

universidade de aveiro



theoria poiesis praxis

JDMI¹⁹

Journal of Digital Media & Interaction

Special Issue on Web3, Vol.8, No.19, (2025)
DigiMedia | University of Aveiro

Title

Special Issue on Web3, Vol.8, No.19

Guest Editors

Ana Patrícia Oliveira, Liliana Vale Costa & Salomé Azevedo

Editors-in-Chief

Lídia Oliveira & Maria João Antunes

Managing Editors

Rita Oliveira

Jennifer Bueno-Rocha

Editorial Board

Adérito Marcos, Álvaro Sousa, Ana Carla Amaro, Ana Isabel Veloso, Ana Jorge, André Neves, Angeliki Monnier, Annamaria Jatobá Palácios, António Coelho, Aurora Cuevas-Cerveró, Bruno Giesteira, Carlos Santos, Cassia Cordeiro Frutado, Claudio Xavier, Cristina Ponte, Emília Duarte, Esteban Clua, Eva Petersson, Federico Tajariol, Fernando Zamith, Guido Lemos, Guilherme Santa Rosa, Heitor Alvelos, Helena Pires, Janet C. Read, Jean-François Diana, Joana Quental, João Canavilhas, Jorge Ferraz, Jorge Hidalgo, Jorge Martins Rosa, José Azevedo, Jussara Borges, Leonel Morgado, Luís Pedro, Lynn Alves, Maite Soto-Sanfiel, Manuela Penafria, Mário Vairinhos, Miguel Carvalhais, Miguel Sicart, Miriam Tavares, Óscar Mealha, Pablo Parra Valero, Patrícia Dias, Paulo Nuno Vicente, Pedro Almeida, Pedro Cardoso, Pierre Humbert, Raimunda Ribeiro, Raquel Recuero, Rita Maia, Roberto Duarte, Rosário Fernandes Falero, Rui Raposo, Ruth Contreras, Soledad Ruano López, Telmo Silva, Vania Ribas Ulbricht, Walter Lima, Xabier Rólan

Logo and Cover*

Joana Beja

Publisher

University of Aveiro

Support

DigiMedia – Digital Media and Interaction

SBIDM – Serviços de Biblioteca, Informação Documental e Museologia

Copyright Information

All work licensed under Creative Commons Attribution License that allows others to share the work with an acknowledgement of the work's authorship and initial publication in this journal. Copyrights to illustrations published in the journal remain with their current copyright holders. It is the author's responsibility to obtain permission to quote from copyright sources.

Mailing Address

Universidade de Aveiro
Departamento de Comunicação e Arte
3810-193 Aveiro – Portugal
E-mail: deca-jdmi@ua.pt

Publication Date

December 2025

ISSN | DOI

2184-3120 | 10.34624/jdmi

Special Issue on Web3 | Volume 8 | Number 19 | 2025

Web3 Technologies in Contemporary Digital Ecosystems (Editorial) 5-8

Ana Patrícia Oliveira, Liliana Vale Costa & Salomé Azevedo

ARTICLES

A Pragmatic Approach for Web3 Software Quality Assurance Based on International Guidelines9-27

Rodrigo Antunes, Liliana Freitas, Pedro Dias, Luís Silva, Federico Guede-Fernandez & Salomé Azevedo

Trust, Privacy and Authenticity in Scientific Data Sharing: The Role of Blockchain and Zero Knowledge Proofs..... 28-45

Joana Almeida, Rita Santos, Ciro Martins, Hélder Gomes, Carmen Guimarães, Fernando Costa, Pedro Colarejo, Afonso Monteiro & Liliana Vale Costa

Threat Modeling a Health Web3 DApp46-65

Ricardo Gomes, Daniela Dinis, João Oliveira, Marisa Maximiano, Vítor Távora, Carlos Machado Antunes, Manuel Dias & Ricardo Correia Bezerra

Integration of Citizen's Card Digital Authentication in Hyperledger Fabric..... 66-86

Carlos Machado Antunes, Marisa Maximiano, Vítor Távora, Ricardo Gomes, Manuel Dias & Ricardo Correia Bezerra

Towards a Generic NFT-Driven Digital Twin Simulation Platform: A Systematic Literature Review..... 87-103

Bernardo J. R. Figueiredo, Marco P. M. Ferreira, João Matos & Marco P. J. P. Cova

VARIA

Artificial intelligence at the service of investigative journalism: A paradigmatic case of designing a prototype to support journalists' routine procedures 104-119

Joana Silva

From paper to digital: Journey into imagination with Alba Digital Stories 120-130

Fabiola Camandona

Fostering Media Literacy through Digital Content Creation..... 131-143

Guendalina Peconio, Michele Ciletti & Giusi Antonia Toto

Viral narratives around the 'Sailor Moon made me gay' controversy on Facebook 144-161

Daniel Eugenio Salinas Lara, Raúl Alejandro Treviño González & Mariana Reyes Abundes

Web3 Technologies in Contemporary Digital Ecosystems (Editorial)

Ana Patrícia Oliveira
*DigiMedia, Department of
Communication and Art,
University of Aveiro, Portugal*
apoliveira@ua.pt
0000-0003-3234-787X

Liliana Vale Costa
*DigiMedia, Department of
Communication and Art,
University of Aveiro, Portugal*
lilianavale@ua.pt
0000-0003-2451-3073

Salomé Azevedo
*Value for Health CoLAB;
CHRC, NMS|FCM,
Universidade Nova de Lisboa;
CEG-IST, Universidade de
Lisboa, Portugal*
salome.azevedo@vohcolab.org
0000-0003-1234-9464

Web3 represents a new paradigm in the evolution of the internet, shifting from platform-centric and data-extractive models (Web2) toward decentralized, user-owned, and trust-minimized digital ecosystems. Built upon Distributed Ledger Technologies (DLT), smart contracts, cryptographic protocols, and token-based economic models, Web3 introduces new forms of value exchange, governance, and digital interaction (Swan, 2015; Buterin, 2014). At its core, Web3 seeks to reconfigure power structures on the internet by enabling peer-to-peer interactions without intermediaries, fostering transparency, immutability, programmability, and algorithmic trust.

A central pillar of Web3 is tokenization, which enables the representation of digital and physical assets through cryptocurrencies, utility tokens, and Non-Fungible Tokens (NFTs). NFTs introduce verifiable digital scarcity, provenance, and ownership, transforming how creative content, virtual assets, digital identities, and real-world assets are produced, exchanged, and preserved (Wang et al., 2021; Razi et al., 2024). These mechanisms underpin new economic and cultural ecosystems such as blockchain gaming, decentralized finance (DeFi), digital art markets, metaverse environments, and decentralized autonomous organizations (DAOs).

Beyond technological infrastructure, Web3 also represents a socio-technical transformation, influencing cultural production, creative industries, governance models, data sovereignty, and participation structures (Leible et al., 2019; Díaz et al., 2025). In scientific contexts, Web3 principles are increasingly connected to Decentralized Science (DeSci), promoting transparency, traceability, and new incentive systems for research, data sharing, and knowledge production (Wilkinson et al., 2016; Weidener & Spreckelsen, 2024).

However, despite its transformative promise, Web3 also introduces complex challenges related to security, privacy, usability, governance, regulatory compliance, software quality, and societal impact. Smart contract vulnerabilities, identity management, data protection, scalability constraints, and the maturity gap between experimental innovation and real-world deployment remain critical research questions (Singh et al., 2021; Alaba et al., 2023). In fact, Web3 today constitutes a dynamic and

multidisciplinary research field situated at the intersection of computer science, digital media, economics, law, design, and cultural studies.

This special issue of the *Journal of Digital Media & Interaction* presents a curated selection of extended and revised papers originally presented at the *WEB3: Tokenization, Technology and Culture Conference*, hosted by the University of Aveiro, Portugal. The conference brought together researchers, industry professionals, creators, and societal stakeholders interested in the technological foundations and cultural implications of tokens and Non-Fungible Tokens (NFTs). It explored both the underlying infrastructures required to support token-based systems and their broader societal, economic, and cultural impacts. The event was supported by BLOCKCHAIN.PT – the “Descentralizar Portugal com Blockchain” Agenda, funded by the PRR – Plano de Recuperação e Resiliência (NextGenerationEU), under reference 02/C05-i01.01/2022.PC644918095-00000033.

Within this context, the current issue emerges at a decisive moment to critically analyze and discuss the real impacts of Web3 technologies and their cultural ecosystems, not only in relation to public perception, but also in how they are reshaping the behaviors of creators, users, institutions, and digital artifacts themselves. The selected contributions reflect the diversity, maturity, and interdisciplinary nature of contemporary Web3 research, spanning domains such as Web3 software quality, decentralized scientific data privacy, Health Web3 cybersecurity, blockchain-based digital identity, and NFT-driven Digital Twins.

Rodrigo Antunes et al., in *A Pragmatic Approach for Web3 Software Quality Assurance Based on International Guidelines*, address one of the most pressing challenges in blockchain-based systems: ensuring software quality in decentralized environments. By translating the ISO/IEC SQuaRE framework into actionable testing practices tailored to Web3, and following a Design Science Research methodology in collaboration with the Exeedme blockchain gaming platform, the authors propose a structured quality assurance guide comprising eight testing domains, 16 subdomains, and 108 targeted tests. This work bridges the gap between theoretical quality models and the operational demands of Web3 applications, contributing to enhanced resilience, compliance, and user trust.

In *Trust, Privacy and Authenticity in Scientific Data Sharing: The Role of Blockchain and Zero Knowledge Proofs*, Joana Almeida et al. examine how blockchain technologies and Zero Knowledge Proofs (ZKP) can strengthen trust, privacy, and authenticity in Open Science and decentralized scientific data sharing. Through a systematic literature review, the authors identify key limitations in current approaches to data provenance, ownership, and privacy preservation. Framed within the emerging Decentralized Science (DeSci) paradigm, the study discusses how these technologies align with FAIR data principles and contribute to the development of secure, transparent, and privacy-preserving scientific infrastructures.

Ricardo Gomes et al., in *Threat Modeling a Health Web3 DApp*, focus on the critical security challenges of decentralized applications in the healthcare sector. Adopting a holistic threat modeling approach that integrates LINDDUN, the OWASP Smart Contract Vulnerability framework, and the Threat Dragon tool, the authors systematically identify risks across smart contracts, decentralized

identity, cross-chain interactions, and data access layers. The study demonstrates that fragmented security assessments are insufficient for healthcare contexts and proposes a hierarchical security framework in which holistic threat modeling becomes the foundation for trust, regulatory compliance, and system resilience in Health Web3 ecosystems.

In *Integration of Citizen's Card Digital Authentication in Hyperledger Fabric*, Carlos Machado Antunes et al. explore how the Portuguese Citizen's Card can be integrated into a permissioned blockchain environment to bridge traditional government-issued digital identities with Web3 infrastructures. Using the Autenticação.Gov SDK and Hyperledger Fabric, the authors demonstrate secure authentication workflows that improve accessibility and user adoption, particularly among non-expert users. The work is especially relevant for e-government services, secure voting systems, and other regulated enterprise applications, illustrating how blockchain technologies can coexist with national digital identity frameworks.

Finally, Bernardo Figueiredo et al., in *Towards a Generic NFT-Driven Digital Twin Simulation Platform: A Systematic Literature Review*, investigate the intersection of Non-Fungible Tokens (NFTs) and Digital Twin technologies. Following PRISMA guidelines, the authors analyze the current state of the art and identify a significant research gap regarding generic NFT-driven simulation platforms. The study highlights how NFT-backed Digital Twins can enable real-time monitoring, provenance tracking, predictive maintenance, and lifecycle management of assets, with applications across sectors such as manufacturing, healthcare, and livestock management, thus reinforcing the role of NFTs beyond digital collectibles and into real-world asset ecosystems.

These contributions expose key challenges related to security, trust, privacy, and interoperability, while showcasing the relevance of interdisciplinary approaches for the sustainable development of Web3 ecosystems. By bridging technological, social, and cultural perspectives, this issue contributes to a critical understanding of how decentralization and tokenization are shaping contemporary digital infrastructures.

References

- Alaba, F. A., Sulaimon, H. A., Marisa, M. I., & Najeem, O. (2023). Smart contracts security application and challenges: A review. *Cloud Computing and Data Science*, 5(1), 15–41. <https://ojs.wiserpub.com/index.php/CCDS/article/view/3271>
- Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. Ethereum White Paper. https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
- Díaz, F., Menchaca, C., & Weidener, L. (2025). Exploring the decentralized science ecosystem: Insights on organizational structures, technologies, and funding. *Frontiers in Blockchain*, 8, Article 1524222. <https://doi.org/10.3389/fbloc.2025.1524222>
- Leible, S., Schlager, T., Schubotz, M., & Gipp, B. (2019). A review on blockchain technology and blockchain projects fostering open science. *Frontiers in Blockchain*, 2, Article 16. <https://doi.org/10.3389/fbloc.2019.00016>

- Razi, Q., Devrani, A., Abhyankar, H., Chalapathi, G. S. S., Hassija, V., & Guizani, M. (2024). Non-fungible tokens (NFTs): Survey of current applications, evolution, and future directions. *IEEE Open Journal of the Communications Society*, 5, 2765–2791. <https://doi.org/10.1109/OJCOMS.2023.3343926>
- Singh, S., Hosen, A. S. M. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access*, 9, 13938–13959. <https://doi.org/10.1109/ACCESS.2021.3051602>
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.
- Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). *Non-fungible token (NFT): Overview, evaluation, opportunities and challenges* (arXiv:2105.07447). arXiv. <https://arxiv.org/abs/2105.07447>
- Weidener, L., & Spreckelsen, C. (2024). Decentralized science (DeSci): Definition, shared values, and guiding principles. *Frontiers in Blockchain*, 7, Article 1375763. <https://doi.org/10.3389/fbloc.2024.1375763>
- Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., et al. (2016). The FAIR guiding principles for scientific data management and stewardship. *Scientific Data*, 3, Article 160018. <https://doi.org/10.1038/sdata.2016.18>

A Pragmatic Approach for Web3 Software Quality Assurance Based on International Guidelines

Rodrigo Antunes
Value for Health CoLAB,
Portugal
rodrigo.antunes@vohcolab.org
0009-0009-0083-5570

Luís Silva
Exeedme, Portugal
luis.silva@exeedme.com

Liliana Freitas
Value for Health CoLAB; CEG-IST, Universidade de Lisboa,
Portugal
liliana.freitas@vohcolab.org
0000-0001-9513-2476

Federico Guede-Fernandez
Value for Health CoLAB;
LIBPhys, NOVA School of
Science and Technology,
Portugal
federico.guede@vohcolab.org
0000-0003-2762-0333

Pedro Dias
Value for Health CoLAB;
CHRC, NMS|FCM,
Universidade Nova de Lisboa,
Portugal
pedro.dias@vohcolab.org

Salomé Azevedo
Value for Health CoLAB;
CHRC, NMS|FCM,
Universidade Nova de Lisboa;
CEG-IST, Universidade de
Lisboa, Portugal
salome.azevedo@vohcolab.org
0000-0003-1234-9464

Received: 4 June 2025

Accepted: 24 November 2025

Abstract

Ensuring software quality in the Web3 ecosystem presents unique challenges due to its decentralized architecture and evolving technical landscape. While international standards such as the SQuaRE (Systems and software Quality Requirements and Evaluation) framework offer structured approaches for quality assurance, they are often perceived as overly theoretical and not directly applicable to blockchain-based applications. This study aims to translate these standards into actionable practices suitable for Web3 environments, thereby supporting compliance and fostering stakeholder trust. Using the Design Science Research methodology, complemented by Lean Startup principles, a practical quality assurance guide was co-developed through collaboration between VOH.CoLAB researchers and the Exeedme project team and inspired by the practical experience in gaming and digital assets trading blockchain-based platforms. The resulting guide includes a structured framework comprising eight testing domains, 16 sub-domains and 108 targeted tests, with the domains addressing critical features of blockchain software, including, functional suitability, integration, security, performance, usability, portability, recoverability and resilience. This work contributes to the operationalization of international quality standards in decentralized technology, promoting more resilient and trustworthy blockchain applications.

Keywords *Web3 software quality, Blockchain applications, SQuaRE framework, Quality assurance, Design Science Research*

1. Introduction

The gaming industry has undergone transformative changes in recent years, driven by the growing integration of blockchain technologies. Games like Counter-Strike 2 (CS2) have fostered robust growth of the economy of virtual items, commonly known as “skins”, with marketplaces facilitating billions of dollars in transactions. The adoption of cryptocurrencies and non-fungible tokens (NFTs) has further expanded this ecosystem, enabling players to buy, sell, and trade digital assets with real-world value (CSGO & CS2 Item Economy, 2024). The rise of blockchain gaming is also evident in the

sector's financial traction, with blockchain-based gaming companies attracting over \$1.1 billion in investment in the second quarter of 2024 alone (NFT statistics in 2024, n.d.). Blockchain technology, which enables the creation of valuable digital assets such as NFTs, remains in a rising trend despite a slowdown in trading volume after the 2022 peak. The NFT market, while having consolidated in recent years, still shows strong growth, with a 50% increase in transaction volume in the first quarter of 2024 (NFT - Worldwide Statista Market Forecast, n.d.).

This rapid growth underscores the importance of ensuring software quality in Web3 applications, particularly in gaming, where user trust and platform stability are essential. Ensuring success and continuous improvement of blockchain-based software requires that its development be accompanied by the verification and enhancement of the solution's technological quality. However, guaranteeing software quality in the Web3 context presents unique challenges due to the decentralized nature of blockchain technology (Hossain Faruk et al., 2024). While the SQuaRE (Systems and software Quality Requirements and Evaluation) international standards provide structured frameworks for software quality assurance (Febrero et al., 2016; Shtefan & Zaporozhets, 2021), they are often considered too theoretical, failing to address the specificities of blockchain-based applications (Gordieiev et al., 2024; Tsuda et al., 2019). Ensuring compliance with these standards is crucial for gaining market advantages and establishing trust among stakeholders, namely developers and users (Mubarkoot et al., 2023), yet the existing frameworks lack a pragmatic implementation guidance tailored to Web3 specific requirements.

This study addresses this gap by proposing a structured and actionable quality assurance guide for blockchain-based applications, built inspired by trading gaming assets platforms. Developed through the collaboration between VOH.CoLAB researchers and the Exeedme project manager - a blockchain company specialized in gaming and skin trading for CS2 - this work draws from real-world experiences to tailor the international standards to the needs of Web3 software development and thus closing the gap between the theoretical ISO standards and the practical needs of the companies working in the gaming sector. The contributions of this study are twofold: it bridges the gap between software quality standards mostly based on Web2 environments and the practical realities of Web3 development and it supports the operationalization of international software quality standards in decentralized technologies, promoting higher trust, robustness, and adoption of Web3 applications.

This study was conducted as part of the Blockchain.PT Decentralizing Portugal with Blockchain agenda that brings together a nationwide coalition of 56 entities, including companies, research centers, associations, and public institutions to harness blockchain technology as a catalyst for innovation and international business development. This agenda aims to deliver 26 scalable, export-oriented products, with a strong focus on practical applications such as farm-to-fork traceability through the integration of IoT and blockchain, digital asset management in real estate and other industries, and solutions for seamless data exchange across different blockchain systems. Ultimately, the project seeks to position Portugal at the forefront of blockchain innovation in Europe and drive the country's digital transformation (BlockchainPT, 2025).

This paper is structured as follows: The next section outlines the methodology used to develop the proposed Web3 software quality testing guide, including the stages of the design process. The results section presents the identified test domains and subdomains, along with examples of specific tests that address both technical functionality and user experience. The discussion section interprets the key findings and highlights theoretical and practical implications. Finally, the conclusion summarizes the contributions of the study and outlines directions for future research.

2. Methodology

The Design Science Research (DSR) methodology (Hevner & Park, 2004) was followed to co-create a structured quality assurance guide tailored to blockchain-based software systems. DSR is particularly suited for addressing complex, practice-oriented problems through the creation of innovative artifacts – such as models, frameworks, and processes – that are rigorously designed and evaluated in collaboration with stakeholders (Hevner & Park, 2004; Peffers et al., 2007). In this context, the artifact developed was a structured quality assurance guide to improve software robustness and compliance in Web3 applications.

Based on the methodological approach of (Londral et al., 2022), this study integrated elements of the Lean Startup method into the DSR methodology. While Londral et al. applied this approach in the health domain by structuring discussions around patient pathways, our study adapts it to the Web3 context by grounding the iterative cycles in the mapping of software quality assurance domains. This integration enabled the development of the guide through short iteration cycles, ensuring agility and responsiveness to real-world constraints and user needs. The methodology included six stages led by the VOH.CoLAB research team, in close collaboration with the Exeedme project manager, enabling a context-driven approach focused on the practical experience needs. Figure 1 presents the stages followed throughout the work.

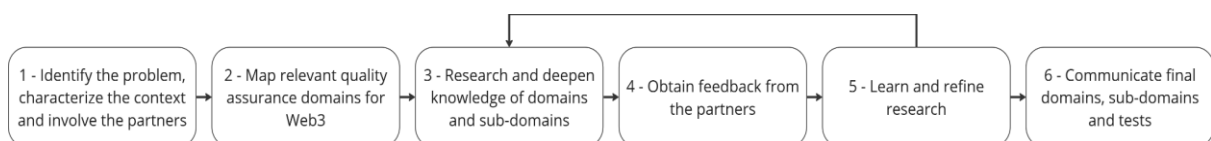


Figure 1. Test roadmap development methodology (adapted from (Londral et al., 2022))

2.1. Stage 1 - Identifying the Problem, Characterizing the Context, and Involving the Partners

The first stage followed the principles of DSR methodology, emphasizing early collaboration between stakeholders to ensure the solution addressed real needs. A series of videoconference meetings were held between the VOH.CoLAB research team and the Exeedme project team to discuss challenges related to software quality in blockchain-based gaming platforms.

These discussions helped both teams bring their perspectives: Exeedme shared insights from their operational experience in developing and managing a blockchain-based marketplace for virtual gaming assets, while VOH.CoLAB contributed expertise in software quality and methodological

frameworks. Together, they explored the limitations of existing standards, such as SQuaRE, for Web3 environments and identified the need for more practical, tailored guidance.

The main output of this stage was a shared understanding of the problem and its context.

2.2. Stage 2 - Map Relevant Quality Assurance Domains

This stage involved mapping test domains and subdomains to capture software development concerns from both teams and to provide the foundation for the following stages of solution development. Building on the challenges identified in Stage 1, an initial exploratory search in peer-reviewed databases (Scopus, Web of Science, and Google Scholar) using keywords such as software quality and blockchain quality assurance was conducted to scope the field and understand the key challenges. The review then concentrated on ISO/IEC documentation, which provided a preliminary set of domains to be used as the structured basis for supporting the definition of the relevant quality assurance domains.

2.3. Stages 3, 4, 5 - Iteration Cycles: Develop, Test and Learn

These stages were repeated for two iterative cycles of development, testing, and refinement, which led to the creation of the structure of the relevant domains and subdomains and to the discussion of potential tests for each domain and sub-domain. During these cycles, the VOH.CoLAB and Exeedme teams collaborated both through videoconference meetings and asynchronously by exchanging documents with the relevant information. The first cycle consisted of refining the preliminary set of test domains identified on Stage 2. With that objective in view, each domain was also divided into multiple sub-domains. The second cycle consisted of collaboratively defining a set of tests for each of the domains and subdomains. VOH.CoLAB proposed a set of tests for each domain and Exeedme provided valuable insights of the main functionalities, concerns and other technical details of Web3 applications, thus obtaining a set of tests that reflected the main areas of concern for platforms that use these technologies.

2.4. Stages 6 - Communicate final Domains, Sub-Domains and Tests

In the final stage, the full set of test domains, sub-domains, and tests was reviewed, finalized, and organized into a structured quality assurance guide. The final version was documented in a clear and practical format, making it easy to use for developers and teams working in Web3. The completed guide was then shared with all stakeholders, concluding the co-development process and preparing it for real-world testing.

3. Results

This section presents the results obtained by following the stages of the methodology. The process began with the partners' joint definition of the problem and characterization of the context. It then advanced to the mapping of internationally recognized software quality assurance domains, followed by iterative cycles of development, testing, and learning focused on the Web3 context. These steps

culminated in the creation of the quality assurance guide designed to strengthen software robustness and ensure compliance in Web3 applications.

3.1. Stage 1 - Identifying the Problem, Characterizing the Context, and Involving the Partners

The discussions between the VOH.CoLAB and Exeedme teams led to a shared aim: to design a quality assurance guide tailored to the specific demands of blockchain gaming applications. Rather than offering general principles, the guide aims to present a structured framework organized into testing domains and subdomains. This structure serves as a practical bridge between the SQuaRE international guidelines and the realities of Web3 development, enabling teams to identify and define tests corresponding to each subdomain. By outlining actionable components, the guide helps developers and organizations implement targeted quality assurance practices that support both compliance with international standards and high-performance outcomes in blockchain-based gaming platforms. This mutual alignment provided a clear foundation for the execution of the remaining stages of this study.

3.2. Stage 2 - Map Relevant Quality Assurance Domains

The focused literature review of international standards highlighted the ISO/IEC 25000 SQuaRE series as the main reference for mapping quality assurance domains. SQuaRE is a series of standards developed by ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) that focuses on defining and assessing the quality of systems and software (Febrero et al., 2016; Shtefan & Zaporozhets, 2021). The main objective of the SQuaRE standards is to provide a framework for evaluating software and system quality, ensuring that products meet quality requirements throughout their lifecycle. The international standards present two assessment models: product quality and quality-in-use, presented in Figure 2.

Product Quality							
Functional Suitability	Reliability	Performance Efficiency	Usability	Maintainability	Security	Compatibility	Portability
Functional completeness	Maturity	Time behaviour	Appropriateness recognisability	Modularity	Confidentiality	Co-existence	Adaptability
Functional correctness	Availability	Resource utilization	Learnability	Reusability	Integrity	Interoperability	Installability
Functional appropriateness	Fault tolerance	Capacity	Operability	Analysability	Non-repudiation		Replaceability
	Recoverability		User error protection	Modifiability	Accountability		
			User interface aesthetics	Testability	Authenticity		
			Accessibility				

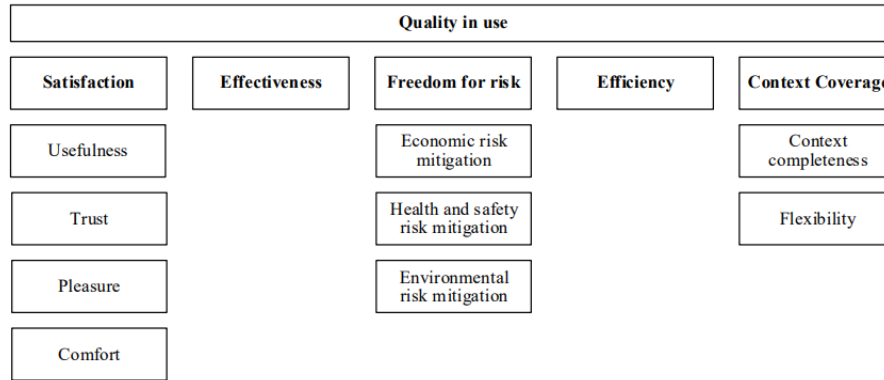


Figure 2. Characteristics and subcharacteristics of the Product Quality and Quality In Use Models Defined by the SQuaRE Standards (Febrero et al., 2016; Shtefan & Zaporozhets, 2021)

The product quality model defines eight characteristics: functional suitability, reliability, performance efficiency, usability, maintainability, security, compatibility, and portability, each subdivided into subcharacteristics that specify aspects of software behavior and value for end users. The quality-in-use model evaluates the impact of the product on stakeholders in real-use contexts, considering satisfaction, effectiveness, freedom from risk, efficiency, and context coverage. Together, these models provide a basis for defining requirements, generating evaluation measures, and supporting software quality assessment.

Based on this mapping, the teams reflected that, while comprehensive, the models were not always directly applicable to the context of decentralized, blockchain-based platforms. Several subcharacteristics required contextual adaptation to address the specificities of Web3 environments, such as smart contracts, decentralized architectures, and asset trading mechanisms. In addition, some re-structuring of the characteristics was deemed necessary so that the teams considered the structure was understandable. These adaptations were discussed in the subsequent iterative cycles of development, testing, and learning, so that teams agreed on a model that truly reflected the practical needs of blockchain-based gaming platforms.

3.3. Stages 3, 4, 5 - Iteration Cycles: Develop, Test and Learn

This first cycle of discussions and refinements led to the definition of the testing domains and subdomains most relevant for the Web3 environment, according to the involved teams. These domains and subdomains, presented in Table 1, aim to cover the widest possible range of functionalities to ensure that the system operates correctly, is secure, and meets business requirements. Thus, the objectives of each were carefully co-defined by the teams, drawing on the SQuaRE standards and on their expertise in the Web3 context. Following Table 1, the main aspects of software and infrastructure that need to be assessed and the main concerns raised in the collaborative discussions are presented, organised by domain.

Table 1. Test Domains and Subdomains and their Objectives.

Test Domain	Objective	Subdomains	Objectives
Functionality	Evaluate whether the platform meets the defined functional requirements.	Functional Completeness	Ensure the existence of the implementation of the expected features.
		Functional Correctness	Validate whether the results obtained within each implemented feature are as expected.
		Functional Appropriateness	Assess whether the provided functions are appropriate for the intended task.
Integration	Verify connectivity between the web platform and the blockchain network, ensuring seamless integration with external APIs (e.g., payment providers, authentication services) and proper data exchange.	Blockchain Integration	Verify that the communication between the Web3 software frontend and the blockchain is consistent, the execution of the programmed functions in the smart contracts produces the expected results and that these results are correctly reflected to the user.
		Integration with third-party APIs	Ensure seamless communication between the software and other APIs, namely from game platforms and other skin marketplaces.
		Payment API Integration	Ensure that the software handles payment responses correctly by only updating the blockchain when payments succeed, preventing changes if they fail and clearly informing the user throughout the process.
Security	Ensure the software's resilience against external attacks.	Smart contracts	Test smart contract code resilience to external attacks.
		Decentralized Apps	Test website resilience to external attacks.
Performance	Confirm that the software utilizes system resources efficiently.	Time Behaviour	Evaluate the speed of actions performed with a special focus on skin transactions.
		Resource Utilization	Assess the system's ability to perform its normal activities without consuming excessive resources.
		Capacity	Evaluate how the platform reacts under increasing loads of users and transactions, in order to identify potential bottlenecks.

Usability	Evaluate how easy and efficient it is for users to interact with the software.	Operability	Evaluate how easy it is to operate in the Web3 application and how this ease encourages users to stay on the platform.
		Navigation	Evaluate how easily users can navigate between different pages of the website, to determine whether their daily interactions are intuitive and free from major difficulties in understanding the steps needed to reach their goals.
		User responsiveness	Ensure a smooth experience where users feel that their activities on the platform are seamless and uninterrupted.
Portability	Assess the software's ability to operate across different environments and devices.	Adaptability	Test the software's compatibility across different browsers and devices.
		Substitutability	Evaluate how easily certain components can be replaced with components with other technologies or providers.
Recoverability	Measure the system's ability to restore data and recover from failures.	-	-
Resilience	Analyze the platform's capability to maintain operations during partial service disruptions.	-	-

3.3.1. Functionality domain

Functionality domain assesses whether the Web3 software defined functions provide everything required to complete the user's tasks and whether they do so accurately and correctly. Finally, it determines whether the offered functionalities are relevant to the software's intended use objectives. *Functionality* domain is divided into three subdomains. The *functional completeness* subdomain aims to ensure the implementation of the expected functionalities in a skin marketplace, such as user registration, login, purchasing, selling and listing skins, whereas the primary purpose of *functional correctness* subdomain is to validate whether the outcomes obtained within each implemented functionality are as expected. The *functional appropriateness* subdomain aims to assess whether the provided functions are suitable for the intended task.

3.3.2. Integration domain

Integration domain verifies the connectivity between the web platform and the blockchain network, ensuring seamless integration with external APIs (e.g., payment providers, authentication services) and proper data exchange. This verification allows the Web3 software to communicate with the blockchain to record and maintain the transaction history and ownership of skins as they are traded,

ensuring greater transparency. The Integration domain is divided into three subdomains. The *Blockchain Integration* subdomain verifies that the communication between the marketplace API and the blockchain is consistent, that smart contract functions execute as intended, and that their results are accurately reflected in the frontend for the user. The *Integration with third-party APIs* subdomain focuses on validating the integration with third-party authentication providers, such as Steam in the case of gaming platforms, to streamline the login process and enhance security through features like two-factor authentication (2FA). Finally, the Payment API Integration subdomain assesses the integration with trusted payment services, such as PayPal, which supports smoother new user onboarding and promotes greater platform usage, since these providers already have established credibility and transparency within the community.

3.3.3. Security domain

Security testing on the platform is of great importance as it ensures the Web3 software resilience to external attacks that could compromise its operation. Responsibility for security is shared between the Web3 application and the underlying blockchain infrastructure, with each requiring targeted tests. For the Web3 software, it is necessary to safeguard all personal data of registered users, ensuring secure registration and login processes. For the blockchain, the primary focus of testing will be on smart contracts, given their central role in recording transactions conducted in the Web3 software. *Security* domain is divided into two subdomains: *Smart Contracts* and *Decentralized Apps*. One of the most critical components in the marketplace's security is testing the *Smart Contracts*, which are responsible for recording key information, such as skin ownership and market value. If these contracts are not regularly audited to identify potential bugs and areas for improvement, the marketplace could be exposed to a wide range of attacks. Potential security vulnerabilities in the marketplace's smart contracts include reentrancy attacks, integer overflow and underflow, return values, access control, front-running, denial of service attacks, uninitialized storage pointers, and timestamp dependency (Jiao et al., 2024). Additionally, as a *Decentralized App*, the Web3 software is susceptible to common web application attacks such as Cross-Site Scripting or SQL injection attacks. Together, these subdomains ensure components are secure, supporting trustworthy and robust Web3 software.

3.3.4. Performance domain

Performance domain refers to how effectively the software utilizes system resources. It is divided into three subdomains. *Time behaviour* subdomain tests should measure how fast the Web3 software performs actions (for e.g., skin transactions in the case of gaming platforms). Faster response times improve the user experience. However, due to the nature of blockchain, instant responses aren't always possible. It's important to also check the delays between the Web3 software, the blockchain, and other systems to find areas that can be optimized. When it comes to the *Resource Utilization* subdomain, blockchain systems can require significant resources to complete transactions or run smart contracts. Higher resource use leads to more energy consumption and higher gas fees. By evaluating gas fees in terms of energy use, we can consider how sustainable the platform is over time. Inefficient blockchains may cause unnecessary financial and environmental costs. The *Capacity*

subdomain evaluates how the platform handles more users and transactions. It helps find performance bottlenecks so improvements can be made without disrupting normal use. Like time behavior tests, capacity testing should assess both the Web3 software and the blockchain, as each can face different challenges that may need unique solutions.

3.3.5. Usability domain

Usability domain aims to assess the overall user experience in the Web3 software and the ease of use of the platform. The clarity of the interfaces will be a crucial factor in the platform's impact on users, contributing to increased usage and user retention. User feedback will play a vital role in evaluating the Web3 software usability and will provide valuable insights for refining the visual design and available functionalities, with the goal of continuously enhancing the user experience. *Usability* domain is divided into three subdomains. *Operability* subdomain aims to evaluate how easy it is to operate in the Web3 software and how this ease encourages users to stay on the platform. *Navigation* subdomain aims to evaluate how easily users can move between different pages of the Web3 software, allowing for an analysis of whether everyday operations are intuitive and can be performed without significant interpretation difficulties. Finally, for a positive user experience, the platform must respond to user actions as promptly as possible, contributing to a seamless experience where users feel that activities on the platform are uninterrupted. The *User Responsiveness* subdomain assesses these aspects of the software utilization.

3.3.6. Portability domain

Portability domain refers to the Web3 software's ability to operate across different environments and devices. It is divided into two subdomains. *Adaptability* subdomain aims to evaluate the platform's compatibility across various browsers (Chrome, Firefox, Safari, etc.) and devices (desktop, mobile, tablet). *Substitutability* subdomain refers to the ease with which specific Web3 software components can be replaced by alternative solutions, to ensure these transitions can occur swiftly, cost-effectively, and without service interruptions, maintaining continuity for both users and systems. The ability to easily replace software components enables organizations to respond rapidly to technological changes or emerging market needs, ensuring that they are using the most suitable or up-to-date solutions.

3.3.7. Recoverability domain

Recoverability domain refers to the Web3 software ability to restore data and recover its state after failures. It is essential to ensure that the marketplace has effective backup and recovery procedures so that if a severe failure occurs that renders the system unavailable, it will be possible to restore the system to its original state without affecting users. It has no defined subdomains.

3.3.8. Resilience domain

Resilience domain aims to assess the Web3 software ability to continue operating during partial service interruptions. Similar to the recoverability testing domain, this domain has no defined subdomains.

3.3.9. The use of domains and subdomains in practice

Following the definition of testing domains and subdomains tailored to the Web3 context, the proposed structure was evaluated through its application in a second iteration cycle. In this phase, a set of 108 tests were systematically defined with Exeedme, aligned with the domains and subdomains and tailored to the requirements of their gaming platform.

The tests were obtained by following the methodology described in section 2. They were initially defined by VOH.CoLAB research team on the basis of research. These were subsequently reviewed by Exeedme, who provided feedback and valuable insights. This collaborative exchange not only validated the methodology but also guided further refinement, ensuring a more comprehensive and rigorous approach of the tests that can be applied in a Web3 platform. This process went through several iterative cycles, ultimately resulting in the tests presented in Table 2, which presents the distribution of these tests across the defined domains and subdomains.

These individual tests were not intended as standalone results, but rather as a demonstration of how the structured model can effectively guide the design of relevant and context-specific quality assurance activities.

Table 2. Distribution of tests by domain (and subdomain when applicable)

Domain	Subdomain (number of tests by subdomain)	Total number of tests
Functionality	Functional Completeness (11) Functional Correctness (13) Functional Appropriateness (10)	34
Integration	Blockchain Integration (9) Payment API Integration (4) Third-party API Integration (2)	15
Security	Smart Contracts (12) Decentralized Apps (8)	20
Performance	Time Behaviour(5) Capacity (4) Resource Utilization (2)	11
Usability	Navigation (5) Operability (5) User Responsiveness (2)	12
Portability	Adaptability (2) Substitutability (4)	6
Recoverability tests	-	3
Resilience tests	-	7

During the iteration cycles, both teams agreed that a critical component in safeguarding the security of a blockchain-based platform lies in the systematic testing of smart contracts, which are responsible for recording highly sensitive information, such as the ownership of skins and their market value. Without frequent audits aimed at identifying potential improvements and vulnerabilities in the code, these contracts could become a major source of risk, leaving the marketplace exposed to a wide spectrum of possible attacks. This spectrum has been analyzed and several tests were defined to cope with potential threats in the platform's smart contracts.

The set of tests were defined in the *Security* domain, namely in the *Smart Contracts* subdomain. They can prevent several attack types, such as the reentrancy attack, where a smart contract makes an external call to another contract before updating its own state. If the external contract calls back into the original contract during this process, the original contract's logic can be exploited, potentially allowing multiple withdrawals of funds before the state is correctly updated. Table 3 shows the tests defined for the *Smart Contracts* subdomain.

Table 3. Smart contracts tests

Test type	Description	Objective
Reentrancy	Simulate consecutive fund withdrawals through smart contract execution	Test the smart contracts' resilience to reentrancy attacks
	Simulate consecutive skin purchases through smart contract execution	
	Simulate consecutive skin sales through smart contract execution	
	Simulate consecutive skin trades through smart contract execution	
Overflow	Trigger overflow in possible integer variables of the smart contract	Ensure that the smart contract has no variables that can cause overflow
Underflow	Trigger underflow in possible integer variables of the smart contract	Ensure that the smart contract has no variables that can cause underflow
Return Values	Check that in smart contracts relying on external contracts, the return values are correct and being validated	Ensure the smart contract has no validation flaws that could cause unexpected results
Execution Authorization	Simulate unauthorized access by users trying to execute smart contracts	Ensure the smart contract can only be executed by authorized users
Front-running	Simulate execution of multiple transactions and verify if they are vulnerable to front-running	Ensure the smart contract has mechanisms to prevent attackers from front-running sensitive transactions
Denial of Service	Simulate execution of multiple transactions and monitor gas costs	Ensure the smart contract has mechanisms to prevent reaching the allowed gas limits

Uninitialized Pointers	Simulate smart contract execution and verify that variable initialization is well-defined	Ensure the smart contract has no pointer vulnerable to data replacement
Timestamp Dependency	Check that there are no variables dependent on timestamps	Avoid unfair transaction mining

Other tests were defined for evaluating the user experience, which is a relevant aspect of the success of a skin marketplace. For example, the *Navigation* subdomain tests defined in Table 4 aim to assess the software capabilities in this area by evaluating some of the generic functionalities of a skin marketplace and how the users respond to the developed frontend.

In practice, the subjects can be asked to complete the most important tasks while their performance (e.g. completion rate, time taken, number of errors) and subjective feedback were recorded. These tests aim to capture both the efficiency of the developed frontend and the intuitiveness of its design. They also assess if the platform matches the users expectations and introduces new features that improve user experience.

Although *Navigation* is used here as an example, similar procedures were applied to other functional areas to ensure a comprehensive evaluation of the overall user experience, such as *Operability* which focuses on measuring simplicity, clarity and ease-of-use, whereas *User Responsiveness* tests measure the users' perception of waiting time for different actions in the platform. The objective is to assess not only the actual system response time but also how this duration is subjectively perceived by users. To this end, the effectiveness of progress indicators and waiting messages is tested, examining whether they help reduce perceived frustration and increase the sense of transparency during the process, again by gathering the subjective feedback of users.

Table 4. *Navigation* subdomain tests

Type	Description	Objective
Navigation	Ask users to list an item for sale	Evaluate whether users can navigate the marketplace easily and quickly find the features.
	Ask users to perform tasks such as finding a specific skin	
	Ask users to access the transaction history	
	Ask users to access their profile	
	Ask users to access notifications	

4. Discussion

This study proposed a structured quality assurance guide for blockchain-based applications. Departing from the ISO/IEC SQuaRE model, the guide defines eight testing domains and 16 associated subdomains tailored to the unique requirements of Web3 systems. This structure was tested in practice for the case of a blockchain-based marketplace for virtual gaming assets, for which 108 tests were defined within the domains and subdomains. The key contribution of this study lies not in the 108 individual tests defined, but in the underlying structure that supports systematic, context-specific quality assurance practices (Precht et al., n.d.; J. Xu et al., 2020). This model enables both developers and quality assurance professionals to bridge the gap between high-level international standards and the operational realities of decentralized application development.

4.1 Defined Domains and Subdomains

The defined domains reflect a balance between user-oriented quality concerns and technical development needs. Domains and subdomains such as *Usability* and *Functional Appropriateness* (in *Functionality*) focus on the end-user experience, ensuring the software provides a satisfactory experience, conveys trust, and meets the main needs of the users. These concerns align with findings that user satisfaction and perceived quality are central to adoption and sustained use of digital platforms (Bevan, 2009; Kitchenham & Pfleeger, 1996). Although user experience is a concern for every platform, and not exclusive to Web3 platforms, there is still a gap in expectations between users that typically use Web2 and Web3 platforms (Hou, 2024). Therefore, the tests designed for evaluating a Web3 platform user experience should be tailored to the specific requirements of its users, such as transaction transparency and system control.

The work of (Vacca et al., 2024) highlights that having functional evaluation framework may contribute to ensuring contract quality prior to deployment, one of the main components tested *Functional Correctness* (in *Functionality* domain). As (Vacca et al., 2024) suggests these tests may be conducted by using tools that assess the smart contracts code. Additionally, the proposed tests for *Functional Appropriateness* subdomain include frontend validation to determine whether the outcomes of marketplace transactions display all relevant information.

Despite not considering user feedback, implementing tests that aim to improve the marketplace's performance will contribute to a faster, more efficient, and smoother marketplace experience. The *Performance* domain aims to evaluate the latency of the system, from the smart contracts time response to the overall time the application takes to complete a transaction and register it in the blockchain. As referred in (Zhang et al., 2021) the gas price is a key parameter controlled by users, so *Resource Utilization* subdomain tests have an important role in maximizing the marketplace's user adoption.

The *Security* domain emerged as particularly vital, given the trust-sensitive nature of blockchain-based marketplaces and the high prevalence of attacks targeting smart contracts (Atzei et al., 2017). Quality assurance for smart contracts is not trivial as errors are immutable post-deployment and can have irreversible financial consequences.

In addition to verifying contract behavior, the model includes tests for common web vulnerabilities and GDPR compliance, acknowledging the increasing importance of privacy, users' trust and regulatory alignment in decentralized systems (Finck, 2018). To assess GDPR compliance in a blockchain-based marketplace, the tests may examine how personal data is collected, stored, and processed, and if it ensures that user rights such as access and erasure are respected despite the immutability of the ledger (Belen-Saglam et al., 2023). Another important aspect would be the Governance quality assessment. This can be evaluated by reviewing the clarity of decision-making structures, transparency of policies, and the presence of accountability mechanisms such as audits or dispute resolution processes (Ibrahimi et al., 2024). The tests raised by both teams focus on document analysis (whether they exist and clarity of the documentation), technical audits of smart contracts and off-chain infrastructure, compliance checklists against legal and governance standards, and user studies to evaluate the accessibility and effectiveness of rights and decision-making processes.

Similar to the *Functionality* domain, the *Portability* domain has aspects that can be evaluated from the user's perspective, such as the *Adaptability* subdomain. Additionally, the *Replaceability* subdomain may also impact development teams. The ability to develop code that is adaptable to various technologies and reusable contributes to greater flexibility in blockchain ecosystems, where rapid technological evolution is the norm (X. Xu et al., 2019).

At last, although domains like *Resilience* and *Recovery* are not directly user-facing, they improve maintainability, uptime, and failure response – factors that significantly contribute to user trust and satisfaction in the long term (Wagner & Deissenboeck, 2007). The tests suggest the simulation of blockchain network failures or timeouts to assess if the marketplace does not compromise important data nor the subsequent pending transactions.

4.2 Practical Implications of the findings

The practical testing of the proposed structure was achieved through its application to a real blockchain gaming platform. The 108 defined tests were not meant to be exhaustive or universal; rather, they illustrate how the structure guides meaningful quality assurance activity within a specific context. This operationalization addresses concerns raised in the literature that international standards like ISO/IEC SQuaRE, while theoretically robust, often lack practical guidance and are difficult to adopt in agile or domain-specific environments (Gordieiev et al., 2024; Suryn et al., 2003).

Theoretically, this study contributes to the broader effort of adapting classical quality assurance models to emerging technologies. It shows how high-level constructs such as *Functional Suitability* or *Compatibility* can be translated into blockchain-based environments. This supports the idea that models like SQuaRE can retain relevance if implemented through context-aware, modular, and testable structures ("ISO/IEC 25010," 2023; Kitchenham & Pfleeger, 1996).

In practice, the model supports integration into modern software engineering pipelines, such as continuous deployment. Many of the tests, particularly those in the *Functionality*, *Security*, and

Resilience domains, can be implemented as automated unit tests to be used, for instance, in the context of releasing new features, where they would be automatically executed whenever a release occurs. This not only enables early error detection and control but also fosters modular architecture and maintainable code, a recognized benefit of test-driven development practices (Janzen & Saiedian, 2005). The *Modularity* test presented under *Resilience* domain, for example, is directly aligned with these software engineering principles.

Beyond the technical implementation, it is important to situate quality assurance within the broader systemic debates surrounding Web3. As highlighted in recent work (Balduf et al., 2023; Esposito et al., 2025; Hawes, 2023), the promise of decentralization is often undermined by infrastructural centralization, for example reliance on cloud providers or concentration of nodes in limited geographies, and by governance asymmetries that concentrate decision-making power in the hands of a few actors. These dynamics directly influence resilience and security, while also shaping how quality and trust are understood within decentralized ecosystems. Ensuring a shared understanding of these dimensions, alongside transparent governance mechanisms and awareness of infrastructural dependencies, is essential to connect software quality assurance with sustainability.

The objective of this framework is that it can be generalized into other Web3 softwares. While the methodology provides a domain-agnostic process for co-developing quality assurance approaches in Web3, the framework organizes Web3 domains and subdomains that could be applicable to other cases. For instance, if one would apply the framework to DeFi, the domain and subdomain structure could be maintained, but the subdomain objectives and examples shift to DeFi risks and features (Ma et al., 2023; Zhou et al., 2023). *Functionality* would test the correctness and appropriateness of smart contract logic for swaps or loans, Integration would validate oracles, wallets, and payment rails. *Security* would focus on resistance to exploits like flash-loan attacks. *Performance* and *Usability* would then assess transaction speed, cost efficiency, and user experience across different wallets and networks, similarly to what is already tested in this framework.

4.3 Strengths and limitations of the study

A key strength of this study lies in its co-design methodology, involving collaboration between researchers and industry actors. This ensured the resulting guide is grounded in both theory and the practical constraints of software teams working in Web3 environments. However, the study is not without limitations. The framework was only applied to one use case, a virtual asset trading platform, so broader applicability remains to be evaluated. Moreover, while the defined tests were developed and refined in collaboration with stakeholders, the defined tests have not yet been deployed and assessed in a live production setting.

5. Conclusions

This study provides a structured and actionable quality assurance guide for blockchain-based applications, that supports teams in identifying and defining tests systematically. We demonstrate that it is possible to use international standards to evaluate and enhance blockchain applications

systematically. This research contributes to bridging the gap between theoretical frameworks and practical implementation, fostering the development of high-quality Web3 applications and assisting the certifying path of Web3 software.

Future research should focus on expanding and refining the proposed domains and subdomains based on the practical insights of Web3 software development teams. Applying the framework to different contexts, such as decentralized finance (DeFi) or NFT platforms, could reveal additional quality dimensions or require new adaptations. Furthermore, estimating the effort required to implement tests in each subdomain would enhance the model's applicability by supporting test prioritization and strategic planning, particularly for teams with limited resources.

References

- Atzei, N., Bartoletti, M., & Cimoli, T. (2017). *A survey of attacks on Ethereum smart contracts*.
- Balduf, L., Korczyński, M., Ascigil, O., Keizer, N. V., Pavlou, G., Scheuermann, B., & Król, M. (2023). The Cloud Strikes Back: Investigating the Decentralization of IPFS. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC, 1*, 391–405. <https://doi.org/10.1145/3618257.3624797>
- Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2023). A systematic literature review of the tension between the GDPR and public blockchain systems. *Blockchain: Research and Applications*, 4(2), 100129. <https://doi.org/10.1016/J.BCRA.2023.100129>
- Bevan, N. (2009). Extending Quality in Use to Provide a Framework for Usability Measurement. In M. Kurosu (Ed.), *Human Centered Design* (pp. 13–22). Springer. https://doi.org/10.1007/978-3-642-02806-9_2
- BlockchainPT*. (2025). <https://blockchain.void.pt/>
- CSGO & CS2 Item Economy: 2023 Overview and 2024 Thoughts. (2024). In *Swap.gg*. <https://swap.gg/blog/csgo-item-economy-2023-overview>
- Esposito, M., Tse, T., & Goh, D. (2025). Decentralizing governance: exploring the dynamics and challenges of digital commons and DAOs. *Frontiers in Blockchain*, 8, 1538227. <https://doi.org/10.3389/FBLOC.2025.1538227/BIBTEX>
- Febrero, F., Calero, C., & Ángeles Moraga, M. (2016). Software reliability modeling based on ISO/IEC SQuaRE. *Information and Software Technology*, 70, 18–29. <https://doi.org/10.1016/j.infsof.2015.09.006>
- Finck, M. (2018). Blockchains and Data Protection in the European Union. *European Data Protection Law Review*, 4(1), 17–35. <https://doi.org/10.21552/edpl/2018/1/6>
- Gordieiev, O., Rainer, A., Kharchenko, V., Pishchukhina, O., & Gordieieva, D. (2024). A Unified Approach to the Development of Technology-Based Software Quality Models on the Example of Blockchain Systems. *IEEE Access*, 12, 118875–118889. <https://doi.org/10.1109/ACCESS.2024.3448271>
- Hawes, B. (2023). *Web3: The Promise & the Reality*.
- Hevner, A., & Park, J. (2004). *Design Science in Information Systems Research*. <https://www.researchgate.net/publication/201168946>
- Hossain Faruk, M. J., Raya, P., Siam, M. K., Cheng, J. Q., Shahriar, H., Cuzzocrea, A., & Bringas, P. G. (2024). A Systematic Literature Review of Decentralized Applications in Web3: Identifying Challenges and Opportunities for Blockchain Developers. *Proceedings - 2024 IEEE International Conference on Big Data, BigData 2024*, 6240–6249.

