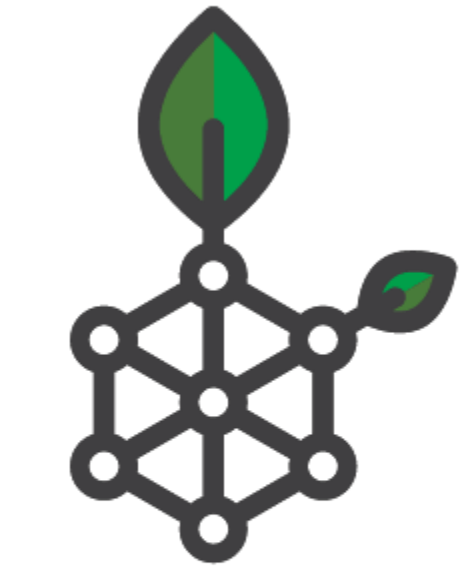

RSK

Descripción general del informe oficial

Revisión: 9
Fecha: 19 de noviembre de 2015
Por Sergio Demian Lerner

Introducción

En 2008, Satoshi Nakamoto revolucionó los pagos con la creación de Bitcoin. Bitcoin incluía una muy limitada implementación de los denominados smart contracts, un concepto introducido en 1993 por Nick Szabo.

Desde entonces, se han realizado muchas investigaciones acerca de la creación de nuevas criptomonedas que soporten programas distribuidos de Turing completos. Hoy en día, existe una confianza generalizada de que es posible construir máquinas virtuales útiles, seguras y determinísticas para alcanzar este objetivo.

Creemos que los nuevos casos de uso son necesarios para que Bitcoin se convierta en la criptomoneda líder en el mundo, y que añadir capacidades de smart contracts es clave para garantizar ese futuro. Con esto en mente, creamos RSK, una plataforma de smart contracts que incorpora una máquina virtual de Turing completa a Bitcoin. También brinda otras mejoras a la red, tales como transacciones más rápidas y mayor escalabilidad, funcionalidades que también creemos posibilitarán nuevos escenarios de uso.

RSK es una evolución de QixCoin, una criptomoneda turing completa creada en 2013 por el mismo equipo de desarrollo. RSK brinda una experiencia de pago mejorada con confirmaciones casi instantáneas. Puede alcanzar 300 tps y confirmar la mayoría de los pagos en menos de 20 segundos. Y aun así, sigue estando basado en las mismas garantías de seguridad con las que cuenta Bitcoin, soportando la minería fusionada SHA-256D.

RSK funciona como una sidechain (cadena lateral) de Bitcoin. Cuando se transfieren bitcoins a un RSK blockchain, se convierten en «SmartBitcoins» (SBTC). Los SmartBitcoins equivalen a bitcoins que viven en el RSK blockchain, y pueden ser transferidos nuevamente hacia bitcoins en cualquier momento sin ningún costo adicional (excepto por las tarifas estándar de RSK y Bitcoin). SBTC es la moneda nativa utilizada en el RSK Blockchain para pagarle a los mineros de bitcoin por las transacciones y el procesamiento de los contratos. No se emiten monedas: todos los SBTC se crean a partir de bitcoins que vienen del Bitcoin blockchain.

RSK potencia a Bitcoin en las siguientes áreas:

- Máquina Virtual de Turing completa de RSK (RVM) que posibilita los smart contracts
- Primera confirmación promedio para las transacciones en 10 segundos
- Minería fusionada segura que combina una PoW con una firma-umbral de respaldo basada en la minería de la federación
- Eje central de bajo retardo y relé rápido integrado en la red gossip entre pares.
- Conexión bidireccional mediante el uso de cadenas laterales (actualmente un conector federado, enteramente automático, sujeto a las mejoras de Bitcoin)

Acrónimos: «RSK» se refiere a Rootstock (la plataforma), otros términos relacionados son «protocolo de RSK» (las especificaciones) y «nodo de referencia de RSK» (la implementación de referencia), la moneda nativa de RSK es el «SmartBitcoin», y «SBTC» es el símbolo de la moneda SmartBitcoin, «BTC» se refiere a la moneda de Bitcoin

y «Bitcoin» se refiere al protocolo de Bitcoin.

¿Cuál es la importancia de RSK para el ecosistema Bitcoin?

Alineación de los agentes de Bitcoin y protección del valor

El principal objetivo de la gestión de RSK es alinear a los principales agentes de Bitcoin mediante la creación de recompensas que estén totalmente alineadas con sus actividades actuales.

Esta filosofía se refleja directamente en el núcleo de su arquitectura, donde los mineros de Bitcoin brindan el poder de hashing necesario para las validaciones de bloques de pruebas de trabajo, los líderes de la industria (Agentes Cambiarios, Wallets y Procesadores de Pagos) integran la Federación que crea los puntos de verificación para validación y firma las transacciones de redención del conector bidireccional.

Además de eso, RSK decide implementar mejoras a su plataforma sobre la base de un sistema de votación en el que mineros, líderes de la industria, agentes de Bitcoin/RSK, y desarrolladores core toman la decisión final.

En los siguientes párrafos describimos cómo funcionan estos incentivos.

Modelo de gestión

Cada miembro de la comunidad tiene el conocimiento necesario para servir a la comunidad de la mejor manera: los agentes cambiarios y web-wallets saben cómo proteger los ahorros de Bitcoin, los mineros saben cómo realizar operaciones de minería a gran escala para asegurar las transacciones de los usuarios, las compañías de Blockchain innovan en nuevos casos de uso y hacen realidad los sueños, los desarrolladores core tienen el conocimiento técnico para superar los desafíos técnicos que puedan surgir, los encargados del mantenimiento de los nodos brindan la infraestructura y la conectividad de la red, y los usuarios son el corazón del sistema, brindando confianza y liquidez.

El modelo de gestión de RSK tiene como fin representar a todas las partes de la comunidad al ofrecer una junta de gestión constituida por 5 miembros. Los mineros podrán votar con poder de hashing (1 voto), los usuarios de Bitcoin y RSK podrán votar con prueba de participación (1 voto), los agentes cambiarios y web-wallets podrán votar a través de la Federación (1 voto), los desarrolladores core de RSK y Bitcoin tendrán un sistema de votación con un límite especial (1 voto), y el último voto será ofrecido a una institución de Bitcoin establecida sin fines de lucro, como la Fundación Bitcoin, que puede representar al ecosistema en el sentido más amplio. A su vez, se podrá ofrecer un voto institucional a la Fundación Ethereum, en caso de representar a la comunidad de Ethereum.

