everiToken

DOCUMENTO TÉCNICO

Versión 3.1

Zug, Suiza

Última actualización: 26 de marzo de 2019

AVISO LEGAL

- - El documento técnico de everiToken es solo para fines informativos.

- - Este documento técnico no representa ninguna garantía expresa o implícita, prueba o expectativa, etc.

- - Las especificaciones técnicas o los métodos de realización escritos en el whitepaper técnico pueden cambiar con el tiempo.

- - El equipo técnico adherido a éste proyecto puede ser disuelto o reestructurado en cualquier momento, o la pérdida de los técnicos principales puede llevar al fracaso o la realización parcial de dicho proyecto.

- - Este documento técnico se proporciona "tal cual". Ni el equipo del proyecto, ni ningún miembro del proyecto son responsables por el contenido o los resultados derivados del uso futuro de este contenido.

- - El token al que hace referencia este documento técnico no tiene ningún valor práctico, solo se usa en el mundo virtual, y su único propósito es confirmar los permisos de usuario del token.

- - Cualquier evento dentro de la cadena de bloques o sus derivados, que se ejecute con la tecnología descrita en este whitepaper técnico, se genera automáticamente mediante la automatización del programa y el equipo no se hace responsable de sus consecuencias. Los individuos u organizaciones dando uso a esta tecnología son responsables de sus consecuencias inherentes al usar la cadena de bloques everiToken.

- - Todo el contenido de este whitepaper técnico se puede utilizar bajo la premisa de uso no comercial, sin embargo, el whitepaper técnico no debe modificarse ni alterarse de ninguna manera. El equipo no se hace responsable de ningún efecto que resulte del uso del contenido de este documento.

everiToken

Contenido

Parte I. Origen y visión

La llegada de la economía del token

La tecnología blockchain (cadena de bloques) cumplió 10 años en febrero de 2019. A pesar de su evolución a lo largo de este tiempo, una pregunta clave aún persiste: ¿Está revolucionando la producción la tecnología blockchain, creando valor para la economía global?

Veamos los datos: Actualmente, los activos administrados en blockchains (referidos como "on-chain") son básicamente una variedad de monedas / monedas digitales, con un valor de mercado total de aproximadamente $ 150 mil millones de dólares. Los activos en estas cadenas se caracterizan generalmente por una alta volatilidad y una fuerte especulación, sin proporcionar beneficios para la economía global. De hecho, desde la aparición de Satoshi Nakamoto , más y más personas han querido convertir estas "monedas" en una divisa con atributos de pago, aunque hasta ahora sirven principalmente como monedas digitales y no desempeñan un papel de moneda tradicional. Una moneda digital es más un nombre que una divisa operativa real.

Por un lado, el derecho a emitir moneda es una decisión política, y el poder monetario debe pertenecer al estado. Por lo tanto, es muy difícil para una criptomoneda reemplazar a una moneda fiduciaria. Sin la autorización y el apoyo del estado, la llamada "moneda digital" es solo una búsqueda idealista.

Por otro lado, la mayoría de los activos globales (tangibles e intangibles) no están en blockchains (denominados "off-chain"), y existe una interacción limitada entre blockchains y activos off-chain.

Entonces, ¿es un token simplemente otra moneda digital? De ningún modo. La definición básica de token es "símbolo, signo" (proveniente del inglés), aunque debería considerarse más apropiadamente como un certificado en lugar de una moneda digital. Dichos certificados pueden representar todo tipo de derechos e intereses, incluidos puntos de compra, cupones, tarjetas de identidad, diplomas, bienes raíces, claves de acceso, boletos para eventos e incluso una amplia variedad de comprobantes de ciertos derechos e intereses. Mirando hacia atrás en la historia, la prueba de los derechos e intereses ha sido un elemento esencial de todas las

civilizaciones de la sociedad humana. Las cuentas, propiedad, calificaciones, pruebas, etc. son todas una representación de derechos e intereses. Como Yuval Noah Grali autor de *Sapiens. De animales a dioses* planteó, "son estos 'hechos ficticios' los que constituyen las razones principales para que los hombres sabios destaquen y construyan una civilización humana". Si estas pruebas de derechos e intereses fueran todas digitales, electrónicas y protegidas criptográficamente para verificar su autenticidad e integridad, la civilización humana sería revolucionada. A este fenómeno lo llamamos la **economía del token**.

La ejecución de certificados on-chain proporciona una base sólida de confianza y trazabilidad que no proporciona ninguna infraestructura centralizada tradicional. Por lo tanto, si un certificado representa la unidad económica en la economía del token, entonces la cadena de bloques (blockchain) es la tecnología que representa los cimientos de la economía del token. Ambos están estrechamente vinculados y son co-dependientes.

Análisis Competitivo

Como blockchain pública, nacida para la economía del token, everiToken tiene actualmente dos competidores principales, Ethereum y EOS. Nuestra ventaja competitiva es indudable, al analizar las fortalezas, debilidades, oportunidades y amenazas dentro de nuestro mercado.

FD (Fortalezas y Debilidades):

everiToken cree que la tecnología blockchain para la economía del token debería gestionar de manera efectiva la prueba de los derechos e intereses, principalmente enfocada en los siguientes tres aspectos:

1. **Prueba de Derechos Digitales e Intereses:** el certificado debe ser un formato de derechos e intereses digital y creíble, respaldado por algo de valor intrínseco e inherente (ya sea tangible o intangible).
2. **Seguridad, Encriptación y Gestión de Autorización:** el certificado debe ser verificable, a prueba de falsificaciones, protegido por la privacidad, supervisado, protegido por criptografía, y ser utilizado únicamente por los autorizados.
3. **Negociabilidad:** El certificado puede ser comercializado e intercambiado convenientemente.

De acuerdo con los requisitos anteriores, presentamos un conjunto de soluciones para satisfacer las necesidades básicas de la economía del token, con el fin de promover la gestión y la circulación de tokens y construir los cimientos técnicos para la economía del token. Por ello, hemos hecho posibles las siguientes tres características principales específicamente de acuerdo con los requisitos anteriores.

- **Emisión de Tokens Rápida y Conveniente:** El usuario no necesitan escribir código, por lo que puede emitir fácilmente sus propios tokens a través de nuestra API (para aplicaciones, páginas web o aplicaciones de terceros).

- **Transferencia de Tokens Eficiente:** habilitando la transferencia de tokens en cuestión de segundos, capaz de soportar simultáneamente un volumen de cientos de millones de tokens.

- **Gestión de Autorización Flexible:** un modelo simple, elegante y unificado que ofrece gestión de autorizaciones, admite la tenencia a múltiples personas, recuperación de claves privadas, autoridad de varios niveles, legalidad, supervisión gubernamental y otros requisitos complejos sin la necesidad de programación adicional.

Echémosle un vistazo a Ethereum y EOS:

Ethereum: ERC20 / ERC721

La principal forma de lograr una economía del token con Ethereum es desarrollar contratos inteligentes (llamados “Smart Contracts”) basados en los protocolos ERC20 y ERC721. Entre ellos, ERC20 admite FT (fichas fungibles) y ERC721 es compatible con NFT (fichas no fungibles). Sin embargo, conlleva serios problemas:

- **TPS:** Actualmente, Ethereum solo puede soportar menos de 20 transacciones por segundo y no alcanza a satisfacer todas las necesidades prácticas de uso y circulación de fichas.

- **Costo:** La implementación de smart contracts en Ethereum requiere una tarifa de gas por cada paso. Para funciones con lógica empresarial compleja (como tenencia de múltiples personas, supervisión, legalidad, etc.), el costo puede llegar ser alto e incontrolable.

- **Popularizar:** La economía del token en Ethereum se basa en contratos inteligentes, los cuales no son accesibles sin el uso de aplicaciones de terceros para personas que no tienen conocimientos de programación, debido a su naturaleza compleja. Esto crea problemas de seguridad y regulatorios, al igual que evita la adopción masiva.

- **No estandarización:** dado que los diferentes contratos inteligentes pueden requerir ideas de desarrollo completamente diferentes, los metadatos de estos tokens virtuales son incompatibles, y por ello aislados. Esto no es propicio para el desarrollo ecológico de la economía del token; Además, los usuarios no disponen de una forma unificada para consultar todos los diferentes tipos de token que tienen en su posesión.

EOS

EOS lanzó su red principal "mainnet" de la cadena de bloques en junio de 2018. El objetivo principal de EOS era remediar los problemas dados en Ethereum mediante la creación de nuevas soluciones. Sin embargo, esto ha creado un rango de problemas totalmente nuevo:

- **Seguridad:** las transacciones de tokens pueden representar entidades reales extremadamente valiosas y no renovables, por lo que es importante que no haya problemas de seguridad. Sin embargo, el desarrollo general que continúa basándose en contratos inteligentes está limitado por el nivel de competencia de los desarrolladores, y es difícil asegurar que todos los tipos de desarrolladores de tokens tengan suficiente conciencia de seguridad.

  Los contratos inteligentes de EOS se basan en **WebAssembly,** que es relativamente nuevo y aún está en la etapa de prueba (Beta). Además, el código de smart contracts (contratos inteligentes) de EOS es de carácter "turing completo" y tiene una autoridad excesiva, lo que lo hace vulnerable a las lagunas de seguridad no intencionales.

  La mayoría de las personas no pueden escribir contratos seguros e inteligentes. Para emitir y transferir tokens, los usuarios deben confiar en aplicaciones de terceros y deben confiar en la calidad del código de dicho tercero. Por lo tanto, el control de los activos no está en manos de los usuarios, sino que el control se cede a un tercero.

