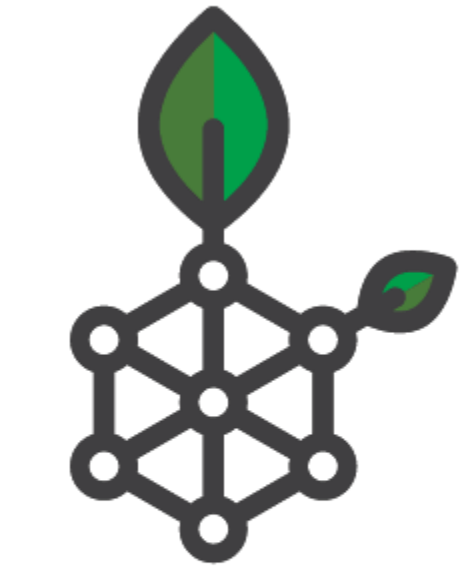

RSK

Visão geral do white paper

Revisão: 9
Data: 19 de novembro de 2015
por Sergio Demian Lerner

Introdução

Em 2008, Satoshi Nakamoto revolucionou a indústria de pagamentos ao criar o Bitcoin. O Bitcoin contemplava uma implementação muito limitada dos chamados “contratos inteligentes”, um conceito introduzido em 1993 por Nick Szabo.

Desde então, muitas pesquisas têm se dedicado à criação de novas criptomoedas compatíveis com programas distribuídos Turing-completos. Hoje, há uma confiança generalizada de que máquinas virtuais úteis, seguras e determinísticas podem ser desenvolvidas para atingir esse objetivo.

Acreditamos que novos casos de uso são necessários para que o Bitcoin se torne a principal criptomoeda global, sendo que a adição de recursos de contrato inteligente é fundamental para que esse futuro se transforme em realidade. Com isso em mente, criamos a RSK, uma plataforma de contratos inteligentes que incorpora uma Máquina Virtual Turing-Completa ao Bitcoin. A plataforma também fornece outros aprimoramentos à rede, como transações mais rápidas e melhor escalabilidade – recursos que, na nossa opinião, também possibilitarão novos cenários de uso.

A RSK é uma evolução do QixCoin, uma criptomoeda turing-completa criada em 2013 pela mesma equipe de desenvolvimento. A RSK oferece uma experiência de pagamento aprimorada com confirmações quase instantâneas. Atualmente, a plataforma atinge 300 tps e confirma a maioria dos pagamentos em menos de 20 segundos. No entanto, é baseada nas mesmas garantias de segurança do Bitcoin, suportando mineração mesclada SHA-256D.

A RSK funciona como uma sidechain do Bitcoin. Quando são transferidos para a blockchain da RSK, os Bitcoins se transformam em “SmartBitcoins” (SBTC). Os SmartBitcoins são equivalentes a bitcoins que vivem na blockchain da RSK e podem ser convertidos novamente em Bitcoins a qualquer momento, sem custo adicional (com exceção das taxas de transação padrão da RSK). O SBTC é a moeda base usada na sidechain da RSK para remunerar os mineradores pelo processamento de transações e contratos. Não há emissão de moeda: todos os SBTCs são criados a partir de Bitcoins provenientes da blockchain do Bitcoin.

A RSK aprimora o Bitcoin nas seguintes áreas:

- Máquina Virtual RSK Turing-Completa (RVM) que permite contratos inteligentes
- Média de 10 segundos para a primeira confirmação de transações
- Mineração mesclada segura, combinando PoW com mineração de federação baseada em assinatura de limite de backup
- Backbone de baixo atraso e retransmissão rápida incorporado em uma rede gossip peer-to-peer.
- Paridade bidirecional através de sidechains (atualmente uma paridade federada e totalmente automática sujeita a melhorias do Bitcoin)

Acrônimos: “RSK” refere-se ao Rootstock (a plataforma), termos relacionados são “protocolo RSK” (a especificação) e “nó de referência RSK” (a implementação de referência), a moeda RSK nativa é o “SmartBitcoin”, “SBTC” é o símbolo da moeda

SmartBitcoin, “BTC” refere-se à moeda Bitcoin, e “Bitcoin” refere-se ao protocolo Bitcoin.

Por que a RSK é importante para o ecossistema Bitcoin?

Alinhamento das partes interessadas do Bitcoin e proteção do valor

O principal objetivo da governança da RSK é alinhar as principais partes interessadas do Bitcoin por meio da criação de recompensas totalmente alinhadas às suas atividades atuais.

Essa filosofia é refletida diretamente em sua arquitetura central, na qual os mineradores de Bitcoin fornecem o poder de hashing necessária para as validações dos blocos através de proof-of-work; os líderes do setor (Câmbios, Carteiras e Processadores de Pagamento) integram a federação que cria pontos de verificação de validação e assinam as transações de resgate da paridade bidirecional.

Além disso, as decisões relativas a melhorias na plataforma RSK baseiam-se num sistema de votação em que mineradores, líderes da indústria, detentores de Bitcoin/RSK e os principais desenvolvedores tomam a decisão final.

Nos parágrafos a seguir, descrevemos como esses incentivos funcionam.

Modelo de governança

Cada participante da comunidade possui o know-how para melhor servir aos interesses da comunidade: os câmbios e as carteiras virtuais sabem como proteger as economias de Bitcoin; os mineradores sabem como realizar operações de mineração em grande escala para proteger as transações do usuário; as empresas de Blockchain inovam em novos casos de uso e fazem com que os sonhos se tornem realidade; os principais desenvolvedores possuem conhecimento técnico para enfrentar os desafios técnicos que surgem; os mantenedores de nós fornecem a infraestrutura e a conectividade de rede; e os usuários são o coração do sistema, proporcionando confiança e liquidez.

