
RSK
ROOTSTOCK PLATFORM
BITCOIN POWERED
SMART CONTRACTS
WHITE PAPER

RSK

Smart Contracts impulsados por Bitcoin

Informe oficial
Descripción general

Revisión: 11
Fecha: 29 de enero de 2019
Por Sergio Demian Lerner

Introducción

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

Desde entonces, se han lanzado diversas criptomonedas con VM que analizan datos, capaces de soportar lenguajes de programación Turing completos, desatando todo el poder de los smart contracts. Se han desarrollado miles de aplicaciones descentralizadas que interactúan con los smart contracts, llamadas dApps, y han surgido nuevos casos de uso. Sin embargo, cada nueva plataforma utiliza un nuevo token nativo altamente especulativo y volátil.

Desde su bloque génesis el 3 de enero de 2009, Bitcoin se ha consolidado como la tienda de valor más adaptada, sólida y segura y el protocolo más seguro entre todas las criptomonedas. Pero la mayoría de las dApps requieren reglas más complejas que no pueden incluirse en el código de los predicados de Bitcoin similares a Forth. Esta limitación dio lugar al nacimiento de RSK en 2015, y al lanzamiento de su MainNet en enero de 2018. RSK es una plataforma que permite la ejecución de smart contracts que utilizan al bitcoin como activo nativo, contribuyendo al valor del Bitcoin como la criptomoneda líder en el mundo y expandiendo su alcance a todos los potenciales casos de uso de dApps. RSK es una cadena lateral de Bitcoin, por lo tanto, tiene su propia red y su propio blockchain, pero no tiene su propio token. La red de RSK brinda mejoras con respecto a Bitcoin, tales como transacciones más rápidas y mayor escalabilidad.

RSK es la evolución de dos plataformas, QixCoin y Ethereum. QixCoin fue una criptomoneda turing completa creada en 2013 por algunos de los fundadores de RSK. QixCoin introdujo el concepto de pago por ejecución, actualmente conocido como gas de transacción. Sin embargo, RSK heredó una serie de conceptos clave de Ethereum, como el formato de cuentas, la VM (máquina virtual) y la interfaz web3. Por lo tanto, RSK es altamente compatible con compiladores, herramientas y dApps de Ethereum.

En comparación con Bitcoin, RSK brinda una experiencia de pago mejorada con confirmaciones casi instantáneas. Sin embargo, RSK también está basado en prueba de trabajo soportando la minería de fusión SHA-256D, el mismo protocolo de consenso y la red de minería que asegura a Bitcoin. Desde enero de 2019, RSK tiene más del 40 % de la tasa de hashing de Bitcoin, dando como resultado la plataforma más segura de smart contracts del planeta en términos de energía invertida en la seguridad de la blockchain.

Para permitir que los bitcoins entren y salgan de RSK, RSK posee un conector bidireccional con Bitcoin. Cuando se transfieren bitcoins a un RSK blockchain, se convierten en «Bitcoins inteligentes» (ticker RBTC[1]). Los bitcoins inteligentes equivalen a bitcoins que viven en el RSK blockchain, y pueden transferirse nuevamente hacia bitcoins en cualquier momento sin ningún costo adicional, excepto por las tarifas estándar de RSK y Bitcoin. RBTC es la moneda nativa utilizada en el RSK Blockchain para pagarle a los mineros de bitcoin por las transacciones y el procesamiento de los

[1] En este informe oficial, «protocolo RSK» hace referencia a las especificaciones del protocolo. «Nodo de referencia de RSK» se refiere a la implementación de referencia. La moneda nativa de RSK es el Smart Bitcoin. El «ticker» o símbolo del smart bitcoin es «RBTC». «BTC» o «bitcoin» se refiere a la moneda nativa de Bitcoin. «Bitcoin» se refiere al protocolo de Bitcoin.

contratos. No se emiten monedas: todos los RBTC se crean a partir de bitcoins que vienen del Bitcoin blockchain.

Actualmente, RSK potencia a Bitcoin en las siguientes áreas:

- La Máquina Virtual de Turing completa de RSK (RVM) posibilita los smart contracts y es altamente compatible con la VM de Ethereum (EVM)
- En promedio, la primera confirmación para las transacciones no supera los 30 segundos.
- Minería de fusión con Bitcoin.
- Cadena lateral de conector bidireccional (actualmente un conector federado)
- Protección contra la minería egoísta utilizando el protocolo DECOR+

Asimismo, la comunidad de RSK está altamente unificada para seguir la visión original de agregar las siguientes funcionalidades en las próximas actualizaciones de la red:

- Renta de almacenamiento
- Optimizaciones en la propagación de bloques
- Proceso de transacción paralelo
- Un protocolo de compresión de transacciones (LTCP) para una mayor escalabilidad
- Soporte para una VM adicional con un mejor rendimiento basado en código byte Java o WAsm.
- Federación híbrida/conector basado en drivechain

Las funcionalidades futuras se describen en las propuestas de mejoras de RSK (RSKIP) descritas en el siguiente repositorio https://github.com/rsksmart/RSKIPs, junto con el código de la PoC.

RSK es un proyecto orientado a la comunidad. RSK Labs es una compañía fundada en 2015 para desarrollar la implementación referente del protocolo de RSK, y desde entonces ha pagado los salarios de algunos de los más destacados desarrolladores Core de RSK. Asimismo, RSK Labs brinda una plataforma de información sobre el sitio web de www.rsk.co y sirve como un host para diferentes servicios informativos.

