
RSK
ROOTSTOCK PLATFORM
BITCOIN POWERED
SMART CONTRACTS
WHITE PAPER

RSK

Contratos inteligentes baseados em Bitcoin

White paper
Visão geral

Revisão: 11
Data: 29 de janeiro de 2019
por Sergio Demian Lerner

Introdução

Em 2008, Satoshi Nakamoto revolucionou os pagamentos criando o Bitcoin. O Bitcoin incluiu uma implementação muito limitada dos chamados "contratos inteligentes", um conceito introduzido em 1993 por Nick Szabo.

Desde então, várias criptomoedas foram lançadas com VMs com informação de estado, capazes de suportar linguagens de programação Turing-completas, liberando toda a potência dos contratos inteligentes. Milhares de aplicativos descentralizados que interagem com os contratos inteligentes (chamados dApps) foram desenvolvidos e novos casos de uso surgiram. No entanto, cada nova plataforma usa um novo token nativo altamente especulativo e volátil.

Desde seu bloco gênese em 3 de janeiro de 2009, o Bitcoin se consolidou como a melhor, mais adotada, mais robusta e mais protegida reserva de valor e como o protocolo mais seguro entre todas as criptomoedas. Mas a maioria dos dApps exigem regras mais complexas que não podem ser codificadas em atributos do Bitcoin semelhantes a Forth. Essa limitação desencadeou o nascimento da RSK em 2015 e o lançamento de sua MainNet em janeiro de 2018. A RSK é uma plataforma que permite a execução de contratos inteligentes que usam bitcoin como ativo nativo, contribuindo para o valor do Bitcoin como principal criptomoeda global e expandindo seu alcance para todos os possíveis casos de uso de dApps. A RSK é uma sidechain do Bitcoin, portanto possui sua própria rede e sua própria blockchain, mas não possui um token próprio. A rede RSK oferece aprimoramentos em comparação ao Bitcoin, tais como transações mais rápidas e melhor escalabilidade.

A RSK é uma evolução de duas plataformas, QixCoin e Ethereum. A QixCoin foi uma criptomoeda Turing-completa, criada em 2013 por alguns dos fundadores da RSK. A QixCoin introduziu o conceito de pagamento por execução, atualmente conhecido como "combustível" da transação. No entanto, a RSK herda vários conceitos fundamentais da Ethereum, como seu formato de conta, sua VM e sua interface web3. Portanto, a RSK é altamente compatível com os compiladores, as ferramentas e os dApps da Ethereum.

Comparada ao Bitcoin, a RSK oferece uma experiência de pagamento aprimorada, com confirmações quase imediatas. E, no entanto, a RSK também é baseada em proof-of-work, suportando a mineração mesclada SHA-256D, o mesmo protocolo de consenso e rede de mineração que garante o Bitcoin. Em janeiro de 2019, a RSK tem mais de 40% da taxa de hashing do Bitcoin, o que a torna a plataforma de contratos inteligentes mais segura do planeta em termos de energia investida na proteção da blockchain.

Para permitir que os bitcoins entrem e saiam da RSK, a RSK possui uma paridade bidirecional com o Bitcoin. Quando os Bitcoins são transferidos para a blockchain RSK, tornam-se "Smart Bitcoins" (cujo ticker é RBTC[1]). Os Smart Bitcoins são equivalentes a bitcoins que residem na blockchain da RSK e podem ser convertidos novamente em Bitcoins a qualquer momento, sem custo adicional, exceto as taxas de transação padrão

[1]Neste white paper, "Protocolo RSK" significa a especificação do protocolo. "Nó de referência RSK" significa a implementação de referência. A moeda RSK nativa é o "Smart Bitcoin". O "ticker", ou símbolo, do smart bitcoin é "RBTC". "BTC" ou "bitcoin" significa a moeda nativa do Bitcoin. "Bitcoin" significa o protocolo Bitcoin.

da RSK e do Bitcoin. O RBTC é a moeda nativa usada na blockchain da RSK para pagar aos mineradores pelo processamento de transações e contratos. Não há emissão de moeda: todos os RBTCs são criados a partir dos bitcoins provenientes da blockchain Bitcoin.

A RSK atualmente aprimora o Bitcoin nas seguintes áreas:

- Máquina Virtual RSK Turing-completa (RVM) que permite contratos inteligentes e é altamente compatível com a VM da Ethereum (EVM).
- Média de 30 segundos para a primeira confirmação de transações.
- Mineração mesclada com o Bitcoin.
- Sidechain com paridade bidirecional (atualmente uma paridade federada)
- Proteção contra a mineração egoísta por meio do protocolo DECOR+

Além disso, a comunidade RSK está fortemente unificada para seguir a visão original de adicionar os seguintes recursos nas futuras atualizações da rede:

- Aluguel de armazenamento
- Otimizações na propagação de blocos
- Processamento de transações paralelas
- Um protocolo de compactação de transações (LTCP) para oferecer maior escalabilidade
- Suporte para uma VM adicional com maior desempenho com base no código de byte Java ou WAsm.
- Paridade híbrida baseada em federação/drivechain

Os recursos futuros são mencionados como Propostas de Aprimoramento da RSK (RSKIPs), descritas no repositório https://github.com/rsksmart/RSKIPs, juntamente com o código PoC.

A RSK é um projeto conduzido pela comunidade. A RSK Labs é uma empresa fundada em 2015 para desenvolver a implementação de referência do protocolo RSK e, desde 2015, paga salários a alguns dos mais proeminentes desenvolvedores do RSK Core. A RSK Labs também fornece informações da plataforma no site www.rsk.co e hospeda vários serviços informativos.

Recursos úteis para começar

Site da RSK Labs: https://www.rsk.co/
RSK Stats: https://stats.rsk.co
RSK Explorer: https://explorer.rsk.co/
RSK Faucet: https://faucet.rsk.co/
Status da RSK Network: https://twitter.com/RskSmartNetwork
Comparação de taxas da RSK: http://rskgasstation.info/

Carteiras de software compatíveis com RSK:

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

Carteiras de hardware compatíveis com RSK:

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

Por que a RSK é importante para o ecossistema Bitcoin?

Nas seções a seguir, listamos vários motivos pelos quais a RSK é importante para o ecossistema Bitcoin.

