

TOKENS

The background features a complex arrangement of dark, translucent 3D geometric shapes, possibly cubes or pyramids, set against a dark teal gradient. Interspersed among these shapes are several glowing lines in bright cyan and orange-yellow, which appear to be laser beams or energy pathways. These lines intersect and connect different parts of the geometric structures, creating a sense of depth and technological complexity.

JOAN AMENGUAL

RESUMEN

En este libro se van a explicar las bases fundamentales y los pilares de los Tokens que actualmente se encuentran tan presentes en el ecosistema Blockchain. Dichos conocimientos se han profundizado y se han explicado detalladamente en los cursos desarrollados en Udemy.

Los cursos de Blockchain en los que hemos estado trabajando durante meses los podéis encontrar rebajados un 90% en el siguiente enlace:

[https://blockstellart.com/rutas-de-aprendizaje/
blockchain/](https://blockstellart.com/rutas-de-aprendizaje/blockchain/)

En estos cursos además de entrar en detalle y profundizar en el ámbito de los Tokens y las criptomonedas también profundizamos con las bases teóricas de la tecnología Blockchain y aprendemos las bases técnicas de criptografía para entender todo el mundo de las criptomonedas y su enorme potencial, entre otros muchísimos conocimientos.

Por si fuera poco, tenemos un curso donde aprendemos a desarrollar Smart Contracts con Solidity. Donde vas a aprender a crear tus propios proyectos y ser un experto como desarrollador en Ethereum.

ÍNDICE

RESUMEN	2
ÍNDICE	3
CAPÍTULO 1: DEFINICIONES PREVIAS	6
¿Qué es un activo digital?	6
¿Qué es una criptomoneda?	8
¿Qué es un token?	10
CAPÍTULO 2: TOKENS, SUS tipos y SUS estándares	14
INTRODUCCIÓN	14
TIPOS DE TOKENS	18
ESTÁNDARES DE TOKENS	21
CAPÍTULO 3: TOKENS NFT	32
INTRODUCCIÓN	32
Componentes técnicos	41
Protocolos	46
Propiedades deseadas de los NFTs	49
Evaluación de seguridad	51
Oportunidades	56

Cuestiones de seguridad y privacidad	63
Consideraciones sobre la gobernanza	66
CAPÍTULO 4: TOKENS ERC-20	70
INTRODUCCIÓN	70
¿Qué significa el estándar ERC-20?	72
Características principales de los tokens ERC-20	74
¿Por qué se crearon los tokens ERC-20?	76
Pros y contra de los tokens ERC-20	78
¿Qué podemos hacer con los tokens ERC-20?	81
REFERENCIAS	84
SOBRE EL AUTOR	85

CAPÍTULO 1: DEFINICIONES PREVIAS

¿QUÉ ES UN ACTIVO DIGITAL?



Si te estás iniciando en el mundo del blockchain y las criptomonedas, es esencial que entiendas la diferencia entre activos digitales, criptomonedas y tokens. Aunque estos términos se utilizan a menudo indistintamente, se diferencian en una serie de aspectos clave. En términos generales, un activo digital es un activo no tangible que se crea, comercia y almacena en un formato digital. En el contexto de la cadena de bloques (blockchain, en inglés), los activos digitales incluyen la criptomoneda y los tokens de criptomonedas.

La criptomoneda y los tokens son subclases únicas de activos digitales que utilizan la criptografía, una técnica avanzada de encriptación que asegura la autenticidad de los criptoactivos al erradicar la posibilidad de falsificación o doble gasto.

La diferencia clave entre las dos clases de activos digitales es que las criptomonedas son el activo nativo de una cadena de

bloques, como BTC o ETH, mientras que los tokens se crean como parte de una plataforma que se construye sobre una cadena de bloques existente, como los numerosos tokens ERC-20 que componen el ecosistema de Ethereum.



¿QUÉ ES UNA CRIPTOMONEDA?



En el curso de '[Crea DApps con Tokens NFT en Ethereum usando Truffle y React](#)' definimos que una criptodivisa es el activo nativo de una red de cadenas de bloques que puede comercializarse, utilizarse como medio de intercambio y como depósito de valor.



Una criptodivisa es emitida directamente por el protocolo de la cadena de bloques en la que se ejecuta, por lo que a

menudo se denomina moneda nativa de la cadena de bloques. En muchos casos, las criptomonedas no sólo se utilizan para pagar las tasas de transacción en la red, sino que también se utilizan para incentivar a los usuarios a mantener la seguridad de la red de criptomonedas.

Las criptomonedas suelen servir como medio de intercambio o depósito de valor. Un medio de intercambio es un activo utilizado para adquirir bienes o servicios. Un depósito de valor es un activo que puede mantenerse o cambiarse por una moneda fiduciaria en una fecha posterior sin incurrir en pérdidas significativas en términos de poder adquisitivo.

Las criptomonedas suelen presentar las siguientes características:

1. Descentralizadas, o al menos no dependen de una autoridad central de emisión. En su lugar, las criptodivisas se basan en un código para gestionar la emisión y las transacciones.
2. Se basan en una cadena de bloques u otra tecnología de libro mayor distribuido (DLT), que permite a los participantes aplicar las normas del sistema de forma automatizada y sin confianza.

3. Utiliza la criptografía para asegurar la estructura subyacente de la criptomonedas y el sistema de red.

¿QUÉ ES UN TOKEN?

En el curso de '[Crea DApps con Tokens NFT en Ethereum usando Truffle y React](#)' nos centramos completamente en los tokens.

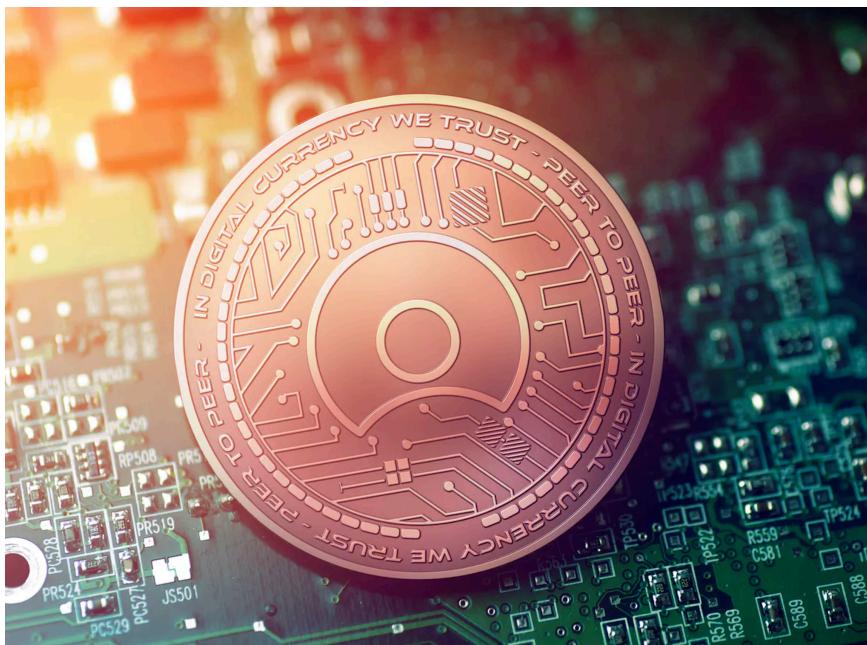
Los tokens, que también pueden denominarse criptofichas, son unidades de valor que las organizaciones o proyectos basados en la cadena de bloques desarrollan sobre las redes de cadenas de bloques existentes. Aunque a menudo comparten una profunda compatibilidad con las criptomonedas de esa red, son una clase de activo digital totalmente diferente.

Las criptomonedas son el activo nativo de un protocolo de cadena de bloques específico, mientras que los tokens son creados por plataformas que se basan en esas cadenas de bloques. Por ejemplo, el token nativo de la cadena de bloques de Ethereum es el ether (ETH). Aunque el ether es la criptomonedas nativa de la cadena de bloques de Ethereum, hay muchos otros tokens diferentes que también utilizan la cadena de bloques de Ethereum. Los tokens criptográficos construidos con Ethereum incluyen DAI, LINK, COMP y CryptoKitties, entre otros. Estos tokens pueden servir para

una multitud de funciones en las plataformas para las que están construidos, incluyendo la participación en mecanismos de financiación descentralizada (DeFi), el acceso a servicios específicos de la plataforma, e incluso jugar.

Existen varios estándares de tokens ampliamente utilizados para crear tokens de criptomonedas, la mayoría de los cuales se han construido sobre Ethereum. Los estándares de tokens más utilizados son el ERC-20, que permite la creación de tokens que pueden interoperar dentro del ecosistema de aplicaciones descentralizadas de Ethereum, y el ERC-721, que fue diseñado para permitir tokens no fungibles que son individualmente únicos y no pueden intercambiarse con otros tokens similares. A partir de 2020, hay cientos de fichas ERC-20 diferentes y miles de fichas ERC-721 en circulación. A medida que se desarrolle nuevos tokens para abordar los crecientes casos de uso de la cadena de bloques, es probable que el número de tokens diferentes siga creciendo a un ritmo notable.

