Una red compartida segura y de última generación

Red de Consenso de Prueba de Trabajo

2024.01.01

Versión 5.0

Abstracto

En este documento técnico se presentan escenarios de aplicación de productos, marcos técnicos y detalles de implementación de Guardnet Network. Este proyecto consta de tres etapas: una plataforma de intercambio de recursos de red segura, una red de consenso verdaderamente descentralizada y una plataforma de desarrollo de Internet de confianza. Actualmente, se ha desarrollado la plataforma segura de intercambio de recursos de red y, después de un período de pruebas beta públicas, lanzamos oficialmente un tipo de hardware de seguridad inteligente llamado Guardnet Connect a principios de 2019. Es tanto un dispositivo de seguridad de red como un dispositivo rentable para compartir recursos de red para los usuarios. Además, Guardnet Connect permite a todos los usuarios construir una red de consenso verdaderamente descentralizada a través del mecanismo de consenso NPoW (Next-Gen Proof-of-work) único de Guardnet, que puede servir además como una plataforma de desarrollo de Internet de confianza. Guardnet Connect es la primera innovación que combina la tecnología de ciberseguridad, la economía colaborativa de redes y la tecnología blockchain.

Guardnet Connect está diseñado con plug-and-play y configuración cero, lo que permite a los usuarios disfrutar de la protección de la tecnología de seguridad de red sin barreras. Los usuarios no necesitan ninguna experiencia o instrucciones. Todo lo que necesitan es un cable de red para conectar el dispositivo entre el módem y el enrutador. Esta sencilla operación puede permitir a los usuarios superar la interferencia de la red, defenderse de los ciberataques, controlar el tráfico, controlar los padres, ganar recompensas por compartir el ancho de banda de la red y la minería de la cadena de bloques web3, etc.

Desde la perspectiva de la tecnología de seguridad de red, Guardnet Connect proporciona una solución de seguridad de red todo en uno. El núcleo de la función

seguridad de la red es AtomOS, un sistema operativo de red, desarrollado de forma independiente por Guardnet Network. AtomOS es el primer sistema operativo de red sin bloqueos del mundo. Su avanzado diseño sin bloqueo garantiza una alta fiabilidad, un alto rendimiento y una alta escalabilidad de todo el sistema. Además, las tecnologías innovadoras de Guardnet, que incluyen Trident Protocol, Adap-tive Tunneling, Intelligent Routing, IP Multiplexing y Tunnel Congestion Control, brindan a los usuarios un profundo nivel de seguridad y una mejor experiencia de usuario.

Desde la perspectiva de la tecnología blockchain, Guardnet implementa su plataforma de intercambio de recursos de red en blockchain a través de contratos inteligentes. Incluye principalmente contratos de tokens, contratos de nodos, contratos de crédito, contratos de staking y contratos de micropagos. Hemos lanzado una nueva plataforma de blockchain de contratos inteligentes llamada Guardnet Chain. The Guardnet Chain utiliza el mecanismo de consenso original de Guardnet basado en NPoW (Next-Gen Proof-of-work) para lograr una plataforma de cadena pública verdaderamente descentralizada. Al mismo tiempo, Guardnet Chain es una plataforma de cadena pública de nueva generación con alta eficiencia, bajo consumo de energía y características de seguridad. Después de que se lanzó la red principal de Guardnet Chain, el dispositivo Guardnet Connect del usuario puede participar en la minería en Guardnet Chain. Los desarrolladores de DApps también pueden desarrollar aplicaciones descentralizadas, como plataformas de comercio de divisas digitales, plataformas sociales y plataformas de comercio electrónico en Guardnet Chain. Estas nuevas aplicaciones basadas en Guardnet Chain no solo satisfacen las necesidades básicas de los usuarios, sino que también protegen mejor la privacidad y los datos de los usuarios, proporcionando así una Internet de confianza en la que se garantiza la soberanía de los datos personales.

Contenido

1. La difícil situación de la era de la Web 2.0

Con el rápido desarrollo de Internet, el mundo en el que vivimos está siendo profundamente cambiado por una cosa: la información. Ya en 1948, el Dr. Shannon fue pionero en la teoría de la información cuantificando matemáticamente la información [46]. Con la llegada de Internet, el flujo de información no tiene precedentes y la cantidad de información disponible para las personas ha aumentado exponencialmente. Internet también ha revolucionado la democratización del conocimiento y la información, haciendo que el conocimiento y la información de alta calidad ya no estén disponibles para la minoría. Desde 2009, el rápido desarrollo de la tecnología blockchain ha abierto la era de la libertad de información descentralizada. Sin embargo, impulsadas por la ola de tecnologías, las personas a menudo solo prestan atención a la conveniencia y los beneficios que aportan las tecnologías desarrolladas, mientras ignoran si los escenarios de aplicación de estas tecnologías están manipulados maliciosamente, así como las graves consecuencias que traen los defectos inherentes a estas tecnologías.

1.1 Cibercrimen

La propagación de virus en la red es una amenaza infinita y causa graves daños económicos [51]. En 2017, 1,65 millones de computadoras fueron secuestradas por virus de red y obligadas a participar en la minería de monedas digitales [36]. Con el desarrollo del Internet de las Cosas (IoT), el alcance de las interferencias maliciosas aumentó a pasos agigantados. Los virus IoT pueden secuestrar computadoras personales, cámaras, electrodomésticos inteligentes, cerraduras de puertas inteligentes, enrutadores y otros dispositivos accesibles a Internet. Comenzando

con el virus Mirai [32] en junio de 2018, más de 600.000 dispositivos en red han sido hackeados [49]. Adicionalmente, Los ataques de phishing lanzados por sitios web maliciosos pueden obtener información personal confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por personas y organizaciones de confianza [39]. En 2017, el sistema Kaspersky Anti-Phishing se activó más de 246 millones de veces, y el 15,9% de sus usuarios se convirtieron en objetivos de sitios de phishing [15]. A raíz de las pérdidas financieras causadas por los sitios web de phishing, desde diciembre de 2013 hasta diciembre de 2016, el FBI investigó 22.000 estafas de phishing en los Estados Unidos, por un total de hasta 1.600 millones de dólares estadounidenses [30]. Se estima que 2020 dejó un récord de pérdidas de casi un billón de dólares, el doble que en 2018 [42]. Esto se debió en parte a la pandemia de coronavirus, ya que los piratas informáticos se aprovecharon de los clientes, las empresas y una gran población que cambió al trabajo remoto. Los piratas informáticos ya no se dirigen a máquinas específicas, sino a organizaciones enteras que utilizan operadores humanos como eslabones débiles para obtener acceso a redes completas. Travelex, empresa de cambio de divisas con operaciones en 70 países, es un ejemplo de esta situación. La empresa tuvo que hacer frente a demandas de pago para descifrar archivos informáticos críticos después de ser golpeada por Sodinokibi, uno de los ataques de ransomware más sofisticados hasta la fecha, que supuso un ataque devastador [14].

Estas cifras no son una sorpresa, ya que el número de usuarios de Internet aumenta constantemente a un ritmo de 1 millón por día. Se estima que para 2030 habrá 7 mil millones de usuarios en todo el mundo [34], con 1 billón de sensores en red integrados en el mundo que nos rodea ya en 2022, y un total de 45 billones en los próximos 20 años [1]. El cibercrimen es el parásito inevitable que sigue a esta actividad humana, a partir de ahora cuesta más que todos los desastres naturales, y

es más rentable que el tráfico de drogas [33]. La ciberdelincuencia se convertirá en uno de los mayores riesgos para las empresas y las personas.

1.2 Supresión de información y censura en Internet

La supresión de la información y la censura en Internet se refieren al acto de negar un cierto grado de libertad de expresión al privar al usuario de ciertos derechos en Internet para que la identificación o IP del usuario no pueda navegar por la web o enviar mensajes [4]. Muchos países de todo el mundo han bloqueado un gran número de sitios web por diversas razones [24], [25], [53], incluido el de Estados Unidos, defensor desde hace mucho tiempo de la libertad de expresión. La reciente prohibición de las cuentas de redes sociales de Donald Trump muestra que incluso en la tierra de la libertad, la libertad de expresión en Internet no está garantizada.

El incidente de las acciones de GME es un ejemplo reciente perfecto de censura, ya que plataformas de negociación como Robinhood y E-market suspendieron todas las operaciones de las acciones involucradas. Incluso la plataforma amigable para los jugadores, Discord, cerró un grupo de chat que lleva el nombre del grupo WSB para frustrar cualquier coordinación adicional de este grupo comercial.

Según Freedom on the Net Global Internet la libertad ha disminuido por décimo año consecutivo, ya que las puntuaciones de 26 países disminuyeron durante la cobertura del período 2019-2020. La puntuación de Estados Unidos bajó por cuarto año consecutivo. A pesar de que Facebook, Twitter y otras plataformas de redes sociales se utilizaron como herramientas para el activismo social, la vigilancia de las redes sociales por parte de las agencias federales y locales de aplicación de la ley anuló la eficacia de estas herramientas, algunas personas sufrieron acoso selectivo o se les imputaron cargos penales falsos por sus publicaciones o retuits. [46]

Junto con todas sus comodidades, las posibilidades de censura y vigilancia también son inherentes a Internet. Estos problemas son tan comunes y generalizados que las personas se han visto obligadas a renunciar a una medida de privacidad a cambio de la comodidad de Internet [54], y a menudo pierden sin saberlo los derechos de privacidad de los datos [18] – Los datos personales a menudo son controlados por proveedores de servicios e incluso vendidos a terceros con fines de lucro [21], [23]. Esa vieja frase de los años 70 nunca ha sido más cierta: "si no pagas por el producto, eres el producto".

Nota: Debido a las diferentes políticas en diferentes regiones y países, Guardnet Network ajustará y restringirá la función de accesibilidad para las versiones vendidas en diferentes regiones, y lanzará diferentes versiones para los países para garantizar que los productos de Guardnet puedan adaptarse a sus leyes y regulaciones. Eso no significa necesariamente que estemos de acuerdo con tales restricciones, ya que imaginamos una Internet libre y sin fronteras. Respetando las leyes locales, seguimos dando pasos pioneros en el largo y colectivo proceso de democratización de la red.

1. Crisis de confianza en Internet

Dado que los proveedores de servicios de Internet y otros peces gordos en línea pueden monitorear, almacenar y vender los datos de los usuarios, es un hecho que Internet carece de privacidad de datos. Sin mencionar el hecho de que, por supuesto, también pueden perfilarlo y compartir esos datos con agencias gubernamentales. El alcance de esta vigilancia es profundo y extremadamente intrusivo. De enero de 2005 a mayo de 2008, hubo más de 200 millones de casos sospechosos de violación de registros personales confidenciales [9]. Como consecuencia, las instituciones médicas perdieron 6.200 millones de dólares en 2014 y 2015 [40]. En 2018, las filtraciones de datos de

Facebook y Cambridge [48] volvieron a atraer la atención mundial sobre la amenaza de la fuga de datos. De hecho, los casos de violación de datos son comunes en todo el mundo [26]. Estas violaciones de datos que provocan pánico son causadas por la naturaleza altamente centralizada de Internet y los efectos secundarios del comercio de información [50]. Teniendo en cuenta los problemas anteriores, no es de extrañar que la Internet actual no sea totalmente confiable, la falta de transparencia y de infraestructura confiable haya generado una crisis de confianza. De hecho, la supresión, la censura, el engaño y otros tipos de actividades maliciosas no lo son raro.

Bitcoin apareció en 2009 como consecuencia de la crisis financiera de 2008. Un evento en el que numerosos bancos y otras instituciones financieras quebraron en todo el mundo, y tuvieron que ser rescatados por los gobiernos a expensas de sus contribuyentes. Esta situación llevó a una pérdida total de confianza en el sistema financiero. Bitcoin tendía a ser una forma descentralizada de dinero digital con el objetivo de eliminar la necesidad de intermediarios tradicionales como bancos y gobiernos para realizar transacciones financieras. La visión original de Satoshi era que cada computadora contribuyera con un voto al proceso de minería. Desafortunadamente, esa visión pronto se deterioró. Para el año 2012 habían aparecido dispositivos de hardware especializados en minería, iniciando la transición hacia la industrialización. Pronto, las enormes granjas industriales sacaron del juego a los mineros aficionados promedio. Este problema que concentra injustamente la oferta en pocas manos se conoce como centralización minera. Si un grupo de mineros controla el 51% del suministro total, la red se centraliza en ese momento.

Guardnet Network cree que la visión de Satoshi es alcanzable y quiere aprovechar el terreno entre sus usuarios mediante la introducción de su algoritmo de consenso de prueba de crédito (PoCr), de modo que todos puedan participar.

Creemos que nuestra visión es posible gracias a la tecnología desarrollada y a la experiencia acumulada por nuestro equipo a lo largo de los años en las áreas de diseño de hardware, sistemas operativos, ciberseguridad y blockchain.

1.3 Creencias fundamentales de Guardnet

Las creencias fundamentales de Guardnet son:

1. Libertad: Democratizando la Red
   Levantar las fuertes restricciones impuestas por la política y la censura sobre el flujo de información para lograr un intercambio de datos sin fricciones entre toda la raza humana.

1. Equidad: Blockchain para todos
   Aprovechar el verdadero valor de la tecnología blockchain para empoderar a la gente común en lugar de constituir uno de los muchos mecanismos a través de los cuales una minoría privilegiada se beneficia. Una red de consenso verdaderamente descentralizada debe ser una plataforma en la que todos puedan participar y beneficiarse. Debe servir a la sociedad en su conjunto y no a una organización centralizada o a un grupo de individuos poderosos.

1. Confianza: La información es poder y pertenece a las personas.
   Al igual que la casa, la tierra y los ahorros, los datos personales son una forma de propiedad privada y, como tales, merecen un nivel de protección acorde a su importancia. La misión final de Guardnet es combinar la seguridad y la tecnología blockchain para crear una Internet confiable que garantice la soberanía de los datos personales.

2 Descripción general del proyecto

2.1 Guardet Connect

2.1.1 Introducción y filosofía de diseño

Guardnet Connect es una solución todo en uno impulsada por blockchain que proporciona una verdadera libertad en Internet con seguridad mejorada y una experiencia de usuario sin fricciones. La filosofía de diseño de Guardnet Connect es plug-and-play sin configuración. Los usuarios pueden disfrutar de la protección de la seguridad de la red sin necesidad de pasar por ningún aro. No se necesitan conocimientos técnicos ni un manual de usuario complejo. Todo lo que hay que hacer es conectar el dispositivo entre el módem y el router, encender el dispositivo y disfrutar de todas sus ventajas: eludir la censura, protección contra ciberataques, establecer controles parentales, participar en el intercambio de ancho de banda de la red y la minería de blockchain.

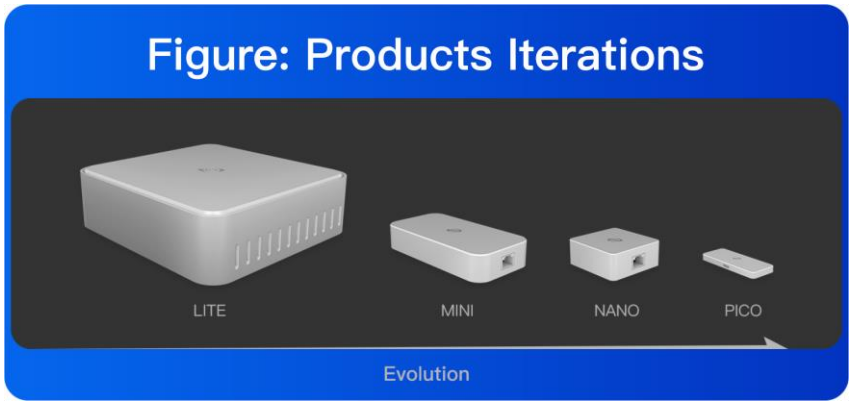

Figura 1: Iteraciones de productos

Guardnet Connect ha visto generaciones de iteraciones que van desde 1) Guardnet Connect Lite hasta 2) Guardnet Connect Mini, 3) Guardnet Connect Nano y ahora 4)

Guardnet Connect Pico, con cada versión más miniaturizada. La visión de Guardnet Connect siempre ha sido hacerlo lo más parecido posible a un cable ethernet, con la creencia de que la gran tecnología se mezcla con el fondo y se aparta del camino de los usuarios. El Guardnet Connect Pico representa la última encarnación de ese espíritu. La gama de dispositivos Guardnet Connect ha tenido una gran adopción por parte de los usuarios desde sus inicios, con miles de unidades vendidas en todo el mundo; el Guardnet Connect Mini es uno de los mejores productos en Indiegogo.

1. Soluciones para una Internet más segura, privada y justa

Guardnet Connect ha visto generaciones de iteraciones que van desde Guardnet Connect Lite hasta Guardnet Connect Pico sirve como un nodo en una red privada descentralizada y un firewall de próxima generación en la red doméstica. Las redes privadas descentralizadas no tienen servidor y están distribuidas; Los datos de los usuarios nunca pueden ser registrados, filtrados, pirateados o citados. Un firewall de nivel empresarial de capa 7 protege toda la red doméstica del usuario. Bloquea anuncios y rastreadores, monitorea el tráfico web y filtra NSFW, NSFC en todos los dispositivos de Internet.

