Papel blanco

Versión 1, julio de 2021

JOEL KASR

FUNDADOR, KAJ LABS Y LITOSFERA

joel @ kaj labs.com

I ithosphere.network

kaj labs.com

HACIENDO CONTRATOS INTELIGENTES INTELIGENTES PARA LA ECONOMÍA DIGITAL

Abstracto

En geografía, una litosfera es la capa rígida más externa de un planeta de tipo terrestre o satélite natural. En la Tierra, está compuesto por la corteza y la porción del manto superior que se comporta elásticamente en escalas de tiempo de miles de años o más. - Wikipedia

Habiendo monitoreado de cerca el espacio de la cadena de bloques durante los últimos 10 años, la Fundación KaJ Labs puede construir una red de cadena de bloques mucho mejor aprendiendo de los errores cometidos por las primeras redes.

En este momento, todos los tipos de tokens han completado algunas funciones básicas de transferencia y distribución de valor, pero aún están muy lejos de los servicios financieros completamente funcionales que requiere el mundo real, razón por la cual, cuando se trata de aplicaciones blockchain en el sector financiero, todo lo que escuchamos son truenos pero no llueve. Las personas necesitan una nueva generación de infraestructura financiera basada en la tecnología blockchain que tenga una funcionalidad financiera completa, pueda vincular diferentes comunidades y tokens, y pueda cerrar la brecha entre organizaciones centralizadas y descentralizadas lo antes posible para marcar el comienzo de la era de la Internet de los valores.

Creamos un "sistema de correo electrónico" completamente nuevo en los albores del Internet de la información, en lugar de transformar el "sistema postal". De manera similar, cuando llegue la Internet de los valores, queremos construir un nuevo sistema: una infraestructura de transferencia de valor basada en una variedad de tokens.
¡Lithosphere (Litho) está lista para la era DeFi! Al establecer una capa de gestión de control sobre varios tokens a través de una gestión distribuida de las claves privadas de los tokens y al proporcionar puertos tanto para organizaciones centrales como para fuentes de datos externas, Lithosphere conectará varios contratos inteligentes pasados y de próxima generación, resolviendo la clave. problema de la insuficiente interoperabilidad de la actual Internet de los Valores.

La litosfera está abierta a todos. Conecta organizaciones centralizadas y descentralizadas, acomoda métodos de autenticación y mecanismos comerciales anónimos e introduce datos dentro y fuera de la cadena mediante la integración de las criptomonedas y cadenas de bloques que existen hoy y las que pueden existir en el futuro. La litosfera es una computadora virtual completa de Turing que permite a DeFi tener un espacio de ensueño ilimitado a través de múltiples tokens en el futuro, abriendo posibilidades impensables de ahora en adelante. El concepto general, la tecnología esencial y la estrategia de desarrollo del proyecto Litho se presentan en este documento técnico, que presenta la perspectiva de la banca descentralizada basada en un examen de la historia de Internet of Values.

Concepto de diseño

Aparición y significado de Blockchain

Debido a la falta de confianza, la economía de mercado convencional tiene un costo significativo. El método principal con el que las personas manejan la confianza de forma continua es a través de una organización o empresa centralizada. El rápido crecimiento de la civilización humana moderna fue ayudado por personas con ideales similares que se organizaron en instituciones como gobiernos, partidos políticos y empresas. Sin embargo, las organizaciones centralizadas enfrentan enormes desafíos: primero, debido a la falta de confianza entre las organizaciones y las disputas conceptuales, varios grupos se ven envueltos en rivalidades violentas, años de guerra e incluso terrorismo nuclear. En segundo lugar, los recursos se han concentrado cada vez más en manos de un pequeño número de personas, lo que amplía la brecha entre clases. Finalmente, existe el concepto de un "punto único de falla", como los vientos solares.

Debido a que algunas agencias han monopolizado una gran cantidad de recursos como el poder, la riqueza, las habilidades y los datos, las repercusiones de su incumplimiento o de ser pirateados serán graves. La visión de Lithosphere es conectar todas las cadenas de bloques y romper las barreras entre las cadenas de bloques al permitirles realizar transacciones entre sí. El objetivo final es crear una red conectada de cadenas de bloques, una red de cadenas de bloques capaces de comunicarse entre sí de forma descentralizada.

Con Lithosphere, las cadenas de bloques pueden mantener la soberanía, procesar transacciones rápidamente y comunicarse con otras cadenas de bloques en el ecosistema, lo que las hace óptimas para una variedad de casos de uso en lugar de estar limitadas a una red de cadenas de bloques, es decir, Polkadot / Bitcoin / Ethereum / Cardano.

Un muy buen caso de uso de Lithosphere será la transferencia de NFT. Actualmente, NFT solo se puede transferir a partes dentro de una red determinada. Por el momento, no se puede enviar Ethereum NFT a un usuario de Smart Chain (BSC) o viceversa. Con Lithosphere, los usuarios del ecosistema podrán recibir y enviar tokens desde cualquier blockchain que admita el consenso Byzantine Fault-Tolerant (BFT).

La transición de la autorización de crédito central por parte de las instituciones a principios matemáticos inviolables para documentar el intercambio de valores es un avance significativo. La moneda es, en esencia, un consenso. Es un símbolo contable estándar para un intercambio de valor más conveniente. Al revisar la historia financiera de la humanidad, desde el trueque de una cosa por otra, hasta el uso de ganado, ovejas o conchas como equivalentes universales, el uso de metales preciosos como dinero, el uso actual de papel moneda con una sólida base crediticia, la moneda humana es acercarse a las matemáticas abstractas, y su naturaleza como símbolos o libros de contabilidad es más evidente. Los conceptos de contabilidad humana se alinean más con las matemáticas como resultado de las cadenas de bloques.

Ayuda a todo el sistema contable a alejarse del control de una sola institución y avanzar hacia un camino más justo y transparente. La inclusión financiera es un concepto que tiene como objetivo brindar acceso al sistema financiero y servicios financieros de bajo costo para personas desfavorecidas y pequeñas empresas en todo el mundo. Dos mil quinientos millones de personas en todo el mundo no pueden utilizar bancos, crear cuentas de ahorro o adquirir tarjetas de crédito, lo que las separa de la economía mundial. Los bancos cobran tarifas exorbitantes por las transferencias transfronterizas. Los inversores ordinarios solo pueden comprar bienes financieros de muy bajo precio en bancos y otras instituciones financieras, y no pueden participar en inversiones iniciales en empresas de tecnología como Google y Alibaba hasta que coticen en la bolsa de valores.

Muchas pequeñas y medianas empresas también tienen dificultades para obtener apoyo crediticio de los bancos, a pesar de tener un crédito sólido y un excelente desempeño, porque no son los clientes objetivo de los bancos tradicionales bajo la regla 80/20. El desarrollo de la tecnología blockchain está alterando las condiciones descritas anteriormente. Bitcoin se usa para pagar a trabajadores en otras naciones, como El Salvador. Los inversores que participaron en las ofertas iniciales de monedas (ICO) de proyectos conocidos de blockchain como Bitcoin y Ethereum obtuvieron rendimientos cientos de veces superiores a sus inversiones iniciales. Las finanzas inclusivas están alcanzando nuevas alturas gracias a la tecnología blockchain. Muchas organizaciones están explorando formas de registrar formas tradicionales de activos, como facturas comerciales y puntos de fidelidad, en cadenas de bloques, generalmente en forma de cadenas de consorcio. Las criptomonedas son cada vez más aceptables como forma de pago en transacciones financieras; muchas organizaciones están explorando formas de registrar formas tradicionales de activos, como facturas comerciales y puntos de fidelidad, en cadenas de bloques, generalmente en forma de cadenas de consorcios. Ha habido la aparición de intercambios de activos digitales, que son comparables a las organizaciones financieras tradicionales.

La función bancaria de intercambiar activos digitales la realizan estos intercambios. Son similares a las bolsas de valores en el sentido de que proporcionan una plataforma para comprar e intercambiar tokens. Las funcionalidades de una plataforma para transferencias de tokens transfronterizas son comparables a las de las remesas bancarias transfronterizas. Sin embargo, estas plataformas operan de manera centralizada en diversos grados, lo que no solo presenta problemas de seguridad asociados con la centralización, sino que también evita el uso generalizado de la tecnología blockchain. Necesitamos un "banco" distribuido basado en este fenómeno, donde múltiples monedas digitales y activos digitales puedan entrar, salir e intercambiarse a través de blockchains. Requerimos una ubicación donde se puedan desarrollar y ejecutar productos y contratos financieros basados en monedas digitales y activos digitales, así como un entorno seguro para salvaguardar la privacidad de las transacciones. Por supuesto, esos "bancos" no se parecerán en nada a los bancos tradicionales, excepto por algunos servicios como débito y crédito, remesas, liquidación y venta de productos financieros. Cualquier empresa o individuo con suficiente experiencia y efectivo puede abrir sus ventanas comerciales. Pueden ofrecer una variedad de servicios mientras mantienen la seguridad de una infraestructura blockchain distribuida, lo que les permite brindar más servicios financieros a más personas. Esta es una futura infraestructura financiera construida sobre activos digitales y un mercado financiero distribuido, para ser más precisos. Cualquier empresa o individuo con suficiente experiencia y efectivo puede abrir sus ventanas comerciales. Pueden ofrecer una variedad de servicios mientras mantienen la seguridad de una infraestructura blockchain distribuida, lo que les permite brindar más servicios financieros a más personas. Esta es una futura infraestructura financiera construida sobre activos digitales y un mercado financiero distribuido, para ser más precisos. Cualquier empresa o individuo con suficiente experiencia y efectivo puede abrir sus ventanas comerciales. Pueden ofrecer una variedad de servicios mientras mantienen la seguridad de una infraestructura blockchain distribuida, lo que les permite brindar más servicios financieros a más personas. Esta es una futura infraestructura financiera construida sobre activos digitales y un mercado financiero distribuido, para ser más precisos.

Objetivos de diseño

El principal beneficio de blockchain es que ayuda a resolver el problema de la confianza que afecta a la humanidad, lo que hace que la tecnología blockchain eleve el nivel de la civilización humana. Su crecimiento es imparable por la necesidad humana de reducir los gastos transaccionales. Debido a que cada blockchain puede realizar una transmisión de valor de igual a igual, a diferencia de la Internet de la información (IoI) original, la tecnología blockchain nos lleva de la era de la IoI a la era de la Internet de los valores (IoV), que puede considerarse la tercera. generación de Internet.

Lithosphere ha establecido los siguientes objetivos basados en la investigación sobre tecnología de cadena cruzada, inteligencia artificial y aprendizaje automático, así como las características de la descentralización y sus escenarios de aplicación, para desarrollar una tecnología blockchain y aplicaciones de activos digitales más ampliamente difundidas:

Transferencia de activos entre cadenas:

- Conectar grandes redes de divisas digitales (como Bitcoin y Ethereum) y completar transacciones de activos sin cambiar los mecanismos de las cadenas originales. Esto permite que Lithosphere incorpore redes de moneda digital recién creadas a un costo muy económico.
- Integre Lithosphere con cadenas de consorcio. Esto maneja transferencias de activos de cadenas originales a Lithosphere, transferencias de activos de Lithosphere a cadenas originales y comercio de activos en Lithosphere.
- Asegúrese de que las transacciones entre cadenas sean seguras y de que los servicios de transacciones entre cadenas sean estables.

Protección de la privacidad de las transacciones:

- Permita que las partes comerciales seleccionen si ejecutar o no transacciones de forma privada.
- Proporcione protección de privacidad para transferencias e intercambios de activos digitales.
- Proporcione a los titulares de activos digitales protección anónima.

Extensibilidad funcional:

- Conviértete en una plataforma descentralizada para el comercio de activos no fungibles y moneda digital.
- Opere una compañía de depósitos y préstamos para varias monedas digitales.
- Utilice el dinero digital como vehículo para las transacciones de activos
- digitales. Cree nuevos activos financieros digitales e intercambielos.

El mundo ha cambiado drásticamente como resultado de Internet de la información. La civilización humana está destinada a sufrir transformaciones sociales masivas como resultado de Internet de los valores. Esto se debe a las cualidades de digitalización, inteligencia, descentralización e inclusión que posee la Internet de los valores basada en la tecnología blockchain. La digitalización y la inteligencia, que pueden ayudar a que la Internet de los valores funcione de manera más eficiente, son elementos que ya existen en la Internet de la información, pero que ahora se están aplicando a la Internet de los valores. La descentralización es una característica aún más importante, ya que ayudará a eliminar el cuello de botella causado por las organizaciones centralizadas. Las personas pueden proteger mejor sus derechos de propiedad personal con claves privadas; pueden resolver mejor los conflictos con mecanismos de consenso,

Las personas se unen a Internet de la era de la información cuando pueden transferir información fácilmente a través de Internet y programar información utilizando algoritmos; Entrarán en la era de Internet of Values cuando puedan enviar valor fácilmente a través de Internet y programar valor mediante contratos inteligentes. Los beneficios de Internet of Values le otorgan una ventaja "de gran dimensión" sobre los modelos de colaboración tradicionales. En blockchains, todos los tipos de "valores" se expresarán y se intercambiarán y programarán fácilmente. Como resultado, las relaciones de colaboración de las personas y la civilización humana indudablemente se alterarían drásticamente.