Normalmente, los tokens criptográficos son programables, sin permisos, sin confianza y transparentes. Programable significa simplemente que se ejecutan en protocolos de software, que se componen de contratos inteligentes que describen las características y funciones del token y las reglas de participación de la red. Sin permisos significa que cualquiera puede participar en el sistema sin necesidad de credenciales especiales. Trustless significa que ninguna



autoridad central controla el sistema, sino que éste se rige por las reglas predefinidas por el protocolo de la red. Y por último, la transparencia implica que las reglas del protocolo y sus transacciones son visibles y verificables por todos.

Aunque los tokens criptográficos, al igual que las criptomonedas, pueden tener valor y ser intercambiados, también pueden ser diseñados para representar activos físicos o activos digitales más tradicionales, o una determinada utilidad o servicio. Por ejemplo, hay tokens criptográficos que representan activos tangibles como bienes inmuebles y arte, así como activos intangibles como la potencia de

procesamiento o el espacio de almacenamiento de datos. Los tokens también se utilizan con frecuencia como mecanismo de gobernanza para votar sobre parámetros específicos como las actualizaciones del protocolo y otras decisiones que dictan la dirección futura de varios proyectos de blockchain. El proceso de creación de tokens criptográficos para servir a estas diversas funciones se conoce como tokenización.

A medida que la industria de la cadena de bloques siga madurando, el número de activos digitales únicos seguirá creciendo de acuerdo con las necesidades multifacéticas de todos los participantes del ecosistema, desde los socios empresariales hasta los usuarios individuales. Dado que la creación de nuevos activos en el mundo digital es menos restrictiva que en el ámbito físico, se espera que estos activos digitales mejoren la forma en que innumerables industrias operan, interactúan y generan valor, permitiendo así una amplia gama de nuevas posibilidades sociales y económicas.



CAPÍTULO 2: TOKENS, SUS TIPOS Y SUS ESTÁNDARES

INTRODUCCIÓN



Las aplicaciones en una red P2P que no están controladas por una sola entidad se denominan aplicaciones descentralizadas (dApps). Por lo general, su front-end es un navegador o una interfaz de aplicación, mientras que su back-end puede ,al menos en parte, realizarse en una blockchain o criptomoneda. Las principales categorías de dApps siguen siendo las finanzas descentralizadas, seguidas de los juegos de azar y los mercados. A menudo, proporcionan su propio token en la dApp.

Un token criptográfico es un activo digital sobre una criptomoneda o blockchain, a menudo como un activo programable gestionado por un contrato inteligente, para su uso dentro de un proyecto o dApp. Los tokens criptográficos son similares a las monedas de una criptomoneda, excepto que no tienen su propia cadena de bloques o libro de

contabilidad distribuido. Más bien, se construyen sobre uno ya existente.

Cuando consideramos que los tokens criptográficos representan el derecho a algo, entramos en el ámbito de la tokenización. La tokenización es una forma de convertir los derechos a algo en un artefacto digital, un llamado token. En el caso de los tokens criptográficos, los beneficios de la tokenización residen principalmente en una mayor liquidez, una programabilidad general y una prueba de propiedad inmutable. Más concretamente, la propiedad digital fraccionada reduce las barreras de entrada para los inversores, al tiempo que aumenta la liquidez de los activos tokenizados. Además, la programabilidad facilita la gestión automatizada de los derechos de los inversores y el cumplimiento de los activos tokenizados, y, por lo tanto, aumenta potencialmente la velocidad. Por último, los rastros inmutables de las transferencias proporcionan pruebas de que las transferencias de la propiedad digital no han sido manipuladas. Sin embargo, todavía faltan normas de tokenización y en muchas jurisdicciones también falta infraestructura legal al respecto.

Como medio de intercambio, los tokens pueden actuar como una moneda en sí mismos. En este sentido, también pueden denominarse como la moneda local de una dApp. En general, los tokens criptográficos se utilizan más allá del mero intercambio aprovechando su característica más

destacada: ser programables. En este sentido, se utilizan para activar determinadas funciones en el contrato o contratos inteligentes de la dApp. Además, los tokens pueden estar vinculados a activos fuera de la cadena. Pueden servir como medio de recaudación de fondos, preorden o inversión, así como para construir un ecosistema o una comunidad.



La creación de tokens sobre una cadena de bloques existente se realiza mediante contratos inteligentes, los llamados contratos de tokens. Dado que se trata de un tipo de aplicación muy extendido, los patrones de codificación y los ejemplos de mejores prácticas están fácilmente

disponibles. Además, existen fábricas de contratos de tokens, ya sea en la cadena o como servicio web.

La adquisición de tokens varía. Por ejemplo, pueden comprarse durante una oferta inicial de monedas (ICO) o a través de un intercambio de criptomonedas, negociarse en la cadena o recibirse libremente durante un lanzamiento aéreo o como recompensa por un servicio o comportamiento.

El valor de un token depende principalmente de la oferta, la demanda y la confianza que la comunidad participante tenga en él, que se basa en la credibilidad y el servicio.

TIPOS DE TOKENS



Así como hemos definido en el curso de 'Crea DApps con Tokens NFT en Ethereum usando Truffle y React' existe una clasificación de alto nivel de los tokens que distingue entre:

1. Tokens de pago
2. Tokens de seguridad
3. Tokens de utilidad.

- La necesidad de aclarar sus diferencias radica en el hecho de que, en la mayoría de las jurisdicciones, los tokens de seguridad están más regulados que otros tokens.



El principal rasgo distintivo es la finalidad de inversión de los tokens de seguridad, frente al valor añadido para el funcionamiento de un producto que es típico de los tokens de utilidad. Los tokens de pago cumplen una función de pago con poca o ninguna otra función.

Los tokens de seguridad son "activos, como un derecho de deuda o de capital sobre el emisor". Por lo tanto, en términos de su función económica, estos tokens son análogos a las acciones, los bonos o los derivados". Normalmente, se trata de una acción de la empresa emisora (equity token).

En cuanto al cumplimiento legal, se está debatiendo cómo podría integrarse en un estándar de tokens, así como en los monederos e intercambios.

Los utility tokens suelen estar respaldados por un proyecto, una aplicación o una dApp con un beneficio definible (como el acceso) y pretenden "proporcionar acceso digital a una aplicación o servicio mediante una infraestructura basada en blockchain". La emisión de tokens de utilidad no requiere la aprobación de la supervisión si el acceso digital a una aplicación o servicio es totalmente funcional en el momento de la emisión de los tokens." La finalidad de un token de utilidad puede incluir derechos de voto, algún tipo de recompensa o la gobernanza de las apuestas.

Dado que estos propósitos y categorías pueden superponerse para un token específico, un esquema de clasificación más fino puede ser más adecuado. Muchos tokens son híbridos en lo que respecta a esta categorización gruesa.



ESTÁNDARES DE TOKENS

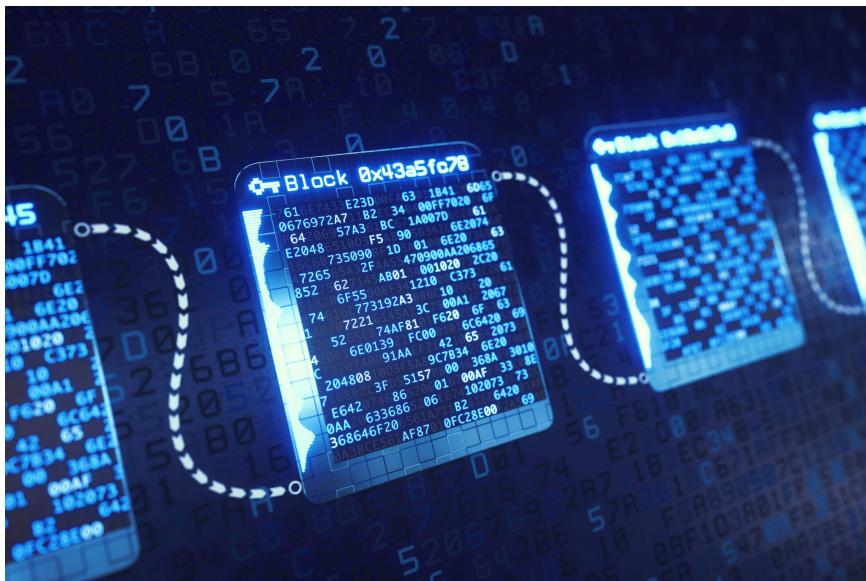


Las interfaces estándar de los tokens permiten que aplicaciones como los monederos reconozcan los tokens e interactúen con ellos. En este punto del libro, primero vamos a aclarar los términos y resumimos las funcionalidades que ofrecen los contratos de tokens. A continuación, presentamos los estándares de tokens ya aceptados junto con los estándares de tokens de seguridad propuestos.

