Guía de referencia

Explorando la blockchain

CURATED BY
TUTELLUS

Índice

Fundamentos de Bitcoin

Introducción al Concepto de Bitcoin y su papel como Moneda Alternativa

En el mundo de la economía digital, Bitcoin emerge como una fuerza disruptiva que redefine el concepto de moneda. Desde su creación en 2008 por una persona o grupo de personas bajo el seudónimo de Satoshi Nakamoto, Bitcoin ha desafiado las normas tradicionales de las transacciones financieras y ha establecido un nuevo paradigma para el intercambio de valor en el siglo XXI. El siguiente documento explora la esencia de Bitcoin y otras tecnologías subyacentes, desentrañando sus características únicas y analizando su papel como moneda alternativa en la economía global.

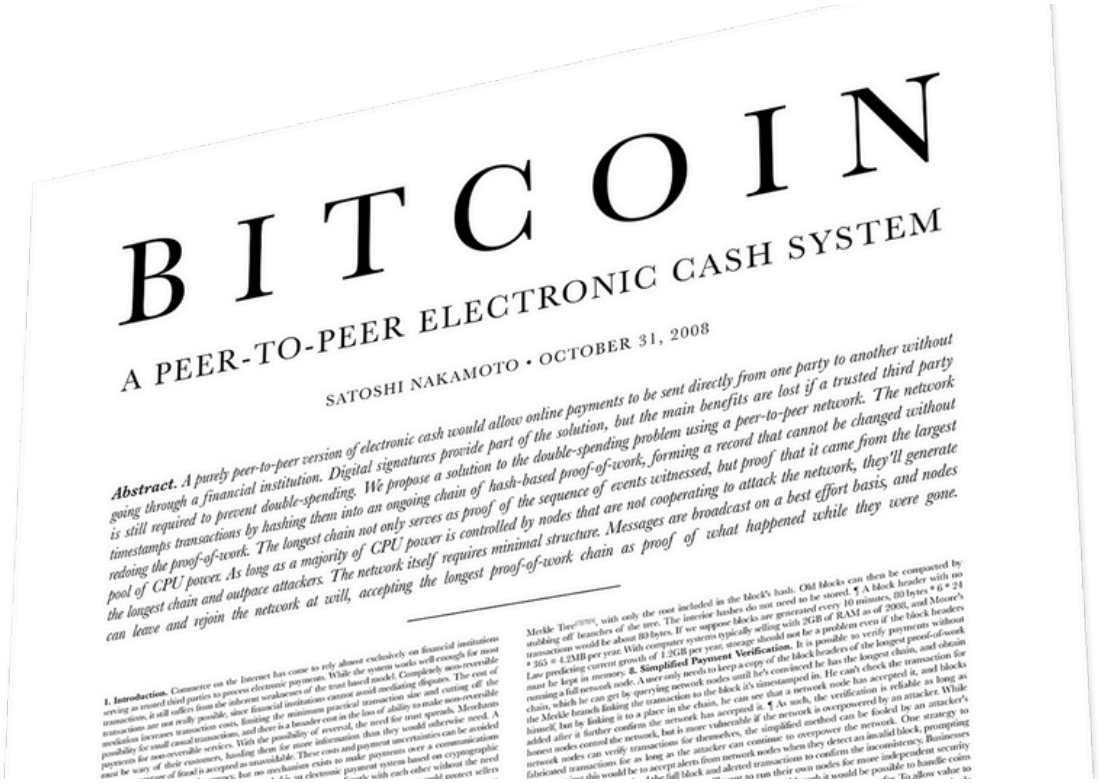
Características Distintivas de Bitcoin

Bitcoin se distingue por varias características clave:

- Escasez Digital: El suministro total de Bitcoin está limitado a 21 millones de unidades, una política que imita la escasez de recursos como el oro y contrasta con las monedas fiduciarias que pueden ser impresas indefinidamente por los gobiernos.
- Descentralización: Al operar en una red distribuida, Bitcoin elimina la necesidad de intermediarios, permitiendo transacciones directas entre usuarios y aumentando la resiliencia del sistema ante ataques o fallas.
- Seguridad y Transparencia: Utilizando la tecnología blockchain, Bitcoin ofrece un libro mayor público y cifrado que registra todas las transacciones. Este sistema asegura la integridad de los datos y facilita la verificación de las transacciones sin comprometer la privacidad de los usuarios.
- Pseudoanonimato: Aunque las transacciones son transparentes y públicas, las identidades de los usuarios se mantienen protegidas detrás de direcciones alfanuméricas conocidas como wallets o billeteras.

Orígenes y Fundamentos de Bitcoin

Bitcoin se presentó al mundo a través de un documento técnico que proponía una versión puramente peer-to-peer (P2P) de dinero electrónico. Este sistema permitiría enviar pagos en línea directamente de una parte a otra sin la intermediación de instituciones financieras. La innovación de Bitcoin radica en su capacidad para resolver el problema del doble gasto (la posibilidad de que una misma moneda digital sea gastada más de una vez) sin necesidad de una autoridad central. En enero de 2009, el primer bloque de Bitcoin, conocido como el bloque génesis, fue minado, marcando el nacimiento de una nueva era financiera.