Recursos útiles para comenzar

Sitio web de RSK Labs: https://www.rsk.co/
Estadísticas de RSK: https://stats.rsk.co
Navegador de RSK: https://explorer.rsk.co/
Grifo de RSK: https://faucet.rsk.co/
Estado de la red de RSK: https://twitter.com/RskSmartNetwork
Comparación de tarifas de RSK: http://rskgasstation.info/

Wallets compatibles con RSK:

MyCrypto: https://mycrypto.com
Jaxx: https://jaxx.io/ https:/
iBitcome: /www.ibitcome.com/
Metamask: https://metamask.io/

Hardware wallets compatibles con RSK:

Ledger: https://www.ledger.com/
Trezor: https://trezor.io/
D'CENT: https://idcent.io/

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

En las siguientes secciones, enumeramos diferentes razones por las cuales RSK es importante para el ecosistema Bitcoin.

Alineación de los agentes de Bitcoin y protección del valor

Uno de los objetivos de RSK es brindar una plataforma de smart contracts que beneficie a los principales actores del ecosistema de Bitcoin y a su comunidad. Esta filosofía se refleja directamente en el núcleo de su arquitectura, donde los mineros de Bitcoin brindan el poder de hashing necesario para asegurar a RSK y a las compañías líderes de la industria que integran la Federación que poseen las claves para proteger los fondos bloqueados en el sistema de conector bidireccional. El modelo de gestión de RSK tiene la meta de representar a todos los actores de la comunidad, participantes de RBTC, mineros, miembros de la federación, así como desarrolladores y usuarios finales de dApps. A largo plazo, el plan de la comunidad es permitir los mecanismos de señalamiento objetivos pero no vinculantes, integrados en las transacciones y los bloques, de modo que los usuarios pueden señalar con su participación, las aplicaciones de wallets y los remitentes puedan señalar etiquetando transacciones, los mineros puedan hacerlo etiquetando bloques, y los receptores puedan señalar etiquetando cuentas para una gestión aun más descentralizada y democrática.

Protección de las inversiones de los mineros de Bitcoin

En mayo de 2020, el margen de rentabilidad de la minería en Bitcoin caerá de 12.5 BTC a 6.25 BTC debido a las decrecientes recompensas de bloques. La reducción de la rentabilidad podría implicar el fin de muchas empresas y personas dedicadas a la minería, y la desconexión de vastas cantidades de hardware que aseguraban a Bitcoin. RSK, gracias a sus capacidades fusionadas de minería, ofrece a esos mineros la oportunidad de continuar llevando a cabo su actividad. 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, a través de la minería de fusión, los mineros estarán soportando nuevas aplicaciones imprevistas, que podrían significar una nueva oportunidad de negocio en el futuro.

Emisión de activos con valor estable mediante Bitcoins colateralizados

RSK permite la emisión de activos con precios vinculados con aquellos de una moneda fiat u otra materia prima bloqueando el bitcoin como garantía. Los activos estables logran una menor exposición a la volatilidad mientras que mantener al bitcoin como una moneda de reserva aumenta el valor general del bitcoin. El bloqueo de grandes

cantidades de Bitcoin reduce la liquidez y, por lo tanto, contribuye al aumento del valor del Bitcoin. Sin embargo, lo más importante es que estos tokens respaldados por Bitcoin en RSK permitirán micropagos con monedas estables, lo cual permitirá a miles de millones de habitantes que actualmente se encuentran marginados por el sistema financiero heredado participar de la economía global digital.

RSK a la vanguardia de la tecnología de cadenas laterales de Bitcoin

RSK Labs está explorando, investigando e implementando conceptos clave que son vitales para cualquier otra cadena lateral futura de Bitcoin. El éxito de RSK impulsará a otros desarrolladores de cadenas laterales a seguirlo y beneficiarse de la eficiente infraestructura de minería de fusión creada, los códigos de operación de drivechain propuestos, y la tecnología desarrollada para la creación segura de las federaciones multi-sig por RSK Labs. Al crear un software de código abierto, al igual que el firmware y el diseño del hardware, RSK Labs está promoviendo la ciencia y mejorando la funcionalidad y la seguridad del ecosistema de las criptomonedas en su totalidad.

RSK como red de pago de bajo costo de Bitcoin

Actualmente, una transacción de Bitcoin cuesta 24 ¢ en promedio[2], mientras que una de RSK cuesta 0,46 ¢ [3], lo cual es 50 veces más bajo. Esta es una mejora radical. Pero las tarifas de Bitcoin suelen aumentar o disminuir sobre la base de la demanda de espacio de bloques, y prevemos un crecimiento en la demanda de transacciones on-chain. Luego de diversos intentos no exitosos de aumentar el tamaño de los bloques de Bitcoin utilizando hard forks, y luego de la mejora única en el espacio de Segwit, no hay ningún plan en la comunidad de Bitcoin para aumentar el tamaño de los bloques. Podemos prever que las tarifas de transacción de Bitcoin pasen a ser prohibitivamente altas para la mayoría de las aplicaciones que impliquen transacciones personales diarias. Los bloques de RSK pueden contener muchas más transacciones que los bloques de Bitcoin debido al reducido tamaño de sus transacciones. Por lo tanto, RSK ofrecerá naturalmente tarifas mucho más bajas con el mismo volumen de transacciones. En la siguiente tabla, comparamos brevemente a Bitcoin y RSK.