O modelo de governança da RSK visa representar todos os atores dessa comunidade por meio de um conselho de governança composto por cinco membros. Os mineradores poderão votar com poder de hashing (um voto), os usuários de Bitcoin e RSK votarão com prova de participação (um voto), os câmbios e as carteiras virtuais votarão por meio da Federação (um voto), os principais desenvolvedores da RSK e do Bitcoin terão um sistema de votação de limite especial (um voto) e o último voto será oferecido a uma instituição Bitcoin estabelecida sem fins lucrativos, como a Bitcoin Foundation, que pode representar o ecossistema mais amplo. Além disso, um voto institucional pode ser oferecido à Fundação Ethereum, se esta for representativa da comunidade Ethereum.

Proteção do investimento do minerador de Bitcoin

Em agosto de 2016, a margem de rentabilidade da mineração de Bitcoin cairá para menos de 50% devido à queda na recompensa de blocos, que passará de 25 BTC para 12,5 BTC. Centenas de milhões de equipamentos de mineração se tornarão instantaneamente

obsoletos. Isso provavelmente inclui todas as máquinas de mineração existentes no mercado atualmente, já que duas gerações de chips (mais rápidos e com menor consumo de energia) serão desenvolvidas e vendidas antes de 2017. Quase todos os mineradores atuais que não substituírem seu hardware terão que fechar seus negócios de mineração. Devido à sua capacidade de mineração mesclada, a RSK representa uma oportunidade para esses mineradores continuarem no mercado por pelo menos mais quatro anos. 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, a redução de 50% da lucratividade da mineração criará uma concentração adicional nos mineradores de baixo custo, o que aumentará a vulnerabilidade da rede Bitcoin. Assim, a RSK também poderia desempenhar um papel fundamental na promoção de uma ampla base de mineradores lucrativos, aumentando a segurança e o valor do Bitcoin.

Se aproveitarem essa oportunidade hoje a um custo mínimo e criarem aplicativos para a RSK, os mineradores de Bitcoin poderão não apenas proteger seu investimento, mas também desenvolver uma nova oportunidade de negócio.

Protegendo a paridade bidirecional Bitcoin/RSK

As principais empresas de Bitcoins integrarão uma Federação que desempenhará o papel fundamental de garantir a transferência de fundos entre as blockchains Bitcoin e RSK. Em troca, essas empresas lucrarão com as taxas geradas pelo acordo entre a entrada e a saída de recursos financeiros.

Taxas de transações de Bitcoin mais baixas e emissão de ativos de valor estável

Os atuais detentores e potenciais usuários de Bitcoin têm visto sua utilização do sistema monetário limitada a determinados casos (por exemplo, investimentos e rede de pagamentos global), principalmente devido à volatilidade de preços do Bitcoin, mas essa restrição pode piorar no futuro devido a um aumento potencial das taxas de transação no próximo corte da recompensa (Bitcoin halving).

A RSK traz uma solução para esse problema, oferecendo uma validação de transações quase instantânea (20 segundos) e a emissão de ativos com preços atrelados a uma moeda fiduciária ou outro commodity estável. A redução da exposição à volatilidade nas transações, mantendo o Bitcoin como moeda de reserva, aumenta o valor global do Bitcoin.

Fortalecimento da segurança do Bitcoin

No próximo corte de recompensa do Bitcoin, centenas de milhões de dólares em equipamentos de hardware de mineração tornados obsoletos serão vendidos por preços baixos em transações privadas ou pela internet. Isso abrirá uma janela de vulnerabilidade, dando a um possível atacante a possibilidade de comprar uma enorme quantidade de poder de hashing por muito pouco dinheiro e executar um ataque de 51%. Além disso, a diminuição da segurança pode afetar o valor percebido da moeda.

Ao aumentar a lucratividade da mineração de Bitcoin com a mineração mesclada da RSK, a rede Bitcoin pode impedir que a taxa de hash despenque.

A RSK como uma rede de pagamento de BTC de baixo custo

Se o tamanho do bloco de Bitcoins não for aumentado por meio de um hard-fork no próximo corte na recompensa do Bitcoin, as taxas de transação de Bitcoin podem se tornar exageradamente altas para certas aplicações. Como os blocos RSK podem realizar muito mais transações do que os blocos Bitcoin, a RSK naturalmente oferecerá taxas mais baixas. Veja a próxima seção para uma análise dos cenários futuros relacionados às taxas de transação.

O futuro do Bitcoin e de suas taxas de transação não é claro: atualmente, propostas controversas sobre mudanças no tamanho máximo dos blocos terão um alto impacto nas futuras taxas de transação. Na tabela a seguir, tentamos prever cenários futuros e comparar RSK e Bitcoin com base em suposições razoáveis sobre crescimento e forks.

Parâmetro	Bitcoin	RSK
Tempo de confirmação com segurança comparável de acordo com a conversão de Satoshi	10 minutos	10 segundos
Tempo mínimo de confirmação para uma probabilidade de reversão de 0,1%	20 minutos (2 blocos)	30 segundos (3 blocos)
Máx. de transações por segundo	3,3 tps (considerando-se uma transação de tamanho médio)	300 tps no lançamento Escalável para 1000 tps
Custo médio atual de uma transação padrão para usuários	USD 0,06 Considerando: - 1,5 tps	Preço de mercado não disponível
Custo atual para os mineradores incluírem uma transação padrão	USD 0,01 Considerando: - A utilização de uma rede de retransmissão rápida - UTXO na memória - tempo de processamento de 1 ms por transação - Recompensa média de 25,2 BTC por bloco USD 0,05 Considerando: - A utilização de uma rede de retransmissão padrão	< USD 0,01 (estimado) Considerando: - Sem troca de hardware específico para RSK. - Quase sem transações RSK USD 0,01 (estimado) - A interrupção de um minerador para carregar um novo cabeçalho resulta na perda de 10 ms do tempo de processamento
Taxas de transação até o final de 2016	USD 1,6 Considerando: - O tamanho do bloco não aumentou - A taxa BTC/USD não mudou - Mesmo nível de segurança - 3 tps	USD 0,01 (estimado) Considerando: - 3 tps

