

DESAFIOS DOS SMART CONTRACTS NA ERA DA COMPUTAÇÃO QUÂNTICA: UMA ANÁLISE SOBRE A SEGURANÇA DO BLOCKCHAIN

MACÁRIO, Luani Maria de Albuquerque¹

MORAIS, Marielli Melo Soares de²

INTRODUÇÃO

A contemporaneidade é caracterizada por uma profunda imersão tecnológica, onde avanços digitais permeiam e redefinem múltiplas esferas de nossa existência. Dentre esses avanços, os contratos inteligentes e a tecnologia blockchain destacam-se, prometendo transformações significativas em diversos setores, dada sua capacidade de proporcionar eficiência, transparência e segurança sem paralelo (BARON, Guilherme; HOPPE, Aurélio, 2018). Contudo, a evolução da computação quântica apresenta-se como um potencial desafio à integridade dessas tecnologias.

A literatura recente tem evidenciado a promissora sinergia entre contratos inteligentes e blockchain, ressaltando sua capacidade de automatizar e validar acordos de forma descentralizada. No entanto, a emergente computação quântica, com seu poder computacional superior, coloca em xeque a segurança dessas inovações (MACÁRIO, L. M. A., MORAIS, M. M. S. de, SILVA, M. A. X. da., 2022). Diante deste cenário, a presente pesquisa emerge como uma tentativa de compreender e antecipar os desafios inerentes a essa intersecção.

O propósito central deste estudo é explorar a interação entre contratos inteligentes e computação quântica, mapeando os riscos e vulnerabilidades inerentes. Através de uma análise crítica, objetiva-se propor medidas que assegurem a robustez dos contratos inteligentes e do blockchain frente à realidade iminente da computação quântica. A relevância deste trabalho reside na imperativa necessidade de antecipar e mitigar potenciais ameaças, garantindo que tais inovações tecnológicas mantenham sua promessa de segurança e confiabilidade em uma sociedade cada vez mais digitalizada (FEDOROV, A. K.; KIKTENKO, E. O.; LVOVSKY, A. I., 2018).

METODOLOGIA

Em nossa jornada de pesquisa, mergulhamos no fascinante mundo dos contratos inteligentes e da computação quântica. Ao explorar diversas fontes acadêmicas, nos deparamos com uma riqueza de informações, cada artigo abrindo uma nova janela de entendimento. O caminho que escolhemos, pautado em uma revisão bibliográfica detalhada, nos levou a

¹ Doutora em Ciências Sociais e Jurídicas pela Universidade Del Museo Argentino, 2019; Pós-graduação em EAD pela Faculdade de Jacarepaguá/RJ; DOCÊNCIA: Faculdade Raimundo Marinho, Faculdade Mauricio de Nassau, Faculdade Fama, Período: 2007 a 2017; POLÍCIA Militar de Alagoas, Bombeiros de Alagoas, Período de 2007 a 2022; Ministério da Ciência e Tecnologia. Coordenação de Bens Sensíveis; Trabalho com a ONU Segurança Antiterrorismo. Armas-químicas, Biológicas, Nuclear; Direito Internacional, braço da Casa Civil. Trabalho Considerado Paramilitar, Período: 2001 a 2006.

² Editora-chefe da Revista de Legal Design & Visual Law; Consultora de Compliance em Privacidade e Proteção de Dados; Membro da Associação Nacional de Compliance (ANACO) e do Comitê de Privacidade e Proteção de Dados; Engenheira de Prompt para Cibersegurança pelo IBSEC; Integrante dos Laboratórios: Comunidade de Estudos LGPD (Facilitadora) e Pesquisadora em Legal Design do Laboratório de Direitos Digitais da Universidade Federal da Bahia (Labid²-UFBA); Pesquisadora do Grupo de Tecnologia e de pesquisa em Inteligência Artificial e Direito da Comissão de Tecnologia, Inovação e Proteção de Dados (CITPD) e da OAB/AL em parceria com a Escola Superior de Advocacia de Alagoas (ESA/AL); Mestranda Profissional em Direito, Justiça e Desenvolvimento pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP-BSB); Pós-Graduada em Direito Internacional (CEDIN/ Milton Campos/BH-MG); Pós-Graduada em Direito Constitucional (IDP/UNISUL/LFG); E-mail: mariellimelo@visuallaw.org. Lattes: <http://lattes.cnpq.br/0389416055398926>. ORCID: <https://orcid.org/0000-0002-4894-6642>.

descobertas intrigantes, revelando os desafios e as promessas que se desenham quando essas duas poderosas tecnologias se encontram.

RESULTADOS

Ao mergulharmos na complexa relação entre a computação quântica e as estruturas de blockchain e contratos inteligentes, desvendamos aspectos críticos e desafios iminentes. A revolução que os contratos inteligentes e a blockchain propõem é inegável, estabelecendo novos patamares de eficiência e transparência nas operações digitais, um avanço bem articulado por Baron, Guilherme; Hoppe, Aurélio (2018). Contudo, a emergência da computação quântica lança sombras sobre esses avanços, introduzindo ameaças potenciais à segurança que sustenta essas inovações tecnológicas (Kappert, Noah; Karger, Erik; Kureljusic, Marko).