2.1.2 Technical Tour de Force: AtomOS, Trident Protocol, IP Multiplexing

AtomOS

El núcleo de la destreza de seguridad de red de Guardnet Connects radica en AtomOS, un sistema de operación de red diseñado y desarrollado por Guardnet. AtomOS es el primer sistema operativo de red sin bloqueos del mundo. Las propiedades del sistema de alta disponibilidad, alto rendimiento y alta escalabilidad dependen de su diseño sin bloqueo de última generación.

Trident Protocol

Guardnet desarrolló su propio protocolo "Trident", un protocolo de comunicaciones descentralizado y compartido basado en la cadena de bloques con tunelización adaptativa y tecnologías de enrutamiento inteligente para proporcionar una protección de seguridad en profundidad, así como una experiencia de usuario mejorada. Evita la censura de la red, asegura las transmisiones de datos, maximiza el uso del ancho de banda de la red y reduce los retrasos en el proceso de transmisión de paquetes de datos. Esto se logra gracias a la integración eficiente de tecnologías de red como la penetración en la intranet, el cifrado de datos, el camuflaje de protocolos y el control de la congestión de la capa de túnel. Más detalles en la sección 5.1.

Multiplexación IP

La tecnología de multiplexación IP patentada de Guardnet permite la configuración de direcciones IP cero y la adaptación inteligente de la dirección IP del router para interactuar automáticamente con Internet, logrando la verdadera experiencia plug-and-play para los dispositivos Guardnet Connect.

2.2 Guardnet Network

El valor de Guardnet radica no solo en el hardware que ofrece, sino también en la plataforma de red que conecta esos dispositivos entre sí. Sus manifestaciones específicas son las siguientes:

- Plataforma segura de uso compartido de recursos de red
- Una red de consenso blockchain verdaderamente descentralizada
- Plataforma de desarrollo de Internet de confianza

La Ley de Metcalfe [47] establece que el valor de una red es proporcional al cuadrado del número de nodos de la red. Por lo tanto, a medida que aumenta el número de dispositivos de hardware extendidos implementados, el valor de la red entre dispositivos aumentará exponencialmente.

2.2.1 La puerta de entrada segura de todos los hogares a la web 3.0

Guardnet Connect es el primer producto de ciberseguridad del mundo basado en la tecnología blockchain. Al interactuar con usuarios de todo el mundo por su diseño plug-and-play, Guardnet Connect elimina las barreras técnicas y proporciona una experiencia de Internet privada, segura y sin restricciones para todos los usuarios. "Guardnet Connect Mini" de Guardnet Network tiene más de 60.000 nodos en más de 150 países y ha recaudado con éxito más de 2,72 millones de dólares en Indiegogo. Como puerta de entrada al ecosistema de Deere, Guardnet Connect está diseñado para llevar la cadena de bloques a las masas y crear conciencia sobre la próxima Web Revolución 3.0.

2.2.2 Red privada descentralizada (DPN)

La red privada descentralizada es una red de intercambio de ancho de banda descentralizada P2P para eludir la censura y garantizar la privacidad. La red no tiene servidor y está distribuida; Los datos de los usuarios nunca pueden ser registrados, filtrados, pirateados o citados. Cada operador de nodo está facultado para ser tanto un cliente como un servidor; Los operadores de nodos ganan recompensas mineras por contribuir con ancho de banda a la red. La incentivación de la minería garantiza la solidez de la red en comparación con los modelos tradicionales de redes P2P. DPN es la primera aplicación asesina en el ecosistema blockchain de Guardnet y un catalizador para una economía colaborativa descentralizada y la soberanía de los datos personales.

2.2.3 Plataforma perimetral descentralizada (DEP)

DEP es una infraestructura descentralizada construida fuera de la cadena y basada en los nodos de dispositivos Guardnet. Se utiliza para liberar tareas descentralizadas. El nodo Guardnet supervisa eventos específicos, analiza los eventos y desencadena el flujo de trabajo de tareas específicas, de acuerdo con la URL de aplicación y la opción de parámetro de operación, las tareas de extracción, programación y supervisión finalizan cuando el estado de ejecución de un nodo cumple ciertas condiciones. Cada nodo puede asumir una aplicación Web2 / Web3 diferente, y se convertirá fácilmente en un proveedor o coproveedor de servicios, ganando recompensa y propiedad al proporcionar el desarrollo y mantenimiento de estos servicios. Una plataforma descentralizada fuera de la cadena de este tipo ofrece la posibilidad de nuevos formularios de solicitud, como predictor, red cero, red relámpago, disparador, servicio de correo, etc.

2.2.4 Decentralized Youtube (D-tube)

D-tube es una plataforma descentralizada para creadores de videos Web3.0 que se basa en la tecnología de seguridad y red de DEP para implementar un almacenamiento seguro de datos y una distribución rápida del tráfico. Las plataformas de contenido tradicionales de la Web2.0 hacen que los creadores sean una parte importante de su plataforma para atraer clientes y tráfico. Estos creadores son los propietarios del valor y el espacio, pero carecen de suficiente control sobre el contenido, los derechos de autor y la publicidad. D-tube utilizará el modo de operación del sitio web descentralizado Web3.0 fuera de la cadena y lo combinará con el método de certificado valorado NFT en la cadena para proporcionar un nuevo modo interactivo web3.0 para todos los creadores. Tanto los mecanismos de ver y ganar como los de crear y ganar se utilizan para estimular la participación y el crecimiento de

más creadores y sus fans, aportando un entorno creativo descentralizado y abierto para los creadores.

2.2.5 Aplicación de chat descentralizada (D-chat)

D-chat es un software de chat Web3.0 descentralizado que se basa en la implementación de aplicaciones descentralizadas del DEP, puede implementar rápidamente nodos de aplicaciones de chat a gran escala; y con la ayuda de la tecnología de red de cifrado de privacidad DPN, puede lograr la transmisión de mensajes privados entre dominios. Con el software de chat Web2.0 tradicional, los usuarios no tienen derecho a disponer de su identidad y sus datos. La plataforma puede restringir el acceso y el permiso de los usuarios de las cuentas personales a su voluntad, y el contenido del chat y los registros de transacciones se pueden monitorear como deseen. D-chat utilizará el nodo de túnel cifrado descentralizado fuera de la cadena, combinará la autenticación de identidad de la cadena de bloques en la cadena y la transacción punto a punto para lograr finalmente que el contenido digital, la propiedad y los derechos de control creados por los usuarios pertenezcan a los usuarios. El valor creado por los usuarios puede ser distribuido mediante la firma de acuerdos con otros a su propia elección.

Con el desarrollo y crecimiento de la comunidad de Deere, basada en la plataforma de ejecución de infraestructura descentralizada de DEP off-chain, Guardnet desarrollará más programas de incentivos para motivar a los desarrolladores de la comunidad y brindar un ecosistema de aplicaciones diverso a los usuarios.

3 Hardware

El objetivo de Guardnet Connect es proporcionar una solución de hardware plug-and-play para la seguridad, la economía colaborativa y la cadena de bloques, una solución todo en uno. A continuación, se describen los aspectos más destacados del hardware de Guardnet Connect.

3.1 Cross-Platform

Guardnet Connect está diseñado para ser compatible con diferentes plataformas de hardware. Ato-mOS se ha ejecutado con éxito en procesadores Intel y ARM64, lo que permite a Guardnet aprovechar ambas plataformas: los procesadores Intel son lo suficientemente potentes como para manejar todo tipo de escenarios de alta sobrecarga de red, lo que permite a Guardnet no solo cubrir los complejos casos de uso de las redes domésticas, sino también satisfacer los requisitos de nivel empresarial. Por otro lado, la plataforma ARM es famosa por su bajo consumo de energía y bajo costo, lo que es suficiente para las necesidades rutinarias de la red doméstica y diferentes tipos de casos de uso móvil. En el futuro, Guardnet también tiene planes para productos ARM32, lo que reduciría aún más el costo del hardware a menos de $10.

3.2 Bajo consume de energía

Según la evaluación de Digiconomist [3], el consumo total anual acumulado de energía de la minería de bitcoin en todo el mundo alcanzó los 68.810 millones de kWh, seis veces el consumo de energía de mayo de 2017 (11.570 millones de kWh). El consumo de energía de todos los mineros de bitcoin en todo el mundo es equivalente al de la República Checa, que representa el 0,31% del consumo mundial de energía. El

consumo medio de energía por cada transacción de bitcoin es de 968 kWh, lo mismo que el consumo de energía de 32 familias estadounidenses en un día. Actualmente, las emisiones anuales de carbono de Bitcoin ascienden a 33,85 millones de toneladas, o 1.300 kilogramos de carbono por bitcoin [29].

El algoritmo único NPoW creado por Guardnet puede resolver fundamentalmente este problema. El algoritmo NPoW puede permitir que cada dispositivo participe en el consenso de la red con un uso muy bajo de electricidad. Guardnet Connect utiliza procesadores integrados de bajo consumo para crear una red de consenso y compartir la red. El consumo máximo de energía de un dispositivo Guardnet Connect es de 15 vatios. Guardnet Connect Pico tiene un consumo máximo de energía de 1W.

Como se ve en la Tabla 1, Guardnet Connect es el producto más eficiente energéticamente en el mercado (aproximadamente tres órdenes de magnitud menos de consumo de energía en comparación con los equipos de minería ASIC/GPU comunes) y tiene el potencial de convertirse en el equipo de minería blockchain más rentable.

Tipo de hardware	**Consumo de energía**
Guardnet Connect	1~15W
ASIC mining rig	2,000~3,000W
GPU mining rig	1,000~2,000W

Tabla 1: Comparación del consumo de energía de la plataforma minera

3.3 Hardware Wallet

El hardware de seguridad de Guardnet también integra una función de billetera de criptomonedas para proporcionar a los usuarios el más alto nivel de seguridad de criptomonedas sin necesidad de ningún conocimiento de blockchain o seguridad de red por parte de los usuarios.

Guardnet Connect proporciona múltiples garantías de seguridad con AtomOS, lo que hace imposible que los crackers y las organizaciones maliciosas obtengan el control del hardware de forma remota. Como resultado, la información clave almacenada en el dispositivo es inaccesible para los crackers. Además, los ataques maliciosos se identificarán y registrarán para ayudar a atrapar a los crackers.

Figure 2: El acceso malicioso será bloqueado y registrado

Guardnet Connect emplea tecnología de triple encriptación para garantizar la seguridad de los dispositivos de almacenamiento. Incluso si se pierde el dispositivo de hardware, nadie puede acceder a los datos almacenados en el dispositivo. La tecnología de cifrado triple incluye el cifrado de dispositivos de bloques, el cifrado de sistemas de archivos y el cifrado de archivos.

3.3.1 Bloquear el cifrado de dispositivos

Si se pierde el dispositivo de almacenamiento, los crackers podrían leer archivos críticos analizando los datos del dispositivo de bloques. Para contrarrestar eso, cada bloque en Guardnet Connect está encriptado con AES-CBC [13] (Figura 3), lo que hace que sea muy difícil descifrar los datos porque los crackers solo pueden acceder a los datos encriptados.

3.3.2 Cifrado del sistema de archivos

El simple hecho de emplear el cifrado de dispositivos en bloque no es suficiente para garantizar la seguridad del dispositivo. Con el fin de proteger aún más nuestros medios de almacenamiento, Guardnet Connect codificó la

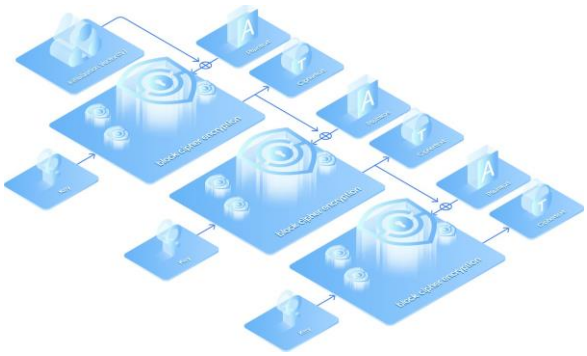

Figure 3: Todos los datos de disco en Guardnet Connect están cifrados con AES-CBC

Estructura de datos clave del sistema de archivos general (Figura 4). Así es como se implementa GuardnetFS, un sistema de archivos único de diseño propio de Guardnet. Debido a la estricta confidencialidad de la estructura de datos de GuardnetFS, los crackers no pueden recuperar ninguna información del dispositivo de bloques relacionada con la estructura del sistema de archivos y, por lo tanto, no pueden acceder a ningún archivo crítico almacenado en el sistema de archivos.

Figura 4: El sistema de archivos encriptado confunde a los crackers

3.3.3 Cifrado de archivos

Todos los archivos críticos almacenados en el sistema de archivos de Guardnet Connect deben estar cifrados por AES-CBC. La clave de descifrado para todos los archivos solo está disponible dentro del código de programa compilado, lo que significa que solo el programa Guardnet puede acceder a la información de texto sin formato si es necesario (Figura 5).

Figure 5: La tecnología de triple encriptación garantiza una mayor seguridad de los datos de conexión

3.4 Plataforma minera con seguridad de red

El 28 de mayo de 2018, se descubrió el "Paquete de la Muerte" en Ethereum (CVE-2018-12018) [38], donde el atacante podía congelar los nodos Geth mediante el envío de un paquete de muerte. Geth es el cliente oficial de Ethereum, extremadamente importante para el proyecto Ethereum: alrededor del 70% de los nodos que ejecutan geth contienen nodos clave para intercambios públicos y grupos de minería. Con este error, un atacante podría derribar Ethereum y desatar un terremoto en el mercado de Ethereum.

Después de proporcionar servicios de uso compartido de redes, Guardnet Connects también se convertirá en equipos de minería de cadena de Deere. Actualmente, se han

pasado por alto los problemas de seguridad de las plataformas mineras. Sin embargo, si un cracker se dirige a errores de software de minería o debilidades de hardware de minería, dicho ataque naturalmente tendría un impacto significativo en el valor de la criptomoneda correspondiente. Todos los productos de Guardnet heredan genes de seguridad de red y todos ellos están meticulosamente diseñados y completamente probados. Los dispositivos de seguridad más profundos que ejecutan AtomOS serán los equipos de minería más seguros del mundo, protegiendo al máximo la cadena Guardnet y los intereses de todos sus mineros.

Figure 6: Guardnet Connect con sus genes de seguridad de red heredados proporciona protección adicional para la cadena más profunda

4 Sistema Operativo

La arquitectura de software de Guardnet consta de un plano de datos, un plano de gestión y un plano de control. El plano de datos, implementado con AtomOS desarrollado de forma independiente por Guardnet, es responsable de manejar la transmisión, recepción e inspección profunda de paquetes de datos del usuario. El plano de gestión debe proporcionar una interfaz fácil de usar para supervisar las operaciones del sistema o cambiar las configuraciones del sistema. El plano de control maneja la comunicación entre el dispositivo y la cadena de bloques, la comunicación entre dispositivos y admite el mecanismo de consenso de la cadena

de bloques. La vista por capas de la arquitectura del software se muestra en la Figura 7.

Figure 7: Vista de capa de software

La clave del software de Guardnet es AtomOS, un sistema operativo de red diseñado a medida para una seguridad profunda. También es el **primer sistema operativo de red sin bloqueos del mundo**. El diseño avanzado de AtomOS es la base de la fiabilidad, eficiencia y seguridad de todo el sistema. Presentaremos brevemente tres aspectos de AtomOS: E/S de paquetes, programación de paquetes e inspección profunda de paquetes.

4.1 Packet I/O

La E/S de paquetes cae en la capa de E/S de AtomOS. Es una de las tecnologías clave que determina la latencia del flujo de datos del usuario y el rendimiento del ancho de banda.

Los sistemas operativos tradicionales utilizan una pila de red de kernel para transmitir y recibir datos. Las principales desventajas de este enfoque son la alta latencia y el bajo rendimiento. Después de atravesar la red hasta un dispositivo de red, el paquete encuentra una serie de obstáculos de procesamiento inmediatos, como la tarjeta de interfaz de red, el controlador del dispositivo de red, la pila de red del kernel y el socket antes de someterse al procesamiento final (consulte la Figura 8). Además, este enfoque puede incurrir en frecuentes cambios de contexto e interrupciones de hardware, lo que aumenta aún más la latencia de los datos y reduce el rendimiento.

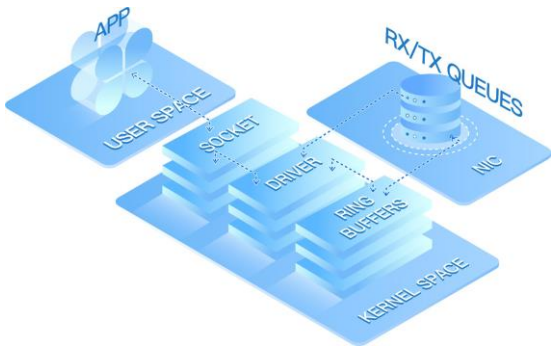

Figura 8: Transceptor de datos del sistema operativo tradicional

AtomOS emplea la tecnología de copia cero para acceder a los paquetes directamente desde los dispositivos de red (consulte la Figura 9). Esta tecnología no solo evita la engorrosa pila de red del kernel de Linux, sino que también evita los frecuentes cambios de contexto e interrupciones de hardware. Reduce en gran medida la latencia de los paquetes de datos y aumenta el rendimiento. AtomOS implementa la tecnología de copia cero con DPDK [11], diseñado por Intel. Los datos de prueba proporcionados por Intel muestran que DPDK multiplica por diez el rendimiento [12].

