Provendo uma Infraestrutura de Software Fatiada, Isolada e Segura de Funções Virtuais através da Tecnologia de Corrente de Blocos

Gabriel Antonio F. Rebello, Gustavo F. Camilo, Leonardo G. C. Silva, Lucas C. B. Guimarães, Lucas Airam C. de Souza, Igor D. Alvarenga, e Otto Carlos M. B. Duarte

[1]

Grupo de Teleinformática e Automação
Universidade Federal do Rio de Janeiro (UFRJ)

{gabriel,franco,leonardo,chagas,airam,alvarenga,otto}@gta.ufrj.br

Resumo. *As tecnologias de fatiamento da rede (Network Slicing), virtualização de funções de rede (Network Function Virtualization - NFV) e redes definidas por software (Software-Defined Networking - SDN) proveem serviços fim-a-fim ágeis e sob demanda. A identificação de uma função virtual defeituosa torna-se obrigatória, pois serviços alocam recursos em um ambiente distribuído e sem confiança entre os pares composto por múltiplos inquilinos e provedores de serviço concorrentes. Este artigo propõe e desenvolve uma arquitetura baseada em correntes de blocos para prover auditabilidade às operações de orquestração de fatias de rede. Um protótipo de um caso de uso foi desenvolvido e implementado,utilizando a plataforma Hyperledger Fabric na qual cada fatia de rede opera sobre um canal isolado. Os resultados mostram que é possível prover segurança à criação de fatias de rede, mas que a obtenção de consenso e o número de transações requeridas pelas fatias de rede são um grande desafio.*

1. Introdução

As redes móveis de próxima geração fornecem um modelo de conectividade com múltiplos serviços de rede adaptados para atender a demanda de cada segmento de cliente. As redes definidas por *software* (*Software-Defined Networking* - SDN) e a virtualização de funções de rede (*Network Function Virtualization* - NFV) são as principais tecnologias que utilizam a virtualização para fornecer a capacidade de programação da rede. Assim, as tecnologias NFV e SDN criam uma cadeia de funções de rede (*Service Function Chain* - SFC) fim-a-fim [Halpern and Pignataro 2017] para fornecer serviços sob demanda e adaptados a cada aplicação. Apesar de a associação de NFV e SDN fornecer a agilidade e o baixo custo desejados pelas telecomunicações, surgem novos desafios de segurança [Medhat et al. 2017]. Além disso, o impacto de possíveis ataques aumenta porque os ataques aos hospedeiros de funções de rede podem comprometer simultaneamente milhares de usuários [Bhamare et al. 2016]. Portanto, é de grande importância reduzir os possíveis vetores de ataque a funções virtuais de rede (*Virtual Network Functions* - VNF) e fornecer um gerenciamento de configuração seguro e confiável. Garantir o isolamento entre fatias de rede é essencial para evitar ataques comuns em infraestruturas compartilhadas. Além disso, os inquilinos de cada fatia compartilham a mesma infraestrutura de

[1] Este artigo é a versão em português de um artigo em inglês submetido para um congresso internacional.

nuvem, e as cadeias podem envolver funções virtualizadas instanciadas em domínios de provedores concorrentes. O ambiente multi-inquilino e multi-domínio aumenta a possibilidade de ataques dentro da nuvem, ao mesmo tempo que dificulta a responsabilização dos provedores de serviços quando ocorre uma falha. É necessário garantir que a cadeia de serviços, formada por uma cadeia de funções virtuais de rede, seja construída de maneira confiável em um ambiente sem confiança entre os pares. Em um ambiente multi-inquilino formado por provedores concorrentes, é vantajoso para um provedor criar uma ataque para prejudicar um concorrente. Logo, a capacidade de auditoria é obrigatória para identificar uma configuração de VNF defeituosa ou comprometida, e a tecnologia de corrente de blocos fornece as características necessárias de não repúdio e imutabilidade do histórico de configuração de uma função virtual.

Este artigo propõe utilizar a tecnologia de corrente de blocos para registrar, como transações assinadas, todos os comandos que criam, modificam, configuram, migram ou destroem as funções de rede de cada fatia da rede. Portanto, todos os problemas de funcionamento da rede podem ser verificados e um erro pode ser atribuído corretamente a um provedor de serviço em um ambiente de concorrência, multi-inquilino, e sem confiança.

Em trabalhos anteriores, os autores deste artigo avaliaram o desempenho do uso de correntes de blocos na virtualização de funções de rede para proteger comandos de gerenciamento, atualizações e migração de funções virtuais de rede com garantias de anonimidade [Alvarenga et al. 2018, Rebello et al. 2019].

Este artigo foca no uso de correntes de blocos para fatiamento da rede (*network slicing*). Fatias de rede suportam requisitos de serviço para atender redes veiculares tolerantes a atraso, internet das coisas (*Internet of Things* - IoT), indústria 4.0 e serviços críticos como saúde eletrônica (*e-Health*), cidades inteligentes (*smart cities*) e redes elétricas inteligentes (*smart grids*). O cenário extraordinariamente diverso requer diferentes correntes de blocos com características específicas adaptadas ao serviço requerido. Por isso, este artigo propõe atender aos diferentes requisitos de cada fatia de rede através de diferentes categorias de correntes de blocos. A estrutura de dados, o protocolo de consenso e o protocolo de comunicação das corrente de blocos são adaptados a cada funcionalidade de fatia de rede específica. O trabalho apresenta uma arquitetura baseada em correntes de blocos para criar fatias de rede fim-a-fim seguras e adaptadas para cada caso de uso. Um protótipo de caso de uso que segue a arquitetura proposta com diferentes tipos de correntes de blocos é implementado usando a plataforma de código aberto Hyperledger Fabric [Androulaki et al. 2018]. O protótipo implementa dois contratos inteligentes (Hyperledger *chaincode*) com formatos de transação específicos para proteger o gerenciamento de fatias de rede e as operações de configuração de VNFs. Cada fatia de rede é executada em um canal Hyperledger isolado. Os resultados mostram que é possível proteger a construção de fatias de rede, mas que estruturas de dados otimizadas são necessárias para aumentar a taxa de transações necessárias para atender às fatias.

