Estudo e Categorização de Vulnerabilidades de Segurança em Tecnologias Blockchain

Helio C. B. Junior[1], **Vitor F. B. A. Carneiro**[1], **Josiel M. Figueiredo**[1], **Nelcileno V. S. Araújo**[1], **Constantino D. C. Neto**[1], **Letízia M. S. Eugênio**[1]

[1]Programa de Pós-Graduação em Computação Aplicada
Universidade Federal de Mato Grosso (UFMT),
Cuiabá, MT, Brasil

helio.junior@sou.ufmt.br, vitorfelip@gmail.com
{josiel, nelcileno}@ic.ufmt.br, constantino.neto@ifmt.edu.br,
letizia.eugenio@sou.ufmt.br

Abstract. *Blockchain technology, known for its security and decentralization, faces critical vulnerabilities that can compromise system integrity and efficiency. This study categorizes these vulnerabilities into smart contracts, consensus mechanisms, network architecture, and analytical tools, based on academic literature from 2015 to 2023. Classic flaws were identified, such as reentrancy attacks in smart contracts, 51% attacks on consensus mechanisms, and network node synchronization issues. The findings indicate that adopting auditing tools, alternative consensus algorithms, and adaptable network architectures are crucial to mitigate risks. The study concludes that blockchain security is a dynamic field, and multidimensional strategies are essential to enhance reliability for critical applications, including finance, healthcare, and logistics.*

Resumo. *A tecnologia blockchain, reconhecida por sua segurança e descentralização, apresenta vulnerabilidades críticas que podem comprometer sua integridade e eficiência. Este estudo categoriza essas vulnerabilidades em contratos inteligentes, mecanismos de consenso, arquitetura de rede e ferramentas de análise, com base em literatura acadêmica entre 2015 e 2023. Foram identificadas falhas clássicas, como ataques de reentrância em contratos inteligentes, ataques de 51% em mecanismos de consenso e problemas de sincronização entre nós da rede. Os resultados indicam que a adoção de ferramentas de auditoria, algoritmos de consenso alternativos e arquiteturas de rede adaptáveis são fundamentais para mitigar riscos. Conclui-se que a segurança em blockchain é um campo dinâmico, e que estratégias multidimensionais são essenciais para tornar a tecnologia mais confiável em aplicações críticas, como finanças, saúde e logística.*

1. Introdução

O surgimento da blockchain remonta o nascimento do Bitcoin em 2009, idealizada como uma moeda digital descentralizada de bancos e Estados [Nakamoto 2008]. Desde então, sua inventividade progrediu consideravelmente, alçando expansões em contratos inteligentes, administração de cadeias de abastecimento, identidade digital e outros campos em que sua aplicação é possível [Chang and Chen 2020, Moosavi et al. 2021].

Apesar de a blockchain inspirar confiança por seus princípios de segurança e imutabilidade, diversos ataques bem-sucedidos evidenciam que essas características não garantem invulnerabilidade [König et al. 2020]. Estudos relatam falhas exploradas em diferentes camadas do sistema, desde contratos inteligentes até mecanismos de consenso, revelando a necessidade de uma compreensão mais profunda sobre os pontos frágeis da tecnologia [König et al. 2020, Amiet 2021].

Nesse contexto, o estudo dessas vulnerabilidades desvela as possibilidades de progresso para resistir mais eficientemente às tentativas de quebra de segurança. Para alcançar a proposta, as vulnerabilidades de segurança contidas em diferentes camadas da blockchain serão categorizadas a partir da identificação das suas causas e consequências em ataques reais bem-sucedidos.

A partir dessa categorização, serão construídas hipóteses iniciais e avaliadas as soluções práticas recomendadas pelo referencial teórico para que seja possível sugerir direções futuras para pesquisas e implementações no âmbito da segurança da tecnologia blockchain. Por fim, pretende-se entender melhor os perigos ligados ao aumento do uso de tecnologias blockchain em aplicações vitais, bem como os caminhos para minimizá-los, auxiliando na criação de sistemas blockchain mais seguros e confiáveis.

