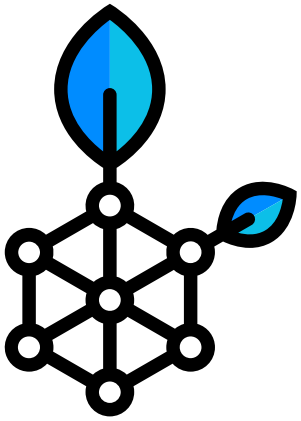


rif

RSK Infrastructure Framework

Arquitetura

Construindo a infraestrutura para a próxima geração de aplicativos distribuídos

V 1.30

Introdução

O RIFOS é um conjunto de protocolos, regras e interfaces projetados para acessar serviços descentralizados que esperamos que sejam necessários para as aplicações de blockchain mais descentralizadas. Chamamos esses serviços de Serviços de Infraestrutura de Raiz, porque juntos eles formam uma infraestrutura coerente na qual as aplicações descentralizadas podem confiar. A princípio, esses protocolos incluem: Análise de nomes, Armazenamento de dados, Comunicações certificadas seguras, Feeds de dados (ex. Oracles) e Processamento de pagamentos. Terceiros podem implementar qualquer um desses protocolos ao criar um "provedor de serviços", que é um software que fornece toda a funcionalidade do serviço ou que conecta o RIFOS a outras redes externas que fornecem esse serviço. Os provedores de serviços dos protocolos RIFOS podem ser acessados diretamente pelos aplicativos do usuário (ou seja, um provedor de serviços de armazenamento RIF pode servir como uma substituição de caixa de depósito descentralizada acessada diretamente da área de trabalho do usuário) ou consumido por outros provedores de serviços (ex., uma carteira pode usar um provedor de serviços de armazenamento RIF para armazenar os dados do usuário criptografados em servidores remotos). Todos os protocolos que fazem parte do RIFOS compartilham algumas características:

(i) Os protocolos estão preparados para interagir, posicionar ou consumir tokens RIF;

(ii) qualquer pessoa pode se tornar um provedor de serviços de um protocolo RIF anunciando o serviço; e

(iii) todos os protocolos RIF devem ser projetados de forma que, se uma camada de contrato inteligente for necessária para fornecer os serviços associados, os serviços poderão ser facilmente implementados sobre o RSK Smart Protocol.

O RIFOS foi projetado para promover um mercado justo para serviços de infraestrutura distribuída, que podem ser fornecidos por qualquer terceiro que tenha como público-alvo a

base de usuários do RIFOS. Por exemplo, o protocolo de armazenamento RIF promove a concorrência de provedores de armazenamento ao possibilitar a existência de um mercado de armazenamento.

O RIFOS facilita o desenvolvimento e a implantação de aplicativos distribuídos para usuários que não possuem um conhecimento avançado da tecnologia subjacente. Isso ocorre porque os protocolos RIFOS são projetados para esconder alguns detalhes técnicos e o funcionamento interno de serviços descentralizados. Neste sentido, o objetivo do RIFOS é aumentar de maneira significativa a adoção de tecnologias distribuídas de Blockchain por parte dos desenvolvedores de aplicativos e, por meio de novos aplicativos, dos usuários finais.

A RIF Labs está construindo o primeiro serviço implementando um dos protocolos RIFOS – o Diretório – mas, por design, o RIFOS é um sistema aberto. Qualquer terceiro pode fornecer um serviço predefinido, desde que o serviço esteja em conformidade com os requisitos do protocolo aplicável.

Inicialmente, o RIFOS será construído para ser compatível com a plataforma RSK Smart, pois enxergamos uma enorme sinergia entre ambos os projetos, aproveitando a segurança da mineração de Bitcoin com a extensibilidade e a funcionalidade do RSK. No entanto, os protocolos RIFOS devem empenhar-se para ser agnósticos de blockchain sempre que possível, e, no futuro, os provedores de serviços poderão abranger qualquer quantidade de blockchains.

O RIFOS no contexto da inclusão financeira

Três bilhões de pessoas estão atualmente excluídas do sistema financeiro, limitando a capacidade das pessoas de vender o resultado de seu trabalho, salvo em tempos mais difíceis, ou de receber microempréstimos para microempresas que geram riqueza em uma comunidade local. Países emergentes em todo o mundo passam por sucessivas crises econômicas e períodos de hiperinflação que, junto com governos ineficientes e incompetentes, impossibilitam aos menos favorecidos economizar dinheiro, impossibilitam o acesso de cidadãos a reservas de valor imutáveis e seguras, sem a necessidade de

permissão. A inclusão financeira que permita o acesso a um sistema financeiro seguro, descentralizado e resistente à censura é uma oportunidade única de promover melhorias abrangentes e em grande escala na vida das pessoas. Contratos estáveis e inteligentes, combinados com a segurança e o efeito da ampla Rede Bitcoin, podem realmente transformar e melhorar as vidas de milhões de indivíduos excluídos do sistema financeiro tradicional em todo o mundo.

O conjunto inicial de serviços fornecidos pelo RIFOS foi selecionado para simplificar os aplicativos desenvolvidos para solucionar problemas de inclusão financeira. No entanto, outros serviços de infraestrutura compatíveis com RIFOS, que demonstram ser úteis e genéricos, visando a outros casos de uso, podem ser integrados à estrutura e oferecidos aos desenvolvedores. O RIFOS é um protocolo padrão que pode ser usado para fornecer soluções para uma ampla variedade de conjuntos de problemas, aproveitando a tecnologia e o ecossistema subjacentes.