O restante deste artigo está organizado da seguinte forma. A Seção 2 discute os trabalhos relacionados. A Seção 3 apresenta o fatiamento seguro de redes através de corrente de blocos. A Seção 4 detalha a arquitetura proposta. A Seção 5 descreve o protótipo desenvolvido e sua avaliação. Por fim, a Seção 6 conclui o artigo.

2. Trabalhos relacionados

Diversos trabalhos exploram o estado da arte de corrente de blocos aplicada a problemas de redes de comunicação e redes de quinta geração (5G) [Yahiatene and Rachedi 2018, Ortega et al. 2018, Thuemmler et al. 2018, Capossele et al. 2018, Rawat and Alshaikhi 2018, Rosa and Rothenberg 2018, Boudguiga et al. 2017]. Os trabalhos se concentram no uso de corrente de blocos como um repositório de dados incrementais replicados, no qual todas as transações realizadas são assinadas e registradas com criptografia de chaves assimétricas. Yahiatene *et al.* e Ortega *et al.* propõem o uso de corrente de blocos como um mecanismo para fornecer segurança em redes veiculares [Yahiatene and Rachedi 2018, Ortega et al. 2018]. Eles argumentam que a corrente de blocos pode fornecer autenticidade e confiança com baixa latência para permitir redes seguras. Thuemler *et al.* e Capossele *et al.* discutem os requisitos necessários ao 5G para prover saúde eletrônica (*e-Health*) com base em experiências reais [Thuemmler et al. 2018, Capossele et al. 2018]. Os resultados do artigo mostram que a corrente de blocos fornece a privacidade e proteção de dados necessários para proteger registros médicos em um ambiente sem confiança. Rawat *et al.* propõem uma solução baseada em corrente de blocos para redes sem fio virtuais que permite a confiança em provedores de nuvem [Rawat and Alshaikhi 2018]. Rosa e Rothemberg fornecem diretrizes para incorporar os aplicativos distribuídos baseados em corrente de blocos em cenários com múltiplos domínios administrativos [Rosa and Rothenberg 2018]. Boudguiga *et al.* apresentam uma solução para atualizar dispositivos IoT através de informações armazenadas no corrente de blocos [Boudguiga et al. 2017]. A proposta do presente artigo fornece uma taxonomia de fatias baseadas em corrente de blocos que engloba e generaliza todas as aplicações de corrente de blocos como casos de uso em fatias de rede.

Outros trabalhos investigam o problema de vulnerabilidades de segurança em ambientes NFV multi-inquilino e multi-domínio [Pattaranantakul et al. 2018, Paladi et al. 2018]. Eles mostram que a confiança nos provedores de nuvem é incerta e que o comprometimento de uma única VNF no núcleo da rede põe em risco todo o serviço fim-a-fim. Zaowat e Hasan propuseram o SECAP, uma estrutura baseada em corrente de blocos para armazenar com segurança uma árvore de proveniência de aplicativos em nuvem [Zawoad and Hasan 2016]. A estrutura protege os registros das mudanças de estado do aplicativo. Bozic *et al.* propõem uma arquitetura para gerenciar estados de execução de máquinas virtuais usando um sistema baseado em corrente de blocos [Bozic et al. 2017]. O sistema usa uma estrutura de corrente de blocos para registrar as instruções do hipervisor de virtualização do sistema na forma de transações.

Com relação à segurança do fatiamento de rede, Bordel *et al.* propõem uma solução baseada em geradores de números pseudo-aleatórios para fornecer segurança dentro de fatias de rede para dispositivos IoT e estações-base em sistemas 5G [Bordel et al. 2018]. Khettab *et al.* propõem utilizar tecnologias NFV e SDN para proteger fatias de rede de múltiplos domínios instanciando funções de rede de segurança, como *firewalls* e sistemas de detecção de intrusão [Khettab et al. 2018]. Os trabalhos, no entanto, não abordam possíveis comportamentos maliciosos de administradores de rede.

Outros trabalhos propõem o uso de corrente de blocos para prover confiança nos administradores de rede e intermediários responsáveis pelo fatiamento da rede. Valtanen

et al. analisam o uso de corrente de blocos em provedores de fatia de rede para coletar, configurar e alocar recursos em automação industrial [Valtanen et al. 2018]. O artigo aponta as vantagens de usar corrente de blocos em casos de uso do 5G. Backman *et al.* propõem o uso de corrente de blocos para gerenciar recursos de rede 5G virtualizados em um cenário de múltiplos administradores [Backman et al. 2017].

Este artigo propõe uma arquitetura para construção de correntes de blocos que protegem e permitem a auditabilidade da criação de fatias de redes e também a atualização das funções de rede das fatias isoladas. A proposta atende ao ambiente multi-inquilino e multi-domínio sem confiança entre os pares.

3. Fatiamento Seguro de Redes através de Corrente de Blocos

A corrente de blocos é uma estrutura de dados replicada que garante a confiança e o funcionamento adequado de um sistema distribuído sem a necessidade de uma autoridade central comum a todos os participantes. Uma representação típica de uma corrente de blocos é mostrada na Figura 1. Um valor resultante de uma função resumo (*hash*) criptográfica identifica cada bloco. Cada bloco contém as transações realizadas em um determinado intervalo de tempo e o identificador do bloco anterior. Nesta estrutura replicada, cada nó participante do consenso possui uma cópia local da corrente de blocos que contém todas as transações desde o início. Como a cópia atual é a mesma em qualquer nó da rede, a propriedade de não repúdio entre membros é garantida porque todas as transações são assinadas e cada membro usa sua chave pública como identificação.

