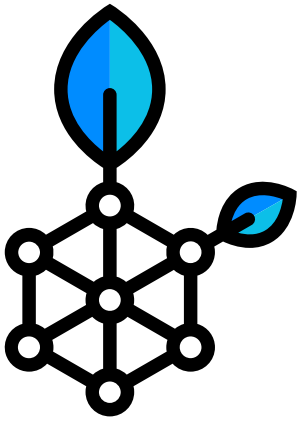


rif

RSK Infrastructure Framework

Protocolo de Identidade RIF (RIF Identity Protocol)

Construindo a infraestrutura para a próxima geração de aplicativos distribuídos

V 1.21

Resumo

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 Protocolo de Diretório RIF (RDP) 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 da plataforma. 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.

Introdução

Um dos pilares da internet é o Sistema de Nomes de Domínio (DNS), que fornece um mapeamento entre nomes legíveis para humanos e endereços IP. A Corporação da Internet para Atribuição de Nomes e Números (ICANN) é uma entidade responsável por coordenar a manutenção e as regras de vários bancos de dados relacionados aos espaços de nomes e espaços numéricos da Internet, garantindo a operação da rede. A ICANN faz a manutenção real técnica dos registros de zona raiz de DNS.

Esses serviços são o ponto central de confiança e falha[1] [2]; eles podem ser colocados offline por ataques DDoS e os mapeamentos para domínios podem ser alterados, forçando alterações nos servidores DNS ou falsificando as respostas deles. Além disso, há algumas preocupações com a segurança, como a capacidade de ISPs de bloquear nomes sem fácil detecção.

O Diretório RIF pretende se tornar um sistema semelhante ao DNS descentralizado e seguro. Os casos de uso para nomenclatura no contexto de inclusão financeira e liberdade individual são infinitos. Os serviços de nomes podem ser usados primeiro para simplificar a transferência de ativos, identificando pontos de extremidade de transações: usuários podem compartilhar um alias com amigos para garantir a segurança da comunicação ou do recebimento de pagamentos. Fundações também podem usar alias para identificar endereços de doações ou fluxos internos de fundos para outras instituições de forma transparente e segura. Serviços de nomes podem ser usados para fornecer localizadores de recursos para sites da Internet descentralizados, armazenando páginas em redes de armazenamento descentralizadas. Nomes também são usados para identificar qualquer entidade que coleta tokens de reputação que sejam públicos.

Diretório RIF e inclusão financeira

Um problema que retarda a adoção em massa de criptomoedas é a dificuldade em lidar com endereços de usuários. É difícil esperar uma adoção ampla se os usuários precisarem copiar e colar endereços hexadecimais longos para transferir ou receber ativos digitais. Por exemplo, um endereço RSK aleatório é “06f1b66ffe49df7fce684df16c62f59dc9adbd3f”, cuja transcrição manual é extremamente propensa a erros – ressaltando que um simples erro de digitação pode causar perda de fundos. Além disso, esse endereço é difícil de lembrar.
Outro caso de uso relacionado é o alias de conta bancária. No sistema financeiro bancário, cada conta bancária tem um número único de identificação. Por exemplo, no sistema bancário da Argentina , o número da conta é chamado CBU e tem 22 dígitos. Devido à sua complexidade, os bancos oferecem a possibilidade de se gerar um alias de CBU, um nome alfanumérico exclusivo composto de 6 a 20 caracteres. Os caracteres do alias devem ser do alfabeto inglês e os únicos caracteres especiais permitidos são o ponto (.) e o traço (-). É útil

em transações entre usuários de bancos. Por exemplo, Bob pode simplesmente informar a Alice seu alias, que é legível por humanos. Em seguida, ela insere o alias de Bob no campo de endereço do destinatário e executa a transação. O uso do alias de contas simplificou as transações bancárias, fazendo com que o modelo fosse adotado por toda a comunidade.
Resumindo, o RDP é um protocolo que permite que os usuários adquiram domínios comerciais que podem ser associados a recursos centralizados ou descentralizados, como páginas da web ou um alias que pode ser exclusivamente associado a recursos pessoais (por exemplo, endereços de carteira, armazenamento ou comunicação). A vantagem do uso de endereços legíveis para humanos é a redução da aparente complexidade da tecnologia Blockchain para o usuário final.