Protección de las inversiones de los mineros de Bitcoin

En agosto de 2016, el margen de rentabilidad de la minería en Bitcoin caerá a menos del 50 % debido a las decrecientes recompensas de bloques de 25 BTC a 12.5 BTC. Cientos de millones de hardware de minería pasarán a ser instantáneamente obsoletos. Es probable que esto incluya a todas las máquinas de minería presentes en el mercado hoy en día,

dado que dos generaciones de chips (más rápidos y con menos consumición de energía) serán desarrolladas y vendidas antes de 2017. Esto representará el fin del negocio de minería para casi todos los mineros que aún no han remplazado su hardware. RSK, gracias a sus capacidades fusionadas de minería, ofrece a esos mineros la oportunidad de continuar llevando a cabo su actividad durante al menos cuatro años más. Dado que los mineros fusionados de Bitcoin pueden minar ambas monedas con costo marginal cero, los mineros podrán continuar minando Bitcoin siempre y cuando el ingreso adicional brindado por RSK compense la brecha de rentabilidad.

Asimismo, la reducción de la rentabilidad de la minería creará una concentración adicional en los mineros de bajo costo, lo cual aumentará la vulnerabilidad de la red de Bitcoin. Por lo tanto, RSK también podría tener una función crucial en la promoción de una amplia base de mineros rentables mediante un aumento en la seguridad y el valor del Bitcoin.

Asimismo, empezando hoy a un costo mínimo, y creando aplicaciones para RSK, los mineros de Bitcoin podrán no solo proteger sus inversiones, sino también desarrollar una oportunidad de negocio completamente nueva.

Cómo se garantizará Bitcoin/conector bidireccional de RSK

Las compañías líderes de Bitcoin integrarán una Federación que tendrá la función fundamental de garantizar las transferencias de fondos entre Bitcoin y RSK blockchains. A cambio de esto, obtendrán ganancias de las tarifas generadas por la liquidación de los fondos entrantes y salientes.

Comisiones por transacciones de Bitcoin más bajas y emisión de activos de valor estable

Los propietarios actuales y potenciales usuarios de Bitcoin han visto su uso del sistema monetario confinado a ciertos casos de uso (por ejemplo, las inversiones, las redes de pago globales), principalmente debido a la volatilidad del precio del bitcoin, pero esta restricción podría empeorar en el futuro debido a un potencial aumento en las comisiones por transacción en la próxima reducción de Bitcoin.

RSK ofrece una solución para esto, brindando una validación casi instantánea para las transacciones (20 segundos) y emisión de activos con precios vinculados a aquellos de una moneda fiat u otro commodity estable. Bajar la exposición a la volatilidad en transacciones mientras que se mantiene al bitcoin como una moneda de reserva aumenta el valor general del bitcoin.

Aumento en la seguridad de Bitcoin

En la próxima reducción de las recompensas de Bitcoin, cientos de millones de dólares de hardware de minería obsoleto se venderán a precios bajos de manera privada o en línea. Esto abrirá una ventana de vulnerabilidad, ya que le dará a los atacantes la posibilidad de comprar una enorme cantidad de poder de hashing a cambio de muy poco dinero y así ejecutar un ataque del 51 %. La disminución de la seguridad también puede afectar el valor percibido de la moneda. Al aumentar la rentabilidad de la minería en Bitcoin con la minería fusionada de RSK, es posible que la red de Bitcoin evite que la tasa de hash se desplome.

RSK como red de pago de bajo costo de BTC

Si el tamaño del bloque de Bitcoin no se aumenta mediante un hard-fork, cuando la próxima recompensa de Bitcoin se reduzca, es posible que las tarifas de transacción de Bitcoin se vuelvan prohibitivamente altas para ciertas aplicaciones. Dado que los bloques de RSK pueden contener muchas más transacciones que los bloques de Bitcoin, RSK ofrecerá, naturalmente, tarifas más bajas. Diríjase a la próxima sección para encontrar un análisis de los escenarios futuros respecto de las comisiones por transacción.

El futuro de Bitcoin y sus comisiones por transacción no son claros: actualmente, existen propuestas contenciosas en cuanto a cambios en el tamaño máximo de los bloques que tendrán un gran impacto en el futuro de las comisiones por transacción. En la siguiente tabla, intentamos predecir los escenarios futuros y comparar a RSK con Bitcoin realizando ciertos supuestos razonables en cuanto al crecimiento y los forks.

Parámetro	Bitcoin	RSK
Tiempo de confirmación con seguridad comparable de acuerdo con la equivalencia Satoshi	10 minutos	10 segundos
Tiempo mínimo de confirmación para una probabilidad de revocación de 0.1 %	20 minutos (2 bloques)	30 segundos (3 bloques)
Máx. Transacciones por segundo	3.3 tps (asumiendo una transacción de tamaño promedio)	300 tps en el inicio Escalable a 1000 tps
Costo promedio actual para los usuarios por una transacción estándar	6 centavos Asumiendo que: - 1.5 tps	Precio de mercado no disponible
Costo actual para mineros para incluir una transacción estándar	1 centavo Asumiendo que: - Utilizando una red de relé rápida - UTXO en la memoria - 1 mili-segundo de tiempo de procesamiento por transacción. Recompensa de bloque promedio de 25.2 BTC 5 centavos Asumiendo que: - Utilizando una red de relé estándar	<1 centavo (estimado) Asumiendo que: No haya ningún cambio específico en el hardware de RSK. - Casi ninguna transacción de RSK 1 centavo (estimado) Interrumpir a un minero para cargar un nuevo encabezado desperdicia 10 milisegundos de tiempo de procesamiento
Tarifas de transacción para fines de 2016	1.6 USD Asumiendo que: - el tamaño del bloque no aumenta - la tasa BTC/USD no cambia - El nivel de seguridad no varía - 3 tps	1 centavo (estimado) Asumiendo que: - 3 tps

Es importante destacar que, para la tabla que aparece más arriba, las estimaciones se basan en el hecho no comprobado de que el precio del BTC permanecerá aproximadamente en 240 BTC/USD durante 2016. Si el precio aumenta diez veces durante este período, entonces también aumentarán las tarifas de transacción, haciendo que el Blockchain de Bitcoin sea viable como un sistema de compensación interbancario,

pero no como una red de pagos. También es importante tener en cuenta que pueden surgir nuevos sistemas de pago por fuera de las cadenas, brindando pagos más baratos, pero al mismo tiempo centralizando la red y cambiando su naturaleza descentralizada.