É importante observar no gráfico acima que as estimativas de taxas de transação são baseadas no fato não comprovado de que o preço do BTC permanecerá em aproximadamente BTC/USD 240 ao longo de 2016. Se o preço aumentar dez vezes durante esse período, as taxas de transação também aumentarão, tornando a Blockchain Bitcoin viável como um sistema de compensação interbancário, mas não como uma rede de pagamentos. Também é importante destacar que sistemas de pagamento off-chain podem surgir, fornecendo pagamentos mais baratos, mas ao mesmo tempo centralizando a rede e mudando sua natureza descentralizada.

A tabela a seguir mostra possíveis cenários futuros até o final de 2016, supondo que a dificuldade de hashing da rede aumente na mesma proporção que o preço do BTC:

Cenário	Custo de transação de Bitcoin para os mineradores	Custo de transação de RSK para os mineradores
O preço do Bitcoin aumenta em 10x	USD 16	USD 0,02
As TPS aumentam em 10x por meio de hard-fork	USD 0,11	USD 0,002
O preço do BTC e as TPS aumentam em 10x	USD 1,1	USD 0,02

À medida que o custo de inclusão de uma transação de Bitcoin aumentar, os usuários migrarão para plataformas com custos de transação mais baixos, como a RSK.

Casos de uso da RSK

A plataforma RSK fornece contratos inteligentes Turing-completos, 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 com Ethereum a oportunidade de se beneficiar da robustez da blockchain do Bitcoin. Apresentamos a seguir uma lista de potenciais contratos inteligentes e casos de uso que podem ser desenvolvidos sobre a plataforma RSK.

Canais de micropagamento e redes Hub-and-Spoke

Os canais de micropagamento permitem que duas partes façam pagamentos regulares e seguros de baixo valor pagando apenas uma taxa quando o canal é fechado, em vez de pagar taxas para cada transação.

As redes Hub-and-Spoke permitem que usuários mutuamente não confiáveis façam pagamentos únicos de baixo custo de maneira indireta, usando canais de pagamento de e para terceiros com confiança mínima. A RSK permite que as redes Hub-and-Spoke sejam implementadas diretamente de forma descomplicada e interagindo de forma nativa com as carteiras eletrônicas padrão.

Troca distribuída peer-to-peer

Utilizando o protocolo TierNolan, a RSK suporta contratos que atuam como trocas peer-to-peer. A correspondência automática em um livro de pedidos também pode ser criada com facilidade. Isso permite mercados distribuídos sobre blockchains independentes, trocando ativos criptográficos sem a presença de terceiros.

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 (de 10 minutos a 1 hora para garantir a irreversibilidade). A RSK permite que os consumidores se beneficiem da segurança do Bitcoin com confirmações que levam apenas alguns segundos. Comerciantes poderão aceitar pagamentos instantaneamente sem exigir gateways de terceiros. Outro elemento fundamental que qualquer plataforma deve ter para ter sucesso no mercado de varejo é a capacidade de suportar uma grande quantidade de transações por segundo (tps). A rede RSK, utilizando o protocolo DÉCOR+, permite processar até 300 tps sobre a Blockchain Bitcoin (o dobro do Paypal)

Serviços de custódia

A RSK permite a criação de serviços de custódia inteligentes em que os oráculos assinam (ou não) uma transação, definindo se esta deve ser executada (ou não) sem ter qualquer contato com os fundos sob custódia.

Criação de ativos criptográficos

A RSK permite a criação de ativos criptográficos (ou altcoins) garantidos pela rede Bitcoin. Dada a flexibilidade da RSK para precificar o combustível do contrato, esses

aplicativos (como todos os outros) poderiam ser usados tanto por estudantes como por bancos e corporações.

Securitização de ativos

A RSK também permite a criação de tokens digitais lastreados em ativos reais. Esses tokens poderiam 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.

Registro/Proteção de IP

A RSK permite o desenvolvimento de contratos que podem replicar o que é conhecido 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 registros de imóveis podem não ser confiáveis.

Sistema de votação

Como um caso particular de ativo criptográfico, a RSK permite a criação de votos digitais que possibilitam eleições extremamente seguras e transparentes a um custo mínimo.

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 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 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, denunciem crimes/abusos e tenham acesso a auxílio financeiro. A RSK permite 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 preocupações dos usuários. Além disso, a empresa 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 moedas RSK equivalentes) para seus pagamentos dentro do jogo ou criem um ativo digital privado protegido pela RSK. Os pagamentos RSK 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 por meio da confirmação de blocos.

Fair-playing

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.

Esses são apenas alguns exemplos entre muitos outros que poderiam ser desenvolvidos e programados na plataforma RSK por meio da tecnologia Bitcoin subjacente. É importante mencionar que são os mineradores de Bitcoin (via mineração mesclada) que executarão esses contratos e se beneficiarão da grande maioria do combustível consumido para esse propósito.