A estrutura deste artigo está organizada da seguinte forma: a Seção 2 apresenta os trabalhos relacionados. A Seção 3 detalha a metodologia de pesquisa. A Seção 4 discute a revisão bibliográfica que embasa o estudo. A Seção 5 propõe a categorização das vulnerabilidades. A Seção 6 apresenta a conclusão e, por fim, a Seção 7 delineia as perspectivas para trabalhos futuros.

2. Trabalhos Relacionados

O estudo das vulnerabilidades em tecnologias blockchain tem produzido múltiplas taxonomias, sendo essencial situar a proposta deste trabalho frente às abordagens existentes. A presente pesquisa adota uma perspectiva multidimensional, em contraste com a tendência predominante de segmentar as análises por camadas isoladas do ecossistema blockchain.

Grande parte dos estudos concentra-se na camada de aplicação, com ênfase nos contratos inteligentes. As análises de [Atzei et al. 2017] e [Luu et al. 2016] identificam vulnerabilidades de codificação e lógica, como a reentrância, mas desconsideram riscos sistêmicos e de infraestrutura. Pesquisas voltadas aos mecanismos de consenso [Conti et al. 2018, Gervais et al. 2016, Bonneau et al. 2015] aprofundam-se em ameaças como ataques de 51% e centralização de mineração, enquanto outros estudos tratam do desempenho e escalabilidade da rede [Dinh et al. 2018]. No entanto, essas abordagens permanecem isoladas, sem integrar a visão completa do sistema.

Alguns *frameworks* de segurança, como o *OWASP Top Ten*, têm sido adaptados ao blockchain. Estudos indicam que muitas de suas vulnerabilidades se aplicam a esse contexto. Iniciativas como o *Decentralized Application Security Project* (DASP) focam em contratos inteligentes. Apesar de úteis, esses *frameworks* não cobrem integralmente vulnerabilidades de Mecanismos de Consenso, Arquitetura de Rede e Ferramentas de Análise [Poston 2020].

A contribuição deste estudo consiste na formulação de uma taxonomia integrada que abrange quatro dimensões interdependentes: Contratos Inteligentes, Mecanismos

de Consenso, Arquitetura de Rede e Ferramentas e Análise. Essa abordagem, em consonância com Li et al. (2020) [Li et al. 2020], propicia uma avaliação holística das vulnerabilidades, permitindo identificar interações entre camadas e propor estratégias de mitigação coordenadas. Tal integração é crucial para aplicações críticas, nas quais a falha em uma camada compromete a segurança e a confiabilidade de todo o sistema.

3. Metodologia

A presente pesquisa adota uma abordagem exploratória, considerando as lacunas de conhecimento identificadas sobre as vulnerabilidades de segurança em sistemas blockchain. Essa escolha metodológica fundamenta-se na natureza do problema proposto, que apresenta características abstratas e carece de informações concretas ou diretrizes estabelecidas para sua solução. O estudo parte de um campo em que as vulnerabilidades são amplamente discutidas de forma fragmentada, dificultando a construção de uma base teórica consistente que subsidie respostas práticas e direcionadas às falhas de segurança.

O problema de pesquisa destaca-se por envolver uma tecnologia emergente que, apesar de sua adoção crescente em diferentes setores, como contratos inteligentes e mecanismos de consenso, ainda apresenta desafios críticos. A complexidade advém da integração de diversos componentes tecnológicos e da multiplicidade de ataques registrados, cujas análises e soluções nem sempre são abordadas de maneira sistemática, especialmente na literatura disponível em língua portuguesa.

Para embasar a pesquisa, foi realizado um levantamento bibliográfico abrangente, buscando identificar as principais vulnerabilidades e soluções propostas na literatura acadêmica recente. A coleta foi realizada em repositórios reconhecidos, incluindo IEEE Xplore, ACM Digital Library, SBC OpenLib e Google Acadêmico. Foram utilizadas as palavras-chave “blockchain vulnerabilities”, “security in blockchain”, “smart contract attacks”, “blockchain consensus issues” e “blockchain security solutions”, que refletem os aspectos centrais do problema estudado.

