

INVESTIGACIÓN DE GLOBAL X ETFs

Ethereum: información básica

Nota del editor: Incluimos un glosario con todos los términos resaltados en **naranja**.

Autor:

Equipo de Activos Digitales
Investigación de Global X

Fecha: 1 de marzo de 2022

Tema: **Activos digitales**

El **bitcoin**, lanzado en 2009, fue la primera aplicación de la tecnología de **cadena de bloques** como moneda descentralizada de suministro finito que tuvo éxito. Parte de este éxito radica en su disponibilidad a cualquier persona. Bitcoin sirvió de inspiración para que los desarrolladores descubriesen herramientas y aplicaciones más amplias que aprovechan la seguridad, transparencia y escalabilidad de la tecnología de cadena de bloques. Aunque la red Bitcoin sentó la base para un medio de intercambio, un joven programador la vio como un método capaz de plantar cara a las entidades centralizadas de toda la economía.

En 2013, con tan solo 19 años, Vitalik Buterin publicó las especificaciones de Ethereum, una novedosa red de cadena de bloques de uso general que permite a los desarrolladores crear condiciones y aplicaciones programables. En esencia, Buterin creó un sistema de dinero programable que revolucionó la forma en que la gente se plantea, crea e implementa la tecnología de cadena de bloques.

Conocimientos esenciales sobre Ethereum, sus componentes clave y cómo funciona

Debido a su crecimiento y atractivo de inversión, este artículo responde a preguntas básicas sobre la red Ethereum.

- **¿Qué es Ethereum?** Una cadena de bloques descentralizada con funcionalidad de contratos inteligentes.
- **¿Qué es el ether (ETH)?** La moneda nativa de Ethereum.
- **¿Qué son los nodos?** Son equipos que ejecutan un cliente Ethereum para validar transacciones y bloques.
- **¿Cómo funciona la minería?** Los nodos especiales resuelven un problema matemático para crear el siguiente bloque de la cadena.
- **¿Cuándo se produce la verdadera liquidación de la operación?** Cuando una transacción tiene un número suficiente de confirmaciones
- **¿Qué son los contratos inteligentes y por qué son importantes?** Son contratos programables basados en condiciones predefinidas.
- **¿Qué son las aplicaciones descentralizadas (decentralized applications, DApps) y por qué son importantes?** Son aplicaciones creadas con contratos inteligentes.
- **¿Qué pasará con la red Ethereum en el futuro?** Hará una transición a un mecanismo de consenso que haga a la red más escalable y ecológica.
- **¿Por qué es valioso el ETH?** Porque dicta la economía de la red.
- **¿Por qué invertir en Ethereum ahora?** Es la cadena de bloques de contratos inteligentes más grande y con mayor adopción, por lo que ofrece potencial de valor y crecimiento.



Ethereum: una cadena de bloques con funcionalidad de contratos inteligentes

El lanzamiento de Ethereum en julio de 2015 introdujo una cadena de bloques novedosa que incorpora **lenguaje Turing completo**, un lenguaje de programación que se puede usar para integrar lógica y completar transacciones más avanzadas que un simple pago. Este lenguaje ha permitido a los desarrolladores crear e integrar aplicaciones en Ethereum, actuando como capa básica de un ecosistema abierto capaz de alojar **contratos inteligentes** y **aplicaciones descentralizadas (DApps)**.

Los contratos inteligentes comprenden gran parte de la propuesta de valor de Ethereum. Un contrato inteligente tiene criterios predefinidos que ejecutan automáticamente una respuesta basada en condiciones programadas, y el acuerdo se registra en la cadena de bloques. Los contratos inteligentes eliminan la necesidad de un tercero intermediario.

Las DApps son aplicaciones de interfaz de usuario y dirigidas al usuario creadas e implementadas a partir de la programabilidad de contratos inteligentes. Estos contratos programables se utilizan para crear **aplicaciones de servicios financieros descentralizados (decentralized finance, DeFi)** y **tokens no fungibles (non-fungible tokens, NFT)**, que representan la propiedad digital de activos únicos. Los contratos inteligentes también se utilizan para crear y coordinar entidades de gobernanza descentralizada llamadas **organizaciones autónomas descentralizadas (decentralized autonomous organizations, DAO)**. El universo de DApps dentro de la red representa el ecosistema Ethereum.

La red Ethereum utiliza la tecnología de cadena de bloques totalmente transparente para registrar **transacciones** y realizar un seguimiento de los **estados** en el libro contable. Los participantes de la red pueden obtener un estado de consenso, que implica el acuerdo con respecto al libro mayor distribuido de la cadena de bloques, al validar de forma independiente las transacciones y los **bloques** atendiendo a las reglas del protocolo. Los bloques son estructuras de datos individuales creados a partir de una lista de transacciones agregadas e incluyen una referencia a su bloque principal o anterior.

La **Ethereum Virtual Machine (EVM)**, que es la máquina de estados distribuidos de Ethereum, es responsable de mantener la estructura y los estándares de datos de la red. En esencia, la EVM define las reglas para calcular un cambio de estado entre bloques. Un cambio de estado podría ser un simple cambio en el saldo de una cuenta, o podría ser el resultado de una interacción más compleja relativa a un contrato inteligente.

Ether (ETH): la criptomoneda nativa de la red Ethereum

El ether (ETH) se puede utilizar para enviar pagos simples, de forma similar al bitcoin, pero es más parecido a una materia prima que a una moneda porque se utiliza principalmente para pagar la computación descentralizada en Ethereum. Todas las transacciones y la implementación de contratos inteligentes en Ethereum cuestan una tarifa variable a pagar en ETH. Un pago simple suele ser más barato que una interacción de contrato inteligente. Este sistema de pago crea una demanda natural de ETH, ya que los usuarios finales de DApps de Ethereum deben comprar ETH para interactuar con la plataforma.



