

Comparação Empírica entre Mecanismos Centralizados e Descentralizados de Autenticação

Douglas V. Fernandes¹

¹Instituto de Ciências Exatas e Informática (ICEI) – Pontifícia Universidade Católica de Minas Gerais (PUC-MINAS)
Av. Brasil, 2023 – Savassi – Belo Horizonte — 30140-008

Abstract. This research presents an empirical and comparative study between authentication mechanisms based on blockchain technology and traditional centralized models. The objective is to evaluate, based on evidence reported in the literature, the effectiveness, limitations, and adoption barriers associated with decentralized authentication systems, considering key Software Engineering dimensions such as security, performance, usability, and operational feasibility. Through the analysis of scientific publications and previously reported experimental results, the study identifies objective criteria for comparing both models and synthesizes the main trade-offs involved. The expected contribution is the development of a comparative matrix and a set of engineering-oriented guidelines to support professionals and researchers in planning, selecting, and implementing secure, auditable, and scalable authentication solutions in distributed architectures.

Resumo. Esta pesquisa realiza um estudo empírico e comparativo entre mecanismos de autenticação baseados em tecnologia blockchain e modelos centralizados tradicionais. O objetivo é avaliar, com base em evidências presentes na literatura, a eficácia, as limitações e as barreiras de adoção associadas aos sistemas descentralizados, considerando dimensões fundamentais da Engenharia de Software, como segurança, desempenho, usabilidade e operacionalidade. A partir da análise de artigos científicos e de resultados experimentais previamente publicados, são identificados critérios objetivos para comparação entre os dois modelos e sintetizados os principais trade-offs observados. A contribuição esperada consiste na elaboração de uma matriz comparativa e de um conjunto de diretrizes orientadas à engenharia, capazes de apoiar profissionais e pesquisadores no planejamento, seleção e desenvolvimento de soluções de autenticação seguras, auditáveis e escaláveis em arquiteturas distribuídas.

Bacharelado em Engenharia de Software - PUC Minas
Trabalho de Conclusão de Curso (TCC)

Orientador de conteúdo (TCC I): Danilo Maia - dqmf88@yahoo.com.br
Orientador de conteúdo (TCC I): Leonardo Vilela - leonardocardoso@pucminas.br
Orientador de conteúdo (TCC I): Raphael Ramos - rrdcostasi@gmail.com
Orientador acadêmico (TCC I): Cleiton Tavares - cleitonvaires@pucminas.br
Orientador do TCC II: (A ser definido no próximo semestre)

Belo Horizonte, 27 de Setembro de 2025.

1. Introdução

Os sistemas de autenticação digital desempenham um papel essencial na proteção de dados e serviços online. Entretanto, mecanismos amplamente utilizados, como OAuth 2.0, OpenID Connect e autenticação baseada em senhas ou TOTP (Time-based One-Time Password – senhas únicas baseadas em tempo), dependem de provedores centralizados para validar identidades. Essa centralização cria limitações recorrentes, tais como pontos únicos de falha, riscos aumentados de comprometimento do servidor, baixa auditabilidade e reduzida autonomia do usuário sobre seus próprios dados (Zhang, Wang Yang, 2019). Em um cenário de aplicações distribuídas e requisitos crescentes de segurança e privacidade, essas vulnerabilidades têm motivado a busca por modelos alternativos.

Nesse contexto, soluções baseadas em *blockchain* têm sido investigadas como uma possível resposta aos desafios da autenticação tradicional. Por meio de contratos inteligentes, provas criptográficas, armazenamento distribuído e propriedades inerentes de imutabilidade e transparência, diferentes trabalhos propõem abordagens que eliminam a necessidade de um verificador centralizado, ampliando a auditabilidade e garantindo maior soberania ao usuário sobre suas credenciais (Kaneriya Patel, 2023). Apesar do potencial técnico, estudos também indicam que a adoção prática de *blockchain* não é trivial: fatores como desempenho, custos operacionais, complexidade de integração e maturidade tecnológica influenciam diretamente sua viabilidade (Li et al., 2023).

