Título do Projeto	Um framework para análise de vulnerabilidades de transações financeiras entre blockchains
Área de Conhecimento	Ciência da Computação
Orientador	Prof. Dr. Fernando Luís Dotti PUCRS - Escola Politécnica Progrma de Pós-Graduação em Ciência da Computação
Tipo de bolsa	Iniciação Científica

1. Fundamentação Teórica (máximo 2 páginas):

Um aspecto disruptivo de *blockchains* é que fornecem um serviço seguro e confiável através de um sistema computacional distribuído constituído de partes que não precisam confiar umas nas outras [1]. Por sistema computacional distribuído entende-se um sistema composto por um conjunto de processos que se comunicam por troca de mensagens, sujeitos a latências de comunicação e falhas de processos. No caso de *blockchains*, falhas arbitrárias, ou bizantinas [22], devem ser toleradas. Estas ocorrem quando um sub-conjunto de processos pode se desviar de sua especificação de qualquer forma, podendo por exemplo: atrasar, omitir, modificar mensagens intencionalmente, agir isoladamente ou em conluio para prejudicar a consistência do sistema, no caso, da *blockchain*. A 'cadeia de blocos' fornece armazenamento de um estado e processamento sobre este, mesmo na presença de participantes bizantinos, satisfazendo níveis de consistência - tipicamente atomicidade e ordenação total - e vivacidade - incluindo aqui disponibilidade do sistema e progresso. O modelo de computação fundamental remonta a Replicação Máquina de Estados (RME) proposta por Lamport [2,3] em que: (i) um conjunto de réplicas (as partes) iniciam em um mesmo estado (mesma cadeia de blocos, em sua gênese); (ii) concordam com uma ordem total das operações aplicadas sobre o estado (ordem dos blocos que são adicionados à cadeia e das transações dentro dos blocos); e (iii) processam as operações de forma determinística sobre o último estado, obtendo o próximo (processam em ordem as transações do bloco decidido). A extensão de RME para tolerar falhas bizantinas tem diversas características importantes comuns a blockchains. Apesar disto, blockchains trazem um conjunto de propriedades e objetivos adicionais que as diferenciam de RME bizantina [4], como escalabilidade (atingir um número consideravelmente maior de participantes) e imutabilidade do histórico de transações, juntamente com a possibilidade de acessá-lo (permitindo conferir/auditar o mesmo). Os desafios técnicos de blockchains tem sido objeto de intensa pesquisa desde seu surgimento, tendo levado a avanços já reportados em 'surveys' como [5, 6, 7, 8, 9, 10, 11, 12]. Nos últimos anos um conjunto considerável de áreas de aplicação tem empregado blockchains. Apesar dos mesmos fundamentos básicos colocados anteriormente, aplicações diferentes utilizam diferentes abordagens/arquiteturas de blockchains [8].

Interoperabilidade. À medida que diferentes áreas sejam apoiadas por blockchains heterogêneas, é também natural que a integração entre as mesmas torne-se cada vez mais importante, permitindo integração entre as áreas de aplicação. Abordagens para interoperabilidade de blockchains tem surgido na indústria, e.g. [15,16]. Em [15] um protocolo chamado Inter-Blockchain Protocol (IBC) define como mensagens podem ser trocadas entre blockchains. A arquitetura adotada para tal é que uma mensagem é registrada em uma blockchain A, sendo endereçada para uma blockchain B. A blockchain B deve contar com um cliente na blockchain A, que percebe a mensagem registrada para si. A arquitetura é simétrica para enbviar de B para A. O componente de interconexão de cadeias chama-se *relayer*. Dependendo da operação entre cadeias, diversas trocas de mensagens podem ser necessárias entre elas. Em [16] uma arquitetura mais abrangente é apresentada envolvendo parte das ideias de [15] e indo além, provendo uma abordagem de gerência de riscos que usa uma forma de atribuir reputação para as entidades responsáveis por transações entre cadeias. A necessidade de utilizar um feedback por reputação revela a dificuldade ou talvez impossibilidade de garantir, por construção, que transações entre cadeias tenham as mesmas propriedades de transações em cadeias únicas. Exemplificando de forma simplista: enquanto transferir uma mesma criptomoeda de uma carteira para outra é uma transação simples na cadeia que suporta a criptomoeda, isto não se generaliza quando queremos transferir de uma criptomoeda em uma carteira para outra carteira em outra criptomoeda, suportada por outra cadeia.