- **No estandarización:** al igual que Ethereum, los metadatos de diferentes contratos inteligentes no pueden interactuar o cooperar juntos.

- **Regulación, confianza y legalidad:** debido a la experiencia técnica requerida por la no estandarización y la lectura de códigos, es difícil para el gobierno lograr la regulación. Del mismo modo, no desarrolladores pueden encontrar dificultades para decidir si pueden confiar en los programas relevantes, lo que dificulta la aceptación de las cadenas de bloques por parte de la gente común y los gobiernos.

- **Eficiencia de ejecución:** para satisfacer diversas necesidades, las funciones de contratos inteligentes de EOS son complejas, los módulos del sistema son numerosos y la programación y distribución de los recursos son difíciles. En conjunto, esto aumenta enormemente la complejidad del sistema y reduce la velocidad de operación. Debido a los posibles conflictos entre diferentes datos y funciones, el uso de "multihilo" (multithread) con el fin de aumentar la velocidad no es fácil, y los costes de programación son altos. Sin embargo, para la economía del token, estas funciones complejas son cruciales y deben ser resueltas.

- **Popularizar:** Las necesidades comerciales de la economía global son complejas, variables y carecen de coherencia. Sin embargo, los contratos inteligentes toman tiempo para desarrollarse y probarse, lo que dificulta la solución de las necesidades de diversos mercados en un corto período de tiempo. Esto es un obstáculo para el desarrollo de la economía del token.

La principal diferencia entre everiToken y otros es que everiToken usa así denominados *safe contracts* (contratos seguros*),* mientras que otros usan contratos inteligentes. Eso significa que everiToken no es turing completo y habrá algunos escenarios de aplicación complicados que everiToken no puede satisfacer. Sin embargo, everiToken puede satisfacer el 99% de la demanda de la economía del token, y everiToken es la cadena pública más segura, rentable y fácil de usar para todas las personas en todo el mundo.

OA (Oportunidades y Amenazas)

Junto con las fortalezas de everiToken, hemos creado el estándar EvtLink, que se utiliza para conectar a pagadores y beneficiarios a través de una variedad de canales

de datos que incluyen NFC, Bluetooth y código QR. Basado en EvtLink, everiPay es un protocolo de pago nacido para **micropagos cara a cara en tokens** que utiliza la blockchain pública everiToken como infraestructura central y everiPass como su protocolo de validación de propiedad de tokens. everiPay/everiPass incluye el estándar de generación de **códigos QR** y la definición de protocolo de comunicación. Hemos logrado una impresionante lista de características con nuestras innovaciones:

- **Liquidación instantánea:** una transacción es una liquidación.
- **Descentralización:** pago P2P, sin plataforma centralizada, nadie puede modificar los datos en la cadena y todos pueden participar en el pricing.
- **Más seguro:** los datos y el contenido dentro de la cadena de bloques no se pueden falsificar ni manipular, a fin de maximizar la protección y la seguridad de las propiedades del usuario.
- **Compatible:** everiPay/everiPass admite todos los tokens compatibles con everiToken, así como divisas, puntos e incluso una llave para abrir una puerta. Puedes usarlo en casi todas partes con solo un teléfono.
- **Más conveniente:** incluso si no puede conectarse a Internet, puede completar la transacción.

Basándose en las cinco características anteriores, everiPay/everiPass puede proporcionar el servicio más seguro, conveniente y fácil de usar del mundo para pagos cara a cara y propiedad de tokens.

Resumen

Todavía existen algunas amenazas. Como se mencionó, Ethereum y EOS pueden ser una gran cadena pública para ciertas necesidades específicas dentro de la economía de fichas. Sin embargo, el mayor problema para Ethereum / EOS es la alta barrera de entrada para los usuarios creada por la naturaleza de los contratos inteligentes. Hemos resuelto este problema con el desarrollo del contrato seguro, y everiToken ahora está preparado para respaldar una economía mundial de fichas para todas las personas.

Basándonos en el análisis anterior, hemos diseñado un nuevo concepto que es

perfectamente adecuado y preferible para la mayoría de las aplicaciones de blockchain y proponemos una nueva cadena pública y ecosistema, **everiToken**, para promover el desarrollo de la economía del token. Los activos, certificados y comprobantes del mundo real se pueden **digitalizar** mediante la emisión de tokens y se pueden usar fácilmente con seguridad, velocidad y compatibilidad de red sin precedentes.

Parte II. Tecnología de everiToken

Contrato seguro “Safe Contract”

Los contratos inteligentes, en teoría, son un medio digital eficaz para facilitar los intercambios descentralizados de bienes o servicios sin la necesidad de un intermediario. Sin embargo, en la práctica, los contratos inteligentes adolecen de vulnerabilidades de seguridad generalizadas que surgen de una implementación incorrecta y errores lógicos, lo que da lugar a consecuencias tales como bloqueos, acceso filtrado y terminaciones incorrectas. Como tales, los contratos inteligentes a menudo no proporcionan un nivel de confianza suficiente y pueden considerarse menos confiables que los contratos o intercambios tradicionales.

everiToken presenta la novedosa idea de *contratos seguros* a través de nuestra capa para APIs. En lugar de codificar directamente, los usuarios confían en contratos seguros para facilitar procesos como la emisión y transferencia de tokens. Al simplificar las funciones a los requisitos básicos, los contratos seguros aseguran que todas las transacciones en cadena sean seguras y sin lagunas, ya que las funciones API disponibles se revisan y verifican por completo. A pesar de que los contratos seguros no son de carácter Turing completo, aún pueden lograr la mayoría de las funciones necesarias a través de las APIs, y proporcionar flexibilidad a los emisores de tokens para completar los servicios fuera de la cadena.

Además, los contratos seguros tienen los beneficios adicionales de aumentar la accesibilidad y las TPS. Con respecto a lo primero, la inclusión de APIs simplifica la fácil integración en los flujos de trabajo existentes sin tener que escribir código de integración en cadena desde cero. En lo que respecta a este último, el uso de API permite distinguir fácilmente varios tipos de traducciones, y las transacciones de token independientes se pueden procesar en paralelo a velocidades más rápidas (10.000 TPS logrados en la red principal: diciembre de 2018).

Base de datos

EOS utiliza una base de datos de memoria basada en Boost.MultiIndex (Chainbase) que admite operaciones de reversión. Los resultados de todas las operaciones del contrato existen en la base de datos de memoria. Para admitir la reversión cuando se

bifurca y la recuperación cuando el código del contrato es anormal, es necesario registrar datos adicionales para la reversión en cada operación. Además, todos los datos se almacenan y procesan en la base de datos de memoria. Con el aumento de usuarios y transacciones a lo largo del tiempo, es previsible que la demanda de memoria aumentará significativamente. Esto dará lugar a una alta demanda de capacidad de memoria de los productores del bloque. Además, si el programa se bloquea o se reinicia, los datos de la memoria se perderán. Para restaurar los datos, deberíamos repetir todas las operaciones en los bloques, lo que lleva a un tiempo de arranque en frío largo y es poco práctico.

Al preservar la base de datos de memoria de EOS, desarrollamos una base de datos de token basada en RocksDB que tiene varios beneficios:

- RocksDB es una base de datos muy madura, de nivel industrial y de valor clave que se ha verificado completamente y se utiliza en el clúster central de Facebook.
- RocksDB se basa en LevelDB, pero proporciona un mejor rendimiento y una funcionalidad más rica que LevelDB. También permite la optimización de situaciones de almacenamiento de baja latencia, como Flash o SSD.
- Si es necesario, RocksDB se puede utilizar como una base de datos de memoria.
- La arquitectura basada en RocksDB, naturalmente, admite el retroceso y la persistencia de las versiones, y su influencia en el rendimiento es extremadamente baja.

Nuestra base de datos de tokens tiene RocksDB como su motor de almacenamiento subyacente. Hemos optimizado completamente las operaciones relacionadas con tokens para maximizar el rendimiento. Con esta tecnología, podemos lograr una reversión a un costo menor. Además, la base de datos de los tokens también admite funciones opcionales, como la persistencia de datos, la copia de seguridad cuantitativa y la copia de seguridad incremental para resolver problemas como el arranque en frío.

Debido a que las operaciones en everiToken son altamente abstractas, el código es fijo y la información requerida para cada operación es mínima. Por lo tanto, la redundancia de datos es muy baja en comparación con los sistemas generales como EOS, que también reduce el tamaño de los bloques.

Modelo del Token

Visión general

Nacido para la economía de token, everiToken es único con su método de gestión de tokens, basado en tokens. Los tokens son diferentes de las monedas digitales emitidas por los bancos centrales y las monedas encriptadas (Bitcoin o ETH).

Definimos un token como una prueba de que usted tiene una participación exclusiva de la economía en un activo, un período de tiempo, un lugar en particular o un servicio basado en el tiempo proporcionado por una entidad en particular. Los tokens se dividen en dos tipos: tokens fungibles (FT) y tokens no fungibles (NFT). Existen algunas diferencias en sus escenarios y estructuras de aplicación. Según nuestro análisis, las fichas no fungibles pueden desempeñar un papel más extenso en la economía de fichas. Por lo tanto, comenzaremos nuestro análisis con fichas no fungibles.

Tokens no fungibles

Antes de comprender los tokens no fungibles, consideremos una gran cantidad de piedras en una playa. En el mundo real, cada piedra en una playa tiene un peso, apariencia y tipo de roca diferentes. No hay dos piedras exactamente idénticas. Además, las piedras no se pueden combinar fácilmente entre sí. Por lo tanto, decimos que cada piedra es "indivisible" y "no se puede combinar".

