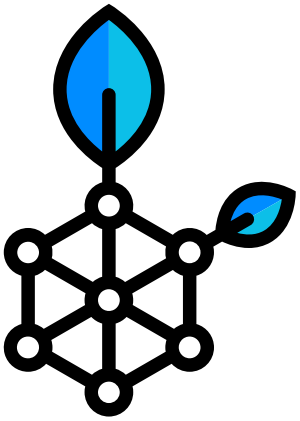


rif

RSK Infrastructure Framework

Protocolo del Identidad RIF (RIF Identity Protocol)

Construcción de la infraestructura para la próxima generación de aplicaciones distribuidas

V 1.21

Sinopsis

Creemos que las criptomonedas crecerán exponencialmente en la próxima década. Sin embargo, para permitir genuinamente una adopción masiva, no solo por parte de la comunidad avezada en tecnología, los usuarios deberían poder administrar billeteras y activos digitales. Entonces, una de las principales barreras para la adopción de las criptomonedas es la complejidad inherente de la tecnología blockchain.

La facilidad de uso es clave para llegar a los usuarios menos técnicos que no están bancarizados. Es difícil esperar una amplia adopción si los usuarios deben copiar y pegar largas direcciones hexadecimales para transferir o recibir activos digitales, solo por mencionar un ejemplo. Además, teclear direcciones manualmente es un proceso propenso a errores, y un simple error tipográfico puede causar la pérdida de fondos. Al agregar un servicio de resolución de nombres, también conocido como “alias” o “dominios”, la probabilidad de errores se reduce mucho, así como la aparente complejidad del sistema; cuanto más fácil es la tecnología, más rápida es su adopción.

El objetivo del Protocolo del Directorio RIF (RDP, por sus siglas en inglés) es encontrar diferentes tipos de recursos a partir de simples nombres de recursos. Los siguientes son ejemplos de recursos: direcciones de RSK, claves públicas de encriptación personal, identificadores de redes sociales, etc.

Además, la centralización del acceso a múltiples recursos asociados con un nombre legible por humanos mejora la experiencia del usuario de la plataforma. Como los nombres de los recursos pueden cambiar con el tiempo, el sistema debe ser flexible, para admitir cambios frecuentes. Por último, el sistema permite a los usuarios comprar, vender y subastar fácilmente nombres mediante el token RIF.

Introducción

Uno de los pilares de la World Wide Web es el sistema de nombres de dominio (DNS, por sus siglas en inglés). Este sistema se encarga de asignar nombres legibles por humanos a direcciones IP. La Corporación de Internet para la Asignación de Nombres y Números (ICANN, por sus siglas en inglés) es una organización responsable de coordinar el mantenimiento y las reglas de varias bases de datos relacionadas con espacios de nombres y espacios numéricos de Internet, asegurando el funcionamiento de la red. La ICANN realiza el mantenimiento técnico real de los registros de zona raíz del DNS.

Estos servicios son un punto central de confianza y fracaso[1][2]; pueden ser desconectados por ataques DDoS y las asignaciones de dominios pueden modificarse forzando cambios en los servidores DNS o falsificando respuestas de ellos. Además, existen algunos problemas de seguridad, como que los proveedores de servicios de Internet sean capaces de censurar nombres sin que sea fácil detectarlo.

El Directorio RIF apunta a convertirse en un sistema descentralizado y seguro similar al DNS. Los casos de uso para la asignación de nombres en el contexto de la inclusión financiera y la libertad individual son innumerables. Los servicios de nombres pueden utilizarse primero para simplificar la transferencia de activos mediante la identificación de extremos de transacciones: la gente puede tener alias para compartir con amigos con el fin de ponerse en contacto de manera segura o recibir pagos. También, las fundaciones pueden usar alias para identificar direcciones de donación o flujos internos de fondos a otras instituciones, todo de forma transparente y segura. Los servicios de nombres podrían usarse con el propósito de proporcionar localizadores de recursos para sitios de Internet descentralizados, y así se almacenarían páginas en redes de almacenamiento descentralizadas. Los nombres también se emplean para identificar a cualquier entidad que recopile tokens de reputación que sean públicos.