Parámetro	Bitcoin	RSK
Tiempo de confirmación de bloque promedio	10 minutos	30 segundos (los mineros pueden bajarlo a 15 segundos)
Tiempo de confirmación sugerido para intercambios	30 minutos (3 bloques)	60 minutos (120 bloques) con la tasa de hash actual de la minería de fusión (40 %).
Máx. Transacciones por segundo	3.3 tps (asumiendo una transacción de tamaño promedio)	10 tps (transacciones externas, desde enero de 2019) 20 tps (transacciones internas)
Costo promedio de transacción actual	24 ¢	0,46 ¢

[2] https://bitcoinfees.info/
[3] http://rskgasstation.info/

El costo de las transacciones de Bitcoin está directamente relacionado con el valor de la recompensa del bloque. Añadir una transacción a un bloque demora su propagación. Cada milisegundo gastado en la propagación se paga proporcionalmente a la recompensa del bloque, ya que disminuye la probabilidad de que el bloque sea elegido por la red. Técnicas de reconciliación de datos (como los códigos Bose–Chaudhuri–Hocquenghem proporcionados por la biblioteca Minisketch) podrían, en caso de ser implementadas en Bitcoin, reducir esta dependencia. Actualmente, si aumenta el precio del Bitcoin, también aumentan las tarifas de las transacciones. Se cree que Bitcoin se convertirá en una suerte de sistema de compensación interbancario, pero no en una red de pagos. También es importante tener en cuenta que los sistemas de pagos off-chain, tales como Lightning Network, están emergiendo, pero es probable que estas redes aumenten la necesidad de transacciones on-chain para el establecimiento y la ampliación de los canales, lo cual también hará que aumenten los costos de transacción. A medida que este costo aumente, los usuarios migrarán a plataformas con costos de transacción más bajos. RSK brinda una excelente oportunidad para realizar transacciones en Bitcoin a un costo mucho más bajo.

¿Cuál es la importancia de RSK para los usuarios y desarrolladores de Ethereum?

Aumentar la base de usuarios de su DApp

RSK posee una base única de usuarios, inicialmente conformada por bitcoiners de Latinoamérica. Actualmente, RSK está creciendo tanto en Latinoamérica como en Asia. Al desplegar DApps compatibles sin dificultades tanto en Ethereum como RSK, los desarrolladores y las empresas pueden alcanzar a una base de usuarios más amplia y, al mismo tiempo, reducir su dependencia con cualquier blockchain en particular. Asimismo, existen actualmente diversas soluciones federadas que actúan como puentes entre Ethereum y RSK y transfieren tokens de una blockchain a la otra, de modo que el mismo token puede vivir en ambas blockchains.

Promover la estandarización de EVM/Web3

La comunidad de Ethereum creó la máquina virtual de smart contracts (EVM) y la interfaz para aplicaciones descentralizadas para interactuar con esta (Web3). Al adoptar estos estándares, RSK facilita a los desarrolladores la migración de sus aplicaciones a RSK y la reutilización de una gran parte del software de infraestructura desarrollado por Ethereum. Pero también ayuda con la estandarización, ya que brinda materiales de aprendizaje unificados y reduce la necesidad de aprender otra arquitectura de ejecución y otro lenguaje de programación. Al mismo tiempo, todas las herramientas desarrolladas por el ecosistema de RSK también estarán disponibles para usuarios de ETH.

Reducir los riesgos de forks persistentes

Ethereum realiza actualizaciones de red de manera periódica. Uno de los hard forks de Ethereum anunciados hace más tiempo, y aun así todavía debatido, es la migración del consenso de prueba de trabajo a prueba de participación. Este es un cambio tecnológico y económico radical, y se espera que los mineros de Ethereum lo confronten. Una nueva separación en la cadena forzará a los desarrolladores a elegir entre la cadena original

PoW y la nueva cadena PoS. Asimismo, también existe cierta incertidumbre en cuanto a la seguridad y estabilidad del nuevo protocolo de consenso. En caso de que falle, todos los usuarios que tengan Ether podrían verse afectados económicamente, de modo que el cambio podría ser reclamado por la comunidad de Ethereum. Además de esto, los desarrolladores core de Ethereum han implementado e implementarán cambios en el algoritmo de suplemento de dinero y prueba de trabajo que corroen la inmutabilidad y la neutralidad de la plataforma. RSK no cuenta con un token nativo especulativo, y los smart Bitcoins siempre pueden volver a transferirse a Bitcoin en caso de que un usuario no esté de acuerdo con una actualización de la red soportada por la comunidad de RSK. Por lo tanto, la comunidad de RSK muestra un nivel muy bajo de confrontación, lo cual minimiza el riesgo de una ruptura de la comunidad. Por otra parte, Bitcoin suele rechazar los hard forks. Por ende, RSK brinda una plataforma mucho más estable a mediano y largo plazo.

Proteger las inversiones de I+D desde el día 0 de las vulnerabilidades de seguridad de Ethereum

La mayor parte de las blockchains reciben actualizaciones de red periódicas, así como también actualizaciones de software. Para la mayoría de los proyectos de blockchain, la tecnología continúa siendo experimental, y los protocolos no son permanentes. Ethereum y RSK están lejos de la madurez. Esto significa que se podrían encontrar nuevas vulnerabilidades en materia de seguridad, tal como se han encontrado y explotado en Ethereum en el pasado. Incluso RSK, que cuenta con un excelente historial de seguridad, no está libre de riesgos. Sin embargo, la existencia de dos plataformas compatibles reduce el riesgo de que se pierdan recursos dedicados al desarrollo de una DApp debido a una falla catastrófica en la plataforma. La probabilidad de una falla conjunta es mucho más baja, especialmente teniendo en cuenta los diferentes protocolos de consenso involucrados.