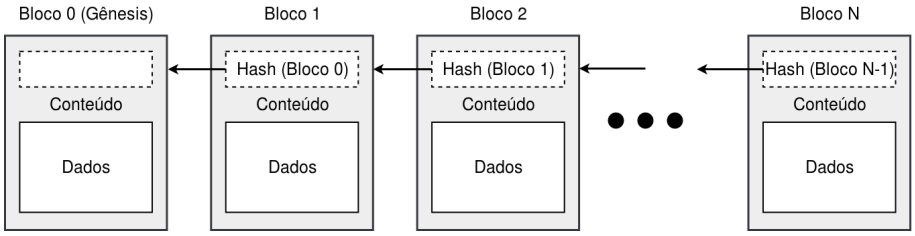

Figura 1. Estrutura de uma corrente de blocos, na qual cada bloco é associado ao bloco anterios e a função resumo criptográfica garante a integridade de cada bloco.

A utilização de corrente de blocos é necessária em ambientes distribuídos em que os participantes não conseguem chegar a um acordo sobre uma autoridade centralizada que governe todos os procedimentos sensíveis de rede. Em centros de dados virtualizados nos quais vários serviços de nuvem são orquestrados, a presença de uma VNF malintencionada em um serviço pode afetar toda a cadeia pela qual os pacotes são roteados sem o conhecimento do administrador da nuvem. Além disso, se um invasor tiver acesso ao orquestrador, o registro de operações pode ser manipulado para ocultar uma ameaça. O uso de corrente de blocos, apesar de envolver uma quantidade maior de processamento como um todo, permite gerenciar e atualizar VNFs de forma distribuída e segura, onde as transações podem ser verificadas localmente por cada nó com a garantia de não repúdio e integridade.

3.1. Modelo de Atacante

Este artigo considera um modelo de atacante de Dolev *et al.*, no qual um atacante pode ler, enviar e descartar uma transação endereçada à corrente de blocos, ou qualquer

pacote da rede [Dolev and Yao 1983]. O atacante pode se conectar passivamente à rede e capturar trocas de mensagens ou injetar, reproduzir, filtrar e trocar informações ativamente. Os ataques podem ter como alvo inquilinos, VNFs, a corrente de blocos em si e a rede.

Ataques à corrente de blocos objetivam impedir que uma transação ou bloco legítimo sejam adicionados à corrente de blocos. Para que um ataque à corrente de blocos seja bem-sucedido, o atacante deve controlar uma parcela significativa da rede para afetar o protocolo de consenso. Um protocolo de consenso tolerante a falhas mitiga esse tipo de ataque. Os ataques que exigem corrupção ou adulteração de transações são impossíveis quando todas as transações incluem seu *hash* assinado correspondente.

Ataques a inquilinos ou VNFs consistem em tentar obter informações de configuração ou personificar o alvo. Os ataques de personificação não são possíveis pois todas as transações enviadas para a corrente de blocos são assinadas por seus emissores. A encriptação de informações confidenciais mitiga ataques que buscam obter informações de configuração, nos quais o atacante precisa obter a chave privada da vítima. Este trabalho não aborda o caso em que um inquilino ou VNF é comprometido através de invasão de terminal ou seqüestro de chave. A arquitetura proposta, no entanto, elimina a necessidade de qualquer serviço de escuta ativo em um VNF, e utiliza terminais em modo somente leitura para mitigar vetores de ataque.Além disso, a arquitetura proposta permite a auditoria de todas as transações passadas. Portanto, se um invasor tentar modificar a corrente de blocos usando pares de chaves roubados, a tentativa será registrada. Após a descoberta de um incidente, o inquilino ou provedor pode facilmente substituir os pares de chaves roubados, restabelecendo a segurança e evitando mais danos.

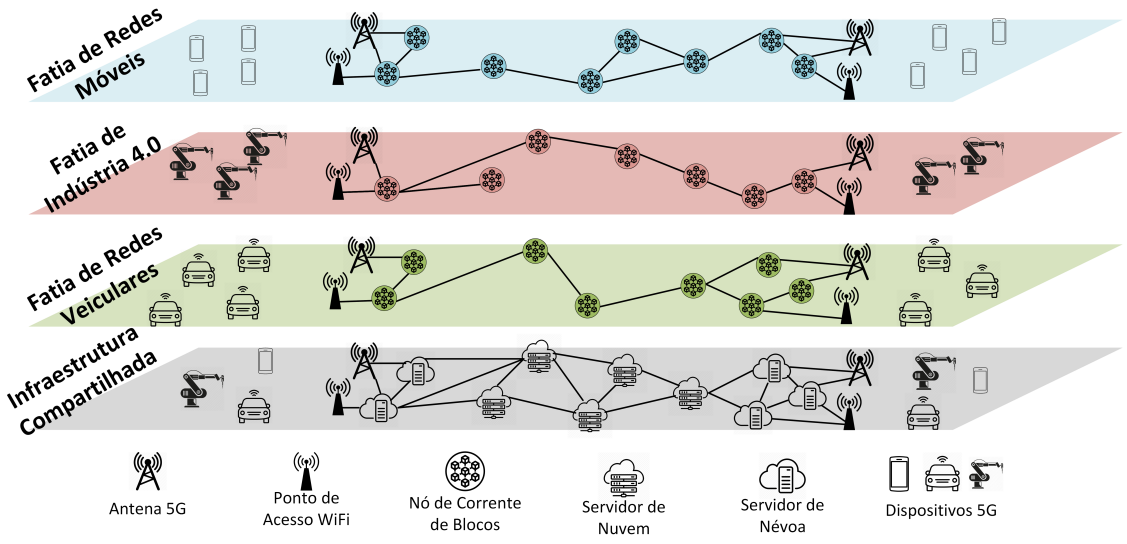

Figura 2. Fatias de rede isoladas através de corrente de blocos em uma infraestrutura física compartilhada. Cada fatia de rede é adaptada às necessidades de um caso de uso.