BITCOIN

A PEER-TO-PEER ELECTRONIC CASH SYSTEM

SATOSHI NAKAMOTO • OCTOBER 31, 2008

Abstract. *A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.*

Introducción al Concepto de Bitcoin y su Papel como Moneda Alternativa

En el mundo de la economía digital, Bitcoin emerge como una fuerza disruptiva que redefine el concepto de moneda. Desde su creación en 2008 por una persona o grupo de personas bajo el seudónimo de Satoshi Nakamoto, Bitcoin ha desafiado las normas tradicionales de las transacciones financieras y ha establecido un nuevo paradigma para el intercambio de valor en el siglo XXI. El siguente documento explora la esencia de Bitcoin, desentrañando sus características únicas y analizando su papel como moneda alternativa en la economía global.

¿Cómo Surge Bitcoin?

Bitcoin representa el culmen de más de cuatro décadas de investigación en diversas disciplinas tecnológicas y económicas. Esta innovadora moneda digital es el resultado de la combinación de tecnologías existentes como redes Peer-to-Peer (P2P), criptografía avanzada, la tecnología de cadena de bloques y principios de la teoría de juegos. Bitcoin no solo se construyó sobre las bases establecidas por proyectos anteriores sino que también aprendió de sus lecciones, adaptando y mejorando sus enfoques. Uno de sus pilares teóricos más destacados es la aplicación de la teoría de juegos, que ayuda a resolver problemas complejos como el de los generales bizantinos, fomenta el equilibrio de Nash y estructura incentivos para asegurar la participación y honestidad de los usuarios en la red.

Precursores de Bitcoin

La creación de Bitcoin por el misterioso Satoshi Nakamoto no solo marcó el nacimiento de la primera criptomoneda descentralizada, sino que también representó la culminación de décadas de investigación y desarrollo en el campo de la criptografía y las finanzas digitales. La génesis de Bitcoin puede ser vista como una obra maestra de la ingeniería y el pensamiento visionario, una que se apoyó fuertemente en los cimientos establecidos por cuatro proyectos pioneros y sus creadores.

Estos proyectos, aunque variados en sus objetivos y aplicaciones, compartían una visión común: la de un sistema financiero digital seguro, privado y sin fronteras.

David Chaum y DigiCash: La Cuna de la Criptomoneda

David Chaum, un visionario en el ámbito de la privacidad digital y la criptografía, legó al mundo varias innovaciones clave que formarían la base sobre la que Bitcoin se erigiría. Su trabajo en DigiCash, una empresa pionera en el dinero digital basada en Ámsterdam, se destacó por la implementación de la criptografía de firmas ciegas. Este mecanismo permitía transacciones anónimas, preservando la privacidad del usuario al tiempo que garantizaba la seguridad y la integridad de las transacciones. Chaum también propuso un sistema de votación electrónica seguro y anónimo en 1981, así como la idea del dinero electrónico no trazable en 1988, colaborando con Amos Fiat y Moni Naor. Estas innovaciones subrayaron la importancia de la privacidad y la seguridad en las transacciones digitales, dos pilares fundamentales en el diseño de Bitcoin.

Adam Back y Hashcash: El Precursor de la Prueba de Trabajo

Adam Back introdujo Hashcash en 1997, una tecnología de prueba de trabajo diseñada originalmente para combatir el spam en el correo electrónico. Este sistema requería que se realizara un trabajo computacional para enviar un correo, imponiendo un costo que desalentaba a los spammers.

La prueba de trabajo de Hashcash se convirtió en un componente crítico de Bitcoin, donde se utiliza para validar y minar nuevos bloques, asegurando la red contra ataques y manipulaciones.

Nick Szabo y Bitgold: El Esbozo de Bitcoin

Nick Szabo, con su propuesta de Bitgold a finales de los 90, presentó un sistema descentralizado de prueba de trabajo para crear y distribuir una moneda digital. Aunque Bitgold nunca se implementó, su concepto de utilizar la criptografía para crear una moneda segura y descentralizada influenció directamente el desarrollo de Bitcoin. Szabo también es conocido por acuñar el término "contrato inteligente", una idea que se ha convertido en una característica fundamental de las criptomonedas y la tecnología blockchain.

Wei Dai y B-Money: La Visión de una Economía Descentralizada

Wei Dai, con su propuesta de B-Money en 1998, esbozó un sistema descentralizado de dinero electrónico. B-Money introdujo la idea de una base de datos distribuida entre los participantes para mantener el registro de las transacciones, un concepto que encontraría su expresión plena en la tecnología blockchain de Bitcoin. Aunque B-Money también quedó en el terreno de las ideas, su visión de una economía descentralizada y una moneda digital sin una autoridad central influyó profundamente en Nakamoto.

IEl Mecanismo de Consenso de Bitcoin: PoW

La red de Bitcoin se sostiene sobre un mecanismo de consenso descentralizado que garantiza la seguridad, transparencia y fiabilidad de las transacciones sin la necesidad de una autoridad central. Este sistema no solo ha permitido el funcionamiento eficiente de la primera y más famosa criptomoneda del mundo, sino que también ha sentado las bases para el desarrollo de innumerables otras criptomonedas y tecnologías blockchain. En el corazón de este mecanismo de consenso, cuatro actores principales juegan roles indispensables: el protocolo, los mineros, los nodos y el token (BTC). Cada uno de estos elementos contribuye de manera única al funcionamiento y seguridad de la red.