- <https://doi.org/10.1109/BIGDATA62323.2024.10826066>
- Hou, C.-C. (2024). *Optimizing User Experience of Decentralized Applications for Web2 and Web3 Users - Case Anonymous Decentralized Social Platform*. <https://aaltodoc.aalto.fi/handle/123456789/133628>
- Ibrahimi, M. M., Norta, A., & Normak, P. (2024). Blockchain-based governance models supporting corruption-transparency: A systematic literature review. *Blockchain: Research and Applications*, 5(2), 100186. <https://doi.org/10.1016/J.BCRA.2023.100186>
- ISO/IEC 25010:2023. (2023). In ISO. <https://www.iso.org/standard/78176.html>
- Janzen, D., & Saiedian, H. (2005). Test-driven development concepts, taxonomy, and future direction. *Computer*, 38(9), 43–50. <https://doi.org/10.1109/MC.2005.314>
- Jiao, T., Xu, Z., Qi, M., Wen, S., Xiang, Y., & Nan, G. (2024). A Survey of Ethereum Smart Contract Security: Attacks and Detection. *Distributed Ledger Technologies: Research and Practice*, 3(3). <https://doi.org/10.1145/3643895>
- Kitchenham, B., & Pfleeger, S. L. (1996). Software quality: the elusive target [special issues section]. *IEEE Software*, 13(1), 12–21. <https://doi.org/10.1109/52.476281>
- Londral, A., Azevedo, S., Dias, P., Ramos, C., Santos, J., Martins, F., Silva, R., Semedo, H., Vital, C., Gualdino, A., Falcão, J., Lapão, L. V., Coelho, P., & Fragata, J. G. (2022). Developing and validating high-value patient digital follow-up services: a pilot study in cardiac surgery. *BMC Health Services Research*, 22(1). <https://doi.org/10.1186/s12913-022-08073-4>
- Ma, W., Zhu, C., Liu, Y., Xie, X., & Li, Y. (2023). A Comprehensive Study of Governance Issues in Decentralized Finance Applications. *ACM Transactions on Software Engineering and Methodology*, 1. <https://doi.org/10.1145/3717062>
- Mubarkoot, M., Altmann, J., Rasti-Barzoki, M., Egger, B., & Lee, H. (2023). Software Compliance Requirements, Factors, and Policies: A Systematic Literature Review. *Computers & Security*, 124, 102985. <https://doi.org/10.1016/J.COSE.2022.102985>
- NFT - Worldwide Statista Market Forecast. (n.d.). In Statista. <https://www.statista.com/outlook/fmo/digital-assets/nft/worldwide>
- NFT statistics in 2024: Growth trends and outlook Kraken. (n.d.). <https://www.kraken.com/pt-br/learn/nft-statistics>
- Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77. <https://doi.org/10.2753/MIS0742-1222240302>
- Precht, H., Wunderlich, S., & Marx Gómez, J. (n.d.). *Applying Software Quality Criteria to Blockchain Applications: A Criteria Catalog*. <https://hdl.handle.net/10125/64511>
- Shtefan, N., & Zaporozhets, O. (2021). Software quality model based on SQuaRE standards. *Radiotekhnika*, 207, 159–165. <https://doi.org/10.30837/rt.2021.4.207.17>
- Suryn, W., Abran, A., & April, A. (2003). *ISO/IEC SQuaRE. The second generation of standards for software product quality*.
- Tsuda, N., Washizaki, H., Honda, K., Nakai, H., Fukazawa, Y., Azuma, M., Komiyama, T., Nakano, T., Suzuki, H., Morita, S., Kojima, K., & Hando, A. (2019). WSQF: Comprehensive Software Quality Evaluation Framework and Benchmark Based on SQuaRE. *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, 312–321. <https://doi.org/10.1109/ICSE-SEIP.2019.00045>
- Vacca, A., Fredella, M., Di Sorbo, A., Visaggio, C. A., & Piattini, M. (2024). Functional suitability assessment of smart contracts: A survey and first proposal. *Journal of Software: Evolution and Process*, 36(7), e2636. <https://doi.org/10.1002/SMR.2636>
- Wagner, S., & Deissenboeck, F. (2007). An Integrated Approach to Quality Modelling. *Fifth International Workshop on Software Quality (WoSQ'07: ICSE Workshops 2007)*, 1. <https://doi.org/10.1109/WOSQ.2007.3>
- Xu, J., Zhang, H., & Gong, J. (2020). *Analysis for Blockchain Application Quality*.

- Xu, X., Weber, I., & Staples, M. (2019). Architecture for Blockchain Applications. *Architecture for Blockchain Applications*. <https://doi.org/10.1007/978-3-030-03035-3/COVER>
- Zhang, L., Lee, B., Ye, Y., & Qiao, Y. (2021, April 19). Evaluation of Ethereum End-To-end Transaction Latency. *2021 11th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2021*. <https://doi.org/10.1109/NTMS49979.2021.9432676>
- Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., & Gervais, A. (2023). *SoK: Decentralized Finance (DeFi) Attacks*. <https://doi.org/10.1109/SP46215.2023.00180>

Trust, Privacy and Authenticity in Scientific Data Sharing: The Role of Blockchain and Zero Knowledge Proofs

Joana Almeida
*Escola Superior de Tecnologia
e Gestão de Águeda, Portugal*
jsalmeida@ua.pt
0009-0007-5316-8455

Rita Santos
*Escola Superior de Tecnologia
e Gestão de Águeda, Portugal*
rita.amaral.santos@ua.pt

Ciro Martins
*Escola Superior de Tecnologia
e Gestão de Águeda, Portugal*
ciro.martins@ua.pt
0000-0003-0970-586X

Hélder Gomes
*Escola Superior de Tecnologia
e Gestão de Águeda, Portugal*
helder.gomes@ua.pt
0000-0001-8443-4196

Cármén Guimarães
*Escola Superior de Design,
Gestão e Tecnologias da
Produção de Aveiro –Norte,
Portugal*
carmenguimaraes@ua.pt
0000-0003-4159-5453

Fernando Costa
*Instituto Superior de
Contabilidade e Administração
da Universidade de Aveiro,
Portugal*
fernando.costa@ua.pt
0000-0002-2346-3038

Pedro Colarejo
Load Interactive, Portugal
pedro.colarejo@load.digital
0000-0003-4734-6319

Afonso Monteiro
Load Interactive, Portugal
afonso.monteiro@load.digital

Liliana Vale Costa
*DigiMedia, Departamento de
Comunicação e Arte,
Universidade de Aveiro,
Portugal*
lilianavale@ua.pt
0000-0003-2451-3073

Received: 6 June 2025

Accepted: 24 November 2025

Abstract

Efficient and secure sharing of scientific data remains a key challenge in the Open Science framework, especially in terms of data authenticity, provenance and privacy. Traditional digital repositories improve access but often lack decentralized mechanisms that guarantee integrity and traceability. Blockchain technology provides a potential solution through tamper-proof records and distributed consensus, while Zero Knowledge Proofs (ZKP) can enhance privacy protection. This study explores how blockchain and ZKP can be integrated for decentralized scientific data management. A systematic literature review reveals limited application of these combined technologies in Open Science, highlighting a research gap and the need for solutions that support transparent, secure and privacy-preserving data sharing in accordance with FAIR principles.

Keywords *Open Science, Scientific Data Sharing, Blockchain, Zero Knowledge Proofs*

1. Introduction

Scientific progress relies on the ability of researchers to generate, analyze and share data in a reliable, transparent and reproducible manner. However, the increasing complexity and volume of scientific datasets, coupled with growing concerns about data ownership, misuse and reproducibility, present significant challenges to the research community. Many scientists face difficulties in obtaining proper recognition for their data contributions, ensuring the long-term integrity of their datasets and verifying the authenticity of research outputs. Furthermore, conventional data-sharing practices frequently lack secure mechanisms for tracking provenance and preventing unauthorized

modifications. These limitations undermine trust in research findings and restrict opportunities for collaboration, transparency and knowledge dissemination.

Advances in digital computing, communications, sensors and storage technologies are transforming scientific, engineering and medical research. These technologies enable researchers to generate, analyze, and share large datasets, address previously intractable questions, refine theoretical models through simulations, and collaborate in interdisciplinary and international teams. As a result, research activities have become more data-intensive and open, connecting researchers, policymakers, and the public more closely (The National Academies Press, 2009).

However, these advancements present significant challenges. Verifying data accuracy becomes more complex due to the sheer volume and intricate processing involved. Rapid technological innovation, lack of standardized practices and concerns over privacy, national security and commercial interests hinder data sharing, affecting reproducibility. Long-term data preservation is also increasingly difficult, particularly for smaller projects, which still represent the majority of research activities (Alsaigh et al., 2024).

Effective data management is essential not as an end in itself, but as a driver of knowledge discovery, innovation and the seamless integration and reuse of data across the research community. Nevertheless, persistent infrastructural and cultural barriers, such as time constraints, concerns over misuse and lack of academic incentives, continue to limit the full realization of research investments (Soeharjono & Roche, 2021).

In this context, emerging technologies such as blockchain technology (BT) and Zero-Knowledge Proofs (ZKP) have been proposed as potential approaches to support trust, privacy and authenticity in scientific data sharing. Blockchain's decentralized and immutable architecture can provide mechanisms to support data integrity, traceability and provenance, although practical implementations may involve trade-offs in cost, scalability and complexity (Anderberg, A. et al., 2019; Nakamoto, 2008). Moreover, ZKP, including succinct non-interactive arguments of knowledge (zk-SNARK), provide advanced cryptographic methods for privacy-preserving data verification (Goldwasser et al., 1985; Liu et al., 2025). These mechanisms allow researchers to validate the integrity and authenticity of scientific data without disclosing sensitive or proprietary information.

Building on the principles of Open Science, which advocates for transparency, accessibility and collaboration in research, Decentralized Science (DeSci) has emerged as an extension of Open Science to build decentralized, community-governed scientific ecosystems (Leible et al., 2019). DeSci aims to address challenges in data ownership, access control and funding through decentralized autonomous organizations (DAO), tokenized incentives and privacy-preserving validation techniques, such as ZKP (Díaz et al., 2025; Weidener & Spreckelsen, 2024). These innovations promote greater inclusivity, transparency and equity in scientific collaboration, while aligning with the FAIR data principles and reinforcing the goals of Open Science (Wilkinson et al., 2016).

This paper explores how BT and ZKP can enhance scientific data management by enabling secure, transparent and privacy-preserving provenance and traceability, in alignment with FAIR data and Open Science principles. It addresses this through the following research questions:

- Research Question 1 (RQ1): What are the primary challenges in managing and sharing scientific data, particularly in terms of authenticity, data provenance and ownership?
- Research Question 2 (RQ2): How can BT and ZKP ensure the integrity, transparency and traceability of scientific data, particularly regarding its provenance?

To address the research questions, the paper begins by outlining the theoretical foundations of Open Science, BT, ZKP and DeSci. It then describes the methodological approach, including data sources and criteria for the literature review. The analysis explores how BT and ZKP contribute to overcoming key barriers in scientific data sharing- particularly regarding authenticity, provenance and privacy. It also identifies existing limitations and proposes future research directions. Finally, the paper reflects on the broader implications for building secure and transparent infrastructures for scientific collaboration.

2. Theoretical Framework

The theoretical framework guiding this research is structured into three core domains: Open Science, BT and ZKP, each of which is discussed in the following subsections.

2.1. Open Science

Open Science requires a clear definition and a shared understanding and considerable efforts have been made in recent years to refine this concept. Initially, Open Science focused on fostering openness and collaboration in knowledge creation and data sharing, emphasizing transparency, accessibility and participation in scientific research (Bartling & Friesike, 2014). Over time, Open Science has evolved beyond access to research outputs, incorporating new practices and technological advancements that facilitate broader dissemination and engagement. The FAIR data principles were introduced later, in 2016, as a complementary framework designed to enhance the management, stewardship and reuse of scientific data within the broader context of Open Science (Wilkinson et al., 2016). While FAIR provides concrete guidelines for data handling and interoperability, Open Science encompasses a wider paradigm that includes open access, open peer review, citizen science and collaborative research initiatives.

According to Benedikt Fecher and Sascha Friesike (2014, p. 17), “Open Science is an umbrella term encompassing a multitude of assumptions about the future of knowledge creation and dissemination”. It represents a scientific culture characterized by openness, where researchers share results rapidly with a broad audience. The Internet has further enabled this openness, transforming scientific collaboration and dissemination methods.

International institutions emphasize science as essential for participatory societies. Among the most significant references is the Universal Declaration of Human Rights, which in Article 27 states that “everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits”. While affirming the right of individuals to benefit from academic research, the declaration simultaneously protects the rights of authors over the scientific knowledge they produce, emphasizing that “everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author” (United Nations General Assembly, 1948, p. 4).

Building upon this global governance framework, the United Nations Educational, Scientific and Cultural Organization (UNESCO) has reinforced the importance of Open Science for public benefit. According to UNESCO, promoting science that is more accessible, inclusive and transparent directly contributes to ensuring that all individuals can share in scientific advancements and their benefits, as outlined in Article 27.1 of the Universal Declaration of Human Rights (UNESCO and Canadian Commission for UNESCO, 2022).

To this end, the UNESCO Recommendation on Open Science provides an overarching definition, describing Open Science as “an inclusive construct that combines various movements and practices aiming to make multilingual scientific knowledge openly available, accessible and reusable for everyone, to increase scientific collaborations and sharing of information for the benefits of science and society and to open the processes of scientific knowledge creation, evaluation and communication to societal actors beyond the traditional scientific community” (UNESCO, 2021, p. 7).

The European Union (EU) has played a central role in promoting Open Science through various initiatives and legislative frameworks over the past two decades. In 2005, the European Commission reaffirmed its commitment to openness in research with the European Charter for Researchers, advocating for accessible scientific results (European Commission, 2005). This was followed in 2007 by the EU Council’s support for open access experimentation, leading to the establishment of an Open Access policy under the FP7 program in 2008 (European Commission, 2016). Over the following years, the EU expanded its Open Science agenda. Key milestones included the 2011 European Code of Conduct for Research Integrity, the 2012 recommendations on scientific information access and the launch of Horizon 2020 in 2014, which mandated Open Access for EU-funded research (ALLEA, 2023; European Commission, 2012; Miedema, 2021). More recently, in 2022 and 2023, the EU reinforced its commitment by advocating open-source solutions for interoperability and data sovereignty and reaffirming principles of transparent and equitable publishing (Council of the European Union, 2023). To support Open Science, the EU has developed strategic initiatives such as the European Open Science Cloud (EOSC) for standardized data access and Open Research Europe (ORE) for Open Access publishing (European Commission, 2025).

In this context, DeSci has emerged as a new paradigm within Open Science, aiming to strengthen transparency, traceability and trust in scientific data sharing. While many DeSci initiatives leverage technologies such as blockchain to support these objectives, these are not the only possible

approaches; alternative technological solutions can also be explored to enable secure and verifiable mechanisms for data provenance and reproducibility. DeSci initiatives seek to promote decentralized, community-driven governance models, aligning with the core principles of Open Science while introducing innovative approaches to address long-standing challenges related to data integrity and access control. (Díaz et al., 2025; Weidener & Spreckelsen, 2024).

2.2. Blockchain Technology

BT has become a key innovation in the digital economy, offering the potential to create new models of collaboration and enhance efficiency across different organizations, services and industries. Its ability to guarantee data immutability and integrity, along with secure, decentralized transaction recording, validation and sharing, allows for the transformation of business models while promoting transparency and trust (Damvakeraki & Charalambous, 2023).

BT is a key driver, opening up numerous opportunities for companies (Damvakeraki & Charalambous, 2023). By adopting and integrating this technology, companies can, first, streamline their operations, build trust with customers and develop innovative products and services, thereby gaining a competitive advantage. Furthermore, they can access new markets by participating in a global, decentralized ecosystem without geographical limitations. Finally, BT drives innovation, particularly through its convergence with other disruptive technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT), which will play a central role in the short-term development of the digital economy.

BT, introduced in 2008 by Satoshi Nakamoto as the foundation for the cryptocurrency Bitcoin, represents one of the most significant technological innovations of the digital era (Nakamoto, 2008). Originally created to solve the problem of “double-spending” in digital currencies, blockchain quickly revealed a potential that extends far beyond financial transactions.

Before BT, one of the main issues with digital currencies was the risk of “double-spending”, where the same unit of currency could be used more than once. For example, this would be akin to attempting to make two purchases with the same banknote. BT addressed this problem by establishing a digital ledger of all transactions, which is distributed and managed by a network of computers known as “nodes” (Kakavand et al., 2017). Each transaction is verified by these nodes and once confirmed, it is permanently recorded across all of them. This ensures that the transaction history remains accessible and can be reviewed on any node by anyone (Nakamoto, 2008). At the core of this technology lies the concept of a distributed and decentralized ledger- Distributed Ledger Technology (DLT). This ledger consists of a series of cryptographically linked blocks, each containing transaction data. Every node in the network maintains a replica of this ledger and the addition of a new block- incorporating new transactions and a link to the previous block- occurs only after these transactions have been validated by the nodes through a decentralized consensus mechanism (Swan, 2015).

After Bitcoin, BT advanced with the introduction of new platforms offering enhanced capabilities. Ethereum, for instance, introduced smart contracts: self-executing agreements that facilitated the creation of innovative applications within the BT ecosystem (International Bank for Reconstruction and Development, 2017). BT stands out for its ability to eliminate intermediaries, enabling direct interactions between parties (Nakamoto, 2008). This decentralized structure not only reduces costs but also fosters greater trust.

As shown in Table 1, the fundamental attributes of blockchain reinforce its versatility as a technological solution:

Table 1. Core attributes of BT (Anderberg, A. et al., 2019; Swan, 2015; Tripathi et al., 2023)

Feature	Description
Decentralization and Peer-to-Peer Communication	Ensures equal access to recorded information and enables direct interactions between network nodes, removing intermediaries.
Immutability	Prevents stored data from being altered or deleted, protecting against fraud and ensuring transactions cannot be repudiated.
Transparency and Pseudonymity	Allows all participants to access the complete transaction history while preserving the privacy of transaction participants.
Consensus Mechanisms	Validates transactions and maintains network integrity using algorithms like Proof of Work (PoW) and Proof of Stake (PoS).
Smart Contracts	Automates processes based on predefined conditions, reducing the need for human intervention and minimizing errors.
Cryptographic Security	Links each block to the previous one via a cryptographic hash, ensuring a secure and tamper-proof chain.

However, several challenges affect the adoption and implementation of this technology, as summarized in Table 2, including:

Table 2. Challenges in the adoption and implementation of BT (Anderberg, A. et al., 2019; Habib et al., 2022; Tripathi et al., 2023)

Challenge	Description
Scalability	As blockchain networks expand, transaction validation and addition may slow down, creating bottlenecks in applications that require high speed and volume, such as financial systems and digital commerce.
Interoperability	A major challenge is enabling different blockchain platforms to communicate and function together. Many blockchains operate as isolated systems, complicating the development of applications that require cross-chain interaction.
Regulatory Compliance	Ensuring compliance with legal requirements, which vary across sectors like finance and healthcare, is particularly challenging for decentralized networks operating on a global scale.
Energy Consumption	Certain consensus mechanisms, such as PoW, demand substantial computational power to validate transactions and add new blocks, leading to high operational costs and environmental concerns. Alternatives like PoS have been explored to address this issue.

2.3. Zero Knowledge Proofs

The concept of ZKP was introduced by et al., (1985) establishing a novel cryptographic framework whereby a prover can assure a verifier of the validity of a statement without disclosing any information beyond the statement's truth itself.

Nevertheless, the original definition of zero-knowledge, as presented by the same authors, does not fully capture the intuitive concept of zero-knowledge. One issue is that the sequential composition

of zero-knowledge protocols does not guarantee that the result is also zero-knowledge (Feige et al., 1988; Goldreich & Krawczyk, 1990). Additionally, the original definition does not account for ZKP being used as subprotocols within larger cryptographic protocols, where a dishonest verifier might use prior information to gain knowledge during the interaction with the prover. The transition from interactive proofs of assertions to interactive proofs of knowledge establishes the definition of unrestricted input ZKP of knowledge (Feige et al., 1988). In this context, the prover demonstrates possession of knowledge without disclosing any computational information, including the single bit revealed in ZKP of assertions. These concepts are significant in identification schemes, where parties confirm their identity by demonstrating their knowledge rather than by validating a specific assertion. A classic illustration, illustrated in Figure 1, is the “Ali Baba’s Cave” example (Quisquater et al., 1990).

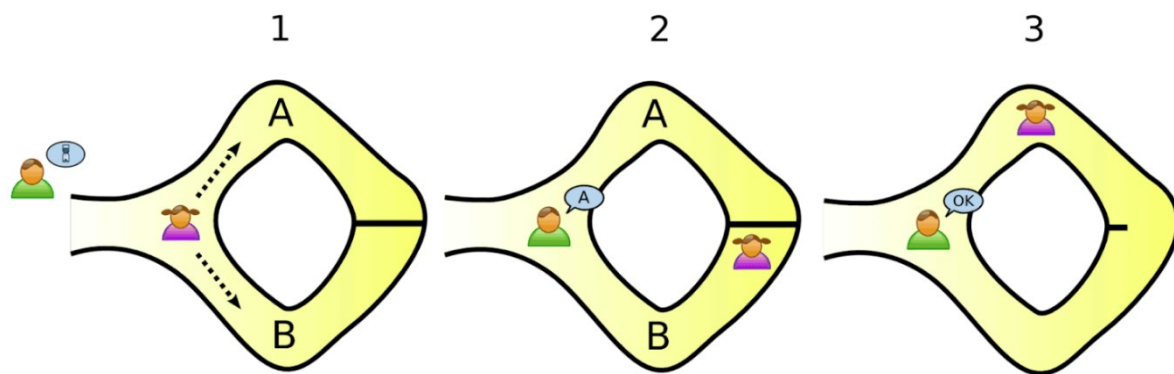


Figure 1. Ali Baba's cave (*Zero-Knowledge Proofs Decoded: A Simple Intro*, 2023).

In this scenario, Peggy claims to know a secret password that opens a magic door between two cave entrances, A and B. To verify her claim, Victor conducts a test: Peggy enters the cave, choosing either path A or B, while Victor, unaware of her choice, randomly calls for her to exit from one of the two paths. If she is on the requested side, she can leave freely; otherwise, she must use the password to pass through the door. If Peggy does not know the password, she has only a 50% chance of exiting correctly. However, after multiple repetitions, the probability of her succeeding by chance alone becomes negligible, convincing Victor that she must indeed know the secret. Crucially, this process reveals no information about the password itself.

Building on these foundational definitions, ZKP have evolved significantly, leading to the development of NIZK proofs and succinct protocols such as Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK), which constitute a subset of NIZK proofs of knowledge (Alghazwi et al., 2024). These advancements have expanded the practical applications of ZKP beyond cryptographic theory, enabling their use in blockchain, privacy-preserving computations and secure authentication. Moreover, zk-SNARK offer the advantages of both non-interactivity and strong security, making them widely used in blockchain applications (Konkin & Zapechnikov, 2023).

3. Methodology

To analyze the role of BT and ZKP in addressing the challenges of scientific data sharing within the Open Science ecosystem, this paper employed a systematic literature review methodology. The design followed Snyder (2019) and PRISMA 2020 (Page et al., 2021), ensuring transparency and reproducibility.

The study used Scopus and Web of Science as primary databases. The database search, conducted in March 2025 and limited to the 2017-2024 period, retrieved 54 records from Scopus and 45 from Web of Science (99 in total). After removing 23 duplicates in Rayyan, 76 unique studies remained.

A structured search (“scientific data sharing” OR “open science”) AND (“blockchain” OR “distributed ledger” OR “zero knowledge proofs”), was used to capture studies at the intersection of Open Science and distributed ledger technologies, focusing on privacy-enhancing mechanisms. Inclusion criteria required relevance to Open Science, data sharing, blockchain and privacy-enhancing technologies, publication in English, and availability as journal or conference papers. Exclusion criteria removed work-in-progress, workshops, posters or papers under five pages.

The screening and eligibility phases were performed in Rayyan, allowing transparent tracking of decisions and facilitating cross-validation within the research team. In the first stage, studies irrelevant to Open Science, blockchain or privacy-enhancing technologies were excluded based on title, keywords and abstract. After this process, 50 studies were excluded, leaving 26 full-text articles analyzed in depth according to predefined criteria.

Given the novelty of this topic, relying solely on traditional academic sources could overlook relevant developments in alternative formats. To address this limitation, gray literature (technical reports, white papers and blockchain-based projects) was also included. The quality of these sources was critically appraised using the AACODS checklist (Tyndall, 2008). This complementary analysis captured the evolving landscape of blockchain applications in Open Science and DeSci.

The findings extracted from the selected studies were synthesized through thematic analysis, enabling the grouping of contributions according to the key challenges identified in data sharing (RQ1) and the corresponding BT/ZKP-based solutions proposed to address them (RQ2). Coding reliability was verified through independent cross-checking by two reviewers, and a PRISMA-style flow diagram (Figure 2) summarizes the identification, screening, eligibility and inclusion stages (Page et al., 2021).

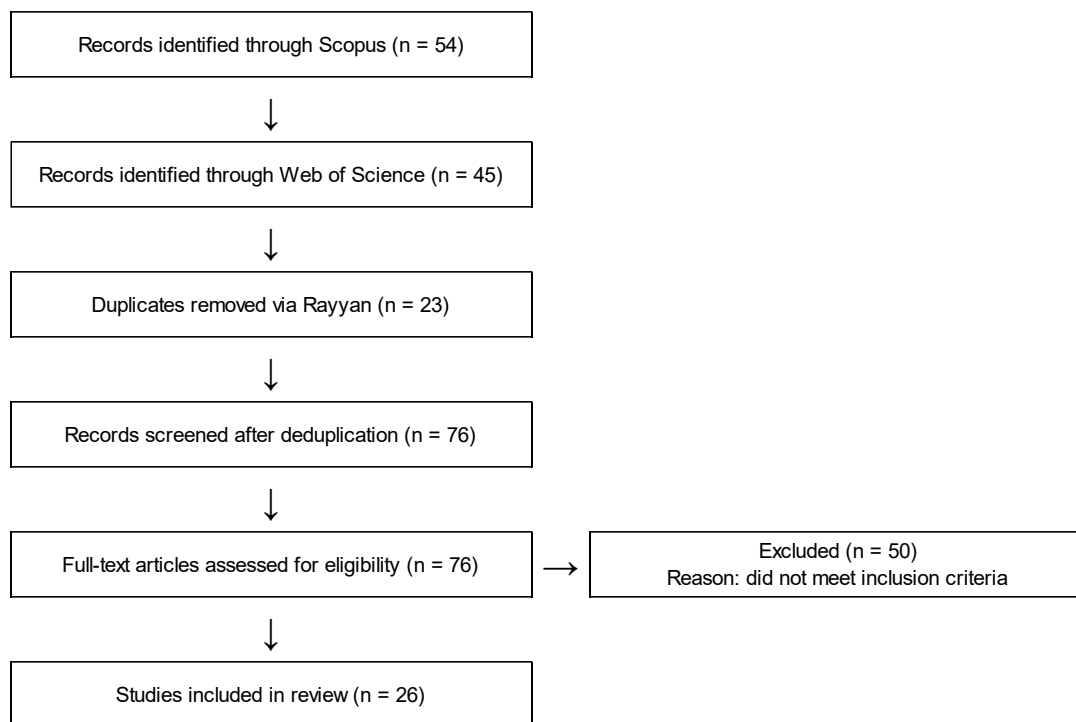


Figure 2. PRISMA 2020 Flow Diagram of Study selection (Page et al., 2021)

4. Results and Discussion

Below are the findings derived from addressing the research questions outlined in the paper's introduction.

4.1. RQ1: What are the primary challenges in managing and sharing scientific data, particularly in terms of authenticity, data provenance and ownership?

The management and sharing of scientific data in modern research are increasingly complex, particularly concerning the authenticity, provenance and ownership of data. These challenges arise due to the growing scale and diversity of datasets, the collaborative and interdisciplinary nature of scientific research and the ongoing transition towards open science practices. Several critical issues have been identified in the literature, revealing gaps in current systems that hinder data integrity, transparency and traceability.

One of the foremost challenges is ensuring the authenticity and integrity of scientific data. Data manipulation, whether intentional or accidental, remains a persistent concern, undermining the trustworthiness of research outputs (Wittek et al., 2020; Gurung et al., 2023). Traditional repositories and centralized data management systems are often inadequate in detecting and preventing tampering or selective reporting, leading to reproducibility crises in several scientific disciplines (Shantharam et al., 2021).

A second critical issue is the lack of robust data provenance mechanisms. Provenance, which tracks the origin, history and transformations of data, is fundamental to establishing trust in research

findings. However, conventional provenance frameworks are frequently insufficient, offering limited transparency over complex research workflows (Jeng et al., 2020). Without comprehensive and verifiable provenance records, researchers and auditors face difficulties in verifying the validity of datasets and ensuring compliance with research standards (Koepsell, 2019). Emerging blockchain-based solutions aim to address these gaps. For instance, ECKOchain enhances data provenance, auditability and FAIR compliance by using on-chain metadata tracking, decentralized governance and smart contract-based access control (Marstein et al., 2024). Similarly, platforms like SMARDY integrate watermarking and fingerprinting technologies to improve data ownership tracking, integrity and security (Filip et al., 2022). While these innovations offer promising improvements, their adoption depends on overcoming challenges such as scalability, integration with existing research infrastructures and user accessibility.

Another major concern is data ownership and rights management. Researchers are often reluctant to share data due to fears of misappropriation, lack of recognition and inadequate legal protections (Zheng & Zhu, 2020). The absence of standardized and enforceable frameworks for data licensing and intellectual property rights leads to uncertainties over who can access, use and benefit from shared datasets (Heurich & Lukács, 2023). These concerns are especially critical in cross-institutional and international research collaborations, where differing regulations and ethical norms further complicate data governance (Duine, 2023).

Additionally, ethical and privacy concerns complicate data sharing, particularly in sensitive fields such as healthcare and genomics. Researchers must balance the need for openness with stringent privacy protections and compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe (Gautam & Kritibhushan, 2024).

Finally, despite the emergence of open science initiatives aimed at fostering transparency and collaboration, systemic barriers remain. These include a lack of infrastructure to support transparent peer review, difficulties in providing reliable attribution for data contributions and insufficient incentives for data sharing (Choi & Seo, 2021; Gurung et al., 2023). BT offer promising solutions by decentralizing academic journal management workflows, immutably recording reviewer contributions and democratizing decision-making processes, such as editorial and funding board selections (Janowicz et al., 2018). Blockchain-based peer review systems, like PeerView, enhance transparency, traceability and reviewer attribution while minimizing centralized control. Built on the bloxberg blockchain, PeerView also improves usability by eliminating the need for cryptocurrency management (Lawton et al., 2021). Similarly, platforms like INFINITCODEX (I8X) use decentralized publishing, smart contracts and cryptoeconomic incentives to enhance transparency and collaboration in scholarly communication, promoting continuous peer review and improving access and preservation of research (Duh et al., 2019).

Academic misconduct, such as plagiarism, data falsification and peer review fraud, undermines trust in research. A permissioned blockchain governed by a consortium could enhance trust, reduce misconduct and align with Open Science principles like Open Peer Review. However, broader

adoption may depend on integrating blockchain with existing publishing models and incentivizing researchers and publishers to participate (Mohan, 2019).

To conclude, the main challenges in managing and sharing scientific data involve ensuring authenticity, verifiable provenance and data ownership rights, while balancing openness with ethical and legal responsibilities. Addressing these issues is crucial for trust and reproducibility in research. Emerging technologies like BT offer solutions by enhancing transparency and mitigating risks, but their adoption requires integration with existing systems, clear regulations and strong incentives for participation.

4.2. RQ2: How can BT and ZKP ensure the integrity, transparency and traceability of scientific data, particularly regarding its provenance?

BT and ZKP provide robust solutions to address the critical challenges of data integrity, transparency and traceability in scientific research. The decentralized and immutable nature of BT enables the secure recording of data access, transformations and transactions in a tamper-proof and auditable ledger. This guarantees the authenticity and provenance of scientific datasets by ensuring that all actions taken on the data are securely logged and verifiable, fostering trust in research outputs.

For instance, BT can enhance data curation, integrity and provenance in microbial databases by decentralizing data entry and improving long-term preservation, with potential applications in enriching existing databases and creating decentralized strain repositories (Mohammadipanah & Sajedi, 2021). Similarly, in scientific consensus-building processes, blockchain-based solutions can decentralize peer review and create tamper-proof records, enhancing transparency, reproducibility and trust (Duh et al., 2019). The integration of the Neuroscience Gateway (NSG) with the Open Science Chain (OSC), through the on-chain storage of cryptographic metadata hashes and the use of customizable metadata fields, enhances reproducibility and transparency in neuroscience workflows (Sivagnanam et al., 2019).

Decentralized peer review systems, as proposed in blockchain-based publishing models, demonstrate how BT can enhance transparency, traceability and governance by recording peer review interactions on immutable ledgers and enabling Open Access by-design. Such systems, while promising, face challenges like scalability and privacy concerns, which could be addressed by integrating privacy-preserving mechanisms like ZKP (Tenorio-Fornés et al., 2019).

Blockchain's ability to enhance traceability, privacy and data integrity is also evident in geospatial applications. It improves geospatial data sharing, land administration and crowdsourcing by addressing key challenges related to privacy, security and data provenance, while promoting the development of decentralized geospatial systems (Zhao et al., 2022). Lastly, the concept of open data blockchain analytics, as demonstrated with the Bitcoin blockchain, highlights how publicly accessible blockchain data can provide insights into transaction patterns, network behavior and security vulnerabilities (McGinn et al., 2018).

Recent advancements in ZKP systems highlight both the theoretical and practical potential of these technologies in decentralized scientific infrastructures. The simulation frameworks proposed by Dodis et al. (2024) contribute to strengthening the cryptographic soundness of ZKP protocols, while the applied approach presented by Filippis & Foysal (2024) demonstrates how these systems can be implemented to preserve privacy and validate data integrity in sensitive scientific domains. Together, these developments provide crucial support for the adoption of secure, verifiable and privacy-preserving mechanisms within Open Science and DeSci ecosystems.

Several practical implementations demonstrate how these technologies contribute to securing scientific data, ensuring transparent provenance and protecting privacy across different domains. Table 3 summarizes key applications where BT and ZKP address these challenges.

Table 3. Applications of zk-SNARKs and BT for Ensuring Data Integrity, Transparency and Provenance

Sector	Problem	Solution with ZKP	Use Case	References
Digital Identity	Authentication requires sharing sensitive personal information.	Users can prove attributes (age, citizenship) without revealing data.	Digital Population Identity (DPI) enables access to services while enhancing security.	(Hasibuan et al., 2025)
Secure Authentication	Passwords are vulnerable to phishing attacks and breaches.	Zero-Knowledge Authentication allows login without passwords or credentials.	Microsoft Entra Verified ID utilizes ZKP for secure authentication.	(Mazzocca et al., 2024)
Decentralized Identity Management	Traditional identity management systems compromise privacy and security.	Blockchain-based decentralized identity with ZKPs for attribute verification.	Self-sovereign identity using ZKPs in blockchain-based identity systems.	(Rafael & Moreno, 2024)
Healthcare Data Security	Healthcare data requires both privacy and accessibility while ensuring integrity.	Patient-centric blockchain with ZKP-enhanced IPFS for off-chain storage.	Secure patient data sharing using off-chain IPFS and ZKPs.	(Gautam & Kritibhushan, 2024)
Verifiable Cloud Computation	Cloud computations need verification while ensuring privacy and integrity.	zk-STARK-based framework for verifiable computation in cloud environments.	VerComp: a zk-STARK framework for cloud-based verifiable computation.	(Salvatelli, 2024)

By combining BT and ZKP, it is possible to establish decentralized infrastructures that address critical challenges in scientific data management. These technologies ensure data authenticity, maintain transparent and immutable provenance records and protect sensitive information throughout the research lifecycle. Their integration into Open Science and DeSci frameworks enhances trust, reproducibility and accountability in scientific research.

5. Challenges and Future Perspectives

The evolution of Open Science and, more recently, DeSci, has revealed structural challenges that limit the adoption of technological solutions for management and sharing of scientific data. Although

Blockchain technology has been proposed as a mechanism to ensure data integrity, authenticity and traceability, significant limitations still hinder its large-scale implementation. Among these limitations are the lack of scalability testing, the absence of empirical validation in real-world research environments and the transaction costs associated with the use of blockchain-based solutions. Furthermore, many of the proposed models remain conceptual, without the development of prototypes or proof-of-concept implementations that demonstrate their technical and operational feasibility.

Another critical issue is the lack of robust mechanisms for preserving privacy in the context of scientific data sharing, particularly in sensitive fields such as healthcare, genomics and the social sciences. The inherent transparency of public Blockchain networks, while essential for ensuring data auditability and integrity, can conflict with confidentiality requirements and legal frameworks such as the GDPR. These challenges are widely recognized in the literature, which highlights the need for solutions that reconcile transparency and trust with the protection of privacy.

In this context, the integration of BT with ZKP emerges as a complementary approach that can address these gaps. ZKP enable the validation of claims or compliance with predefined rules without the need to reveal the underlying data. This capability is particularly relevant for ensuring data confidentiality during validation and sharing processes, protecting sensitive information while simultaneously guaranteeing the auditability necessary to foster trust. The combined application of Blockchain and ZKP thus offers a balance between transparency and privacy- an aspect that, to date, has not been adequately explored in proposals for scientific data management within Open Science and DeSci frameworks.

Our study is particularly relevant as it addresses a critical gap in literature. The systematic analysis conducted demonstrates that, despite numerous initiatives employing BT to enhance data integrity in science, approaches that integrate ZKP mechanisms to resolve privacy and confidentiality challenges are virtually nonexistent. By proposing the integration of these two technologies, this work contributes to the development of more robust, transparent and ethically responsible models for scientific data governance.

Looking ahead, future research should develop and test integrated BT–ZKP prototypes in real-world environments. Further studies should assess scalability, interoperability and governance frameworks to ensure transparency and data protection within Open Science and DeSci ecosystems.

6. Conclusion

The increasing complexity and volume of scientific data, coupled with the demands for transparency, ethics and collaboration inherent to Open Science, have exposed structural limitations in current data management and sharing practices. This study examined how blockchain technology and ZKP can, in a complementary manner, address these challenges by ensuring the integrity, authenticity, traceability and privacy of data throughout the entire research lifecycle.

Through a systematic literature review, the main obstacles faced by researchers were identified, notably the lack of robust mechanisms for provenance verification, concerns over data ownership and misuse and the absence of effective incentives for open data sharing. It was also found that, despite growing interest in the application of blockchain to Open Science, its integration with privacy-preserving mechanisms such as ZKP remains a significant gap in the literature.

The combination of these technologies enables, on the one hand, the transparency and immutability of scientific records and on the other, the protection of sensitive data confidentiality without compromising auditability or ethical and legal compliance. This balance is essential for enabling scientific infrastructures that are more open, secure and sustainable, aligned with the FAIR principles and the values of DeSci.

In this regard, this paper contributes to addressing a gap in literature by proposing an integrated approach that simultaneously values trust and privacy. The combination of these technologies proves promising in reinforcing trust, transparency and accountability in scientific data sharing, contributing to the development of more ethical, auditable and sustainable research ecosystems.

Acknowledgments

This work was financially supported by Project Blockchain.PT – Decentralize Portugal with Blockchain Agenda, (Project no 51), WP 8, Call no 02/C05-i01.01/2022, funded by the Portuguese Recovery and Resilience Program (PPR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program.

References

- Alghazwi, M., Bontekoe, T., Visscher, L., & Turkmen, F. (2024). *Collaborative CP-NIZKs: Modular, Composable Proofs for Distributed Secrets*.
- ALLEA. (2023). *The European Code of Conduct for Research Integrity - Revised Edition 2023*. <https://doi.org/10.26356/ECOC>
- Alsaigh, R., Mehmood, R., Katib, I., Liang, X., Alshantqiti, A., Corchado, J. M., & See, S. (2024). Harmonizing AI governance regulations and neuroinformatics: perspectives on privacy and data sharing. In *Frontiers in Neuroinformatics* (Vol. 18). Frontiers Media SA. <https://doi.org/10.3389/fninf.2024.1472653>
- Anderberg, A., Andonova, E., Bellia, M., Calès, L., Inamorato dos Santos, A., Kounelis, I., Nai Fovino, I., Petracco Giudici, M., Papanagiotou, E., Sobolewski, M., Rossetti, F., & Spirito, L. (2019). *Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies* (EUR (Luxembourg. Online)). Publications Office. <https://doi.org/10.2760/901029>
- Bartling, S., & Friesike, S. (2014). Opening Science: The Evolving Guide on How the Internet is Changing Research, Collaboration and Scholarly Publishing. In *Opening Science*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-00026-8>
- Choi, D. H., & Seo, T. S. (2021). Development of an open peer review system using blockchain and reviewer recommendation technologies. *Science Editing*, 8(1), 104–111. <https://doi.org/10.6087/kcse.237>
- Council of the European Union. (2023). *High-quality, transparent, open, trustworthy and equitable*

scholarly publishing - Council conclusions (approved on 23 May 2023).

- Damvakeraki, T., & Charalambous, M. (2023). *Blockchain & Europe's Governance Transformation: From Global to Local*.
- Díaz, F., Menchaca, C., & Weidener, L. (2025). Exploring the decentralized science ecosystem: insights on organizational structures, technologies, and funding. *Frontiers in Blockchain*, 8. <https://doi.org/10.3389/fbloc.2025.1524222>
- Dodis, Y., Jain, A., Lin, H., Luo, J., & Wichs, D. (2024). How to Simulate Random Oracles with Auxiliary Input. *Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS*, 1207–1230. <https://doi.org/10.1109/FOCS61266.2024.00080>
- Duh, E. S., Duh, A., Droftina, U., Kos, T., Duh, U., Korošak, T. S., & Korošak, D. (2019). Publish-and-flourish: Using blockchain platform to enable cooperative scholarly communication. *Publications*, 7(2). <https://doi.org/10.3390/publications7020033>
- Duine, M. (2023). Summary Report APE 2023, 10-12 January, Berlin, Germany Berlin Re-Visited: Building Technological Support for Scholarship and Scientific Publishing. *Information Services and Use*, 44(1), 1–13. <https://doi.org/10.3233/ISU-230189>
- European Commission. (2005). Commission Recommendation on the European Charter for Researchers and on a Code of Conduct for the Recruitment of Researchers. *Official Journal of the European Union*.
- European Commission. (2016). *Commission presents its evaluation of the 7th Framework Programme for Research*.
- European Commission. (2025). *Open Research Europe*. <https://open-research-europe.ec.europa.eu/>
- Fecher, B., & Friesike, S. (2014). Open Science: One Term, Five Schools of Thought. In *Opening Science* (pp. 17–47). Springer International Publishing. https://doi.org/10.1007/978-3-319-00026-8_2
- Feige, U., Fiat, A., & Shamir, A. (1988). Zero-Knowledge Proofs of Identity. *Journal of Cryptology*, 1, 77–94.
- Filip, I. D., Ionite, C., Gonzalez-Cebrian, A., Balanescu, M., Dobre, C., Chis, A. E., Feenan, D., Buga, A. A., Constantin, I. M., Suciu, G., Iordache, G. V., & Gonzalez-Velez, H. (2022). Smardy: Zero-Trust FAIR Marketplace for Research Data. *Proceedings - 2022 IEEE International Conference on Big Data, Big Data 2022*, 1535–1541. <https://doi.org/10.1109/BigData55660.2022.10020710>
- Filippis, R. de, & Foyals, A. Al. (2024). Blockchain Brains: Pioneering AI, ML, and DLT Solutions for Healthcare and Psychology. *OALib*, 11(12), 1–25. <https://doi.org/10.4236/oalib.1112543>
- Gautam, P. B., & Kritibhushan. (2024). Patient-Centric Blockchain Model for Healthcare Data Security using Off-Chain IPFS Storage and ZKP. *2024 International Conference on Cybernation and Computation, CYBERCOM 2024*, 217–222. <https://doi.org/10.1109/CYBERCOM63683.2024.10803172>
- Goldreich, O., & Krawczyk, H. (1990). On the Composition of Zero-Knowledge Proof Systems. In *Lecture Notes in Computer Science* (Vol. 443). Springer Verlag.
- Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, 291–304. <https://doi.org/10.1145/22145.22178>
- Gurung, I., Adhikari, S., Marouane, A., Pandey, R., Dhakal, S., & Maskey, M. (2023). *Exploring Blockchain to Support Open Science Practices*. 1205–1208. <https://doi.org/10.1109/igarss52108.2023.10283181>
- Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet 2022, Vol. 14, Page 341, 14(11)*, 341. <https://doi.org/10.3390/FI14110341>
- Hasibuan, N., Sihite, T. H., Daulay, F., Sihotang, D., & Saputra, H. (2025). The Influence of

- Community Readiness on the Level of Digital Population Identity (DPI) Activation in Sibolga City. *Jurnal Multidisiplin Sahombu*, 5(2), 466–473. <https://doi.org/10.58471/jms.v5i02>
- Heurich, B., & Lukács, B. (2023). Are we close(d)? Debating the openness paradox in science. *Distance Education*, 44(4), 731–744. <https://doi.org/10.1080/01587919.2023.2267482>
- International Bank for Reconstruction and Development. (2017). *Distributed Ledger Technology (DLT) and Blockchain*.
- Janowicz, K., Regalia, B., Hitzler, P., Mai, G., Delbecque, S., Fröhlich, M., Martinet, P., & Lazarus, T. (2018). On the prospects of blockchain and distributed ledger technologies for open science and academic publishing. *Semantic Web*, 9(5), 545–555. <https://doi.org/10.3233/SW-180322>
- Jeng, W., Wang, S. H., Chen, H. W., Huang, P. W., Chen, Y. J., & Hsiao, H. C. (2020). A decentralized framework for cultivating research lifecycle transparency. *PLoS ONE*, 15(11 November). <https://doi.org/10.1371/journal.pone.0241496>
- Kakavand, H., Kost De Sevres, N., & Chilton, B. (2017). The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. *SSRN Electronic Journal*. <https://doi.org/10.2139/SSRN.2849251>
- Koepsell, D. (2019). Blockchain, Wikis, and the Ideal Science Machine: With an Example From Genomics. *Frontiers in Blockchain*, 2. <https://doi.org/10.3389/fbloc.2019.00025>
- Konkin, A., & Zapechnikov, S. (2023). Zero knowledge proof and ZK-SNARK for private blockchains. *Journal of Computer Virology and Hacking Techniques*, 19(3), 443–449. <https://doi.org/10.1007/S11416-023-00466-1/TABLES/2>
- Lawton, J., Uzdogan, K., & Cox, P. (2021). Peer Review Aggregation utilizing blockchain technology. *2021 3rd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2021*, 8–11. <https://doi.org/10.1109/BRAINS52497.2021.9569802>
- Leible, S., Schlager, S., Schubotz, M., & Gipp, B. (2019). A Review on Blockchain Technology and Blockchain Projects Fostering Open Science. In *Frontiers in Blockchain* (Vol. 2). Frontiers Media SA. <https://doi.org/10.3389/fbloc.2019.00016>
- Liu, X., Zhang, J., Wang, Y., Yang, X., & Yang, X. (2025). SmartZKCP: Towards Practical Data Exchange Marketplace Against Active Attacks. *Blockchain: Research and Applications*, 100272. <https://doi.org/10.1016/j.bcr.2024.100272>
- Marstein, K. E., Grytnes, J. A., & Lewis, R. J. (2024). ECKOchain: A FAIR blockchain-based database for long-term ecological data. *Methods in Ecology and Evolution*. <https://doi.org/10.1111/2041-210X.14280>
- Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2024). *A Survey on Decentralized Identifiers and Verifiable Credentials*. <https://doi.org/10.1109/COMST.2025.3543197>
- McGinn, D., McIlwraith, D., & Guo, Y. (2018). Towards open data blockchain analytics: A bitcoin perspective. *Royal Society Open Science*, 5(8). <https://doi.org/10.1098/rsos.180298>
- Mohammadipanah, F., & Sajedi, H. (2021). Potential of blockchain approach on development and security of microbial databases. *Biological Procedures Online*, 23(1). <https://doi.org/10.1186/s12575-020-00139-z>
- Mohan, V. (2019). On the use of blockchain-based mechanisms to tackle academic misconduct. *Research Policy*, 48(9). <https://doi.org/10.1016/j.respol.2019.103805>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. In *BMJ* (Vol. 372). BMJ Publishing Group. <https://doi.org/10.1136/bmj.n71>
- Quisquater, J. J., Guillou, L. C., & Berson, T. (1990). How to explain zero-knowledge protocols to your

- children. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 435 LNCS, 628–631. https://doi.org/10.1007/0-387-34805-0_60
- Rafael, D., & Moreno, T. (2024). *Distributed Technologies in Identity Management: An Approach to Enhancing Security and Privacy*. Universidad de Murcia.
- Salvatelli, R. (2024). *VerComp: A Framework for Verifiable Computation in Cloud Environments Using zk-STARK Proofs* [Master Degree Thesis]. Politecnico di Torino.
- Shantharam, M., Lin, K., Sakai, S., & Sivagnanam, S. (2021, July 17). Integrity protection for research artifacts using open science chains command line utility. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3437359.3465587>
- Sivagnanam, S., Nandigam, V., & Lin, K. (2019, July 28). Introducing the open science chain - Protecting integrity and provenance of research data. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3332186.3332203>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Soeharjono, S., & Roche, D. G. (2021). Reported Individual Costs and Benefits of Sharing Open Data among Canadian Academic Faculty in Ecology and Evolution. In *BioScience* (Vol. 71, Issue 7, pp. 750–756). Oxford University Press. <https://doi.org/10.1093/biosci/biab024>
- Swan, M. (2015). Blockchain Thinking: the Brain as a Decentralized Autonomous Corporation. *IEEE Technology and Society Magazine*, 34(4), 41–52. <https://doi.org/10.1109/MTS.2015.2494358>
- Tenorio-Fornés, A., Jacynycz, V., Llop, D., Sánchez-Ruiz, A. A., & Hassan, S. (2019). Towards a Decentralized Process for Scientific Publication and Peer Review using Blockchain and IPFS. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 4635–4644. <https://hdl.handle.net/10125/59901>
- The National Academies Press. (2009). Ensuring the Integrity, Accessibility, and Stewardship of Research Data in the Digital Age. In *Ensuring the Integrity, Accessibility, and Stewardship of Research Data in the Digital Age*. National Academies Press. <https://doi.org/10.17226/12615>
- Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytics Journal*, 9, 100344. <https://doi.org/10.1016/J.DAJOUR.2023.100344>
- Tyndall, J. (2008). *How low can you go? Toward a hierarchy of grey literature*. <http://www.alia2008.com>
- UNESCO. (2021). *UNESCO Recommendation on Open Science*.
- UNESCO and Canadian Commission for UNESCO. (2022). *An introduction to the UNESCO Recommendation on Open Science*.
- United Nations General Assembly. (1948). *Universal Declaration of Human Rights*.
- Weidener, L., & Spreckelsen, C. (2024). Decentralized science (DeSci): definition, shared values, and guiding principles. *Frontiers in Blockchain*, 7. <https://doi.org/10.3389/fbloc.2024.1375763>
- Wilkinson, M. D., Dumontier, M., Aalbersberg, Ij. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J. W., da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., ... Mons, B. (2016). Comment: The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, 3. <https://doi.org/10.1038/sdata.2016.18>
- Wittek, K., Krakau, D., Wittek, N., Lawton, J., & Pohlmann, N. (2020). Integrating bloxberg's Proof of Existence Service With MATLAB. *Frontiers in Blockchain*, 3. <https://doi.org/10.3389/fbloc.2020.546264>
- Zero-Knowledge Proofs Decoded: A Simple Intro*. (2023, May 15). <https://mightyblock.co/blog/zero-knowledge-proof/>
- Zhao, P., Ceden Jimenez, J. R., Brovelli, M. A., & Mansourian, A. (2022). Towards geospatial

blockchain: A review of research on blockchain technology applied to geospatial data. *AGILE: G/Science Series*, 3, 1–6. <https://doi.org/10.5194/agile-giss-3-71-2022>

Zheng, X., & Zhu, Y. (2020). Blockchain based Architecture for Digital-right Management in Scientific Data Sharing. *IOP Conference Series: Earth and Environmental Science*, 502(1). <https://doi.org/10.1088/1755-1315/502/1/012004>

Threat Modeling a Health Web3 DApp

Ricardo Gomes
*School of Technology and
Management, Polytechnic of
Leiria, Portugal*
ricardo.p.gomes@ipleiria.pt
0000-0002-0438-9119

Daniela Dinis
*School of Technology and
Management, Polytechnic of
Leiria, Portugal*
daniela.o.dinis@ipleiria.pt
0009-0004-2541-2463

João Oliveira
*School of Technology and
Management, Polytechnic of
Leiria, Portugal*
joao.a.oliveira@ipleiria.pt
0009-0005-9903-5223

Marisa Maximiano
*School of Technology and
Management, Polytechnic of
Leiria; CIIC, Portugal*
marisa.maximiano@ipleiria.pt
0000-0002-1212-7864

Vitor Távora
*School of Technology and
Management, Polytechnic of
Leiria, Portugal*
vitor.tavora@ipleiria.pt
0009-0004-0404-9378

Carlos Machado Antunes
*School of Technology and
Management, Polytechnic of
Leiria, Portugal*
carlos.machado@ipleiria.pt
0009-0005-7010-4328

Manuel Dias
BioGHP, Portugal
manuel@bioghp.com
0009-0000-1830-6479

Ricardo Correia Bezerra
BioGHP, Portugal
ricardo@bioghp.com
0009-0005-1237-6632

Received: 6 June 2025

Accepted: 24 November 2025

Abstract

The healthcare sector increasingly explores Distributed Ledger Technology (DLT) and Health Web 3.0 Decentralized Applications (DApps) as promising solutions for patient-centric data management, data sovereignty, and privacy-preserving systems. Despite significant research at the intersection of blockchain and healthcare, current efforts predominantly address isolated technical challenges—focusing narrowly on specific mechanisms such as confidentiality, privacy, or individual smart contract vulnerabilities. Even cybersecurity assessments typically examine discrete attack vectors rather than comprehensive threat landscapes. This fragmented approach limits our ability to build trustworthy systems and delays real-world adoption, as stakeholders lack frameworks to holistically evaluate security posture.