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 com paridade bidirecional (para o comércio denominado em BTC)
- Um protocolo de consenso dinâmico, híbrido, federado/de mineração mesclada (para segurança de consenso) e uma rede 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 em paralelo por uma alta porcentagem dos nós 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. O nível de código operacional da RVM é compatível com a EVM, para permitir que os contratos da Ethereum sejam executados sem falhas na RSK. Na primeira versão, a máquina virtual é executada por interpretação. Para a próxima versão, planeja-se emular a EVM por meio do redirecionamento dinâmico dos códigos operacionais da EVM para um subconjunto de código de bytes semelhante a Java, sendo que uma máquina virtual semelhante a Java com segurança reforçada e memória restrita será a nova VM (RVM2). Isso levará a execução do código RSK a um desempenho próximo ao código nativo.

Principais características:

- Máquina virtual (VM) independente, mas compatível com a EVM no nível do código operacional.
- A RSK oferece aos usuários da Ethereum a possibilidade de executar seus projetos com a segurança da rede Bitcoin.
- Novos códigos operacionais para aritmética int32 rápida e melhor compilação just-in-time (planejada), proporcionando um melhor desempenho.

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 SmartBitcoin (SBTC) possui uma paridade bidirecional com o BTC (mais precisamente, um Rootoshi, a unidade de conta mínima do RSK, é atrelado a um Satoshi, a unidade de conta mínima do Bitcoin).

Na prática, quando BTCs são trocados por RTSs, nenhuma moeda é “transferida” entre as blockchains em uma única transação, pois o Bitcoin não consegue verificar a autenticidade dos saldos em outra blockchain. Quando ocorre uma transferência, alguns BTCs são bloqueados no Bitcoin e a mesma quantidade de SBTCs é desbloqueada na RSK. Quando os SBTCs precisam ser convertidos novamente em BTCs, os SBTCs são bloqueados novamente na RSK e a mesma quantidade de BTCs é desbloqueada no Bitcoin.

Sidechains semi-livres-de-confiança

Paridades bidirecionais totalmente confiáveis e sem terceiros podem ser criadas usando contratos inteligentes em ambas as plataformas. Mas como o Bitcoin atualmente não suporta contratos inteligentes nem códigos operacionais nativos para validar provas SPV externas, parte do sistema de paridade bidirecional na RSK exige confiança em um conjunto de terceiros semiconfiáveis (STTP). Nenhum STTP único pode controlar os BTCs bloqueados – é preciso uma maioria de STTPs para liberar fundos de BTC. Os STTPs armazenam temporariamente os BTCs que estão bloqueados e desbloqueiam os BTCs para pagar os usuários do Bitcoin. Os SBTCs ficam bloqueados na RSK para serem transferidos de volta para o Bitcoin.

Na RSK, os STTPs que protegem os fundos bloqueados são os membros da Federação. Isso ocorre porque os incentivos da Federação estão altamente alinhados com os STTPs: devem ser atores respeitados da comunidade (como universidades, por exemplo) e também ter a capacidade técnica de manter um nó de rede seguro. O bloqueio e desbloqueio de fundos é feito por esses nós de rede seguros sem qualquer intervenção humana. Portanto, 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 sobre a liberação de fundos BTC. Planejamos criar um hardware à prova de adulteração que reforçará o algoritmo de validação federado para melhorar ainda mais a segurança.

Após o Bitcoin adicionar códigos operacionais 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 equipe RSK implementará as mudanças para adaptar a RSK ao sistema livre de confiança.

Mineração mesclada híbrida dinâmica/Federação

Acreditamos que o PoW é o único sistema de consenso capaz de impedir a reescrita do histórico da blockchain a um custo baixo. Todos os outros sistemas de consenso que não consomem recursos valiosos para a mineração têm essa desvantagem, contam com a reputação e impedem a participação anônima na mineração. Todos os outros sistemas de consenso exigem que novos usuários confiem em um conjunto de partes para encontrar um ponto de verificação autenticado do ledger.

O consenso PoW de alta taxa baseado em blocos periódicos com baixo desperdício órfão exige que os mineradores interrompam seus mineradores de hardware e os reiniciem para realizar a mineração em novos estados intermediários de header cada vez que um novo bloco é resolvido pela rede. Isso resulta em lacunas de tempo de mineração ou em latências de rede maiores para a comutação de estado intermediário, em média. Essas lacunas reduzem a eficiência da mineração de Bitcoin mesmo que consumam alguns milissegundos. Portanto, a RSK usa o esquema de compartilhamento de recompensa de bloco DECOR+ para reduzir a concorrência e permitir que os mineradores migrem para o melhor bloco RSK no futuro. Se os mineradores trocarem seu hardware cada vez que um bloco RSK for encontrado, eles competem por uma recompensa completa de bloco RSK. Caso se atrasem e continuem minerando as pontas de blocos passados, eles criam uncles e ganham uma parte da recompensa de bloco. Em nenhum desses casos eles são totalmente órfãos, pois o DECOR+ paga uma recompensa aos uncles e a regra GHOST conta os uncles como blocos normais e assegura a melhor cadeia. A eficiência da mineração de BTC é, portanto, maximizada.

Como antecipamos um período em que o poder de hashing do RSK estará abaixo de 50% do poder total de hashing do BTC, a rede estaria vulnerável a um ataque de 51%, em que o poder de hashing restante supera o poder de hashing da RSK existente para produzir um gasto duplo.

Para evitar essa situação, a RSK inclui pontos de verificação federados para blocos minerados por PoW. Os pontos de verificação federados são assinados pelos membros da Federação, sendo que os clientes podem usar a maioria das assinaturas para decidir qual é a melhor cadeia. A RSK também tem um protocolo de último recurso, segundo o qual a Federação poderá criar blocos assinados se a energia de mineração cair para abaixo de 5% do poder de hashing do Bitcoin. Por padrão, os clientes param de usar pontos de verificação federados quando o poder de hashing do Rootstock ultrapassa 66% da dificuldade máxima de hashing do BTC observada na melhor cadeia e as taxas pagas em um bloco são maiores ou iguais à recompensa média de um bloco de Bitcoin.