La siguiente tabla muestra posibles escenarios futuros para fines de 2016, asumiendo que la dificultad de la red de hashing aumente en la misma proporción que el precio del BTC:

Escenario	Costo de la transacción en Bitcoin para mineros	Costo de la transacción en RSK para mineros
El precio del Bitcoin aumenta x10	16 USD	2 centavos
Los TPS aumentan x10 mediante hard-fork	11 centavos	0,2 centavos
El precio del BTC y el TPS aumentan x10	1,1 USD	2 centavos

A medida que el costo de incluir una transacción en Bitcoin aumente, los usuarios migrarán a plataformas con menores costos por transacción, como RSK.

Casos de uso de RSK

La plataforma RSK brinda smart contracts turing completos de acuerdo con lo propuesto por Nick Szabo en 1993. Al mismo tiempo, la VM de RSK es totalmente compatible con la VM de Ethereum, por lo tanto, RSK ofrece a los desarrolladores la oportunidad de trabajar en Ethereum para beneficiarse de la robustez del Blockchain de Bitcoin. A continuación, presentamos una lista de potenciales smart contracts y casos de uso que pueden ser desarrollados en RSK.

Canales de micropagos y redes Hub-and-Spoke

Los canales de micropagos permiten que dos partes realicen pagos regulares con valores bajos de manera segura sin tener que pagar comisiones por cada pago, pero solo una vez cuando el canal se cierra.

Las redes Hub-and-Spoke permiten a usuarios que no confían unos en otros realizar pagos únicos de bajo costo indirectamente utilizando canales de pagos hacia y desde terceros con mínima confianza. RSK permite que las redes Hub-and-spoke sean implementadas directamente con mínimas molestias y tengan una interfaz nativa en relación con las e-wallets.

Intercambio distribuido entre pares

Utilizando el protocolo de TierNolan, RSK soporta contratos que actúan como intercambios entre pares. El emparejamiento automático en una cartera de pedidos puede crearse con facilidad. Esto permite la distribución de mercados con blockchains independientes, intercambiando criptoactivos sin la necesidad de incluir a terceros.

Sistema de pagos al por menor

RSK permite adoptar el BTC globalmente para operaciones minoristas cotidianas. Una de las principales limitaciones de Bitcoin para su uso en compras minoristas es el tiempo de confirmación (de 10 minutos a 1 hora para asegurar la irreversibilidad). RSK permite a los consumidores beneficiarse de la seguridad de Bitcoin con confirmaciones que tardan tan solo unos segundos. Los comerciantes podrán aceptar pagos instantáneamente sin requerir pasarelas de pagos de terceros. Otro elemento clave que cualquier plataforma debería tener para triunfar en el mercado minorista es poder soportar una gran cantidad de transacciones por segundo (tps). La red de RSK, utilizando el protocolo de DÉCOR+, permite procesar en el Blockchain de Bitcoin hasta 300 tps (el doble que PayPal)

Servicios de depósitos en garantía

RSK permite crear servicios de depósitos en garantía inteligentes en los que los oráculos firman (o no) transacciones definiendo si deben ser ejecutadas (o no) sin la necesidad de tener contacto con los fondos en garantía.

Creación de criptoactivos

RSK permite la creación de criptoactivos (o altcoins) asegurados por la red de Bitcoin. Dada la flexibilidad de RSK en cuanto al precio del fuel del contrato, esta aplicación (al igual que todas las demás) puede ser utilizada tanto por estudiantes como por bancos y empresas.

Securitización de activos

RSK también permite la creación de tockens digitales respaldados por activos reales. Esto puede ser utilizado para comercializar REIT, acciones, emisiones de deudas o cualquier otro activo (actual o futuro) de manera digital. Este caso de uso en particular brindará una solución única para aquellas pequeñas empresas en países en vías de desarrollo donde los mercados tradicionales no satisfacen la demanda de capital de trabajo o de crecimiento.

Remesas descentralizadas

Este caso de uso es particularmente importante en el caso de economías en desarrollo en las que la población no bancarizada o indocumentada tiene que pagar tarifas de usura para enviar dinero a sus familiares como fuente de alimento y refugio.

Protección de IP/Registry

RSK permite el desarrollo de contratos que pueden replicar lo que se conoce como prueba de existencia, que permite a personas y empresas probar la existencia de determinado documento (o derecho de propiedad) en cualquier momento con la seguridad del Blockchain de Bitcoin. Esta caso de uso podría ser particularmente importante en sociedades de Latinoamérica, África y Asia con mecanismos poco confiables de registro de tierras.

Sistema de votación

Como un caso particular de criptoactivo, RSK permite la creación de votos digitales que permiten elecciones extremadamente seguras y transparentes a costos mínimos.

Micropréstamos

Más del 50 % de la población mundial no tiene acceso al sistema financiero tradicional. Esta falta de acceso a los créditos es una causa directa de la desigualdad económica que nuestra sociedad mundial enfrenta hoy en día. RSK posibilita el desarrollo de contratos digitales escalables de micropréstamos que podrían brindar acceso a créditos a los 3 mil millones de habitantes más pobres del planeta.

Seguimiento de cadenas de suministro

RSK permite la creación de wallets digitales para rastrear y seguir (digitalmente) la ubicación física de un determinado producto o partida. Este tipo de contrato podría ser particularmente útil en el caso de la industria minorista, alimenticia y sanitaria, entre otras. Al igual que en todos los demás casos de uso, al utilizar RSK se podría lograr esto con la seguridad del blockchain de Bitcoin, a un costo mínimo.

Reputación online e identidad digital

Uno de los principales problemas del mundo en vías de desarrollo es la falta de documentación e identificación para las personas en situación de pobreza. Esto impide que estas personas puedan votar, acceder al sistema de salud, reportar crímenes

y abusos y acceder a ayudas económicas. RSK permite crear registros digitales globales tan seguros como el Blockchain de Bitcoin a un costo extremadamente bajo.

Moneda global in-game

Muchos juegos multi-jugador tienen economías in-game, lo cual incluye monedas privadas. A medida que estos juegos evolucionan, las monedas virtuales se vuelven tan valiosas para los jugadores como el dinero fiat, y suelen intercambiarse en mercados secundarios. La inflación, las trampas y los robos online pasan a ser preocupaciones de los usuarios. Asimismo, las compañías creadoras de los juegos pueden llegar a enfrentar obstáculos legales y de seguridad por tener el dinero virtual de los usuarios en consignación. A medida que el mundo se vuelve más global, también lo harán los juegos virtuales, y los jugadores se sentirán molestos con el hecho de que el dinero ganado en un juego no pueda gastarse fácilmente en otro juego. RSK puede resolver estos problemas al permitir que los juegos acepten BTC (en su equivalente de monedas RSK) para sus pagos in-game, o crear un activo digital privado protegido por RSK. Los pagos de RSK pueden ser tan rápidos como los sistemas de ciclo cerrado para denominaciones bajas, de modo que los motores de juegos pueden utilizar a RSK como el sistema de compras in-game, para intercambios entre jugadores y para ofertas virtuales entre la empresa y sus jugadores. Con un simple clic en una URL o escaneando un código QR, se puede accionar una operación utilizando el software de e-wallet externo del jugador, y también pagando comisiones a la compañía de juegos.

