Estudo de Oráculos em Neo para Auditoria de Dados de Robótica Móvel em Locais Remotos

Mateus Nazário Coelho[1], **Vitor Nazário Coelho**[2], **Igor Machado Coelho**[3], **Bruno Nazário Coelho**[1]

[1]Programa de Pós-Graduação em Instrumentação, Controle e Automação de Processos de Mineração – PROFICAM
Universidade Federal de Ouro Preto – Ouro Preto – MG – Brasil

mateusnazarioc@gmail.com, brunonazario@ufop.edu.br

[2]OptBlocks Consultoria Ltda
Ouro Preto – MG – Brasil

vncoelho@gmail.com

[3]Instituto de Computação
Universidade Federal Fluminense – Niterói – RJ – Brasil

imcoelho@ic.uff.br

Abstract. *The use of mobile robotics for data collection in remote environments has become increasingly common in the industry, driven by advancements in access to open software packages and low-cost hardware. The integration of these devices with blockchain still poses challenges, especially in scenarios with high latency and non-determinism of transactions in decentralized peer-to-peer networks. As a case study, we propose a scenario involving a government agency focused on auditing data from mobile robots, using smart contracts and oracles from the Neo Blockchain. Experiments with remote sensing in a Starlink satellite network explore strengths and limitations of the proposed audit system.*

Resumo. *O uso de robótica móvel para coleta de dados em ambientes remotos tem se tornado cada vez mais comum na indústria, seja pelos avanços no acesso a pacotes de software aberto e hardware de baixo custo. A integração desses dispositivos com blockchain ainda se mostra desafiadora, especialmente em cenários de maior latência e não determinismo das transações em redes par-a-par descentralizadas. Como estudo de caso, propomos um cenário envolvendo uma agência governamental com foco em auditoria de dados de robôs móveis, utilizando contratos inteligentes e oráculos da Neo Blockchain. Experimentos com sensoriamento remoto em uma rede de satélites Starlink exploram vantagens e limitações do sistema de auditoria desenvolvido.*

1. Introdução

Robôs têm se tornado mais acessíveis para o uso cotidiano, todavia, devido à complexidade de componentes e ferramentas, em geral, requer-se mão de obra especializada na sua construção e utilização [Murphy 2014]. Desta forma, o desenvolvimento de uma plataforma robótica de alto nível, que desempenhe diversas tarefas, requer conhecimentos

em diversas áreas, tanto para o desenvolvimento do hardware embarcado quanto para o software [Azpurua et al. 2019]. O último serve como camada de integração de *drivers*, sensores e também para a disponibilização de uma interface comunicável com o usuário. Nessa linha, o *Robot Operating System* (ROS) [Quigley et al. 2009] é um meta sistema operacional e um framework de código aberto desenvolvido com o intuito de diminuir o tempo dedicado para reimplementar e integrar as diversas camadas de software presentes em uma plataforma robótica.

Blockchain é uma tecnologia de registro descentralizado originalmente projetada para que transações financeiras eletrônicas do Bitcoin fossem registradas permanentemente como uma cadeia de blocos, resolvendo o problema de gasto duplo [Nakamoto 2008]. A evolução da tecnologia trouxe a possibilidade de programação Turing-completa, o que permite maior grau de programabilidade do que originalmente previsto pelo protocolo do Bitcoin, como os Contratos Inteligentes da Neo Blockchain [Hongfei and Zhang 2018]. Algumas diferenças importantes entre blockchains são: mecanismos distintos para consenso; diferentes maneiras de programar contratos inteligentes; e recursos integrados de acesso à Web 2.0 [Berners-Lee 2010], como Oráculos.

