

Autenticação Descentralizada com Blockchain: Eficácia, Barreiras de Adoção e Contribuições da Engenharia de Software

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 conducts a comparative and empirical study of authentication mechanisms based on blockchain technology and traditional centralized models. It aims to analyze the effectiveness, limitations, and implementation barriers of decentralized authentication systems, with a particular focus on software engineering practices that support their adoption. Through the examination of technical literature and case-based evidence, the study identifies objective criteria for evaluating security, performance, and usability. The expected contribution is a set of engineering-oriented guidelines to support the design of secure, auditable, and scalable authentication solutions based on distributed architectures.

Resumo. Esta pesquisa realiza um estudo comparativo e empírico entre mecanismos de autenticação baseados em tecnologia blockchain e modelos centralizados tradicionais. O objetivo é analisar a eficácia, as limitações e as barreiras de implementação de sistemas de autenticação descentralizados, com ênfase em práticas da Engenharia de Software que viabilizem sua adoção. Por meio da análise da literatura técnica e de evidências baseadas em casos, identificam-se critérios objetivos para avaliação de segurança, desempenho e usabilidade. A contribuição esperada consiste em um conjunto de diretrizes orientadas à engenharia para apoiar o 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 - cleiton.tavares@pucminas.br
Orientador do TCC II: (A ser definido no próximo semestre)

Belo Horizonte, DIA de MÊS de ANO.

1. Introdução

A compreensão sobre os mecanismos de autenticação digital se mostra essencial para o desenvolvimento de sistemas seguros em contextos cada vez mais distribuídos e conectados. Zhang, Wang e Yang destacam que modelos amplamente utilizados como o *OAuth*

2.0 e o *OpenID Connect* concentram a responsabilidade da verificação de identidade em entidades centralizadas, o que pode gerar riscos relacionados à confiabilidade da fonte, à rastreabilidade limitada das ações e à existência de pontos únicos de falha. Essa limitação estrutural tem motivado pesquisadores e profissionais a investigar alternativas capazes de oferecer maior descentralização, transparência e autonomia ao usuário.

Nesse cenário, propostas baseadas em *blockchain* têm ganhado destaque. Kaneriya e Patel desenvolveram um sistema de verificação de credenciais estudantis que se apoia em *smart contracts* e em armazenamento distribuído para oferecer controle seletivo sobre os dados autenticados, com foco em privacidade e descentralização. Complementarmente, Li, Wang, Gasevic, Yu e Liu exploram como fatores humanos, técnicos e contextuais interferem na adoção de soluções em *blockchain*, propondo um modelo de engenharia orientado à adoção prática dessas tecnologias em ambientes educacionais reais.

A Engenharia de Software tem oferecido caminhos para superar desafios associados à aplicação de *blockchain* em mecanismos de autenticação. Ahmed, Iqbal, Hussain, Khan, Helfert, Imran e Kim sugerem abordagens específicas para estimativa de esforço em projetos que envolvem essa tecnologia, enquanto Mazeli propõe um *framework* para apoiar desenvolvedores na implementação de recursos de privacidade desde as fases iniciais do desenvolvimento. Além disso, Fatima, Funke e Lago apresentam um modelo voltado à criação e avaliação de *Key Performance Indicators* (KPIs), reforçando a importância de práticas estruturadas na mensuração da qualidade e eficiência de soluções descentralizadas.

A integração de tecnologias descentralizadas, como a *blockchain*, em sistemas de autenticação tem se mostrado promissora, mas também complexa. Ahmed, Iqbal, Hussain, Khan, Helfert, Imran e Kim observam que, além dos aspectos técnicos, iniciativas desse tipo demandam atenção especial à estimativa de esforço, uma vez que a aplicação de *blockchain* requer competências específicas e planejamento detalhado para evitar sobrecargas e atrasos no desenvolvimento. Kassab, Destefanis, DeFranco e Pranav reforçam esse ponto ao demonstrar que o mercado já exige engenheiros de software com domínio em desenvolvimento com *blockchain*, habilidades técnicas especializadas e competências em segurança e arquitetura de sistemas distribuídos. Esses achados indicam que a viabilidade de soluções descentralizadas depende não apenas da tecnologia em si, mas também da formação e da experiência da equipe envolvida no projeto.