Apuestas por Internet y mercados de predicción

Los pagos rápidos equivalen a cobros rápidos. Algunos sitios de apuestas de Bitcoin como SatoshiDice han encontrado la forma de brindar una experiencia de apuesta rápida sin registro utilizando confirmación cero y transacciones encadenadas, pero con riesgos de seguridad para el sitio de apuestas. RSK permite realizar apuestas con cobros casi instantáneos mediante la confirmación de bloque.

Juego limpio

Al incorporar smart contracts, y en conjunto con protocolos criptográficos cuidadosamente estudiados, tales como Mental Poker, RSK es capaz de brindar una plataforma abierta y justa para jugar juegos de cartas sin el requisito de contar con un tercero de confianza que cobre comisiones.

Existen unos pocos ejemplos entre muchos otros que podrían ser desarrollados y programados en la plataforma de RSK mediante el uso de la tecnología Bitcoin subyacente. Es importante mencionar que los mineros de Bitcoin (a través de la minería fusionada) serán quienes gestionen estos contratos y obtengan beneficio de la mayor parte del fuel consumido para gestionar esos contratos.

Descripción general de la tecnología

La plataforma de RSK es, en esencia, la combinación de:

- Una máquina virtual determinística de Turing completa de recursos contabilizados (para smart contracts)
- Una cadena lateral de Bitcoin de conector bidireccional (para la operación denominada en BTC)
- Un protocolo híbrido dinámico de consenso de minería fusionada/federada (para consenso en materia de seguridad), y una red de baja latencia (para pagos rápidos).

Máquina virtual de Turing completa

La máquina virtual de RSK (RVM) es el núcleo de la plataforma de smart contracts. Los smart contracts son ejecutados en paralelo por un alto porcentaje de nodos de la red. El resultado de la ejecución de un smart contract puede ser el procesamiento de mensajes intercontractuales, creando transacciones monetarias y cambiando el estado de la memoria persistente de los contratos. El nivel del código de operación de RVM compatible con EVM, para permitir que los contratos de Ethereum fluyan sin problemas en RSK. En la primera versión, la VM se ejecuta por interpretación. Para la próxima versión, se planea emular a EVM reorientando dinámicamente a los códigos de operación de EVM hacia un subconjunto de bytecode similar al Java, y una VM con seguridad aumentada y memoria restringida, también similar a Java, será la nueva VM (RVM2). Esto hará que se ejecuten los códigos de RSK a un rendimiento cercano al código nativo.

Principales funcionalidades:

- VM independiente, pero compatible con EVM a nivel del código de operación.
- RSK le brinda a los usuarios de Ethereum la posibilidad de gestionar sus proyectos con la seguridad de la red de Bitcoin.
- Nuevos códigos de operación para aritmética int32 rápida y mejor compilación en tiempo de ejecución (planeado) para una mejora en el rendimiento.

Cadena lateral (sidechain)

Una cadena lateral es un blockchain independiente cuya moneda nativa está vinculada al valor de otra moneda de blockchain automáticamente mediante el uso de pruebas de pago. Existe un conector bidireccional cuando dos monedas pueden ser intercambiadas libre y automáticamente, y sin incurrir en una negociación del precio. En RSK, el SmartBitcoin (SBTC) cuenta con conectores bidireccionales a BTC (más precisamente, un Rootoshi, la unidad mínima de cuenta de RSK, está vinculado con un Satoshi, la unidad mínima de cuenta de Bitcoin).

En la práctica, cuando los BTC son intercambiados por RTS, no se «transfiere» ninguna moneda entre los blockchains en ninguna transacción, dado que Bitcoin no puede verificar la autenticidad de los balances en otro blockchain. Cuando se realiza una transferencia, algunos BTC se bloquean en Bitcoin y la misma cantidad de RBTC se desbloquea en RSK. Cuando es necesario volver a convertir SBTC en BTC, los SBTC se bloquean de nuevo en RSK y la misma cantidad de BTC se desbloquea en la blockchain de Bitcoin.

Cadenas laterales *Semi-Trust-Free*

Es posible crear conectores bidireccionales totalmente confiables y sin participación de terceros mediante el uso de smart contracts en ambas plataformas. Pero dado que Bitcoin no soporta contratos ni códigos de operación nativos para validar pruebas externas de SPV, parte del sistema de conectores bidireccionales en RSK requiere confiar en un conjunto de terceros semi-confiables (STTP). Ningún STTP por sí solo puede controlar los BTC bloqueados, pero solo una mayoría de ellos tiene la habilidad de liberar fondos BTC. Los STTP almacenan temporalmente los BTC que se encuentran bloqueados, y desbloquean los BTC para pagarle a los usuarios de Bitcoin. Los SBTC son bloqueados en RSK para ser transferidos nuevamente a Bitcoin.

En RSK, los STTP que protegen los fondos bloqueados son precisamente los miembros de la Federación. Esto se debe a que los incentivos de la Federación están altamente alineados con los STTP: deben ser miembros respetados de la comunidad, como universidades, y también deben contar con la habilidad técnica para mantener la seguridad de un nodo de red. El bloqueo y desbloqueo de fondos se realiza a través de estos nodos de red seguros sin ninguna intervención humana. Por lo tanto, un requisito para formar parte de la Federación es la capacidad de auditar el comportamiento apropiado del software que maneja el nodo, en especial la corrección del componente que decide sobre la liberación de fondos de BTC. Planeamos crear hardware a prueba de alteraciones que haga cumplir el algoritmo de validación federado para continuar mejorando la seguridad.

Una vez que Bitcoin agrega códigos de operación especiales o extensibilidad para validar pruebas de SPV como hard-fork, y una vez que se corrobora que el nuevo sistema es seguro y trust-free, el rol de la Federación como STTP ya no será necesario, y el equipo de RSK implementará los cambios para adaptar a RSK al sistema trust-free.

Minería fusionada híbrida dinámica/Federación

Creemos que una PoW es el único sistema de consenso que evita que se reescriba el historial de blockchain a un bajo costo. El resto de los sistemas de consenso que no consumen un recurso valioso para la minería tienen esta desventaja, confían en la reputación, y previenen la participación anónima en la minería. Todos los demás sistemas de consenso requieren que los nuevos usuarios confíen en una serie de partes para encontrar un punto de verificación autenticado en el libro.