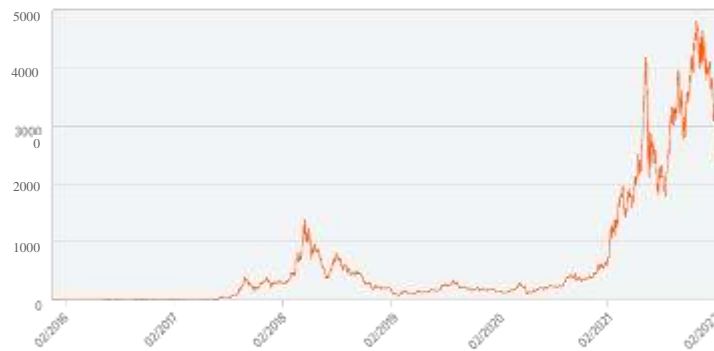
El ETH no tiene representación física: es un activo digital al portador que le pertenece a quien tenga la clave privada correspondiente. Al igual que Bitcoin, Ethereum utiliza **criptografía de clave pública** y **firmas digitales** para evitar que personas malintencionadas gasten los ETH de otra persona. Para profundizar en la criptografía de clave pública y las firmas digitales, consulte **Bitcoin: información básica**.

ETH comenzó a venderse el 2 de septiembre de 2014, con un precio de 2000 ETH por bitcoin (BTC). Actualmente, el ETH es la segunda criptomoneda más importante y tiene una capitalización total de mercado de 356 000 millones de USD.¹

PRECIO ACTUAL DEL ETHER (ETH) Fuente: Etherscan.io al 1 de marzo de 2022.

PRECIO ACTUAL DEL ETHER (ETH)

Fuente: Etherscan.io al 1 de marzo de 2022.



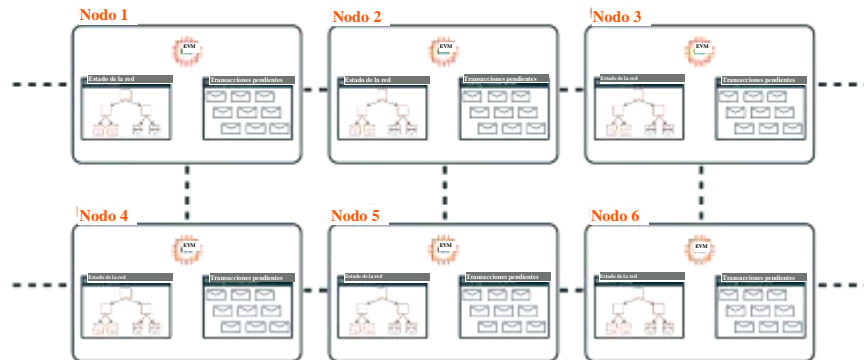
Nodos: las computadoras que validan las transacciones y protegen la red

Los **nodos** son las computadoras de la red Ethereum que ejecutan un **cliente Ethereum**. Un cliente Ethereum es el software que implementa el protocolo Ethereum, es decir, las reglas de la red. La red Ethereum es una acumulación de nodos conectados, cada uno de los cuales verifica que las transacciones y los bloques recibidos son válidos de conformidad con las reglas del protocolo antes de añadirlos a la cadena de bloques.



LA RED INTERCONECTADA DE NODOS

Fuente: Global X ETFs



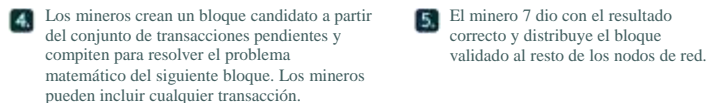
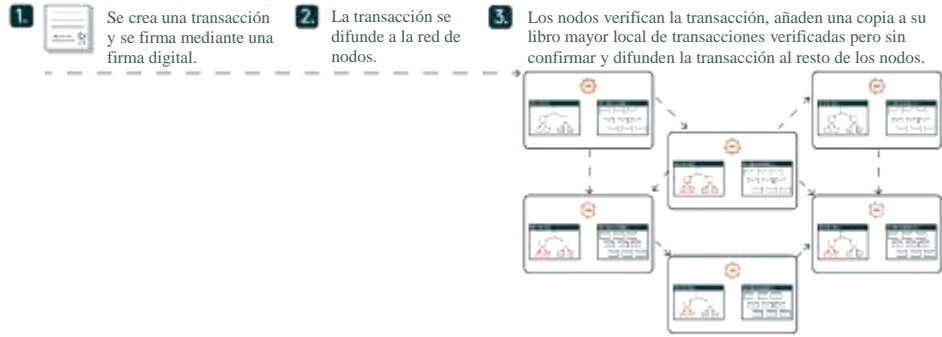
Las transacciones alteran el estado de los datos dentro de la red, y generalmente implican la transferencia de activos digitales o la ejecución de contratos inteligentes. Todas las transacciones deben incluir una tarifa por transacción denominada en ETH, conocida como **comisión de gas**, que representa el costo de publicación, validación, ejecución y almacenamiento de la transacción en la cadena de bloques.

Cuando un usuario firma digitalmente una transacción con la clave privada, dicha transacción se transmite a la red de nodos conectados. A continuación, cuando un nodo recibe la nueva transacción, el cliente Ethereum verifica de forma independiente la validez de esta transacción con respecto a un conjunto completo de criterios descritos en las reglas del protocolo, lo que incluye una evaluación de la firma digital. Si la transacción es válida, el nodo guarda la transacción en su conjunto local de transacciones pendientes y la difunde a todos sus nodos vecinos. Esta red de nodos interconectados permite que las transacciones sean distribuidas, validadas y registradas por todos los participantes en cuestión de segundos.



ANALICEMOS UNA TRANSACCIÓN DE ETHEREUM

Fuente: Global X ETFs



Nodos de minería: nodos especiales que resuelven un problema matemático para crear el siguiente bloque

Todos los nodos de Ethereum verifican las transacciones de forma independiente, pero los **nodos de minería**, o mineros, son un tipo especial que añaden transacciones a los bloques que se registran en la cadena de bloques para su liquidación. En ese sentido, los nodos de minería son distintos porque crean bloques de transacciones en la cadena.

Cada nodo mantiene un conjunto de transacciones verificadas pero pendientes conocido como “la mempool”. Las transacciones se eliminan de la mempool cuando un minero las incluye en un bloque minado. Los nodos de minería emplean una gran cantidad de recursos informáticos en una competencia para ser los primeros en resolver un desafiante problema matemático. La solución al problema se conoce como **prueba de trabajo**, el mecanismo de consenso que garantiza la integridad de la red.