This study addresses this gap by conducting a comprehensive threat modeling analysis of Health Web 3.0 DApps, taking into account the complex and interconnected security challenges inherent in blockchain-based healthcare systems. We employ a multi-framework approach integrating LINDDUN threat modeling methodology, OWASP Top 10 Smart Contract Vulnerabilities catalog, and Threat Dragon analytical tool to systematically identify, categorize, and evaluate security risks across the entire application stack. Our analysis maps threats spanning smart contract design flaws, cross-chain interaction vulnerabilities, decentralized identity management weaknesses, unauthorized data access risks, and denial-of-service attack vectors.

The primary contribution of this work is demonstrating the critical importance and practical value of holistic threat modeling in blockchain healthcare systems. Our findings reveal interdependencies between seemingly isolated vulnerabilities and show how comprehensive security assessment enhances data privacy protection, smart contract integrity, and overall application resilience. This research provides stakeholders with a systematic methodology for deriving trust in blockchain healthcare solutions, advancing both regulatory compliance and user confidence in decentralized medical data management systems.

Keywords *Blockchain, Healthcare, Threat Modeling*

1. Introduction

The modern healthcare landscape is experiencing unprecedented digital transformation, driven by the exponential growth of health data generation and the increasing demand for patient-centric care models. Electronic Health Records (EHRs), Internet of Medical Things (IoMT) devices, genomic sequencing, and telemedicine platforms collectively generate vast amounts of sensitive health information that require sophisticated management approaches. However, traditional centralized data management systems face significant challenges in addressing contemporary healthcare requirements, particularly concerning data sovereignty, interoperability, patient privacy, and regulatory compliance (Austin et al., 2024; Limna, 2023).

Current healthcare data infrastructure is characterized by fragmented systems, proprietary databases, and centralized architectures that create data silos and limit patient control over personal health information. These limitations become increasingly problematic as healthcare providers, researchers, and patients demand seamless data sharing capabilities while maintaining stringent privacy and security standards. The growing emphasis on patient empowerment and the shift toward value-based care models further amplifies the need for innovative data management solutions that can provide transparency, auditability, and patient ownership of health data (Shen et al., 2025).

Distributed Ledger Technology (DLT), particularly Blockchain technology, has emerged as a transformative paradigm that addresses many fundamental limitations of traditional healthcare data management systems, with a focus on the primary components shown in Figure 1. The inherent characteristics of DLT - including immutability, transparency, decentralization, and cryptographic security - align closely with healthcare requirements for secure, auditable, and patient-controlled data management. Blockchain technology enables the creation of tamper-resistant health records, facilitates secure data sharing among authorized stakeholders, and provides patients with unprecedented control over their personal health information (Agbo et al., 2019; Xia et al., 2024).



Figure 1. Main components of a Health Web 3 Ecosystem

The application of DLT in healthcare extends beyond simple data storage to encompass complex workflows, including clinical trial management, pharmaceutical supply chain tracking, insurance claim processing, and medical research collaboration. Smart contracts, self-executing programs with terms directly written into code, enable automated and trustless execution of healthcare agreements, reducing administrative overhead and eliminating intermediaries. These capabilities position DLT as a

foundational technology for next-generation healthcare systems that prioritize patient autonomy, data integrity, and system interoperability (Agbo et al., 2019).

The evolution toward Health Web 3.0 represents a paradigm shift from centralized, institution-controlled health data systems to decentralized, patient-centric ecosystems. Health Web 3.0 leverages blockchain technology, decentralized storage systems, and cryptographic protocols to create an internet of health data where patients maintain sovereignty over their information while enabling authorized access for healthcare delivery and research purposes. This ecosystem is primarily realized through Decentralized Applications (DApps) that operate on blockchain networks and provide user interfaces for interacting with decentralized health data systems (Narayan et al., 2024).

Health Web 3.0 DApps encompass a diverse range of applications, including decentralized health record management systems, peer-to-peer telemedicine platforms, decentralized clinical trial coordination tools, and blockchain-based health insurance solutions. These applications leverage various blockchain architectures, including public blockchains like Ethereum, private consortium chains, and hybrid solutions that balance transparency with regulatory compliance requirements. The integration of additional Web 3.0 technologies, such as decentralized identity (DID) systems, InterPlanetary File System (IPFS) for distributed storage, and cross-chain interoperability protocols, create sophisticated ecosystems that require comprehensive security considerations (Song et al., 2024).

Despite the promising potential of Health Web 3.0 DApps, their adoption in healthcare environments introduces complex security challenges that significantly differ from traditional web application security concerns (Jeršič et al., 2024). The decentralized nature of these systems, combined with the immutable characteristics of blockchain technology, creates unique attack vectors and vulnerability patterns that require specialized security assessment methodologies. Smart contracts, which serve as the core logic layer for many Health Web 3.0 DApps, are particularly susceptible to design flaws, coding errors, and economic attacks that can result in catastrophic failures (Alotaibi, 2025).

The multi-layered architecture of Health Web 3.0 DApps, spanning user interfaces, smart contract layers, blockchain networks, and external data sources, creates complex interaction patterns that can introduce systemic vulnerabilities. Cross-chain interactions, decentralized identity management systems, and integration with legacy healthcare infrastructure further complicate the security landscape. Additionally, the regulatory requirements for healthcare data protection, including Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and emerging blockchain-specific regulations, necessitate (Alotaibi, 2025).

Current literature on blockchain security primarily focuses on general smart contract vulnerabilities and cryptocurrency-related attacks (Gharavi et al., 2024), with limited attention to healthcare-specific security requirements and the unique characteristics of health data management applications. The

intersection of healthcare regulatory compliance, patient privacy requirements, and blockchain security represents a significant research gap that requires comprehensive investigation and specialized threat modeling approaches.

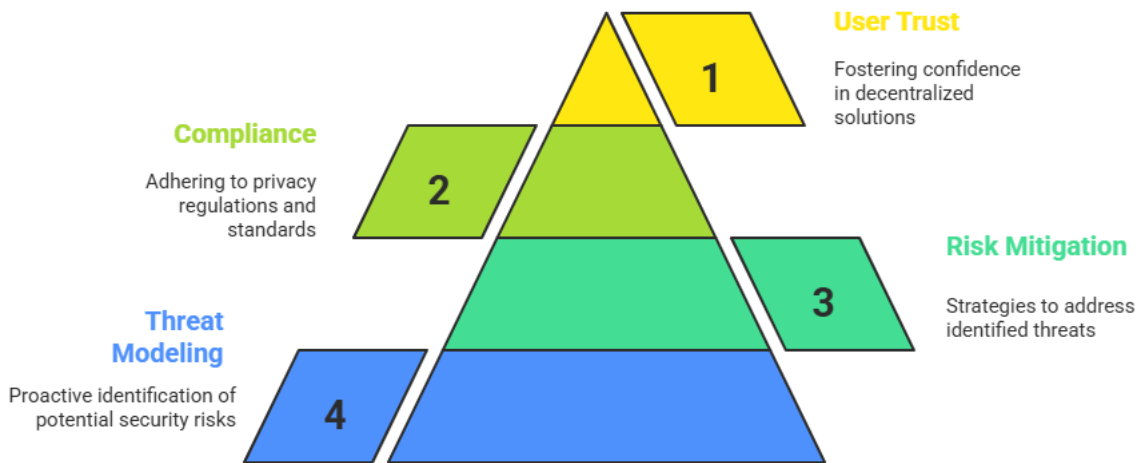


Figure 2. Proposed Hierarchical Security Framework for Blockchain Healthcare Systems.

Our research motivation is grounded in addressing a critical gap in blockchain healthcare security: while existing research predominantly examines isolated technical challenges—individual smart contract vulnerabilities, specific privacy mechanisms, or discrete attack vectors—the complex, interconnected nature of Health Web 3.0 ecosystems demands comprehensive security assessment. As illustrated in our research framework (depicted in Figure 2), we propose a hierarchical security model where holistic threat modeling (4) serves as the foundational layer upon which all other security considerations are built. Without systematic identification of potential security risks across the entire application stack and their interdependencies, it becomes impossible to develop effective risk mitigation (3) strategies, achieve meaningful compliance with healthcare privacy regulations (2), or ultimately foster the user trust (1) necessary for widespread adoption of decentralized healthcare solutions.

The pyramid structure of our approach emphasizes that user trust, the ultimate goal for any healthcare technology, cannot be achieved through fragmented security assessments that address only individual components. Healthcare stakeholders, including patients, providers, and regulatory entities, require demonstrable evidence that Health Web 3.0 DApps can meet stringent security and privacy standards through comprehensive rather than piecemeal evaluation. By establishing holistic threat modeling practices as the cornerstone of our security framework, we bridge the gap between current narrow-focus research and the integrated security perspective required for real-world healthcare implementation.

The key contributions of this study are: (1) demonstrating the critical importance and practical value of comprehensive threat modeling in blockchain healthcare systems by revealing interdependencies

between seemingly isolated vulnerabilities; (2) providing a replicable multi-framework methodology for holistic security assessment of Health Web 3.0 DApps.

The remainder of this paper is organized as follows: Section 2 presents the necessary related concepts of existing research on blockchain security, healthcare data protection, and threat modeling methodologies. Section 3 describes the architecture of our target Health Web3 DApp, and application of the threat modeling exercise. Section 4 details the methodology employed in our threat modeling exercise. Section 5 presents our findings, including identified threats, vulnerability categories, and risk assessments specific to Health Web 3.0 DApps. Finally, Section 5 concludes the paper with a summary of the key contributions and directions for future research in Health Web 3.0 security.

2. Related Concepts

This section establishes the foundational concepts required for understanding the security challenges inherent in Health Web 3.0 DApps. We examine four interconnected domains: distributed ledger technologies that enable decentralized healthcare applications, digital healthcare management solutions that define the application context, cybersecurity principles specific to healthcare environments, and threat modeling methodologies that provide systematic frameworks for security assessment. Understanding these concepts is essential for comprehending the multi-dimensional security challenges addressed in our research and the rationale behind our chosen threat modeling approach.

2.1. Blockchain and Distributed Ledger Technology

Blockchain technology represents a fundamental shift from traditional centralized data management systems to distributed, cryptographically secured networks. At its core, a blockchain is a distributed ledger that maintains a list of records, called blocks, which are linked and secured using cryptographic principles. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data, creating an immutable chain of information that is resistant to modification (Gorkhali et al., 2020).

Distributed Ledger Technology (DLT) encompasses blockchain and other distributed database technologies that enable multiple parties to maintain synchronized copies of a shared database without requiring a central authority or intermediary (Somma et al., 2024). The key characteristics of DLT include: decentralization, where no single entity controls the network; immutability, where recorded data cannot be easily altered or deleted; transparency, where all participants can verify transactions; and consensus mechanisms that ensure all network participants agree on the validity of transactions.

Smart contracts (Alaba et al., 2024) are self-executing programs with contract terms directly written into code that automatically execute when predetermined conditions are met. These programmable contracts eliminate the need for intermediaries and enable complex business logic to be implemented directly on the blockchain. In healthcare contexts, smart contracts can automate processes such as

insurance claim processing, clinical trial protocols, and patient consent management while ensuring transparency and reducing administrative overhead.

Different blockchain architectures serve various use cases: public blockchains offer maximum transparency and decentralization but may raise privacy concerns for sensitive healthcare data; private blockchains provide greater control and privacy but sacrifice some benefits of decentralization; and consortium or hybrid blockchains attempt to balance transparency with privacy requirements, making them particularly suitable for healthcare applications where multiple trusted organizations need to collaborate while maintaining regulatory compliance (Abrar & Sheikh, 2024).

In blockchain-enabled healthcare systems, it is crucial to differentiate between on-chain and off-chain data storage mechanisms. On-chain data encompasses information permanently recorded within the blockchain ledger, such as transactions, smart contract parameters, and cryptographic hashes. While this method guarantees immutability and transparency, it is limited by block size constraints and high transaction fees, rendering it unsuitable for storing large-scale medical datasets (e.g., imaging records). Conversely, off-chain storage refers to data maintained outside the blockchain, with the ledger retaining only cryptographic proofs or reference pointers. By combining these approaches, healthcare applications can achieve both scalability and cost efficiency while maintaining verifiable integrity and authenticity of sensitive medical information (Hepp et al., 2018).

2.2. Digital Solutions for Healthcare Management

The healthcare industry has undergone significant digital transformation (Shen et al., 2025), with technology solutions addressing various aspects of medical care delivery, administration, and research. Electronic Health Records (EHRs) serve as the foundation of modern healthcare information systems, digitizing patient medical histories, treatment plans, and clinical outcomes. However, traditional EHR systems often operate in silos, limiting interoperability and patient control over personal health information.

Telemedicine platforms have revolutionized healthcare delivery by enabling remote consultations, monitoring, and treatment, particularly gaining prominence during the COVID-19 pandemic. These systems rely on secure communication technologies, digital identity verification, and remote monitoring devices to provide healthcare services across geographical boundaries. The Internet of Medical Things (IoMT) encompasses connected medical devices, wearable sensors, and smart healthcare equipment that continuously collect patient data and enable real-time health monitoring (El-Saleh et al., 2024).

Health Information Exchanges (HIEs) facilitate the secure electronic movement of health-related information among healthcare organizations, enabling coordinated care and reducing duplicate testing. However, current HIE systems face challenges related to data standardization, privacy protection, and patient consent management. Clinical Decision Support Systems (CDSS) leverage artificial intelligence and machine learning to assist healthcare providers in making informed treatment

decisions by analyzing patient data and providing evidence-based recommendations (Shojaei et al., 2024).

Digital health solutions also encompass pharmaceutical supply chain management systems that track medications from manufacturing to patient delivery, ensuring authenticity and preventing counterfeit drugs. Research platforms facilitate clinical trial management, patient recruitment, and data collection while ensuring regulatory compliance and participant privacy. The integration of these various digital solutions creates complex healthcare ecosystems that require sophisticated security and privacy protection mechanisms (Dhingra et al., 2024).

2.3. Cybersecurity

Healthcare cybersecurity presents unique challenges due to the sensitive nature of medical data, the critical importance of system availability for patient safety, and the complex regulatory environment governing health information protection. Healthcare organizations face a diverse threat landscape that includes ransomware attacks targeting hospital systems, data breaches exposing patient records, insider threats from employees with privileged access, and sophisticated advanced persistent threats seeking valuable health information.

The Health Insurance Portability and Accountability Act (HIPAA) in the United States (United States, 1996) establishes comprehensive privacy and security requirements for protected health information, mandating specific safeguards for electronic health data. The General Data Protection Regulation (GDPR) in Europe (European Parliament & European Council, 2016) provides additional privacy protection for health data, requiring explicit consent for data processing and establishing strict breach notification requirements. These regulatory frameworks create complex compliance requirements that healthcare organizations must navigate while implementing cybersecurity measures.

Healthcare cybersecurity challenges are compounded by the proliferation of connected medical devices, many of which were not designed with security as a primary consideration. Legacy medical equipment often lacks security features such as encryption, authentication, and updating mechanisms, creating potential entry points for attackers. The critical nature of healthcare services means that security measures must be implemented without disrupting patient care or clinical workflows (Dobrovolska et al., 2024).

Traditional cybersecurity approaches in healthcare focus on perimeter defense, access controls, and monitoring systems to protect centralized databases and networks (Rahim et al., 2024). However, the shift toward decentralized health data management introduces new security paradigms that require an understanding of cryptographic protocols, consensus mechanisms, and distributed system vulnerabilities. The integration of blockchain technology with healthcare systems creates hybrid environments that require security expertise spanning both traditional IT security and distributed ledger technologies.

2.4. Threat Modeling

Threat modeling is a systematic approach to identifying, quantifying, and addressing security threats in software systems and IT infrastructure. This proactive security methodology enables organizations to understand potential attack vectors, assess risk levels, and implement appropriate countermeasures before systems are deployed, or attacks occur. Threat modeling typically involves defining system boundaries, identifying assets and data flows, enumerating potential threats, and evaluating the likelihood and impact of successful attacks (Hammami, 2024).

Several established threat modeling frameworks provide structured approaches to security assessment. STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) focuses on categorizing threats based on the type of security violation (Van Landuyt & Joosen, 2022). PASTA (Process for Attack Simulation and Threat Analysis) emphasizes business impact and risk assessment throughout the threat modeling process (Wolf et al., 2020). LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance) specifically addresses privacy threats and is particularly relevant for healthcare applications handling sensitive personal data (Nweke et al., 2022).

In the context of blockchain and smart contract security, specialized threat modeling approaches have emerged to address unique vulnerabilities such as reentrancy attacks, integer overflow, access control flaws, and economic manipulation attacks. The OWASP (Open Web Application Security Project) Smart Contract Top 10 (OWASP, 2025a) provides a comprehensive catalog of the most critical smart contract vulnerabilities, serving as a foundation for blockchain-specific threat assessment.

Threat modeling tools such as Threat Dragon (OWASP, 2025b), Microsoft Threat Modeling Tool (Microsoft, 2022), and CAIRIS (CAIRIS, 2025) provide automated support for the threat modeling process, enabling systematic documentation of system architecture, threat identification, and mitigation planning. These tools facilitate collaboration among development teams, security professionals, and stakeholders while maintaining comprehensive documentation of security assessments.

The application of threat modeling to Health Web 3.0 DApps requires integration of traditional application security concerns with blockchain-specific vulnerabilities and healthcare privacy requirements. This multi-dimensional approach must consider technical vulnerabilities in smart contracts, privacy threats related to health data exposure, regulatory compliance requirements, and the complex interaction patterns between decentralized components and traditional healthcare infrastructure.

3. Architecture

This section presents our threat modeling architecture, for analyzing Health Web 3.0 DApps. Our approach recognizes that effective security assessment of decentralized healthcare applications requires a multi-layered methodology that addresses the distinct components of DApp infrastructure

while leveraging specialized frameworks and tools designed for privacy and smart contract security analysis. Figure 3 depicts the landscape of our research efforts, showing the conceptual abstractions of the target health care application and our main components for the threat modeling exercise, both detailed in the following sub-sections.

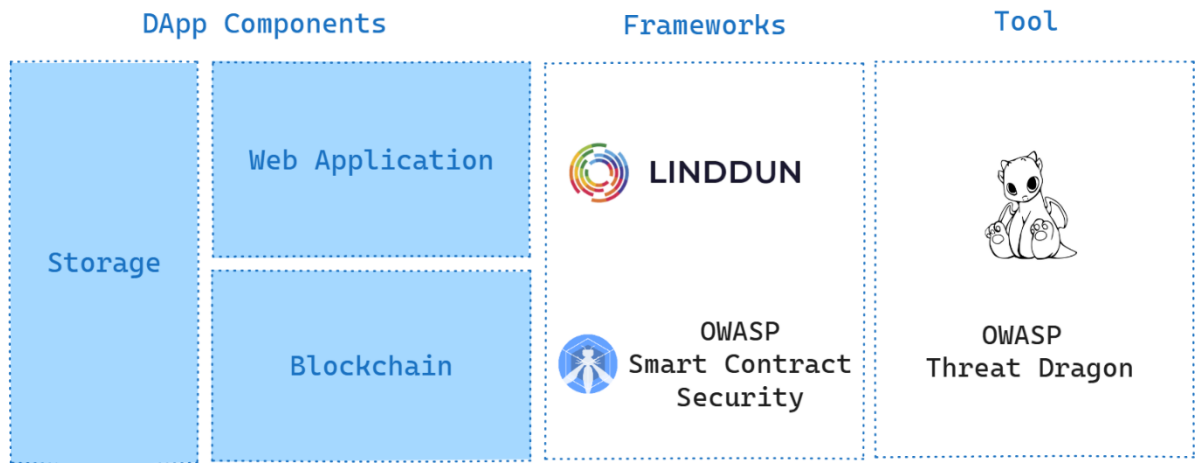


Figure 3 - Threat Modeling Landscape

3.1. DApp Component Analysis Framework

Our threat modeling analysis focuses on a Health Web 3.0 DApp currently being developed by a parallel research team, examining its abstracted architectural design rather than implementation-level code. This approach deliberately leverages the application's development status as an advantage: threat modeling frameworks are most effective when integrated throughout the software development lifecycle rather than applied retrospectively to completed systems. By conducting our security assessment during the active development phase, we demonstrate the practical value of proactive threat identification—enabling developers to address vulnerabilities during design and implementation rather than after deployment.

Health Web 3.0 DApps consist of three fundamental architectural layers, each presenting unique security challenges that require targeted assessment approaches. Our analysis framework systematically examines each component at the architectural level to ensure comprehensive threat identification across the entire application stack, providing actionable security insights that can inform ongoing development decisions.

3.1.1. Storage Layer

The storage component encompasses both on-chain and off-chain data management systems used by Health Web 3.0 DApps. On-chain storage includes data directly recorded on the blockchain, such as transaction records, smart contract state variables, and cryptographic hashes of medical documents. Off-chain storage systems, including decentralized storage networks like IPFS (InterPlanetary File System) (Daniel & Tschorsch, 2022) and traditional cloud storage solutions, handle larger data files such as medical images, detailed patient records, and clinical documentation.

Security considerations for the storage layer include data encryption mechanisms, access control implementations, data integrity verification, and compliance with healthcare data protection regulations. The immutable nature of blockchain storage creates unique challenges for data correction and patient privacy rights, while off-chain storage systems introduce additional attack vectors related to data availability and unauthorized access.

3.1.2. Web Application Layer

The web application layer represents the user interface and client-side logic that enables healthcare stakeholders to interact with the underlying blockchain infrastructure. This component includes web browsers, mobile applications, and specialized healthcare software interfaces that provide functionality for patient data management, clinical workflow automation, and healthcare service delivery.

The web application layer faces traditional web security threats such as cross-site scripting (XSS), SQL injection, and authentication vulnerabilities, while also introducing DApp-specific concerns related to wallet integration, transaction signing, and blockchain communication protocols. The integration of healthcare-specific requirements, including patient identity verification and clinical workflow support, creates additional complexity in the user interface layer (Al-Kahla et al., 2021).

3.1.3. Blockchain Layer

The blockchain component forms the core infrastructure that enables decentralized functionality, including smart contract execution, consensus mechanisms, and network communication protocols. This layer encompasses the underlying blockchain network (such as Ethereum or Hyperledger), smart contract implementations, and cross-chain interoperability protocols.

Security analysis of the blockchain layer focuses on smart contract vulnerabilities, consensus mechanism attacks, network-level threats, and economic manipulation attempts. The programmable nature of smart contracts introduces unique vulnerabilities that differ significantly from traditional software security concerns, requiring specialized assessment of methodologies and tools.

3.2. Multi-Framework Assessment Approach

Our threat modeling methodology integrates two complementary frameworks that address different aspects of Health Web 3.0 DApp security. This multi-framework approach ensures comprehensive coverage of both privacy-specific threats relevant to healthcare data and technical vulnerabilities inherent in smart contract implementations.

3.2.1. LINDDUN Framework for Privacy Threat Analysis

LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance) (LINDDUN, 2025) provides a systematic approach to identifying privacy threats in healthcare applications. This framework is particularly relevant for Health Web 3.0 DApps due to the sensitive nature of medical data and stringent regulatory requirements for patient privacy protection.

The LINDDUN methodology enables systematic evaluation of how patient data flows through DApp components, identification of potential privacy breaches, and assessment of compliance with healthcare privacy regulations such as HIPAA and GDPR. By applying LINDDUN principles to each DApp component, we can identify privacy risks that might not be apparent through traditional security assessment approaches.

3.2.2. OWASP Smart Contract Security Framework

The OWASP Smart Contract Top 10 (OWASP, 2025a) provides a comprehensive catalog of the most critical vulnerabilities affecting smart contract implementations. This framework addresses technical security concerns specific to blockchain-based applications, including coding errors, design flaws, and economic attack vectors that can compromise smart contract functionality.

Our application of the OWASP framework focuses on evaluating smart contracts used in Health Web 3.0 DApps, including patient consent management contracts, clinical trial automation logic, and healthcare payment processing systems. This analysis identifies potential vulnerabilities that could lead to unauthorized access to patient data, manipulation of clinical records, or disruption of healthcare services.

3.3. OWASP Threat Dragon

OWASP Threat Dragon (OWASP, 2025b) serves as our primary implementation tool for conducting systematic threat modeling across DApp components and frameworks. Threat Dragon provides a collaborative platform for documenting system architecture, identifying potential threats, and developing mitigation strategies while maintaining comprehensive documentation of the threat modeling process.

The tool's visual modeling capabilities enable clear representation of data flows between DApp components, identification of trust boundaries, and systematic enumeration of potential attack vectors. Threat Dragon's integration with established threat modeling methodologies supports consistent application of both LINDDUN and OWASP frameworks while providing structured documentation of findings and recommendations.

Our use of Threat Dragon facilitates collaborative analysis among security researchers, healthcare domain experts, and blockchain developers, ensuring that threat identification incorporates both technical security expertise and healthcare-specific knowledge. The tool's reporting capabilities support the development of actionable mitigation strategies and compliance documentation required for healthcare technology implementations.

3.4. Integrated Analysis Methodology

The integration of DApp component analysis, multi-framework assessment, and Threat Dragon implementation creates a comprehensive methodology for Health Web 3.0 DApp security evaluation. This approach ensures that threat identification spans technical vulnerabilities, privacy concerns, and healthcare-specific requirements while providing systematic documentation and mitigation planning.

Our methodology recognizes that effective security assessment of Health Web 3.0 DApps requires understanding of the complex interactions between traditional web application security, blockchain-specific vulnerabilities, and healthcare privacy requirements. By combining established threat modeling frameworks with specialized tools and systematic component analysis, we aim to provide comprehensive security guidance for developers and healthcare organizations implementing decentralized healthcare solutions.

The architectural framework presented in this section forms the foundation for our empirical analysis and findings, which will be detailed in subsequent sections of this paper. This methodology represents an initial step toward developing standardized approaches for Health Web 3.0 DApp security assessment, with future research building upon these foundational principles to address emerging threats and evolving regulatory requirements.

4. Threat Modeling Exercise Methodology

This study presents a preliminary threat modeling assessment of a Health Web 3.0 DApp currently undergoing active development by a parallel research team. The preliminary nature of this exercise is both intentional and methodologically advantageous, as threat modeling frameworks are designed to function as iterative security practices integrated throughout the software development lifecycle. By conducting our assessment during the design and development phases, we enable early identification and mitigation of vulnerabilities before they manifest in production systems. Our primary objective is to identify potential threats to patient confidentiality and privacy—the paramount security concerns in healthcare applications—while establishing a systematic framework that can be refined and expanded as the underlying application evolves.

We employed a multi-framework approach that integrates two complementary security methodologies to ensure comprehensive threat coverage. Our core methodology utilizes the LINDDUN framework (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance), a privacy-centric threat modeling approach that aligns directly with our focus on patient confidentiality and data protection. LINDDUN provides systematic categories for identifying privacy risks across data flows, storage mechanisms, and user interactions within decentralized architectures, making it particularly well-suited for healthcare applications where protecting sensitive medical information is critical. To address blockchain-specific vulnerabilities, we integrated the OWASP Smart Contract Security Guidelines as a complementary knowledge base. Smart contracts serve as the trust and access control layer in Health Web 3.0 DApps, and the OWASP guidelines provide a structured catalog of common vulnerabilities, that could compromise patient data confidentiality or enable unauthorized access to medical records.

Our threat modeling exercise focused on the abstracted architectural design of the Health Web 3.0 DApp rather than implementation-level code. This abstraction approach serves dual strategic purposes: it enables threat identification during the design phase when vulnerabilities are less costly to address, and it produces generalizable security insights applicable to similar blockchain healthcare

applications beyond this specific implementation. Working with the development team's architectural documentation, we decomposed the application into three fundamental components. The Web Application component represents the user-facing interface where patients, healthcare providers, and administrators interact with the system, handling authentication, data input, and results presentation. The Blockchain component serves as the notarization layer where health data integrity is verified, and access permissions are managed through smart contracts, ensuring tamper-proof audit trails without storing sensitive information on-chain. The Storage component encompasses off-chain decentralized storage solutions where actual private patient data, like medical records, diagnostic images, and personal health information, resides, separated from the public blockchain to maintain confidentiality while leveraging blockchain-based access control.

For each architectural component, we systematically applied LINDDUN privacy threat categories to identify potential risks to patient confidentiality, examining how data flows between components, where trust boundaries exist, and which interaction points could expose sensitive information. Concurrently, we cross-referenced potential attack vectors documented in OWASP smart contract security guidelines, focusing particularly on vulnerabilities in the Blockchain component that could lead to unauthorized data access or compromise the integrity of access control mechanisms. This layered analysis approach ensures comprehensive threat identification across user-facing interfaces, blockchain transaction logic governing data permissions, and storage mechanisms handling sensitive medical records. Identified threats were then prioritized based on their potential impact on patient confidentiality, data privacy, and regulatory compliance requirements under frameworks such as GDPR. This preliminary assessment establishes a baseline threat landscape that demonstrates the practical value of integrating holistic security assessment throughout the software development lifecycle, with findings that will inform ongoing development decisions and can be iteratively refined as the application architecture matures.

5. Discussion

This section presents our preliminary findings and insights gained from the initial phases of our Health Web 3.0 DApp threat modeling research. As an introductory study, our work has focused on establishing the foundational framework and conducting preliminary analysis across representative Health Web 3.0 applications. The insights presented here reflect our current understanding of the security landscape and provide direction for comprehensive threat assessment in decentralized healthcare systems.

5.1. Research Overview and Current Progress

Our research has progressed through several key phases, beginning with the systematic identification and categorization of Health Web 3.0 DApp components across multiple healthcare use cases. We have examined representative applications including decentralized patient record management systems, blockchain-based clinical trial coordination platforms, and peer-to-peer

telemedicine DApps. This analysis has provided valuable insights into the architectural patterns and security challenges common across different types of healthcare decentralized applications.

The application of our multi-framework approach—integrating LINDDUN privacy threat modeling, OWASP smart contract vulnerability assessment, and Threat Dragon systematic analysis—has revealed the complexity of security considerations in Health Web 3.0 environments. Our preliminary findings indicate that traditional cybersecurity frameworks, while necessary, are insufficient for addressing the unique challenges posed by the intersection of healthcare privacy requirements and blockchain technology constraints.

Through our systematic component analysis, we have identified recurring patterns in how Health Web 3.0 DApps handle sensitive health data, implement patient consent mechanisms, and manage cross-system interoperability. These patterns suggest both common vulnerabilities that span multiple applications and specialized threats that emerge from specific healthcare workflow implementations.

5.2. Key Insights from Privacy Threat Analysis

The application of LINDDUN methodology to Health Web 3.0 DApps has yielded significant insights into privacy-specific threats that differ substantially from general blockchain privacy concerns. Our analysis reveals that healthcare DApps face unique challenges in balancing the transparency inherent in blockchain technology with the stringent privacy requirements mandated by healthcare regulations, namely:

- **Linkability and Identifiability Concerns:** Our preliminary findings indicate that even when patient data is pseudonymized or encrypted, the immutable and transparent nature of blockchain transactions can create linkability patterns that potentially compromise patient privacy. The correlation of transaction patterns with external healthcare data sources presents risks that traditional privacy impact assessments may not adequately address.
- **Detectability and Disclosure Challenges:** Health Web 3.0 DApps often require complex data sharing scenarios involving multiple healthcare stakeholders. Our analysis suggests that current implementations may inadvertently create data disclosure pathways that violate healthcare privacy principles. The challenge lies in maintaining necessary clinical data accessibility while preventing unauthorized detectability of patient health status.
- **Regulatory Compliance Complexity:** The intersection of blockchain immutability with healthcare regulations requiring data correction and deletion rights (such as GDPR's "right to be forgotten") presents fundamental architectural challenges. Our research indicates that current Health Web 3.0 DApp designs often lack robust mechanisms for addressing these regulatory requirements without compromising system integrity.

5.3. Smart Contract Vulnerability Patterns

Our application of OWASP smart contract security analysis to healthcare DApps has revealed concerning patterns of vulnerabilities that are amplified in healthcare contexts due to the critical nature of medical data and processes. The economic incentives and attack motivations in healthcare applications differ significantly from traditional cryptocurrency applications, creating unique threat vectors. These are the main patterns:

- **Access Control Vulnerabilities:** Healthcare smart contracts typically implement complex access control mechanisms to manage different stakeholder roles (patients, healthcare providers, researchers, regulators). Our preliminary analysis suggests that many implementations suffer from inadequate access control validation, potentially allowing unauthorized parties to access or modify sensitive health information.
- **Business Logic Flaws:** The translation of complex healthcare workflows into smart contract logic introduces opportunities for business logic vulnerabilities. Our research indicates that clinical decision support contracts and automated treatment protocols may contain logic flaws that could lead to incorrect medical recommendations or treatment decisions.
- **Integration Security Issues:** Health Web 3.0 DApps frequently integrate with external healthcare systems and oracles providing real-world medical data. Our analysis reveals that these integration points often represent significant security vulnerabilities, particularly regarding data validation and source authentication.

5.4. Systemic Security Challenges

Beyond component-specific vulnerabilities, our research has identified systemic security challenges that emerge from the complex interactions between DApp layers and the healthcare ecosystem:

- **Cross-Chain Security Implications:** Many Health Web 3.0 applications use cross-chain protocols to achieve interoperability with different blockchain networks and healthcare systems. Our preliminary findings suggest that these cross-chain implementations introduce additional attack vectors related to bridge security, consensus validation, and data integrity across networks.
- **Legacy System Integration:** The integration of blockchain-based Health Web 3.0 DApps with existing healthcare infrastructure creates hybrid environments with complex security dependencies. Our analysis indicates that security vulnerabilities in legacy systems can potentially compromise the security assumptions of blockchain components, creating systemic risks.
- **Scalability and Security Trade-offs:** Healthcare applications require high throughput and low latency to support clinical workflows. Our research suggests that performance optimizations in Health Web 3.0 DApps often involve security trade-offs that may not be apparent to healthcare stakeholders but could significantly impact system security.

These challenges require holistic security approaches that consider the entire healthcare technology stack.

5.5. Implications for Healthcare Web3 Technology Adoption

Our preliminary findings have important implications for the adoption of Health Web 3.0 technologies in healthcare environments. The security challenges identified through our research suggest that current DApp implementations may not meet the stringent security and privacy requirements necessary for widespread healthcare adoption.

Healthcare organizations considering Health Web 3.0 DApp adoption face significant challenges in conducting appropriate risk assessments due to the novel nature of these technologies and the limited availability of healthcare-specific security guidance. Our research indicates that traditional healthcare technology risk assessment frameworks require substantial adaptation to address blockchain-specific threats.

The regulatory landscape for Health Web 3.0 applications remains largely undefined, creating challenges for healthcare organizations seeking to ensure compliance. Our analysis suggests that current DApp implementations may struggle to demonstrate compliance with existing healthcare regulations, potentially limiting adoption in regulated healthcare environments.

The deployment and maintenance of secure Health Web 3.0 DApps requires specialized expertise spanning healthcare domain knowledge, blockchain technology, and cybersecurity. Our findings indicate that the current shortage of professionals with this interdisciplinary expertise represents a significant barrier to secure implementation.

6. Conclusion

This paper presents a foundational investigation into the security challenges of Health Web 3.0 Decentralized Applications (DApps), establishing a comprehensive threat modeling framework specifically designed for healthcare blockchain environments. Our research addresses a critical gap in the current understanding of security risks associated with decentralized healthcare systems by integrating established privacy and smart contract security methodologies with healthcare-specific requirements.

Our primary contribution lies in the development of a multi-layered threat modeling architecture that systematically addresses the three fundamental components of Health Web 3.0 DApps: storage systems, web applications, and blockchain infrastructure. By integrating LINDDUN privacy threat modeling with OWASP smart contract security analysis and implementing this approach through Threat Dragon, we have established a comprehensive methodology for identifying and evaluating security risks unique to decentralized healthcare applications.

The research demonstrates that traditional cybersecurity frameworks, while necessary, are insufficient for addressing the complex security landscape of Health Web 3.0 environments. Our analysis reveals that the intersection of healthcare privacy requirements, regulatory compliance

mandates, and blockchain technology constraints creates novel security challenges that require specialized assessment approaches. Through our systematic component analysis, we have identified recurring security patterns across different types of healthcare DApps, including decentralized patient record management systems, blockchain-based clinical trial platforms, and peer-to-peer telemedicine applications.

Our preliminary analysis has yielded several critical insights that advance the understanding of Health Web 3.0 security challenges. The application of privacy-focused threat modeling reveals fundamental tensions between blockchain transparency and healthcare privacy requirements, particularly regarding patient data linkability and regulatory compliance with data protection laws. The smart contract security analysis highlights patterns of vulnerabilities that are amplified in healthcare contexts due to the critical nature of medical data and processes, including access control vulnerabilities, business logic flaws, and integration security issues that could compromise patient safety and data integrity.

The findings have significant implications for healthcare organizations considering the adoption of Health Web 3.0 technologies. The security challenges identified suggest that current DApp implementations may not meet the stringent requirements necessary for deployment in regulated healthcare environments. Healthcare technology stakeholders must carefully evaluate these risks and implement comprehensive security frameworks before adopting decentralized healthcare solutions.

The preliminary nature of this research opens several critical avenues for future investigation that are essential for advancing the security and adoption of Health Web 3.0 technologies. The development of standardized security assessment frameworks specifically designed for Health Web 3.0 applications represents the highest priority research direction, requiring purpose-built assessment methodologies that integrate healthcare regulatory requirements, blockchain security considerations, and privacy protection mechanisms. Future research should also investigate novel privacy-preserving technologies, including zero-knowledge proofs and homomorphic encryption, for healthcare blockchain applications while conducting comprehensive threat modeling to identify potential vulnerabilities.

Additionally, the development of comprehensive economic security models that account for the unique incentive structures and attack motivations present in healthcare environments requires significant research attention. Traditional blockchain economic security models may not adequately address the non-financial motivations and regulatory constraints that characterize healthcare applications. The evolving regulatory landscape for Health Web 3.0 applications also requires ongoing research to understand compliance requirements and develop practical implementation guidance.

Despite the significant contributions of this study, it is essential to acknowledge certain limitations. First, the analysis remains primarily conceptual, supported by structured threat modeling but lacking empirical validation through a real-world deployment or large-scale case study. Although the integration of LINDDUN with established knowledge bases offers a comprehensive theoretical

foundation, the effectiveness of the proposed mitigations remains untested in operational healthcare environments.

Second, the architecture presented constrained the scope of the threat modeling exercise. These omissions may underestimate systemic vulnerabilities that emerge in more heterogeneous Health Web 3.0 ecosystems.

Third, the study focused primarily on privacy-related threats (linkability, identifiability, unawareness, and non-compliance) identified via LINDDUN but did not equally explore adversarial dynamics such as advanced persistent threats, insider misuse, or emerging AI-driven attack strategies.

Future work could complement this privacy-centric approach with broader resilience assessments using STRIDE, DREAD, or hybrid models. Looking ahead, several avenues for further research are evident. Empirical validation through prototyping and penetration testing of a functional Health Web 3.0 DApp would provide secure evidence of the practicality of the mitigations proposed.

This research establishes a foundational understanding of the security challenges inherent in Health Web 3.0 DApps and provides a systematic approach for identifying and evaluating these risks. While our findings reveal significant security challenges that must be addressed before widespread healthcare adoption, they also demonstrate the potential for developing secure and privacy-preserving decentralized healthcare solutions through careful design and comprehensive security assessment. The complexity of Health Web 3.0 security requires sustained research effort and collaboration among healthcare professionals, blockchain developers, security experts, and regulatory authorities. The threat modeling framework and preliminary findings presented in this work provide a starting point for this collaborative effort, establishing the foundation for developing more secure and trustworthy decentralized healthcare systems.

Acknowledgments

This work was financially supported by Project BlockchainPT – Decentralize Portugal with Blockchain Agenda, WP 2: Health and Wellbeing, 02/C05-i01.01/2022.PC644918095-00000033, funded by the Portuguese Recovery and Resilience Program (PPR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program.

References

- Abrar, I., & Sheikh, J. A. (2024). Current trends of blockchain technology: architecture, applications, challenges, and opportunities. *Discover Internet of Things*, 4(1), 1–17.
<https://doi.org/10.1007/S43926-024-00058-5/TABLES/3>
- Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain Technology in Healthcare: A Systematic Review. *Healthcare 2019*, Vol. 7, Page 56, 7(2), 56.
<https://doi.org/10.3390/HEALTHCARE7020056>
- Alaba, F. A., Sulaimon, H. A., Marisa, M. I., & Najeem, O. (2024). Smart Contracts Security Application and Challenges: A Review. *Cloud Computing and Data Science*, 5, 15–41.
<https://doi.org/10.37256/CCDS.5120243271>

- Al-Kahla, W., Shatnawi, A. S., & Taqieddin, E. (2021). A Taxonomy of Web Security Vulnerabilities. *2021 12th International Conference on Information and Communication Systems, ICICS 2021*, 424–429. <https://doi.org/10.1109/ICICS52457.2021.9464576>
- Alotaibi, B. (2025). Cybersecurity Attacks and Detection Methods in Web 3.0 Technology: A Review. *Sensors 2025*, Vol. 25, Page 342, 25(2), 342. <https://doi.org/10.3390/S25020342>
- Austin, J. A., Lobo, E. H., Samadbeik, M., Engstrom, T., Philip, R., Pole, J. D., & Sullivan, C. M. (2024). Decades in the Making: The Evolution of Digital Health Research Infrastructure Through Synthetic Data, Common Data Models, and Federated Learning. *J Med Internet Res* 2024;26:E58637 <https://www.jmir.org/2024/1/E58637>, 26(1), e58637. <https://doi.org/10.2196/58637>
- CAIRIS. (2025). *Threat Modelling, Documentation and More*. <https://cairis.org/cairis/tmdocsmore/>
- Daniel, E., & Tschorsch, F. (2022). IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks. *IEEE Communications Surveys and Tutorials*, 24(1), 31–52. <https://doi.org/10.1109/COMST.2022.3143147>
- Dhingra, S., Raut, R., Naik, K., & Muduli, K. (2024). Blockchain Technology Applications in Healthcare Supply Chains - A Review. *IEEE Access*, 12, 11230–11257. <https://doi.org/10.1109/ACCESS.2023.3348813>
- Dobrovolska, O., Ortmanns, W., Dotsenko, T., Lustenko, V., & Savchenko, D. (2024). Health Security and Cybersecurity: Analysis of Interdependencies. *Health Economics and Management Review*, 5(2), 84–103. <https://doi.org/10.21272/HEM.2024.2-06>
- El-Saleh, A. A., Sheikh, A. M., Albreem, M. A. M., & Honnurvali, M. S. (2024). The Internet of Medical Things (IoMT): opportunities and challenges. *Wireless Networks*, 31(1), 327–344. <https://doi.org/10.1007/S11276-024-03764-8/FIGURES/14>
- European Parliament, & European Council. (2016). *Regulation - 2016/679 - EN - gdpr - EUR-Lex*. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- Gharavi, H., Granjal, J., & Monteiro, E. (2024). Post-Quantum Blockchain Security for the Internet of Things: Survey and Research Directions. *IEEE Communications Surveys and Tutorials*, 26(3), 1748–1774. <https://doi.org/10.1109/COMST.2024.3355222>
- Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: a literature review. *Journal of Management Analytics*, 7(3), 321–343. <https://doi.org/10.1080/23270012.2020.1801529;WGROU:STRING:PUBLICATION>
- Hammami, A. (2024). The Art of Threat Modeling. *Journal of Computer Sciences and Informatics*, 1(1), 1. <https://doi.org/10.5455/JCSI.20240710052550>
- Hepp, T., Sharinghousen, M., Ehret, P., Schoenhals, A., & Gipp, B. (2018). On-chain vs. off-chain storage for supply-and blockchain integration. *IT - Information Technology*, 60(5–6), 283–291. <https://doi.org/10.1515/itit-2018-0019>
- Limna, P. (2023). The Digital Transformation of Healthcare in The Digital Economy: A Systematic Review. *International Journal of Advanced Health Science and Technology*, 3(2), 127–132. <https://doi.org/10.35882/IJAHST.V3I2.244>
- LINDDUN. (2025). *linddun.org | Privacy Engineering*. <https://linddun.org/>
- Microsoft. (2022). *Microsoft Threat Modeling Tool overview - Azure | Microsoft Learn*. <https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool>
- Narayan, A., Weng, K., & Shah, N. (2024). Decentralizing Health Care: History and Opportunities of Web3. *JMIR Formative Research*, 8(1), e52740. <https://doi.org/10.2196/52740>
- Nweke, L. O., Abomhara, M., Yayilgan, S. Y., Comparin, D., Heurtier, O., & Bunney, C. (2022). A LINDDUN-Based Privacy Threat Modelling for National Identification Systems. *Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, NIGERCON 2022*. <https://doi.org/10.1109/NIGERCON54645.2022.9803177>
- OWASP. (2025a). *OWASP Smart Contract Top 10 | OWASP Foundation*. <https://owasp.org/www->

project-smart-contract-top-10/

- OWASP. (2025b). *OWASP Threat Dragon* | OWASP Foundation. <https://owasp.org/www-project-threat-dragon/>
- Rahim, J., Ihsan, M., Rahim, I., Afroz, A., & Akinola, O. (2024). Cybersecurity Threats in Healthcare IT: Challenges, Risks, and Mitigation Strategies. *Journal of Artificial Intelligence General Science (JAIGS)* ISSN:3006-4023, 6(1), 438–462. <https://doi.org/10.60087/JAIGS.V6I1.268>
- Shen, Y., Yu, J., Zhou, J., & Hu, G. (2025). Twenty-Five Years of Evolution and Hurdles in Electronic Health Records and Interoperability in Medical Research: Comprehensive Review. *J Med Internet Res* 2025;27:E59024 <https://www.jmir.org/2025/1/E59024>, 27(1), e59024. <https://doi.org/10.2196/59024>
- Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y. W. (2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers* 2024, Vol. 13, Page 41, 13(2), 41. <https://doi.org/10.3390/COMPUTERS13020041>
- Somma, A., De Benedictis, A., Esposito, C., & Mazzocca, N. (2024). The convergence of Digital Twins and Distributed Ledger Technologies: A systematic literature review and an architectural proposal. *Journal of Network and Computer Applications*, 225, 103857. <https://doi.org/10.1016/J.JNCA.2024.103857>
- Song, X., Xu, G., Huang, Y., & Dong, J. (2024). DID-HVC-based Web3 healthcare data security and privacy protection scheme. *Future Generation Computer Systems*, 158, 267–276. <https://doi.org/10.1016/J.FUTURE.2024.04.015>
- United States. (1996). *Health Insurance Portability and Accountability Act of 1996*. <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>
- Van Landuyt, D., & Joosen, W. (2022). A descriptive study of assumptions in STRIDE security threat modeling. *Software and Systems Modeling*, 21(6), 2311–2328. <https://doi.org/10.1007/S10270-021-00941-7/FIGURES/10>
- Wolf, A., Simopoulos, D., D'Avino, L., & Schwaiger, P. (2020). The PASTA threat model implementation in the IoT development life cycle. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, P-307, 1195–1204. https://doi.org/10.18420/INF2020_111
- Xia, L., Cao, Z., & Zhao, Y. (2024). Paradigm Transformation of Global Health Data Regulation: Challenges in Governance and Human Rights Protection of Cross-Border Data Flows. *Risk Management and Healthcare Policy*, 17, 3291. <https://doi.org/10.2147/RMHP.S450082>

Integration of Citizen's Card Digital Authentication in Hyperledger Fabric

Carlos Machado Antunes
*School of Technology and
Management, Polytechnic of
Leiria, Portugal*
carlos.machado@ipleiria.pt
0009-0005-7010-4328

Marisa Maximiano
*School of Technology and
Management, Polytechnic of
Leiria; CIIC, Portugal*
marisa.maximiano@ipleiria.pt
0000-0002-1212-7864

Vítor Távora
*School of Technology and
Management, Polytechnic of
Leiria, Portugal*
vititor.tavora@ipleiria.pt
0009-0004-0404-9378

Ricardo Gomes
*School of Technology and
Management, Polytechnic of
Leiria, Portugal*
ricardo.p.gomes@ipleiria.pt
0000-0002-0438-9119

Manuel Dias
BioGHP, Portugal
manuel@bioghp.com
0009-0000-1830-6479

Ricardo Correia Bezerra
BioGHP, Portugal
ricardo@bioghp.com
0009-0005-1237-6632

Received: 7 June 2025

Accepted: 24 November 2025

Abstract

This study investigates the integration of the Portuguese Citizen's Card authentication with Hyperledger Fabric blockchain technology, addressing the challenge of bridging traditional government-issued digital identities with blockchain-based systems, particularly focusing on reducing barriers to Web3 adoption for users unfamiliar with decentralized technologies. The proposed solution leverages the Autenticação.gov Software Development Kit (SDK), developed by the Portuguese Agency for Administrative Modernization (AMA) to create a secure bridge between the Citizen's Card authentication system and Hyperledger Fabric's permissioned blockchain framework. The study examines how this approach can facilitate the development of transparent, tamper-proof authentication systems suitable for critical applications such as e-voting and digital government services, and also feasible for on-premises systems. The findings suggest that integrating existing digital identity systems with blockchain technology can promote wider acceptance of decentralized solutions while maintaining security, privacy, and accessibility standards required for public sector applications.

Keywords *Blockchain, Authentication, Smart Card, Private Key Management*

1. Introduction

Hyperledger Fabric (HLF) is a modular and extensible open-source system for deploying and operating permissioned blockchains and one of the Hyperledger projects hosted by the Linux Foundation (George, 2022). As one of the flagship projects under the Hyperledger umbrella, Fabric has emerged as a leading solution for organizations seeking to implement blockchain technology in enterprise environments where privacy, scalability, and controlled access are mandatory.

Unlike public blockchains that operate in a trustless environment with anonymous participants (Hope, 2019), HLF is specifically designed for permissioned networks where all participants have known and authenticated identities. In this system, X.509 certificates are the foundation of identity and authentication (Santhosh & Reshmi, 2023). They are used to represent the digital identity of nodes

(peers, orderers), clients, and administrators, ensuring secure communication and access control within the blockchain network. These certificates are issued by a Certificate Authority (CA) and define the permissions and roles of each participant. HLF includes a CA called Fabric CA that provides certificate management services for the network.