La Internet de los valores permitirá a las personas manejar los valores como si estuvieran informados, y su función principal será comunicar valores.

Sin embargo, para cumplir con este propósito, el valor de Internet debe mejorar en tres áreas. La interoperabilidad es la primera. Los valores residen en muchas cadenas de bloques, organizaciones de centralización y centros de datos, e Internet of Values necesita cadenas públicas u otras soluciones que puedan interactuar a través de cadenas de bloques, organizaciones de centralización y fuentes de datos, así como transferir valores y realizar contratos inteligentes. El segundo factor es la escalabilidad. La Internet de los valores debe adaptarse a una variedad de circunstancias, incluidas la banca, la industria y la administración gubernamental. El último punto a considerar es la utilidad. La Internet de los valores requiere un ecosistema sólido y la capacidad de operar una amplia gama de aplicaciones sin problemas para que los desarrolladores puedan crear aplicaciones rápidamente y los consumidores puedan utilizarlas fácilmente.

Sin embargo, en comparación con la Internet de la información, la Internet de los valores se encuentra todavía en sus primeras fases, con limitaciones de interoperabilidad, escalabilidad y usabilidad.

En términos de interoperabilidad, aunque Internet de la información ha sido capaz de transmitir y programar palabras, fotos, audio y video como un bit unificado de información, Internet de los valores sigue luchando por comunicar valores entre blockchains, mucho solo fuera de la cadena. valores y datos.

Internet de los valores no solo requiere conectividad entre cadenas, sino que también requiere conexión con entidades centralizadas y fuentes de datos externas. Los tokens en cadenas de bloques separadas no pueden intercambiarse entre sí, ya que las cadenas de bloques existentes no pueden comunicarse entre sí (sincronización de máquinas de estado). Debido a que las cadenas de bloques actualmente no pueden comunicarse con organizaciones centralizadas fuera de la cadena de bloques, es difícil trasladar los activos fuera de la cadena a la cadena de bloques. Debido a que las cadenas de bloques existentes no pueden leer datos fuera de la cadena, los contratos "inteligentes" son ciegos o tontos, incapaces de ver o comunicarse con el mundo exterior.

Tomando la tecnología de cadena cruzada como ejemplo, la comunicación entre cadenas, y mucho solo la construcción de contratos inteligentes entre cadenas, ahora es sumamente desafiante. Hay miles de tipos diferentes de tokens disponibles ahora, pero cada uno solo puede moverse libremente en una sola cadena de bloques y tiene su ecosistema de billeteras, herramientas de creación de contratos inteligentes, etc. Las redes blockchain existentes son esencialmente ecosistemas insulares, e Internet de los valores aún está muy lejos de ser realmente interoperable.

En términos de escalabilidad, mientras que Internet de la información se expande constantemente al codificar varios datos como bits y programar la lógica de comunicación de varios escenarios como aplicaciones, Internet de los valores apenas está comenzando mediante la tokenización de varios valores como tokens y el mapeo de transacciones de varios escenarios. lógica como contratos inteligentes.

La escala de Internet of Values está severamente restringida debido a su falta de compatibilidad. La transferencia de valores fuera de la cadena a la Internet de los valores se ve obstaculizada por la dificultad de mapear escenarios de aplicaciones reales que involucran varias monedas, numerosas organizaciones y múltiples fuentes de datos a una cadena de bloques para construir una solución distribuida.

En términos de usabilidad, mientras que el poder de procesamiento, la capacidad de almacenamiento y la velocidad sincrónica de la Internet de la información fueron suficientes para manejar la mayoría de las necesidades de gestión de la información, la Internet de los valores solo puede acomodar proyectos algo más grandes. En términos de estandarización, plataforma, modularidad funcional, ecología de aplicaciones, interoperabilidad y ataques anti-cuánticos, Internet de los valores tiene mucho trabajo por delante.

La interoperabilidad es el más urgente de los tres tipos de obstáculos enumerados anteriormente, ya que nos permite mover activos entre cadenas de bloques, diseñar contratos inteligentes con varias monedas y mejorar la escalabilidad de las actualizaciones. La usabilidad, por otro lado, es un esfuerzo a largo plazo, pero la interoperabilidad y la escalabilidad, que han ralentizado el crecimiento de Internet de los valores, requieren una solución rápida y se han convertido en las dos barreras más urgentes que deben abordarse.

Contratos inteligentes y finanzas descentralizadas (DeFi)

El objetivo de Internet of Values es vincular diferentes valores a las cadenas de bloques para que los contratos inteligentes puedan controlarlos. La Internet de los valores permite la colaboración descentralizada, desintermediada, inclusiva y programable entre las personas. Debido a estos aparentes beneficios, los diversos valores correrán para ser asignados a las cadenas de bloques. La Internet de los valores, sin duda, se expandirá a un ritmo más rápido a medida que se aborden las limitaciones de la cadena de bloques.

El proceso de mapeo de valores a cadenas de bloques requiere desvincular la lógica financiera de la lógica empresarial, lo que implica que Internet de los valores se creó con un componente financiero significativo. Las aplicaciones financieras de Internet of Values son aquellas aplicaciones en Internet of Values que tienen características financieras particularmente significativas. Las finanzas descentralizadas se refieren a las operaciones financieras en cadena en la Internet de los valores, así como a sus correspondientes actividades financieras fuera de la cadena (DeFi).

Debido a que Internet of Values se basa en redes peer-to-peer que utilizan el Protocolo de datagramas de usuario, existen ciertos obstáculos. El desempeño de Internet de los Valores se acercará progresivamente al de Internet de la Información en el futuro, permitiendo que los escenarios de negocios y las transacciones financieras se escriban en el mismo software. Sin embargo, dado el estado actual de las cosas, esperamos que esto lleve mucho tiempo. La actual Internet de los valores apoyará principalmente las aplicaciones financieras, es decir, las aplicaciones DeFi serán las aplicaciones principales.

Internet de la información ya ha tenido una influencia significativa en nuestras vidas. También podemos anticipar cambios significativos en nuestras vidas como resultado de Internet of Values. Es posible que estemos familiarizados con las muchas formas de información disponibles en Internet, pero pocas personas hablan del "valor" de Internet de los valores.

Para empezar, los valores en Internet of Values son tokens representados por la cadena de bloques, y el proceso de mapeo de valores en Internet of Values se conoce como tokenización de activos. Los activos conectados se expresarán mediante tokens en cadena y formarán parte de Internet of Values si los tokens en las cadenas representan el título, la ganancia y el control de los activos subyacentes fuera de la cadena. La Internet de los Valores permite que cada vez más valores ingresen a sí misma a través de este proceso, evitando el "doble gasto" a través de libros distribuidos y haciendo que transferir valor sin intermediarios sea tan simple como enviar información y programar valores tan simple como programar información, haciendo de la Internet de los Valores ' perspectivas similares a las que hemos visto anteriormente en materia de telecomunicaciones.

En segundo lugar, la tokenización es una forma de titulización de activos en la que los valores fuera de la cadena se asignan a las cadenas como criptoactivos. Debido a que los tokens pueden dividirse indefinidamente y transferirse a lo largo del tiempo y el espacio, pueden usarse en transacciones financieras como hipotecas, préstamos y seguros. Como resultado, la tokenización se define como el proceso de titulizar activos y convertir activos fuera de la cadena en activos criptográficos que se pueden administrar mediante claves privadas.

Por último, Internet de los valores incluirá una gama más amplia de valores. Las identidades, firmas, datos, derechos de voto y otros datos se asignarán a Internet of Values siempre que la tokenización sea rentable. Como resultado, Internet de los valores tendrá una gama de valores más amplia que los mercados financieros tradicionales.

Posicionamiento

Proponemos el proyecto Lithosphere a la luz del brillante futuro de DeFi y los desafíos que presenta el Internet de los valores actual. El objetivo de Lithosphere es crear una cadena pública a nivel de plataforma en la era de la economía digital que pueda conectar todo tipo de valores, proporcionar funciones financieras completas, comunicar diversas comunidades y tokens, y unir organizaciones centralizadas y descentralizadas para llevar el Internet de los valores como lo antes posible con la ayuda de blockchain, IA y otras tecnologías.

Arquitectura y tecnología de la litosfera

Gestión distribuida de claves privadas y máquina virtual de contrato inteligente

Debido a que los activos DeFi se muestran como tokens, pueden mejorar sustancialmente la interoperabilidad de Internet of Values y hacer que el aumento de la escalabilidad sea mucho más fácil si se pueden implementar contratos inteligentes de múltiples tokens. La tecnología actual de cadena cruzada es principalmente tecnología de cadena lateral, que utiliza una vinculación bidireccional para transferir transacciones a cadenas laterales y firmas múltiples para salir de las cadenas laterales. Tal método solo puede producir transferencias atómicas y los resultados son insatisfactorios en casi todos los sentidos. Necesitamos crear una cadena pública que permita que se le asignen otros tokens de una manera más inventiva, de modo que se puedan crear contratos inteligentes de múltiples tokens. Podemos mejorar sustancialmente la interoperabilidad de la Internet de los Valores de esta manera, y esta cadena pública sin duda se convertirá en una de las infraestructuras DeFi más importantes. No solo comunica valores entre cadenas de bloques, sino que también permite interfaces con organizaciones centralizadas y fuentes de datos fuera de la cadena para aumentar la escalabilidad de Internet of Values. En una nueva cadena pública, ¿cómo se expresarán varios tokens? Prevemos que las claves privadas de los tokens en varias cadenas de bloques pueden ser controladas de forma segura y distribuida por una cadena pública y, de esta manera, la cadena de bloques gestiona los derechos de control de los tokens. Será como una "autopista" en Internet of Values, que puede implementar fácilmente las transferencias de valor entre varios tokens y contratos inteligentes de múltiples tokens para proporcionar varios servicios DeFi. ¿Cómo se expresarán varios tokens? Prevemos que las claves privadas de los tokens en varias cadenas de bloques pueden ser controladas de forma segura y distribuida por una cadena pública y, de esta manera, la cadena de bloques gestiona los derechos de control de los tokens. Será como una "autopista" en Internet of Values, que puede implementar fácilmente las transferencias de valor entre varios tokens y contratos inteligentes de múltiples tokens para proporcionar varios servicios DeFi. ¿Cómo se expresarán varios tokens? Prevemos que las claves privadas de los tokens en varias cadenas de bloques pueden ser controladas de forma segura y distribuida por una cadena pública y, de esta manera, la cadena de bloques gestiona los derechos de control de los tokens. Será como una "autopista" en Internet of Values, que puede implementar fácilmente las transferencias de valor entre varios tokens y contratos inteligentes de múltiples tokens para proporcionar varios servicios DeFi.

Dado que casi todos los tokens de blockchain están controlados por claves privadas, los valores en Internet of Values se pueden administrar de forma distribuida mediante contratos inteligentes siempre que las claves privadas de sus tokens puedan ser controladas por nodos distribuidos de una cadena pública. Con los contratos inteligentes completos de Turing, la cadena pública también puede proporcionar varias funciones de finanzas descentralizadas (DeFi) en una forma más sofisticada.

Esta cadena de bloques, que conecta todos los tokens, no requiere una lógica compleja para varios escenarios de aplicación. Su propósito es crear una capa de administración en todas las cadenas de bloques, permitiendo que todos los tokens interactúen. Debido a que no necesita ejecutar una lógica de aplicación pesada, en su usabilidad actual es capaz de cumplir con varias funciones DeFi.

Gestión de claves distribuidas de Myriad (MDKM)

La litosfera se basa en las teorías y los logros de la generación de claves distribuidas (DKG) en el campo del intercambio de cifrado. La clave pública y la clave privada son generadas por nodos que cooperan para comunicarse. La clave pública se transmite en la cadena pública, la clave privada es almacenada por separado por cada nodo de una manera distribuida a través de Variable Secret Sharing (VSS). La clave pública común es generada por el algoritmo DKG, y luego la dirección de cuenta del Lock-in es generada por el algoritmo correspondiente para realizar el control descentralizado.