Maximal Extractable Value (MEV). Em paralelo a isso, considerando somente o cenário com cadeia única, segundo [13], de 2020 a 2022, corretores 'oportunísticos' obtiveram centenas de milhões de dólares excluindo, incluindo e mudando a ordem de transações financeiras. Este problema é chamado na área de Maximal Extractable Value (MEV), em geral, e se origina devido ao conteúdo de uma transação ser visível antes de que sua ordem relativa de efetivação seja estabelecida [14]. De fato, conforme o modelo fundamental de execução de RME, adotado em blockchains, um participante continuamente recebe transações, propõe uma ordem para as mesmas, uma vez acordada a ordem (usando consenso), as transações são executadas. O conteúdo da transação está disponível antes de sua execução. Abordagens para evitar MEV no contexto de blockchains tem surgido nos últimos anos, e.g. [17,18,19,20,21]. Entre elas, a técnica de 'commit-reveal' [23] em que o conteúdo de uma transação só é revelado para execução depois de seu ordenamento em relação às demais, assim como técnicas para evitar interferência no ordenamento, assegurando 'order-fairness' [24,25,26].

MEV e Interoperabilidade. Dado que a interação entre blockchains não acontece com mesmas propriedades de transações em uma blockchain única, o problema de MEV pode ser mais complexo no primeiro caso: dadas as várias fases de comunicação entre cadeias, como por exemplo as adotadas em [15,16], mais oportunidades existem para que o conteúdo de uma transação se torne visível e seja utilizado de forma indevida, podendo vir a ser alvo de uma reordenação, ou inserção de transação de interesse. Os mecanismos propostos para evitar MEV em cadeia única não generalizam para o cenário inter-cadeias. O problema de MEV no contexto inter-cadeias tem recebido atenção recente na literatura. Em [28] os autores elencam uma lista de fragilidades que podem ocorrer com questões ainda abertas de trabalho. Um formalismo é proposto para análise de MEV entre-cadeias, tratando-se de trabalho em progresso conforme colocado pelos autores. Em [29] os autores fazem uma análise de dados de transações inter-cadeias, concluindo que MEV entre cadeias será uma ameaça para a descentralização de Ethereum e deixando questões de pesquisa. De forma análoga, porém mais detalhada, em [30] também é feita uma análise sobre transações existentes levando a afirmar que existe espaço para arbitragem inter-cadeias com ganhos dos além dos possíveis em cadeias únicas e concluindo com diversas perguntas em aberto. Também publicado em 2024, [31] aponta para problemas de projeto em arquiteturas para interconectar cadeias diferentes afirmando que: "o estado corrente de arquiteturas entre cadeias é que elas são ambíguas e há praticamente nenhuma noção sobre como diferentes arquiteturas se seus componentes estão relacionados a diferentes vulnerabilidades". Um recente 'survey' na área [32] avalia de forma mais sistemática o problema. De forma análoga, os autores elencam uma série de questões em aberto e algumas possíveis direções de trabalhos. Não alongando este texto com outras referências, a observação comum é de que diversas questões estão em aberto e que esta linha de trabalhos está em sua infância, apesar de operacoes entre cadeias serem indispensáveis.

Referências: vide item 5

2. Objetivos (máximo 1 página):

O proponente tem produção continuada há uma década na área de Replicação Máquina de Estados. Vem trabalhando com o modelo bizantino de falhas desde 2018 (vide publicação em DSN 2018 em fldotti.github.io) e mais recentemente considerando ordens parciais de transações em blocos visando aumento de desempenho (vide publicação em LADC 2023 em fldotti.github.io). Esta solicitação de bolsa IC, junto com outras, fazem parte de uma iniciativa maior de trabalhos relacionados ao contexto de múltiplas blockchains. Esta agenda de pesquisa será conduzida em cooperação com o colega da Universidade de Lugano, Prof. Dr. Fernando Pedone, em cujo laboratório o proponente esteve em visita de dezembro de 2023 a fevereiro de 2024 no escopo do programa PUCRS-Print. Durante esta visita, o proponente teve oportunidade de iniciar trabalhos de pesquisa em co-autoria com membros da Informal Systems (https://informal.systems/) responsáveis pelos principais módulos da arquitetura Cosmos, desde seu princípio voltada para o contexto de múltiplas blockchains. Esta área de atividades requer o domínio de diversos fundamentos não triviais de sistemas distribuídos em geral e também específicos de blockchains. A formação nesta área envolve o domínio destes conceitos e, dada a

natureza da área, também o entendimento de problemas concretos atualmente enfrentados em blockchains existentes. **O principal objetivo geral deste projeto é:**

OG1) ***Formar estudantes nesta área****, possibilitando o contato com os colaboradores mencionados acima tanto da academia como da indústria.*

No contexto acima descrito, este projeto tem também o objetivo geral de:

OG2) *Fortalecer a colaboração internacional com a Universidade de Lugano, apoiada via PUCRS-Print, e expandir a colaboração para membros da indústria cfe. mencionado.*

Como objetivos técnicos ao ao bolsista, ao final do período ele deve ter:

OT1) *Domínio de conceitos fundamentais: arquitetura geral de blockchains, consenso em blockchains*

OT2) *Domínio das principais arquiteturas para comunicação entre cadeias*

OT3) *Domínio da arquitetura de aplicações financeiras típicas em blockchains: criptomoeadas, tokenização, finanças descentralizadas, etc*

OT4) *Conhecimento dos principais ataques em blockchains e no contexto inter-blockchain*

OT5) *Saber analisar a vulnerabilidade da combinação de blockchain, protocolo inter-blockchain e aplicação aos ataques estudados*

OT6) *Dominar tecnologia de uma blochchain específica, sendo capaz de instanciar e realizara experimentos com a mesma.*

Como resultados da pesquisa, temos como objetivo:

OR1) *Um framework de análise de vulnerabilidade de trasações entre blockchains aos ataques estudados* ***- este sendo o resultado central de pesquisa***

OR2) *Relatos de aplicação do framework a diferentes configurações de < blockchain, protocolo de interconexão, aplicação, ataque MEV >*

OR3) *Comprovação dos pontos de vulnerabilidade identificados em OR2 com protótipos instanciando as configurações avaliadas.*

A respeito de produção científica, nossos objetivos são:

OP1) *1 artigo em conferência e* ***OP2)*** *1 artigo em journal*

Por fim, a depender do andamento dos trabalhos, o proponente tem como objetivo configurar um grupo de pesquisa em Tecnologias Financeiras (FinTechs). Este grupo iniciaria com este projeto, abordando fraudes/ataques MEV, mas pode vir a crescer para outros aspectos de FinTechs. Conforme o andamento, prevê-se a necessidade de interdisciplinaridade envolvendo pesquisadores da área de Economia e futuro uso de Ciência de Dados para avaliar correlação de origens e reordenação de transações financeiras.

3. Materiais e Métodos:

Materiais:

esta pesquisa será desenvolvida com software disponível e sobre plataformas distribuídas de desenvolvimento também disponíveis como o CloudLab https://www.cloudlab.us/ o qual já é utilizado pelo grupo de pesquisa. Em caso de dificuldades, podemos também utilizar um cluster na Universidade de Lugano, parceira em atividades de pesquisa e já utilizadas pelos alunos do grupo.

Métodos:

Um dos objetivos técnicos centrais do estudo (O6) é o desenvolvimento de um framework de análise de vulnerabilidade de transações entre blockchains a ataques MEV. Tal framework, se concebido, trará importante contribuição à área.

No que se refere à colaboração internacional, o proponente tem reuniões semanais regulares com o grupo Suíço, contando inclusive com um doutorando em dupla titulação PUCRS/USI. Os bolsistas terão oportunidade de interagir neste contexto. Ademais, como mencionado, dada a aproximação de trabalhos com colegas da Informal Systems, poderemos discutir de forma concreta sobre cargas de trabalho executadas e ataques mais danosos aos sistemas. Assim, o framework de análise seria aplicado com dados de casos reais.

4. Bibliografia:

Referencias mencionadas no item 1.

[1] Sherman, A. T., Javani, F., Zhang, H., and Golaszewski, E. On the origins and variations of blockchain technologies. IEEE Security Privacy 17, 1 (2019), 72–77.

[2] L. Lamport, *Time, Clocks, and the Ordering of Events in a Distributed System*. Association for Computing Machinery, 2019, pp. 179–196.

[3] F. B. Schneider, “Implementing fault-tolerant services using the state ma- chine approach: A tutorial,” *ACM Computing Surveys (CSUR)*, vol. 22, no. 4, pp. 299–319, 1990.

[4] A. Bessani, E. Alchieri, J. Sousa, A. Oliveira and F. Pedone, "From Byzantine Replication to Blockchain: Consensus is Only the Beginning," 2020 50th IEEE/IFIP International Con-ference on Dependable Systems and Networks (DSN), Valencia, Spain, 2020, pp. 424-436,

[5] Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., and Danezis, G. Sok: Consensus in the age of blockchains. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies (2019), ACM, pp. 183–198.

[6] Cachin, C., and Vukolić, M. Blockchain consensus protocols in the wild. In DISC (2017).

[7] Correia, M., Veronese, G. S., Neves, N. F., and Verissimo, P. Byzantine consensus in asynchronous message-passing systems: a survey. International Journal of Critical Computer-Based Systems 2, 2 (2011), 141–161.

[8] Natoli, C., Yu, J., Gramoli, V., and Esteves-Verissimo, P. Deconstructing blockchains: A com-prehensive survey on consensus, membership and structure. arXiv preprint arXiv:1908.08316 (2019).

[9] Nguyen, G.-T., and Kim, K. A survey about consensus algorithms used in blockchain. Journal of Information processing systems 14, 1 (2018).