Aumentar el rendimiento de transacciones portando DApps a RSK

A nivel técnico, RSK se destaca por encima de otras plataformas debido a cuatro propuestas de la comunidad que brindan una mayor escalabilidad on-chain. El primero es el proceso de transacción paralelo, especificado por RSKIP4, que permite que las arquitecturas multi-núcleo logren una utilización completa de los núcleos de procesamiento para el procesamiento de transacciones. Esto permite un aumento en el límite de gas del bloque, posibilitando un mayor rendimiento en las transacciones. El segundo es LTCP, especificado por RSKIP53, que posibilita la compresión de transacciones y el agregado de firmas de transacciones, permitiendo procesar muchas más transacciones con el mismo espacio y los mismos recursos de procesamiento. El tercero es el escalamiento de blockchains llamado shrinking-chain, una extensión de LTCP para reducir el espacio de firma y el proceso de firma aun más. El cuarto es una nueva y mejorada VM que brinda compilación JIT y está siendo probada, y cuya especificación se está finalizando para ser propuesta como un RSKIP.

Al utilizar estas mejoras, RSK puede soportar un mayor volumen de transacciones y ofrecer un costo de transacciones más bajo.

Reducir el costo de transacción portando DApps a RSK

El costo de transacción es una limitación de muchas DApps. A medida que RSK se prepara para mejorar las capacidades de procesamiento on-chain con las propuestas

descritas anteriormente, se espera un descenso en las tarifas de transacción. Esto habilitará casos de uso que han pasado a ser prohibitivamente costosos en Ethereum.

Reducir el riesgo de devaluación para participaciones de monedas y tiendas de valores

Muchas DApps requieren el staking de criptomonedas. Las participaciones son depósitos de seguridad que tienen el fin de brindar prioridad a la hora de ser elegido para prestar un servicio. Asimismo, algunas DApps requieren depósitos en garantía como seguros contra comportamientos malintencionados. Otras DApps, tales como objetos de acceso a datos y microfinanciaciones colectivas, requieren que los fondos sean bloqueados durante largos períodos de tiempo para consolidación. En todas estas situaciones, la volatilidad de la criptomoneda nativa reduce el incentivo de bloquear monedas. Bitcoin ha demostrado una mayor resiliencia como plataforma y una menor varianza como tienda de valor, cualidades heredadas por la Smart Bitcoin. Por lo tanto, RSK se encuentra mejor posicionado para servir a estas aplicaciones.

Casos de uso de RSK

La plataforma RSK brinda smart contracts «turing completos»[4] 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 beneficiar la robustez de la moneda de Bitcoin y la seguridad del Blockchain de RSK. A continuación, presentamos una lista de potenciales smart contracts y casos de uso que pueden ser desarrollados en RSK.

Canales de micropagos

Los canales de micropagos permiten que dos partes realicen pagos regulares con valores bajos de manera segura sin tener que pagar tarifas on-chain por cada pago, sino solo una vez cuando el canal se cierra. Estas aplicaciones serán clave para construir bloques para un nuevo sistema financiero justo e inclusivo que brindará alternativas a miles de millones de usuarios marginados por el sistema actual.

Redes de pagos de segundo nivel y redes de canales de estado

Los canales de micropagos brindan una base para las redes de pagos off-chain de segundo nivel. Las redes de segundo nivel tienen la capacidad de dirigir pagos de cualquier participante a cualquier otro siempre que haya suficiente capacidad de canal, y con baja confianza en terceros.

Las redes de segundo nivel pueden ejemplificarse por gráficos aleatorios de nodos o pueden convertirse en redes hub-and-spoke, en cuyo caso un bajo número de centros altamente interconectados canalizan la mayor parte de los pagos entre usuarios. Las redes de canales de estado permiten a un grupo de participantes ejecutar protocolos con varias partes creados sobre la marcha, tales como juegos, que podrían dar como resultado cambios en los estados on-chain, como transferencias de tokens, pero demorando todos los efectos on-chain hasta el momento en que los canales se cierran, eliminando la posibilidad de hacer trampa para todas las partes. El rico lenguaje de programación de RSK permite que este tipo de redes de segundo nivel sean implementadas directamente con mínimos inconvenientes.

Intercambios descentralizados (DEX)

Los Intercambios Descentralizados permiten la creación de un token descentralizado y mercados de criptomonedas sin la necesidad de confiar en terceros. RSK soporta los Intercambios Descentralizados en todas sus variantes, con carteras de pedidos online y offline, con pruebas precisas para la concordancia de pedidos, desde el protocolo más simple de TierNolan hasta protocolos más complejos basados en zk-SNARK.

[4] A pesar de que los contratos pueden ser Turing completos, por estar escritos para un conjunto de instrucciones Turing completo, utilizando lenguajes de uso general, los recursos disponibles para la VM son limitados.

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 de pagos en tan solo un minuto. Los comerciantes podrán aceptar pagos casi instantáneamente sin requerir pasarelas de pagos de terceros. RSK también brinda una gran cantidad de transacciones por segundo (tps), necesarias en el mercado minorista. La red de RSK utiliza un protocolo de consenso de DÉCOR+ para prevenir la centralización de minería cuando el volumen de transacciones aumenta.