Em meio aos avanços, a criptografia quântica surge com um brilho de esperança, destacando-se como uma estratégia inovadora capaz de enfrentar os complexos desafios trazidos pela computação quântica (ILIE DI, KNOTTENBELT WJ, STEWART ID, 2020). Essa percepção acende um alerta: estamos diante da necessidade de elaborar estratégias de segurança mais robustas, que possam resistir às ameaças desencadeadas pela era quântica.

Nossa pesquisa (Macário, L. M. A., Morais, M. M. S. de, Silva, M. A. X. da., 2022) vai além de meramente reconhecer a dinâmica desse campo em rápida transformação; ela clama por uma postura ativa na busca por soluções. A jornada através das inovações tecnológicas não é um caminho livre de obstáculos, mas um trajeto que demanda discernimento e preparação. Enquanto nos maravilhamos com as possibilidades do novo mundo digital, devemos estar prontos, também, para navegar pelas suas incertezas, assegurando que a integridade e o potencial dessas novas ferramentas sejam preservados no amanhã que se desenha.

FUNDAMENTAÇÃO TEÓRICA

Ao mergulharmos na intrincada relação entre computação quântica, blockchain e contratos inteligentes, nossa análise revela implicações profundas dessas inovações. Apoiados nas descobertas de Baron e Hoppe (2018), evidenciamos como os contratos inteligentes e a blockchain reformularam as práticas nas operações online, estabelecendo um novo paradigma para transações seguras e descentralizadas.

No entanto, ao sondarmos, com maior profundidade, a computação quântica, é notório a emersão de desafios significativos que colocam em risco a segurança dessas infraestruturas pioneiras (Kappert, Karger e Kureljusic, 2020). A evolução acelerada da computação quântica representa uma ameaça tangível, que exige respostas ágeis e proativas.

Nesse cenário, a criptografia quântica surge como um farol de esperança, propondo uma abordagem revolucionária para combater os riscos impostos pela computação quântica (Ilie, Knottenbelt e Stewart, 2020). Seus métodos avançados oferecem uma camada extra de proteção, tornando-se indispensável à medida que nos aproximamos da era quântica.

Assim, as conclusões de nosso estudo (Macário, Morais e Silva, 2022) acendem um alerta sobre os desafios iminentes e a urgência de estratégias de segurança aprimoradas. O futuro das operações online reserva inúmeras possibilidades, mas é vital estarmos equipados para preservar a integridade dessas inovações frente às incertezas que se aproximam. Compreender o contexto atual e as alternativas disponíveis é fundamental para assegurar que os méritos da blockchain e dos contratos inteligentes não sejam obscurecidos pelo progresso da computação quântica.

Ao olharmos para o futuro, ressalta-se a importância de não apenas continuar, mas também expandir nossas investigações. Precisamos explorar a robustez da criptografia quântica, entender as ramificações da computação quântica em estruturas como a blockchain, e ir além,

sondando as vulnerabilidades potenciais dos contratos inteligentes e considerando novos métodos de proteção.

A atenção dedicada ao potencial da computação quântica e da tecnologia blockchain está se intensificando no mundo a cada dia que passa. No Brasil, já é possível notar movimentos como o Programa e-Cidadania e ideias para novas leis, como o projeto de lei 1979/2022 também o 1458/2022. Essas ações demonstram como temos um forte interesse em desenvolver normas para essas tecnologias emergentes.

Os Estados Unidos já aprovaram leis como o National Quantum Initiative Act of 2018 (S. 3143), que cutuca e atiza a curiosidade sobre estudos na esfera da computação quântica, sem esquecer o Quantum Computing Cybersecurity Preparedness Act of 2022 (H.R. 7535), que aborda o significado essencial de salvar essas tecnologias.

O empreendimento dessas medidas legislativas reforça o pilar de que é necessária uma postura que abrace uma investigação preventiva e instruída para assegurar que inovações, como a computação quântica e a tecnologia blockchain, sejam executadas de forma protegida, eficiente e adequada às diretrizes legais e regulatórias, salientando que esse despertar do conhecimento não dita o fim do nosso caminho, mas marca o início de onde devemos nos direcionar enquanto nos aprofundamos no universo dessas tecnologias.

CONCLUSÕES

Neste estudo, ao desbravarmos a complexa interação entre os contratos inteligentes, a blockchain e a computação quântica, nos deparamos com um território repleto de possibilidades e, ao mesmo tempo, desafios inerentes. Reconhecemos que os contratos inteligentes e a blockchain revolucionaram a maneira como as operações online são conduzidas, trazendo um novo nível de confiança para o cenário digital. Porém, a chegada da computação quântica traz consigo nuances que podem abalar as fundações de segurança dessas inovações pioneiras.