A. Términos

Ethereum distingue entre cuentas de propiedad externa, a menudo llamadas usuarios, y cuentas de contrato o simplemente contratos. Las cuentas se identifican de forma única mediante direcciones de 20 bytes. Los usuarios pueden emitir transacciones (paquetes de datos firmados) que transfieren valor a usuarios y contratos, o que llaman o crean contratos. Estas transacciones se registran en la cadena de bloques. Los contratos tienen que ser activados, ya sea por una transacción de un usuario o por una llamada (un mensaje) de otro contrato. Los mensajes no se registran en la cadena de bloques, ya que son consecuencias deterministas de la transacción inicial. Sólo existen en el entorno de

ejecución de la máquina virtual de Ethereum (EVM) y se reflejan en el rastro de ejecución y en los posibles cambios de estado. Utilizamos "mensaje" como término colectivo para cualquier transacción (externa) o mensaje (interno).



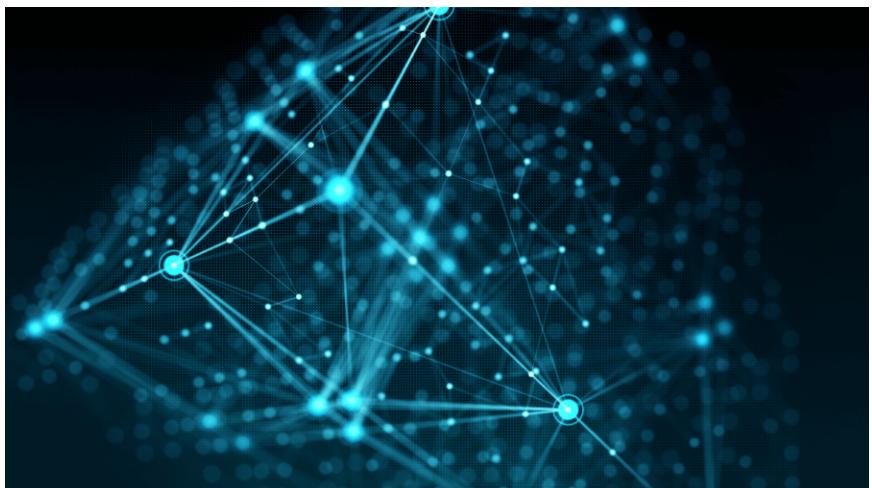
Interfaz binaria abstracta (ABI). La mayoría de los contratos en el universo Ethereum se adhieren al estándar ABI, que identifica las funciones mediante firmas que consisten en los primeros cuatro bytes del hash Keccak-256 del nombre de la función junto con los tipos de parámetros. Así, el bytecode de un contrato contiene instrucciones para comparar los cuatro primeros bytes de los datos de la llamada con las firmas de sus funciones. La presencia de una

función concreta en un contrato puede comprobarse localizando el hash de 4 bytes correspondiente en su bytecode desplegado. Así, la conformidad de un contrato con los estándares de la interfaz puede determinarse a través de su bytecode.

B. Funcionalidades de los contratos de tokens

La funcionalidad básica de un contrato de tokens comprende:

1. La contabilidad de las tenencias de tokens.
2. La transferencia de la propiedad de los tokens según los cambios en el libro de tenencias de tokens en el respectivo contrato de tokens.
3. La emisión de eventos para registrar las transferencias de propiedad en los registros.



La transferencia segura es un mecanismo en el que los tokens se extraen (se retiran) de una dirección después de su aprobación, en lugar de ser empujados (transferidos) a una dirección donde pueden perderse en caso de que la dirección no esté preparada para recibir tokens.

Otras funcionalidades relacionadas con los tokens incluyen la creación y destrucción de tokens (llamadas acuñación y quema), así como su distribución y comercio (por ejemplo, a través de ICOs y airdrops). A menudo, los contratos de tokens también implementan funcionalidades generales que incluyen la autenticación y los roles, el control (como la pausa, el bloqueo), suministro de información (como las funciones de visualización), y utilidades (como las operaciones matemáticas seguras).

C. Estándares de tokens aceptados

La comunidad discute continuamente y establece interfaces estándar para tokens en el lenguaje de programación Solidity, que es el que prevalece en Ethereum. Los siguientes estándares han sido aceptados hasta ahora.

1. El estándar de tokens **ERC-20** es el más utilizado y el más general que "proporciona la funcionalidad básica para transferir tokens, así como permite que los tokens sean aprobados para que puedan ser gastados por otro tercero en la cadena". Enumera seis funciones obligatorias y tres

opcionales, así como dos eventos que deben ser implementados por una API conforme.



2. El estándar de tokens no fungibles **ERC-721** se refiere a tokens en los que cada token es distinto (también conocido como no fungible) y, por tanto, permite el seguimiento de activos distinguibles. Cada activo debe tener un seguimiento individual y atómico de su propiedad. Esta norma requiere que los tokens que cumplan con ella implementen 10 funciones obligatorias y tres eventos.



3. El estándar de tokens **ERC-777** define funciones avanzadas para interactuar con los tokens sin dejar de ser compatible con ERC-20. Define operadores para enviar tokens en nombre de otra dirección, y ganchos para enviar y recibir con el fin de ofrecer a los titulares de tokens más control sobre sus tokens. Esta norma requiere que los tokens que cumplen con ella implementen 13 funciones obligatorias y cinco eventos.



4. El estándar **ERC-1155** Multi Token permite la gestión de cualquier combinación de tokens fungibles y no fungibles en un único contrato, incluyendo la transferencia de múltiples tipos de tokens a la vez. Esta norma requiere que

los tokens que cumplen con ella implementen seis funciones obligatorias y cuatro eventos.



C. Normas propuestas para los tokens de seguridad

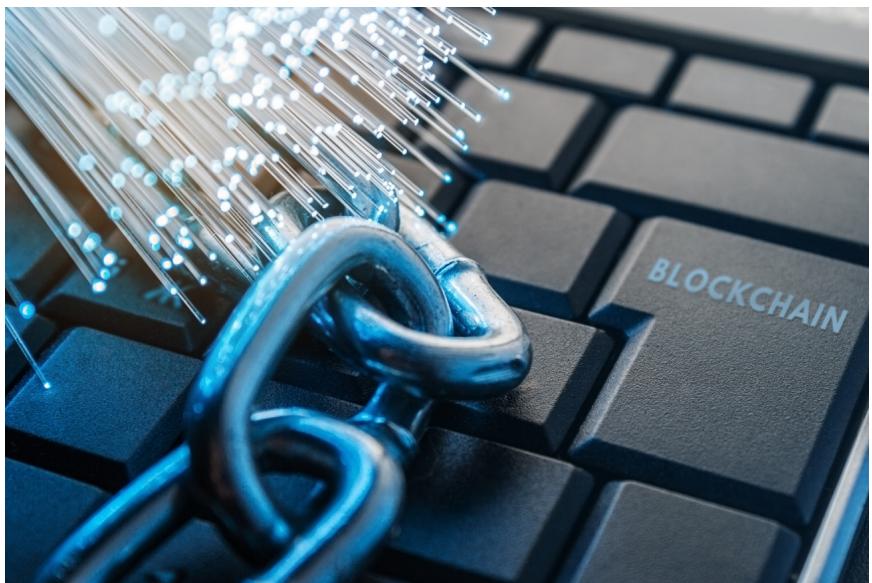
Aparte de las normas aceptadas, se han propuesto y debatido otras, pero aún no se han finalizado. Desde el punto de vista legal, las siguientes normas de tokens de seguridad parecen interesantes. Mientras que el primero es bastante general, los otros dos son específicos de un proyecto y están respaldados por una empresa.

ERC-1462 Base Security Token es una extensión mínima de ERC-20 que "proporciona el cumplimiento de las regulaciones de valores y la aplicabilidad legal" y tiene como objetivo los casos de uso general, mientras que la funcionalidad adicional y las limitaciones relacionadas con los proyectos o los mercados pueden aplicarse por separado.

Además, incluye "regulaciones KYC (Know Your Customer) y AML (Anti Money Laundering) y la capacidad de bloquear tokens para una cuenta, y restringir su transferencia debido a una disputa legal". Además, proporciona medios para adjuntar documentos a los tokens. Esta norma exige que los tokens que cumplan con ella implementen otras cuatro funciones de comprobación obligatorias (además de la ERC-20) y dos funciones de documentación opcionales.

ERC-1450 LDGRToken es un "token de seguridad para la emisión y el comercio de valores conformes con la SEC" que amplía ERC-20. Este estándar "facilita el registro de la propiedad y la transferencia de los valores vendidos en cumplimiento de la Ley de Valores Act Regulations CF, D and A".

Además de sus propias funciones obligatorias, hace que algunas partes opcionales del ERC-20 sean obligatorias. Además, requiere que se implementen ciertos modificadores y argumentos del constructor.



El Estándar de Operación de Tokens de Controladores ERC-1644 "permite que un token declare de forma transparente si un controlador puede o no transferir unilateralmente tokens entre direcciones". Esto está motivado por el hecho de que "en algunas jurisdicciones el emisor (o una entidad delegada por el emisor) puede necesitar retener la capacidad de forzar la transferencia de tokens." Esta norma requiere que los tokens que cumplan con ella implementen tres funciones obligatorias y dos eventos.