Servicios de depósitos en garantía

RSK permite crear servicios de depósitos en garantía inteligentes en los que los oráculos firman transacciones definiendo si se debe liberar el depósito en garantía sin la necesidad de tener los fondos en garantía en custodia.

Creación de criptoactivos

RSK permite la creación de criptoactivos (tokens, altcoins, etc) asegurados por la red de Bitcoin. Estos activos pueden ser puntos de lealtad, tokens de utilidad, o tokens de seguridad. Asimismo, los tokens pueden denominarse en fiat y monedas respaldadas por fiat. Eventualmente, podrían ser creados por los gobiernos o los Bancos Centrales como una forma de brindar dinero programable a bajos costos a todos los ciudadanos.

Ofertas de tokens respaldadas por Bitcoin (BTO)

Los BTO son un caso especial de creación de un criptoactivo cuando los bitcoins son intercambiados con tokens recientemente acuñados. Esta herramienta ha sido ampliamente utilizada para financiamiento colectivo en blockchains, como por ejemplo el financiamiento colectivo de Ethereum.
En el caso particular de RSK, los BTO permiten a las nuevas empresas recibir fondos directamente en Bitcoin, la criptomoneda más segura y estable que existe, al tiempo que se crean los tokens en RSK blockchain asegurados por la red Bitcoin. El proceso de emisión de tokens puede hacerse sin la necesidad de confiar en terceros utilizando los servicios del puente de RSK.

Securitización de activos

RSK permite la creación de tokens 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. RSK permite los tokens denominados por fiat y potenciar la infraestructura existente de intercambios y opciones de cobro para criptoactivos puede brindar remesas a costos significativamente bajos.

Protección de IP/Registry

RSK permite el desarrollo de contratos que proporcionan prueba de existencia (PoE). La PoE permite a personas y empresas probar la existencia de ciertos documentos (o derechos de propiedad) en cualquier momento con la seguridad del Blockchain de Bitcoin. Este caso de uso podría ser particularmente importante en sociedades de Latinoamérica, África y Asia con mecanismos poco confiables de identificación y registro de tierras.

Sistemas de votación

RSK permite la creación de votos digitales que permiten elecciones extremadamente seguras y transparentes a costos mínimos. Asimismo, podría ser utilizado para asegurar un proceso de votación transparente para juntas de empresas u organizaciones descentralizadas.

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 escalables, digitales y programables 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 del comercio internacional y 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 delitos y abusos y acceder a ayudas económicas. RSK permite crear registros digitales globales tan seguros como 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 se convierten en grandes riesgos y preocupaciones para los usuarios. Asimismo, las compañías creadoras de los juegos pueden llegar a enfrentarse a 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 permitiéndole a los juegos aceptar BTC (en su equivalente de Smart Bitcoins o RBTC) para sus pagos in-game, o crear un activo digital privado protegido por RSK. Los pagos de RSK proporcionados por redes off-chain de segundo nivel 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 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 justo

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.

Tokens no fungibles (NFT)

Los NFT son tokens únicos que pueden vincularse con una determinada propiedad, licencia, producto o servicio. Los NFT pueden ser creados fácilmente en RSK, permitiendo casos de uso en múltiples industrias que van desde los coleccionables deportivos hasta las funcionalidades de juegos o «temas».

Descripción general de la tecnología

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

- Una máquina virtual determinística Turing completa de recursos contabilizados (para smart contracts)
- Una cadena lateral de Bitcoin con conector bidireccional (para intercambio denominado por BTC) basada en una Federación asegurada con módulos HSM personalizados. Una vez que el protocolo de drivechain sea implementado en Bitcoin, el plan original es cambiar a un mecanismo de drivechain híbrido.
- Un protocolo de consenso basado en la minería de fusión resistente a la mineríaegoísta
- Una red de propagación de bloques con baja latencia (para pagos rápidos).

Máquina virtual Turing completa

La máquina virtual de RSK (RVM) es el núcleo de la plataforma de smart contracts. Los smart contracts son ejecutados por todos los nodos completos 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. La RVM es compatible con la EVM a nivel del código de operación, para permitir que los contratos de Ethereum fluyan sin problemas en RSK. Actualmente, la VM se ejecuta por interpretación. En una actualización de la red futura, la comunidad de RSK tiene el objetivo de mejorar el rendimiento de la VM de manera sustancial. Una propuesta es la de 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). Puede que esto haga que se ejecuten los códigos de RSK a un rendimiento cercano al código nativo.

Principales funcionalidades:

- VM independiente, pero altamente compatible con EVM a nivel del código de operación.
- Utilice las DApps de Ethereum con la seguridad de la red de Bitcoin.
- Proceso de mejora del rendimiento documentado en numerosas RSKIP (Propuestas de mejora de RSK) creadas por la comunidad de RSK.

Cadena lateral

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 Smart Bitcoin (RBTC) está conectado de manera bidireccional con el BTC.

En la práctica, cuando se cambian BTC por RBTC, no se “transfiere” ninguna moneda entre blockchains en una única transacción. 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 RBTC en BTC, los RBTC se bloquean de nuevo en RSK y la misma cantidad de BTC se desbloquea en Bitcoin.

