seguridad, sino que también fomenta un entorno en el que los usuarios pueden interactuar y realizar transacciones de manera fluida. Se establece así un paradigma sin confianza y de igual a igual.

Capítulo 2: ¿Cómo funciona la blockchain?

Una blockchain actúa como un libro de contabilidad digital seguro que registra las transacciones entre partes y protege esta información contra accesos no autorizados. El proceso implica una red distribuida de computadoras especializadas, conocidas como nodos, ubicadas en todo el mundo.

Cuando un usuario inicia una transacción, como una transferencia de una cantidad específica de criptomonedas, los detalles se difunden por la red. Cada nodo desempeña un papel crucial en el proceso de verificación, analizando las firmas digitales y otros datos de la transacción para autenticar su validez.

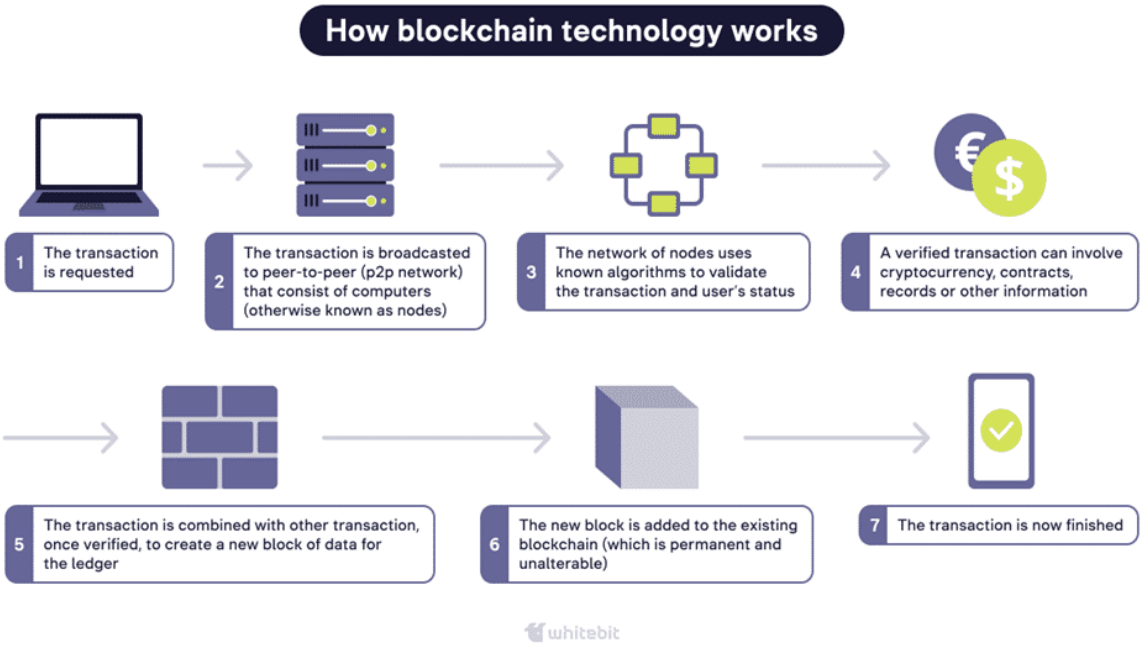
Una vez que se aprueba una transacción, se convierte en parte de un bloque, que se une a otras transacciones autorizadas. Estos bloques se enlazan secuencialmente mediante técnicas criptográficas, formando la estructura inmutable conocida como blockchain. La validación e inclusión de transacciones en la blockchain dependen de un mecanismo de consenso, que es un conjunto de reglas que guían a los nodos para coordinarse y llegar a un acuerdo sobre el estado de la blockchain y la aprobación de las transacciones.

La criptografía juega un papel fundamental en garantizar la seguridad, transparencia y resistencia a manipulaciones de los registros de transacciones dentro de la blockchain. Una técnica criptográfica básica utilizada es el hashing, un proceso que

transforma datos de entrada de diferentes tamaños en una cadena de caracteres de longitud fija.

Las funciones hash de la blockchain priorizan la resistencia a colisiones, lo que disminuye la posibilidad de que dos conjuntos de datos diferentes generen el mismo resultado. Además, cualquier modificación en los datos de entrada provoca un cambio total en el resultado del hashing, lo cual mejora la integridad y seguridad del historial de transacciones de la blockchain.