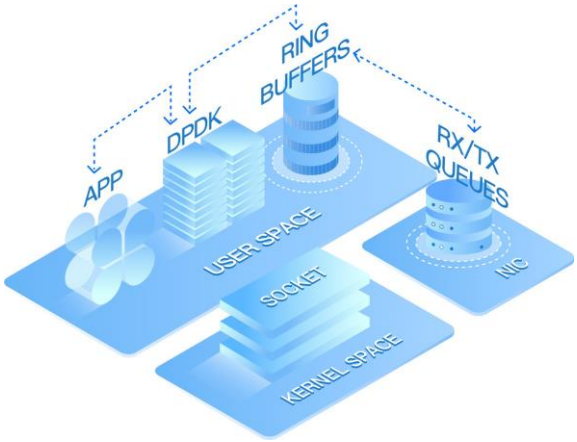

Figura 9: Transceptor de datos DPDK

4.2 Packet Scheduling

AtomOS implementa el primer sistema operativo de red sin bloqueos del mundo con la estructura de datos HIPE única de Guardnet. Todos los problemas del sistema operativo de red se pueden resolver en una estructura basada en HIPE; Encarna los componentes de nuestra filosofía de diseño: simple, eficiente y bajo control. Antes de ilustrar la implementación detallada de HIPE, echemos un vistazo a los límites generales de los sistemas operativos de red actuales.

1. Alto rendimiento y alta escalabilidad

   A medida que el tamaño de los transistores de la CPU disminuye, la ley de escalado de Dennard [10] se rompe gradualmente. El tamaño reducido del transistor aumenta el consumo de energía estática y detona una conversión de energía térmica grave. Además, el calor acumulado entre los transistores es considerable, lo que hace que la refrigeración de la CPU sea un problema urgente. Simplemente aumentar la frecuencia de la CPU ya no es factible debido al problema de enfriamiento. Por lo tanto, los principales fabricantes de chips han

detenido sensatamente la investigación sobre chips de alta frecuencia. En su lugar, han comenzado a investigar la arquitectura multinúcleo de baja frecuencia. Cavium, un conocido fabricante de procesadores, lanzó un procesador de red de 48 núcleos en 2012 [8]. AMD planea lanzar un procesador multinúcleo de 128 hilos en 2019 [22].

El desarrollo de procesadores multinúcleo también conlleva desafíos para el diseño de sistemas operativos de red. Los sistemas operativos de red tradicionales suelen basarse en vxWorks, FreeBSD, Linux u otros sistemas operativos clásicos. Vx-Works fue diseñado como un sistema operativo integrado en tiempo real de un solo núcleo y ha sido eliminado gradualmente por los proveedores de dispositivos de red en la última década. Tanto Linux como FreeBSD se derivan de UNIX, mientras que UNIX fue diseñado originalmente para sistemas de control en lugar de sistemas de reenvío de datos. Los defectos de diseño heredados de estos sistemas operativos clásicos les dificultan disfrutar de los beneficios de los procesadores multinúcleo e incluso de muchos núcleos.

1. Alta disponibilidad

   Los sistemas operativos de red generalmente se implementan en los límites de una variedad de dispositivos de red, lo que significa que si un dispositivo de red está inactivo, todos los dispositivos conectados en la red que dependen de ese dispositivo también fallarán. Por lo tanto, los clientes generalmente tienen demandas extremadamente altas de disponibilidad de dispositivos de red. En general, se requiere que la disponibilidad de los equipos de red alcance el 99,999%, es decir, solo cinco minutos de tiempo de inactividad al año es aceptable. Actualmente, los dispositivos de red (especialmente los dispositivos de seguridad de red) tienen que manejar más rendimiento de tráfico y más

funciones, lo que hace que sea cada vez más difícil mantener una alta disponibilidad.

1. Packet Order

   Cuando un usuario accede a un sitio web, es posible que haya docenas de dispositivos de red involucrados. Si estos dispositivos no mantienen el orden de los paquetes, es posible que los paquetes de datos del usuario remitente se entreguen al usuario receptor en un orden completamente aleatorio. El desorden de paquetes activa el algoritmo de control de congestión [20] del protocolo TCP para reducir el tamaño de la ventana de transmisión TCP, lo que reduce seriamente el rendimiento del flujo de datos y afecta la experiencia del usuario. Como se mencionó anteriormente, los procesadores multinúcleo e incluso de muchos núcleos ahora son la corriente principal. Aunque los procesadores multinúcleo pueden procesar paquetes de datos en paralelo, pueden producirse graves problemas fuera de orden si no se les presta la debida consideración. Aprovechar el potencial de los procesadores multinúcleo mientras se mantiene el orden de los paquetes se ha convertido en un hueso duro de roer para los sistemas operativos de red.

   Actualmente, todos los sistemas operativos tienen que emplear bloqueos [28] para resolver estos problemas. Sin embargo, el diseño de la cerradura se ha convertido a su vez en un problema en los sistemas operativos de red. Si la granularidad de la cerradura es demasiado grande, estas cerraduras grandes se convertirán en el cuello de botella de todo el sistema para los procesadores con más y más núcleos. Si la granularidad del bloqueo es demasiado pequeña, podría provocar interbloqueos y problemas de condición de carrera, aunque el rendimiento del sistema operativo pueda mejorar. Si no se manejan adecuadamente, estos problemas afectarán significativamente la estabilidad

del sistema.

Con el fin de satisfacer las necesidades generales de los sistemas de red y resolver los problemas de los sistemas operativos tradicionales, AtomOS emplea la estructura de datos HIPE para manejar la programación global de los recursos compartidos en el sistema operativo de red. Garantiza la corrección del sistema al tiempo que aprovecha al máximo los beneficios del rendimiento multinúcleo. A continuación, se presenta brevemente la implementación de HIPE.

Varios recursos compartidos del sistema operativo se clasifican en *N* grupos.

Los recursos compartidos grandes pueden abarcar varios grupos, y los recursos compartidos pequeños pertenecen a un solo grupo (consulte la figura 10 a continuación).

Figura 10: Recursos compartidos categorizados en *N* grupos

El acceso a cada grupo de recursos se desencadena mediante eventos. Cada evento que necesita acceder a un recurso compartido se coloca en la cola sin bloqueos para el grupo de recursos correspondiente. Cuando se extrae un evento en la cola, se asigna automáticamente un núcleo de CPU para procesarlo. Dado que HIPE conserva todos los eventos en la cola sin bloqueo correspondiente de cada grupo de recursos, deben procesarse

secuencialmente y no se pueden procesar al mismo tiempo, protegiendo así los recursos compartidos.

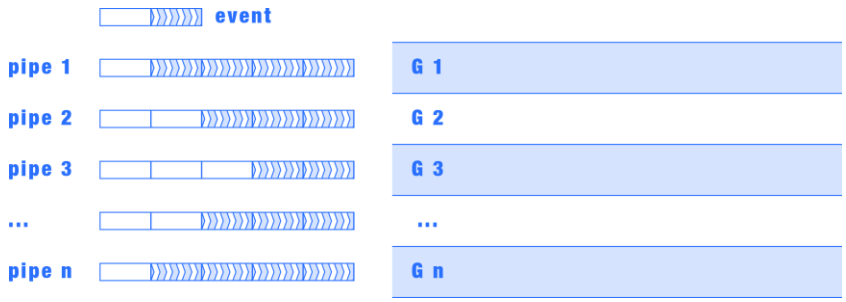

Figura 11: El acceso a cada grupo de recursos se desencadena mediante un evento en una cola sin bloqueos

1. Dado que el número de grupos de recursos en el sistema es mucho mayor que el número de núcleos de CPU, hay un flujo continuo de datos disponible para que cada CPU lo procese constantemente, lo que hace que el rendimiento de todo el sistema sea escalable con el número de núcleos de CPU.

Figure 12: Grupos de recursos procesados en paralelo por CPU

2. El diseño sin bloqueos no solo hace que el procesamiento de paquetes sea altamente escalable, sino que también evita los diversos problemas de condición de carrera que se generan como moscas cuando los procesos se ejecutan en paralelo. Además, dado que los paquetes de datos atraviesan secuencialmente la canalización HIPE, garantiza que el orden de los paquetes en un flujo de datos determinado después del procesamiento de AtomOS sea coherente con su orden original al recibir.

4.3 Deep Packet Inspection

La inspección profunda de paquetes es clave para garantizar el flujo de datos bajo

una protección integral. AtomOS proporciona seguridad de conexión para cada capa en el modelo OSI (consulte la Tabla 2), lo que proporciona a Guardnet Connect un conjunto completo de funciones de seguridad de red.

Hoy en día, el enfoque de la seguridad de la red se ha desplazado de los protocolos de capa baja a los de capa superior. Además de las diversas protecciones para las capas de red 1 a 3, AtomOS también implementa las siguientes funciones avanzadas de firewall para las capas 4 a 7:

7. Capa de aplicación	Identificación de aplicaciones, detección de flujo de datos maliciosos
6. Capa de presentación	Data encryption and decryption to prevent replay attacks
5. Capa de sesión	Comprobación de la capa de sesión de protocolo, como HTTP/SIP
4. Capa de transporte	Comprobación estricta del estado para evitar ataques de inundación
3. Capa de red	Protección contra ataques de fragmentación, protección contra la suplantación de IP
2. Capa de enlace de datos	Protección contra la suplantación de ARP
1. Capa física	Retención de la conexión durante un corte de energía

Tabla 2: OSI 7-Protección de capas en profundidad

- Comprobación estricta del estado de TCP para evitar posibles enmascaramientos y secuestros de TCP: para cada conexión TCP, AtomOS realiza un seguimiento de su estado en la tabla de sesión, y solo se reenviarán los paquetes que satisfagan estrictamente la máquina de estado TCP. Al mismo tiempo, se hizo referencia a los casos de prueba de firewall de NSS Labs autorizados en la industria durante la implementación para garantizar la contención de los diversos métodos de evasión TCP conocidos.

- Identificación de aplicaciones y control de flujo: AtomOS integra un motor de identificación de aplicaciones que es confiable, eficiente y escalable. Identifica el tráfico de red común y realiza un control de flujo o enrutamiento inteligente para optimizar la experiencia del usuario para aplicaciones clave. Además, garantiza un servicio de túnel fluido sin consumir excesivos recursos locales.

- Filtrado de URL: AtomOS puede filtrar automáticamente sitios web maliciosos (incluidas descargas de malware, sitios web de phishing, etc.) para proporcionar un entorno de Internet seguro. Los usuarios también pueden habilitar los controles parentales para calificar el contenido de Internet y asignar los niveles de acceso adecuados a cada miembro de la familia.

- Traducción de direcciones de red y puertos (NAPT): De forma predeterminada, AtomOS evita la traducción de direcciones y puertos de red para los flujos internos, para que sea un acceso a Internet de configuración cero en vivo por cable. Sin embargo, en algunas situaciones, AtomOS puede utilizar el modo simétrico de NAPT para ocultar aún más la estructura de la red interna si es necesario.

5 Networking

Además de la función de inspección de paquetes Guardnet descrita en la Sección 4.3, Guardnet también diseñó de forma independiente el protocolo Trident, la tunelización adaptativa, el enrutamiento inteligente, la multiplexación IP y el control de congestión de la capa de túnel. Estas tecnologías proporcionan la inspección de paquetes más profunda y la mejor experiencia de usuario.

5.1 Trident Protocol

El objetivo de la tecnología de tunelización de Guardnet (implementada por el protocolo Trident) es eludir la censura de la red. Por diversas razones, algunos gobiernos de todo el mundo están llevando a cabo con mayor frecuencia una inspección y un filtrado profundos del tráfico de la red de los usuarios [19]. La censura de red se basa en firewalls o dispositivos de análisis de tráfico fuera de línea desplegados en el límite de las redes centrales. Por lo tanto, para presentar la función de omisión del protocolo Trident, revisemos la funcionalidad de los firewalls. En la actualidad, los modos cortafuegos han ido evolucionando desde la lista básica de control de acceso basada en puertos hasta la identificación avanzada de aplicaciones basada en contenido. El modo avanzado se puede implementar de las siguientes maneras. Los primeros cuatro enfoques pertenecen al método de identificación pasiva y el último es proactivo. Algunos firewalls pueden emplear varios enfoques para identificar aplicaciones de flujos de datos de usuario. Además, algunos enfoques de inteligencia artificial, como el teorema de Bayes [45] o el árbol de decisión [43], podrían emplearse para realizar la identificación de aplicaciones.

1. Filtrado básico de puertos

   El filtrado básico de puertos hace referencia al enfoque de identificación de aplicaciones que se basa en el puerto de destino. La Autoridad de Números Asignados de Internet (IANA, por sus siglas en inglés) [17] es la organización que asigna los puertos de red y sus correspondientes aplicaciones de red. A partir de ahora, casi todos los puertos del 0 al 1024 han sido asignados [27]. Los cortafuegos son capaces de obtener una idea básica de las aplicaciones de usuario simplemente basándose en los puertos de red. Por ejemplo, el puerto de destino comúnmente utilizado por el protocolo NFS es 2049. Incluso sin un patrón de contenido claro, los firewalls pueden identificar la aplicación en función del puerto de destino específico.

1. Identificación de contenido

   La identificación de contenido se refiere al enfoque de identificación de aplicaciones que se basa en el contenido de los flujos de datos. Dado que las aplicaciones de red tienen que seguir el protocolo de red predefinido, los flujos de datos tienden a tener un patrón de contenido distinto. Por ejemplo, los comandos comúnmente utilizados por HTTP (GET/POST, etc.) siempre aparecen como el primer paquete después del protocolo de enlace TCP. Además, la primera línea de datos siempre termina con HTTP/X.X (la versión HTTP utilizada). Los firewalls son capaces de identificar las aplicaciones HTTP que se producen en un puerto de destino determinado en función de este patrón. Del mismo modo, todos los protocolos estándar tienen un patrón de contenido identificable. En el caso de algunos protocolos no estándar, los patrones de contenido pueden cambiar debido a las actualizaciones de la versión del protocolo, por lo que los firewalls también tienen que actualizar regularmente sus bases de datos de patrones de contenido para adaptarse a estos cambios.

1. Identificación de la longitud del paquete

   La identificación de la longitud del paquete se refiere al enfoque de identificación de la aplicación basado en el orden de la longitud del paquete o la distribución de la longitud del paquete en los flujos de datos. Este enfoque funciona muy bien, especialmente cuando no se dispone de un patrón de contenido claro para los flujos de datos. La longitud del paquete atravesado entre el cliente y el servidor generalmente sigue algún patrón en la fase de negociación de un protocolo de red. Si un protocolo de red especifica durante la fase de negociación que el cliente tiene que enviar un paquete TCP con una longitud de carga útil de 60 bytes como solicitud, el servidor tiene que enviar un paquete de 40 bytes como respuesta

seguido de otro paquete de 20-30 bytes. En este caso, el protocolo de red tiene un patrón claro en términos de longitud de paquete, que puede ser fácilmente identificado por un firewall. Con el fin de evadir la identificación de la longitud del paquete, las aplicaciones deben codificar o cifrar los paquetes de datos para ocultar el patrón de longitud del paquete.

1. Identificación de intervalos de paquetes

   La identificación de intervalos de paquetes se refiere al enfoque de identificación de aplicaciones basado en paquetes de mantenimiento periódicos especificados en un protocolo de red. En el protocolo de tunelización, el servidor y el cliente necesitan enviar periódicamente paquetes keepalive para supervisar la disponibilidad del túnel. Los paquetes keepalive generalmente se envían a un intervalo fijo y su tamaño es bastante pequeño. Los protocolos de tunelización no estándar siguen manteniendo este patrón. Como resultado, los firewalls utilizados para la censura de red pueden identificar y bloquear las aplicaciones de tunelización basadas en este patrón.

1. Identificación de detección activa

   La identificación de detección activa significa que el firewall actúa como intermediario para modificar el contenido del paquete de datos entre el cliente y el servidor, e identificar la aplicación de acuerdo con el contenido del paquete de datos devuelto por el servidor. Por ejemplo, los canales de control IRC suelen ser utilizados por el malware [41]. A pesar de que se ajustan al protocolo IRC estándar (un protocolo de chat en red especificado por IETF), no admiten la mutación simple de los comandos IRC de uso común. Basándose en este patrón, los firewalls pueden enviar solicitudes de forma proactiva y analizar la respuesta del servidor para distinguir si la aplicación de red es un software de chat normal o un malware. Este enfoque permite a los firewalls supervisar el contenido

de los flujos de datos, pero también modificar o enviar paquetes de datos de forma proactiva para la identificación de aplicaciones.

Apuntando a todos los enfoques de identificación anteriores, el protocolo Trident combina dos

Modos de túnel para evitar cualquier intento de identificación del cortafuegos: modo de ofuscación de protocolo y modo de camuflaje de protocolo. Dado que los firewalls no pueden identificar ningún patrón de tráfico en el modo de ofuscación de protocolo, la censura de Internet no es posible. Sin embargo, para los sistemas con lista blanca, todas las aplicaciones no identificables también se bloquean. En este caso, el protocolo Trident cambiará automáticamente al modo de camuflaje de protocolo para eludir la censura de Internet.