El problema se resuelve mediante el cálculo por fuerza bruta, que implica que los mineros iteran diferentes entradas en una **función hash criptográfica** en busca de un resultado inusual o **hash**. Ethereum se basa en una función hash criptográfica diferente a la de Bitcoin, y los mineros no compiten directamente entre sí. La prueba de trabajo es difícil de obtener, pero cualquier nodo puede verificar de manera trivial que el minero empleó los recursos informáticos para encontrar la solución. Del mismo modo que una transacción solo se considera válida si tiene una firma digital válida, un bloque candidato requiere una prueba de trabajo para convertirse en un bloque válido. Obtener el resultado particular a través de la prueba de trabajo antes que los demás participantes permite al minero validar, registrar y difundir el bloque candidato.

Una vez que un minero se convierte en el primer participante en resolver el problema matemático del siguiente bloque, difunde el bloque validado a la red. Cada nodo verifica la validez del bloque recién recibido y, a continuación, lo añade a su copia de la cadena de bloques. La recepción de un nuevo bloque válido reinicia el juego de minería. Todos los mineros crean un nuevo bloque candidato de transacciones e intentan ser los primeros en resolver el problema del siguiente bloque que se incluirá en la cadena de bloques. Los **tiempos de creación de bloques**, que suelen ser de entre 12 y 14 segundos, dictan este flujo constante de nuevos bloques. Además, el **tamaño del bloque** es limitado y no todas las transacciones pendientes se incluyen en un bloque.

Se incentiva económicamente a los mineros a ser los primeros en resolver este problema. El primer minero que envíe un nuevo bloque con una prueba de trabajo válida puede reclamar 2 ETH como **recompensa por bloque** y una parte de las comisiones de gas de ese bloque. Además, al establecer el orden de las transacciones en sus bloques y mediante tácticas de **inversión ventajista**, los mineros pueden generar un flujo de ingresos incremental conocido como **valor extraíble del minero (miner extractable value, MEV)**.

Las comisiones de gas en un bloque pueden dividirse en una tarifa base y una propina, cuyos precios fluctúan según la demanda de espacio en el bloque. La propina se paga directamente al minero como incentivo por priorizar la inclusión de una transacción en un bloque. La tarifa base se asemeja a una recompra de acciones, ya que se quema y el ETH correspondiente se elimina del suministro circulante.

Las **propuestas de mejora de Ethereum (Ethereum Improvement Proposals, EIP)** están diseñadas para incentivar a los participantes y constructores de la red a mejorar constantemente la red Ethereum. Una de las propuestas fue esta estructura de comisiones de gas. Implementada en agosto de 2021 a través de la propuesta de mejora de Ethereum 1559 (EIP-1559), creó una correlación directa entre el uso de la red y la emisión de ETH.

La EIP-1559 crea valor para los tenedores de ETH porque el mecanismo de quema reduce la tasa de emisión neta de suministro. A medida que se realizan más transacciones **en la cadena**, se quema más gas, lo que tiene el potencial de reducir o eliminar el impacto del suministro de nuevos ETH creados a partir de recompensas por bloque. Si la demanda de la red es alta y el mecanismo de quema supera la nueva emisión derivada de recompensas por bloque, ETH puede convertirse en un activo deflacionario. Desde la implementación de la EIP-1559 hasta la fecha, se han quemado más de 1,9 millones de ETH, lo que ha reducido la emisión neta de ETH en más de un 68 %.²

El aumento de la popularidad de los NFT y el volumen de transacciones que generan ha creado más demanda de espacio en bloques, lo que aumenta la cantidad de ETH que se queman. OpenSea, un mercado de NFT, ha sido el mayor contribuyente a las comisiones de gas quemadas desde la implementación de la EIP-1559, con un total de 230 041 ETH.³



EL EFECTO DE LA QUEMA EN LA TASA DE EMISIÓN DESDE EL INICIO

Fuente: Etherscan.io al 1 de marzo de 2022.



Liquidación verdadera: cuando una transacción tiene un número suficiente de confirmaciones

Se suele decir que una transacción está liquidada cuando está incluida en un bloque. Pero dado que ciertos escenarios pueden provocar que la cadena de bloques se bifurque temporalmente y se reorganice en el corto plazo, ciertas condiciones deben cumplirse para que ocurra una verdadera liquidación.

La verdadera liquidación ocurre después de que se reciba un número suficiente de **confirmaciones**, lo que implica que se añadan bloques a la cadena por encima del bloque que incluye una transacción específica. Dado que los bloques están vinculados y cada bloque recién minado hace referencia al hash del bloque anterior, las transacciones se vuelven más seguras e inmutables a medida que aumenta el número de bloques que se encuentran por encima. Para dar contexto, las plataformas de intercambio centralizadas populares suelen considerar que una transacción es válida después de que se registran de 20 a 50 confirmaciones, algo que debería llevar solo unos minutos dados los tiempos de creación de bloques de Ethereum.

Si una persona malintencionada quisiera revertir una transacción, necesitaría volver al bloque que contiene la transacción que desea manipular. Por lo tanto, si dicha transacción tuviera 50 confirmaciones, tendría que retroceder 50 bloques. Y luego tendría que volver a minar ese bloque y los bloques subsiguientes en una **cadena bifurcada** y obtener una prueba de trabajo válida para cada uno de estos bloques. Al mismo tiempo, los participantes que siguen las reglas del protocolo estarán minando y ampliando la **cadena principal**, que es la cadena con mayor acumulación de trabajo de minería.

Para superar el déficit de bloques con respecto a la cadena principal, la persona malintencionada tendría que controlar más del 50 % del poder computacional total de la red durante un período suficiente de tiempo. Además, esta persona se enfrentaría a un riesgo considerable porque, si fallara, malgastaría su electricidad sin ninguna recompensa de ETH.



Contratos inteligentes: la infraestructura programable para DApps

Los contratos inteligentes ofrecen la capacidad de programar programas y acuerdos de ejecución automática en Ethereum a través de lenguajes de programación específicos que cumplen con los estándares de la EVM. Los desarrolladores pueden usar Solidity, un lenguaje de programación patentado que se creó para facilitarles a los participantes menos especializados el acceso a las herramientas de programación. Los desarrolladores también pueden utilizar lenguajes más avanzados como Vyper y Yul.