El consenso en las tasas elevadas de una PoW basado en bloques periódicos con pérdidas bajas de huérfanos requiere que los mineros detengan su hardware de minería y lo reinicien para minar nuevos encabezados de estatus medio cada vez que un nuevo bloque sea resuelto por la red. Esto da como resultado brechas de tiempo, o mayores latencias de red para cambios de estatus medio. Estas brechas temporales reducen la eficiencia de la minería en Bitcoin incluso si consumen tan solo algunos milisegundos. Por lo tanto, RSK utiliza el esquema de reparto de recompensas de bloques DECOR+ para reducir la competencia y permitir a los mineros la conmutación tardía al mejor bloque de RSK. Si los mineros cambian su hardware cada vez que se encuentra un bloque de RSK, compiten por una recompensa total de bloque de RSK. Si lo cambian más tarde y continúan con su actividad de minería, crean tíos y ganan una parte de la recompensa del bloque. En ninguno de estos casos son completamente huérfanos, dado que DECOR+ paga una recompensa a los bloques tíos y la regla de GHOST cuenta a los tíos como bloques

normales y así asegura la mejor cadena. Por lo tanto, se maximiza la eficiencia de la minería de BTC.

Esperamos un período en el que el poder de hashing de RSK se encuentre por debajo del 50 % del total del poder de hashing de BTC. Esto dejaría a la red vulnerable a un ataque del 51 % en el que el poder de hashing restante supere al poder de hashing existente de RSK hasta un gasto por duplicado.

Para evitar dicha situación, RSK incluye puntos de verificación federados para bloques minados de PoW. Los puntos de verificación de la Federación son firmados por los miembros de la Federación y los clientes pueden usar la mayoría de las firmas para decidir cuál es la mejor cadena. Asimismo, RSK cuenta con un protocolo de último recurso de acuerdo con el cual si el poder de minería cae por debajo del 5 % del poder de hashing de Bitcoin, la Federación tiene la posibilidad de crear bloques firmados. Por defecto, los clientes dejan de usar puntos de verificación federados cuando el poder de hashing de Roostock se encuentra por encima del 66 % de la dificultad máxima de hashing de BTC observada en la mejor cadena y las tasas pagadas en un bloque son mayores o iguales a la recompensa promedio de un bloque de bitcoin.

La plataforma de RSK se publicará con una federación de conocidos y respetados miembros de la comunidad. Cada miembro es identificado con un código público para el sistema de firma de los puntos de verificación. La federación puede agregar o quitar miembros utilizando e integrando un sistema de votación, aunque estas acciones requerirían un alto porcentaje de votos de los miembros.

El objetivo de los fundadores de RSK es que la red de RSK incentive la minería fusionada. Sin embargo, RSK es robusto en contra de la escasez en la minería fusionada, e integra automáticamente a la Federacación para asegurar a la red en caso de escasez.

Principales funcionalidades:

- 1 día de maduración para las recompensas de minería.
- Puntos de verificación de los miembros federados
- Puntos de verificación integrados por código durante el período de arranque.
- No se espera ninguna pérdida en la eficiencia de la minería en Bitcoin como consecuencia de la minería de fusión (menos del 0,1 % para cambios de estatus medio inmediato y 0 % para cambios tardíos)

Pagos rápidos y red con baja latencia

RSK tiene el objetivo de ser una mejor red de pagos. Para lograr rapidez en los pagos, se han desarrollado diversas soluciones:

- Uso de selección de bloques libre de competencia (por ejemplo, Hyperledger, Ripple, sistemas de ciclo cerrado)
- Utilización de redes hub-and-spoke (por ejemplo, la red Lightning de Bitcoin)
- Uso de tasas altas en bloques de PoW

Las redes Hub-and-spoke agregan nuevos nodos de centralización y requieren la adaptación completa de las wallets de clientes a un nuevo y totalmente diferente modelo de pago. A pesar de que esta alternativa puede ser implementada fácilmente en RSK, no es un sistema nativo de pagos rápidos. RSK adopta los protocolos de DECOR+ y

FastBlock5, que permiten alcanzar una tasa promedio de bloqueo de 10 segundos que no incentiva la centralización de la minería, previene el egoísmo en la minería y es compatible con los incentivos.
Principales funcionalidades:

- Intervalo de bloques de 10 segundos
- Protocolo de propagación de bloques en dos etapas (2SBP)
- Protocolo para impulsar transacciones faltantes (PMT)
- Propagación completa por la red de los bloques más recientes para prevenir el egoísmo en la minería y reducir la tasa de bloques huérfanos.
- Heurística para la inclusión de transacciones demoradas (DTI). Las transacciones se demoran 5 segundos en cada cola de transacción de bloque de los mineros para permitir una rápida verificación de los bloques, dado que las transacciones ya están presentes en los grupos de cada nodo en la red.
- Nuevo comando de red para difundir los encabezados de bloques priorizando el tiempo.
- Nuevo comando de red para difundir la lista de hash de las transacciones de bloques inmediatamente después de propagar el encabezado del bloque.
- Heurística para la minería en bloques sin verificar (MUB). Minería en encabezados de bloques con transacciones sin verificar con una demora de 5 segundos.
- Los encabezados de bloques son señalados cuando no tienen transacciones (excepto por Coinbase)
- Dos flujos priorizados para cada protocolo de conexión (2PSC). Nueva capa de transporte de mensajes con división de mensajes, que permite dos sesiones paralelas con diferente prioridad. Esto permite que los encabezados de bloques se envíen en la sesión de alta prioridad e interrumpan cualquier mensaje que esté siendo transmitido en la sesión de baja prioridad.
- Protocolo de optimización de ruta local (LRO). Ruta local óptima para bloques basada en las prioridades de pares. Ruta local óptima para transacciones basada en las prioridades de pares
- Protocolo DECOR+ para compartir recompensas entre bloques competidores.
- Protocolo GHOST para ponderación de cadenas.

Comparación de funcionalidades de RSK

Intentamos comparar las funcionalidades de RSK con aquellas de otras blockchains, y mostramos que, esencialmente, RSK presenta mejores opciones técnicas sin afectar la descentralización, donde esta se mide como el costo inverso de gestionar una instancia de nodo completo.