Figura 4. Funcionamiento de la tecnología blockchain (M1-U2-4)



Fuente: Creada por el autor para este módulo.

"¿Cómo funciona la tecnología blockchain?"

1. *Se solicita la transacción.*
2. *La transacción se transmite a una red de pares (p2p) que consiste en computadoras (también conocidas como nodos).*
3. *La red de nodos utiliza algoritmos conocidos para validar la transacción y el estado del usuario.*
4. *Una transacción verificada puede involucrar criptomonedas, contratos, registros u otra información.*
5. *Una vez verificada, la transacción se combina con otras transacciones para crear un nuevo bloque de datos para el libro contable.*
6. *El nuevo bloque se añade a la blockchain existente (que es permanente e inalterable).*
7. *La transacción ahora está finalizada.*

Un libro contable y una firma digital

Imagina que tú y tu amiga, Alicia, deciden llevar un registro de los gastos compartidos utilizando un libro contable digital y firmas digitales. El libro contable es como un cuaderno digital compartido en el que ambos registran todos sus gastos compartidos. Cada "página" del cuaderno representa un bloque en el libro contable y cada vez que gastan dinero o contribuyen a un gasto compartido, lo anotan en un nuevo bloque. El libro contable no se guarda en un solo lugar, sino que se duplica y comparte con ambos, para que tanto tú como Alicia tengan una copia idéntica; cualquier cambio se actualiza simultáneamente para todos.

Ahora, cuando quieras confirmar tus contribuciones al libro contable sin temor a que alguien más se haga pasar por ti, utilizas **una firma digital**. Piénsalo como un apretón de manos único y secreto que solo tú tienes. Cuando agregas una entrada al libro contable, la firmas con tu firma digital, que se basa en tu apretón de manos secreto (clave privada). Alicia, y cualquier otra persona, puede usar tu apretón de manos público (clave pública) para verificar la firma y confirmar que realmente fuiste tú quien hizo esa entrada. Si la firma no coincide o la entrada en el libro parece haber sido manipulada, sabrán que algo no está bien.

Para ejemplificarlo, digamos que decides comprar víveres por $20 y agregarlo al libro contable. Firmas esta entrada con tu firma digital, indicando que tú eres quien lo pagó. El libro contable se actualiza para ambos y muestra la nueva entrada con tu firma. Más tarde, cuando

Alicia revisa el libro contable, ve tu entrada y verifica tu firma digital usando tu clave pública. Si la firma es válida, ella sabe que efectivamente pagaste por las compras. De esta manera, el libro contable contiene un registro transparente de los gastos compartidos y las firmas digitales aseguran la autenticidad de cada entrada, lo que previene manipulaciones y brinda confianza entre tú y Alicia en sus transacciones financieras compartidas.

Libro contable

- En el contexto de las finanzas y las transacciones, un libro contable es un sistema de registro que rastrea y gestiona transacciones financieras. Tradicionalmente, los libros contables eran libros físicos en los que las empresas registraban sus débitos y créditos. En la era digital, los libros contables ahora electrónicos e incluso muchos son descentralizados y están distribuidos a través de una red de computadoras.

- Una blockchain, que es un tipo de libro contable descentralizado, es una cadena secuencial de bloques, cada uno de los cuales contiene una lista de transacciones. Proporciona una forma transparente y segura de registrar y verificar transacciones sin necesidad de una autoridad central.

Firma digital

- Una firma digital es una técnica criptográfica utilizada para verificar la autenticidad e integridad de mensajes o documentos digitales. Proporciona una manera para que el remitente de un mensaje pruebe su identidad y asegure que el mensaje no ha sido alterado durante la transmisión.

- En el contexto de las transacciones, las firmas digitales se utilizan a menudo para firmar documentos electrónicos o confirmar el origen de un mensaje digital. Se basan en un par de claves criptográficas: una clave privada conocida solo por el firmante y una clave pública que otros pueden usar para verificar la firma.

- El proceso implica crear una huella digital única (hash) del documento o mensaje usando la clave privada. Este hash, junto con la clave privada, forma la firma digital. El destinatario luego puede usar la clave pública del remitente para verificar la firma y confirmar la autenticidad del documento.