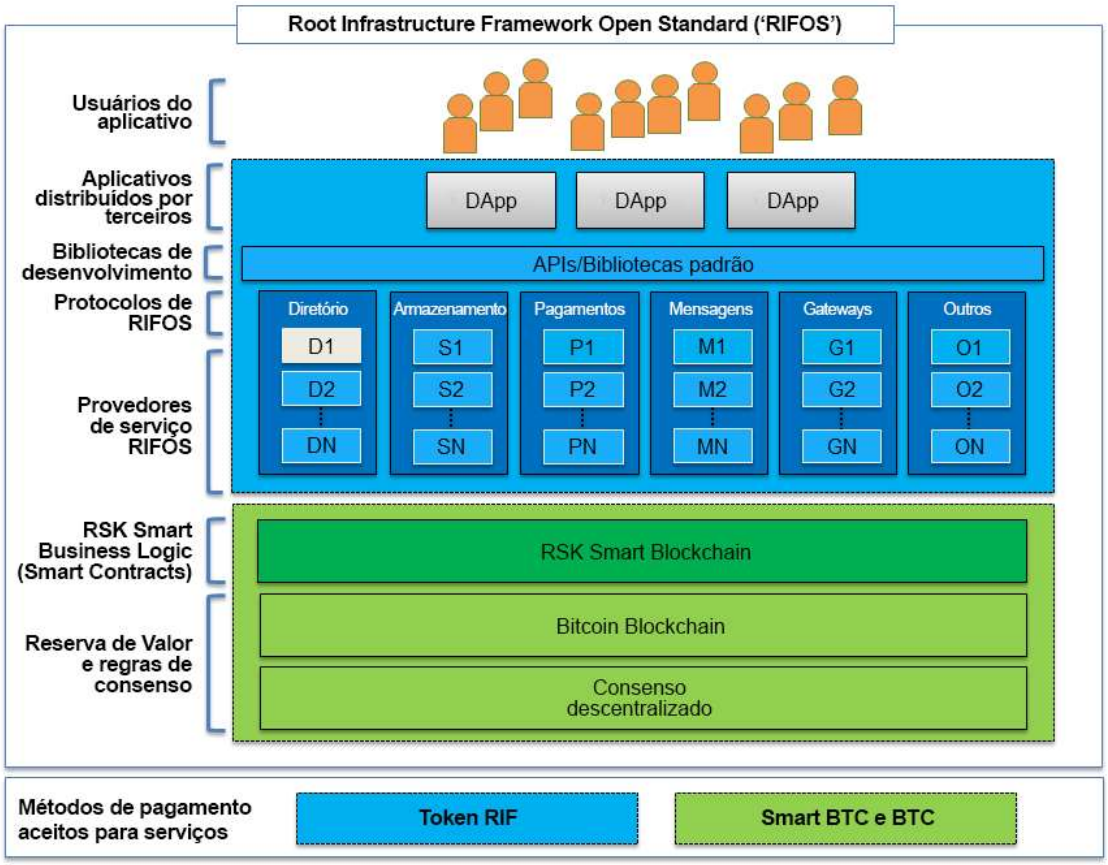
Arquitetura

O RIFOS é um conjunto de protocolos que ajuda aplicativos de usuários a consumirem serviços descentralizados. Os protocolos são implementados por provedores de serviços, que podem atender a aplicativos de usuários e também a outros provedores de serviços. Não existe uma hierarquia de protocolos RIFOS inerente, mas uma hierarquia de protocolos se materializa para cada aplicativo distribuído específico. Ou seja, alguns protocolos podem ser "protocolos suportados" de outros provedores de serviços em alguns aplicativos ou fornecer a funcionalidade principal para outros aplicativos distribuídos. Quanto mais protocolos o RIFOS integrar, mais benefícios para o desenvolvedor.

O RIFOS tem o objetivo de facilitar e agilizar a implantação de aplicativos que usem a tecnologia distribuída de Blockchain, dispensando o aprovisionamento antecipado de serviços de infraestrutura. Assim, por exemplo, um aplicativo de carteira pode crescer de um aplicativo leve, que roda em modo SPV e tem requisitos de armazenamento e largura de banda muito baixos, para uma carteira multimoeda completa, que se conecta a vários nós completos e consome diversos gigabytes de armazenamento e largura de banda, sem atualizar uma única linha de código. A mudança na funcionalidade pode ser realizada por

meio da alteração dos provedores de serviços. O RIFOS foi idealizado para possibilitar a existência de um mercado que possa satisfazer a demandas crescentes. Os desenvolvedores podem integrar seus produtos e serviços compatíveis com RIF ao ecossistema RIFOS, sem interrupções.

Os serviços RIFOS podem ser executados por qualquer pessoa. O RIFOS é baseado em um token utilitário chamado Token RIF. O Token RIF é gerenciado por um contrato inteligente executado no RSK Smart Protocol. Embora os protocolos RIFOS não obedeçam a uma estrutura hierárquica, ao considerar o RIFOS junto com o RSK e o Bitcoin, o RIFOS se torna uma pilha de desenvolvimento com várias camadas.



D1 refere-se ao Serviço de Nomenclatura RIF que é implantado no RSK blockchain.

Componentes centrais do RIFOS

Uma das principais características do design do RIFOS é permitir que provedores terceiros usem os protocolos de infraestrutura existentes. Além disso, novos protocolos de infraestrutura podem ser adicionados no futuro, pela RIF Labs ou por qualquer membro da comunidade RIFOS, a fim de aprimorar essa abordagem de padrão aberto e oferecer maior funcionalidade à base de usuários do RIFOS. Qualquer componente do RIFOS que esteja em conformidade com os princípios de design do RIFOS deve ser capaz de interoperar perfeitamente com outros componentes, utilizar os recursos disponíveis no ecossistema e competir de forma justa pelos usuários e empresas.

A RIF Labs implantará inicialmente os seguintes protocolos RIFOS (também chamados de "componentes centrais"):

- **Pagamentos RIF:** Um protocolo para acessar qualquer rede de pagamento fora da rede, especialmente redes baseadas no canal de pagamento. Esse protocolo deve permitir pagamentos fora da rede escaláveis, baratos e de alta velocidade; o RIF Payments permite o uso de diferentes redes de pagamento fora da rede e que podem ser implantadas em cima do RSK, suportando bitcoins inteligentes e tokens fungíveis padrão. O protocolo fornece métodos com semântica clara para permitir uma interação uniforme entre o usuário, uma carteira hipotética compatível com RIF e redes de pagamentos distintas. A API do RIF Payments pode ajudar na criação de pontes entre diferentes redes. A natureza de código aberto e provedor aberto da API permite que novas redes anunciem seus serviços usando o Protocolo de Diretório RIF. Cada rede de pagamento recebe um namespace de endereço distinto, fazendo com que os endereços sejam sempre exclusivos. Usando a API do RIF, serviços como gateways de ponto de venda podem ser construídos, e esses serviços de PDV podem funcionar em todas as redes de pagamento existentes e futuras de pagamento integradas ao RIF. O objetivo final do protocolo RIF Payments é a produção de um ambiente competitivo, em que as redes de pagamento possam prosperar e fornecer taxas baixas e baixa latência, e que possa ser dimensionado para corresponder ao volume e exceder o desempenho das redes de cartão de crédito legado. O RIF

Payments também propõe uma estrutura conceitual intuitiva e dependente de conceitos legados, como contas de poupança, contas correntes e depósitos a prazo.

