



# Autenticação de Usuários na Web 3.0: Um Estudo sobre Mecanismos Descentralizados com Blockchain

Wissam Jaffal  
Centro Universitário UDC  
Foz Do Iguaçu, Brasil  
wissamjaffal1@gmail.com

Luciano Santos Cardoso  
Centro Universitário UDC  
Foz Do Iguaçu, Brasil  
luciano.cardoso@udc.edu.br

Alessandra Bussaador  
Centro Universitário UDC  
Foz Do Iguaçu, Brasil  
alebussador@gmail.com

**Abstract**—This study explores the integration of blockchain technology with Web 3.0, highlighting decentralized user authentication. Web 3.0 marks a new era of the internet, focused on data decentralization and a token-based economy, providing greater security and user control over data. The research investigates how blockchain can be utilized to implement a secure and decentralized authentication method, comparing its benefits and limitations with traditional centralized authentication methods. The study covers the evolution of blockchain, from its origins as the underlying technology of Bitcoin to its contemporary applications, including smart contracts and digital identification. Additionally, the work analyzes the main features of Web 3.0, such as web semantics and the capacity for machine information processing. A prototype of a user registration system using blockchain is developed and evaluated, highlighting the advantages of decentralized authentication, such as increased security, transparency, and fault resilience. The methodology used includes a detailed literature review, technical analysis of blockchain, and practical prototype development. This study contributes to the understanding of the potentials and challenges of decentralized authentication, providing valuable insights for future applications and research in the field.

**Keywords**—Blockchain; Web 3.0; Authentication;

**Resumo**—Este estudo explora a integração da tecnologia blockchain com a Web 3.0, destacando a autenticação descentralizada de usuários. A Web 3.0 inaugura uma nova era na internet, focada na descentralização de dados e em uma economia baseada em tokens, proporcionando maior segurança e controle dos dados aos usuários. A pesquisa investiga como o blockchain pode ser utilizado para implementar um método de autenticação seguro e descentralizado, comparando seus benefícios e limitações em relação aos métodos tradicionais de autenticação centralizada. O estudo abrange a evolução do blockchain, desde suas origens como tecnologia subjacente ao Bitcoin até suas aplicações contemporâneas, incluindo contratos inteligentes e identificação digital. Além disso, o trabalho analisa as principais características da Web 3.0, como a web semântica e a capacidade de processamento de informações por máquinas. Um protótipo de sistema de registro de usuários utilizando blockchain é desenvolvido e avaliado, destacando as vantagens da autenticação descentralizada, como maior segurança, transparência e resiliência a falhas. A metodologia utilizada inclui uma revisão bibliográfica detalhada, análise técnica do blockchain e o desenvolvimento prático do protótipo. Este estudo contribui para o entendimento das potencialidades

e desafios da autenticação descentralizada, fornecendo insights importantes para futuras aplicações e pesquisas na área.

**Palavras-chave**—Blockchain; Web 3.0; Autenticação;

## I. INTRODUÇÃO

A integração entre a Web 3.0 e a tecnologia blockchain constitui um campo estratégico de pesquisa, especialmente no que se refere à autenticação de usuários. A Web 1.0, idealizada por Tim Berners Lee no final da década de 1980, era caracterizada por ser estática e essencialmente de leitura, sem permitir a interação dos usuários com o conteúdo. Com a chegada da Web 2.0 em 2004, liderada por Dale Dougherty, a internet evoluiu para uma plataforma dinâmica e colaborativa, permitindo aos usuários criar e compartilhar conteúdo [1].

Em 2008, Satoshi Nakamoto apresentou o Bitcoin, um sistema de pagamento eletrônico baseado em criptografia, que introduziu a tecnologia blockchain, destacando-se pela sua capacidade de garantir a transparência das transações e o anonimato dos usuários [2]. A blockchain rapidamente se tornou uma tecnologia disruptiva, possibilitando, além de transações financeiras, a autenticação de documentos e o registro descentralizado de ativos [3].