4. Revisão Bibliográfica

Com os avanços tecnológicos das aplicações da blockchain, suas vulnerabilidades de segurança e nas soluções propostas têm sido amplamente investigadas na literatura [Siam et al. 2025, Zamani et al. 2020]. Este trabalho apoia-se em artigos que analisam aspectos técnicos e teóricos da tecnologia, buscando uma categorização das falhas e seus impactos.

De início, o trabalho “A Survey of Attacks on Ethereum Smart Contracts (SoK)” [Atzei et al. 2017], realiza um levantamento detalhado sobre vulnerabilidades em contratos inteligentes na rede Ethereum, focando na análise de falhas que tornam os contratos suscetíveis a ataques exploráveis. Para categorizar essas vulnerabilidades, o estudo categoriza diferentes classes, como erros de codificação, limitações na linguagem Solidity e problemas relacionados à lógica de execução descentralizada. Os autores enfatizam a necessidade urgente de ferramentas e práticas robustas para auditoria e validação de contratos inteligentes antes de sua implantação. Os pesquisadores sugerem que a mitigação de falhas depende tanto do aprimoramento das linguagens de programação, como Solidity, quanto do desenvolvimento de padrões de segurança que auxiliem os desenvolvedores na criação de contratos confiáveis.

O estudo “A Survey on Security and Privacy Issues of Bitcoin” [Conti et al. 2018] analisa os desafios de segurança e privacidade do Bitcoin, com foco no protocolo Prova de Trabalho (PoW), identificando vulnerabilidades como ataques de gastos duplos, manipulação de timestamps e centralização da mineração, que podem comprometer a estrutura descentralizada da rede. Os autores destacam que, apesar da segurança teórica do PoW, suas falhas práticas exigem aprimoramento, sugerindo mecanismos complementares de autenticação entre nós e alternativas menos centralizadas, como Prova de Participação (PoS), para reduzir riscos e equilibrar segurança e eficiência à medida que o sistema cresce em escala e complexidade.

Em “On the Security, Performance and Privacy of Proof of Work Blockchains” [Gervais et al. 2016], conduzem uma investigação aprofundada sobre a segurança, privacidade e desempenho de blockchains que utilizam o protocolo de consenso Prova de Trabalho (PoW). O estudo apresenta uma análise quantitativa inovadora, que avalia como mudanças nos parâmetros de configuração das blockchains afetam sua escalabilidade e resistência a ataques. Para isso, discutiram cenários adversos, como ataques de 51% e manipulações de taxa de hash, identificando as vulnerabilidades mais críticas enfrentadas por redes descentralizadas.

Por fim, concluem que as blockchains baseadas em PoW enfrentam um dilema intrínseco entre segurança e desempenho. Os autores sugerem que futuras implementações explorem alternativas de consenso, como Prova de Participação (PoS) e mecanismos híbridos, para mitigar as limitações observadas. Concomitantemente, o estudo recomenda o desenvolvimento de ferramentas para monitorar continuamente o desempenho e a segurança das redes, permitindo ajustes em tempo real para prevenir ataques e manter a integridade do sistema, visando contribuir para a evolução de blockchains mais seguras e eficientes, especialmente em aplicações de larga escala.

Em “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies” [Bonneau et al. 2015], apresenta uma análise abrangente sobre os desafios técnicos e econômicos enfrentados por sistemas baseados em Bitcoin e outras criptomoedas. O artigo examina a intersecção entre consenso distribuído e economia comportamental, abordando como incentivos econômicos impactam a segurança e a operação desses sistemas. Para tanto, exploram questões como sustentabilidade energética, centralização da mineração e o papel dos mecanismos de consenso em redes descentralizadas, oferecendo uma base teórica para compreender os fatores que afetam o sucesso das criptomoedas.