Aquí nos referimos al dominio de VSS y DKG basado en el protocolo de generación de claves distribuidas de criptografía de curva elíptica y la investigación de aplicaciones sobre el proceso que se describe a continuación:

Dada la curva elíptica E, existe un campo finito GF (q), q es un número primo con n conjuntos de participantes Q = {P1, P2, ..., Pn}, pi denota la identidad del i-ésimo participante Pi y Pi ∈ GF ∗ (q), donde GF ∗ (q) es un grupo multiplicativo en GF (q). Mientras tanto, pi y yo somos intercambiables durante el cálculo. E / GF (q) representa el grupo aditivo en E. T es E / GF (q), el orden de E / GF (q) es un número primo o factor primo, marcando este primo o factor primo como p.

En este protocolo de generación de claves, se supone que tanto la multiplicación escalar como la multiplicación de puntos se realizan en δ y que las demás operaciones se realizan en GF (q). Para calcular Q (x) T, primero calculamos Q (x) y luego p (x) mod p, y Q (x) mod p es la multiplicación escalar en T. Supongamos que E tiene otro punto base T′ en la curva elíptica δ.

Firma de umbral

La técnica de firma de umbral puede abordar el problema de las firmas creadas por los nodos de salida de Lithosphere y, al mismo tiempo, mejorar la estabilidad de la red blockchain. Según los estudios sobre la adaptación de nodos en redes de generación de claves distribuidas, Lithosphere elegirá los nodos apropiados para unir y actualizar los parámetros clave compartidos en circunstancias extremas para asegurar el funcionamiento exitoso de la cadena.

Moneda Litho

Litho es la moneda nativa de la litosfera. Tanto las transacciones entre cadenas como dentro de la cadena consumen una cierta cantidad de Litho. Litho también se utiliza en depósitos de seguridad para los nodos de verificación de cadena cruzada. Litho / $ LITHO es la moneda de elección en la red Lithosphere, aunque también se puede usar otra criptografía, ya que la cadena de bloques Lithosphere admite la interoperabilidad.

LAX - Moneda estable algorítmica

La moneda estable algorítmica litográfica (LAX) es similar a los protocolos algorítmicos de monedas estables que operan en la cadena de bloques Ethereum, pero a diferencia de las monedas como US Dollar Coin (USDC) y Tether (USDT), que están respaldadas por tenencias auditadas de dólares estadounidenses o criptoactivos como PAX Gold. (PAXG), la moneda Litho USD no está vinculada al dólar estadounidense ni a ninguna garantía de cifrado. En lugar de utilizar criptografía, moneda fiduciaria o productos básicos como garantía, el protocolo Lithosphere ajusta su suministro de criptografía LAX cada 24 horas en un proceso llamado "rebase" para mantener un precio estable.

Mecanismo de consenso

Lithosphere adapta un mecanismo de consenso de prueba de participación.

El objetivo de Lithosphere es utilizar la tecnología blockchain para construir una plataforma de infraestructura para ejecutar aplicaciones descentralizadas y en la plataforma, múltiples tipos de tokens podrán interactuar libremente a través de contratos inteligentes para lograr una interoperabilidad de valor. Lithosphere tiene como objetivo implementar Myriad Distributed Key Management para construir contratos inteligentes para DeFi.

Cuando un activo no registrado se mueve de la cadena de origen a Lithosphere, Lithosphere construirá un nuevo activo basado en la información de transacciones entre cadenas, utilizando una plantilla de activos incorporada para implementar un nuevo contrato inteligente. Cuando un activo registrado se traslada de la cadena original a Lithosphere, Lithosphere emitirá tokens iguales en los contratos existentes, lo que garantiza que los activos de la cadena original aún puedan comercializarse en Lithosphere.

Integración entre cadenas

El mapeo de activos se refiere al proceso de producir tokens coincidentes para la contabilidad en Lithosphere para un artículo controlado. Un token puede interactuar libremente con otros activos mapeados gracias al mapeo. Las operaciones de bloqueo y cierre se utilizan para establecer y eliminar el control distribuido.

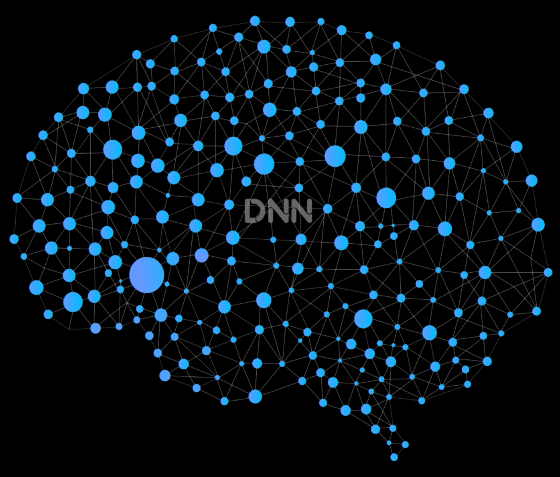
Transacciones entre cadenas

Asset Lock-in es un proceso que permite una gran cantidad de gestión de claves distribuidas y mapeo de activos para todos los tokens gestionados por claves.

Asset Lock-out) es la reversión del Lock-in y consta de dos partes: gestión de derechos de control y desmontaje del mapeo de activos. Una vez que se completa el bloqueo, el control del activo digital se devuelve al propietario, restaurando el almacenamiento completo de claves y la administración centralizada de claves. Al mejorar las aplicaciones de seguridad, liquidez y DeFi de los activos digitales actuales, la adopción de una gestión de distribución de claves múltiple mejorará el valor de los activos digitales.

Redes neuronales profundas (DNN)

David Yang PhD, propone redes neuronales profundas (DNN) para contratos inteligentes de Lithosphere. Los DNN son muy útiles en aplicaciones blockchain como el comercio DeFi y NFT. Sin embargo, entrenar / ejecutar DNN a gran escala como parte de un contrato inteligente no es factible en las plataformas blockchain actuales, debido a dos problemas de diseño fundamentales de estas plataformas. Primero, las cadenas de bloques hoy en día generalmente requieren que cada nodo mantenga el estado mundial completo en cualquier momento, lo que significa que el nodo debe ejecutar todas las transacciones en cada bloque. Esto es prohibitivamente caro para los contratos inteligentes computacionalmente intensivos que involucran DNN. En segundo lugar, las plataformas blockchain existentes esperan que las transacciones de contratos inteligentes sean deterministas, resultados y efectos reproducibles. Por el contrario, DNN generalmente se entrena / ejecuta sin bloqueos en dispositivos de computación masivamente paralelos como GPU, TPU y / o clústeres de computación, que a menudo no producen resultados deterministas.



Por primera vez en contratos inteligentes, Lithosphere implementa DNN para hacer que los contratos inteligentes sean inteligentes al incorporar redes neuronales profundas (DNN) a gran escala en el código, que tiene numerosas aplicaciones potenciales. Por ejemplo, en las finanzas descentralizadas (DeFi), un DNN podría ayudar a detectar movimientos anormales en los precios de los tokens, que podrían ser parte de un ataque de préstamos relámpago. Una organización autónoma descentralizada (DAO) podría intercambiar tokens automáticamente con un DNN capacitado continuamente a través del aprendizaje por refuerzo. Un creador de contenido puede aplicar una red generativa de confrontación (GAN) para generar imágenes de arte visual y, posteriormente, convertirlas en tokens no fungibles (NFT) negociables en un intercambio descentralizado.

Estándar de token multicadena LEP100

El LEP100 es un estándar novedoso para múltiples tokens, que permite que un solo contrato represente múltiples tokens fungibles (moneda) y no fungibles (NFT) y operaciones por lotes para aumentar la eficiencia del gas propuesto por Joel Kasr, creador de Lithosphere. Lo más importante es que los tokens LEP100 pueden intercambiarse por cualquier otro equivalente de token. Los tokens LEP100 se alimentan con la moneda Litho nativa (LITHO).

. Cuando está vinculado con los tokens LEP100, también puede vincularse a cualquier red que utilice los principales activos digitales. El token es compatible con varios contratos y tiene características básicas como transferir, devolver un saldo y examinar la posesión de un token. Un token LEP100, a diferencia de ERC20 o BEP20, permite que un solo contrato represente numerosos tokens fungibles y no fungibles, lo que permite una amplia gama de aplicaciones en el uso diario. Es el token más eficiente para plataformas DeFI, plataformas de juegos, NFT y otras plataformas compatibles con contratos de alta demanda. LEP100 también se puede integrar fácilmente en cualquier dApps de Ethereum u otras cadenas porque se puede intercambiar por tokens ERC20, ERC-721, ERC-1155, BEP2 y BEP20. El LEP100 establece las mejores prácticas para la gestión de tokens entre cadenas. Debido a sus similitudes, los tokens son compatibles con ERC20, ERC-721,

El estándar de token LEP100 también permite la división del tiempo de token en contratos inteligentes. Cuando se divide un token, se divide en dos partes: una es una porción de tiempo limitado (aquí TL es para Time-Lent), y la otra es un final infinito (aquí TL significa Time Restricted, ya que su utilidad es limitada por un tiempo pero no bloqueado). Ambos segmentos se pueden dividir en dos segmentos de tiempo más si es necesario, lo que permite DeFi sofisticado, como el comercio de opciones y futuros.

Validadores

En los algoritmos bizantinos clásicos tolerantes a fallas (BFT), cada nodo tiene el mismo peso. En la litosfera, los nodos tienen una cantidad no negativa de poder de voto, y los nodos que tienen un poder de voto positivo se denominan validadores. Los validadores participan en el protocolo de consenso transmitiendo firmas criptográficas, o votos, para acordar el siguiente bloque.

Los poderes de voto de los validadores se determinan en la génesis o se modifican de forma determinista por la cadena de bloques, según la aplicación. Por ejemplo, en una aplicación de prueba de participación como LithoSwap, el poder de voto puede determinarse por la cantidad de tokens de participación vinculados como garantía.

Consenso BFT de comunicación lineal

El protocolo Litho utiliza un algoritmo BFT (BFT significa Byzantine Fault-Tolerance) para lograr esto. Un algoritmo de consenso bizantino tolerante a fallas garantiza la seguridad de hasta un tercio de los actores bizantinos o maliciosos. Las fallas bizantinas dentro de los sistemas distribuidos son algunas de las más difíciles de tratar.

Un marco de blockchain como Lithosphere impulsado por BFT permite que las blockchains públicas y privadas se transfieran tokens entre sí.

Una red blockchain impulsada por BFT (Lithosphere) permite la interoperabilidad con otras blockchains PoS / de finalidad rápida como Cosmos, Binance o Proof of Authority & PoW blockchains.

Lithosphere adapta un nuevo algoritmo de consenso, LinBFT propuesto por el Dr. David Yang. El protocolo BFT de comunicación lineal (LinBFT) se aplica a un sistema blockchain público sin permisos, en el que no hay infraestructura de clave pública, basado en el clásico PBFT con 4 mejoras importantes:

- Consenso por bloque. Hay consenso para cada bloque, más que para un grupo de bloques. Esto limita el poder del proponente de bloques y, por lo tanto, mitiga la minería egoísta.
- Líder rotatorio. El protocolo LinBFT cambia el líder (es decir, el proponente de bloque) para cada bloque, lo que reduce el riesgo de ataques de denegación de servicio en el líder.
- Cambiando la honestidad. En Pyramid LinBFT, un participante puede ser honesto para un bloque y malicioso para otro (por ejemplo, uno que contenga una transacción de interés para el participante), siempre y cuando más de 2/3 de todos los participantes sean honestos para cada bloque. En otras palabras, es posible que todos los participantes sean maliciosos en algún momento y, sin embargo, la cadena de bloques permanece segura en todo momento.
- Conjunto de participantes dinámicos. LinBFT permite que los nodos se unan y abandonen el protocolo al comienzo de las épocas. Como resultado, diferentes bloques pueden ser verificados por conjuntos de nodos completamente diferentes.

Además, en el caso ordinario, LinBFT implica solo una ronda de votación en lugar de dos en PBFT, lo que reduce tanto la sobrecarga de comunicación como el tiempo de confirmación y emplea el esquema de prueba de participación para recompensar a todos los participantes. Experimentos extensos que utilizan datos obtenidos de la red de prueba Ethereum demuestran que LinBFT supera de manera consistente y significativa los protocolos BFT en producción existentes para blockchains.

Gestión de claves distribuidas innumerables

Myriad Distributed Key Management realiza la generación de pares y direcciones de claves público-privadas y las firmas de transacciones en la cadena de bloques de destino de manera distribuida a través de varios nodos y de acuerdo con los algoritmos de firma digital adoptados por la cadena de bloques de destino, realizando así el control y la gestión de cuentas. y activos en la cadena de bloques de destino de manera distribuida.