1. El Protocolo: La Espina Dorsal de Bitcoin

El protocolo de Bitcoin es el conjunto de reglas codificadas que definen cómo opera la red. Incluye el algoritmo de prueba de trabajo (Proof of Work - PoW), el límite de 21 millones de bitcoins, el tamaño y la frecuencia de los bloques, y las reglas de validación de transacciones. Este protocolo asegura que todos los participantes de la red trabajen bajo los mismos estándares, manteniendo la red segura y previniendo el doble gasto sin la necesidad de una autoridad central. Los cambios en el protocolo requieren de un consenso amplio dentro de la comunidad, lo que asegura su estabilidad y resistencia frente a cambios arbitrarios.

2. Los Mineros: Guardianes de la Red

Los mineros son participantes que utilizan su poder computacional para resolver complejos acertijos criptográficos, un proceso conocido como minería. Este esfuerzo asegura la adición de nuevos bloques de transacciones a la blockchain de Bitcoin de manera secuencial y resistente a alteraciones. Como recompensa por su trabajo, los mineros reciben bitcoins recién creados (la recompensa por bloque) y las tarifas de transacción. La minería es crucial para la seguridad de la red, ya que la dificultad de los acertijos requiere de una enorme cantidad de recursos computacionales para ser resueltos, protegiendo a la red de ataques maliciosos.

3. Los Nodos: Vigilantes de la Verdad

Los nodos son computadoras que mantienen una copia completa de la blockchain y siguen las reglas del protocolo de Bitcoin. Estos verifican de manera independiente todas las transacciones y bloques contra las reglas del protocolo antes de aceptarlos, rechazando cualquier bloque o transacción inválida. Al hacerlo, los nodos mantienen la integridad y el consenso de la red, asegurando que todos los participantes tengan una visión unificada del estado de la blockchain. Los nodos completos juegan un papel fundamental en la descentralización de Bitcoin, ya que permiten que el sistema opere sin la necesidad de una autoridad central de confianza.

El Token: BTC

Bitcoin (BTC) no es solo el token o unidad de cuenta de la red de Bitcoin, sino también el incentivo que motiva a mineros y participantes a mantener y proteger la red. El límite fijo de 21 millones de bitcoins asegura su naturaleza deflacionaria, diferenciándolo de las monedas fiduciarias que pueden ser impresas indefinidamente.

La propiedad descentralizada y la transferencia de bitcoins se facilitan a través de la criptografía, proporcionando un medio de intercambio seguro y anónimo.

El halving

El "halving" de Bitcoin es un evento programado que sucede aproximadamente cada cuatro años, o después de que se hayan minado 210,000 bloques. Este evento reduce a la mitad la recompensa que los mineros reciben por validar y añadir nuevos bloques a la blockchain de Bitcoin, un mecanismo que fue diseñado por el creador de Bitcoin, Satoshi Nakamoto, para controlar la inflación de esta criptomoneda.

- Orígenes y Propósito

El sistema de halving fue implementado como una forma de simular la escasez de recursos naturales, similar a la extracción de oro. Al igual que es cada vez más difícil y requiere más recursos extraer oro, el halving asegura que obtener nuevos Bitcoins sea progresivamente más desafiante, imitando la escasez y añadiendo valor. Este mecanismo es fundamental para evitar la inflación, manteniendo el suministro total de Bitcoin limitado a 21 millones de unidades.

- Impacto en la Minería

Para los mineros de Bitcoin, el halving puede tener un impacto significativo en su rentabilidad. La reducción a la mitad de la recompensa significa que, de un día para otro, recibirán la mitad de Bitcoin por el mismo trabajo realizado. Esto puede llevar a una consolidación en la industria minera, donde solo los participantes más eficientes y con menores costos operativos pueden seguir siendo rentables.

	Nuevos BTC por bloque antes del evento de halving	Nuevos BTC por bloque después del evento de halving	Precio del BTC el día del evento de halving	Precio del BTC 150 días después	Precio del BTC 365 días después
2012 Halving	50 BTC	25 BTC	12,35 $	127,00 $	1.003,38 $
2016 Halving	25 BTC	12,5 BTC	650,53 $	758,81 $	2.518,44 $
2020 Halving	12,5 BTC	6,25 BTC	8.821,42 $	10.943,00 $	55.986,51 $

- Efectos en el Mercado

Históricamente, los eventos de halving han estado asociados con aumentos en el precio de Bitcoin, aunque estos aumentos no siempre ocurren inmediatamente. Muchos analistas sugieren que el halving tiene un efecto positivo en el precio a largo plazo, ya que reduce la oferta de nuevos Bitcoins que ingresan al mercado. Sin embargo, es importante notar que el mercado de criptomonedas está influenciado por muchos factores, y el halving es solo uno de ellos.

- Halvings Pasados y Futuros

Desde la creación de Bitcoin en 2009, ha habido varios eventos de halving:
- 2012: La recompensa por bloque pasó de 50 a 25 bitcoins.
- 2016: La recompensa se redujo de 25 a 12.5 bitcoins.
- 2020: La recompensa se redujo a 6.25 bitcoins.

El próximo halving está previsto para 2024, y reducirá la recompensa a 3.125 bitcoins por bloque.

Bitcoin avanzado y tokenomics

Tipos de almacenamiento

En el mundo de las criptomonedas, la seguridad y la gestión de nuestros activos digitales son de suma importancia. Para esto, las carteras o wallets juegan un papel central, funcionando como el puente entre los usuarios y sus criptomonedas. Dependiendo de sus características y la tecnología que emplean, estas wallets pueden clasificarse en diferentes categorías, cada una adaptada a necesidades específicas de seguridad, accesibilidad y control. En esta sección exploraremos las diferencias fundamentales entre wallets frías y calientes, centralizadas y descentralizadas, así como las particularidades de las wallets diseñadas específicamente para Bitcoin y aquellas que integran soluciones de la Lightning Network.