En el ámbito de las monedas digitales y la tecnología blockchain, los libros contables y las firmas digitales juegan roles cruciales para

asegurar la seguridad, transparencia y confiabilidad de las transacciones. Los libros contables blockchain utilizan técnicas criptográficas, como las firmas digitales, para asegurar y validar la integridad de las transacciones dentro de una red descentralizada.

Función hash

Exploremos el concepto de una función hash criptográfica, específicamente el algoritmo SHA-256.

Imagina que quieres asegurar un mensaje que le envías a tu amigo, Bob, utilizando una función hash criptográfica, en este caso, SHA-256.

Escribes el mensaje "¡Hola, Bob!" y deseas crear un hash usando SHA-256. El algoritmo SHA-256 procesa este mensaje y genera una cadena de caracteres de longitud fija, típicamente de sesenta y cuatro caracteres, conocida como valor hash. Envías este valor hash junto con tu mensaje.

Ahora, Bob recibe el mensaje y el valor hash. Él ejecuta el mismo algoritmo SHA-256 en el mensaje recibido y, si el valor hash que calcula coincide con el que tú enviaste, puede estar seguro de que el mensaje no ha sido manipulado.

Definición: una función hash criptográfica, como **SHA-256** (secure hash algorithm 256-bit), es un algoritmo matemático que toma datos

de entrada (como un mensaje o archivo) y produce una cadena de caracteres de tamaño fijo, que típicamente es un número hexadecimal.

Las propiedades clave de las funciones hash criptográficas son:

- Determinista: la misma entrada siempre producirá la misma salida (valor hash).
- Cálculo rápido: el valor hash se calcula de manera eficiente y rápida.
- Irreversibilidad: es ser computacionalmente inviable revertir el proceso y derivar la entrada original a partir del valor hash.
- Resistencia a colisiones: es poco probable que dos entradas diferentes produzcan el mismo valor hash.

En el caso de SHA-256, produce específicamente un valor hash de 256 bits (32 bytes). Este tipo de función hash se utiliza ampliamente en diversas aplicaciones de seguridad y forma un componente crucial de la tecnología blockchain, lo que asegura la integridad y autenticidad de los datos.

Tipos de redes blockchain

Existen varios tipos de redes blockchain, cada una con características y casos de uso distintos. Los tipos principales son:

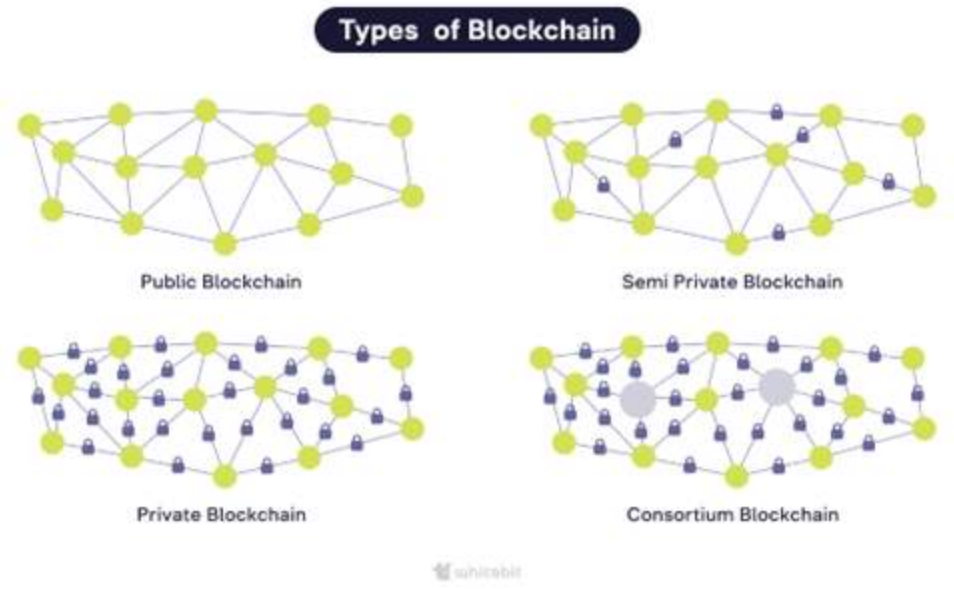
Blockchain pública. Redes abiertas y descentralizadas accesibles para cualquiera. Las transacciones son transparentes y la red opera en una base de confianza, permitiendo la participación universal. Ejemplos: Bitcoin y Ethereum.