Esta ruta técnica permite que MDKM sea compatible con tantos activos digitales controlados por algoritmos de cifrado como sea posible, ya sea que estos activos digitales se generen de forma centralizada o descentralizada. Al admitir un algoritmo de firma con MDKM, se puede controlar y administrar una serie de activos digitales cifrados con el mismo algoritmo de firma.

En la actualidad, la mayoría (más del 80%) de las monedas digitales cifradas adoptan el mismo algoritmo de firma ECDSA que Bitcoin y Ethereum, por lo que MDKM primero elige implementar el soporte para el algoritmo de firma ECDSA. Además, MDKM admitirá monedas de cifrado que utilicen diferentes algoritmos de firma, como el algoritmo de firma Ed25519 de Stellar [JL17] y el algoritmo de firma de Schnorr.

Estándar de token LEP100

Todas las fichas de Lithosphere siguen las especificaciones de LEP100. La red Lithosphere es una arquitectura de cadenas múltiples que permite a cualquiera desarrollar dApps y otros activos digitales basados en blockchain. También garantiza el comercio entre cadenas, un consumo mínimo de gas y transacciones rápidas con transacciones seguras.

LEP100 hace posible que los tokens de la cadena de bloques Lithosphere funcionen correctamente. Como consecuencia, todos se benefician de tarifas de transacción bajas.

Además, independientemente de la estructura de la red blockchain, el mecanismo DeFI entre cadenas mejora la interoperabilidad de todos los contratos pequeños. El entorno Lithosphere es de gran apoyo y Litho Launchpad financia todos los bootstraps con varios programas DeFI.

¿Por qué su proyecto DeFi debería utilizar el estándar de token LEP100?

Los tokens LEP100 se pueden usar para representar una variedad de activos, incluidas acciones, moneda fiduciaria y criptoactivos. Otros tokens de varias cadenas de bloques se pueden vincular fácilmente al token LEP100. Como resultado, permite a los desarrolladores construir diferentes versiones de activos criptográficos utilizando los mismos tokens.

Todos los validadores que transfieran el token LEP100 recibirán LITHO como recompensa. El incentivo se paga en forma de cargo por transacción. En comparación con otros estándares de tokens como ERC20, tiene precios mínimos de gas para todas las transacciones. Está construido sobre la red Lithosphere, que ofrece velocidades de transacción rápidas de más de 10,000 TPS en comparación con los 15 TPS de ERC20 de Ethereum y los 4 TPS de Bitcoin.

La integración de proyectos DeFI con tokens LEP100 es simple. También puede enumerar elementos de forma gratuita en DEX como LithoSwap, PancakeSwap y Uniswap

Características del token LEP100

El token LEP100 ofrece muchas características destacadas, que incluyen

- Velocidades de transacción de alta velocidad: el estándar de token LEP100 permite tasas de transacción de alta velocidad, lo que lo hace extremadamente escalable.
- Tarifas de transacción bajas: a diferencia de Ethereum Networks, a los usuarios no se les cobrarán altos precios de gas.
- Compatibilidad entre cadenas: los tokens LEP100 son compatibles con las redes y blockchains ERC20, ERC-721, ERC-1155, BEP2 y BEP20.
- Compatible con casi todas las carteras de criptomonedas más importantes del mercado actual.
- Fácil de vender en los intercambios: los tokens LEP100 son fáciles de enumerar en los intercambios y tienen una mayor probabilidad de ser vendidos.

Nodos de verificación

Para ganar una parte de las tarifas de transacción, un Validador completa el registro de transacciones en Lithosphere. De acuerdo con la participación que posee, un Validador recibe una participación clave correspondiente y calcula la participación de la firma asociada que se agregará a la transacción. De acuerdo con el porcentaje de participación clave, el Validador obtiene la tarifa de transacción asociada con la transacción de verificación. La tarifa de transacción no se puede cobrar si la información de intercambio de claves no está disponible o se pierde. Si los nodos firman la transacción incorrecta, las credenciales del Validador también se eliminarán.

En resumen, el sistema de incentivos del nodo de verificación alentará a los Autenticadores a proporcionar una prueba de transacción adecuada, a los Validadores a terminar fielmente la grabación de Lithosphere y a los Registradores a permanecer en línea y mantener seguras sus acciones clave.

Los nodos de verificación solo están disponibles para personas con una participación lo suficientemente grande en la red Lithosphere. Los nodos generales son nodos que no califican como nodos de verificación. Los nodos generales no pueden participar en el proceso de verificación de transacciones entre cadenas, pero pueden comprometer sus intereses en los nodos de verificación de confianza. Las tarifas de transacción recibidas por los nodos de verificación encomendados se distribuyen a los nodos generales en proporción a las participaciones encomendadas. Los nodos generales sufrirán una pérdida comparable si se penaliza al nodo de verificación delegado.

Las partes interesadas en Lithosphere pueden obtener ventajas relacionadas con las participaciones y, al mismo tiempo, estar motivadas para comprometer sus participaciones en nodos de verificación confiables gracias a este mecanismo de incentivos. Esto mejora la seguridad y estabilidad de Lithosphere.

Esquema de generación de cuenta bloqueada

El esquema de generación de cuentas bloqueadas se basa en el uso compartido de claves de umbral y la informática segura de múltiples partes.

Introducción

La base teórica de la criptografía distribuida y un desafío básico de la computación distribuida son la computación segura de múltiples partes.

La hipótesis se basa en el libro de 1982 "El problema de los millonarios de Yao". La computación multipartita segura y definida de manera simple se refiere a un conjunto de jugadores conocidos como P1 Pn que colaboran para calcular de manera segura la función f (x1, xn) = (y1, yn). Entonces, cada uno de los n participantes tiene una de las entradas de la función f. Pi tiene la entrada secreta xi y recibe la salida yi después del cálculo. En este caso, la seguridad requiere garantizar la validez del resultado de la computación, incluso si algunas personas hacen trampa durante todo el proceso de computación. Esto implica que una vez finalizados los cálculos, cada participante debe recibir el resultado correcto yi, y todas las entradas de los participantes están protegidas. A través del cálculo, Pi no puede obtener más información que (xi, yi).

Nodos generales

El método de umbral compartido de claves está destinado a abordar el problema de la gestión segura de claves. La seguridad de la criptografía depende de la seguridad de las claves, de acuerdo con los principios de diseño de criptografía contemporáneos. La seguridad de la criptografía se verá comprometida si las claves seguras se ven comprometidas. Como resultado, la gestión de claves es fundamental en la investigación y el diseño de la seguridad de la criptografía. Puede ser un desafío manejar la distribución de claves de manera segura cuando una cuenta es mantenida por numerosas personas con diversos intereses. El criptógrafo Adi Shamir ideó la técnica de intercambio de claves de umbral de intercambio secreto de Shamir para abordar este problema.

Una llave se divide en n piezas y se entrega a n participantes en este sistema. Cada participante tiene una parte de la clave compartida, y la clave debe reconstruirse utilizando un mínimo de k claves compartidas. Como resultado, cada actividad en una cuenta necesitará la cooperación de al menos k individuos para mantener la seguridad y confiabilidad de la cuenta.

Basándonos en el cálculo seguro de múltiples partes y el uso compartido de claves de umbral, creamos la técnica de creación de cuentas bloqueadas. Los Validadores de Litosfera (Registradores) son los encargados de mantener y administrar las claves de las Cuentas Bloqueadas para garantizar que sean seguras y confiables. Además, en una red ad-hoc sin topología establecida, esta técnica reduce el peligro de pérdida de claves y ofrece una gran flexibilidad y estabilidad.

El siguiente es el esquema de generación de cuentas bloqueadas:

Descripción del diseño

Paso 1: elija un número aleatorio seguro.
En la litosfera, hay n validadores conocidos como P1 ..... Pn. Cada validador elige un di entero aleatorio seguro así como un polinomio de k grados fi (x) = di + ai, 1 x ++ ai, k-1xk-1. La técnica entrega fi (j) a otros validadores a través de un canal seguro y transmite di G a cada nodo de la red, siendo G el punto base de la curva elíptica.

Paso 2: Verifique que los mensajes sean correctos.
Pj examinará la corrección de los mensajes después de recibir mensajes de otros validadores: lag = Check (f1 (j), ..., fn (j)) lag = Check (f1 (j) ,., fn (j)) lag = Check (f1 Pj acepta y almacena localmente si flag = true. If flag = falso, Pj rechaza el mensaje y necesita que otros validadores lo reenvíen.

Paso 3: Se le dará una clave para distribuir.
Cuando todos los mensajes se han entregado y verificado, cada validador recibe su clave compartida de la siguiente manera: fj (k), k = 1, ..., n clave compartida k = (j = 1) fj (k), k = 1, ..., n

Paso 4: Determine la dirección de la cuenta bloqueada.
Dirección de cuenta bloqueada = GenerateAddress (d1 G, ..., dn G) n Cualquier actividad en la cuenta bloqueada requerirá la participación de al menos k de n validadores.

Generación de esquemas

La clave privada nunca se produce ni se reconstruye en toda la red durante el procedimiento de creación de la cuenta bloqueada. Se requiere la participación de al menos k validadores para generar la firma de la Cuenta Bloqueada. Calculan los recursos compartidos de firmas de forma independiente utilizando los recursos compartidos de claves que poseen y luego usan los recursos compartidos de firmas para reconstruir la firma completa. El esquema de firmas para cuentas bloqueadas es el siguiente:

Calcule los recursos compartidos de firmas en el paso 1 Mediante el uso de recursos compartidos de claves, varios validadores n Lithosphere calculan los recursos compartidos de firmas del mensaje.

Paso 2: Distribuya las firmas.
Cada Validador transmite su parte de firma a los demás.

Paso 3: Vuelva a montar y difunda toda la firma.
Cuando un Validador obtiene más de k acciones de firma, reconstruye la firma en su totalidad y la transmite a otros Validadores:
firma = Construct Sig (firma share1,., firma sharek)

Paso 4: Producen la firma completa de la cuenta bloqueada, que incluye la siguiente información: firma sharej = Generate Sig (m, key sharej)

Ventajas

Incluso si una parte de la red se paraliza o se pierden algunos recursos compartidos importantes, todo el sistema mantiene la estabilidad y la seguridad. Para reducir la amenaza que representa la exposición a las acciones clave, la acción clave de cada validador se actualiza periódicamente o cuando se cumple una circunstancia desencadenante.

Fácil integración y almacenamiento de datos eficiente

La transacción inicial de la cadena original se utiliza para realizar cualquier operación en la Cuenta bloqueada. No hay nuevos tipos de transacciones ni mecanismos de verificación. Como resultado, teóricamente cualquier cadena puede fusionarse con Lithosphere a bajo costo. Al mismo tiempo, a diferencia del esquema de cuenta de múltiples firmas, que utiliza la lógica de contrato inteligente para lograr la gestión de múltiples partes, la estrategia de creación de cuenta bloqueada utiliza principios criptográficos para lograr la gestión de múltiples partes. Solo hay una firma en la transacción final, no varias. Como resultado, esta técnica es más eficiente en el almacenamiento de datos.

Anonimato de transacción de token de contrato inteligente

Para lograr el anonimato en las transacciones de tokens de contratos inteligentes en Lithosphere, se utilizan firmas de anillo y cuentas únicas. Para que el remitente sea anónimo, la firma de anillo combina el remitente de la transacción con un grupo de miembros falsos. Cada transacción genera una cuenta única que no se puede conectar al propietario real.

Se requiere una técnica para bloquear los activos de la cadena de origen en casi todos los esquemas de transacciones entre cadenas. Los activos bloqueados solo se desbloquearán y se devolverán a la cuenta original u otra cuenta después de que se cumpla la condición de activación.

El sistema de contrato Hashed TimeLock, la estrategia de cuenta de depósito en garantía de terceros de confianza y el método de cuenta de firma múltiple son ejemplos de técnicas existentes.

Totalmente descentralizado sin participación de terceros

La computación segura de múltiples partes se utiliza para generar la cuenta bloqueada. En este procedimiento no se requiere una participación o respaldo de terceros de confianza. Todo lo que necesitamos son rutas seguras para el intercambio de información y el cálculo por parte de los validadores. La técnica de generación de cuentas bloqueadas es menos costosa y más flexible que el esquema de cuentas en garantía de terceros de confianza.

Seguro y estable

El esquema de intercambio secreto de Shamir (también conocido como esquema de intercambio secreto de umbral (k, n) de Shamir) se utiliza para distribuir la clave de la cuenta bloqueada a los validadores de la litosfera. Cada Validador posee un componente de la clave compartida. Incluso si varios validadores se desconectan o pierden sus claves compartidas, la firma de la cuenta bloqueada aún se puede producir y la transacción aún se puede completar con al menos k validadores. Como resultado, la estrategia de creación de cuentas bloqueadas puede garantizarlo.