A plataforma RSK será lançada com uma federação de membros conhecidos e respeitados na comunidade. Cada membro é identificado por uma chave pública para o esquema de assinatura do ponto de verificação. A federação é capaz de adicionar ou remover membros usando e incorporando o sistema de votação, embora essas ações precisem de uma alta porcentagem de votos dos membros.

O objetivo dos fundadores da RSK é que a rede RSK incentive a mineração por mesclagem. No entanto, a RSK é robusta para a escassez de mineração mesclada, pois a Federação é automaticamente trazida para proteger a rede no caso de escassez.

Principais características:

- Maturidade de 1 dia para a recompensa de mineração.
- Pontos de verificação de membros federados
- Pontos de verificação incorporados em código durante o período de bootstrapping.
- Nenhuma perda de eficiência esperada na mineração de Bitcoin em decorrência da mineração mesclada (menos de 0,1% para comutação imediata de estado intermediário e 0% para comutação tardia)

Pagamentos rápidos e rede de baixa latência

O objetivo da RSK é ser uma rede de pagamentos melhor. Para possibilitar pagamentos rápidos, várias soluções foram desenvolvidas:

- Uso de seleção de bloco livre de concorrência (por exemplo, Hyperledger, Ripple, sistemas de circuito fechado)
- Uso de redes hub-and-spoke (por exemplo, rede Lightning do Bitcoin)
- Uso de taxas de blocos de alto PoW

As redes hub-and-spoke adicionam novos nós de centralização e exigem uma adaptação completa das carteiras de clientes para um modelo de pagamento novo e completamente diferente. Embora essa alternativa possa ser facilmente implementada na RSK, não constitui o sistema nativo para pagamentos rápidos. A RSK adota os protocolos DECOR+ e FastBlock5, os quais permitem atingir uma taxa de blocos média de 10 segundos que não cria incentivos para a centralização da mineração, é livre de mineração egoísta e é compatível com incentivos.

Principais características:

- Intervalo de blocos de 10 segundos
- Protocolo de propagação de blocos de dois estágios (2SBP)
- Protocolo de envio de transações ausentes (PMT)
- Propagação total dos últimos blocos concorrentes na rede para impedir a mineração egoísta e reduzir a taxa de blocos obsoletos.
- Heurística de inclusão de transação adiada (DTI). As transações são atrasadas 5 segundos na fila de transações de blocos de cada minerador para permitir a verificação de bloco mais rápida possível, pois as transações já estão presentes nos pools de todos os nós da rede.
- Novo comando de rede para distribuir cabeçalhos de blocos com prioridade urgente.
- Novo comando de rede para espalhar a lista de hash de transações de blocos imediatamente após a propagação do cabeçalho do bloco.
- Heurística de mineração em blocos não verificados (MUB). Mineração de cabeçalhos de bloco com transações não verificadas com um atraso de 5 segundos.
- Os cabeçalhos de blocos são sinalizados quando não possuem transações (exceto a Coinbase)
- Protocolo de dois fluxos priorizados para cada conexão (2PSC). Nova camada de transporte de mensagens com fatiamento de mensagens, que permite duas sessões paralelas com prioridades distintas. Isso permite que os cabeçalhos de bloco sejam enviados pela sessão de alta prioridade e interrompam qualquer mensagem que estiver sendo transmitida pela sessão de baixa prioridade.
- Protocolo de otimização de rota local (LRO). Roteamento de bloco ideal local baseado em prioridades de pares. Roteamento de transação ideal local baseado em prioridades de pares
- Protocolo DECOR+ para o compartilhamento de recompensas entre blocos concorrentes.
- Protocolo GHOST para ponderação de cadeia.

Comparação dos recursos da RSK

Fizemos uma comparação entre a RSK e outras blockchains e demonstramos que, essencialmente, a RSK apresenta melhores opções técnicas sem causar qualquer desgaste na descentralização, que é medida como o inverso do custo de execução de uma instância de nó completo.

Item	Bitcoin	Ethereum	Factom	Contraparte	RSK
Tempo médio de confirmação	10 min.	12 seg (GHOST)	1 min. (Servidores federados)	10 min.	10 seg. (DECOR+GHOST)
Limite de segurança (devido à mineração egoísta)	~30%	Entre 30% e 50%	~30%	~30%	50% (DECOR+GHOST)
Contratos inteligentes Turing-completos	Não	Sim	Sim	Planejado	Sim
Adiciona valor ao Bitcoin	-	Não	Não	Não	Sim (mineração mesclada)
Integração com o Bitcoin	-	Não	Protocolo overlay	Protocolo overlay	Sidechain
Escalabilidade por meio de verificação probabilística e provas de fraude	Não	Não	Não	Não	Sim
Clientes SPV	Sim	Sim	Não	Não	Sim
Backbone de retransmissão de blocos	Sim	Não	Sim	Sim	Sim
Suporte nativo para estruturas de acesso definidas pelo usuário	Sim	Não	Sim	Não	Sim
Suporte nativo para esquemas de assinatura definidos pelo usuário	Não	Não	Não	Não	Sim
Fácil integração de carteira de hardware	Não	Sim	Não	Não	Sim
Garantia de segurança	Mineradores SHA256D	Mineradores Ethash	Mineradores SHA256D + federação	Mineradores SHA256D	Mineradores por mesclagem SHA256D + federação
Transações confidenciais	Não	Via contrato	Via programa externo	Não	Suporte nativo planejado por protocolo AppeCoin
ID de transação único	Não (maleável)	Sim	Não	Não	Sim
Escalabilidade [tps]	3 a 24	ilimitada	ilimitada	3 a 24	300 no lançamento
Token nativo	BTC	ETH	FACTOID	XCP	BTC via paridade bidirecional