Na análise apresentada, destacam que o equilíbrio entre incentivos econômicos e segurança é essencial para manter a confiabilidade dos sistemas baseados em blockchain, uma vez que, em redes sem intermediários confiáveis, como o Bitcoin, o desenho de mecanismos de incentivo precisa considerar possíveis ameaças, como ataques de 51% e manipulação de ordens de transações. Assim, concluem que o sucesso de sistemas descentralizados depende da capacidade de alinhar incentivos econômicos com a segurança técnica. O artigo propõe o desenvolvimento de mecanismos mais robustos para contratos autossuficientes, como formas avançadas de consenso que incorporem elementos de governança e adaptação a cenários adversos. Além disso, enfatizam a importância de políticas que reduzam a centralização e promovam a equidade na distribuição de poder computacional como passos fundamentais para fortalecer a resiliência das criptomoedas e seus sistemas em longo prazo.

No estudo "Under-Optimized Smart Contracts Devour Your Money" [Chen et al. 2017], são investigadas ineficiências operacionais e vulnerabilidades em contratos inteligentes na Ethereum, focando em padrões de codificação inadequados. O estudo apresenta o GASPER, ferramenta projetada para identificar padrões subótimos em bytecodes, mostrando que práticas ineficientes não apenas elevam os custos de execução, mas também expõem os contratos a falhas de segurança. A análise evidencia que redundância de instruções e cálculos desnecessários aumentam drasticamente o consumo de gás, comprometendo a segurança e permitindo exploração de comportamentos inesperados.

Os autores concluem que a adoção de ferramentas como o GASPER é crucial para mitigar custos e riscos, reforçando a necessidade de diretrizes claras de codificação e boas práticas de desenvolvimento. Além disso, defendem que a conscientização sobre eficiência e segurança do código deve integrar processos de auditoria, garantindo contratos economicamente viáveis e tecnicamente seguros, passo fundamental para fortalecer a confiabilidade de contratos inteligentes em aplicações do mundo real.

Já em "Untangling Blockchain: A Data Processing View of Blockchain Systems" [Dinh et al. 2018], os autores investigam o desempenho de blockchains privadas sob a perspectiva do processamento de dados, comparando suas capacidades com sistemas tradicionais de gerenciamento de banco de dados. O estudo analisa como as características fundamentais da blockchain – imutabilidade, descentralização e transparência – afetam sua eficiência operacional por meio de experimentos detalhados, avaliando cenários de cargas de trabalho intensivas, buscando identificar os pontos fortes e as limitações das blockchains privadas em relação às tecnologias convencionais.

Em sua análise, enfatizam que a imutabilidade, embora essencial para a segurança e confiabilidade da blockchain, introduz restrições significativas ao desempenho, especialmente em operações de alta frequência e baixo tempo de resposta. Os autores discutem como a replicação de dados entre nós da rede aumenta a latência e reduz a eficiência em comparação com bancos de dados centralizados. Além disso, a transparência, uma característica desejável em muitas aplicações, pode se tornar um entrave quando o processamento em larga escala exige maior sigilo ou segmentação de dados.

Em conclusão, Dinh et al. (2018) argumentam que o equilíbrio entre segurança e desempenho é um desafio central para a adoção de blockchains privadas em cenários práticos, sugerindo que o uso de blockchains híbridas, que combinam elementos de descentralização com características de sistemas centralizados, pode ser uma solução viável.

Por fim, os autores também recomendam o desenvolvimento de algoritmos de consenso otimizados e arquiteturas de rede flexíveis, por serem capazes de adaptar-se a diferentes tipos de cargas de trabalho, visando por meio das recomendações aumentar a eficiência das blockchains privadas, tornando-as competitivas com sistemas tradicionais em termos de desempenho, sem comprometer os princípios de segurança e transparência.