El Directorio RIF y la inclusión financiera

Un problema que demora la adopción masiva de las criptomonedas es la dificultad para manejar las direcciones de los usuarios. Es difícil esperar una amplia adopción si los usuarios deben copiar y pegar largas direcciones hexadecimales para transferir o recibir activos digitales. Por ejemplo, una dirección de RSK al azar es “06f1b66ffe49df7fce684df16c62f59dc9adbd3f”, la cual es evidentemente propensa a errores se la escribe a mano, y un simple error de escritura puede derivar en la pérdida de fondos. Además, también es difícil de recordar.
Otro caso afín es el alias de cuenta bancaria. En el sistema financiero de bancos, las cuentas bancarias tienen un número que las identifica de manera única. Por ejemplo, en el sistema bancario de la Argentina, el número de cuenta se llama CBU y tiene 22 dígitos. Debido a su

complejidad, los bancos brindan la posibilidad de crear un alias del CBU, que es un nombre alfanumérico exclusivo con una longitud de entre 6 y 20 caracteres. Los caracteres del alias deben pertenecer al abecedario inglés, y los únicos caracteres especiales permitidos son el punto (.) y el guion (-). Es útil en transacciones entre usuarios de bancos. Por ejemplo, Bob simplemente le envía a Alice su alias legible por humanos. Luego, ella pone el alias de Bob en el campo de dirección del destinatario y realiza la transacción. Debido a la mayor simplicidad de las transacciones bancarias cuando se utiliza un alias como cuenta, toda la población los ha adoptado.
En síntesis, el RDP es un protocolo que permite a los usuarios adquirir dominios comerciales que pueden asociarse con recursos descentralizados o centralizados, tales como páginas web, o con un alias que puede asociarse de manera unívoca con recursos personales (p. ej., direcciones de comunicación, billetera o almacenamiento). La ventaja de usar direcciones legibles por humanos es reducir la aparente complejidad de la tecnología blockchain para el usuario final.

Las pautas iniciales proporcionadas en este protocolo pueden estar sujetas a cambios adicionales, ya que las ideas y la arquitectura serán discutidas y mejoradas por el ecosistema en el futuro.

Una implementación del Directorio RIF

RIF Labs ha implementado un primer proveedor de servicio para el RDP, que se llama Servicios de Nombres RIF. El RNS utiliza la blockchain de RSK para mantener y controlar el acceso a la información sobre nombres. Por lo tanto, el RNS garantiza la descentralización y la seguridad de la blockchain de RSK. Si bien es posible que se registren otros proveedores de servicio de RDP en el futuro, pensamos que la asignación de nombres es inherentemente un servicio que se beneficia en gran medida de los efectos de la red, y por consiguiente prevemos que, a largo plazo, la comunidad del RSK y el RIF elijan uno solo.

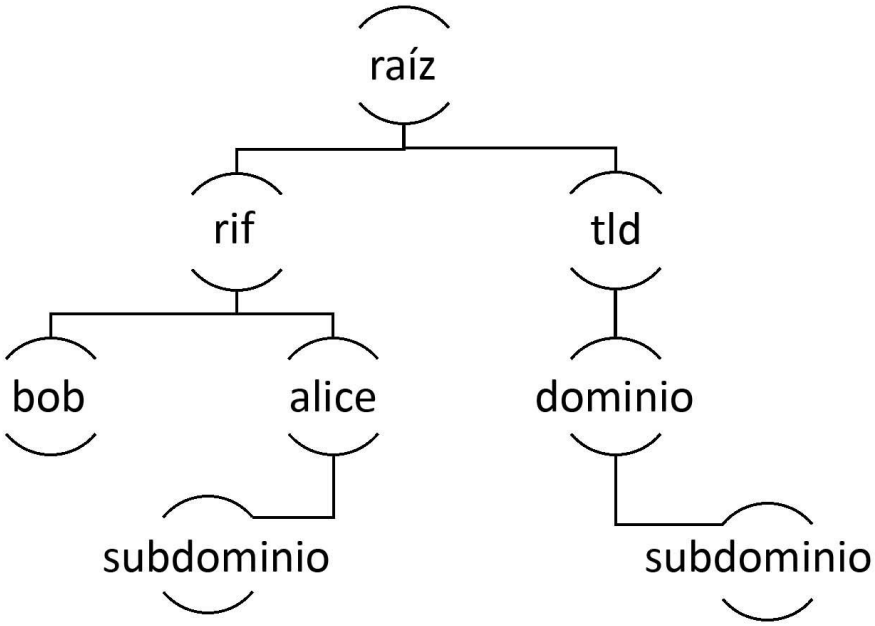
El diseño del Protocolo del Directorio RIF

El Protocolo del Directorio RIF define una interfaz con el fin de simplificar el uso de direcciones.
Es esencial implementar un mecanismo que asigne a los recursos (p. ej., una dirección de RSK) un nombre de dominio fácil de recordar para el usuario. El sistema debe ser transparente: los usuarios deben poder demostrar que poseen un dominio determinado, que han pagado las tarifas exigidas y que la fecha de vencimiento es clara, de manera que puedan efectuar pagos por adelantado a fin de reducir el riesgo de pérdida accidental de derechos sobre nombres. El diseño debe considerar también el caso frecuente de que diferentes usuarios deseen adquirir el mismo nombre de dominio, e intentar resolver esta situación antes de que se adquiera el nombre, con lo cual se evitan costosas etapas de resolución de disputas.