Alinhamento das partes interessadas do Bitcoin e proteção de valor

Um dos objetivos da RSK é fornecer uma plataforma de contratos inteligentes que beneficie as principais partes interessadas do ecossistema Bitcoin e sua comunidade. Essa filosofia é refletida diretamente em sua arquitetura central, onde os mineradores de Bitcoin fornecem o poder de hashing necessário para garantir que a RSK e as empresas líderes do setor integrem a Federação, a qual possui as chaves que protegem os fundos bloqueados no sistema de paridade bidirecional. O modelo de governança da RSK tem como objetivo representar todos os atores da comunidade: partes interessadas do RBTC, mineradores, membros da federação e desenvolvedores e usuários finais dos dApp. A longo prazo, o plano da comunidade é habilitar mecanismos de sinalização objetivos, mas não vinculativos, embutidos nas transações e nos blocos, para que os usuários possam sinalizar com seus stakes; os aplicativos de carteira e remetentes possam sinalizar marcando as transações; os mineradores possam sinalizar marcando os blocos; e os receptores possam sinalizar marcando as contas, de modo a alcançar uma governança ainda mais descentralizada e democrática.

Proteção do investimento dos mineradores de Bitcoin

Em maio de 2020, em razão da queda na recompensa de blocos, a margem de rentabilidade da mineração de Bitcoin cairá de BTC 12,5 para BTC 6,25. A redução da lucratividade pode implicar o fim de muitas empresas e indivíduos que realizam mineração, e enormes quantidades de hardware de mineração que protegiam o Bitcoin podem ser desconectados. Devido a suas capacidades de mineração mesclada, a RSK representa uma possibilidade para esses mineradores continuarem no mercado por mais tempo. Como os mineradores de Bitcoin por mesclagem podem minerar ambas as moedas com custo marginal zero, eles ainda poderão minerar Bitcoins, desde que a renda adicional fornecida pela mineração RSK compense a lacuna de rentabilidade.

Além disso, se optarem pela mineração por mesclagem neste momento, os mineradores estarão apoiando novas aplicações imprevistas, que no futuro poderão fornecer novas oportunidades de negócios.

Emissão de ativos de valor estável por Bitcoins caucionados

A RSK permite a emissão de ativos com preços atrelados a uma moeda fiduciária ou outra commodity estável mediante o bloqueio de Bitcoins como garantia. Os ativos

estáveis alcançam menor volatilidade, enquanto a manutenção de Bitcoins como moeda de reserva aumenta o valor geral do Bitcoin. O bloqueio de grandes quantidades de Bitcoin reduz a liquidez e, portanto, contribui para o aumento do valor do Bitcoin. No entanto, o mais importante, esses tokens estáveis de Bitcoin na RSK permitirão micropagamentos em moedas estáveis que, por sua vez, possibilitarão que bilhões de habitantes atualmente não atendidos pelo sistema financeiro tradicional participem da economia digital global.

A RSK na vanguarda da tecnologia sidechain do Bitcoin

A RSK Labs está explorando, pesquisando e implementando conceitos-chave vitais para qualquer outra sidechain futura do Bitcoin. O sucesso da RSK encorajará outros desenvolvedores de sidechains a seguirem e se beneficiarem da eficiente infraestrutura de mineração mesclada criada, dos opcodes de drivechain propostos e da tecnologia desenvolvida para a criação segura de federações multi-assinatura (multisig) pela RSK Labs. Com designs de software, firmware e hardware de código aberto, a RSK Labs está promovendo o avanço da ciência e melhorando a funcionalidade e a segurança do ecossistema de criptomoedas como um todo.

RSK como uma rede de pagamentos de Bitcoin de baixo custo

Atualmente, as transações com Bitcoin custam em média USD 0,24,[2] enquanto o custo do RSK é de USD 0,0046 [3], ou seja, 50 vezes menor. Trata-se de uma melhoria radical. Mas também as taxas de Bitcoin geralmente aumentam ou diminuem com base na demanda por espaço de bloco, e prevemos uma crescente demanda por transações on-chain. Após várias tentativas malsucedidas de aumentar o tamanho do bloco do Bitcoin por meio de hard-forks, e após a atualização única de espaço do Segwit, não há, na comunidade Bitcoin, nenhum plano para aumentar o tamanho do bloco. Podemos esperar que as taxas de transação do Bitcoin se tornem exageradamente altas para a maioria das aplicações envolvendo transações diárias pessoais. Os blocos RSK podem realizar muito mais transações do que os blocos Bitcoin devido ao tamanho reduzido de suas transações, portanto, a RSK naturalmente oferecerá taxas muito mais baixas, com o mesmo volume de transações. Na tabela a seguir, comparamos brevemente o Bitcoin com o RSK.

Parâmetro	Bitcoin	RSK
Tempo médio de confirmação de blocos	10 minutos	30 segundos (os mineradores podem reduzi-lo para 15 segundos)
Tempo de confirmação sugerido para câmbios	30 minutos (3 blocos)	60 minutos (120 blocos) com a taxa de hash de mineração mesclada atual (40%).
Máx. de transações por segundo	3,3 tps (considerando-se uma transação de tamanho médio)	10 tps (transações externas, em janeiro de 2019) 20 tps (transações internas)
Custo de transação médio atual	USD 0,24	USD 0,0046

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

O custo das transações com Bitcoins está diretamente relacionado ao valor da recompensa do bloco. A adição de uma transação a um bloco atrasa sua propagação. Cada milissegundo gasto em propagação é pago proporcionalmente à recompensa do bloco, pois diminui a probabilidade de o bloco ser escolhido pela rede. Técnicas de reconciliação de conjuntos (como códigos Bose–Chaudhuri–Hocquenghem fornecidos pela biblioteca Minisketch) poderiam, se implementadas no Bitcoin, reduzir essa dependência. Atualmente, se o preço do Bitcoin aumentar, as taxas de transação também aumentarão. Acredita-se que o Bitcoin se tornará uma espécie de sistema de compensação interbancário, mas não uma rede de pagamentos. Também é importante notar que estão surgindo sistemas de pagamento off-chain, como o Lightning Network, mas essas redes provavelmente aumentarão a necessidade de transações on-chain para liquidação e recarga de canais, elevando também o custo de transação. À medida que esse custo aumentar, os usuários migrarão para plataformas com custos de transação mais baixos. A RSK oferece uma excelente oportunidade para realizar transações em Bitcoin por um custo muito menor.