Apesar do avanço dessas propostas, identifica-se uma lacuna evidente na literatura: não há estudos comparativos sistemáticos, baseados em evidências empíricas, que confrontem mecanismos tradicionais de autenticação e modelos descentralizados baseados em *blockchain*. A maior parte dos trabalhos descreve soluções isoladas, sem compará-las diretamente quanto a aspectos essenciais como segurança, desempenho e auditabilidade. Como consequência, permanece incerto em que medida a descentralização realmente oferece vantagens concretas ou em quais contextos técnicos e organizacionais seu uso se justifica. Essa ausência de sínteses comparativas dificulta a adoção informada de novas arquiteturas e reforça a necessidade de análises estruturadas que integrem resultados dispersos na literatura.

Diante dessa lacuna, este trabalho conduz um estudo empírico e comparativo, fundamentado na análise documental de métricas reportadas em artigos científicos recentes. Com base nas evidências disponíveis e nas limitações identificadas na literatura, surge a necessidade de compreender se, de fato, a descentralização oferece vantagens concretas sobre os modelos tradicionais. Assim, este estudo se orienta pela seguinte questão de pesquisa: *em que medida mecanismos de autenticação baseados em blockchain superam ou complementam modelos centralizados no que diz respeito à segurança, ao desempenho e à auditabilidade/operacionalidade?*

Essa análise possibilita compreender os *trade-offs* envolvidos na adoção de *blockchain* para autenticação, oferecendo uma síntese crítica baseada em resultados empíricos reais.

Portanto, o objetivo geral deste estudo é comparar, com base em evidências empíricas publicadas, mecanismos de autenticação tradicionais e modelos descentralizados baseados em blockchain, identificando benefícios, limitações e condições de adoção.

Os objetivos específicos são:

- Identificar e organizar métricas empíricas reportadas na literatura sobre mecanismos de autenticação tradicionais e descentralizados.
- Construir uma matriz comparativa com base nessas métricas, contemplando segurança, desempenho e auditabilidade.
- Analisar criticamente os *trade-offs* entre os dois modelos, destacando vantagens e limitações observadas.
- Sintetizar diretrizes de Engenharia de Software que auxiliem na compreensão das condições de adoção prática da autenticação baseada em *blockchain*.

Como contribuição, este trabalho oferece um panorama comparativo estruturado que auxilia pesquisadores e profissionais a compreenderem quando a tecnologia *blockchain* apresenta ganhos reais e quais barreiras ainda impedem sua adoção ampla em processos de autenticação. A análise, orientada por evidências e princípios de Engenharia de Software, busca esclarecer por que a descentralização ainda não é uma solução trivial ou generalizada, apesar de seu potencial técnico.

2. Trabalhos Relacionados

Os estudos sobre autenticação com *blockchain* têm avançado em diferentes direções, oferecendo implementações práticas que permitem comparar seus benefícios com modelos tradicionais. Zhang, Wang e Yang (2019) apresentam um protocolo de autenticação baseado em senhas descartáveis (*One-Time Passwords*) no qual a própria rede *blockchain* atua como verificador das credenciais. O estudo fornece medições de latência e resistência a ataques de falsificação e força bruta, constituindo uma das poucas propostas com resultados quantitativos que permitem comparação direta com mecanismos centralizados.

Kaneriya e Patel (2023) propõem um sistema descentralizado de verificação de credenciais educacionais utilizando Ethereum, *smart contracts* e IPFS. Sua arquitetura enfatiza privacidade, auditabilidade e autonomia do usuário, e o protótipo foi avaliado experimentalmente, apresentando melhorias de confiabilidade e mitigação de pontos únicos de falha. Esse estudo contribui para o presente trabalho por demonstrar, de forma prática, como a descentralização pode impactar diretamente a segurança e a governança dos dados autenticados.