De acordo com [Elommal and Manita 2022], a tecnologia da blockchain é capaz de trazer grandes mudanças para processos de auditoria, pois fornece uma nova forma à maneira que um auditor acessa e analisa os dados. Assim, propomos neste trabalho um estudo de caso considerando uma agência governamental com foco em auditoria de dados de robôs móveis, através da tecnologia blockchain e seu recurso de oráculos em contratos inteligentes. O sistema de oráculos da Neo Blockchain exige que os dados externos obtidos sejam determinísticos, para que exista consenso na integridade desses dados. Por isso, projetamos uma arquitetura com blockchain e *Application Programming Interface* (API) em *Representational State Transfer* (REST) para agregar dados de sensores, atrelando cada valor ao *timestamp* associado à medição. O objetivo é prover um sistema de log seguro com dados auditados dentro do contrato inteligente, no formato *append-only*, considerando possíveis atrasos e perdas de mensagens por parte da rede e dos sensores envolvidos, a fim de integrar de forma robusta as tecnologias ROS, Neo e Starlink.

2. Conceitos Básicos

O ROS é um meta sistema operacional de código aberto para robôs, possuindo serviços esperados de um sistema operacional comum, como: abstrações de hardware; controle de dispositivos de baixo nível; passagem de mensagens entre processos; e manutenção de pacotes. Ele provê as informações coletadas entre os sensores através do padrão *publish-subscribe*, em tópicos, serviços e ações. A estrutura de uma topologia simples do ROS se comunica através do sistema de tópicos. Os Nós[1] são como processos que realizam tarefas dentro do ecossistema ROS, identificados na imagem como o */talker*, *rosbridge_websocket* e *rosapi*. Tópicos[2] transmitem informação entre nós através de um tipo de mensagem definido.

Já sobre os contratos inteligentes (do inglês, *smart contracts*), eles permitem a programação de códigos confiáveis *trustless*, sendo implantados em redes descentralizadas, especialmente para situações em que as partes não se confiam. O Neo permite

[1]ROS Nodes: `http://wiki.ros.org/Nodes`
[2]ROS Topics: `http://wiki.ros.org/Topics`

programação de contratos em linguagens de programação populares como C#, Java, Go e Python, sendo compiladas para a plataforma de código de máquina NeoVM[3].

Por fim, a tecnologia de Oráculos permite o acesso direto à Web 2.0, mesmo dentro de contratos inteligentes a partir da web descentralizada (também conhecida popularmente como Web 3). Esse recurso é tido como um *building block* fundamental das tecnologias blockchain modernas, permitindo pontes entre diversas tecnologias da Web 2.0, e também blockchains diferentes da web descentralizada. Entretanto, programar com o uso de oráculos exige grande maturidade e conhecimento da arquitetura blockchain, tendo um alto custo computacional (e também monetário), por isso deve ser usado apenas em situações que é fundamental a obtenção de informações verificáveis do "mundo exterior" para o "mundo da blockchain". O contrato inteligente com oráculos do Neo opera em duas fases, sendo necessária a invocação de uma função de acesso exterior (incluindo protocolos populares como *https*) e registro de uma função de *callback*, cuja execução apenas acontece quando o dado requisitado pelo oráculo já se encontra verificado. A documentação do Neo Oracle Service pode ser encontrada no website do Neo[4].

3. Trabalhos relacionados

Em [Alsamhi and Lee 2021], um framework conceitual utilizando blockchain para um sistema multi-robôs é proposto, com o intuito de combate a pandemia da COVID-19. A blockchain, nesta abordagem apresentada por eles, permitiria que robôs homogêneos e heterogêneos combatam a COVID-19 de forma colaborativa e eficiente, compartilhando informações de forma autônoma e acessando as informações uns dos outros. Já em [Ferrer et al. 2022], é proposto a utilização de blockchain como ferramenta de comunicação de forma a garantir que, se um robô bizantino, que age de forma maliciosa, tentar modificar o conteúdo de um bloco na rede, a consequência será uma mudança na hash de forma que este bloco perderá sua conexão com os anteriores. Por fim, em [Zhang et al. 2022], é proposto um framework envolvendo o ROS e a rede do Ethereum, onde os usuários não precisam se preocupar com a implementação da transação ou algoritmos de criptografia, focando apenas em inserir o nome dos tópicos que queiram transmitir dados. Os testes foram rodados em uma rede Ethereum privada, com 3 nós e o robô conectado diretamente ao nó mestre do ROS. Conforme descrito por [Afanasyev et al. 2019], estudos recentes mostram que a blockchain desempenha um grande papel no desenvolvimento de sistemas e aplicações robóticas, de forma que possam conduzir de forma efetiva suas tarefas utilizando técnicas de consenso, registro de dados e alocação de tarefas de forma descentralizada.