Un ejemplo en blockchain es CryptoKitties, que en su día fue un juego candente en el mundo de blockchain. Cada gato tiene números y atributos únicos. Un NFT es similar a un gato individual, piedra o blockchain. Es naturalmente diferente y único en el mundo real, al igual que los NFT en nuestro sistema.

En términos generales, los NFT se dividen en diferentes categorías según sus diversos tipos de valor. Podemos categorizar tipos similares de NFT para formar un dominio.

Concentrarse en tokens permite la característica de alta estandarización de everiToken. Todos los tokens personalizados emitidos por los usuarios satisfacen la misma estructura. Específicamente, cada token contiene un **nombre de dominio**, que corresponde a un **dominio** específico (es decir, la clasificación a la que pertenece el token). El emisor también designa un **nombre al token**, que debe ser único dentro del

dominio. Un nombre de token por lo general tiene un significado especial. Por ejemplo, el código de barras de un producto se puede utilizar como una regla de denominación, que incluye información sobre el país de origen y el fabricante del producto. La unicidad de cada token está determinada por el nombre de dominio junto con el nombre del token. Además, se incluye información sobre la propiedad y cada token tiene al menos un **propietario**.

Como se mencionó anteriormente, la **identificación** de un token está determinada únicamente por el nombre de dominio y el nombre del token. La estructura básica de un token se muestra en la Figura 1. Además de la ID del token, la estructura también muestra el propietario del token y otra información necesaria.

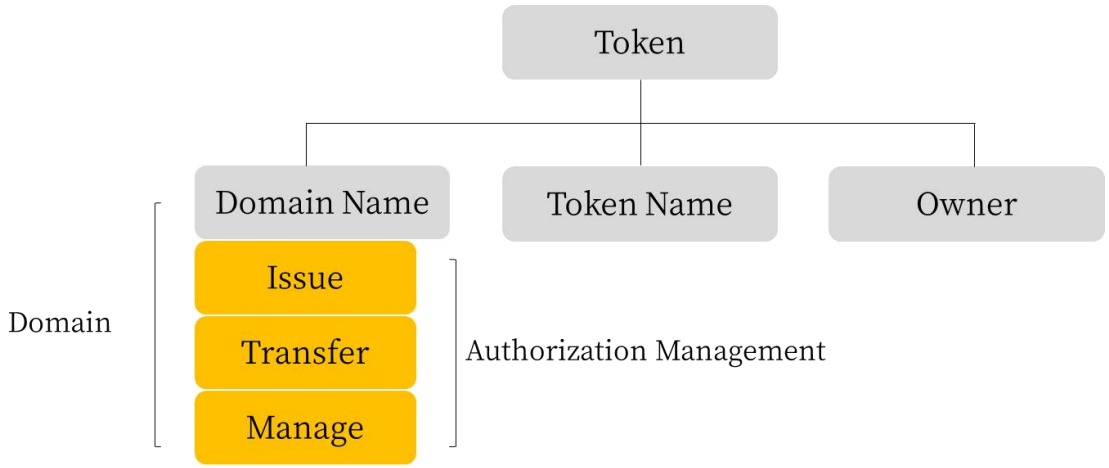


Figura 1. La estructura simbólica de everiToken.

Los detalles del dominio pueden ser consultados por el nombre del dominio. Cada dominio también muestra su información relativa a la administración de autorizaciones.

Toda persona tiene derecho a emitir su propio token. El token en sí no tiene ningún valor y su utilidad está respaldada por el crédito real del emisor. Una vez que se emite un token nuevo, se puede transferir a otros a través de transacciones.

Para los NFT, la transferencia de un token significa cambiar el propietario de ese token. Cada token tiene un **grupo de propietarios** (puede haber uno o más propietarios). Cuando se necesita un cambio en el grupo propietario, un miembro de la circulación del token puede confirmar la operación generando una firma digital, y el grupo propietario del token cambia después de que el nodo de everiToken confirme

que la transacción cumple con los requisitos de permiso y se sincroniza con el otro. nodos

Gestión de autorizaciones

El sistema everiToken contiene tres tipos de permisos con respecto a la administración de autorizaciones: Emisión, transferencia y administración.

(1) **El problema** es el derecho a emitir tokens en este dominio.

(2) **La transferencia** es el derecho de transferir tokens en este dominio.

(3) **Administrar** es el derecho de modificar el dominio, incluida la administración de autorizaciones y otros parámetros.

Cada autorización específica sigue una estructura de árbol y, por lo tanto, se denomina **árbol de autorización**. Como raíz, cada permiso tiene un umbral y está conectado a uno o más actores.

Los actores

Los actores se pueden clasificar en tres grupos: cuentas, grupos regulares y grupos de propietarios. Las cuentas son usuarios individuales, los grupos son cuentas agrupadas y un grupo propietario es una forma especial de grupo regular.

Un grupo puede ser un club, una empresa, un departamento gubernamental, una fundación o incluso un individuo. Un grupo retiene la clave pública del grupo, las claves públicas y los pesos de cada miembro. Las operaciones se aprueban cuando el peso total de todos los miembros autorizados en un grupo que aprueba la operación cumple con el umbral requerido del grupo.

Al mismo tiempo, el miembro que posee la clave pública del grupo puede autorizar modificaciones en los miembros del grupo y sus ponderaciones. Este mecanismo se denomina **autonomía grupal**.

Cuando se inicia un grupo, el sistema genera una ID de grupo automáticamente. Cuando el emisor diseña la gestión de autorizaciones para un dominio, puede invocarse haciendo referencia directamente al ID de grupo existente a su sistema de permisos. Debido a la autonomía del grupo, cada grupo puede ser reutilizado convenientemente.

El propietario del token tiene un nombre de grupo especial con nombre fijo '.owner' que representa una colección de los propietarios de un token. Es especial y dinámico

porque siempre se refiere a los propietarios reales de cada token, y la condición de autorización del grupo es que todos estén de acuerdo dentro del grupo (es decir, el peso de cada persona en el grupo es 1, y el umbral del grupo es el número de miembros en el grupo).

Administración

Las autorizaciones son iniciadas por los emisores de tokens, y cada autorización es administrada por al menos un grupo. Cuando se emite el token, el emisor especifica la información y el peso relativo de cada grupo bajo cada autorización y también establece un umbral asociado al token. Antes de ejecutar una operación en un determinado dominio, el sistema primero verificará si el grupo operativo tiene suficientes ponderaciones, y la operación solo se aprobará si las ponderaciones superan el umbral. Este diseño de agrupación es adecuado para muchas situaciones en el mundo real, y la configuración flexible de pesos y umbrales satisface todo tipo de necesidades complejas. Un ejemplo se da en la Figura 2.

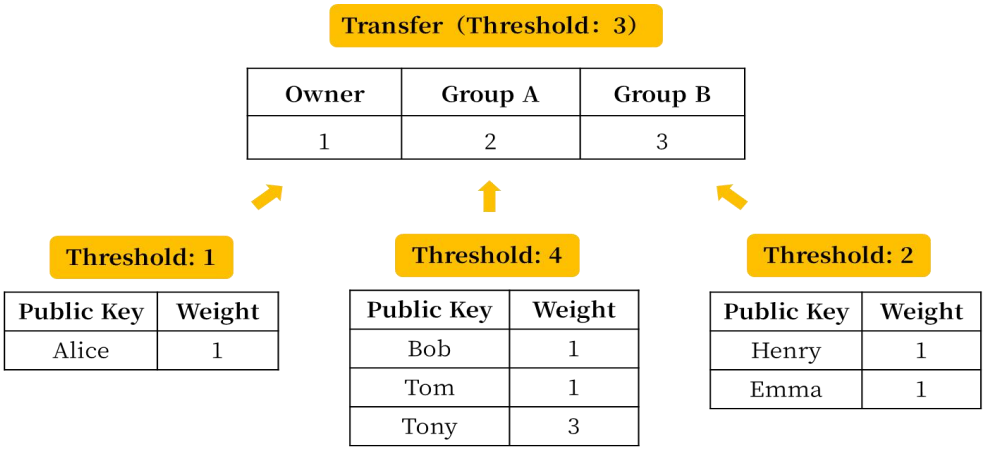


Figura 2. Permisos de transferencia

La figura 2 describe los permisos de transferencia de un dominio. El valor de umbral es 3, y hay tres grupos involucrados: Propietario, Grupo A y Grupo B. Según el conjunto actual de ponderaciones para cada grupo (1, 2 y 3, respectivamente), el Propietario y el Grupo A necesitan autorizar juntos, o el Grupo B puede autorizar solo para cumplir el umbral de transferencia.

Para cada grupo, el propietario está autorizado solo por Alicia; El Grupo A puede satisfacer su umbral (4) mediante autorizaciones de al menos Bob/Tony o Tom/Tony; El grupo B debe ser autorizado por Henry y Emma para cumplir con el umbral (2).

Cualquier usuario tiene el derecho de emitir tokens, pero los escenarios de destino de tokens en cada dominio son diferentes. Por ejemplo, la transferencia de propiedad debe ser revisada por agencias gubernamentales relacionadas con una supervisión estricta; Las tarjetas de membresía y los cupones de la cadena necesitan la marca de la compañía para respaldarlos; un boleto de un concierto no sirve para nada después del concierto, pero el propietario de un espacio de estacionamiento fijo puede cambiar con el tiempo

Al emitir tokens, el emisor del token puede implementar la administración de autorizaciones mediante el diseño de permisos en el dominio. El siguiente escenario demuestra la conveniencia de la gestión de autorizaciones.