- **Diretório RIF:** Um protocolo para sistemas de alias (Serviços de Nomenclatura) que permite ações de nomenclatura e segundos mercados. Acreditamos que as criptomoedas crescerão exponencialmente na próxima década. No entanto, o primeiro passo para a verdadeira adoção em massa é fazer com que qualquer pessoa, e não apenas o público com conhecimento técnico, seja capaz de gerenciar carteiras e ativos digitais. Portanto, uma das principais barreiras para a adoção é a complexidade inerente da tecnologia blockchain. A facilidade de uso é importante para alcançar os usuários que não têm conhecimento técnico ou acesso ao sistema bancário. É difícil esperar uma adoção ampla se os usuários precisarem copiar e colar endereços hexadecimais longos para transferir ou receber ativos digitais, para citar apenas um exemplo. Além disso, digitar manualmente endereços é um processo passível de erros, e um simples erro pode causar perdas de fundos. A introdução de um serviço de análise de nomes, também conhecido como "pseudônimos" ou "domínios", reduz de forma significativa a probabilidade de erros, bem como a complexidade aparente do sistema; quanto mais fácil for a tecnologia, mais rápida será sua adoção. A meta do Diretório RIF é encontrar diferentes tipos de recursos através de nomes de recursos simples. Exemplos de recursos incluem: Endereços RSK, chaves públicas de criptografia pessoal, usuários de redes sociais, e assim por diante. Além disso, a centralização do acesso a múltiplos recursos associados a um nome legível para humanos melhora a experiência do usuário na plataforma RSK. O Diretório RIF também pode permitir que organizações sem fins lucrativos adicionem transparência à gestão de tesouraria, divulgando publicamente seus nomes nos endereços públicos. Como nomes de recursos podem mudar com o tempo, o sistema precisa ser flexível para suportar mudanças frequentes. Por último, o sistema permite que os usuários facilmente comprem, vendam e leiloem nomes através do token RIF.

- **Comunicações Seguras RIF**: Um protocolo Peer Discovery para comunicações autenticadas e criptografadas. A Infraestrutura de Comunicações Seguras RIF (RSCI) é um protocolo cuja função é permitir que diferentes partes que precisam se comunicar entre si registrem seus métodos de comunicação, descubram outras partes e entrem em

contato com elas usando um método de comunicação preferido e suas chaves públicas como um mecanismo de descoberta. Ao usar o protocolo, Alice pode publicar seu pseudônimo no Diretório RIF, junto com a chave pública de sua comunicação. Sempre que ela usa seu pseudônimo para estabelecer uma conexão, a outra parte pode pesquisar a chave pública de sua comunicação e usá-la para criar uma conexão segura, permitindo uma comunicação pseudônima entre os participantes. A RSCI visa a atender a necessidade de se estabelecer links de comunicação seguros entre partes ou serviços do SO RIF. Esses links de comunicação devem, no mínimo, assegurar confidencialidade, integridade e autenticidade. Além das propriedades mencionadas acima, é possível criar recursos adicionais, como comunicações de grupo, não-repúdio e sigilo futuro.

- **Armazenamento RIF:** Protocolo de acesso ao armazenamento de dados descentralizado e redundante. A Camada de Armazenamento de Dados RIF (RDSL) é um protocolo que atua como uma camada de conectividade para provedores de armazenamento de terceiros. Esse protocolo introduz conceitos para permitir a transferência contínua de dados e a negociação de preços entre Provedores de Armazenamento e Clientes sobre o blockchain RSK. A natureza de código aberto e provedor aberto do protocolo permite que novas redes anunciem seus serviços no Diretório RIF. A maioria das pessoas enxerga a capacidade de armazenar dados pessoais de forma confiável como um direito inerente. As redes de armazenamento distribuído visam a proporcionar a qualquer pessoa no mundo uma conexão à Internet, independentemente de localização ou de condição financeira, a capacidade de armazenar sua identidade digital, recursos e informações confidenciais, com a confiança de que seus dados estão criptograficamente seguros e privados. A Camada de Armazenamento de Dados RIF permite que diferentes redes de armazenamento de terceiros coexistam e concorram, de modo que cada rede de armazenamento registrada na Camada de Armazenamento de Dados RIF tenha um namespace de endereço distinto para que os endereços sejam sempre exclusivos. Usando a API do RFI, será possível desenvolver serviços compatíveis que funcionem em todas as redes de armazenamento. O objetivo final da Camada de Armazenamento de Dados RIF é permitir um ambiente competitivo em que as redes de armazenamento possam oferecer soluções de armazenamento escaláveis com baixas taxas e baixa latência, permitindo que

os usuários armazenem suas informações críticas de ID criptografadas em servidores distribuídos em todo o mundo.

- **Gateways de dados RIF**: Protocolo Oracle para acesso a feeds de dados externos. Protocolos Blockchain com contratos inteligentes na rede devem se comunicar com sistemas externos por meio do Oracle. O Serviço de Gateways de Dados RIF fornece um protocolo independente de implementação para o consumo de dados externos por meio de provedores de serviços de dados. Alguns exemplos de dados externos que frequentemente precisam ser consumidos por contratos inteligentes são feeds de preços e estados de blockchains estrangeiros. A notificação segura de contratos sobre o estado de transações estrangeiras permite a transferência de tokens por meio da construção de pontes entre blockchains.