Já em "A Survey on the Security of Blockchain Systems" [Li et al. 2020], é apresentado uma revisão sistemática abrangente sobre ameaças à segurança em blockchains populares, organizando os riscos identificados de acordo com suas origens e impactos. Para tanto, exploram uma ampla gama de vulnerabilidades, incluindo falhas em mecanis-

mos de consenso, problemas em contratos inteligentes e questões de sincronização entre nós da rede. A abordagem dos autores combina uma análise teórica com casos reais de ataques, oferecendo uma visão teórica e prática dos desafios que afetam a confiabilidade e segurança das blockchains.

O estudo revela que os mecanismos de consenso, como Prova de Trabalho (PoW) e Prova de Participação (PoS), estão entre os componentes mais suscetíveis a ataques, discutindo como estratégias de ataques focadas no consenso – como ataques de 51%, manipulação de timestamps e problemas de centralização – podem comprometer a integridade das transações.

Em relação aos contratos inteligentes, o artigo destaca vulnerabilidades de reentrância e má gestão de condições, que tornam os contratos suscetíveis a exploração. Além disso, os problemas de sincronização entre nós, especialmente em redes descentralizadas de grande escala, são apresentados como barreiras significativas para a eficiência e segurança, vez que essas vulnerabilidades são frequentemente agravadas pela falta de ferramentas avançadas de análise e monitoramento, característica de tecnologias inovadoras.

Em conclusão, defendem que estratégias proativas são necessárias para mitigar os riscos identificados e fortalecer a segurança das blockchains. Como exemplo, propõem o desenvolvimento de novos protocolos de consenso que combinem resiliência contra ataques com maior eficiência energética. Paralelamente, os autores enfatizam a importância de ferramentas aprimoradas para análise e auditoria de contratos inteligentes, visando identificar e corrigir falhas antes da implantação. Finalmente, destacam a necessidade de melhorias na sincronização entre nós da rede, sugerindo arquiteturas mais robustas para lidar com os desafios de escalabilidade e descentralização.

O artigo "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" [Zheng et al. 2017] apresenta uma análise da arquitetura da blockchain, com foco em mecanismos de consenso e tendências de evolução, examinando como Prova de Trabalho (PoW), Prova de Participação (PoS) e Prova de Autoridade (PoA) lidam com escalabilidade, segurança e eficiência. Os autores destacam que o PoS reduz consumo energético, mas enfrenta concentração de riqueza, enquanto o PoA exige maior confiança entre validadores, podendo comprometer a descentralização. Concluem que a escolha do consenso deve ser adaptada a cada aplicação, sugerem modelos híbridos para mitigar desafios e ressaltam a importância de explorar aplicações emergentes, como identidade digital e cadeias de suprimento, evidenciando o potencial transformador da blockchain quando suas limitações são adequadamente abordadas.

O estudo "Making Smart Contracts Smarter" [Luu et al. 2016] analisa vulnerabilidades críticas em contratos inteligentes na Ethereum, destacando falhas como dependência de timestamps e ordenação de transações, que podem ser exploradas por mineradores ou agentes maliciosos. Os autores apresentam a ferramenta Oyente, voltada para detectar erros em tempo de execução, e ressaltam que a ausência de práticas seguras de programação e o uso de ferramentas limitadas expõem os contratos a riscos significativos. Concluem que a integração de auditorias automatizadas e verificações de segurança nos fluxos de desenvolvimento, aliada à conscientização sobre vulnerabilidades específicas do ambiente Ethereum, é essencial para prevenir perdas financeiras, fortalecer a confiabili-

dade dos contratos e promover a evolução segura da tecnologia blockchain.

De forma geral, a literatura aponta que os desafios de segurança em blockchain estão fortemente associados ao equilíbrio entre descentralização e desempenho. As vulnerabilidades em contratos inteligentes e mecanismos de consenso aparecem como os pontos mais críticos, o que evidencia a necessidade de estratégias integradas que envolvam auditoria automatizada, novos protocolos de consenso e padronização de boas práticas de desenvolvimento.