Wallets Frías (Cold Wallets) vs. Wallets Calientes (Hot Wallets)

La principal distinción entre wallets frías y calientes se refiere a su conexión con Internet. Las wallets frías son dispositivos o medios de almacenamiento que mantienen las claves privadas de las criptomonedas fuera de línea, lo que las hace inmunes a ataques cibernéticos y a robos online. coin y aquellas que integran soluciones de la Lightning Network.

Estas incluyen hardware wallets, como dispositivos USB específicamente diseñados para este fin, y paper wallets, que son simplemente impresiones físicas de las claves privadas. Por su naturaleza, las wallets frías son ideales para el almacenamiento a largo plazo de cantidades significativas de criptomonedas.

En contraste, las wallets calientes están conectadas a Internet, lo que facilita el acceso rápido y la gestión de las criptomonedas para operaciones diarias. Sin embargo, esta conveniencia viene con un riesgo aumentado de seguridad, ya que están más expuestas a ataques informáticos. Las wallets calientes incluyen aplicaciones de software en computadoras y dispositivos móviles, así como wallets en línea.

Wallets Centralizadas (Custodial) vs. Wallets Descentralizadas (Non-Custodial)

Otra clasificación importante es la distinción entre wallets centralizadas y descentralizadas. Las wallets centralizadas, también conocidas como custodial, son administradas por terceros, como exchanges de criptomonedas. Estas instituciones mantienen el control sobre las claves privadas y, por ende, sobre los activos de los usuarios. La ventaja principal es la simplicidad para el usuario, que no necesita gestionar directamente sus claves privadas, pero esto también implica un nivel de confianza en la entidad que las custodia.

Por otro lado, las wallets descentralizadas, o non-custodial, otorgan al usuario el control total sobre sus claves privadas y, por lo tanto, sobre sus activos. Esto elimina la necesidad de confiar en terceros para la seguridad de los fondos, pero también significa que la responsabilidad de mantener seguras las claves privadas recae completamente en el usuario.

Las wallets descentralizadas ofrecen una mayor autonomía y seguridad, en línea con la filosofía de descentralización de las criptomonedas.

Wallets Específicas para Bitcoin

Las wallets de Bitcoin están diseñadas específicamente para almacenar, enviar y recibir BTC, la criptomoneda pionera. Estas pueden ser tanto frías como calientes, y custodial o non-custodial, dependiendo de las necesidades y preferencias del usuario. La elección de una wallet de Bitcoin adecuada es crucial para la gestión segura de los activos digitales, especialmente considerando las particularidades de la blockchain de Bitcoin.

Wallets BTC + Lightning Network (LN)

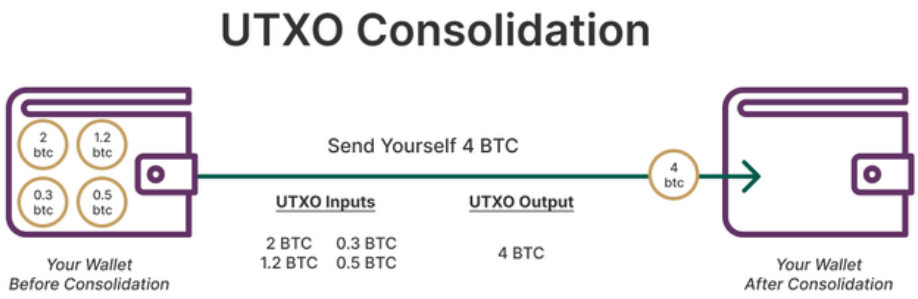
Con el crecimiento de Bitcoin, la escalabilidad se convirtió en un desafío significativo. La Lightning Network (LN) es una solución de segunda capa que facilita transacciones instantáneas y de bajo costo. Las wallets que integran LN permiten a los usuarios aprovechar las ventajas de esta red, combinando la seguridad de Bitcoin con la velocidad y eficiencia de LN. Estas wallets son particularmente útiles para quienes realizan transacciones frecuentes y de pequeño valor, ofreciendo una experiencia de usuario fluida y económica.

Elementos clave

ID	Definición	Uso
Wallet	Software que ejecuta el protocolo bitcoin; permite la comunicación con la nueva obra; genera, almacena y gestiona claves privadas.	Acceder a la red Bitcoin; construir transacciones y permitir el envío y la recepción.
Seed phrase o semilla	Frase mnemotécnica de 12 a 24 palabras utilizada para generar claves privadas en una billetera.	Generar una copia de seguridad para generar claves privadas idénticas en diferentes billeteras.
Clave privada	Genera una dirección a la que puede enviar fondos y desbloquear los fondos recibidos en esa dirección.	Demostrar la propiedad de la dirección vinculada - habilita 'Spending'
Dirección	Un identificador único al que se pueden enviar criptomonedas. Mejores prácticas de privacidad = usar una vez.	Ver el historial de transacciones del asociado.

Terminología básica a dominar: UTXO

Una UTXO, sigla en inglés para "Unspent Transaction Output" o "Salida de Transacción no Gastada", es un concepto fundamental en la red de Bitcoin y forma la base de cómo Bitcoin rastrea la propiedad y el movimiento de los fondos dentro de su sistema. Cada transacción en Bitcoin transfiere bitcoins de una dirección a otra a través de estos UTXOs, y el conjunto total de UTXOs en la red Bitcoin representa todas las monedas que están disponibles para ser gastadas.