A Web 3.0, também chamada de Web3, objetiva criar uma internet mais segura e privada, focando na descentralização de dados e na eliminação de intermediários por meio da tecnologia blockchain. Este estudo pretende analisar como o blockchain pode ser utilizado para proporcionar um método eficaz de autenticação na Web 3.0, oferecendo maior segurança, transparência e confiança nas interações digitais. Além disso, são abordados os benefícios e desafios de um sistema de login anônimo, onde os dados não são rastreáveis até o usuário [4], [5].

### A. Problema

Quais são os principais desafios e benefícios ao implementar a autenticação da tecnologia blockchain na Web3.0, con-

siderando a natureza descentralizada e os princípios específicos da Web3.0?

### B. Objetivo

1) *Objetivo Geral:* Compreender o funcionamento da autenticação de usuários utilizando a tecnologia blockchain na Web 3.0 e analisar os benefícios e limitações dessa tecnologia por meio da implementação de um protótipo.

#### 2) *Objetivos Específicos:*

- Investigar as características principais da Web 3.0 e sua evolução em comparação às tecnologias anteriores;
- Entender os princípios básicos e o funcionamento da tecnologia blockchain;
- Desenvolver um protótipo de sistema descentralizado para cadastro de usuários utilizando blockchain;
- Comparar os prós e contras dessa abordagem em relação aos sistemas de autenticação centralizados.

### C. justificativa

O avanço tecnológico acelerado trouxe consigo uma ampla gama de métodos de segurança, desde autenticação por Serviço de Mensagens Curtas (SMS, do inglês Short Message Service), Senhas de Uso Único Baseadas em Tempo (TOTPs, do inglês Time-based One-Time Passwords), até métodos mais avançados, como a Autenticação de Dois Fatores (2FA, do inglês Two-Factor Authentication) e a autenticação baseada em blockchain na Web 3.0. Entretanto, ao considerar a implementação da autenticação descentralizada via blockchain na Web 3.0, é fundamental justificar essa escolha, equilibrando os desafios inerentes e os benefícios propostos. A justificativa deste estudo se fundamenta na necessidade de explorar as potencialidades da autenticação via blockchain na Web 3.0. Ao compreender as vantagens oferecidas e os obstáculos enfrentados, este estudo visa fornecer uma base sólida para a implementação dessa tecnologia, buscando uma transição fluida e informada para um sistema de autenticação mais seguro e eficaz.

## II. BLOCKCHAIN

A blockchain começou como a tecnologia subjacente à criptomoeda Bitcoin, que foi proposta em 2008 por uma pessoa ou grupo de pessoas sob o pseudônimo de Satoshi Nakamoto. O Bitcoin é uma moeda digital descentralizada que permite pagamentos instantâneos para qualquer pessoa, em qualquer lugar do mundo, sem a necessidade de uma autoridade central. É baseado na tecnologia P2P e fornece vários níveis de segurança que tornam todo o sistema resiliente a falsificações [2].

### A. Evolução do Blockchain

A partir de 2009, com o desenvolvimento do Bitcoin, a tecnologia blockchain evoluiu para além das transações financeiras, destacando-se pela descentralização, armazenamento de dados distribuídos e ausência de uma autoridade central [3]. A Blockchain 1.0, iniciada com o Bitcoin, resolveu problemas de duplo gasto e processamento de transações digitais de forma descentralizada. Em seguida, a Blockchain 2.0, introduziu o conceito de Contratos Inteligentes, expandindo o uso da blockchain para além das criptomoedas, permitindo a descentralização de mercados e a transferência de diversos ativos, como ações e propriedades e executando contratos automaticamente sem intermediários. Por fim, a Blockchain 3.0 aplicou a tecnologia em várias indústrias, como governo, saúde e cultura, desenvolvendo aplicativos distribuídos e mais seguros [6].

### B. Aplicações do Blockchain

A tecnologia Blockchain tem aplicações potenciais em uma variedade de campos, incluindo o setor bancário, serviços de seguro, Internet das Coisas (do inglês Internet of Things ou IoT), governança, compartilhamento de energia e dados, entre outros. Sua natureza segura, transparente e imutável oferece uma revolução nas formas como as transações são realizadas e registradas, com implicações significativas para a economia, a segurança de dados e a privacidade [3].