Dicho de otro modo, los contratos inteligentes son contratos ejecutados mediante programación basados en código. Las fuentes de datos, condiciones, reglas y acuerdos integrados en el contrato activan automáticamente un resultado predefinido sin necesidad de un intermediario de confianza que ejecute el contrato. Cualquier aplicación descentralizada puede implementar un contrato inteligente e incorporar funcionalidades, como permutas de activos o primitivas de préstamos.

Los contratos inteligentes de Ethereum se activan e implementan al enviar el contrato como una transacción. También tienen saldos en ETH que pueden iniciar transacciones en la red una vez que se cumplen las condiciones del contrato. Dado que es una red de código abierto, hay disponible un repositorio de contratos inteligentes implementados que los desarrolladores pueden consultar, lo que mejora la componibilidad del desarrollo de aplicaciones.

Los contratos inteligentes a menudo incorporan fuentes de datos del mundo real como variables de entrada para determinar el resultado. Las entidades que facilitan la conexión e interoperabilidad entre las cadenas de bloques y los sistemas externos se denominan oráculos u Oracles. Los oráculos permiten que los contratos inteligentes se ejecuten con base en datos de entrada que no están disponibles de forma nativa en la cadena de bloques. Algunos ejemplos comunes incluyen datos de precios, datos meteorológicos, resultados electorales, lecturas de sensores de Internet de las cosas (Internet of Things, IoT), verificación de ID para estándares de confianza a su cliente (know your customer, KYC) y funciones aleatorias verificables.

Dado que los datos proporcionados por oráculos pueden determinar el resultado de muchos contratos inteligentes, permitir que una entidad centralizada proporcione esta información sería contrario al propósito de usar una cadena de bloques sin confianza. Chainlink es un buen ejemplo de una red oráculo descentralizada diseñada para resolver este problema. Se basa en una red de nodos de oráculos independientes que reciben incentivo económico por ofrecer datos precisos del mundo real de forma no confiable en la cadena.

DApps: aplicaciones creadas con contratos inteligentes

Los contratos inteligentes permiten a las aplicaciones descentralizadas crear protocolos con diversos casos de uso y reglas. Las DApps utilizan la cadena de bloques de Ethereum para almacenar datos y mantenerlos seguros, y utilizan tecnología de contratos inteligentes para la lógica de aplicaciones. En esencia, una DApp es parecida a una aplicación habitual en cuanto a que tiene una interfaz de usuario alojada en la web, pero su funcionamiento operativo lo facilita un contrato inteligente que se ejecuta en una red descentralizada de computadoras.



Esta función aporta resiliencia a las DApps porque la ejecución del código no depende de un proveedor de nube centralizado. La red Ethereum ofrece una gama de DApps, incluidas aplicaciones financieras, estructuras de gobernanza, proyectos de gestión de la cadena de suministro, almacenamiento de archivos e iniciativas de tokenización no fungible.

Las aplicaciones de servicios financieros descentralizados son prominentes dentro del ecosistema de DApps de Ethereum. Algunos de estos protocolos DeFi cuentan con tokens nativos y muchas de las principales aplicaciones DeFi cumplen con los estándares ERC-20. Las monedas estables populares, como USDT, USDC y DAI, también utilizan estándares ERC-20. Los estándares ERC-20 permiten a los desarrolladores crear tokens fungibles e interoperables siguiendo las mismas pautas y marco de compatibilidad, lo que crea condiciones óptimas para la comonibilidad de contratos inteligentes y aplicaciones.

Las aplicaciones DeFi descentralizan muchas transacciones financieras tradicionales, como los préstamos, las permutas de activos, los derivados, los seguros y la gestión de activos. Dos de las aplicaciones más populares actualmente son Uniswap y Aave. Uniswap es un creador de mercado automatizado descentralizado, de código abierto y sin custodia que proporciona pools de liquidez para compradores y vendedores que buscan intercambiar activos. Uniswap permite a las personas actuar como creadores de mercado al depositar liquidez en pools de negociación y obtener comisiones de transacción sobre las operaciones de los usuarios frente a su liquidez. En enero de 2022, los pools de liquidez de Uniswap negociaron aproximadamente 58 000 millones de USD en volumen.⁴ Aave es un mercado de liquidez y dinero descentralizado y sin custodia para préstamos de activos digitales. Por ejemplo, un participante en el mercado puede utilizar Aave para obtener un préstamo instantáneo respaldado por activos sobre sus activos digitales.

Otra aplicación de contrato inteligente popular incluye un estándar de token Ethereum alternativo. ERC-721 estandariza la creación de tokens no fungibles. Los NFT son tokens no intercambiables que no se pueden replicar, lo que significa que no hay dos tokens iguales. Hasta la fecha, el arte digital es el caso de uso predominante para los NFT. Pero dado su amplio alcance potencial, esperamos que surjan más aplicaciones creativas de NFT en áreas como juegos para ganar dinero (play-to-earn), la tokenización de bienes raíces, la emisión de tiques, las experiencias, las etiquetas de identidad, el acceso exclusivo, las membresías y las marcas de tiempo en las cadenas de suministro.

Las organizaciones autónomas descentralizadas (decentralized autonomous organizations, DAO) en la cadena también utilizan la infraestructura de cadena de bloques y la tecnología de contratos inteligentes de Ethereum para los derechos de voto y la toma de decisiones. Entre los casos de uso populares se incluyen las DAO DeFi, en las que los participantes pueden intercambiar activos digitales por tokens de gobernanza. Los titulares de tokens pueden votar en relación con la asignación de activos y las decisiones de inversión de la tesorería de los activos acumulados, y puede que las recompensas de dichas asignaciones se paguen a los titulares de tokens.

Qué pasará con la red Ethereum en el futuro: actualizaciones que facilitan la escalabilidad

Teniendo en cuenta el crecimiento de la red Ethereum, los desarrolladores han acordado una hoja de ruta con varias actualizaciones. Estas actualizaciones incluyen un cambio en el mecanismo de consenso en un intento por hacer que la red sea más escalable y ecológica.