5. Categorização das Vulnerabilidades

Com base na revisão bibliográfica realizada, as vulnerabilidades da tecnologia blockchain foram organizadas em categorias específicas, considerando suas características, impactos e exemplos práticos. Essa categorização tem como objetivo sistematizar os riscos identificados, facilitar sua compreensão e propor estratégias direcionadas para mitigação.

A primeira categoria, Contratos Inteligentes, abrange falhas relacionadas à codificação e execução de contratos em plataformas, tais como: Ethereum. Essas vulnerabilidades incluem problemas como reentrância, má gestão de estados e dependência de timestamps, que permitem a exploração de inconsistências por agentes maliciosos. Um exemplo clássico é o ataque à DAO em 2016, que resultou em perdas significativas de Ether devido a uma falha de reentrância (Atzei et al., 2017; Luu et al., 2016). Além disso, padrões de codificação subótimos, tais como: redundâncias e cálculos desnecessários, também foram destacados por Chen et al. (2017), evidenciando a necessidade de boas práticas no desenvolvimento.

Os Mecanismos de Consenso foram identificados como uma das áreas mais críticas, com vulnerabilidades, tais como: ataques de 51%, manipulação de timestamps e centralização de mineração. Esses problemas podem comprometer a integridade e a descentralização das redes blockchain. Por exemplo, Conti et al. (2018) e Bonneau et al. (2015) discutem como grandes pools de mineração podem obter controle significativo sobre a rede, viabilizando ataques de 51%. Gervais et al. (2016) e Zheng et al. (2017) também destacam o dilema entre segurança e desempenho, especialmente em redes baseadas em Prova de Trabalho (PoW).

Na Arquitetura de Rede, foram identificados problemas de sincronização entre nós, ausência de autenticação robusta e desafios de escalabilidade. Bonneau et al. (2015) e Li et al. (2020) discutem como a falta de validação entre os nós facilita a inserção de agentes maliciosos. Além disso, Dinh et al. (2018) apontam que a replicação de dados e a transparência excessiva podem prejudicar o desempenho em cenários de alta carga, limitando a eficiência das blockchains em aplicações práticas.

Outra categoria relevante é a de Ferramentas e Análise, que destaca a falta de soluções robustas para auditoria e validação de contratos inteligentes antes de sua implantação. Atzei et al. (2017) e Chen et al. (2017) ressaltam a importância de ferramentas, tais como: Oyente e GASPER para identificar vulnerabilidades e otimizar a qualidade do código. Adicionalmente, Gervais et al. (2016) e Li et al. (2020) sugerem a necessidade de monitoramento contínuo para permitir ajustes em tempo real no desempenho e na segurança das redes.

A Tabela 1 apresenta as principais vulnerabilidades de segurança em sistemas

blockchain, organizadas por tipo, descrição, exemplos e referências. Essa categorização evidencia a interdependência dos riscos e reforça a necessidade de abordagens integradas para aprimorar a segurança e a confiabilidade da tecnologia.