Ataques à rede representam a tentativa de isolar um único inquilino, um grupo de inquilinos ou um grupo de VNFs da rede, impedindo assim que a rede execute transações ou leia conteúdo da corrente de blocos. Esta categoria de ataque contempla ataques

clássicos de rede, que podem ser mitigados através do estabelecimento de caminhos redundantes entre a corrente de blocos e VNFs ou inquilinos. Este trabalho assume uma rede pública redundante, como a Internet, que interconecta todos os participantes. A suposição dificulta o isolamento de uma única entidade se o invasor não estiver em sua rede adjacente. A mitigação completa de ataques de rede está fora do escopo deste trabalho. A arquitetura proposta foca nos ataques à corrente de blocos e transações antecipadas. No entanto, ao eliminar os serviços de escuta das VNFs, a arquitetura elimina os ataques de negação de serviço da camada de aplicação, que são uma ameaça comum em ambientes de nuvem compartilhados.

4. A Arquitetura Proposta

Diferentes casos de uso exigem funcionalidades específicas e incorrem em diferentes características de corrente de blocos para cada fatia de rede. Em vez de tentar abordar todos os casos de uso, este trabalho propõe classes de corrente de blocos que atendem a muitos casos de uso. Assim, uma simples taxonomia de fatias baseadas em corrente de blocos composta de quatro categorias de fatias pode abordar uma infinidade de possíveis casos:

- **Fatias de administrador único.** Essa categoria trata casos de uso nos quais a fatia de rede inteira é administrada por uma única entidade. Neste caso, as correntes de blocos atuam apenas como um banco de dados distribuído, no qual as decisões da rede são controladas por uma autoridade central, como em redes privadas.
- **Fatias multi-domínio tolerantes a falhas desastrosas**. Essa categoria trata casos de uso nos quais nós individuais na rede podem falhar, mas a rede está livre de comportamentos mal-intencionados. Essa categoria fornece alta eficiência para ambientes descentralizados de vários domínios que garantem a segurança da rede por meio de políticas baseadas em contrato. Este cenário é ideal para redes de até dezenas de administradores. Exemplos incluem comunicação horizontal e concordância entre os controladores SDN para implementar um serviço. Este tipo de fatia é baseia-se em correntes de blocos federadas e utiliza os protocolos RAFT e PAXOS.
- **Fatias multi-domínio tolerantes a falhas bizantinas.** Essa categoria usa protocolos de consenso tolerantes a falhas bizantinas (*Byzantine Fault Tolerance* - BFT) para proteger a rede contra comportamentos maliciosos. Os protocolos BFT fornecem eficiência razoavelmente alta para ambientes com até algumas centenas de nós identificados. Casos de uso incluem ambientes NFV em vários domínios e com vários inquilinos que implementam serviços fim-a-fim. Esta categoria baseia-se em correntes de blocos federadas robustas a ataques de conluio [Alvarenga et al. 2018, Sousa et al. 2017].
- **Fatias públicas totalmente descentralizadas.** Esse tipo de fatia de rede fornece escalabilidade de milhares de nós, sacrificando a eficiência e a taxa de transferência. Essas fatias dependem de protocolos baseados em provas que determinam um estado global por meio de consenso probabilístico0. As fatias de rede baseadas em provas fornecem alta escalabilidade, pois não precisam conhecer todos os nós da rede para obter consenso. Portanto, esse tipo de fatia é mais adequado para redes públicas com muitos dispositivos, como fatias de IoT.

Este trabalho propõe uma arquitetura na qual cada categoria fatia de rede baseada em corrente de blocos aborda um ou mais casos de uso do 5G, criando redes isoladas com segurança e confiança. A figura 2 descreve um cenário que usa corrente de blocos para três fatias de rede: uma fatia de rede móvel, uma fatia de indústria 4.0 e uma fatia de redes veiculares. Para garantir a justiça no protocolo de consenso, cada centro de dados pode hospedar no máximo um nó de corrente de blocos por fatia de rede. Os nós de corrente de blocos em uma fatia são invisíveis para qualquer entidade fora da fatia. O trabalho propõe fornecer a capacidade de auditoria de criação e gerenciamento de fatias, registrando todas as operações de orquestração da VNF em uma corrente de blocos de gerenciamento. A corrente de blocos de gerenciamento registra as operações de orquestração que criam ou modificam uma fatia de rede. Toda operação é assinada pelo cliente que solicitou a modificação. Os participantes da corrente de blocos devem validar cada operação por consenso e fornecer uma prova assinada irrefutável de que a transação foi aceita antes que as operações sejam realizadas. A solicitação assinada combinada com o registro permanente fornecido pela corrente de blocos garante que um comportamento malicioso seja rastreável. Assim, a proposta de corrente de blocos gerencial garante a procedência, a prestação de contas e a rastreabilidade das falhas em um ambiente NFV multi-inquilino e multi-domínio. Além disso, o trabalho propõe o uso de contratos inteligentes para fornecer automação e transparência em ambientes sem confiança distribuídos, em vez de confiar em um determinado nó para receber e processar transações. As propriedades de automação e transparência dos contratos inteligentes são ideais para criar fatias de rede fim-a-fim seguras que envolvem VNFs em vários domínios concorrentes, pois garantem que todos os nós da rede obedeçam ao mesmo conjunto de regras e que o código executado seja visível para qualquer nó participante.