La Figura 3 muestra cómo se pueden resolver problemas complejos utilizando el mecanismo de administración de autorizaciones de everiToken.

Una empresa ha construido un nuevo edificio de oficinas y espera emitir 1000 fichas con los derechos de propiedad del edificio. La compañía configura un SPV (Vehículo de propósito especial) para emitir y mantener estos tokens. En la vida real, la emisión de tokens y la transferencia de la propiedad deben ser examinadas y aprobadas por la oficina de propiedad local. Deben emitirse de conformidad con los estándares locales, y luego los detalles del token (total, emisor, estructura de gestión de autoridad, etc.) se pueden mostrar en su plataforma oficial. Además de eso, el departamento central de propiedad tiene la autoridad más alta para limitar y administrar la oficina de propiedad y los propietarios locales.

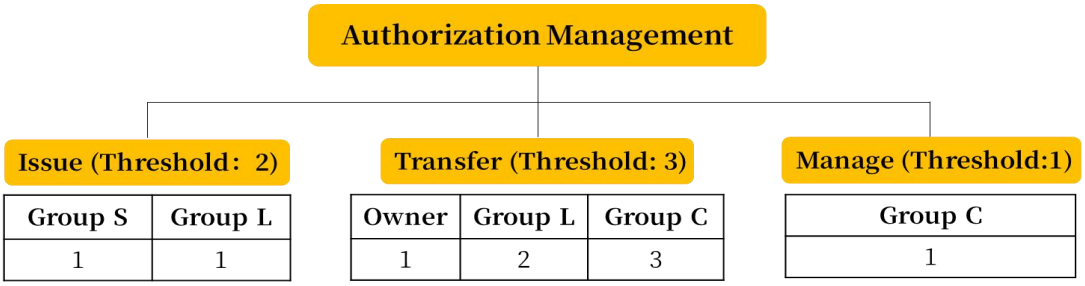


Figura 3. La estructura de gestión de autoridad.

El grupo S representa el SPV, el emisor y el propietario inicial del token en el dominio. El **Grupo L** representa la oficina de propiedad local, y el **Grupo C** representa el departamento de propiedad central.

En la mayoría de los casos, la transferencia de un token solo necesita la autorización del propietario y la oficina de propiedad local (peso combinado de 3, que cumple con el umbral). En este proceso, la oficina de propiedad local audita la operación de transferencia. En el caso de un accidente, como el propietario de un token que ha fallecido o perdido una clave privada, el departamento central de propiedad puede transferir la propiedad del token al heredero legal después de un juicio, revisión del tribunal o departamento correspondiente.

Si tanto el SPV como otros propietarios de tokens aceptan agregar tokens nuevos, pueden agregarlos al obtener la autoridad emisora para satisfacer las necesidades reales. Además, la estructura de gestión de autorizaciones también es adecuada para el manejo de casos extremos. Por ejemplo, si el departamento central de propiedad necesita congelar temporalmente la propagación de este tipo de token, puede cambiar el umbral de los permisos de transferencia a través de los permisos de administración que posee, con lo que se congela la circulación de todos los tokens en el dominio.

Tokens Fungibles

Emisión

Todos pueden emitir tokens fungibles después de registrarse con un símbolo único, como EVT. Los usuarios pueden establecer el número total de tokens en circulación con este símbolo. Luego, los usuarios pueden decidir la cantidad de tokens que desean emitir de inmediato.

Transferencia

Todos los que tengan su propia clave privada pueden transferir sus tokens a otros.

Otros detalles

Cada cuenta registrará la cantidad de fichas que se guardarán junto con los símbolos asociados. Habrá un registro independiente de clave-valor para almacenar información básica de tokens con diferentes símbolos. Los usuarios también pueden permitir que otra clave privada tenga derecho a transferir números específicos de tokens con un símbolo específico. Esta función se denomina **asignación de tokens** y se puede utilizar en el intercambio de tokens.

Modelo de transacción basado en tokens

Visión general

everiToken emplea el **modelo de transacción basado en token** en relación con todos los tokens dentro de nuestro sistema.

En resumen, para cada token en un libro de contabilidad (“ledger”) basado en tokens, creamos un espacio de datos independiente para almacenar el historial completo de la propiedad de un token. De esta manera, es muy fácil lograr paralelismo de multi-núcleo (“multi-core paralleling”) y fragmentación (“sharding”), dado que el espacio de datos de un token no tiene relación con otros tokens. Como resultado, las operaciones de varios tokens se pueden hacer fácilmente de manera paralela sin conflicto. Esto permite un rendimiento súper alto y mejora constante de TPS al fragmentar o agregar fácilmente más núcleos de CPU.
El modelo de transacción basado en token fue inventado por varios miembros del equipo central de everiToken y se ha comprobado que funciona perfectamente para NFT en everiToken.

Un blockchain basado en el modelo de transacción basado en tokens, como everiToken, podría dividir la base de datos en dos partes, una es Token DB y la otra Block DB. La primera es donde opera el modelo de transacción basado en token, que almacena y administra los espacios de datos de todos los tokens no fungibles. El bloque DB, el segundo, almacena los bloques originales.

Tanto Token DB como Block DB deben ser una base de datos de varias versiones para un rápido retroceso cuando se invierte un bloque. Por ejemplo, everiToken utiliza Rocks DB como sistema de base de datos subyacente al Token DB.

Tanto Token DB como Block DB son bases de datos de solo apéndice. Entonces, cada vez que alguien actualiza un registro, el nuevo valor con la versión aumentada se agregará a la base de datos. Sin embargo, el registro que contiene la versión anterior no se eliminará.

Token DB

Token DB es una base de datos indexada para buscar y cambiar rápidamente el estado

más reciente de la cadena de bloques, como la propiedad de los tokens y el saldo de la cuenta de tokens fungibles en la cadena.

Token DB podría considerarse una base de datos clave-valor. La clave indica el ID de los tokens y el valor representa la propiedad actual de los tokens. Debido a que la base de datos es solo de adición, habrá muchos valores para cada clave, pero solo el último valor representa el estado actual de propiedad del token, mientras que los otros son solo para referencia histórica y reversión. Para cada token, habrá un espacio de datos independiente que incluye todo el historial de propiedad, al igual que una cadena separada.

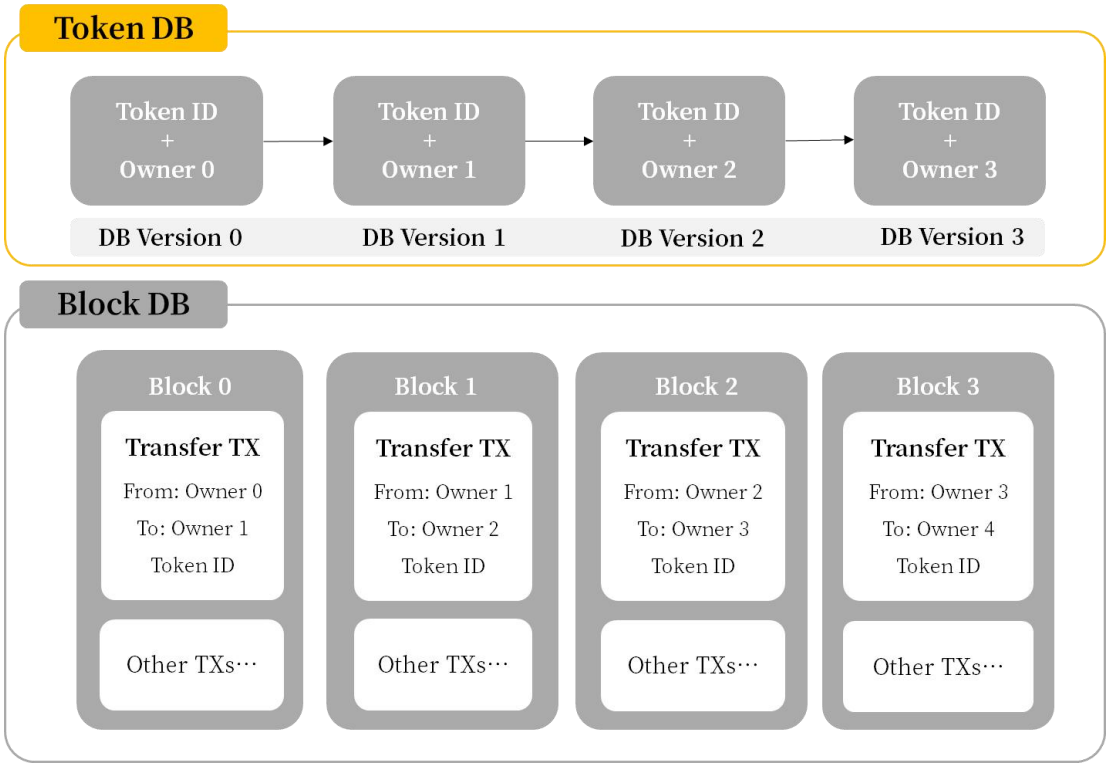
El primer valor de la cadena es la propiedad inicial. Por ejemplo, cuando uno ejecuta una transacción, la nueva propiedad se agregará a la base de datos. Las versiones antiguas podrían usarse para revertir el valor si el bloque necesita ser revertido y eventualmente se recolectará la basura.