A adoção efetiva da *blockchain* também está vinculada à forma como os princípios de Engenharia de Software são incorporados desde as fases iniciais de concepção dos sistemas. Mazeli propõe um *framework* voltado ao suporte de desenvolvedores na implementação de requisitos de privacidade, destacando a importância de práticas que favoreçam conformidade regulatória e decisões conscientes sobre o uso de dados sensíveis. Essa perspectiva se alinha à proposta de Fatima, Funke e Lago, que apresentam um modelo para criação e avaliação de KPIs, aplicado a contextos de engenharia organizacional, mas com potencial adaptativo para o desenvolvimento de sistemas seguros e auditáveis.

O **objetivo geral** deste trabalho é comparar, sob a perspectiva da Engenharia de Software, os mecanismos de segurança e autenticação empregados em sistemas descentralizados.

tralizados baseados em *blockchain* e em sistemas tradicionais centralizados, identificando seus trade-offs de segurança, desempenho e usabilidade e sintetizando diretrizes de projeto para adoção prática.

Os **objetivos específicos** são:

1. Conduzir uma *revisão sistemática da literatura* (RSL) com protocolo explícito (bases, cadeia de busca, critérios de inclusão/exclusão e extração de dados) sobre autenticação descentralizada e modelos tradicionais.
2. Construir uma *matriz comparativa* de abordagens, derivando e operacionalizando métricas de avaliação (p. ex., resistência a ataques, latência de autenticação, disponibilidade, requisitos de governança e evidências de auditabilidade).
3. Analisar *estudos de caso* e evidências empíricas reportadas na literatura recente para identificar padrões de falhas, ameaças à validade e condições de contexto (domínio, escala, restrições regulatórias).
4. Propor um *conjunto de diretrizes de engenharia* (checklist de requisitos, decisões arquiteturais e riscos) para a adoção de autenticação baseada em *blockchain* ou híbrida em sistemas reais.
5. Delinear um *modelo conceitual de referência* que integre segurança, desempenho e usabilidade, indicando pontos de integração com práticas de métricas e KPIs.

Como contribuição, espera-se apresentar um panorama técnico comparativo que auxilie pesquisadores e profissionais no entendimento das potencialidades e limitações da tecnologia *blockchain* em processos de autenticação, com base em evidências empíricas e práticas consolidadas da Engenharia de Software.

2. Trabalhos Relacionados

Kaneriya e Patel (2023) propõem um sistema de verificação de credenciais educacionais baseado em *blockchain*, com foco em segurança, privacidade e controle descentralizado dos dados pelos estudantes. O modelo utiliza a rede Ethereum, *smart contracts* e o sistema de arquivos descentralizado IPFS (*Interplanetary File System*) para emissão e validação de credenciais. A arquitetura incorpora contratos distintos para registro, emissão, consentimento e verificação, garantindo que os estudantes possam decidir quais atributos de suas credenciais serão revelados. A solução foi validada experimentalmente e apresentou ganhos de desempenho e confiabilidade, indicando a viabilidade de sistemas autenticadores descentralizados aplicáveis em contextos reais de validação acadêmica. Este trabalho é relevante para a presente pesquisa por oferecer uma implementação prática de autenticação soberana, demonstrando como a descentralização pode reduzir dependência de autoridades centrais.

Li et al. (2023) avançam na discussão ao propor o modelo BOSE-HAP (*Blockchain-oriented Software Engineering Approach for Higher Adoption Possibility*), que adota uma metodologia de Engenharia de Software centrada na adoção prática de soluções baseadas em *blockchain*. O estudo foi conduzido em ambiente educacional real, envolvendo testes de usabilidade, entrevistas e ciclos iterativos com 112 participantes. A metodologia demonstrou que fatores humanos e contextuais são determinantes para o sucesso de sistemas descentralizados, ressaltando a importância da integração entre aspectos técnicos e organizacionais. Essa abordagem contribui diretamente com esta pesquisa ao evidenciar que o sucesso de mecanismos de autenticação descentralizados depende tanto

da arquitetura tecnológica quanto da experiência de uso e da percepção de confiança do usuário.

Zhang, Wang e Yang (2019) apresentam uma proposta de autenticação com senhas de uso único (*One-Time Passwords* — OTP), nas quais a própria rede *blockchain* atua como verificador das credenciais, eliminando a necessidade de servidores centrais. O protocolo foi testado em ambiente de simulação e mostrou resistência a ataques de falsificação e força bruta, além de bom desempenho em termos de latência e verificação . Este estudo fornece base técnica essencial para a comparação de modelos neste trabalho, pois evidencia como o uso de consenso distribuído pode aumentar a confiabilidade do processo de autenticação.