Apresentação da tecnologia de pagamentos instantâneos

Desde a criação do Bitcoin, existe uma corrida para se alcançar intervalos menores para criptomoedas baseadas em blockchains e PoW. Primeiro, surgiu o Bitcoin com um intervalo de 10 minutos, depois veio o LiteCoin com um intervalo de 2,5 minutos, seguidos pelo DogeCoin, com 1 minuto, o QuarkCoin, com 30 segundos, e o Ethereum, com 12 segundos. Cada nova criptomoeda diminui um pouco esse intervalo, mas pouquíssimos designers realmente sabem quais são as implicações disso. Para entender como o intervalo de blocos afeta a estabilidade e a capacidade da rede de criptomoedas, vários fatores devem ser levados em consideração. Em primeiro lugar, o fator mais importante que afeta a viabilidade de intervalos de confirmação curtos é o número de blocos obsoletos gerados. Dois outros fatores afetam a taxa de blocos obsoletos: o protocolo de propagação de blocos e o tempo de propagação de blocos dos principais mineradores para os principais mineradores. Na RSK, analisamos cuidadosamente esses fatores e executamos simulações para verificar o desempenho, a usabilidade e a segurança da rede. Nesta seção, revisaremos os novos protocolos usados pela RSK para reduzir a taxa de blocos obsoletos.

Protocolo DECOR+

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 mineradores restantes geralmente não se importam com qual deles será escolhido. No entanto, todos os mineradores e usuários honestos restantes prefeririam que todos escolhessem a mesma ponta de cadeia, pois isso reduz a probabilidade de reversão natural. A solução ideal incentivaria os mineradores em conflito a também escolherem o mesmo pai, e o DECOR+ define os incentivos econômicos certos para uma escolha convergente, sem exigir interação adicional entre os mineradores. O 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 resolução escolhida é aquela que maximiza a receita de todos os mineradores, tanto daqueles em conflito quanto dos demais.
3. A resolução do conflito leva um tempo insignificante.

O protocolo de propagação de blocos

O Bitcoin e o Ethereum encaminham cada bloco empacotando o cabeçalho do bloco com todas as transações contidas no mesmo. Essa estratégia, embora seja a mais fácil de analisar, é conhecida por ter um desempenho ruim em relação à latência de propagação dos blocos e ao uso da largura de banda, que é duplicado. Os mineradores de Bitcoin resolveram parcialmente esse problema recorrendo à Rede de Retransmissão Rápida: um backbone centralizado que retransmite os blocos de forma comprimida e é mantido por um único usuário. A RSK nasceu com uma rede de retransmissão rápida incorporada ao protocolo de rede, e as propriedades de baixa latência emergem da topologia da rede e não exigem centralização.

Propagação de blocos de dois estágios (2SBP)

Os blocos RSK são enviados em dois estágios: no primeiro, somente o cabeçalho do bloco é enviado. No segundo estágio, a lista de hashes de transações incluídas no bloco é enviada. Com o 2SBP, a capacidade do canal é duplicada, permitindo que mais transações sejam armazenadas em cada bloco. Após cada nó ter recebido o cabeçalho do bloco e a lista de hash da transação tiver sido associada ao cabeçalho, o nó tenta reconstruir o bloco a fim de verificá-lo completamente.

Protocolo de envio de transações ausentes (PMT)

Como cada nó armazena os hashes das transações anunciadas por seus pares, o minerador também envia imediatamente as transações incluídas no bloco que ele sabe que estão faltando no pool de cada par. Isso elimina completamente a necessidade de uma segunda interação para solicitar transações adicionais. O envio das demais transações antes que elas sejam solicitadas por um par é uma terceira fase do protocolo 2SBP.

Heurística de inclusão de transação adiada (DTI)

Os mineradores incluem apenas transações que foram recebidas até alguns segundos atrás. Isso garante, com alta probabilidade, que as transações já tenham sido recebidas pelos pares antes de o bloco ser minerado. Observe que o atraso das transações é bom para o minerador, pois reduz o tempo de verificação do bloco e consequentemente diminui as chances de haver blocos concorrentes. Essa otimização não é necessária quando a heurística de mineração em blocos não verificados (MUB) estiver em vigor na rede.

Propagação imediata do cabeçalho do bloco (IBHP)

Quando o cabeçalho de um bloco atualizado é recebido, os nós encaminharão esse cabeçalho antes de verificar as transações ou a validade do bloco, verificando apenas o PoW e a altura do bloco no momento do encaminhamento. Isso permite que o cabeçalho se espalhe pela rede em menos de um segundo.

Protocolo de dois fluxos priorizados para cada conexão (2PSC)

Cada conexão de rede compreende dois fluxos lógicos bidirecionais com duas prioridades diferentes. O fluxo de alta prioridade é usado para enviar o cabeçalho do bloco imediatamente, mesmo se uma mensagem de prioridade mais baixa estiver sendo enviada no fluxo de baixa prioridade.

Heurística de mineração em blocos não verificados (MUB)

Os nós podem, então, iniciar a mineração de um bloco vazio na parte superior do cabeçalho, mesmo se as transações ainda não tiverem sido enviadas, durante um

intervalo fixo. Após esse intervalo, eles retomam a mineração em qualquer bloco que estivessem minerando antes. Esses blocos vazios reduzem o uso efetivo de largura de banda e armazenamento da blockchain, mas simulações mostram que, se for usado DBI, o número de blocos vazios gerados, o espaço necessário para armazená-los e o decréscimo nas TPS são baixos.