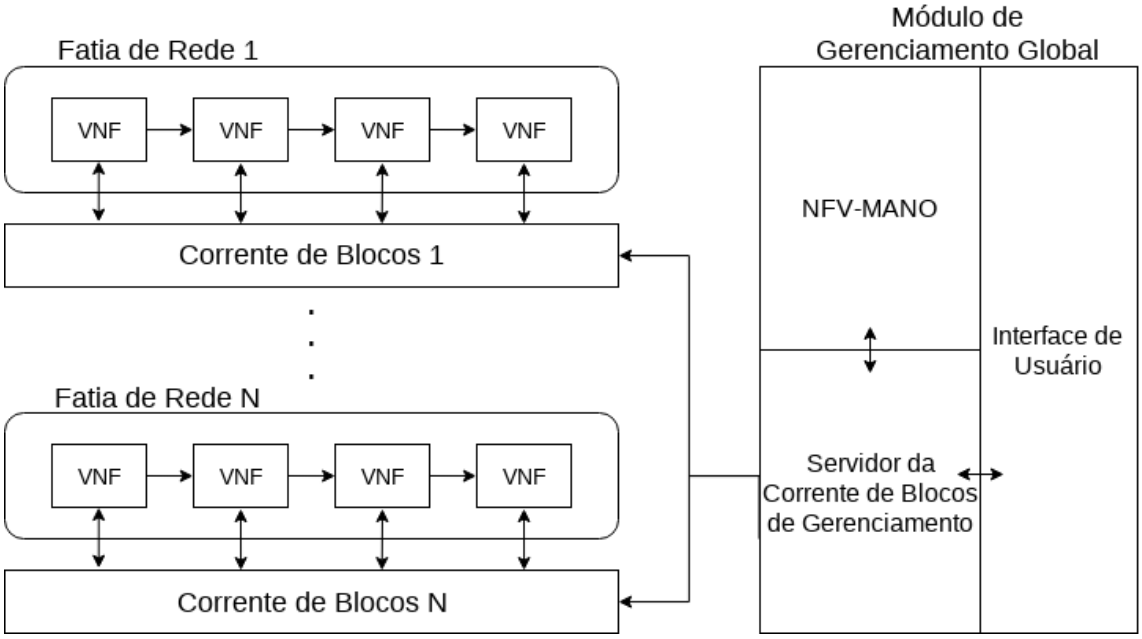

Figura 3. A arquitetura proposta baseada em corrente de blocos para fatiamento de rede. O usuário interage com o módulo de gerenciamento global para criar fatias de rede seguras. Cada VNF em uma fatia de rede é conectada a uma corrente de blocos responsável por registrar solicitações de configuração e informações relevantes, conforme especificado pelo usuário.

A arquitetura proposta, representada na figura 3, compreende quatro componentes principais: uma interface de usuário, o módulo de gerenciamento e orquestração NFV (NFV-MANO), um módulo de servidor de criação de corrente de blocos e um módulo de gerenciamento de corrente de blocos. Os módulos compõem o módulo de gerenciamento global, que é responsável por conectar o cliente aos serviços oferecidos. Nesta arquitetura, o cliente interage com o módulo de gerenciamento global por meio de uma interface de usuário para criar/modificar uma fatia de rede segura ou para solicitar informações de fatia, como configurações de VNFs e cadeias de funções. O cliente especifica as características da fatia, como VNFs desejadas e restrições de posicionamento, e a categoria de corrente de blocos correspondente. O módulo de interface do usuário converte as especificações em operações de criação de fatias/corrente de blocos e as envia como transações assinadas para aprovação na corrente de blocos de gerenciamento. Depois que as transações são aprovadas, o módulo NFV-MANO e o módulo de criação de corrente de blocos verificam a corrente de blocos de gerenciamento para obter operações pendentes. Os módulos executam as operações para criar novas fatias seguras e emitem transações de resposta assinadas para a corrente de blocos de gerenciamento. O cliente pode então interagir com o módulo de interface do usuário para verificar se a fatia segura solicitada foi criada com sucesso.

5. O Protótipo baseado no Hyperledger Fabric

Este trabalho desenvolve um protótipo da arquitetura proposta que usa a plataforma Hyperledger Fabric [Androulaki et al. 2018]. O Hyperledger Fabric é uma plataforma de código aberto para implementar correntes de blocos entre organizações em ambientes sem confiança. Cada organização mantém uma réplica da corrente de blocos e pode acrescentar blocos através de um protocolo de consenso. A arquitetura modular do Hyperledger Fabric permite aos administradores de rede projetar sistemas baseados em sub-redes isoladas que suportam correntes de blocos específicas. As correntes de blocos no Hyperledger Fabric suportam protocolos de consenso plugáveis que proveem a personalização proposta para atender a casos de uso e modelos de confiança específicos. Os desenvolvedores das correntes de blocos podem configurar permissões de leitura e escrita para criar redes privadas, federadas ou públicas. O Hyperledger Fabric fornece um serviço de identidade e associação de membros que gerencia os identificadores dos usuários e provedores, e autentica todos os participantes na rede para criar redes permissionadas. Nós e canais são os conceitos chave mais importantes de uma rede baseada em corrente de blocos permissionada do Hyperledger Fabric.

Os nós representam as entidades que participam do processamento de uma transação ou mantêm uma cópia da corrente de blocos. O Hyperledger Fabric provê três tipos de nós: clientes, pares (*peers*) e ordenadores. Um cliente representa um usuário que envia transações aos pares para validação e assinatura, e transmite propostas de transação assinadas para o serviço de ordenação. Os pares são um elemento fundamental da rede porque executam propostas de transação, validam transações e mantém os registros na corrente de blocos. Os pares também instanciam contratos inteligentes e armazenam o estado global, uma representação sucinta do estado mais recente da corrente de blocos. Os nós ordenadores formam coletivamente o serviço de ordenação, que é responsável por estabelecer a ordem total e o empacotamento de todas as transações em um bloco usando um protocolo de consenso. Os ordenadores não participam da execução da transação nem

validam transações. O desacoplamento das funcionalidades de ordenação e validação aumenta a eficiência da rede, pois permite o processamento paralelo de cada fase. A Figura 4 descreve um exemplo de uma corrente de blocos permissionada com quatro organizações no Hyperledger Fabric. Cada organização recebe transações de clientes e as retransmite para os ordenadores após a validação pelos pares. Cada organização possui um único ordenador, garantindo a justiça no protocolo de consenso.