Cómo funciona el modelo UTXO en Bitcoin:

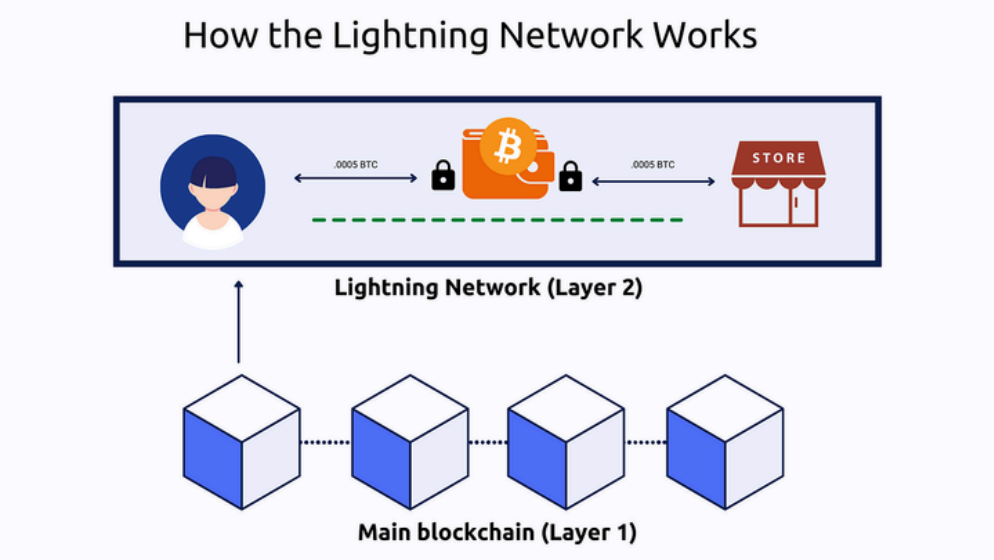
- Transacciones y Salidas: Cuando se realiza una transacción en Bitcoin, esta consume uno o varios UTXOs como entradas y crea nuevos UTXOs como salidas. Los UTXOs consumidos en una transacción son considerados "gastados" y no pueden ser usados en futuras transacciones. Las nuevas salidas generadas (nuevos UTXOs) quedan disponibles para ser gastadas en transacciones futuras.
- Propiedad de los UTXOs: Cada UTXO está asociado a una dirección específica en la red de Bitcoin, la cual es derivada de la clave pública del receptor. Solo el poseedor de la clave privada correspondiente a esa dirección puede gastar esos UTXOs en una nueva transacción, asegurando así la propiedad y seguridad de los fondos.
- No Divisibles: A diferencia de una cuenta bancaria que muestra un saldo total disponible para gastar, los UTXOs son indivisibles. Si un UTXO representa una cantidad mayor de bitcoins de lo que se desea transferir, este se debe gastar en su totalidad en una transacción, enviando el excedente (el "cambio") de vuelta a una dirección controlada por el emisor, como un nuevo UTXO.
- Cálculo de Saldo: El saldo total de bitcoins de una dirección (o de una wallet) se calcula sumando todos los UTXOs asociados a esa dirección que aún no han sido gastados. Esto significa que el "saldo" de una dirección es en realidad la suma de todas las salidas de transacciones no gastadas que puede usar.

Este sistema permite que cada transacción sea trazada y verificada desde su origen, manteniendo un registro claro y auditable de los movimientos de fondos. Además, cada UTXO solo puede ser gastado por el poseedor de la clave privada correspondiente, lo que añade una capa de seguridad robusta al sistema. Al consumir UTXOs específicos en cada transacción y generar nuevos, Bitcoin previene eficazmente el doble gasto, una preocupación clave en cualquier sistema de dinero digital. Este enfoque no solo subraya la transparencia y la seguridad en la red de Bitcoin sino que también refuerza la propiedad y el control sobre los activos digitales.

Solucionando la rapidez y de operabilidad de Bitcoin: Lightning Network

Lightning Network es una segunda capa agregada a la cadena de bloques de Bitcoin (BTC) que permite transacciones fuera de la cadena, es decir, transacciones entre partes que no están en la red de la blockchain. Múltiples canales de pago entre partes o usuarios de Bitcoin conforman la segunda capa. Un canal de Lightning Network es un método de transacción de dos partes en el que las partes pueden realizar o recibir pagos entre sí. La capa dos mejora la escalabilidad de las aplicaciones de la cadena de bloques mediante la gestión de transacciones fuera de la red principal de la blockchain (capa uno), al mismo tiempo que se beneficia del poderoso paradigma de seguridad descentralizado de la red principal.

La escalabilidad es una barrera importante que restringe la adopción generalizada de las criptomonedas. Si se escala correctamente, una red de blockchain puede manejar de millones a miles de millones de transacciones por segundo (TPS). En este contexto, Lightning Network cobra tarifas bajas al realizar transacciones y liquidaciones fuera de la cadena, lo que permite nuevos casos de uso como micropagos instantáneos que pueden resolver el enigma tradicional "¿puedes comprar café con criptomonedas?", acelerando los tiempos de procesamiento y reduciendo los gastos (costos de energía) asociados con la cadena de bloques de Bitcoin.



¿Cómo Funciona la Lightning Network?