ERC-1644 forma parte de ERC-1400, una biblioteca de estándares para tokens de seguridad, que requiere que los estándares contenidos sean compatibles con ERC-20 y, mediante extensiones, también con ERC-777. Además, la biblioteca contiene el ERC-1410 para la propiedad diferenciada y las restricciones transparentes, el ERC-1594 para las restricciones dentro y fuera de la cadena, y el ERC-1643 para la gestión de documentos y leyendas.

E. Patrones de codificación para los contratos de tokens

La mayoría de los tokens pretenden establecer confianza y credibilidad revelando su código fuente en el principal explorador de blockchain para Ethereum, Etherscan. Como servicio, esta plataforma comprueba que el bytecode desplegado es el resultado de compilar el código fuente

proporcionado con la configuración del compilador dada, y lo etiqueta como "código fuente verificado".



Además, muchos proyectos relacionados con tokens se desarrollan públicamente en la plataforma GitHub.



CAPÍTULO 3: TOKENS NFT

INTRODUCCIÓN

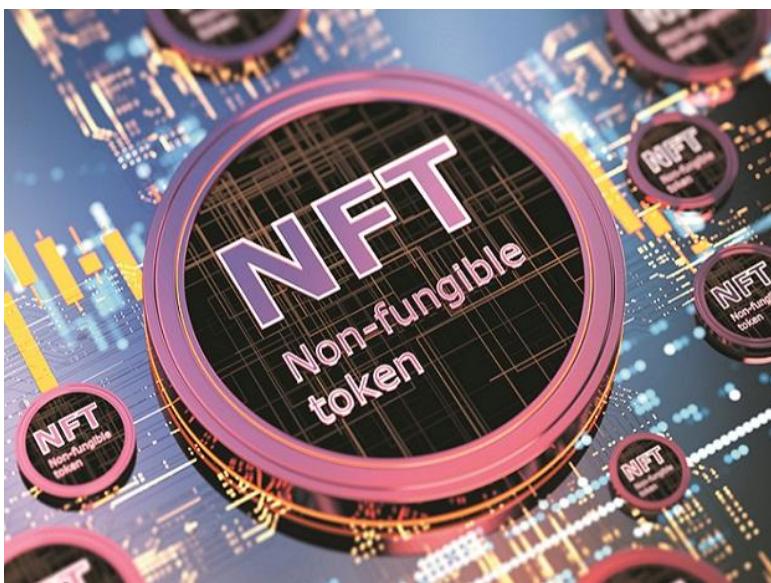


En el curso de '[Crea DApps con Tokens NFT en Ethereum usando Truffle y React](#)' nos centramos completamente en los tokens NFT y en el desarrollo tecnológico de estos.

El token no fungible (NFT) es un tipo de criptomonedas que se deriva de los contratos inteligentes de Ethereum. El NFT se propuso por primera vez en la Propuesta de Mejora de Ethereum (EIP)-721 y se desarrolló posteriormente en la EIP-1155. NFT se diferencia de las criptomonedas clásicas como Bitcoin en sus características inherentes. Bitcoin es una moneda estándar, en la que todas las monedas son equivalentes e indistinguibles. Por el contrario, NFT es único y no puede ser intercambiado de igual a igual (equivalentemente, no fungible), lo que la hace adecuada para identificar algo o alguien de forma única.

En concreto, utilizando NFT en un contrato inteligente (en Ethereum), un creador puede demostrar fácilmente la existencia y la propiedad de los activos digitales en forma de vídeos, imágenes, artes, entradas para eventos, etc.

Además, el creador también puede ganar derechos de autor cada vez que se realiza una operación con éxito en cualquier mercado de NFT o mediante el intercambio entre pares. La posibilidad de comerciar con todo el historial, la gran liquidez y la cómoda interoperabilidad permiten que los NFT se conviertan en una prometedora solución de protección de la propiedad intelectual (PI).



Aunque, en esencia, los NFT representan poco más que un código, para un comprador los códigos tienen un valor atribuido al considerar su escasez comparativa como objeto digital. Esto asegura bien los precios de venta de estos productos relacionados con la propiedad intelectual que pueden parecer impensables para los activos virtuales no fungibles.

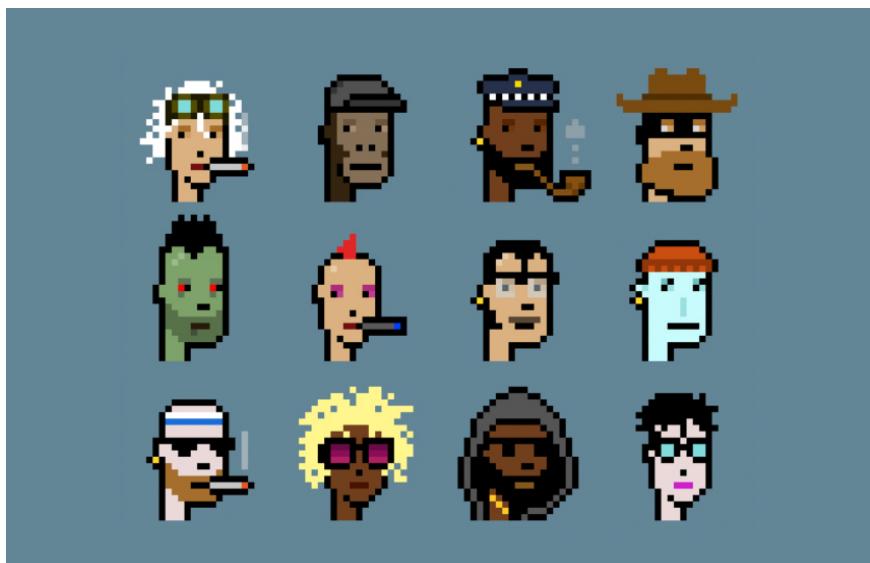
En los últimos años, los NFT han suscitado una notable atención tanto en la comunidad industrial como en la científica. Se ha informado de que el volumen de negociación de 24 horas de media del mercado de NFT es de 4, 592, 146, 914 USD, mientras que el volumen de negociación de 24 horas de todo el mercado de criptodivisas es de 341.017.001.809 USD. La liquidez de las soluciones relacionadas con NFT ha representado el 1,3% de todo el mercado de criptodivisas en un periodo tan corto (5 meses).

Los primeros inversores obtienen rendimientos mil veces superiores por la venta de colecionables digitales únicos. El mercado relacionado con las NFT ha aumentado significativamente en comparación con el de hace un año. En concreto, el número total de ventas es de 25.729 y sus importes totales gastados en las ventas completadas alcanzan los 34.530.649,86 USD. En particular, el número total de ventas en el mercado primario ocupa 17.140, mientras que el número de ventas secundarias (de usuario a usuario) es de 8.589. En consecuencia, el total de USD utilizados en las

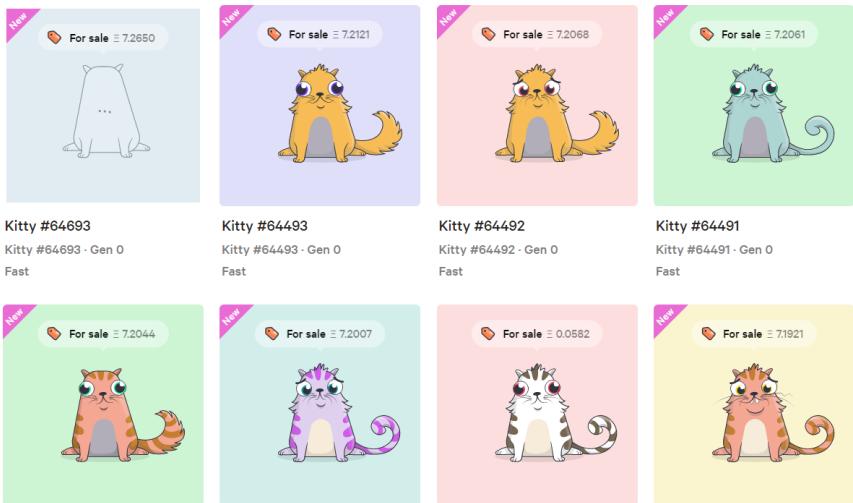
ventas del mercado primario es de 8.816.531,10. Además, los monederos activos del mercado alcanzan los 12.836, que siguen aumentando a gran velocidad a medida que pasa el tiempo. Sorprendentemente, la venta de NFTs se estimó en 12 millones (diciembre de 2020), pero explotó a 340 millones en sólo dos meses (febrero de 2021). Este desarrollo vertiginoso hace que los NFT se conviertan en una moda, o incluso sean descritas por algunos como el futuro de los activos digitales.