Blockchain privada: redes blockchain cerradas, generalmente controladas por una sola organización. El acceso está restringido y las reglas son establecidas por la entidad controladora para la visibilidad y el registro de transacciones.

Blockchain de consorcio: un modelo híbrido que combina elementos de blockchains públicas y privadas. Varias organizaciones gestionan de manera colaborativa una red blockchain compartida. Puede ser abierta o cerrada, dependiendo de los objetivos del consorcio.

Blockchain híbrida semiprivada: una combinación de blockchains públicas y privadas que ofrece características de ambas. Ciertos aspectos de la blockchain pueden ser públicos para mayor transparencia y otros son privados para acceso restringido.

Figura 5. Tipos de blockchain (M1-U2-5)



Tipos de blockchain	
Blockchain pública	Blockchain semiprivada
Blockchain privada	Blockchain de consorcio

Fuente: Creada por el autor para este módulo.

Blockchain permisionada: similar a las blockchains privadas, pero cuenta con un grupo definido de participantes que tienen autorización para acceder y validar transacciones. Este tipo de blockchain se utiliza frecuentemente en entornos empresariales que requieren un control más estricto.

Sidechain (cadena lateral): es una red blockchain independiente conectada a la blockchain principal, que permite ejecutar funciones

específicas sin afectar directamente la cadena principal. Esto contribuye a mejorar la escalabilidad y la funcionalidad.

Multichain: se trata de una plataforma blockchain privada o de consorcio que permite crear múltiples blockchains independientes (subcadenas) dentro de la misma red. Cada subcadena puede tener sus propias reglas y permisos.

Capítulo 3: Mecanismos de consenso

En los debates anteriores, exploramos el problema de los generales bizantinos y sus implicaciones en los sistemas distribuidos. Para enfrentar los desafíos que presentan los actores malintencionados y garantizar el consenso entre los participantes de la red, se han desarrollado varios mecanismos de consenso. Estos mecanismos son fundamentales para la tecnología blockchain, ya que ofrecen soluciones al problema de los generales bizantinos y establecen un marco descentralizado y sin confianza para validar transacciones y mantener la integridad del libro mayor distribuido. En este capítulo, analizaremos diferentes mecanismos de consenso, desglosando sus enfoques únicos, fortalezas y posibles desafíos.

Prueba de trabajo (PoW)

La prueba de trabajo (PoW) es un mecanismo de consenso utilizado en redes blockchain para validar y confirmar transacciones. En un

sistema PoW, los participantes, conocidos como mineros, compiten para resolver acertijos matemáticos complejos. El primer minero que resuelve el acertijo obtiene la oportunidad de añadir un nuevo bloque a la blockchain y es recompensado con criptomonedas recién creadas y tarifas de transacción. Este proceso requiere un poder computacional considerable y un alto consumo de energía.

Ventajas

- **Seguridad**: La PoW es reconocida por su sólida seguridad. La complejidad computacional necesaria para resolver los acertijos hace que sea prácticamente inviable para un solo participante o grupo controlar la mayor parte de la red, lo que previene ataques maliciosos.

- **Descentralización**: La PoW fomenta la descentralización al permitir que un grupo diverso de mineros participe en el proceso de consenso. La naturaleza distribuida de la minería ayuda a evitar la centralización del control dentro de la red.

- **Distribución justa**: el proceso de minería brinda una oportunidad para una distribución equitativa de nuevas criptomonedas. Los participantes que invierten en equipos de minería y aportan poder computacional son recompensados por sus esfuerzos.

- **Historial comprobado**: La PoW tiene un historial comprobado, especialmente en el caso de Bitcoin, que ha estado en funcionamiento desde 2009. La longevidad de las redes PoW contribuye a su percepción de fiabilidad y confianza.

- **Resistencia a ataques** Sybil: Los sistemas PoW son resistentes a los ataques Sybil, en los cuales un solo participante intenta hacerse pasar por múltiples entidades para obtener control sobre la red. El costo y esfuerzo requeridos para la minería actúan como disuasivos contra este tipo de ataques.