Cambio de la prueba de trabajo a la prueba de participación



Anteriormente conocida como Ethereum 2.0, la capa de consenso de Ethereum es la hoja de ruta actualizada de Ethereum que incluye cambios en la red a medida que avanza en su transición a un nuevo estado. Esta actualización permite una mejor escalabilidad y necesidades de hardware y energía más modestas.

La prueba de trabajo proporciona sólidas garantías de seguridad, pero requiere una cantidad significativa de hardware y energía. En comparación, la **prueba de participación** requiere mucha menos energía. Los **validadores** en un consenso de prueba de participación son análogos a los mineros en un consenso de prueba de trabajo. Los validadores son responsables de ordenar transacciones, crear nuevos bloques y certificar los bloques que otros validadores crean.

En lugar de usar electricidad para evitar la manipulación de la red, la prueba de participación requiere que los validadores depositen ETH como garantía para proteger la red. Al depositar sus activos, los validadores saben que estos serán incautados si actúan malintencionadamente o no cumplen con sus responsabilidades, un proceso conocido como **slashing**. El riesgo del **slashing** incentiva a los validadores a adherirse a las reglas del protocolo y actuar en el mejor interés de la red. Para convertirse en validador, los participantes del mercado deben tener 32 ETH. Los participantes del mercado más pequeños pueden participar en pools de **staking** líquidos a través de plataformas como Lido, agregando cantidades más pequeñas de ETH en incrementos de 32 ETH y dividiendo las recompensas según corresponda.

Los validadores se pueden dividir en dos categorías: **proponentes** y **certificadores**. Los proponentes se eligen al azar del conjunto de validadores para proponer el siguiente bloque en la cadena. Los validadores que no sean elegidos como proponentes deben certificar la propuesta. Los certificadores revisan el bloque propuesto y certifican que es válido según las reglas del protocolo. Por su participación, se incentiva con recompensas en ETH a los proponentes y a los certificadores. Sin embargo, sus activos en **stake** están en riesgo si actúan malintencionadamente o no cumplen con sus responsabilidades. Un comportamiento explícitamente malintencionado o una colusión deliberada tendrán como consecuencia la pérdida total de su **stake**. Actos menos malintencionados, como no validar debido a una interrupción del servidor, pueden dar lugar a que solo se deduzca un pequeño porcentaje del **stake**.

Soluciones de escalabilidad utilizadas para Ethereum

La red Ethereum tiene limitaciones de capacidad debido a que su creciente base de usuarios interactúa con un número creciente de DApps. La mayor demanda y el limitado espacio en bloques de Ethereum ha aumentado la volatilidad de los precios del gas en los últimos años y ha hecho que la red sea demasiado cara para todos los participantes, excepto los más grandes del mercado.

Las comisiones de gas de Ethereum están denominadas en **Gwei**, que representa una milmillonésima de un ETH. Las exorbitantes comisiones de gas han llevado a los usuarios a buscar métodos alternativos de capacidad y reducción de costos.



LA ALTA DEMANDA CONDUCE A LA VOLATILIDAD DE LOS PRECIOS DEL GAS

Fuente: Etherscan.io al 1 de marzo



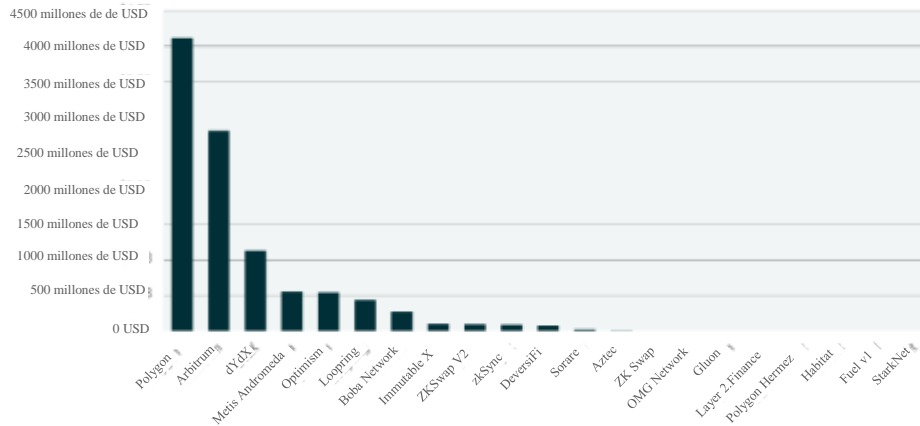
EIP-1559 ofrece una mejor estructura de precios con más previsibilidad de precios del gas, pero no garantiza que los precios del gas disminuyan. En la actualidad, las soluciones rentables de escalabilidad utilizadas para Ethereum incluyen escalabilidad en la cadena y fuera de ella. La escalabilidad en la cadena implica encontrar métodos que mejoren el costo y el rendimiento en la capa básica de Ethereum. Por ejemplo, como parte de la implementación de la capa de consenso de Ethereum, la red Ethereum planea introducir cadenas de fragmentos. Las cadenas de fragmentos se refieren al proceso de dividir horizontalmente una base de datos en varias secciones para reducir la congestión de la red y aumentar el número de transacciones por segundo. Se requiere la implementación de la prueba de participación para la fragmentación. En un sistema de prueba de trabajo, la fragmentación diluiría las propiedades de seguridad y permitiría a los mineros malintencionados corromper los fragmentos individuales más fácilmente.

La escalabilidad fuera de la cadena tiene como objetivo crear protocolos de escalabilidad alternativos además de Ethereum, que se denomina capa 1 (C1). Las soluciones implementadas fuera de Ethereum se denominan capa 2 (C2). Las capas 2 obtienen en última instancia seguridad de la *mainnet*, la red principal de Ethereum. Estas aplicaciones generalmente procesan transacciones individuales en un estado separado y se comunican de varias maneras con la *mainnet* de Ethereum para su liquidación, dependiendo del tipo de solución.