Por último, el diseño debe reducir al mínimo el riesgo de censura de nombres y de ciberocupación de nombres. De gran importancia para el diseño del RDP es el token RIF, que es el token de preferencia para la adquisición de nombre por primera vez. El token RIF se emplea como medio de retención de tokens en subastas de nombres y también para pagar el alquiler del mantenimiento del nombre.

Adquisición de dominios

La base de datos de nombres de dominio se interpreta como un árbol. La raíz del árbol (denominada nodo raíz) tiene el control de todos los posibles nombres de dominio de nivel superior, o TLD (por sus siglas en inglés). A los hijos de los TLD se los llama dominios. Además, a los hijos de los dominios se los llama subdominios.
Todo nombre de RDP debe ajustarse al siguiente formato: "subdominio(n)… .subdominio(1).dominio.tld". Los nombres consisten en una serie de etiquetas separadas por puntos. La última etiqueta corresponde al TLD, y los hijos siempre anteceden a los padres. Además, cada etiqueta debe ser una etiqueta normalizada válida como se describe en UTS46 [3] con las restricciones siguientes: transitional debe ser falso y use STD3AsciiRules debe ser verdadero.



Obtención de un dominio por subastas ciegas

El mecanismo para obtener un dominio por primera vez es a través de una subasta ciega de Vickrey [4]. "Una subasta de Vickrey es un tipo de subasta con ofertas a sobre cerrado. Los licitadores envían ofertas por escrito sin conocer las ofertas de los demás participantes de la subasta. Quien más oferta gana, pero el precio que se paga es el de la segunda oferta más

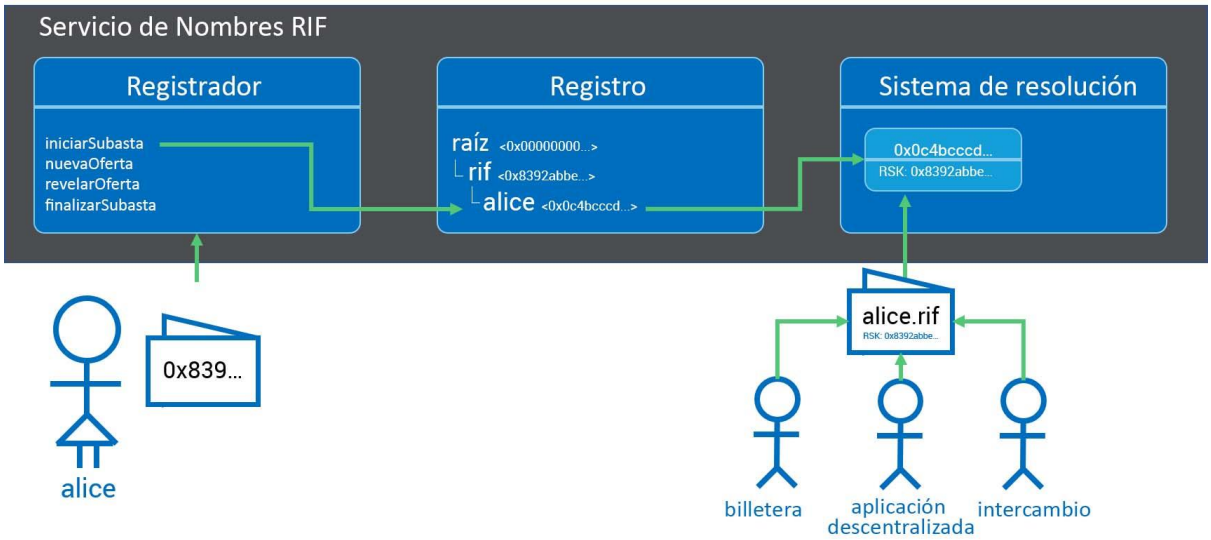
alta" [4]. La práctica ha demostrado que son las peculiaridades psicológicas humanas, y no solo la oferta y la demanda, las que impulsan las subastas. El mecanismo de subasta de Vickrey reduce la probabilidad de que un postor pague de más por un artículo y también aumenta la probabilidad de que el vendedor obtenga lo máximo que puede obtener por él.
Por ejemplo, si ".rif" es el TLD y un usuario llamado Alice quiere obtener el dominio "alice.rif" (como se muestra en la figura anterior), ella puede abrir una subasta de este dominio, hacer una oferta, y si resulta ser la más alta, se convertirá en la nueva propietaria del dominio "alice.rif".