Por que a RSK é importante para usuários e desenvolvedores da Ethereum?

Aumenta sua base de usuários DApp

A RSK tem uma base de usuários peculiar, inicialmente composta por adeptos do Bitcoin da América Latina. Atualmente, a RSK está em uma trajetória de forte crescimento tanto na América Latina quanto na Ásia. Ao implantar DApps compatíveis na Ethereum e na RSK de forma ágil e eficaz, os desenvolvedores e as empresas podem alcançar uma base de usuários mais ampla, reduzindo sua dependência de qualquer blockchain específica. Hoje, existem também várias soluções federadas para conectar a Ethereum e a RSK e transferir tokens de uma blockchain para a outra, de modo que o mesmo token possa residir em ambas as blockchains.

Promove a padronização da EVM/Web3

A comunidade Ethereum criou a máquina virtual de contratos inteligentes (EVM) e a interface para que aplicativos descentralizados interajam com ela (Web3). Ao adotar esses padrões, a RSK torna mais fácil para os desenvolvedores migrarem seus aplicativos para a RSK e reutilizarem a maioria dos softwares de infraestrutura desenvolvidos para a Ethereum. Mas também ajuda na padronização, fornecendo material de aprendizado unificado e reduzindo a necessidade de se aprender mais uma arquitetura de execução e linguagem de programação. Ao mesmo tempo, todas as ferramentas desenvolvidas pelo ecossistema RSK também estarão disponíveis para os usuários da ETH.

Reduz riscos de fork persistentes

A Ethereum é periodicamente submetida a atualizações de rede. Um dos mais antigos forks da Ethereum anunciados e ainda debatidos é a migração do consenso Proof-of-Work (prova de trabalho) para o Proof-of-Stake (prova de participação). Essa é uma mudança tecnológica e econômica radical, que deve ser enfrentada pelos mineradores da Ethereum. Uma nova divisão de cadeia forçará os desenvolvedores a escolherem entre a cadeia PoW original e a nova cadeia PoS. Além disso, ainda existem incertezas em relação à segurança e à estabilidade do novo protocolo de consenso. Em caso de falha,

todos os usuários que possuírem ether podem ser impactados economicamente, gerando uma possível rejeição à mudança por parte da comunidade Ethereum. Além disso, os principais desenvolvedores Ethereum implementaram e implementarão mudanças no algoritmo de oferta de dinheiro e prova de trabalho, o que corrói a imutabilidade e a neutralidade da plataforma. A RSK não possui um token especulativo nativo – os Smart Bitcoins podem sempre ser transferidos de volta para o Bitcoin caso um usuário não concorde com uma atualização da rede RSK apoiada pela comunidade. Portanto, a comunidade RSK apresenta um nível muito baixo de confronto, o que minimiza o risco de uma cisão da comunidade. Por outro lado, o Bitcoin tem uma tradição em rejeitar hard forks. Portanto, a RSK fornece uma plataforma muito estável em médio e longo prazos.

Protege o investimento em P&D contra as vulnerabilidades de segurança de dia zero da Ethereum

A maioria das blockchains passa por atualizações de rede periódicas e atualizações de software frequentes. Para a maioria dos projetos de blockchain, a tecnologia ainda é experimental e os protocolos não foram estabelecidos de forma definitiva. As plataformas Ethereum e RSK estão longe de serem maduras. Isso significa que novas vulnerabilidades de segurança podem ser encontradas, assim como já foram identificadas e exploradas anteriormente na Ethereum. Mesmo a RSK, que tem um excelente histórico de segurança, não está livre de riscos. No entanto, a existência de duas plataformas compatíveis reduz o risco de que os recursos dedicados ao desenvolvimento de um DApp sejam perdidos devido a uma falha catastrófica de uma plataforma. A probabilidade de uma falha conjunta é muito menor, especialmente levando em conta os diferentes protocolos de consenso envolvidos.

Aumenta o volume de processamento de transações ao transportar DApps para a RSK

A RSK é tecnicamente superior a outras plataformas por causa de quatro propostas da comunidade que podem fornecer maior escalabilidade dentro da cadeia. A primeira é o processamento paralelo de transações, especificado pelo RSKIP4, que permite que as arquiteturas multinúcleo alcancem o uso completo dos núcleos de processamento no processamento das transações. Isso, por sua vez, permite o aumento do limite de combustível dos blocos, permitindo um maior volume de processamento de transações. A segunda é o LTCP, especificado pelo RSKIP53, que permite a compactação de transações e o agrupamento de assinaturas, de modo que muitas transações podem ser processadas com a mesma quantidade de espaço e recursos de processamento. A terceira é o escalamento de cadeia encolhida (shrinking-chain scaling), que é uma extensão do LTCP para reduzir ainda mais o espaço e o processamento de assinaturas. A quarta é uma nova VM aprimorada que fornece uma compilação JIT que está sendo testada, e cuja especificação está sendo finalizada para ser proposta como um RSKIP.

Ao usar essas melhorias, a RSK pode suportar um maior volume de transações e/ou menor custo de transação.

Reduz o custo de transação ao transferir DApps para a RSK

O custo de transação é uma limitação para muitos DApps. Como a RSK está se preparando para aumentar os recursos de processamento on-chain com as propostas de escalamento descritas acima, espera-se uma redução nas taxas de transação. Isso possibilitará casos de uso que se tornaram exageradamente caros na Ethereum.

Reduz o risco de desvalorização de stakes de moedas e reservas de valor

Muitos DApps exigem o staking de criptomoedas. Stakes são depósitos de segurança destinados a garantir a prioridade de ser escolhido para fornecer um serviço. Além disso, alguns DApps exigem depósitos de segurança como garantia contra comportamentos maliciosos. No entanto, outros DApps, como DAOs e crowdfunds, exigem que os fundos sejam bloqueados por longos períodos de tempo para conferência. Em todas essas situações, a volatilidade da criptomoeda nativa reduz o incentivo para bloquear moedas. O Bitcoin tem mostrado maior resiliência como plataforma e menor variância como reserva de valor, qualidades herdadas pelo Smart Bitcoin. Portanto, a RSK está melhor posicionada para atender a esses aplicativos.