1. Modo de ofuscación de protocolo.

    - Puerto aleatorio
        - Negociar aleatoriamente el puerto de sesión de datos.
    - Contenido encriptado
        - Todo el contenido de los paquetes está encriptado.
        - Asegúrese de que las características del contenido no se puedan expresar en expresiones regulares (regex).
    - Ofuscación de la longitud del paquete
        - Todas las longitudes de los paquetes son aleatorias.
    - Sin paquetes de datos de mantenimiento periódicos
        - Paquete de datos a cuestas paquete keepalive.
        - No existen paquetes de datos keepalive independientes.
    - Evitar la detección activa

- Los servidores se niegan a responder a los paquetes que no siguen las especificaciones del protocolo.

2. Modo de camuflaje de protocolo. Hay dos modos de camuflaje disponibles:
    1. Protocolo HTTP
        - El protocolo de tunelización está completamente encapsulado en un cuerpo de mensaje "HTTP GET" y "HTTP POST". El comando "GET Response" se utiliza para recibir datos descendentes y el cuerpo del mensaje POST se utiliza para enviar datos ascendentes. Dado que el cliente y el servidor negocian el puerto de antemano, no hay ningún patrón de nombre de cadena específico disponible en los campos HTTP.
    1. Protocolo TLS
        - En este modo, se utiliza la función de ticket de sesión de TLS 1.2. El tráfico de tun- nel es como una conexión HTTPS estándar que utiliza el ticket de sesión negociado. Dado que no hay una fase de negociación, el firewall no puede descifrar ni cifrar como intermediario. AtomOS también utilizará mecanismos de encriptación y anti-identificación similares al modo de ofuscación de protocolo descrito anteriormente.

Otro problema común con las redes P2P es el cruce de NAT [35]. NAT es una función común de los dispositivos de red en un entorno de red IPv4. Los dispositivos de red suelen configurarse con direcciones IP privadas en LAN. Sin embargo, para transmitir paquetes a Internet, la dirección IP de destino y la dirección IP de origen del paquete deben traducirse a direcciones IP públicas. Para resolver esta contradicción, el dispositivo de red que sirve como puerta de enlace puede usar NAT para convertir la

dirección IPv4 privada en la dirección IP pública de la puerta de enlace cuando los paquetes de datos viajan de la LAN a Internet. Este enfoque no solo resuelve el problema de limitación de las direcciones IPv4, sino que también satisface el requisito de las organizaciones de ocultar la estructura de la red interna y aislar las redes externas. En la práctica, Guardnet Connect podría colocarse detrás del dispositivo NAT de los proveedores de servicios y asignarle una dirección IP privada. Sin embargo, eso haría que Guardnet Connect no pudiera recibir solicitudes de conexión de dispositivos de Internet. Utilizamos las siguientes técnicas para resolver este problema:

- Si el lado receptor de la conexión tiene una dirección IP privada y el remitente tiene una dirección IP pública, el receptor inicia las solicitudes de conexión a la inversa.
- Si ambas partes utilizan direcciones IP privadas, se requiere además la identificación del tipo NAT para determinar la forma correcta de iniciar la solicitud de conexión. AtomOS implementa un protocolo similar al protocolo STUN (RFC3489 [44]). El dispositivo de red es capaz de identificar el tipo de NAT y publicarlo junto con otra información sobre el nodo durante la etapa inicial del registro de red. La eventualidad de que ambos dispositivos de red utilicen NAT simétrica o NAT de cono restringido por puerto se puede evitar al configurar la conexión. Para los otros tipos de NAT (NAT de cono o NAT de cono restringido), la configuración de la conexión debe proporcionar una solución.

5.2 Tecnología de túnel adaptivo

Guardnet Connect utiliza un protocolo de tunelización patentado eficiente, flexible y

adaptable en lugar de uno estándar como IPSEC. En el proceso de diseño e implementación de la tecnología de túneles adaptativos, hemos tomado prestado ampliamente de varias tecnologías de aceleración WAN aprobadas por la industria [52]. Dada la alta latencia, la alta tasa de pérdida de paquetes y los problemas fuera de servicio de Internet multinacional, mejoramos estas tecnologías en la capa de túnel de datos, lo que maximiza efectivamente la utilización del ancho de banda y mejora significativamente la experiencia en línea del usuario.

1. Compresión y fusión de datos adaptables

   Con la tecnología de tunelización adaptativa, Guardnet Connect puede determinar si los paquetes en el flujo de datos son comprimibles y decidir si realizar la compresión. Por ejemplo, el protocolo HTTP más común se compone principalmente de caracteres latinos, que se pueden comprimir para ahorrar aproximadamente un 70% de ancho de banda y, por lo tanto, mejorar en gran medida la eficiencia de la transmisión. Mientras tanto, dado el hecho de que MP4 y otros formatos comúnmente utilizados en el tráfico de video y audio (o protocolos de redes como HTTPS / SFTP que usa cifrado SSL y TLS) ya se han acercado al límite teórico de la entropía de la información [47], la compresión adicional solo aumentaría el consumo de CPU sin ahorrar ancho de banda, lo que resultaría en un procesamiento de compresión y, a su vez, una reducción de la velocidad de transmisión. Por lo tanto, la tunelización adaptativa debe identificarse y procesarse en consecuencia en función del contenido para la eficiencia de la CPU y el ancho de banda.

   A través de la tecnología de tunelización adaptativa, Guardnet Connect también puede mejorar la eficiencia de transmisión mediante la combinación de pequeños paquetes de datos. Muchos protocolos de red tienen una gran cantidad de paquetes de control con pocos o ningún dato en la carga útil. Tomando como

ejemplo un flujo de transporte HTTP de 30 KB, incluso si la pila de protocolos del cliente optimiza TCP ACK por cada dos paquetes, el 40% de los paquetes siguen siendo inferiores a 100 bytes. Una proporción tan grande de paquetes que contienen una cantidad muy pequeña de datos provoca un retraso considerable en la eficiencia de la transmisión. Para una eficiencia de transmisión óptima, la tecnología de tunelización adaptativa puede combinar o comprimir y transmitir paquetes de datos de múltiples flujos de datos sin afectar la latencia de la conexión TCP (consulte la Figura 13).

1. Control de tráfico basado en aplicaciones

   El control de tráfico basado en aplicaciones funciona de acuerdo con el tipo de aplicación del flujo de datos, para garantizar que las aplicaciones sensibles a la latencia o al volumen disfruten de un mayor nivel de QoS. En una red doméstica, el ancho de banda suele ser limitado. Cuando se utilizan varias aplicaciones simultáneamente, la demanda de ancho de banda suele ser

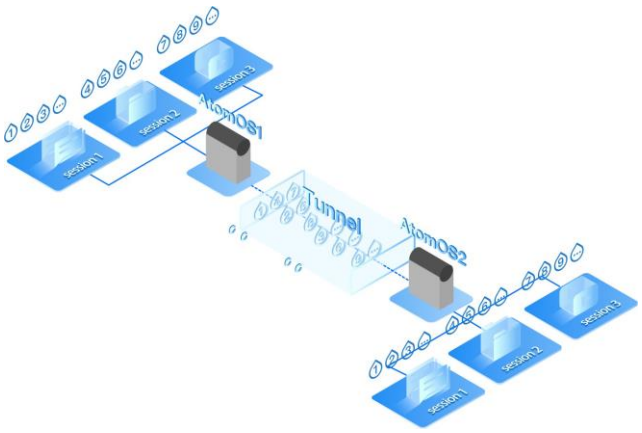

Figure 13: Consolidación automatizada de paquetes, esquema de transferencia comprimida

mucho más grande de lo que está disponible. Para solucionar este problema de

asignación, el ajuste adaptativo puede determinar automáticamente el tipo de aplicación de acuerdo con el flujo de datos del usuario y otorgar el nivel de QoS correspondiente. Por ejemplo, la navegación web o las descargas de correo electrónico deben clasificarse como sensibles a la latencia, mientras que las aplicaciones como las descargas de archivos no lo son. La tunelización adaptativa primero estima automáticamente el ancho de banda real del túnel de red y sus requisitos de ancho de banda. Si la demanda supera el suministro, la tunelización adaptativa controlará el uso del ancho de banda en función del nivel de QoS de la aplicación. Las aplicaciones de nivel inferior se almacenarán temporalmente en búfer en una cola de paquetes limitada. Si la cola de paquetes está llena, se descartarán los paquetes de desbordamiento. Aunque el uso general de la aplicación puede verse afectado debido al aumento de la latencia y la pérdida de paquetes, la experiencia general del usuario mejora significativamente.

5.3 Tecnología de enrutamiento inteligente

El enrutamiento inteligente se refiere a la configuración automática del enrutamiento de red en función de las características del flujo de datos y de si se debe transmitir a través de un túnel. Ofrecemos dos modos, un

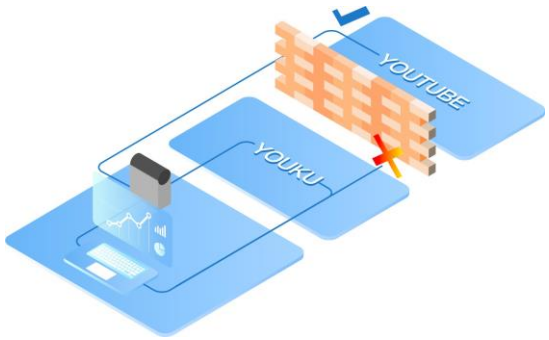

Figura 14: Enrutamiento inteligente

modo de protección de la privacidad y un modo de elusión de la red. El modo predeterminado es el modo de elusión de red.

- Modo de protección de la privacidad: En este modo, todos los flujos de datos relacionados con el rastreo de la navegación en línea se procesarán a través del túnel en función del nivel de anonimato establecido por el usuario.
- Modo de elusión de red: En este modo, todos los flujos de datos en línea se procesarán a través del túnel dependiendo de si la base de datos del sitio web muestra o no si está bloqueada en el área local.

El enrutamiento inteligente proporciona a los usuarios las siguientes ventajas:

1. Ahorros monetarios

   Los túneles de red son establecidos por dos o más Guardnet Connects. Cuando un Guardnet Connect intenta conectarse con otro para establecer un túnel, se requiere el pago en criptomoneda (calculado de acuerdo con el ancho de banda y el volumen de tráfico) a través de la plataforma de red compartida segura. Obviamente, los servicios de tunelización no pueden ofrecerse de forma gratuita. El enrutamiento inteligente determina automáticamente si se debe transmitir a través del túnel de acuerdo con los atributos del flujo de datos. Este enfoque no solo reduce la cantidad de uso del túnel, sino que también evita la latencia causada por el túnel, lo que proporciona una mejor experiencia en línea sin incurrir en gastos adicionales.

1. Servicio de anonimato

   El servicio de anonimato se refiere a ocultar la dirección IP del usuario para eludir el seguimiento. Dado que el túnel de red está cifrado de extremo a

extremo, el flujo de datos transmitido a través de él no dejará rastro. Estableceremos los niveles de acuerdo con la visibilidad de los objetos de acceso del usuario y, en función de la configuración del usuario, decidiremos si realizar la encapsulación en el flujo de datos correspondiente. Los flujos de datos de usuario altamente visibles, como las visitas a páginas web, se encuentran en el nivel más alto de servicio de anonimato. Para este nivel del flujo de datos de usuario, la encapsulación es obligatoria. Los flujos de datos de usuario menos disponibles públicamente, como las descargas P2P, pertenecen al segundo nivel más alto de servicios anónimos. Para este nivel, la encapsulación es una configuración opcional para reducir los costos de usuario. No solo eso, los usuarios también pueden elegir un modo de enrutamiento de múltiples saltos para servicios de anonimato más rigurosos. En un entorno de enrutamiento de varios saltos, el túnel de red se establecerá mediante varias conexiones más profundas en lugar de las dos habituales. La ventaja de esto es que Guardnet Connect, como nodo intermedio, no puede echar un vistazo al contenido porque no puede descifrar el flujo de datos del usuario. El último nodo de Guardnet Connect puede descifrar el flujo de datos del usuario, pero no puede conocer el origen. Por lo tanto, cuantos más nodos de Guardnet Connect haya en la ruta, más difícil será realizar un seguimiento de las actividades de los usuarios.

5.4 Tecnología de Multiplexación IP

AtomOS es el primer sistema operativo de configuración cero del mundo que puede implementar enrutamiento inteligente y encapsulación de túnel en modo de cable virtual. Todos los dispositivos de red actualmente en el mercado que implementan la función de túnel funcionan en modo de enrutamiento. Es decir, el usuario debe tener cierta tecnología de red, así como conocimientos prácticos de planificación de

direcciones IP y configuración del protocolo de túnel para establecer correctamente el túnel. También requiere una cierta cantidad de conocimientos de enrutamiento para reenviar el tráfico requerido al túnel para una encapsulación y desencapsulación adecuadas. AtomOS cambia esto por completo, ya que no se requieren conocimientos profesionales de los usuarios de Guardnet Connect. Después de que el usuario conecte el dispositivo AtomOS al enlace ascendente del router doméstico, AtomOS entrará en la fase de aprendizaje. No afecta al reenvío del tráfico, y determina automáticamente la dirección de su conexión de acuerdo con las reglas estadísticas de las direcciones IP que aparecen en los dos puertos. Hay cientos de millones de nodos en Internet, mientras que el número de direcciones IP locales es relativamente pequeño y fijo. Entonces, después de analizar brevemente el tráfico, podemos decir cuál es el puerto de enlace ascendente y cuál el enlace descendente. AtomOS procederá a aprender la dirección IP/MAC del enlace ascendente, el servidor DNS y otra información para la futura negociación y encapsulación del túnel.

Creemos que la puerta de enlace doméstica inteligente en sí misma es un producto con una frecuencia de operación de usuario muy baja. No es necesario que los usuarios sean conscientes de su existencia la mayor parte del tiempo, y se requiere poca configuración para alterar las funciones. Especialmente en combinación con nuestra exclusiva tecnología de enrutamiento inteligente, la privacidad del usuario y los requisitos de transmisión de red se cumplen al menor coste y sin ninguna curva de aprendizaje.

5.5 Control de la congestión de túneles

Uno de los principales casos de uso de Guardnet Network es proporcionar a los usuarios el anonimato de la red, lo que protege su privacidad y les permite acceder abiertamente al contenido de Internet sin ser censurados o bloqueados. En el servicio de anonimato (como se muestra en la Figura 15), el usuario transmite datos a través del túnel seguro de AtomOS entre los nodos de Guardnet, de modo que el servicio de Internet al que se accede no puede rastrear los datos privados del usuario (por ejemplo, dirección IP, ubicación). Al mismo tiempo, dado que los paquetes de datos en el túnel de AtomOS están estrictamente encriptados, los cortafuegos de censura están efectivamente cegados e incapaces de identificar el contenido de Internet al que accede el usuario.

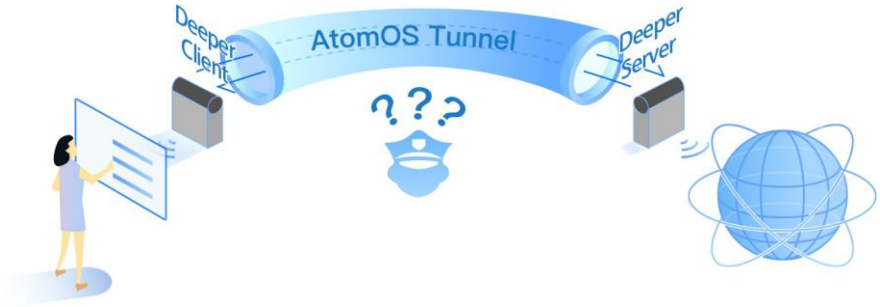

Figura 15: Servicio compartido seguro (SSS)

A través de la combinación de la seguridad de red única de Guardnet y las tecnologías de cadena de bloques, SSS garantiza de manera efectiva la seguridad y estabilidad de los servicios de anonimato de Guardnet Network. Sin embargo, la eficiencia de la transmisión de datos en el túnel AtomOS sigue siendo una pregunta abierta. Con SSS, hay dos desafíos principales para la transmisión de datos:

1. El SSS está destinado principalmente a acceder a contenidos de Internet en

otros países o regiones. La transmisión de datos a larga distancia, el gran retraso en la transmisión y la alta tasa de pérdida de paquetes o desorden son problemas asociados con este tipo de acceso internacional a Internet.

2. Aunque los paquetes en el túnel de AtomOS están estrictamente encriptados y, por lo tanto, los cortafuegos de censura no pueden identificarlos, los firewalls pueden adoptar una política de caída aleatoria de paquetes (por ejemplo, 1% de caída aleatoria de paquetes) para flujos de datos no reconocidos con el fin de degradar su experiencia de usuario.