Zareei e Shajari (2022) expandem o uso da *blockchain* para a verificação de diplomas acadêmicos, propondo uma arquitetura descentralizada baseada em *smart contracts* e estruturas Merkle para otimização de armazenamento e custo de transação. O sistema propõe o uso de identificadores criptográficos únicos para preservar a confidencialidade dos dados sem comprometer sua verificabilidade . A proposta é relevante ao demonstrar a escalabilidade e a eficiência computacional de sistemas de autenticação descentralizados, aspecto diretamente comparável às análises de desempenho desta pesquisa.

Rehman et al. (2021) complementam as abordagens anteriores ao propor uma arquitetura híbrida para autenticação de certificados digitais, utilizando consenso *Proof of Authority* (PoA). O modelo integra a verificação descentralizada com interfaces web e móveis, demonstrando redução significativa no tempo de autenticação e menor dependência de autoridades certificadoras tradicionais . Essa integração entre descentralização e eficiência de uso reforça o potencial de arquiteturas híbridas, que unem características da *blockchain* e mecanismos convencionais — linha de investigação também adotada neste estudo.

De modo geral, observa-se que os trabalhos relacionados convergem quanto à relevância da *blockchain* como base para autenticação segura e auditável, mas divergem em suas estratégias de implementação. Enquanto alguns autores enfatizam o aprimoramento técnico e o desempenho dos protocolos (como Zhang et al. e Zareei & Shajari), outros destacam o papel da Engenharia de Software e dos fatores humanos na viabilização prática dessas soluções (como Li et al. e Kaneriya & Patel). Assim, esta pesquisa se posiciona de forma complementar, ao propor uma análise comparativa entre sistemas de autenticação centralizados e descentralizados, com foco em critérios de segurança, desempenho e usabilidade — integrando perspectivas técnicas e empíricas identificadas na literatura.

3. Materiais e Métodos

Esta pesquisa adota uma abordagem **mista**, combinando métodos **qualitativos** e **quantitativos**, com o objetivo de comparar e analisar os mecanismos de autenticação e segurança empregados em sistemas centralizados e descentralizados baseados em *blockchain*. O delineamento metodológico foi elaborado para assegurar rigor científico, reproduzibilidade e relevância prática, integrando análise documental, estudo de casos e avaliação comparativa de métricas técnicas e qualitativas.

3.1. Tipo e natureza da pesquisa

O presente trabalho caracteriza-se como uma **pesquisa aplicada**, com abordagem **exploratória e descritiva**, orientada pela Engenharia de Software. O foco recai sobre a compreensão dos fatores técnicos e organizacionais que influenciam a implementação de mecanismos de autenticação em diferentes arquiteturas. Do ponto de vista epistemológico, adota-se o paradigma **sociotécnico**, reconhecendo que a segurança e a confiabilidade de sistemas digitais emergem da interação entre tecnologia, contexto de uso e comportamento humano.

3.2. Estratégia metodológica

A estratégia metodológica é baseada em um **estudo comparativo de casos múltiplos**, envolvendo dois grupos de referência:

- **Grupo A — Sistemas Centralizados:** soluções de autenticação amplamente utilizadas, como *OAuth 2.0* e *OpenID Connect*, implementadas em plataformas como Google, Microsoft e GitHub. Essas soluções representam o paradigma tradicional de confiança institucional, no qual as credenciais dos usuários são armazenadas e verificadas por provedores centrais.
- **Grupo B — Sistemas Descentralizados:** soluções baseadas em *blockchain*, que utilizam contratos inteligentes, senhas de uso único e consenso distribuído para autenticação. Entre os estudos representativos estão Kaneriya e Patel (2023), Li et al. (2023), e Rehman et al. (2021), que abordam desde autenticação educacional até certificação digital descentralizada.

A comparação entre esses grupos visa identificar diferenças estruturais e operacionais, bem como avaliar como a descentralização influencia a **segurança**, a **usabilidade**, a **privacidade** e a **auditabilidade**. Essa abordagem possibilita observar tanto a maturidade técnica das implementações quanto a viabilidade prática de adoção em contextos corporativos e públicos.

