Estudo de um Modelo de Camadas para uso de Ferramentas de Gerenciamento de Redes *Blockchain*

André Ribeiro Vieira[1], **Wilson S. Melo Jr.**[2], **Claudio M. de Farias**[1]

[1] Universidade Federal do Rio de Janeiro (UFRJ)
Programa de Pós-Graduação em Informática (PPGI) – Rio de Janeiro, RJ – Brasil

[2]Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro)
Duque de Caxias, RJ – Brasil

arvieira@labnet.nce.ufrj.br, wsjunior@inmetro.gov.br

claudiofarias@nce.ufrj.br

Resumo. *Redes blockchain são redes dinâmicas, onde nodos e aplicações precisam ser adicionados e removidos sem comprometer sua disponibilidade. Neste novo ambiente tecnológico, diversas ferramentas são desenvolvidas e disponibilizadas, seja para proporcionar uma infraestrutura flexível, seja para facilitar seu gerenciamento e administração. Novas aplicações para redes blockchain são propostas a todo o tempo, assim como mudanças de paradigma podem ocorrer a cada nova configuração. Este trabalho propõe um modelo de camadas para abstração do uso de ferramentas de gerenciamento de uma rede blockchain, de modo a prover maior facilidade no entendimento e planejamento da rede, bem como maior eficiência na criação de novas aplicações e produtos.*

1. Introdução

Um *blockchain* pode ser definido como uma estrutura de armazenamento de dados decentralizada e somente de escrita, organizada em uma cadeia de blocos ligados criptograficamente, que são replicados e mantidos por meio de consenso entre um conjunto de nodos que definem uma rede *blockchain* [Christidis and Devetsikiotis 2016, Zheng et al. 2017]. Uma das principais vantagens associadas a uma rede *blockchain* é o fato de permitir que as diferentes organizações que controlam diferentes subconjuntos de nós implementem aplicações seguras por meio de contratos inteligentes, sem necessariamente confiarem umas nas outras [Christidis and Devetsikiotis 2016]. Tal característica tem impulsionado o crescente uso de *blockchains* em diferentes aplicações nos mais variados segmentos de negócios e áreas de conhecimento [Zheng et al. 2017].

Uma vez que o gerenciamento de uma rede *blockchain* é totalmente decentralizado (i.e., não existe a figura de um controle central) [Christidis and Devetsikiotis 2016, Sousa et al. 2018]. O comportamento da rede é dinâmico, e a execução de tarefas de manutenção pode se tornar um problema à medida em que esta cresce. Nodos são adicionados e removidos de forma independente por administradores em cada organização. Com ações não coordenadas entre as múltiplas organizações, a execução pode se tornar complexa para os administradores. De igual modo, as múltiplas aplicações suportadas por uma rede *blockchain* precisam ser gerenciadas pelos respectivos provedores de solução. Basicamente, as aplicações são implementadas como contratos inteligentes, e estes por sua vez precisam ser adicionados, atualizados ou desativados, conforme o

ciclo de vida da aplicação. Em razão disso, o gerenciamento de uma rede *blockchain* depende de ferramentas específicas que sejam adequadas à uma estrutura decentralizada [Androulaki et al. 2018], variando conforme a plataforma adotada. No entanto, existe uma escassez de informação associada ao correto uso de tais ferramentas. Em muitos casos, essas ferramentas ainda se encontram em fase de desenvolvimento ou projeto. Ao mesmo tempo, a literatura não traz uma metodologia voltada ao uso de ferramentas de gestão de forma integrada em um ambiente de rede decentralizado.

Assim como em problemas complexos, a divisão da gerência e a administração de uma rede *blockchain* em partes menores é de grande importância. Observa-se que essa abstração já é utilizada em outras áreas do conhecimento, como no caso de protocolos de redes organizados em camadas (e.g., modelos OSI e TCP/IP), onde camadas superiores utilizam serviços das inferiores, assim como as inferiores fornecem serviços prontos para as superiores. Essa estratégia evita que ferramentas e protocolos tenham funcionalidades sobrepostas. De igual modo, cada ferramenta desenvolvida terá uma aplicação específica e maior eficiência.

Neste trabalho, é proposto um novo modelo em camadas para estudo, segmentação e compartimentação de tecnologias referentes às ferramentas de gerenciamento de uma rede *blockchain*. O modelo é constituído por quatro camadas independentes, que modificam o grau de abstração e o foco das atividades de gerenciamento envolvidos. Uma quinta camada auxiliar é proposta como meio de suporte para operações do dia a dia da administração das redes. As principais contribuições são: (i) a apresentação de um estudo sistemático referente a modelos descritos na literatura que podem ser usados para organizar ferramentas de gerenciamento de uma rede *blockchain*, permitindo comparações; e (ii) a proposta de um novo modelo em camadas para o uso otimizado de ferramentas de gerenciamento de redes *blockchain*. Uma vez que o gerenciamento de uma rede *blockchain* é caracteristicamente decentralizado, o modelo proposto é útil para orientar administradores de redes de diferentes organizações.