Sistema de cuenta única

El método de la cuenta de una sola vez es particularmente esencial como base para el anonimato. Cada usuario tiene una sola cuenta principal y varias subcuentas. Por lo tanto, si alguien desea permanecer en el anonimato en una transacción de token de contrato inteligente, debe crear una cuenta relacionada y una cuenta principal única además de la original.

Esquema de firma de anillo

En 2001, se introdujo el método Ring Signature. Es un tipo de esquema de firma de grupo que es un poco diferente. Se requiere un centro de confianza y una configuración segura para un esquema de firma de grupo, lo que significa que el centro de confianza puede rastrear al firmante. Al eliminar el concentrador confiable y asegurar el sistema, el método Ring Signature supera este importante problema.

Desde la introducción del método Ring Signature, se han desarrollado numerosos sistemas prácticos basados en la criptografía de curva elíptica (ECC), como el enfoque de trampilla. Firma de anillo de trampilla, Firma de anillo enlazable, Firma de anillo revocable de anonimato y Firma de anillo denegable son los cuatro tipos de sistemas de Firma de anillo.

El método Ring Signature basado en ECC se desarrolla en Lithosphere para ofrecer anonimato en las transferencias de Token de contrato inteligente.

El esquema Ring Signature se divide en tres secciones. Los siguientes son los detalles, usando el firmante (P, x) como ejemplo:

Obtenga los parámetros públicos usando GEN. El firmante usa el método GeneratePublicKeySet () con la clave pública como parámetro para construir un conjunto de claves públicas con n miembros del estado global:
publickeyset = GeneratePublicKeySet (P) I = GenerateKeyImage ((P, x)) = I = GenerateKeyImage ((P, x)) = I = GenerateKeyImage ((P, x)) = I = GenerateK eyImage ((P, x)) = I = GenerateKeyImage ((P, x)) = I = GenerateKeyImage ((P, x)) = I
FIRMA DEL ANILLO: crea la firma del anillo. El firmante usa GenerateRingSignature () para producir la firma de anillo para el mensaje m, usando el conjunto de claves públicas, I, yx: ringsig = GenerateRingSignature (m, conjunto de claves públicas, I, x)
VERIFICAR LA SIGNIFICACIÓN DEL ANILLO VerifyRingSignature (), que devuelve verdadero o falso con conjunto de claves públicas, I y anillos: lag = VerifyRingSignature valida la firma de anillo del mensaje m. (m, publickeyset, I, ringsig) La firma del anillo es válida si la bandera es verdadera. De lo contrario, es nulo.

La imagen de clave y la firma de anillo en el esquema de Firma de anillo no se pueden comparar con un firmante del conjunto de claves públicas. Cualquiera puede comprobar si una firma es auténtica o no, pero nadie puede identificar al firmante.

Garantía de seguridad basada en criptografía

Muchos intercambios existentes entre cadenas emplean mecanismos de seguridad lógicos, que dependen de que los participantes velen por sus propios intereses. Para decirlo de otra manera, los jugadores no interrumpirán las transacciones entre cadenas si eso significa dañar sus intereses. Esto se conoce como "La hipótesis de los participantes racionales". Lithosphere emplea tecnología de umbral de intercambio de secretos, así como criptografía de curva elíptica original, para garantizar la seguridad de la solución de firma original.

La solución de administración de cuentas bloqueadas basada en computación de múltiples partes;

Las firmas de anillo y el método de protección de privacidad basado en cuentas de una sola vez para transacciones de token de contrato inteligente.

Después de comenzar una transacción entre cadenas, todas las siguientes acciones se realizan automáticamente entre los nodos del validador de Lithosphere y no requieren la coordinación de los participantes de la transacción. Esto deja la seguridad de los métodos criptográficos para garantizar el funcionamiento perfecto del sistema.

Contratos inteligentes

Identificar y definir los vínculos financieros de varias partes Mejoras en los contratos inteligentes.

Un contrato inteligente es un contrato que define la relación y las condiciones de interacción de valor de uno o más activos digitales entre múltiples participantes en términos de sucesión temporal y ubicación espacial y se utiliza para completar transacciones financieras de uno o múltiples activos digitales entre múltiples participantes.

Los activos mapeados en la cadena Lithosphere mediante Lock-in de activos digitales, que permite que los contratos inteligentes de Lithosphere especifiquen conexiones entre muchos activos digitales diferentes al mismo tiempo, se conocen como activos digitales.

Los propietarios o consumidores de varios activos digitales se denominan participantes múltiples. Se representan como cuentas en la cadena Lithosphere, incluidas las cuentas de usuario y de contrato. Los participantes del contrato en los contratos inteligentes criptográficos pueden comprender numerosas cuentas de usuario, así como muchas cuentas de contrato.

La definición de transacciones financieras a través de contratos inteligentes se convierte en una descripción de las conexiones entre varios activos digitales y la propiedad diversa en el tiempo y el espacio porque el núcleo de las finanzas es el intercambio de valores en el tiempo y el lugar.

Las siguientes son las limitaciones de los contratos inteligentes actuales:

- Solo puede operar en el mismo activo digital entre dos partes de la misma cadena; Solo puede
- transferir la propiedad de los activos digitales, haciendo que el uso y la propiedad sean indivisibles;
- Solo se puede activar mediante una transacción, sin condiciones de activación fuera de la cadena o entrada de información fuera de la cadena legítima.
- Realizar aplicaciones de propiedad y usufructo entre múltiples partes y múltiples activos digitales; Obtenga
- efectivamente la entrada de datos fuera de la cadena;
- Llame a otros contratos inteligentes en un contrato inteligente de manera cerrada o paralela como si el contrato inteligente fuera un contrato inteligente.

La distribución de claves en la gestión de Myriad Token ha permitido la interacción entre varios activos digitales y se ha convertido en el objeto a definir y programar para los contratos inteligentes de Lithosphere. Como resultado, tiene la capacidad y la necesidad de implementar funciones DeFi como separación de funciones múltiples, múltiples fichas y usufructo (derechos).

La capacidad de un contrato inteligente para manejar muchos tipos de cuentas distintos y, al mismo tiempo, definir las conexiones entre numerosos usuarios y varios contratos inteligentes se conoce como función múltiple.

Después de mapear distintos activos digitales en Lithosphere usando Lock-in, un contrato inteligente en Lithosphere puede describir la relación entre muchos activos digitales diferentes al mismo tiempo.

La separación de usufructos se refiere a la capacidad de separar los usufructos (derechos) y la propiedad de los activos digitales. El presente contrato inteligente solo puede transferir tokens en su conjunto de una parte a otra, y no es factible que una de las partes obtenga la propiedad de un activo digital mientras que la otra parte obtiene el usufructo, lo que implica que la propiedad y el usufructo están separados en el sistema inteligente tradicional. Contratos. Es simple establecer más de dos cuentas de usuario o cuentas contractuales en un solo contrato inteligente, lo que permite la separación de cuentas de propiedad y uso, así como actividades financieras como préstamos hipotecarios en varios activos digitales.

La transferencia de activos digitales será posible si el vínculo entre ellos se especifica únicamente en términos de espacio. Es una conexión prestada entre ellos si la relación se caracteriza en términos de tiempo. Cuando la conexión se describe en términos de atribución de objeto, representa la propiedad y el usufructo de los objetos. Como resultado, la abstracción lógica de una o más relaciones en términos de atribuciones de tiempo, espacio y objeto puede conducir a la construcción de varias transacciones que van desde simples a complejas entre varios activos digitales, incluso provocando finanzas aún por realizar. innovaciones, lo que permite una imaginación ilimitada.

Mecanismo de activación múltiple por contrato Diversidad de condiciones de activación

Debido a que el contrato inteligente actual se activa mediante una transferencia al contrato, la implementación actual de los contratos inteligentes se basa en la transferencia de propiedad de los activos digitales.

Cuando un usuario inicia una transferencia a un contrato inteligente, por ejemplo, un nodo debe primero validar la legalidad de la transferencia, lo que incluye determinar si el saldo financiero actual del usuario en la cadena de bloques respalda la transacción. El contrato inteligente luego ejecuta la función relevante para aceptar el regalo y lo juzga en función de la condición de respuesta predeterminada de la función. Por ejemplo, el contrato inteligente examinará el monto total de la donación y solo lo aceptará si no supera la cuota. Finalmente, se colocará un valor de contrato modificado o un estado de contrato inteligente en el bloque para indicar que la transacción ha tenido lugar.

Podemos ver en el análisis anterior que las funciones del contrato inteligente implicarán juicios sobre algunos criterios, pero estas condiciones no se verificarán si el contrato inteligente no se activa en primer lugar. La ejecución de las siguientes reglas en el contrato inteligente no se activará incluso si se cumplen las circunstancias requeridas. Muchos escenarios de transacciones financieras, como una estrategia comercial cuantitativa pasiva, son imposibles de ejecutar si un contrato inteligente no puede activarse por factores distintos a una transacción. Como resultado, mejorar el mecanismo de activación es el primer paso para mejorar los contratos inteligentes para las aplicaciones DeFi. Además de admitir el método de activación activa existente, se introducen dos nuevos mecanismos de activación: activación por tiempo y activación por evento.

Los tres modos de activación de los múltiples mecanismos de activación son los siguientes:

- El modo de activación activa es similar al modo de activación de contrato inteligente actual y es compatible con todos los contratos inteligentes.
- El modo de activación por tiempo se refiere a la capacidad de un contrato inteligente para ser activado por circunstancias de tiempo, como un punto de tiempo o duración.
- El modo de activación de eventos indica que se activará un contrato inteligente cuando ocurra un evento determinado, como los intercambios habituales a lo largo del tiempo, y dichas aplicaciones serán totalmente compatibles con el modo de activación por tiempo. La captura de eventos es fundamental en el comercio automatizado y el comercio cuantitativo, por ejemplo. El modo de activación de eventos debe usarse para iniciar tales ocurrencias.

Por el momento, los contratos inteligentes solo pueden manejar información desde dentro de su cadena de bloques, sin embargo, en el caso de múltiples mecanismos de activación, parte de la información de activación vendrá del exterior. Como resultado, los contratos inteligentes proporcionarán una interfaz de entrada de información externa y utilizarán diferentes técnicas para verificar la validez y autenticidad de los datos fuera de la cadena.

Para hacerlo, Lithosphere primero transmitirá datos externos a través de HTTP o socks a los nodos, dependiendo de las API comunes ofrecidas por fuentes de datos de terceros. Lithosphere encapsulará las llamadas de datos de ciertas fuentes de datos fuera de la cadena ampliamente utilizadas, que funcionarán de manera similar a una llamada al sistema para suministrar datos para la adquisición de nodos. Sin embargo, los nodos pueden crear sus fuentes de datos utilizando las rutas de recopilación de datos antes mencionadas para obtener información de datos importante.

El proceso de consenso verifica la validez de los datos adquiridos fuera de la cadena. Cuando un nodo descubre que los datos fuera de la cadena están vinculados a circunstancias específicas que desencadenan un contrato inteligente, el nodo se ejecutará y transmitirá el contrato inteligente. Si un nodo malicioso transmite intencionalmente un contrato inteligente en toda la red, la red puede simplemente rescindir el contrato inteligente durante la fase de ejecución si se considera malicioso, porque otros nodos honestos volverán a verificar el contrato inteligente antes de la ejecución. Tal conducta malévola no tendrá ningún impacto en la operación real del contrato inteligente, y no habrá oportunidad de beneficiarse de ganancias no devengadas o de arbitraje.

Los métodos de incentivos también pueden ayudar con el problema de la efectividad de la entrada de datos fuera de la cadena. Debido a que la confirmación de datos requiere el consenso de la red, los nodos solo pueden aumentar sus ingresos buscando fuentes de datos más rápidas y confiables y validando con precisión las circunstancias desencadenantes. Los nodos de red de alta eficiencia serían recompensados debido a la naturaleza del mercado eficiente y la asignación de recursos. La validez de los datos finales no se ve afectada por los datos generados por algunos nodos no autorizados.

Mejoras y compatibilidad

Basado en Ethereum y otros contratos inteligentes de blockchain, el contrato inteligente de Lithosphere se actualizará y desarrollará. Las adiciones de funcionalidad, como los mecanismos de activación, se agregarán según la compatibilidad con los contratos inteligentes existentes. Los contratos inteligentes que ya operan en Ethereum y otras cadenas de bloques podrán simplemente pasar a Lithosphere, y los desarrolladores de contratos inteligentes podrán crear rápidamente en Lithosphere.