Las soluciones de C2 son cada vez más populares porque pueden ayudar a procesar pequeñas transacciones de forma más rápida y barata mientras utilizan la *mainnet* de Ethereum para obtener seguridad y transparencia. Polygon, que ayuda a los desarrolladores a crear DApps escalables con tarifas de transacción mínimas, es una de las soluciones de C2 predominantes. Las plataformas de contratos inteligentes de la competencia, como Solana, han tenido éxito intercambiando un grado de descentralización por una mejora del rendimiento de las transacciones; sin embargo, las soluciones de C2 ofrecen una forma económica de realizar transacciones mientras permanecen en el ecosistema de Ethereum. Las C2 tienen una cantidad considerable de valor total bloqueado (total value locked, TVL), que es el valor total de los criptoactivos en sus plataformas.



EL ECOSISTEMA DE SOLUCIONES DE CAPA 2 TIENE UN VALOR TOTAL BLOQUEADO DE 10 000 MILLONES DE USD
Fuente: DeFillama.com & L2beal al 1 de marzo de 2022



Valor del ETH: fomenta una economía orientada al crecimiento para la red

Como moneda de liquidación, el ETH obtiene su valor de la demanda de la red Ethereum. El ETH se utiliza comúnmente para:

- Pagar las comisiones de gas o por transacción.
- Interactuar con DApps DeFi.
- Pagar por la implementación de contratos inteligentes en la cadena de bloques.
- Unidad de cuenta principal en mercados y operaciones de NFT.

Con unos 114 000 millones de USD, Ethereum lidera el panorama de las criptomonedas en valor total bloqueado dentro de DApps.⁵ En DeFi, el valor total bloqueado es una métrica importante porque proporciona información sobre el valor monetario depositado en las aplicaciones y sirve como indicador fiable de la confianza y el crecimiento. El bloqueo de activos dentro de los protocolos indica crecimiento, utilidad y confianza del usuario en el ecosistema. Además, aproximadamente 9,7 millones de ETH, el equivalente a unos 28 000 millones de USD, está bloqueado por el contrato de prueba de participación del validador para asegurar la red en su estado futuro, reduciendo aún más la cantidad de ETH en circulación.⁶

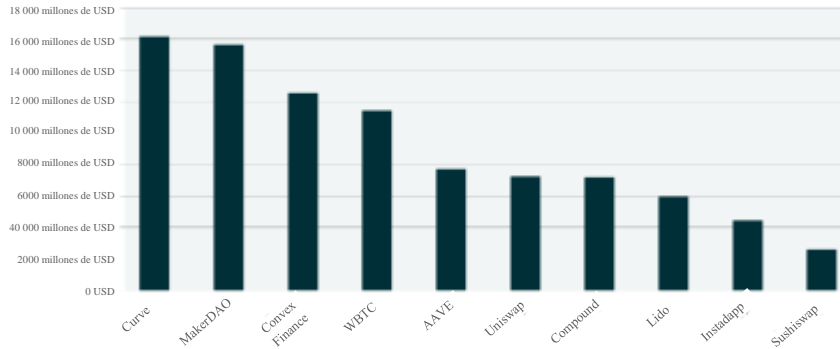


ETHEREUM LIDERA LA CARRERA EN EL VALOR TOTAL BLOQUEADO DE 211 000 MILLONES DE USD EN DEFI
Fuente: Defillama.com al 1 de marzo de 2022



Lo mejor de Ethereum es que el valor total bloqueado se distribuye entre muchas DApps DeFi.

DESGLOSE DE LOS 10 PRINCIPALES CONTRIBUYENTES AL VALOR TOTAL BLOQUEADO DE 114 000 MILLONES DE USD DE ETHEREUM EN DAPPS DE CONTRATOS INTELIGENTES
Fuente de datos: Defillama.com al 1 de marzo



Además, las métricas en la cadena, como el número de monederos y el número de transacciones diarias, han aumentado con el tiempo, lo que indica mayor demanda del ecosistema Ethereum. El número de transacciones se correlaciona directamente con las tarifas de transacción pagadas.



TOTAL DE TRANSACCIONES DE ETHEREUM POR DÍA

Fuente: Etherscan.io al 1 de marzo de 2022.



En 2021, Ethereum generó 9900 millones de USD en ingresos a través de las tarifas de transacción pagadas por los usuarios y el volumen de transacciones de ETH alcanzó los 11,5 billones de USD.⁷

LOS INGRESOS POR TRANSACCIONES CONTINUÁN CRECIENDO EN UNA BASE ANUALIZADA

Fuente de datos: Tokenterminal.com al 1 de marzo de 2022



En teoría, el suministro de ETH es ilimitado porque no hay límites en cuando a la cantidad de monedas que pueden entrar en circulación en forma de recompensas por bloque. EIP-1559 alteró la política monetaria del ETH porque permite una tasa variable de emisión de recompensas por bloque. La tasa variable es posible debido al efecto que tiene el volumen de transacciones en la cantidad de ETH eliminada de la circulación.

Con el mecanismo de quema, la tasa variable de emisión puede disminuir a medida que aumenta la demanda de la red, y puede hacer que la flotación del token disminuya a medida que la demanda de transacciones continúa aumentando. El impacto del mecanismo de quema en las comisiones de gas y la emisión anual se suma a la escasez de ETH.

La emisión anual actual de la red Ethereum es de aproximadamente el 4,5 %, con 2 ETH como recompensa por bloque.⁸ Con el tiempo, la curva de recompensa por bloques puede continuar disminuyendo en la transición a una versión mejorada y más escalable de Ethereum.



Por qué invertir en Ethereum: una cadena de bloques de contratos inteligentes con mecanismos para crear valor y escalabilidad

Comprender el creciente atractivo y valor de Ethereum es reconocer lo que Buterin articuló en sus especificaciones: el potencial de expandir las propiedades descentralizadas de la cadena de bloques mediante programación. Para los inversores interesados en la exposición a Ethereum, la primera aplicación exitosa de una cadena de bloques programable, esperamos que:

- el valor bloqueado dentro de su ecosistema, la utilidad e interoperabilidad de tokens y contratos inteligentes, y el creciente número de transacciones y su efecto en la quema de ETH puedan seguir impulsando el valor;
- las actualizaciones como la transición a la prueba de participación y los avances de escalabilidad en la cadena y fuera de ella, incluida la implementación de la capa de consenso de Ethereum y la mejora en las aplicaciones de capa 2, proporcionen escalabilidad a Ethereum. Estas actualizaciones también atraerán a más desarrolladores a este ecosistema en crecimiento debido a su efecto de red, lo que aumentará aún más la demanda de la utilidad de ETH.