La Lightning Network utiliza canales de pago bidireccionales que permiten a las partes realizar un número ilimitado de transacciones sin necesidad de registrar cada una de ellas en la blockchain de Bitcoin. En lugar de ello, solo se registran en la blockchain dos eventos: la apertura del canal y su cierre. Dentro de un canal, las transacciones se realizan de manera privada y casi instantánea entre las partes, con la capacidad de liquidar el saldo final en cualquier momento en la blockchain de Bitcoin.

Características Principales

- Transacciones Instantáneas: La LN permite transacciones casi instantáneas, superando los tiempos de espera de confirmación de la blockchain de Bitcoin que pueden llevar varios minutos o incluso horas.
- Bajas Tarifas: Al evitar el registro de cada transacción en la blockchain, se minimizan las tarifas asociadas, lo que hace económicamente viables las transacciones de bajo valor.
- Escalabilidad: Teóricamente, la LN puede manejar millones de transacciones por segundo, superando con creces la capacidad de la red Bitcoin original y de muchos sistemas de pago tradicionales.
- Privacidad Mejorada: Las transacciones dentro de un canal no son públicas, lo que ofrece un mayor nivel de privacidad para las partes involucradas.

Introducción a Ethereum y Smart Contracts

Ethereum emergió en el panorama de las criptomonedas como una solución innovadora a una limitación fundamental de Bitcoin: la falta de programabilidad nativa. Si bien Bitcoin revolucionó el concepto de dinero digital al introducir una moneda descentralizada segura y confiable, su enfoque se centró primordialmente en las transacciones financieras.

Este enfoque dejaba poco espacio para la expansión hacia aplicaciones más complejas directamente sobre su blockchain.

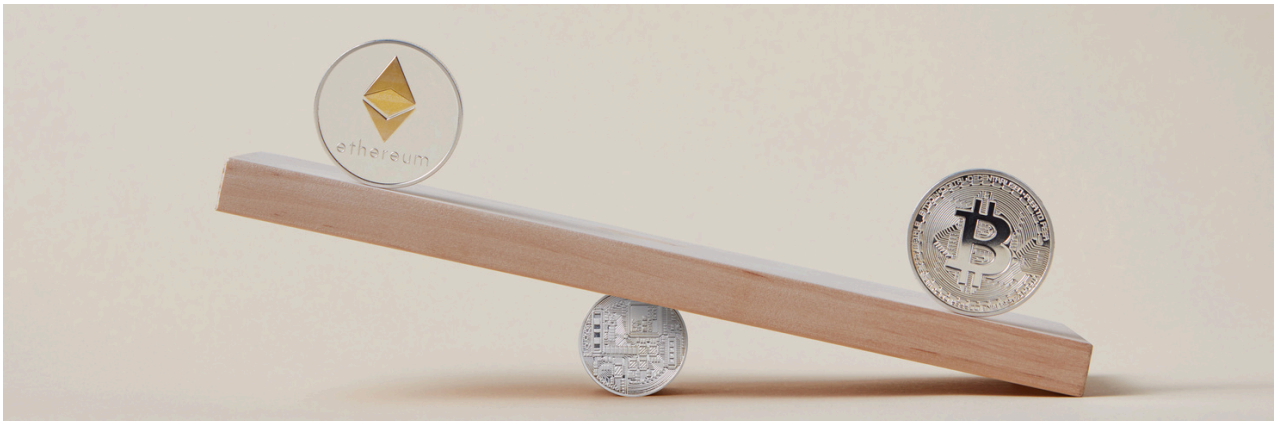
Ethereum, concebido por Vitalik Buterin y lanzado en 2015, se presentó como una plataforma versátil diseñada específicamente para superar este obstáculo, abriendo un nuevo mundo de posibilidades para el desarrollo descentralizado.

Programabilidad y Contratos Inteligentes

La principal innovación que Ethereum trae a la mesa es la introducción de los contratos inteligentes. A diferencia de Bitcoin, que requiere de scripts muy básicos para la ejecución de transacciones, Ethereum implementa una máquina virtual (Ethereum Virtual Machine, EVM) capaz de ejecutar código de programación complejo. Esto significa que en Ethereum no solo se pueden realizar transacciones de valor, sino también desplegar contratos inteligentes que se ejecutan automáticamente cuando se cumplen condiciones específicas. Estos contratos inteligentes son programas almacenados en la blockchain que pueden automatizar una amplia gama de operaciones, desde la creación de tokens hasta la ejecución de aplicaciones descentralizadas (dApps), sin necesidad de intermediarios.

Ethereum como Plataforma Descentralizada

Mientras Bitcoin fue diseñado con un enfoque estrecho en la seguridad y la simplicidad para las transacciones financieras, Ethereum apuesta por la versatilidad y la expansión de la tecnología blockchain hacia nuevos horizontes. La plataforma de Ethereum sirve como un terreno fértil para el desarrollo de aplicaciones descentralizadas (dApps), organizaciones autónomas descentralizadas (DAOs), y una multitud de otros usos que van más allá de las transacciones puramente monetarias. Esta flexibilidad ha dado lugar a una explosión de innovación en el espacio de las finanzas descentralizadas (DeFi), los tokens no fungibles (NFTs), y más allá.



Ethereum Virtual Machine (EVM):

La Ethereum Virtual Machine o EVM es el entorno de tiemo de ejecución para los contratos inteligentes en Ethereum. Funciona como una máquina virtual global descentralizada que ejecuta el código de los contratos inteligentes de manera precisa y aislada del resto de la red, garantizando así la seguridad y la integridad de la ejecución. La EVM es completamente aislada, lo que significa que el código que se ejecuta dentro de ella no tiene acceso al sistema de archivos de la red, a otros contratos inteligentes o a Internet. Esto la hace extremadamente segura, ya que evita posibles vectores de ataque malicioso.