Para hacer frente a los desafíos anteriores, Guardnet es pionera en un protocolo de transmisión fiable y orientado a la conexión en la capa del túnel. Esto es principalmente para resolver el problema de la eficiencia de la transmisión de datos en SSS desde la perspectiva del control de la congestión de la red. El conjunto completo de soluciones de control de congestión en la red más profunda se denomina TBBR (ancho de banda de cuello de botella de túnel y tiempo de propagación de ida y vuelta). Se compone de dos partes principales: 1) Implementar el nuevo algoritmo de control de congestión llamado BBR en el túnel AtomOS para que, en caso de una alta tasa de pérdida de paquetes, el túnel AtomOS pueda mantener una alta velocidad de transmisión y una baja latencia de transmisión; 2) Permitir la detección y retransmisión rápida de pérdida de paquetes, a fin de adaptarse mejor a la alta tasa de pérdida de paquetes en SSS. TBBR se centra principalmente en mejoras en el lado del remitente. No es necesario que el lado del receptor realice ningún cambio. El emisor no confía en ninguna retroalimentación adicional del receptor. Este es uno de los principios de diseño importantes de TBBR. Permite una implementación más fácil de TBBR, ya que no se requieren cambios desde el lado del receptor. Y lo que es más importante, en el escenario de alta latencia y alta tasa de pérdida de paquetes de

SSS, cualquier retroalimentación adicional del lado del receptor sin duda aumentará la carga de la red, y en tal caso entorno, no se puede garantizar una retroalimentación estable.

Traditional congestion control algorithms (such as CUBIC [16], TCP Vegas [6], TCP Reno [37]) are usually based on packet loss events. Packet loss is treated as a signal of network congestion. These kinds of algorithms control data sending rate via a sending window. The window size $W(t)$ at time t is controlled by the AIMD

(Additive-Increase/Multiplicative-Decrease) algorithm:

$$W(t+1) = \begin{cases} W(t) + \alpha & \text{if no packets loss is detected} \\ W(t) * \beta & \text{otherwise} \end{cases}$$

(1)

Claramente, el algoritmo AIMD tiende a seguir aumentando el tamaño de la ventana (es decir, la velocidad de transmisión) hasta que se detecta la pérdida de paquetes. Una vez que se detecta la pérdida de paquetes, el tamaño de la ventana experimentará una fuerte caída. Esto conduce a dos problemas principales:

1. Es contraproducente tratar todos los eventos de pérdida de paquetes como señales de congestión de la red. De hecho, la pérdida de paquetes también puede deberse a errores de red. Además, cuando se utiliza SSS, los firewalls de censura también pueden descartar paquetes deliberadamente. De acuerdo con el algoritmo AIMD, cuando se produce una pérdida de paquetes, la velocidad de transmisión se reduce drásticamente. Cuando la tasa de pérdida de paquetes alcanza un cierto nivel (por ejemplo, una pérdida de paquetes del 1% causada por los cortafuegos de censura), toda la transmisión de la red se atasca.

2. Dado que AIMD sigue aumentando la velocidad de transmisión hasta que se detecta la pérdida de paquetes, dicho mecanismo tiende a llenar todo el búfer de red (es decir, la cola). Cuanto mayor sea el número de paquetes en espera en la cola, mayor será el retraso en la cola. Dado que los precios de la memoria son cada vez más baratos en los últimos años, el espacio de búfer de la red está aumentando en consecuencia, lo que provoca enormes retrasos en las colas.

Se puede ver que los algoritmos tradicionales de control de congestión no logran ni una velocidad de transmisión óptima ni una latencia de red óptima.

Guardnet implementa un nuevo tipo de algoritmo de control de congestión llamado TBBR en el túnel de AtomOS. TBBR se desarrolló en base al algoritmo BBR [7] combinado con tecnologías de tunelización. BBR fue introducido por primera vez por Google y ha sido ampliamente utilizado en la WAN (Red de Área Amplia) de Google. A diferencia de los algoritmos tradicionales de control de

congestión, TBBR/BBR ya no se basa en eventos de pérdida de paquetes como señales de congestión de la red, sino que vuelve a la esencia de la congestión de la red: el lado del remitente transmite datos más rápido de lo que la capacidad de la red puede manejar. Con el fin de medir la capacidad actual de la red, TBBR/BBR mide continuamente dos métricas clave, a saber, BtlBw (ancho de banda de cuello de botella) y RTprop (tiempo de propagación de ida y vuelta). Si el trayecto de la red fuera una tubería de agua, la anchura de banda del cuello de botella BtlBw sería el diámetro mínimo y el tiempo de propagación de ida y vuelta RTprop sería la longitud. La capacidad de toda la red, es decir, BDP (Bandwidth Delay Product), es el producto de los dos:

$$BDP = BtlBW * RTprop \quad (2)$$

BDP también se puede interpretar como la cantidad máxima de datos pendientes que se pueden transportar en la red sin causar ningún retraso en la cola (es decir, sin ocupar ningún espacio de búfer).

La idea principal de TBBR/BBR es que cuando la tasa de llegada de datos en el cuello de botella de la red es igual a BtlBw y la cantidad de datos en tránsito en la red es igual a la capacidad de la red BDP, la red está funcionando en el estado óptimo de máximo rendimiento y mínima latencia. TBBR/BBR controla la velocidad de transmisión midiendo BtlBw y RTprop. Vale la pena señalar que la capacidad de toda la red está cambiando dinámicamente. Por lo tanto, TBBR/BBR debe medir continuamente BtlBw y RTprop para actualizar la velocidad de transmisión. Además, BtlBw y RTprop no se pueden medir al mismo tiempo. Para medir BtlBw, se debe llenar el búfer de red para obtener el máximo rendimiento; para medir RTprop, el búfer de red debe estar lo más vacío posible (es decir, sin retraso en la cola) para obtener una latencia mínima. Para abordar este problema, TBBR/BBR mide las dos métricas alternativamente y las estima por utilizando los

valores muestreados durante una determinada ventana de tiempo WR en el momento T :

$$\hat{Btl}Bw = \max(r_t), \forall t \in [T - W_R, T] \quad (3)$$

$$\hat{RT}prop = \min(RTT_t), \forall t \in [T - W_R, T] \quad (4)$$

Donde rt es la velocidad de transmisión de datos medida *en el tiempo t*, y $RTTt$ es el tiempo de ida y vuelta medido en el tiempo t.

TBBR/BBR possesses the following two properties:

1. A una cierta tasa de pérdida de paquetes, TBBR/BBR aún mantiene una velocidad de transmisión estable que está cerca del ancho de banda de la red.

2. Mientras se mantiene el rendimiento máximo, TBBR/BBR tiende a no ocupar el búfer de red y, por lo tanto, reduce el retraso en la cola.

Google ha implementado BBR en sus servidores Google.com y YouTube. BBR ha reducido por completo la latencia media de transmisión de la red de YouTube en un 53%. En los países en desarrollo, este valor llega al 80% [7].

Guardnet ha trasplantado la exitosa experiencia de BBR a la aplicación de SSS, e implementado TBBR, el primer control de congestión de túneles del mundo, en el túnel AtomOS. Con TBBR, descubrimos que Guardnet Connect reduce eficazmente el retraso del acceso internacional a Internet al tiempo que mantiene una velocidad de transmisión de red estable cuando los cortafuegos provocan deliberadamente caídas de paquetes.

La Figura 16 compara el rendimiento de la red del túnel AtomOS con TBBR y el del túnel tradicional IPSEC sin control de congestión bajo diferentes tasas de pérdida de

paquetes. La configuración experimental es 1 Flujo de datos, BtlBW = 100Mbps, y RTT = 100ms. La curva gris en la parte superior representa la velocidad de transmisión ideal, i.e., BtlBW * (1 -

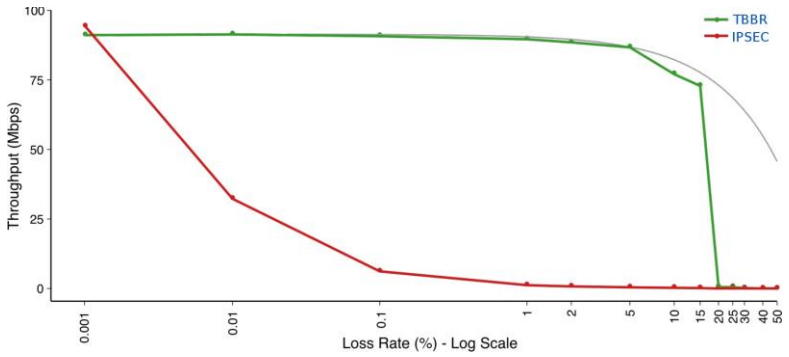

Figura 16: Rendimiento de la red a diferentes tasas de pérdida de paquetes

p) , donde *p* es la tasa de pérdida de paquetes. Como podemos ver en la figura, una tasa de pérdida de paquetes muy pequeña (0.01%) puede hacer que el rendimiento de IPSEC caiga a solo un 30 % de ancho de banda. A medida que aumenta la tasa de pérdida de paquetes, IPSEC tiene un rendimiento de solo el 5% del ancho de banda restante, donde la transmisión está casi en pausa. En marcado contraste, el rendimiento del túnel AtomOS se mantiene cerca del rendimiento ideal incluso con una tasa de pérdida de paquetes extrema del 5%. Con una pérdida de paquetes del 15 %, el túnel AtomOS aún mantiene un ancho de banda del 75 %. En SSS, suponiendo que los firewalls de censura descarten aleatoriamente el 1% de los paquetes no reconocidos, el rendimiento del túnel AtomOS prácticamente no se vería afectado y se mantendría cerca del rendimiento ideal; mientras que IPSEC tendría un rendimiento de solo el 5% del ancho de banda restante.

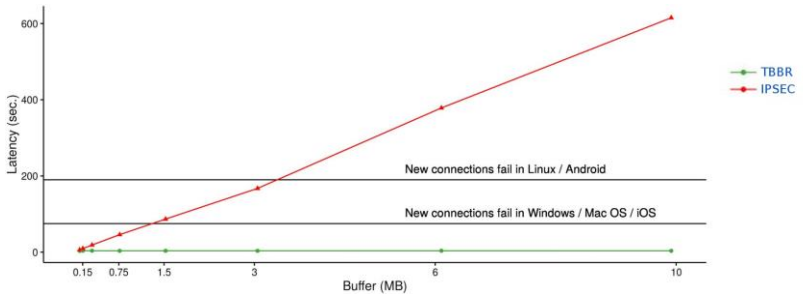

Figura 17: Latencia de red para diferentes tamaños de búfer

La Figura 17 compara la latencia de red del túnel AtomOS e IPSEC en diferentes tamaños de búfer. La configuración experimental es de 8 flujos de datos, BtlBW = 128 kbps y RTT = 40 ms. El túnel IPSEC tradicional tiende a ocupar todo el espacio del búfer de red, lo que hace que la latencia aumente linealmente con el tamaño del búfer. Peor aún, si la latencia es mayor que el tiempo de espera de la conexión inicial de red (SYN) establecido por diferentes sistemas operativos, hará que la conexión falle. En marcado contraste, el túnel AtomOS siempre mantiene la latencia al mínimo, independientemente del tamaño del búfer.

Además de BBR, el túnel AtomOS implementa optimizaciones adicionales para la detección y retransmisión rápida de pérdida de paquetes.

El TCP tradicional maneja principalmente la pérdida de paquetes de dos maneras:

1. Si el acuse de recibo (ACK) de un paquete no se recibe dentro de un cierto período de tiempo, es decir, el tiempo de espera de retransmisión (RTO), el paquete se considera perdido y se activa la retransmisión.

2. En lugar de esperar a que se agote el tiempo de espera, si se reciben tres confirmaciones duplicadas del receptor, el remitente también considera que un paquete se ha perdido y activa la retransmisión. Este mecanismo se denomina retransmisión rápida.

En TCP, cuando el receptor encuentra que se omitieron algunos paquetes, enviará confirmaciones duplicadas para recordarle al remitente que aún faltan algunos paquetes. Hay dos razones por las que se puede omitir un paquete: o se pierde o los paquetes llegaron fuera de servicio, es decir, paquetes originalmente programados después de que un determinado paquete llegara primero al lado del receptor. Cuando el remitente recibe una confirmación duplicada, no puede determinar

inmediatamente cuál de los dos escenarios ocurrió. Por lo tanto, es necesario esperar a que se produzcan más confirmaciones duplicadas para determinar que la pérdida de paquetes se produjo con una alta probabilidad. Si la pérdida de paquetes se determina prematuramente, dará lugar a una retransmisión innecesaria que aumentará la carga de la red; Por otro lado, si la pérdida de paquetes se determina demasiado tarde, provocará una respuesta lenta a los eventos de pérdida de paquetes.

Hoy en día, un mecanismo de retransmisión rápida de uso común se basa en tres ACK duplicados. Requiere que se envíen al menos 4 paquetes de datos (es decir, el tamaño de la ventana de envío es de al menos 4) para observar tres confirmaciones duplicadas; de lo contrario, el remitente solo puede confiar en el tiempo de espera de RTO para la retransmisión. Por lo tanto, el mecanismo de retransmisión rápida actual funciona mal o no funciona en absoluto en los siguientes casos:

1. Los estudios [2] han demostrado que, desde la perspectiva de la capa de aplicación, una conexión TCP a menudo necesita enviar un total de menos de cuatro paquetes de datos. En estos casos, el mecanismo de retransmisión rápida actual nunca se activará.

2. La congestión de la red puede hacer que la ventana de envío se reduzca por debajo de 4, lo que también deshabilita la retransmisión rápida.

3. En el modo de confirmación acumulativa, el receptor puede optar por retrasar el envío de confirmaciones para fusionar varias confirmaciones en una sola con el fin de ahorrar ancho de banda. En este caso, se necesitan aún más paquetes de datos para poder activar una retransmisión rápida.

Un mecanismo eficaz de retransmisión rápida debería detectar la pérdida de paquetes y activar la retransmisión a tiempo, al tiempo que se reducen las

retransmisiones superfluas. TBBR adopta un algoritmo dinámico de umbral de retransmisión rápida. En pocas palabras, si no se pueden enviar más paquetes de datos (ya sea debido al límite de tamaño de la ventana de envío o porque la capa de aplicación no tiene más datos para enviar), el umbral de retransmisión rápida se ajusta dinámicamente de acuerdo con el número de paquetes que aún no se han reconocido; de lo contrario, se utiliza un umbral de 3.

Con respecto al tiempo de espera de retransmisión RTO, TCP tradicional adopta un algoritmo llamado retroceso exponencial, es decir, si se agota el tiempo de espera de un paquete bajo el RTO actual, el paquete es

Algorithm 1 Algorithm for fast retransmission threshold τ in TBBR

```
1: Assume that the number of currently unacknowledged packets is k
2: if there are no more packets to send then
3:     τ = max(min(k − 1, 3), 0)
4: else
5:     τ = 3
```

retransmitted and the RTO is doubled. In extreme cases, if packet timeout happens n consecutive times, the RTO will explode to 2^n times the original RTO, which greatly stalls transmission rate. TBBR uses a smoother RTO growth curve that sets RTO to 1.5 times the previous value per timeout.

Although the overall design of TBBR is focused on the sender side, we can still improve network transmission efficiency from the receiver side. There are two main approaches:

1. Adopte el acuse de recibo selectivo (SACK [31]) en el lado del receptor. A diferencia del acuse de recibo acumulativo, en el que el receptor sólo retroalimenta el número de secuencia mínimo de los paquetes que aún no se han recibido, SACK permite al receptor indicar explícitamente al remitente qué paquetes se han recibido y cuáles no. El remitente puede retransmitir

selectivamente solo aquellos paquetes que aún no se han recibido. Además, si se pierden varios paquetes de datos en la ventana de envío actual, el acuse de recibo acumulativo solo informa al remitente de una pérdida de paquetes a la vez, lo que resulta en ineficiencia. SACK puede retroalimentar todos los paquetes perdidos a la vez. La investigación muestra que en redes de alta latencia y alta tasa de pérdida, SACK puede reducir en gran medida el número de paquetes retransmitidos y mejorar la eficiencia de la transmisión.

2. Ajuste dinámicamente el retraso de confirmación. Como se mencionó anteriormente, el receptor puede optar por retrasar el envío de ACK. Si bien al hacerlo se hace un mejor uso del ancho de banda, también se retrasa el reconocimiento de paquetes y se retrasa la retransmisión rápida. Especialmente en un entorno de alto retraso y alta pérdida de paquetes, es crucial que el receptor reconozca cada paquete a tiempo. Por lo tanto, en el lado del receptor, el retardo de acuse de recibo se puede ajustar dinámicamente de acuerdo con las condiciones de retardo y pérdida de paquetes de la red actual.

6 Blockchain

Hay dos capas en la cadena más profunda (Figura 18). La capa superior consta de cientos de nodos validadores como cualquier otra cadena de bloques. La capa inferior, también llamada capa Guardnet, consta de millones de dispositivos Guardnet. Estos dispositivos ganan créditos al proporcionar servicios en la red Guardnet, por ejemplo, compartir ancho de banda.