Se pueden crear conectores bidireccionales con confianza minimizada y libres de terceros si dos plataformas tienen smart contracts Turing completos. Pero dado que Bitcoin no soporta contratos ni códigos de operación nativos para validar pruebas externas de SPV, parte del sistema de conector bidireccional de RSK requiere confiar en una serie de terceros semi-confiables (STTP), a los que denominamos conjuntamente la Federación. Ningún STTP por sí solo puede controlar los BTC bloqueados, pero solo la mayoría de ellos tiene la habilidad de liberar fondos BTC. Cada STTP tiene una clave para proteger a los BTC que están bloqueados, y luego de recibir comandos de la RSK blockchain, desbloquea a los BTC que necesitan ser transferidos nuevamente a Bitcoin. Tenga en cuenta que si un usuario transfiere BTC a RBTC y luego vuelve a transferirlos a BTC, normalmente no recibirá bitcoins que estén directamente conectados por UTXO con el BTC original enviado. Por lo tanto, no bloquee RBTC para usuarios específicos, sino para toda la red de RSK.

El bloqueo y desbloqueo de fondos se realiza a través de la Federación sin ninguna intervención humana. 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. RSK Labs desarrolló un firmware para un Módulo de Seguridad de Hardware (HSM) que los STTP pueden usar, para brindar la máxima seguridad para sus claves privadas y, en el futuro, para poder implementar un protocolo de validación de transacciones con el objetivo de mejorar la seguridad aun más.

A partir de enero de 2019, la Federación de RSK incluye 15 notarios reconocidos y altamente seguros. Empresas líderes de Blockchain integran actualmente la Federación de RSK y participan en un protocolo autónomo para bloquear bitcoins de manera segura. A cambio de su trabajo, los miembros de la Federación reciben el 1 % de las tarifas de transacción generadas en RSK, para cubrir el hardware y los costos de mantenimiento. Existe un proceso automatizado para modificar la composición de la federación. Cada miembro de la federación puede aceptar o rechazar un cambio en la composición. El proceso, que es poco frecuente, es comandado por un smart contract, de modo que es abierto al público. El protocolo tiene una demora aprobada por consenso de una semana hasta que se activa el cambio. Esto permite a los usuarios transferir los bitcoins de vuelta a la red de Bitcoin en caso de que no confíen en la nueva composición de la Federación.

Si 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 la comunidad de RSK podrá implementar los cambios para adaptar a RSK al sistema trust-free. Asimismo, la comunidad de RSK ha propuesto una BIP de Drivechain, que permite a los mineros participar en el proceso de seguridad de los bitcoins en el conector, y disminuye la confianza necesaria en los STTP aun más.

Minería fusionada

El consenso de Satoshi, basado en la prueba de trabajo, es el único sistema de consenso que evita que se reescriba el historial de blockchain a un bajo costo. La comunidad académica está avanzando en el conocimiento y el estudio de la prueba de participación como alternativa, pero actualmente la prueba de trabajo brinda la mayor seguridad comprobada. La minería fusionada es una técLa 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 recompensa a los mineros con tarifas de transacción adicionales, el incentivo para la minería fusionada es alto.

Hemos identificado tres fases para el crecimiento de la minería fusionada en RSK:

- Fase de inicio: la minería fusionada se encuentra por debajo del 30 % de la tasa de hash de Bitcoin.
- Fase estable: la minería fusionada se encuentra entre el 30 y el 60 % de la tasa de hash de Bitcoin.
- Fase madura: la minería fusionada se encuentra por encima del 60 % de la tasa de hash de Bitcoin.

RSK ha dejado atrás su fase inicial, cuando los mineros de fusión con malas intenciones podían revertir la RSK blockchain a un bajo costo. A partir de enero de 2019, más del 40 % de los mineros de Bitcoin se encuentran involucrados en la minería fusionada de RSK. Pero dado que las tarifas de RSK continúan siendo bajas en comparación con la recompensa de bloques de Bitcoin, el costo de atacar a RSK mediante un doble gasto es más bajo que el de Bitcoin.
RSK tiene algunas propiedades para reducir el riesgo de sufrir un ataque de doble gasto, como por ejemplo la madurez larga de las recompensas para mineros. El equipo de investigación de RSK Labs ha desarrollado diversas protecciones para prevenir ataques durante la fase estable y la fase madura del proyecto:

- **Notificaciones firmadas:** Los clientes de RSK pueden hacer uso de las notificaciones firmadas por notarios. Los nodos pueden utilizar estas notificaciones para detectar ataques Sybil e informar a los usuarios.
- **Rastros transparentes de doble gasto**: se trata de un método por el que todas las etiquetas de minería fusionada de RSK son aumentadas con información adicional que puede utilizarse para detectar forks egoístas en RSK que sean públicos en la blockchain de Bitcoin. Las pruebas para forks egoístas se construyen automáticamente y se presentan a los nodos de RSK, que las distribuyen a lo largo de la red. Estas pruebas obligan a los nodos a entrar en un «modo seguro» cuando ninguna transacción se anuncia como confirmada. El modo seguro evita que los comerciantes y agentes cambiarios acepten pagos que podrían ser dobles gastos. Una vez que el fork egoísta es superado por la mainchain de RSK en la prueba de trabajo acumulada, la red regresa a su estado normal. Este método previene cualquier tipo de intento de doble gasto (en los que los mineros maliciosos continúan intentando cobrar las recompensas de Bitcoin al minar el fork egoísta).

Una vez que la plataforma entre en la fase de madurez, estimamos que la seguridad de RSK será suficiente para soportar la economía de la inclusión financiera global.

