Libro Blanco de

ZEROLIMIT

Abra un modelo de aplicación móvil descentralizado
confiable, de bajo costo y eficiente

2019-5-28

Equipo de desarrollo básico de ZEROLIMIT

Catalogar

1 Breve introducción a la tecnología blockchain

Blockchain es una combinación orgánica de una serie de tecnologías maduras que distribuyen registros efectivos de cuentas y proporcionan scripts perfectos para soportar diferentes lógicas de negocios. En un sistema típico de Blockchain, los datos se generan y almacenan en bloques, y se vinculan en una estructura de datos en cadena en orden cronológico. Todos los nodos participan en la validación de datos, el almacenamiento y el mantenimiento del sistema Blockchain. La creación de nuevos bloques generalmente debe ser confirmada por la mayoría de los nodos (el número depende de diferentes mecanismos de consenso) y difundirse a cada nodo para lograr la sincronización de la red, que no se puede cambiar o eliminar después de eso. La tecnología Blockchain es un nuevo modo de aplicación de tecnología informática, que integra el almacenamiento distribuido, la transmisión punto a punto, el mecanismo de consenso y la criptografía. Como la tecnología básica de Bitcoin, la tecnología Blockchain ha sido reconocida como una tecnología revolucionaria para subvertir Internet desde su nacimiento, e incluso se espera una nueva revolución industrial. Sin embargo, después de casi diez años de desarrollo, lamentamos ver que la tecnología de la cadena de bloques solo refleja sus atributos financieros y no puede servir a la economía real. La razón es que aunque el pensamiento de Blockchain expresa sus perspectivas de aplicación sólidas y amplias, incluso la cadena pública global representativa no ha expresado realmente el pensamiento de Blockchain en la realización de la tecnología, y todavía hay muchos puntos dolorosos que restringen la aplicación de la tecnología Blockchain a la tierra:

(1) Todo tipo de algoritmos de consenso en la tecnología Blockchain son para determinar que los mineros individuales o los mineros disfrazados obtendrán el derecho de rendir cuentas. La existencia de los mineros agravará la inequidad o desperdiciará gran cantidad de energía, lo que eventualmente llevará a una tendencia cada vez más seria de centralización, pero pondrá en peligro la seguridad de la puesta en marcha de Blockchain y Blockchain. La intención original del corazón es contraria a la intención original.

(2) La cantidad de transacciones que se pueden procesar por unidad de tiempo (TPS) es limitada e insuficiente para soportar escenarios de uso concurrente alto en todo el mundo. A medida que aumenta el número de usuarios, inevitablemente se producirá congestión.

(3) La cantidad de transacciones que se pueden utilizar para la unidad de tiempo (TPS) es limitada e insuficiente. A medida que aumenta el número de usuarios, inevitablemente se producirá congestión.

(4) La creciente capacidad de los nodos requiere cada vez más nodos Blockchain. Con el paso del tiempo, cada vez menos nodos pueden mantener la seguridad de Blockchain, y la aplicación basada en Blockchain estará

sobrecargada. Bajo las condiciones actuales de la tecnología Blockchain, solo la participación de todos los nodos de Blockchain puede hacer una contribución efectiva a la seguridad de Blockchain. Para la cadena de bloques de Bitcoin de crecimiento más lento, el requisito de almacenamiento aumenta a una velocidad de 6 MB por hora y el crecimiento anual es de más de 50 GB. Si la red de Bitcoin quiere alcanzar el volumen de transacciones de 2000 TPS que procesan el nivel VISA, el incremento de almacenamiento anual superará los 8TB. Tal escenario de aplicación puede ser posible. Como resultado, solo un pequeño número de empresas y entusiastas de alto nivel ejecutarán todo el nodo, lo que conlleva el riesgo de la centralización de Blockchain.

(5) Los altos costos de transacción exacerban el aumento de los costos de aplicación.

(6) El rápido desarrollo de la tecnología informática cuántica plantea una gran amenaza y un desafío para la criptografía. Una vez que aparezcan las computadoras cuánticas prácticas, los Cryptosystems de clave pública basados en logaritmo discreto y la descomposición de enteros (incluyendo RSA / ECC / DH) se desglosarán rápidamente, lo que amenaza directamente la seguridad del ecosistema de Blockchain existente.

ZEROLIMIT, como explorador de la nueva generación de tecnología Blockchain, desarrolla el concepto de TXCHAIN móvil orientado a los puntos críticos y los cuellos de botella de las aplicaciones de la tecnología Blockchain actual. Surge para eliminar el umbral de aplicación de Blockchain y popularizar el aterrizaje práctico de Blockchain.

2 Resumen de ZEROLIMIT

ZEROLIMIT es un nuevo modo de aplicación de tecnología informática, como el almacenamiento distribuido, la transmisión de velocidad extrema punto a punto, el consenso de código, la criptografía de computación anti-cuántica, etc. Es una red de aplicación completamente descentralizada basada en nodos de dispositivos móviles para cumplir con el Requisitos de almacenamiento bajo y transacciones de alta frecuencia. El concepto TXCHAIN móvil de ZEROLIMIT es alojar nodos TXCHAIN en dispositivos móviles, como teléfonos inteligentes y tabletas, que pueden ejecutar nodos TXCHAIN. Mobile TXCHAIN realmente encarna las características de la descentralización. Cada nodo adicional agrega un chip a la seguridad de toda la cadena. Cuantos más nodos estén involucrados, más rápida será la velocidad de confirmación de la transacción y más fuerte será la capacidad de rendimiento del sistema. La figura 1 muestra la arquitectura del sistema ZEROLIMIT.