Casos de uso da RSK

A plataforma RSK fornece contratos inteligentes Turing-completos[4], conforme proposto por Nick Szabo em 1993. Ao mesmo tempo, a VM RSK é retrocompatível com a VM Ethereum. Portanto, a RSK oferece aos desenvolvedores que trabalham na Ethereum a oportunidade de se beneficiar da robustez da moeda Bitcoin e da segurança da blockchain RSK. Apresentamos a seguir uma lista de potenciais contratos inteligentes e casos de uso que podem ser desenvolvidos sobre a plataforma RSK.

Canais de micropagamentos

Os canais de micropagamentos permitem que duas partes realizem pagamentos frequentes, e geralmente de baixo valor, de maneira segura pagando apenas uma taxa quando o canal é fechado, em vez de pagar taxas para cada transação. Essas aplicações serão blocos fundamentais para um novo sistema financeiro justo e inclusivo, que fornecerá alternativas aos bilhões de usuários não atendidos pelo sistema atual.

Redes de pagamentos off-chain de 2ª camada e redes de canal de estado

Os canais de micropagamentos fornecem a base para as redes de pagamentos off-chain de 2ª camada. As redes de 2ª camada são capazes de encaminhar pagamentos de qualquer participante para qualquer outro participante, desde que haja capacidade de canal suficiente, e com baixa confiança de terceiros.

A rede de segunda camada pode ser instanciada por grafos aleatórios de nós ou tornar-se uma rede hub-and-spoke, na qual um pequeno número de hubs altamente interconectados canaliza a maioria dos pagamentos entre os usuários. As redes de canal de estado permitem que um conjunto de participantes execute protocolos multilaterais criados de maneira rápida, como jogos, que podem resultar em alterações de estado on-chain, como transferências de tokens, mas adiando todos os efeitos na cadeia até o momento em que os canais são fechados, contanto que não haja tentativa de fraude por nenhuma das partes. A rica linguagem de programação da RSK permite que todos esses tipos de redes de 2ª camada sejam implementados diretamente com o mínimo de trabalho.

Câmbios descentralizados (DEXs)

Os câmbios descentralizados permitem a criação de mercados descentralizados de tokens e criptomoedas sem a confiança de terceiros. A RSK suporta câmbios descentralizados em todas as suas variantes, com carteiras de pedidos online ou off-chain e provas sucintas de correspondência de pedidos, desde o protocolo TierNolan mais simples até os protocolos mais complexos baseados em zk-SNARKs.

Sistemas de pagamento de varejo

A RSK permite que o BTC seja adotado globalmente para transações de varejo diárias. Uma das principais limitações do Bitcoin para uso no varejo é seu tempo de confirmação

[4]Embora os contratos possam ser Turing-completos – por terem sido escritos para um conjunto de instruções Turing-completo, usando linguagens de uso geral –, os recursos disponíveis para a VM são limitados.

(de 10 minutos a 1 hora para garantir a irreversibilidade). A RSK permite que os consumidores se beneficiem da segurança do Bitcoin com confirmações de pagamentos em apenas um minuto. Os comerciantes poderão aceitar pagamentos de maneira quase instantânea, sem exigir gateways de terceiros. A RSK também fornece uma quantidade maior de transações por segundo (tps), o que é necessário para ter sucesso no mercado de varejo. A rede RSK usa o protocolo de consenso DÉCOR+ para impedir a centralização da mineração quando o volume de transações aumenta.

Serviços de custódia

A RSK permite a criação de serviços de custódia inteligentes, em que os oráculos podem assinar uma transação para definir se o valor sob custódia deve ser liberado, sem que o oráculo tenha os valores sob custódia em depósito.

Criação de ativos criptográficos

A RSK permite a criação de ativos criptográficos (tokens, altcoins, etc.) garantidos pela rede Bitcoin. Esses recursos podem ser pontos de fidelidade, tokens utilitários ou tokens de segurança. Além disso, os tokens podem ter valor fiduciário e ser lastreados em moeda fiduciária. Eventualmente, poderiam ser criados por governos ou bancos centrais como forma de fornecer dinheiro programável de baixo custo a todos seus cidadãos.

Ofertas de tokens lastreados em Bitcoins (BTOs)

As BTOs são um caso especial de criação de ativos criptográficos em que os bitcoins são trocados por tokens recém-criados. Essa ferramenta tem sido amplamente utilizada para o financiamento coletivo de blockchains, como o da Ethereum. No caso específico da RSK, as BTOs permitem que as startups recebam o financiamento diretamente em Bitcoins, que é a criptomoeda mais segura e estável que existe, enquanto criam os tokens na blockchain da RSK protegidos pela taxa de hash do Bitcoin que faz mineração mesclada na RSK. Todo o processo de emissão de tokens pode ser feito sem confiança por meio dos serviços da ponte RSK.

Securitização de ativos

A RSK possibilita a criação de tokens digitais lastreados em ativos reais. Esses tokens podem ser usados para o comércio digital de REITs, ações, títulos de dívida ou qualquer outro ativo (ou procedimento futuro). Este caso de uso específico fornecerá uma solução exclusiva para as pequenas empresas nos países em desenvolvimento, onde os mercados financeiros tradicionais não atendem à demanda por capital de giro ou capital para financiar uma expansão.

Remessas descentralizadas

Este caso de uso específico é especialmente importante nos mercados em desenvolvimento, onde a população sem acesso a serviços bancários/sem documentação precisa pagar um ágio sobre as remessas enviadas para suas famílias, destinadas a pagar por alimentos e habitação. A RSK possibilita tokens com valor fiduciário, e a mobilização da infraestrutura existente de câmbios e opções de saque para ativos criptográficos pode fornecer remessas a custos significativamente mais baixos.

Registro/Proteção de PI (propriedade intelectual)

A RSK permite o desenvolvimento de contratos que fornecem Prova de Existência (PoE). A PoE permite que indivíduos e empresas comprovem a existência de um determinado documento (ou direito de propriedade), a qualquer momento, com a segurança da Blockchain Bitcoin. Este caso de uso poderia ser particularmente importante em países da América Latina, África e Ásia, onde os mecanismos de identidade e registros de imóveis podem não ser confiáveis.