Las características adaptativas de Ethereum también la posicionan bien para desempeñar un papel central en movimientos disruptivos como la evolución de Internet a la web 3.0, que en esencia es un ecosistema de cadena de bloques propiedad del usuario. Teniendo en cuenta avances como estos y la demanda que podrían crear para ETH, consideramos que este activo digital y la red de cadena de bloques que respalda tienen un potencial de crecimiento significativo.

Notas al pie:

1. CoinMarketCap. (1 de marzo de 2022). *Instantánea histórica: 1 de marzo de 2022*.
2. Watch the Burn. (1 de marzo de 2022). *Blocks*.
3. Ultrasound.money. (1 de marzo de 2022). *Ultra sound awakening: Track ETH become ultra sound*.
4. Uniswap. (1 de marzo de 2022). *Ethereum: Overview*.
5. DeFi Llama. (1 de marzo de 2022). *DeFi TVL rankings: Ethereum*.
6. Etherscan. (1 de marzo de 2022). *Contract: 0x00000000219ab540356cBB839Cbe05303d7705Fa*.
7. Token Terminal. (1 de marzo de 2022). *Projects: Ethereum*.
8. EthHub. (sin fecha) *Ethereum basics: Monetary policy*.
9. Hotchkiss, G. I. (19 de diciembre de 2019). *The 1.x files: The state of stateless Ethereum. Ethereum Foundation Blog*.
10. Agarwal, A., Smith, C., Wackerow, P., Samani, Q., Joshua, Leung, N. H., Singh, H. y Richard, S. (4 de febrero de 2022). *Miner extractable value (MEV). Ethereum*.



Glosario

Los términos se enumeran en el orden en que aparecen.

Bitcoin: un activo digital al portador que existe completamente como saldo contable en la cadena de bloques de Bitcoin. Es la criptomoneda nativa de la red Bitcoin.

Cadena de bloques: un libro contable distribuido, compartido y de conciliación constante entre pares que facilita el registro de las transacciones y el seguimiento de los activos sin necesidad de un intermediario de confianza.

Lenguaje Turing completo: lenguaje de programación que puede realizar cualquier operación computacional.

Contratos inteligentes: contratos basados en código ejecutados mediante programación.

Aplicaciones descentralizadas (DApps): aplicaciones descentralizadas desarrolladas sobre la base de contratos inteligentes respaldados por tecnología de cadena de bloques.

Aplicaciones de servicios financieros descentralizados (DeFi): las DApps ofrecen instrumentos financieros sin necesidad de intermediarios. Las DApps DeFi están respaldadas por contratos inteligentes. DeFi permite a los usuarios participar en actividades del mercado monetario, como préstamos, a través de vías descentralizadas.

Tokens no fungibles (NFT): activos no intercambiables y de identificación única.

Organizaciones autónomas descentralizadas (DAO): organizaciones descentralizadas cuyas reglas y autoridad se determinan en un contrato inteligente.

Transacciones: un paquete de datos firmado que almacena un mensaje que se enviará desde una cuenta de propiedad externa. Las transacciones representan instrucciones firmadas criptográficamente. Una transacción puede considerarse como la transferencia de activos digitales disponibles a otra dirección y la publicación o ejecución de un contrato inteligente.

Estados: describe el estado actual de todas las cuentas y saldos, así como de los datos de los contratos inteligentes.

Bloques: estructuras de datos dentro de la red Ethereum que contienen detalles de transacciones. Cada nuevo bloque creado contiene una referencia a su bloque principal o anterior.

Máquina virtual Ethereum (EVM): la plataforma subyacente utilizada por los desarrolladores para crear DApps y alojar cuentas y contratos inteligentes. La EVM almacena los datos de la red y mantiene actualizado el estado de la red.

Firma digital: obtenida matemáticamente a partir de una clave privada y el hash de una transacción. Una firma digital prueba que una persona es propietaria de una clave privada y la clave pública asociada sin tener que revelar la clave privada.

Criptografía de clave pública: también conocida como criptografía asimétrica, utiliza dos claves distintas pero conectadas matemáticamente, una para el cifrado y otra para el descifrado; la clave pública se utiliza para recibir ETH y la clave privada se utiliza para firmar transacciones de gasto de ETH.

Nodos: red distribuida de computadoras que ejecutan el software de la red Ethereum para verificar transacciones y mensajes antes de que entren en la cadena de bloques. Hay diferentes tipos de nodos.

Cliente de Ethereum: la aplicación necesaria para ejecutar un nodo completo. Básicamente, los nodos ejecutan software del cliente, que está disponible en múltiples lenguajes de codificación de



código abierto. El objetivo del cliente es actuar como el software que verifica las transacciones en relación con los estándares de la red.

Comisión de gas: las transacciones en la red Ethereum tienen un costo. Las comisiones de gas representan la cantidad de ether que se paga para validar, incluir y proteger transacciones en la cadena de bloques. Las comisiones de gas están denominadas en Gwei, y el gas necesario para procesar una transacción generalmente se basa en la demanda de la red.

Nodos de minería: un subconjunto especial de nodos que agregan transacciones en los bloques que se registran en la cadena de bloques para su liquidación. Los nodos de minería compiten por ser los primeros en resolver un desafiante problema matemático basado en una función hash criptográfica. Los mineros emplean grandes cantidades de recursos informáticos para calcular por fuerza bruta el resultado de diferentes entradas en una función hash criptográfica lo más rápido posible.

Función hash criptográfica: una función unidireccional que se puede utilizar para vincular datos de una longitud arbitraria a un resultado determinístico de longitud fija. Las funciones hash criptográficas incluyen estas propiedades clave: 1) Son repetibles; para cualquier entrada, el resultado (hash) es siempre el mismo. 2) Son funciones unidireccionales en las que es imposible determinar la entrada a partir de un resultado dado. 3) La naturaleza ópticamente aleatoria de la función hace imposible adaptar un resultado realizando pequeños ajustes en una entrada. El proceso de minería se basa en calcular repetidamente el resultado de una función hash criptográfica lo más rápido posible para obtener un resultado determinado. Estas funciones también se utilizan para obtener una dirección a partir de una clave pública.