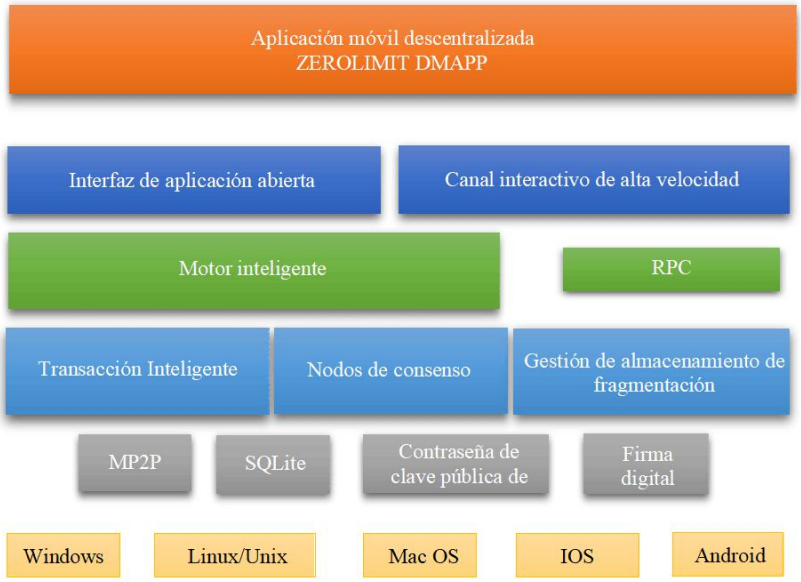

Figura 1 Marco ZEROLIMIT

La aplicación principal de ZEROLIMIT se carga directamente en el motor inteligente a través de la interfaz de aplicación abierta y el canal interactivo de alta velocidad, por lo que la aplicación ZEROLIMIT se integra perfectamente con la red ZEROLIMIT. El cliente de ZEROLIMIT también es el cliente del programa de aplicación ZEROLIMIT. ZEROLIMIT se esfuerza por proporcionar una plataforma sin umbral para los desarrolladores y usuarios de aplicaciones.

Las aplicaciones ZEROLIMIT y ZEROLIMIT son multiplataforma y pueden ejecutarse en una variedad de dispositivos de nodo, compatibles con los sistemas operativos Windows, Linux, Unix, MacOS, IOS y Android. Los nodos que participan en ZEROLIMIT no son necesariamente adecuados para ejecutarse en terminales móviles, como los de grandes empresas, que a menudo tienen direcciones fijas. El número de transacciones generadas por sus propios nodos puede ser enorme.

Mobile TXCHAIN hace que la implementación de aplicaciones basada en TXCHAIN sea simple. Cada nodo móvil es tanto un servidor como un cliente. El costo de la aplicación basada en TXCHAIN móvil se reducirá en gran medida, ya que no hay necesidad de soporte de servidor back-end, todas las aplicaciones están verdaderamente descentralizadas.

ZEROLIMIT garantiza la ligereza de los nodos desde el diseño del protocolo subyacente para cumplir con los requisitos de despliegue de los nodos móviles de consenso en toda la red. ZEROLIMIT adopta el método de código consenso. Todos los nodos

participantes tienen la misma capacidad de consenso. Tienen igual estatus y ninguna relación de competencia. No pueden formar una ventaja centralizada. Por lo tanto, es imposible formar un nuevo centro. Debido a que todos los nodos participantes tienen la capacidad de tratar transacciones, cada nodo adicional en toda la red aumentará la capacidad de procesamiento. Cuantos más nodos participen, más rápida será la velocidad de procesamiento general de toda la red, y no habrá límite en la capacidad de procesamiento.

Ligero, la capacidad de procesamiento ilimitada y la descentralización completa sin servidor hacen que ZEROLIMIT brinde un entorno de red de alta eficiencia y bajo costo para aplicaciones ilimitadas en todo el mundo, y crea un modo de aplicación de red de igual a igual totalmente descentralizado Los modos de aplicación C / S y B / S en la era de Internet.

En una palabra, ZEROLIMIT está a punto de abrir un modo de aplicación móvil descentralizado confiable, de bajo costo y eficiente. Con el aumento infinito de nodos participantes en la red de polo cero, ZEROLIMIT logrará espacio de almacenamiento distribuido ilimitado, velocidad de procesamiento de transacciones ilimitada, seguridad de datos ilimitada y aplicaciones de carga ilimitada. Cero representa el origen y la fundamentalidad en la filosofía. La red ZEROLIMIT se da cuenta de la idea básica de Blockchain desde un punto de vista técnico único, resuelve todos los puntos débiles de la tecnología Blockchain tradicional y representa el comienzo de la era de la aplicación de la tecnología Blockchain.

3. Red de igual a igual (MP2P) basada en nodos móviles

La red Peer-to-Peer (P2P) es la base de la idea descentralizada de Blockchain. Al mismo tiempo, tiene las características de escalabilidad, robustez, rendimiento de alto costo, protección de privacidad, balanceo de carga, etc. En las redes P2P anteriores a Blockchain 2.0, los nodos participantes suelen ser nodos de PC o servidor con direcciones IP estables, mientras que la red P2P de ZEROLIMIT Los nodos son generalmente nodos de dispositivos móviles. Las direcciones IP de los nodos generalmente no son fijas, y pueden interrumpir o cambiar las redes IP en cualquier momento, lo que plantea mayores requisitos para la capacidad de procesamiento de red de ZEROLIMIT.

La red Peer-to-Peer, que constituye ZEROLIMIT, es una red MP2P compuesta por nodos ZEROLIMIT, cada uno de los cuales es un cliente y un servidor. No es solo el

proveedor de información sino también el solicitante de información. Como nodo de servicio, puede estar conectado con múltiples nodos de clientes para proporcionar servicios de información. Como nodo de cliente, también puede estar conectado con múltiples nodos de servicio para solicitarles información de servicio. Estos nodos pueden unirse o salir de la red ZEROLIMIT en cualquier momento.

La red ZEROLIMIT adopta una red dinámica estructurada (Kademila), cada nodo necesita mantener la tabla de enrutamiento local, y completar la construcción y el mantenimiento de la tabla de enrutamiento, la búsqueda de nodos, la transmisión de datos y la recepción de datos. El algoritmo de difusión del nodo basado en la tabla de enrutamiento en ZEROLIMIT La red MP2P proporciona un soporte efectivo para el almacenamiento distribuido de información de transacciones de nodos y evita la tormenta de difusión de la red.