Sistemas de votação

A RSK possibilita a criação de votos digitais que poderão permitir eleições extremamente seguras e transparentes a um custo mínimo. Além disso, poderia ser usada para garantir um processo de votação transparente para conselhos de administração de empresas ou organizações descentralizadas.

Microcrédito

Mais de 50% da população global não tem acesso ao sistema financeiro tradicional. Essa falta de acesso ao crédito é uma causa direta da desigualdade econômica que a sociedade global enfrenta hoje em dia. A RSK permite o desenvolvimento de contratos de microcrédito digitais e programáveis escalonáveis, capazes de fornecer acesso ao crédito para os 3 bilhões de habitantes mais pobres do mundo.

Rastreabilidade da cadeia de suprimentos

A RSK também permite a criação de carteiras digitais para rastrear e seguir (digitalmente) a localização física de um determinado produto ou lote. Esse tipo de contrato pode ser particularmente útil no comércio internacional e nos setores de varejo, alimentos e saúde, entre outros. Como todos os outros casos de uso, a RSK possibilita a rastreabilidade por meio da segurança do blockchain Bitcoin, a um custo mínimo.

Reputação online e identidade digital

Um dos principais problemas dos mercados em desenvolvimento é a falta de documentação e identificações para os pobres. Isso impede que os pobres votem, tenham acesso a serviços de saúde e auxílio financeiro e denunciem crimes/abusos. A RSK possibilita a criação de registros globais digitais tão seguros quanto o blockchain da Bitcoin a um custo extremamente baixo.

Moeda global para jogos

Muitos jogos multi-player têm economias próprias, incluindo moedas privadas. À medida que esses jogos evoluem, as moedas virtuais se tornam tão valiosas para os usuários quanto a moeda fiduciária e são frequentemente negociadas em mercados secundários. A inflação, a fraude e o roubo online se tornam grandes riscos e preocupações para os usuários. Além disso, as empresas de jogos pode enfrentar problemas jurídicos e de segurança por ter o dinheiro virtual dos usuários em consignação. À medida que o mundo se torna globalizado, o mesmo acontece com os jogos virtuais, e os jogadores ficarão desconfortáveis se o dinheiro acumulado em um jogo não puder ser facilmente gasto em

outro jogo. A RSK pode resolver esses problemas ao permitir que os jogos aceitem BTC (em Smart Bitcoins ou RBTC) para seus pagamentos dentro do jogo ou criem um ativo digital privado protegido pela RSK. Os pagamentos RSK fornecidos por redes off-chain de 2ª camada podem ser tão rápidos quanto os sistemas de circuito fechado para valores baixos, permitindo que os motores de jogos usem a RSK como o sistema de compras dentro dos jogos para negociações entre jogadores e ofertas virtuais da empresa aos jogadores. Ao clicar em um URL ou escanear um código QR, a negociação pode ser acionada usando o software externo de e-wallet do jogador padrão, também pagando comissões para a empresa de jogos.

Sites de jogos de azar e mercados de previsão

Pagamentos rápidos também significam reembolsos rápidos. Os sites de jogos de azar que usam Bitcoin, como o SatoshiDice, conseguiram proporcionar uma experiência de apostas rápidas sem registro, usando confirmações 0 e transações encadeadas, mas com risco de segurança para o site. A RSK permite apostar com pagamentos quase imediatos com confirmação de blocos diferente de zero.

Jogos justos

Ao incorporar contratos inteligentes, e em conjunto com protocolos criptográficos bem estudados, como o Mental Poker, a RSK é capaz de fornecer uma plataforma aberta e justa para jogos de cartas sem a exigência do pagamento de comissão para um terceiro de confiança.

Tokens não fungíveis (NFTs)

Os NFTs são tokens exclusivos que podem ser vinculados a uma propriedade, uma licença, um produto ou um serviço específico. Os NFTs podem ser facilmente criados na RSK, permitindo casos de uso em vários setores, desde itens esportivos colecionáveis até recursos de jogadores ou “skins”.

Visão geral da tecnologia

A plataforma RSK é, em sua essência, a combinação de:

- Uma máquina virtual determinista Turing-completa com contabilidade de recursos (para contratos inteligentes)
- Uma sidechain do Bitcoin com paridade bidirecional (para câmbio em BTC) baseada em uma Federação protegida com módulos HSM personalizados. Uma vez implementado o protocolo Drivechain no Bitcoin, o plano original é passar para um mecanismo drivechain híbrido.
- Um protocolo de consenso baseado em mineração mesclada e resistente à mineração egoísta
- Uma rede de propagação de blocos de baixa latência (para pagamentos rápidos).

Máquina virtual Turing-completa

A máquina virtual RSK (RVM) é o núcleo da plataforma de contratos inteligentes. Os contratos inteligentes são executados por todos os nós completos da rede. O resultado da execução de um contrato inteligente pode ser o processamento de mensagens entre contratos, criando transações monetárias e alterando o estado da memória persistente dos contratos. A RVM é compatível com a EVM no nível do opcode, permitindo que os contratos da Ethereum sejam executados sem falhas na RSK. Atualmente, a máquina virtual é executada por interpretação. Em uma atualização de rede futura, a comunidade RSK está planejando melhorar substancialmente o desempenho da VM. Uma proposta é emular a EVM por meio do redirecionamento dinâmico dos opcodes da EVM para um subconjunto de bytecodes semelhante a Java, sendo que uma máquina virtual semelhante a Java com segurança reforçada e memória restrita será a nova VM (RVM2). Isso poderá levar a execução do código RSK para um desempenho próximo ao código nativo.

Principais características:

- Máquina virtual independente, mas altamente compatível com a EVM no nível do opcode.
- Executa Ethereum DApps com a segurança da rede Bitcoin.
- Pipeline de melhoria de desempenho documentada em várias RSKIPs (Propostas de Aprimoramento da RSK) criadas pela comunidade RSK.

Sidechain

Uma sidechain é uma blockchain independente cuja moeda nativa é vinculada automaticamente ao valor de outra moeda blockchain por meio de provas de pagamento. Existe uma paridade bidirecional quando duas moedas podem ser trocadas livremente, de maneira automática, sem incorrer em uma negociação de preço. Na RSK, o Smart Bitcoin (RBTC) tem paridade bidirecional com o BTC.