Debido a que cada token tiene un espacio de datos independiente, la fragmentación se vuelve muy fácil. Por ejemplo, si tenemos dos computadoras para un nodo, podríamos dejar que cada computadora procese la mitad de los tokens. Si hubiera 100 tokens, la primera computadora procesaría los tokens 1 a 50, y la segunda para los tokens 51 a 100. Debido a que cambiar el propietario de un token no afectará a otros tokens, las dos computadoras podrían procesar de manera paralela.

Bloque DB

El bloque DB se encarga de almacenar todos los bloques originales e irreversibles de la cadena. Cada bloque almacena toda la información detallada, incluidos los nombres, los parámetros de las acciones ejecutadas, las firmas en el bloque y más.

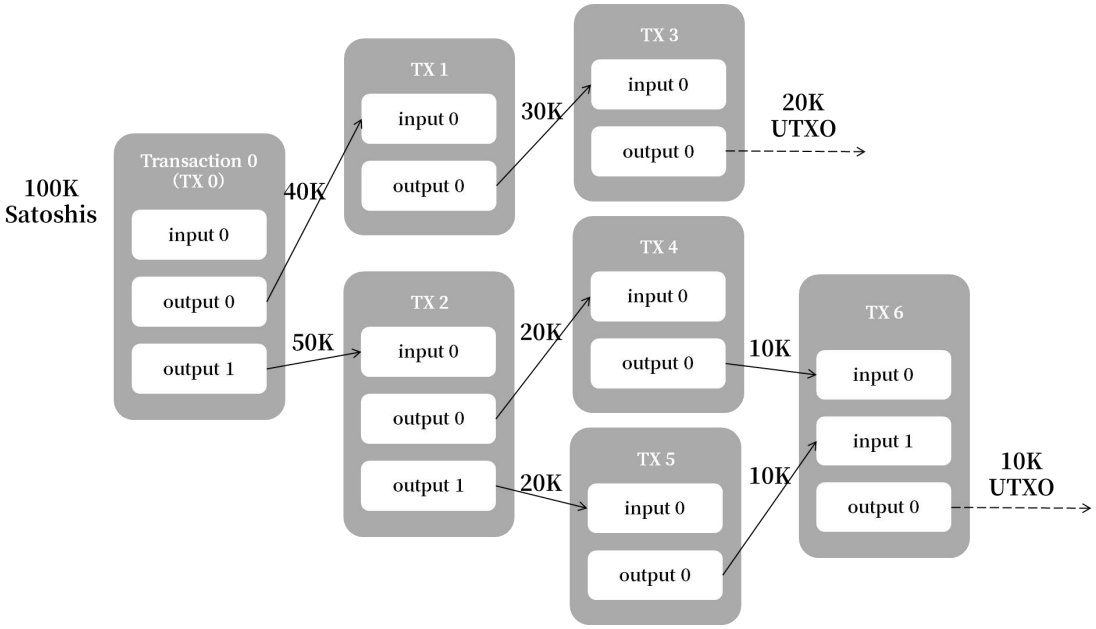
El siguiente gráfico muestra cómo dos tipos de bases de datos trabajan juntas para los NFT:



Comparaciones de modelos de transacción

a) UTXO

En el modelo UTXO, cada propietario de tokens transfiere un token que tiene en posesión a otro propietario firmando digitalmente el hash de una transacción anterior y la clave pública (dirección) del siguiente propietario, agregando esto al final de la moneda. El mecanismo es esencialmente una transgresión continua de entradas y salidas donde el propietario de tokens en realidad no posee directamente los tokens, sino que posee la salida a un número específico de tokens que luego se pueden firmar como una entrada para un nuevo propietario, que luego controla las nuevas salidas.



(Fuente: bitcoin.org)

Como puede ver, UTXO es ideal para evitar "double-spending" (doble gasto), ya que es obvio que cualquier entrada solo se puede usar una vez, pero también tiene algunas desventajas:

- BTC no es un tipo de NFT, es un FT. Es inútil mantener una ID única para cada UTXO. (everiToken soporta tanto NFT como FT)

- UTXOs son únicas. Es un desperdicio de recursos informáticos y volumen de disco, almacenar una gran cantidad de UTXO.

b) Basado en cuentas

El modelo de transacción basado en cuentas es como lo que hace un banco. Crea una cuenta en un banco y luego ahorra dinero en la cuenta, cambiando el saldo. Esto es completamente diferente de la forma en que funciona UTXO. Es más eficiente que UTXO porque solo se tiene que actualizar el saldo en la base de datos, en vez de crear nuevos UTXO. Como resultado, el modelo UTXO no es adecuado para NFT.

Además, el modelo basado en el saldo no es bueno en la fragmentación porque al transferir algo a otra persona, requiere dos pasos: el primero es modificar la cuenta del titular anterior, y el segundo es modificar la cuenta del nuevo titular. Por razones de seguridad, debe realizar dos pasos como una operación atómica, pero en un entorno de fragmentación es difícil y el nivel de rendimiento es bajo. Sin embargo, en el

modelo de transacción basado en tokens solo hay un paso, que es agregar la nueva propiedad del token.

Seguridad

Centrándose en las funciones relacionadas de los tokens, everiToken agiliza las abstracciones innecesarias, que no solo aumentan en gran medida la eficiencia, sino que también proporcionan una seguridad notable. Aunque los tipos de tokens en everiToken pueden ser muy abundantes y teóricamente ilimitados, la estructura de tokens unificada permite al sistema o a cualquier organización de terceros auditarlos siguiendo los mismos principios. Se puede considerar que el sistema solo reconoce una forma única de contratos inteligentes, lo que evita complicadas implicaciones de auditoría y seguridad como consecuencia.

Código-base central de EveriToken

A partir de la primavera de 2019, everiToken ha presentado cuatro organizaciones que revisan todo el código central de la cadena pública everiToken, incluyendo Hacken Proof, Chaitin y otros. Se incluyeron análisis estáticos y dinámicos.

Dado que everiToken utiliza *contratos seguros*, una vez que se comprueba que nuestra "core codebase" (código base central) es segura, todos los contratos basados en everiToken también son seguros.

Script (everiSigner)

everiSigner es un complemento de firmas offline para navegadores. Todo el proceso de firma se realiza dentro de este complemento para que las claves privadas nunca estén expuestas. El sitio web interactúa con everiSigner creando un nuevo canal para garantizar la seguridad; el sitio web pasa el contenido para iniciar sesión en el canal y, a continuación, everiSigner devuelve los datos firmados.

Clave privada perdida

Sobre la base de la gestión de autorizaciones, los terceros pueden proporcionar muchos servicios. Por ejemplo, la Compañía C se especializa en servicios de

protección de contraseñas y Alice teme que haya olvidado o perdido la clave privada de su propio token. Alice puede administrar el permiso de transferencia del dominio al Propietario (1), Grupo C (1) y establecer el umbral en 1. En este caso, si Alice ha olvidado su clave privada y no puede obtener la autorización por sí misma, todavía puede obtener la autorización a través del Grupo C si se demuestra que es Alice (a través de la tarjeta de identidad o las huellas digitales) de la Compañía C. De este modo, Alice puede recuperar el token transfiriéndolo a una nueva cuenta después de la verificación.

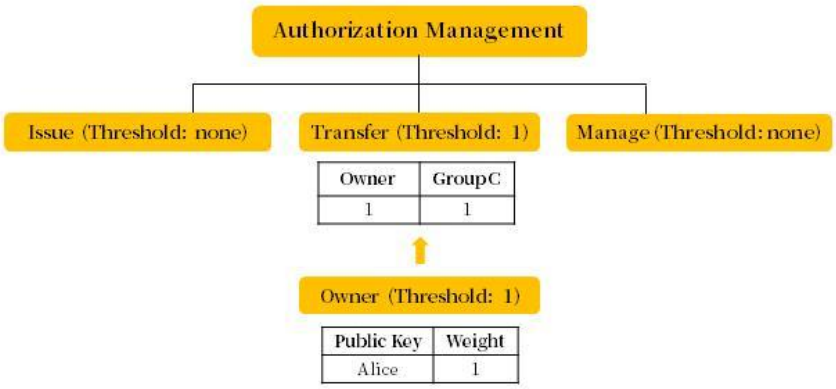


Figura 4. La empresa C proporciona servicio para recuperar la clave.

Por supuesto, el Grupo C podría robar el token de Alice, pero todas las operaciones se registrarán en la cadena de bloques, lo que destruiría la credibilidad del Grupo C.

Algoritmo de consenso

everiToken usa BFT-DPOS como su algoritmo de consenso. Se ha demostrado que DPOS es capaz de cumplir los requisitos de rendimiento de las aplicaciones on-chain. Bajo este algoritmo, aquellos que tienen EVT pueden seleccionar productores de bloques a través de un sistema de votación de aprobación continua. Cualquiera puede optar por participar en la producción de bloques y se le dará la oportunidad de producir bloques, siempre que puedan persuadir a los poseedores de tokens para que les voten.

everiToken permite que los bloques se produzcan cada 0.5 segundos, y exactamente

un productor está autorizado para producir un bloque en cualquier momento dado. Si el bloque no se produce a la hora programada, entonces se omite el bloque para ese intervalo de tiempo. Cuando se omiten uno o más bloques, hay un espacio de 0.5 segundos o más en la cadena de bloques.

El número de productores de bloques para la cadena pública everiToken es dinámico. Para el año inicial, se establecen 15 productores. Entonces el número será decidido por un comité de gobierno en cadena. Para mayor comodidad, utilizaremos 15 para el whitepaper.