This study investigates the integration of the Portuguese Citizen's Card with Fabric CA and the HLF blockchain, focusing on secure authentication processes. The primary objective is to explore how existing authentication systems, such as digital authentication through the Citizen's Card, can be adapted to enhance user security and accessibility within blockchain environments, addressing the challenge of bridging traditional government-issued digital identities with blockchain-based systems, particularly focusing on reducing barriers to Web3 adoption for users unfamiliar with decentralized technologies. We demonstrate how digital authentication through the Citizen's Card can be accomplished using the Autenticação.Gov Software Development Kit (SDK) (Agência para a Modernização Administrativa, 2025).

The remainder of this document is organized as follows: the next section presents the research questions and describes the research method used. Section 3 provides an overview of the related concepts and work. Section 4 presents our main contribution with the proposed solutions for the integration of digital authentication through the Citizen's Card. Finally, the last section shows the conclusions and future work challenges.

2. Research Questions and Methodology

This document reflects the efforts employed to answer the following research questions:

1. Is it possible to authenticate and control access of an end-user using the digital authentication through a smart card, such as the Portuguese Citizen's Card, in HLF?
2. What processes can be implemented to register and authenticate the end-user through the Portuguese Citizen's Card in HLF?
3. What are the performance impacts of integrating the digital authentication through the Portuguese Citizen's Card in HLF?

The methodology we follow is depicted in Figure 1 and comprises three stages: we start by reviewing the related concepts, followed by a review of existing libraries, frameworks and SDKs. The final stage is dedicated to the implementation of exploratory code to assert the validity of our proposed solutions.

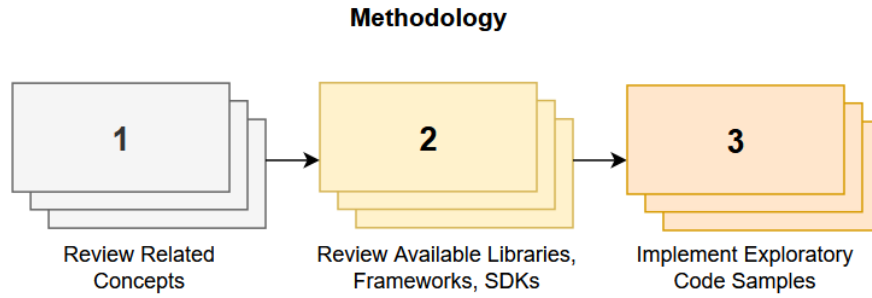


Figure 1. Methodology

The exploratory code samples for Research Question 1 and 2 required the creation of a HLF v2.5 network with one channel and two organizations, including the setup of Fabric CA for each organization, and the development of a desktop client application and a Representational State Transfer (REST) service for testing the authentication processes, as shown in Figure 2.

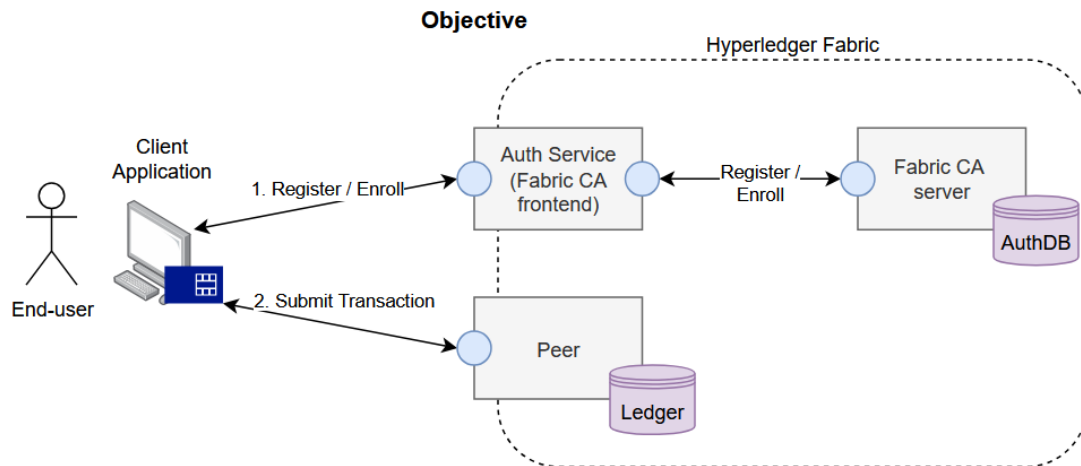


Figure 2. Research Objective

3. Related Concepts and Work

This section begins by presenting the key concepts that are at play in this study. We review three fundamental domains: Distributed Ledger Technology (DLT) and blockchains that enable the creation of decentralized applications, smart card technology allowing for secure authentication processes.

The last sub-section reviews the related work by identifying other blockchain-based platforms that use digital authentication through smart cards and provides a comparison between these platforms and the work presented in this document.

3.1. Blockchain

Blockchain, originally developed for cryptocurrencies, is a decentralized, peer-to-peer ledger technology that distributes data across a network of nodes (Belotti et al., 2019). This structure ensures that no single entity controls the entire system, enhancing security and transparency among all the participants. Transactions are grouped into cryptographically linked blocks, forming an

immutable chain resistant to tampering. Each block contains a hash of the previous block, a timestamp, and transaction data organized in a Merkle tree structure. This design allows for data integrity verification and pseudo-anonymization of transactions while maintaining traceability. The consensus mechanism and the chain's structure make unauthorized modifications practically impossible, as altering one block would require changing all subsequent blocks and gaining network-wide agreement (Gorkhali et al., 2020).

Blockchain networks can be fundamentally categorized into two distinct architectural models: permissionless model operates as open networks where anyone can participate without requiring approval from a central authority, and permissioned model restricts network participation to a predefined set of authorized nodes, organizations, or users. These systems require explicit permission to join the network, validate transactions, or participate in consensus processes (Somma et al., 2024).

Hyperledger Fabric exemplifies the permissioned blockchain approach, serving as a modular enterprise-grade platform specifically designed for business applications. Unlike permissionless networks that rely on anonymous participation, Hyperledger Fabric implements a comprehensive identity management system using X.509 digital certificates to authenticate and authorize all network participants. Each organization, peer node, orderer, and client application must possess valid X.509 certificates issued by CAs before they can interact with the network. This certificate-based identity framework enables fine-grained access control policies, ensuring that only authorized entities can perform specific operations such as invoking smart contracts, querying ledger data, or participating in transaction endorsement processes (Fadele Ayotunde Alaba et al., 2023).

3.2. Smart Cards

Smart cards, such as the Portuguese Citizen's Card, are a fundamental technology used in modern digital authentication systems, serving as secure hardware tokens that combine portability with robust cryptographic capabilities (Gupta & Quamara, 2019). A smart card is a secure microcontroller that is typically used for generating, storing and operating on cryptographic keys, fundamentally transforming how digital identity verification and transaction authentication are conducted across various domains. These tamper-resistant devices have evolved from simple storage mechanisms to sophisticated cryptographic processors capable of executing complex authentication protocols while maintaining the highest security standards. The cryptographic architecture of modern smart cards, such as the Portuguese Citizen's Card, enables both authentication and digital signature capabilities through sophisticated key management systems. The Citizen's Card contains dual-certificate structures, where the authentication signatures allow the card to prove his identity and the certificate also contains privacy-sensitive information such as gender, date of birth, and national number, just to mention a few. The non-repudiation signature is used for generating electronic signatures.

One of the methods available that allows the integration of digital authentication through the Portuguese Citizen's Card is by using the Autenticação.Gov SDK with a smart card reader to access

the Citizen's Card X.509 certificates and to generate digital signatures, required for signing and submitting transactions to the HLF network. The Portuguese Agency for Administrative Modernization (AMA) is the agency responsible for the development of Autenticação.Gov SDK, a SDK that provides a set of tools and libraries that allow to perform several operations with the Portuguese Citizen's Card, such as signing documents (or any other type of content), secure authentication, and access to citizen's personal data (Agência para a Modernização Administrativa, 2025). The SDK abstracts the Application Protocol Data Unit (APDU) commands used to communicate with the Citizen's Card in a class library originally written in C++ but also available in Java. Besides Typescript and Go, Java is also supported by HLF (Mansour et al., 2024), so this was the programming language we selected for the development of the exploratory code. The code also depends on Bouncy Castle library (Legion of the Bouncy Castle Inc., 2025b) to support some of the cryptographic operations required to implement the authentication process.

3.3. Related Work

The integration of blockchain technology with smart card-based digital authentication represents an emerging frontier in national identity systems. While several countries have implemented advanced smart card identity systems, the degree of blockchain integration varies significantly. This review examines notable implementations including Estonia's ID-card system, the United Arab Emirates' Emirates ID, Luxembourg's EDDITS project, along with their use of distributed ledger technologies.

3.3.1. Estonia's ID-card system

Estonia represents one of the most advanced implementations of blockchain technology in conjunction with smart card identity systems. The Estonian ID-card utilizes Keyless Signature Infrastructure (KSI), a blockchain-like technology that ensures the integrity of digital assets while providing verifiable proof of time, identity, and authenticity (Estonian Business and Innovation Agency, 2025).

The blockchain infrastructure underlying Estonia's digital identity system serves multiple security functions. The immutable ledger records every piece of data interaction, creating an auditable trail that guarantees data has not been tampered with. This technology supports various security features including two-factor authentication and fraud detection mechanisms. The Estonian system has achieved a considerable scale, with over 1.3 billion electronic signatures executed through the platform as of 2021, demonstrating both the robustness and user acceptance of blockchain-integrated smart card authentication (Parsovs, 2020).

3.3.2. United Arab Emirates Emirates ID system

The United Arab Emirates (UAE) has implemented the Emirates ID card as a mandatory identification document for all citizens and residents, featuring advanced biometric security including fingerprint recognition (TDGRA, 2024). While the UAE has articulated ambitious blockchain strategies, including the Emirates Blockchain Strategy 2021, the direct integration of blockchain technology with the physical Emirates ID card itself is less documented compared to Estonia's implementation (TDGRA, 2022).

The UAE government's blockchain strategy envisions using distributed ledger technology for digital transactions, with plans to assign each customer a unique identification number pointing to their information on a secure chain. The Emirates ID has been integrated with various smart services and e-government platforms, including the UAE Pass – a digital identity and signature solution enabling secure login to government and private sector services (TDGRA, 2024).

Recent developments indicate the UAE is moving toward a facial recognition-based digital identity system, with plans announced in 2025 to potentially replace physical Emirates ID cards.

3.3.3. Luxembourg's EDDITS project

Luxembourg has developed an innovative approach to blockchain-based digital identity through the Ethereum Decentralized Digital Identity Trust Services (EDDITS) project. This initiative represents a collaboration between LuxTrust, a government-backed digital identity firm formed in 2005, and INTECH, launching what was described as a world first in the blockchain industry for identity verification (Kuperberg Michael and Kemper, 2019).

EDDITS operates on INFRACHAIN, Luxembourg's governance-trusted permissioned blockchain platform, and provides a solution to one of blockchain's persistent challenges: identity verification. The service allows users to link their LuxTrust strong identity credentials to their blockchain identity (specifically Ethereum addresses), enabling any Ethereum service provider to verify such identity through cryptographic claims (Tanzim Nawar et al., 2023). This bridge between traditional trusted identity systems and decentralized blockchain applications represents a significant architectural innovation.

Users can prove specific attributes such as their name, email, or postal address to online service providers without revealing unnecessary information. The system enables users to manage their digital identity through smart contracts, control access keys, review claims, and even digitally sign documents using their blockchain identity.

EDDITS demonstrates a practical model for integrating existing national eID infrastructure (Luxembourg's electronic identity cards and LuxTrust certificates) with blockchain-based identity systems. Rather than replacing the physical smart card infrastructure, EDDITS creates a trusted linkage layer that extends traditional identity credentials into the blockchain ecosystem, providing strong authentication guarantees for decentralized applications.

3.3.4. Comparative analysis

The examination of these systems reveals several architectural approaches to integrating distributed ledger technologies with smart card authentication:

- Estonia employs a hybrid model where blockchain technology (KSI) provides an immutable audit trail and integrity verification layer, while smart cards handle the actual authentication and digital signing operations. This separation allows for robust security while maintaining user privacy.

- The UAE is pursuing a more ambitious transformation, with blockchain infrastructure planned for the backend of digital identity services, though the extent of integration with physical smart cards remains evolving. The emphasis on mobile digital identity suggests a transition toward software-based authentication that may eventually supersede physical cards.
- Luxembourg's EDDITS represents a bridging architecture that connects existing trusted identity systems (smart cards and digital certificates) to blockchain platforms. Rather than replacing physical credentials, EDDITS extends their utility into decentralized ecosystems, demonstrating how legacy infrastructure can be preserved while gaining blockchain benefits.

Luxembourg's EDDITS project is close to what we demonstrate in this paper, but in comparison with all these systems, we show in the following section that it's also possible to integrate smart card digital authentication, such as the Portuguese Citizen's card, with Hyperledger Fabric platform, a platform that is not used by any of the national identity systems mentioned. The use of this platform is significant, mainly due to the private and permissioned nature of Hyperledger Fabric blockchain. Anyone can use this platform for any business purpose other than providing government services, with complete control over the blockchain infrastructure, and still use smart card digital authentication that is trusted nation-wide.

4. Research

Following our comprehensive review of the relevant concepts and work, and extensive testing, we confidently respond to Research Question 1 affirmatively, it is technically possible to use X.509 certificates stored in a smart card, such as the Portuguese Citizen's Card, to authenticate, sign and submit transactions to the HLF blockchain, as long as the following two core requirements are met:

1. The cryptographic algorithm supported by the smart card X.509 certificates must match the algorithm used by HLF for transaction signature and validation, which is Elliptic Curve Digital Signature Algorithm (ECDSA) with curve P-256. Since June 2024, and in compliance with the EU Regulation 2019/1157 of the European Parliament (European Parliament & European Council, 2019), the Portuguese State began issuing a new version of the Portuguese Citizen's Card (Governo da República Portuguesa, 2024), which includes X.509 certificates generated with ECDSA with curve P-256 key pairs (Agência para a Modernização Administrativa, 2025). Previous versions of the Citizen's Card used Rivest-Shamir-Adleman (RSA) cryptography with 3072-bit key size.
2. If HLF Node Organizational Units (OU) are enabled, the OU of the certificate's Distinguished Name (DN) must match one of the supported roles by HLF, which are named as "peer", "orderer", "admin", or "client".

Besides these requirements, it's also important to consider that HLF uses Attribute Based Access Control (ABAC) to allow or deny access to chaincode functions based on the attributes of the caller's identity certificate. These attributes are defined as key-value pairs associated with user identities during enrollment with Fabric CA and some are reserved for use by HLF itself. The attributes are

added to the X.509 extensions section of the certificate as a Javascript Object Notation (JSON) document with Object Identifier (OID) “1.2.3.4.5.6.7.8.1”, as in the following example shown in Figure 4.

```

23      X509v3 extensions:
24      X509v3 Key Usage: critical
25      Digital Signature
26      X509v3 Basic Constraints: critical
27      CA:FALSE
28      1.2.3.4.5.6.7.8.1:
29      {"attrs":{"hf.Affiliation":"","hf.EnrollmentID":"org1admin","hf.Type":"admin"}}

```

Figure 4. HLF X.509 extension attributes

The knowledge of these requirements is critical to provides answers to Research Question 2, which focuses on the processes to implement end-user registration and authentication processes through the Portuguese Citizen's Card. The next sections detail the steps required to implement these processes.

4.1. End-user Registration

Typically, the end-user is registered with Fabric CA by an administrator, but this operation can also be performed autonomously. The proposed solution is a two-step process detailed on the sequence diagrams shown in Figure 5 and 6, where a client application obtains the required data from the Citizen's Card inserted on a smart card reader using Autenticação.Gov SDK.

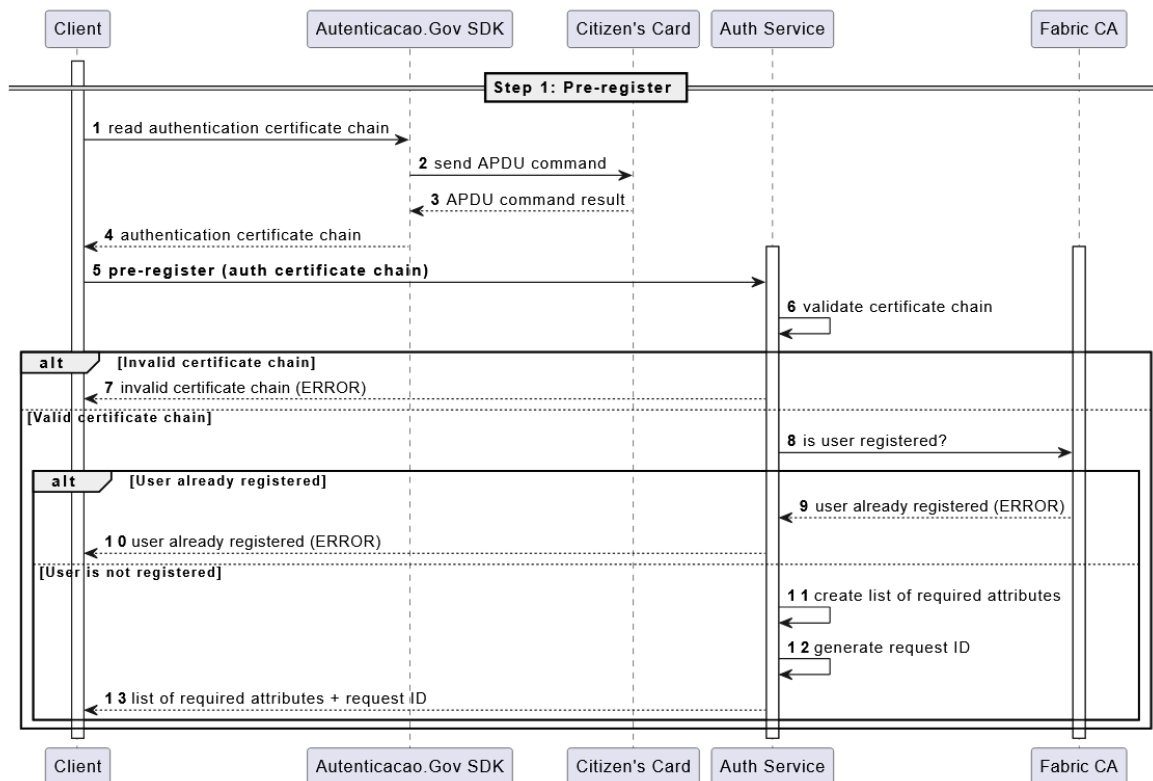


Figure 5. End-user pre-registration through Citizen's Card (step 1)

In the first step, the certificate chain is read from the Citizen's Card and sent to the authentication service. The service then validates the certificate chain and, if it's valid, replies to the client application with a list of attributes that the end-user must provide to complete the registration (for instance, date of birth). It is recommended to also include an attribute that corresponds to some identifier that is unique to the end-user, such as the Citizen's Card Number, the Social Security Number, etc. to be used as the user ID that is going to be registered in Fabric CA. A nonce should also be sent to the client application to be included in the signed document to prevent replay attacks.

In the second step, depicted in Figure 6, the client application reads the attribute values from the Citizen's Card that corresponds to the list of attributes requested by the authentication service.

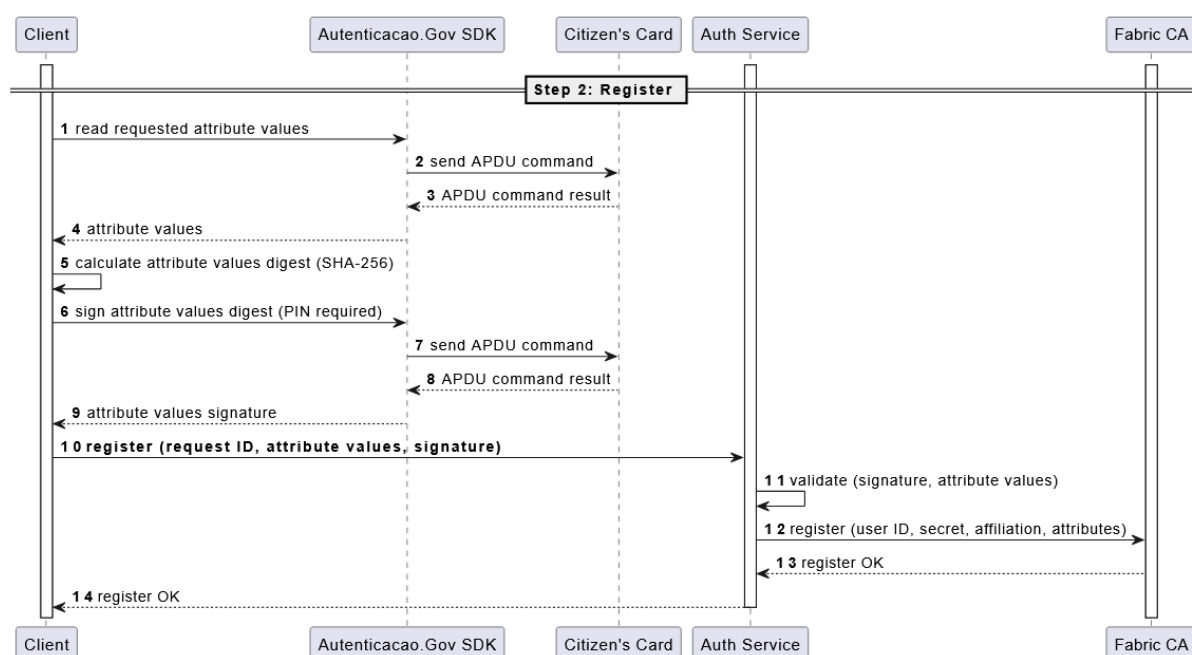


Figure 6. End-user registration through Citizen's Card (step 2)

The client application collects all the attribute values in an Extensible Markup Language (XML) document, adds the nonce to the document, and asks to digitally sign that document with the Citizen's Card. The end-user must insert the Personal Identification Number (PIN) to successfully sign the XML document. Afterwards, the client application sends the XML document and the digital signature to the authentication service to complete the registration process. Fabric CA also requires an enrollment secret to be provided in order to fulfill the registration request, which is automatically generated by the authentication service based on the SHA-256 thumbprint of the Citizen's Card certificate sent by the client application in step 1. When the registration process is completed, a new record is added to the 'users' table in Fabric CA database with the following example data presented in Table 1 (some columns omitted for brevity).

Table 1. 'Users' table in Fabric CA database

id	token	type	attributes
123456789	\$2a\$10\$1baN7AWIGnKkFdlBI81ieOtBrpJ5KEp9Z	client	[{"name":"hf.EnrollmentID","value":"123456789", "ecert":true},

azC433E27ytWpxHYuEeq	{ "name": "hf.Type", "value": "client", "ecert": true}, {"name": "hf.Affiliation", "value": "", "ecert": true}, {"name": "birthDate", "value": "20010203", "ecert": true}]
----------------------	---

Table 1 shows that, along with the end-user attributes, Fabric CA also adds the attributes reserved by HLF to the table record when the user is registered.

4.2. End-user Authentication

Following the registration process, the end-user identity must be created, and this is accomplished by enrolling the end-user with Fabric CA. The proposed solution for this operation is also a two-step process detailed on the sequence diagrams shown in Figures 7 and 8, and it also starts with a client application reading the authentication certificate chain from the Citizen's Card and sending it to the authentication service.

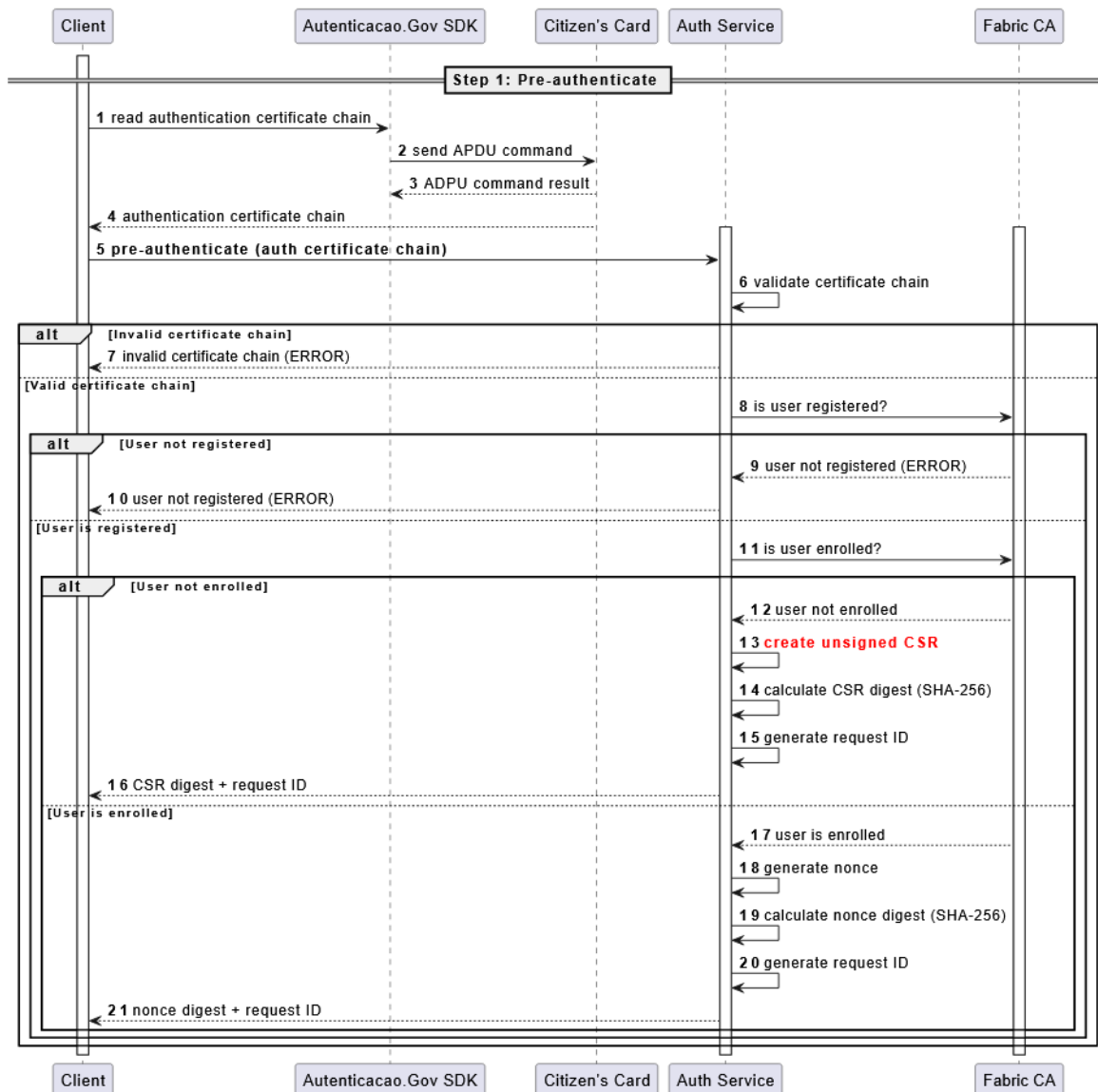


Figure 7. End-user pre-authentication through Citizen's Card (step 1)

The first time the end-user tries to authenticate to the authentication service, Fabric CA is requested to issue a X.509 certificate with the appropriate DN and user attributes. The critical action is emphasized in bold red in Figure 7 (action number 13), which is the action of creating an unsigned Certificate Signing Request (CSR). A private key is not required to create an unsigned CSR because, as the name implies, it is created without a signature. Nevertheless, it is possible to calculate the unsigned CSR's digest and request the end-user to sign that digest. The resulting signature is then embedded in the CSR, thus completing its definition. Neither the JDK nor Bouncy Castle (for Java) provides support to create this type of CSR, but the .NET implementation of the Bouncy Castle library provides this feature (Legion of the Bouncy Castle Inc., 2025a), so we ported the CSharp code to Java.

The unsigned CSR is created with the same public key and DN defined in the certificate sent by the end-user, except that:

- The Organizational Unit (OU) attribute value of the DN is replaced with the term “client”.
- The Common Name (CN) attribute value of the DN must match the user ID registered in Fabric CA, so it is also replaced if needed.

The CSR's SHA-256 digest is calculated and then sent back to the client for the end-user to digitally sign it. As depicted in Figure 8, the digital signature is sent to the authentication service to sign the CSR and send it to Fabric CA for enrolling the end-user by issuing a new X.509 certificate. If the operation succeeds, the issued certificate includes the attributes that were previously recorded in the 'users' table during end-user registration process.

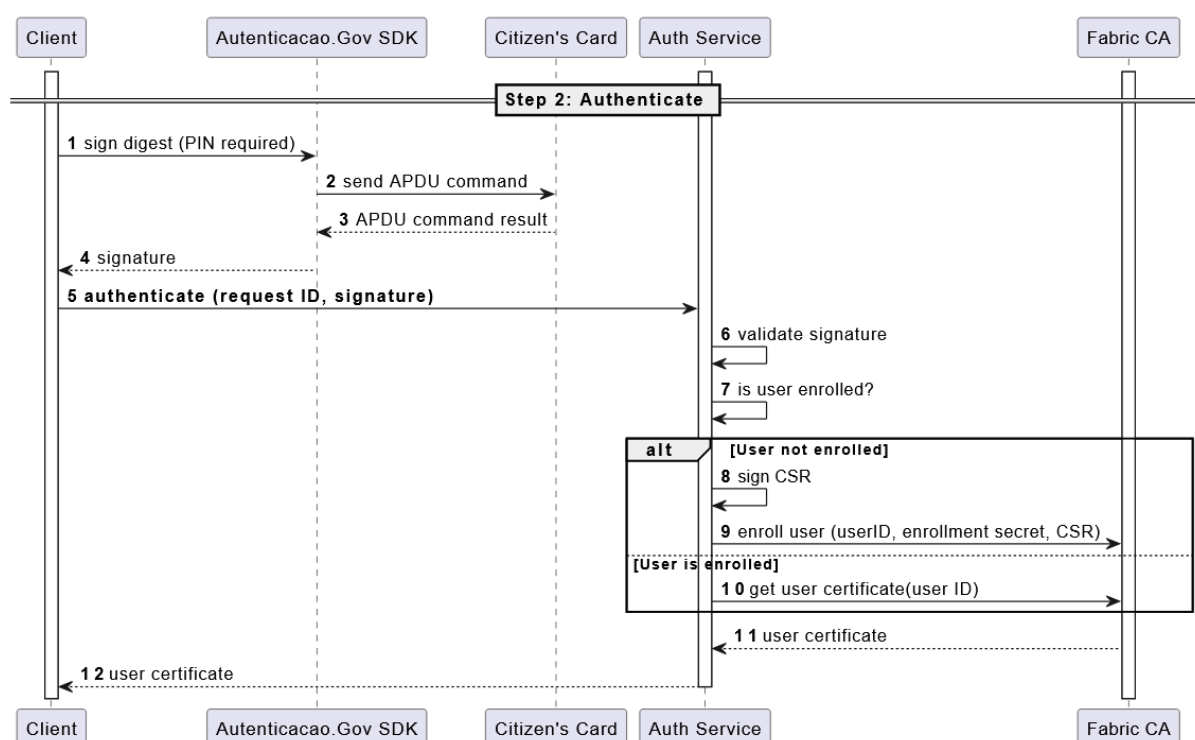


Figure 8. End-user authentication through Citizen's Card (step 2)

If the end-user is already enrolled, the authentication service simply generates a nonce, calculates its SHA-256 digest and sends it to the client for the end-user to digitally sign it. The digital signature is sent back to the authentication service, validates it and gets the X.509 certificate from Fabric CA.

In the end of this process, the client application gets the X.509 certificate provided by Fabric CA and can use the Citizen's Card private key, through the Autenticação.Gov SDK, to sign and submit transactions to HLF network. To achieve this, the client application uses the Hyperledger Fabric Gateway Client Application Programming Interface (API) to connect to a HLF peer and invoke chaincode to submit transactions to the HLF network (Hyperledger, 2025). In order to connect to a HLF peer, the client application must specify an instance of Identity and Signer, which are two interfaces that are included in the Gateway Client API. The Identity is an abstraction of the X.509 certificate provided by Fabric CA and the Signer is a custom implementation that signs a digest using the Citizen's Card through the Autenticação.Gov SDK. An example of such an implementation is presented in Figure 9:

```
1 package ...;
2
3 import java.security.GeneralSecurityException;
4 import org.hyperledger.fabric.client.identity.Signer;
5 import pt.gov.cartao decidadao.*;
6
7 public class CitizenCardSigner implements Signer {
8
9     @Override
10    public byte[] sign(byte[] digest) throws GeneralSecurityException {
11        try {
12            PTEID_ReaderSet readerSet = PTEID_ReaderSet.instance();
13            PTEID_ReaderContext reader = readerSet.getReader();
14            if (reader == null) {
15                throw new GeneralSecurityException("Smart card reader not found.");
16            }
17            if (!reader.isCardPresent()) {
18                throw new GeneralSecurityException("Citizen's card not present.");
19            }
20            PTEID_Card card = reader.getCard();
21            // PIN is requested to the end-user whenever Sign() method is called.
22            PTEID_ByteArray signature = card.Sign(new PTEID_ByteArray(digest, digest.length));
23            return signature.GetBytes();
24        } catch (PTEID_Exception ex) {
25            throw new GeneralSecurityException("Smart card error.", ex);
26        }
27    }
28 }
```

Figure 9. Custom implementation of Signer interface

Whenever the client needs to sign a transaction, the code presented in Figure 9 is executed, thus requiring the end-user to provide the PIN to fulfill the signature request. This means that, to submit a transaction, the client must wait for user input, and this has a great impact on the overall time to complete the transaction, as we demonstrate in the following section.

The next section tries to answer Research Question 3, where we show the performance tests and corresponding results that allow us to estimate the performance impacts of the proposed integration of smart card digital authentication in Hyperledger Fabric.

4.3. Performance Analysis

To measure the performance of the proposed integration, we implemented another version of the authentication service to serve as our reference. This version simply acts as a proxy to Fabric CA to register and enroll users with randomly generated enrollment secrets, and without performing any data validations. All the charts presented in this section show the time in microseconds and simulate the sequential registration and authentication of 1000 users.

The chart depicted in Figure 10 shows the time to register and enroll users with our reference version. On average, it takes around 68 milliseconds to register and 64 milliseconds to enroll a user.

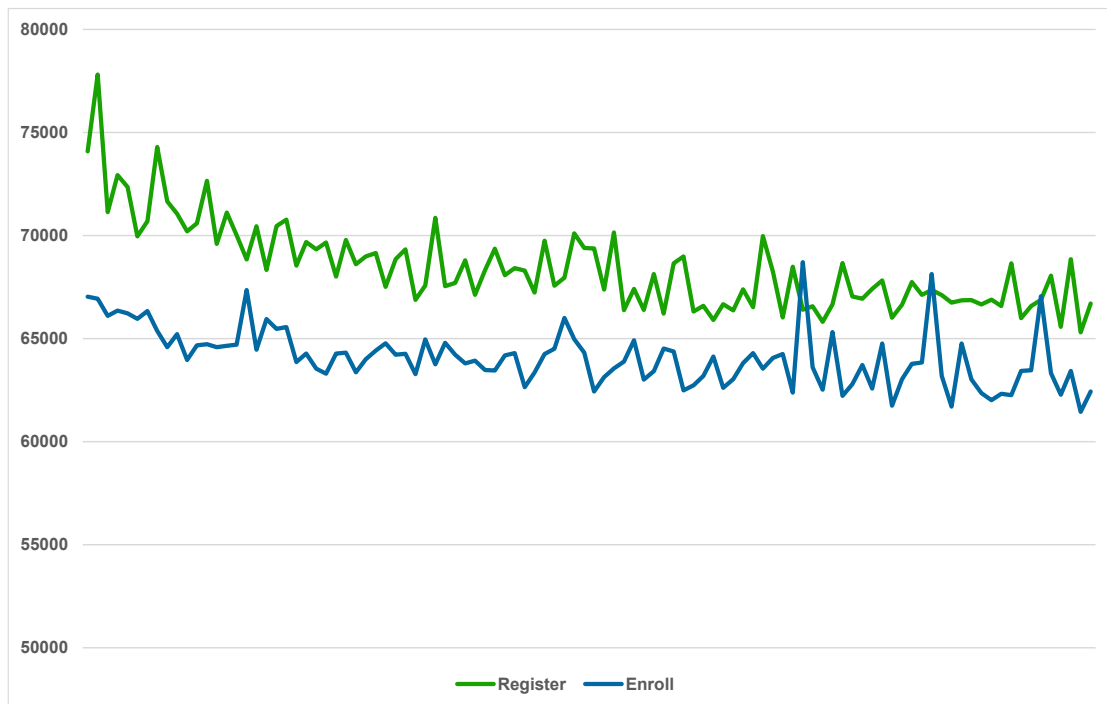


Figure 10. Reference time to register and enroll users

To compare the values with our reference version, we used the version of the authentication service that integrates smart card authentication with Fabric CA to run tests and measure the time to register and authenticate users. With this version, we executed the tests with three different configurations, all concerned with certificate revocation validation of the Citizen's Card certificate: i) without revocation validation, ii) with revocation validation and without Certificate Revocation List (CRL) caching and iii) with revocation validation and with CRL caching. The main reason for having these three configurations is to allow us to better estimate the time the authentication service takes to process the request and the time it takes to download the CRLs to check if the Citizen's Card was revoked.

4.3.1. Test results without revocation validation

Figure 11 shows a stacked line chart with the time to pre-register and register users with the authentication service that integrates smart card authentication with Fabric CA with revocation validation disabled. On average, it takes around 76 milliseconds to pre-register and register a user.

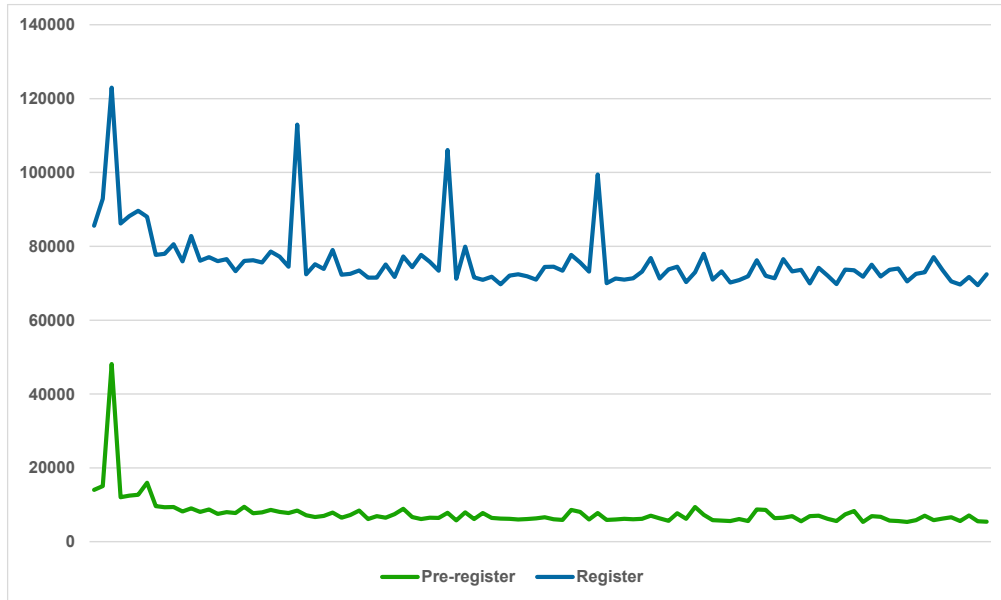


Figure 11. Time to register users with revocation validation disabled

Figure 12 shows a stacked line chart with the time to pre-authenticate and authenticate users with revocation validation disabled. On average, it takes around 28 milliseconds to pre-authenticate and authenticate a user, which is less than our reference version. This is because neither our service nor Fabric CA is required to generate a new key pair for the user's certificate.

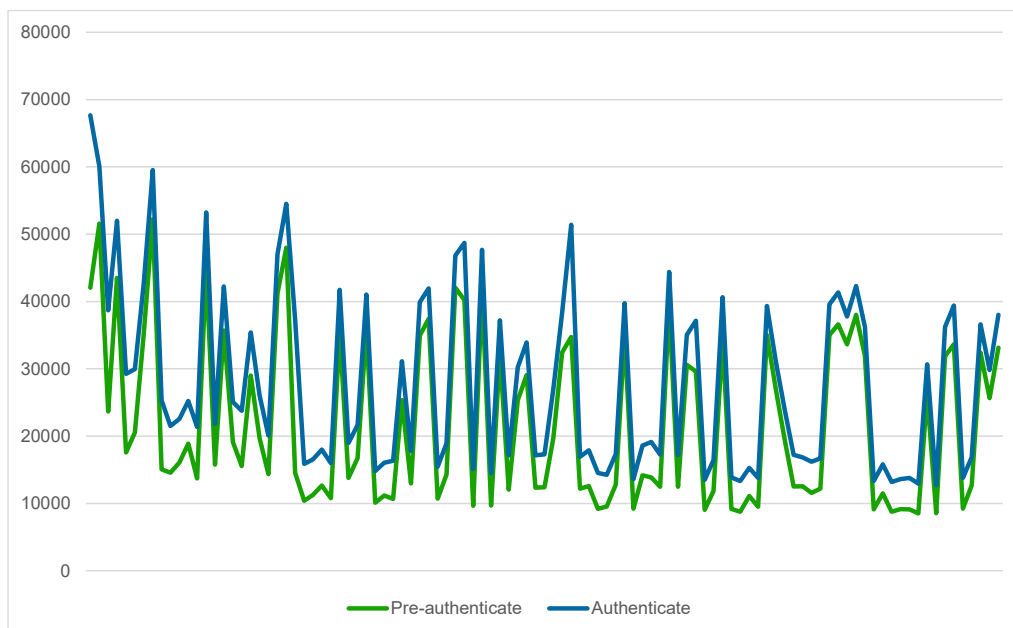


Figure 12. Time to authenticate users with revocation validation disabled

4.3.2. Test results with revocation validation

Figure 13 shows a stacked line chart with the time to pre-register and register users with revocation validation enabled. On average, it takes around 1.1 seconds to pre-register and register a user which is more than 14 times greater than the times measured with the reference version. Whenever the service needs to validate a Citizen's Card certificate it also downloads the CRLs from the Portuguese Citizen's Card CA to check if the certificate was revoked, causing this drastic increase of time to process the request.

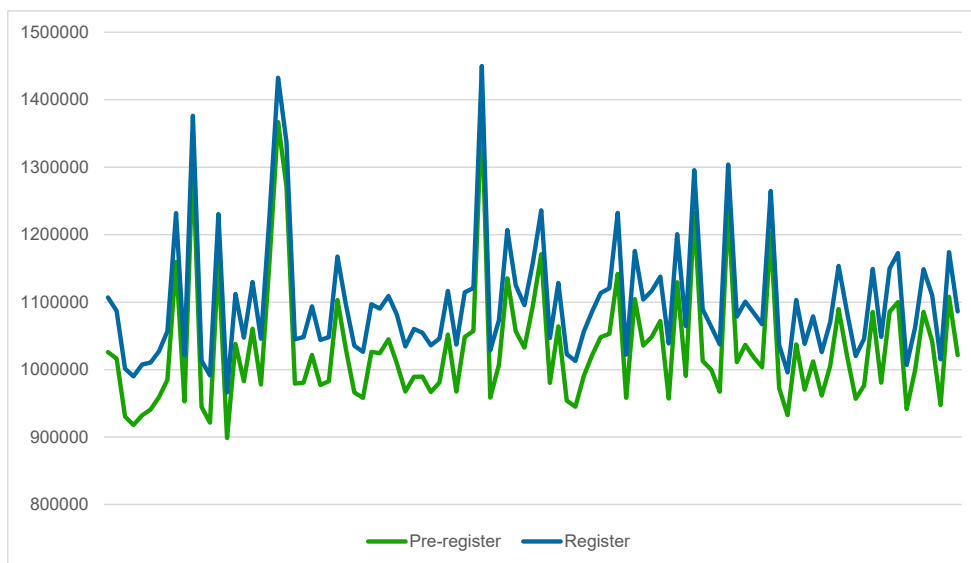


Figure 13. Time to register users with revocation validation enabled

Figure 14 shows a stacked line chart with the time to pre-authenticate and authenticate with revocation validation enabled. On average, it takes around 1.02 seconds to pre-register and register a user which also represents a drastic increase of time to process the request in comparison with the results obtained with the reference version.

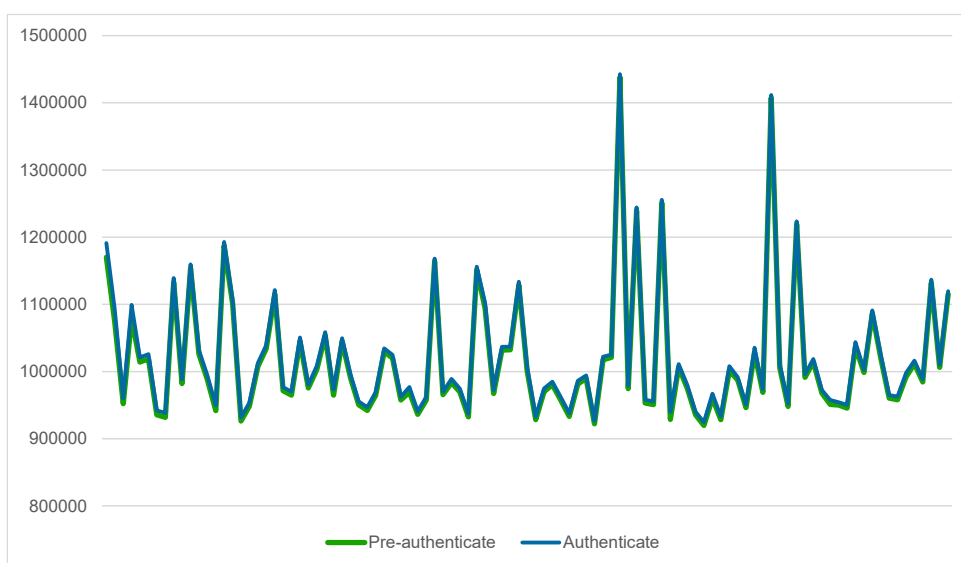


Figure 14. Time to authenticate users with revocation validation enabled

4.3.3. Test results with revocation validation and caching

Figure 15 shows a stacked line chart with the time to pre-register and register users with revocation validation and CRL caching enabled. This means that service downloads a CRL to check if the user's certificate is revoked and stores the CRL in cache for two minutes. Whenever a new CRL is required for validation, the service first checks if it is in the cache and it only tries to download the CRL again if it is missing. The chart shows that on average, it takes around 245 milliseconds to pre-register and register a user, nevertheless it also reveals that after caching all the required CRLs, the time it takes to process the request is well below 100 milliseconds.

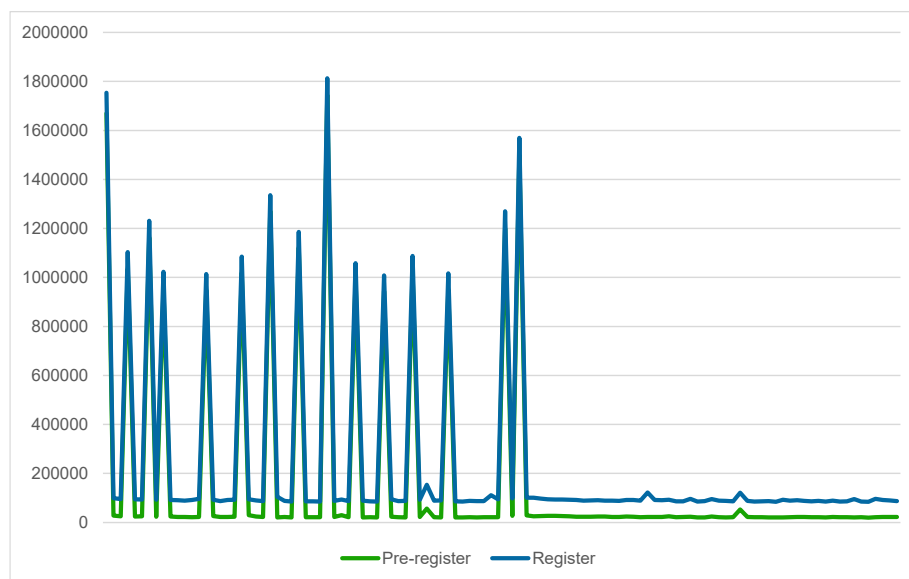


Figure 15. Time to register users with revocation validation and CRL caching enabled

Figure 16 depicts a stacked line chart with the time to pre-authenticate and authenticate with revocation validation and CRL caching enabled. On average, it takes around 67 milliseconds to complete the request. Although with less spikes than the chart in Figure 15, it also shows that there is a drastic increase in time to process the request whenever there is a cache miss.

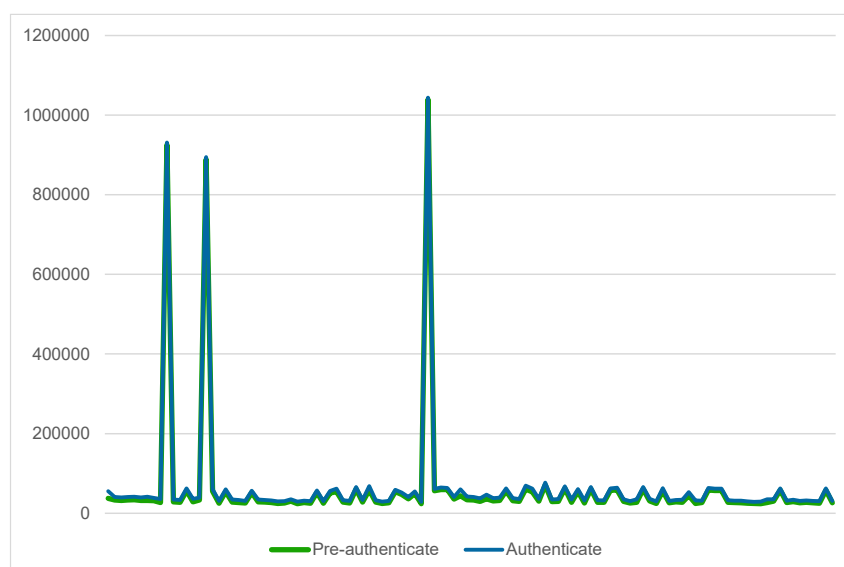
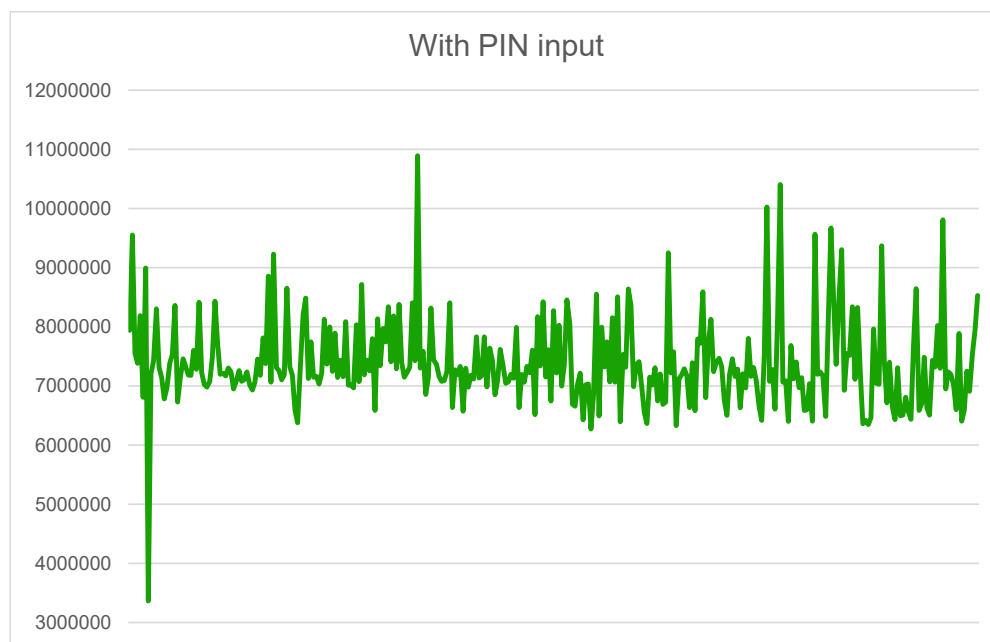


Figure 16. Time to authenticate users with revocation validation enabled

The test results we presented in this section show that the authentication service performs well when revocation validation is disabled, with response times similar or even better than our reference version. It also shows that running the service with revocation validation enabled and with CRL caching can be considered a good compromise between security and performance.