Desafíos

- **Consumo de energía**: una de las críticas más importantes a la PoW es su elevado consumo energético. El proceso de resolver acertijos complejos requiere una cantidad significativa de poder computacional, lo que genera preocupaciones sobre el impacto ambiental y la sostenibilidad de las redes PoW.

- **Centralización del poder de minería**: a lo largo del tiempo, las redes PoW han visto una centralización del poder de minería, donde unos pocos grupos

controlan una gran parte de la capacidad computacional total. Esto genera preocupaciones sobre posibles ataques del 51%.

- **Escalabilidad limitada**: Las redes PoW enfrentan desafíos relacionados con la escalabilidad a medida que los requisitos computacionales aumentan con el crecimiento de la red. Esto puede dar lugar a tiempos de procesamiento de transacciones más lentos y tarifas más altas durante la congestión de la red.

- **Carrera armamentista de hardware de minería**: la naturaleza competitiva de la minería ha llevado a una carrera armamentista en el desarrollo de hardware especializado, como circuitos integrados de aplicación específica (ASIC). Esto crea una barrera de entrada para mineros individuales y puede contribuir a la centralización.

- **Ineficiencia económica**: los críticos sostienen que la PoW es económicamente ineficiente debido al alto consumo de energía y la necesidad de hardware especializado. Esta ineficiencia contrasta con los mecanismos de consenso más recientes diseñados para abordar las preocupaciones ambientales.

En resumen, la prueba de trabajo ha demostrado su eficacia al proporcionar seguridad y descentralización a las redes blockchain. Sin embargo, los desafíos del consumo de energía, la centralización y la escalabilidad han llevado a largos debates sobre la sostenibilidad y la viabilidad futura de la PoW en el panorama en rápida evolución de la tecnología blockchain.

Prueba de participación (PoS)

La prueba de participación (PoS) es un mecanismo de consenso utilizado en redes blockchain para validar y confirmar transacciones. A diferencia de la prueba de trabajo (PoW), donde los participantes (mineros) compiten para resolver acertijos matemáticos complejos para añadir bloques a la blockchain, en la PoS los validadores son seleccionados para crear nuevos bloques y verificar transacciones según la cantidad de criptomonedas que poseen o "participan". En la PoS, la probabilidad de ser elegido para crear un nuevo bloque es proporcional a la cantidad de participación del participante en la red.

Ventajas

- **Eficiencia energética**: una de las principales ventajas de PoS es su eficiencia energética en comparación con PoW. Al no requerir el proceso intensivo de resolver acertijos complejos, PoS consume significativamente

menos energía, lo que lo convierte en una alternativa más amigable con el medio ambiente.

- **Seguridad**: Los sistemas PoS están diseñados para desalentar comportamientos maliciosos al requerir que los participantes pongan en juego su propia criptomoneda. Este incentivo económico alinea los intereses de los participantes con la seguridad y estabilidad de la red, ya que cualquier acción maliciosa pondría en riesgo sus propios activos en juego.

- **Descentralización**: La PoS promueve la descentralización al permitir que una variedad más amplia de participantes se involucre en el proceso de consenso. Esto contrasta con la PoW, donde el proceso tiende a ser dominado por mineros con gran poder computacional.

- **Reducción de la centralización del poder de minería**: La PoS mitiga la centralización del poder de minería que se observa en las redes PoW, donde unas pocas entidades pueden controlar la mayor parte de la capacidad de minería. Esto ayuda a evitar el riesgo de un ataque del 51%.

- **Escalabilidad**: La PoS se considera generalmente más escalable que la PoW. La ausencia de cálculos intensivos permite un procesamiento de

transacciones más rápido, lo que contribuye a una mejor escalabilidad a medida que la red crece.

Desafíos

- **Distribución inicial**: la efectividad de la PoS depende de una distribución justa y amplia de criptomonedas entre los participantes. Si una cantidad pequeña de entidades posee la mayoría de la participación, esto podría dar lugar a preocupaciones sobre la centralización.

- **Problema de "nada en juego"**: el problema de "nada en juego" se refiere a la situación en la que los validadores no enfrentan costos al respaldar múltiples historias de blockchain en conflicto. Esto puede provocar una falta de consenso, ya que los validadores pueden optar por múltiples bifurcaciones.