En las redes móviles, no todos los tipos de nodos pueden establecer una comunicación punto a punto a través de la penetración. En este momento, el reenvío de datos debe completarse a través de nodos intermedios. En las redes ZEROLIMIT, los nodos que completan el reenvío de datos se denominan "estaciones base de datos". Los nodos NAT de cono completo en la red IPV4 y los nodos IP de red pública fija, así como los nodos en la red IPV6, pueden asumir las funciones de la estación base de datos. El software de nodo de la red ZEROLIMIT puede detectar si el nodo mismo puede actuar como una estación de base de datos y proporcionar opciones de participación. La red ZEROLIMIT alienta a los nodos capaces a participar en el plan de la estación de base de datos y ofrece los incentivos correspondientes.

4 Desbloquear móvil TXCHAIN

ZEROLIMIT encarna la idea real de Blockchain, pero no es el Blockchain tradicional en la implementación técnica. Debido a que ZEROLIMIT no tiene el concepto de bloque, solo el concepto de unidad de transacción. Todas las transacciones enviadas por nodos constituyen lógicamente un conjunto de múltiples gráficos acíclicos dirigidos MDAG. Aquí llamamos al conjunto de MDAG compuesto de transacciones TXCHAIN. Como se muestra en la Figura 1 (en el que el tiempo se mueve de izquierda a derecha), los bordes de este gráfico se forman de la siguiente manera: cuando llega una nueva transacción, debe verificar las dos transacciones anteriores, y estas relaciones de validación están representadas por bordes dirigidos, con la

flecha apuntando al verificador. Si solo hay una ruta de borde dirigida entre la transacción B y la transacción A, decimos que la transacción B verifica directamente la transacción A. Si hay al menos dos rutas de borde dirigidas entre la transacción B y la transacción A, decimos que la transacción B verifica indirectamente la transacción A .

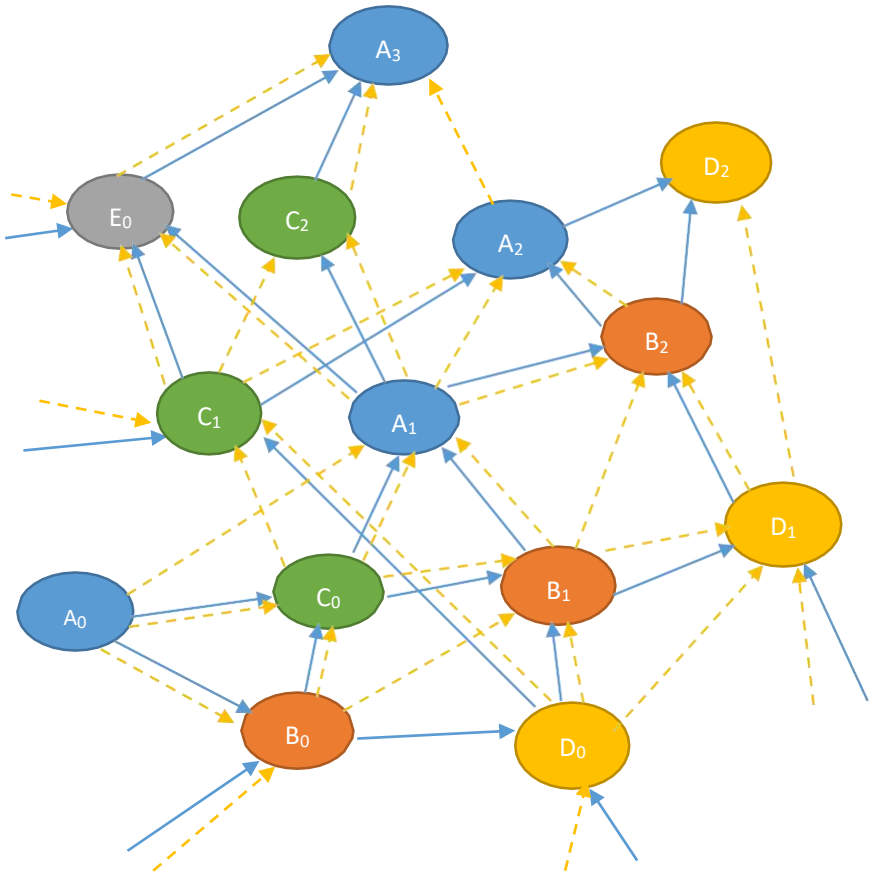

Figura 1 -TXCHAIN Diagrama Lógico

En el esquema TXCHAIN anterior, asumimos que A, B, C, D y E son direcciones de cinco nodos, y que sus subíndices representan el número secuencial de transacciones emitidas por esa dirección. Las flechas sólidas en la figura representan la relación de validación. Por ejemplo, la transacción A1 valida directamente la transacción C0 e indirectamente la transacción B0. La flecha discontinua representa tanto la relación de conexión (que implica la relación temporal) como la relación de almacenamiento. Las transacciones emitidas por cada dirección de nodo constituyen el orden TXCHAIN del propio nodo, y la validación TXCHAIN está formada por la relación de validación entre TXCHAIN de diferentes nodos.

Llamamos a la dirección de origen la transacción de la propia dirección del nodo como la

transacción de salida del nodo, y la dirección de destino la transacción de la propia dirección del nodo como la transacción de entrada del nodo. Los nodos deben guardar todas las transacciones de salida y entrada relacionadas con sus direcciones, así como las transacciones reales de otros nodos que se validan directamente. Cuando se genera una transacción y se difunde a toda la red a través de la tabla de enrutamiento de nodos, no todos los nodos confirmarán la transacción. Solo cuando la transacción se verifique y cumpla con la condición de nodo de distribución distribuida de la transacción, la transacción se almacenará, es decir, se completará el proceso de confirmación. Las transacciones ilegales serán abandonadas por los nodos y no serán transmitidas, mientras que las transacciones legítimas serán confirmadas y aceptadas instantáneamente por la red.