As diretrizes iniciais fornecidas neste protocolo podem estar sujeitas a mudanças adicionais, pois as ideias e a arquitetura serão discutidas e aprimoradas pelo ecossistema no futuro.

Uma implementação de Diretório RIF

A RIF Labs implementou um primeiro provedor de serviços para o RDP, chamado Serviços de Nomenclatura RIF. O RNS usa o blockchain RSK para manter e controlar o acesso às informações de nome. Portanto, o RNS garante a descentralização e segurança do blockchain RSK. Embora outros provedores de serviços RDP possam ser registrados no futuro, acreditamos que a nomenclatura é inerentemente um serviço que se beneficia muito dos efeitos de rede e, portanto, esperamos que um único provedor seja escolhido pela comunidade RIF e RSK no longo prazo.

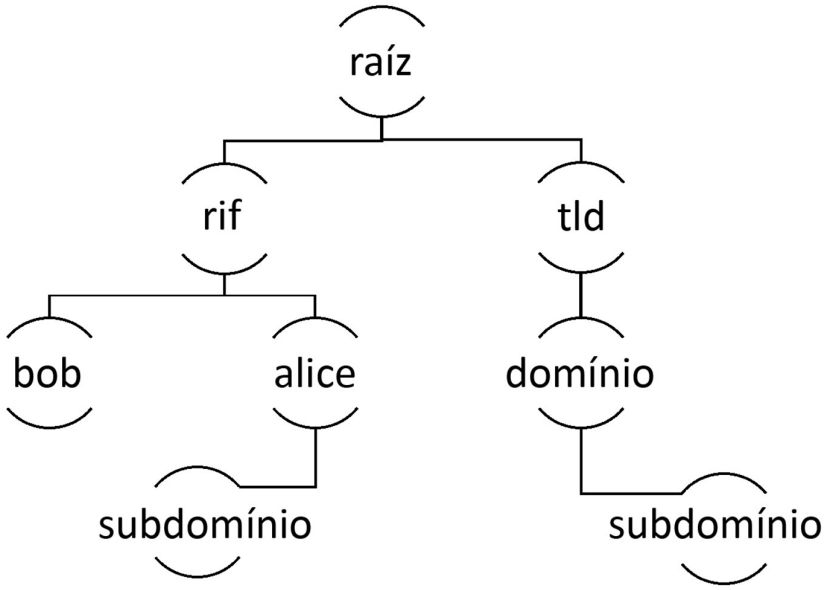
O Design do Protocolo de Diretório RIF

O Protocolo de Diretório RIF define uma interface para simplificar o uso de endereços.
Isso é essencial para implementar um mecanismo que mapeie um nome de domínio amigável para um recurso (por exemplo, um endereço RSK). O sistema deve ser transparente: os usuários devem poder atestar que possuem um determinado domínio, que pagaram as taxas necessárias e que a data de expiração está claramente definida. Assim, poderão fazer pagamentos antecipadamente e reduzir o risco da perda acidental de direitos de nome. Além disso, o design deve considerar os casos em que diferentes usuários desejam adquirir o mesmo nome de domínio (uma ocorrência frequente) e tentar resolvê-los antes que o nome seja adquirido, evitando etapas dispendiosas de resolução de disputas. Por fim, o design deve minimizar o risco de censura e o “name squatting”. Importante para o design do RDP é o token RIF, que é o token preferido para a primeira aquisição de nomes. O Token RIF é usado como um meio para apostar fichas em leilões de nomes e também para pagar o aluguel de manutenção de um nome.