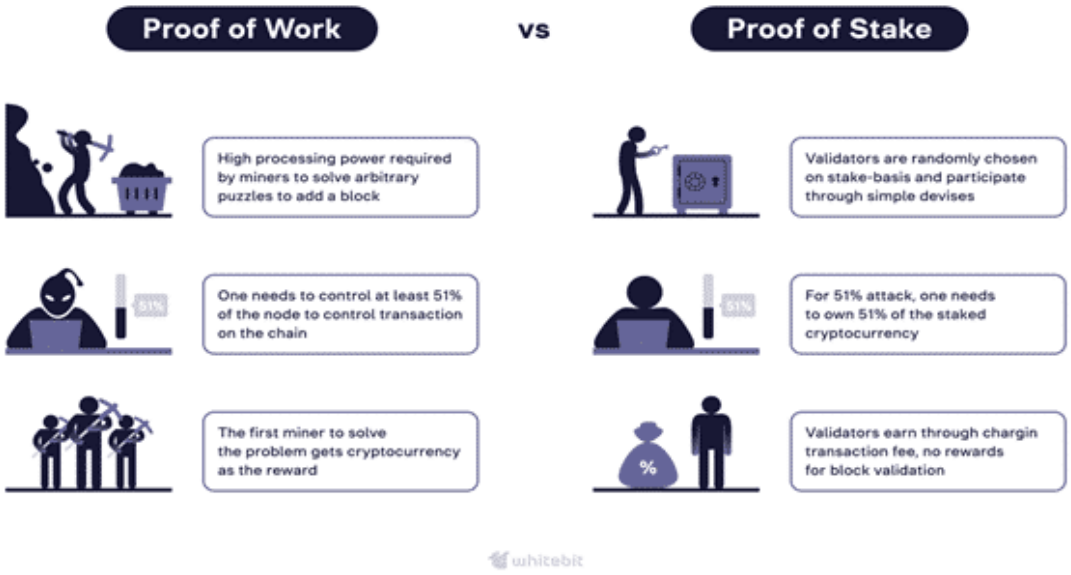
- **Ataque a largo plazo**: Las redes PoS son vulnerables a ataques a largo plazo, donde un atacante puede crear una bifurcación desde un punto anterior en la blockchain y construir una nueva cadena. Este desafío requiere medidas de seguridad adicionales.

- **Riesgo de censura**: en PoS, la capacidad de crear nuevos bloques está vinculada a la cantidad de criptomonedas en juego. Esto trae aparejadas preocupaciones sobre la posible censura, donde aquellos con participaciones más grandes podrían influir en el proceso de consenso para favorecer sus propios intereses.

- **Centralización de la participación**: Las redes PoS pueden enfrentar desafíos relacionados con la centralización del participación, donde unos pocos pero grandes participantes dominan el proceso de consenso. Esto podría socavar los objetivos de descentralización del sistema.

En resumen, la prueba de participación ofrece ventajas destacadas en términos de eficiencia energética, seguridad y escalabilidad. Sin embargo, es necesario abordar cuidadosamente desafíos como la distribución inicial, el problema de "nada en juego" y el potencial de centralización de participación para garantizar la efectividad y descentralización de las redes blockchain basadas en PoS.

Figura 6: POW y POS



Prueba de trabajo	Prueba de participación
Los mineros requieren una alta potencia de procesamiento para resolver acertijos arbitrarios y añadir un bloque.	Los validadores son seleccionados al azar en función de su participación y utilizan dispositivos sencillos.
Para controlar las transacciones en la cadena, es necesario poseer al menos el 51% de los nodos.	Para llevar a cabo un ataque del 51%, se necesita poseer el 51% de la criptomoneda en cuestión.
El primer minero que resuelve el problema recibe criptomonedas como recompensa.	Los validadores obtienen ganancias mediante las tarifas de transacción, sin recibir recompensas por la validación de bloques.

Fuente: Elaboración propia. Creada por el autor para este texto.

Capítulo 4: El futuro de la tecnología blockchain. Aplicaciones y casos de uso

¿Para qué se utiliza la tecnología blockchain? La tecnología blockchain es versátil y ha sido adoptada en diversas industrias gracias a sus características únicas, como la descentralización, la transparencia, la seguridad y la inmutabilidad.