Protocolo de otimização de rota local (LRO)

Para reduzir o número de blocos obsoletos, é importante reduzir a latência da transferência entre mineradores. A rede RSK é otimizada dinamicamente para reduzir a latência e priorizar o tráfego entre os mineradores. Ou seja, a RSK incorpora uma rede de retransmissão rápida na rede de peers, aprimorando o protocolo gossip com geolocalização e rotas locais ideais. O caminho de encaminhamento de blocos entre mineradores é um caminho crítico para a propagação de blocos e, portanto, é de extrema importância para a rede de peers. A existência de nós de rede não mineradores na rede de peers no caminho crítico tende a aumentar a taxa de blocos obsoletos. Os nós não mineradores (como usuários finais ou nós de monitoramento) presentes no caminho crítico podem servir aos mineradores apenas como saltos fracos de anonimização. Para criar os caminhos críticos somente a partir de decisões de nós locais, é feita uma priorização de nós por meio do protocolo LRO. Esse protocolo cria uma incorporação dinâmica de um grafo acíclico dirigido (DAG) na topologia aleatória da rede RSK, na qual esse DAG conecta os mineradores da melhor maneira possível.

Reutilizando a rede de mineração Bitcoin

Uma rede de mineração concentrada, com grandes pools de mineração, tende a gerar muito menos blocos obsoletos do que uma topologia de mineração distribuída completa. Portanto, no que diz respeito aos pagamentos rápidos, as criptomoedas baseadas em PoW SHA-256D têm uma vantagem sobre as criptomoedas baseadas em PoW não compatível com ASIC.

A topologia real da rede

O design do Bitcoin assume que a rede é semelhante a um grafo aleatório, com um certo grau médio de saída e de entrada. Embora isso esteja longe de ser verdade, os nós de rede tomam decisões locais para evitar a formação de clusters geográficos (pelo menos para as conexões de saída). Essa não é a melhor topologia para ajudar a propagação de blocos. A melhor topologia para a propagação de blocos é aquela que melhor atende os melhores mineradores, encorajando conexões diretas ou roteando blocos entre eles de maneira mais rápida. Além disso, um backbone direto de minerador para minerador pode ajudar a diminuir consideravelmente o número de blocos obsoletos. Isso foi proposto para o Bitcoin aumentar a capacidade de resistência a ataques. A RSK utiliza a heurística LRO para estabelecer um backbone dinâmico, sem implicar custos de autenticação de minerador para minerador, privacidade do minerador, divulgação de endereços IP e possivelmente ataques DoS associados.

Tempo de verificação da função PoW

O SHA-256 executa as avaliações de maneira muito rápida e, portanto, o tempo de verificação do Bitcoin PoW é insignificante. Um scrypt PoW, ao contrário, pode levar de 3 a 30 milissegundos para avaliar dependendo dos parâmetros escolhidos ("resistência" GPU ou ASIC). Para proteger a rede contra spam e ataques DoS, cada nó precisa verificar o PoW do bloco antes de encaminhar o cabeçalho do bloco novamente, para que o atraso de verificação seja multiplicado pelo número de saltos no caminho crítico do bloco entre os mineradores.

Pilha de rede do cliente

Quando um nó recebe um cabeçalho de bloco, o melhor que pode fazer para reduzir a criação de blocos obsoletos na rede é encaminhá-lo o mais rápido possível. Isso significa que todas as outras atividades do nó devem ser pausadas ou interrompidas. O design da RSK permite que operações de baixa prioridade sejam imediatamente canceladas e aceitem novas tentativas. Para permitir o encaminhamento imediato, a pilha de rede do cliente não bloqueia o cliente em procedimentos de verificação de transação ou em outras atividades de manutenção, como reorganizações de cadeia. Isso é possível graças a um cliente RSK que permite a execução de múltiplos threads e atribui prioridades de thread de maneira dinâmica para impulsionar o thread que recebeu o cabeçalho do bloco.

A sobrecarga do bloco

Os cabeçalhos de bloco na maioria das criptomoedas são pequenos (~100 bytes), portanto o tamanho do cabeçalho (comparado ao tamanho total do bloco) não representa uma sobrecarga significativa. O cabeçalho RSK é maior, mas a sobrecarga do cabeçalho do bloco tem um impacto negativo perceptível no tempo de propagação, já que o MTU da rede de baixo nível geralmente é de 1500 bytes, o que é superior ao tamanho do cabeçalho do bloco.

Simulações

Simulamos a propagação de blocos usando uma simulação de eventos discretos construída especificamente para esse propósito. O simulador simula a interação entre um pequeno conjunto dos melhores mineiros, cada um em um gráfico aleatório, onde a distância de salto entre eles é próxima à distância média entre os nós da rede. Mesmo que este não seja o pior cenário, uma vez que é de interesse dos melhores mineiros estarem bem conectados, assumimos que os mineiros não têm desempenho pior do que a média. Os eventos simulados são a criação de um bloco em um dos locais e a propagação do bloco para cada um dos outros locais de mineração. Os resultados a seguir mostram a simulação RSK com um intervalo de blocos de 5 segundos e 300 TPS (atualmente o intervalo de blocos é de 10 segundos). O principal resultado da simulação é que uma transação é aceita com probabilidade de 99,98% (probabilidade de reversão de 0,02%) antes de 20,35 segundos. Observe que essa probabilidade de reversão não leva em conta que o fork substituto também pode conter a transação removida, portanto, na prática, esse valor pode ser muito menor.