Na prática, quando BTCs são trocados por RBTCs, nenhuma moeda é “transferida” entre as blockchains em uma única transação. Quando ocorre uma transferência, alguns BTCs são bloqueados no Bitcoin e a mesma quantidade de RBTCs é desbloqueada na RSK. Quando os RBTCs precisam ser convertidos novamente em BTCs, os RBTCs são bloqueados novamente na RSK e a mesma quantidade de BTCs é desbloqueada no Bitcoin.

Paridades bidirecionais com confiança totalmente minimizada e livres de terceiros podem ser criadas se duas plataformas tiverem contratos inteligentes Turing-completos. Mas como o Bitcoin atualmente não suporta contratos inteligentes nem opcodes nativos para validar provas SPV externas, parte do sistema de paridade bidirecional na RSK exige confiança em um conjunto de terceiros semiconfiáveis (STTP), que chamamos coletivamente de Federação. Nenhum STTP único pode controlar os BTCs bloqueados – é preciso uma maioria de STTPs para liberar fundos de BTC. Cada STTP tem uma chave para proteger os BTCs bloqueados e, ao receber comandos da blockchain RSK, desbloqueia os BTCs que precisam ser transferidos de volta para o Bitcoin. Observe que, se um usuário transferir BTCs para RBTCs e vice-versa, ele normalmente não receberá bitcoins que estão diretamente conectados por UTXOs com os BTCs originais enviados. Portanto, não bloqueia RBTCs para usuários específicos, mas para toda a rede RSK.

O bloqueio e o desbloqueio de fundos é feito pela Federação, sem qualquer intervenção humana. Um requisito para fazer parte da Federação é a capacidade de auditar o comportamento adequado do software que alimenta o nó, especialmente em relação à exatidão do componente que decide liberar os fundos em BTCs. A RSK Labs desenvolveu um firmware para um Módulo de Segurança de Hardware (HSM) que os STTPs podem usar para fornecer segurança máxima a suas chaves privadas e, no futuro, poderem aplicar um protocolo de validação de transações para melhorar ainda mais a segurança.

Em janeiro de 2019, a Federação RSK é composta por 15 notários conhecidos e altamente seguros. As principais empresas de blockchain atualmente integram a Federação RSK e participam de um protocolo autônomo para bloquear bitcoins com segurança. Em troca de seu trabalho, os membros da Federação recebem 1% das taxas de transação geradas na RSK para cobrir os custos de hardware e manutenção. Existe um processo automatizado para modificar a composição da Federação. Cada membro da Federação pode aceitar ou rejeitar uma alteração de composição. O processo, que é pouco frequente, é comandado por um contrato inteligente e portanto é aberto ao público. O protocolo tem um atraso consensual de uma semana até que a alteração seja ativada. Isso permite que os usuários transfiram os bitcoins de volta para a rede Bitcoin caso não confiem na nova composição da Federação.

Após o Bitcoin adicionar opcode especiais ou extensibilidade para validar provas SPV como um hard-fork e o novo sistema provar ser seguro e livre de confiança, a função da Federação como um STTP não será mais necessária e a comunidade RSK implementará as mudanças para adaptar a RSK ao sistema livre de confiança. A comunidade RSK também propôs um Drivechain BIP, que permite que mineradores participem da segurança dos bitcoins na paridade e diminui ainda mais a confiança exigida nos STTPs.

Mineração mesclada

Baseado em Proof-of-Work, o consenso Satoshi é o único sistema de consenso que impede a reescrita do histórico da blockchain a um custo baixo. A comunidade acadêmica está aprofundando o conhecimento e as pesquisas sobre a Proof-of-Stake (Prova de participação) como uma alternativa, mas atualmente o PoW oferece a mais alta segurança comprovada. A mineração mesclada é uma técnica que permite que mineradores de Bitcoin minerem simultaneamente outras criptomoedas com custo marginal próximo de zero. A mesma infraestrutura e configuração de mineração que eles usam para minerar Bitcoins é reutilizada para minerar RSK simultaneamente. Isso significa que, como a RSK recompensa os mineradores com taxas de transação adicionais, o incentivo para mineração mesclada se torna maior.

Identificamos três fases para o crescimento da mineração mesclada da RSK:

- Fase de bootstrapping – a mineração mesclada está abaixo de 30% da taxa de hash do Bitcoin.
- Fase estável – a mineração mesclada está entre 30% e 60% da taxa de hash do Bitcoin.
- Fase madura – a mineração mesclada é superior a 60% da taxa de hash do Bitcoin.

A RSK abandonou sua fase de bootstrapping, quando mineradores por mesclagem maliciosos poderiam reverter a blockchain RSK por um baixo custo. Em janeiro de 2019, mais de 40% dos mineradores de Bitcoin estavam envolvidos na mineração mesclada da RSK. Mas como as taxas da RSK permanecem baixas em comparação à recompensa de bloco do Bitcoin, o custo para atacar a RSK através de gasto duplo é menor do que o do Bitcoin.
A RSK possui algumas propriedades para reduzir o risco de ataques por gasto duplo, como a longa maturidade para as recompensas dos mineradores. Ainda assim, a equipe de pesquisa da RSK Lab desenvolveu várias proteções para evitar ataques durante as fases estável e madura do projeto:

- **Notificações assinadas:** Os clientes RSK podem fazer uso de notificações assinadas por notários. Os nós podem usar essas notificações para detectar ataques de Sybil e informá-los aos usuários.
- **Trilhas de gasto duplo transparentes:** método em que todas as tags de mineração mesclada da RSK são reforçadas com informações adicionais, que podem ser usadas para detectar forks RSK egoístas que são públicos na blockchain do Bitcoin. As provas de fork egoísta são construídas automaticamente e apresentadas aos nós RSK, que as espalham pela rede. As provas forçam os nós a entrarem em um “modo de segurança”, em que nenhuma transação é anunciada como confirmada. O modo de segurança impede que os comerciantes e os câmbios aceitem pagamentos que possam ser de gasto duplo. Uma vez que o comprovado fork egoísta é ultrapassado pela cadeia RSK principal no PoW acumulado, a rede retorna ao seu estado normal. Este método é um impedimento para qualquer tentativa de ataque de gasto duplo à RSK (no qual o minerador malicioso ainda tenta coletar recompensas de Bitcoin ao minerar o fork egoísta).

