# Um Estudo Comparativo sobre Segurança e Autenticação em Sistemas Descentralizados e Sistemas Tradicionais

**Douglas V. Fernandes**[1]

[1]Instituto 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 investigates authentication and security mechanisms in decentralized systems based on blockchain technology, comparing them with traditional centralized approaches. By examining how immutability, transparency, and distributed consensus can enhance reliability and reduce vulnerabilities, the study explores how blockchain-based authentication can strengthen digital trust and user sovereignty. Through a comparative analysis supported by literature from multiple domains, the research seeks to identify the advantages, limitations, and design implications of decentralized authentication frameworks. The expected outcome is a conceptual model that integrates security, performance, and usability perspectives to support future implementations of sovereign and auditable authentication systems.*

***Resumo.*** *Esta pesquisa investiga os mecanismos de autenticação e segurança em sistemas descentralizados baseados na tecnologia blockchain, comparando-os com abordagens tradicionais centralizadas. Ao examinar como a imutabilidade, a transparência e o consenso distribuído podem aprimorar a confiabilidade e reduzir vulnerabilidades, o estudo analisa de que forma a autenticação baseada em blockchain pode fortalecer a confiança digital e a soberania do usuário. Por meio de uma análise comparativa sustentada pela literatura de múltiplos domínios, busca-se identificar as vantagens, limitações e implicações de projeto associadas a frameworks de autenticação descentralizados. O resultado esperado consiste em um modelo conceitual que integre as perspectivas de segurança, desempenho e usabilidade, oferecendo subsídios para futuras implementações de sistemas de autenticação soberanos e auditáveis. página do artigo.*

**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 - cleitontavares@pucminas.br
Orientador do TCC II: (A ser definido no próximo semestre)

Belo Horizonte, DIA de MÊS de ANO.

## 1. Introdução

A segurança e a autenticação de usuários constituem elementos essenciais para a confiabilidade dos sistemas de software modernos. Com a crescente digitalização de serviços e a expansão da Web 3.0, novas demandas emergem para garantir integridade, privacidade e controle sobre identidades digitais. A tecnologia *blockchain* tem se destacado como uma solução promissora nesse contexto, oferecendo descentralização, imutabilidade e auditabilidade em processos de autenticação [Dong et al. 2023]. Sua capacidade de eliminar intermediários e registrar transações de forma inviolável permite o desenvolvimento de sistemas autônomos e auditáveis, capazes de lidar com vulnerabilidades inerentes aos modelos centralizados. Além disso, estudos recentes demonstram a aplicabilidade da *blockchain* na autenticação descentralizada de usuários na Web 3.0, reforçando seu potencial para proporcionar maior segurança e transparência nas interações digitais [**?**].

Os modelos tradicionais de autenticação, como *OAuth 2.0* e *OpenID Connect*, dependem de provedores centrais que concentram informações sensíveis, tornando-se alvos frequentes de ataques e violações de dados. Essa arquitetura de confiança baseada em terceiros cria pontos únicos de falha e dificulta a rastreabilidade de ações, comprometendo a soberania do usuário e a auditabilidade das operações. Nesse cenário, evidencia-se um desafio de engenharia: **como integrar mecanismos descentralizados de autenticação que garantam segurança, privacidade e desempenho sem comprometer a usabilidade?** Tal problema envolve não apenas a substituição de componentes tecnológicos, mas também a redefinição do próprio paradigma de autenticação, migrando de sistemas baseados em confiança institucional para estruturas de confiança distribuída.

A importância dessa investigação é ressaltada por trabalhos que buscam aprimorar a segurança e a eficiência da autenticação utilizando *blockchain*. Zhang et al. [Zhang et al. 2019] propõem um método de autenticação baseado em *blockchain* com senhas de uso único (*One-Time Passwords* — OTP), no qual a própria rede atua como verificador das credenciais, resistindo a ataques de falsificação e força bruta. Dong et al. [Dong et al. 2023] reforçam que as propriedades de descentralização, consenso e transparência da *blockchain* podem solucionar limitações de instituições centralizadas, oferecendo uma base sólida para a gestão autônoma de identidades. Complementarmente, Jaffal et al. [**?**] analisam a aplicação prática desses conceitos em sistemas Web 3.0, demonstrando que a integração entre *blockchain* e autenticação de usuários amplia a resiliência e reduz riscos de manipulação de credenciais.

Outros estudos da Engenharia de Software também contribuem para esse debate ao abordar como princípios de automação e métricas podem apoiar o desenvolvimento de sistemas descentralizados seguros. Mazeli [**?**] propõe um *framework* para auxiliar desenvolvedores na implementação de recursos de privacidade desde as etapas iniciais do design, o que reforça a necessidade de incorporar segurança como requisito fundamental no ciclo de vida do software. Gao et al. [Gao et al. 2025] exploram a transformação de modelos de processos (*Business Process Modeling Notation* — BPMN) em *smart contracts* utilizando grandes modelos de linguagem (*Large Language Models* — LLMs), destacando o potencial de automação e formalização na geração de sistemas confiáveis. Já Fatima et al. [Fatima et al. 2025] propõem um modelo de indicadores de desempenho (*Key Performance Indicators* — KPIs) para apoiar decisões em Engenharia de Software, fornecendo uma base para mensurar a eficiência e a segurança de implementações dis-

tribuídas. Esses estudos, em conjunto, indicam uma tendência clara: a convergência entre automação, descentralização e governança transparente como caminho para aumentar a confiança e a segurança em sistemas de software.