Diante disso, fica claro a intensificação das defesas no mundo digital. A criptografia quântica se apresenta como um farol de esperança, sugerindo um caminho para neutralizar as ameaças que a computação quântica pode impor. É essencial que, como comunidade de pesquisadores e tecnólogos, mantenhamos nossos olhos abertos e nossas mentes alertas para navegar por esses desafios.

Ao olharmos para o futuro, ressalta-se a importância de não apenas continuar, mas também expandir nossas investigações. Precisamos explorar a robustez da criptografia quântica, entender as ramificações da computação quântica em estruturas como a blockchain, e ir além, sondando as vulnerabilidades potenciais dos contratos inteligentes e considerando novos métodos de proteção.

Em suma, este estudo serve como um lembrete de que o equilíbrio é a chave. Devemos celebrar e adotar os avanços tecnológicos, mas sem esquecer de exercer cautela e nos dedicar à pesquisa incessante, assegurando que a segurança e a eficiência acompanhem o ritmo da inovação no vibrante ecossistema digital.

REFERÊNCIAS

Bravyi, S., Dial, O., Gambetta, J. M., Gil, D., & Nazario, Z. (2022). The future of quantum computing with superconducting qubits. *Journal of Applied Physics*, 132(16), 160902. doi:10.1063/5.0082975.

Brasil. Câmara dos Deputados. Projeto de Lei nº 1458/2022. Disponível em:

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2318660>. Acesso em: 18 out. 2023.

Brasil. Câmara dos Deputados. Projeto de Lei nº 1979/2022. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2318661>. Acesso em: 18 out. 2023.

Brasil. Programa e-Cidadania. Senado Federal. Disponível em: <https://www12.senado.leg.br/ecidadania>. Acesso em: 18 out. 2023.

Brasil. Senado Federal. Requerimento nº 2351, de 2020. Autoria: Senador Plínio Valério. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/144809>. Acesso em: 18 out. 2023.

Carette, J., James, R. P., & Sabry, A. (2018). Embracing the laws of physics: Three reversible models of computation. arXiv preprint arXiv:1811.03678.

Daley, A. J., Bloch, I., Kokail, C., et al. (2022). Practical quantum advantage in quantum simulation. *Nature*, 607, 667–676. doi:10.1038/s41586-022-04940-6.

Estados Unidos. National Quantum Initiative Act of 2018. S. 3143. Disponível em: <https://www.congress.gov/bill/115th-congress/senate-bill/3143>. Acesso em: 18 out. 2023.

Estados Unidos. Quantum Computing Cybersecurity Preparedness Act of 2022. H.R. 7535. Disponível em: <https://www.congress.gov/bill/117th-congress/house-bill/7535>. Acesso em: 18 out. 2023.

Kirmani, A., Bull, K., Hou, C.-Y., Saravanan, V., Saeed, S. M., Papić, Z., Rahmani, A., & Ghaemi, P. (2022). Probing Geometric Excitations of Fractional Quantum Hall States on Quantum Computers. *Physical Review Letters*, 129(5), 056801. doi:10.1103/PhysRevLett.129.056801.

Macário, L. M. A., Morais, M. M. S. de, Silva, M. A. X. da. (2022). O advento da computação quântica e seus riscos para o paradigma blockchain/smart contracts. *In: Pensando as novas tecnologias*, organizado por Maria do Carmo Boaventura Motta e Mariana de Almeida Motta Rezende (p. 15-32). Deerfield Beach, Florida: Pembroke Collins.

Stanisic, S., Bosse, J. L., Gambetta, F. M., Santos, R. A., Mruzckiewicz, W., O'Brien, T. E., Ostby, E., & Montanaro, A. (2022). Observing ground-state properties of the Fermi-Hubbard model using a scalable algorithm on a quantum computer. *Nature Communications*, 13(1), 5743. doi:10.1038/s41467-022-33335-4.

Tennie, C., & Palmer, T. (2023). Quantum Computers for Weather and Climate Prediction: The Good, the Bad and the Noisy. *Bulletin of the American Meteorological Society*. [https://journals.ametsoc.org/configurable/content/journals\\$002fbams\\$002f104\\$002f2\\$002fBAMS-D-22-0031.1.xml?t%3Aac=journals%24002fbams%24002f104%24002f2%24002fBAMS-D-22-0031.1.xml](https://journals.ametsoc.org/configurable/content/journals$002fbams$002f104$002f2$002fBAMS-D-22-0031.1.xml?t%3Aac=journals%24002fbams%24002f104%24002f2%24002fBAMS-D-22-0031.1.xml).

Washington. Washington State Legislature. Disponível em:

<https://app.leg.wa.gov/billsummary?BillNumber=6414&Year=2022&Initiative=false>. Acesso em: 18 out. 2023.