Hay dos motivaciones para la verificación de transacciones, una es la verificación pasiva, es decir, el trabajo de verificación debe realizarse antes de emitir nuevas transacciones; la otra es la verificación activa, que está basada en los beneficios, pero este trabajo de verificación no puede ser recompensado de inmediato. Debido a que algunos nodos tienen suficiente espacio de almacenamiento para acomodar más transacciones, están dispuestos a contribuir a la seguridad de la red. De esta manera, siempre que la transacción se valide, la transacción relacionada con el TXCHAIN validado se puede almacenar. Cuando el nodo asociado con la transacción almacenada necesita volver a descargar la transacción, el nodo guardado de la transacción puede obtener la recompensa correspondiente. Otro tipo de transacción de transferencia sin activos es el despliegue de la aplicación ZEROLIMIT en todo TXCHAIN. Una aplicación se divide en varias transacciones, que se verifican mediante nodos de verificación activos o pasivos para lograr un almacenamiento distribuido. Cuando el nodo móvil descarga estas transacciones para acceder a la aplicación, el editor de la aplicación pagará una tarifa determinada por los nodos descargados. Por supuesto, cuando la misma cuenta de nodo descarga los mismos recursos de la aplicación muchas veces, el editor solo paga por la primera descarga.

5 Intelligent Transaction

En el protocolo tradicional de Blockchain, la interpretación de las transacciones se realiza a través de un intérprete de script basado en la pila. Bitcoin se basa en un sistema de secuencias de comandos limitado, extendido por ETF para ejecutar secuencias de comandos a través de máquinas virtuales. Tanto el sistema de secuencias de comandos limitado de Bitcoin como el sistema completo de secuencias de comandos de ETF, Turing, se ejecutan según la interpretación de la secuencia de comandos, y su eficiencia se descuenta en términos de velocidad de procesamiento de

transacciones. ZEROLIMIT se basa en dispositivos móviles y los recursos informáticos son limitados. Es necesario garantizar la capacidad de procesamiento de transacciones lo suficientemente rápido en el protocolo. Así que abandonamos el sistema de scripting e introdujimos el concepto de comercio inteligente en el diseño ZEROLIMIT.

La llamada transacción inteligente se refiere a la introducción de características programables en la estructura de datos de la transacción y al procesamiento de transacciones mediante la ejecución de códigos programables. El área de código programable admite el estándar ECMA6 JavaScript para escribir el código de la aplicación. Puede activar el código enviando mensajes a la transacción inteligente o ejecutar el código cuando el nodo confirma la transacción. El código de transacción inteligente es ejecutado por el motor inteligente ZEROLIMIT. El motor inteligente contiene el motor V8 de Google. Usando la tecnología JIT, el código JavaScript puede compilarse en el código de máquina de la plataforma de ejecución objetivo para mejorar la eficiencia de ejecución del código.

El código de transacción inteligente extiende la función de transacción y mejora la flexibilidad del procesamiento de la transacción.

La publicación de transacciones en la plataforma ZEROLIMIT está libre de tarifas de transacción, lo que es especialmente adecuado para escenarios de aplicaciones de micropago.

6 Código de Consenso CODEC

El consenso de blockchain se logra a través de un mecanismo muy riguroso. Agregar el siguiente bloque a Blockchain requiere la competencia de varias partes y el acceso a bloqueos o tarifas de transacción. Debido a esto, el consenso y la generación de transacciones son separados y realizados por una pequeña parte de la red, generalmente con un umbral más alto (como Bitcoin), lo que lleva a una mayor centralización.

En la red ZEROLIMIT, todos los derechos e intereses (activos) se crean solo una vez en la transacción de creación, y todas las transacciones subsiguientes solo existen en la transferencia de activos de capital, y no se volverán a crear. Por lo tanto, no es necesario determinar el derecho de cuenta por minería. Necesitamos deshacernos de la mentalidad tradicional de Blockchain para entender esto. En la implementación de la tecnología tradicional Blockchain, todos los nodos tienen la misma réplica de datos. No es necesario diseñar un mecanismo de consenso especial para juzgar la validez de los datos. La réplica de datos en sí es un consenso. La función del mecanismo de

consenso es determinar el derecho a la cuenta, porque en un nodo de ciclo de tiempo, solo el único nodo puede implementar el comportamiento de la contabilidad, que también es la raíz de la ineficiencia de la tecnología tradicional de Blockchain.

ZEROLIMIT no tiene cuentas en cadena. Todas las transacciones forman un gráfico acíclico dirigido lógicamente múltiple a través de relaciones de conexión, almacenamiento y verificación. Una vez que se valida una transacción, será almacenada por el nodo de validación, es decir, confirmada por el nodo de validación. Las transacciones se transmiten a toda la red a través de tablas de enrutamiento de nodos, y los nodos las verifican y almacenan en rutas específicas de acuerdo con el algoritmo de distribución de almacenamiento distribuido. Es decir, todos los nodos en la red ZEROLIMIT tienen derechos de contabilidad iguales. El propósito del mecanismo de consenso ya no es determinar los derechos contables, sino verificar y confirmar transacciones.

Las características ligeras de los nodos ZEROLIMIT hacen que sea imposible juzgar la validez de las transacciones mediante el rastreo de los datos completos de los nodos verificados. Es para lograr el consenso de todos los nodos en la red, como la unión de nodos, la generación de transacciones, las firmas digitales, la verificación de transacciones, etc. Todos los nodos ejecutarán el mismo código de consenso en el entorno de consenso. Las consecuencias de abandonar el entorno de consenso o cambiar el código de consenso se descartan mediante nodos honestos.

ZEROLIMIT aboga por el espíritu del código abierto, pero tiene sus propios principios de licencia únicos. Todo el código fuente de ZEROLIMIT es solo para fines de investigación y aprendizaje, y no se puede difundir, modificar ni revender para otros fines personales o comerciales. Cuando el código ZEROLIMIT se mejora y se vuelve a agregar al ecosistema ZEROLIMIT, se debe obtener la firma digital oficial de ZEROLIMIT. Es decir, cuando un nodo se une a la red ZEROLIMIT, el código de consenso verificará la validez del nodo y los nodos ilegales se eliminarán.