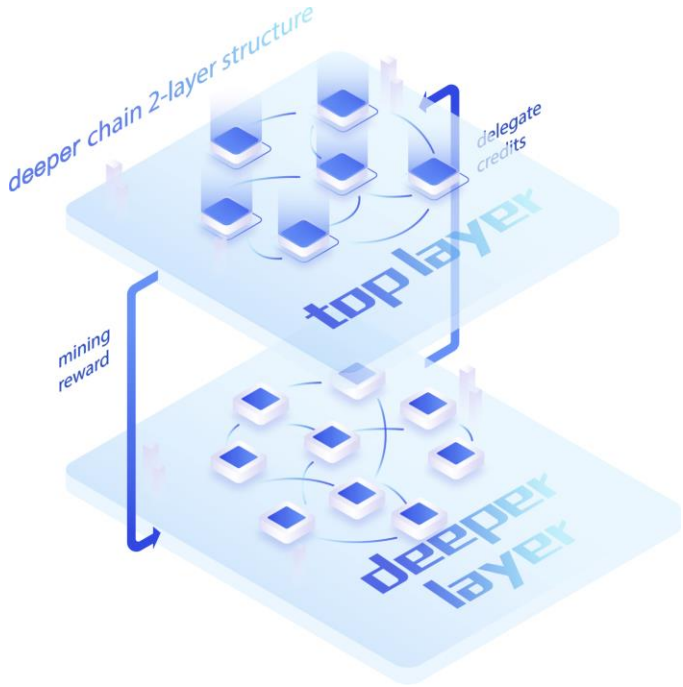

Figura 18: Estructura de 2 capas de cadena más profunda

A diferencia de los protocolos de consenso estándar de Nakamoto, nuestro mecanismo de consenso no utiliza un algoritmo de escape de hash. Nuestro mecanismo

de consenso es similar a la prueba de participación, pero el poder de voto de un validador depende tanto de los tokens apostados como del crédito delegado

Puntuaciones. Por un lado, la capa superior está asegurada por los puntajes de crédito de los dispositivos Guardnet. Cuantas más personas participen en los servicios de Guardnet, más segura será la red. Por otro lado, la recompensa de minería distribuida a los dispositivos de Guardnet incentivará a más personas a participar en los servicios de Guardnet. Este circuito cerrado aumentará y asegurará toda la red.

Con el fin de tener el desarrollo sostenible del ecosistema de Guardnet Network, hablaremos sobre el mecanismo de consenso y el algoritmo de consenso NPoW proof-of-work. El primero es garantizar la seguridad del apagón de la cadena de bloques, y el segundo es alentar a los nodos a contribuir a la red.

6.1 Mecanismo de concenso

6.1.1 Overview

Guardnet Network utiliza un mecanismo avanzado de consenso PoCr, que consta de dos mecanismos importantes (módulos): un sistema de créditos y un sistema representativo. Estos dos mecanismos forman el núcleo del mecanismo de consenso de la Red Más Profunda. A continuación, se incluye una breve descripción de cada uno de ellos.

1. Sistema de Crédito

PoCr, es decir, prueba de crédito. El sistema de crédito es el componente más importante entre los dos mecanismos básicos de PoCr. Como su nombre lo indica, refleja la contribución de cada participante en función de la puntuación crediticia de cada nodo, y distribuye recompensas en bloque en función de esto.

Hay dos formas de aumentar la puntuación crediticia: (1) apostando tokens DPR en la etapa inicial; (2) participando en el uso compartido del ancho de banda y en las actividades de red y consenso sobre la Cadena Más Profunda. (1) Está respaldado por fondos, (2) está respaldado por contribuciones de la red. Esta es la forma en que Guardnet Network construye su sistema de crédito.

Cada nodo acumula su propia puntuación crediticia apostando o participando en las aplicaciones de la cadena Guardnet, colaborando conjuntamente para resistir los ataques de Sybil. Dado que esto no se hace mediante el uso de potencia informática, recursos financieros o espacio de almacenamiento, este diseño puede reducir el consumo de energía y el desperdicio de hardware casi a cero. Asimismo, también puede motivar a cada nodo a participar en numerosas aplicaciones valiosas en la cadena, lo que puede considerarse un diseño que se ajusta a múltiples propósitos.

Podemos tomar el sistema de crédito estadounidense relativamente perfecto existente como una comparación con el sistema de crédito PoCr de Guardnet Network. En los Estados Unidos, todo el mundo tiene un SSN (Número de Seguro Social) vinculado a casi todo su historial crediticio de por vida. Cualquier persona puede usar su SSN para verificar su información personal, como edad, sexo, educación, historial laboral, impuestos, seguros, banca, antecedentes penales, etc. La Asociación de Administración de Crédito de Estados Unidos, la Asociación de Informes de Crédito y la Asociación de Cobro de Deudas de Estados Unidos utilizan datos de crédito para otorgar calificaciones crediticias a las personas y obtener límites de crédito que, en última instancia, afectan todos los aspectos de la vida de los estadounidenses. La calificación crediticia en el mecanismo de consenso de prueba de crédito es similar. Los usuarios pueden recibir diferentes incentivos de consenso y derechos de participación en la gobernanza on-chain en función de su puntuación crediticia, lo cual es muy importante. Garantiza que todos los

participantes puedan contribuir y que se les pague por sus contribuciones, lo que hace que Guardnet Network sea altamente descentralizada, más segura y más justa que la mayoría de las otras redes blockchain.

1. Sistema representativo

Antes de hablar sobre el sistema representativo de Guardnet Network, repasemos la estructura de toda la red de Guardnet Network.

Guardnet Network se compone de dos capas: los validadores en la capa superior y los dispositivos Guardnet Connect (también conocidos como nodos) en la capa inferior. Los validadores de la capa superior se encargan principalmente de generar bloques, mientras que los dispositivos o nodos Guardnet Connect de la capa inferior se encargan principalmente de supervisar y seleccionar la

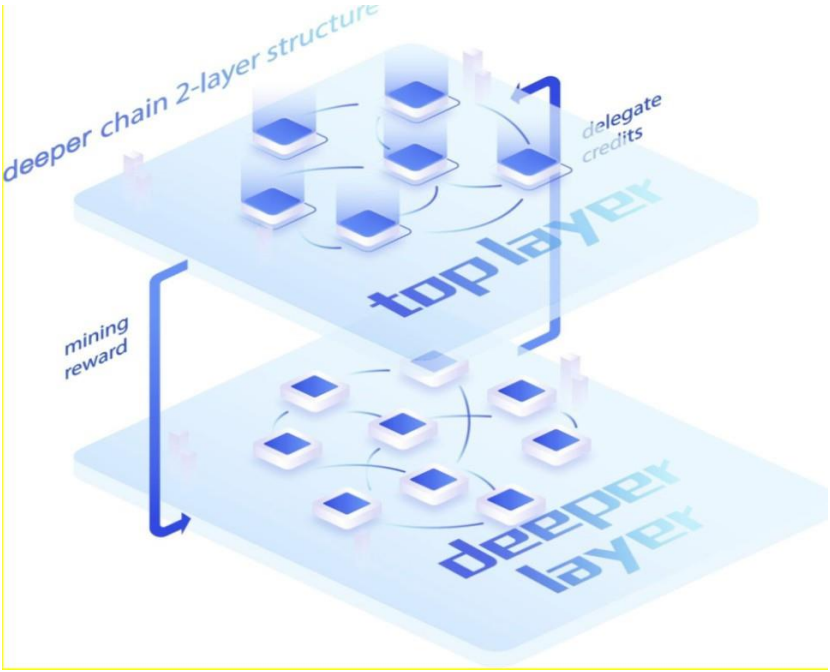

Figura 19: Guardnet chain 2-layer

estructura en los validadores de la capa superior.

Este diseño se inspira en el sistema representativo adoptado por algunos países,

es decir, los ciudadanos forman un parlamento a través de representantes electos, y el parlamento representa formalmente a la opinión pública para ejercer el poder estatal. En la cadena de Guardnet Network, el validador es seleccionado por los nodos del dispositivo a través de su oferta de puntaje de crédito, a su vez, el validador seleccionado representa al colectivo de nodos que les permite participar en la construcción del consenso de Guardnet Network.

Lo que más importa es que el nodo validador sirve al nodo de capa inferior y necesita asignar la mayor parte de las recompensas de bloque al nodo de capa inferior, que es fundamentalmente diferente de los supernodos de EOS y ecosistemas EOS similares.

Esta arquitectura también aporta dos características principales a Guardnet Network:

La primera característica importante es la escalabilidad de consenso. Proyectos tradicionales de blockchain,

como Bitcoin y Ethereum, tienen un poco más de 10.000 nodos en toda su red. El problema al que se enfrentan actualmente no es la imposibilidad de aumentar su número de nodos, sino cuánto menor será la velocidad de consenso si dichos nodos se incrementan significativamente. Por lo tanto, desde la perspectiva del consenso, es difícil que los proyectos tradicionales de blockchain continúen expandiendo el número de nodos, lo que afectará su eficiencia operativa.

Sin embargo, el sistema representativo de Guardnet Network es una arquitectura de dos capas que permite que cualquier número de participantes llegue a un consenso, y cada nodo puede participar en el consenso para obtener el incentivo correspondiente sin afectar la eficiencia, lo que refleja plenamente la equidad de la red.

La segunda característica importante es la escalabilidad de TPS (transacciones por segundo). La arquitectura de dos capas de Guardnet Network es una

arquitectura naturalmente escalable de capa 1 + capa 2. Cada dispositivo tiene su propia potencia de cálculo y es capaz de realizar transferencias de micropagos. Esta potencia de cálculo se integra en los dispositivos y se añade a la cadena Guardnet, mejorando en gran medida la eficiencia operativa de todo el sistema. Tiene características integradas para resolver el problema de escalabilidad de TPS.

Guardnet utiliza HotStuff [74] como su marco de replicación de máquina de estado (SMR). Hot-Suff es el primer protocolo bizantino tolerante a fallos (BFT) con una complejidad de comunicación lineal (es decir, $O(n)$) y una latencia de red receptiva (es decir, el tiempo de latencia depende de la velocidad real de la red). HotStuff abstrae el paradigma de la cadena de los protocolos de estilo BFT e introduce la arquitectura de canalización para mejorar en gran medida el rendimiento de la red.

A diferencia de otros protocolos BFT, donde hay diferentes formatos de votación para cada ronda (es decir, proponer, pre-enviar, enviar, etc.), cada ronda en Hotstuff ya no se trata de manera diferente. Una votación en un bloque también se puede considerar la votación de la siguiente etapa en el bloque principal al que hace referencia. Es decir, un voto sobre un bloque se considera un voto sobre el

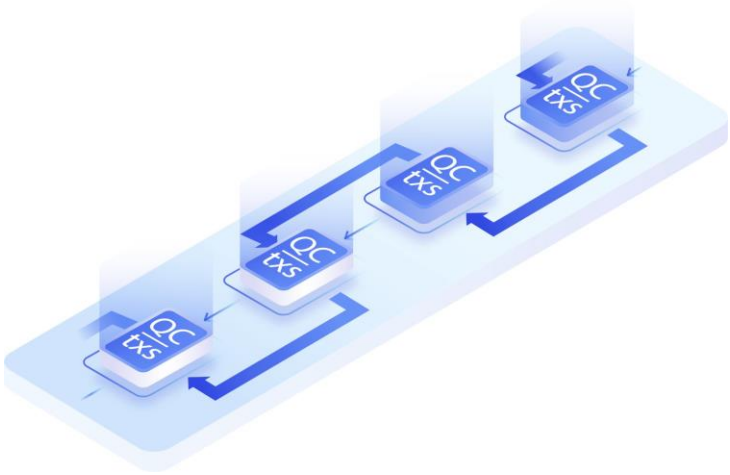

Figure 20: Arquitectura de canalización de HotStuff

propuesta del bloque en sí, así como una votación previa a la presentación en el bloque de su padre, una votación de presentación en el bloque de su abuelo y una votación decisiva en el bloque de su antepasado de tercera generación. Un bloque se ejecuta solo si su bloque de tercera generación se vota con éxito. En comparación con otros protocolos de consenso de BFT, la introducción de la arquitectura canalizada mejora el rendimiento aproximadamente tres veces.

Además, HotStuff utiliza un patrón de comunicación en estrella (es decir, todos se comunican a través del líder) y firmas de umbral para garantizar una comunicación lineal por bloque: el líder envía el bloque a los validadores, producen firmas parciales y el líder simplemente reconstruye una firma de umbral que sirve como prueba de validez del bloque. Esto le permite escalar el consenso a un gran número de validadores simultáneamente.

En Tendermint y PBFT, solo hay 2 rondas para llegar a un consenso. Al agregar 1 (una) ronda de consenso con la ayuda de una firma de umbral, Hotsuff puede actualizar la complejidad del cambio de líder a lineal y garantizar que la velocidad de producción de bloques sea el retraso real de la red. Por el contrario, la complejidad del cambio de nodo principal de PBFT *es* $O(n2)$, mientras que la velocidad de producción de bloques de Tendermint está determinada por parámetros definidos por el sistema y no es óptima en función de la velocidad de la red. La cadena más profunda proporciona una funcionalidad de protección privada del usuario, por lo que, además de la necesidad de protegerse contra los ataques de Sybil en la cadena de bloques pública, los nodos también pueden estar sujetos a prohibiciones específicas por parte de los gobiernos y los proveedores de servicios, lo que puede resultar en el bloqueo de los nodos principales. Con la complejidad

lineal del cambio de líder inicial de HotStuff, este único punto de falla no ralentizará considerablemente la red.

6.1.2 Selección de Nodos

Hotstuff en su forma básica abstrae las partes de la vitalidad y la selección de líderes del consenso. Estas funciones deben implementarse por separado en cada instancia particular de Hotstuff, dependiendo de la topología de red y la dinámica del validador. Además, Hotstuff no tiene en cuenta la rotación de los comités, que también debe implementarse por separado.

En Guardnet, la vida se logra a través de los llamados certificados de tiempo de espera. Cuando el validador espera una propuesta de bloque de un nuevo líder de ronda durante el período de tiempo de espera especificado y no llega, envía un mensaje de tiempo de espera parcialmente firmado al siguiente líder, seleccionado a través de un programa de round robin determinado. El nuevo líder, al recibir suficientes firmas parciales, produce un certificado de tiempo de espera, que transmite con un mensaje de nueva ronda a todos los validadores.

La rotación de comités se realiza en redes sin permiso para aprovechar los beneficios de los protocolos BFT y, al mismo tiempo, garantizar la robustez contra los llamados ataques adversos adaptativos. El adversario adaptativo es un modelo de amenaza, en el que el adversario es capaz de corromper dinámicamente las réplicas correctas, siempre que no controlen más de $(n-1)/3$ réplicas (o, equivalentemente, 1/3 del peso total de los validadores de red) a la vez. Se supone que el tiempo que se tarda en montar un ataque adaptativo es inferior, lo que significa que la rotación del comité debe realizarse con la frecuencia suficiente para evitarlo.

Para la rotación de comités, Guardnet utiliza una baliza de aleatoriedad basada en un VDF [5]. Los VDF son similares a los VRF: funciones criptográficas con

resultados impredecibles, que también generan una prueba que se puede utilizar para verificar la corrección del cálculo del VRF. Los VDF, además, requieren un número predeterminado de pasos secuenciales para calcular, lo que pone un límite inferior en el tiempo que se tarda en producir una salida. Al mismo tiempo, verificar un VDF es significativamente más rápido que calcularlo. La imposición de un retraso entre la adquisición de la entrada y la salida de aleatoriedad garantiza que el primer actor que pueda adquirir la salida no pueda retenerla para volver a tirar el valor de aleatoriedad.

El VDF se calcula en función de la firma de umbral para una propuesta de bloque en la ronda $k - 2$, donde k *es* el último bloque del ePoCrh. El VDF está configurado para calcularse en aproximadamente dos rondas. De esa manera, si un líder defectuoso intenta calcular un VDF por su cuenta y decide si debe retener la entrada de todos los demás, se forzará un tiempo de espera. Cuando se calcula el VDF, los miembros del comité son seleccionados por el Algoritmo 2.

Tenga en cuenta que este algoritmo implica que cada validador solo se puede seleccionar una vez por ePoCrh, y cada validador participa en la fracción de ePoCrhs igual a su fracción de peso total.

Después de seleccionar un comité, los líderes de la ronda se eligen de forma rotatoria iterando a través de C. Cada ePoCrh en Guardnet dura 17,280[1] bloques (slightly over 24 hours assuming 5 sec/block).

[1]Este valor debe ser divisible por el tamaño del comité, de modo que cada miembro del comité pueda producir un número igual de bloques por ePoCrh, lo cual es importante para la economía.

Algorithm 2 Algoritmo para la selección de los miembros del comité

R – El valor de la baliza de aleatoriedad en el ePoCrh;
$H(x)$ – a hash function;
n – El número total de validadores de staking;
m – El número total de validadores seleccionados;
W_i – El peso de la i-th Validador en consenso;
TW – La suma de todas las ponderaciones de los validadores en consenso;

$C \rightarrow \{\}$
$S \rightarrow 0$
for $k \in \{0, \ldots, m-1\}$ **do**
    $V \rightarrow H(R||k)\%(TW - S)$
    $P \rightarrow 0$
    for $i \in \{0, \ldots, n-1\}/C$ **do**
        $P \rightarrow P + W_i$
        if $V < P$ **then**
            $C[k] \rightarrow i$
            $S \rightarrow S + W_i$
            break
return C

6.2 NPoW

Guardnet Network consta de dos capas. La capa superior contiene cientos de nodos de validación que generan constantemente nuevos bloques. Y la capa inferior, la capa más profunda, está formada por millones de dispositivos que están conectados a la red más profunda. El certificado NPoW permite a los dispositivos de red Guardnet ganar tokens completando varias tareas de valor económico. Cada dispositivo estará asociado a una cuenta. Cuantas más tareas realice el dispositivo, mayor será el puntaje de crédito que obtendrá la cuenta correspondiente. Cada dispositivo puede delegar su puntuación de crédito al nodo de validación. Si más de 2/3 del total de votos de los nodos de verificación votan por un nuevo bloque, el bloque se determina. Después de que se confirme un nuevo bloque, los dispositivos

serán recompensados con tokens proporcionales a su puntaje de crédito. Al igual que el sistema de crédito en la sociedad moderna, el crédito de cada cuenta el registro C tiene un valor máximo como límite superior Cmax.