Hash: el resultado de una función hash criptográfica.

Bloque candidato: un bloque de transacciones pendientes que un minero intenta añadir a la cadena de bloques mediante la obtención de una prueba de trabajo válida. Después de obtener una prueba de trabajo, el bloque candidato se convierte en un bloque válido y se añade a la cadena. Los mineros suelen formar bloques candidatos seleccionando las transacciones de un conjunto de memoria con las comisiones de transacción más altas.

Prueba de trabajo: la solución a un desafiante problema matemático basado en una función hash criptográfica que los mineros tratan de resolver. Debido a las propiedades de las funciones hash criptográficas, la prueba de trabajo es difícil de obtener, pero cualquier nodo puede verificar de manera trivial que el minero empleó recursos informáticos para encontrar la solución. La prueba de trabajo ayuda a resolver los desacuerdos cuando se extraen o “minan” dos bloques simultáneamente, y protege la red al hacer que los bloques históricos sean extremadamente costosos de manipular.

Tiempo de creación de bloque: el tiempo que se tarda en minar un nuevo bloque.

Tamaño del bloque: la capacidad de datos por bloque.

Recompensa por bloque: es una transacción especial que permite al minero enviarse a sí mismo un monto fijo del ETH recién creado como incentivo financiero por resolver el bloque.

Inversión ventajista: detección de oportunidades de arbitraje rentables dentro de la mempool. La idea es identificar estas oportunidades y enviar transacciones con un límite de gas más alto para beneficiarse de la oportunidad arbitraria, por lo que es una ventaja con respecto a la transacción original.

Valor extraíble del minero o máximo (MEV): se refiere al valor máximo que se puede extraer de la producción de bloques, además de la recompensa por bloque estándar y las comisiones de gas, al incluir, excluir y cambiar el orden de las transacciones en un bloque.¹⁰

En la cadena: se refiere a las transacciones que se producen en la cadena de bloques real.



Propuestas de mejora de Ethereum (EIP): describen los estándares actuales de la red Ethereum y todas las actualizaciones acordadas. Los creadores de red pueden proponer nuevas ideas y cambios a la red existente.

Confirmaciones: el número de bloques añadidos a la cadena de bloques después de que una transacción en particular se incluyera en un bloque. La primera confirmación es cuando una transacción se incluye en un bloque. Se añade una confirmación adicional cada vez que se mina un nuevo bloque válido en la cadena.

Cadena bifurcada: una cadena de bloques que se bifurca en dos cadenas diferentes. Estas cadenas comparten la misma historia, pero llegan a un punto en el que sus nuevos bloques dejan de ser los mismos. Se producen bifurcaciones temporales cuando dos mineros minan un bloque simultáneamente, pero las reglas del protocolo hacen que estas vuelvan a converger en una única cadena principal.

Cadena principal: la cadena de bloques que asumió más acumulación de trabajo de minería en función de la dificultad de los bloques subyacentes. Normalmente, la cadena principal tiene más bloques.

ERC-20: un token estándar de EVM basado en contratos inteligentes. Los tokens ERC-20 proporcionan un conjunto común de reglas para incentivar la componibilidad entre tokens.

Monedas estables: tokens de criptomoneda diseñados para replicar el dólar estadounidense en una proporción 1:1 y destinados a estabilizar el mercado añadiendo liquidez y vías de negociación.

Componibilidad: la capacidad de operar e interactuar con otros activos similares.

ERC-721: un token estándar de EVM basado en contratos inteligentes. La diferencia clave entre ERC-20 y ERC-721 es la capacidad de programar un token no fungible y las reglas que lo sustentan.

Prueba de participación: un mecanismo de consenso en el que los validadores deben "hacer *stake*" de sus activos para confirmar y registrar transacciones.

Validadores: participantes de la red que validan y confirman transacciones en un mecanismo de consenso de prueba de participación.

Slashing: sanciones del validador en virtud de un mecanismo de consenso de prueba de trabajo en el que se incauta la totalidad o una parte de los activos en *stake*.

Proponentes: validadores que se eligen de forma algorítmica para proponer un nuevo bloque.

Certificadores: los validadores que no sean elegidos para proponer un bloque deben certificar la propuesta de bloque del proponente y confirmar que la información respeta los estándares.

Gwei: Giga-wei o Gwei se utiliza a menudo para describir los costos del gas en la red Ethereum y representa una milmillonésima de un ether.

Mainnet: término utilizado para describir la cadena de bloques principal.

Descargos de responsabilidad

Las inversiones en activos digitales son especulativas e implican altos grados de riesgo, incluida una pérdida parcial o total de los fondos invertidos. Estas inversiones no son adecuadas para ningún inversor que no pueda permitirse la pérdida total de su inversión. Ethereum (ETH) es una clase de activos relativamente nueva. Está sujeta a riesgos únicos y sustanciales, e históricamente ha estado sujeta a una volatilidad de precios significativa. El valor de estas inversiones podría disminuir significativamente y sin previo aviso, y podría incluso llegar a cero. Debe estar preparado para perder toda su inversión.



La diversificación no garantiza una ganancia ni constituye una garantía contra una pérdida. Esta información no pretende ser asesoramiento individual o personalizado de inversión ni tributario y no debe utilizarse con fines comerciales. Consulte a un asesor financiero o profesional tributario para obtener más información sobre su inversión o situación tributaria.

Este material representa una evaluación del entorno de mercado en un momento específico y no pretende ser una previsión de eventos futuros ni una garantía de resultados futuros. Esta información no pretende ser asesoramiento individual o personalizado de inversión ni tributario y no debe utilizarse con fines comerciales. Consulte a un asesor financiero o profesional tributario para obtener más información sobre su inversión o situación tributaria.

Ethereum (ETH) está muy poco regulada y las inversiones pueden ser más susceptibles al fraude y la manipulación que las inversiones más reguladas. Ethereum (ETH) está sujeta a oscilaciones rápidas de precios, incluso como resultado de acciones y declaraciones de *influencers* y los medios de comunicación.