Artículo	Bitcoin	Ethereum	Factom	Contraparte	RSK
Tiempo de confirmación promedio	10 min.	12 segundos (GHOST)	1 min. (Servidores federados)	10 min.	10 segundos (DECOR+GHOST)
Umbral de seguridad (debido a la minería egoísta)	~30 %	Entre 30 % y 50 %	~30 %	~30 %	50 % (DECOR+GHOST)
Smart contracts Turing completos	No	Sí	Sí	Planeado	Sí
Agrega valor al Bitcoin	-	No	No	No	Sí (orientado a la fusión)
Integración con Bitcoin	-	No	Protocolo de superposición	Protocolo de superposición	Cadena lateral (sidechain)
Escalabilidad vía verificación probabilística y pruebas de fraude	No	No	No	No	Sí
Clientes SPV	Sí	Sí	No	No	Sí
Columna vertebral del relé de bloque	Sí	No	Sí	Sí	Sí
Soporte nativo para estructuras de acceso definidas por el usuario	Sí	No	Sí	No	Sí
Soporte nativo para esquemas de firma definidos por el usuario	No	No	No	No	Sí
Fácil integración del hardware wallet	No	Sí	No	No	Sí
Garantía de seguridad	Mineros de SHA256D	Mineros de Ethash	Mineros de SHA256D + federación	Mineros de SHA256D	Mineros de fusión de SHA256D + federación
Transacciones confidenciales	No	A través de un contrato	A través de un programa externo	No	Soporte nativo planeado utilizando el protocolo de AppeCoin
ID de transacción único	No (maleable)	Sí	No	No	Sí
Escalabilidad [tps]	de 3 a 24	ilimitado	ilimitado	de 3 a 24	300 en el inicio
Token nativo	BTC	ETH	FACTOID	XCP	BTC mediante conector bidireccional

Adelanto de la Tecnología de pagos instantáneos

Desde la creación de Bitcoin, ha habido una carrera por lograr menores intervalos para criptomonedas basadas en el blockchain de una PoW. Primero, estuvo Bitcoin con un intervalo de 10 minutos, luego vino LiteCoin utilizando un intervalo de a 2,5, luego DogeCoin con 1 minuto, QuarkCoin con 30 segundos, y Ethereum con 12 segundos. Cada criptomoneda nueva lo baja un poco más, pero muy pocos diseñadores saben realmente cuáles son las consecuencias de hacerlo. Para entender cómo el intervalo entre bloques afecta la estabilidad y la capacidad de la red de cripromonedas, es necesario tomar en cuenta diversos factores. Antes que nada, el factor más importante que afecta la viabilidad de los intervalos cortos de confirmación es el número de bloques huérfanos generados. Otros dos factores principales afectan la tasa de bloques huérfanos: el protocolo de propagación de bloques y el tiempo de propagación de los bloques entre los principales mineros. Para RSK, hemos analizado cuidadosamente estos factores y realizado simulaciones a fin de verificar el rendimiento, el uso y la seguridad de la red. En esta sección, revisaremos los nuevos protocolos de RSK para reducir la tasa de bloques huérfanos.

Protocolo DECOR+

En la red Bitcoin, cuando dos o más mineros han resuelto bloques a la misma altura, se crea un claro conflicto de intereses. Cada minero competidor quiere que su bloque sea seleccionado por el resto de los mineros como la mejor punta de la cadena, mientras que al resto de los mineros no suele importarles cuál es elegido. Sin embargo, todo el resto de mineros y usuarios honrados preferiría que todos eligiesen la misma punta de bloque, porque esto reduce la probabilidad de revocación de bloque. La solución ideal incentivaría a los mineros en conflicto a elegir el mismo padre también, y DECOR+ establece los incentivos económicos apropiados para una elección convergente, sin requerir mayor interacción entre mineros. DECOR+ es una estrategia que comparte recompensas e incentiva económicamente a resolver el conflicto de modo que:

1. El conflicto se resuelva de manera determinística cuando todas las partes tengan acceso a la misma información en cuanto al estado de un blockchain.
2. La resolución elegida sea la que maximice todas las ganancias de los mineros, tanto de aquellos que están en conflicto como de los demás.
3. El tiempo necesario para resolver el conflicto sea insignificante.

Protocolo de propagación de bloques

Bitcoin e Ethereum envían cada bloque incluyendo todas las transacciones contenidas en el bloque en su encabezado. Si bien esta estrategia es la más fácil de analizar, es sabido que su rendimiento no es bueno tanto en cuanto a la latencia en la propagación de bloques como en el uso de banda ancha, que se doblega. Los mineros de Bitcoin resolvieron este problema parcialmente utilizando la red de relé rápido: es una columna vertebral centralizada que transmite bloques de manera comprimida, y es mantenida por un usuario único. RSK nació con una red de relé rápido integrada en el protocolo de red, y las propiedades de baja latencia surgen de la topología de la red y no requieren centralización.

Propagación de bloques en dos etapas (2SBP)

Los bloques de RSK son enviados en dos etapas: en la primera parte, solo se envía el encabezado del bloque. En la segunda parte, se envía la lista de hashes de las transacciones incluidas en el bloque. Utilizando 2SBP, se duplica la capacidad del canal, permitiendo almacenar más transacciones en cada bloque. Una vez que cada nodo ha recibido el encabezado del bloque y la lista de hashes de transacciones con el encabezado del bloque, el nodo intenta reconstruir el bloque para verificarlo completamente.

Protocolo para impulsar transacciones faltantes (PMT)

Dado que cada nodo almacena los hashes de las transacciones publicitadas por sus pares, el minero también envía inmediatamente las transacciones incluidas en el bloque que reconoce como faltantes en el grupo de cada par. Esto elimina completamente la necesidad de una segunda interacción para solicitar transacciones adicionales. Enviar las transacciones faltantes antes de que sean solicitadas por un par es una tercera fase del protocolo de 2SBP.

Heurística para la inclusión de transacciones demoradas (DTI)

Los mineros solo incluyen transacciones que han sido recibidas tan solo unos pocos segundos atrás. Esto asegura con alta probabilidad que las transacciones ya habrán sido recibidas por pares antes de que el bloque sea minado. Tenga en cuenta que demorar las transacciones es el mayor interés de los mineros, ya que reduce el tiempo de verificación de los bloques y disminuye las chances de que aparezcan bloques competidores. Esta optimización no es necesaria cuando la heurística para la minería en bloques sin verificar (MUB) se encuentra en efecto en la red.

Propagación inmediata de los encabezados de bloques (IBHP)

Cuando se recibe un encabezado de un bloque que se encuentra actualizado, los nodos envían el encabezado del bloque antes de chequear las transacciones o la validez del bloque, y solo chequean la PoW del bloque y la altura al momento del envío. Esto permite que el encabezado se propague por la red en menos de un segundo.

