UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA
Autorizada pelo Decreto Federal nº 77.496 de 27/04/76
Recredenciamento pelo Decreto nº17.228 de 25/11/2016
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
COORDENAÇÃO DE INICIAÇÃO CIENTÍFICA

XXIV SEMINÁRIO DE INICIAÇÃO CIENTÍFICA DA UEFS
SEMANA NACIONAL DE CIÊNCIA E TECNOLOGIA - 2020

IMPLEMENTAÇÃO DE AMBIENTE DE EMULAÇÃO EM NÉVOA COM SUPORTE A BLOCKCHAIN

Eduardo Marques dos Santos[1]; Antonio Augusto Teixeira Ribeiro Coutinho[2];
1. Estagiário PEVIC, Graduando em Engenharia de Computação, Universidade Estadual de Feira de Santana, e-mail: esantos@ecomp.uefs.br
2. Orientador, Departamento de Tecnologia (DTEC), Universidade Estadual de Feira de Santana, e-mail: acoutinho@uefs.br

PALAVRAS-CHAVE: Blockchain; Computação em Névoa; Emulação.

INTRODUÇÃO

Um modelo centralizado baseado em nuvem tornou-se a abordagem padrão para a Internet das Coisas (*Internet of Things*, IoT) (GUBBI et al., 2013). Devido às limitações dessa arquitetura, propostas recentes estão propondo mudanças em direção a modelos e arquiteturas descentralizadas. A Computação em Névoa (*fog computing*) (BONOMI et al., 2012) tem trazido os recursos de computação em nuvem para perto das fontes de dados com o intuito de superar problemas relacionados a arquitetura IoT.

O desenvolvimento de aplicações em IoT acoplada a uma arquitetura em névoa exige uma infraestrutura escalável e que forneça segurança, confiabilidade e tolerância a falhas. O emprego de plataformas em névoa de testes (*testbed*) torna a validação dessas aplicações mais simples e diminui o custo de desenvolvimento de soluções [4]. A tecnologia Blockchain (GREVE et al., 2018) vem sendo aplicada em IoT por oferecer confiabilidade e segurança nas transações entre entidades desconhecidas.

Entretanto, integrar Blockchain com as atuais soluções IoT em uma arquitetura em névoa não é uma tarefa trivial. A Blockchain possui alto custo computacional [5] com contratos inteligentes, criptografia, mineração, reputação, etc. Assim, no mundo real, as funcionalidades da Blockchain são gerenciadas em uma rede separada denominada *rede de transação*, e as aplicações que utilizam os recursos da Blockchain são executadas fora da Blockchain (*off-chain*) em uma rede lateral (*sidechain*). Isso facilita a oferta da Blockchain como um serviço em nuvem para aplicações remotas.

Este trabalho apresenta a elaboração de uma arquitetura baseada em névoa que fornece suporte à tecnologia Blockchain e que permite a validação de aplicações IoT em larga escala para o desenvolvimento de pesquisas inovadoras neste domínio.

MATERIAL E MÉTODOS

Para a elaboração deste projeto, foi necessário um levantamento bibliográfico buscando compreender o funcionamento dos modelos e ferramentas que possibilitassem a implementação de uma arquitetura Blockchain em névoa. Foram estudados o ambiente

de emulação em névoa Fogbed (COUITNHO et al., 2018), além de conceitos sobre *middlewares* Blockchain para o desenvolvimento de aplicações.

Identificou-se que o Hyperledger Fabric[1] (HL Fabric) seria a melhor opção disponível, devido a esta ferramenta ser customizável, colaborativa e possuir código aberto. O ambiente Fogbed foi usado para possibilitar a escalabilidade do projeto, permitindo a implementação de nós em névoa utilizando técnicas de conteinerização, baseadas no ambiente Docker[2] na criação de *testbeds* virtuais.

Após os estudos das ferramentas, foi realizada a integração do HL Fabric com o Fogbed. Para isso, foi implementado um protocolo baseado em Blockchain para permitir transações seguras entre instâncias de névoa virtuais na rede. Neste processo, foram levantados requisitos funcionais dos componentes do HL Fabric, além da adaptação dos componentes do Fogbed necessários para oferecer suporte a Blockchain.

Na realização das etapas do projeto, foram utilizadas uma rede de computadores física e estações de trabalho do Laboratório de Redes e Sistemas Distribuídos (LARSID) da Universidade Estadual de Feira de Santana (UEFS), além de recursos do estagiário e do orientador na etapa final do trabalho, devido ao isolamento do laboratório pela pandemia de COVID-19 no Estado da Bahia.