Jaffal, Cardoso e Bussador (2024) exploram mecanismos de autenticação no contexto da Web 3.0, discutindo modelos descentralizados, carteiras digitais e mecanismos criptográficos aplicados à verificação de identidade. Embora de caráter mais conceitual, o estudo fornece uma sistematização das abordagens contemporâneas de autenticação descentralizada, permitindo situar tecnologias emergentes no panorama atual.

Complementando os aspectos técnicos, Li et al. (2023) investigam a adoção prática de soluções baseadas em blockchain por meio do modelo BOSE-HAP, desenvolvido e avaliado com usuários em um ambiente educacional real. Os resultados evidenciam que fatores como complexidade tecnológica, experiência do usuário e infraestrutura institucional influenciam diretamente a viabilidade de sistemas descentralizados, sugerindo que abordagens de autenticação com blockchain dependem não apenas da robustez técnica, mas também de sua operacionalidade.

No âmbito da autenticação tradicional, o estudo de Fett, Küsters e Schmitz (2016) representa uma das análises formais mais abrangentes sobre o OAuth 2.0, revelando vulnerabilidades estruturais decorrentes da centralização. Entre as falhas identificadas estão ataques de *redirect*, confusão de provedores (*mix-up attacks*), substituição de tokens e comprometimento sistêmico quando o servidor de identidade é violado. Essas vulnerabilidades demonstram que modelos centralizados dependem de confiança absoluta no provedor de identidade, constituindo um ponto único de falha, o que é uma característica ausente nas arquiteturas distribuídas baseadas em blockchain.

De maneira geral, os trabalhos analisados revelam duas tendências: (i) modelos descentralizados têm demonstrado avanços técnicos e melhorias em auditabilidade, mitigação de falhas centrais e autonomia do usuário; e (ii) modelos tradicionais apresentam fragilidades inerentes à centralização, embora ainda ofereçam desempenho superior e ampla compatibilidade. Assim, a presente pesquisa se diferencia ao realizar uma análise comparativa estruturada entre esses dois paradigmas, com base em métricas empíricas reportadas na literatura, buscando compreender de forma objetiva os *trade-offs* que orientam a adoção da autenticação baseada em *blockchain*.

3. Metodologia

A metodologia adotada neste estudo foi projetada para garantir rigor científico, reproduzibilidade e coerência com referências metodológicas consolidadas na Engenharia de Software. O objetivo central é comparar mecanismos de autenticação centralizados e descentralizados com base exclusivamente em evidências empíricas publicadas, evitando qualquer inferência não suportada pelos dados. Para isso, o estudo foi dividido em quatro etapas principais: (i) definição e caracterização dos materiais analisados; (ii) extração sistemática das métricas relevantes; (iii) normalização qualitativa dos dados; e (iv) síntese analítica por meio de matriz comparativa. No TCC I, essas etapas foram planejadas e formalizadas; no TCC II, serão executadas integralmente.

3.1. Materiais

Os materiais utilizados consistem em nove artigos científicos selecionados por relevância direta à temática de autenticação, *blockchain*, segurança, desempenho e Engenharia de Software. A seleção levou em conta três critérios: (i) publicação em veículos acadêmicos reconhecidos (IEEE, ACM, SBC); (ii) apresentação explícita de dados empíricos ou análises formais; e (iii) contribuição direta para pelo menos uma das dimensões avaliativas definidas neste estudo.

Além de servirem como base para a fundamentação teórica, esses estudos constituem o *corpus* analítico do TCC II. Cada material foi examinado em profundidade para identificar métricas, modelos, arquiteturas e cenários experimentais relevantes. No TCC II, esse corpus será novamente validado e poderá ser estendido caso surjam novas publicações pertinentes.

3.2. Tipo de pesquisa

O estudo é classificado como um **estudo empírico documental comparativo**. A natureza empírica decorre do uso exclusivo de dados reportados em experimentos, análises formais, testes de desempenho e estudos de caso publicados na literatura primária. Trata-se de uma pesquisa **documental**, pois toda a análise é baseada em evidências extraídas

diretamente de artigos científicos revisados por pares, sem realização de experimentos próprios. Além disso, possui caráter **comparativo**, pois confronta dois paradigmas tecnológicos distintos: mecanismos de autenticação centralizados (como OAuth 2.0) e mecanismos baseados em *blockchain*, com base em métricas e resultados reportados.