Finally, we also measured the time it takes to sign a transaction on the client side, with and without user's PIN input. The results are shown in Figure 17 which reveals that it takes, on average, 7.4 seconds to sign a transaction when PIN input is required, whereas without PIN it takes around 2 milliseconds. Besides the time user spends typing the PIN and press the 'Enter' key, the time the smart card takes to sign the transaction's digest must also be accounted for.

**Figure 17. Time to sign a transaction with PIN input**

The chart depicted in Figure 17 should be interpreted with some caution because it always depends on the user's ability to type the PIN correctly and expeditiously. Nevertheless, the obvious consequence of this requirement is that the overall time to completely process the transaction by the blockchain network increases dramatically, albeit without spending CPU cycles, because on the client-side the application is simply waiting for user input and on the server-side the transactions are processed asynchronously.

5. Conclusions

This study investigated the integration of the Portuguese Citizen's Card with Hyperledger Fabric (HLF) blockchain technology to enable secure authentication processes in enterprise blockchain environments. Through a comprehensive methodology involving literature review, technical analysis, and exploratory implementation, we addressed three primary research questions concerning the feasibility, implementation processes, and broader applicability of smart card-based authentication in blockchain systems.

Our investigation confirmed that it is technically feasible to authenticate and control access for end-users using digital authentication through the Portuguese Citizen's Card in Hyperledger Fabric environments. This feasibility is contingent upon two critical requirements: compatibility between the cryptographic algorithms used by the smart card X.509 certificates and HLF's transaction signature validation mechanisms (specifically ECDSA with curve P-256), and proper configuration of Organizational Unit attributes in certificate Distinguished Names to match HLF's supported roles. The recent adoption of ECDSA cryptography in Portuguese Citizen's Cards issued since June 2024, in compliance with EU Regulation 2019/1157, addresses the first requirement and enables seamless integration with modern blockchain systems.

We developed and validated comprehensive processes for both end-user registration and authentication through the Portuguese Citizen's Card in HLF networks. The registration process involves a two-step authentication mechanism where users provide certificate chains and digitally signed attribute documents using the Autenticação.Gov SDK. The authentication process similarly employs a two-step approach, utilizing Certificate Signing Requests and digital signatures to establish user identity within the Fabric CA framework. These processes leverage existing government-issued digital identity infrastructure while maintaining the security and access control requirements of permissioned blockchain networks.

The technical contributions of this work include the development of a custom Signer interface implementation that integrates smart card operations with HLF's Gateway Client API, enabling seamless transaction signing using Citizen's Card private keys.

5.1 Limitations and Practical Considerations

Despite the technical feasibility demonstrated in this research, several important limitations affect the practical deployment of smart card-based authentication in blockchain environments. The most significant constraint stems from HLF's transaction execution model, which requires multiple cryptographic signatures throughout the transaction lifecycle. End-users must provide their PIN at least once for read operations and twice for write operations: first to endorse the transaction and subsequently to submit the endorsed transaction to the network. Depending on the transaction submission approach – whether synchronous or asynchronous – a third signature may be required to verify the commit status of the transaction (Hyperledger, 2023).

This multi-signature requirement creates substantial usability challenges that limit the applicability of our proposed solution. For applications with minimal user interactions, such as electronic voting systems or infrequent credential verification scenarios, the authentication overhead remains acceptable. However, for applications requiring frequent blockchain interactions or real-time user engagement, the repeated PIN entry significantly degrades user experience and may discourage adoption.

These constraints highlight the tension between security and usability in blockchain-based authentication systems. While smart card integration provides enhanced security through hardware-

based private key protection and established government identity verification, the associated user experience challenges may limit practical deployment to specific use cases where security requirements outweigh convenience considerations.

5.2 Future Work

Future research should address these usability limitations through several potential approaches. Investigating session-based authentication mechanisms that reduce the frequency of PIN entry while maintaining security standards could significantly improve user experience. For instance, depending on the criticality of data, we could replace the authentication service with a complete frontend to the Hyperledger Fabric network, and all read operations would be carried out by the service itself. Only write operations would require the end-user to input the PIN to sign and submit transactions.

Additionally, exploring mobile-compatible authentication alternatives, such as integration with mobile secure elements or trusted execution environments, could extend the applicability of government-issued digital identity integration to mobile platforms.

The development of hybrid authentication models that combine smart card security with mobile convenience represents another promising research direction. Such approaches might investigate how emerging technologies like contactless authentication and biometric verification could complement existing smart card infrastructure.

Another topic to take into consideration for future studies concerns the planning and execution of a thorough threat model analysis which this paper currently lacks.

This research demonstrates the practical viability of integrating established government digital identity infrastructure with cutting-edge blockchain and decentralized identity technologies. While current limitations constrain immediate widespread deployment, the foundation established here provides a pathway for more accessible and secure blockchain-based applications that can evolve to leverage existing user authentication familiarity while maintaining the security and decentralization benefits of distributed ledger systems.

Acknowledgments

This work was financially supported by Project BlockchainPT – Decentralize Portugal with Blockchain Agenda, WP 2: Health and Wellbeing, 02/C05-i01.01/2022.PC644918095-00000033, funded by the Portuguese Recovery and Resilience Program (PPR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program.

References

- Agência para a Modernização Administrativa. (2025). *Manual do SDK – Middleware do Cartão de Cidadão*. https://amagovpt.github.io/docs.autenticacao.gov/manual_sdk.htm
- Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys and Tutorials*, 21(4), 3796–3838. <https://doi.org/10.1109/COMST.2019.2928178>

- Estonian Business and Innovation Agency. (2025). *KSI Blockchain - e-Estonia*. <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>
- European Parliament, & European Council. (2019, July 12). *Regulation (EU) 2019/1157*. <https://eur-lex.europa.eu/eli/reg/2019/1157/oj/eng>
- Fadele Ayotunde Alaba, Hakeem Adewale Sulaimon, Madu Ifeyinwa Marisa, & Owamoyo Najeem. (2023). Smart Contracts Security Application and Challenges: A Review. *Cloud Computing and Data Science*. <https://doi.org/10.37256/ccds.5120233271>
- George, J. T. (2022). Hyperledger Fabric. *Introducing Blockchain Applications*, 125–147. https://doi.org/10.1007/978-1-4842-7480-4_6
- Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: a literature review. *Journal of Management Analytics*, 7(3), 321–343. <https://doi.org/10.1080/23270012.2020.1801529;WGROU:STRING:PUBLICATION>
- Governo da República Portuguesa. (2024, June 11). *Novo Cartão de Cidadão a partir de 11 de junho*. <https://www.portugal.gov.pt/pt/gc24/comunicacao/noticia?i=novo-cartao-de-cidadao-a-partir-de-11-de-junho>
- Gupta, B. B., & Quamara, M. (2019). *Smart Card Security*. CRC Press. <https://doi.org/10.1201/9780429345593>
- Hope, J. (2019). What Is Blockchain and How Does It Work? *The Department Chair*, 29(4), 11–11. <https://doi.org/10.1002/DCH.30250>
- Hyperledger. (2023). *Architecture Reference - Hyperledger Fabric Documentation*. <https://hyperledger-fabric.readthedocs.io/en/release-2.5/architecture.html>
- Hyperledger. (2025). *Fabric Gateway - Hyperledger Fabric Docs*. <https://hyperledger-fabric.readthedocs.io/en/release-2.5/gateway.html>
- Kuperberg Michael and Kemper, S. and D. C. (2019). Blockchain Usage for Government-Issued Electronic IDs: A Survey. In J. Proper Henderik A. and Stirna (Ed.), *Advanced Information Systems Engineering Workshops* (pp. 155–167). Springer International Publishing.
- Legion of the Bouncy Castle Inc. (2025a). *Bouncy Castle CSharp - Pkcs10CertificationRequestDelaySigned source code*. <https://github.com/bcgjt/bc-csharp/blob/31a3d18e4b38c53f49d71d08ee3f83e22d939615/crypto/src/pkcs/Pkcs10CertificationRequestDelaySigned.cs>
- Legion of the Bouncy Castle Inc. (2025b). *Bouncy Castle open-source cryptographic APIs*. <https://www.bouncycastle.org/>
- Mansour, M., Salama, M., Helmi, H., & Mursi, M. (2024). A Survey on Blockchain in E-Government Services: Status and Challenges. *ArXiv Preprint ArXiv:2402.02483*.
- Parsovs, A. (2020). Solving the Estonian ID Card Crisis: the Legal Issues. In Amanda Hughes, Fiona McNeill, & Christopher W. Zobel (Eds.), *ISCRAM 2020 Conference Proceedings* (pp. 459–471). Virginia Tech.
- Santhosh, M. G., & Reshmi, T. (2023). Enhancing PKI Security in Hyperledger Fabric with an Indigenous Certificate Authority. *2023 IEEE International Conference on Public Key Infrastructure and Its Applications, PKIA 2023 - Proceedings*. <https://doi.org/10.1109/PKIA58446.2023.10262412>
- Somma, A., De Benedictis, A., Esposito, C., & Mazzocca, N. (2024). The convergence of Digital Twins and Distributed Ledger Technologies: A systematic literature review and an architectural proposal. *Journal of Network and Computer Applications*, 225, 103857. <https://doi.org/10.1016/j.jnca.2024.103857>
- Tanzim Nawar, T., Khan, F. J., Akter, J., Authro, A. S., Ullah, S. M. W., & Hossain, M. N. (2023). A Design for Managing Smart National Identity Cards Securely through the Utilization of Blockchain Technology. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4638825>

TDGRA. (2022). *Emirates Blockchain Strategy 2021*. <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-until-2021/emirates-blockchain-strategy-2021>

TDGRA. (2024a). *Emirates ID* . <https://u.ae/en/information-and-services/visa-and-emirates-id/emirates-id>

TDGRA. (2024b). *The UAE Pass*. <https://u.ae/en/about-the-uae/digital-uae/digital-transformation/platforms-and-apps/the-uae-pass-app>

Towards a Generic NFT-Driven Digital Twin Simulation Platform: A Systematic Literature Review

Bernardo J. R. Figueiredo
VOID Software S.A., Portugal
bernardo.figueiredo@voidsoftware.com
0000-0003-3577-5108

Marco P. M. Ferreira
VOID Software S.A., Portugal
marco.ferreira@voidsoftware.com
0000-0003-2397-1697

João Matos
VOID Software S.A., Portugal
joao.matos@voidsoftware.com

Marco P. J. P. Cova
VOID Software S.A., Portugal
marco.cova@voidsoftware.com
0009-0002-7511-8065

Received: 17 June 2025

Accepted: 24 November 2025

Abstract

A new approach to asset management and traceability emerges upon the integration of Non-Fungible Tokens (NFTs) and Digital Twin (DT) technology. While NFTs are widely used in digital art and gaming, their potential for securing real-world assets in DT simulations remains under-explored. A generic NFT-driven DT simulation platform could transform asset management by enhancing traceability, optimizing operations, and fostering sustainability within and across industries. In livestock management, DTs can model individual animals in real time, capturing data on health and growth. Linking this data to NFTs ensures ownership and provenance, improving traceability and accountability. Similarly, in manufacturing, DTs can identify inefficiencies, reducing waste and energy use. It is pressing to improve decision-making and operational efficiencies throughout distinct contexts. A Systematic Literature Review (SLR) was conducted following PRISMA. The goal was to build a solid, unbiased foundation for our research, contribute lasting value to the community, and identify where our work can make the most impact. From an initial set of 114 papers, the authors screened and classified the most relevant. This led to a final selection of 8 papers for full-text reading and in-depth analysis. They are presented in detail and compared in order to depict the current state of the art in the field. Results reveal a significant gap concerning the topic, particularly highlighting the absence of simulation environments that align with the previous proposal presented by the authors: a comprehensive NFT-driven and DT simulation platform that transforms NFT-based asset management from static ownership records to dynamic, provides simulation operational tools, enables real-time monitoring, predictive maintenance, and performance optimization for real-world assets.

Keywords *Blockchain, Non-Fungible Token (NFT), Digital Twins (DT), Traceability, Simulator, Generic*

1. Introduction

The emergence of Non-Fungible Tokens (NFTs) and their integration into Digital Twin (DT) simulation platforms have the potential to revolutionize asset management across various industries. By leveraging the unique properties of NFTs, such platforms can enhance traceability, optimize operations, and foster sustainability. This systematic literature review aims to explore the existing research surrounding NFT-driven DT simulation platforms and their implications for asset management, with a particular focus on how these technologies can transform industry practices.

NFTs serve as digital certificates of ownership, providing a tamper-proof record of an asset's history, which is critical for fostering transparency and traceability in asset management (Caldera et al., 2021). Using blockchain technology in this context aids in establishing the provenance of assets and facilitates real-time monitoring and management, which are vital for enhancing the operational efficiency of asset utilization (Wang et al., 2024). Moreover, frameworks for risk management that incorporate these technologies are increasingly recognized for their ability to mitigate risks associated with asset degradation and lifecycle management (Santosa et al., 2024).

Digital Twins, being virtual representations of physical assets, can significantly improve the management of lifecycle processes by simulating different operational scenarios. Integrating NFT technology with DT frameworks enhances simulations through a detailed lineage of asset data, thus supporting smarter decision-making processes (Papic & Cerovšek, 2019). For instance, the convergence of Building Information Modeling (BIM) with Digital Twins has been documented to improve infrastructure asset management, highlighting how these methodologies can be synthesized to yield better outcomes in various sectors (Garramone et al., 2020).

The challenges of managing physical assets in a rapidly evolving technological landscape need new solutions that promote smart asset management. The strategic integration of NFTs within DT platforms can synchronize asset management practices across diverse industries, leading to improved resource allocation and sustainability. Recent literature indicates that using advanced digital infrastructure, such as an NFT-driven DT simulation platform, can streamline operations and enhance the effectiveness of decision-making frameworks in asset management (Hirschowitz Nel & Jooste, 2016).

Systematic literature reviews (SLRs) play a crucial role in synthesizing existing research and providing a comprehensive overview of a particular field of study. SLRs enable researchers to uncover patterns, identify gaps, and recommend future research directions. This structured approach enhances the reliability of conclusions drawn from diverse sets of literature.

For instance, the systematic review by Semeraro et al. focused on the digital twin paradigm, examining key features and challenges associated with their implementation. The study used a rigorous methodological framework, integrating findings from numerous sources to establish a coherent understanding of current digital twin concepts and applications in various sectors, including manufacturing and healthcare (Semeraro et al., 2021). Similarly, the review conducted by Nunes et al. on NFTs in healthcare elucidates how NFTs can serve as digital representations of healthcare products, ensuring ownership and provenance across the supply chain (Corte-Real et al., 2022). Both studies exemplify how SLRs synthesize existing research, underscoring the potential of NFTs and DTs within their corresponding domains.

Moreover, the SLR process is particularly valuable in fields characterized by rapid technological advancements. For example, in their review, Coorey et al. highlighted how digital twins can significantly impact precision medicine by enabling patient-specific treatment pathways through continuous monitoring and data integration (Coorey et al., 2022). By systematically collecting and

analyzing literature, this review facilitates the identification of emerging trends, benefits, and barriers related to digital twin technologies and their applications.

However, despite the growing body of literature on NFTs and digital twins, there is a notable gap of systematic literature reviews specifically addressing Generic NFT-Driven Digital Twin Simulations. This gap indicates a critical opportunity for researchers to explore how NFTs can enhance digital twin functionality across various sectors. By conducting a dedicated SLR on this topic, researchers could effectively see the intersections between NFTs and digital twins, thus creating innovative solutions that leverage the strengths of both technologies.

As industries aim for more sustainable and efficient asset management strategies, the integration of NFT-driven DT simulation platforms offers a promising avenue. We aim to continue to develop a simulation platform and we need to uncover what is already being done in the world related to this. Specifically, by assigning a unique, immutable NFT to each digital twin, the asset's lifecycle can be securely tracked and verified. This provenance data improves trust among stakeholders and enables more informed, data-driven decisions, reducing waste and extending asset lifespans. It also supports predictive maintenance and resource optimisation by linking real-time simulation outputs to automated workflows, ensuring interventions occur only when necessary. Furthermore, NFT-backed digital twins enhance interoperability. Smart contracts embedded in NFTs can even automate transactions and maintenance processes.

This systematic literature review will critically assess current research to identify current work, technologies used, and future directions in the application of these technologies to foster an evolved understanding of asset management in both a theoretical and practical context. The authors have already proposed the creation of a generic simulation platform NFT-driven and digital twin (DT) simulation platform (Ferreira et al., 2025; Figueiredo et al., 2025). The goal for the SLR is to find related and relevant work that could be used as guidance, comparison and create benchmarks with other projects that integrate these technologies with simulation tools, enable real-time monitoring, support predictive maintenance, and facilitate performance optimization for real-world assets.

2. Methods

We conducted a systematic review that aims to identify and synthesize relevant studies about the connection of Non-Fungible Tokens (NFT) with Digital Twins (DT) and the usage of a simulation environment to replicate real world scenarios where they are used. While conducting the systematic literature review (SLR), the PRISMA methodology was adopted to ensure a structured, transparent, and reproducible process (Preferred Reporting Items for Systematic Reviews and Meta-Analyses and (Page et al., 2021). The review followed the core PRISMA stages of identification, screening, and inclusion, which allowed the collection of relevant studies, the elimination of duplicates and irrelevant records, and the final selection of publications that met the predefined criteria. The eligibility stage, often considered a distinct step in PRISMA, was not explicitly separated in this review. Instead, its function, the assessment of full-text articles against inclusion criteria, was integrated into the

screening and inclusion phases. Likewise, the data extraction and synthesis steps, while essential for analysis, fall outside the scope of the PRISMA flow itself and were treated as part of the subsequent review methodology, to streamline the process and reduce redundancy. This adaptation maintains methodological rigour while customizing the process to the specific goals and scope of this study. The workflow is described in Figure 1 (Haddaway et al., 2022).

After conducting some initial research that enabled some pre-adjustments to the conduction of the SLR we selected the keywords (“NFT” OR “Non-Fungible Token”) AND “Digital Twin*” AND (“simulator” OR “simulation environment”). These keywords were then used in advanced searches within trusted sources and scientific databases: IEEE Xplore, ACM Digital Library and Scopus. The selection of IEEE Xplore, ACM Digital Library, and Scopus as primary databases is justified by their broad coverage, scientific quality, and relevance to the domains under analysis. IEEE Xplore and ACM Digital Library are the most authoritative sources for peer-reviewed publications in computer science, software engineering, and emerging digital technologies, ensuring access to high-quality and domain-specific research. Scopus complements these with its multidisciplinary scope and extensive indexing of journals, conference proceedings, and book chapters, thus reducing the risk of omitting relevant studies. Together, these databases provide a balanced combination of depth, rigor, and breadth, making them sufficient and appropriate for systematic data collection.

The cutout date was June 1st, 2025. Initial results revealed the lack of work that associated NFTs, Digital Twins and simulators, since some of the sources provided 0 results to the search. Due to this constrain we chose to exclude (“simulator” OR “simulation environment”) from 2 of the 3 libraries, keeping the entire search terms for ACM Digital Library. This allowed us to collect results that allow us to understand the work that is currently being conducted with NFTs and Digital Twins and include additional references of simulation environments.

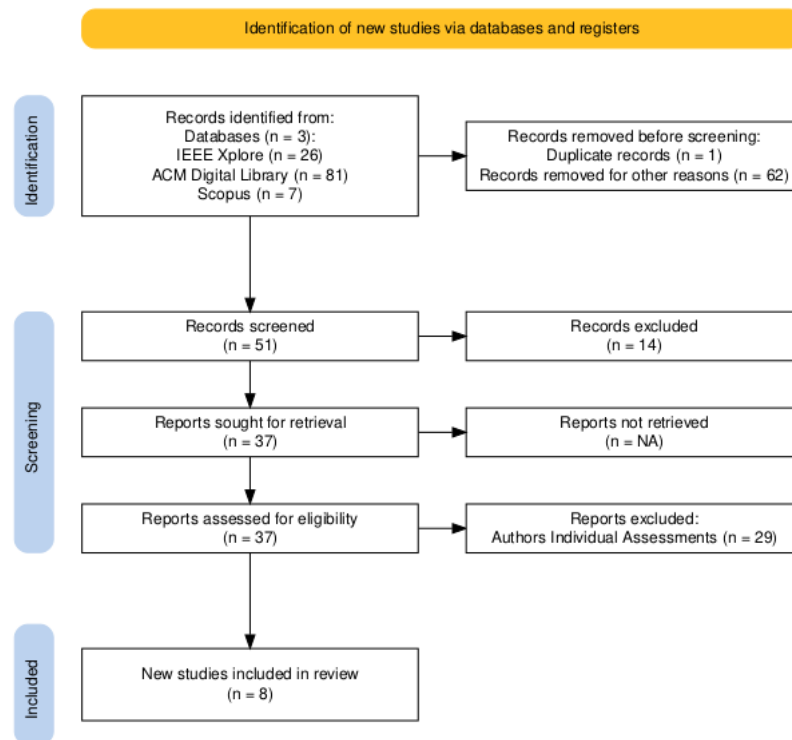


Figure 1. PRISMA Flow Diagram for the SLR

From the first 114 overall results of the searches conducted, we validated that the papers were in English, were peer-reviewed articles or conference papers, and their full-text was available. From the 114, one duplicate was found and 62 proceedings' prefaces that included sparse references to the topics were excluded. This left us with 51 paper references that were used for the initial screening. Both the title and the abstract of the papers were filtered to explicitly find the words ("NFT" OR "Non-Fungible Token") AND "Digital Twin". All of the papers that failed to present the search terms were excluded (n=14).

The remaining 37 papers were sought for retrieval and assessed for eligibility by the authors that used a scale of "-1: off context; 0: neutral; 1: advisable to read and 2: must read" points to classify each one of them for relevance, based on the title and abstract. Appendix A provides a full list of these 37 papers.

Following the authors' individual assessments, we reached consensus on the exclusion of 29 papers due to the lack of relevance: at least one negative or neutral classification (-1 or 0 points); overall classification of less than 4 points out of 8; and, no single classification of 2 points by, at least, one of the authors. The final selection of papers led to the choice of 8 papers that are presented and compared in the Results and Discussion section.

3. Results and Discussion

Selected papers are chronologically distributed across the period from 2022 to 2024, with two studies published in 2022, four in 2023, and the remaining two in 2024. We present them, first, summarized, listed by Authors, in alphabetical order and, later, compare them.

Cao et al. (Cao et al., 2022) presents BDTwins, a comprehensive framework integrating blockchain with digital twin technology (DT) to enhance lifecycle management. It recognizes the increasing complexity and high demand for data-driven strategies in industrial settings, particularly under Industry 4.0, where cloud computing, artificial intelligence (AI), and the Internet of Things (IoT) play relevant roles in smart manufacturing. The authors assert that while the concept of digital twins significantly transforms processes throughout the product lifecycle, from design to operational control, existing research predominantly focuses on earlier stages, often neglecting data processing post-retirement. The framework emphasizes the utility of Non-Fungible Tokens (NFTs) within a seven-dimensional model, ensuring secure data sharing and management throughout the lifecycle of digital assets. Critical to its design is the acknowledgment that stakeholders, often from diverse departments, might not inherently trust one another; thus, the framework incorporates mechanisms for permission control while also recognizing the need for environmental factors (such as IP address and network conditions) to be considered to mitigate security and privacy.

Moreover, the paper underscores the foundational role of data in DT implementations, describing DT as a representation that evolves throughout the asset's lifecycle, ensuring that it accurately reflects current operational states and facilitates better decision-making. Despite the clear advantages presented by the integration of blockchain technology, primarily its decentralization and tamper-proof characteristics, the literature review indicates that prior work has largely overlooked the complexities inherent in post-retirement data management within the digital twin lifecycle, thereby providing a definitive rationale for the authors' focus on this critical aspect.

Elmay et al. (Elmay et al., 2023) investigates the integration of Non-Fungible Tokens (NFTs) and blockchain technologies to enhance the security and management of Digital Twins (DTs) in the maritime shipping sector. The authors recognize the critical need for reliable data traceability and management in shipping container logistics, an area that typically involves numerous stakeholders and complex processes. Traditional methods of managing DTs have often relied on a centralized entity, which may lead to potential data manipulation or tampering, thereby destroying trust among users. The paper addresses these challenges by proposing a decentralized framework that leverages NFTs to tokenize the shipping container DTs and their relevant data. This tokenization allows for the creation of an immutable and transparent ledger using blockchain technology, specifically Ethereum smart contracts.

The authors articulate a framework comprising five modules, designed to facilitate the integration and optimization of DTs throughout the supply chain. These modules encompass the physical supply chain, interface, simulation, optimization, and reporting, thus enabling improved decision-making processes. By implementing such a framework, the authors envision a significant reduction in mistrust

and an increase in collaboration between various stakeholders, thereby fostering a more efficient logistics environment.

Gebreab et al. (Gebreab et al., 2022) presents an innovative approach to overcoming traceability issues in the healthcare sector by leveraging non-fungible tokens (NFTs). It addresses significant challenges posed by counterfeit medical devices, which continue to jeopardize patient safety. The authors emphasize the complex architecture of the proposed system, using NFTs for tracking and managing ownership of medical devices throughout their lifecycle, from production to sale. This is particularly critical given the rising incidence of counterfeit devices that amplify risks within the healthcare supply. The proposed system relies on smart contracts and decentralized storage solutions, such as IPFS (InterPlanetary File System), to record and manage essential documentation about the devices, including certifications, manufacturing dates, and warranty information. This blockchain-enabled approach ensures tamper-proof maintenance of records, thereby enhancing transparency and accountability within the supply chain. Furthermore, the implementation of QR codes and PUF-enabled RFID tags contributes to the validation of product authenticity at a hardware level, which is crucial for post-market surveillance, particularly in cases of device recalls.

The study outlines that unlike other blockchain solutions that provide basic traceability features, the NFT-based system allows for enriched data representation, enabling the integration of multiple product attributes along with a unique digital identification. While the paper presents a conceptual framework and architecture for the NFT solution, it identifies a gap in the technical implementation details, which could delay practical deployment.

Gebreab et al. (Gebreab et al., 2024) investigates the intersection of non-fungible tokens (NFTs), digital twins (DTs), and the metaverse, proposing a novel framework that leverages these technologies to enhance user experiences and facilitate the decentralized management of digital assets. NFTs are positioned as essential elements that offer a secure and verifiable link between the physical and digital realms, allowing the integration of digital artifacts within the metaverse. The uniqueness and traceability of NFTs contribute significantly to ensuring authenticity in digital interactions, which has made them relevant for applications beyond mere collectibles, including the representation and monetization of assets in diverse fields such as healthcare and manufacturing. The paper discusses the potential for NFTs not only to represent ownership but also to facilitate version tracking and real-time updates through dynamic NFTs, which automatically adjust to changes in their corresponding physical entities. This integration ensures that digital representations maintain alignment with their physical counterparts, enhancing the user experience with accurate depictions of physical changes in the metaverse.

Moreover, the paper identifies existing research gaps, particularly in the secure and efficient integration of DTs into the metaverse ecosystem. While studies have outlined interoperability necessities and explored decentralized service models within the metaverse, they often overlook the practical implementation of secure content exchanges that use blockchain protocols in conjunction with NFTs. As such, this work offers valuable solutions by proposing a structured approach that

includes leveraging smart contracts for operations and decentralized storage solutions to uphold data integrity and availability for NFTs.

Gebreab et al. (Gebreab et al., 2023) focuses on using blockchain technology, specifically through the implementation of Non-Fungible Tokens (NFTs), to enhance the traceability and certification processes for refurbished medical devices. The motivation behind this research stems from the increasing reliance on refurbished medical devices as a cost-effective and sustainable option in healthcare settings, particularly because these devices can help mitigate high medical costs while maintaining quality and safety standards. However, the reuse of such devices poses significant challenges, notably the risks associated with quality assurance and potential fraud, such as counterfeiting.

Authors propose a novel framework that leverages the Ethereum blockchain to create a decentralized, immutable record of the refurbishment lifecycle of medical devices. Dynamic composable NFTs serve as digital counterparts to physical devices, maintaining an auditable history of each item's status and any alterations made during the refurbishment process. This ensures that stakeholders can verify authenticity and compliance with safety standards, contributing to the mitigation of concerns regarding the quality of refurbished devices. This solution incorporates smart contracts to automate various operations and ensure transactional integrity, which are essential for maintaining trust among users. And also, reputation-based oracles and InterPlanetary File System (IPFS) for efficient data management. The integration of these technologies enhances the visibility of the supply chain while aiming to establish a secure method for documenting and accessing medical data that preserves individual privacy.

Hasan et al. (Hasan et al., 2023) examines the integration of digital twins (DTs) with non-fungible tokens (NFTs) within the context of smart manufacturing. A digital twin is understood as a precise digital replica of a physical asset that facilitates effective management, monitoring, and control of its real-world counterpart. The evolution of digital-driven manufacturing, propelled by advancements in the Internet of Things (IoT), artificial intelligence (AI), and big data analytics, highlights the increasing reliance on digital technologies in modern manufacturing processes. The uniqueness of NFTs, characterized by their blockchain foundation, provides verification of ownership and authenticity, which is essential when tracking the ownership and lifecycle of DTs. The paper argues that the combination of NFTs and DTs enhances the traceability and accountability of ownership as DTs are created, traded, and transferred among various stakeholders. The authors propose an approach where NFTs represent DTs and their subcomponents, allowing for a dynamic ownership model adaptable to the life cycles of physical assets.

The authors also highlight the potential of smart contracts, enabled by programming languages like Solidity, which allow for customizable interactions tailored to specific marketplace needs. Maintaining a transparent ledger through blockchain technology strengthens trust among stakeholders, fostering an environment with truthful information sharing and cooperation. Moreover, the concept of composability is discussed, indicating that DTs should be designed to accommodate ongoing changes to their physical counterparts over time. This flexibility facilitates the trading of DT

subcomponents and creates a framework for multiple ownership scenarios throughout an asset's lifecycle.

Saeed et al. (Saeed et al., 2023) introduces an innovative gaming-based education system aimed at enhancing road safety awareness among children within the context of smart cities. Leveraging immersive technologies such as augmented reality (AR), virtual reality (VR), artificial intelligence (AI), and the Internet of Things (IoT), the system offers interactive simulations that allow children to engage with realistic road scenarios. Authors detail how the integration of AR into this educational framework allows children to visualize virtual traffic signs and signals overlaid onto their real environment, augmenting their practical learning experiences in familiar locales. Furthermore, VR technology immerses them in a controlled yet realistic setting where they can practice critical skills such as safely crossing streets, adhering to traffic signals, and making sound judgments regarding vehicle speeds. The use of digital twins for simulating real-time situations enhances the educational experience, making it both engaging and informative.

Although the work proposes the integration of several technologies, that include DT and a simulation environment, it does not mention the integration of NFTs or any other blockchain related technology.

Sai et al. (Sai et al., 2024) presents a comprehensive exploration of using digital twin technology in the management and support of patients suffering from chronic diseases. Through the development of a novel AI-based and IoT-supported digital twin framework, the authors propose a solution that addresses several challenges in chronic disease management, including patient monitoring, nutrition tracking, and personalized treatment recommendations. At its core, the digital twin serves as a virtual representation of the patient, continuously updated with real-time data from various IoT sensors. This ensures that the model reflects the patient's real-world health status and allows for advanced analysis and optimization of treatment strategies. The proposed digital twin platform incorporates multiple machine learning models to enhance functionality. For instance, one model is dedicated to diet analysis, which monitors patients' food intake and issues alerts regarding unhealthy consumption while offering tailored dietary recommendations. Further, the framework integrates algorithms for drug recommendation and disease stage detection, ensuring that interventions remain personalized and relevant.

This work integrates a NFT-based platform that servers two essential functions: securing medical data storage and health information exchange. The ultimate goal of the digital twin system not only revolves around enhancing patient health outcomes but also motivating patient engagement through innovative approaches.

Table 1 is a comparison table that summarizes the attributes of these papers regarding NFTs, Digital Twins (DTs) and simulation environments (simulator).

Table 1 – Selected Studies Comparison

ID	Use Case	Traceability	Technology	Simulation Env.
(Cao et al., 2022)	generic - management of digital twins throughout their lifecycle	yes	Ethereum Solidity Smart Contracts Cumulus Encrypted Storage System (CESS)	NA
(Elmay et al., 2023)	shipping containers - traceability and management	yes	Ethereum Solidity Smart Contracts Azure Digital Twins Interplanetary File System (IPFS)	NA
(Gebreab et al., 2022)	medical devices - traceability and ownership management	yes	Ethereum Solidity Smart Contracts Interplanetary File System (IPFS)	NA
(Gebreab et al., 2024)	cross-metaverse interoperability and monetization for DT and digital artifacts	yes	Ethereum Polygon Solidity Smart Contracts Interplanetary File System (IPFS) or Ceramic Network or Swarm Oracle (timer)	NA
(Gebreab et al., 2023)	refurbished medical devices - management	yes	Ethereum Solidity Smart Contracts Interplanetary File System (IPFS) or Ceramic Network or Swarm	NA
(Hasan et al., 2023)	generic - management of digital twin ownership and proof of delivery of physical asset	yes	Ethereum Solidity Smart Contracts Interplanetary File System (IPFS) or FileCoin or Swarm	NA
(Saeed et al., 2023)	metaverse - gaming-based education system about road safety	track players	Unity – simulator NFTs – rewards (NA)	yes - Unity
(Sai et al., 2024)	chronic disease patients - monitoring and assisting	track daily activities	Ethereum Solidity Smart Contracts Interplanetary File System (IPFS)	yes

In examining these publications, four aspects emerge: use cases; the presence of traceability as a feature; specific NFT (blockchain), DT and simulation technologies employed; and, the inclusion of a simulator or simulation environment within the respective studies.

3.1. Use Cases

Each paper focuses on distinct domains. Gebreab et al. (Gebreab et al., 2022, 2023) address the healthcare domain, specifically for tracking and managing medical devices and refurbished medical devices (DT). Elmay et al. (Elmay et al., 2023) apply digital twins (DTs) for shipping containers, leveraging NFTs for managing container data and ensuring transparency. In contrast, the work by Sai et al. (Sai et al., 2024) introduces an AI-empowered monitoring framework for chronic disease patients, linking health management with blockchain technology through NFTs that are used to secure

patients information and transactions. Saeed et al. (Saeed et al., 2023) presents a game-based education framework for road safety that uses NFTs as a reward system.

Although these varied applications showcase the versatility of NFTs in enhancing traceability and ownership across different industries, three studies provide generic approaches that are meant to be used for any use case. Hasan et al. (Hasan et al., 2023) delve into ownership management of digital twins and asset delivery proof, upon delivery of the physical asset. Gebreab et al. (Gebreab et al., 2024) introduce a cross-metaverse platform that deals with interoperability within blockchain infrastructures and transfer ownership between distinct infrastructures. Finally, Cao et al. (Cao et al., 2022) presents BDTwins, a generic framework used to manage digital twins throughout their lifecycle.

3.2. Traceability

All the selected papers mention a form of traceability in their proposed solution. Only six of them use the inherent traceability characteristic of the blockchain where the NFT is implemented to keep track of the DT that maps a real-world physical asset.

Both Saeed et al. (Saeed et al., 2023) and Sai et al. (Sai et al., 2024) report to have tracking features: for the daily activities of patients with chronic conditions; and, for the players of the educational game for road safety. However, none of these features is implemented using a blockchain structure. NFTs in both cases are used to (1) secure patient data and transactions (partially using the blockchain infrastructure) and (2) a rewards system.

3.3. Technology

These studies primarily focus on Ethereum as the base blockchain infrastructure due to its robust support for smart contracts, developed in Solidity. Thus, NFTs are mainly developed using the standard ERC-721, deployed to Ethereum testnets, but with no explicit referral to deployed solutions in the actual Ethereum public network. Additionally, Gebreab et al. (Gebreab et al., 2024) also presents Polygon, a Layer 2 infrastructure that is used for the interoperability assessment they conduct – transfer NFTs from Ethereum to Polygon. Only Saeed et al. (Saeed et al., 2023) do not disclose the infrastructure that supports their NFT reward system.

Regarding the off-chain storage of information, mainly used for storing the metadata for the DT, most of the studies report usage of the Interplanetary File System (IPFS). Some alternatives to distributed and decentralized storage such as Cumulus Encrypted Storage System (CESS), Ceramic Network, Swarm, FileCoin are also presented in some studies (Cao et al., 2022; Gebreab et al., 2022, 2023, 2024).

Only Elmay et al. (Elmay et al., 2023) mention Azure Digital Twins as the specific technology used to manage, create and modify the digital twins. And, only Saeed et al. (Saeed et al., 2023) mention Unity as the simulation environment that supports their game-educational platform.

3.4. Simulation Environment

There is a noticeable gap in explicitly stated simulation environments within these papers. While all papers describe architectural implementation and testing of their frameworks, none sufficiently discuss simulation environments by name or detail their use in demonstrating the operation of blockchain solutions, including NFTs and smart contracts. The absence of this information indicates a potential area for future exploration in ensuring simulated outcomes can be derived before real-world implementations.

In summary, the studies demonstrate a rich landscape of innovative applications using blockchain technologies and NFTs, primarily within the Ethereum ecosystem. They emphasize automated systems through smart contracts while lacking attention to the use of simulation environments, highlighting a unique research opportunity for further development, as the authors already proposed (Ferreira et al., 2025; Figueiredo et al., 2025).

4. Conclusions and Future Work

The results reveal a significant gap concerning the topic, particularly highlighting the absence of simulation environments that align with the previous proposal presented by the authors: a comprehensive NFT-driven and digital twin (DT) simulation platform that transforms NFT-based asset management from static ownership records into a dynamic framework. Such a platform would integrate simulation tools, enable real-time monitoring, support predictive maintenance, and facilitate performance optimization for real-world assets.

Although the present systematic literature review identified only eight studies that satisfied the inclusion criteria, this limited number should not be interpreted as a methodological shortcoming but rather as an indicator of the current state of research in this area. The small corpus of relevant studies reflects a clear and significant gap of literature directly addressing the topic, suggesting that this is still an emerging and underexplored field.

Despite growing interest in NFTs for verifiable ownership and provenance, there is an absence of integrated simulation environments that leverage NFTs and DTs. This highlights the need for continued research and development of platforms that assign a unique, immutable NFT to each digital twin, enabling secure lifecycle tracking and verification. Such capabilities would strengthen stakeholder trust, support informed, data-driven decision-making, and contribute directly to reducing waste.

Moreover, the results show that existing solutions rarely exploit the potential of linking real-time simulation outputs to automated workflows, a crucial step for enabling predictive maintenance and resource optimisation. The limited integration of smart contracts and automation further constrains the transition from static ownership records to dynamic, self-managed asset ecosystems. Addressing these gaps will require moving beyond simple representation toward platforms where NFTs act as active gateways into interoperable digital ecosystems.

As future work, we aim to advance the conceptual architecture and further developing the proof-of-concept platform proposed in earlier stages. This platform integrates NFTs that are linked to real-world physical assets, mapped to Digital Twins, and with real-time simulation capabilities. This includes designing standardized metadata structures, defining interoperability layers between NFT registries and simulation engines, and evaluating performance in industrial case studies. Moreover, research will also focus on trust and governance mechanisms, ensuring data integrity, security and access control across decentralized environments. Through these steps, we intend to bridge the existing gap and provide a foundational contribution toward operationalizing NFT-enhanced digital twins.

Acknowledgments

This work was financially supported by Project Blockchain.PT – Decentralize Portugal with Blockchain Agenda, (Project no 51), WP 1: Agriculture and Agro-food, Call no 02/C05-i01.01/2022, funded by the Portuguese Recovery and Resilience Program (PPR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program.

References

- Caldera, S., Mostafa, S., Desha, C., & Mohamed, S. (2021). Exploring the Role of Digital Infrastructure Asset Management Tools for Resilient Linear Infrastructure Outcomes in Cities and Towns: A Systematic Literature Review. *Sustainability*. <https://doi.org/10.3390/su132111965>
- Cao, X., Li, X., Xiao, Y., Yao, Y., Tan, S., & Wang, P. (2022). BDTwins: Blockchain-based Digital Twins Lifecycle Management. *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, 2003–2010. <https://doi.org/10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00290>
- Coorey, G., Figtree, G. A., Fletcher, D. F., Snelson, V. J., Vernon, S. T., Winlaw, D., Grieve, S. M., McEwan, A., Yang, J. Y. H., Qian, P., O'Brien, K., Orchard, J., Kim, J., Patel, S., & Redfern, J. (2022). The health digital twin to tackle cardiovascular disease—a review of an emerging interdisciplinary field. *Npj Digital Medicine*, 5(1), 126. <https://doi.org/10.1038/s41746-022-00640-7>
- Corte-Real, A., Nunes, T., Santos, C., & Rupino da Cunha, P. (2022). Blockchain technology and universal health coverage: Health data space in global migration. *Journal of Forensic and Legal Medicine*, 89. <https://doi.org/10.1016/j.jflm.2022.102370>
- Elmay, F. K., Madine, M., Salah, K., & Jayaraman, R. (2023). NFTs for Trusted Traceability and Management of Digital Twins for Shipping Containers. *2023 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops)*, 433–438. <https://doi.org/10.1109/PerComWorkshops56833.2023.10150331>
- Ferreira, M. P. M., Figueiredo, B. J. R., Santos, A., Matos, J., & Cova, M. (2025). *Digital Twin Traceability with DLT: Towards a Multi-Context and Universal Platform*. <https://doi.org/10.36227/techrxiv.174361162.22972539/v1>
- Figueiredo, B. J. R., Ferreira, M. P. M., Matos, J., & Cova, M. (2025). *Towards a Generic NFT-Driven Digital Twin Simulation Platform*. c. <https://doi.org/978-989-9253-09-4>
- Garramone, M., Moretti, N., Scaioni, M., Ellul, C., Cecconi, F. R., & Dejacco, M. C. (2020). Bim and Gis Integration for Infrastructure Asset Management: A Bibliometric Analysis. *Isprs Annals of the*

Photogrammetry Remote Sensing and Spatial Information Sciences.
<https://doi.org/10.5194/isprs-annals-vi-4-w1-2020-77-2020>

- Gebreab, S. A., Hasan, H. R., Salah, K., & Jayaraman, R. (2022). NFT-Based Traceability and Ownership Management of Medical Devices. *IEEE Access*, 10, 126394–126411. <https://doi.org/10.1109/ACCESS.2022.3226128>
- Gebreab, S. A., Musamih, A., Hasan, H. R., Salah, K., Jayaraman, R., Al Hammadi, Y., & Omar, M. (2024). NFTs for accessing, monetizing, and teleporting digital twins and digital artifacts in the metaverse. *Comput. Commun.*, 228(C). <https://doi.org/10.1016/j.comcom.2024.107965>
- Gebreab, S. A., Salah, K., Jayaraman, R., & Zemerly, J. (2023). Trusted Traceability and Certification of Refurbished Medical Devices Using Dynamic Composable NFTs. *IEEE Access*, 11, 30373–30389. <https://doi.org/10.1109/ACCESS.2023.3261555>
- Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. *Campbell Systematic Reviews*, 18(2), e1230. <https://doi.org/https://doi.org/10.1002/cl2.1230>
- Hasan, H. R., Madine, M., Yaqoob, I., Salah, K., Jayaraman, R., & Boscovic, D. (2023). Using NFTs for ownership management of digital twins and for proof of delivery of their physical assets. *Future Generation Computer Systems*, 146, 1–17. <https://doi.org/10.1016/j.future.2023.03.047>
- Hirschowitz Nel, C. B., & Jooste, W. (2016). A Technologically-Driven Asset Management Approach to Managing Physical Assets - A Literature Review and Research Agenda for 'Smart' Asset Management. *The South African Journal of Industrial Engineering*. <https://doi.org/10.7166/27-4-1478>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372. <https://doi.org/10.1136/bmj.n71>
- Papic, D., & Cerovšek, T. (2019). *Digital Built Environment Maturity Model: Digital Twins Advancing Smart Infrastructure Asset Management*. <https://doi.org/10.35490/ec3.2019.234>
- Saeed, M., Khan, A., Khan, M., Saad, M., El Saddik, A., & Gueaieb, W. (2023). Gaming-Based Education System for Children on Road Safety in Metaverse Towards Smart Cities. *Proceedings of 2023 IEEE International Smart Cities Conference, ISC2 2023*, 1–5. <https://doi.org/10.1109/ISC257844.2023.10293623>
- Sai, S., Gaur, A., Hassija, V., & Chamola, V. (2024). Artificial Intelligence Empowered Digital Twin and NFT-Based Patient Monitoring and Assisting Framework for Chronic Disease Patients. *IEEE Internet of Things Magazine*, 7(2), 101–106. <https://doi.org/10.1109/IOTM.001.2300138>
- Santosa, A., Gunarsih, T., & Wening, N. (2024). Implementation of Risk Management in Asset Management Governance Towards Optimizing Asset Utilization at Public Service Agency State Universities (Case Study of UPN Veteran Yogyakarta). *Jurnal Nawala*. <https://doi.org/10.62872/xc8e9v88>
- Semeraro, C., Lezoche, M., Panetto, H., & Dassisti, M. (2021). Digital twin paradigm: A systematic literature review. *Computers in Industry*, 130, 103469. <https://doi.org/https://doi.org/10.1016/j.compind.2021.103469>
- Wang, H., Zhang, Y., Chen, X., & Wu, J. (2024). Construction of Enterprise Asset Management Accounting System Based on Blockchain Technology. *Applied Mathematics and Nonlinear Sciences*. <https://doi.org/10.2478/amns-2024-0231>

Appendix A

1	Alnuaimi, N., Almemari, A., Madine, M., Salah, K., Breiki, H. Al, & Jayaraman, R. (2022). NFT Certificates and Proof of Delivery for Fine Jewelry and Gemstones. <i>IEEE Access</i> , 10, 101263–101275. https://doi.org/10.1109/ACCESS.2022.3208698
2	Banaeian Far, S., Imani Rad, A., Hosseini Bamakan, S. M., & Rajabzadeh Asaar, M. (2023). Toward Metaverse of everything: Opportunities, challenges, and future directions of the next generation of visual/virtual communications. <i>J. Netw. Comput. Appl.</i> , 217(C). https://doi.org/10.1016/j.jnca.2023.103675
3	Bartoli, C., Fasano, F., Cappa, F., & Boccardelli, P. (2025). Opportunities and Challenges in the Metaverse and NFTs for Business Model Innovation: A Managerial Point of View. <i>IEEE Transactions on Engineering Management</i> , 72, 1685–1698. https://doi.org/10.1109/TEM.2025.3560910
4	Bouraga, S. (2023). We Are Launching our Own NFT! Characterizing Fashion NFT Transactions - Preliminary Results. 2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 1–8. https://doi.org/10.1109/BRAINS59668.2023.10316824
5	Cao, X., Li, X., Xiao, Y., Yao, Y., Tan, S., & Wang, P. (2022). BDTwins: Blockchain-based Digital Twins Lifecycle Management. 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta), 2003–2010. https://doi.org/10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00290
6	Chen, C., Li, Y., Wu, Z., Mai, C., Liu, Y., Hu, Y., Kang, J., & Zheng, Z. (2024). Privacy computing meets metaverse: Necessity, taxonomy and challenges. <i>Ad Hoc Netw.</i> , 158(C). https://doi.org/10.1016/j.adhoc.2024.103457
7	Daneshfar, F., & Jamshidi, M. (Behdad). (2023). An octonion-based nonlinear echo state network for speech emotion recognition in Metaverse. <i>Neural Netw.</i> , 163(C), 108–121. https://doi.org/10.1016/j.neunet.2023.03.026
8	Dastagir, M. B. A., Tariq, O., & Han, D. (2022). A Smart Card based Approach for Privacy Preservation Authentication of Non-Fungible Token using Non-Interactive Zero Knowledge Proof. 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta), 2428–2435. https://doi.org/10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00339
9	Elmay, F. K., Madine, M., Salah, K., & Jayaraman, R. (2023). NFTs for Trusted Traceability and Management of Digital Twins for Shipping Containers. 2023 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops), 433–438. https://doi.org/10.1109/PerComWorkshops56833.2023.10150331
10	Gebreab, S. A., Hasan, H. R., Salah, K., & Jayaraman, R. (2022). NFT-Based Traceability and Ownership Management of Medical Devices. <i>IEEE Access</i> , 10, 126394–126411. https://doi.org/10.1109/ACCESS.2022.3226128
11	Gebreab, S. A., Musamih, A., Hasan, H. R., Salah, K., Jayaraman, R., Al Hammadi, Y., & Omar, M. (2024). NFTs for accessing, monetizing, and teleporting digital twins and digital artifacts in the metaverse. <i>Comput. Commun.</i> , 228(C). https://doi.org/10.1016/j.comcom.2024.107965
12	Gebreab, S. A., Salah, K., Jayaraman, R., & Zemerly, J. (2023). Trusted Traceability and Certification of Refurbished Medical Devices Using Dynamic Composable NFTs. <i>IEEE Access</i> , 11, 30373–30389. https://doi.org/10.1109/ACCESS.2023.3261555
13	Hammi, B., Zeadally, S., & Perez, A. J. (2023). Non-Fungible Tokens: A Review. <i>IEEE Internet of Things Magazine</i> , 6(1), 46–50. https://doi.org/10.1109/IOTM.001.2200244
14	Han, J., Simeone, A. L., & Vande Moere, A. (2024). Superarchitectural: Challenging the Architectural Design of the Metaverse. <i>Proceedings of the 2024 ACM Designing Interactive Systems Conference</i> , 1895–1913. https://doi.org/10.1145/3643834.3661637
15	Hasan, H. R., Madine, M., Yaqoob, I., Salah, K., Jayaraman, R., & Boscovic, D. (2023). Using NFTs for ownership management of digital twins and for proof of delivery of their physical assets. <i>Future Gener. Comput. Syst.</i> , 146(C), 1–17. https://doi.org/10.1016/j.future.2023.03.047
16	Hawashin, D., Salah, K., Jayaraman, R., & Musamih, A. (2023). Using Composable NFTs for Trading and Managing Expensive Packaged Products in the Food Industry. <i>IEEE Access</i> , 11, 10587–10603.

	https://doi.org/10.1109/ACCESS.2023.3241226
17	Huynh-The, T., Pham, Q.-V., Pham, X.-Q., Nguyen, T. T., Han, Z., & Kim, D.-S. (2023). Artificial intelligence for the metaverse: A survey. <i>Eng. Appl. Artif. Intell.</i> , 117(PA). https://doi.org/10.1016/j.engappai.2022.105581
18	Jain, A., Garg, M., Gupta, A., Batra, S., & Narwal, B. (2024). IoMT-BADT: A blockchain-envisioned secure architecture with a lightweight authentication scheme for the Digital Twin environment in the Internet of Medical Things. <i>J. Supercomput.</i> , 80(11), 16222–16253. https://doi.org/10.1007/s11227-024-06026-8
19	Jamshidi, M. (Behdad), Sargolzaei, S., Foorginezhad, S., & Moztarzadeh, O. (2023). Metaverse and microorganism digital twins: A deep transfer learning approach. <i>Appl. Soft Comput.</i> , 147(C). https://doi.org/10.1016/j.asoc.2023.110798
20	Khati, P., Shrestha, A. K., & Vassileva, J. (2022). Non-Fungible Tokens Applications: A Systematic Mapping Review of Academic Research. 2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 323–330. https://doi.org/10.1109/IEMCON56893.2022.9946500
21	Lee, L.-H., Braud, T., Zhou, P. Y., Wang, L., Xu, D., Lin, Z., Kumar, A., Bermejo, C., & Hui, P. (2024). All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda. <i>Found. Trends Hum.-Comput. Interact.</i> , 18(2–3), 100–337. https://doi.org/10.1561/11000000095
22	Makanyadevi, K., Rithika, S., Biratheep, S., & Subanki, S. (2023). QR Code with Block Chain Technology for Medical Device Ownership. 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), 1, 1760–1764. https://doi.org/10.1109/ICACCS57279.2023.10112771
23	Maksymyuk, T., Gazda, J., Bugár, G., Gazda, V., Liyanage, M., & Dohler, M. (2022). Blockchain-Empowered Service Management for the Decentralized Metaverse of Things. <i>IEEE Access</i> , 10, 99025–99037. https://doi.org/10.1109/ACCESS.2022.3205739
24	Musamih, A., Salah, K., Jayaraman, R., Yaqoob, I., Puthal, D., & Ellahham, S. (2023). NFTs in Healthcare: Vision, Opportunities, and Challenges. <i>IEEE Consumer Electronics Magazine</i> , 12(4), 21–32. https://doi.org/10.1109/MCE.2022.3196480
25	Nnadiakwe, C. A., Igboanusi, I. S., Lee, J. M., & Kim, D.-S. (2025). Revolutionizing Healthcare Supply Chains With a Blockchain Framework for NFT-Based Product Certification and Inventory Management. 2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC), 454–458. https://doi.org/10.1109/ICAIIIC64266.2025.10920857
26	Pengiran Omarali, P. S. (2023). Exploring the Intersections between the Metaverse and Web3 Emerging Technologies. 2023 6th International Conference on Applied Computational Intelligence in Information Systems (ACIIS), 1–7. https://doi.org/10.1109/ACIIS59385.2023.10367245
27	Prakash, R., & Thomas, T. (2025). Towards Secure AI-driven Industrial Metaverse with NFT Digital Twins. 2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS), 721–729. https://doi.org/10.1109/COMSNETS63942.2025.10885606
28	Qu, M., Sun, Y., & Feng, Y. (2022). Digital Media and VR Art Creation for Metaverse. 2022 2nd Asia Conference on Information Engineering (ACIE), 48–51. https://doi.org/10.1109/ACIE55485.2022.00018
29	Qu, Q., Xu, R., Sun, H., Chen, Y., Sarkar, S., & Ray, I. (2023). A Digital Healthcare Service Architecture for Seniors Safety Monitoring in Metaverse. 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), 86–93. https://doi.org/10.1109/MetaCom57706.2023.00027
30	Que, P., Zeng, Y., & Gao, F. (2022). The Current Situation and Prospect of the Development of Metaverse Technology. 2022 4th International Conference on Applied Machine Learning (ICAML), 1–5. https://doi.org/10.1109/ICAML57167.2022.00089
31	Raman, R., Mandal, S., Gunasekaran, A., Papadopoulos, T., & Nedungadi, P. (2025). Transforming business management practices through metaverse technologies: A Machine Learning approach. <i>International Journal of Information Management Data Insights</i> , 5(1), 100335. https://doi.org/https://doi.org/10.1016/j.jjime.2025.100335
32	Saeed, M., Khan, A., Khan, M., Saad, M., El Saddik, A., & Gueaieb, W. (2023). Gaming-Based Education System for Children on Road Safety in Metaverse Towards Smart Cities. 2023 IEEE International Smart Cities Conference (ISC2), 1–5. https://doi.org/10.1109/ISC257844.2023.10293623

33	Sai, S., Gaur, A., Hassija, V., & Chamola, V. (2024). Artificial Intelligence Empowered Digital Twin and NFT-Based Patient Monitoring and Assisting Framework for Chronic Disease Patients. <i>IEEE Internet of Things Magazine</i> , 7(2), 101–106. https://doi.org/10.1109/IOTM.001.2300138
34	Sai, S., Hassija, V., Chamola, V., & Guizani, M. (2024). Federated Learning and NFT-Based Privacy-Preserving Medical-Data-Sharing Scheme for Intelligent Diagnosis in Smart Healthcare. <i>IEEE Internet of Things Journal</i> , 11(4), 5568–5577. https://doi.org/10.1109/JIOT.2023.3308991
35	Villa, A., Buccella, G., Barbieri, L., Palladini, D., & D'Avanzo, G. (2023). A multi-resolution method for internal partial discharge simulation. <i>J. Comput. Phys.</i> , 491(C). https://doi.org/10.1016/j.jcp.2023.112362
36	Xiao, Y., Xu, L., Zhang, C., Zhu, L., & Zhang, Y. (2023). Blockchain-Empowered Privacy-Preserving Digital Object Trading in the Metaverse. <i>IEEE MultiMedia</i> , 30(2), 81–90. https://doi.org/10.1109/MMUL.2023.3246528
37	Zhang, Q., Xiong, Z., Zhu, J., Gao, S., Yang, W., & Niyato, D. (2023). Ownership Tokenization and Incentive Design for Learning-based User-Generated Content. <i>2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)</i> , 306–313. https://doi.org/10.1109/MetaCom57706.2023.00061

Artificial intelligence at the service of investigative journalism: A paradigmatic case of designing a prototype to support journalists' routine procedures

(A inteligência artificial ao serviço do jornalismo de investigação: caso paradigmático da idealização de um protótipo de apoio ao procedimento habitual do jornalista)

Joana Silva
Universidade do Porto, Portugal
joana.rodrigues.silva@gmail.com

Received: 1 September 2023

Accepted: 7 February 2025

Abstract

When we talk about investigative journalism, we try to understand a series of steps that aim to search evidence, findings and everything that can be used in social and legal contexts and that attest a certain piece of information is true and not false. The role of the investigative journalist is often placed at the base of the fourth estate, or as an intellectual powerhouse that contrasts with the forces that rule the governance system of most nations. The journalist's experience and performance is integrated in the concept that everything is questionable and subject of analysis. This premise attests to an increased responsibility in the investigation and treatment of these matters which, to a large extent, are discussed in the public regime. We are often faced with the role of the investigative journalist being minimized, even being made inferior, as the governments and companies that financially support this practice do not intend to invest in what could one day take away their position. Given the decreasing level of monetization of this practice, we decided to develop the idea of a tool to make the practice of investigative journalism more democratic, through the automation of the most strenuous processes of the investigative process, opting for tools that help the journalist to think, inquire and visualize the links of the investigation in a pragmatic way based on image design. This desire to make the practice of investigative journalism faster and less dependent on funding from large groups - the aim is to outline a more advanced reality in the practice of investigative journalism - an idea that could also be applied to other types of professionals, such as private investigators and historians.