El Gas:

El Gas es un mecanismo que mide la cantidad de esfuerzo de computación requerido para ejecutar operaciones en la red Ethereum, desde transacciones simples hasta la ejecución de contratos inteligentes complejos. Cada operación tiene un costo de Gas asignado, que debe ser pagado por el usuario que realiza la operación en Ether (la criptomoneda de Ethereum). Este sistema no solo previene el abuso de recursos (como los ataques de denegación de servicio) al hacer que los atacantes paguen potencialmente altos costos por sus acciones maliciosas, sino que también asigna recursos de la red de manera eficiente, asegurando que las operaciones con mayor prioridad se ejecuten más rápidamente.

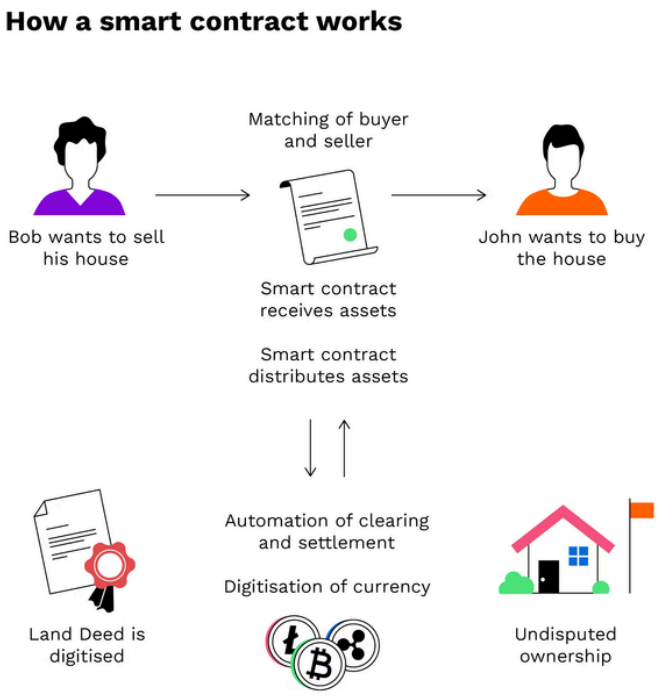
.

Contratos inteligentes:

Los contratos inteligentes de Ethereum representan una de las innovaciones más transformadoras en el campo de la tecnología blockchain, proporcionando un mecanismo para ejecutar acuerdos de manera automática, sin necesidad de intermediarios. Estos contratos son programas almacenados dentro de la blockchain de Ethereum que se ejecutan cuando se cumplen condiciones preestablecidas, revolucionando así la forma en que se realizan las transacciones digitales y se establecen los acuerdos en el mundo virtual.

¿Qué son los Contratos Inteligentes?

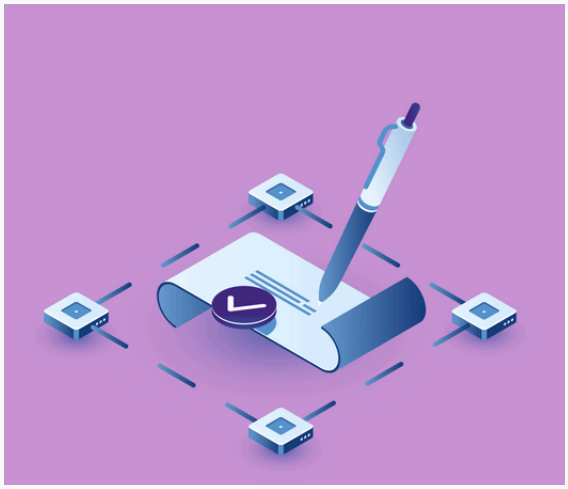
Los contratos inteligentes son fragmentos de código que se autoejecutan bajo las condiciones que las partes acuerdan previamente, escritas en su código. Una vez que se cumplen estas condiciones, las acciones programadas en el contrato se ejecutan automáticamente.



Esta capacidad de autoejecución elimina la necesidad de intermediarios o terceros para validar o facilitar las transacciones, reduciendo los costos y aumentando la eficiencia y la seguridad.

.

Funcionamiento de los Contratos Inteligentes en Ethereum



Ethereum proporciona la plataforma ideal para el desarrollo y la ejecución de contratos inteligentes a través de su Ethereum Virtual Machine (EVM). La EVM es un entorno de tiempo de ejecución completamente aislado que opera en todos los nodos de la red Ethereum, asegurando que los contratos inteligentes se ejecuten exactamente como fueron programados sin posibilidad de censura, inactividad, fraude o interferencia de terceros.

Para su ejecución, los contratos inteligentes utilizan "gas", que mide el costo computacional de las operaciones. El gas asegura que los contratos se ejecuten de manera eficiente y previene el abuso del sistema, requiriendo que los usuarios paguen por los recursos computacionales utilizados por sus transacciones y contratos.