- **Explorador RIF**: Explora os serviços registrados para cada componente do RIFOS. A Plataforma RIFOS fornece uma série de abstrações e APIs para apoiar implementações de terceiros na forma de provedores de serviços RIFOS. Essa dissociação permite que a plataforma mude para implementações novas e potencialmente mais aprimoradas à medida que a tecnologia de cada serviço evolui e surgem novas soluções. Nesse contexto, é necessário fornecer mecanismos para registrar e descobrir essas implementações, permitindo que desenvolvedores e clientes escolham qual delas desejam usar para seus casos de uso específicos. O RIF Explorer é um serviço da Plataforma RIFOS que fornece a funcionalidade necessária para registrar e descobrir implementações de terceiros dos Serviços RIFOS (também conhecido como provedores de serviço) na Plataforma RIFOS. O RIF Explorer estende os recursos do Serviço de Nomenclatura RIF (RNS) para suportar recuperação de endereços de provedores de serviços não apenas pelo nome de domínio, mas também por critérios diferentes, como tipo de serviço ou metadados opcionais.

Como novos protocolos podem ser divulgados

Protocolos RIF podem ser divulgados por meio do serviço Diretório RIF. Resolvedores de nome são usados para expor links para informações relevantes para cada protocolo, como

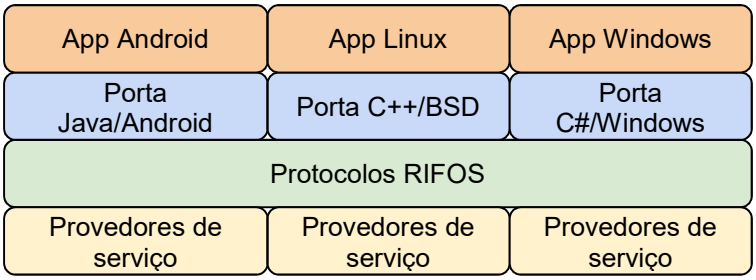
autores, licença, URLs, repositórios, documentação, preços e assim por diante. Qualquer pessoa pode registrar um novo nome e associá-lo a um protocolo RIF. Além disso, aplicativos de usuário podem descobrir protocolos disponíveis usando o RIF Explorer. Por meio de curadoria, a RIF Labs manterá uma lista desenvolvida de protocolos divulgados que foram testados e atendem à visão de inclusão financeira, mas qualquer pessoa é livre para fornecer um diretório de protocolo que selecione ou priorize os protocolos com base em outros critérios. Aplicativos auxiliares podem ser usados para automatizar as tarefas ou importar interfaces de protocolo.

Um exemplo de componente hipotético do RIFOS que pode ser adicionado é um protocolo para acessar carteiras de hardware que podem gerenciar tokens, incluindo RIF, e a correspondente implementação de um provedor de serviço para tal protocolo seria na forma de uma biblioteca de software. Outros fornecedores podem conectar bibliotecas compatíveis que estejam em conformidade com o protocolo.

Outro exemplo hipotético de um protocolo RIF útil a ser adicionado seria o RIF Reputation, que permite que os usuários marquem os protocolos com base em sua utilidade, quantidade de bugs e resposta da equipe de desenvolvimento em caso de vulnerabilidades de segurança.

Portas RIFOS

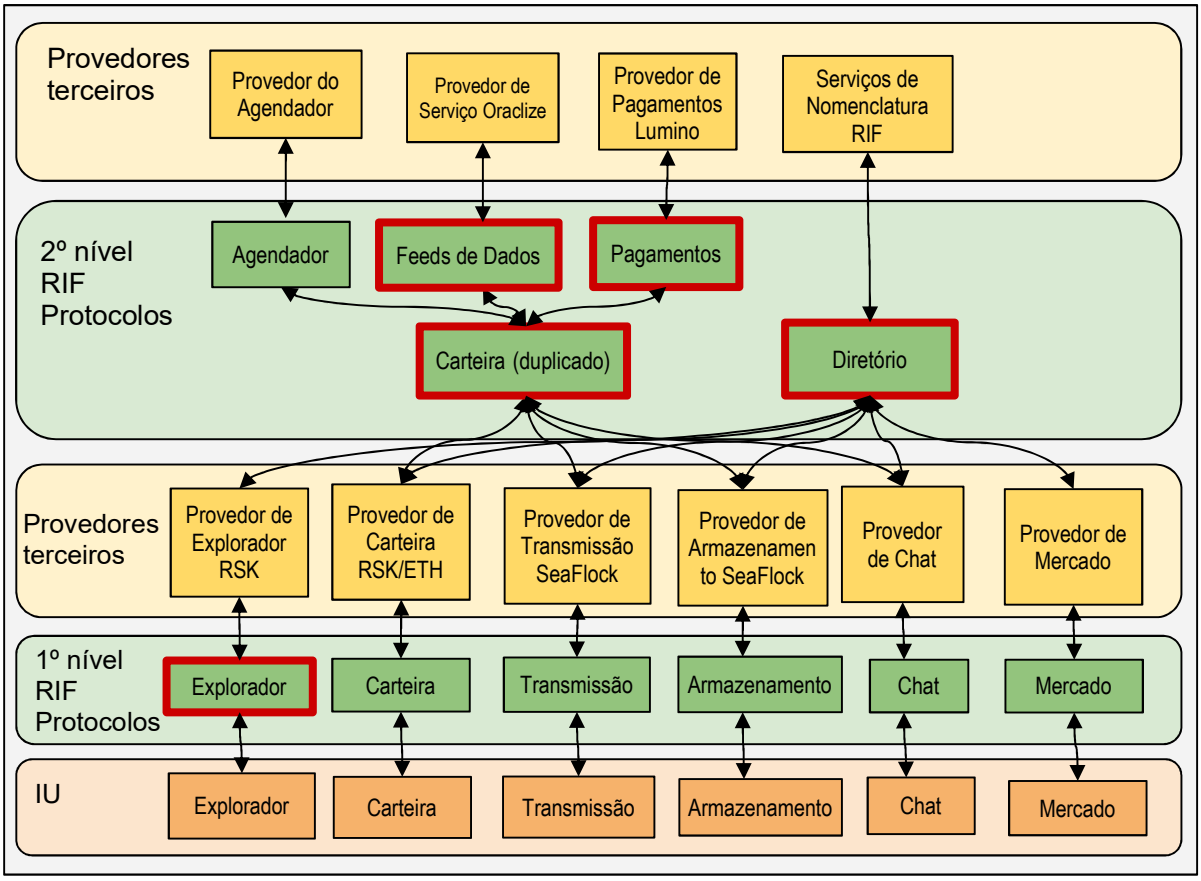
Além das interfaces iniciais fornecidas pelo RIFOS, as interfaces dos protocolos RIF podem ser implementadas em outras linguagens de programação e para outras plataformas de destino por terceiros na forma de “portas”. Os implementadores dessas portas devem cuidar de fornecer o código de cola necessário na forma de bibliotecas de software para simplificar a descoberta e a conexão de provedores de serviços com as interfaces reais, conforme exigido pelos protocolos. Embora a RIF Labs possa trabalhar para fornecer uma primeira porta dos protocolos, nenhuma porta deve ser vista como “a porta de referência”, e todas as portas devem tentar cumprir os protocolos RIFOS de maneira independente. O diagrama a seguir ilustra três possíveis portas das interfaces do protocolo RIFOS, para Android e Linux.