Obtención de un dominio por delegación

El propietario de un dominio puede delegar la propiedad de un subdominio a un comprador sin pasar por el proceso de subasta. Por ejemplo, si un usuario llamado Bob es el propietario de "bob.rif" y Alice quiere el subdominio "alice.bob.rif", Bob puede delegar la propiedad del subdominio a Alice sin un proceso de subasta.
Desde la perspectiva del nivel de dominio, la delegación puede llevarse a cabo mediante una transferencia de propiedad. Una vez que Alice obtiene un dominio, debe establecer un sistema de resolución que lleve a cabo la resolución entre el nuevo dominio y el recurso deseado, como explicaremos en la próxima sección.

Resolución de direcciones de dominios

La resolución de un dominio es el proceso en el cual el sistema busca el nombre en la base de datos, comprueba que esté presente, y si lo está, devuelve la información asociada. Esta resolución puede usarse en billeteras, intercambios o aplicaciones descentralizadas, para manejar nombres fáciles de utilizar, en lugar de direcciones complejas. Por ejemplo, para que Alice le envíe dinero a Bob, Bob primero tiene que enviarle a Alice su alias registrado, y luego Alice puede buscar la dirección de Bob (deberá escribir el alias en la aplicación de la billetera); la billetera buscará su nombre en la base de datos del RDP y, para continuar, usará la información obtenida por el sistema de resolución asociado con el alias.



Mercados secundarios

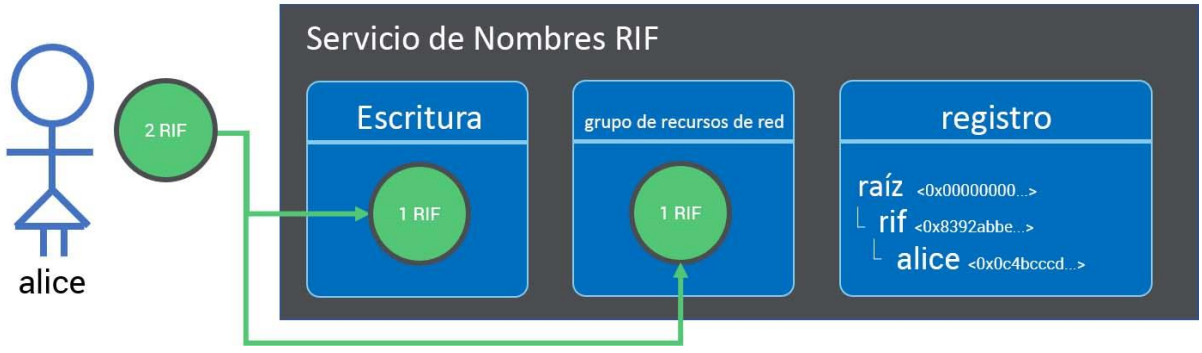
Si bien el Directorio RIF no especifica un mercado secundario en particular para usar con el fin de vender dominios cuando se los ha adquirido, ya hay soluciones descentralizadas de mercado secundario para que la gente los compre y los venda. Si la demanda es alta, prevemos que la comunidad del RIF creará nuevos mercados secundarios ajustados específicamente a la venta de dominios. Los mercados secundarios podrían aceptar el pago de dominios con otras criptomonedas, y además podrían servir para otras clases de subastas, o transferencias simples del tipo “primera en ingresar, primera en realizarse”. Los mercados secundarios para nombres de dominio también podrían utilizar el token RIF, pero no están limitados a utilizar solo este token.

Ingresos de los proveedores de servicio

Los proveedores de servicio podrían cobrar tarifas de las subastas y los alquileres de nombres. Podrían elegir entre consumir las tarifas, donarlas o usarlas para obtener una ganancia. Las tarifas del token RIF también sirven para prevenir la ciberocupación de nombres, porque los usuarios deben pagar un alquiler de mantenimiento anual por cada dominio adquirido.

Tokens bloqueados

Cuando un usuario participa en una subasta, los tokens RIF que se ofrecen se bloquean en la Escritura, como se muestra en el siguiente diagrama.