## III. WEB 3.0

A Web 3.0, iniciada em torno de 2014 e também conhecida como a Web Semântica, procura fazer com que a internet seja utilizável por máquinas de uma maneira que elas possam entender [7]. Este estágio visa transformar a web em um banco de dados global, onde as informações são conectadas de maneira semântica para que possam ser compreendidas pelos computadores, não apenas apresentadas [1]. A Web 3.0 é caracterizada pela capacidade de processar informações através de inteligência artificial, utilizando tecnologias como RDF (do inglês Resource Description Framework ou RDF), OWL (do inglês Web Ontology Language ou OWL) e SPARQL (uma linguagem de consulta para bancos de dados RDF). Estas tecnologias permitem a descrição de informações de maneira que os computadores possam entender o contexto e os relacionamentos entre diferentes pedaços de dados [1].

### A. Características da Web 3.0

A Web 3.0 é vista como uma internet mais inteligente, onde máquinas processam informações de forma autônoma, facilitando a interpretação semântica dos conteúdos e melhorando a precisão das buscas [8].

Essa evolução permite experiências mais personalizadas e interativas para os usuários, utilizando tecnologias que analisam o comportamento e adaptam conteúdos às suas preferências [9].

A arquitetura descentralizada da Web 3.0 promove a distribuição global de dados e aplicativos, tornando a internet mais democrática e acessível. Além disso, avanços na inteligência artificial tornam as buscas e a navegação mais eficientes e contextualmente relevantes [10].

#### IV. AUTENTICAÇÃO NA BLOCKCHAIN E WEB3.0

A integração da tecnologia blockchain com a Web 3.0 em sistemas de autenticação representa uma transformação significativa na maneira como os usuários são verificados em plataformas digitais. Com o crescente foco em segurança e privacidade, essas tecnologias oferecem métodos inovadores que prometem revolucionar a autenticação de usuários, garantindo um controle aprimorado e maior segurança sobre os dados pessoais [5].

##### A. Autenticação em IoT Usando Blockchain

A tokenização de identidades de usuários envolve o uso de endereços de contrato em redes blockchain para gerar identidades digitais únicas. Cada usuário é associado a uma identidade digital representada por um NFT ou token equivalente, garantindo uma ligação segura entre o usuário e suas chaves criptográficas. Este processo inclui a criação de um endereço de contrato no blockchain, que é vinculado a chaves criptográficas, assegurando a segurança e a integridade da identidade digital [4].

De acordo com [11] contratos inteligentes são usados para definir políticas de controle de acesso baseadas no endereço de contrato do usuário. Esses contratos automatizam o processo de autenticação, reforçando as medidas de segurança e eliminando a necessidade de intermediários. A utilização de contratos inteligentes permite implementar regras e condições específicas para o acesso a dispositivos ou serviços IoT, baseando-se nas chaves criptográficas associadas ao usuário.

##### B. Autenticação Web 3.0

O modelo de autenticação descentralizada faz uso da blockchain Ethereum para fornecer uma plataforma segura e descentralizada para a autenticação dos usuários, eliminando o controle central sobre os dados e melhorando a privacidade e a segurança [12].

Com isso, os usuários mantêm o controle total sobre seus próprios dados, diferentemente dos sistemas centralizados tradicionais, onde fornecedores terceirizados podem acessar e alterar os dados conforme sua conveniência [12]. A implementação utiliza uma arquitetura web moderna, aprimorando a interação e a experiência do usuário, resultando em um processo de autenticação mais eficiente e intuitivo.

#### V. PROCEDIMENTOS METODOLÓGICOS

Este capítulo descreve os procedimentos metodológicos adotados para avaliar a implementação de blockchain na autenticação de usuários em ambientes Web 3.0.

Para tal, o trabalho foi dividido em 05 (cinco) etapas, ilustradas na Figura 12 e explicados a seguir.