Además de los datos anteriores, la gente ha expresado su interés en varios tipos de NFT. Participan con entusiasmo en juegos o intercambios relacionados con las NFT. CryptoPunks, uno de los primeros NFT en Ethereum, ha creado más de 10.000 punks colecciónables (6039 hombres y 3840 mujeres) y ha promovido la popularidad del estándar ERC-721.



CryptoKitties puso oficialmente en evidencia a los NFT, y llegó al mercado en 2017 con la gamificación de la mecánica de cría. Los participantes compitieron ferozmente a altos precios para subastar los gatos raros.



Otro ejemplo destacado es NBA Top Shot, que es una plataforma de comercio de NFT utilizada para comprar/vender vídeos cortos digitales de momentos de la NBA. Miles de aficionados a la NBA de en todo el mundo han recogido más de 7,6 millones de momentos de máxima audiencia, construyendo la lista de novatos, veteranos y estrellas emergentes.



No cabe duda de que existe un ciclo de hype en torno a las NFT en el que la mayoría de los productos pueden venderse a precios elevados, algunos incluso a cientos o miles de ETH.

Además de los juegos y los coleccionables, las NFT también promueven el desarrollo del arte, la venta de entradas, el valor, el IoT y las finanzas. Otros tipos de mercados circundantes también desempeñan un papel importante para proporcionar información instantánea y entornos seguros, como los sitios web de estadísticas (por ejemplo, NonFungible, DappRadar, NFT bank, DefiPulse, Coingecko), el mercado de comercio (cryptoslam, Opensea, SuperRare, Nifty Gateway, Rarible , Zora) y el llamado ecosistema NFT (como Dego).



A pesar de que las NFT tienen un enorme impacto potencial en los actuales mercados descentralizados y en las futuras oportunidades de negocio, las tecnologías de NFT se encuentran todavía en una fase muy temprana. Es necesario abordar cuidadosamente algunos retos potenciales, mientras que hay que destacar algunas oportunidades prometedoras.

Además, aunque hay mucha literatura sobre las NFT, procedente de blogs, wikis, mensajes de foros, códigos y otras fuentes, a disposición del público, falta un estudio sistemático.



COMPONENTES TÉCNICOS



En el curso de '[Crea DApps con Tokens NFT en Ethereum usando Truffle y React](#)' nos centramos enfocados en los componentes técnicos de los NFT. Así que en esta parte, del libro mostramos los componentes técnicos relacionados con las actividades de los NFT. Estos componentes sientan las bases de un esquema NFT plenamente funcional.

Blockchain fue propuesto originalmente por Nakamoto, donde Bitcoin utiliza el algoritmo de prueba de trabajo (PoW) para llegar a un acuerdo sobre los datos de las transacciones en una red descentralizada. Blockchain se define como una base de datos distribuida y adjunta que mantiene una lista de registros de datos vinculados y protegidos mediante protocolos criptográficos.



Blockchain proporciona una solución al antiguo problema bizantino, que se ha acordado con una gran red de participantes no confiables. Una vez que los datos compartidos en la cadena de bloques se confirman en la mayoría de los nodos distribuidos, se vuelven inmutables porque cualquier cambio en los datos almacenados invalidará todos los datos posteriores.

La plataforma de blockchain más utilizada en los esquemas NFT es Ethereum, que proporciona un entorno seguro para ejecutar los contratos inteligentes. Además, varias soluciones dejan caer sus motores de cadena personalizados o plataformas de blockchain para soportar sus aplicaciones especializadas, y algunas de ellas son Flow, EOS, Hyperledger, y Fast Box.



Los contratos inteligentes fueron introducidos originalmente por Szabo, con el objetivo de acelerar, verificar o ejecutar la negociación digital. Ethereum desarrolló aún más los contratos inteligentes en el sistema blockchain.



Los contratos inteligentes basados en la cadena de bloques adoptan lenguajes de scripting completos de Turing para lograr funcionalidades conformes y ejecutan la replicación de transiciones de estado a través de algoritmos consensibles para lograr la consistencia final. Los contratos inteligentes permiten a las partes no familiares y a los participantes descentralizados llevar a cabo intercambios justos sin un tercero de confianza y, además, proponen un método unificado para construir aplicaciones en una amplia gama de industrias. Las aplicaciones que operan sobre los contratos inteligentes se basan en mecanismos de transición de estados. Los estados que contienen las instrucciones y los parámetros son compartidos por todos los participantes, lo que garantiza

la transparencia de la ejecución de estas instrucciones. Además, las posiciones entre los estados tienen que ser las mismas en todos los nodos distribuidos, lo que es importante para su consistencia. La mayoría de las soluciones NFT se basan en plataformas de blockchain basadas en contratos inteligentes para garantizar sus ejecuciones sensibles a las órdenes.

La dirección de la cadena de bloques y la transacción son un concepto esencial en las criptomonedas. Una dirección de blockchain es un identificador único para que un usuario envíe y reciba los activos, que es similar a una cuenta



bancaria cuando se gastan los activos en el banco. Consiste en un número fijo de caracteres alfanuméricicos generados a

partir de un par de claves públicas y privadas. Para transferir los NFT, el propietario debe demostrar estar en posesión de la clave privada correspondiente y enviar los activos a otra(s) dirección(es) con una firma digital correcta. Esta sencilla operación suele realizarse mediante un monedero de criptomonedas y se representa como el envío de una transacción para involucrar a los contratos inteligentes en el estándar ERC-777.

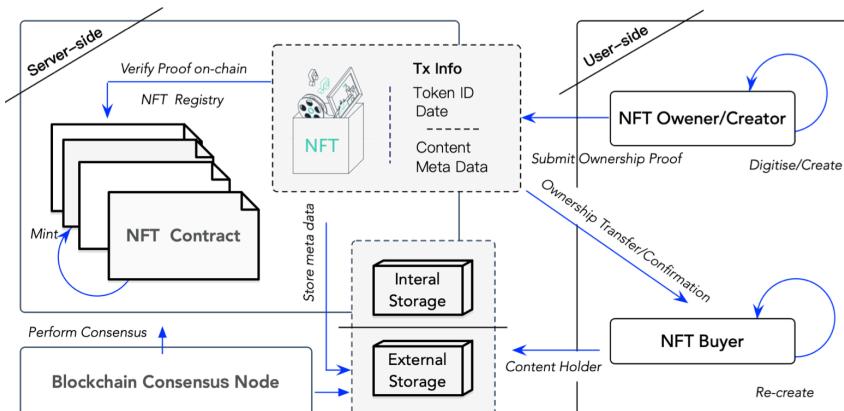
PROTOCOLOS



El establecimiento de la NFT requiere un libro de contabilidad distribuido subyacente para los registros, junto con transacciones intercambiables para el comercio en la red de pares. En particular, asumimos que el libro mayor tiene características básicas de seguridad, consistencia, integridad y disponibilidad. Además, un sistema de NFT también consta de otros dos roles: Propietario de NFT y comprador de NFT. El protocolo detallado es el siguiente.

- **Digitalización de NFT.** El propietario de la NFT comprueba que el archivo, el título y la descripción son completamente correctos. A continuación, digitaliza los datos en bruto en un formato adecuado.
- **Almacenar NFT.** El propietario de la NFT almacena los datos en bruto en una base de datos externa fuera de la cadena de bloques. También puede almacenar los datos en bruto dentro de la cadena de bloques, aunque esta operación consume mucho gas.

- **Firma de la NFT.** El propietario de la NFT firma una transacción, incluyendo el hash de los datos de la NFT, y luego envía la transacción a un contrato inteligente.
- **NFT Mint&Trade.** Una vez que el contrato inteligente recibe la transacción con los datos del NFT, comienza el proceso de acuñación y comercio.
- **Confirmación NFT.** Una vez confirmada la transacción, se completa el proceso de acuñación. Con este enfoque, los NFT se vincularán para siempre a una dirección única de la cadena de bloques como prueba de su persistencia.



En un sistema blockchain, cada bloque tiene una capacidad limitada. Cuando la capacidad de un bloque se llena, otras transacciones entrarán en un bloque futuro vinculado al bloque de datos original. Al final, todos los bloques vinculados han creado un historial a largo plazo que permanece permanente. El sistema NFT, en esencia, es una aplicación basada en la cadena de bloques. Cada vez que se acuña o se vende un NFT, es necesario enviar una nueva transacción para invocar el contrato inteligente. Una vez confirmada la transacción, los metadatos del NFT y los detalles de la propiedad se añaden a un nuevo bloque, garantizando así que el historial del NFT no se modifique y se conserve la propiedad.

PROPIEDADES DESEADAS DE LOS NFTS



Los esquemas NFT son esencialmente aplicaciones descentralizadas, y por lo tanto disfrutan de los beneficios/propiedades de sus libros de contabilidad públicos subyacentes. Resumimos las propiedades clave como sigue.