En everiToken, los bloques se producen en rondas de 180 (12 bloques cada uno, multiplicados por 15 productores). Al comienzo de cada ronda, 15 productores de bloques únicos son elegidos por preferencia de votos emitidos por los titulares de EVT. Los productores seleccionados están programados en un orden acordado por 11 o más productores.

Si un productor pierde un bloque y no ha producido ningún bloque en las últimas 24 horas, se eliminará de consideración hasta que notifiquen a la cadena de bloques su intención de comenzar a producir bloques nuevamente. Esto garantiza que la red funcione sin problemas al minimizar la cantidad de bloques que se pierden al no determinar a los productores que no son fiables.

La tolerancia al problema de los generales bizantinos (“Byzantine fault tolerance”) se usa para brindar seguridad adicional a los usuarios al requerir que todas las confirmaciones estén firmadas por todos los productores. Ningún productor puede firmar dos bloques con la misma marca de tiempo o la misma altura de bloque. Una vez que 11 productores han firmado un bloque, se considera irreversible. Cualquier productor bizantino que firma dos bloques con la misma marca de tiempo o altura de bloque estaría generando evidencia criptográfica de su traición.

Diseño de bonificaciones

Se agregaron bonos con el lanzamiento de everiToken 3.0 en febrero de 2019. Es un

elemento poderoso, flexible y conveniente para combinar con las características existentes. Está diseñado principalmente con el propósito de distribuir beneficios a sus accionistas de acuerdo con un conjunto de reglas. Hay dos tipos de bonificaciones admitidas ahora según las diferentes formas de recaudar ganancias: bonificaciones pasivas y bonificaciones activas.

Para la bonificación pasiva, el beneficio se recopila durante cada transacción bajo un token fungible. Por lo tanto, si los administradores de una ficha fungible deciden establecer una bonificación pasiva, en cada transacción no solo se cargará EVT como combustible, sino que también se cobrará una tarifa adicional por la ficha fungible.

Hay varias opciones para controlar las tarifas reales en una transacción. La opción principal es la tasa de transacción. El resultado de las tarifas es la tasa multiplicada por el monto de la transacción. También hay opciones de control mínimo y umbral que limitan los límites superior e inferior de las tarifas finales. Esto evita un costo abrumador para transacciones de alto valor.

El administrador del token fungible puede decidir cómo se cobrarán las tarifas, por ejemplo, qué parte será responsable de la tarifa y el método de fijación de la tarifa. El primer método es como una tarjeta de crédito, con el pagador pagando una cantidad *n*, pero el beneficiario recibe menos de la cantidad *n* porque la tarifa se resta de la cantidad inicial. El segundo método es más como una transacción bancaria tradicional. Si desea transferir una cantidad *n* a otra, debe pagar una tarifa adicional por esta transacción además de la cantidad original.

En cuanto a la bonificación activa, es de carácter manual, similar a los dividendos de las acciones. El responsable del token fungible decide la cantidad de bonificación que debe dividirse.

Ya sea un bono activo o pasivo, debe tener una definición establecida de reglas de distribución. Tres tipos de reglas son actualmente válidas: fija, porcentaje y porcentaje restante. La regla fija es la cantidad fija garantizada para el receptor, mientras que la regla de porcentaje se calcula con el valor porcentual multiplicado por la cantidad total de la bonificación. La regla de porcentaje restante es independiente de las reglas fijas y de porcentaje, y consiste en la cantidad restante multiplicada por el valor

porcentual.

Para cada regla, también es necesario asignar el receptor. El receptor no está limitado a una sola dirección, sino que también puede ser el titular de un token fungible, y cada titular puede recibir la cantidad según su saldo en relación con el suministro total de dicho token fungible. Además, las partes interesadas de los tokens fungibles aquí no se limitan al token fungible utilizado con fines de lucro, sino que todo token fungible registrado en everiToken es aceptable. Por lo tanto, es posible emitir un `token de bonificación 'únicamente para la distribución con fines de lucro, y se beneficiará de la transparencia, imparcialidad y liquidez que proporciona everiToken.

Durante la implementación, se requiere tomar una instantánea de todas las direcciones de las partes interesadas junto con el saldo cuando el receptor tenga más de una dirección. Se necesitará mucho más almacenamiento porque cada dirección de los interesados costará 34 bytes. Hemos optimizado esta situación y, en la mayoría de los casos, cada dirección solo costará 4 bytes para almacenar. Con un millón de partes interesadas o más, el costo será de alrededor de 4 megabytes frente a 34 megabytes. Debido a la optimización del ajuste preciso de nuestra base de datos de tokens, el sistema puede leer y actualizar los saldos de las partes interesadas a un costo extraordinariamente bajo.

Funciones de bloqueo

Las funciones de bloqueo son compatibles con el sistema de everiToken. Se permite bloquear tanto tokens no fungibles como tokens fungibles por un período de tiempo. Esto depende de las condiciones, que se establecen durante la propuesta de bloqueo. Ya sea que se cumplan o no las condiciones durante el tiempo de bloqueo, después de un período de tiempo establecido, los activos desbloqueados se transferirán a diferentes direcciones registradas. Actualmente, las condiciones de bloqueo solo pueden ajustarse mediante claves públicas, lo que significa que durante el tiempo de bloqueo solo las claves aprobadas para una propuesta determinada pueden proporcionar acceso.

Otros detalles técnicos

Cadena de bloques básica

No queremos reinventar la rueda. Como resultado, hemos absorbido las partes excelentes del sistema de cadenas públicas existentes y mejorado sus debilidades. Hemos adoptado Graphene (DPOS + PBFT) como nuestro algoritmo de consenso. El código del algoritmo de consenso se genera a partir de DPOS3.0 (proveniente del código base de EOS) el cual hemos optimizado. Reconocemos que EOS tiene una excelente estructura en su código, por lo que hemos conservado parte de la estructura. Pero aparte de esto, la cadena pública ha sido desarrollada completamente.

Sobre esta base, hemos desarrollado un contrato seguro (en lugar de contratos inteligentes), un nuevo modelo de base de datos (basado en RocksDB para obtener un desempeño mejor) y el protocolo de pago de token everiPay.

Hay muchas ventajas para tal práctica:

- Graphene ha sido validado por un largo periodo de tiempo. DPOS y otros mecanismos centrales han sido completamente probados en proyectos como BitShares y EOS.
- Reutilizar el algoritmo de consenso puede reducir parte de la carga de trabajo, lo que nos permite concentrarnos más funciones centrales del desarrollo.

Operación de Autorización

Las operaciones de autorización de everiToken incluyen principalmente la firma múltiple, el cálculo del peso, la configuración del umbral, etc. Dado que la transferencia de cada token es independiente de las otras, la operación de transferencia de diferentes tokens se puede ejecutar en paralelo. Además, como el estado de permisos de cada grupo es independiente, las operaciones de emisión y administración también se pueden ejecutar en paralelo entre diferentes grupos.

Cada transacción se compone de un paquete de datos más una lista de firmas. En el caso de verificar autorizaciones, solo necesitamos verificar cada firma. No existe una relación entre las firmas, por lo que las operaciones de autorización se pueden ejecutar en paralelo.

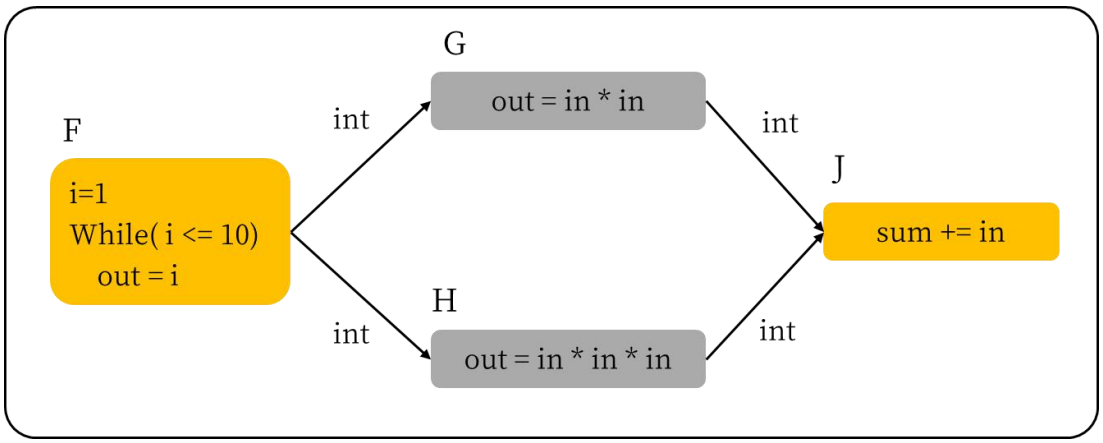
Motor de ejecución

En el sistema de everiToken, ya que cada operación de tokens es completamente

independiente, los procesos paralelos no requieren cargas de partición adicionales. Además, debido a que el tipo de operación de token es limitado, el código también está incorporado. Mientras cada tipo de operación se pruebe repetidamente, el sistema es completamente estable.