El siguiente paso será optimizar los lenguajes de programación y las máquinas virtuales para un entorno de desarrollo de aplicaciones más robusto, así como proporcionar herramientas de desarrollo de aplicaciones más intuitivas y entornos de depuración para desarrolladores con menos conocimientos de codificación.

Contrato adjunto convocatoria

Las mejoras anteriores a los contratos inteligentes actuales eventualmente permitirán que los contratos inteligentes en Lithosphere definan relaciones y reglas de interacción basadas en diversas condiciones, entre varios valores y participantes, en el tiempo y el espacio, permitiendo que los contratos inteligentes en Lithosphere creen aplicaciones DeFi.

En Lithosphere, un contrato inteligente no solo puede cambiar el estado y los datos de la cuenta, sino que también puede llamar a otro contrato inteligente durante la ejecución si se cumplen ciertos criterios.

Se deben completar las siguientes actividades para implementar la llamada del Smart Contract A al Smart Contract B:

(1) Cree un contrato inteligente de llamada adjunto.

Un juicio de condición preestablecido y una regla de condición preestablecida para invocar el contrato inteligente B se agregan al código del contrato inteligente A, y se genera el parámetro del índice de dirección del contrato inteligente objetivo. La entrada de datos cuando se activa el contrato inteligente A, así como el resultado del cálculo de datos, proporciona la base para el juicio de condición. Si se cumplen los criterios predefinidos, el nodo descargará y ejecutará el contrato inteligente B.

La condición de la llamada se divide en dos partes: reglas y tiempo. Las reglas son rutinas de cálculo preprogramadas en un contrato inteligente. Las condiciones de tiempo pueden ser una condición predefinida en un contrato inteligente que se activa cuando se ejecuta el contrato inteligente o una condición que verifica el estado de un contrato inteligente con regularidad.

(2) El procedimiento para realizar una llamada adjunta.

I.Cuando se activa el contrato inteligente A, determinará si es necesario o no ejecutar el contrato inteligente B en función de las circunstancias de llamada preestablecidas.

ii.Cuando se satisfacen las circunstancias de la llamada, se llama a la función de cálculo preestablecido y el resultado se utiliza como entrada del contrato inteligente B.

iii.El nodo que realizó el contrato inteligente A descarga el contrato inteligente B en el entorno informático local, ingresa los datos determinados en el paso anterior como los datos de entrada del contrato inteligente B y comienza a ejecutar el contrato inteligente B.

Los procedimientos descritos anteriormente se pueden usar para ejecutar la llamada del contrato inteligente A para contratar B. Llamamos al enlace lógico entre ellos una llamada adjunta de un contrato inteligente porque el contrato inteligente B se basa en el estado del contrato inteligente A como el disparador y los datos de entrada .

Los contratos inteligentes no solo toman decisiones basadas en su lógica comercial, sino que también pueden invocar otros contratos inteligentes basados en criterios predefinidos. Por lo tanto, es simple crear interacciones de llamadas similares a una red entre distintos contratos inteligentes, estableciendo la interacción de valor entre las aplicaciones financieras conectadas y permitiendo así la creación de aplicaciones complicadas. Como consecuencia, los servicios financieros sofisticados, como una solicitud de préstamo basada en el flujo de caja futuro, pueden desarrollarse utilizando llamadas de contrato inteligente adjuntas. La plataforma Lithosphere puede realizar actividades financieras complicadas gracias a estas características y al mecanismo de múltiples disparadores, que se explicará en la sección de mecanismos de múltiples disparadores.

Desarrollo de contrato

Para cumplir con un contrato inteligente, se deben completar los siguientes pasos:

(1) Construya un contrato inteligente

Los contratos inteligentes Lithosphere son una evolución de los contratos inteligentes actuales. Debe haber dos componentes en el contrato: definición y descripción.

La sección de definición es consistente y cumple con los contratos inteligentes de Ethereum. Como resultado, los contratos inteligentes actuales de Ethereum son compatibles con Lithosphere. Contiene el estado del contrato, los valores del contrato y los métodos para definir las condiciones y reglas de respuesta.

(2) Lanza un contrato inteligente

Tras la publicación del contrato inteligente, la sección de definición se registra en la cadena de bloques siguiendo los contratos inteligentes actuales. La sección de descripción se fusionará con las condiciones de activación de todos los contratos inteligentes en la cadena de bloques actual para crear una lista de llamadas que se registrará en el bloque y será accesible para toda la red.

Cada fila de entradas en la lista de llamadas corresponde a un contrato inteligente. Además del material en la descripción, cada registro tiene una dirección de índice que corresponde al contrato inteligente almacenado.

El siguiente paso será optimizar los lenguajes de programación y las máquinas virtuales para un entorno de desarrollo de aplicaciones más robusto, así como proporcionar herramientas de desarrollo de aplicaciones más intuitivas y entornos de depuración para desarrolladores con menos conocimientos de codificación.

Condiciones de tiempo y activación

Los activadores proactivos son similares a cómo se activan los contratos inteligentes en Ethereum, que es mediante una transferencia a una dirección de contrato. Los siguientes procedimientos se utilizarán para crear el nuevo modo de activación por tiempo y el modo de activación por evento:

(1) Juzgue las condiciones de activación por nodos

Para su ejecución, la lista de llamadas se descarga en el nodo local. Para determinar si cada elemento de la lista coincide con la condición de activación, el nodo sondeará la lista y descargará datos coincidentes o locales.

(2) Activar un contrato inteligente

Cuando el nodo de contabilidad descubre que se cumple la condición de un determinado contrato inteligente durante el sondeo en un momento específico, el nodo adquiere la dirección del contrato inteligente de la lista de llamadas y envía una transacción particular para activar el contrato inteligente. Al mismo tiempo, toda la red de nodos contables descargará el contrato inteligente de la transacción seleccionada.

(3) Ejecute el contrato inteligente

Un contrato inteligente se realiza de la misma manera que el contrato inteligente actual, es decir, se ejecuta en el entorno operativo del nodo (máquina virtual). El contrato se diferencia en que tiene desencadenantes adicionales y puede integrarse en otros contratos a través de condiciones desencadenantes, lo que da lugar a una cadena de sucesos.

Interfaz y desarrollo rápidos

Lithosphere proporcionará entornos de desarrollo para contratos inteligentes, así como bibliotecas de funciones. Los desarrolladores pueden utilizar estas funciones para acelerar la creación de contratos inteligentes. Para facilitar el acceso e interactuar con los datos, el entorno de desarrollo encapsulará diferentes cadenas de bloques, contratos inteligentes, fuentes de datos, etc., como interfaces.

A continuación, se muestran algunas interfaces típicas:

(1) Gestión de claves

- Inicializar el par de claves, crear y devolver la dirección de clave pública son todas funciones que deben implementarse.

- Devolver el valor hash de la firma después de ingresar la dirección de clave pública y la firma asociada.

(2) Adquisición de datos de Blockchain

Si se piensa en las cadenas de bloques como sistemas que permiten aplicaciones distribuidas (DApps), los contratos inteligentes que recopilan datos de la cadena de bloques serán lo mismo que obtener las variables globales del sistema de cadenas de bloques. Los contratos inteligentes pueden acceder a la siguiente información en la cadena de bloques utilizando esta interfaz:
Apunta a una altura de bloque específica. La información del remitente. La información del destinatario.

(3) Convocatoria de contratos inteligentes

Los contratos inteligentes se utilizan para implementar todas las funcionalidades de Lithosphere.
El uso de un contrato inteligente de transferencia se puede utilizar para realizar una transferencia en un contrato inteligente. Para abarcar las aplicaciones financieras típicas, Lithosphere empleará contratos inteligentes más básicos. Como resultado, desarrollar un contrato inteligente en Lithosphere implica incorporar contratos inteligentes simples en aplicaciones financieras convencionales y luego mejorar su funcionalidad agregando funcionalidades más complicadas.

Lithosphere identificará los contratos financieros fundamentales, lo que dará como resultado una biblioteca de contratos inteligentes para que los desarrolladores la empleen.

(4) Interfaz de origen de datos fuera de la cadena

En circunstancias desencadenantes, los contratos inteligentes emplean datos fuera de la cadena. Estos datos se obtienen con frecuencia mediante un HTTP estándar o una API basada en calcetines proporcionada por un tercero. Una función de llamada de interfaz de terceros, por ejemplo, obtendrá la dirección URL de destino a través de HTTP y devolverá un paquete JSON.

Este método de interfaz también se puede utilizar para obtener información de otras cadenas de bloques, como consultar y confirmar si una transacción en otra cadena es confirmada por el bloque donde se encuentra.

Lithosphere utilizará la Fundación para descubrir interfaces de terceros y crear interfaces de terceros para que los contratos inteligentes llamen.

(5) Desarrollo rápido

Lithosphere proporcionará varias plantillas de contratos inteligentes para aplicaciones comunes para referencia y uso por parte de los desarrolladores de aplicaciones en las primeras fases del proyecto. Sin embargo, los desarrolladores de aplicaciones aún deben cumplir con ciertos estándares de código.

Los desarrolladores de aplicaciones pueden usar contratos inteligentes creando condiciones previas para actualizar las aplicaciones financieras deseadas a medida que las funcionalidades subyacentes de la plataforma y las aplicaciones financieras básicas comunes se vuelven más ingeniosas y complejas. . Para mejorar aún más dicho entorno de desarrollo y reducir drásticamente el umbral de desarrollo para los desarrolladores, el plan de Lithosphere incluye herramientas de desarrollo de aplicaciones visuales y modulares, un entorno de compilación, un entorno de prueba de aplicaciones, que permitirá a los desarrolladores de contratos inteligentes centrarse en innovaciones en aplicaciones financieras y un Launchpad para iniciar dApps.

(6) Lenguaje de programación y máquina virtual

Para la interoperabilidad con contratos inteligentes y la transferencia rápida de contratos inteligentes existentes, Lithosphere empleará inicialmente el lenguaje de programación Solidity de Ethereum. Proporcionaremos compiladores para varios lenguajes en el futuro para dar cabida a lenguajes de desarrollo de contratos más inteligentes.

Crearemos un sistema de sandboxing de contrato inteligente que realiza comprobaciones particulares a prueba de fallas y minimización del costo de combustible mediante un navegador o editor de programación.

Utilizar múltiples activadores para realizar funciones financieras complejas.

Los contratos inteligentes existentes solo pueden esperar pasivamente a que el desencadenante de una transacción sea realizado por una transacción, lo que presenta el problema de la necesidad de la introducción de un corredor de confianza para establecer quién tiene derecho a activar un contrato inteligente y bajo qué condiciones. En la plataforma Lithosphere, los contratos inteligentes describirán las relaciones entre las partes a través del código (ya sea por contrato inteligente común o por contratos adjuntos). Múltiples activadores automatizarán la ejecución de estos contratos inteligentes, lo que les permitirá participar uno tras otro sin la necesidad de interacción humana. Como resultado, muchas partes pueden confiar entre sí utilizando códigos de contrato inteligentes para realizar una variedad de actividades financieras complicadas. Los contratos inteligentes de Lithosphere brindan la capacidad de programar la propiedad y el usufructo de forma independiente,

Los contratos inteligentes ahora pueden realizar una amplia gama de actividades financieras gracias a esta funcionalidad. Por ejemplo, si desea pedir dinero prestado, puede diseñar el contrato inteligente Lithosphere para pedir prestado tokens, devolver moneda fresca y pagar intereses. Usando la plataforma Lithosphere como ejemplo, un contrato inteligente puede administrar un fondo de manera autónoma, lo que incluye llevar el usufructo de varios tokens a un contrato inteligente, mantener varios activos digitales, producir tarifas de administración, pagar el dividendo, etc. Utilizando el ejemplo de varios derivados, el contrato inteligente puede tomar márgenes y realizar operaciones como modificar márgenes, liquidar y liquidar utilizando activadores de fuentes de datos externos.

Plan de operación comunitaria

La Fundación KaJ Labs, como patrocinador principal del proyecto, tiene como objetivo un ecosistema blockchain prometedor en lugar de la rentabilidad corporativa como lo hacen las iniciativas empresariales y de inicio típicas. La plataforma Lithosphere, que beneficia a todos los poseedores de tokens, no es propiedad de una sola entidad o persona. Toda la comunidad de tokens de blockchain es propietaria de la plataforma Lithosphere. Lithosphere hace que el uso de tokens sea más flexible y accesible, además de darles a los tokens el potencial de ofrecer servicios sofisticados de DeFi. El valor de todas las fichas aumentará.