Una parte de la oferta ganadora, correspondiente al monto de la segunda oferta más alta, se bloquea a cambio de la propiedad del dominio. Los otros montos bloqueados correspondientes a las ofertas perdedoras se reembolsan a sus dueños legítimos previa solicitud.
Los tokens RIF bloqueados se reembolsarán al propietario cuando se libere el dominio, suma a la que se le descontarán las tarifas definidas por los Proveedores de Servicio.

Pagos anuales

Para obtener y retener la propiedad del dominio, el propietario debe pagar una suma anual recurrente denominada alquiler. Después de nueve meses desde el último alquiler anual pagado, el propietario tendrá la opción de pagar para mantener la propiedad durante un año más o renunciar a ella.
Si el propietario no paga el alquiler anual, significa que opta por renunciar a la propiedad; en este caso, sus tokens originalmente bloqueados serán devueltos al usuario, menos una tarifa definida por el proveedor del servicio

El futuro

Hemos creado un protocolo que es justo y útil, que brinda incentivos a los usuarios para comerciar nombres y a la vez reduce el abuso. Sin embargo, creemos que el protocolo puede evolucionar o que otros protocolos de RIF mejores pueden reemplazarlo en el futuro. Analizaremos brevemente qué direcciones podría tomar el protocolo.

Mejoras

Un proveedor de servicio del RDP podría introducir actualizaciones del código para agregar funcionalidad o corregir errores. Esas actualizaciones las dispondría el propietario del proveedor de servicio. Las actualizaciones deberían ser compatibles con versiones anteriores. En otras palabras, la propiedad de los dominios no se modificaría (con la excepción de los dominios de DNS, como se explica en la próxima sección). Lo que sí podría modificarse son las estructuras tarifarias, los modelos de subastas y otras funciones.

Oráculos y dominios de DNS

El RDP abre la posibilidad de migrar direcciones de DNS regulares al RDP; con ese propósito, hace corresponder dominios y TLD de DNS con dominios y TLD de RDP. Con el fin de que esto sea justo para los propietarios de dominios de DNS, estos deben poder reclamar un dominio en el RDP y demostrar que son los propietarios legítimos ya sea mediante el uso de oráculos o cadenas de certificación digitales. En caso de conflicto entre un dominio de nombre ICANN y un dominio de RDP, se utilizará un sistema de arbitraje para resolver los conflictos. Dicho sistema de arbitraje podría implementarse a través de oráculos o de manera descentralizada. Aunque la versión actual del Directorio RIF no proporciona una interfaz específica para esto, prevemos que el protocolo podría evolucionar en versiones futuras de modo de admitir esta funcionalidad.

Anonimato

Los usuarios podrían querer ocultar la dirección de pago a la cual se asignan sus alias. Esto se puede hacer con recursos encriptados. El propietario necesitaría transferir la clave de

desencriptación a un usuario a pedido por medio de un canal de comunicación externo a la cadena, posiblemente ofrecido por un proveedor de servicios de comunicaciones de RIF. Además, las direcciones encriptadas pueden ser direcciones sigilosas. Las direcciones sigilosas permiten que el pagador derive nuevas direcciones únicas para cada pago, lo cual reduce la probabilidad de vincular los pagos.

Creación de nuevos dominios de máximo nivel

RIF Labs actúa de proveedor de servicio para RDP. Han implementado un registrador inicial para TLD. Con este proveedor, RIF Labs puede, en el futuro, dejar que los usuarios creen, compren y vendan sus propios TLD.

Resumen

Para la creación del Protocolo del Directorio RIF se partió de la base de los conocimientos reunidos por muchas organizaciones anteriores que han trabajado en servicios de nombres; ofrece una única interfaz unificada que es a la vez simple y compatible con los proveedores de servicios de nombres actuales. La interfaz permite a los usuarios adquirir dominios, hacer ofertas en subastas de dominios, administrar subdominios y pagar las tarifas requeridas con tokens RIF, todo esto con facilidad; se trata de un servicio que puede prestar una red descentralizada y sin censura.

Referencias

[1] M. Ali, R. Shea, J. Nelson, M. J. Freedman, "Blockstack: A New Internet for Decentralized Applications" (2017) https://blockstack.org/whitepaper.pdf
[2] "Namecoin FAQS" (preguntas frecuentes sobre Namecoin) https://namecoin.org/docs/faq/
[3] Biblioteca de NPM https://www.npmjs.com/package/idna-uts46
[4] “Vickrey Auction" (subasta de Vickrey) https://en.wikipedia.org/wiki/Vickrey_auction