2. Trabalhos Relacionados

Diversos trabalhos referentes a redes *blockchain* tem sido desenvolvidos no intuito de simplificar o problema de gestão da rede. Nosso trabalho se atém à análise em camadas de tecnologias relacionadas a construção e gerenciamento de redes *blockchain*, propondo a separação de ferramentas para um melhor entendimento, assim evitando retrabalhos.

Dentre os trabalhos na área, pode-se citar [Dhillon et al. 2017], [Singhal et al. 2018] e [Lu 2019], relacionados a estudos em camadas em redes *blockchain*. Em [Dhillon et al. 2017], é descrito detalhadamente o projeto *Hyperlegdger*, que é composto por sete subprojetos menores: *Sawtooth*, *Iroha*, *Fabric*, *Burrow*, *Indy*, *Composer*, *Explorer* e *Cello*. Nesse contexto, pode-se identificar que as ferramentas que compõem o *Hyperledger* inicialmente sugerem uma arquitetura modular que induz a um modelo de camadas. No entanto, não é exposto um modelo propriamente dito para o estudo. O trabalho de [Singhal et al. 2018] propõe um modelo de estudo de redes *blockchain* em camadas de aplicação, execução, semântica, propagação e consenso. No entanto, o foco da divisão é diferente do proposto neste trabalho. O trabalho de [Lu 2019] propõe outro modelo de camadas para a divisão das funcionalidades na rede *blockchain*. Contendo camadas de dados, redes, consensos, contratos, serviços e aplicações. Este

modelo dialoga com o modelo de [Singhal et al. 2018], embora possua um foco estrutural na realização das segmentações.

Os trabalhos de [Silva et al. 2019] e [Wan et al. 2018] possuem exemplos de uso de alguns níveis de abstração correlatos camadas. Por exemplo, [Silva et al. 2019] propõe uma forma de gerir recursos e ativos de uma empresa, usando uma base ontológica em rede *blockchain*. Neste trabalho, os autores não desejam interagir diretamente com a infraestrutura necessária. Como foco é a aplicação, o autor propõe utilizar a ferramenta *Hyperledger Composer*, que trata diretamente da lógica do negócio. Pode-se assim associar este trabalho às camadas de aplicação propostas em [Singhal et al. 2018] e [Lu 2019].

Uma outra abordagem de segmentação em camadas vem do trabalho de [Wan et al. 2018], que propõe uma mudança de paradigma em redes *blockchain*. Em tal mudança, redes *blockchain* passam a ser tratadas como um serviço, e comercializadas por empresas detentoras de grandes recursos de *hardware* (e.g.,*Clouds*). Desse modo, são citados exemplos como o *Microsoft Azure*, *Corda*, *Amazon AWS* e *IBM Bluemix*.

Já em [Rane and Dixit 2019] é proposto uma forma de guardar registro de *logs* de servidores em uma *Cloud* usando *blockchains*, no intuito de possibilitar análises forenses. Ao apresentar sua solução, os autores utilizam diretamente o *Hyperledger Fabric*. Desse modo, apesar do foco do trabalho ser uma aplicação (i.e., análise forense), este acaba por se utilizar uma ferramenta demasiadamente detalhada para o nível de abstração demandado.

O presente trabalho propõe um modelo de segmentação em camadas de uma rede *blockchain* de uma forma ainda não tratada pelos trabalhos mencionados. Nossa abordagem introduz uma organização semelhante ao paradigma de orientação a objetos (OO), no qual apenas os detalhes próprios do problema a ser resolvido devem ser tratados em cada nível. Deste modo, se o foco de uma tarefa é na aplicação executada pela rede, o administrador deve se ater apenas aos detalhes intrínsecos desse nível de abstração, sem se preocupar com níveis mais baixos (e.g., implementação de servidores ou especificação com protocolos).

3. Um Novo Modelo de Camadas para Redes *Blockchain*

Nossa proposta consiste de um modelo de divisão e organização do conhecimento e das ferramentas envolvendo redes *blockchain*. O surgimento de redes *blockchain*, alavancado pelo apelo de criptomoedas como o *Bitcoin* [Nakamoto 2008], e com a velocidade de disponibilização de ferramentas relacionadas ao tema, introduz a necessidade de organização e segmentação da tecnologia, tornando um modelo de camadas uma demanda real.