3.3. Procedimentos de coleta de dados

A coleta de dados foi estruturada em três etapas complementares:

- 1) **Revisão Sistemática da Literatura (RSL):** fundamentada nas diretrizes de Kitchenham e Charters (2007), adaptadas ao contexto da Engenharia de Software. As buscas foram realizadas nas bases *IEEE Xplore*, *ACM Digital Library*, *Scopus* e *SpringerLink*, utilizando combinações de descritores como *blockchain authentication*, *decentralized identity* e *user trust*. O protocolo da RSL está detalhado no Apêndice ??.
- 2) **Análise Documental e Técnica:** foram analisadas publicações científicas, whitepapers, relatórios técnicos e documentação de implementações reais de autenticação centralizada e descentralizada. As fontes foram avaliadas conforme critérios de relevância, ano de publicação (2018–2025) e evidência empírica apresentada.
- 3) **Estudo de Casos Comparativos:** foram selecionados dois casos de referência para comparação empírica:

- **Caso 1:** sistema de autenticação centralizado baseado em *OAuth 2.0*, conforme especificação RFC 6749 e implementações amplamente difundidas em ambientes corporativos;
- **Caso 2:** sistema de autenticação descentralizado baseado em *blockchain*, com validação por consenso e uso de contratos inteligentes para emissão e verificação de credenciais digitais.

Cada caso foi descrito quanto à arquitetura, protocolos de autenticação, níveis de segurança e requisitos de usabilidade, conforme o modelo proposto por Li et al. (2023) e Mazeli (2022). Foram coletadas evidências de desempenho, escalabilidade e resiliência frente a ataques de força bruta, falsificação e comprometimento de identidade.

3.4. Critérios de análise e instrumentos de avaliação

A análise comparativa entre os casos foi conduzida com base em três eixos metodológicos:

- Eixo 1: Segurança e integridade:** análise de mecanismos de autenticação, distribuição de chaves, resistência a ataques e verificabilidade das transações.
- Eixo 2: Desempenho e escalabilidade:** medição teórica (quando disponível) e análise documental de tempo médio de autenticação, consumo de recursos e capacidade de resposta do sistema.
- Eixo 3: Usabilidade e soberania do usuário:** análise qualitativa de fatores de experiência do usuário, controle sobre credenciais e percepção de confiança, conforme métricas do modelo SUS (System Usability Scale) e diretrizes da ISO/IEC 25010.

As informações obtidas foram organizadas em uma matriz comparativa (vide Tabela ??) e sintetizadas por meio de análise cruzada, buscando padrões de convergência e divergência entre os modelos. Essa análise será complementada por uma discussão crítica sobre os fatores que limitam a adoção massiva de autenticação via *blockchain*.

3.5. Abordagem de análise dos resultados

Os resultados serão analisados sob duas perspectivas complementares:

- **Quantitativa:** consolidação de métricas de desempenho e segurança em tabelas de comparação, visando identificar tendências e outliers entre os modelos estudados;
- **Qualitativa:** interpretação das evidências à luz da literatura revisada, com base na técnica de análise de conteúdo proposta por Bardin (2011), permitindo compreender as relações entre descentralização, soberania do usuário e auditabilidade.

A triangulação dos resultados buscará evidenciar em que medida a *blockchain* oferece melhorias mensuráveis frente aos modelos centralizados, e quais limitações ainda persistem quanto à escalabilidade, conformidade e facilidade de integração com sistemas legados.

Tabela 1. Cronograma resumido das atividades da pesquisa

Tarefas	2025						
	março		abril		maio		junho
	1ªQ	2ªQ	1ªQ	2ªQ	1ªQ	2ªQ	1ªQ
Planejamento da RSL e definição do protocolo	X						
Coleta e análise de dados da literatura		X	X				
Seleção e descrição dos casos comparativos			X	X			
Avaliação e cruzamento dos resultados				X	X		
Discussão e elaboração da análise final					X	X	X

3.6. Cronograma de execução

A Tabela 1 apresenta a distribuição das atividades ao longo do semestre letivo.

Com essa estrutura, a metodologia demonstra alinhamento entre objetivos, procedimentos e resultados esperados, conferindo solidez científica e aplicabilidade prática à pesquisa. O detalhamento dos instrumentos de coleta e análise, aliado à triangulação entre abordagens qualitativas e quantitativas, assegura robustez e credibilidade ao estudo comparativo entre autenticação centralizada e descentralizada.

Apêndice

A. Exemplo de Seção em um Apêndice