Keywords *Investigative journalism, Artificial intelligence, Journalist workflow, Automation processes, Investigation platform, Digital media.*

Resumo

Quando falamos de jornalismo de investigação, procuramos compreender uma série de passos que visam encontrar provas, constatações e tudo aquilo que possa ser utilizado em contextos sociais e jurídicos que atestem se uma determinada informação é verdadeira e não falsa. Muitas vezes o papel do jornalista de investigação é colocado na base do quarto poder, ou como uma potência intelectual que contrasta com as forças que regem o sistema de governação da maioria das nações. O jornalista tem à partida uma base interrogatória muito forte sobre tudo aquilo que existe no sistema e tudo o que constitui a própria vida - a curiosidade sobre tudo o que se passa no mundo. Esta premissa, atesta uma responsabilidade acrescida na investigação e tratamento destes assuntos que, em boa medida, são discutidos no regime público. Muitas vezes, somos confrontados com a minimização do papel do jornalista de investigação, sendo até inferiorizado, já que os governantes e as empresas que sustentam financeiramente esta prática, não pretendem investir naquilo que um dia lhes poderá tirar o cargo. Face ao nível decrescente de monetização desta prática, decidimos desenvolver a ideia de uma ferramenta para tornar a prática de jornalismo de investigação mais democrática, através da automação de processos mais extenuantes do processo investigativo, optando por ferramentas que

ajudem o jornalista a pensar, indagar e visualizar os enlaces da investigação de uma forma pragmática baseado no design da imagem. Desta vontade de tornar a prática de jornalismo de investigação mais rápida e menos dependente do financiamento de grandes grupos, pretende-se esboçar uma realidade mais avançada da prática de jornalismo de investigação - uma ideia que também poderá ser aplicada a outros tipos de profissionais, como investigadores privados e historiadores.

Palavras-chave *Jornalismo investigativo, Inteligência artificial, Workflow do jornalista, Processos de automação, Plataforma de investigação, Media digitais.*

1. Introdução

Durante os últimos quatro anos, desenvolvemos uma investigação que ambicionava propor uma ferramenta baseada na automação e na inteligência artificial, para que pudesse ajudar o jornalista de investigação a produzir mais conteúdo. Conteúdo este com maior qualidade e que pudesse também ser uma ferramenta de apoio à própria análise e pensamento crítico sobre questões fundamentais da área do jornalismo de investigação.

“O objetivo principal do jornalismo é fornecer aos cidadãos as informações de que precisam para serem livres e autogovernados” (Walth et al., 2019, p. 178), pelo que quando falamos de jornalismo de investigação, falamos do tratamento de questões sensíveis, nomeadamente de situações da sociedade atual que não estão equilibradas com os valores básicos do jornalismo e os valores básicos de qualquer ser humano. Questões estas que nos levam a pessoas que praticam, não necessariamente crimes, mas que agindo de má-fé - as suas ações prejudicam de alguma forma outros seres humanos, animais ou até mesmo a mãe natureza. Neste enquadramento, podemos falar aqui de casos de corrupção, de homicídios, de tráfico de droga, negligências, ou seja, tudo aquilo que, do ponto de vista conceptual, não está equilibrado na sociedade, referindo por exemplo as forças judiciais e tribunais que não têm feito o trabalho necessário para resolver esse tipo de questões.

É preciso, talvez, dar a conhecer de uma forma pública essas questões, para que elas tenham outros olhares sobre os mesmos factos e que estas situações possam ser de facto, resolvidas. “Reportar e informar o público são considerados parte das funções normativas que os teóricos da democracia liberal assinam para a média de notícias nas democracias” (Carson & Farhall, 2018, p. 1900). Portanto, o jornalista de investigação, e o jornalismo de investigação em concreto, procura sempre atingir este equilíbrio entre a democracia e a justiça social, tendo sempre em consideração que o jornalista vai apenas expor/informar sobre uma situação em específico que, possivelmente, não está a ter o melhor tratamento usando a metodologia habitual. Quando referimos esta exposição, abordámos sempre questões sensíveis, porque, em última instância, ninguém quer essa conotação de criminoso, de alguém que agiu de má-fé e é conhecido apenas por esse ato negligente. Ninguém quer ser reconhecido por algo que fez de mal. Quando o jornalista expõe publicamente que algo aconteceu a uma pessoa ou determinadas pessoas e que estas foram responsáveis por determinadas situações de índole criminosa, estamos a expor em praça pública, como acontecia nos tempos medievais, em que os próprios crimes e criminosos eram resolvidos em praça pública através de açoites e outras formas de punição que envolviam violência física.

Da mesma forma que antigamente, se expunha o crime pela vergonha em praça pública, os jornalistas de investigação também têm um papel preponderante nesta visibilidade pela vergonha. Dada as calamidades que encontramos atualmente relativamente ao conflito entre a Rússia e a Ucrânia, as repercussões da pandemia do coronavírus e outros casos particulares de criminalidade que surgem a nível mundial, ergue-se então, uma necessidade acrescida de incrementar valor às ferramentas e práticas tecnológicas do jornalista de investigação, para que o mesmo possa fazer o seu papel e que possa implementar a sua força como quarto poder. Foi com esse intuito que, esboçamos/idealizámos uma plataforma, que pudesse ajudar a produzir melhor jornalismo de investigação, auxiliado por um assistente virtual que amplifique o valor desta plataforma. Um dos objetivos primordiais desta ideia, é também proteger a integridade destes profissionais, que muitas vezes colocam a vida em risco para poder fazer o seu trabalho.

2. Contextualização

2.1. O cenário híbrido da exposição de informação nos gadgets

“O conceito de gatekeeping capta a ideia de que a informação pode ser impedida de várias formas ou repassada no processo de comunicação. Nem todas as informações de notícias são publicadas e amplamente disponibilizadas. Há uma matriz de forças em jogo que impacta as decisões de controle, incluindo diferenças ou vieses cognitivos individuais, rotinas de trabalho para produção de notícias, características organizacionais, atores institucionais sociais externos, como anunciantes ou governos, e sistemas sociais, como cultura ou ideologia” (Diakopoulos, 2019, p. 947).

Um dos pontos históricos mais impactantes de toda a evolução tecnológica foi o surgimento de smartphones. Passamos de utilizar, em exclusivo, o computador como uma ferramenta de trabalho e passamos a dar preferência aos telemóveis e smartphones, para fazermos praticamente tudo aquilo que fazíamos no computador.

Com a chegada do ecrã reduzido e por conseguinte, com o desenvolvimento de aplicações e plataformas que funcionam através do toque, ficamos apetrechados com ferramentas que nos permitem fazer jornalismo em qualquer sítio e em qualquer circunstância. Com a utilização desenfreada dos smartphones, deparámo-nos com duas situações antagónicas, que devem e merecem ser analisadas através do fenómeno da inteligência artificial e da automação no jornalismo de investigação. A primeira, incide sobre o facto de todas as pessoas terem acesso aos mesmos recursos que, antes da utilização destes gadgets, só os utilizadores de computador tinham acesso. A partir deste momento, todas as pessoas que tenham telemóvel conseguem fazer quase tudo o que os utilizadores do computador conseguem fazer. Este acesso generalizado fez também com que houvesse um outro fenómeno paradigmático que é o excesso de informação nas redes. Neste sentido surge “a adoção da automação num número crescente de redações em todo o mundo que levou os pesquisadores a começar a explorar as perceções do público sobre artigos de notícias escritos por algoritmos” (Tandoc et al., 2020).

Qualquer pessoa com um smartphone/gadget, é capaz de consumir, mas é também capaz de produzir informação. O facto desta informação, sendo produzida tanto a nível dos gadgets como os smartphones, não ser uma informação filtrada, acaba por ser contraproducente, porque acabamos por aceder a informações que achamos que são fidedignas. Quando na verdade, não tem qualquer tipo de controlo sobre as suas fontes ou sobre a sua veracidade. Portanto, vivemos na era da desinformação. Parece-nos que estamos mais capacitados para utilizarmos telemóvel e criarmos informação, mas o facto é que grande percentagem de informação que existe nas redes sociais, nas plataformas informativas e também nos sites de procura de informação, como é o caso da Google, não é seriada. Muitas vezes aquilo que vemos ou percebemos nos gadgets e computadores, são informações que transmutam em conteúdos digitais, de uma plataforma para a outra, fazendo com que alguma dessa informação fique perdida na re-partilha dos conteúdos. Isso faz com que a maior parte dos adolescentes e todos aqueles utilizadores menos literados que, consideram que estão a produzir e a consumir informação credível, estão simplesmente numa bolha de desinformação e muito provavelmente estarão cada vez mais a ficarem incapacitados intelectualmente, relativamente à informação que deviam estar a utilizar. Este fenómeno, cria muito lixo digital aumentando uma pegada digital que se baseia na perda de referências das fontes. A informação é deliberada e não conseguimos perceber o que é que de facto verdade e o que não é - isto cria muito ruído informativo e desinformação no que diz respeito à utilização de plataformas digitais.

2.2. A influência da inteligência artificial na eficiência cognitiva

Quando analisamos a inteligência artificial, comparativamente com a inteligência humana, tendencialmente acreditamos que a inteligência artificial é superior à inteligência humana, no entanto, é preciso frisar que a inteligência humana será sempre superlativa à inteligência artificial, até porque foi a inteligência humana que inventou a AI. Entendemos que alguns métodos e recursos da inteligência artificial, e também de automação, superam algumas habilidades do ser humano. Isto não é generalizável para todas as pessoas. Recentemente, ouvimos falar em ferramentas como o ChatGPT e outras ferramentas que foram criadas, para que de alguma maneira, façam o trabalho do ser humano. No mesmo sentido ao esboçarmos a ideia da plataforma “Connect-the-Dots” baseamo-nos nestes processos algorítmicos que poderão recriar os processos humanos.

A questão é que tudo aquilo que a inteligência artificial faz é uma replicação e uma repetição dos atos do ser humano. De alguma forma, o conteúdo gerado no final será sempre conteúdo inovador, mas é sempre baseado em processos padrão do ser humano. Portanto, como sabemos, os processos de algoritmos funcionam como se fosse uma receita, portanto, analisamos o procedimento do ser humano e depois vamos tentar automatizá-lo o repeti-lo através da máquina. O'Regan acredita que os “métodos de pesquisa visual encorajam o uso de metáforas para comunicar conhecimento e experiência. A metáfora visual atua como um canal que torna possível dizer coisas em forma de imagem que são difíceis ou impossíveis de articular verbalmente. Isso fornece um meio de aceder as

reservas cognitivas conscientes e subconscientes, facilitando os processos de emoção e comunicação” (O'Regan et al., 2019, p. 11).

Quando a consciência global fica cética com a inteligência artificial, é porque de facto o ser humano está a utilizar a inteligência artificial de formas que não se baseiam na boa-fé e que não tem em consideração os resultados e o impacto no ser humano. Estas utilizações, de uma forma generalizada, não têm em consideração o porquê da inteligência artificial existir. Em primeiro lugar, porque a inteligência artificial existe para ajudar o ser humano, em questões sensíveis - por exemplo - o facto de o ser humano precisar de dormir, de comer e de todas as necessidades fisiológicas inerentes à existência, que por sua vez a máquina não necessita. Então, surge o papel da inteligência artificial e dos robots para poderem trabalhar estas questões que são mais sensíveis. Portanto, quando o jornalista precisa de descansar, a máquina trabalha por ele. É nesta lógica que deveríamos olhar para a AI como forma de ajudar o ser humano nos processos em que ele é mais frágil, capacitando os processos de produção de informação com ferramentas que agilizem as metodologias do jornalismo de investigação.

2.3. A exposição mediática na camada mais jovem: cenários de guerra

Uma das questões mais sensíveis que tem estado na ribalta é a exposição de documentação relativa ao conflito entre a Rússia e a Ucrânia. Esta exposição mediática tem sido cada vez mais impactante e tem ocupado grande percentagem dos noticiários, de hoje em dia, não só através da televisão, mas também nas redes sociais. Constatámos que existe uma grande exposição de conteúdos violentos e conteúdos gráficos, e que de alguma forma, estes conteúdos começam a tornar-se naturais para o ser humano e sobretudo para as camadas mais jovens.

Na primeira fase da guerra, o TikTok foi uma das ferramentas, nas redes sociais, mais utilizadas pelos soldados na linha da frente do conflito entre a Rússia e a Ucrânia. Tanto os russos como os ucranianos, mais jovens, achavam aquele fenómeno da guerra interessante do ponto de vista da exposição mediática. Assim, nas primeiras semanas do conflito, verificou-se a exposição de vários vídeos de soldados russos e ucranianos nas linhas da frente a dançarem fardados e mulheres maquilhadas nos tanques, o que, numa primeira fase mostrou uma falta de consciência na camada mais jovem relativamente às preocupações globais. Mais tarde veio-se a saber que grande parte desses jovens acabaram por morrer e que só deixaram ficar, de facto, esses conteúdos mais populares a nível das redes sociais, que por si só denotavam, exatamente a falta de consciencialização das camadas mais jovem relativamente ao que se está a passar a nível mundial.

Tal como afirma Traquina "pela importância da relativa autonomia dos jornalistas, a existência de valores e normas profissionais, bem como a força de toda uma cultura que atrai um número significativo de jovens crédulos na mitologia jornalística, a capacidade acrescida por parte de vários agentes sociais a participar e, às vezes ganhando no jogo da notícia, defendemos a posição de que seria mais correto dizer que o jornalismo é um Quarto Poder que periodicamente consegue realizar seu potencial de contrapoder" (Traquina, 2005).

Podemos refletir que os jovens, não têm a mesma capacidade que existia nos anos 70, falando aqui da revolução pela paz mundial, portanto vemos jovens que não se enquadram no conceito de guerra, mas também não se enquadram no conceito da vida, como ela é em termos de sociedade. Aquilo que podemos verificar é que os confrontos pela paz e as revoluções mais jovens acabam em mortes não significativas. Encontramos grandes exemplos de jovens que morreram, justamente em protestos, mas infelizmente algumas mortes foram apenas registos numéricos sem grande impacto para alteração paradigmática da sociedade. Em grande medida não existe método para chegar à paz mundial. Percebemos assim que a saúde mental dos jovens se tem degradado exponencialmente com as redes sociais e com a exposição a imagens violentas e gráficas de conflitos que o planeta terra tem suportado.

2.4. O limiar que separa a projeção das teorias científicas e a ficção científica

“Essa sinergia gera refinamentos simultâneos de teoria e prática à medida que a teoria é gerada e refinada por meio de sua aplicação; na verdade, abordagens e teorias educacionais emergem reciprocamente (Bell et al., 2004). A sinergia ajuda a gerar princípios que informam o próprio design, bem como o pensamento e as ações de pesquisadores, designers e profissionais” (Wang & Hannafin, 2005, p. 13).

Uma grande preocupação que tivemos logo desde o início ao idealizar este projeto, foi o facto de termos consciência que a comunidade científica tem delimitações muito precisas para aquilo que é a ciência e para aquilo que não é considerado ciência.

As regras que foram implementadas ao longo dos séculos na própria metodologia científica daquilo que deve ser validado e que não deve ser validado, pode às vezes também ser um constrangimento, porque muitas teorias e muitas perceções daquilo que poderá ser construído a nível técnico e prático não chega a se exprimir porque existem muitos entraves. Entraves conceptuais e de metodologias bastante precisas que, na prática, não chegam a ter expressão no mundo prático. Por isso, é muito habitual termos esta perceção daquilo que é uma teoria em contraste com aquilo que é um exemplo paradigmático do que poderá ser, no futuro. Existe uma delimitação, muitas vezes, ilógica, do potencial das teorias científicas derivada às próprias delimitações do ser humano e das estruturas de poder que existem na comunidade científica.

Constatamos a nível histórico casos em que vários elementos da comunidade científica tentaram delimitar o potencial de grandes cientistas, simplesmente porque não cabiam nas conceções da forma como se produz ciência. Falámos, por exemplo, de casos como Albert Einstein, Leonardo da Vinci, e até mesmo Isaac Newton. Todos estes génios debateram-se inicialmente com a rigidez do sistema e com as práticas metodológicas que validam o conhecimento científico. Hoje em dia sabemos que a Teoria da Relatividade não tem a sua expressão total na ciência, porque ainda hoje é uma teoria avançada para o seu tempo. É necessário enfatizar que as crenças pessoais não podem delimitar o que é ou não ciência e a sua própria validação metodológica deve ter em consideração diferentes formas de perceber a realidade em que estamos inseridos.

Hoje em dia existe um cruzamento metodológico de várias áreas científicas e que a percepção do que é ou que poderá ser é muito relativa, porque quando falamos em questões de análise física do universo e percebemos que existe uma grande parte da realidade que nós não percebemos e não conseguimos analisar com os nossos métodos físicos e humanos atuais. Parte da nossa idealização daquilo que pode não ser compreensível ao ser humano pelas suas delimitações sensoriais não devem ser retirado da sua pertinência a nível da escala universal.

Neste sentido, podemos considerar que existem ferramentas, no âmbito do jornalismo de investigação automatizado, que poderão se posicionar numa área mais cinzenta da percepção daquilo que é praticável, mas acreditamos que não hoje nem amanhã - mas daqui a algumas décadas ou séculos - poderá haver tecnologia suficiente para expressar as nossas ideias.

2.5. Os robots que ajudam os jornalistas

Nas idealizações mais arrojadas que ambicionamos fazer, destacamos o assistente pessoal DODO, que poderá um dia se edificar como um robot. Quando idealizamos esta ferramenta, totalmente automatizada, pensámos num amigo virtual que pudesse ser o melhor amigo do jornalista aquando da investigação. E quando falamos do DODO que ajuda o jornalista no âmbito digital, também idealizamos esta possibilidade a nível da sua expressão física como robot, que poderá, eventualmente, ajudar o jornalista de investigação em trabalho de campo, sobretudo nas zonas de conflito do planeta.

3. Metodologia

3.1. Design-based-research

Como a essência do nosso estudo depende de uma experimentação científica que deve ser validada num contexto real, devemos aplicar seletivamente o design-based-research como metodologia para o nosso estudo. Sendo uma metodologia com poucos anos de experiência empírica, foi identificada como um método de validação científica pelo seu carácter estruturante do conhecimento prático, bem como pela introdução de estruturas de conhecimento. O principal desafio da nossa investigação é incorporar processos automatizados ao processo de jornalismo investigativo. Como observam Juuti e Lavonen (2012), o design-based-research pode funcionar como um importante método de identificação e gestão de necessidades. Os designers e jornalistas podem definir objetivos para otimizar artefactos durante a fase de teste (Juuti & Lavonen, 2012, p. 61).

É fundamental integrar sistemas automatizados em projetos que permitam a melhoria do jornalismo de investigação tendo em conta os desenvolvimentos científicos e empíricos neste domínio. Na pesquisa-ação participativa, “os investigadores trabalham em conjunto com os participantes, usam práticas locais para apoiar a teorização sistemática e melhoram a prática e a teoria. (...) Da mesma forma, o projeto de intervenção – às vezes equiparado à avaliação formativa – é frequentemente realizado para gerar evidências usadas para orientar possíveis revisões em um projeto em andamento (Reeves & Hedberg, 2003)” (Wang & Hannafin, 2005, p. 6).

Quando falamos em design de intervenção, pensamos em desenvolver uma ideia e aplicar essa mesma ideia para resolver um problema que enfrentamos no nosso cotidiano. A plataforma Connect-the-Dots é uma ideia, um conceito que se tornou um projeto de ajudar o jornalista investigativo a obter melhores resultados no seu trabalho e, como o jornalismo de investigação representa o quarto poder, deve ser dado mais credibilidade e fé aos processos de automação que podem ser combinados com o fluxo de trabalho padrão no jornalismo investigativo.

3.2. Processos de iteração

Hoadley (2004, p. 203) argumenta que os métodos de investigação baseados num único design podem ser úteis se puderem demonstrar a relevância de um design ou produto para o processo de pesquisa, portanto, fornecer feedback científico e pragmático. O processo de investigação baseado no design antevê dois tipos de análise. A primeira pressupõe uma abordagem de testagem, o que significa que as extrapolações feitas durante a investigação podem ser alteradas dependendo dos resultados intermediários. Uma vez que “a pesquisa baseada em design também é caracterizada por um ciclo iterativo de design, promulgação ou implementação, análise e redesenho” (Wang & Hannafin, 2005, p. 9), na prática, o design pode ser reajustado pelo consumidor final, mas para que isso seja eficaz, algumas iterações terão que ser feitas para testar conceitualmente a ideia por meio de sua apresentação aos consumidores finais. É interessante a possibilidade de fazer medições intermediárias para a estrutura científica dependendo dos resultados intermediários e, assim, poder testar o processo de pesquisa e antecipar erros. Vislumbramos que o Connect-the-Dots possa ser um projeto capaz de interpretar a realidade do jornalismo e concluir como a inteligência artificial pode ser um método influente para alcançar mais resultados na reportagem investigativa e também para tirar conclusões conceptuais que possam realmente mudar o paradigma da era digital.

3.3. Primeira iteração através da Observação Participada

Acreditamos que a melhor forma de validar cientificamente uma hipótese sobre o estado atual da ciência nos meios digitais é entender a realidade do jornalismo nas redações. Por isso, foi nossa intenção desde o início examinar as práticas do jornalismo durante sua aplicação no campo e escolhemos a empresa portuguesa de televisão pública, porque acreditamos que os seus métodos de trabalho são fiáveis e replicáveis, visto que estamos a falar de uma estação de televisão com mais de 60 anos de existência.

Dentro do método de observação participante, utilizamos diversas formas de medir a realidade estudada, levando em consideração o nosso foco de estudo. Neste capítulo vamos focar-nos essencialmente na observação direta para avaliar o fluxo de trabalho dos atuais jornalistas e dos jornalistas de investigação, bem como das ferramentas digitais utilizadas no contexto das redações e no contexto da reportagem de campo, para integrar as plataformas digitais no contexto convencional do processo de fazer notícia.

Deve-se reconhecer que, além de documentar a experiência etnográfica num diário de bordo, também utilizamos o método de etnografia visual para captar momentos-chave nos ambientes de produção noticiosa, aproveitando para tirar conclusões sobre o comportamento dos jornalistas tendo em conta que estavam a ser estudados, para a construção de um conceito de protótipo de suporte à sua atividade.

Couto acredita que “a pesquisa participante está relacionada ao poder e o poder está relacionado à mudança ou à manutenção do status quo. Ele baseia-se fortemente em Marx e em teóricos sociais contemporâneos, como Paulo Freire, e incorpora a análise de classe. As suas preocupações centrais são a pesquisa, a produção de conhecimento e o empoderamento relacionado à situação de pessoas oprimidas, pessoas pobres, pessoas em desvantagem política ou econômica” (Couto, 1987, p. 84).

Assim, é nosso sistema de crenças que integramos nos nossos estudos ambientes que sejam replicáveis do ponto de vista de que são um exemplo de conduta dentro da ideia jornalística.

3.4. Segunda iteração através de métodos de recolha de dados

Tendo em conta que “a recolha de dados é um processo de escolha seletiva de fenómenos empíricos e de lhes atribuir relevância relativamente à questão de investigação” (Bergman & Coxon, 2005, p. 4) consideramos pertinente, para além das conclusões retiradas de observação participante, estruturar formas de recolha de dados específicos capazes de nos orientar sobre as necessidades detalhadas de automação no jornalismo que podem ser fundamentais para a idealização de ferramentas de apoio à produção jornalística. “A qualidade do processo de coleta de dados em métodos qualitativos pode ser dividida conceitualmente na qualidade do instrumento ou outro método de coleta de dados e na qualidade dos dados obtidos do instrumento” (Bergman & Coxon, 2005, p. 4).

Para além dos resultados teóricos e empíricos que conseguimos extrair através da observação participante, consideramos relevante a recolha de dados específicos através de dois métodos. A primeira foi conseguida através da aplicação de 64 inquéritos aos diferentes setores estudados no CPN da RTP.

“A observação é uma componente chave da pesquisa etnográfica, embora nem todos os estudos observacionais usem a etnografia. Embora alguns livros distingam entre dados observacionais e dados de entrevistas ao descrever a pesquisa etnográfica, é provável que ocorra uma confusão considerável entre os dois durante o trabalho de campo” (Moriarty, 2011, p. 21), portanto, consideramos que os dados recolhidos nas investigações e entrevistas são uma forma de agregar valor e credibilidade ao estudo de observação participante e, assim, tornar um estudo de caso relevante tanto para o design da ideia do protótipo como para tirar conclusões sobre o uso de IA e automação na produção jornalística.

O segundo método foi conseguido através da aplicação de entrevistas centradas em profissionais de interesse, onde foi possível compreender, de um ponto de vista mais qualitativo e aprofundado, as necessidades tecnológicas dos jornalistas e a sua opinião alargada sobre assuntos associados à inteligência artificial e investigação jornalística. A qualidade tanto dos inquéritos como dos guiões de

entrevista deve ser avaliada com base na forma como foram construídos, razão pela qual devemos realçar que tanto os inquéritos como as entrevistas foram realizados numa fase inicial da investigação, pelo que a sua duração e conteúdo são compartilhadas por um carácter generalista.

4. Resultados

4.1. Procedimento habitual do jornalista de investigação

O fluxo de trabalho do jornalismo de investigação na redação televisiva da RTP tem uma gestão diferente dos restantes jornalistas que tratam de assuntos da atualidade. Como muitas vezes se trata da análise de conteúdos sensíveis e que exigem um certo grau de anonimato, grande parte do conteúdo da investigação só é conhecida no dia em que os programas da série “Sexta às 9” são emitidos.

De modo geral, após interagir com os jornalistas investigativos deste programa, conseguimos perceber que o tema de cada episódio pode ser um tópico inovador ou uma continuação de um episódio anterior. Normalmente, os temas surgem através de sugestões dos jornalistas que integram o programa, ou são sugeridos pela equipa de gestão, que na altura era liderada por Sandra Felgueiras.

Após o aprofundamento do caso, segue-se a análise de documentos, elementos multimédia e outros dados relacionados com a investigação. Após a análise desses dados, são feitas filmagens no local do evento e as pessoas que se dispõem a falar sobre o assunto são entrevistadas em vídeo. Podemos referir que nem sempre as pessoas se sentem à vontade para fazê-lo, o que se pode tornar num trabalho redobrado para encontrar alguém disponível para falar publicamente sobre um assunto. Após a captação dessas imagens, há, como no jornalismo de atualidade, a escrita da locução, que é combinada com as imagens que são editadas à posteriori. É de referir que neste tipo de jornalismo são frequentemente utilizados infográficos, ou efeitos de transição de partes de um documento, ou frações de uma imagem, elementos que se combinam no ecrã para explicar algo ao telespectador.

4.2. Ferramentas baseadas no procedimento habitual do jornalista

Conforme referido na secção anterior, tanto a plataforma CTD como o desenvolvimento do algoritmo prevêem a integração de ferramentas open-source e a utilização de projetos open-source, de forma a aproveitar todo o conhecimento científico e empírico, para que haja uma reutilização das ferramentas disponíveis para integração no desenvolvimento de back-end. Durante todo o tempo de investigação, dedicado a perceber que tipos de ferramentas já foram desenvolvidas por diferentes entidades e que podem ser integradas no projeto CTD, conseguimos chegar a uma lista significativa de ferramentas que têm o mesmo carácter empírico de algumas das ferramentas que idealizamos.

Podemos dizer que a maioria das ferramentas identificadas está relacionada a processos de automação de tarefas e criação de conteúdos informativos e visuais por meio de inteligência artificial.

Durante o processo de idealização das ferramentas que seriam úteis e necessárias para uma melhor atuação do jornalista investigativo em projetos de informação, surgiu a necessidade de encontrar soluções de código aberto, ou ferramentas que estejam disponíveis gratuitamente para integração em sistemas, de forma a criar um projeto capaz de reaproveitar trabalhos já realizados por outros investigadores e designers.

4.3. Timeline para organização visual

Se a timeline for exibida em relação às categorias ou parâmetros selecionados na lista de dados, pode haver a possibilidade de visualizar os dados da timeline na perspetiva de uma linha do tempo vertical ou em camadas, onde é possível alterar, por exemplo, o ano de visualização de dados. Nomeadamente os dados referentes ao ano de 2010, e outra camada referente aos dados de 2011, portanto, são duas perspetivas diferentes de relação dos dados. Podemos falar aqui sobre uma linha de tempo tridimensional.

5. Resultados

5.1. Plataforma de apoio no desktop

“O objetivo é o mesmo de outros exercícios de brainstorming: criar o maior número possível de novas ideias, sem criticá-las. O uso de vídeo, combinado com maquetes de papel ou papelão, encoraja os participantes a experimentar ativamente os detalhes da interação e entender cada ideia da perspectiva do usuário” (Beaudouin-Lafon & Mackay, 2000, p. 1011).

Conforme a imagem da maquete criada, iremos explicar com mais detalhe cada parte do protótipo não funcional, nomeadamente os clusters de ferramentas, que se distinguem claramente pelo seu posicionamento no ecrã e no espaço de trabalho idealizado para a plataforma Connect-the-Dots. Na parte central encontra-se o espaço idealizado para apresentação do mapa visual e linha do tempo referente ao projeto de pesquisa. Na parte inferior da tela, apresentamos as ferramentas para interagir com a timeline. Do lado direito estão expressos os campos nos quais o usuário pode escolher os filtros pelos quais deseja organizar os dados. Na parte superior é possível conferir a barra de pesquisa de forma genérica, e os botões principais, escolhidos pelo usuário, que representam as ferramentas mais utilizadas pelo utilizador nos projetos. No lado esquerdo, são exibidas todas as ferramentas do sistema não incluídas no menu principal, bem como a guia para escolher as especificidades do arquivo de saída.

A dashboard idealizada para a plataforma CTD, está relacionada com a combinação ideal de todas as ferramentas no mesmo espaço de trabalho permitindo ao jornalista e outros investigadores terem acesso a tudo o que é necessário para estudar e investigar um determinado assunto. Desta forma, a dashboard será composta por inúmeros botões agrupados em diferentes quadros, cada um com uma finalidade específica. Os botões serão agrupados de acordo com a sua funcionalidade. Haverá alguns painéis informativos sobre dados e metadados relacionados ao projeto de pesquisa. A parte mais

central do painel será ocupada pela expressão visual da linha do tempo da investigação ou mapa visual. Ao visualizar os dados de forma criativa, o CTD permitirá a interação entre os jornalistas e a timeline para obtenção de informações mais específicas. Também será permitido aumentar e diminuir um detalhe da linha do tempo, como excluir itens indesejados.

5.2. Aplicação móvel como extensão da plataforma

“A prototipagem rápida é a atividade de prototipagem que ocorre no início do ciclo de vida do desenvolvimento de software. Como estamos a considerar apenas a prototipagem inicial, usamos os termos “prototipagem” e “prototipagem rápida” de forma intercambiável. Existem dois métodos de prototipagem: descartável e evolutiva. Frequentemente, a prototipagem é um processo iterativo, envolvendo um procedimento cíclico de design/modificação/revisão de vários estágios. Este procedimento termina quando se ganha experiência suficiente com o desenvolvimento do protótipo (no caso de prototipagem descartável), ou quando o sistema está completo (no caso de prototipagem evolutiva)” (Gordon & Bieman, 1995, p. 11).

Dada esta noção de prototipagem rápida, consideramos interessante esboçar um protótipo para integrar em telemóveis. Ao longo do processo de investigação deste projeto e protótipo, e face aos últimos acontecimentos em zonas de conflito, consideramos importante idealizar uma extensão da plataforma CTD para a versão mobile. Não estamos aqui a falar de um design orientado para a utilização da plataforma via telemóveis, mas sim da criação de ferramentas que só existem na plataforma mobile e que funcionam como uma extensão da ferramenta de introdução de dados recolhidos em relatórios de campo podendo ser tratados posteriormente na versão desktop.

O CTD Explorer também permitirá o acesso a funções específicas que auxiliam os jornalistas nas pesquisas de campo, principalmente em zonas sensíveis e de conflito, como, por exemplo, acesso a ferramentas off-line, mapas de recursos de sobrevivência, postos e pontos de água e eletricidade.

5.3. Timeline

“Os processos estruturados característicos das abordagens atomizadas das notícias podem fornecer mais opções para o público, mas exigem que os jornalistas “escrevam para máquinas” inscrevendo uma estrutura inflexível, bem como delegam elementos de controle a processos computacionais” (Jones & Jones, 2019, p. 1175).

“Vivemos em um mundo em que é cada vez mais importante entender fenômenos socioeconômicos e ecológicos complexos para facilitar decisões bem informadas. Os jornalistas desempenham um papel importante nesse esforço, descobrindo padrões e relacionamentos ocultos para informar, esclarecer e entreter” (Stoiber et al., 2019, p. 700).

Dessa forma, a expressão visual pode enfatizar essas relações de informação. A expressão visual da linha do tempo é a ferramenta central do sistema CTD. De modo que seja o suporte central para jornalistas investigativos e demais pesquisadores, para que possam, de forma ampla e global, encontrar informações básicas de pesquisa que precisam ser estudadas em seu contexto. “A desinformação visual está proliferando e os jornalistas são frequentemente cúmplices na amplificação de informações visuais com proveniência desconhecida e precisão desconhecida” (Thomson et al., 2022, p. 938). O CTD tem como foco reduzir o tempo gasto pelo jornalista investigativo na análise de

dados, além de gerar um mapa mental que permita uma melhor compreensão das diferentes relações entre os diferentes dados.

5.4. Dossier e esquemas finais

O output é o resultado de todos os processos que foram realizados na plataforma, ou seja, um infográfico com os resultados da investigação - uma expressão visual de todas as relações criadas entre os dados, os resultados estatísticos em formato visual de relações específicas entre os dados. Ou seja, tudo o que o jornalista investigativo pode usar para criar a peça jornalística, seja em texto, vídeo ou áudio.

“Estruturar as informações e integrar os dados de várias fontes oferece às redações melhores maneiras de explorar os dados e facilitar a adoção da IA. Por exemplo, pode facilitar a implementação de serviços de recuperação de informação e sistemas de recomendação e a automação de processos de criação de notícias e detecção de notícias falsas e eventos noticiáveis” (Ocaña & Opdahl, 2022, p. 4).

A saída será um resumo do processo investigativo numa única página, essa saída pode ser utilizada como base para relatórios de campo, como guia informativo para a produção de documentários, programas de televisão, áudio, texto ou rádio, sem descuidar do conteúdo digital e relatórios interativos. É importante mencionar que esta saída será uma publicação digital das conclusões tiradas da investigação e sugestões semióticas da expressão visual dos dados e da relação dos dados. As estatísticas conclusivas permitem ao pesquisador calcular a probabilidade de que uma propriedade conjecturada dos dados seja devida ao acaso e estimar a escala do efeito hipotético (Gorman & Johnson, 2013), por isso será importante incluir infográficos com base em estatísticas de relacionamento para observação factual de relacionamento de dados.

“Como atestam os inúmeros exemplos apresentados anteriormente, os jornalistas têm responsabilidade pela visão que incorporam na sua cobertura de notícias e amplificam nas plataformas de redes sociais, especialmente durante crises (...). Da mesma forma, eles também têm a responsabilidade de aumentar sua alfabetização midiática e perspicácia técnica para garantir que possam realizar sua missão de verificação e desmascaramento com o digital” (Thomson et al., 2022, p. 957).

6. Discussão e síntese geral dos trabalhos mais relevantes

“Os designers, é claro, se beneficiam dos resultados da pesquisa científica e podem usar métodos científicos para avaliar sistemas interativos” (Beaudouin-Lafon & Mackay, 2000, p.1010).

Atendendo ao âmbito do nosso projeto de estudo da aplicação do design na produção de informação, ao longo dos últimos quatro anos de investigação, fizemos muitos desenvolvimentos e recuos em termos de confluências científicas sobre inteligência artificial no jornalismo investigativo, bem como na pesquisa de ferramentas com jornalistas experientes que impactassem diretamente na performance e execução do jornalismo investigativo.

“Nem todos os jornalistas estão posicionados para servir como intermediários de dados com o público. Os jornalistas legados, na maioria dos casos, carecem das habilidades de alfabetização

de dados para interagir com sucesso com o 'público de programação' - as diversas partes interessadas (jornalistas, hackers e cidadãos) que se reúnem em torno da produção e consumo de notícias digitais (Ananny, 2013: 637)" (Boyles, 2020, p. 1340).

Assim, “na exploração e avaliação de ideias: A Prototipagem de Experiência pode fornecer inspiração, confirmação ou rejeição de ideias com base na qualidade da experiência que elas engendram. Produz respostas e feedback às perguntas dos designers sobre as soluções propostas em termos de “como seria se...” (Buchenau & Suri, 2000, p. 431).

Compreendemos que o jornalismo investigativo perde território de execução pelo simples fato de haver pouco investimento dos grandes grupos de media nesse tipo de jornalismo, porque se estende no tempo e utiliza muitos recursos, ou simplesmente porque não é prioridade investir em recursos de contrapoder em uma sociedade em que os governantes usam os media como palco de autoridade. Acreditamos que é “crítico e desafiador fazer continuamente ambos os tipos de argumentos, argumentos que têm significado próximo da experiência e relevância distante da experiência” (Barab e Squire, 2004, p. 6), portanto, a implementação de nosso esboço foi baseada em observação participante de um ambiente próximo e pode ser testado por meio de uma experiência de teste de usabilidade com pessoas de interesse remotamente. “O designer deve realizar e iterar seus projetos. Esse processo envolve a coleta de dados sobre as propriedades dos projetos propostos e a antecipação de impactos dentro de um sistema” (Hoadley & Campos, 2022, p.209).

7. Considerações finais

“A Inteligência Artificial se tornou uma parte essencial das nossas vidas. Sem dúvida, tornou a vida muito mais fácil e prática, seja em escala global, como o desenvolvimento econômico e político, ou em escala menor, como o nosso dia-a-dia. A última meia década marcou o início do desenvolvimento de robôs que possuem a capacidade de realizar tarefas humanas. Originalmente, esperava-se que a principal desvantagem da tecnologia de IA estivesse relacionada à perda de perspectivas de trabalho, uma vez que os humanos seriam substituídos por máquinas capazes de operar de forma mais eficiente” (Saidi, 2022, p. 357).

Além do desenvolvimento da pandemia em nível global, a nossa investigação foi realizada num momento crítico em que nos deparamos com uma crise humanitária de invasão russa ao território ucraniano. Embora existam diferentes zonas de conflito globalmente, esta crise mais recente destacou uma necessidade mais premente na execução e aplicação do jornalismo investigativo como um contrapoder contra as atrocidades cometidas entre seres humanos.

“No emprego da IA nas Forças Armadas, uma das preocupações mais sérias da comunidade internacional é o armamento da IA. Esse rápido avanço indica que a inteligência artificial já está a mudar a guerra e que os estados certamente continuarão a construir os sistemas de armas automatizados que a IA permitirá” (Pandya, 2019).

“Na verdade, alguns especialistas acham que a IA terá um impacto favorável na guerra” (Saidi, 2022, p. 358).

Levando em consideração esses acontecimentos, decidimos incluir algumas soluções que podem ajudar o jornalismo investigativo a ganhar força em crises humanitárias por meio da inteligência artificial. O DODO será preponderante neste sentido através da sua expressão enquanto robô,

auxiliando o jornalista de investigação no trabalho de campo, sobretudo em territórios que possam comprometer a vida do jornalista. Também projetamos a versão móvel do CTD Explorer com recursos específicos para a sobrevivência de jornalistas investigativos em zonas de conflito.

Referências

- Beaudouin-Lafon, M., & Mackay, W. (2000). Prototyping tools and techniques. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1006–1031). ACM.
- Bergman, M., & Coxon, A. (2005). The quality in qualitative methods. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 6(2). <https://doi.org/10.17169/fqs-6.2.457>
- Boyles, J. (2020). Laboratories for news? Experimenting with journalism hackathons. *Journalism*, 21(10), 1338–1354. <https://doi.org/10.1177/1464884917737213>
- Buchenau, M., & Suri, J. F. (2000). Experience prototyping. In *Proceedings of the 3rd Conference on Designing Interactive Systems* (pp. 425–433). ACM.
- Carson, A., & Farhall, K. (2018). Understanding collaborative investigative journalism in a “post-truth” age. *Journalism Studies*, 19(13), 1899–1911. <https://doi.org/10.1080/1461670X.2018.1494515>
- Couto, R. (1987). Participatory research: Methodology and critique. *Center for Social Welfare Research*, 5(1). <https://digitalcommons.wayne.edu/csr/vol5/iss1/9>
- Diakopoulos, N. (2019). *Automating the news: How algorithms are rewriting the media*. Harvard University Press.
- Gordon, S., & Bieman, J. (1995). Rapid prototyping: Lessons learned. *IEEE Software*, 12(1), 85–95.
- Gorman, K., & Johnson, D. E. (2013). Quantitative analysis. In R. Bayley, R. Cameron, & C. Lucas (Eds.), *The Oxford handbook of sociolinguistics*. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780199744084.013.0011>
- Hoadley, C., & Campos, F. C. (2022). Design-based research: What it is and why it matters to studying online learning. *Educational Psychologist*, 57(3), 207–220. <https://doi.org/10.1080/00461520.2022.2079128>
- Hoadley, C. (2004). Methodological alignment in design-based research. *Educational Psychologist*, 39(4), 203–212. https://doi.org/10.1207/s15326985ep3904_2
- Juuti, K., & Lavonen, J. (2012). Design-based research in science education: One step towards methodology. *Nordic Studies in Science Education*, 8(2). <https://doi.org/10.5617/nordina.424>
- Moriarty, J. (2011). *Qualitative methods overview*. London School of Economics. http://eprints.lse.ac.uk/41199/1/SSCR_Methods_Review_1-1.pdf
- Ocaña, M., & Opdahl, A. (2022). Supporting newsrooms with journalistic knowledge graph platforms: Current state and future directions. In *CIKM 2020 Workshops. Technologies*, 10(3), 68. <https://doi.org/10.3390/technologies10030068>
- O'Regan, T., Robinson, L., Newton-Hughes, A., & Strudwick, R. (2019). A review of visual ethnography: Radiography viewed through a different lens. *Radiography*, 25(3). <https://doi.org/10.1016/j.radi.2019.06.007>
- Saidi, I. (2022). The weaponization of artificial intelligence in the military: The importance of meaningful human control. *MAS Journal of Applied Sciences*, 7(2), 357–363.
- Stoiber, C., Rind, A., Grassinger, F., Gutounig, R., Goldbruger, E., Sedlmair, M., Emrich, S., & Aigner, W. (2019). netflower: Dynamic network visualization for data journalists. *Computer Graphics Forum*, 38(3). <https://doi.org/10.1111/cgf.13721>
- Tandoc, E. C., Jr., Yao, L., & Wu, S. (2020). Man vs. machine? The impact of algorithm authorship on news credibility. *Digital Journalism*, 8(5), 548–562. <https://doi.org/10.1080/21670811.2020.1762102>

- Traquina, N. (2005). *Teorias do jornalismo: Por que as notícias são como são* (2.^a ed.). Insular.
- Thomson, T., Angus, D., Dootson, P., Hurcombe, E., & Smith, A. (2022). Visual mis/disinformation in journalism and public communications: Current verification practices, challenges, and future opportunities. *Journalism Practice*, 16(5), 938–962.
<https://doi.org/10.1080/17512786.2020.1832139>
- Wang, F., & Hannafin, M. J. (2005). Design-based research and technology-enhanced learning environments. *Educational Technology Research and Development*, 53(4), 5–23.
- Walth, B., Dahmen, N., & Thier, K. (2019). A new reporting approach for journalistic impact: Bringing together investigative reporting and solutions journalism. *Newspaper Research Journal*, 40(2), 177–189. <https://doi.org/10.1177/0739532919834989>

From paper to digital: Journey into imagination with Alba Digital Stories

Fabiola Camandona
University of Turin, Italy
fabiola.camandona@unito.it
0009-0001-4963-2637

Received: 15 November 2024

Accepted: 10 January 2025

Abstract

In a context where creativity and critical understanding of media are crucial, the Alba Digital Stories project explores digital storytelling as an innovative educational approach to media literacy. Using the ToonTastic app, preschool children develop storytelling and digital literacy skills in a playful and collaborative environment. Integrated into the DigComp 2.2 framework, the project promotes creative expression and critical analysis of media, encouraging children to share stories and interact consciously in the digital landscape. Final interviews revealed that while 10 out of 15 children found digital drawing more intuitive and rewarding than drawing on paper, all were excited to see their characters and scenarios come to life in digital format. The teachers observed how the use of the tablet enhanced the children's ability to explore aesthetic details and turn mistakes into new creative opportunities. This approach not only encourages individual creativity, but also allows the children to experiment as storytellers and little directors, developing confidence and skills in an environment that combines tradition and innovation.

Keywords *Digital storytelling, ToonTastic, Pedagogy, Children*

1. Introduction

In recent decades, the rapid spread of digital media has profoundly transformed people's learning, communication and interaction, especially among young people. In an increasingly connected world, the ability to understand, evaluate and create multimedia content is becoming more and more predominant. In line with DigComp 2.2, key areas of digital literacy and security, content production are identified. Indeed, today, becoming media literate does not only mean acquiring the technical skills to use devices and platforms, but also implies the development of critical thinking that enables children, young people, and adults to navigate the flow of digital information in a conscious and responsible manner (Hunt, Sun & al. 2023). The importance of media literacy is underlined by the increasing complexity of the media ecosystem, in which digital content multiplies and circulates on a global scale. In this context, literacy is not limited to passive reading, but promotes active participation in the creation of meaning and content. According to Robin (2016), 21st century skills, including digital Literacy, global Literacy and visual Literacy, are increasingly in demand, not only to interpret and analyse content but also to contribute productively to global digital conversations. Among the innovative educational approaches related to media literacy is digital storytelling (Ranieri, 2018; Pandian, 2020), a narrative practice developed in California, which involves the construction of a short narrative on video, combining recorded voice, images, music and other sounds (Lambert, 2006). However, the term digital storytelling

(DST) can encompass different modes of expression, such as gaming, interactive storytelling (Miller, 2019), and the wide range of personal representations shared on social media. The 'Alba Digital Stories' project is part of this framework with a view to sensitising children in the last year of preschool to the conscious use of technology by co-constructing an animated narrative, since a story is defined as such if it has a plot, a topic of interest and a certain level of involvement (Bruschi, 2017).