Esse delineamento foi escolhido por três motivos principais:

1. A literatura sobre autenticação descentralizada é predominantemente composta por estudos experimentais isolados, o que inviabiliza conclusões consolidadas sem uma comparação estruturada.
2. Os artigos selecionados apresentam métricas empíricas robustas (latência, custos de verificação, vulnerabilidades, *throughput*, consumo computacional, modelos formais de segurança), permitindo análise documental rigorosa.
3. O objetivo central da pesquisa é sintetizar padrões, contrastes e *trade-offs* entre os dois paradigmas tecnológicos, exigindo comparação sistemática das evidências disponíveis.

Dessa forma, o estudo se enquadra em diretrizes contemporâneas de pesquisas empíricas em Engenharia de Software, especialmente no contexto de avaliação de tecnologias emergentes com múltiplas dimensões analíticas.

Tabela 1. Corpus de Estudos Incluídos na Comparação

Artigo	Evidências Empíricas Extraídas
Fett et al. (OAuth 2.0)	Modelo formal de segurança; vulnerabilidades estruturais; ataques documentados; ausência de auditabilidade distribuída.
Zhang et al. (2019)	Latência de geração e verificação OTP na <i>blockchain</i> ; resistência a ataques de força bruta e falsificação; estrutura do consenso.
Kaneriya & Patel (2023)	Tempo de emissão e verificação de credenciais; latência de recuperação IPFS; custo de transação; segurança via árvore de Merkle; auditoria descentralizada.
Jaffal et al. (2024)	Comparação funcional entre autenticação Web 2.0 e Web 3.0; impacto na autonomia do usuário; implicações de confiança distribuída.
Li et al. (2023)	Barreiras técnicas e organizacionais para adoção; evidências qualitativas com 112 participantes; impacto em usabilidade e viabilidade.
Kassab et al. (2021)	Competências técnicas requeridas para desenvolvimento com <i>blockchain</i> ; impacto na complexidade de adoção.
Mazeli (2022)	Requisitos de privacidade e conformidade no desenvolvimento; impacto em decisões arquiteturais.
Fatima et al. (2025)	Estruturas de KPIs aplicáveis a sistemas auditáveis.
Ahmed et al. (2022)	Estimativas de esforço em projetos <i>blockchain</i> ; medição de produtividade.

3.3. Protocolo de Extração de Dados

A extração seguiu um protocolo sistemático composto por quatro passos:

1. Identificação das métricas publicadas: foram mapeadas métricas como latência, segurança, verificabilidade, custos, *throughput* e estrutura de ataque, sempre conforme definidas pelos autores originais.
2. Leitura dirigida das seções experimentais: cada artigo foi analisado especificamente nas seções de resultados, análise de desempenho, segurança e validações, com foco exclusivo nas evidências empíricas.
3. Registro em planilha padronizada: cada métrica recebeu um identificador, unidade de medida, sistema avaliado (centralizado ou *blockchain*) e contexto experimental (rede pública, privada ou ambiente simulado).
4. Validação do dado extraído: cada métrica foi verificada em múltiplas partes do artigo (texto, tabelas, gráficos, pseudocódigo), evitando interpretações livres ou extrapolações não suportadas.

Para evitar vieses, apenas valores explicitamente reportados foram utilizados — nenhum cálculo derivado ou interpolação foi realizado com base em dados incompletos.

3.4. Métricas Extraídas

As métricas foram agrupadas em quatro dimensões avaliativas, alinhadas com os objetivos do estudo e com a literatura analisada: segurança, desempenho, auditabilidade e adoção/operacionalidade.