Las tecnologías de criptomonedas y blockchain están cerrando la brecha entre los equipos deportivos y sus fans. Proporcionan soluciones innovadoras a problemas tradicionales con una experiencia más inclusiva e interactiva para los fans.

Aprendamos ahora cómo las criptomonedas fortalecen la conexión entre equipos y fans a través de aplicaciones para fans, membresías digitales y tokens para fans.

Venta de entradas y *fan engagement*

Caso de uso: el mercado ilegal ha sido un problema persistente en la industria del deporte. Sin embargo, la incorporación de la tecnología blockchain en los sistemas de venta de entradas representa una solución prometedora. Las organizaciones deportivas que adoptan blockchain pueden reducir efectivamente el riesgo de fraude y garantizar a los fans un acceso seguro a las entradas a precios justos. El uso innovador de blockchain también permite verificar fácilmente la autenticidad de las entradas y crear así un mercado confiable donde las transacciones son inmediatas, compartidas y completamente transparentes. Esto no solo mejora la integridad de los procesos de venta de entradas, sino que también enriquece la experiencia del fan al promover un entorno seguro y confiable para el intercambio de entradas.

Consideremos el caso de la Selección Nacional de Fútbol de Ucrania, que tiene una asociación oficial con el intercambio de criptomonedas WhiteBIT.

Las entradas para los partidos locales contra Italia, Malta e Inglaterra estaban disponibles para su compra utilizando criptomonedas. Esta opción fue posible gracias a la integración del servicio Whitepay en el sistema de venta de entradas. Whitepay, un servicio de adquisición de criptomonedas y parte del ecosistema WhiteBIT, facilitó esta integración técnica.

Los usuarios de criptomonedas tuvieron la ventaja de acceder anticipadamente a las entradas, lo que les permitió conseguir asientos preferenciales varios días antes de que comenzara oficialmente la venta de entradas. Los precios de las entradas se mantuvieron fijos tanto en criptomonedas como en moneda fíat.

Mientras que los fans que optaron por comprar en criptomonedas pudieron obtener entradas en todas las categorías, se observó una mayor disponibilidad de entradas de categorías más caras. Esta tendencia resaltó la flexibilidad y el atractivo de utilizar criptomonedas para adquirir entradas.

Autenticidad de objetos de colección

Caso de uso: blockchain se puede utilizar para verificar la autenticidad de recuerdos u objetos de colección. Cada artículo puede recibir un token digital único en la blockchain con un registro transparente y a prueba de manipulaciones sobre su origen y propiedad.

Contratos y transferencias de jugadores

Caso de uso: blockchain simplifica y asegura la gestión de contratos de jugadores, transferencias y pagos. Los contratos inteligentes automatizan la ejecución de contratos basándose en condiciones predefinidas; se reduce así el riesgo de disputas y se garantizan los pagos en tiempo y forma.

Antidopaje e historias clínicas

Caso de uso: blockchain puede utilizarse para asegurar y gestionar los registros de salud de los deportistas y los resultados de las pruebas de dopaje. Esto garantiza la integridad de los datos y otorga a los deportistas un mayor control sobre su información personal.

Cadena de suministro para equipos deportivos

Caso de uso: blockchain mejora la transparencia en la cadena de suministro de equipos deportivos. Permite a los consumidores rastrear el origen y la autenticidad del equipo deportivo; así, se aseguran de que cumplan con los estándares de calidad y seguridad.

Coleccionables digitales y NFT

Caso de uso: los tokens no fungibles (NFT) en la blockchain permiten la creación y el comercio de coleccionables digitales, como momentos destacados de eventos deportivos, jugadas de jugadores y mercancía virtual. Esto proporciona una nueva fuente de ingresos y oportunidades de fan engagement.

Tokenización y votación de los fans

Caso de uso: blockchain permite a los equipos deportivos emitir tokens de fans y darles participación en la propiedad y derechos de voto en ciertas decisiones. Esto fomenta un sentido de comunidad y participación entre los seguidores.