Nosso modelo desenvolve quatro camadas sobrepostas e mais uma quinta camada auxiliar para o processo. Conforme demonstrado na Figura 1, tal esquema prevê que a camada compartimentalize um dado conhecimento, de modo que o uso de uma camada mais externa abstrai os detalhes técnicos contidos nas camadas mais internas. Caso haja a sobreposição de funcionalidades em ferramentas que se propõem a objetivos de diferentes camadas, tem-se uma perda de eficiência. Logo, tanto o estudo como o desenvolvimento de soluções para redes *blockchains* pode ser segmentado nas camadas descritas a seguir.

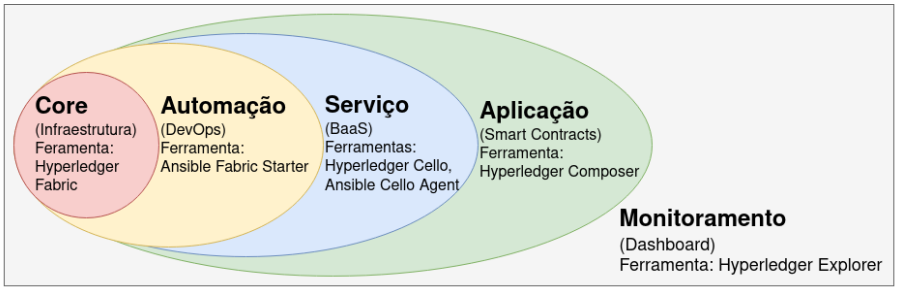

Figura 1. Modelo de estudo em camadas para redes *blockchain*.

3.1. Camada Núcleo *CORE*

A primeira camada é denominada *Core* e consiste no nível mais interno de abstração e mais próximo ao código realmente implementado na rede *blockchain*. Nesta camada, são tratados os conceitos de programação e do funcionamento propriamente dito da rede, assim como a implementação da infraestrutura de suporte. Pode-se dizer que essa camada inclui toda a configuração de rede, assim como instalação de programas, customização de serviços, definições de segurança e demais pontos intrínsecos da estrutura.

Neste ponto, elaborar grandes redes *blockchain* se torna uma tarefa difícil, uma vez que todos os detalhes do funcionamento e de configurações devem ser tratados pelos administradores da rede. O trabalho nesse nível de abstração é específico para desenvolvimento de características peculiares da rede, próprias para a solução em questão. Outro objetivo de se trabalhar nesta camada é o desenvolvimento de novas tecnologias relacionadas às redes, nas quais se deseja customizar o consenso, algoritmos de rede ou segurança, protocolos, uso de certificados digitais, entre outros pontos. Como exemplo, podemos citar o uso do *framework* denominado *Hyperledger Fabric* [1].

3.2. Camada *AUTOMAÇÃO*

A segunda camada é denominada *Automação*. Este nível de abstração, tem por objetivo evitar que os administradores necessitem realizar trabalhos específicos de desenvolvimento de cada ponto da rede *blockchain*. Desse modo, eles dispõem ferramentas para automatizar processos de instalação, configuração e entrega de pontos da infraestrutura em um modo *out of the box*, de modo que o administrador pode criar e gerir redes maiores e mais complexas.

Nesse momento, ambientes envolvendo diversas organizações, múltiplos nós, assim como configurações específicas e diferenciadas são viáveis. Como exemplo deste nível de abstração, dentre as tantas ferramentas disponíveis no mercado, se pode citar uma customização denominada *Ansible Fabric Starter*[2], construída pela empresa *Altoros* usando a ferramenta *Ansible* da empresa *Red Hat*. Nesta camada, a infraestrutura da rede *blockchain* se confunde com a programação e a entrega do produto se torna mais rápida e eficiente.

[1] https://www.hyperledger.org/use/fabric
[2] https://github.com/Altoros/Ansible-Fabric-Starter

3.3. Camada *SERVIÇO*

Na camada seguinte, chamada *Serviço*, a abstração aumenta de modo que o interesse do administrador de construir e desenvolver sua rede muda para a ideia de trabalhar como um serviço. Nesse momento, redes *blockchain* passam a ser um serviço, denominado *Blockchain as a Service*. O serviço em questão consiste em, havendo um *datacenter* poderoso o suficiente, estabelecer dentro dele, de maneira virtual, tantas redes *blockchain* quanto possíveis. Com isso, caso um cliente necessite de nodos para uma rede *blockchain*, basta que ele compre ou alugue de outra empresa especialista nisto. Nesse momento, o foco do administrador muda da forma como vai desenvolver sua infraestrutura para a melhor forma de entregar um serviço. Este ponto pode ser exemplificado pelas ferramentas *Hyperledger Cello*[3].