3.4.1. Segurança

Nesta dimensão, foram considerados:

- **OAuth 2.0 e modelos centralizados:** vulnerabilidades a *mix-up attacks*, substituição de *tokens*, *open redirect* e falhas estruturais de confiança, documentadas por Fett et al.
- **Modelos baseados em blockchain:** validação via árvore de Merkle (Kaneriya & Patel), assinaturas distribuídas, uso de consenso para evitar ponto único de falha e resistência a ataques de repetição e falsificação em esquemas OTP (Zhang et al.).

Além das vulnerabilidades explícitas, também foram catalogadas as garantias formais de segurança quando presentes, como modelos de prova, análises formais ou demonstrações de impossibilidade de certos ataques em determinadas configurações.

3.4.2. Desempenho

Na dimensão de desempenho, foram analisadas métricas como:

- **Geração de OTP em blockchain:** Zhang et al. reportam latência média de autenticação inferior a 150 ms em rede privada, considerando o tempo de construção e verificação dos desafios criptográficos.

- *Verificação de credenciais descentralizadas*: Kaneriya & Patel reportam aproximadamente 1 s em média para verificação completa em rede Ethereum, incluindo recuperação de dados no IPFS e validação de provas de Merkle.
- *OAuth 2.0 e modelos centralizados*: diversos estudos e relatórios técnicos indicam valores médios de 5–50 ms por autenticação, dependendo da infraestrutura do provedor de identidade (IdP) e da proximidade de rede entre cliente e servidor.

Embora esses valores não sejam diretamente comparáveis em termos absolutos, eles permitem identificar padrões de ordem de grandeza: modelos centralizados tendem a operar com latência menor, enquanto modelos baseados em *blockchain* mostram maior custo na fase de emissão, mas desempenho aceitável na verificação em cenários específicos.

3.4.3. Auditabilidade

Na dimensão de auditabilidade, foram avaliados:

- **Modelos centralizados**: presença de logs internos controlados pelo IdP, com possibilidade de alteração, ausência de trilhas verificáveis por terceiros e dependência de confiança institucional (Fett et al.).
- **Modelos em blockchain**: existência de trilhas imutáveis de eventos, verificabilidade pública ou entre participantes autorizados, uso de provas de inclusão (como árvores de Merkle em Kaneriya & Patel) e capacidade de reconstruir o histórico de autenticações sem depender de um único operador.

Essa dimensão é particularmente relevante em contextos regulados, onde a prova de que um evento ocorreu, e não foi adulterado, é tão importante quanto a autenticação em si.

3.4.4. Adoção e Operacionalidade

Por fim, foram consideradas métricas e evidências relacionadas à adoção prática e operacionalidade:

- Complexidade técnica: Kassab et al. mostram que soluções com *blockchain* exigem competências específicas em criptografia, arquitetura distribuída e segurança, o que eleva a barreira de entrada de equipes tradicionais.
- Barreiras organizacionais: Li et al. apontam que fatores como aceitação institucional, infraestrutura existente, percepção de risco e curva de aprendizado influenciam diretamente a adoção de soluções descentralizadas, mesmo quando tecnicamente viáveis.

Esses achados reforçam que a escolha entre modelos centralizados e descentralizados não é apenas técnica, mas envolve aspectos humanos, organizacionais e econômicos.

3.5. Normalização dos Dados

Como os artigos apresentam métricas produzidas em ambientes distintos, foi aplicada uma normalização qualitativa baseada em três parâmetros principais:

- Contexto experimental: classificação dos ambientes como rede privada, rede pública, emulador ou ambiente real em produção.
- Unidade de medida: padronização textual das unidades (por exemplo, latência em milissegundos, custos em unidades monetárias, *throughput* em transações por segundo).
- Natureza da métrica: distinção entre métricas quantitativas (como tempo, custo, número de ataques) e métricas qualitativas (como presença ou ausência de determinado tipo de vulnerabilidade, existência de trilha auditável).

Nenhum dado foi padronizado numericamente (por exemplo, por meio de escalas normalizadas), de modo a evitar distorções decorrentes de contextos experimentais muito distintos. Em vez disso, as métricas foram organizadas de forma a permitir comparações relativas e identificação de padrões.