6.2.1 Visión General

La prueba de trabajo tradicional suele utilizar una función hash para realizar cálculos complejos, y su proceso exhaustivo hacia adelante es complicado. El proceso de verificación es relativamente sencillo para lograr una prueba de trabajo. Su desventaja es que la finalización del cálculo no genera un valor de beneficio real, y el resultado de su trabajo no puede proporcionar beneficios económicos para otros. Además, el mecanismo inicial de prueba de trabajo se diseñó para reducir el umbral y el proceso de prueba de participación de los usuarios y lograr un grado justo de descentralización.

Sin embargo, se desvió gradualmente de esta dirección durante su desarrollo, y la potencia de hash se concentró cada vez más en los dispositivos especializados, contrariamente al objetivo original. Por lo tanto, proponemos el mecanismo proof-to-work de próxima generación. Al hacer que los nodos completen muchas tareas económicas diferentes, el demandante quema los certificados de valor correspondientes para demostrar la carga de trabajo por medios económicos. Los resultados de su trabajo pueden aportar un valor real a otros y lograr una utilización razonable y eficaz de los recursos de hardware. La aleatoriedad y el anonimato de la distribución de tareas aseguran que no sea difícil controlar la recompensa esperada cuando se produce una trampa, y utilizar el costo económico para restringir las trampas.

6.2.2 EZC Certificado

En cuanto a las aplicaciones Web3.0, la mayoría de las partes del proyecto utilizan su token nativo para pagar las transacciones directamente, pero para los usuarios habituales, sin duda existe una alta barrera de entrada. A medida que el valor de los tokens nativos fluctúa, no puede proporcionar a los usuarios un servicio estable y predecible, lo que dificulta el crecimiento a gran escala de las aplicaciones. Por lo tanto, sobre la base de sus tokens nativos, Guardnet emite un crédito/moneda estable EZC (Easy Cent), que tiene un tipo de cambio atado al dólar estadounidense (1EZC = 0,01 USD) como medio de intercambio para el pago de solicitudes y tarifas de servicio en Guardnet Chain. Esto ayuda a promover el uso de aplicaciones on-chain a un precio estable y predecible.

Cuando los usuarios graban EZC para usar servicios de aplicaciones en cadena, se generarán los certificados de trabajo correspondientes y los nodos filtrarán y ejecutarán diferentes tareas en función de sus propias reglas de configuración. Después de completar las tareas, se emitirán los certificados de trabajo correspondientes y los nodos de servicio obtendrán recompensas del sistema en función de los certificados de trabajo acumulados. EZC es un tipo de crédito de aplicación emitido dentro del sistema, que es intransferible y no negociable. Su objetivo es satisfacer las necesidades de los usuarios que no están familiarizados con la tecnología blockchain. Los usuarios pueden obtener EZC quemando DPR. El tipo de cambio de la RPD fluctúa y la cantidad de EZC intercambiada se ajustará en función del precio de mercado de la RPD. Además, los usuarios pueden utilizar muchos tipos de métodos de pago, como tarjetas de crédito, PayPal, Apple Pay y otros para realizar compras de EZC.

6.2.3 PoCr Seguridad

La prevención de ataques Sybil es una consideración de seguridad clave en las cadenas de bloques públicas. Después de Ethereum 1.0, muchas cadenas de bloques adoptan la prueba de participación en la que un validador elegido votará por un nuevo bloque y el poder de voto es proporcional a la cantidad total de tokens que apostó. La red más profunda utiliza un enfoque similar al de Proof of Stake. El poder de voto depende no solo de los tokens apostados, sino también de los puntajes de crédito delegados. Por lo tanto, la cadena Guardnet es en realidad una mezcla de Proof of Stake y Proof of Credit. La seguridad de Proof of Stake está bien estudiada. Por lo tanto, nuestra principal preocupación es la seguridad de la prueba de crédito.

El primer paso para hacer que PoCr sea seguro es controlar el número de nodos maliciosos en Guardnet Network. Para lograr este objetivo, Guardnet aumenta la dificultad y el costo para que una parte maliciosa controle otros nodos en dos aspectos: 1) Staking tokens. Guardnet requiere que todos los dispositivos depositen algunos tokens antes de unirse a la red durante la fase de registro. Por lo tanto, si una parte maliciosa quiere controlar muchos nodos, tiene que depositar una gran cantidad de tokens, que es esencialmente el mecanismo de prueba de participación. Esto aumentará significativamente el costo de las partes malintencionadas; 2) Requisito mínimo de crédito. Un nodo tiene que alcanzar un umbral mínimo τ de créditos antes de poder unirse a la red y ganar recompensas. De esta manera, alentamos a los usuarios a participar en el uso compartido de ancho de banda para acumular créditos y también evitar que los nodos maliciosos recién creados se unan a la red de inmediato.

A continuación, analizamos la seguridad de PoCr desde la perspectiva de cómo se distribuyen las recompensas y cómo se actualizan los créditos. Supongamos que un nodo de servidor cobra pagos $[p_1, p_2, \ldots, p_m]$ de m clientes durante un tiempo de

bloque y recibe la recompensa R después de que finaliza el bloque. La tasa de comisión de la tarifa de transacción es μ. El beneficio neto P viene dado por:

$$P = R + (1 - \mu) * (p_1 + p_2 + \ldots + p_m) \tag{5}$$

Ahora analizamos la seguridad de PoCr. Supongamos que la parte malintencionada puede controlar una fracción θ *(por ejemplo,* θ = 10%) del número total de dispositivos n. Durante cada ePoCrh, suponiendo que un nodo malicioso elige aleatoriamente k vecinos, entre los cuales el número de malintencionados es una variable aleatoria X. La probabilidad de que haya i vecinos maliciosos es:

$$P(X = i) = \frac{\binom{n\vartheta}{i}\binom{n(1-\vartheta)}{k-i}}{\binom{n}{k}} \tag{6}$$

Assuming k is small relative to n (i.e., $k \ll n$), the probability to have one malicious

neighbor is close to ϑ (i.e., $P(X = 1) \approx \vartheta$) and the probability to have more than one malicious neighbor $P(X > 1)$ is much smaller than ϑ. Suppose this malicious server cannot provide service by refusing all other good peers but just collect fees from its malicious neighbors, the net profit is given by $P = R + (1 - \mu) * p_1$, assuming it can only obtain one malicious neighbor.

Design 1: Notice that the reward R is a function of credits core and which in turn is a function of $[p_1, p_2, \ldots, p_m]$. We define $R = 0$ if $m = 1$, i.e., no reward if a server only serves one neighbor. In this case, the net profit of a malicious node is negative $-\mu * p_1$ while the net profit of an honest node is positive $(1 - \mu) * p_1$. This simple design is equivalent to removing the PoCr component from our system.

Our hypothesis is that in the long term, the micropayments will close to the operational cost of a server node. Thus, by removing PoCr, the users are not incentivized enough to share their bandwidth. Since the reward is proportional to the credit scores, the credit score update function should be designed in such a way that incentivizes the node to serve more clients. When the commission ratio μ is not set to 0, the commission fee will also be compensated when a node serves multiple nodes.

Diseño 2: También podemos eliminar la comisión de micropago configurando $\mu = 0$. En este caso, no actualizaremos la puntuación de crédito del nodo del servidor si solo sirve a un cliente durante un bloque. En este caso, nos basamos en el hecho de que la probabilidad de hacer coincidir dos o más nodos maliciosos es muy pequeña. Por lo tanto, en el bloque $T + 1$, el crédito se calcula actualizando su crédito actual en el bloque T con un factor de amortiguación ajustable λ:

$$C(T+1) = \begin{cases} \min(C(T) + \lambda \sum_{i=1}^{m} p_i, C_{max}) & \text{if } m > 1 \\ C(T) & \text{otherwise} \end{cases} \quad (7)$$

Design 3: Basándonos en los dos diseños anteriores, adoptaremos el diseño 2 y también agregaremos

comisión del 10%. La comisión tiene dos propósitos. En primer lugar, mejorará aún más la seguridad de la red en comparación con el diseño 2. En segundo lugar, la comisión cobrada se depositará en un fondo de tesorería. Describiremos el uso del fondo de tesorería en una sección posterior.

En el análisis anterior, asumimos que ϑ *es* pequeño, que es la proporción de dispositivos maliciosos en todos los dispositivos. Esto está garantizado por el depósito inicial de tokens en el registro y el requisito mínimo de crédito, como discutimos antes. En conclusión, una parte malintencionada preferiría seguir el protocolo y jugar honestamente para obtener una mejor recompensa.

Además de asegurar los nodos de la capa superior que producen bloques, también es necesario analizar el problema del "crédito falso" entre los nodos de Guardnet para garantizar la seguridad de la prueba de trabajo, controlar el comportamiento de "agricultura de clics" de los nodos defectuosos y analizar el costo del sabotaje. Tomando la aplicación DPN como ejemplo, nuestra capa de protocolo controla la aleatoriedad de los diferentes enlaces para evitar que los usuarios deslicen, y cada vez que un micropago deducirá una cierta cantidad de tarifa de transacción y hará que el sabotaje sea costoso.

Tomando como ejemplo la tarea DEP, el nodo Guardnet funciona en base a la estrategia de arrebatar órdenes y ejecutarlas aleatoriamente. Suponiendo que la condición de ejecución de la tarea A es la siguiente: si el crédito > 100 y el número de nodos de tarea > 1000, el resultado final se calcula en función del algoritmo de votación de consenso mayoritario, entonces el nodo defectuoso necesita controlar al menos 500 dispositivos con una puntuación de crédito de más de 100 para modificar el resultado.

Debido a la aleatoriedad del arrebato de tareas y al gran número total de nodos (N), la probabilidad de que las tareas se asignen a nodos incorrectos es de 500/N. A medida que

aumenta el número de nodos, también aumenta la seguridad general de la red, y el costo de ser saboteado aumenta exponencialmente en función de la puntuación crediticia y el número total de nodos. En resumen, el costo de hacer el mal es muy incontrolable para la parte maliciosa, y las recompensas de seguir las reglas superan con creces las recompensas de hacer el mal.

6.2.4 Mecanismos de incentivación

El protocolo Guardnet Network incluye varios objetivos entre los que se encuentran: (1) alentar a los usuarios a compartir el ancho de banda inactivo, (2) alentar a los dispositivos Guardnet Network a permanecer en línea y (3) aumentar el tamaño de la red de manera orgánica. El primer objetivo ya se ha discutido en las secciones de micropagos y PoCr. Los dos puntos restantes se discutirán en las dos subsecciones siguientes.

Decaimiento del crédito

Cuando un dispositivo Guardnet deja de unirse a la red, el sistema reducirá gradualmente su crédito hasta algunos umbrales predefinidos *τ0*. Supongamos *que τ es el umbral* en el que un usuario puede delegar su puntuación crediticia para ganar recompensas, establecemos el umbral predefinido $\tau_0 < \tau$. Si el puntaje de crédito de la cuenta es menor que τ_0, No habrá disminución del puntaje de crédito. Si el crédito de la cuenta es mayor que τ y no se une a las actividades de uso compartido de la red (ya sea del lado del servidor o del lado del cliente), es decir, está inactivo durante mucho tiempo, su puntaje de crédito caerá gradualmente a τ (e.g. a couple of months), Y luego su puntaje de crédito caerá asintóticamente a *τ0*, pero no más.

Compra inicial de crédito

Para animar a más usuarios a participar en la red Guardnet, necesitamos una forma de permitirles ganar créditos lo más rápido posible. Aquí es donde entra en juego la

compra inicial de crédito. Solo afecta a las cuentas que tienen puntajes de crédito inferiores a (que es el umbral que permite a un usuario ganar recompensas). Para un usuario cuyo puntaje de crédito actual C es menor que t, el usuario puede pagar $\delta(\tau - C)$ tokens para comprar su crédito hasta τn, Dónde δ es un parámetro ajustable que debe determinarse. Los tokens utilizados para comprar créditos se distribuirán como recompensa en bloque a los mineros, incluidos validadores, stakers y delegadores de puntajes de crédito.

6.2.5 Mining Rewards Distribution Mechanism

Diseñamos los siguientes mecanismos de incentivos para animar a más usuarios a unirse a la red:

Recompensa de minería: el nodo validado necesita suficiente staking y credit score para ser nominado y obtiene la calificación de emisión de bloques de blockchain, por lo que necesita el dispositivo para votar y confiar el staking y credit score a un validador. Al producir bloques normalmente, el validador puede recibir recompensas mineras. El sistema distribuirá recompensas a los nodos de los dispositivos en función de la contribución a la puntuación crediticia que proporcionen los dispositivos.

Recompensa por trabajo: el uso de tareas sostenibles anima a los nodos a ganar recompensas. Al completar la tarea web3, los nodos del dispositivo obtendrán un certificado de trabajo EZC. El sistema borrará automáticamente los certificados EZC del día anterior. En función de la proporción de la contribución del nodo y la contribución total del día, el sistema calculará automáticamente la recompensa por trabajo y los usuarios podrán reclamar sus recompensas en cualquier momento.

Recompensa de staking: los nodos de dispositivos pueden aumentar su puntaje de crédito a través del staking. El sistema distribuirá diferentes recompensas de staking en función de los diferentes niveles de crédito que elijan los usuarios. Con

el aumento gradual de los nodos, la disponibilidad entre los nodos y el ecosistema de aplicaciones en cadena se convierte gradualmente en un nuevo enfoque, de modo que, en el futuro, la recompensa de participación eventualmente será reemplazada por recompensas de trabajo.

7 Tokenomics

7.1 Overview

DPR, el token nativo de Guardnet, se utiliza para incentivos financieros y pagos por diversos servicios. Es la principal moneda de valor de Guardnet Network.

El suministro total de DPR es de 10 mil millones. De estos, 6 mil millones se asignan como recompensas en bloque. El principal mecanismo de incentivos es NPoW, Proof-of-Credit y bloques producidos por validadores. Además del token DPR nativo, Guardnet también utiliza el crédito EZC principalmente para pagar varias aplicaciones y servicios.

DPR, como token comercial externo del mercado secundario, se puede utilizar en múltiples sistemas o ecosistemas, como Polkadot, Ethereum, BSC, etc. La fluctuación del precio de mercado es determinada por numerosos participantes en el mercado secundario. EZC, como moneda estable interna, tiene un valor fijo y solo se puede usar en el ecosistema interno de Guardnet. Una vez más, EZC no es transferible ni comerciable. La compra y el uso de EZC no están relacionados con la inversión. EZC ayuda a promover el uso de aplicaciones on-chain a un precio estable y predecible.

7.2 Gobernanza

Hay dos tipos de gobernanza: la gobernanza fuera de la cadena y la gobernanza dentro de la cadena. El gobierno fuera de la cadena requiere una gran cantidad de

coordinación entre los desarrolladores y las comunidades. En la cadena Guardnet, elegimos esta última. En la mayoría de los modelos de gobernanza on-chain, las personas usan sus tokens para apostar por una lista de opciones. Por ejemplo, la situación más común es que el sistema solo se puede actualizar si la mayoría de las partes interesadas deciden actualizarlo.

En la cadena Guardnet, utilizamos PoCr, el sistema de créditos, para resolver este problema. Para cualquier

Actualización del sistema o cambio de protocolo, el proponente publicará una lista de opciones y se le dará una ventana de tiempo para votar. En lugar de hacer staking, cualquier cuenta de usuario votará de acuerdo con su puntaje de crédito. Siempre que su puntaje de crédito sea mayor que el valor de umbral (por ejemplo, el puntaje de crédito total es 100 y el valor de umbral es 60), entonces es un votante legítimo. Esto es muy similar a una persona que tiene "la edad suficiente" para votar. Las grandes partes interesadas no pueden simplemente aumentar los puntajes de crédito fácilmente. En PoS, una gran parte interesada puede obtener mucho poder de voto de inmediato. En PoCr, si bien una gran parte interesada aún puede obtener ventaja dividiéndose en varias cuentas y acumulando créditos, se necesita tiempo y esfuerzo para aumentar y mantener los puntajes de crédito. Por supuesto, si una gran parte interesada crea y mantiene una gran cantidad de cuentas de alto crédito, significa que su contribución a la red es mayor que la de otras y, a cambio, tendrá más poder de voto. Pero, en general, este diseño simple y efectivo puede aliviar en gran medida el problema del desequilibrio entre las grandes partes interesadas y los usuarios normales.