Quando a plataforma entrar na fase de Maturidade, estimamos que a segurança da RSK será suficiente para suportar a economia da inclusão financeira mundial.

Principais características:

- Protocolo de consenso DECOR+
- Maturidade de 1 dia para a recompensa de mineração.
- Nenhuma perda de eficiência esperada na mineração de Bitcoin em decorrência da mineração mesclada (para troca tardia de estado intermediário)

Pagamentos rápidos e rede de baixa latência

A RSK já permite redes de pagamentos off-chain de 2ª camada, mas mesmo assim pretende oferecer uma rede de pagamentos on-chain muito melhor em comparação ao Bitcoin. Para alcançar esse objetivo, a RSK adota os protocolos DECOR+ e FastBlock5, os quais permitem atingir uma taxa de blocos média de 15 segundos que não cria incentivos para a centralização da mineração e a mineração egoísta.

Principais características:

- Intervalo de bloco de 15 a 30 segundos (dependendo da eficiência de troca de estado dos mineradores)
- Propagação total dos últimos blocos concorrentes na rede para impedir a mineração egoísta e reduzir a taxa de blocos obsoletos.
- Novo comando de rede para distribuir cabeçalhos de blocos com prioridade urgente.
- Protocolo DECOR+ para o compartilhamento de recompensas entre blocos concorrentes.
- Protocolo GHOST para ponderação de cadeia.

Desde a criação do Bitcoin, existe uma corrida rumo a intervalos menores para criptomoedas baseadas em blockchains PoW. Porém, o baixo intervalo de blocos pode afetar a estabilidade e a capacidade da rede de criptomoedas, de modo que vários fatores de design devem ser considerados. Em primeiro lugar, o fator mais importante que afeta a viabilidade de intervalos de confirmação curtos é o número de blocos obsoletos gerados. O principal fator que afeta a taxa de blocos obsoletos é o protocolo de propagação de blocos. Na RSK, analisamos cuidadosamente esse protocolo e executamos simulações para verificar o desempenho, a usabilidade e a segurança da rede.

No Bitcoin, quando dois ou mais mineradores resolvem blocos na mesma altura, surge um claro conflito de interesses. Cada minerador concorrente deseja que seu bloco seja selecionado pelos mineradores restantes como a melhor ponta da cadeia, enquanto os demais mineradores geralmente não se importam com qual dos dois blocos será escolhido. No entanto, todos os demais mineradores e usuários honestos preferem racionalmente que a mesma ponta de bloco seja escolhida, pois isso reduz a probabilidade de reversão. O protocolo de consenso DECOR+ estabelece os incentivos econômicos certos para uma escolha convergente, sem requerer interação adicional entre os mineradores. O protocolo DECOR + é uma estratégia de compartilhamento de recompensas que incentiva a resolução econômica do conflito de tal forma que:

1. O conflito é resolvido deterministicamente quando todas as partes têm acesso às mesmas informações de estado da blockchain.
2. A solução escolhida maximiza as receitas de todos os mineradores (coletivamente)

e de ambos os mineradores em conflito, caso as recompensas de bloco apresentem uma grande diferença
3. A solução escolhida maximiza a resistência à censura se os blocos concorrentes tiverem aproximadamente as mesmas recompensas.
4. A resolução do conflito leva um tempo insignificante.

Privacidade de transações

A RSK não fornece por si só melhor privacidade de transações do que Bitcoin e baseia-se em pseudônimos. No entanto, a VM da RSK é Turing-completa, portanto as tecnologias de anonimização, como CoinJoin, Ring Signatures ou zCash podem ser implementadas com segurança sem a confiança de terceiros.

Escalabilidade

A RSK pode se expandir muito além do Bitcoin em seu estado atual. Um pagamento da RSK requer 1/5 do tamanho de um pagamento padrão do Bitcoin. Com o protocolo LTCP proposto, o tamanho de transação pode ser reduzido para 1/50 do tamanho de transação do Bitcoin. Isso leva imediatamente a um aumento substancial na capacidade de volume de transações. Além disso, existem propostas da comunidade (RSKIPs) para permitir esquemas de assinatura selecionáveis pelo usuário: ECDSA, Schnorr e Ed25519. Como o Ed25519 tem melhor desempenho do que a curva Bitcoin ECDSA, o uso desse esquema pode levar a uma capacidade ainda maior.

Comparação dos recursos da RSK

A tabela a seguir é uma tentativa de comparar os principais recursos da RSK com os recursos de outras alternativas, incluindo a sidechain Liquid (Blockstream) e o token WBTC (BitGo). Tanto a Liquid quanto o WBTC estão atrelados ao BTC. Mostramos que, essencialmente, a RSK apresenta melhores soluções técnicas com baixo impacto na descentralização.

Item	Bitcoin BTC	Ethereum ETH	Ethereum WBTC	Liquid LBTC	RSK RBTC
Tempo médio de confirmação	10 min.	15 seg. (GHOST)	Igual a Ethereum	60 seg.	15 a 30 seg. (DECOR+GHOST)
Limite de segurança (devido à mineração egoísta ou conluio)	~30%	Menor que 30%	Igual a Ethereum	50%	50% (DECOR+GHOST)
Contratos inteligentes Turing-completos	Não	Sim	Sim	Não	Sim
Adiciona valor ao Bitcoin	-	Não	Sim	Sim	Sim (mineração mesclada)
Integração com o Bitcoin	-	Não	Não	Sidechain	Sidechain
Clientes SPV	Sim	Sim	Sim	Sim	Sim
Integração de carteira de hardware	Sim	Sim	Parcial	Não	Sim
Garantia de finalidade de transação	Consenso Nakamoto. SHA256D	Consenso Ethereum. Ethash	Igual a Ethereum	Federação	DECOR+GHOST. SHA256D PoW
Transações confidenciais	Não	Via contrato	Não	Sim	Via contrato. Suporte nativo previsto
Escalabilidade [tps]	3 (6 com segwit)	Não consolidado, atualmente 15	Igual a Ethereum	3 (6 com segwit)	Não consolidado, atualmente 10
Tamanho da blockchain	200 GB	> 1,5 TB	> 1,5 TB	~300 MB	~2 GB
Segurança de indexação do token	--	--	Empresa única	Federação	Federação
Token	BTC	ETH	WBTC	LBTC	RBTC