2. Why create digital stories?

Creating digital stories through digital storytelling methodology is an educational practice that goes beyond simple storytelling, supporting the development of children's cognitive, social and digital skills. This approach uses multimedia tools to build complex stories involving images, sounds and text narration, allowing children to explore and express their creativity in a personalised way. Digital storytelling is closely linked to media literacy, which is defined as the ability to access, understand and create media content in a critical and informed manner (European Commission, 2022). In a context where society increasingly demands digital skills to interpret and produce content, it is crucial that students learn to navigate, understand and use media in a reflective and responsible manner (European Commission, 2022; Dozza, 2017). The DigComp 2.2 framework, developed by the European Commission, is a guide to help educators, teachers and institutions integrate these skills in schools through five key areas: information management, communication, collaboration, content creation and digital safety. Digital storytelling fits well into these areas, offering students opportunities to construct complex meanings and interact with others in a meaningful way (Robin, 2008). Indeed, echoing the points made above, digital storytelling is capable of:

- Manage information. During the Alba Digital Stories project, children being preschoolers and not yet able to read, are able to select, organise and structure digital content - such as images, sounds and colours - to create a coherent story. The use of a simple storyboard, divided into three main steps, enabled them to define narrative scenes, introducing them to effective media management.
- Creating communication. Children and young people are often faced with creative uncertainty, finding it difficult to express their thoughts; instead, through digital storytelling, barriers are broken down. In fact, good participation and interaction with one's own group occurs even in the most difficult person (Miller, 2010). This narrative process becomes a means of developing social-emotional skills such as empathy and emotional awareness, which are fundamental elements in learning to explore one's own and others' emotions. Digital storytelling allows students to interweave stories with personal experiences, enhancing their understanding of disciplines, content, episodes, fostering fluency in storytelling (Gurrieri, 2018). Furthermore, in order to personalise the story and give it humanity, students can record their own voice, practising speech and improving their speaking skills (Nair, 2021). As will be explained in more detail in the following sections, the use of tools such as ToonTastic (an interactive application for creating animated stories) guides children in constructing plots, helping them understand

narrative structures, explore characters' emotions, and grasp the dynamics of the story. (Russell, 2010; Contreras, 2023).

- Collaboration. Digital storytelling stimulates critical thinking and problem-solving by requiring students to make narrative decisions and solve problems during the creation of the story, skills that will also be valuable in future contexts (Robin, 2008; Indrowati, 2024). Reviewing their own stories and receiving feedback from peers encourages self-assessment and autonomy, and helps children reflect on their progress and improve their skills. In addition, the multimedia nature of the methodology allows traditional learning barriers to be overcome, and gives students access to an alternative communicative channel to express themselves and share their stories, which does not have to be written (Benmayor, 2008; Choo, 2020). This possibility of personalisation makes DST a valuable resource for inclusive education, in line with the goals of educational equity promoted by the European Union.
- Addressing the issue of digital security. In this case, it was not an issue taken into consideration by the project as it is hoped that pre-schoolers will not use online tools without adult supervision. Nevertheless, for primary school children (from grade three onwards), it is important to make them aware of safe online behaviour, such as protecting their own data and respecting the information of others. For example, in story sharing activities, emphasis is placed on privacy and respect for digital property, teaching them to recognise the limits of access to their creations and the rules for responsible behaviour in a digital environment.

3. Alba Digital Stories

The Alba Digital Stories project was born out of the collaboration between the Department of Philosophy and Educational Sciences of the University of Turin, coordinated by Professor Manuela Repetto, and the 'La Casa dei Bambini Elena e Gabriella Miroglio' kindergarten and nursery school. The focus is on children attending the last year of preschool, with a view to fostering the development of narrative skills and media literacy through digital storytelling. The activities consisted of five meetings, each lasting two hours, using the ToonTastic application. The latter facilitates the creation of animated stories, structured in several scenes and divided into narrative phases such as introduction, conflict, climax and resolution. Google's application, still available on Android devices manufactured in 2018, features an intuitive interface, allowing children to easily proceed through the narrative sequence, customising characters and settings.

3.1. Project Goals

The main objectives of the Alba Digital Stories project were:

- To develop creativity and storytelling skills by stimulating children's imagination, encouraging them to invent original stories and experiment with building characters, settings and plots. Thanks to ToonTastic's guided structure, children were able to exercise their creativity in a playful and autonomous way.

- Introducing the basic concepts of media literacy. Through the use of the ToonTastic app, the children were familiarised with digital tools and discovered how to create and organise media content.
- Developing social and collaborative skills: The project involved sharing and discussion activities among the children, who worked both individually and in groups. The sharing of stories and mutual feedback encouraged collaboration, listening and respect for the ideas of others, promoting an inclusive and collaborative learning climate.

3.2. Project structure and methodology

The project was divided into five meetings and revolved around the story of 'Mr. Scarabocchio' by Jim Capobianco and Anna Laura Cantone (2020), which tells the story of a character, Mr. Scarabocchio, who lives in a chaotic and colourful world. Throughout the narrative, the protagonist tries to identify with objects, animals, characters, coming to the realisation that disorder and imperfection can be a source of beauty. Furthermore, emphasis is placed on free creativity and the importance of expressing oneself without fear of making mistakes, showing how art can come to life even through a simple doodle. The reading of the story was carried out together with the school educators, following which the meetings were structured as follows:

1. First meeting. In order to facilitate the writer's acquaintance with the class group, an ice-breaking activity was presented to introduce the guiding character: Pinetta, a small pine cone that serves as the representative icon of the project. Pinetta arose from the need to have an effective interlocutor to engage the specific target group of children. The use of a guiding character is a common choice in educational and popularisation projects, as it facilitates the transmission of complex content in an accessible and engaging way. Often these characters are children or teenagers, such as Talma in the ALMA Kids series¹ – The Adventures of Talma, or fictional figures, such as Paxi², the friendly alien created by ESA for the ESA Kids programme, aimed at children aged 6 to 10. Paxi is not only the star of a series of space-themed animated videos, but has become a real ESA mascot, also present on the International Space Station (Casu, 2023). The presence of a mascot for each project represents an added value capable of further engaging the target audience. Furthermore, through the request received directly from the guiding character, it was possible to sound out the uses and habits of the children with respect to the use of the tablet. Below are some of the phrases expressed by the children:

"I play the pizza and ice cream game" (P.)

"You can buy clothes". (A.)

"You can play, I play the recycling game". (C.)

"I watch videos, mum tells me not to watch them every day on Tik Tok." (F.)

2. Second meeting. In this phase, the children were guided through the discovery process of constructing a story, introducing the main components by using the images in the application

(sunrise, beginning - sunrise, climax - sunset, conclusion) starting with a fantasy pair: a monkey befriending a musician pinecone.

"We have seen the fantastic theme - the inspiration for a story - arise from a single word. In reality, one electric pole is not enough to arouse a spark, it takes two. The single word only acts when it encounters a second one that provokes it, forces it out of the rails of habit, to discover new capacities of meaning [...] In the fantastic pair, words are not taken in their everyday meaning, but freed from the verbal chains of which they are part every day. They are estranged, bewildered, thrown against each other in a sky never seen before. Then the best conditions are found to generate a story." (Rodari, , 2001, pp.17-19).

Next, the ToonTastic application was presented, leaving space for children to play and explore, encouraging the expression of ideas, emotions and personal narratives, and reinforcing the sharing of ideas. This approach reflects Dewey's concept of experiential learning: learning occurs when children are involved in activities that stimulate curiosity, imagination and problem-solving (Waks, 2024).

3. Third meeting. The focus was on how the increasing presence of digital technologies influences children's awareness of creative processes and the results of their productions. Through targeted activities, the meeting encouraged children to reflect on the value of their creations and how they can evolve during the creative process, even in the presence of errors or imperfections. Starting from the idea that

"Imperfection is a fascinating exploration of this worldview, from the fundamentals to the deeper meaning inherent in all its aspects". (Suzuki, 2023).

The central idea was to help children understand that creativity does not necessarily imply perfection, but is an evolving process that can transform what seems 'wrong' into something beautiful and meaningful (Nosari, 2021). During the meeting, the idea was discussed that a digital production, such as a story or a drawing, can be appreciated even when it has imperfections, and that these can become part of the aesthetic and emotional value of the final result. A central moment of the activity was the invitation for each child to share an experience in which an apparent mistake was transformed into a creative opportunity (Zhang, 2023). Some children shared personal examples, such as turning a 'small circle' into a 'coloured ball' or a 'yellow doodle' into a 'sun'. These experiences enabled the children to understand that mistakes can be creatively reinterpreted, fostering a more positive and flexible awareness of the creation process. Finally, the meeting also stimulated the children to consider that technology can make creativity an open and transformative experience. The children's comments - such as 'even if it's not perfect, it's still beautiful, we're not perfect either' - reflect a growing awareness of the possibility of improving and modifying one's own work. This view not only values imperfection as an integral part of creativity, but also encourages acceptance of oneself and one's evolving abilities. In this sense, digital storytelling becomes a context in which the process of personal growth and expression is valued above the perfect end result, fostering an educational environment in which students feel free to explore and adapt their work to their own visions and abilities (Anichini, 2021).

4. Fourth and fifth meetings. Towards the end of the project, the children were divided into small groups by the educators to develop and complete their narrative. In this phase, they identified the scenario, chose and drew the characters, and set up their interaction. An important step in which they had to negotiate meanings, collaborate, generating a shared plot. This process of negotiating meanings helped the children to develop listening and mediation skills, as they discussed ideas and chose the characters, the setting and how to move them in the environment (Figure. 1).



Figure 1. Children choose characters on ToonTastic

Once the storyline was established, the children worked on the creation of their drawings on paper and the subsequent transposition into digital format using ToonTastic. The children saw the transformation of their character from 2D to 3D. As shown in Figure 2, there was a good level of adherence to the scribbles drawn on paper represented in Figure 3 and Figure 4.



Figure 2. Children move the characters chosen and recreated in the application



Figure 3. A character drawn by a child and drawn again in the ToonTastic application. The character is indicated in Figure 2 by the letter A

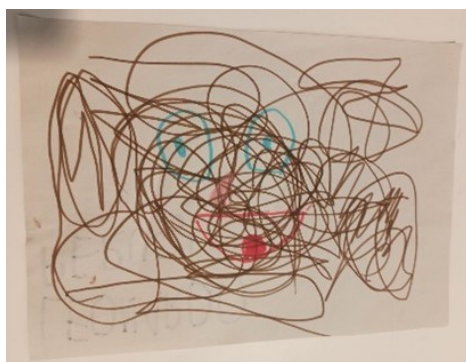


Figure 4. A character drawn by a child and drawn again in the ToonTastic application. The character is indicated in Figure 2 by the letter B

This phase allowed the children to visualise their creations through an interactive, animated medium, enabling them to see how ideas can also come to life in a digital format (Somigli, 2020). The possibility of animating the drawings strengthened their involvement and motivated them to make the character visually consistent with the image they had previously created on paper (Tindaon et al. 2023). Many of them chose to represent their characters directly in the ToonTastic app, which required attention to detail and stimulated digital creativity.

- Afterwards, each child had the opportunity to narrate a part of the story, recording their own voice. This storytelling exercise posed some challenges for the children, as they had to memorise and expose their piece of the story correctly, practising expression skills and narrative coherence (Sam & Hashim, 2022). The recording process was a significant moment for the children, as it confronted them with the need to communicate clearly, while staying within a timeline set by the application. The greatest difficulty was when one child was narrating the story, another member of the group was in charge of the visual part, moving and animating the characters in ToonTastic's digital space. This introduced children to spatial management, teaching them how to position characters and make them move on the screen to represent actions and interactions between characters. Manipulating characters in real time helped to make the narrative process more dynamic and allowed children to directly experience the concept of digital spatiality, which

is fundamental for understanding visual and scenic dynamics (Bottone & Zancato, 2021). This activity also contributed to strengthening their understanding of how visual choices influence the narrative experience, as they were able to observe first-hand how characters' movements and positions contribute to the construction of the scene. It was interesting to observe how even the more introverted children found room to participate by narrating an excerpt of a scene.

4. Double interviews: children and educators

At the conclusion of the meetings, short interviews were conducted with the children and their educators. From the children's answers, a diversity of perceptions emerged regarding the ease of digital versus traditional drawing. Out of 15 children interviewed, five found it difficult to draw on the tablet, while 10 reported that using the device was relatively easy, although only three had previous experience of digital drawing in the family environment. When questioned on the decoration between digital and paper drawing, 10 children preferred digital drawing, indicating it as 'more beautiful', while the remaining 5 preferred drawing on paper. This comparison between digital and traditional allows us to reflect on how children perceive the aesthetic quality and attractiveness of the digital medium compared to the physical one, suggesting a fascination for digital that could be further exploited in educational projects. In line with what the children expressed, the kindergarten teachers and headmistress were asked for their opinion on the enthusiasm they showed in graphically representing their doodles, first on paper and then via the tablet:

"I think that by participating in the various meetings, the children were enthusiastic about the fact that they were able, from their drawing, to redraw it on the tablet. In fact, at the beginning the children looked for the characters already pre-drawn by the ToonTastic application, but during the meetings, someone asked them to draw it because seeing their finger sliding on the screen and making the mark (and it is the same drawing that they drew on the paper), increased their expectations. In fact, from the first lessons everyone wanted to try out the characters that were already there, from the second lesson, after constructing their story, some then asked to draw their own 'doodle' because it was something that also brought their potential into play." (Tiziana Paola Borsa, director of 'La Casa dei Bambini Elena e Gabriella Miroglio').

'The tablet used in this way, on the other hand, is very constructive because they learn to interact, they do their story, they see but interact with that story. At least I think it's completely different. So now they will be proud, when they see it in total [the digital story], that they have chosen and created the characters, chosen their scenery, heard their voice. It's like they've created a film, starting from a story they built together.' (Carla Accossato, educator)

The educators noted that the digital format allows for the addition of nuances and details that children tend to overlook in traditional drawing, showing a more exploratory approach to the aesthetic possibilities offered by the tablet. However, the idea of drawing is still driven by factors such as the delivery and context of the story, making the content personal and connected to the themes.

"The underlying message is also extremely important to them. This is something we work on a lot in class, namely that from the mistake either something else can be corrected or something else can be born. This is something we as a class group work on a lot. So, in my opinion, even going a little bit to review what has been, right? I imagine that they all started again from the doodle, then they recreated it [digitally] and it's a nice re-living, in another format, of what the process was that they actually already had in hand. I can tell you in class that they were enthusiastic about this project. (Marta Pagnotta, educator).

The educators also discussed the influence of the tablet on the children's expectations of creative possibilities. According to them, the use of the tablet in activities such as digital storytelling, which involves interaction and narrative construction, is seen by the children as a tool that expands their ability to tell and share stories. One of the aspects most appreciated by the educators is precisely the possibility of a constructive use of the tablet, which allows the children not to limit themselves to being a passive user, but to become little directors of the story.

5. Conclusion

One of the main outcomes of the project was to improve the children's media literacy. Through digital storytelling, participants became more aware of how to use media and understand how digital content can be created, transformed and shared. The process of animating and recording stories made the experience highly engaging and encouraged participants to explore new ways of communicating. The combination of images, sound and storytelling allowed children to explore spatiality and the use of visual resources to effectively communicate emotions and meanings, stimulating critical thinking and problem solving skills (Dozza, 2017; Robin, 2008). Indeed, the theme of spatiality is explored in depth in this age group and is consolidated by the workshops already proposed in the curriculum. An example is the sewing workshop "The thread creates the fabric, the fabric creates the dress", during which the children play with wool threads to create wefts according to the horizontal and vertical arrangement of the threads, passing the thread over and under the fabric. Similarly, in the Digital Storytelling workshop, they consolidated this aspect by making the three-dimensional characters move, for example, in and out of the hut, over and under the ladder, and in unseen spaces. In addition, although some children found it difficult at first to respect each other's turns and ideas, and to be patient while waiting for everyone to interact with the tablet, digital storytelling also proved to be an effective tool for developing empathy and understanding of different points of view. Indeed, the children were able to identify with the characters and stories created by and with their peers, learning to negotiate meanings, share ideas and work together to achieve common goals. At each meeting, there was an awareness in each group that a richer story could emerge from the idea of one. This approach encouraged the development of social skills, such as active listening, and facilitated the inclusion of even the shyest children, who are often less inclined to participate in group activities. This collaborative dimension not only improved group dynamics but also boosted participants' self-esteem, encouraging them to express themselves freely and value their contribution. Stories are thus a powerful educational tool: through them, children can better understand themselves and the world around them, learn social skills and develop cultural understanding in a playful and stimulating environment (White, Gaffney et al. 2024). These aspects are consistent with socio-cultural perspectives on learning, according to which children create personal meanings through their interactions with others (Bruner, 1986; Wells, 1986). Personal stories are not only narratives of experience, but also opportunities to explore identities and relationships. Children told stories that reflected their interests, feelings and experiences, demonstrating how narrative can be a

powerful tool for self-expression, exploring their own culture and that of others (Ministry of Education, 2017, p.5).

Acknowledgements

We thank the director Tiziana Paola Borsa of 'La Casa dei Bambini Elena and Gabriella Miroglio' in Alba for the trust and opportunity provided. We thank the educators Carla Accossato, Marta Pagnotta, Michela Tortoroglio and all the children in the 'flowers' section for their enthusiasm and participation. We would like to thank the trainee Alessia Seziam for her support in the final stages of the course.

References

- Anichini, A., Di Bari, C., Dalbon, M., & Lunel, F. (2021). *Narrazione digitale per l'infanzia*. Ricerca IUL, 2 (4), 280-293.
- Benmayor, R. (2008). Il digital storytelling come pedagogia distintiva per le nuove discipline umanistiche. *Arti e studi umanistici nell'istruzione superiore*, 7(2), 188-204.
- Bottone, M., Giromini, D., & Zancato, F. (2021). Piccoli mondi di pongo. Manipolazione e passo uno nella scuola dell'infanzia. *IUL Research*, 2(4), 236-244.
- Bruner, J. (1986). *Actual Minds, Possible Worlds*. Harvard University Press.
- Bruschi, B. (2017). *Ludodigitalstories. Un progetto per raccontare storie alla comunità*. Franco Angeli.
- Choo, YB, Abdullah, T., & Naw, AM (2020). Narrazione digitale vs. narrazione orale: un'analisi dell'arte di raccontare storie oggi e allora. *Universal Journal of Educational Research*, 8 (5A), 46-50.
- Commissione europea. (2022). *Orientamenti per gli insegnanti e gli educatori volti a contrastare la disinformazione ea promuovere l'alfabetizzazione digitale*. Estratto da <https://ec.europa.eu>.
- Contreras, EL (2023). *Trasformare lo sviluppo linguistico per MLL con UDL e Toontastic 3D*. WAESOL Educator, 48 (2), 45-48.
- Casu, S., Deiana, Luca, A., Simbula, F., & Melis, M. (2023). *Blu e il cielo: un progetto didattico sperimentale per la scuola dell'infanzia*. OA Cagliari.
- Dozza, L. (2017). *Costruttivismo e apprendimento attivo: Approcci educativi nelle università per bambini*. Franco Angeli.
- Gauntlett, D. (2011). *Making is Connecting: il significato sociale della creatività, dal fai da te e dal lavoro a maglia a YouTube e Web 2.0*. Malden, MA: Polity.
- Gurrieri, L., & Drenten, J. (2019). Visual storytelling and vulnerable health care consumers: normalising practices and social support through Instagram. *Journal of Services Marketing*, 33(6), 702-720.. J. Serv. Mark., 33, 702-720.
- Hunt, CL, Sun, K., Dhuliawala, Z., Tsukiyama, F., Matkovic, I., Schwemler, Z., ... & Yip, J. (2023, giugno). *Progettare insieme, a chilometri di distanza: un'avventura di telepresenza da tavolo longitudinale nella progettazione condivisa online con i bambini*. In Atti della 22a conferenza annuale ACM Interaction Design and Children (pp. 52-67).
- Indrowati, M. (2024). Migliorare le capacità di valutazione attraverso l'apprendimento basato sui problemi capovolti con l'attività di narrazione digitale: una revisione sistematica. *Journal of Higher Education Theory & Practice*, 24 (1).
- Merjovaara, O., Nousiainen, T., Turja, L., & Isotalo, S. (2020). Digital stories with children: Examining digital storytelling as a pedagogical process in ECEC. *Journal of Early Childhood Education Research*, 9(1).
- Miller, CH (2019). *Digital Storytelling 4e: una guida per i creatori all'intrattenimento interattivo*. CRC

Press .

- Miller, LC (2010). *Make me a story: insegnare a scrivere attraverso la narrazione digitale*. Stenhouse Publishers .
- Ministry of Education (2017) *Te WhāRiki: He WhāRiki MāTauranga Mō Ngā Mokopuna o Aotearoa. Early Childhood Curriculum*. Wellington, New Zealand: Author.
- Nair, V., & Yunus, MM (2021). Una revisione sistematica dello storytelling digitale nel miglioramento delle capacità di parlare. *Sustainability*, 13 (17), 9829.
- Nosari, S. (2021). L'inatteso pedagogico del soggetto "a responsabilità illimitata". *STUDIUM EDUCATIONIS*, 2 , 87-93.
- Pandian, A., Baboo, SB, & Yi, LJ (2020). Digital storytelling: coinvolgere i giovani nella comunicazione per l'alfabetizzazione ai media digitali. *Jurnal Komunikasi: Malaysian journal of communication*, 36 (1), 187-204.
- Rahiem, M. D. (2021). Storytelling in early childhood education: Time to go digital. *International Journal of Child Care and Education Policy*, 15(1), 4.
- Raj, W. M. J. (2021, November). 3 Promoting Students' Speaking Fluency and Social Collaboration through Toontastic 3D. In *10th International English Language Teaching Conference* (p. 27).
- Ranieri, M., & Bruni, I. (2018). Digital and media literacy in teacher education: Preparing undergraduate teachers through an academic program on digital storytelling. In *Handbook of Research on Media Literacy in Higher Education Environments* (pp. 90-111). IGI Global.
- Robin, B. R. (2008). Digital storytelling: A powerful technology tool for the 21st century classroom. *Theory into practice*, 47(3), 220-228.
- Robin, B. R. (2016). The power of digital storytelling to support teaching and learning. *Digital education review*, (30), 17-29.
- Rodari, G. (2001). Grammatica della fantasia. Einaudi .
- Russell, A. (2010). *ToonTastic: una rete globale di narrazione per bambini*, di Kids. Università di Stanford .
- Sam, I., & Hashim, H. (2022). Percezioni degli alunni sull'adozione e l'uso di Toontastic 3D, un'applicazione di narrazione digitale per l'apprendimento delle capacità di parlare. *Creative Education*, 13 (2), 565-582.
- Sardo, M. (2023). *Gamification: modelli di progettazione, rendimento scolastico e valore pedagogico*.
- Scolari, C. A. (2019). Dalla alfabetizzazione mediatica all'alfabetizzazione transmediale. *Digitcult*. 2019; 4 (1): 37-46. DOI: 10.4399/97888255263184.
- Somigli, P. e Parricchi, MA (2020). *Bambini all'università: Diario di un'esperienza*. Franco Angeli
- Suzuki, N. (2023). Wabi Sabi: *La filosofia dell'imperfezione*. Edizioni Mediterranee .
- Tindaon, J., Sinaga, ERL, Siregar, DEB, Sinaga, RJ, & Suka, SNBG (2023). La socializzazione dell'applicazione 3D di animazione Toontastic suscita l'interesse crescente degli studenti di classe V della scuola elementare statale 040447 Kabanjahe. *Jurnal Pengabdian Masyarakat Bestari*, 2 (9), 837-842.
- Waks, LJ (2024). John Dewey sul gioco: teoria e pedagogia. *American Journal of Play*, 16 (1), 10-31.
- Wells, G. (1986). *Children learning language and using language to learn*. Heinemann Educat. Books.
- White, A., Gaffney, J. S., & Hedges, H. (2024). Toddlers as active, competent story weavers: Lexie's story. *Journal of Early Childhood Literacy*, 24(1), 165-190.
- Zhang, Q., & Fiorella, L. (2023). An integrated model of learning from errors. *Educational Psychologist*, 58(1), 18-34.

¹ <https://www.almaobservatory.org/en/publications/the-adventures-of-talma/>

² https://www.esa.int/kids/it/chi_e_Paxi/Paxi

Fostering Media Literacy through Digital Content Creation: An Educational Initiative at the Buck Festival of Foggia

Guendalina Peconio
*Università degli studi di Foggia,
Italy*
guendalina.peconio@unifg.it
0000-0003-2858-6923

Michele Ciletti
*Università degli studi di Foggia,
Italy*
michele_ciletti.587188@unifg.it
0009-0004-3829-8866

Giusi Antonia Toto
*Università degli studi di Foggia,
Italy*
giusi.toto@unifg.it
0000-0001-5538-5858

Received: 15 November 2024

Accepted: 27 February 2025

Abstract

In the contemporary educational landscape, digital citizenship and media literacy constitute essential competencies for preparing students to engage critically and consciously with digital media. This study describes an experimental educational initiative conducted at the Buck Festival in Foggia, aimed at developing digital competencies and multimedia expression skills among middle school students. Drawing upon the Theory of Change framework proposed by McDougall & Rega (2022) the project identifies the interventions required to foster transformative learning, whereby students acquire not only technical skills but also civic awareness and autonomous expression capabilities.

The project's primary objective was to actively engage students in creating digital content, including podcasts, blogs, and web TV reportage, connected to festival events. The adopted methodology, both experiential and collaborative in nature, employed focus groups with guiding questions to gather data on students' perceptions regarding the project's educational impact.

Preliminary findings indicate enhanced digital competencies and civic engagement, aligning with the transformative perspective proposed by the Theory of Change. Future research directions encompass a longitudinal analysis of the same student cohort and comparative studies with other educational institutions to assess the model's applicability across different contexts and evaluate the effectiveness of the educational pathway.

Keywords *Digital content creation, Podcasting, Citizen journalism, Media literacy, Media education, Digital skills*

1. Introduction

For fourteen years, the city of Foggia has hosted the Buck Festival, an event entirely dedicated to children's and young adult literature. Each October, for one week, the city's cultural heritage sites – libraries, museums, art galleries – welcome hundreds of children and young people as protagonists of educational activities and events. National and international authors and illustrators enliven the Festival through animated readings, creative workshops, theatrical performances, and a publishing fair. In 2024, the overarching theme was storytelling, featuring over one hundred and fifty scheduled events, involving twenty-two guests and numerous local associations and volunteers.

The Festival is not merely a cultural event but functions as an educational platform aimed at promoting literacy and reading among younger generations. Reading and narrative play crucial roles in young people's cognitive, emotional, and social development. Recent studies demonstrate that early and continuous exposure to meaningful narratives correlates with enhanced comprehension abilities,

enriched language skills, and more developed empathic capabilities (Suggate, 2016). Furthermore, storytelling serves not only as an effective educational tool but also as a practice that strengthens cultural identity and belonging (East et al., 2010). In an increasingly digital world, traditional and multimedia narrative modes integrate to support the development of transversal competencies and multilevel literacy.

The initiative to connect the Buck Festival with an educational activity designed for middle school students aligns perfectly with these dynamics. The project, focused on creating multimedia communication content and promoting digital literacy, corresponds with European Union recommendations (2018) on developing digital and cultural competencies as fundamental pillars of active citizenship. According to TPACK (Technological Pedagogical Content Knowledge) principles, integrating digital tools in cultural and creative contexts enhances not only students' technical abilities but also their capacity to interpret and produce meaningful content (Mishra & Koehler, 2006).

In designing the activity, the Festival was not conceived as a mere backdrop but as a structuring element of the educational intervention. The connection with real-world context is recognized as a crucial lever for motivation and meaningful learning. As Fredricks, Blumenfeld, and Paris (2006) assert, student engagement is maximized when educational activities are perceived as relevant and connected to their world. Involving young people in local cultural heritage sites, combined with direct experience of a public event like the Buck Festival, enhanced their interest by providing an authentic and stimulating learning environment.

The multimedia content produced by participants served a dual purpose: documenting and communicating Festival activities while demonstrating how cultural heritage can be enhanced through contemporary languages and tools. This approach aligns with recent theories on situated and collaborative learning, which emphasize the role of social interactions and context in acquiring new competencies (Bloch et al., 1994) (Gee, 2003).

The Buck Festival demonstrates how local events can transform into powerful educational tools, capable of uniting creativity, technology, and cultural heritage. Such projects not only address the educational needs of new generations but also strengthen the bond between youth, community, and territory, promoting integral development that combines cognitive, emotional, and social competencies.

2. Media Literacy and Digital Cultural Heritage Education

Cultural heritage represents a strategic educational resource for student development, capable of enriching the learning journey through authentic and contextualized experiences. Integrating digital technologies in the appreciation and enhancement of cultural heritage transforms education into a process of knowledge co-construction, based on students' active participation and civic engagement (Borgia et al., 2019) (Luigini & Panciroli, 2018). Contemporary pedagogy recognizes how these digitally-supported experiences can foster not only cognitive learning but also experiential and reflective learning, wherein students can "dialogue" with culture, exploring and reinterpreting heritage elements through a modern and participatory lens (Giglietto et al., 2019) (Casonato et al., 2022).

This approach aligns with Jenkins' (2008) concept of "participatory cultures," which centers educational experience on students' ability to utilize digital tools such as web and social media for creative expression and development of civic responsibility and belonging. Through these tools, young people become conscious actors and protagonists of their own education, experiencing learning as a social and cultural experience connected to contemporary world issues.

In this context, media education and digital literacy emerge as key competencies for understanding and responsibly utilizing technologies applied to cultural heritage. Media literacy, as described by Potter (2004), refers to the ability to access, analyze, evaluate, and create content—essential skills for critical and conscious interpretation of media and digital content. In educational settings, this competency enables students to develop analytical and reflective abilities that help them evaluate information reliability, understand production dynamics, and question source origins.

New media literacy enriches the educational journey with additional expressive tools, enabling students to develop and produce interactive and multimedia content. It introduces an encoding aspect that extends beyond information decoding, encouraging students to create original content, shaping their vision through video, images, and sound. This competency stimulates creative expression and supports autonomous knowledge construction, fundamental for learning that values each student's unique contribution and ensures genuine inclusivity (Rivoltella, 2022).

Digital media literacy encompasses three principal dimensions essential for building digital cultural heritage education: critical, ethical, and aesthetic (Valgolio, 2021) (Rivoltella, 2022). The critical dimension enables students to exercise thorough and conscious content interpretation, developing the ability to evaluate information reliability and source authenticity. The ethical dimension refers to awareness of one's digital actions and the importance of maintaining respectful and responsible behavior. The aesthetic dimension promotes appreciation of digital expressive forms, encouraging youth to use images, video, and sound to communicate effectively and express their vision creatively.

In secondary education, these competencies are crucial not only for navigating the digital context safely and critically but also form part of civic education aimed at developing informed and responsible citizens. Information technologies have revolutionized civic participation, giving rise to digital citizenship, which implies using digital technologies for active and responsible engagement in social, political, and cultural dynamics (Sudulich, 2008).

Internet has become a crucial resource for accessing civic and political information, providing content from governments, community organizations, interest groups, political campaigns, and media outlets. However, this increased accessibility requires specific competencies for responsible digital navigation and informed decision-making (Hobbs, 1998). These competencies, essential for digital citizenship, enable individuals to benefit not only personally and professionally but also socially, accessing reliable news that creates opportunities for themselves and their families.

Media literacy and digital literacy education address these needs by providing students with fundamental competencies for active and responsible participation in contemporary democratic society.

These skills include reading and writing, listening and dialogue, knowledge of new technologies, critical viewing of visual content, and the ability to create messages through various digital tools (Potter, 2004). Digital messages or “texts” may include languages, images, graphic design, icons, sounds, and music, representing a complex form of symbolic communication requiring a critical and conscious approach for full comprehension and ethical use (Buckingham, 2003).

Furthermore, media literacy and digital literacy education, with its emphasis on critical and reflective competencies, provides students with tools to evaluate messages concerning public agenda and engage with philosophical, social, and democratic values. These reflective abilities not only promote critical thinking but also encourage the formation of an informed and active citizenship, capable of participating in social life constructively and responsibly.

3. Fostering Media Literacy through digital content creation

Research has demonstrated that one effective approach to promoting digital literacy involves direct experimentation with digital communication content creation tools, such as podcasts, radio broadcasts, TV programs, and blog articles (Rivoltella, 2020). This approach consequently fosters the development of critical thinking and responsible consumption regarding similar content created and distributed by others (Hobbs & Jensen, 2022). In a society where individuals are increasingly interconnected from an early age, and where ambiguous and disinformative media content proliferates (Buckingham, 2019), such strategies for promoting informed communication are fundamental, particularly in educational contexts.

Direct content production offers additional benefits. First, it promotes reflection on the mechanisms underlying various phases of media content ideation, structuration, and distribution. Second, by directing efforts toward culturally or educationally relevant topics, it can spark creators’ interest in promoting these themes, potentially leading to future independent engagement in citizen journalism, blogging, and podcasting. However, merely encouraging young people to freely create and publish media material is insufficient. Without guidance on good online communication practices, there is a risk of inadvertently contributing to disinformation or unethical practices. Instead, a specific curriculum is essential for effectively teaching virtuous communication strategies (Rivoltella & Rossi, 2024). Simultaneously, technical and accessibility components cannot be underestimated. Teaching content creation methods that are not easily replicable, either due to resource availability or difficulty level, would preclude the possibility of stimulating autonomous continuation of learned practices. Focusing on free, open-source, and user-friendly tools helps ensure that individual educational experiences transcend their specific context and become the foundation for future established practice.

Specifically, podcasting represents one potential theme for such an initiative. By nature, podcasts are purely auditory content, often organized into episodes, characterized by primarily narrative or opinion-based structures (McHugh, 2016). Positioned between talk shows and radio programs, they have gained recent popularity through streaming platforms, particularly among younger generations (Van den Bulck & Roskos-Ewoldsen, 2020). Writing and designing podcasts requires multiple digital

competencies. Basic storytelling structure is essential: distinguishing one's podcast and making it engaging requires clear identity and effective narrative techniques. Beyond this, podcasting demands performance skills: clear and pleasant voice, functional content presentation, and engaging personality are just some success conditions. Accurate research for content development is also indispensable, especially for narrative podcasts. Technical skills include basic recording techniques, audio editing (including music selection and mixing), and online publication through streaming platforms. For videopodcasts, additional video recording and editing competencies are required. Fortunately, minimal requirements include modern smartphones capable of effective recording, potentially aided by low-cost portable microphones, and high-quality video recording. Free and open-source editing software is available for both PC and smartphone platforms, and online content publication is simple and cost-free.

Web TV content follows a similar nature. As a digital evolution of cable television, web TV offers the advantage of free online availability through simple internet access. Content-wise, it differs from videopodcasting primarily through more predominant visual medium utilization: reports, in-depth analysis, and interviews can be conveyed naturally visually, while podcasts must consider their audio-only audience.

Blogging, while structurally different, yields similar results. Among the earliest forms of digital self-expression, it involves publishing brief articles on an online platform (Nardi et al., 2004). Social media's advent has reconceptualized it: platforms like Twitter essentially represent collective microblogging environments where users share ideas and opinions in brief formats on a common platform. Required competencies primarily involve writing: blog posts share formal requirements with newspaper articles.

Interviewing serves as a common thread among these formats: whether audio or video, it represents an excellent opportunity for dialogue, where the interviewer must engage with external perspectives to enrich their podcast, program, or blog content. This requires considerable preliminary research to ensure interesting and relevant interviews, along with strong presentation, improvisation, and entertainment skills.

The educational experience of digital content creation can be enriched by framing it within a context of interest to participants. Emotional and intellectual engagement, crucial in education generally (Tyng et al., 2017), can develop intrinsic motivation potentially making the educational project more fruitful (Howard et al., 2021). This perspective underlies the initiative to establish a youth multimedia editorial team documenting the 2024 Buck Festival events in Foggia.

4. Implementation of a Digital Content Creation Workshop: A Case Study with Middle School Students

Drawing upon the aforementioned theoretical principles and practical considerations, a theoretical-practical educational activity was designed for middle school students centered around the Buck Festival context. Specifically, 11 students from 2 schools in Foggia participated in the project. The students, informed by their referring teachers, volunteered spontaneously to participate in the activities.

The overall project was developed using McDougall and Rega's (2022) theory of change as a theoretical framework of reference. Details are outlined in Table 1.

Table 1. Theory of Change framework

	Needs	Inputs	Outputs	Outcomes	Impacts
Access	Students need access to digital content creation tools and platforms; opportunities to engage with cultural events and digital media production; guidance on using digital tools effectively	Access to University web radio and TV equipment; Training on software (Audacity, DaVinci Resolve, WordPress); Access to Festival events and cultural spaces; Technical guidance from educators	Technical projects made by students: podcasts, interviews, blog articles	Students gain practical experience with digital media tools, develop technical skills in audio/video production, learn to navigate digital publishing platforms; Increased confidence in using digital media tools	Sustained access to digital creation tools through knowledge of free/open-source options; Long-term engagement with digital content creation; Bridge built between students and cultural institutions
Awareness	Students need critical understanding of digital media, awareness of content creation processes, understanding of media representation	Theoretical training on media formats; Guidance on content planning and production; Exposure to professional authors and cultural events; Mentoring on media literacy concepts	Reflections shared during focus group	Enhanced understanding of media production processes; Improved critical analysis skills; Greater awareness of content quality and credibility; Better understanding of different media formats	Development of critical media consumption habits; Increased awareness of media representation issues; Long-term engagement with cultural content
Capability	Students need practical content creation skills, collaborative work experience, autonomous decision-making abilities	Hands-on training sessions; Group work opportunities; Independent project choices; Technical and creative guidance	Technical projects made by students: podcasts, interviews, blog articles	Developed technical production skills; Enhanced collaborative abilities; Improved creative expression capabilities; Increased autonomy in content creation	Sustained content creation practices; Development of personal media projects; Enhanced digital citizenship capabilities
Consequences	Students need to understand impact of media creation; Community needs quality cultural content; Festival needs documentation and promotion	Guidance on ethical content creation; Platform for publishing student work; Connection with cultural events; Real audience engagement opportunities	Public sharing of created content as official Festival news	Understanding of content impact; Contribution to cultural documentation; Enhanced community engagement; Development of ethical content practices	Long-term cultural participation; Sustained ethical media practices; Positive contribution to digital ecosystem; Enhanced cultural documentation practices

The project included an initial theoretical training phase, followed by substantial practical experience. The first day, lasting approximately 5 hours, was conducted at the University of Foggia's Web Radio and Web TV facility. During this session, participating students first received general information about the characteristics of podcasts, television programs, and blogs. They then utilized available equipment to familiarize themselves with technical aspects of digital content creation. Specifically, they experimented with audio recording using professional microphones, video recording with cameras, direction, audio editing (using Audacity, open-source software), video editing (using DaVinci's Resolve, free software), and blog management (using Wordpress.com, also free). Participants also practiced program and podcast design, dividing into three groups. This division was encouraged to promote active participation according to individual interests and aptitudes in content creation.

The following two days took place across various locations in Foggia: using a computer lab as an operational base, where content was edited and uploaded online, groups moved between different cultural venues (museums, art galleries, libraries) where Buck Festival activities were occurring. Demonstrating considerable autonomy, they freely chose events aligned with their interests. Visiting authors, festival staff, and even passersby were involved in content creation. Among the interviewed authors of national and international renown were Simone Rea, Gek Tessaro, Sonia Maria Luce Possentini, and many others. The second practical day was entirely dedicated to the Festival's roundtable discussion, attended by all guests and organizers.

The final day was primarily devoted to finalizing content recorded during previous activities. Additionally, in the project's last hour, a focus group was conducted with all students, aiming both to gather information about participants' opinions of the project and to obtain feedback for future activity modifications. Complete content was published partly on the University of Foggia's Web Radio and Web TV platforms, and partly on the Festival's dedicated blog. Students were provided with access credentials for the latter, with encouragement to continue freely publishing content related to children's literature.

5. Qualitative analysis

Building on the detailed account of the workshop's design and implementation, it is essential to further explore how these innovative educational interventions resonated with the participants. The previous sections have delineated the strategic integration of digital tools and cultural contexts aimed at fostering media literacy and civic engagement. In order to comprehensively assess these outcomes, the subsequent qualitative analysis delves into the nuanced reflections, emotional responses, and collaborative dynamics manifested during the project. This integrative discussion not only contextualizes the technical and pedagogical achievements described earlier but also illuminates the emergent personal and collective perceptions that underscore the transformative potential of digital content creation in educational settings.

The qualitative analysis of the focus group conducted in the present project revealed a series of significant reflections on the techniques of interviewing, podcasting, and editing. Through targeted questions, the aim was to explore the level of digital competencies and media literacy, as well as to collect feedback regarding the overall experience and the value of the activity for the local community. This approach is in line with Hobbs (1998), who emphasizes the importance of developing critical skills in young people for responsible media navigation.

The focus group was structured around specific questions, including those concerning the perception of the techniques learned and their usefulness. The questions included: “What do you think of the techniques you have learned (interviews, podcasts, articles, editing)?” This question enabled the participants to reflect on the characteristics of the various formats and on their level of digital competencies, in accordance with Rivoltella’s (2020) guidelines on the importance of direct content production.

Other questions, such as “What did you like most about the overall experience and what would you change?”, were intended to gather useful information for potential future modifications of the project. Additional inquiries addressed the difficulties encountered during the creative process and the interest in pursuing similar experiences independently, thereby contributing to an exploration of the potential for developing new content. Finally, attention was given to group work and to the impact of the festival on the city, with the intention of assessing cultural awareness and the importance of communication.

The primary objective of the investigation was twofold: on the one hand, to assess the effectiveness of the communication techniques learned by the participants, and on the other, to understand the impact of the activity on their approach to citizen journalism and cultural awareness. It was also intended to gather indications for any potential future modifications of the project.

The categorical analysis was carried out in several steps, inspired by Grounded Theory Charmaz (2006). Initially, familiarization with the data was achieved through repeated readings of the focus group transcripts. Subsequently, codes were generated by identifying significant segments of text. These codes were then grouped into themes, leading to the emergence of the main categories. Finally, the themes were defined and named to accurately reflect the content expressed by the participants.

The categories that emerged from the analysis are as follows:

- Inclusion and Participation

The focus group evidenced a strong sense of inclusion. The participants felt welcomed and actively involved in the project. The expressions of enthusiasm and active participation suggest that the environment was conducive to cooperation, in line with Jenkins’s (2006) theories on participatory cultures.

- Difficulties/Successes Encountered During the Process

The narratives reveal both difficulties—such as the initial anxiety when conducting interviews—and successes, such as the creation of engaging and significant content. The testimony of overcoming

anxiety demonstrates how the group supported its members in becoming more confident, in accordance with the change theory of McDougall and Rega (2022).

- Activities

The activities undertaken—such as the creation of articles, podcasts, and video editing—are described with enthusiasm. This suggests that the various techniques had a positive impact on the participants' learning and creativity, as evidenced by Rivoltella (2020).

- Emotions and States of Mind

The emotions shared by the participants reveal a mix ranging from joy to satisfaction. The repetition of phrases such as “it was very enjoyable” underscores the importance of fun in the learning process, a crucial aspect according to Deci and Ryan's (1985) intrinsic motivation theories.

- Impact of the Festival on the Territory

The festival is perceived as an opportunity to enhance the city's reputation, countering negative prejudices. The participants recognize the cultural significance of the event and its potential for social inclusion, in line with Sudulich (2008) ideas.

- Ideation/Innovation – Inspiration

The discussions reveal that the participants felt inspired by the activities undertaken. The idea of producing podcasts and interviews is seen as a way to express individual creativity and acquire new skills, supporting Rivoltella's (2022) recommendations on education for digital citizenship.

- Cooperation/Confrontation

Group work is emphasized, with the participants feeling more connected through collaboration. However, there are also moments of tension, highlighting the complexity of group dynamics, as described by Vygotsky (1978).

- Self-Perception

The participants express an increased awareness of their own abilities. Personal growth is a recurring theme, with some feeling more comfortable in public speaking and collaboration, reflecting the importance of agency as proposed by Bandura (1999).

- Practical Feedback from the Podcast

The practical experiences with podcasting are described as formative. The participants acknowledge both the utility of the created content and its capacity to reach a broader audience, thereby supporting the idea that the production of digital content can amplify educational impact (Hobbs & Jensen, 2022).

- Hobbies

Extracurricular activities and personal interests emerge in the discourse, suggesting that the project stimulated curiosity and creativity beyond the school context—a key factor for student engagement (Tyng et al., 2017).

It is thus possible to highlight that the analysis demonstrates how the experience of citizen journalism can not only enhance the practical skills of the participants but also stimulate a deeper reflection on their own cultural identity and on the value of information within the community, in line with the recommendations of the European Union (2018) for the development of digital and cultural competences.

6. Conclusions and future perspectives

The educational project developed for the Buck Festival in Foggia represents a significant milestone in the evolution of pedagogical practices aimed at promoting digital and multimedia citizenship competencies among middle school students. The direct involvement of students in creating digital content linked to a real event enabled the integration of technical, communicative, and critical dimensions into a unified educational experience. This approach responds to the principles of “new media literacy” (Rivoltella, 2020), which advocates the need to educate young people to understand and use digital media not merely as passive consumers but as conscious and creative content producers.

The educational activity encouraged active participation, enriching the learning journey with an authentic and meaningful experience that promotes responsible digital citizenship development (Sudulich, 2008). The project aligns with social constructivist theories, emphasizing the importance of situated learning and collective knowledge construction (Vygotsky, 1978); through group work and interaction with adults and peers, students developed a sense of agency—awareness of their power to act and impact reality (Bandura, 1999). The opportunity to explore and utilize digital technologies for self-expression fostered the development of fundamental transversal competencies such as collaboration, problem-solving, and critical thinking. These competencies, often overlooked in traditional educational contexts, prove essential for civic education and democratic participation, providing students with necessary tools for active and responsible societal interaction (Hobbs, 1998).

The Buck Festival experience also demonstrated the importance of stimulating students’ cognitive and emotional engagement through authentic and situated tasks. Aligned with intrinsic motivation theories (Deci & Ryan, 1985), the project leveraged activity meaningfulness, contributing to active involvement and personal fulfillment. Students had the opportunity to report on their immediate reality, assuming roles as reporters and critical observers of their environment. This facilitated not only content learning but also the development of intrinsic motivation which, according to recent research, is crucial for long-term success and meaningful learning (Hattie & Donoghue, 2016).

In light of preliminary results, the project's next steps will be fundamental for consolidating and deepening emerging conclusions. The first subsequent phase will involve analyzing data collected through a focus group conducted with participants, using ten structured questions on key themes to evaluate experience perception and acquired competencies. This focus group will be analyzed through thematic analysis and sentiment analysis techniques, utilizing advanced tools like T-Lab and Python, which enable exploration of affective and cognitive dynamics in student feedback. These tools will allow a more nuanced understanding of their experience, highlighting not only acquired competencies but also emotions and reflections arising from the project.

From a longitudinal perspective, the project plans to repeat the experience with the same students over time, monitoring their competency evolution and personal development. This longitudinal approach is supported by psycho-pedagogical studies demonstrating how long-term educational experiences can promote stable and profound growth in socio-emotional and digital competencies (Zimmerman, 2000). Through continuous monitoring, it will be possible to evaluate not only the immediate impact of the experience but also its potential contribution to individual growth and responsible digital citizenship construction.

Simultaneously, the project will expand transversally, involving students from other educational institutions. This comparative approach will explore how different educational contexts may influence digital competency and citizenship learning. Comparing student groups from different schools will help understand whether and how factors like locality, school resources, or socio-economic level may affect learning modalities and outcomes. Such data will offer valuable insights for developing educational interventions adapted to various contexts' specificities, aligned with principles of educational equity and inclusivity.

In this scenario, adopting a psycho-pedagogical approach focused on promoting digital citizenship and students' intrinsic motivation represents an important step toward education that not only values technical competencies but promotes personal growth and social participation. The Buck Festival project could thus constitute a replicable model of digital civic education, contributing to the formation of aware and active citizens. In an increasingly digitalized world, where technologies transform ways of communicating, gaining information, and participating in public life, this educational initiative represents an essential investment for developing a democratic and inclusive society.

References

- Bandura, A. (1999). Self-Efficacy: The Exercise of Control - By Albert Bandura. In *Journal of cognitive psychotherapy*. (Vol. 13, Issue 2).
- Baoill, A. (2008). Jenkins, H. (2006). Convergence Culture: Where Old and New Media Collide. In *Social Science Computer Review* (Vol. 26, Issue 2).
<https://doi.org/10.1177/0894439307306088>
- Bloch, M., Lave, J., & Wenger, E. (1994). Situated Learning: Legitimate Peripheral Participation. *Man*, 29(2). <https://doi.org/10.2307/2804509>

- Borgia, E., Di Berardo, M., Occorsio, S., & Rainone, G. (2019). *Minilemmi della cultura - Una rubrica per l'educazione al patrimonio*. Gangemi.
- Buckingham, D. (2003). Media Education and the End of the Critical Consumer. In *Harvard Educational Review* (Vol. 73, Issue 3).
<https://doi.org/10.17763/haer.73.3.c149w3g81t381p67>
- Buckingham, D. (2019). *The Media Education Manifesto*. Polity.
- Casonato, C., Vedoà, M., & Cossa, G. (2022). *Discovering the everyday landscape: A cultural heritage education project in the urban periphery*. LetteraVentidue Edizioni.
- Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage.
- Council of the European Union. (2018). Key competences for lifelong learning: A European Reference Framework. *Official Journal of the European Union*, 2.
- Deci, E. L., & Ryan, R. M. (1985). Intrinsic Motivation and Self-Determination in Human Behavior. In *Intrinsic Motivation and Self-Determination in Human Behavior*.
<https://doi.org/10.1007/978-1-4899-2271-7>
- East, L., Jackson, D., O'Brien, L., & Peters, K. (2010). Storytelling: an approach that can help to develop resilience. *Nurse Researcher*, 17(3).
<https://doi.org/10.7748/nr2010.04.17.3.17.c7742>
- Gee, J. P. (2003). What video games have to teach us about learning and literacy. *Computers in Entertainment*, 1(1). <https://doi.org/10.1145/950566.950595>
- Giglietto, D., Claisse, C., Cioffi, L., & Lockley, E. (2019). Bridging cultural heritage and communities through digital technologies: Understanding perspectives and challenges. *ACM International Conference Proceeding Series*.
<https://doi.org/10.1145/3328320.3328386>
- Hattie, J. A. C., & Donoghue, G. M. (2016). Learning strategies: a synthesis and conceptual model. *Npj Science of Learning*, 1(1). <https://doi.org/10.1038/npscilearn.2016.13>
- Hobbs, R. (1998). The seven great debates in the media literacy movement. In *Journal of Communication* (Vol. 48, Issue 1). <https://doi.org/10.1111/j.1460-2466.1998.tb02734.x>
- Hobbs, R., & Jensen, A. (2022). The Past, Present, and Future of Media Literacy Education. *Journal of Media Literacy Education*. <https://doi.org/10.23860/jmle-1-1-1>
- Howard, J. L., Bureau, J., Guay, F., Chong, J. X. Y., & Ryan, R. M. (2021). Student Motivation and Associated Outcomes: A Meta-Analysis From Self-Determination Theory. *Perspectives on Psychological Science*, 16(6). <https://doi.org/10.1177/1745691620966789>
- Luigini, A., & Panciroli, C. (2018). Ambienti digitali per l'educazione all'arte e al patrimonio. *FrancoAngeli*.
- McDougall, J., & Rega, I. (2022). Beyond Solutionism: Differently Motivating Media Literacy. *Media and Communication*, 10(4). <https://doi.org/10.17645/mac.v10i4.5715>
- McHugh, S. (2016). How podcasting is changing the audio storytelling genre. *Radio Journal*, 14(1). https://doi.org/10.1386/rjao.14.1.65_1
- Mishra, P., & Koehler, M. J. (2006). Technological pedagogical content knowledge: A framework for teacher knowledge. In *Teachers College Record* (Vol. 108, Issue 6).
<https://doi.org/10.1111/j.1467-9620.2006.00684.x>
- Nardi, B. A., Schiano, D. J., & Gumbrecht, M. (2004). Blogging as social activity, or, would you let 900 million people read your diary? *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*. <https://doi.org/10.1145/1031607.1031643>
- Potter, W. J. (2004). Theory of media literacy: A cognitive approach. In *Theory of Media Literacy: A Cognitive Approach*. <https://doi.org/10.4135/9781483328881>
- Rivoltella, P. C. (2020). *Nuovi alfabeti. Educazione e culture nella società post-mediale* (Vol. 124). Scholè-Morcelliana.