4. Sistema Proposto e Experimentos

O caso de uso estudado envolve a interligação e uso das seguintes tecnologias e componentes (uma uma visão geral do sistema é apresentada na Figura 1): ROS para o sensor e disponibilização dos dados; Node.js e Express.js para a API REST; Mempool não-determinística em P2P para recepção de transações na blockchain; Contratos inteligentes e oráculos com Consenso; Interações do usuário via transações criptográficas.

[3]`https://github.com/neo-project/neo-vm/`

[4]`https://docs.neo.org/docs/en-us/advanced/oracle.html`

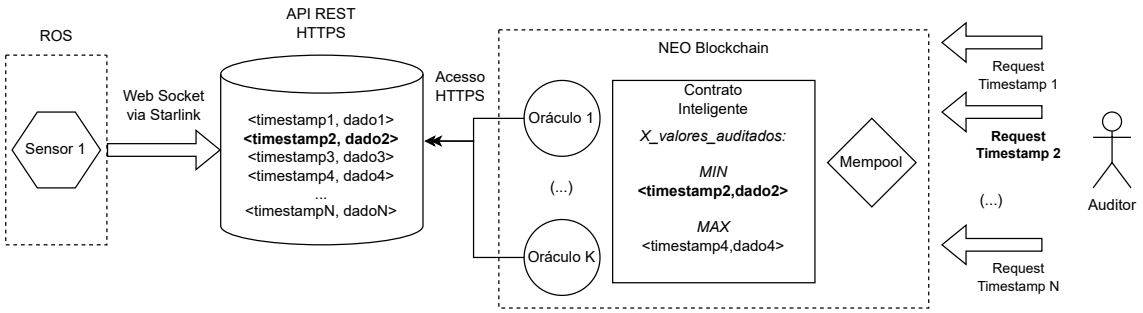

Figura 1. Fluxograma do sistema desenvolvido no trabalho

De forma a ressaltar a utilização de robôs em áreas remotas e isoladas, os módulos dos sensores e disponibilização dos dados do robôs são feitos de forma remota, utilizando uma conexão via satélite. Para tal, o núcleo do ROS cria uma conexão Web Socket [Fette and Melnikov 2011], da qual um backend em nodejs é utilizado para criação de APIs REST [Balachandar 2017] através de um domínio certificado https (requerimento necessário dos oráculos da Neo Blockchain). Desta forma, a API disponibilizará os N últimos valores do sensor (e respectivas *timestamp*), para fins de acesso preciso e determinístico pelos nós de oráculos na blockchain.

A rede experimental do Neo está disponível na web, seja por uma combinação de nós espalhados pelo globo terrestre ou em redes privadas que simulam uma rede descentralizada. Em primeiro lugar, o contrato inteligente (Seção 4.1) armazenado na blockchain é acionado por uma entidade validadora (pode ser visto na Figura 1 como as N requisições do Auditor). Essa transação chegam aos nós de consenso, que acionam o comitê dos K oráculos para que este acesse a url solicitada através do contrato. Ao entrar na mempool, o consenso da blockchain irá incluir um subconjunto de transações disponíveis em um bloco, não havendo garantia de ordem, nem mesmo garantia de entrega, devido à natureza não-determinística da mempool. Assim, as informações são consolidadas e salvas na base de dados da blockchain, invocando a execução do contrato inteligente para fins de auditoria de cada dado recebido. O contrato deve lidar com a assincronia inerente das transações enviadas (que chegam fora de ordem ou falham), assumindo possíveis ataques de Sybil (ou DDoS), processando no contrato apenas dados com timestamp mais recentes.