- **Verificabilidad.** La NFT con sus metadatos de tokens y su propiedad puede ser verificada públicamente.
- **Ejecución transparente.** Las actividades de los NFT, como la acuñación, la venta y la compra, son públicamente accesibles.
- **Disponibilidad.** El sistema de NFT nunca se cae. Por otra parte, todas las fichas y los NFT emitidos están siempre disponibles para vender y comprar.
- **Resistencia a la manipulación.** Los metadatos de la NFT y sus registros de negociación se almacenan de forma

persistente y no pueden manipularse una vez que las transacciones se consideran confirmadas.

- **Facilidad de uso.** Cada NFT dispone de información actualizada sobre la propiedad, que es fácil de usar y clara en cuanto a la información.
- **Atomicidad.** Las NFT de comercio pueden completarse en una transacción atómica, consistente, isolada y duradera (ACID). Las NFT pueden ejecutarse en el mismo estado de ejecución compartido.
- **Negociabilidad.** Cada NFT y sus correspondientes productos pueden ser negociados e intercambiados de forma arbitraria.



EVALUACIÓN DE SEGURIDAD



Un sistema NFT es una tecnología combinada que consta de blockchain, almacenamiento y aplicación web. La evaluación de la seguridad en el sistema NFT es un reto, ya que cada componente puede convertirse en una interfaz de ataque que hace que todo el sistema sea realmente vulnerable frente al atacante.

- **Spoofing.** La suplantación es la capacidad de hacerse pasar por otra entidad (por ejemplo, otra persona u ordenador) en el sistema, lo que corresponde a la autenticidad. Cuando un usuario interactúa para acuñar o vender los NFT, un atacante malintencionado puede explotar las vulnerabilidades de autenticación o robar la clave privada del usuario para transferir la propiedad de los NFT de forma ilegal. Por lo tanto, recomendamos tener una verificación formal para el contrato inteligente de NFT y utilizar el monedero frío para evitar la fuga de la clave privada.

- **Manipulación.** La manipulación se refiere a la modificación maliciosa de los datos de NFT, que viola la integridad. Supongamos que el blockchain es un libro de contabilidad de transacciones públicas robusto y un

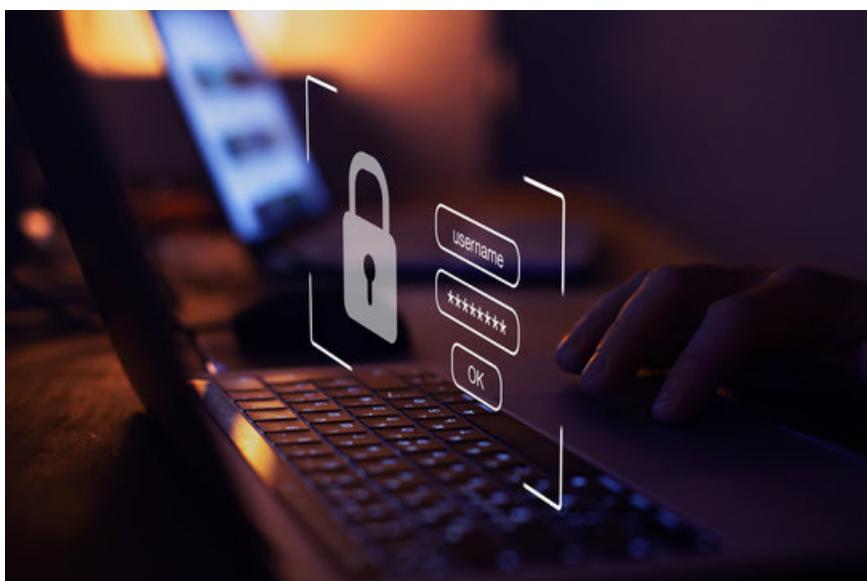
algoritmo de hash es resistente a la preimagen y a la segunda preimagen. Los metadatos y la propiedad de los NFT no pueden ser modificados de forma maliciosa una vez confirmada la transacción. Sin embargo, los datos almacenados fuera de blockchain pueden ser manipulados. Por lo tanto, recomendamos a los usuarios que envíen tanto los datos hash como los datos originales al comprador de NFT cuando comercien/intercambien propiedades relacionadas con NFT.



- **Repudio.** El repudio se refiere a la situación en la que el autor de un estado no puede disputar, lo que está relacionado con la propiedad de seguridad de no repudiabilidad. En particular, el hecho de que un usuario envíe NFT a otro usuario no puede negarlo. Esto está garantizado por la seguridad de la cadena de bloques y la propiedad de no falsificación de un esquema de firma. Sin embargo, los datos hash pueden ser robados por un atacante malicioso, o los datos hash pueden vincularse con la dirección de un atacante. Por ello, creemos que el uso de un contrato multifirma puede resolver en parte este problema, ya que cada vinculación debe ser confirmada por más de un participante.

- **Fuga de información.** La fuga de información se produce cuando la información se expone a usuarios no autorizados, lo que viola la confidencialidad. En el sistema NFT, la información de estado y el código de instrucciones en los contratos inteligentes son totalmente transparentes, y cualquier estado y sus cambios son accesibles públicamente por cualquier observador. Incluso si el usuario sólo pone el hash de NFT en la cadena de bloques, los atacantes maliciosos pueden explotar fácilmente la vinculación del hash y la transacción. Por lo tanto, recomendamos al desarrollador de NFT que utilice contratos inteligentes que preserven la privacidad en lugar de contratos inteligentes simples para proteger la privacidad del usuario.

- **Negación de servicio (DoS).** El ataque de denegación de servicio es un tipo de ataque a la red en el que un atacante malintencionado pretende hacer que un servidor no esté disponible para los usuarios a los que va dirigido, interrumpiendo las funciones normales.



El DoS viola la disponibilidad e interrumpe el servicio NFT, que puede ser utilizado por usuarios no autorizados. Afortunadamente, el blockchain garantiza la alta disponibilidad de las operaciones de los usuarios. Los usuarios legítimos pueden utilizar la información requerida cuando la necesiten y no perderán recursos de datos debido a errores accidentales. Sin embargo, el DoS también puede ser utilizado para atacar las aplicaciones web centralizadas o los

datos en bruto fuera de la blockchain, lo que resulta en una denegación de servicio para el servicio NFT. Recientemente, se ha propuesto una nueva arquitectura híbrida de blockchain con un algoritmo de consenso débil, mediante la cual esta arquitectura resuelve los problemas de disponibilidad utilizando dos algoritmos.

- **Elevación de privilegios.** La elevación de privilegios es una propiedad relacionada con la autorización. En este tipo de amenaza, un atacante puede obtener permisos más allá de los inicialmente concedidos. En el sistema NFT, los permisos de venta son gestionados por un contrato inteligente. De nuevo, un contrato inteligente mal diseñado puede hacer que los NFT pierdan estas propiedades.

OPORTUNIDADES



En el curso de '[Crea DApps con Tokens NFT en Ethereum usando Truffle y React](#)' hemos explicado las grandes oportunidades que existen con los NFT. En esta parte del libro nos centraremos en explicar algunas de estas oportunidades.

Los NFT tienen un gran potencial en la industria del juego. Ya existen algunos criptojuegos como CryptoKitties, Cryptocats, CryptoPunks, Meebits, Axie Infinity, Gods Unchanged y TradeStars. Una característica fascinante de estos juegos es el mecanismo de "cría". Los usuarios pueden criar personalmente a sus mascotas y dedicar mucho tiempo a la cría de nuevos fuera de serie. También pueden comprar mascotas virtuales de edición limitada o rara y venderlas a un precio elevado. La recompensa extra atrae a muchos inversores que se unen a los juegos, lo que hace que los NFT cobren protagonismo. Otra función interesante de las NFT es que proporcionan registros de propiedad de los objetos en los juegos y favorecen el mercado económico en el ecosistema, lo que beneficia tanto a los desarrolladores como a los jugadores. En particular, los desarrolladores de juegos que son editores de NFT de los elementos (por ejemplo, armas y

skins) pueden ganar regalías cada vez que sus artículos son (re)vendidos en el mercado abierto. Los jugadores pueden obtener artículos de juego de exclusividad personal. Esto creará un modelo de negocio mutuamente beneficioso en el que tanto los jugadores como los desarrolladores se beneficiarán de los mercados de NFT de segunda mano. Después, las comunidades de blockchain amplían los NFT a una gran extensión que abarca varios tipos de activos digitales.



Los eventos online tradicionales dependen de empresas centralizadas que proporcionan confianza y tecnología. Aunque blockchain se encarga de varios tipos de actividades como la recaudación de dinero (ya sea mediante ICO/IFO/

IEO/etc.), sus aplicaciones siguen estando limitadas a una pequeña gama de eventos. Las NFT amplían en gran medida el alcance de las aplicaciones de la cadena de bloques con la ayuda de sus propiedades adicionales (singularidad, propiedad, liquidez). Esto permite que cada individuo se vincule a un evento específico al igual que los patrones en nuestra vida real. Damos el ejemplo de la venta de entradas. Al comprar entradas en un mercado tradicional de entradas para eventos, los consumidores deben confiar en el tercero. Por lo tanto, existe el riesgo de comprar entradas fraudulentas o no válidas, que son falsas o posiblemente falsificadas o que pueden ser canceladas. La misma entrada puede venderse muchas veces u obtenerse extrayendo de las imágenes de las entradas publicadas en Internet, en un caso extremo.