7.3 Treasury Pool

Como mencionamos en la sección de Seguridad PoCr, cobraremos el 10% de la comisión por micropagos. Tiene dos propósitos. Una de ellas es evitar que Sybil

ataque a las transacciones de micropagos entre identidades falsas para obtener puntajes de crédito. La otra es utilizar la comisión para establecer un fondo de tesorería. Este fondo de tesorería se puede utilizar de múltiples maneras.

Podemos dedicar una parte de este fondo de tesorería al desarrollo de nuestro ecosistema. Por ejemplo, cualquier desarrollador puede solicitar una subvención para ayudar a mejorar el ecosistema, por ejemplo, desarrollar herramientas o solucionar problemas de seguridad de la red Guardnet.

Podemos reservar una parte del grupo para recomprar el DPR de los usuarios y quemarlo. es decir, esta parte de DPR se intercambiará por monedas estables y cualquier usuario que haya quemado su DPR será reembolsado por la cantidad correspondiente de monedas estables. Este mecanismo permite a nuestro sistema controlar la circulación total de DPR de forma descentralizada.

Eventualmente, la comunidad decidirá cómo usar el DPR en este grupo.

7.4 Otros mecanismos de combustión

Además de la quema de EZC, también utilizamos otros mecanismos de quema para estabilizar el nivel de inflación de la RPD.

Quema de tesorería: La tesorería es la principal fuente de financiación para que los usuarios de Guardnet lleven a cabo la gobernanza en la cadena. Por lo general, se financia con tarifas de transacción y multas para todas las transacciones en cadena. El 1 (uno) por ciento de los fondos se quemará cada 24 días.

Quema de crédito: Un dispositivo sin conexión hará que su puntaje de crédito disminuya, lo que podría afectar el nivel de participación del usuario y la liberación de recompensas. Los usuarios pueden recuperar su puntaje de crédito perdido a través de la quema $DPR.1credit\ score = 50$DPR. El usuario no puede superar su puntaje de crédito más alto a través de la quema $DPR.$

8 Planificación de proyectos

8.1 Roadmap

Ver Tabla 3.

2018 Q3	Versión beta de AtomOS, el primer sistema operativo de seguridad de red sin bloqueos del mundo Detección de seguridad de red de siete capas de alto rendimiento Protocolo Trident único para proporcionar a los usuarios una VPN descentralizada segura y privada
2018 Q4	Nuestra primera puerta de enlace de seguridad de hardware para el hogar viene equipada con el sistema operativo AtomOS, plug-and-play, configuración cero
2019 Q1	Prueba de red pública de equipos Guardnet Connect. Por el momento, 200+ nodos de pago participan en la prueba.
2019 Q2	Asociaciones con múltiples firmas de capital de riesgo tradicionales de Silicon Valley e instituciones de blockchain de renombre
2019 Q3	Sale a la venta la tercera generación de Guardnet Connect
2020 Q1	El producto de cuarta generación, Guardnet Connect Mini, se prueba y entra en producción en masa
2020 Q2	Guardnet Connect Mini se pone en marcha en la plataforma Indiegogo
2020 Q3	Guardnet Connect Mini se lanza en BestBuy, la plataforma de ventas 3C más grande del mundo. Cooperó con China Mobile para desarrollar productos de ciberseguridad para hogares inteligentes
2021 Q1	La cadena pública descentralizada Guardnet Connect se pone en marcha y comienza el proceso de minería.

Tabla 3: Roadmap

8.2 Plan de distribución económica de tokens

Our token's abbreviation is DPR (Guardnet Token).
Los tokens se emiten a través del valor legal en forma de depósitos de Ethereum.
Total de tokens emitidos por el proyecto Guardnet: 10 mil millones (10,000,000,000).
Los tokens DPR no vendidos se reasignarán a proyectos de pool de minería y recompensas para los participantes de la comunidad.

8.2.1 Token Matrix

Apreciamos a nuestros principales contribuyentes, ¡nos referimos a USTED! Es por eso que hemos decidido asignar el 60% de los tokens a la comunidad, a nuestros queridos participantes y a los partidarios de Guardnet Network (ver Tabla 4). A través del concepto de compartir es minería, puede disfrutar y beneficiarse sin esfuerzo del viaje minero.

Asignación de tokens	Ratio
Minería	60%
Token privado	20%
Equipo	10%
Operación de mercado + cooperación + Token Treasure	5%
IDO de usuario principal	5%

Taba 4: Matriz de tokens

Apéndice A Terminología

A. IDO

El modelo IDO no financia al usuario. No se trata del dinero, es solo para la gente de la comunidad. La identidad de una persona en la comunidad es múltiple. Es el producto, el servicio y el personal del proyecto, todo en uno. Remuneración: porque las recompensas simbólicas son equivalentes al patrimonio del proyecto y a la identidad de los accionistas.

B. SSS

Abreviatura de Secure Shared Service: una nueva especie que combina la seguridad de la red, la economía compartida y la tecnología blockchain.

C. HIPE

HIPE es la estructura de datos original de Guardnet. AtomOS gestiona los recursos compartidos a través de HIPE para el funcionamiento sin bloqueos de todo el sistema operativo de la red, mejorando así en gran medida la fiabilidad, el rendimiento y la escalabilidad del sistema.

D. Middleman changes

O ataque Man-in-the-middle (MITM): En el campo de la criptografía y la seguridad informática, esto significa que el atacante y los dos extremos de la comunicación establecen dos sesiones independientes y reenvían los datos recibidos de una sesión a la otra sesión para hacer que ambos extremos de la comunicación piensen que se están comunicando con la otra parte directamente a través de una única sesión privada. Pero, de hecho, toda la sesión está completamente controlada por el atacante.

E. NAT traversal

El cruce NAT se refiere al problema de establecer una conexión cuando el servidor conectado está detrás de un dispositivo NAT. Dado que el dispositivo detrás de la NAT no tiene una dirección IP pública dedicada, es necesario un método para detectar si hay una asignación entre la intranet y la IP y el puerto de la red pública: si la hay, puede ser posible una conexión directa; si no es así, un servidor intermedio realiza el reenvío bidireccional, consulte el protocolo STUN [44].

Appendix B Disclaim

Este es un documento conceptual ("Libro Blanco") que describe nuestra propuesta de plataforma Guardnet y tokens Guardnet. Puede ser modificado o reemplazado en cualquier momento. Sin embargo, no existe ninguna obligación de actualizar el Libro Blanco ni de proporcionar al destinatario acceso a ninguna información adicional.

Este documento técnico no constituye una oferta de compra de valores ni una solicitud de inversión en valores en ninguna jurisdicción, ya sea en los Estados Unidos o en otro lugar, ni constituye un contrato de ningún tipo. La información proporcionada en este documento no ha sido revisada por ninguna autoridad reguladora. La publicación y distribución de este documento técnico no se interpretará como que este documento técnico ha cumplido con las leyes, los requisitos reglamentarios, las normas y/o los reglamentos de su jurisdicción.

No se hacen representaciones ni garantías en cuanto a la exactitud o integridad de la información, declaraciones, opiniones u otros asuntos descritos en este documento o comunicados de otro modo en relación con el proyecto. Sin limitación, no se ofrece ninguna representación o garantía en cuanto al logro o la razonabilidad de cualquier declaración conceptual o prospectiva. Nada en este

documento es o debe ser considerado como una promesa o representación en cuanto al futuro. En la medida en que lo permita la legislación aplicable, se renuncia a toda responsabilidad por cualquier pérdida o daño (ya sea previsible o no) que surja de o en relación con cualquier persona que actúe en relación con este Libro Blanco, o cualquier aspecto del mismo, a pesar de cualquier negligencia, incumplimiento o falta de cuidado. En la medida en que la responsabilidad pueda ser restringida pero no totalmente rechazada, se restringe en la medida máxima permitida por la ley aplicable.

Aunque la empresa ha tomado medidas razonables para garantizar que la información contenida en este documento se publique con precisión y en el contexto adecuado, la empresa no llevó a cabo ninguna revisión independiente de la información extraída de fuentes externas de terceros y no confirmó la exactitud o integridad de dicha información o las suposiciones en las que se basa. Por lo tanto, la empresa no estará obligada a proporcionar ninguna actualización sobre las declaraciones o garantías con respecto a la exactitud o integridad de dicha información.

Ninguna información proporcionada en este documento debe interpretarse o percibirse como asesoramiento comercial, legal, fiscal o financiero con respecto a Guardnet Network, la empresa y/o los tokens. Si no está seguro acerca de las decisiones financieras y legales, debe consultar a asesores profesionales independientes, como asesores financieros y legales, con respecto a los tokens de Guardnet, Guardnet y/o la empresa y sus respectivas operaciones y negocios, y el estado general de las criptomonedas y otros activos digitales en su jurisdicción. Usted reconoce que es posible que deba asumir el riesgo legal y financiero de cualquier compra de tokens Guardnet durante un período de tiempo indefinido o incurrir en pérdidas en caso de circunstancias imprevistas o interferencia de factores extraños.

Referencias

[1] V. Afshar, “cisco enterprises are leading the internet of things,” 2017. [Online]. Available: https://www.huffpost.com/entry/cisco-enterprises-are-leading-the-internet-of-things_b_59a41fcee4b0a62d0987b0c6.

[2] M. Allman, K. Avrachenkov, U. Ayesta, J. Blanton, and P. Hurtig, “RFC5827: Early retransmit for TCP and stream control transmission protocol (SCTP),” Tech. Rep., 2010.

[3] “Bitcoin Energy Consumption Index.” [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption.

[4] “Block Internet.” [Online]. Available: https://en.wikipedia.org/wiki/Block_(Internet).

[5] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch, “Verifiable delay functions,” in *Proc. Annual international cryptology conference*. Springer, 2018, pp. 757–788.

[6] L. S. Brakmo and L. L. Peterson, “TCP Vegas: End to end congestion avoidance on a global Internet,” *IEEE Journal on selected Areas in communications*, vol. 13, no. 8, pp. 1465–1480, 1995.

[7] N. Cardwell, Y. Cheng, C. S. Gunn, S. H. Yeganeh, and V. Jacobson, “BBR: Congestion-based congestion control,” *Queue*, vol. 14, no. 5, p. 50, 2016.

[8] “Cavium™ Unveils 48-core, 2.5GHz OCTEON® III MIPS64 Processor Family: First SoC with Breakthrough Search Processing and Over 100Gbps Single-chip Application Performance for Enterprise, Data-Center and Service Provider In-

frastructure." [Online]. Available: https://www.cavium.com/newsevents-cavium-unveils-48-core-octeon-iii-mips64-processor.html.

[9] "Data Breach." [Online]. Available: https://www.privacyrights.org/data-breaches.

[10] R. H. Dennard, F. H. Gaensslen, V. L. Rideout, E. Bassous, and A. R. LeBlanc, "Design of ion-implanted MOSFET's with very small physical dimensions," *IEEE Journal of Solid-State Circuits*, vol. 9, no. 5, pp. 256–268, 1974.

[11] "DPDK." [Online]. Available: https://www.dpdk.org/.

[12] "DPDK Performance." [Online]. Available: https://www.intel.com/content/www/us/en/communications/data-plane-development-kit.html.

[13] S. Frankel, R. Glenn, and S. Kelly, "RFC 3602: The AES-CBC cipher algorithm and its use with IPsec," Tech. Rep., 2003.

[14] B. Goodwin, "Cyber gangsters demand payment from Travelex after Sodinokibi attack," 2020. [Online]. Available: https://www.computerweekly.com/news/252476283/Cyber-gangsters-demand-payment-from-Travelex-after-Sodinokibi-attack.

[15] D. Gudkova, M. Vergelis, T. Shcherbakova, and N. Demidova, "Spam and Phishing in 2017," 2018. [Online]. Available: https://securelist.com/spam-and-phishing-in-2017/83833/.

[16] S. Ha, I. Rhee, and L. Xu, "CUBIC: a new TCP-friendly high-speed TCP variant," *ACM SIGOPS operating systems review*, vol. 42, no. 5, pp. 64–74, 2008.

[17] "Internet Assigned Numbers Authority." [Online]. Available: https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority.

[18] C. India, “Privacy Awareness Week-Are We Responsible for Our Data Breach?” [Online]. Available: https://securingtomorrow.mcafee.com/consumer/privacy-awareness-week-are-we-responsible-for-our-data-breach/.

[19] “Internet Censorship.” [Online]. Available: https://en.wikipedia.org/wiki/Internet_censorship.

[20] V. Jacobson, “Congestion avoidance and control,” in *Proc. ACM SIGCOMM computer communication review*, vol. 18, no. 4. ACM, 1988, pp. 314–329.

[21] A. Johnson, “Trump Signs Measure to Let ISPs Sell Your Data Without Consent,” 2017. [Online]. Available: https://www.nbcnews.com/news/us-news/trump-signs-measure-let-isps-sell-your-data-without-consent-n742316.

[22] P. Kennedy, “AMD EPYC Rome Details Trickle Out 64 Cores 128 Threads Per Socket.” [Online]. Available: https://www.servethehome.com/amd-epyc-rome-details-trickle-out-64-cores-128-threads-per-socket/.

[23] M. Kosinski, D. Stillwell, and T. Graepel, “Private traits and attributes are predictable from digital records of human behavior,” *Proceedings of the National Academy of Sciences*, p. 201218772, 2013.

[24] “List of Websites Blocked in India.” [Online]. Available: https://en.wikipedia.org/wiki/Websites_blocked_in_India.

[25] “List of Websites Blocked in Russia.” [Online]. Available: https://en.wikipedia.org/wiki/List_of_websites_blocked_in_Russia.

[26] “List of Data Breaches.” [Online]. Available: https://en.wikipedia.org/wiki/List_of_data_breaches.

[27] “List of TCP and UDP Port Numbers.” [Online]. Available: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

[28] “Lock (computer science).” [Online]. Available: https://en.wikipedia.org/wiki/Lock_(computer_science).

[29] C. Malmo, “One Bitcoin Transaction Consumes As Much Energy As Your House Uses in a Week.” [Online]. Available: https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change.

[30] L. Mathews, “Phishing Scams Cost American Businesses Half A Billion Dollars A Year.” [Online]. Available: https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year.

[31] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, “RFC 2018: TCP selective acknowledgment options,” 1996.

[32] “Mirai Source Code.” [Online]. Available: https://github.com/jgamblin/Mirai-Source-Code.

[33] S. Morgan, “Cybercrime To Cost The World $10.5 Trillion Annually By 2025,” 2020. [Online]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[34] S. Morgan, “Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion,” 2020. [Online]. Available: https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/.

[35] “Network address translation.” [Online]. Available: https://en.wikipedia.org/wiki/Network_address_translation.

[36] M. Orcutt, “Hijacking Computers to Mine Cryptocurrency Is All the Rage,” 2017. [Online]. Available: https://www.technologyreview.com/s/609031/hijacking-computers-to-mine-cryptocurrency-is-all-the-rage/.

[37] J. Padhye, V. Firoiu, D. F. Towsley, and J. F. Kurose, “Modeling TCP Reno performance: a simple model and its empirical validation,” *IEEE/ACM Transactions on Networking (ToN)*, vol. 8, no. 2, pp. 133–145, 2000.

[38] PeckShield, “EPoD: Ethereum Packet of Death (CVE-2018–12018).” [Online]. Available: https://medium.com/@peckshield/epod-ethereum-packet-of-death-cve-2018-12018-fc9ee944843e.

[39] “Phishing.” [Online]. Available: https://en.wikipedia.org/wiki/Phishing.

[40] M. Rechtoris, “Data breaches cost healthcare industry $6.2B.” [Online]. Available: https://www.beckersasc.com/asc-turnarounds-ideas-to-improve-performance/data-breaches-cost-healthcare-industry-6-2b-4-points.html.

[41] D. Reed *et al.*, “RFC 1459: Internet Relay Chat Protocol,” 1993.

[42] T. Riley, “The Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds,” 2020. [Online]. Available: https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/.

[43] L. Rokach and O. Z. Maimon, *Data mining with decision trees: theory and applications*. World scientific, 2008, vol. 69.

[44] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy, “RFC3489: STUN-Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs),” 2003.

[45] S. J. Russell and P. Norvig, *Artificial intelligence: a modern approach*. Malaysia; Pearson Education Limited„ 2016.

[46] A. Shahbaz and A. Funk, "The pandemic's digital shadow," 2020. [Online]. Available: https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow.

[47] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE mobile computing and communications review*, vol. 5, no. 1, pp. 3–55, 2001.

[48] O. Solon, "Facebook Says Cambridge Analytica May Have Gained 37M More Users' Data." [Online]. Available: https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought.

[49] "Study: Attack on KrebsOnSecurity Cost IoT Device Owners $323K," 2018. [Online]. Available: https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot-device-owners-323k/.

[50] B. Sullivan, "Online Privacy Fears Are Real." [Online]. Available: http://www.nbcnews.com/id/3078835/t/online-privacy-fears-are-real/.

[51] "Timeline of computer viruses and worms." [Online]. Available: https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms.

[52] "WAN optimization." [Online]. Available: https://en.wikipedia.org/wiki/WAN_optimization.

[53] "Websites Blocked in Mainland China." [Online]. Available: https://en.wikipedia.org/wiki/Websites_blocked_in_mainland_China.

[54] M. Zomorodi, “Do You Know How Much Private Information You Give Away Every Day?” [Online]. Available: http://time.com/4673602/terms-service-privacy-security/.