O **objetivo geral deste trabalho** é comparar os mecanismos de segurança e autenticação empregados em sistemas descentralizados baseados em *blockchain* e em sistemas tradicionais centralizados, identificando vantagens, limitações e oportunidades de melhoria sob a perspectiva da Engenharia de Software. Para alcançar esse objetivo, definem-se os seguintes objetivos específicos: (i) revisar criticamente a literatura recente sobre autenticação descentralizada e mecanismos tradicionais de verificação de identidade; (ii) identificar critérios técnicos e métricas de avaliação de segurança, desempenho e usabilidade; (iii) analisar comparativamente os principais modelos identificados; e (iv) propor diretrizes conceituais que orientem o projeto de soluções híbridas de autenticação seguras e auditáveis.

Como resultados esperados, prevê-se o estabelecimento de um panorama comparativo detalhado sobre os modelos de autenticação atuais, destacando os impactos da descentralização na segurança, eficiência e autonomia do usuário. Espera-se também identificar lacunas técnicas e teóricas que possam direcionar futuras pesquisas sobre a integração entre *blockchain*, automação e privacidade. O estudo visa contribuir para a Engenharia de Software ao propor uma visão estruturada sobre como os princípios de segurança distribuída podem ser aplicados de forma prática e escalável em diferentes domínios.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta a fundamentação teórica sobre autenticação, descentralização e *blockchain*; a Seção 3 descreve a metodologia de pesquisa, incluindo os critérios de análise comparativa; a Seção 4 discute os resultados e implicações; e a Seção 5 apresenta as conclusões e trabalhos futuros, destacando as contribuições teóricas e aplicadas da pesquisa.

## 2. Trabalhos Relacionados

### 2.1. Sections and Paragraphs

Section titles must be in boldface, 13pt, flush left. There should be an extra 12 pt of space before each title. Section numbering is optional. The first paragraph of each section should not be indented, while the first lines of subsequent paragraphs should be indented by 1.27 cm.

#### 2.1.1. Subsections

The subsection titles must be in boldface, 12pt, flush left.

### 2.2. Tables

In tables, try to avoid the use of colored or shaded backgrounds, and avoid thick, doubled, or unnecessary framing lines. When reporting empirical data, do not use more decimal digits than warranted by their precision and reproducibility. Table caption must be placed before the table (see Table 1) and the font used must also be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.

**Tabela 1. Variables to be considered on the evaluation of interaction techniques**

| | Chessboard top view | Chessboard perspective view |
|---|---|---|
| Selection with side movements | 6.02 ± 5.22 | 7.01±6.84 |
| Selection with in-depth movements | 6.29±4.99 | 12.22±11.33 |
| Manipulation with side movements | 4.66± 4.94 | 3.47±2.20 |
| Manipulation with in-depth movements | 5.71 ±4.55 | 5.37 ±3.28 |

# 3. Materiais e Métodos

## 3.1. Exemplo de Listing

```
public class Phone {
  private final String unformattedNumber;

  public String getNumber() {
    return unformattedNumber.substring(6,10);
  }
}
```

**Listing 1. Code Example**

## 3.2. Exemplo de Algorithm

**Algorithm 1:** Código fonte em Java

```
void printOwing (double amount){
  print Banner();
  //print details
    System.out.println("name: " + _name);
    System.out.println("amout: " + amount);
}
```

## 3.3. Exemplo de Cronograma

Esta seção apresenta um exemplo de tabela para construção de cronograma.

## 3.4. References

Bibliographic references must be unambiguous and uniform. We recommend giving the author names references in brackets, e.g. [**?**], [**?**], and [**?**].

Cormen et al. (2016) representa uma citação direta.

**Tabela 2. Distribuição de tarefas por datas**

| | **2025** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **fevereiro** | | **março** | | **abril** | | **maio** |
| **Tarefas** | 1ªQ | 2ªQ | 1ªQ | 2ªQ | 1ªQ | 2ªQ | 1ªQ |
| Desenvolvimento do *script* para coleta dos repositórios | X | | | | | | |
| Coleta de dados dos repositórios | | X | | | | | |
| *Desenvolvimento da solução* | | X | | | | | |
| Coleta de dados | | | X | X | | | |
| Aplicação do Método | | | X | X | X | | |
| Geração dos painéis | | | | | | X | |
| Discussão e avaliação dos resultados | | | | | | | X |

The references must be listed using 12 point font size, with 6 points of space before each reference. The first line of each reference should not be indented, while the subsequent should be indented by 0.5 cm.

## Referências


Dong, S., Abbas, K., Li, M., and Kamruzzaman, J. (2023). Blockchain technology and application: an overview. *PeerJ Computer Science*, 9:e1705.

Fatima, I., Funke, M., and Lago, P. (2025). Providing guidance to software practitioners: A framework for creating key performance indicators. *IEEE Software*, 42(4):68–78.

Gao, S., Liu, W., Zhu, J., Dong, X., and Dong, J. (2025). Bpmn-llm: Transforming bpmn models into smart contracts using large language models. *IEEE Software*, 42(4):50–57.

Zhang, M., Wang, L., and Yang, J. (2019). A blockchain-based authentication method with one-time password. In *2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)*, pages 1–9.


## Apêndice

## A. Exemplo de Seção em um Apêndice