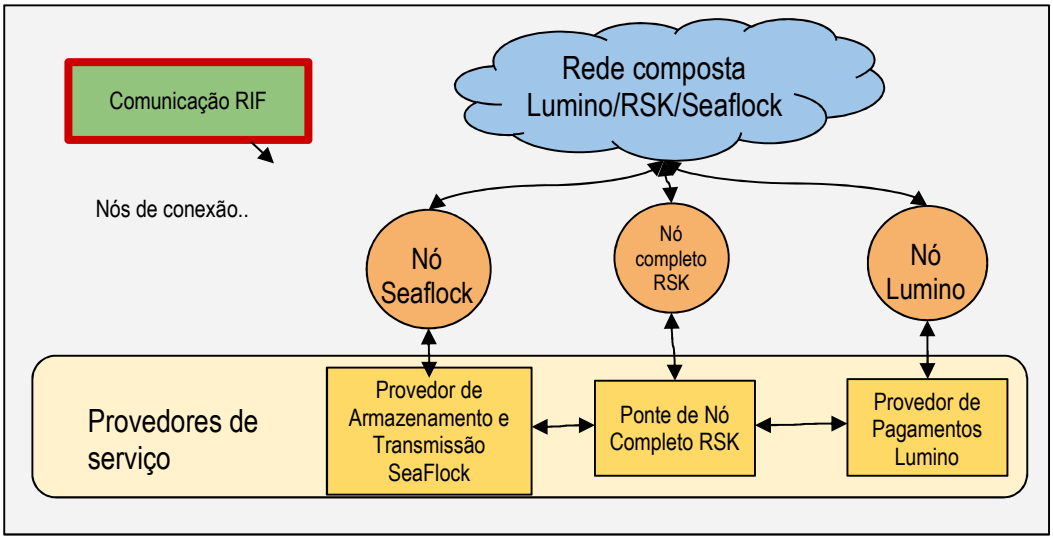
Extensibilidade

A RSK Labs arquitetou cinco protocolos centrais, mas muitos outros protocolos interessantes e que poderiam aprimorar as aplicações de descentralização são possíveis. Para ilustrar o crescimento possível dos protocolos RIFOS, apresentamos uma série de exemplos sobre uma Carteira Descentralizada (“Carteira”) hipotética, que interage com uma rede social descentralizada hipotética (“Chat”), um serviço descentralizado de transmissão de mensagens (“Publicar”) e um mercado descentralizado de aplicativos habilitados para RIFOS (“Mercado”). Esses exemplos nos permitirão demonstrar como os diferentes protocolos interagem e porque alguns protocolos (tal como armazenamento) são fundamentais para tantos casos de uso. Além disso, esses exemplos nos mostrarão como o RIFOS pode ser usado para atender às necessidades de inclusão financeira.

Na figura a seguir, ilustramos a arquitetura de uma extensão hipotética que adiciona novos protocolos e serviços para integrar uma carteira descentralizada, uma rede de mensagens de grupo descentralizada e uma rede de armazenamento descentralizada.



O diagrama a seguir ilustra como cada provedor de serviço interage com os nós da rede.



Todas as caixas verdes com bordas em vermelho representam os componentes atualmente divulgados do RIFOS. Todas as outras caixas verdes representam componentes hipotéticos a

serem adicionados no futuro. As caixas amarelas representam os provedores de serviços. Os círculos laranja representam nós da rede.

Uma nova rede descentralizada é criada, integrando as funcionalidades de várias redes em um único backbone (a rede "composta"). Cada ponto dessa rede pode anunciar e fornecer um ou mais dos diversos serviços oferecidos. Três desses serviços são Armazenamento (armazenamento de longo prazo de informações de terceiros), Pagamentos (fornecimento de pagamentos externos por meio de um caminho de canal de pagamento de saltos múltiplos) e Transmissão (fornecimento de armazenamento temporário de mensagens para suportar uma rede de transmissão de mensagens). Essa rede também fornece uma rede alternativa incentivada para a propagação de blocos e transações RSK (incluindo para qualquer outra criptomoeda).

Para cada um desses serviços fundamentais, apresentamos suas interfaces de usuário (IUs), além de uma IU de configuração e de mercado de aplicativos. Esses serviços usarão os protocolos RIFOS atuais, além de protocolos que podem ser adicionados ao RIFOS. A seguir, oferecemos uma breve descrição desses componentes:

- **Carteira RIF:** O protocolo Wallet facilita a execução de transações monetárias em blockchains suportados por RIF. Alguns dos recursos que poderiam ser suportados incluem:
    - Controle de assinatura múltipla com limites configuráveis de acordo com os valores de pagamento
    - Convênios com lista de permissões de endereços e diferentes períodos configuráveis para diferentes valores de pagamento
    - Proteção DoS reembolsável com base em depósitos para assinaturas parciais
    - Assinaturas únicas/códigos de revogação
    - Limites de taxa configurável

    - Limites de retirada configuráveis para diferentes tokens especificados em qualquer moeda FIAT/criptomoeda
    - Backup por semente mnemônica criptografada e compartilhamento de segredos
    - Pagamentos de dispositivo para dispositivo
    - Transferências dentro e fora da cadeia

- **Provedor de Carteira ETH/RSK** (para o protocolo Carteira RIF): Fornece uma carteira baseada em contrato inteligente, que é implantada em um ou mais blockchains compatíveis com RSK ou ETH. A interação com blockchains (sejam esses compatíveis com RIF ou com UTXO, como o Bitcoin) é executada usando nós completos auto-hospedados por meio de canais de comunicação seguros RIF. Para suportar carteiras baseadas em UTXO, é necessário um provedor de Carteira UTXO.