- Rivoltella, P. C. (2022). Educating to Digital Citizenship: conceptual development and a framework proposal. *Journal of E-Learning and Knowledge Society*, 18(3). <https://doi.org/10.20368/1971-8829/1135821>
- Rivoltella, P. C., & Rossi, P. G. (2024). *Tecnologie per l'educazione*. Pearson.
- Sudulich, M. L. (2008). Digital Citizenship, The Internet, Society, and Participation. *Information, Communication & Society*, 11(7). <https://doi.org/10.1080/13691180802258738>
- Suggate, S. P. (2016). A Meta-Analysis of the Long-Term Effects of Phonemic Awareness, Phonics, Fluency, and Reading Comprehension Interventions. *Journal of Learning Disabilities*, 49(1), 77–96. <https://doi.org/10.1177/0022219414528540>
- Tyng, C. M., Amin, H. U., Saad, M. N. M., & Malik, A. S. (2017). The influences of emotion on learning and memory. In *Frontiers in Psychology* (Vol. 8, Issue AUG). <https://doi.org/10.3389/fpsyg.2017.01454>
- Valgolio, E. (2021). Competenza digitale: Uno strumento per il curricolo della Media Literacy Education (MLE). *Essere a Scuola*, 4, 58–64.
- Van den Bulck, J., & Roskos-Ewoldsen, D. R. (2020). *The international encyclopedia of media psychology*. John Wiley & Sons, Incorporated.
- Vygotsky, L. S. (1978). Mind and Society: The Development of Higher Psychological Processes. In *Harvard University Press*.
- Zimmerman, B. J. (2000). Attaining self-regulation: A social cognitive perspective. In *Handbook of Self-Regulation*.

Viral narratives around the “Sailor Moon made me gay” controversy on Facebook

(Narrativas virales alrededor de la controversia “Sailor Moon me hizo gay” en Facebook)

Daniel Eugenio Salinas Lara
Tecnológico de Monterrey,
México
a00600084@tec.mx
0009-0009-7401-8354

Raúl Alejandro Treviño
González
Tecnológico de Monterrey,
México
a00600233@tec.mx
0000-0001-5427-1277

Mariana Reyes Abundes
Tecnológico de Monterrey,
México
a01550689@tec.mx
0000-0002-7908-0677

Received: 07 November 2024

Accepted: 28 March 2025

Abstract

Social media viral narratives create stereotyped and simplified representations of situations, events or individuals and can reflect the users' emotions, feelings, identities or discourses. This article is a case study of the controversy “Sailor Moon made me gay”, which arose from the viralization of a humanities master's thesis of the same name by a Tecnológico de Monterrey graduate in Mexico. Using a mixed method qualitative and quantitative content analysis of the comments from the four Facebook posts with the most engagement, five main thematic categories that fed the viral narratives were identified: mockery, sexuality, criticism of the research, criticism of institutions, and interest in the thesis. Driven mainly by mockery, the main narrative involved a literal interpretation of the title of the thesis, homophobic discourse, dismissal of the importance of the work's findings, anger because of the author's scholarship and the interpretation of the phenomenon as a sign of educational decline and Mexico's downfall. These findings can aid researchers and institutions in understanding what is the social perception of pop culture and marginalized identities research.

Keywords *Viral narratives, Social Media, Text mining, homophobia, virality*

Resumen

Las narrativas virales de redes sociales construyen representaciones estereotipadas y simplificadas de situaciones, eventos o individuos y pueden reflejar las emociones, sentimientos, identidades o discursos de los usuarios. Este artículo es un caso de estudio de la controversia "Sailor Moon me hizo gay", surgida de la viralización de una tesis de maestría homónima del área de humanidades de un graduado del Tecnológico de Monterrey en México. Mediante una técnica mixta de análisis de contenido cuantitativo y cualitativo de los comentarios de las cuatro publicaciones con más interacciones en Facebook, se identificaron las cinco categorías temáticas principales que alimentaron las narrativas virales: burla, sexualidad, crítica a la investigación, crítica a las instituciones e interés por la tesis. Motivados principalmente por hacer burla, se encontró una narrativa predominante que interpretaba de manera literal el título de la tesis, reproducía discurso homofóbico, desestimaba la importancia de los hallazgos, generaba enojo por la beca otorgada al autor y finalmente consideraba que esto reflejaba una decadencia de la educación y situación del país. Estos hallazgos pueden servir a investigadores e instituciones para conocer la percepción social de la investigación de la cultura popular e identidades marginadas.

Palabras clave *Narrativas virales, redes sociales, minería de textos, homofobia, viralidad*

1. Introducción

A temprana hora del viernes 16 de agosto de 2024 dentro de la red social Reddit¹, en el subreddit r/mexico, se publicó una captura de pantalla de la portada de una tesis de maestría titulada *Sailor Moon me hizo gay*. La subjetividad e identidad del hombre gay millennial mexicano desde el consumo de Sailor Moon elaborada por el graduado del Tecnológico de Monterrey (de ahora en adelante Tec) Daniel Salinas. Se usó un emoji de expresión neutral “😐” como título y el tag “Humor mexicano mx Puro desmadre” (ver Figura 1). A partir de esta publicación la existencia de la tesis se viralizó en otras redes sociales como Facebook, X y TikTok, para después ser reportado como controversia en medios digitales (Tapia Sandoval, 2024), donde se hablaba de un discurso predominante de rechazo hacia el trabajo, pero también un cuestionamiento metodológico y politización de las circunstancias alrededor del financiamiento (García Orozco, 2024).



Figura 1. Publicación inicial el 16/08/2024 a las 12:39:37 AM CST

Imagen obtenida el 05/09/2024 de <https://www.reddit.com/r/mexico/comments/1ethxm3>. El nombre del autor aparecía oculto para cumplir con las reglas anti-acoso de la plataforma.

Los fenómenos virales pueden reflejar emociones y sentimientos de los usuarios de redes sociales (Berger y Milkman, 2012), servir como una manera de participar en el discurso público y fortalecer la identidad (Dafonte Gómez, 2015) e incluso llegar a tener repercusiones de índole político (Espina Vergara, 2017), económico (Shiller, 2019) o de salud pública (Sharma et al., 2022), sobre todo cuando se trata de desinformación o fake news. Dado que las redes sociales se han incorporado en la vida cotidiana de millones de personas y pueden reflejar problemas sociales (Ashar, 2024), el estudio de fenómenos virales digitales puede contribuir al entendimiento del clima social, político y cultural de una población en un determinado momento. El presente artículo es un caso de estudio de un fenómeno viral en México y busca identificar y describir las principales narrativas virales (Aguilar et al., 2022)

discutidas alrededor de la controversia suscitada por la tesis de Salinas (2024). Para ello se recurrió al análisis de contenido cuantitativo y cualitativo de las cuatro publicaciones relacionadas con el fenómeno con más comentarios en Facebook.

La tesis de Salinas (2024) es un estudio cualitativo sobre el consumo por parte de una muestra de diez hombres gays millennials mexicanos del anime Sailor Moon (1992), el cual por estar dirigido a un público femenino les permitió explorar en su infancia y juventud aspectos de su subjetividad, masculinidad y feminidad, que más adelante en la adultez relacionarían con su orientación e identidad sexual. En palabras del autor de la tesis, el título es irónico y buscaba incentivar la curiosidad de lectores de intereses académicos: "Obviamente, el título es provocador o llamativo. Eso es con toda la intención. Es, por así decirlo, irónico porque obviamente un programa de televisión no te hace gay..." (citado en Rubín, 2024). Adicionalmente en el texto en cuestión hay una aclaración sobre los hallazgos de la investigación, los cuales no buscaban ser generalizables (Salinas, 2024, p.58). La tesis fue aprobada por un comité conformado por tres doctores del Tec y una de la UNAM, siguiendo los lineamientos institucionales del posgrado de Maestría en estudios humanísticos².

El fenómeno viral resaltó la imagen de la portada de tesis para crear un contraste entre el título y el logotipo del Tec, cuya percepción es de ser una de las universidades privadas mexicanas de mayor prestigio (Izquierdo, 2024). Podría considerarse que se convirtió en meme, pues se compartieron también imágenes para adjudicar la tesis a otros autores (Velázquez, 2024) o para denostar otros trabajos, como en la publicación del medio satírico El Deforma (Ver Figura 2). La información sobre la intención del autor, el programa de posgrado y el financiamiento económico fue mayormente omitida durante la difusión del contenido entre los usuarios de redes sociales. El alcance de la controversia fue suficiente para ser reportada en medios digitales de amplio alcance como Milenio, Univision, El Financiero, MVS Noticias, entre otros, donde se hablaba de que las reacciones eran "diversas y polarizadas" (Tapia Sandoval, 2024). En el presente trabajo se analizará con mayor profundidad esta diversidad de opiniones.



Figura 2. Publicación en El Deforma

Obtenido de <https://www.facebook.com/share/p/99aiSH7E7FRfV4kk/>

2. Marco teórico

El concepto de virus mediático, y derivados como viralización o viralidad, proviene de la comunicación y marketing y se define, como analogía de un virus biológico, como contenido que se expande a través de las redes digitales “infectándolas” con un código ideológico informativo o de entretenimiento (Dafonte Gómez, 2015). De acuerdo con Aguilar et al. (2022) las narrativas virales construyen representaciones estereotipadas y simplificadas de situaciones, eventos o individuos. Estas suelen estigmatizar a personas o situaciones al reducirlas a ciertos aspectos descontextualizados, exagerados o llamativos que se presentan como representativos de todo su ser, similar a la descripción de la imagen pública del individuo de Goffman (1989): “parecería estar constituida por una reducida selección de acontecimientos verdaderos que se inflan hasta adquirir una apariencia dramática y llamativa...” (p. 89).

La viralización se potencia por las emociones intensas que provocan estos contenidos, como la ira o la ansiedad, las cuales son factores clave en la decisión de los usuarios para compartirlos (Berger y Milkman, 2012). Estos no solo consumen pasivamente estas narrativas virales, sino que juegan un papel activo en su expansión al compartir opiniones, imágenes o videos que contribuyen a la perpetuación de las representaciones simplificadas. El mismo acto de compartir puede funcionar como expresión personal, asociación con los contenidos y valores de lo emitido, declaración de conocimiento de temas novedosos o como parte de una construcción y proyección de identidad (Dafonte Gómez, 2015).

Sîrbu et al. (2019) explican que los algoritmos de redes sociales están diseñados para recolectar el mayor número de impresiones o interacciones, lo cual da pie al surgimiento de polarización, cámaras de eco y una homogeneización del discurso, ya que el flujo de información en redes sociales se guía no por el valor de la información, sino por su popularidad. Por lo anterior se puede inferir que las mismas plataformas se benefician de la existencia de las narrativas virales. En este contexto los memes, entendidos como una unidad cultural —usualmente una imagen— laxa, replicable y reinterpretable capaz de transmitirse y sobrevivir en un determinado ecosistema social digital, contribuyen a articular el discurso público, generalmente de manera humorística, y como una forma de reflejar estados de opinión, al grado de poder considerarse capital cultural (Ruiz, 2019), lo cual ha resultado en que sean utilizados de manera deliberada incluso en la comunicación política (Espina Vergara, 2017).

3. Metodología

Para esta investigación se implementó una metodología mixta que combina un enfoque cualitativo y cuantitativo para identificar categorías de análisis mediante la visualización de patrones de datos usando métodos digitales, así como la posterior interpretación de temas y patrones de los comentarios (Creswell, 2014). Para adaptar la metodología a las características propias de Facebook, se diseñó un proceso para la extracción y manejo de comentarios en tres etapas: selección, extracción y análisis de datos.

En la primera fase se seleccionó el corpus, que consiste en las cuatro publicaciones relacionadas con la controversia que generaron mayor interacción y comentarios en Facebook, elegida por ser la red social más utilizada en México con 90.2 millones de usuarios (Silverio, 2024). Se descartaron las de carácter meramente humorístico con el fin de evitar que las reacciones y comentarios se enfocaran solo en la percibida comicidad del fenómeno. Las publicaciones elegidas³ fueron las de las páginas: Serena Moonie (206 mil me gusta, 458 mil seguidores), del 20 de agosto de 2024; El Editorial (53 mil seguidores), del 26 de agosto; Política Básica (132 mil me gusta, 164 mil seguidores), del 19 de agosto; y Cadena Informativa Campeche (9.4 mil me gusta, 16 mil seguidores), del 20 de agosto. Se consideró la cantidad de comentarios como factor decisivo para la selección de publicaciones, para así recolectar una mayor cantidad de datos para análisis, y representar con mayor precisión el comportamiento de los usuarios en la construcción de las narrativas virales. La siguiente tabla (ver Tabla 1) muestra el desglose de interacciones de cada página.

Tabla 1. Detalles de las publicaciones sobre la controversia al 05/09/2024

Página	Reacciones	Desglose de reacciones	Comentarios	Compartidos
Serena Moonie	63,635	😊 50 mil 😊 5.9 mil 👍 4.7 mil ❤️ 1.3 mil 😂 487 😞 229 🙄 168	6,597	14,597
El Editorial	4,094	😊 2.3 mil 👍 998 😊 460 ❤️ 130 😞 86 😂 30 🙄 17	2, 237	1,995
Política Básica	9,062	😊 5.1 mil 👍 2.3 mil ❤️ 1.3 mil 😊 158 🙄 56 😂 13 😞 3	1,427	2,104
Cadena Informativa Campeche	3,274	😊 1.8 mil 👍 717 😊 544 ❤️ 86 😞 38 😂 23 🙄 21	1,289	1,833

Para la extracción de comentarios se usó la técnica de web scrapping, que consiste en tomar los datos de cada página web y descargarlos en archivos individuales. Posteriormente se realizó la limpieza de los datos y se unieron en una sola base con los más relevantes: nombre de usuario, comentarios, hace cuántos días se publicó, “me gusta” e imágenes descargadas. Se tomó como muestra todos los comentarios que se podían visualizar en las páginas para obtener una aproximación desde la analítica cultural (Manovich, 2020), y de este modo analizar los comentarios como un todo y disminuir el sesgo.

Dado que algunos comentarios aparecían vacíos, resultado de etiquetar a otras personas o adjuntar imágenes, el número total de comentarios analizables mediante minería de textos fue de 3,818: 1,840 de Serena Moonie, 1,129 de El Editorial, 411 de Política Básica y 438 de Cadena Informativa Campeche. Se detectaron solo 17 ocasiones en que algunos usuarios comentaron en más de una publicación, por lo que no se considera significativo. Como limitante debe considerarse la posibilidad de que algunos de estos comentarios de usuarios repetidos puedan provenir *bots* (Cobos, 2024), no obstante, se decidió no profundizar en esta detección de usuarios falsos debido a que ello representaría un estudio aparte, ya que conlleva examinar a detalle dichos perfiles si se opta por una metodología cualitativa para hacerlo, o de manera alternativa, se podría recurrir a software especializado para la

detección automatizada de *bots*, lo cual conlleva un costo que excede los recursos disponibles para esta investigación.

La base de datos fue posteriormente analizada en R Studio mediante técnicas de Procesamiento del Lenguaje Natural: análisis de frecuencia directa con *tidytext* (Silge y Robinso, 2022) para encontrar las palabras más repetidas y correlación entre palabras con *widyr* (Robinson, 2021) para visualizar las relaciones y comportamiento entre palabras. A partir de este análisis identificaron categorías para la descripción de las narrativas virales.

4. Análisis de contenido

4.1. Descripción de las publicaciones

La publicación con más reacciones fue la de Serena Moonie (2024), un blog personal humorístico y de autoayuda que utiliza personajes de Sailor Moon en su contenido. Se incluía una foto de un monitor mostrando la portada de la tesis, acompañada de un breve texto sobre su aprobación por el Tec y la frase “México mágico”, comúnmente usada para señalar lo ilógico o surreal del país (Hinojosa y Quezada, 2017), lo cual pudo haber influido en las interpretaciones de los usuarios.

La nota de El Editorial (2024), un medio que ofrece periodismo político, deportivo y general en Tamaulipas y México incluyó imágenes de la silueta de Sailor Moon, la portada de la tesis, una página con una imagen de la transformación de la protagonista del anime, otra con una historia de redes sociales y una de la lista de entrevistados. El texto de siete párrafos explicaba la controversia, resaltando que el trabajo supuestamente discutía la influencia del anime en la identidad sexual del autor y que con diez entrevistas pretendía abarcar una muestra de hombres gays mexicanos. También se mencionaba el financiado por “Conacyt [sic]”.

La publicación de Política Básica (2024), una página de análisis político y económico que comparte noticias, memes y opiniones, precedió a las otras tres aquí seleccionadas y compartía la portada de la tesis y mencionaba que, tras leer el documento, consideraba que el contenido estaba bien estructurado y que la polémica era intencional por parte del autor. Además, destacaba que los resultados no eran generalizables y en tono humorístico señalaba que haría una investigación similar sobre el anime One Piece. Esta fue la única nota con un enfoque favorable hacia la tesis.

La publicación del medio informativo Cadena Informativa Campeche (2024) incluyó imágenes similares a las de El Editorial, excepto que mostró la página de agradecimientos de la tesis en lugar de la silueta de Sailor Moon. Se explicaba que el trabajo exploraba el consumo de Sailor Moon entre hombres gays mexicanos que vieron la serie en los noventa y siguen siendo fans. El copy empezaba con “Presentan Tesis basada en Sailor Moon en el Tec de Monterrey. ‘SAILOR MOON ME HIZO GAY’ 🙌👀”, y finalizaba con “¿Qué dices de esta tesis?”. El uso de emojis de sorpresa y miedo puede haber influido en polarizar las reacciones.

Se observa que, debido a la viralidad del tema, estas páginas compartieron casi las mismas imágenes (ver Figura 3). El Editorial y Cadena Informativa Campeche reutilizaron las capturas de

pantalla inicialmente compartidas por el periodista @jorgegogdl en X el 18 de agosto (ver Figura 4). En este hilo de X de más de dos millones de vistas se describe la tesis como “entrevistas a 10 personas... pagadas con recursos públicos del @Conahcyt_Mex”, se describe el contenido con lenguaje irónico e incluso menciona a la exdirectora del Consejo Nacional de Humanidades, Ciencias y Tecnologías. Con esto se evidencia la replicación de contenido entre redes sociales.



Figura 3. Captura de pantalla de las publicaciones



Figura 4. Fragmentos del hilo de X

4.2. Análisis cuantitativo de los comentarios

El primer acercamiento realizado para analizar los comentarios fue un análisis de frecuencia directa. A modo de nube se visualizaron las cien palabras más repetidas del total de la muestra (ver Figura 5), donde aquellas con mayor frecuencia se observan en mayor tamaño. Previamente se eliminaron las palabras “tesis” y “sailormoon” de la visualización para un análisis más detallado.



Figura 5. Nube con las cien palabras más repetidas del total de comentarios

La frecuencia total permitió conocer, en primera instancia, de qué hablaban los comentarios sin necesidad de profundizar demasiado y comenzar a esbozar las categorías de análisis. La expresión de mayor frecuencia fue “jaja”, correspondiente a las variantes de risa que escribieron los usuarios, con lo que se intuye que el tono general de los comentarios es de burla o comicidad. Se observan también palabras como “tema”, “título” y “maestría”, en referencia al documento y al grado de estudio, así como “tec” y “monterrey”, con relación a la institución académica que acreditó la tesis. Asimismo, se puede ver que se nombran otras “series” y “animés”, resultado del título de la tesis que refiere a Sailor Moon e incita a mencionar otras.

Al comparar la frecuencia de cada una de las publicaciones (ver Figura 6), se constata que las palabras más repetidas son similares, en donde destaca “jaja”, la referencia a “gay” y a otros animes como “ranma”. Difieren ligeramente los comentarios de Política Básica, con mayor enfoque en cuestiones académicas como “investigación” o “entrevistas”, puesto que la publicación hace referencia a la estructura del documento. Sin embargo, en general las palabras de los comentarios son parecidas en todas las publicaciones, lo que muestra que a pesar del tono diferente de cada página, las reacciones de los usuarios fueron similares. Por lo que posteriormente se analizaron todos los comentarios en conjunto y no por publicación separada.

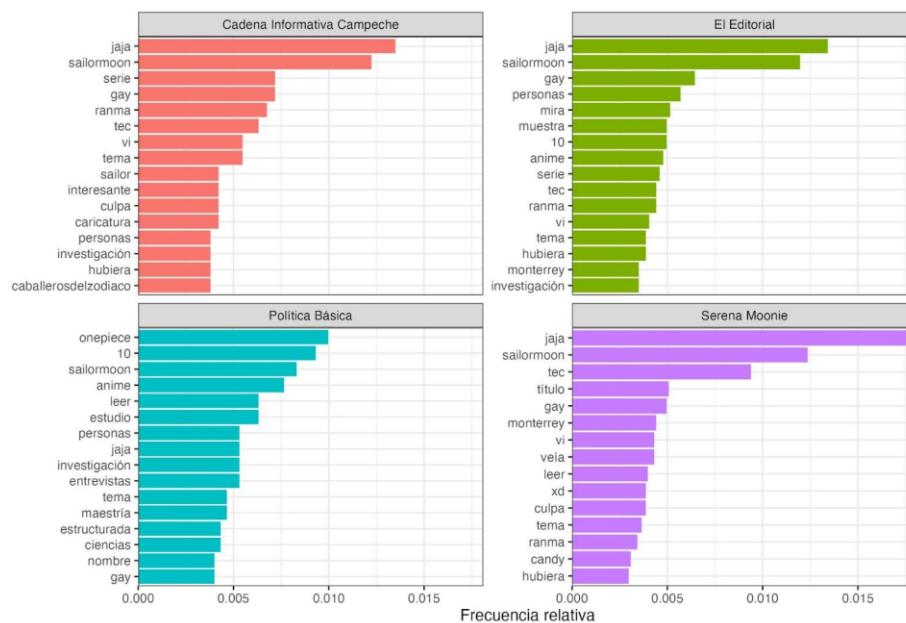


Figura 6. Frecuencia relativa dividida por publicación

Posteriormente se analizaron las relaciones entre las palabras mediante dos técnicas: la correlación y los n-gramas o pares de palabras. La primera es una medida para entender la relación lineal entre dos palabras y la segunda muestra conjuntos de palabras que tienen una relación directa entre ellas. La correlación muestra qué palabras aparecen próximas entre sí y los n-gramas que palabras tienden a aparecer después de otras. Se escogieron las palabras que tuvieran más del .15 de correlación, así como los n-gramas de mayor frecuencia para visualizar estas conexiones en clústers de palabras. Después se agruparon de manera manual (tabla 2) estos conjuntos de palabras en las siguientes categorías para el análisis cualitativo: burla, sexualidad, crítica al trabajo de investigación, crítica a las instituciones e interés por la investigación.

Tabla 2. Categorías de análisis resultado de las técnicas de relaciones entre palabras

Categoría	Correlación (>.15)	Bigramas
Burla	pensé-broma; prisma-lunar-transformación; series-super-campeones-chicas-sayayin-dragonball-caballerosdelzodiaco; gustos-imagino-vieron-serie-contexto-debió-culpar; tanta-caricatura; vuelve-anime	mira:jaja; bad:bunny; lady:gaga; one:piece; sakura:card:captor; tuxedo-torcido:mask; power:rangers: tortugas:ninja; bob:esponja; saint:seiya; méxico:mágico; ah:caray; digas:mmds; prisma:lunar; hice:gay:jajaja; señor:calamardo; death:note; chicas:super:poderosas; super:sayayin; mazinge:z
Orientación sexual	homosexualidad-subjetividad-mexicano-identidad-género-sexual-orientación-amor; dragon-ball-lesbiana; gustos-imagino-vieron -serie-contexto-debió-culpar	preferencias:sexuales; orientación:identidad:sexual
Investigación	marco-teórico; aporte-científico; esperaban-humanidades; estudio-cualitativo-social; muestra-población-entrevistas-10-amigos-nivel-estructurada; ciencias-sociales; metodología-tema-realmente;conclusión-hipótesis-medio-información	estudio:cualitativo; investigación:cualitativa; examen:profesional; marco-teórico: ciencias:sociales; 10: personas-entrevistas-amigos-años; método:científico; título:debería; excelente:tesis; próxima:tesis

Instituciones	tecnológico-tec-monterrey; institución-seria; calidad-sinodales-escuela;	recursos:públicos; institución:educativa; estudios:humanísticos-humorísticos; mejores:universidades; nivel-mundial
Interés	leerla-interesante; necesito-quiero-leer	ve:interesante:leerla; quiero:leerla; necesito:leer

4.3. Categorías de análisis cualitativo

4.3.1. Burla

La burla hacia la tesis fue la respuesta más notoria cuando se analizan las reacciones en las cuatro publicaciones y las palabras repetidas en los comentarios. La reacción “me divierte” (😊) fue por mucho la más prevalente, incluso en la publicación favorecedora de Política Básica. Igualmente la expresión de risa “jaja” se observa como la de mayor frecuencia en tres de las cuatro publicaciones y es la de mayor tamaño en la nube de palabras.

@Rafael: Jajajajaja WTF

@Vanessa: Jajaja no lo creo Se pasan jajaja

@Alice: Quería ser una Sailor Scoutt. JAJAJA

El título es la principal razón de la burla. Algunos usuarios interpretan literalmente la frase “Sailor Moon me hizo gay” y utilizan la ironía para bromeear con lo absurdo de la premisa.

@Magaly: Hice gay a mis primos los obligaba a ver sailor moon para después salir a jugar a la calle

@Judith: Se transformo en gay "por el poder del prisma lunar"

@Jesus: Que sigue, una tesis de como dragon ball me hizo lesbiana?

Como se aprecia en la última cita, también se hacen menciones irónicas a los supuestos efectos de otras producciones de la cultura popular, evidenciado por las prevalentes menciones a otros animes como *Dragon Ball*, *Ranma ½*, *Los Caballeros del Zodiaco*, entre otros.

@Fernando: me volví diabólico por el consumo excesivo de Pokémon y Dragon Ball durante mi infancia

@Alejandra: Y los drags queens fue por ver Ranman ½

@Rafael: Si es cierto , a mi los caballeros del zodiaco me enseñaron a pegarle igual a mujeres que a hombres

@Liz: Ahora entiendo, mi deseo de que la gente que me caga se muera es por andar viendo Death Note.

En algunos comentarios la burla deja entrever una preocupación por que se revivan narrativas conservadoras o patologizantes sobre los efectos de ver anime como creen que afirma la tesis, lo cual a ojos del usuario justificaría el escarnio.

@Grace: Si fuera real su pseudo teoría, entonces habría que eliminar juegos y caricaturas de violencia y armas porq generaría el mismo efecto, creo q le falta algo al título “Sailor Moon hace gay a quienes no tienen las capacidades de discernir la fantasía de la realidad ”

Como se verá a continuación los comentarios asociados a otros temas pueden estar enmarcados de manera humorística, lo cual puede explicar también el porqué de la gran prevalencia de la risa en reacciones y comentarios. Con excepción de los comentarios de interés por leer el documento, se

observa una predisposición a opinar sobre este, sin haberlo leído, con un prejuicio sobre su falta de seriedad.

4.3.2. Sexualidad

Los comentarios sobre orientación o identidad sexual fueron recurrentes en las cuatro publicaciones. La prevalencia de culpa o culpar responde a respuestas de rechazo al tema de la tesis. En este tipo de comentarios fue común el uso de lenguaje homofóbico:

@Raquel: Qué fácil es culpar a los demás por sus desviaciones. De ser meramente una preferencia no estuviera culpando a nadie.

@Kiara: No le echen la culpa a una caricatura, La culpa es de los genes de los padres

Algunos que aseguran haber visto la serie mencionan en tono de burla o defensivo que su sexualidad no fue influida por el anime.

@Trinny: O sea que si soy mujer y vi sailor moon... Soy lesbiana??... Que absurdo!!

@Lynette: Lo triste es que se lo dieran por bueno, porque muchos incluyendome, vimos sailor moon y en definitiva no influyó en que me quisiera hacer lesbiana o trans, o que me gustara salir con un adulto siendo menor de edad.

En un esfuerzo por reforzar su heterosexualidad, algunos hombres mencionan disfrutar de la sexualización de los personajes e incluso aluden, con un tono más agresivo, a masturbarse con el contenido de la serie.

@Fabio: A ver, yo me ví sailor moon y lo único que me daban ganas era de que se le subiera más la falda. Jamás pensé en volverme g@¥ por verlas. Es más, me la hice varias veces a nombre de ellas

@William: Sailor Moon me hizo hetero , sacaba al ganso a pasear de solo verla transformarse. No hayan como justificar que les gusta el chile por la cola.

También, aunque con menos frecuencia, se encontró discusión o crítica dirigidos al alcance de la tesis. En contados casos se predice, posiblemente sin leer el documento, algún hallazgo de la investigación.

@Micael: [...] Lo que si considero debió colocar es mas sobre la Homosexualidad en Oriente (en específico Japón) y hacer mas referencia a como se ve la Homosexualidad en el Manga y Anime, mencionar tal vez géneros como el Yaoi o Shonen Ai (ausentes en mención en la tesis)

@Vane: Quizás solo hubo una identificación con la serie que reafirmó una identidad sexual latente...

En general el lenguaje de los usuarios habla de un rechazo hacia la idea de explorar la relación del consumo mediático con la orientación sexual. Los casos de lenguaje más agresivo pueden corresponder a una muestra de homofobia, ya sea por la discusión abierta sobre la homosexualidad o por la interpretación literal del título y las consecuencias lógicas de esto. La errónea narrativa sobre que los hallazgos de la tesis corresponden literalmente al título fue sumamente prevalente.

4.3.3. Crítica al trabajo de investigación

Las críticas hacia el texto académico estuvieron enfocadas en la temática, su metodología y al área de estudios a la que pertenece. La principal crítica fue la cantidad de participantes de la muestra, evidenciada por la repetición de los términos “10” y “personas”, ya que muchos detractores consideran que diez entrevistas son insuficientes para obtener conclusiones representativas, aunque esa no fuera la intención del estudio, y concluyen que los hallazgos son limitados y subjetivos.

@Guillermo 10 individuos no son una muestra adecuada para el total de la población g@y del país, es absurdo.

@Alvar: Con una muestra de 10 amigos, frente a miles de espectadores entre los años 90 y 2000, millones quizá a nivel mundial, es prácticamente inválido estadísticamente hablando. Una muestra más de que la educación universitaria está en franco decaimiento.

Algunos usuarios sugieren maneras de fortalecer su rigor metodológico, como ampliar el número de entrevistados, especificar en el título que se trata de un estudio de caso con un grupo reducido o delimitar geográficamente.

@Ileana: Yo solo se que, 10 sujetos de estudio no son suficientes, quizá si hubiera hecho una delimitación geográfica, que justificara la muestra pss igual y si

@Agustin: Fuera del argumento de la tesis, quien le dijo que una muestra de 10 personas era lo suficientemente grande para representar a la población de la comunidad G4Y Mexicana, las técnicas de muestra que uso no son correctas, con diez personas es imposible hacer una inferencia real que verdaderamente refleje la realidad.

La temática de la tesis también fue fuertemente criticada, ya que algunos usuarios no consideran el impacto de Sailor Moon sea un tema relevante. Se encontraron descalificaciones hacia el estudio como calificarlo de "estupidez" o "pendejada".

@Angel: Si se gradúan con tesis clonadas y copiadas, que no se gradúen con una pendejada como sailor moon sería ir en contra de la mediocridad universitaria en México

@Fauss: QUE. BÁRBARO ESOS SON LOS FUTUROS PROFESIONALES DEL PAIS. NO SE QUIEN ESTE MAS MAL SI LA ESCUELA QUE PERMITE ESA ESTUPIDEZ O EL ALUMNO. YA EN POCO TIEMPO HACER TESIS VA SER OBJETO DE IDIOTECES Y SERAN ACEPTADA EN LA SOCIEDAD ATARANTADA.

Algunos usuarios cuestionan la legitimidad de las humanidades frente a las ciencias exactas que consideran más objetivas o valiosas. Estos comentarios críticos desestiman una disciplina que estudia la subjetividad y las experiencias del ser humano.

@Chris: Bueno, son estudios humanísticos, que esperaban? algo comprobable? metodologia científica con prueba de doble ciego? estadística rigurosa con muestras gigantescas?

@Luis: Siempre he pensado que esos estudios "humanitarios" y "culturales" son puras idioteces y esto lo demuestra. Únicamente han servido para promover las "ideologías de género" que tanto daño están haciendo a la sociedad.

Los comentarios sobre la metodología y temática de la tesis refuerzan una percepción social negativa de las humanidades y ciencias sociales frente a ciencias duras, y el método científico, como ontológicamente y epistémicamente superiores.

4.3.4. Crítica a las instituciones

El Tec y el Conahcyt fueron también blanco de fuertes críticas, evidenciado por la repetición de las palabras "Tec", "Monterrey" e "instituciones". En el caso de la universidad privada los cuestionamientos se centraron en sus métodos de evaluación y sus estudiantes, insinuando que con suficiente dinero cualquier alumno puede aprobar, lo cual explicaría según estos usuarios la aprobación de la tesis.

@Mer: Ahí es donde se confirma que no es necesario ser inteligente para entrar o salir del Tec, simplemente hace falta que papi pague la colegiatura.

@Pedro: El tec de monterrey para fifis, mientras sea de una familia pudiente haran lo imposible para que apruebes, a un becado le van a exigir 20 veces mas no es el mismo trato

Otros comentarios afirman decepcionados que investigaciones como la de Sailor Moon reflejan una disminución en la calidad académica del Tec.

@Abe: [...] Esa tesis es una m3rd3, no debería de existir como tal, no le llega a las de ciencias e ingeniería. El Tec ya no es lo que era.[...]

@Manuel: El Tecnológico de Monterrey al aceptar esa tesis solo demuestra que ha bajado su nivel, sin contar que su muestreo fueron solo 10 personas... Y lo peor, que ese sujeto que hizo esa tesis, era becado del Conahcyt, es decir, que parte de nuestros impuestos se fueron en eso...

Como se observa en el último comentario, parte de la indignación proviene del hecho de que Salinas era becario del Conahcyt. Los internautas se cuestionaron sobre cuánto dinero recibió el becario, incrementando su descontento al considerar que otras investigaciones presuntamente más significativas no reciben apoyo. La repetición de la palabra “recursos” refleja cómo algunos usuarios sienten que tienen derecho a reclamar lo anterior, pues argumentan que ese dinero proviene de sus impuestos.

@Juan Carlos: El problema no es el título es que conacyt le diera 100K pesos para hacer esto. Que un junior del tec reciba 100k para jugar a hacer su tesis de anime me parece insultante y soy muy fan del anime.

@David: Y el CONACYT le dio beca, yo haciendo tesis sobre cáncer de estómago e inteligencia artificial y me dieron una batería hahaha

Algunos usuarios se expresan de manera más pesimista y muestran desencanto con la educación o la situación del país en general, considerando la tesis como un reflejo de ello. Frases como “por eso estamos como estamos” o pensar que el país está “jodido” reflejaban este sentimiento. También se culpó en ocasiones al presidente y su gobierno o a organismos externos como la ONU como causantes de esta percibida decadencia.

@Em: Y siempre le ando echando la culpa de que nos está cargando la vrg por cabecita de algodón, pero me encuentro con esto y mis respetos para el presidente... Que mal estamos

@Cristian: Así de torcidos estamos como el miembro del chanco quien en su sano juicio acepta tales cosas pero imagínense la calidad de profesionales! Todo por la agenda 2030 y claro sus jugosas aportaciones \$\$

Comentarios que expresaban frustración, enojo, decepción y hasta desesperanza con la situación actual del país alimentaron una narrativa pesimista y hasta fatalista del clima sociopolítico de México.

4.3.5. Interés por la investigación

A pesar de las críticas y descalificaciones, un grupo menor de usuarios expresó interés por leer la tesis, evidenciado por la repetición notoria de las palabras “interesante” y “leer”. Estos comentarios consideran relevante estudiar fenómenos culturales como el que expone el documento, y perciben a primera vista que se trata de un trabajo bien fundamentado y justificado. Algunos usuarios piden la liga para descargar la tesis o intuyen que el título busca captar la atención, pero que detrás puede haber una buena investigación.

@Ale: Me encantaría leerla, para que le aceptarán la tesis debe tener muy buenos argumentos

@Marbe: Creo que el título es meramente para llamar la atención. Creo que nos estamos dejando llevar por primeras impresiones. Sería interesante leerla y salir de dudas.

Adicionalmente algunos usuarios comentan ya haber leído secciones de la tesis y por ende ofrecen una crítica informada. En ciertos casos argumentan que se trata de un buen trabajo, destacando que la tesis “tiene lógica” y está bien estructurada, o también proporcionan críticas constructivas para fortalecer el estudio.

@Mary: Leí acerca de esa tesis y la verdad tiene lógica de ser... Y te informa desde su punto de vista que factores influyen para destaparse... No lo veo ni ridículo ni malo...

@Julián: Es una muy buena tesis. La perspectiva desde la que aborda género desde la investigación cualitativa, estando esta palgada de positivismo, genera una reflexión onto-epistemológica bastante interesante.

En contra de las otras narrativas predominantes, la opinión informada y constructiva permitía matizar el fenómeno viral y daba el beneficio de la duda al graduado.

4.4. Resumen de los hallazgos

Tras analizar de manera cuantitativa y cualitativa los comentarios de las cuatro publicaciones sobre la controversia con más interacciones, se pudieron identificar las principales narrativas virales alrededor del fenómeno viral. Se constató, tal como mencionan Aguilar et al. (2022), cómo los hechos fueron simplificados y reducidos, distorsionando tanto los hallazgos de la investigación como el contexto alrededor de su elaboración. Una gran cantidad de usuarios parece haber entendido y reproducido la siguiente narrativa: se encontró que un estudiante del Tec realizó un tesis que afirma que ver el anime *Sailor Moon* convertía al espectador en gay, lo cual por ser evidentemente un absurdo no era merecedor de una beca financiada con recursos públicos y esto es una muestra de la decadencia de la educación mexicana y el país.

Aunque sí había usuarios con una opinión más favorecedora sobre la investigación, estos no eran una proporción tan significativa comparada con la opinión negativa. Con base en las reacciones y palabras más utilizadas se pudo constatar que la risa como muestra de burla fue la principal emoción que propició la viralización de la tesis, y es así como se enmarcaron una gran proporción de los comentarios y discusiones que se suscitaron. Esto contribuyó a que las discusiones no se matizaran y en general no buscaran hablar sobre los verdaderos temas que planteaba la tesis o sus hallazgos.

5. Discusión y conclusiones

Dado que la primera parte del título fue posiblemente el factor más importante en la viralización del documento, es apropiado para investigadores preguntarse si la elección de un título llamativo o irónico es beneficioso o perjudicial a largo plazo para su trabajo. Por un lado, el alcance de la investigación de Salinas (2024) fue muy amplio y llegó a tener la atención de un público que posiblemente no tendría de otra manera. Sin embargo, el hecho de que la tesis esté asociada con esta controversia, al grado de haberse convertido por un tiempo en un meme asociado a la ridiculización, posiblemente pueda disuadir a alguien de leerla. De igual manera, el estudio de la cultura popular como el anime parece gozar de poco o nulo reconocimiento ante los ojos del público general, y controversias como la presente podrían reforzar la percepción negativa de las investigaciones de comunicación, humanidades o

estudios culturales mientras no haya un discurso que contrarreste la negatividad, lo cual es difícil que ocurra debido a la naturaleza de los algoritmos de redes sociales que favorecen discursos populares (Sîrbu et al, 2019).

El fenómeno viral también evidenció la presencia de homofobia en el discurso cotidiano de redes sociales. Aunque el título contribuyó en parte a la reacción negativa, la mera atención al fenómeno de estudio que explora tesis fue suficiente para que usuarios expresaran negatividad hacia hombres gays o LGBTQ+ en general. Se pudo observar un discurso que menospreciaba la idea de los hallazgos de la tesis, parte sentimiento de rechazo común en redes sociales hacia lo que se considera coloquialmente *woke* o *progre* (Brandariz, 2024), como puede ser la enseñanza o investigación de temas de diversidad sexo-genérica. Esto habla de la necesidad de continuar con esfuerzos sociales para fomentar la inclusión y el respeto hacia poblaciones oprimidas por su orientación sexual.

Una emoción subyacente a la burla que fue evidenciada por las narrativas asociadas a la crítica al trabajo de investigación y a las instituciones es la de la ira o enojo. Es evidente que muchos usuarios, usando como excusa la controversia, aprovecharon la oportunidad para expresar su frustración hacia el país y sus instituciones, los cuales perciben como decepcionantes o incluso en decadencia, en particular con lo que se refiere a los gastos del gobierno. La tesis sobre *Sailor Moon* de un estudiante de una universidad privada —financiada con recursos públicos— se convierte entonces en un símbolo, un meme como parte del discurso público (Ruiz, 2019), asociado a la superficialidad o falta de seriedad de la educación superior frente a problemas considerados de mayor prioridad en México. Relacionado con lo anterior, las ciencias exactas se asocian con una mayor objetividad y por ende más útiles para ayudar al país, contrario a la exploración de las distintas realidades y subjetividades que abordan las humanidades. El trabajo de quienes se desempeñan en humanidades y ciencias sociales es entonces también divulgar el valor de sus investigaciones y cómo se pueden complementar a otras áreas de conocimiento y resolución de problemas prioritarios.

Es importante también destacar el papel de los medios digitales como las páginas de Cadena Informativa Campeche y El Editorial en la propagación de las narrativas virales a través de la presentación y lenguaje de la nota. Se ha identificado que el *clickbait* es una estrategia muy utilizada en espacios virtuales para atraer la atención del usuario y guiar tráfico e interacciones a un sitio web o perfil de redes (Palau Sampio, 2016). Por ello la distorsión y simplificación de un fenómeno con fines de generar una reacción visceral del usuario puede ser algo premeditado para beneficiarse del funcionamiento del algoritmo, lo cual es una discusión aún en pie sobre la ética de los medios y el periodismo en redes sociales (Rahman, 2023).

Entre las limitaciones de esta investigación, es importante reconocer que algunos comentarios podrían provenir de *bots* o un programa de respuestas automatizadas no humanas, lo cual puede afectar la autenticidad de las opiniones registradas (Cobos, 2024). Dado que este artículo se enfocó únicamente en Facebook, quedaron fuera plataformas como X o TikTok, lo que limita la comprensión del fenómeno por parte de otras audiencias. Dado que solo se trabajó con texto escrito, no se analizaron imágenes o videos que algunos usuarios podrían haber incluido y que aportarían un


contexto visual adicional. Por último es relevante mencionar que las páginas de Facebook elegidas no son homogéneas; unos son medios informativos y otras son de carácter menos serio, lo cual diversificó la muestra pero podría haber afectado la consistencia del análisis.

La metodología propuesta en este trabajo permite replicar la manera en la que se pueden analizar comentarios en línea, por lo cual se puede usar para acercarse a otro tipo de fenómenos virales similares. Para futuras investigaciones similares se recomienda expandir el análisis a varias plataformas sociales y considerar tanto el contenido visual (imágenes, memes) como el texto de los comentarios. Asimismo, sería útil emplear métodos que permitan verificar la autenticidad de los comentarios y optar por muestras más homogéneas o bien categorizar las fuentes para un análisis más controlado. Se podría incluir también un análisis de temas de tendencia previos que permitan analizar el contexto sociopolítico antes y durante la controversia para identificar actores que pudieran beneficiarse del fenómeno viral.

Como recapitulación, aunque la tesis *Sailor Moon me hizo gay* generó fuertes críticas y descalificaciones, también despertó en menor medida un interés genuino y discusión entre usuarios que valoran la temática propuesta para matizar un fenómeno complejo como lo es el de la construcción de identidad de hombres gays en el país. El presente trabajo evidenció que la realidad sociopolítica y las desigualdades de México están presentes en la mente de muchos usuarios de redes sociales, por lo que se puede intuir que el humor a través de la burla puede ser una estrategia para liberar tensión. Tanto los actores individuales como los medios de comunicación e instituciones tienen el poder de influir en las narrativas virales mediante la forma en la que divulgan la información, de manera distorsionada y amarillista o informada y matizada.

Referencias

- Aguilar Pérez, M., Pérez Díaz, M., & Salazar Nieva, D. (2022). Entre la celebración y el vilipendio: narrativas virales sobre la docencia en medios de comunicación y redes sociales. *Diálogos Sobre Educación. Temas Actuales En Investigación Educativa*, 13(24), 1–16.
- Ashar, L. C. (2024). Social Media Impact: How Social Media Sites Affect Society. In *Business and Management Blog. American Public University*. <https://www.apu.apus.edu/area-of-study/business-and-management/resources/how-social-media-sites-affect-society/>
- Básica, P. (2024). ¿Me puse a leer la tesis de sailor moon y su relación con la identidad gay millennial en México? Sí [publicación con imagen]. In *Facebook*. <https://www.facebook.com/photo/?fbid=895540035936487>
- Berger, J., & Milkman, K. L. (2012). What Makes Online Content Viral? *Journal of Marketing Research*, 49(2), 192–205. <https://doi.org/10.1509/jmr.10.0353>
- Brandariz, C. (2024). Corrección política, woke y progre: un ensayo para entender todas esas ideas. *Clarín*. https://www.clarin.com/cultura/correccion-politica-woke-progre-ensayo-entender-todas-ideas_0_XouMFTbgHJ.html
- Campeche, C. I. (2024). *Presentan Tesis basada en Sailor Moon en el TEC de Monterrey. "SAILOR MOON ME HIZO GAY"* 🤔🤔 La tesis [publicación con imágenes]. <https://www.facebook.com/share/p/Ht4WnoAWbkKHxka/>

- Cobos, T. L. (2024). El problema de los bots y las audiencias digitales. In *Attúa: Revista de periodismo científico*. <https://attuaautb.com/index.php/2024/02/03/el-problema-de-los-bots-y-las-audiencias-digitales/>
- Conahcyt. (2024). Convocatoria Becas Nacionales para Estudios de Posgrado 2022. In *Conahcyt: Consejo Nacional de Humanidades, Ciencias y Tecnologías*. <https://conahcyt.mx/convocatorias/convocatorias-becas-nacionales/convocatoria-becas-nacionales-para-estudios-de-posgrado-2022/>
- Creswell, J. W. (2014). *Research design: qualitative, quantitative and mixed methods approaches*. SAGE Publications Inc.
- Dafonte Gómez, A. (2015). *Aproximación teórica al concepto de viralidad desde el punto de vista de la comunicación: aplicación y repercusiones en los contenidos publicitarios audiovisuales*. <http://hdl.handle.net/11093/390>
- de Monterrey, T. (2024). Maestría en Estudios Humanísticos (MEH). In *ecnológico de Monterrey: Posgrados y Educación Continua*. <https://maestriasydiplomados.tec.mx/posgrados/maestria-en-estudios-humanisticos>
- Deforma, E. (2024). Los becarios podrían burlarse de estas formas de titulación, pero no pueden porque no se han titulado... [carrusel de imágenes]. In *Instagram*. https://www.instagram.com/p/C-5c2jViobS/?utm_source=ig_web_copy_link&igsh=MzRIODBiNWFIZA%3D%3D
- Editorial, E. (2024).  SE VIRALIZA POLÉMICA TESIS DE MAESTRÍA SOBRE "SAILOR MOON"... En redes sociales, se ha hecho viral una tesis [publicación con imágenes]. In *Facebook*. <https://www.facebook.com/EIEditorialTam/posts/pfbid0837KYMxbTt9JXYCGPR1A2cV6cuz4n8uWGfbRpJAJJykvG1AwzeHDd4J723k67ogwl>
- Espina Vergara, A. (2017). De memes, cartones y política. Cuando la cultura viral aterriza en la política. *Gobierno y Bien Común*, 273, 5–8. https://auroraespinavergara.com/wp-content/uploads/2020/09/822_aurora_espina-de_memes_cartones_y_politica.pdf
- García Orozco, J. (2024). Lo de la tesis de Sailor Moon del Tec no es broma. Ya la leí y se trata de un [publicación con imágenes]. In *X*. <https://x.com/jorgegogdl/status/1825285266946560398>
- Goffman, E. (1989). *Estigma: la identidad deteriorada*. Amorrortu.
- Hinojosa, S., & Quezada, A. (2017). México mágico: surrealismo latinoamericano. *Casa Del Tiempo*, 3(40), 16–19.
- Izquierdo, I. (2024). ¿UNAM o Tec de Monterrey? Esta es la universidad que tiene más prestigio a nivel internacional. In *Infobae*. <https://www.infobae.com/mexico/2024/05/11/unam-o-tec-de-monterrey-esta-es-la-universidad-que-tiene-mas-prestigio-a-nivel-internacional/>
- Manovich, L. (2020). *Cultural Analytics*. MIT Press.
- Moonie, S. (2024). Contexto: El Tecnológico de Monterrey aprobó una tesis titulada "Sailor Moon me hizo gay. La subjetividad e identidad del hombre [publicación con imagen]. In *Facebook*. <https://www.facebook.com/photo/?fbid=1092661908886573>
- Rahman, H. U. (2023). Media Ethics in the Era of Clickbait Journalism: Ethical Dilemmas and Solutions in Online Media. *JSSR*, 3(4), 11–20. <https://doi.org/10.54183/jssr.v3i4.392>
- Robinson, D. (2021). *Package "widyr". widyr: Widen, Process, then Re-Tidy Data*. <https://cran.r-project.org/web/packages/widyr/index.html>
- Rubín, T. (2024). No creí que fuera a tener ese impacto'. *Reforma*. <https://www.reforma.com/no-crei-que-fuera-a-tener-ese-impacto/ar2860413>
- Ruiz Martínez, J. M. (2019). Memes y transmedia: los memes como fenómeno transmedial y la memética como factor de la expansión transmedial. In *Narrativas transmediales: la metamorfosis del relato en los nuevos medios digitales* (pp. 107–123). Gedisa.
- Salinas Lara, D. E. (2024). *Sailor Moon me hizo gay: la subjetividad e identidad del hombre gay millennial mexicano desde el consumo de Sailor Moon*. <https://hdl.handle.net/11285/676844>

- Sharma, K., Zhang, Y., & Liu, Y. (2022). COVID-19 Vaccine Misinformation Campaigns and Social Media Narratives. *Proceedings of the International AAAI Conference on Web and Social Media*, 16(1), 920–931. <https://doi.org/10.1609/icwsm.v16i1.19346>
- Shiller, R. J. (2019). *Narrative economics: how stories go viral & drive major economic events*. Princeton University Press.
- Silge, J., & Robinson, D. (2022). *Package 'tidytext'. Tidytext: Text Mining using "dplyr", "ggplot2", and Other Tidy Tools*. <https://cran.r-project.org/web/packages/tidytext/index.html>
- Silverio, M. (2024). Las redes sociales más usadas en 2024. In *PrimeWeb*. <https://www.primeweb.com.mx/redes-sociales-para-empresas>
- Sîrbu, A., Pedreschi, D., Giannotti, F., & Kertész, J. (2019). Algorithmic bias amplifies opinion fragmentation and polarization: A bounded confidence model. *PLOS ONE*, 14(3), e0213246. <https://doi.org/10.1371/journal.pone.0213246>
- Tapia Sandoval, A. (2024). "Sailor Moon me hizo gay": Tesis del Tec de Monterrey genera intenso debate en redes sociales. In *Infobae*. <https://www.infobae.com/mexico/2024/08/19/sailor-moon-me-hizo-gay-polemica-tesis-del-tec-de-monterrey-genera-intenso-debate-en-redes-sociales/>
- Velázquez, A. (2024). Tesis que alude a anime 'Sailor Moon' no es del periodista Genaro Lozano. In *Animal Político*. <https://animalpolitico.com/verificacion-de-hechos/desinformacion/tesis-sailor-moon-no-periodista>

¹ Reddit es una red social que funciona como una colección masiva de foros de temas diversos cuyos comentarios pueden ser promovidos o rechazados a través de votación por parte de cualquier usuario.

² Este posgrado es un programa interdisciplinario de humanidades orientado hacia la investigación, alineado con los Objetivos de Desarrollo Sostenible 2015-2030 de la ONU, que busca promover el análisis y reflexión crítica de fenómenos culturales contemporáneos (Tecnológico de Monterrey, 2024). Como posgrado adscrito al Conahcyt, en 2022 los alumnos del programa recibían un apoyo mensual inicial de \$13,162.90 mensuales que se prolongaría hasta concluir en un máximo de dos años (Conahcyt, 2024).

³ Los me gusta y seguidores se revisaron el 05/09/2024.