Adquirindo domínios

O banco de dados de nomes de domínio é interpretado como uma árvore. A raiz da árvore (chamada nó raiz) tem controle de todo os nomes de domínio de nível superior possíveis, também chamados de TLDs. Os filhos dos TLDs são chamados de domínios. Além disso, filhos de domínios são chamados de subdomínios.

Qualquer nome do RDP deve respeitar o seguinte formato: "subdomain(n)....subdomain(1).domain.tld". Os nomes consistem em uma série de rótulos separados por pontos. O último rótulo corresponde ao TLD e os filhos sempre precedem os pais. Além disso, cada rótulo deve ser um rótulo normalizado e válido, conforme descrito em UTS46 [3], com as seguintes restrições: transitional deve ser falso e use STD3AsciiRules deve ser verdadeiro.



Obtendo um domínio em leilão às cegas

O mecanismo para se obter um domínio pela primeira vez é através de um leilão de Vickrey com lances fechados [4]. "Um leilão de Vickrey é um tipo de leilão com lances fechados. Os participantes enviam ofertas por escrito sem conhecer o lance das outras pessoas no leilão. O maior lance ganha, mas o preço pago é o segundo lance mais alto"[4]. A prática mostra que traços psicológicos humanos, e não apenas a oferta e a procura, comandam os leilões. O mecanismo de leilão de Vickrey reduz a probabilidade de um proponente pagar mais por um item, bem como também aumenta a probabilidade de o vendedor conseguir o máximo que ele puder.

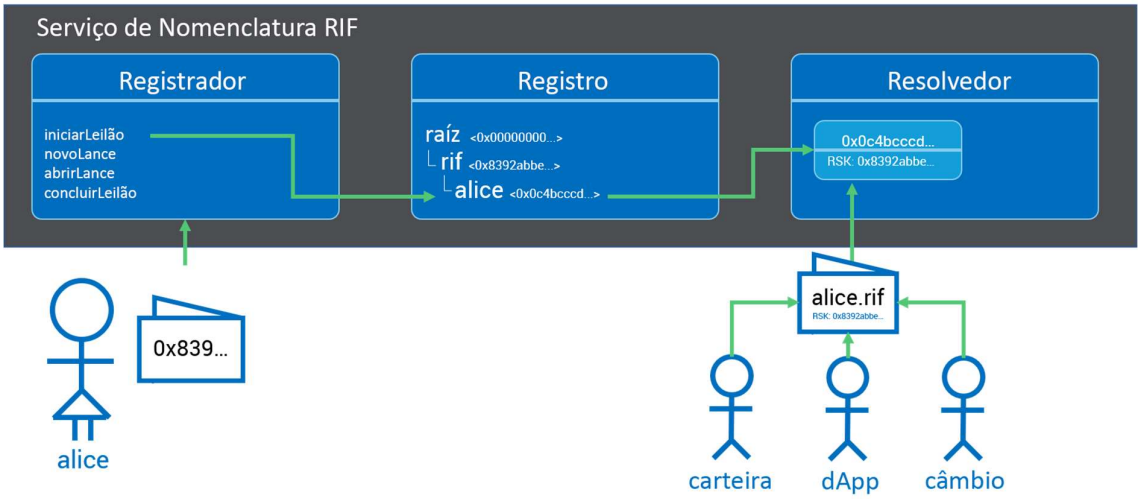
Por exemplo, se ".rif" for o TLD e uma usuária Alice quiser obter o domínio "alice.rif" (conforme mostrado na figura acima), ela poderá abrir um leilão para esse domínio, fazer uma oferta e, se for a mais alta, ela se tornará a nova proprietária do domínio "alice.rif".

Obtendo um domínio por delegação

Um proprietário de domínio pode delegar a propriedade do subdomínio a um comprador sem passar por um processo de leilão. Por exemplo, se um usuário Bob for o proprietário de "bob.rif" e Alice quiser o subdomínio "alice.bob.rif", Bob poderá delegar a propriedade do subdomínio a Alice sem um processo de leilão.
Do ponto de vista de nível de domínio, a delegação pode ser executada por meio de uma transferência de propriedade. Assim que Alice adquirir um domínio, ela deve definir um resolvedor que fará a resolução entre o novo domínio e o recurso desejado, como explicaremos na próxima seção.