- **Chat RIF**: O protocolo de Chat permite que grupos conversem com segurança e privacidade. O protocolo utiliza o Diretório RIF como um repositório de chaves públicas para encontrar as chaves públicas do contato. Estabelece conexões peer-to-peer usando Comunicação RIF e pode negociar em contratos multilaterais em linguagem natural, desde a simples transferência de tokens até operações mais complexas, como as de troca atômica.

- **Transmissão RIF:** Um protocolo para disseminar mensagens um-para-muitos por meio de uma rede descentralizada incentivada (como um Twitter descentralizado). As mensagens têm um tempo limite especificado, e os nós armazenam essas mensagens por esse período.

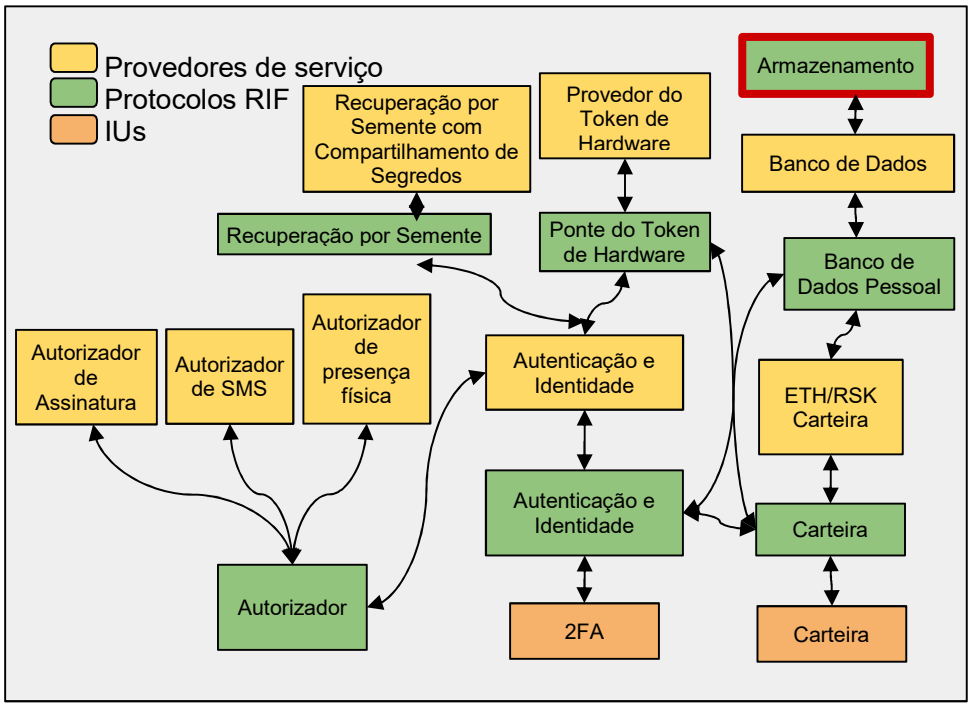
- **Ponte de Nó Completo RSK:** Este componente permite a comunicação com nós completos remotos por meio de sua interface JSON-RPC, encapsulada em um canal de comunicação seguro autenticado e criptografado.

- **Provedor de Armazenamento e Transmissão SeaFlock:** Este é um provedor único para os serviços de armazenamento e transmissão. Micropagamentos peer-to-peer por meio de canais de pagamento incentivam a rede. De forma periódica, os nós devem desafiar os

pares a atender aos requisitos de armazenamento temporário (serviço de transmissão) e penalizar os pares que não atendam a esses requisitos. O nó do provedor de armazenamento também verifica outros pares, armazenando os mesmos dados e competindo pela mesma recompensa.

- **Rede composta Lumino/SeaFlock/RSK**: essa é uma nova rede composta na qual os nós podem fornecer um ou mais serviços anunciados. Os nós podem estabelecer canais de pagamento peer-to-peer para executar micropagamentos em requisitos de comunicação, dados e computação.

O diagrama a seguir ilustra como a Carteira interage com os protocolos RIF hipotéticos para autenticação e identidade, além de mostrar como a Carteira armazena informações privadas de usuários em uma rede de armazenamento descentralizada.



Os novos componentes a seguir são apresentados no diagrama:

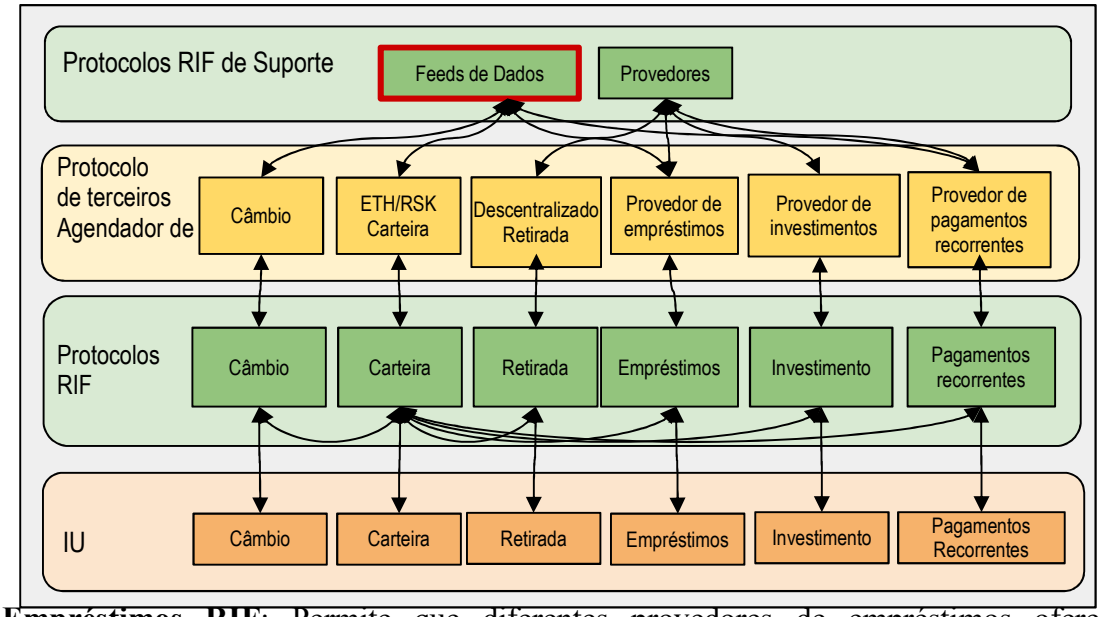
- **Ponte Hardware-Carteira RIF:** Um protocolo para se conectar a carteiras de hardware de diferentes fornecedores e fornecer serviços de transações e serviços gerais de assinatura.