Tabela 1. Categorização de Vulnerabilidade de Segurança da Blockchain

Categoria	Descrição	Exemplo de Ataque	Estratégias de Mitigação	Referências
Contratos Inteligentes	Falhas de codificação, reentrância, má gestão de estados e dependência de timestamps	Ataque à DAO (2016)	Adoção de ferramentas robustas de auditoria (como Oyente e GASPER). Implementação de padrões de codificação seguros e boas práticas no desenvolvimento.	Atzei et al. (2017), Luu et al. (2016), Chen et al. (2017)
	Problemas em padrões de codificação que aumentam custos de execução e introduzem vulnerabilidades	—	Uso de testes formais e auditorias de gás para prevenir ineficiências e vulnerabilidades.	Atzei et al. (2017), Chen et al. (2017)
Mecanismos de Consenso	Ataques de 51%, manipulação de timestamps, centralização de mineração e problemas de incentivo econômico	Ataque 51% no Bitcoin	Desenvolvimento de algoritmos de consenso alternativos (como PoS e modelos híbridos). Políticas para reduzir a centralização do poder computacional.	Conti et al. (2018), Bonneau et al. (2015)
	Desequilíbrio entre segurança e desempenho em redes PoW	Manipulação de taxa de hash	Busca por equilíbrio entre segurança, eficiência e descentralização. Uso de mecanismos de incentivo robustos que alinhem segurança técnica e econômica.	Gervais et al. (2016), Zheng et al. (2017)
Arquitetura de Rede	Problemas de sincronização entre nós, ausência de autenticação e validação robusta	Inserção de agentes maliciosos	Implementação de mecanismos complementares de autenticação entre nós. Desenvolvimento de arquiteturas flexíveis e robustas.	Bonneau et al. (2015), Li et al. (2020)
	Falhas de escalabilidade devido à replicação de dados e transparência excessiva	—	Uso de blockchains híbridas e técnicas de particionamento para otimizar desempenho e privacidade.	Dinh et al. (2018)
Ferramentas e Análise	Falta de ferramentas robustas para auditoria e validação de contratos antes da implantação	—	Desenvolvimento e adoção de ferramentas aprimoradas para análise e auditoria de contratos inteligentes.	Atzei et al. (2017), Chen et al. (2017)
	Necessidade de monitoramento contínuo para ajustes de desempenho e segurança	—	Monitoramento contínuo do desempenho e segurança das redes com ajustes em tempo real.	Gervais et al. (2016), Li et al. (2020)

6. Conclusão

A presente pesquisa analisou vulnerabilidades de segurança na tecnologia blockchain, consolidando uma categorização baseada em estudos fundamentais da literatura.

Os contratos inteligentes, conforme analisado por Atzei et al. (2017) e Luu et al. (2016), representam áreas sensíveis, com falhas de reentrância, má gestão de estados e dependência de timestamps sendo exploradas em ataques. A análise aponta para a necessidade de ferramentas robustas, como Oyente e GASPER, para garantir a qualidade do código antes da implantação, conforme discutido por Chen et al. (2017).

Os mecanismos de consenso também foram identificados como um ponto central de vulnerabilidade. Estudos como os de Conti et al. (2018) e Bonneau et al. (2015) destacam os riscos associados à centralização de mineração e ataques de 51%, enquanto Gervais et al. (2016) e Zheng et al. (2017) apontam para o dilema entre segurança e desempenho em redes baseadas em Prova de Trabalho (PoW). A transição para algoritmos alternativos, como Prova de Participação (PoS) e modelos híbridos, surge como uma possibilidade promissora para mitigar essas limitações.

Na arquitetura de rede, problemas de sincronização e a falta de autenticação robusta entre nós foram destacados por Bonneau et al. (2015) e Li et al. (2020) como barreiras significativas para a confiabilidade e escalabilidade. Adicionalmente, Dinh et al. (2018) argumentam que a transparência e a replicação de dados podem limitar a eficiência das blockchains em cenários práticos, especialmente em aplicações de alta carga.

A análise também apontou a importância das ferramentas e práticas de auditoria, com autores como Atzei et al. (2017) e Chen et al. (2017) enfatizando a necessidade de soluções automatizadas para identificar vulnerabilidades antes do deployment. Além disso, Gervais et al. (2016) e Li et al. (2020) sugerem que monitoramento contínuo

e arquiteturas adaptáveis são fundamentais para lidar com os desafios de segurança e desempenho em tempo real.

É importante ressaltar, contudo, que este estudo possui limitações. A categorização baseia-se em uma revisão da literatura que, apesar de abrangente, pode estar sujeita a um viés de publicação e é predominantemente focada em trabalhos de língua inglesa. Adicionalmente, a análise não incluiu uma validação prática ou empírica das vulnerabilidades e das soluções de mitigação discutidas, baseando-se inteiramente nos resultados reportados pelos estudos revisados. O rápido avanço da tecnologia blockchain também implica que novas vulnerabilidades podem ter emergido após o período de coleta desta revisão.