Caminhos de mensagens diferentes, chamados canais, isolam as correntes de blocos. Um canal Hyperledger Fabric é uma sub-rede de comunicação privada e isolada entre um subconjunto de nós da rede específicos para fornecer privacidade e confidencialidade às transações. Todos os dados transmitidos em um canal, incluindo transações, contratos inteligentes, configurações de associação e informações de canal, são invisíveis e inacessíveis a qualquer entidade externa a um canal. A funcionalidade do canal é ideal para a proposta de oferecer correntes de blocos personalizadas para diferentes serviços de rede, pois permite que os administradores dos canais estabeleçam diferentes formatos de bloco e transação, além do protocolo de consenso, para cada canal. Portanto, podemos usar canais para oferecer fatias de rede protegidas por correntes de blocos configuradas de forma específica. Formatos de transação são definidos em contratos inteligentes, chamados de *chaincode* no Hyperledger Fabric, escritos em Go, Node.js ou linguagem Java.

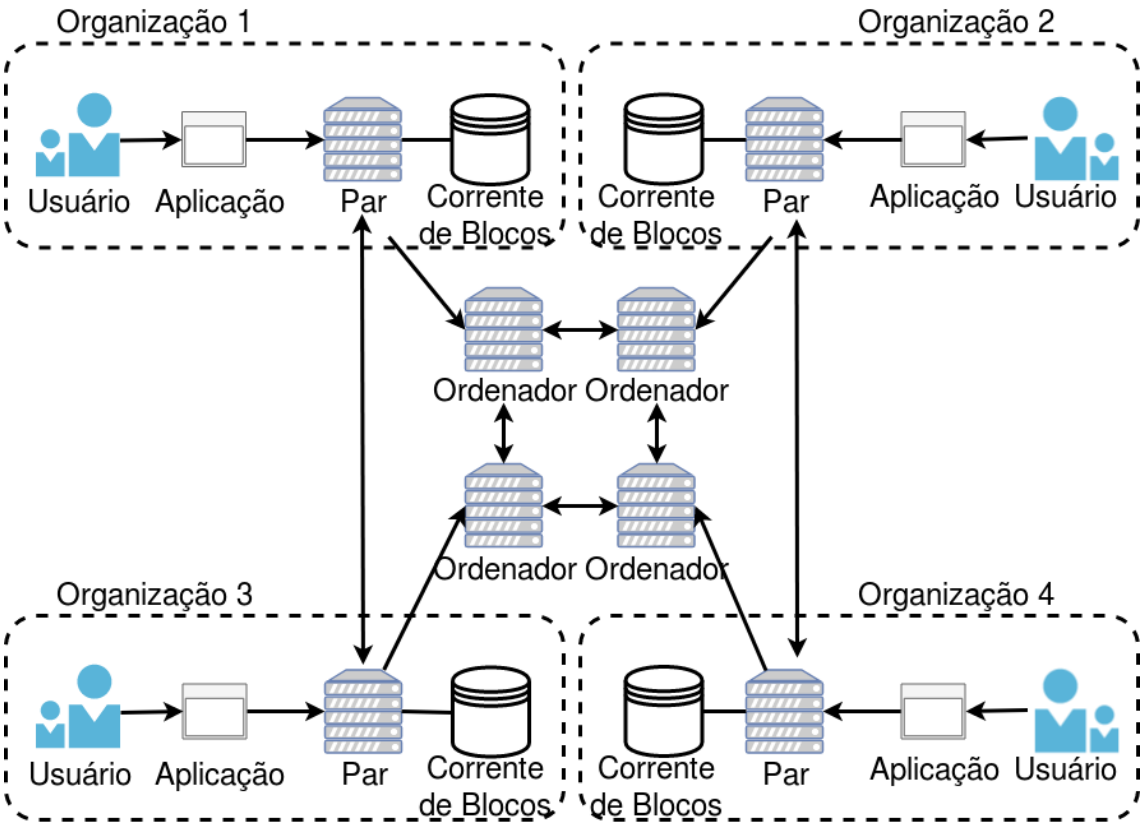

Figura 4. Uma corrente de blocos permissionada do Hyperledger Fabric. Usuários de cada organização usam aplicações para emitir transações as retransmitem para os ordenadores para o ordenamento global e a adição em um bloco. Depois de um bloco ser proposto e aceito pelos ordenadores através do consenso, os pares atualizam a corrente de blocos e o estado global.

5.1. Avaliação do Protótipo

O trabalho implementa duas correntes de blocos que representam, respectivamente, a corrente de blocos de gerenciamento e um exemplo de corrente de blocos para proteger uma fatia de rede. O exemplo de corrente de blocos protege a atualização de configuração da VNF e a migração em uma fatia de rede por registrar permanentemente configurações na corrente de blocos. Um consórcio com três organizações controla as duas implementações de corrente de blocos. Cada uma das três organizações controla um nó que possui direitos administrativos sobre a rede. Todas as três organizações recebem transações de um número variável de nós clientes na rede de corrente de blocos. Um computador Intel Core i7-7700 CPU 3.60GHz com 64 GB RAM cria todos os nós como contêineres Docker. Contêineres constroem múltiplos ambientes isolados de espaços de usuários que permitem a otimização de recursos computacionais da rede de corrente de blocos.