El "billete basado en NFT" representa un billete emitido por la cadena de bloques para demostrar el derecho de acceso a cualquier evento, como la cultura o el deporte. Una entrada basada en NFT es única y escasa, lo que significa que el titular de la entrada no puede revenderla una vez vendida. El contrato inteligente basado en blockchain proporciona una plataforma transparente de comercio de entradas para las partes interesadas, como el organizador del evento y el cliente. Los consumidores pueden comprar y vender la entrada criptográfica desde el contrato inteligente en lugar de depender de terceros de forma eficiente y fiable.

Los colecciónables digitales contienen una gran variedad de tipos, que van desde las tarjetas comerciales, los vinos, las imágenes digitales, los videos, los bienes inmuebles virtuales, los nombres de dominio, los diamantes, el sello criptográfico y otras propiedades reales/intelectuales. Tomamos como ejemplo el campo de las artes. En primer lugar, los artistas de forma tradicional tienen muy pocos canales para



exponer las obras. Los precios no pueden reflejar el verdadero valor de sus obras debido a la ausencia de atención. Incluso sus obras publicadas en las redes sociales tienen un coste de intermediación por parte de las plataformas y los anuncios.



Los NFT transforman sus obras en formatos digitales con identidades integradas. Los artistas no tienen que transferir la propiedad y los contenidos a los agentes. Esto les proporciona un impulso con muchos beneficios. Algunos ejemplos típicos son el REPLICATOR de Mad Dog Jones (vendido con 4,1 millones de dólares), la obra de Grimes (vendida en total alrededor de 6 millones de dólares) y otras obras de grandes criptoartistas como Beeple. Además, los

artistas, en general, no pueden recibir derechos de autor por las futuras ventas de sus obras. En cambio, las NFT pueden programarse para que el artista reciba un canon predeterminado cada vez que su obra de arte digital se intercambie en los mercados (por ejemplo, SuperRare o MakersPlace). Se trata de una forma eficaz de gestionar y proteger las obras maestras digitales. Además, varias plataformas (por ejemplo, Mintbase y Mintable) han establecido incluso herramientas para ayudar a la gente corriente a crear sus propias obras NFT con facilidad.



El metaverso es un espacio colectivo virtual compartido que permite todo tipo de actividades digitales. En general, abarca un conjunto de técnicas como la realidad aumentada e Internet para establecer el mundo virtual. El concepto surge en las últimas décadas y tiene un gran proceso con el rápido desarrollo de blockchain. Blockchain proporciona un entorno descentralizado ideal para los mundos virtuales en línea. Los participantes en estas realidades alternativas alimentadas por blockchain pueden tener muchos tipos de casos de uso intrigantes como disfrutar de juegos, mostrar artes hechas por uno mismo, comerciar con activos y propiedades virtuales (artes, parcelas, nombres, tomas de vídeo, wearables), etc.

Además, los usuarios también tienen oportunidades de obtener beneficios de la economía virtual. Pueden alquilar los edificios (como las oficinas) a otros para ganar el bono o criar mascotas raras y venderlas para obtener las recompensas. Los principales proyectos impulsados por blockchain son Decentraland, Cryptovoxels, Somnium Space, MegaCryptoPolis y Sandbox.

De hecho, el ecosistema de metaversos abarca todas las aplicaciones mencionadas. Lo enumeramos aquí por separado simplemente porque aún se encuentra en una fase inicial debido a su complejidad.

CUESTIONES DE SEGURIDAD Y PRIVACIDAD



Los datos de los usuarios son la primera prioridad de cualquier sistema. Sin embargo, los datos (almacenados fuera de la cadena pero relacionados con las etiquetas de la cadena) se enfrentan al riesgo de perder la vinculación o de ser utilizados de forma indebida por personas malintencionadas. Los detalles son los siguientes.

En los principales proyectos de NFT, un "hash" criptográfico como identificador, en lugar de una copia del archivo, se etiquetará con el token y luego se registrará en la blockchain para ahorrar el consumo de gas. Esto hace que el usuario pierda la confianza en la NFT porque el archivo original podría perderse o dañarse. Varios proyectos de NFT integran su sistema con un sistema de almacenamiento de archivos especializado, como IPFS, en el que los avisos de IPFS permiten a los usuarios encontrar un contenido siempre que alguien en algún lugar de la red IPFS lo aloje. Aun así, estos sistemas tienen fallos inevitables. Cuando los usuarios "suben" metadatos NFT a los nodos IPFS, no hay garantía de que sus datos se repliquen entre todos los nodos. Los datos

pueden dejar de estar disponibles si el activo se almacena en IPFS y el único nodo que lo almacena se desconecta de la red. Este problema ha sido reportado por DECRYPT.IO y CHECKMYNFT.COM. Además, un NFT podría apuntar a una dirección de archivo errónea. Si ese es el caso, un usuario no puede probar que realmente es dueño de la NFT. En una palabra, depender de un sistema externo como componente principal (almacenamiento) para un sistema NFT es vulnerable.



En la etapa actual, el anonimato y la privacidad de las NFT siguen siendo poco estudiados. La mayoría de las transacciones de NFT se basan en su plataforma subyacente Ethereum, que sólo proporciona un pseudoanonimato en lugar de un anonimato o privacidad estrictos. Los usuarios pueden ocultar parcialmente sus identidades si los vínculos

entre sus identidades reales y las direcciones correspondientes son conocidos por el público. En caso contrario, todas las actividades de los usuarios bajo la dirección expuesta son observables.



Las soluciones existentes para preservar la privacidad (por ejemplo, la encriptación homomórfica, la prueba de conocimiento cero, la firma en anillo, el cálculo multipartito) no se han aplicado todavía a los esquemas relacionados con la NFT debido a sus complicadas primitivas criptográficas y a sus supuestos de seguridad. Al igual que en otros tipos de sistemas basados en blockchain, la disminución de los costos de computación se convierte en la clave para implementar los esquemas con promesa de privacidad.

CONSIDERACIONES SOBRE LA GOBERNANZA



Al igual que ocurre con la mayoría de las criptomonedas, las NFT también se enfrentan a obstáculos como la gestión estricta de la gobernanza. Por otro lado, también es un reto cómo regular adecuadamente esta tecnología naciente con el mercado correspondiente. Analizamos dos cuestiones típicas de ambos lados.

- **Escollos legales.** Las NFT se enfrentan a problemas legales y políticos en una amplia gama de áreas. Las áreas potencialmente afectadas abarcan las materias primas, las transacciones transfronterizas, los datos de KYC (Know Your Customer), etc. Es importante entender el escrutinio normativo y los litigios relacionados antes de adentrarse en las vías de las NFT. En algunos países, como India y China, la situación legal es estricta para las criptodivisas, y también para las ventas de NFT. El intercambio, el comercio, la venta o la compra de NFT tienen que superar las dificultades del gobierno. Legalmente, los usuarios sólo pueden comerciar con derivados en bolsas autorizadas, como acciones y materias primas, o intercambiar tokens

con alguien de persona a persona. Varios países, como Malta y Francia, están intentando aplicar leyes adecuadas con el fin de regular el servicio de activos digitales. En otros lugares, los problemas se resuelven utilizando las leyes existentes. Éstas exigen a los compradores el cumplimiento de condiciones complejas o incluso contradictorias. Por lo tanto, es necesario llevar a cabo la diligencia debida antes de invertir tokens serios en NFT.



- **Cuestiones de propiedad fiscal.** Los productos relacionados con la propiedad intelectual (incluidas las artes, los libros, los nombres de dominio, etc.) se tratan como propiedad imponible en el marco jurídico actual. Sin embargo, las ventas basadas en NFT quedan fuera de este ámbito. Aunque algunos países, como Estados Unidos (Internal Revenue Service, IRS), gravan las criptomonedas como propiedad, la mayoría de las zonas del mundo aún no lo han considerado. Esto puede aumentar en gran medida los delitos financieros al amparo del comercio de NFT.

A los gobiernos les gustaría que la venta de NFT fuera fiable y tuviera consecuencias fiscales. En concreto, los participantes individuales deberían tener la responsabilidad fiscal sobre cualquier ganancia de capital que esté relacionada con las propiedades NFT. Asimismo, deberían gravarse los intercambios de NFT por NFT, NFT por IP y Eth por NFT (o viceversa).

Además, en el caso de los inmuebles de alta rentabilidad, o los coleccionables, debería aplicarse un tramo impositivo más alto. Por lo tanto, se sugiere que los intercambios relacionados con el NFT busquen más asesoramiento de los departamentos fiscales profesionales después de las profundas discusiones.

CAPÍTULO 4: TOKENS ERC-20

INTRODUCCIÓN



En el curso de '[Crea DApps con Tokens NFT en Ethereum usando Truffle y React](#)' hemos visto el nacimiento de Blockchain y la importancia de esta tecnología, ahora centremos en la Blockchain de Ethereum.