4.1. Experimentos com o Contrato Inteligente desenvolvido

O código desenvolvido para ser utilizado na Blockchain do Neo, assim como todos os outros módulos do sistema, está disponível no GitHub[5]. Os gráficos na Figura 2 exploram cenários com a ponte WebSocket do ROS através do serviço Starlink, em uma realidade bastante próxima do uso de sensores em áreas remotas (longe da blockchain de registro de validação). Novamente, em vermelho aparecem os intervalos de dados capturados, enquanto em azul estão apenas os valores de dados auditados (sempre os mais recentes). Com fluxo normal, a média em vermelho deve se aproximar de 10, dado que a frequência do ROS está definida para 10 Hz, enquanto os serviços de logs e de geração de blocos estão definidos para 1000 ms. Assim, é possível perceber um maior grau de perda com o uso de Starlink em 100ms (somente 45,33%), possivelmente pela maior sobrecarga na

[5]`https://github.com/mateusnazarioc/neo-ros-blockchain-bridge`

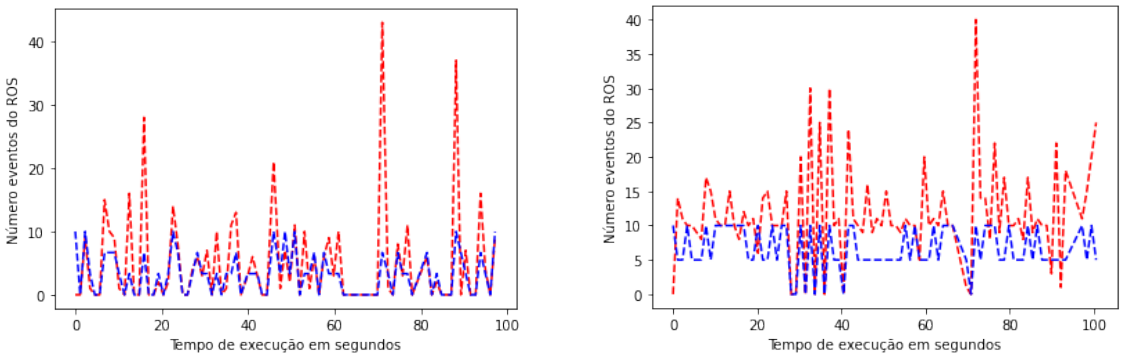

Figura 2. Starlink REST com ROS 10 Hz e verificação por oráculos a cada 100 ms e 500 ms. Produção de blocos e *logs* a cada 1000ms. Experimento de 100 segundos. Taxas de verificação de 45,33% e 57,05%, respectivamente.

rede remota par-a-par, visto a influência de diversos fatores como: obstrução do satélite e intempérie climática.

No mínimo, foi observadas taxas de 45,33% com disparos rápidos de 100ms, aumentando para 57,05% com disparos a cada 500ms, considerando uma coleta assíncrona via oráculos. Para 500ms (2 transações por segundo), a rede de blockchain provavelmente conseguiu encadear os blocos de uma maneira mais efetiva, com menor gargalo nas transações pendentes. Por outro lado, com menos disparos e também com redes mais lentas, podemos esperar uma menor sobrecarga da blockchain (com menor utilização da *mempool*) e maior estabilidade do processo de consenso, tópico a ser explorado em trabalhos futuros. É importante ressaltar que o experimento executado tem como resultado uma porcentagem que valida os dados buscados em uma taxa de tempo definida, respeitando a ordem de chegada (por segurança, o contrato e oráculo só aceitam os valores mais recentes, caso contrário seria necessário esperar indefinidamente por dados possivelmente falhos). Isto não significa uma perda de dados na blockchain, sendo possível para o usuário externo verificar os dados restantes diretamente nos blocos da rede.