Dos flujos priorizados para cada protocolo de conexión (2PSC)

Cada conexión de red incluye dos flujos lógicos bidireccionales con dos prioridades diferentes. El flujo de alta prioridad se utiliza para enviar el encabezado del bloque inmediatamente incluso si se está enviando un mensaje de baja prioridad en el flujo de baja prioridad.

Heurística para la minería en bloques sin verificar (MUB)

Los nodos pueden entonces comenzar la minería con un bloque vacío además del encabezado incluso si las transacciones aún no están allí, durante un intervalo fijo. Luego

del intervalo, continúan con la minería en cualquier bloque que estuvieran minando previamente. Estos bloques vacíos reducen el ancho de banda efectivo y el uso del almacenamiento del blockchain, pero las simulaciones demuestran que si se utiliza un DBI, el número de bloques vacíos generados y el espacio requerido para almacenarlos, así como la reducción en el TPS, son bajos.

Protocolo de optimización de ruta local (LRO)

Para reducir el número de bloques huérfanos, es importante reducir la latencia de transferencia entre mineros. La red de RSK se optimiza de manera dinámica para reducir la latencia entre mineros y para priorizar el tráfico entre mineros. En otras palabras, RSK integra una red de relé rápida en la red de pares, mejorando el protocolo gossip con geolocalización y rutas locales óptimas. La ruta de envío de bloques entre mineros es una ruta crítica para la propagación de bloques y, por lo tanto, es de extrema importancia para la red de pares. La existencia de nodos de red no mineros en la red de pares en la ruta crítica tiende a aumentar la tasa de bloques huérfanos. Los nodos no mineros (tales como los usuarios finales o los nodos de monitoreo) en la ruta crítica solo pueden servir a los mineros como débiles saltos de anonimización. Para crear las rutas críticas desde decisiones de nodos únicamente locales, se realiza una priorización de nodos utilizando el protocolo LRO. Este protocolo crea una integración dinámica de un grafo acíclico dirigido (DAC) hacia la topología aleatoria de la red de RSK, donde este DAC conecta a los mineros de manera óptima.

Reutilización de la red de minería de Bitcoin

Una red de minería concentrada, con grandes grupos de minería, tiende a generar muchos menos bloques huérfanos que una topología de minería de distribución completa. Por lo tanto, con respecto a los pagos rápidos, las criptomonedas basadas en SHA-256D PoW tienen una ventaja por sobre las criptomonedas no compatibles con ASIC basadas en PoW.

La verdadera topología de la red

El diseño de Bitcoin asume que la red es similar a una gráfica aleatoria, con cierto promedio de grado de salida y entrada. Si bien esto está lejos de ser cierto en la realidad, los nodos de la red toman decisiones locales para evitar formar conglomerados geográficos (al menos para el caso de las conexiones salientes). Esta no es la mejor topología para ayudar a la propagación de bloques. La mejor topología para la propagación de bloques es aquella que sea más beneficiosa para los mineros principales, al impulsar las conexiones directas entre ellos y brindar una ruta más rápida para los bloques entre ellos. Asimismo, un eje central directo de minero a minero puede ayudar a reducir notablemente el número de bloques huérfanos. Esto ha sido propuesto por Bitcoin para aumentar la resiliencia a los ataques. RSK utiliza heurística LRO para establecer una columna vertebral dinámica para los mineros, sin incurrir en el costo de la autenticación de minero a minero, en la privacidad del minero, en la divulgación de la dirección IP y en posibles ataques DoS relacionados.

Tiempo de verificación de la función de PoW

SHA-256 es muy rápido de evaluar, por lo tanto, la verificación de tiempo de PoW de Bitcoin es insignificante. Un scrypt PoW, por el contrario, puede tardar de 3 a 30 milisegundos en ser evaluado según los parámetros elegidos (GPU o «resistencia» ASIC). Para proteger a la red del spam y de los ataques DoS, cada nodo necesita verificar la PoW del bloque antes de volver a enviar el encabezado del bloque, de modo que la demora de la verificación se multiplica por la cantidad de saltos en la ruta crítica del bloque entre mineros.

Pila de redes de clientes

Una vez que un nodo recibe un encabezado de bloque, lo mejor que puede hacer para reducir la creación de bloques huérfanos en la red es reenviarlo tan rápido como sea posible. Esto significa que toda otra actividad de nodo debería pausarse o detenerse. El diseño de RSK permite que las operaciones con baja prioridad se cancelen inmediatamente y acepta reintentos. Para permitir el envío inmediato, la pila de redes del cliente no bloquea al cliente en los procedimientos de verificación de las transacciones ni en ninguna otra actividad de gestión, tales como las reorganizaciones de cadenas. Esto se logra a través de un cliente de RSK al que se le permite el multihilo y se le asignan dinámicamente prioridades de hilos para impulsar al hilo que acaba de recibir del encabezado del bloque.

Gastos generales del bloque

Los encabezados de bloques en la mayoría de las criptomonedas son pequeños (~100 bytes) de modo que el tamaño del encabezado (en comparación con el de todo el bloque) no implique un gasto significativo. El encabezado de RSK es más grande, pero los gastos generales por el encabezado del bloque no tienen un impacto notoriamente negativo en el tiempo de propagación, dado que la red de bajo nivel MTU suele ser de 1500 bytes, lo cual está por encima del tamaño del encabezado del bloque.

Simulaciones

Hemos simulado la propagación de bloques utilizando una simulación de eventos discreta construida específicamente para este propósito. El simulador simula la interacción entre una pequeña serie de grandes mineros, cada uno en un gráfico aleatorio en el que la distancia de salto entre ellos es cercana a la distancia promedio entre los nodos de la red. Incluso si este no es el peor de los casos, dado que el estar bien conectados es el mejor interés de los grandes mineros, asumimos que los mineros tienen un rendimiento que no es peor que el promedio. Los eventos simulados son la creación de un bloque en una de las ubicaciones y la propagación del bloque a cada una de las demás ubicaciones de los mineros. Los siguientes resultados muestran la simulación RSK con un intervalo de 5 bloques y 300 TPS (actualmente, el intervalo entre bloques es de 10 segundos). El resultado de simulación clave es que una transacción es aceptada con una probabilidad del 99,98 % (probabilidad de revocación del 0,02 %) antes del transcurso de 20,35 segundos. Tenga en cuenta que esta probabilidad de revocación no toma en cuenta que el fork de remplazo también puede contener la transacción eliminada, de modo que en la práctica puede ser mucho más bajo.

