DESENVOLVIMENTO DE UM SOFTWARE DE DENÚNCIA ANÔNIMA COM BLOCKCHAIN

Renata Sousa da Silva[1]

Julio Cesar Carou Felix de Lima[2]

Olinda Nogueira Paes Rizzo[3]

Resumo

Introdução

A denúncia de irregularidades é um instrumento essencial para assegurar a transparência, a ética e a responsabilidade em organizações públicas e privadas. Em diferentes contextos, esses canais de comunicação funcionam como mecanismos de controle social, permitindo que casos de assédio, corrupção, fraudes e má conduta sejam identificados e tratados de forma adequada (Rodrigues, 2009). No entanto, apesar da relevância desse instrumento, a confidencialidade e a segurança do denunciante ainda representam grandes desafios. Pesquisas apontam que, em muitos casos, o medo de retaliações e a desconfiança em relação à proteção de dados desestimulam a participação ativa da sociedade em canais formais de denúncia (ABNT, 2011).

De acordo com dados da Association of Certified Fraud Examiners (ACFE, 2022), aproximadamente 42% dos casos de fraude corporativa no mundo são descobertos por meio de denúncias internas ou externas. Entretanto, a efetividade desses canais depende diretamente da confiança dos usuários na integridade do sistema, especialmente em relação ao sigilo das informações fornecidas. No Brasil, casos amplamente divulgados de irregularidades em instituições públicas e privadas reforçam a necessidade de soluções tecnológicas que assegurem o anonimato do denunciante e a inviolabilidade dos registros.

Nesse cenário, tecnologias emergentes vêm sendo avaliadas como alternativas para aprimorar a gestão de informações sensíveis. Entre elas, o blockchain tem se destacado por sua arquitetura de registro distribuído, imutável e verificável, que elimina a necessidade de uma autoridade central e garante maior confiabilidade aos processos (Narayanan et al., 2016). Cada transação registrada em blockchain é permanentemente validada por meio de algoritmos criptográficos, o que impossibilita sua alteração posterior (Tanenbaum; Wetherall, 2011). Essa característica oferece grande potencial de aplicação em sistemas de denúncia, assegurando que informações não sejam adulteradas após o envio e protegendo a identidade do denunciante (Muller; Saffaro, 2011). Além da questão técnica, a adoção de blockchain em softwares de denúncia também possui impacto social relevante. A possibilidade de integrar anonimato, rastreabilidade e integridade da informação contribui não apenas para a proteção do denunciante, mas também para o fortalecimento da confiança da sociedade nos mecanismos de controle. Dessa forma, organizações públicas e privadas podem se beneficiar de soluções mais transparentes, seguras e auditáveis, ampliando a efetividade das medidas de prevenção e combate a irregularidades (Petrobras, 2007). Este estudo apresenta uma proposta de software de denúncia anônima baseado em tecnologia blockchain, que busca conciliar anonimato, segurança e confiabilidade no registro de denúncias. Trata-se de um estudo exploratório com proposta de solução tecnológica, cujo objetivo é fornecer subsídios conceituais para futuras implementações práticas. A pesquisa pretende demonstrar que o uso de registros distribuídos e imutáveis pode reduzir significativamente os riscos de adulteração de dados,

[1]Graduanda em Engenharia de Software da Universidade Santo Amaro, SP. E-mail: lrenata2y@estudante.unisa.br.
[2] Professor Mestre, Universidade Santo Amaro, SP. E-mail: jclima@prof.unisa.br.
[3] Professora Mestra, Universidade Santo Amaro, SP. E-mail: orizzo@prof.unisa.br.

ao mesmo tempo em que garante proteção ao denunciante. Por fim, a estrutura deste trabalho está organizada da seguinte forma: após esta introdução, apresenta-se os objetivos gerais e específicos; em seguida, descreve-se a metodologia utilizada; posteriormente, discute-se o desenvolvimento da proposta tecnológica; por fim, são apresentados os resultados, a discussão e as conclusões.

Objetivo

Objetivo Geral

Desenvolver uma proposta de software de denúncia anônima utilizando tecnologia blockchain, que assegure segurança, integridade e confidencialidade das informações registradas.