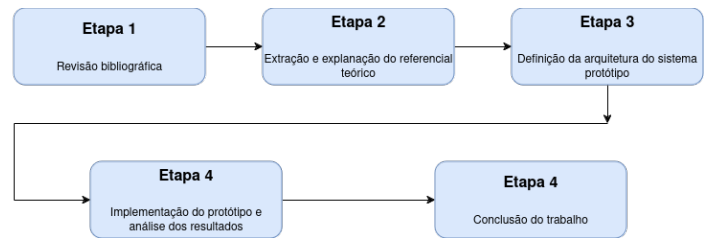


Fig. 1. Divisão de etapas do trabalho.

Para a primeira etapa deste trabalho é foi feito uma pesquisa de materiais, realizada por meio de uma revisão bibliográfica abrangente, através de livros, artigos, bases de código e outros materiais pertinentes disponíveis na internet, visando garantir uma pesquisa com conteúdo de qualidade e atualizado para o trabalho.

A segunda etapa envolve a explanação de aspectos técnicos fundamentais, como os conceitos e aplicações de Web 3.0, tecnologias descentralizadas ou distribuídas, com foco na tecnologia de Blockchain. Esse referencial teórico será essencial para estabelecer a base teórica para aprofundar em conceitos mais avançados de autenticação distribuída com Blockchain.

Na terceira etapa é realizada uma análise detalhada da tecnologia Blockchain, incluindo sua arquitetura, componentes, instalação e utilização. Nessa etapa também serão utilizadas implementações de Blockchain que tiverem sido encontradas nas bases de código pesquisadas na primeira etapa, de modo a otimizar o trabalho.

A quarta etapa concentra-se no desenvolvimento de um protótipo de aplicação de cadastro de usuários utilizando blockchain com o objetivo de viabilizar a análise da utilização da tecnologia conforme o objetivo proposto do trabalho. Essa etapa deverá ser finalizada com uma análise das vantagens e desvantagens percebidas na implementação do protótipo.

#### VI. RESULTADOS E DIFERENÇAS

A gestão de identidades digitais está passando por uma transformação com a introdução de sistemas descentralizados, que contrastam significativamente com os métodos centralizados tradicionais. Enquanto os sistemas centralizados, como o Domain Name System (DNS), são eficientes e escaláveis,

enfrentam desafios críticos em termos de segurança e privacidade, devido à dependência de uma autoridade central e a vulnerabilidade a pontos únicos de falha [13].

Por outro lado, os sistemas descentralizados, como os Identificadores Descentralizados (DIDs) baseados em blockchain, oferecem maior segurança, controle de privacidade pelo usuário e resistência a alterações não autorizadas. A tecnologia blockchain garante que os dados sejam imutáveis e distribuídos, o que reduz os riscos de manipulação e melhora a segurança [13].

Embora os sistemas centralizados possam enfrentar dificuldades de interoperabilidade e escalabilidade, os sistemas descentralizados, devido à sua natureza distribuída e base em plataformas abertas, são mais resilientes e propensos à interoperabilidade, facilitando a integração entre diferentes serviços e aplicações [13], a figura 2 mostra a comparação de sistemas de identidades digitais descentralizados e centralizados.

IDENTIDADE DIGITAL NA WEB 3.0	SISTEMAS TRADICIONAIS DE GERENCIAMENTO DE IDENTIDADE
Descentralizado	Centralizado
Os usuários têm controle sobre suas informações de identidade	As autoridades centrais (terceiros) têm controle sobre as informações de identidade do usuário
Baseado na tecnologia Blockchain	Baseado em Sistemas tradicionais de Gerenciamento de Banco de Dados
Mais seguro e privado	Potencialmente vulnerável a violações de dados e ataques hacker
Permite o compartilhamento seletivo de informações de identidade	As informações de identidade geralmente são amplamente compartilhadas

Fig. 2. Comparação de sistemas de identidades digitais descentralizados e centralizados.