Mineração mesclada segura

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 paga taxas de transação adicionais, o incentivo para mineração mesclada é alto. Mas isso também significa que o custo para atacar a rede por meio de pump-and-dump e cadeias paralelas está abaixo do custo de atacar criptomoedas não mescladas. A RSK possui várias proteções para evitar ataques durante a fase inicial de bootstrapping:

- Pontos de verificação federados: Os clientes da RSK esperam pontos de verificação assinados pelos membros da Federação. A Federação incluirá câmbios e outras partes altamente seguras envolvidas no sucesso da plataforma. Os nós usam pontos de verificação federados para detectar ataques Sybil e informá-los aos usuários.

- Maturidade das moedas mineradas: cada moeda tem um prazo de maturidade de 24 horas, ligeiramente superior ao do Bitcoin. O aumento do tempo de maturidade das moedas reduz os incentivos para ataques do tipo pump-and-dump.

- Pontos de verificação incorporados no código-fonte

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 ou AppeCoin, podem ser implementadas com segurança sem a confiança de terceiros.

Segurança

A mineração mesclada não tem sido amplamente usada por moedas alternativas, pois durante o período de bootstrap inicial das criptomoedas, ela permite que grandes pools de mineração de Bitcoin destruam as novas criptomoedas com ataques de 51%. A RSK implementa pontos de verificação federados como uma maneira segura de inicializar a plataforma e reduzir notavelmente esse risco. Além disso, a RSK será lançada com um poder mínimo de hashing equivalente a 30% do poder de hashing do Bitcoin. A Fundação RSK monitorará a integridade da rede e usará seu sistema de alerta para informar os usuários e proteger a rede contra ataques de reversão.

Escalabilidade

A RSK pode se expandir muito além do Bitcoin em seu estado atual. Um pagamento da RSK requer um quinto do tamanho de um pagamento padrão do Bitcoin, sendo que a carga útil do bloco por intervalo de tempo é 8 vezes maior do que no Bitcoin. A RSK também fornecerá vários esquemas de assinatura selecionáveis pelo usuário: ECDSA,

Schnorr e Ed25519. O último, em geral, é várias vezes mais eficiente do que a curva Bitcoin ECDSA.

Em uma situação normal, a RSK consome em média 50% menos largura de banda do que o Bitcoin, já que os blocos não contêm dados de transação, mas apenas referências a transações previamente conhecidas. O uso de armazenamento e largura de banda pode ser ainda mais reduzido através de verificação probabilística e provas de fraude.

Verificação probabilística e provas de fraude

O custo de possuir um nó completo é o principal fator que afeta o grau de centralização de uma criptomoeda. Quanto maior o custo, maior a centralização. Acreditamos, no entanto, que a posição extrema na descentralização implica que a criptomoeda não pode se tornar uma rede de pagamentos global. Ambos os objetivos estão em contradição. O Bitcoin já fornece uma rede altamente descentralizada, pois o limite de tamanho da blockchain é suficientemente baixo para garantir que a maioria dos usuários individuais possa participar. Isso permite que a sidechain da RSK aumente a escalabilidade além do Bitcoin enquanto mantém a rede Bitcoin como um protetor contra a centralização do controle da moeda.

Acreditamos que um tradeoff entre a confiança de terceiros, a confiança dos nós da rede e a autoverificação seja possível, e convidamos os usuários a encontrar a proporção com a qual estejam confortáveis. Na plataforma RSK, os nós podem armazenar e validar um subconjunto da blockchain completa, a fim de reduzir o custo do nó. Isso é feito por meio de verificação probabilística e provas de fraude. A verificação probabilística é uma técnica em que um nó (parcial) escolhe aleatoriamente os blocos que serão verificados e aceita que os blocos restantes sejam aceitáveis, desde que algumas condições sejam atendidas: algum tempo tenha se passado, alguns blocos de confirmação tenham sido adicionados, a conectividade da rede seja adequada, não tenha havido transmissão de prova de fraude válida e, opcionalmente, alguns pontos de controle autorizados tenham sido transmitidos. As provas de fraude são blocos sinalizados como “fraudulentos”. Quando um nó recebe uma prova de fraude, ele verifica se um bloco com a mesma altura foi aceito localmente (mas não validado) e, nesse caso, valida o bloco. Se for inválido, a melhor cadeia local é reorganizada adequadamente. O custo para transmitir uma prova de fraude fraudulenta é alto, uma vez que as provas de fraude também contêm provas de trabalho. Ao receber uma prova de fraude fraudulenta de um par, o nó exclui o par fraudulento. Se necessário, os nós solicitarão uma prova inicial de trabalho dos pares para impedir um ataque DoS barato usando IPs comprometidos. Os mineradores (tanto PoW quanto Federados) devem ser nós completos, de modo que um invasor que retenha os dados do bloco (mas transmita o cabeçalho) não afetará a melhor cadeia, pois os mineradores descartarão rapidamente o bloco de invasores.

Conclusões

A RSK representa o resultado de 4 anos de melhorias na tecnologia blockchain e permitirá que o ecossistema de criptomoedas utilize as melhores características do dinheiro e dos pagamentos programáveis, aumentando simultaneamente o valor do bitcoin (a moeda).

A plataforma permitirá que desenvolvedores ao redor do 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.

Isso permitirá que os mineradores de Bitcoin participem do mercado de Contratos Inteligentes, adicionando valor significativo à indústria de mineração e garantindo sua sustentabilidade a longo prazo.

A RSK contribuirá para a criação de uma base mais ampla de mineradores, fortalecendo a segurança da rede Bitcoin e

permitirá o desenvolvimento de um sistema financeiro descentralizado, instantâneo e de baixo custo, que criará inclusão e oportunidades para três bilhões de pessoas que continuam sem acesso aos bancos e financeiramente prejudicadas em nosso mundo.

Equipe central da RSK