- **Autenticação e Identidade RIF**: um protocolo universal de autenticação de segundo fator U2F-FIDO que usa a ponte hardware-carteira RIF para se conectar a signatários implementados em carteiras de hardware. Também gerencia um conjunto de tokens de acesso e tokens de reputação que preservam a privacidade para gerenciar uma identidade descentralizada.

- **Autorizador RIF**: Permite que o usuário selecione autorizações de terceiros para diferentes ações seguras, como retirada de fundos, transferências de alta quantidade ou divulgação de informações privadas. Os provedores podem oferecer métodos para delegar autorização, como mensagens SMS, chaves de assinatura de terceiros, senhas de uso único ou confirmação de identidade de evento por meio de presença física e biometria.

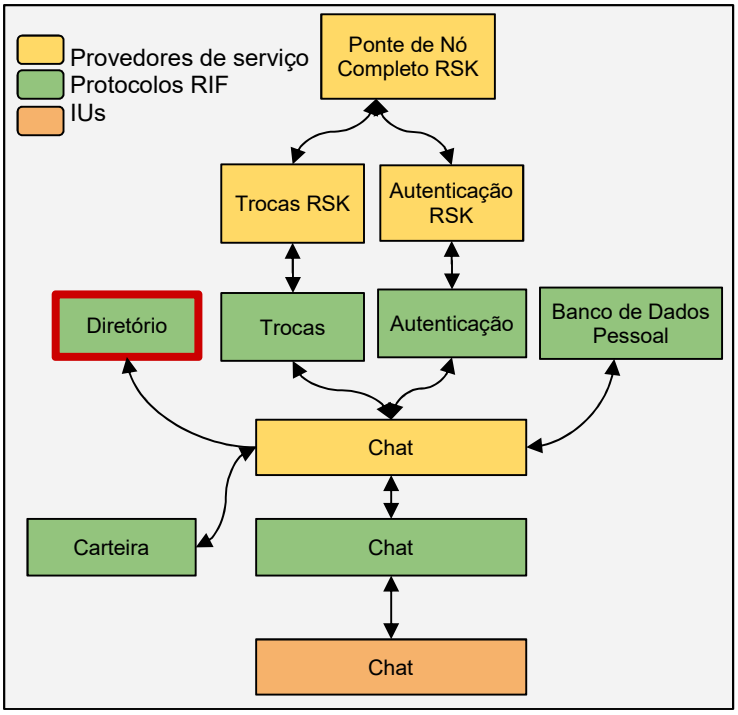
- **Banco de Dados Pessoal RIF:** O Banco de Dados Pessoal gerencia um espaço de memória pessoal criptografado, que é automaticamente replicado em servidores terceirizados usando o Armazenamento RIF. O espaço de memória inclui uma lista de identidades e, para cada uma dessas identidades, contém um backup do histórico de transações, tokens de autenticação e identificadores ativos para sistemas de terceiros, senhas, semente de chave privada, identificadores de reputação e tokens de informações pessoais que preservam a privacidade.

O diagrama a seguir mostra a decomposição da Carteira RIF com possíveis protocolos bank-in-a-box:



- **Empréstimos RIF**: Permite que diferentes provedores de empréstimos ofereçam empréstimos ao usuário. Exemplos de provedores de empréstimos incluem sistemas descentralizados ou bancos centralizados. Também permite empréstimos comerciais na modalidade crowdfunding.
- **Investimento RIF:** Permite que diferentes provedores de investimento ofereçam empréstimos ao usuário. Exemplos de provedores de investimento incluem projetos financiados por meio de crowdfunding ou depósitos a prazo fornecidos por bancos.
- **Pagamentos Recorrentes RIF:** Permite que os pagamentos sejam agendados periodicamente, tanto para montantes fixos quanto para montantes variáveis (ex., contas de luz). No caso de montantes variáveis, os provedores de serviços podem notificar os usuários sobre alterações nas tarifas e os usuários podem configurar pagamentos automáticos de montantes variáveis restritos aos valores selecionados pelo usuário.
- **Retirada RIF:** A Retirada RIF permite a retirada de fundos em espécie em moeda FIAT em pontos de venda (PoS), caixas eletrônicos ou com a ajuda de outros usuários. Também permite a retirada por terceiros em caso de remessas. Os provedores podem ser centralizados (ex., Western Union) ou descentralizados, como a rede de retiradas ABRA.

O diagrama a seguir ilustra a decomposição do componente Chat RIF, apresentando vários outros serviços hipotéticos que enriquecem a experiência do chat:



O protocolo de Chat permite o acionamento de pagamentos e trocas atômicas de ativos digitais entre os usuários do grupo diretamente da interface do chat. Além disso, qualquer texto escrito pode receber um carimbo de data e hora e ser autenticado (assinado pelo grupo de participantes ou por uma entidade externa). O comprovante é armazenado no blockchain na forma de um resumo dos dados e das assinaturas (nenhuma informação é divulgada a terceiros). Uma cópia do texto com firma reconhecida é salva automaticamente por cada participante em seu Banco de Dados Pessoais.