Objetivos Específicos

- Analisar sistemas existentes de denúncia anônima e identificar lacunas relacionadas à segurança e ao anonimato;
- Investigar arquiteturas de blockchain adequadas para implementação em sistemas de registro de denúncias;
- Propor um modelo conceitual de software que integre blockchain para armazenamento seguro e imutável das informações;
- Elaborar fluxogramas, diagramas e representações gráficas que ilustrem a operação do sistema, atribuindo clareza às etapas de funcionamento; Avaliar, de forma conceitual, os benefícios do uso da tecnologia em relação à confiabilidade e à proteção do denunciante;
- Discutir as contribuições e limitações do modelo proposto, relacionando-o a pesquisas e práticas já existentes na área de segurança da informação.

Metodologia

A pesquisa caracteriza-se como estudo exploratório, de natureza qualitativa, com desenvolvimento de uma proposta de solução tecnológica. O objetivo principal é avaliar conceitualmente a viabilidade de integrar a tecnologia blockchain em sistemas de denúncia anônima, a fim de garantir segurança, anonimato e integridade dos registros O procedimento metodológico foi estruturado em três etapas principais: **Levantamento bibliográfico**: Realizou-se uma busca sistemática de referências em bases acadêmicas e científicas, incluindo Google Scholar, SciELO, IEEE Xplore e o Portal de Periódicos da CAPES. As palavras-chave utilizadas foram: anonymous reporting, whistleblowing systems, blockchain security, denúncia anônima e segurança da informação. Critérios de inclusão: trabalhos publicados entre 2010 e 2025, em português e inglês, que abordassem diretamente tecnologias de segurança da informação, blockchain e mecanismos de denúncia. Critérios de exclusão: fontes sem revisão por pares, materiais opinativos ou sem relação direta com o problema de pesquisa. Processo de seleção: em uma primeira triagem, foram analisados título, resumo e palavras-chave. Em seguida, os trabalhos mais relevantes foram lidos integralmente, resultando em um conjunto de obras que fundamentaram a análise conceitual. Essa etapa permitiu identificar as lacunas nos sistemas tradicionais de denúncia e reconhecer as contribuições potenciais da tecnologia blockchain para solucionar tais fragilidades. **Análise de arquiteturas de blockchain**: Após o levantamento bibliográfico, foram comparadas as principais arquiteturas de blockchain — públicas, privadas e permissionadas. A análise considerou critérios como segurança, escalabilidade, custo de implementação e confiabilidade, destacando ferramentas já consolidadas, como o Hyperledger Fabric. Essa avaliação embasou a escolha do modelo conceitual mais adequado para aplicação em softwares de denúncia anônima. **Desenvolvimento conceitual do software:** Com base nas referências teóricas e nas análises realizadas, elaborou-se uma proposta de arquitetura para o sistema, dividida em três camadas: 1. Interface do usuário: ambiente digital para envio das denúncias de forma anônima. 2. Camada de aplicação: responsável por validação, criptografia e encaminhamento

das informações. 3. Camada de blockchain: destinada ao registro imutável dos dados e auditoria dos registros. Foram produzidos fluxogramas e quadros que ilustram o funcionamento do sistema, incluindo etapas de registro, criptografia, armazenamento e auditoria. O desenvolvimento manteve foco conceitual, sem testes empíricos de campo, mas com simulações teóricas que permitem avaliar a viabilidade da proposta.

Resultado e Discussão

A proposta de software de denúncia anônima com blockchain foi analisada de forma conceitual, considerando segurança, integridade, anonimato e escalabilidade. Não houve coleta de dados empíricos de campo, mas foram realizadas simulações teóricas e comparações com sistemas tradicionais de denúncia.

Comparação com Sistemas Tradicionais

O Quadro 2 compara as características essenciais entre sistemas tradicionais (baseados em BD centralizado) e o modelo proposto baseado em blockchain, destacando diferenças em integridade, anonimato, transparência, risco de fraude, escalabilidade e custos.

Quadro 2: Comparação entre sistemas tradicionais e sistema proposto (blockchain).