La plataforma Ethereum fue creada en 2015 por Vitalik Buterin. Surgió como un instrumento de código abierto para aplicaciones descentralizadas y adoptó la tecnología de cadena de bloques (*blockchain*). Su criptomoneda nativa se llama Ether (ETH) y es un *token* que puede usarse para realizar transacciones en un mismo *software*. [2]



Uno de los motivos por los que se empezó a indagar hasta llegar a una nueva cadena de bloques fue la ausencia de flexibilidad de Bitcoin. Otro de los logros que se han conseguido ha sido mejorar la capacidad de crear nuevas monedas en una *blockchain* existente. Todo con el objetivo de lograr un ecosistema integrado.



¿QUÉ SIGNIFICA EL ESTÁNDAR ERC-20?



Así como hemos explicado en '[Crea DApps con Tokens NFT en Ethereum usando Truffle y React](#)' las siglas ERC significan Ethereum *request for comments*. O lo que es lo mismo, solicitud de comentarios de Ethereum. Un *token* ERC-20 no es más que un *smart contract* o contrato inteligente con una estructura de datos ya preestablecida. Dicho de otra manera, permite una perfecta interacción con otros contratos inteligentes. En cuanto a los objetivos de los



ERCS, el principal es facilitar la implementación de diversas funcionalidades en Ethereum.

Por otro lado, es importante que conozcas que el número 20 proviene del EIP donde se describe. Hoy en día, por su facilidad de creación y versatilidad de usos, son uno de los más populares. El número de tokens ERC-20 está subiendo cada vez más y sus cifras no paran de crecer.

CARACTERÍSTICAS PRINCIPALES DE LOS TOKENS ERC-20



El motivo por el que Ethereum necesita un *token* estándar es por la interoperabilidad. Y como ya se ha mencionado, los tokens ERC-20 se caracterizan por su capacidad de adaptación. Pero para ello tienen que tener una estructura donde se aproveche todo su potencial. A continuación, se nombran algunas de sus características principales:

- Cuentan con un identificador o nombre y un símbolo asociado: Es una manera de poder identificar todos los *tokens* dentro de la *blockchain* de Ethereum.
- Son capaces de manejar aspectos económicos relacionados con su emisión: Hay partes imprescindibles en la estructura de datos de un *token*, como el sistema de precisión decimal y la emisión total.
- Permiten manejar una interfaz y revisar las direcciones de sus dueños: A través de una dirección específica se conoce la cantidad total de los fondos.
- Manejan los retiros parciales de fondos desde una dirección. Para entenderlo mejor, si una persona le pide a otra que retire una cantidad de 1000 ETH, solo podrá

retirar 250 ETH la primera vez. En el próximo retiro, podrá terminar de retirar el resto hasta llegar a los 1000 ETH.



Ethereum se ha posicionado como la segunda criptomonedra más importante del mercado.

¿POR QUÉ SE CREARON LOS TOKENS ERC-20?



Uno de los principales puntos de atención en el curso de '[Crea DApps con Tokens NFT en Ethereum usando Truffle y React](#)' son los motivos que hacen importantes a los tokens ERC-20 y en los objetivos que tienen estos tokens para la sociedad.

Uno de los principales objetivos era la creación de un sistema de capacidad múltiple. Todo dentro de una interfaz que fuese reutilizable por otras aplicaciones como monederos o intercambios descentralizados y en un API (interfaz de programación de aplicaciones) que garantizase ciertas ventajas como las siguientes:

- Uniformidad en la programación: Esta interfaz de programación de aplicaciones (API) es estable y estándar. Esto facilita la tarea de programar cuando se crea el nuevo software.
- Usar la API reduce las dificultades del *software*. Se permite, por tanto, una mayor seguridad y lectura del código escrito. [2]

- La API permite múltiples lenguajes de programación. Entre ellos están JavaScript, Solidity, o Python.
- Mayor facilidad para comprender cada tipo de token implementado.
- Menor riesgo de romper contratos.

PROS Y CONTRA DE LOS TOKENS ERC-20



Los *tokens* ERC-20, como se ha mencionado, son contratos inteligentes que se ejecutan en la *blockchain* de Ethereum. De este modo, tienen su propia unidad de cuenta, evitando así la

mezcla de saldos de Ether de las direcciones. Todo en un marco garantizado por la transparencia, trazabilidad y seguridad que proporciona Ethereum.

Por otro lado, el protocolo ERC-20 no es más que un estándar para crear *tokens*. Esto significa que no todos son útiles o funcionales. A continuación, os mostramos algunas de sus ventajas y desventajas:

Aquí podrás encontrar las ventajas de manera más detalladas:

- Fungibles: Cada unidad puede ser intercambiada con otra. Podrías intercambiar tu *token* por el de otra persona y seguirían siendo iguales.
- Flexibles: Los *tokens* son personalizables y se adaptan a todo tipo de aplicaciones diferentes.
- Populares: Gracias a su gran popularidad, ya podemos encontrar monederos y contratos inteligentes compatibles con los *tokens*.
- Facilitan el trabajo de creación de nuevos *tokens*.
- Los desarrolladores pueden unificar criterios de trabajo dentro de la *blockchain* de Ethereum.

- Interoperatividad de los sistemas.
- Ayudan a la liquidez e incluyen múltiples usos en la *blockchain* de Ethereum.

En cuanto a las desventajas:

- Gran número de *tokens* similares. Esto puede ser confuso para los inversores.
- Escalabilidad: Si envías una transacción en horas claves, puede que se generen comisiones altas y retrasos. Lo mismo ocurre si la red se congestionada. En este caso, la usabilidad podría verse afectada.
- Fraudes: Antes de invertir, asegúrate de estar haciéndolo correctamente. La facilidad de poder lanzar un *token* hace que aumenten las estafas. [2]

¿QUÉ PODEMOS HACER CON LOS TOKENS ERC-20?



Así como se ha comentado en el curso '[Crea DApps con Tokens NFT en Ethereum usando Truffle y React](#)' con los *tokens* ERC-20 podemos consultar el suministro total, transferir fondos y verificar saldos. Además, podemos otorgar permisos a otras DApps para que puedan administrar tokens por nosotros.

Stablecoins

Los *stablecoins* son activos digitales creados para replicar el valor de monedas como el euro o dólar. Con ellos, se permite transferir valor a nivel internacional de manera rápida. Eso sí, esto se lleva a cabo manteniendo siempre una estabilidad del precio.

En el contexto de los *tokens* ERC-20, los *stablecoins*, usan el estándar ERC-20. Explicado en otras palabras, un usuario realiza un contrato con 10.000 *tokens* y otros usuarios podrán canjear esos *tokens* por la cantidad proporcional de moneda fiduciaria.



Security tokens

Pueden entenderse de una forma similar a los *stablecoins*. Operan de la misma forma pero se distinguen por su emisor. Estos representan acciones, activos físicos, valores o bonos. También proporcionan al titular participaciones en negocios o bienes.

Utility tokens

Los *utility tokens* son los más comunes del mercado. Estos no están respaldados por nada. Además, pueden ajustarse a numerosos casos y pueden usarse como moneda de juegos o puntos de fidelidad.



REFERENCIAS

- [1] Tokens, Types, and Standards: Identification and Utilization in Ethereum, https://publik.tuwien.ac.at/files/publik_287890.pdf
- [2] Una introducción a los tokens ERC-20, <https://www.monederosmart.com/una-introduccion-a-los-tokens-erc-20/>
- [3] What are ERC-20 Tokens?, <https://help.crypto.com/en/articles/3957428-what-are-erc-20-tokens>
- [4] Measuring Ethereum-Based ERC20 Token Networks, https://link.springer.com/chapter/10.1007%2F978-3-030-32101-7_8
- [5] Etherless Ethereum Tokens: Simulating Native Tokens in Ethereum, <https://eprint.iacr.org/2021/766.pdf>
- [6] Tokens, Types, and Standards: Identification and Utilization in Ethereum, https://publik.tuwien.ac.at/files/publik_287890.pdf

SOBRE EL AUTOR

Mi nombre es Joan Amengual, y soy graduado en Ingeniería Telemática por la Universidad de las Islas Baleares (UIB). En los últimos años he estudiado y trabajado sobre la tecnología Blockchain.

Concretamente, desarrollé una Aplicación Distribuida basada en Blockchain como Proyecto de Fin de Carrera para solventar la falsificación de títulos universitarios. Juntamente con el equipo de investigación SECOM de la UIB, publicamos el artículo del proyecto Blockchain en la conferencia española de ingenieros telemáticos, JITEL 2021.

En el campo profesional estoy trabajando en el campo de la Inteligencia Artificial (IA) basada en el razonamiento y los almacenes asociativos basados en la memoria con una empresa tecnológica de Silicon Valley, USA. Mediante este pequeño libro pretendo dar a conocer las bases fundamentales y los pilares principales de la tecnología blockchain y de los tokens, y así dar a conocer todo su potencial de cara al presente y al futuro que nos espera.