En la implementación de la tecnología tradicional Blockchain, el proceso de generación y verificación de transacciones se separa del proceso de consenso. ZEROLIMIT ha cambiado este proceso. Integra la generación de transacciones, la firma digital, el almacenamiento distribuido y la validación en el proceso de consenso, y ejecuta el mismo código de consenso en todos los nodos de la red para lograr resultados no autorizados, inolvidables e innegables de los datos de transacción. Los nodos de ZEROLIMIT son ligeros. En comparación con toda la cuenta de la red, un solo nodo solo mantiene una cantidad muy pequeña de datos de transacción. El nodo local no solo guarda las transacciones de entrada y salida completas de su propia cuenta, sino que también guarda el árbol de estados de información de la característica de la transacción con una cuenta conjunta. Los "nodos

relacionados" aquí se refieren a estos tipos de nodos, uno es el nodo correspondiente a la dirección de destino en la transacción de salida, el otro es el nodo de envío de la transacción confirmada y el tercero es el nodo correspondiente al editor del DMAPP utilizado por el nodo. El árbol de estado de información característica es un tipo de información simplificada. Determina las transacciones almacenadas de acuerdo con el algoritmo de distribución de transacciones distribuidas. Constituye un punto de control clave en el árbol de estado de información de características, y todas las transacciones consecutivas que solo verifiquen y no se almacenen entre los puntos de control se comprimirán como puntos de control de características. Este método verifica la validez, validez y corrección de las transacciones del nodo a través del árbol de estados de información característica del nodo, que se denomina mecanismo de "Prueba de consistencia" en ZEROLIMIT. El mecanismo de PoC resuelve la contradicción entre el almacenamiento ligero y la seguridad de datos, de modo que todos los nodos participantes puedan participar en el proceso de consenso.

El código es la regla, solo todos los nodos siguen la misma regla, es el mejor consenso. El código de consenso garantiza un alto rendimiento y seguridad de ZEROLIMIT. Debido a que cada nodo participante tiene la capacidad de tratar transacciones, es decir, tiene la capacidad de consenso, por lo que cada nodo adicional, toda la red aumentará la capacidad de procesamiento. Cuantos más nodos se involucren, más rápido se procesarán las transacciones, de modo que nunca habrá congestión. En otras palabras, ZEROLIMIT puede soportar la creciente demanda global de aplicaciones.

7 Fragmentacion endogena

El mecanismo de consenso de membresía de ZEROLIMIT y el mecanismo de distribución de almacenamiento distribuido son en realidad el mecanismo de procesamiento de fragmentación a lo largo de una ruta específica en toda la red. Cada nodo en toda la red puede publicar transacciones al mismo tiempo, y distribuirlas a través de la tabla de enrutamiento de nodos y ser confirmado por otros nodos. Este proceso de consenso es concurrente, no solo garantiza las características de los nodos de luz ZEROLIMIT del protocolo, sino que también no tiene un límite superior en la velocidad de procesamiento y realmente logra la deducción perfecta del tiempo y el espacio.

El consenso del código y el mecanismo de procesamiento por partes hacen que ZEROLIMIT sea muy adecuado para la implementación en sistemas con recursos limitados, como dispositivos móviles. La capacidad de procesamiento de procesamiento de transacciones superalta es suficiente para satisfacer todas las aplicaciones en la vida real.

8 Seguridad computacional cuántica

La criptografía resistente cuántica (QRC) se refiere esencialmente a "una contraseña matemática que puede resistir los ataques informáticos cuánticos". En la actualidad, hay principalmente el algoritmo Grover y el algoritmo Shor que se pueden usar en el cálculo cuántico para la decodificación criptográfica. Para la decodificación criptográfica, el algoritmo Grover puede reducir a la mitad la longitud de la clave secreta. El algoritmo de Shor puede atacar el protocolo de acuerdo de clave secreta DH y RSA, DSA, ECC y el protocolo de clave secreta DH que se utilizan ampliamente en la actualidad Esto muestra que en el entorno de computación cuántica, el algoritmo criptográfico utilizado por la cadena de bloques tradicional ya no será seguro.

Hay muchos sistemas criptográficos que pueden resistir ataques informáticos cuánticos, como la criptografía basada en HASH, la criptografía basada en código de corrección de errores, la criptografía basada en celosía, la criptografía de sistema cuadrático multivariable, etc. Sin embargo, estos sistemas criptográficos no son adecuados para aplicaciones Blockchain, especialmente Blockchain móvil basado en nodos de dispositivos móviles, debido a la larga longitud de la clave secreta y la información de la firma, y al largo tiempo de operación.

ZEROLIMIT adopta un esquema de firma única SHA3 de 512 bits mejorada, que resuelve los problemas de la clave secreta y la información de firma demasiado largas y la velocidad de cálculo demasiado lenta, y es especialmente adecuada para el despliegue de nodos móviles. La Oficina de Propiedad Intelectual del Estado ha examinado y aprobado dos patentes del esquema de firma digital contra ataques informáticos cuánticos.

9 Motor inteligente

La máquina virtual provista en la implementación de la tecnología tradicional Blockchain traducirá el lenguaje de scripting en un código de bytes que la máquina virtual puede entender, y luego interpretará y ejecutará estos códigos de bytes por la máquina virtual. Sin lugar a dudas, el modo de interpretación del código byte reducirá en gran medida la eficiencia de ejecución. No es adecuado que los dispositivos móviles actúen como nodos Blockchain bajo la carga de un alto rendimiento de transacciones.

ZEROLIMIT no proporciona una máquina virtual en sentido general, sino un motor inteligente de muy alto rendimiento (zolEngine). No solo puede ejecutar el código JS en

transacciones inteligentes, sino que también zolEngine es el mecanismo de ejecución de DMAPP. Puede lograr diferentes transferencias de DMAPP mediante la carga y descarga dinámica de DMAPP.

La transacción inteligente y el código de implementación del programa de aplicación ZEROLIMIT (DMAPP) son el lenguaje completo general de alto nivel de Turing, que actualmente admite javascript. El zolEngine puede compilar el código en un código de máquina compatible con el procesador host y ejecutarlo en todas las plataformas. Es compatible con Win32 / Win64, Linux, Android, Mac OS, simulador de iOS y dispositivos iOS.

10 Interfaz de aplicación abierta

El canal interactivo de alta velocidad del motor inteligente convierte a ZEROLIMIT en una plataforma de aplicaciones completamente abierta. ZEROLIMIT no solo proporciona aplicaciones de terceros con acceso directo a la API de ZEROLIMIT, lo que permite que las aplicaciones de terceros integren las aplicaciones Blockchain de forma rápida y sencilla; y ZEROLIMIT proporciona una interfaz API subyacente común para todos los tipos de DMAPP.