[10] Platania, M., Obenshain, D., Tantillo, T., Amir, Y., and Suri, N. On choosing server-or client-side solutions for bft. ACM Computing Surveys 48, 4 (2016), 61

[11] Wang, W., Hoang, D. T., Xiong, Z., Niyato, D., Wang, P., Hu, P., and Wen, Y. A survey on consensus mechanisms and mining management in blockchain networks. arXiv preprint arXiv:1805.02707 (2018).

[12] Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., and Zheng, K. Survey on blockchain for internet of things. Computer Communications (2019)

[13] K. Qin, L. Zhou, and A. Gervais, “Quantifying blockchain extractable value: How dark is the forest?” in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 198–214.

[14] Vincent Gramoli, Zhenliang Lu, Qiang Tang, Pouriya Zarbafian. AOAB: Optimal and Fair Ordering of Financial Transactions. 54th International Conference on Dependable Systems and Networks. DSN 2024. Brisbane, Australia, June 24-27. accepted paper

[15] Interblockchain Communication Protocol (IBC). Interchain Standards. https://github.com/cosmos/ibc https://github.com/cosmos/ibc

[16] Chainlink *Cross-Chain Interoperability Protocol (CCIP).* https://docs.chain.link/ccip

[17] L. Heimbach and R. Wattenhofer, “SoK: Preventing Transaction Re- ordering Manipulations in Decentralized Finance,” in *4th ACM Confer- ence on Advances in Financial Technologies*, September 2022.

[18] D. Malkhi and P. Szalachowski, “Maximal extractable value (MEV) protection on a DAG,” in *4th International Conference on Blockchain Economics Security and Protocols*, 2022.

[19] M. Kelkar, S. Deb, S. Long, A. Juels, and S. Kannan, “Themis: Fast, strong order-fairness in byzantine consensus,” in *ConsensusDays 21*, 2021.

[20] C. Cachin, J. Mic´ic´, N. Steinhauer, and L. Zanolini, “Quick order fairness,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2022, pp. 316–333.

[21] Y.Zhang,S.Setty,Q.Chen,L.Zhou,andL.Alvisi,“Byzantine ordered consensus without byzantine oligarchy,” in *OSDI*, 2020, pp. 633–649.

[22] L. Lamport, R. Shostak, and M. Pease. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, Pages 382-401.

[23] D. Malkhi and P. Szalachowski, “Maximal extractable value (MEV) protection on a DAG,” in *4th International Conference on Blockchain Economics Security and Protocols*, 2022.
[24] Y.Zhang,S.Setty,Q.Chen,L.Zhou,andL.Alvisi,“Byzantine ordered consensus without byzantine oligarchy,” in *OSDI*, 2020, pp. 633–649.
[25] P. Zarbafian and V. Gramoli, “Brief announcement: Ordered reliable broadcast and fast ordered byzantine consensus for cryptocurrency,” in *35th International Symposium on Distributed Computing, DISC*, ser. LIPIcs, vol. 209. Schloss Dagstuhl - Leibniz-Zentrum fu ̈r Informatik, 2021, pp. 63:1–63:4.
[26] P. Zarbafian and V. Gramoli, “Lyra: Fast and scalable resilience to reordering attacks in blockchains,” in *Proceedings of the IEEE International Parallel & Distributed Processing Symposium (IPDPS)*, 2023.
[27] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In 2020 IEEE Symposium on Security and Privacy (SP), pages 910–927. IEEE, 2020.
[28] Obadia, A., Salles, A., Sankar, L., Chitra, T., Chellani, V., & Daian, P. (2021). Unity is strength: A formalization of cross-domain maximal extractable value. *arXiv preprint arXiv:2112.01472*.
[29] J. H. Sjursen, W. Meng and W. -Y. Chiu, "A Closer Look at Cross-Domain Maximal Extractable Value for Blockchain Decentralisation," *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Dubai, United Arab Emirates, 2023, pp. 1-3, doi: 10.1109/ICBC56567.2023.10174971.
[30] O. Mazor and O. Rottenstreich, "An Empirical Study of Cross-Chain Arbitrage in Decentralized Exchanges," 2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2024, pp. 488-496.
[31] Notland, J. S., Li, J., Nowostawski, M., & Haro, P. H. (2024). SoK: Cross-Chain Bridging Architectural Design Flaws and Mitigations. *arXiv preprint arXiv:2403.00405*.
[32] Panpan Han, Zheng Yan, Wenxiu Ding, Shufan Fei, and Zhiguo Wan. 2023. A Survey on Cross-chain Technologies. Distrib. Ledger Technol. 2, 2, Article 15 (June 2023), 30 pages. https://doi.org/10.1145/3573896