La ejecución de una transacción se puede dividir en varias fases, como la recuperación de firmas, verificaciones de autorización, cómputo, escritura de base de datos, etc. Todas las fases deben ejecutarse secuencialmente, pero algunas fases son independientes entre sí en diferentes transacciones. Una de estas fases se llama recuperación de firma. No hay ninguna dependencia lógica en las firmas de cada transacción, y cada firma de una transacción también es independiente. Por lo tanto, no es un problema recuperar firmas de una manera totalmente paralela. Otra de estas fases son las verificaciones de autorización. Parece ser lo mismo que recuperar firmas a primera vista, pero imagina que se comprueba la autorización de dos transacciones de transferencia de tokens. Aunque cada token no desempeña ningún papel en la función de otro, si hay dos transacciones que transfieren el mismo token, entonces el sistema encontrará un comportamiento inesperado si continúa verificando en paralelo. Debido a que los propietarios del token participan en la verificación, se cambiará en la primera transacción.

Por lo tanto, no hay forma de ejecutar algunas fases en paralelo, pero estas situaciones se pueden planificar cuidadosamente. Lo que hemos implementado se muestra a continuación en el gráfico de dependencia. Nuestro sistema paraleliza el flujo de datos utilizando el paralelismo de gráficos. Los cálculos se representan mediante nodos y los canales de comunicación entre estos cálculos se representan mediante bordes.



Arriba hay un ejemplo de cómo calcular la suma de las secuencias de los cuadrados y cubos del 1 al 10. En nuestra implementación, cada nodo representa una fase de una transacción, y hay un programador que recibirá las transacciones y las dividirá para construir el grafico.

Transacción suspendida

Una transacción suspendida es una transacción que se completa después de varias demoras. Las transacciones ordinarias no suspendidas se realizan de una sola vez, y todas las condiciones deben cumplirse cuando se envía la transacción. Por ejemplo, todos los firmantes deben firmar juntos. Sin embargo, en realidad muchas transacciones se completan con un proceso. Es posible que los participantes de la transacción no puedan completar las firmas al mismo tiempo. La transacción suspendida permite que las firmas se proporcionen paso a paso hasta que la transacción sea exitosa.

everiPay / everiPass / EvtLink

everiPay / everiPass

everiPay/everiPass es un método de pago creado para micropagos cara a cara mediante el uso de la cadena de bloques pública everiToken.

EvtLink incluye el estándar de generación de códigos QR y la definición de protocolo de comunicación.

Aquí hay algunos puntos destacados relacionados con everiPay/everiPass/EvtLink:

- **Liquidación instantánea:** cada transacción es una liquidación.
- **Descentralización:** pago P2P, sin plataforma centralizada, nadie puede modificar los datos en la cadena y todos pueden participar en la creación de precio.
- **Más seguro:** los datos y el contenido de la cadena de bloques no se pueden falsificar ni manipular, a fin de maximizar la seguridad y la protección de las propiedades del usuario.

- **Más conveniente:** incluso si no puede conectarse a Internet, puede completar la transacción. El pagador / beneficiario no necesita ingresar la cantidad de dinero manualmente. El pagador y el beneficiario recibirán una notificación tan pronto como la transacción sea exitosa.

- **Compatible:** everiPay/everiPass es compatible con todos los tokens emitidos en everiToken. Además, se admiten operaciones cotidianas funcionales, como una llave para abrir una puerta. La mejor parte es que puede usarlo en casi todas partes, simplemente con su teléfono.

- **A la velocidad del rayo:** everiToken rápidamente ha logrado unas TPS muy altas, y las transacciones se pueden completar en 1 a 3 segundos, dependiendo de la calidad del equipo o la red.

- **Estandarización:** Con una tecnología única con respecto a su cartera, EvtLink es un estándar cross-wallet (cartera interoperable), cadena interoperable y aplicación interoperable, forjado directamente para todo el ecosistema. Cualquier aplicación es compatible para crear o analizar.

Basándose en las siete características anteriores, everiPay/everiPass puede proporcionar el servicio más seguro, conveniente y fácil de usar en la industria de pagos cara a cara.

Para everiPay/everiPass, el beneficiario debe usar una aplicación que admita el análisis de EvtLink y la transferencia de transacciones a everiToken. Ha sido creado de carácter simple y fácil, ya que proporcionamos API y ejemplos de código fáciles de usar para los desarrolladores. Es similar a agregar soporte AliPay/WeChat para su tienda, pero incluso mucho más fácil.

Código QR del Beneficiario

El código QR de un beneficiario no admite muchas de las funciones que proporciona everiPay. Por ejemplo, los pagadores deben conectarse a Internet para completar una transacción de código QR del beneficiario, y tanto los pagadores como los beneficiarios deben ingresar el monto de la transacción manualmente. Además, no reciben una notificación automática cuando finaliza el pago.

Sin embargo, los beneficiarios no necesitan utilizar una aplicación que admita este método de pago. De hecho, todo lo que deben hacer los beneficiarios es simplemente usar una cartera con el respaldo de everiToken en su teléfono para verificar si han recibido el dinero del pagador. Es adecuado para todos los tipos y tamaños de proveedores, así como para intercambios entre personas.

Se recomienda a cualquier persona el uso de everiPay en lugar de un código QR del beneficiario, porque es más transparente, seguro y fácil de usar.

¿Cómo funciona EvtLink?

EvtLink es el estándar de formato binario que representa everiPay/everiPass. La cadena pública everiToken utiliza acciones en everiPay y everPass para ejecutar la transacción en evtLink.

Aquí está el proceso de pagos a través de everiPay/everiPass desde un punto de vista técnico:

1. El pagador selecciona un tipo de token a usar, y luego la cartera del pagador muestra una serie de códigos QR dinámicos que consisten en un LinkId único de 128 bits, una firma del pagador y el símbolo del token utilizado para el pago . Tenga en cuenta que el LinkId no debe cambiarse durante el intercambio de códigos QR a menos la transacción haya sido ejecutada. Esto evita el riesgo de un pago duplicado, ya que la cadena de bloques no permite dos acciones en EvtLink con el mismo LinkId.
2. La cartera del pagador debe consultar continuamente la transacción relacionada con el LinkId llamando a la API 'get_trx_id_for_link_id' hasta que devuelva un ID de transacción válido. La billetera debe cambiar el LinkId la próxima vez que muestre un código QR. Además, la cartera debe mostrar el resultado de la transacción consultando el ID de la transacción. Las carteras pagadoras no necesitan enviar transacciones directamente.
3. Mientras tanto, el beneficiario escanea el código QR con su teléfono, escáner o dispositivo inteligente. Una vez EvtLink ha sido analizado, se debe envolver dentro de una acción y emitirla a la cadena. Después de eso, todos los nodos de la cadena se sincronizarán como resultado, y el 'get_trx_id_for_link_id' devolverá el ID de transacción.

Codificación Base42

Base42 es un algoritmo de codificación para conversiones de binario a cadena ("binary-to-string"). Es similar a la codificación hexadecimal, pero en su lugar utiliza 42 como su base y, en consecuencia, utiliza una secuencia de alfabeto única. Los caracteres del alfabeto son los mismos que los de la codificación del modo alfanumérico de un código QR, por lo que es eficiente empaquetar una cadena codificada en *base42* en un código QR. Esto da como resultado un código QR más pequeño que permite un escaneo más conveniente.

En everiToken, se utilizará *base42* para codificar el contenido de EvtLink.

Parte III. Modelo económico

Tarifa de transacción/combustible (EVT)

Con el fin de evitar ataques contra el sistema, por ejemplo DDoS, para participar en la votación de DPOS y para ofrecer una recompensa razonable a los productores, emitiremos EVT como nuestro combustible. Cualquier operación cobrará un EVT determinado como tarifa de servicio, que será una recompensa para el productor. La cantidad de EVT que se cobrará flotará automáticamente, y las tarifas cobradas son principalmente para evitar ataques maliciosos y no afectarán al uso habitual de la mayoría de los usuarios.

El método de generación y transferencia de EVT es igual al de la moneda cifrada de la cadena de bloques convencional. EVT se utiliza para recompensar los recursos proporcionados por los productores y prevenir el comportamiento malicioso.

Se entregarán 150 millones de EVT (15% en total) al equipo central (14% para los cinco cofundadores de everiToken y un 1% adicional para los contribuyentes principales).
Se entregarán 400 millones de EVT (40% en total) a aquellos miembros de la comunidad que crean aplicaciones basadas en everiToken y contribuyen en gran medida al ecosistema de everiToken al proporcionar tecnología, recursos, promoción, financiación, etc.
450 millones de EVT (45% en total) son para inversores de varias rondas.

Todos los servicios en everiToken costarán una tarifa de combustible de servicio.

$$TarifaDeCombustibleDeServicio = CombustibleConsumido \times R$$

En esta fórmula, *CombustibleConsumido* es el precio de una acción específica. La unidad del precio es EVT. *R* representa la **tasa de ajuste**. Los nodos BP pueden decidir y realizar un aumento de las tasas independientemente y en cualquier momento, cuando la cadena está demasiado congestionada o bajo ataque. También pueden hacer un recorte de tasas si el precio del EVT es demasiado alto. La *R* real se calcula como el número mediano de 15 BPs.

Los usuarios de la cadena pueden asumir que *R* es 1, la primera vez que se conectan a una API. Siempre que *R* no haya sido modificado por los BPs, la conexión se

completará. Si *R* ha sido modificado, la conexión fallará con el valor de *R* de la respuesta de BP. Entonces, el usuario tendría que intentar la acción de nuevo.

Por ejemplo, deje que el precio de la API para la *creación de una cuenta* sea 2 EVT.
Por lo general, un usuario puede llamar a la API de *creación de cuenta* con 2 EVT.
Si los BP hacen una subida de tasas a $R = 1.1$, entonces el precio se ajustará a 2.2 EVT.