10.1 Canal interactivo de alta velocidad Speed (HSIC）

El canal interactivo de alta velocidad (hsic) es un mecanismo que permite que la aplicación ZEROLIMIT (DMAPP) y la capa inferior de ZEROLIMIT se puedan referenciar. La capa inferior de ZEROLIMIT puede intercambiar mensajes y datos con DMAPP a través de (HSIC) y puede iniciar llamadas de función directamente. La lógica de "cliente" de DMAPP y la lógica de "servidor" también pueden interactuar a través de (HSIC). La capa inferior de ZEROLIMIT y la aplicación ZEROLIMIT (DMAPP) están interrelacionadas e independientes entre sí. La red ZEROLIMIT proporciona una gama completa de Interfaz de aplicación abierta e interfaz de datos para la aplicación ZEROLIMIT a través del Canal interactivo de alta velocidad. Al mismo tiempo, el acceso a las funciones y datos de la aplicación ZEROLIMIT se proporciona en forma predefinida. En otras palabras, este canal interactivo de alta velocidad es un canal de dos vías a través del cual las aplicaciones se pueden integrar sin problemas con las redes ZEROLIMIT.

10.2 Interfaz gráfica de usuario

El programa de aplicación ZEROLIMIT (DMAPP) es una aplicación móvil descentralizada que se ejecuta completamente en el motor inteligente ZEROLIMIT. Puede implementarse mediante lenguajes

de alto nivel como JavaScript y C ++. Para unificar la interfaz de usuario, la interfaz del programa de aplicación ZEROLIMIT y el software de nodo ZEROLIMIT están integrados. El software de nodo ZEROLIMIT y DMAPP que se ejecutan en ZEROLIMIT utilizan el lenguaje de descripción de la interfaz para realizar la interfaz gráfica de usuario e implementan el lenguaje de descripción de la interfaz a través del motor inteligente ZEROLIMIT.

10.3 SDK dinámico distribuido

El objetivo de ZEROLIMIT es proporcionar el soporte más bajo para la aplicación en cadena de toda la industria. Con la popularización de la aplicación, el SDK que soporta el desarrollo de DMAPP se volverá muy voluminoso, lo que es inconsistente con el requisito de las características de los nodos de peso ligero de ZEROLIMIT. Por esta razón, diseñamos el mecanismo de SDK dinámico distribuido. En primer lugar, se distribuye el despliegue de SDK en la cadena. En segundo lugar, el desarrollo y la invocación de SDK son dinámicos. El SDK está diseñado como parte del software de nodo, pero se puede conectar dinámicamente. El SDK se compila en las instrucciones de la máquina del entorno operativo del host, que puede ejecutarse rápidamente y garantizar la eficiencia de DMAPP. En cierto sentido, DMAPP puede entenderse como el "front end" y el SDK puede entenderse como el "back end". El SDK de la cadena se descarga a pedido con DMAPP o se puede desinstalar con DMAPP.

11 Aplicación ZEROLIMIT (DMAPP)

La aplicación ZEROLIMIT (DMAPP) puede lograr cualquier función que desee. El motor inteligente y el lenguaje completo de alto nivel de Turing proporcionan un grado completo de libertad, permitiendo a los usuarios crear una variedad de aplicaciones, incluso aplicaciones móviles con interfaz gráfica de usuario.

Crear una aplicación ZEROLIMIT, o un proyecto de aplicación, es publicar una o más transacciones inteligentes con código ejecutable. Cada nodo ZEROLIMIT tiene solo una cuenta y una dirección, pero puede crear múltiples aplicaciones. Cada aplicación corresponde a la dirección inherente de la cuenta del nodo. Enviar un mensaje con el número de índice de la aplicación a esta dirección puede descargar la transacción relacionada con la aplicación desde la red ZEROLIMIT y restaurarla a DMAPP localmente, que está integrada con el software de nodo local ZEROLIMIT. Cada DMAPP es una aplicación descentralizada, porque El código de esta aplicación se divide en

diferentes partes y se almacena en múltiples transacciones inteligentes, una vez que estas transacciones inteligentes son verificadas por otros nodos. Estos nodos de validación se guardan, por lo que la aplicación se distribuye en ZEROLIMIT, e incluso si el nodo del editor de la aplicación está fuera de línea, no impide que se acceda a la aplicación.

La publicación de aplicaciones en redes ZEROLIMIT requiere pago, que se paga en parte por los validadores de transacciones y en parte se recompensa a los nodos que proporcionan descargas de aplicaciones.

Todas las aplicaciones se integran automáticamente en el cliente de nodo, porque el propio cliente de nodo es una aplicación, y la aplicación ZEROLIMIT está integrada en esta aplicación, por lo que parece que el cliente de nodo de ZEROLIMIT es una aplicación basada en la aplicación.

(1) Entorno de desarrollo DMAPP

ZEROLIMIT proporciona un entorno de desarrollo programable (IDE) para transacciones inteligentes integradas a nivel de escritorio, un editor de código resaltado en sintaxis visual, un depurador de seguimiento de un solo paso, ejecuciones de simulación y herramientas de implementación. El entorno de desarrollo es una herramienta de escritorio proporcionada por ZEROLIMIT. No es parte del software de nodo ZEROLIMIT. Contiene todas las funciones del software de nodo ZEROLIMIT y ejecuta la simulación de la aplicación en la cadena de prueba de ZEROLIMIT.

El entorno de desarrollo también admite el resaltado de sintaxis del lenguaje JavaScript y proporciona el compilador de código correspondiente. También proporciona un depurador de seguimiento de nivel de código fuente visual. Desarrollar una aplicación ZEROLIMIT es más fácil y más intuitivo que desarrollar una aplicación móvil tradicional, ya que esta aplicación no solo está descentralizada, sino que también es multiplataforma, y puede ejecutarse en múltiples sistemas operativos con solo una codificación.