O trabalho implementa dois contratos inteligentes[1] escritos em Go, que são executados em todos os nós da rede [Alvarenga et al. 2018, Rebello et al. 2019]. O primeiro contrato inteligente, parcialmente descrito na Lista 1, gerencia autonomamente o gerenciamento e a orquestração de VNF através de transações de instrução e resposta. Quando um cliente solicita uma fatia, o servidor da corrente de blocos de gerenciamento de emite uma transação de instrução com o comando de instrução. O contrato coloca a transação de instrução em uma fila de transações pendentes de instrução. O código notifica o módulo NFV-MANO, que executa a instrução pendente e envia a saída do comando para o servidor da corrente de blocos de gerenciamento. O módulo NFV-MANO emite uma transação de resposta que inclui um campo contendo o identificador da transação de instrução correspondente. Isso fornece a rastreabilidade de cada transação executada na corrente de blocos e, portanto, a responsabilização de entidades maliciosas.

```
struct instructionTransaction
{
    command                 string
    transactionType         string
    transactionName         string
    issuer                  string
}
initialize queue
initInstruction (instruction <command,name,issuer>)
{
    if instruction is not unique or instruction is not well-formatted:
        return error
    putState (instruction.name, instruction)
    put (transactionID, queue)
    notify orchestrator
    return success
}
```

Listing 1. Parte do pseudo-código do contrato inteligente que emite transações de instrução. O campo de comando contém a operação de orquestração a ser executada pelo módulo NFV-MANO. O contrato estabelece uma fila de instruções pendentes a serem processadas pelo orquestrador NFV.

[1]O código completo está disponível em https://github.com/gta-ufrj/hpsr-smart-contracts

O segundo contrato inteligente, descrito na Lista 2, define e atualiza uma configuração de uma VNF. Um cliente emite uma transação para a corrente de blocos conectada a cada VNF em uma fatia de rede. A transação contém um texto descritivo com a configuração associada no campo de descrição, assim como os dados de configuração no campo de configuração.

```
struct configurationTransaction
{
    configurationIdentifier string
    versionIdentifier       string
    description             string
    configuration           string
    transactionType         string
    transactionName         string
    issuer                  string
}
initConfiguration (configuration <description,configuration,name,issuer
    >){
    if configuration is not unique or configuration is not well-formed:
        return error
    putState (configuration.name, configuration)
    return success
}
```

Listing 2. Pseudo-código parcial para emitir transações de configuração. O campo configurationIdentifier contêm um identificador único para a configuração.

O protótipo usa os certificados de autoridade (*Certificate Authorities* - CA) do Hyperledger Fabric para criar e gerenciar certificados digitais em cada nó da rede de corrente de blocos. Certificados digitais garantem auditabilidade e que somente nós certificados e autorizados podem participar da rede de corrente de blocos.

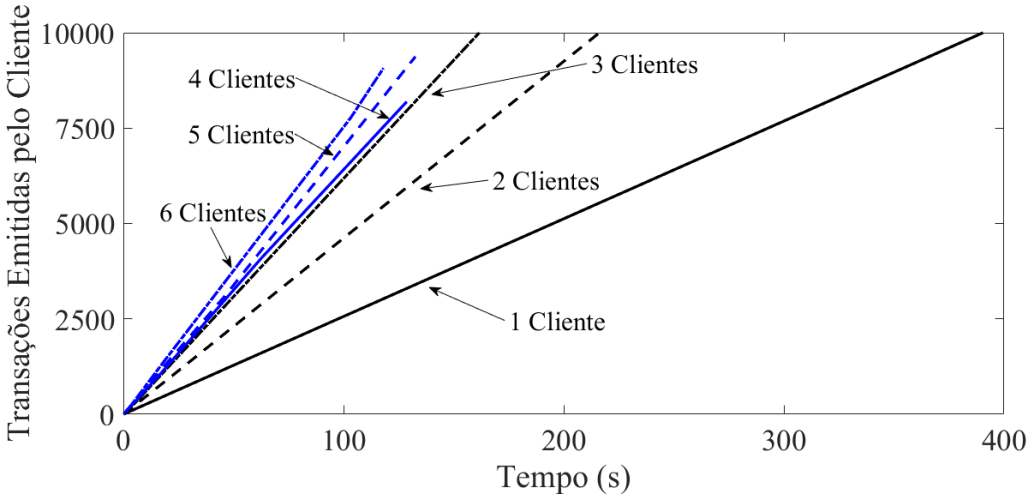

Figura 5. Tempo total decorrido para processar as transações na corrente de blocos à medida que o número de transações emitidas e o número de clientes aumentam. Os resultados mostram que a vazão aumenta com o número de clientes que emitem transações.

O protótipo implementa cada nó da rede do Hyperledger Fabric como um

contêiner em um único computador e envia transações simultaneamente. O trabalho avalia a vazão de transação enviando um número crescente de transações e medindo o tempo decorrido que os clientes precisam para propor todas as transações para a rede baseada em corrente de blocos. A Figura 5 apresenta o resultado da avaliação da taxa de transação do cliente. A taxa de transação na fatia de rede atinge um valor de pico de 71,31 transações por segundo no lado do cliente.

O trabalho ajusta as configurações de criação de bloco de acordo com avaliações de desempenho realizadas anteriormente no Hyperledger Fabric [Thakkar et al. 2018, Gorenflo et al. 2019]. O trabalho define o tamanho preferido do bloco sem cabeçalho em 99 MB, o número máximo de transações em um bloco em 10 e o tempo limite para inicializar uma rodada de consenso em dois segundos. Se alguma das condições for atendida, o nó ordenador inicia uma nova rodada de consenso e envia a proposta de novo bloco. Depois de alcançar o consenso, os nós acrescentam o novo bloco à sua cópia da corrente de blocos.