5. Conclusão e Trabalhos Futuros

Neste trabalho, abordamos um processo de validação de dados de sensores do ROS através de uma blockchain privada com consenso bizantino. O processo é altamente complexo e desafiador, dada a pouca quantidade de material online para estudos e o pioneirismo envolvido no trabalho. O uso de oráculos é considerado hoje o estado-da-arte em tecnologias blockchain, permitindo a comunicação entre sistemas *trustless* de contratos inteligentes com o "mundo exterior" da Web 2 via *https*. Dada a natureza verificável da blockchain Neo, consideramos um servidor de agregação de dados via websocket e REST, pelo qual os oráculos podem se comunicar e obter informações precisas e determinísticas, viabilizando um consenso de tempo real e validação em cima dos dados de sensores. Foram feitos experimentos para validar a proposta, utilizando intervalos de transação de validação por oráculo de 100 ms e 500 ms, em uma rede blockchain privada com geração de blocos e logs a cada 1000 ms, enquanto dados eram gerados pelo ROS em 10 Hz, com acesso via Starlink. Com Starlink e taxa de 100 ms foi possível auditar e registrar no contrato 45% das informações enviadas pelo ROS. Portanto, a utilização da blockchain como fer-

ramenta de melhoria para sistemas de log e validação de dados obtidos em plataformas robóticas se mostra viável em um futuro próximo. Este trabalho pode ser estendido de diversas formas no futuro, seja com maior amplitude nos experimentos, considerando cenários e arquiteturas diversas, bem como buscando maior detalhamento no processo interno da blockchain durante os experimentos, exigindo maior grau de sofisticação dos mecanismos de log e também maiores modificações do contrato inteligente.

Agradecimentos

Os autores gostariam de agradecer ao apoio das agências de fomento brasileiras CNPq, CAPES e FAPERJ, e ao PROFICAM, pelo apoio financeiro e bolsas; bem como o apoio tecnológico da comunidade livre da Neo Blockchain.

Referências

Afanasyev, I., Kolotov, A., Rezin, R., Danilov, K., Mazzara, M., Chakraborty, S., Kashevnik, A., Chechulin, A., Kapitonov, A., Jotsov, V., Topalov, A., Shakev, N., and Ahmed, S. (2019). Towards blockchain-based multi-agent robotic systems: Analysis, classification and applications.

Alsamhi, S. H. and Lee, B. (2021). Blockchain-empowered multi-robot collaboration to fight covid-19 and future pandemics. *IEEE Access*, 9:44173–44197.

Azpurua, H., Rocha, F., Garcia, G., Santos, A. S., Cota, E., Barros, L. G., Thiago, A. S., Pessin, G., and Freitas, G. M. (2019). Espeleorobô - a robotic device to inspect confined environments. In *2019 19th International Conference on Advanced Robotics (ICAR)*, pages 17–23.

Balachandar, B. M. (2017). *RESTful Java Web Services: A pragmatic guide to designing and building RESTful APIs using Java*. Packt Publishing Ltd.

Berners-Lee, T. (2010). Long live the web. *Scientific American*, 303(6):80–85.

Elommal, N. and Manita, R. (2022). How Blockchain Innovation could affect the Audit Profession: A Qualitative Study. *Journal of Innovation Economics*, 0(1):37–63.

Ferrer, E. C., Jiménez, E., Lopez-Presa, J. L., and Martín-Rueda, J. (2022). Following leaders in byzantine multirobot systems by using blockchain technology. *IEEE Transactions on Robotics*, 38(2):1101–1117.

Fette, I. and Melnikov, A. (2011). Rfc 6455: The websocket protocol.

Hongfei, D. and Zhang, E. (2018). Neo white paper. *https://docs.neo.org/docs/en-us/basic/whitepaper. html*, 31(07):2020.

Murphy, R. R. (2014). *Disaster robotics*. MIT press.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260.

Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., Wheeler, R., Ng, A. Y., et al. (2009). Ros: an open-source robot operating system. In *ICRA workshop on open source software*, volume 3, page 5. Kobe, Japan.

Zhang, S., Tang, M., Li, X., Liu, B., Zhang, B., Hu, F., Ni, S., and Cheng, J. (2022). ROS-ethereum: A convenient tool to bridge ROS and blockchain (ethereum). *Security and Communication Networks*, 2022:1–14.