	Sistemas tradicionais	Sistema proposto (Blockchain)
Integridade dos dados	Vulnerável a alterações	Imutável após o registro
Confidencialidade	Depende de políticas internas	Criptografia e anonimato garantidos
Transparência	Limitada, auditoria interna	Auditável com registro garantido
Risco de fraude	Alto, dados podem ser manipulados	Baixo, hash e validação distribuída
Escalabilidade	Depende do servidor central	Alta, Blockchain distribuído
Custos de manutenção	Moderados	Inicialmente alto, mas menor a longo prazo

Fonte: Autor (2025)

Observa-se que o sistema baseado em blockchain apresenta vantagens significativas, principalmente na integridade das denúncias, garantindo que o conteúdo não seja alterado após o registro (ver quadro 2).

Simulação Conceitual de Segurança

Para avaliar a robustez da plataforma, foram consideradas três categorias de ataques comuns a sistemas de denúncias: 1. Alteração de registros: impossibilitada pelo uso de blockchain com hash criptográfico; 2. Rastreamento do denunciante: mitigado por endereços criptográficos e anonimização de metadados; 3. Invasão de servidores: risco reduzido pela natureza distribuída da rede blockchain, que não possui ponto central de falha. A Figura 2 ilustra o processo de segurança implementado no software proposto, demonstrando de forma visual como a tecnologia blockchain atua na proteção das informações. O diagrama representa as etapas da denúncia, desde o envioanônimo pelo usuário até o bloqueio de ataques externos, evidenciando os mecanismos de criptografia, registro imutável e validação dis-

tribuída que asseguram a integridade e a confidencialidade dos dados. Essa simulação teórica reforça a robustez do sistema frente a tentativas convencionais de invasão ou manipulação de registros.

Figura 2 – Simulação de Segurança do Sistema,Fonte: Autor, 2025

Análise de Desempenho

Embora sistemas centralizados possuam alta velocidade em pequenas cargas, eles apresentam limitações quanto à confiabilidade e transparência. O blockchain distribuído, embora ligeiramente mais lento, garante rastreamento, auditoria e integridade em escala global. O Gráfico 1 apresenta uma comparação conceitual entre o desempenho de sistemas tradicionais e o modelo proposto baseado em blockchain. A análise considera três variáveis principais, tempo médio de registro, integridade e transparência, evidenciando o equilíbrio entre desempenho e segurança. Embora o sistema blockchain apresente um tempo de processamento ligeiramente superior, observa-se ganho expressivo em integridade e transparência, o que reforça sua adequação para o registro de denúncias sensíveis. Essa visualização contribui para compreender que o aumento de confiabilidade compensa as limitações de velocidade, justificando o uso da tecnologia em contextos que demandam alto nível de proteção e rastreabilidade.

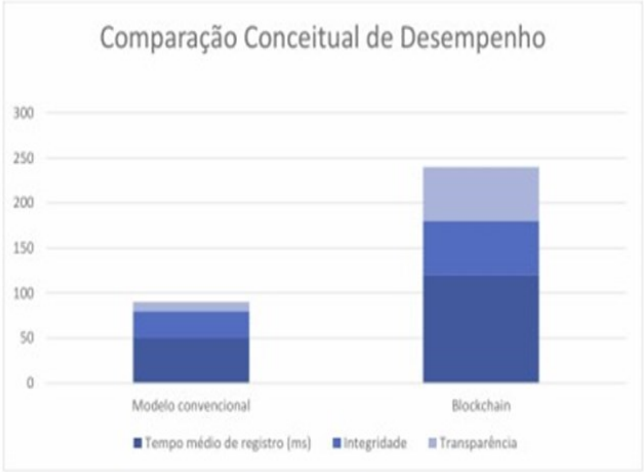

Gráfico 1 – Comparação Conceitual de Desempenho,Fonte: Autor, 2025.

Observa-se que (ver Gráfico 1) mesmo com maior tempo de registro, o ganho em segurança e integridade supera as limitações de desempenho, sendo adequado para denúncias sensíveis.