3.4. Camada *APLICAÇÃO*

Esse nível de abstração tem como foco as regras de negócio e as aplicações suportadas pela rede. Por exemplo, no caso da criptomoeda *BitCoin*, essa camada gerencia o modo como a própria moeda funciona, englobando regras de negócio para garantir a validade da aplicação. Isso inclui o gerenciamento de transações, a forma como uma transação é feita, como funciona cada uma das carteiras, entre outros pontos específicos dessa criptomoeda. Logo, esta camada tem como foco principal os *smart contracts*, ou os contratos inteligentes que serão executados pela rede *blockchain*. Como exemplo de ferramenta nesta camada, dentre tantas outras como o *Ethereum*[4] com a linguagem *Solidity*, se pode relacionar o *Hyperledger Composer*[5], que tem como foco a construção da lógica do negócio em uma rede que utiliza o *Hyperledger Fabric*.

3.5. Camada Auxiliar de *MONITORAMENTO*

Por último, não se tratando de uma camada propriamente dita, mas sim como uma base auxiliar para suportar todas as outras camadas, tem-se o *Monitoramento*. Tal abstração tem como objetivo extrair informações de todas as quatro camadas anteriores, provendo ao administrador uma forma de visualizar o funcionamento de sua rede, nos mais diversos níveis de abstração. Nesse nível, nenhuma estrutura é modificada em si, mas todas as aplicações implementadas utilizando a abstração de camadas podem ser monitoradas de modo a exibir um quadro de informações sintético para o administrador do sistema, agindo como um nível auxiliar de abstração. Como exemplo desta camada auxiliar, tem-se a ferramenta *Hyperledger Explorer*[6], que coleta diversas informações nas camadas citadas e provê um *dashboard* para os administradores da rede.

4. Conclusão

Neste trabalho, foi proposto um modelo para estudo e organização de ferramentas de implementação, configuração e gerência de redes *blockchain*. Este modelo é baseado na segmentação por camadas, sendo que em cada camada tem-se um nível de abstração diferente, de modo a facilitar tarefas menores e possibilitar o foco no que realmente é o objetivo dos administradores. É proposta também uma camada auxiliar de Monitoramento,

[3]https://www.hyperledger.org/use/cello
[4]https://ethereum.org/pt-br/
[5]https://www.hyperledger.org/use/composer
[6]https://www.hyperledger.org/use/explorer

que apesar de não incluir ferramentas para modificar a rede em si, gera informações de seu funcionamento, o que possibilita uma melhor visualização da estrutura da rede *blockchain*, constituindo um último nível de gerência. Desse modo, o método de estudo proposto demonstra simplificação e uma melhoria no entendimento acerca do gerenciamento de redes *blockchain*. Os próximos passos desse trabalho incluem um aprofundamento em cada camada do modelo proposto. Nesta busca, diferentes ferramentas podem ser propostas e analisadas, diante da constante evolução tecnológica presente nos dias de hoje. Do mesmo modo, o estudo de cada camada citada neste trabalho pode ser aprofundado de forma específica, conforme o objetivo em questão.

Referências

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S. W., and Yellick, J. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, Porto, Portugal.

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4:2292–2303.

Dhillon, V., Metcalf, D., and Hooper, M. (2017). *The Hyperledger Project*, pages 139–149. Apress, Berkeley, CA.

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration*.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at https://bitcoin.org/bitcoin.pdf.

Rane, S. and Dixit, A. (2019). Blockslaas: Blockchain assisted secure logging-as-a-service for cloud forensics. In Nandi, S., Jinwala, D., Singh, V., Laxmi, V., Gaur, M. S., and Faruki, P., editors, *Security and Privacy*, pages 77–88, Singapore. Springer Singapore.

Silva, D., Guerreiro, S., and Sousa, P. (2019). Decentralized enforcement of business process control using blockchain. In Aveiro, D., Guizzardi, G., Guerreiro, S., and Guédria, W., editors, *Advances in Enterprise Engineering XII*, pages 69–87, Cham. Springer International Publishing.

Singhal, B., Dhameja, G., and Panda, P. S. (2018). *Introduction to Blockchain*, pages 1–29. Apress, Berkeley, CA.

Sousa, J., Bessani, A., and Vukolić, M. (2018). A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. In *48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*.

Wan, Z., Cai, M., Yang, J., and Lin, X. (2018). A novel blockchain as a service paradigm. In Chen, S., Wang, H., and Zhang, L.-J., editors, *Blockchain – ICBC 2018*, pages 267–273, Cham. Springer International Publishing.

Zheng, Z., Xie, S., Dai, H.-N., and Wang, H. (2017). Blockchain Challenges and Opportunities : A Survey. *International Journal of Web and Grid Services*, pages 1–24.