(2) Despliegue DMAPP

Una vez que la aplicación ZEROLIMIT se haya desarrollado y verificado en el entorno de desarrollo, el siguiente paso es implementar la aplicación en la red ZEROLIMIT. El proceso de implementación es en realidad el proceso de dividir el código de máquina de la aplicación en múltiples transacciones inteligentes y enviarlas a la red ZEROLIMIT.

DMAPP debe someterse a auditorías oficiales de la red ZEROLIMIT y obtener firmas

digitales oficiales antes de realizar la implementación en línea. Cuando el DMAPP se carga en el motor inteligente, se verificará la firma y se rechazarán las firmas inválidas o caducadas.

La cuenta de nodo de ZEROLIMIT puede implementar múltiples aplicaciones. Los editores deben pagar por el lanzamiento de cada aplicación por adelantado. Todos los ahorradores de la aplicación (incluidos los propios editores) guardarán y sincronizarán la información de la cuenta de la aplicación. El tamaño del código y la cantidad de usuarios de DMAPP determinan el costo de ejecución de la aplicación. Los editores también pueden recargar la cuenta de la aplicación en cualquier momento para garantizar el funcionamiento continuo en línea de la aplicación.

(3) Actualización de DMAPP

Las aplicaciones se pueden actualizar en línea en cualquier momento. Esta actualización puede ser actualizaciones parcheadas de módulos locales o actualizaciones incrementales con funciones adicionales. Para la carga de trabajo de descarga adicional del nodo causada por la actualización de la aplicación y la parte de actualización, el editor no necesita asumir costos adicionales, pero para la parte de actualización incremental, el editor debe soportar los costos de descarga correspondientes.

(4) Sincronización entre nodos DMAPP

Cuando el DMAPP se descarga desde el nodo ZEROLIMIT y se carga en el motor inteligente, el nodo ZEROLIMIT se transforma en el nodo DMAPP al mismo tiempo. Todos los nodos en línea del mismo DMAPP forman sus propias redes, que constituyen una subred de ZEROLIMIT y también una parte de la red ZEROLIMIT. También podemos llamar a esta subred el grupo de aplicaciones de DMAPP, en el que tanto la información de estado de la cuenta del editor de DMAPP y los datos de aplicación de DMAPP deben estar sincronizados. Por ejemplo, la información como el DMAPP en la cadena de tiendas, la actualización de los productos en el estante y el inventario, y la evaluación del usuario, deben actualizarse de forma sincrónica con todos los nodos de DMAPP en línea.

(5) Llamada de función entre DMAPP

Las funciones principales de DMAPP se encapsulan como bibliotecas dinámicas y se cargan en el software de nodo ZEROLIMIT. La red ZEROLIMIT define la interfaz de llamada estándar entre ellos. No solo es adecuado para la interacción entre la parte inferior de DMAPP y ZEROLIMIT, sino que también es adecuado para la llamada de función entre DMAPP y ZEROLIMIT. Por ejemplo, si un nodo ZEROLIMIT está equipado con DMAPP social y DMAPP comercial, y ambos tienen interfaces funcionales abiertas, la función de compra se puede importar fácilmente a DMAPP social, y la función de chat se puede incrustar en DMAPP comercial para lograr una reutilización funcional entre DMAPP, que puede ahorrar recursos de desarrollo y recursos de implementación.

12 Ecologia zerolimit

12.1 Cuenta ZEROLIMIT

Usa el modelo de cuenta en ZEROLIMIT. Las cuentas se dividen en dos tipos: cuenta básica y cuenta de aplicación. La cuenta básica se controla mediante una clave privada, mientras que la cuenta de la aplicación se controla mediante un código de consenso. La dirección de la cuenta de la aplicación se calcula de acuerdo con la dirección de la cuenta básica. Cada nodo ZEROLIMIT tiene una cuenta de aplicación y cuenta básica única, y guarda el árbol de estado completo de la cuenta de aplicación y cuenta básica, mientras que los otros nodos solo guardan su árbol de estado de información característica. Un nodo ZEROLIMIT puede publicar varias aplicaciones (DMAPP). Todas las aplicaciones comparten la misma cuenta de aplicación. Todos los nodos que usan DMAPP deben sincronizar la aplicación de la cuenta básica y el árbol de estado de información característica de la cuenta de la aplicación del nodo de publicación. El costo de funcionamiento de DMAPP y el costo de recompensa de proporcionar la descarga de DMAPP se deducen automáticamente de la cuenta de la aplicación del nodo de publicación de la aplicación. El nodo de publicación de la aplicación puede conocer el saldo de la cuenta de la aplicación en cualquier momento y puede recargar la cuenta de la aplicación y retirarla de la cuenta de la aplicación a la cuenta básica a través de la cuenta básica en cualquier momento.

12.2 ID única ZID

En la red ZEROLIMIT, cada nodo tiene una dirección de cuenta única, que representa la identidad única (ZID) del nodo en la red ZEROLIMIT. Las cuentas pueden tener una variedad de atributos de rol al mismo tiempo, como los desarrolladores de DMAPP, operadores de juegos,

comerciantes en línea, empresas, agencias gubernamentales, etc. Se pueden definir hasta 65536 roles. Todas las DMAPP constituyen un completo ecosistema ZEROLIMIT, y la identidad de los nodos es única y coherente cuando se participa en todos los escenarios de aplicación DMAPP.