Comparação com Sistemas Tradicionais

Ao comparar o modelo proposto com sistemas de denúncia baseados em bancos de dados centralizados, verificam-se avanços significativos: Integridade: enquanto sistemas tradicionais são vulneráveis a alterações, o blockchain assegura imutabilidade. Anonimato: nos modelos convencionais, a confidencialidade depende de políticas internas; no proposto, a criptografia e endereços anônimos garantem maior proteção. Transparência: a auditoria distribuída elimina a necessidade de confiança em intermediários.
Escalabilidade: a arquitetura distribuída do blockchain permite expansão sem comprometer a integridade dos dados.

Valor da Pesquisa e Lacunas Preenchidas

O presente estudo contribui para preencher lacunas identificadas em pesquisas anteriores sobre sistemas de denúncia: Segurança: muitos canais ainda operam em servidores centralizados, vulneráveis a ataques e manipulações internas. A proposta com blockchain elimina pontos únicos de falha.

Escalabilidade: enquanto soluções tradicionais enfrentam limitações de capacidade e custos crescentes, o modelo distribuído permite crescimento sustentável. Confiança social: a maior barreira à efetividade das denúncias é a desconfiança dos usuários quanto à proteção de sua identidade (Rodrigues, 2009).

O uso do blockchain, por sua natureza transparente e auditável, fortalece a confiança da sociedade nos canais de denúncia. Assim, a pesquisa não apenas apresenta uma proposta tecnológica inovadora, mas também avança na discussão acadêmica sobre segurança da informação aplicada à cidadania digital, demonstrando que soluções baseadas em blockchain podem contribuir para ampliar a efetividade de mecanismos de controle e participação social.

Considerações Finais

O presente estudo exploratório apresentou e discutiu uma proposta de software de denúncia anônima com suporte em tecnologia blockchain, evidenciando que é possível conciliar três dimensões essenciais: anonimato do denunciante, integridade dos registros, e transparência no gerenciamento das informações.

Os resultados indicam que a solução proposta supera as limitações de sistemas tradicionais, ao oferecer maior proteção contra adulterações, rastreabilidade confiável e auditoria permanente. Dessa forma, constitui-se em uma alternativa tecnológica segura e confiável para organizações públicas e privadas que necessitam gerir denúncias de forma ética e transparente.

A pesquisa reforça a relevância da aplicação de tecnologias distribuídas em contextos que demandam alto nível de confiabilidade, como os canais de denúncia de irregularidades. Além disso, aponta caminhos para estudos futuros, como: Realização de testes de campo para validar a aceitação e usabilidade do sistema, a coleta de feedback de usuários para aperfeiçoamento da plataforma, e a integração com inteligência artificial, permitindo a priorização automática das denúncias conforme critérios de gravidade e relevância.

Assim, este trabalho contribui tanto para o avanço da discussão acadêmica quanto para a proposição de soluções práticas voltadas à proteção do denunciante e à consolidação da confiança social nos mecanismos de participação e controle.

Palavras-chave

Denúncia anônima; Blockchain; Segurança da informação; integridade de dados; Tecnologia aplicada.

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6023: Informação e documentação – Referências – Elaboração. Rio de Janeiro, 2018.

MULLER, R.; SAFFARO, R. Segurança da Informação em Sistemas Distribuídos. São Paulo: Atlas, 2011.

NARAYANAN, A. et al. Bitcoin and Blockchain Technology. Princeton: Princeton University Press, 2016.

PETROBRAS. Manual de Ética e Conduta. Rio de Janeiro: Petrobras, 2007. Disponível em: https://transparencia.petrobras.com.br/etica. Acesso em: 28 set. 2025.

RODRIGUES, J. Transparência e Ética Organizacional. São Paulo: Saraiva, 2009.

SÃO PAULO (Estado). Lei n.º 8.209, de 4 de março de 1993. Dispõe sobre o Programa Estadual de Defesa do Usuário do Serviço Público. Diário Oficial do Estado de São Paulo, São Paulo, 5 mar. 1993. Disponível em: https://www.al.sp.gov.br/. Acesso em: 28 set. 2025.

TANENBAUM, A.; WETHERALL, D. Redes de Computadores. 5. ed. Rio de Janeiro: Elsevier, 2011.

ASSOCIATION OF CERTIFIED FRAUD EXA-

MINERS (ACFE). Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse. Austin, TX: ACFE, 2022. Disponível em: https://www.acfe.com/report-to-the-nations/2022/. Acesso em: 28 set. 2025