O papel da RSK Labs

A RSK Labs se consolidou como uma referência dentro da comunidade ao criar a implementação de referência do nó RSK. Atualmente, a RSK Labs continua realizando atividades técnicas e comunitárias, como:

- Estímulo ao desenvolvimento da plataforma de referência RSK por meio de atualizações periódicas
- Colaborações com a comunidade acadêmica
- Manutenção de canais de discussão comunitários, fóruns e FAQs
- Coordenação de conferências e encontros locais
- Promoção do uso da blockchain RSK
- Solicitação e publicação de auditorias de segurança externas periódicas
- Participação em discussões sobre atualizações de rede propostas pela comunidade
- Auditoria de segurança na base de código da RSK
- Assessoramento de governos, startups, empreendedores e empresas sobre as melhores formas de se beneficiarem da rede RSK

O compromisso contínuo da RSK Labs com a RSK é recompensado pela plataforma RSK: 20% das taxas de transação da plataforma são pagas a uma conta controlada pela RSK Labs.

O futuro da RSK

A trajetória da RSK foi definida pela comunidade RSK. Durante os primeiros anos de desenvolvimento da RSK, a RSK Labs teve um papel ativo na construção da implementação de referência. Depois que a RSK foi lançada, a RSK Labs continuou altamente envolvida na comunidade, melhorando a base de código e propondo melhorias através do sistema de repositório de propostas RSKIP. O repositório ajuda os membros da comunidade a coordenarem discussões, rejeições, aceitações e implantações em várias bases de código. A quantidade de propostas de melhoria é enorme. Veja uma lista de algumas das principais propostas apresentadas até dezembro de 2018:

Memória distribuída, Dependência dinâmica de contrato, Execução paralela usando dependências estáticas de contrato, Execução paralela usando dependências de contrato de tempo de execução, Operações de shift, Limite de tamanho dos blocos, Aluguel de armazenamento persistente pago por código, Mineração sem verificação, Preço mínimo de combustível negociado, Transações que nunca invalidam blocos, TXINDEX Opcode, Suspensão de contratos, Suporte para ativos estáveis e emissão de tokens, Contrato Inteligente do Reward Manager (REMASC), Contrato Inteligente Simplificado do Reward Manager (REMASC), Árvore de estado combinado, Aluguel de armazenamento persistente simplificado, Rápido despertar de hibernação usando Trie, Formatos de endereço RSK, Espaços de memória Survive e Ephemeral, Aluguel de armazenamento persistente eficiente, Vínculo com o número de elementos da árvore Merkle, POUBS em cadeia, Nova trie binária, Caches de memória, Opcodes DUPN e SWAPN, Aluguel de armazenamento de alta eficiência , Segwit efêmero, Alteração no custo de criação de conta, Paginação de código, Compressão de hibernação, Endereços com hash duplo, CODEREPLACE opcode, Seções de dados Contract const, Gerenciamento dos membros da federação BridgeMaster, Encapsulamento de transações, Carteiras inteligentes de Endereço único , Compressão de assinaturas, Contas multichave, Ponte básica para paridade bidirecional com o Bitcoin, Transações na ponte Bitcoin estendidas, Remover world midstates dos recibos, Formato de endereço sequencial , Remover o desconto de zero bytes nos dados, Nova árvore de eventos e LOG estendido, Mecanismo de informações de taxas de mineração de blocos, Opcode CALLNUM, Informar o combustível livre médio por bloco, Canais de pagamento de hub de um a múltiplos, Versões de script usando o pseudo-opcode HEADER, Registro de configuração mapeado por memória, Aluguel de armazenamento orientado por cache , Compactação de transações Lumino (LTCP), Privacidade de valor e destino das transações, Pagamentos probabilísticos nativos, Mineração sem verificação esporádica, Caminho de derivação para carteiras deterministas hierárquicas, Manuseio de forks do Bitcoin, Contratos filhos, Codificação de endereços Checksum , Aluguel de armazenamento orientado por cache (coletar na versão EOT), Propagação de blocos compactada usando lote de atualização state trie (COBLO), Assinatura dupla para agregação de assinatura atrasada, Dados TX padrão, Pagamentos probabilísticos off-chain nativos, Ajuste de dificuldade mais suave,

DELEGATECALL como uma extensão do conjunto de instruções, Gerenciamento dos membros da federação BridgeMaster

Embora algumas propostas ainda sejam imaturas, outras evoluíram após várias rodadas de discussão e provavelmente ganharam apoio da comunidade para se tornarem parte de futuras atualizações da rede.

Conclusões

A RSK é a primeira sidechain do Bitcoin em produção que fornece contratos inteligentes Turing-completos, é compatível com os padrões Ethereum e garantida pela mineração mesclada de Bitcoins.

A RSK representa o resultado de 5 anos de melhorias na tecnologia blockchain e permite que o ecossistema Bitcoin utilize as melhores características do dinheiro e dos pagamentos programáveis, aumentando simultaneamente o valor e o uso do bitcoin.

O design inovador da RSK permite maior escalabilidade e custos de transação reduzidos.

A RSK permite que os desenvolvedores em todo o mundo criem soluções descentralizadas corporativas e pessoais executáveis na rede mais segura do mundo, com um baixo custo de transação que atende a uma ampla gama de necessidades e casos de uso.

A RSK permite que os mineradores de Bitcoins participem do mercado de Contratos Inteligentes, adicionando valor significativo à indústria de mineração de Bitcoins e garantindo sua sustentabilidade em longo prazo. Contribui para a sustentabilidade econômica dos mineradores de Bitcoin e para o crescimento da segurança da rede Bitcoin.

A RSK oferece aos usuários e empresas Ethereum uma nova plataforma compatível para implantar suas soluções usando o Bitcoin como moeda nativa, confiando na infraestrutura de mineração Bitcoin para sua segurança e acessando uma base de usuários mais ampla.

A RSK permite a criação de um sistema financeiro baseado em blockchain descentralizado, seguro e de baixo custo, que criará inclusão e oportunidades para mais de três bilhões de pessoas que continuam sem acesso aos bancos e com dificuldades financeiras em nosso mundo.