3.6. Matriz Comparativa Final

A Tabela 2 sintetiza as evidências extraídas, organizando-as em uma matriz comparativa que contrasta diretamente modelos centralizados e baseados em *blockchain* nas quatro dimensões avaliadas.

Tabela 2. Matriz Comparativa Baseada em Evidências Empíricas Publicadas

Dimensão	Centralizado	Blockchain
Segurança	Vulnerável a ataques estruturais: <i>mix-up</i> , <i>token substitution</i> , <i>open redirect</i> (Fett et al.).	Resiliente por natureza; consenso distribuído; provas criptográficas (Zhang et al.; Kaneriya & Patel).
Desempenho	Autenticação média de 5–50 ms dependendo do IdP.	Aproximadamente 150 ms para geração/validação OTP (Zhang et al.); cerca de 1 s para verificação completa (Kaneriya & Patel).
Auditabilidade	Logs privados e modificáveis; dependência do servidor.	Imutabilidade, verificabilidade pública; prova de inclusão em árvore de Merkle.
Operacionalidade / Adoção	Alta maturidade; baixa complexidade de integração.	Alta complexidade técnica; barreiras organizacionais; necessidade de habilidades específicas.

3.7. Confiabilidade e Limitações

A confiabilidade dos resultados decorre da utilização exclusiva de métricas publicadas em estudos revisados por pares e da aplicação consistente do protocolo de extração. No entanto, algumas limitações permanecem:

- diferenças entre ambientes experimentais (redes privadas, públicas, cenários simulados);

- ausência de *benchmarks* unificados para avaliar autenticação baseada em *block-chain*;
- heterogeneidade metodológica entre os artigos analisados;
- prevalência de protótipos acadêmicos sem replicação em larga escala.

Apesar dessas limitações, a triangulação das evidências permite construir uma análise comparativa sólida, detalhada e aderente aos padrões metodológicos da Engenharia de Software. As próximas etapas, a serem desenvolvidas no TCC II, aprofundarão essa análise com foco na interpretação dos resultados e na formulação de diretrizes de Engenharia de Software para adoção prática da autenticação baseada em *blockchain*.

3.8. Etapas Realizadas no TCC I

No contexto do TCC I, foram executadas as seguintes etapas:

- definição do tema, problema de pesquisa, justificativa e relevância;
- formulação da questão de pesquisa;
- revisão preliminar e aprofundada da literatura;
- seleção e validação do corpus de estudos;
- elaboração da fundamentação teórica;
- definição das dimensões avaliativas e das métricas-alvo;
- planejamento da metodologia e do protocolo de extração de dados;
- elaboração do presente documento conforme o template institucional.

3.9. Etapas Previstas para o TCC II

Para o TCC II, estão previstas as etapas:

1. Revisão e atualização do corpus bibliográfico, incorporando novos estudos relevantes, se necessário.
2. Execução completa do protocolo de extração de métricas a partir dos artigos selecionados.
3. Consolidação e verificação das planilhas de dados extraídos.
4. Aplicação sistemática da normalização qualitativa descrita nesta seção.
5. Construção detalhada da matriz comparativa, incluindo exemplos representativos das métricas.
6. Análise crítica dos resultados e discussão à luz da fundamentação teórica.
7. Redação das seções de Resultados, Discussão, Conclusão e Ameaças à Validade.
8. Revisão final do texto, adequação às normas da instituição e preparação para defesa.

3.10. Cronograma do TCC II

O cronograma previsto para execução das etapas do TCC II está apresentado na Tabela 3.

Tabela 3. Cronograma Previsto para o TCC II

Atividade	Ago	Set	Out	Nov
Revisão e atualização da literatura	X			
Extração das métricas	X	X		
Normalização dos dados		X		
Construção da matriz comparativa		X	X	
Análise crítica e discussão			X	
Conclusão e ameaças à validade			X	X
Revisão, ajustes finais e entrega				X

Apêndice