## VII. CONCLUSÃO

Esta revisão bibliográfica explora as possibilidades e os desafios relacionados à implementação de mecanismos de autenticação descentralizados com o uso da tecnologia blockchain no contexto da Web 3.0. Estudos comparativos entre sistemas de autenticação centralizados e descentralizados indicam que, embora os métodos tradicionais centralizados ofereçam eficiência e escalabilidade, eles também apresentam riscos substanciais à segurança e à privacidade dos usuários. Por outro lado, a literatura aponta que os sistemas descentralizados baseados em blockchain proporcionam maior segurança, maior controle sobre a privacidade e resiliência a falhas e ataques, destacando-se como uma alternativa promissora para o futuro da gestão de identidades digitais.

A Web 3.0, com sua ênfase na descentralização e em uma economia baseada em tokens, tem o potencial de transformar a forma como interagimos e gerenciamos nossas identidades

na internet. A integração da blockchain como camada de autenticação na Web 3.0 não apenas elimina a dependência de autoridades centrais, mas também reforça a segurança e a confiança nas transações digitais.

Apesar dos desafios, como questões de escalabilidade e a complexidade técnica envolvida, a adoção dessas tecnologias oferece oportunidades significativas para aumentar a segurança e a privacidade em ambientes digitais. Portanto, o uso do blockchain para autenticação na Web 3.0 revela-se uma solução viável e inovadora, capaz de superar as limitações dos sistemas centralizados e de atender às exigências de um ambiente digital cada vez mais dinâmico e interconectado.

## REFERÊNCIAS

- [1] K. JacksI and S. M. Abass, "Development history of the world wide web," *International Journal of Scientific & Technology Research*, vol. 8, no. 9, 2019, acesso em: 3 jul. 2024. [Online]. Available: [https://www.researchgate.net/publication/336073851\\_Development\\_History\\_Of\\_The\\_World\\_Wide\\_Web](https://www.researchgate.net/publication/336073851_Development_History_Of_The_World_Wide_Web)
- [2] S. Sarmah, "Understanding blockchain technology," *International Journal of Applied Research*, 2018.
- [3] N. Kumar and S. Aggarwal, "History of blockchain-blockchain 1.0: Currency," in *Advances in Computers*. Elsevier, 2020, vol. 121.
- [4] S. Gupta, "Blockchain and decentralized authentication: New approaches for web 3.0," *Journal of Emerging Technologies*, 2023.
- [5] T. Adrian, J. Smith, and L. Davis, "Anonymous login systems in the decentralized web," *International Journal of Information Security*, 2023.
- [6] Z. A. Bhutta, A. Khan, and M. Javed, "Blockchain evolution: From bitcoin to smart contracts and beyond," *Journal of Computer Networks*, 2021.
- [7] D. Khazode and R. Sarode, "The future of web: From web 1.0 to web 3.0," *International Journal of Computer Science and Information Security*, 2016.
- [8] M. L. de A. Campos, "O documento e as ferramentas de trabalho e recuperação da informação na web semântica: um novo espaço de identidade," in *Documento Gênese e contextos de uso: estudos da informação*. Niterói: UFF, 2010.
- [9] Datateca, "Características de la web 3.0," 2018, acesso em: 2 jul. 2024. [Online]. Available: [http://datateca.unad.edu.co/contenidos/MDL000/ContenidoTelematica/caractersticas\\_de\\_la\\_web\\_30.html](http://datateca.unad.edu.co/contenidos/MDL000/ContenidoTelematica/caractersticas_de_la_web_30.html)
- [10] F. R. de Oliveira, R. C. Maziero, and L. S. de Araújo, *Um estudo sobre a Web 3.0: evolução, conceitos, princípios, benefícios e impactos*. Faculdade de Tecnologia de Catanduva (FATEC) – SP, 2018.
- [11] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for iot," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2018, pp. 1–6, acesso em: 3 jul. 2024. [Online]. Available: <https://ieeexplore.ieee.org/document/8487449>
- [12] A. Petcu, B. Pahontu, and M. Frunzete, "A secure and decentralized authentication mechanism based on web 3.0 and ethereum blockchain technology," *Applied Sciences*, 2023.
- [13] H. Li, Y. Jing, and Z. Guan, "The review and comparison between centralized and decentralized digital identity systems," Beihang University; China Academy of Information and Communications Technology, Beijing, China, Tech. Rep., 2024.