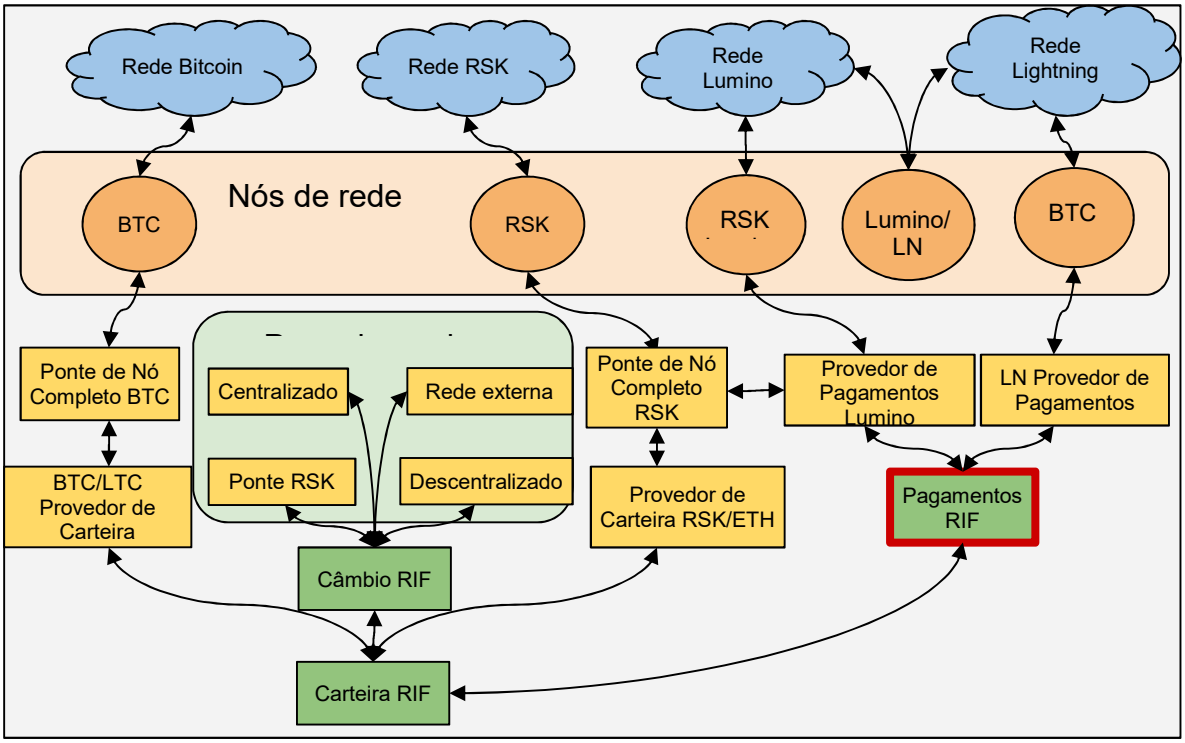
- **Autenticação RIF**: Um protocolo que permite que as informações sejam autenticadas por meio de assinaturas digitais e sejam marcadas com a data e a hora no blockchain usando um resumo de hash.

- **Provedor de Autenticação RSK**: Usa os dados efêmeros RSK para distribuir mensagens com marcação de data e hora e um contrato inteligente para que agregadores de mensagens anônimas enviem hashes de raiz candidatos para coleções merkelizadas de mensagens publicadas. Um protocolo automático de resolução de conflitos permite que as partes apliquem punições a agregadores que não cumprem as regras. Ao fazer isso, pode-

se realizar a autenticação a um custo baixo, uma vez que não há uma parte central responsável pela agregação.

- **Trocas RSK**: Um protocolo para criar trocas atômicas entre tokens fungíveis, criptomoedas e tokens não fungíveis.

O diagrama a seguir ilustra como os componentes do RIFOS podem interagir com o Bitcoin no futuro por meio de serviços de ponte hipotética fornecidos por terceiros.



Um Protocolo de Câmbio RIF hipotético define as interfaces de câmbio entre moedas e tokens. Quatro provedores hipotéticos são apresentados. O provedor Descentralizado usa um câmbio descentralizado executado sobre o RSK. O provedor de câmbio de rede externa permite que os bitcoins bloqueados nos canais de pagamento da Rede Lightning sejam enviados diretamente para os canais de pagamento Lumino por meio de um nó hipotético Lumino/LN Bridging. O provedor de câmbio de Ponte RSK permite que o BTC seja trocado por Bitcoins inteligentes e vice-versa por meio da ponte autônoma RSK. Portanto, a carteira poderia gerenciar pelo menos quatro métodos para os Bitcoins serem trocados por Bitcoins inteligentes e vice-versa, permitindo maior liquidez e o menor atrito possível.

As carteiras exibidas interagem com dois provedores hipotéticos de carteira, o provedor de carteira RSK permite gerenciar tokens baseados em RSK e bitcoins inteligentes, enquanto o fornecedor de carteira BTC permite o gerenciamento de BTC e moedas coloridas. O protocolo de Pagamentos RIF interage com dois provedores de pagamento hipotéticos: Um que possibilita a rede BTC Lightning e outro que possibilita Lumino. Desse modo, o usuário pode enviar bitcoins ou bitcoins inteligentes de forma instantânea e a baixo custo.

Como divulgar protocolos no site da RIF Labs

A RIF Labs estabeleceu um critério simples para anunciar protocolos RIFOS em sua própria página na Web, com base nos princípios do RIF. Os usuários estão livres para criar seus próprios anúncios de protocolo RIFOS de acordo com quaisquer outros critérios de sua preferência, em seus próprios sites. Nesse sentido, nossa lista de anúncios é semelhante a um site de rastreador de arquivos p2p, que fornece links para descentralizar protocolos, mas não necessariamente armazena o protocolo em si. A lista de anúncios da RIF Labs deverá priorizar protocolos que ajudam na inclusão financeira, mas a RSK Labs pode alterar ou adaptar os critérios a qualquer momento. Atualmente, os critérios dão preferência às seguintes propriedades de protocolo:

- O protocolo deve auxiliar no desenvolvimento de aplicações descentralizadas.
- O protocolo deve ser aberto para o registro de provedores de serviço.
- O protocolo deve suportar o token RIF, consumir o token RIF ou ser destinado a aumentar os recursos e o potencial de outros protocolos RIF.

Por exemplo, um protocolo de ponte carteira-hardware RIF não “consome” tokens RIF diretamente, mas aumenta a segurança para carteiras compatíveis com RIF, para que possa ser selecionado para a lista da RIF Labs.