12.3 Garantia Ecologica ZEROLIMIT

Los activos digitales de ZEROLIMIT (ZOL) tienen una circulación total de mil millones, lo que representa la prueba de los derechos e intereses ecológicos de ZEROLIMIT. Durante el período de colocación privada del proyecto ZEROLIMIT, las suscripciones se ofrecen en forma de activos sustitutos de la cadena, con un volumen de suscripción total de solo 12 millones. Después de la suscripción, los activos de la cadena de descendientes se incluirán en los intercambios principales, y la circulación total de los activos de la cadena de sustitución no superará los 50 millones, es decir, el 95% de los activos de capital se bloqueará para la aplicación de desembarque y la promoción del DMAPP posterior. Una vez que se haya completado el desarrollo de la cadena principal, los activos de la cadena de generación se convertirán en los activos de la cadena principal uno a uno. Los Activos Digitales de ZEROLIMIT (Zollar) son la personificación del valor del ecosistema de ZEROLIMIT. ZEROLIMIT, como líder de la nueva generación de tecnología Blockchain, enfatiza su aplicación de aterrizaje endógeno. Cuando se completa el desarrollo de su cadena principal, se pueden desarrollar varias aplicaciones descentralizadas en la cadena. En comparación con las aplicaciones tradicionales, estas aplicaciones pueden reducir considerablemente los costos, ya que las aplicaciones basadas en ZEROLIMIT son aplicaciones móviles en la cadena y no necesitan el soporte de servidores de fondo. ZEROLIMIT tiene una amplia gama de escenarios de aplicaciones, y puedes usar tu imaginación tanto como sea posible. El activo digital de ZEROLIMIT (Zollar) incorpora completamente su valor de aplicación. Con la popularización continua de su aplicación en el futuro, la escasez de Zollar aumentará rápidamente su precio.

12.4 Nodo Equity ZEROLIMIT

Frente a la red principal de ZEROLIMIT, el equipo de ZEROLIMIT ha emitido pedidos de reclutamiento para la promoción de aplicaciones en todo el mundo, invitando a personas de todos los ámbitos de la vida a dibujar planos de aplicaciones, compartir los derechos e intereses ecológicos de ZEROLIMIT y presenciar la llegada de la era de aplicaciones de Blockchain. Cuando una cuenta de nodo ZEROLIMIT tiene un promedio de 500,000 Zollars por día en los últimos seis meses, el nodo ZEROLIMIT se promueve a un nodo de promoción de aplicaciones. Cuando el proyecto de aplicación promovido por el nodo de promoción de la aplicación se ejecute con éxito en la red ZEROLIMIT y aporte los beneficios correspondientes a la red ZEROLIMIT, el nodo de promoción de la aplicación obtendrá un derecho de dividendo del 70%. Cuando una cuenta de nodo

ZEROLIMIT tiene un promedio de 1 millón de Zollars por día en los últimos 12 meses, el nodo ZEROLIMIT se promueve a un nodo de derechos ecológicos. Además de los derechos e intereses de los nodos de aplicación y promoción, el nodo de derechos ecológicos también disfruta del derecho de dividendos del 1% del ecosistema ZEROLIMIT en su conjunto.

El nodo de equidad es un concepto lógico. El tamaño de la equidad no afecta el estado del nodo en sí en la red ZEROLIMIT. Todos los nodos en la red ZEROLIMIT son funcionalmente iguales, y no hay ninguna ventaja de agregación de recursos que amenace la seguridad de toda la red.

12.5 Escenario de aplicación ZEROLIMIT

La red ZEROLIMIT puede satisfacer el crecimiento ilimitado de la demanda de aplicaciones en todo el mundo. El objetivo de la aplicación de la red ZEROLIMIT es hacer que la aplicación Blockchain sea civil, de modo que las aplicaciones basadas en ZEROLIMIT cubran todos los aspectos de la vida de las personas.

(1)Las características del nodo móvil de ZEROLIMIT y la alta capacidad de procesamiento de transacciones son particularmente adecuadas para aplicaciones financieras.

(2) El escenario de pago es la aplicación nativa de ZEROLIMIT. ZEROLIMIT tiene ventajas inherentes en pagos móviles, micropagos y pagos transfronterizos.

(3) ZEROLIMIT tiene una ventaja única en el comercio electrónico móvil. Todos pueden abrir una tienda en línea en ZEROLIMIT, solo tienen que pagar una pequeña cantidad de costos de operación y mantenimiento, sin costos de depósito y plataforma, y sin soporte de servidor backstage.

(4) El software social Ciphertext también es una aplicación que vale la pena esperar.

(5) Las aplicaciones de juego deben ser benévolas. La drástica caída en los costos operativos animará a los operadores de juegos a beneficiar a los jugadores, y un mejor sentido de la experiencia llevará a más fanáticos.

(6) Las características de nodo ligero y micropago de ZEROLIMIT son particularmente adecuadas para el despliegue de los nodos de Internet de las cosas.

(7) El teléfono móvil ZEROLIMIT integra el núcleo inferior de ZEROLIMIT con el sistema operativo móvil. Cada teléfono móvil es un nodo de ZEROLIMIT. Puede instalar y ejecutar directamente DMAPP en el teléfono móvil para darse cuenta del verdadero sentido del teléfono móvil Blockchain.

(8)El motor de búsqueda, la popularización de DMAPP, convertirá a la red

ZEROLIMIT en el sistema de red Peer-to-Peer más grande del mundo. El nuevo motor de búsqueda podrá localizar de manera precisa y rápida la información requerida de la información masiva almacenada en el almacenamiento distribuido.

(9) La publicidad directa, las redes de nodos masivos y los grupos de aplicaciones exclusivas de DMAPP pueden lograr una publicidad precisa y un efecto de entrega directa en toda la red.

(10) El nuevo sistema de nombres de dominio, la visualización personal y la visualización empresarial se realizarán a través de nuevas formas. Es decir, el sitio web tradicional será reemplazado por la nueva aplicación de pantalla y conectado a través del nuevo sistema de nombres de dominio.

(11) El equipo de ZEROLIMIT continuará explorando los escenarios de aplicación de diferentes industrias, incluyendo seguridad social, gobierno electrónico, comercio electrónico, trazabilidad de alimentos, certificación contra la falsificación, archivos electrónicos, gestión comercial, impuestos electrónicos, derecho electrónico, finanzas, y proporcionar prototipos de diseño de referencia.

DMAPP significa que las futuras aplicaciones de Internet ya no necesitarán el soporte de servidores centrales, y reducirán directamente el costo de la aplicación en el horizonte. Todas las aplicaciones basadas en redes ZEROLIMIT no necesitan considerar la escalada de costos causada por el aumento del tráfico.

13 Red mayor plan online

El equipo central de ZEROLIMIT está impulsando el desarrollo del proyecto según lo planeado. Se espera que la red principal se lance oficialmente en el primer trimestre de 2020, junto con el pago de DMAPP y Mall DMAPP. Además, el DMAPP fiscal y el DMAPP de la seguridad social también están en curso.