Principales funcionalidades:

- Protocolo de consenso DECOR+
- 1 día de maduración para las recompensas de minería.
- No se espera ninguna pérdida en la eficiencia de la minería de Bitcoin como consecuencia de la minería de fusión (para cambios de estados medios y tardíos)

Pagos rápidos y una red con baja latencia

RSK ya permite las redes de pagos off-chain de segundo nivel, pero aún tiene el objetivo de brindar una red de pagos on-chain mucho mejor en comparación con Bitcoin. Para lograr esto, RSK adopta los protocolos de DECOR+ y FastBlock5, que permiten alcanzar una tasa promedio de bloqueo de 15 segundos que no incentiva la centralización de la minería ni el egoísmo en la minería.

Principales funcionalidades:

- Intervalos de bloques de 15 a 30 segundos (según la eficiencia de cambio de estado de los mineros)
- Propagación completa por la red de los bloques competidores más recientes para prevenir el egoísmo en la minería y reducir la tasa de bloques huérfanos.
- Nuevo comando de red para difundir los encabezados de bloques priorizando el tiempo.
- Protocolo DECOR+ para compartir recompensas entre bloques competidores.
- Protocolo GHOST para ponderación de cadenas.

Desde la creación de Bitcoin, ha habido una carrera por lograr menores intervalos para criptomonedas basadas en la blockchain de una PoW. Pero los intervalos bajos entre bloques pueden afectar la estabilidad y la capacidad de la red de cripromonedas, de modo que es necesario tener en cuenta diversos factores de diseño. Antes que nada, el factor más importante que afecta la viabilidad de los intervalos cortos de confirmación es el número de bloques huérfanos generados. El principal factor que afecta la tasa de bloques huérfanos es el protocolo de propagación de bloques. Para RSK, hemos analizado cuidadosamente este protocolo y realizado simulaciones para verificar el rendimiento, la usabilidad y la seguridad de la red.

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 el elegido de los dos. Sin embargo, todo el resto de mineros y usuarios honestos tienen una preferencia racional por que se elija la misma punta de bloque, porque esto reduce la probabilidad de revocación de bloque. El protocolo de consenso DECOR+ establece los incentivos económicos adecuados para la convergencia de elecciones, sin requerir que los mineros tengan interacciones posteriores entre sí. El protocolo 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 maximiza las ganancias de los todos mineros (de manera colectiva) y para ambos mineros en conflicto en caso de que las recompensas de bloques difieran en un margen alto
3. La resolución elegida maximiza la resistencia a la censura si los bloques

competidores tienen recompensas aproximadamente similares.
4. El tiempo necesario para resolver el conflicto es insignificante.

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 terceras partes.

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. Utilizando el protocolo LTCP propuesto, el tamaño de las transacciones puede reducirse a 1/50 del tamaño de una transacción de Bitcoin. Esto conduce inmediatamente a un aumento sustancial en la capacidad en cuanto al volumen de transacciones. Además, existen propuestas de la comunidad (RSKIP) para permitir el uso de esquemas de firma elegibles por el usuario: ECDSA, Schnorr y Ed25519. Dado que Ed25519 funciona mejor que la curva de Bitcoin ECDSA, utilizar este esquema puede dar como resultado una capacidad aun mayor.

Comparación de funcionalidades de RSK

La siguiente tabla tiene la intención de comparar las principales funcionalidades de RSK respecto de aquellas presentes en otras alternativas, incluida la cadena lateral de Liquid (Blockstream), y el token de WBTC (BitGo). Tanto Liquid como WBTC están vinculados con el BTC. Mostramos que, esencialmente, RSK presenta mejores soluciones técnicas con bajo impacto en la descentralización.

Artículo	Bitcoin BTC	Ethereum ETH	Ethereum WBTC	Liquid LBTC	RSK RBTC
Tiempo de confirmación promedio	10 min.	15 segundos (GHOST)	Igual que Ethereum	60 segundos	15 a 30 segundos (DECOR+GHOST)
Umbral de seguridad (debido a la minería egoísta o la colusión)	~30 %	Menos del 30 %	Igual que Ethereum	50 %	50 % (DECOR+GHOST)
Smart contracts Turing completos	No	Sí	Sí	No	Sí
Agrega valor al Bitcoin	-	No	Sí	Sí	Sí (orientado a la fusión)
Integración con Bitcoin	-	No	No	Cadena lateral	Cadena lateral
Clientes SPV	Sí	Sí	Sí	Sí	Sí
Integración del hardware wallet	Sí	Sí	Parcial	No	Sí
Garantía de finalidad de la transacción	Consenso de Nakamoto. SHA256D	Consenso de Ethereum. Ethash	Igual que Ethereum	Federación	DECOR+GHOST. SHA256D PoW
Transacciones confidenciales	No	Via contrato	No	Sí	Via contrato. Soporte nativo planeado
Escalabilidad [tps]	3 (6 con segwit)	Ilimitado, actualmente 15	Igual que Ethereum	3 (6 con segwit)	Ilimitado, actualmente 10
Tamaño de blockchain	200 GB	> 1.5 TB	> 1.5 TB	~300 MB	~2 GB
Seguridad del token peg	--	--	Compañía única	Federación	Federación
Token	BTC	ETH	WBTC	LBTC	RBTC

El rol de RSK Labs

RSK Labs se ha establecido como un agente fuerte en la comunidad mediante la creación de la implementación de referencia del nodo de RSK. Actualmente, RSK Labs continúa llevando a cabo actividades técnicas y en la comunidad, tales como:

- Impulsar el desarrollo de la plataforma de referencia de RSK a través de actualizaciones periódicas
- Establecer una colaboración con la academia
- Mantener los canales de discusión, foros y preguntas frecuentes de la comunidad
- Coordinar conferencias y reuniones locales
- Promover el uso de RSK Blockchain
- Solicitar y publicar auditorías de seguridad externas de manera periódica
- Participar en debates de actualizaciones de red propuestas por la comunidad
- Auditar la seguridad del código de base de RSK
- Aconsejar a gobiernos, empresas emergentes, empresarios y compañías acerca de las mejores formas de beneficiarse de la red de RSK

El compromiso continuo de RSK Labs con RSK es recompensado por la plataforma RSK: El 20 % de las tarifas de transacción se pagan a una cuenta controlada por RSK Labs.