Resolução de endereço de domínios

A resolução de um domínio é o processo em que o sistema procura o nome no banco de dados, verifica se ele está presente e, em caso afirmativo, retorna as informações associadas. Essa resolução pode ser usada em carteiras, trocas ou dApps, para lidar com nomes amigáveis ao usuário, em vez de endereços complexos . Por exemplo, para Alice enviar dinheiro para Bob, Bob primeiro informa seu alias registrado a Alice e, em seguida, Alice pode consultar o endereço de Bob, digitando o alias no aplicativo de carteira; a carteira consultará esse nome no banco de dados RDP e usará as informações de endereço obtidas pelo Resolvedor associado ao alias.



Mercados secundários

Embora o Diretório RIF não especifique um mercado secundário em particular a ser usado para vender domínios depois que eles foram adquiridos, já existem soluções descentralizadas de segundo mercado para as pessoas comprarem e venderem. Se a demanda for alta, esperamos que a comunidade RIF crie novos mercados secundários especificamente

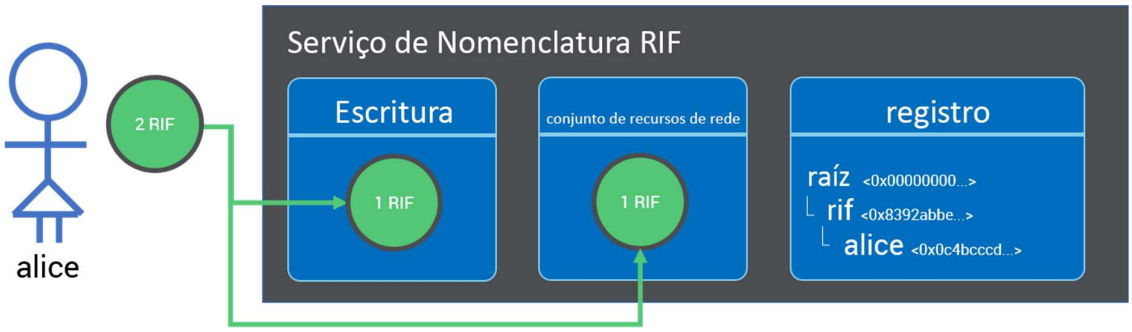
adaptados para as vendas de domínio. Mercados secundários podem aceitar o pagamento de domínios com outras moedas criptográficas e também podem aceitar outros tipos de leilões, ou simples transferências por ordem de chegada. Mercados secundários para nomes de domínio podem usar também o token RIF, mas não estão limitados a usar apenas o token.

Receitas do provedor de serviços

Prestadores de serviços podem cobrar taxas de leilões de nomes e aluguéis. Eles podem optar por gastar, doar ou reverter em lucro os recursos obtidos por meio dessas taxas. As taxas de token RIF também servem para evitar o golpe conhecido por "name squatting", pois os proprietários precisam pagar um aluguel anual de manutenção para cada domínio adquirido.

Tokens bloqueados

Quando um usuário participa de um leilão, os tokens RIF oferecidos são bloqueados na escritura como mostrado no diagrama a seguir.



Uma parte da oferta vencedora, correspondente ao valor da segunda oferta vencedora, é bloqueada em troca da propriedade do domínio. Os outros valores bloqueados correspondentes aos lances perdedores são reembolsados aos seus legítimos proprietários mediante solicitação.
Os tokens RIF bloqueados serão devolvidos ao proprietário quando o domínio for liberado, deduzidas as taxas definidas por provedores de serviços.