En realidad, el ecosistema de cadenas cruzadas de Internet of Values es un proyecto enorme. La Fundación Kaj Labs debe hacer progresar el ecosistema, al que debe unirse y participar toda la comunidad, y cuya cadena de bloques debe mejorarse mediante la iteración continua. Estas son exactamente las características de un proyecto blockchain. Las iniciativas de blockchain comienzan con una necesidad o problema crítico que debe abordarse, que los participantes y aquellos que necesitan deben investigar continuamente para fomentar el progreso continuo. Al mismo tiempo, atraerá a más personas a la comunidad, lo que hará que la demanda cambie los proyectos en una mejor dirección y fomente el avance de su tecnología. El propósito de los ecos es generar un ciclo de retroalimentación positiva de incentivos, aplicaciones y uso. Como resultado,

Las siguientes personas componen la comunidad:

- El equipo de desarrollo de Core y la Fundación Kaj Labs. Son patrocinadores y facilitadores de la plataforma del proyecto.

  Programadores que quieran formar parte del proyecto. Pueden unirse al equipo de desarrollo de la Fundación o crear y optimizar de forma independiente Lithosphere como un tercero si están interesados en proyectos o tecnologías de proyectos.

- Los nodos participantes en la Litosfera Ganan dinero al realizar un seguimiento de los libros de contabilidad y al operar contratos inteligentes al mismo tiempo que mantienen la Litosfera.

- Usuarios de la plataforma Lithosphere. Para DeFi y otros servicios, emplean la plataforma Lithosphere. • En la plataforma Lithosphere, proveedores de servicios DeFi como institutos de pago, intercambios centralizados o descentralizados, institutos de préstamos y otros proveedores de servicios financieros.

- Titulares de tokens de Lithosphere, como empresas de capital privado, inversores en etapa inicial, inversores en etapa tardía e inversores potenciales.

- Otras partes involucradas en el desarrollo de la litosfera, como los medios de comunicación, el gobierno, etc.
  El objetivo de las operaciones de la comunidad es reunir tanta fuerza como sea posible y organizarla de la manera más eficiente posible para que Lithosphere pueda iterar, mejorar, influir y servir a una comunidad más amplia.

  El crecimiento de la comunidad está indisolublemente ligado tanto a las comunidades centrales como a las periféricas. Los dos son mutuamente beneficiosos, y la comunidad central actúa como punto focal. La comunidad periférica, por otro lado, debe continuar participando en la creación de la comunidad clave, ya que la comunidad central se originará y tomará prestado de la comunidad periférica, y la comunidad periférica requerirá los recursos de la comunidad central para apoyarla. Descubrimos que Bitcoin, Ethereum y otros proyectos han crecido de la misma manera. La comunidad principal está formada por los primeros en adoptar, las comunidades de tecnología blockchain y las comunidades de valor de blockchain, mientras que los recursos periféricos incluyen inversores, usuarios, desarrolladores, periodistas y otras partes interesadas adicionales.

Método de promoción de proyectos

- El concepto separa las operaciones de la comunidad en dos categorías: centro y periferia. El primero prefiere el modo fuera de línea, mientras que el segundo prefiere el modo Internet. La siguiente es la estrategia para las operaciones comunitarias clave:

- Equipo de la Fundación Lithosphere: el equipo será recompensado con tokens. Una razón es compensar los recursos utilizados en el tiempo anterior y la otra es permitir que cualquiera se convierta en accionista y esperar que contribuya a Lithosphere en el futuro.

- Comunidad para la tecnología blockchain.

- La tecnología es tanto el aspecto más importante como el más difícil del desarrollo de blockchain. Utilizaremos métodos en línea y fuera de línea para descubrir y nutrir un grupo de talentos de primer nivel para promover la comunidad tecnológica, utilizando la experiencia técnica y los recursos sociales del equipo fundador.

- Comunidad de valor de blockchain: utilizando la comunidad de tecnología de blockchain, podemos organizar reuniones con los titulares para difundir el conocimiento de blockchain y al mismo tiempo promover oportunidades de colaboración con la comunidad de valor privado.

Movimiento para promover la tecnología Blockchain

La Internet de los valores tiene actualmente un cuello de botella en la usabilidad, que requerirá un trabajo continuo en el futuro para mejorar. La utilidad de Internet of Values está fuertemente relacionada con el proyecto Lithosphere. Para contribuir a la utilidad de la tecnología blockchain, iniciaremos el "movimiento de promoción de la tecnología blockchain". Para la Fundación Kaj Labs, este será un proyecto a largo plazo.

En forma de salones técnicos, campos de entrenamiento y seminarios, este movimiento continuará acumulando habilidades e información técnica. Alentaremos a los participantes a que proporcionen contenido, que se publicará en numerosos sitios web y en los medios de comunicación. Para hacer crecer la comunidad técnica de blockchain, brindaremos sesiones de capacitación mensuales para reclutar empleados de Internet convencionales y otro personal técnico.

El movimiento de promoción de la tecnología blockchain reunirá a todas las fuerzas, incluidas universidades, institutos de investigación, empresas, instituciones, gobiernos y alianzas, para crear una asociación cooperativa y unir recursos para apoyar el avance de la tecnología blockchain.

La estandarización del movimiento de interfaces Blockchain

Internet de los valores tiene problemas de interoperabilidad y escalabilidad que requieren que muchas partes los aborden. El proyecto Lithosphere está indisolublemente ligado al avance y desarrollo de estos dos obstáculos. Al establecer el "Movimiento de estandarización de la interfaz Blockchain", ayudaremos a mejorarlos. Para la Lithosphere Foundation, este será un proyecto a largo plazo.

El movimiento fomentará la estandarización de interfaces no solo entre cadenas de bloques, sino también entre organizaciones descentralizadas y centralizadas, así como entre cadenas de bloques y fuentes de datos externas.

Aplicaciones de la litosfera

Empréstitos y préstamos

El uso del dinero digital para producir nuevo valor y obtener ingresos es una tendencia inevitable a medida que crece en importancia como medio de intercambio de valor y como soporte de almacenamiento de valor. Bitcoin, por ejemplo, se utiliza para financiar empresas mineras de blockchain y otras iniciativas de cifrado. Las opciones de inversión directa para la moneda digital se han expandido a medida que ha crecido la variedad de aplicaciones para el dinero digital.

Aquellos que generan valor con monedas digitales necesitan más, y las personas que poseen monedas digitales quieren aumentar su valor, por lo que aumentará la demanda de préstamos y préstamos de monedas digitales.

Considere la criptomoneda Ethereum (ETH). En Lithosphere, un proveedor de servicios crea una aplicación de depósito y establece la tasa de interés mediante un contrato inteligente.

A través de una transacción entre cadenas, un usuario envía ETH desde Ethereumblockchain a la dirección del contrato inteligente de Lithosphere. El depósito en Lithosphere genera un comprobante (tokens de Lithosphere que parecen recibos bancarios de depósito) que se acredita a la cuenta de Lithosphere del usuario. Luego, el contrato inteligente calcula el interés por usted. Cuando el usuario quiere retirar el dinero, el bono se envía a una dirección intermedia y se realiza una transacción entre cadenas. En la cadena original, el ETH correspondiente al cupón se desbloquea y se envía de vuelta a la cuenta del usuario original. Las reservas de depósito (los activos bloqueados en la cadena de origen que corresponden a la dirección intermedia) están siempre visibles.

Pago y liquidación

Las empresas aceptan cada vez más activos digitales como Bitcoin como forma de pago. Habrá más aplicaciones en el futuro que empleen una variedad de monedas digitales para el pago. Hay varias opciones de pago disponibles en la actualidad, incluidas VISA, Paypal y Alipay, cada una con su propio conjunto de procedimientos de pago y liquidación. La litosfera es una plataforma distribuida multidivisa que combina muchos libros de contabilidad bancarios en un solo libro de contabilidad unificado. Sin necesidad de instalar varias carteras de monedas digitales, cualquier empresa o usuario puede utilizar la cartera Lithosphere para realizar pagos y liquidaciones en varias monedas.

Transacción e intercambio

Por el momento, se requieren intercambios centralizados y mercados de venta libre para completar las operaciones de moneda digital. Cada transacción depende de la confianza de las bolsas y los intermediarios. Después de que varias monedas se hayan vinculado con la litosfera, los intercambios e intermediarios pueden usar contratos inteligentes para permitir el comercio de subastas en múltiples monedas y las transacciones de acera uno a uno. En Lithosphere, el mecanismo de transacción de protección de la privacidad admite transacciones que requieren protección de la privacidad. Importar dinero digital a Lithosphere, iniciar transacciones privadas en Lithosphere y mover la moneda digital de regreso a la cadena original es posible con Lithosphere. La privacidad de la cadena original está protegida hasta cierto punto al ocultar las rutas de seguimiento de fondos. La litosfera puede manejar 10,

1,700 TPS. Visa realiza alrededor de 1.700 transacciones por segundo en promedio (según un cálculo derivado de la afirmación oficial de más de 150 millones de transacciones por día).

Inversión y Financiamiento

Las instituciones tradicionales recurren cada vez más a cadenas de consorcios para almacenar activos como facturas comerciales, puntos de fidelidad, derechos de ganancias futuras y cuentas por cobrar. En el futuro, se registrarán más activos financieros en libros de contabilidad distribuidos basados en cadenas de consorcios. Cuando estas cadenas de consorcios se conectan a Lithosphere, se convierten en proveedores de activos financieros y los inversores pueden adquirir estos activos con sus monedas digitales. Es similar a comprar bienes financieros en un banco, como en la empresa bancaria tradicional. La principal distinción es que pueden participar más intermediarios y los propietarios de activos pueden financiarse directamente.

En el mundo de la cadena de bloques, las ofertas iniciales de monedas (ICO) / ofertas de intercambio inicial (IEO) se han convertido en una forma popular de recaudar fondos, y la práctica se está expandiendo a dominios que no pertenecen a la cadena de bloques. Los contratos inteligentes se utilizan directamente para las ICO en un número cada vez mayor de proyectos, en particular los que se basan en Ethereum o BSC, lo que hace que el proceso sea más abierto y equitativo. Sin embargo, las ICO que aceptan exclusivamente Ether molestan a los inversores que poseen otras monedas digitales. El emisor de ICO puede usar Lithosphere para crear un contrato inteligente que permita inversiones en múltiples monedas. Los inversores pueden invertir más fácilmente utilizando Ethereum, Bitcoin o cualquier otro token de blockchain vinculado con Lithosphere, y los emisores pueden administrar sus fondos de manera más simple. Además, cuando se lanza una nueva cadena de bloques, Las transacciones entre cadenas de Lithosphere se pueden utilizar para convertir las acciones financiadas por crowdfunding a la moneda local. Con Lithosphere, estamos entrando en una nueva era de emisión de derechos digitales basada en blockchain

Más aplicaciones

Las aplicaciones financieras mencionadas anteriormente están destinadas a ayudar a los lectores a comprender mejor el fundamento y el valor de Lithosphere. Más ejemplos incluyen tarjetas de crédito multidivisa basadas en dinero digital, valores respaldados por activos que agrupan una variedad de activos, empresas de préstamos entre pares basadas en monedas digitales y crowdfunding, entre otros.

Los principales bancos ven la tecnología blockchain como una estrategia esencial, pero también están analizando cómo podría usarse para alterar los negocios tradicionales.

La banca, como el cambio de divisas, ha prosperado en el ámbito del dinero digital. En estos sectores, las cadenas de bloques están progresando en dos vías paralelas, pero con el surgimiento de los activos digitales y su creciente integración en la economía real, estas dos vías eventualmente se cruzarán. Los balances bancarios se trasladarán en gran medida a cadenas de bloques, y los activos digitales se incorporarán en los balances bancarios (bancos que permiten el préstamo y depósito de activos digitales) (el dinero fiduciario está representado y contabilizado por tokens de cadena de bloques). Esta futura integración contará con el respaldo de la tecnología entre libros mayores de Lithosphere.

Características actuales de la litosfera

Interoperabilidad

Interoperabilidad entre cadenas a través de un modelo de custodia descentralizado (MDKM)

Blockchain de próxima generación para NFT

Una red escalable, descentralizada y entre cadenas diseñada para llevar tokens no fungibles a todos.

Función de bloqueo de tiempo

La función de bloqueo de tiempo única de Lithosphere le permite extraer valor de tiempo de sus activos digitales

Seguridad

Gestione y controle las claves privadas de forma distribuida con la tecnología MDKM

Escalabilidad

Resolver el problema de escala es un tema abierto para las cadenas de bloques PoW como Bitcoin y Ethereum v1. Actualmente, los nodos de Bitcoin y Ethereum procesan cada transacción y también almacenan todos los estados. Dado que la prueba de participación de Lithosphere puede comprometer bloques mucho más rápido que la prueba de trabajo, las zonas de EVM impulsadas por el consenso de Lithopshere y que operan en criptografía en puente pueden proporcionar un mayor rendimiento a las cadenas de bloques de PoW Ethereum, Litecoin y Bitcoin.