Minería fusionada segura

La minería fusionada es una técnica que permite a los mineros de Bitcoin minar simultáneamente otras criptomonedas con un costo marginal casi igual a cero. La misma infraestructura y configuración de minería que utilizan para minar Bitcoins se reutiliza para minar RSK de manera simultánea. Esto significa que, dado que RSK paga tarifas de transacción adicionales, el incentivo para la minería fusionada es alto. Sin embargo, también significa que el costo de atacar a la red utilizando la técnica de *pump-and-dump* o cadenas paralelas está por debajo del costo de atacar criptomonedas no fusionadas. RSK cuenta con diversas protecciones para prevenir ataques durante la fase inicial de arranque:

- Puntos de verificación federados: Los clientes de RSK esperan puntos de verificación firmados por miembros de la Federación. La Federación incluirá cambios y otras partes altamente seguras involucradas en el éxito de la plataforma. Los nodos utilizan nodos federados para detectar ataques de Sybil e informar a los usuarios.

- Madurez de las monedas minadas: cada moneda de un minero tiene un tiempo de maduración de 24 horas, apenas mayor en el caso de Bitcoin. El aumento en el tiempo de madurez de las monedas reduce los incentivos para los ataques de tipo *pump-and-dump*.

- Puntos de verificación integrados en el código fuente

Privacidad en las transacciones

RKS no brinda por sí mismo una mejora en la privacidad de las transacciones con respecto a Bitcoin, y utiliza seudónimos. Sin embargo, la VM de RSK es Turing completa, de modo que es posible implementar tecnologías de anonimización como CoinJoin, firmas de anillo o zCash de manera segura sin la necesidad de confiar en terceros.

Seguridad

La minería fusionada no ha sido ampliamente utilizada por las monedas alternativas, dado que durante el período inicial de arranque de una criptomoneda, ofrece grandes grupos de minería de Bitcoin para perturbar a las nuevas criptomonedas con ataques del 51 %. RSK implementa códigos de verificación federados como una forma segura de dar arranque a la plataforma y reducir notablemente este riesgo. A su vez, RSK será lanzado con un poder de hasing mínimo equivalente al 30 % del poder de hashing de Bitcoin. La Fundación RSK se encargará de monitorear la salud de la red y utilizará su sistema de alerta para informar a los usuarios y proteger a la red de ataques de retroceso.

Escalabilidad

RSK puede escalar mucho más allá de Bitcoin en su estado actual. Un pago de RSK requiere un quinto del tamaño de un pago estándar de Bitcoin, y la carga del bloque por intervalo de tiempo es 8 veces más alta que en el caso de Bitcoin. Asimismo, RSK proporcionará esquemas de firma seleccionables por el usuario: ECDSA, Schnorr y Ed25519. Este último tiene, por lo general, un rendimiento varias veces mayor que el de la curva ECDSA de Bitcoin.

Si todo lo demás permaneciera igual, RSK consume en promedio 50 % menos de banda ancha que Bitcoin, dado que los bloques no contienen datos de transacciones, sino que solo hacen referencia a transacciones previamente conocidas. El uso de almacenamiento y ancho de banda pueden reducirse aun más mediante verificación probabilística y técnicas de fragmentación.

Verificación probabilística y pruebas de fraude

El costo de tener un nodo completo es el factor principal que afecta el grado de centralización de una criptomoneda. Cuanto más alto es el costo, más alta es la centralización. Sin embargo, creemos que la posición maximalista respecto de la descentralización implica que la criptomoneda no puede convertirse en una red de pago global. Ambas metas se contradicen. Bitcoin ya proporciona una red altamente descentralizada, dado que el límite del tamaño del blockchain es lo suficientemente bajo para asegurar que la mayoría de los usuarios individuales puedan participar. Esto permite a la cadena lateral de RSK aumentar la escalabilidad más allá de Bitcoin, teniendo a la red de Bitcoin como una protección en contra de la centralización del control de la moneda.

Creemos que es posible encontrar un equilibrio entre terceras partes confiables, nodos de red confiables y auto-verificación, e invitamos a los usuarios a encontrar la relación con la que se sientan cómodos. La plataforma de RSK permite a los nodos almacenar y validar un subgrupo del blockchain completo para reducir el costo del nodo. Esto se realiza a través de la verificación probabilística y las pruebas de fraude. La verificación probabilística es una técnica mediante la cual un nodo (parcial) elige de manera aleatoria qué bloques verificará, y acepta al resto de los bloques siempre y cuando se cumpla con ciertas condiciones: que haya pasado determinado tiempo, que se hayan agregado ciertos bloques de confirmación, que la conectividad de red sea adecuada, que no haya ninguna publicación de prueba de fraude y, opcionalmente, que se hayan publicado algunos puntos de verificación válidos. Las pruebas de fraude son bloques etiquetados como «fraudulentos». Cada vez que un nodo recibe una prueba de fraude, verifica si se ha aceptado (pero no validado) de manera local un bloque con la misma altura y, de ser así, valida el bloque. Si es inválido, se reorganiza la mejor cadena local en consecuencia. El costo de publicar una prueba de fraude fraudulenta es alto, ya que las pruebas de fraude también implican pruebas de trabajo. Un nodo que recibe una prueba de fraude fraudulenta de un par, expulsa al par que hace trampa. De ser necesario, los nodos requerirán una prueba de trabajo inicial de los pares para prevenir DoS barato utilizando direcciones IP comprometidas. Los mineros (tanto de PoW como federados) deben ser nodos completos, para que un atacante que posea datos sobre un bloque (pero esté publicando el encabezado) no afecte a la mejor cadena, ya que los mineros descartarán el bloque del atacante rápidamente.

Conclusiones

RSK representa la culminación de 4 años de mejoras de tecnología en blockchain y permitirá que el ecosistema de las criptomonedas utilice las mejores funcionalidades del dinero y los pagos programables, a la vez que aumenta el valor del bitcoin (la moneda).
Permitirá a desarrolladores de todo el planeta crear soluciones personales y corporativas descentralizadas que funcionen en las redes más seguras de todo el mundo, con costos de transacciones bajos que se adecuen a una amplia gama de necesidades.

Permitirá a los mineros de Bitcoin participar en el mercado de Smart Contracts añadiendo mucho valor a la industria de la minería y asegurando su sostenibilidad a largo plazo.

Contribuirá a la creación de una base más amplia de mineros, que fortalecerán la seguridad de la red de Bitcoin.

Posibilitará el desarrollo de un sistema financiero instantáneo y accesible que creará inclusión y oportunidades para tres mil millones de personas que permanecen fuera del sistema bancario y perjudicados desde el punto de vista financiero en nuestro mundo.

Equipo Core de RSK