Pagamentos anuais

Para obter e reter a propriedade do domínio, o proprietário deve pagar uma taxa anual recorrente, chamada de aluguel. Nove meses após o pagamento do último aluguel, o proprietário do domínio terá a opção de pagar a taxa para manter a propriedade por mais um ano ou renunciar à propriedade sobre o domínio.

Se o proprietário não pagar o aluguel anual, isso significa que o proprietário está optando por desistir da propriedade. Nesse caso, os tokens que haviam sido bloqueados serão devolvidos ao usuário, deduzidos de uma taxa definida pelo provedor de serviços

O Futuro

Criamos um protocolo justo e útil, que incentiva os usuários a comercializar nomes ao mesmo tempo que reduz o comportamento abusivo. No entanto, acreditamos que o protocolo pode evoluir ou que outros protocolos RIF melhores podem substituí-lo no futuro. A seguir, apresentamos uma breve análise dos possíveis rumos para o protocolo.

Upgrades

Um provedor de serviços RDP pode habilitar atualizações de código para adicionar uma funcionalidade ou corrigir bugs. Esses upgrades seriam conduzidos pelos proprietários do provedor de serviços. Upgrades de serviço devem ser compatíveis com versões anteriores. Em outras palavras, a propriedade dos domínios não deve ser alterada (com exceção dos domínios DNS, conforme explicado na próxima seção). Estruturas de taxas, modelos de leilão e outras funções podem ser alteradas.

Domínios DNS e oráculos

O RDP abre a possibilidade de migração de endereços DNS regulares para o RDP, realizando o mapeamento entre domínios DNS e TLDs e domínios RDP e TLDs. Para que isso seja feito de uma forma que seja justa com os proprietários de domínios DNS, um proprietário de domínio DNS deve poder reivindicar um domínio no RDP e provar que é o legítimo proprietário usando oráculos ou cadeias de certificação digital. No caso de colisão entre um domínio de nome da ICANN e um domínio RDP, um sistema de arbitragem pode ser usado para resolver os conflitos. Esse sistema de arbitragem poderia ser implementado por meio de oráculos ou de forma descentralizada. Embora a versão atual do Diretório RIF não forneça uma interface específica para isso, prevemos que o protocolo possa evoluir em versões futuras para permitir essa funcionalidade.

Anonimato

Os usuários podem querer ocultar o endereço de pagamento para o qual seus alias mapeiam. Isso pode ser feito com recursos de criptografia. O proprietário precisaria transferir a chave de decodificação para um usuário, mediante solicitação, por meio de um canal de comunicação fora da rede, possivelmente disponibilizado por um provedor de serviços de comunicações RIF. Além disso, os endereços criptografados podem ser um endereço invisível. Endereços discretos permitem que o pagador obtenha um novo endereço exclusivo para cada pagamento, reduzindo a probabilidade de os pagamentos serem vinculados.

Criando novos domínios de primeiro nível

A RIF Labs atua como um provedor de serviços para RDP. Eles implantaram um registrador inicial para TLD. Dentro desse provedor, a RIF Labs pode, no futuro, permitir que os usuários criem, comprem e vendam seus próprios TLDs.

Considerações Finais

O Protocolo de Diretório RIF foi criado com base no conhecimento coletado ao longo do tempo por diversas organizações que trabalharam com serviços de nomenclaturas e fornece uma interface unificada, simples e compatível com os provedores de serviços de nomes existentes. A interface permite que os usuários adquiram domínios, façam um lance em um leilão de domínio, gerenciem subdomínios e usem tokens de RIF para pagar por um serviço que pode ser fornecido por uma rede descentralizada e sem censura.

Referências

[1] M. Ali, R. Shea, J. Nelson, M J. Freedman, "Blockstack: A New Internet for Decentralized Applications" (2017) https://blockstack.org/whitepaper.pdf
[2] "Namecoin FAQS" https://namecoin.org/docs/faq/
[3] NPM Library https://www.npmjs.com/package/idna-uts46
[4] "Vickrey Auction" https://en.wikipedia.org/wiki/Vickrey_auction