El futuro de RSK

La hoja de ruta de RSK ha sido establecida por la comunidad de RSK. Durante los primeros años de desarrollo de RSK, RSK Labs tuvo un rol activo en la construcción de la implementación de referencia. Luego del lanzamiento de RSK, RSK Labs continuó altamente involucrado con la comunidad mediante la mejora del código de base y propuestas para mejoras a través del sistema repositorio de propuestas RSKIP. El repositorio ayuda a los miembros de la comunidad a coordinar debates, rechazo, aceptación y despliegue en múltiples códigos de base. La cantidad de propuestas de mejoras es vasta. La siguiente es una lista con algunas de las propuestas clave a partir de diciembre 2018:

Memoria distribuida, Dependencia dinámica de contratos, Ejecución paralela utilizando dependencias estáticas de contratos, Ejecución paralela utilizando dependencias de tiempo de ejecución de contratos, Operaciones de cambio, Límite de tamaño del bloque, Renta de almacenamiento persistente pagada por código, Minería sin verificación, Precio mínimo del gas negociado, Las transacciones nunca invalidan a los bloques, Código de operación TXINDEX, Contract Sleep, Soporte para activos estables y emisión de tokens, Reward Manager Smart Contract (REMASC), Simplified Reward Manager Smart Contract (REMASC), Árbol de estados combinado, Renta de almacenamiento persistente más simple, Fast Hibernation Wakeup using Trie, Formatos de direcciones de RSK, Espacios de memoria de Survive y Ephemeral, Renta de almacenamiento persistente eficiente, Compromiso con el número de elementos del árbol de Merkle, Onchain PoUBS, Nuevo trie binario, Memory caches, Códigos de operación DUPN y SWAPN, Renta de almacenamiento altamente eficiente, Ephemeral segwit, Cambio en el costo de creación de las cuentas, Paginación de código, Compresión de hibernación, Direcciones Double-Hashed, Código de operación CODEREPLACE, Secciones de dato de construcción de contratos, Gestión de los miembros de la Federación BridgeMaster, Encapsulación de

transacciones, Smart Wallets con una sola dirección, Compresión de firmas, Cuentas multi-clave, Puente básico para conector bidireccional con Bitcoin, Transacciones puente con Bitcoin extendidas, Eliminar los midstates de los recibos, Formato de dirección secuencial, Remover el descuento de cero byte en los datos, Nuevo árbol de eventos y LOG extendido, Mecanismo de información de tarifas de minería de bloques, Código de operación CALLNUM, Informar el gas gratis promedio por bloque, Demasiados canales de pago hub , Versiones de Script Versions utilizando el seudo-código de operación HEADER, Registro de configuración mapeado en memoria, Renta de almacenamiento orientada al cache, Lumino Transaction Compression (LTCP), Privacidad de montos y destinos de transacción, Pagos probabilísticos nativos, Minería sin verificación esporádica, Ruta de derivación para wallets determinísticas jerárquicas, Manejo de forks de Bitcoin, Contratos para niños, Codificación de dirección checksum, Renta de almacenamiento orientada al cache (versión EOT), Propagación de bloques comprimida utilizando un batch de actualización de state tries (COBLO), Doble firma para un retraso en el agregado de la firma, Datos de transacción por defecto, Pagos probabilísticos nativos Off-Chain, Ajustes de dificultad más fluidos, DELEGATECALL como extensión de conjunto de instrucciones, Gestión de los miembros de la Federación BridgeMaster

Si bien algunas propuestas todavía están inmaduras, otras han evolucionado luego de varias rondas de debate y es probable que hayan ganado apoyo de la comunidad para formar parte de futuras actualizaciones de la red.

Conclusiones

RSK es la primera cadena lateral de Bitcoin en producción que brinda smart contracts Turing completos, compatibles con los estándares de Ethereum, y asegurados por la minería fusionada de Bitcoin.

RSK representa la culminación de 5 años de mejoras de tecnología en blockchain y permitirá que el ecosistema de Bitcoin utilice las mejores funcionalidades del dinero programable y los pagos, a la vez que aumenta el valor y la utilización de bitcoin.

El diseño innovador de RSK permite una mayor escalabilidad y menores costos de transacción.

RSK permite 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 y casos de uso.

RSK permite a los mineros de Bitcoin participar en el mercado de Smart Contracts añadiendo mucho valor a la industria de la minería de Bitcoin y asegurando su sostenibilidad a largo plazo. Contribuye a la sostenibilidad económica de los mineros de Bitcoin y al crecimiento de la seguridad de la red de Bitcoin.

RSK brinda a los usuarios y compañías de Ethereum una nueva plataforma compatible para desplegar sus soluciones utilizando el Bitcoin como moneda nativa, confiando en la infraestructura de minería de Bitcoin para su seguridad, y accediendo a una base de usuarios más amplia.

RSK posibilita la creación de un sistema financiero basado en blockchain, descentralizado, seguro, económico y abierto, 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.