Derechos de medios y regalías

Caso de uso: blockchain puede agilizar la gestión de derechos de medios y regalías para los deportistas y los equipos. Los contratos inteligentes automatizan la distribución de pagos según acuerdos predefinidos con menos disputas y garantía de una compensación justa.

Apuestas deportivas e integridad

Caso de uso: blockchain mejora la transparencia y la integridad de las apuestas deportivas. Al registrar y sellar temporalmente los datos de apuestas en la blockchain, se vuelve más resistente a la manipulación y se reduce el riesgo de arreglo de partidos.

Plataformas deportivas descentralizadas

Caso de uso: blockchain facilita la creación de plataformas deportivas descentralizadas con interacciones directas entre deportistas, fans patrocinadores. Esto puede dar lugar a nuevos modelos de negocio, oportunidades de patrocinio y canales de distribución de contenido.

Socios importantes en la industria blockchain y el deporte profesional

El intercambio de criptomonedas WhiteBIT, uno de los mayores intercambios de criptomonedas en Europa, es un claro ejemplo de la sinergia entre la tecnología blockchain y el deporte profesional.

Como socio oficial de criptomonedas del famoso club de fútbol Barcelona, WhiteBIT demuestra un enfoque integral e inclusivo, apoyando no solo a los equipos de fútbol masculino y femenino, sino también colaborando con diversas ramas deportivas del club: el equipo de esports de League-of-Legends, así como los equipos de baloncesto, hockey sobre hielo, minifútbol y balonmano.

Estas asociaciones reflejan el compromiso de WhiteBIT con la mejora e integración de los deportes tradicionales, los esports y la tecnología blockchain.

Además, WhiteBIT es socio de la Selección Nacional de Fútbol de Ucrania, brindando apoyo y contribuyendo al desarrollo y promoción del fútbol a nivel nacional en Ucrania.

También, la colaboración con el club de fútbol turco Trabzonspor subraya aún más el respaldo al fútbol en diferentes países.

La asociación de WhiteBIT con ESL FACEIT GROUP, la principal plataforma para competiciones de esports, resalta su participación activa y apoyo al desarrollo de la comunidad de esports. Al organizar eventos conjuntos para traders y jugadores, WhiteBIT y FACEIT promueven el desarrollo de los esports y crean oportunidades para la interacción y cooperación entre industrias. Esta asociación refleja la comprensión de WhiteBIT sobre la relación sinérgica entre los esports y el sector de criptomonedas.

Resumiendo

En la segunda unidad de nuestro módulo, hemos explorado las complejidades de los elementos esenciales de blockchain, enfatizando la distinción entre Bitcoin y el concepto más amplio de blockchain, así como la importancia de la descentralización en esta tecnología

revolucionaria. Cubrimos también los mecanismos internos de blockchain con los componentes de los libros de contabilidad, las firmas digitales, las funciones hash y las diferentes redes blockchain. La discusión se adentró en los mecanismos de consenso críticos: la prueba de trabajo y la prueba de participación. Finalmente, reflexionamos sobre el futuro de la tecnología blockchain con sus aplicaciones versátiles y varios casos de uso que van más allá de las criptomonedas. A modo de cierre de este módulo, hemos establecido una base sólida para entender los conceptos y mecanismos fundamentales que impulsan la innovación en blockchain, con todo listo para una exploración y aplicación más profunda en el dinámico mundo de las tecnologías emergentes.

CONTINUAR

Referencias

Chaum, D. (1983). *Blind Signatures for Untraceable Payments*. Departamento de Ciencias Informáticas. Universidad de California.

Nakamoto, S. (2008a). *Re: Bitcoin P2P e-cash paper.* The Mail Archive. https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html.

Nakamoto, S. (2008b). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org. https://Bitcoin.org/Bitcoin.pdf.

[Imagen sin título de minería de Bitcoin]. (s. f.). https://xcoins.com/es/blog/como-funciona-el-minado-de-Bitcoin/.

WhiteBIT. (2023a). *Step-by-step KYC verification on WhiteBIT Web Version [archivo de video]*. YouTube. https://www.youtube.com/watch?v=jyQkn0RpMJg.

WhiteBIT. (2 de febrero de 2023). *What is KYC: Meaning, Process, and Advantages*. WB Blog. https://blog.whitebit.com/en/chto-takoe-kyc/.

CONTINUAR