DISCUSSÃO E ANÁLISE DOS RESULTADOS

A arquitetura proposta apresenta duas redes sobrepostas em uma mesma estrutura hierárquica. Na primeira rede, instanciada com o Fogbed, são executados os serviços e as aplicações em névoa. Essa rede é dividida em subdomínios de IoT, onde cada subdomínio representa uma aplicação IoT diferente ou *sidechain*. A segunda rede é uma rede P2P de transações, criada usando o HL Fabric, onde sua finalidade é fornecer confiança, baseada na prova de identidades para validação das transações da rede da aplicação. Esta arquitetura em duas redes foi adotada por representar a forma convencional da oferta dos serviços Blockchain em uma infraestrutura IoT real.

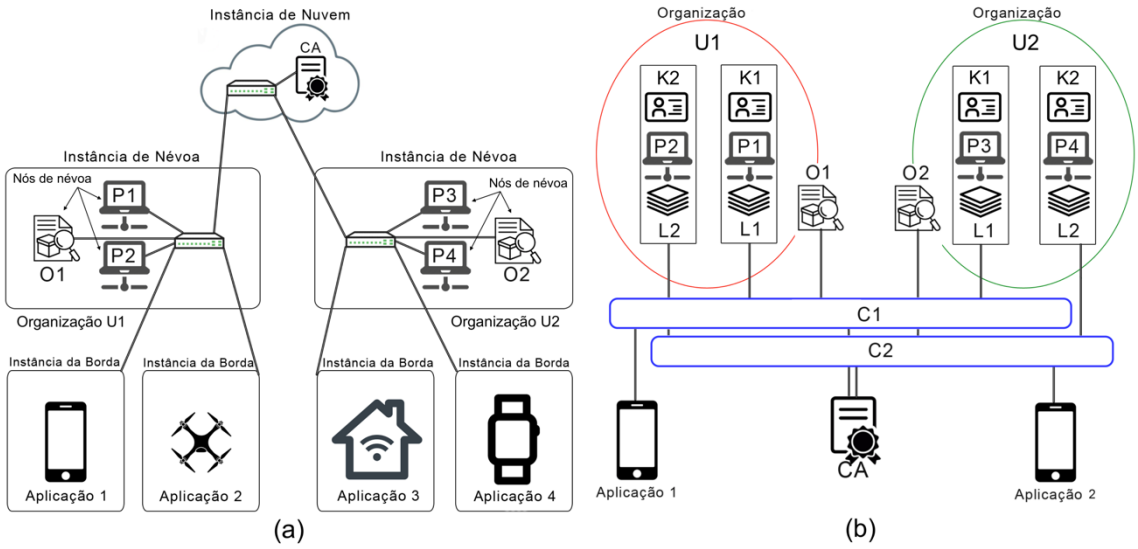

Figura 1. (a) Arquitetura da rede de aplicação em névoa.

[1] https://www.hyperledger. org/projects/fabric
[2] https://www.docker.com

(b) Rede de transação em termos da topologia do Hyperledger Fabric.

O *Membership Service Provider* (MSP) (HYPERLEDGER, 2019) é o componente do HL Fabric que oferece uma abstração das operações de associação. Na arquitetura proposta, o MSP foi implementado através de uma infraestrutura de chave pública (*Public Key Infrastructure*, PKI), configurando autoridades certificadoras (*Certificate Authority*, CA) que emitem certificados para componentes e usuários.

A Figura 1(a) apresenta a arquitetura da rede de transação através da implementação de duas unidades organizacionais `U1` e `U2` em instâncias de névoa. A autoridade de certificação *`Fabric-CA`* é mantida em nuvem, mas sua autoridade é estendida a cada sidechain da primeira rede seguindo uma arquitetura em névoa. O MSP identifica quais CAs (raiz e intermediárias) são aceitas para definir seus membros, e transforma uma identidade em uma função, identificando privilégios que um ator (cliente, aplicação, administrador, etc.) possui na unidade organizacional.

Na arquitetura proposta foi utilizado o consenso PBFT (GREVE et al., 2018), que pode oferecer uma taxa de transação apropriada aos serviços da IoT. Além da CA, MSP, e o consenso PBFT, existem componentes fundamentais do HYPERLEDGER (2019) que foram empregados como: *ledger*, *peers*, *chaincodes*, *orderer* e *channel*.