Aplicaciones de los Contratos Inteligentes

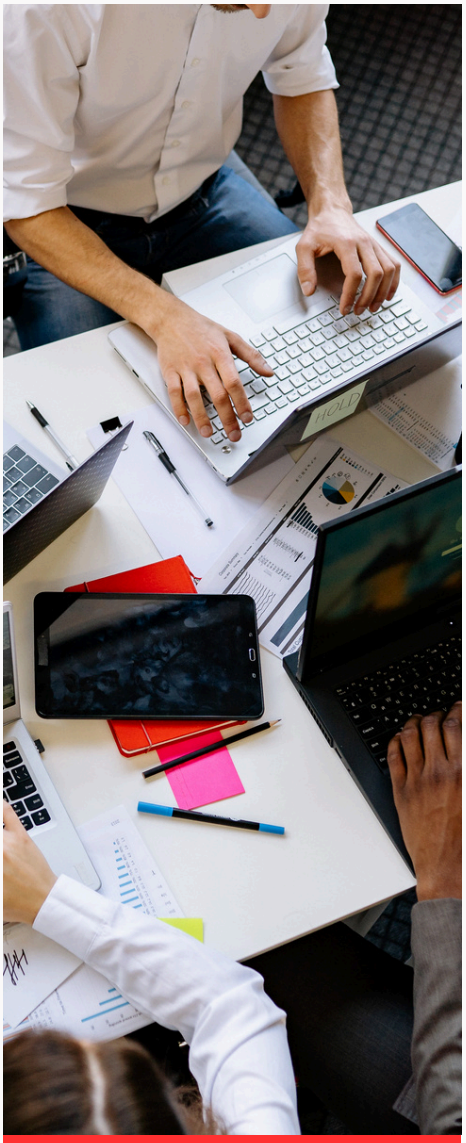
Las aplicaciones de los contratos inteligentes son vastas y variadas, abarcando desde las finanzas descentralizadas (DeFi) hasta los juegos en línea, seguros, votaciones digitales, y más. En el ámbito de las DeFi, por ejemplo, los contratos inteligentes permiten crear préstamos automáticos, intercambios descentralizados (DEX), y otras herramientas financieras sin la necesidad de bancos o instituciones financieras tradicionales.
Los contratos inteligentes también han habilitado la creación y el comercio de tokens no fungibles (NFTs), que representan la propiedad o la prueba de autenticidad de activos digitales únicos, como obras de arte digitales, coleccionables, y derechos de autor.

.

Tokens y tokenización

Los términos "token" y "criptomoneda" a menudo se utilizan, pero no siempre se entienden completamente. Sin embargo, representan conceptos fundamentales que están redefiniendo cómo concebimos el valor, la propiedad y el intercambio en el ámbito digital.

Esta sección se sumerge en la esencia de los tokens y las criptomonedas, explorando su taxonomía y, lo más importante, cómo están solucionando problemas concretos dentro del entorno empresarial.



Token: Más Allá de una Simple Moneda

Un token es la representación digital de un activo dentro de una blockchain. Este activo puede ser tangible, como bienes inmuebles o arte, o intangible, como derechos de autor o licencias. Los tokens encapsulan valor a través de un activo subyacente, lo que los diferencia de las criptomonedas tradicionales. Estos pueden ser diseñados con características y reglas específicas que rigen su uso y transferencia, lo que permite una amplia gama de aplicaciones.

Criptomoneda: La Moneda de la Blockchain

Por otro lado, una criptomoneda es, en esencia, la representación digital de una moneda dentro de una blockchain. Diseñadas primordialmente como medios de intercambio, las criptomonedas buscan replicar y mejorar las funciones de las monedas tradicionales, ofreciendo ventajas como descentralización, seguridad criptográfica y transparencia.

Soluciones Empresariales a través de Tokens

La adopción de tokens dentro de las empresas está solucionando desafíos clave, abriendo nuevas oportunidades y eficiencias:

- Liquidez: Convertir activos tradicionalmente ilíquidos en tokens facilita su comercio en mercados globales, aumentando la liquidez y el valor percibido de estos activos.
- Propiedad Fraccionada: La tokenización permite dividir la propiedad de activos costosos, como bienes raíces o arte, en fracciones más accesibles, democratizando el acceso a inversiones previamente fuera del alcance de muchos inversores.
- Reducción de Burocracia: Al automatizar acuerdos y transacciones a través de contratos inteligentes, se eliminan intermediarios y trámites burocráticos, agilizando procesos y reduciendo costos.
- Transparencia: La naturaleza inmutable de la blockchain asegura que todas las transacciones y cambios en la propiedad del token sean transparentes y verificables por todos los participantes.
- Acceso Global: Los tokens se pueden enviar o recibir instantáneamente desde cualquier parte del mundo, eliminando barreras geográficas y facilitando el acceso a mercados globales.

"Estimado alumno,

Nadie podría haber previsto hace pocos años la
que se iba a liar, ¿verdad? COVID, Ucrania, inflación galopante...

Los que confiamos en Bitcoin y Blockchain como “un instrumento de libertad” sabemos que este momento llegaría. El sistema financiero mundial está colapsando. La única solución que proponen los Bancos Centrales es inyectar más dinero al sistema, empobreciendo así [todavía más] al ciudadano... es todo de locos.

En toda esta confusión, la Tokenización empieza a coger una tracción increíble. Estamos rodeados de activos, pero pocos son líquidos. La liquidez se ha convertido en el “Santo Grial”, y aunque está en el subyacente de cualquier activo "tokenizado", comos pocos los que conocemos este nuevo Orden Mundial. Y tú tienes la increíble oportunidad de ser parte de él. Dentro de unos años todos estaremos rodeados de activos tokenizados, pero las grandes oportunidades de negocio son para los primeros, los más inquietos, los más determinados y los más persistentes.”

Miguel Caballero

CEO Tutellus

Tutellus