Usaremos el número mediano de todas las distribuciones de *R* para los productores de bloques. Si 3 productores sugieren *R* como 1.15, 5 productores como 1.2, 2 como 1.1, 2 como 1.3 y 1, 1.4 y 1.45 con 1 productor, entonces el valor final de R es 1.2.

EVT Anclado

Un EVT anclado es similar a un EVT pero no se puede transferir. Solo se puede utilizar como tarifa de combustible. Se permite la conversión de EVT a EVT anclado. El tipo de cambio del EVT contra el EVT anclado es siempre 1. **Dado que el EVT anclado no es una moneda**, es lo suficientemente seguro como para lanzar el EVT anclado a alguien.

En general, no se deben convertir EVT en EVT fijados, ya que pueden usar EVT para pagar las tarifas de combustible. Si uno decide convertir EVT a EVT anclado, el EVT anclado se vinculará automáticamente al receptor, de ahí su nombre, **EVT anclado**.

El EVT anclado pertenece a una cuenta y no se puede transferir a otros. Es conveniente y seguro distribuir EVT anclado a los usuarios. Las empresas y organizaciones pueden convertir EVT en EVT anclados y publicarlas en cuentas específicas. Los EVT fijados no se pueden transferir a través de direcciones.

Un **pagador** es la cuenta que paga una transacción determinada. everiToken permite a los usuarios especificar pagadores en una transacción. Esto es útil para crear cuentas. Por seguridad, los pagadores deben tener firmas adicionales para la transacción.

Cada dominio tiene un balance especial de EVT anclado.
La cadena prefiere consumir el saldo EVT anclado del dominio (si no es cero) durante acciones como transferir o destruir tokens en el dominio.
Los usuarios pueden pagar por adelantado el saldo de EVT fijo de un dominio a través de su EVT.

Emisión adicional de EVT

El volumen inicial de EVT es de un billón. La cadena podría emitir EVT extra anualmente. La emisión real será decidida por el comité de gobernanza en cadena de everiToken. No emitiremos EVT extras hasta el 1 de enero de 2020, como muy pronto.

Productores de bloques (BPs)

- Número de BPs: Dinámicos

Le damos pocos permisos a los BP, por lo que es muy difícil para los BP hacer el mal. Lo único que pueden hacer los BP malvados es DoS (denegación de servicio). Para equilibrar las ganancias de los BP y garantizar la descentralización, utilizamos un recuento dinámico que es igual o mayor que 15. En 2019 usaremos realmente 15 BPs. Para los años siguientes, el conteo se decidirá por el comité de gobernanza en cadena.

Parte IV. Ecosistema

Herramientas

EveriWallet

Como su nombre lo indica, everiWallet es una billetera everiToken que admite navegadores web y teléfonos móviles. Visite aquí para obtener más información: https://www.everiwallet.com/

EVTJS

EVTJS es la biblioteca de enlaces API de everiToken para JavaScript y es compatible con NodeJS y con los navegadores. EveriSigner también lo admite, por lo que puede usar esta biblioteca para crear aplicaciones web en everiToken fácilmente. Por favor visite aquí para más información:
https://www.github.com/everitoken/evtjs

evtScan

evtScan es el navegador blockchain de everiToken. Cualquiera puede buscar información específica sobre todos los bloques presentes generados por los nodos en la red principal de everiToken. Esto incluye los detalles de transacciones, cuentas, grupos y dominios en la cadena, así como estadísticas y análisis. Para los desarrolladores, evtScan es una herramienta eficiente para confirmar si la información está correctamente vinculada a la cadena. Para los usuarios, proporciona un método para verificar la autenticidad de las transacciones. Por favor visite aquí para más información:
https://evtscan.io/

Comité on-chain de gobernanza descentralizada

La cadena pública everiToken tendrá un comité de gobierno descentralizado en la cadena para decidir cosas importantes como el recuento de BP y la emisión adicional de EVT. El futuro está en desarrollo y se espera que el comité esté en línea antes del 1 de enero de 2020.

Empresa Fideicomisa/custodia

everiToken no se involucra con los activos o monedas de los usuarios, excepto por el ID de token. El valor de un token está avalado por las **compañías de custodia**. Las compañías de custodia pueden firmar una firma adicional durante la emisión de tokens, por lo que todos pueden confiar en el token si confían en la compañía que hace la firma en el token. Es como SSL.

Parte V. Conclusiones.

La economía del token está en camino de tocar todos los rincones del mundo. Los contratos inteligentes de Ethereum y EOS fueron un buen comienzo, pero no son adecuados para desarrollar una economía simbólica que todas las personas del mundo puedan utilizar.

everiToken nació con el objetivo de crear una tecnología blockchain basada en tokens que beneficie a todos, en todas partes. Hemos construido un sistema revolucionario que hace que los desarrolladores, las empresas y los usuarios finales, de bajo costo y simples, puedan emitir, transferir y verificar el uso de tokens dentro de nuestro sistema. Nuestros contratos seguros han eliminado la posibilidad de "Turing Complete", pero como resultado, la abstracción y las complicaciones dentro del sistema se reducen considerablemente. En lugar de crear constantemente modelos personalizados, creamos un modelo de talla única, convirtiéndonos en la solución preferible para más del 99% de las personas. Hemos mejorado la velocidad, la seguridad, la operatividad, la estabilidad y la supervisión necesarias para crear una economía de fichas eficiente y próspera, al tiempo que proporcionamos una plataforma descentralizada para que todas las personas del mundo aprendan, creen, interactúen e intercambien valor de forma digital. Únase a la revolución de la economía del token y visite nuestro sitio web
www.everitoken.io

Fundadores

Hengjin Cai, Científico Jefe

El Dr. Hengjin Cai es profesor y Ph.D. asesor en la Escuela de Ciencias de la Computación en la Universidad de Wuhan desde 2005. Es un experto residente en el *Global FinTech Lab*, investigador visitante en el Instituto de Tecnología Avanzada de Shenzhen de la Academia de Ciencias de China y miembro del comité de expertos de *China AI and Big Data Committee of 100*. Activamente involucrado en SSME (ciencia de servicios, administración e ingeniería), inteligencia artificial y tecnología blockchain, recientemente publicó un libro llamado *A Blockchain System with Integrated Human-Machine Intelligence*. En 2017, ganó el Premio *WU Wenjun de Inteligencia Artificial de Ciencia y Tecnología*. Recibió el Premio del Presidente por Contribuciones Extraordinarias a la Enseñanza en la Universidad de Wuhan en 2012. Como asesor dedicado, ha llevado a los estudiantes a ganar más de 80 premios en competiciones influyentes en China y al rededor del mundo, incluyendo la Microsoft Imagine Cup, Microsoft y Morgan Stanley Cup. de Computación de Alto Rendimiento en Finanzas, el Concurso de Innovación de Software Universitario Nacional de la Copa Intel y el Concurso de Emprendimiento de Estudiantes Universitarios de China.

Brady Luo, CEO Brady-everiToken

Brady es un verdadero creyente en la economía global tokens basada en la tecnología blockchain.

Recibió su licenciatura de la Universidad de Aeronáutica y Astronáutica de Beijing en ingeniería eléctrica, una maestría en finanzas de la Universidad de Brandeis en los Estados Unidos y estudió el plan de estudios acerca de estrategia blockchain en la Escuela de Negocios Said de la Universidad de Oxford. Empresario natural y en serie, fue elegido en el tercer grupo del plan de talentos de *Shanghai 1000 talents plan (venture group)* y vendió dos de sus empresas anteriores. Trabajó como analista durante casi cuatro años en uno de los principales administradores de fondos de los Estados Unidos, el *New York Oppenheimer Funds*, en el grupo de inversión de activos alternativos (Ciudad de Nueva York) y en el grupo financiero más grande de Japón,

MITSUBISHI UFJ securities (sede en Tokio, Hong Kong y Shanghái).

Bozhen Chen, director de operaciones

Bozhen posee gran experiencia en operaciones de proyectos gubernamentales y se especializa en comunicaciones y relaciones públicas. Se graduó de la Universidad de Aston con una licenciatura en administración de empresas. Bozhen ha trabajado con proveedores de comercio electrónico, cadenas de suministro de prendas de vestir, servicios B2B y organizaciones gubernamentales. A lo largo de este tiempo, desarrolló un sólido conjunto de habilidades de ejecución, comunicación y relaciones públicas en una variedad de industrias e intereses. Es el anfitrión permanente de la *Internet Conference*, líder del Centro de Servicios Públicos de Comercio Electrónico de Tongxiang y director del Centro de Servicios de Emprendimiento de Internet para Jóvenes. Ha ganado numerosos premios como uno de los líderes juveniles de China, incluyendo *Outstanding Youth* en Jiaxing y *2018 Motivated and Kind Youth,* otorgados por la Liga de la Juventud Comunista de China.

Ceeji Cheng, CPO

Ceeji es un desarrollador *full stack*, experimentado arquitecto de sistemas con más de 10 años de experiencia en desarrollo de software, empresarial y de gestión. Ganó el primer premio en la Olimpiada Nacional de Informática y anteriormente trabajó en su propia empresa (como CTO y cofundador).

Harry Wang, CTO

Harry es un experimentado arquitecto e ingeniero de sistemas con más de 10 años de experiencia en el sector financiero y de Internet. Anteriormente trabajó en Tianfeng Securities en Shanghai antes de participar en la fundación de una compañía de fondos de cobertura cuantitativa como socio técnico. Desarrolló un sistema de comercio cuantitativo de alto rendimiento, que hoy en día se opera en múltiples mercados y productos en todo el mundo.