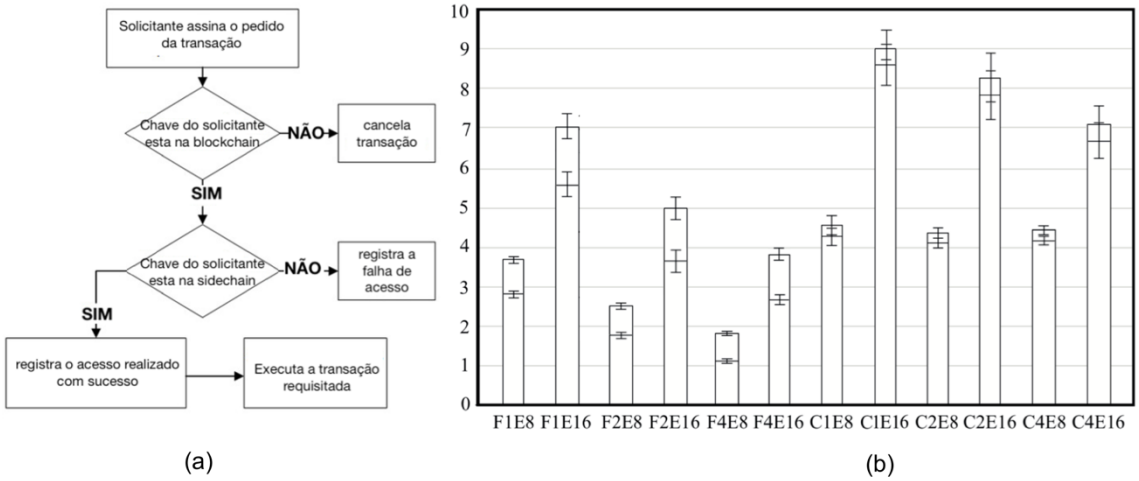

Figura 2. (a) Protocolo genérico de autenticação implementado com Blockchain. (b) Cenários de emulação usando a estratégia em névoa e nuvem, onde cada cenário foi avaliado com e sem o protocolo de autenticação baseado em Blockchain proposto.

A Figura 1(b) mostra a rede de transação representada em termos da topologia do Hyperledger Fabric. No estudo de caso, os *peer* na rede de transações mantém um par de chaves `K` públicas assimétricas para validação de transações ou permissões na sua unidade organizacional. Cada organização representa ou é mantida em uma instância de névoa diferente, onde os *peers* `P1` e `P2` estão localizados na organização `U1`, e os *peers* `P3` e `P4` estão localizados na organização `U2`. O *orderer* `O1` é responsável pela ordenação e composição de transações no *channel* `C1`, e o *orderer* `O2` é responsável pela ordenação e composição de transações no *channel* `C2`. O *channel* `C1` mantém uma cópia do *ledger* `L1`, sendo responsável pelo endereçamento e comunicação entre os *peers* `P1` e `P3`. O *channel* `C2` mantém uma cópia do *ledger* `L2`, sendo responsável pelo endereçamento e comunicação entre os *peers* `P2` e `P4`.

A Figura 2 (a) apresenta o protocolo genérico de autenticação implementado na rede de transação e executado antes da aplicação de saúde executar uma consulta (*query*) para obter o escore com a lista dos usuários. Antes do médico submeter uma query, ele assina o pedido com sua chave privada, mas se a chave pública relacionada não está na Blockchain, o médico não tem acesso a rede da aplicação ou consórcio de saúde e a consulta é cancelada. Depois, o pedido de acesso prossegue na sidechain específica à organização ou plano de saúde dos usuários: se a chave do médico também for autorizada para sidechain, o acesso para instalação da query no dispositivo e ou execução da query em nós de névoa é autorizada.

A Figura 2 (b) apresenta a latência do serviço em névoa da rede de aplicação para concluir uma consulta *top-k*, executada com e sem o protocolo de autenticação baseado em Blockchain. No gráfico, é possível notar que o tempo de latência do serviço *top-k* diminui usando uma estratégia em névoa. Isso porque, na estratégia em nuvem, todos os dados são sempre enviados a um centro de dados remoto na Internet. É possível notar que o tempo de atraso relativo ao protocolo de autenticação permanece quase constante, e vai se tornando mais significativo ao tempo total do serviço. Isso acontece porque o protocolo de autenticação fornecido como um serviço pela rede de transação não tira proveito de uma estratégia de névoa, sofrendo mais com a latência da rede. Acreditamos então que uma arquitetura Blockchain que explore de forma eficiente os recursos em névoa pode melhorar de forma significativa o tempo total de latência do serviço.

CONSIDERAÇÕES FINAIS

Este trabalho obteve como resultado principal a elaboração de uma arquitetura em névoa que oferece suporte à tecnologia Blockchain em ambiente Fogbed. Esta arquitetura foi projetada visando a prototipagem e testes de aplicações em névoa, executadas em ambientes virtuais ou em nuvem, e utilizando como plataforma o *framework* HL Fabric. Como trabalhos futuros, espera-se o desenvolvimento de um *testbed* escalável, que possibilite a prototipagem e integração de tecnologias reais de névoa e Blockchain para ambientes de produção.

REFERÊNCIAS

BONOMI, F. et al. 2012. Fog computing and its role in the internet of things, Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. ACM, pp. 13–16.

GUBBI, J. et al. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions, Future generation computer systems 29.7: 1645-1660.

COUTINHO, A. et al. 2018. Fogbed: A rapid-prototyping emulation environment for fog computing, in Communications Workshops (ICC Workshops), 2018 IEEE International Conference, pp. 1-7.

GREVE, F. et al. 2018. Blockchain e a Revolução do Consenso sob Demanda. Livro de Minicursos do SBRC, pp. 1-52.