Conclui-se que a segurança na tecnologia blockchain é um campo dinâmico e em constante evolução, exigindo esforços colaborativos de pesquisa e desenvolvimento. A categorização realizada neste trabalho fornece uma base sólida para compreender os riscos associados e propor estratégias direcionadas para mitigá-los. Por fim, a aplicação crescente da blockchain em setores críticos, como finanças, saúde e logística, torna ainda mais urgente a necessidade de fortalecer sua segurança. Este estudo contribui para ampliar a compreensão sobre as vulnerabilidades existentes e os caminhos possíveis para garantir a confiabilidade e sustentabilidade dessa tecnologia transformadora.

7. Trabalhos Futuros

Como desdobramento deste estudo, recomenda-se a validação e o refinamento da taxonomia aqui proposta, aplicando-a a vulnerabilidades emergentes. Sugere-se um foco especial em domínios como Finanças Descentralizadas (DeFi), aplicações que recriam serviços financeiros tradicionais em blockchain, e soluções de Camada 2, que são protocolos construídos sobre a blockchain principal para melhorar a escalabilidade, áreas que não foram o foco desta revisão. Adicionalmente, uma linha de pesquisa promissora seria a análise das interdependências entre as categorias, investigando, por exemplo, como falhas de arquitetura de rede podem amplificar ataques aos mecanismos de consenso. Por fim, propõe-se uma análise comparativa de ferramentas modernas de auditoria para validar sua eficácia na detecção das falhas clássicas aqui catalogadas.

Referências

Amiet, N. (2021). Blockchain vulnerabilities in practice. *Digital Threats: Research and Practice*, 2(2):1–7.

Atzei, N., Bartoletti, M., and Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). In Maffei, M. and Ryan, M., editors, *Principles of Security and Trust*, volume 10204, pages 164–186. Springer Berlin Heidelberg, Berlin, Heidelberg. Series Title: Lecture Notes in Computer Science.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., and Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy*, pages 104–121, San Jose, CA. IEEE.

Chang, S. E. and Chen, Y. (2020). When blockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE access*, 8:62478–62494.

Chen, T., Li, X., Luo, X., and Zhang, X. (2017). Under-optimized smart contracts devour your money. In *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pages 442–446, Klagenfurt, Austria. IEEE.

Conti, M., Sandeep Kumar, E., Lal, C., and Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, 20(4):3416–3452.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., and Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, 30(7):1366–1385.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., and Capkun, S. (2016). On the Security and Performance of Proof of Work Blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 3–16, Vienna Austria. ACM.

König, L., Unger, S., Kieseberg, P., Tjoa, S., and Blockchains, J. R. C. (2020). The risks of the blockchain a review on current vulnerabilities and attacks. *J. Internet Serv. Inf. Secur.*, 10(3):110–127.

Li, X., Jiang, P., Chen, T., Luo, X., and Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107:841–853.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., and Hobor, A. (2016). Making Smart Contracts Smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 254–269, Vienna Austria. ACM.

Moosavi, J., Naeni, L. M., Fathollahi-Fard, A. M., and Fiore, U. (2021). Blockchain in supply chain management: a review, bibliometric, and network analysis. *Environmental Science and Pollution Research*, pages 1–15.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Available at SSRN 3440802*.

Poston, H. (2020). Mapping the owasp top ten to blockchain. *Procedia Computer Science*, 177:613–617. The 11th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2020) / The 10th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2020) / Affiliated Workshops.

Siam, M. K., Saha, B., Hasan, M. M., Hossain Faruk, M. J., Anjum, N., Tahora, S., Siddika, A., and Shahriar, H. (2025). Securing decentralized ecosystems: A comprehensive systematic review of blockchain vulnerabilities, attacks, and countermeasures and mitigation strategies. *Future Internet*, 17(4).

Zamani, E., He, Y., and Phillips, M. (2020). On the security risks of the blockchain. *Journal of Computer Information Systems*, 60(6):495–506.

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 557–564, Honolulu, HI, USA. IEEE.