Recursos digitales

Cree, administre o incluso preste sus propios activos digitales y NFT utilizando el protocolo LEP100 de Lithosphere.

Activos de juego entre cadenas.

Economías de juego, propiedad de los jugadores.
Crea recursos en el juego que estarán disponibles para siempre. Aporta un valor duradero a los jugadores permitiéndoles llevar su botín a otro juego o al mundo real en la cadena de bloques JOT ART impulsada por Litho.

Productos de litosfera

- Lithosphere blockchain (PoS) Litho token nativo de cadena cruzada
- LithoSwap: DEX de cadena cruzada con soporte de intercambio NFT.
- LEP100 Token Launchpad - Litho Launchpad
- Cartera Thanos multidivisa con cadena cruzada
- Plataforma JOT NFT (mercado NFT, NFT DEX, SDK para distribuir NFT en cualquier lugar de manera rentable, entre cadenas) FLEEK:
- plataforma de conciertos descentralizada impulsada por la comunidad en la cadena de bloques.
- LAX - Moneda estable algorítmica

Gobernanza del proyecto de la litosfera

Miembros del Consejo

Elegido para representar a las partes interesadas pasivas en dos roles principales de gobernanza: proponer referendos y vetar referendos peligrosos o maliciosos. El creador de la litosfera, Joel Kasr, preside el comité del consejo.

Comité técnico

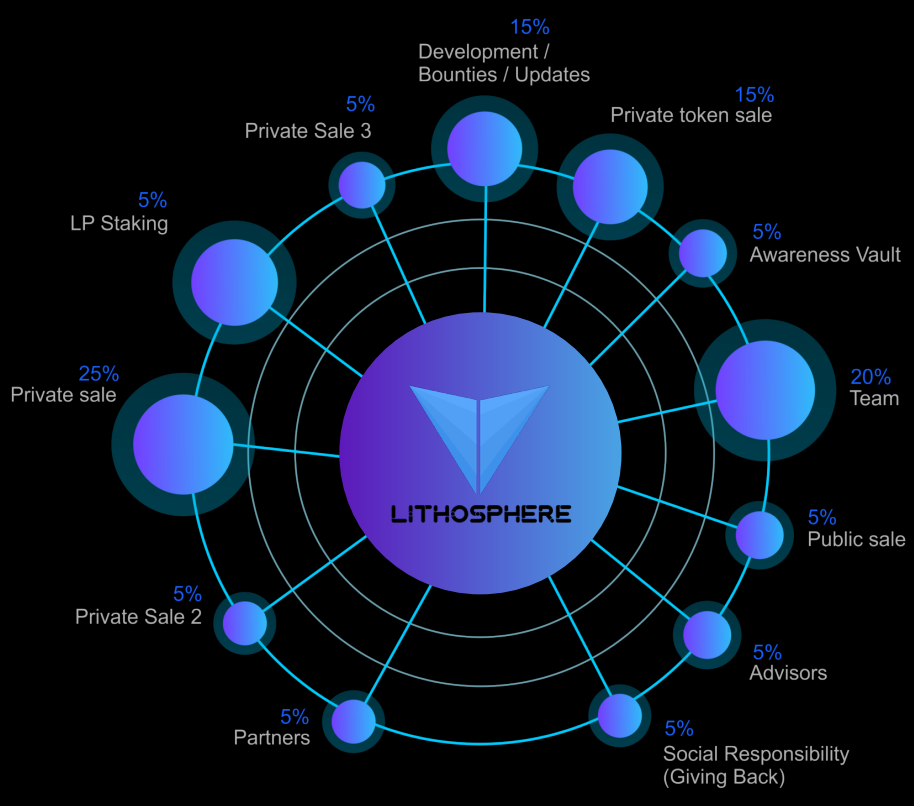
Compuesto por equipos centrales que construyen activamente Litho. Puede proponer referendos de emergencia, junto con el consejo, para una votación e implementación aceleradas.

Miembros de la comunidad

Puede hacer y votar propuestas para mejorar la litosfera.

Tokenomics

Suplemento total



Financiamiento del proyecto:

La distribución inicial de monedas litográficas y validadores en Kamet (la primera versión de la red Lithosphere) irá a los donantes de Lithosphere Fundraiser (70%), donantes principales (5%), KaJ Labs Foundation (10%), conciencia de la red (10%) y los miembros del equipo central (10%). Desde Kamet en adelante, 1/3 del monto total de $ Litho será recompensado a validadores y delegadores vinculados cada año.

Se instalará una de las bóvedas / cápsulas de la litosfera para almacenar fondos de marketing / concienciación.

Mapa vial

Tercer trimestre de 2021

- Finalizar el concepto de red
- Desarrollo central formación de equipo
- Lithopshere Blanco artículo publicado
- Establecer clave asociaciones
- Anuncios importantes

Cuarto trimestre de 2021

- NFT DEX Testnet
- Presencia en los medios
- Introducir nuevo token estándar - LEP100
- Introducción de gobernanza en el Red de la litosfera usando Litho nativo simbólico.
- Preventa de fichas litográficas

T1 2022

- Lanzamiento de la red de prueba de la plataforma Jot NFT
- Lanzamiento de cadena cruzada billetera - Thanos Wallet
- Expansión del equipo

T2 2022

- Mainnet del mercado de Jot Art NFT en vivo.
- Implementar DNN en LithoSwap
- Equipo central de la litosfera aumento.
- Establecer Litho red de prueba
- Venta pública de tokens / IEO.

Tercer trimestre de 2022

- Implementar DNN en Cartera Thanos.
- Venta Privada de JOT Token
- Iniciar el desarrollo de Plataforma de conciertos descentralizada impulsada por la comunidad en Blockchain - Fleek
- Lanzamiento del SDK de Jot Art
- Lanzar Litho Launchpad
- Liberar blockchain juego móvil en la plataforma JOT NFT
- LAX - Moneda estable algorítmica

Conclusión

El proyecto Lithosphere ha creado un algoritmo BFT, un nuevo estándar de token, moneda Litho (LITHO) y un mecanismo de distribución de claves para lograr el objetivo de la plataforma descentralizada inclusiva. El diseño del token nativo se compone principalmente de los siguientes cinco elementos:

1.Número. Hay un total de mil millones de tokens disponibles. Esta cantidad permitirá que el token se lance a un precio aceptable y continúe creciendo de manera constante desde allí.

2.Un sistema para distribuir tokens. Para lograr la idea de no inflación, el suministro de tokens debe ser limitado. Esto beneficia a los primeros miembros y hace que el sistema sea más estable a largo plazo.

3.La asignación de tokens. Para realizar la noción descentralizada, la distribución de tokens debe estar correctamente equilibrada. Otorgamos una proporción del 10% al equipo de Lithosphere debido a su dedicación y esfuerzos continuos para promover la inclusión de Lithosphere en iniciativas de cadenas cruzadas, organizaciones cruzadas y fuentes de datos cruzadas. Además, debido a que los nodos de contabilidad de Lithosphere realizan funciones más complejas que las cadenas públicas ordinarias, obtendrán alrededor de un tercio de la suma total. El resto se utilizará para edificios ecológicos.

4.Construcción ecológica. Más de la mitad de los fondos se destinarán a la Fundación para ayudar a que el proyecto prospere, especialmente en términos de características de cadena cruzada, organización cruzada y datos cruzados. Para permitir que se transmita valor adicional en la cadena y ayudar al desarrollo de nuevas aplicaciones de contratos inteligentes, el proyecto también requerirá un mecanismo de intercambio de tokens.

5.Combustibles y mineros En un sistema de control de nodo distribuido, un rango de valores ingresará a la litosfera. Para controlar los tokens, la cadena requiere una gran cantidad de nodos dispersos. Cuantos más nodos haya, más segura será la cadena y se necesitarán más nodos a medida que aumenta el valor de la cadena. La cadena debe compensar a los mineros liberando tokens y cobrando tarifas de servicio para mantener la cantidad de nodos y el poder de cálculo.

La litosfera nació por necesidad. Nuestros equipos de desarrollo siempre se han distribuido por todo el mundo desde el comienzo de KaJ Labs, pero siempre hemos tenido problemas para trabajar de forma eficaz. Tenemos que mejorar todo nuestro rendimiento y procesos para que nuestros equipos se mantengan distribuidos.

Reconocimos que había varias ineficiencias con las cadenas de bloques que se utilizan comúnmente como Ethereum, Cardano y otras después de trabajar en numerosos proyectos de cadenas de bloques. El problema más grave fue que estas redes blockchain no pudieron conectarse. No podía comprar ERC721 NFT usando un token BEP20, BTC, DOT o BNB hasta Lithosphere. Las redes blockchain deben estar sincronizadas entre sí para que blockchain y DeFi crezcan en el futuro que todos queremos. Los gastos de transacción / tarifas de gas son otros desafíos que enfrentan redes como Ethereum. En la red Ethereum, casi todas las actividades cuestan dinero. El equipo de KaJ Labs se propuso crear una red mundial de cadenas de bloques que sea más rápida, más barata y más respetuosa con el medio ambiente que las cadenas de bloques existentes como Cardano, Polkadot y Ethereum 2.0. La litosfera puede considerarse la base de las cadenas de bloques nuevas y antiguas. El ecosistema de la litosfera funciona con la moneda nativa $ LITHO / Litho.

Descargo de responsabilidad

Este Whitepaper de Lithosphere es solo para fines informativos. La Fundación KaJ Labs no garantiza la precisión o las conclusiones alcanzadas en este documento técnico, y este documento técnico se proporciona "tal cual". KaJ Labs Foundation no hace y renuncia expresamente a todas las representaciones y garantías, expresas, ya sean explícitas, implícitas, legales o de otro tipo, lo que incluye, entre otros: (i) que el contenido de este documento técnico está libre de errores; (ii) que dichos contenidos no infringirán derechos de terceros; y (iii) garantías de idoneidad para un propósito, idoneidad o función en particular. KaJ Labs Foundation y sus afiliadas no serán responsables por daños de ningún tipo que surjan del uso, referencia o dependencia de este documento técnico o de cualquiera de sus contenidos. incluso si se le advierte de la posibilidad de tales daños. En ningún caso KaJ Labs Foundation o sus afiliadas serán responsables ante cualquier persona o entidad por daños, pérdidas, responsabilidades, costos o gastos de cualquier tipo, ya sean directos o indirectos, consecuentes, compensatorios, incidentales, reales, ejemplares, punitivos o especial para el uso, la referencia o la confianza en este documento técnico o en cualquier contenido aquí incluido, incluyendo, sin limitación, cualquier pérdida de negocios, ingresos, ganancias, datos, uso, buena voluntad u otras pérdidas intangibles.

Glosario

LEP100: Propuesta de evolución de la litosfera

PAPEL BLANCO: Una guía sobre un tema específico y la problemática que lo rodea. Está destinado a educar a los lectores y ayudarlos a comprender y resolver un problema.

CADENA DE BLOQUES: Una lista cada vez mayor de registros, llamados bloques, que están vinculados entre sí mediante criptografía.

SIMBÓLICO: Un token representa un conjunto de reglas codificadas en un conjunto de contratos inteligentes. Cada token pertenece a una dirección de blockchain. Es esencialmente un activo digital que se almacena de forma segura en la cadena de bloques.

DESCENTRALIZADO: Tipo de intercambio de criptomonedas que permite que el intercambio directo de criptomonedas entre pares se lleve a cabo en línea de forma segura y sin la necesidad de un intermediario.

EVM: La máquina virtual Ethereum es un motor de cálculo que actúa como una computadora descentralizada que tiene millones de proyectos ejecutables.

BSC: Cadena inteligente Binance

MONEDAS PEGADAS: Tokens LEP100 vinculados a activos externos.

DAPPS: Las aplicaciones descentralizadas son aplicaciones digitales que se ejecutan en una cadena de bloques o una red de computadoras de igual a igual en lugar de una sola computadora.

NFT: Un token no fungible es una unidad de datos almacenada en un libro de contabilidad digital, llamado blockchain, que certifica un activo digital y, por lo tanto, no es intercambiable.

INTEROPERABILIDAD: La capacidad de los sistemas informáticos o software para intercambiar y hacer uso de información.

ERC: Solicitud de comentarios de Ethereum

QUEMAR: Un proceso mediante el cual los mineros y desarrolladores de moneda digital pueden retirar tokens o monedas de la circulación.

TRACCIÓN: Tasa de extracción o extracción en una empresa.

DEFI: Finanzas descentralizadas

CADENA EN CRUZ: Es la interoperabilidad entre dos cadenas de bloques relativamente independientes.

DEX: Intercambio descentralizado