6. Conclusão

A tecnologia de fatia de redes fornece serviços fim-a-fim customizados através encadeando funções virtuais de rede entre infraestruturas de nuvens concorrentes em um ambiente distribuído multi-inquilino e multi-domínio sem confiança entre os pares. A alta programabilidade resultante proveniente da virtualização da rede expõe todo o tráfego a um maior número de ameaças. Portanto, é obrigatório precisamente definir e localizar falhas e usos indevidos para identificar agentes maliciosos que podem comprometer simultaneamente o bom comportamento e a qualidade de serviço de milhares de usuários.

O trabalho propõe uma arquitetura baseada em corrente de blocos para proteger fatias de redes customizadas. A multiplicidade de características diferentes exigidas por cada fatia impõe o uso de várias correntes de blocos personalizadas com diferentes números de participantes, estruturas de dados, tipo de transações, taxa de transferência de transação, tipo de consenso, tipo de redes, etc.

O trabalho implementa um protótipo de prova de conceito usando duas correntes de blocos que garantem proteger a criação de fatia e a atualização e migração de funções virtualizadas de rede. O trabalho usa a plataforma Hyperledger Fabric que facilita a criação de várias correntes de blocos em diferentes canais. Para trabalhos futuros, usaremos estruturas de dados otimizadas para melhorar a taxa de transação e usar um protocolo de consenso diferente.

7. Agradecimentos

Este trabalho foi financiado pela CAPES, CNPq, FAPERJ e FAPESP (2015/24514-9, 2015/24485-9 e 2014/50937-1).

Referências

Alvarenga, I. D., Rebello, G. A. F., and Duarte, O. C. M. B. (2018). Securing management, configuration, and migration of virtual network functions using blockchain. In *IEEE/IFIP NOMS*.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, page 30. ACM.

Backman, J., Yrjölä, S., Valtanen, K., and Mämmelä, O. (2017). Blockchain network slice broker in 5G: Slice leasing in factory of the future use case. In *Internet of Things Business Models, Users, and Networks*, pages 1–8.

Bhamare, D., Jain, R., Samaka, M., and Erbad, A. (2016). A survey on service function chaining. *Journal of Network and Computer Applications*, 75:138–155.

Bordel, B., Orúe, A. B., Alcarria, R., and Sánchez-De-Rivera, D. (2018). An intra-slice security solution for emerging 5G networks based on pseudo-random number generators. *IEEE Access*, 6:16149–16164.

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., and Sirdey, R. (2017). Towards better availability and accountability for IoT updates by means of a blockchain. In *IEEE EuroS&PW*, pages 50–58.

Bozic, N., Pujolle, G., and Secci, S. (2017). Securing virtual machine orchestration with blockchains. In *CSNet'17*.

Capossele, A., Gaglione, A., Nati, M., Conti, M., Lazzeretti, R., and Missier, P. (2018). Leveraging blockchain to enable smart-health applications. In *IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI)*, pages 1–6.

Dolev, D. and Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on information theory*, 29(2):198–208.

Gorenflo, C., Lee, S., Golab, L., and Keshav, S. (2019). Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second. https://arxiv.org/pdf/1901.00910.pdf.

Halpern, J. and Pignataro, C. (2017). Service Function Chaining (SFC) architecture. RFC7665. `http://www.rfc-editor.org/rfc/rfc7665.txt`. Accessed Mar. 14, 2019.

Khettab, Y., Bagaa, M., Dutra, D. L. C., Taleb, T., and Toumi, N. (2018). Virtual security as a service for 5G verticals. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6.

Medhat, A. M., Taleb, T., Elmangoush, A., Carella, G. A., Covaci, S., and Magedanz, T. (2017). Service function chaining in next generation networks: State of the art and research challenges. *IEEE Comm. Mag.*, 55(2):216–223.

Ortega, V., Bouchmal, F., and Monserrat, J. F. (2018). Trusted 5G vehicular networks: Blockchains and content-centric networking. *IEEE Vehicular Technology Magazine*, 13(2):121–127.

Paladi, N., Michalas, A., and Hai-Van, D. (2018). Towards secure cloud orchestration for multi-cloud deployments. In *EuroSys-CrossCloud*.

Pattaranantakul, M., He, R., Song, Q., Zhang, Z., and Meddahi, A. (2018). NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures. *IEEE Communications Surveys & Tutorials*.

Rawat, D. B. and Alshaikhi, A. (2018). Leveraging distributed blockchain-based scheme for wireless network virtualization with security and QoS constraints. In *International Conference on Computing, Networking and Communications (ICNC)*, pages 332–336.

Rebello, G. A. F., Alvarenga, I. D., Sanz, I. J., and Duarte, O. C. M. B. (2019). BSec-NFVO: A blockchain-based security for network function virtualization orchestration. In *IEEE International Conference on Communications (ICC)*. To be published.

Rosa, R. and Rothenberg, C. E. (2018). Blockchain-based decentralized applications for multiple administrative domain networking. *IEEE Communications Standards Magazine*, 2(3):29–37.

Sousa, J., Bessani, A., and Vukolić, M. (2017). A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. *arXiv preprint arXiv:1709.06921*.

Thakkar, P., Nathan, S., and Viswanathan, B. (2018). Performance benchmarking and optimizing hyperledger fabric blockchain platform. In *IEEE MASCOTS*, pages 264–276.

Thuemmler, C., Rolffs, C., Bollmann, A., Hindricks, G., and Buchanan, W. (2018). Requirements for 5G based telemetric cardiac monitoring. In *14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 1–4.

Valtanen, K., Backman, J., and Yrjölä, S. (2018). Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case. In *IEEE WCNCW'18*, pages 185–190.

Yahiatene, Y. and Rachedi, A. (2018). Towards a blockchain and software-defined vehicular networks approaches to secure vehicular social network. In *IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 1–7.

Zawoad, S. and Hasan, R. (2016). SECAP: Towards securing application provenance in the cloud. In *2016 IEEE 9th International Conference on Cloud Computing*, pages 900–903.