Establishing a Blockchain-based Architecture for Fake News Detection

Valdemar Vicente Graciano-Neto
valdemarneto@ufg.br
Federal University of Goiás (UFG)
Goiânia, Brazil

Jacson Rodrigues Barbosa
jacson_rodrigues@ufg.br
Federal University of Goiás (UFG)
Goiânia, Brazil

Eliomar Araújo de Lima
eliomar.lima@ufg.br
Federal University of Goiás (UFG)
Goiânia, Brazil

Luiza Martins de Freitas Cintra
cintraluiza@discente.ufg.br
Federal University of Goiás (UFG)
Goiânia, Brazil

Samuel Venzi
samuel.venzi@goledger.com.br
GoLedger
Brasília, Brazil

Mohamad Kassab
mkassab@ieee.org
The New York University at Abu Dhabi
Abu Dhabi, Arabi Emirates

ABSTRACT

Fake News are a contemporary phenomenon with potential devastating effects. For inquiry and auditability purposes, it is essential that the news, once classified as false, can be persisted in an immutable means so that interested parties can query it. Although Blockchain clearly satisfies the main requirements for Fake News Management Software Systems, the prescriptive architectural solutions for that domain that cohabit Blockchain with other technologies in a single proposal still need to be made available. This paper's main contribution is presenting a prescriptive architectural solution for blockchain-based fake news management software systems. The Hoffmeister process for software architecture design is systematically followed to culminate in a software solution for that domain. The implementation of a candidate architecture and a brief simulation-based evaluation show the feasibility of the solution to satisfy the functional and quality requirements.

KEYWORDS

fake news, blockchain, disinformation, blocking, detection

1 INTRODUCTION

Fake News are a contemporary concern that impacts several scenarios over the world [4, 6]. According to the World Economic Forum, misinformation[1] is at the top of global risks in 2024 [39]. Although Artificial Intelligence (AI) models can recognize potentially false information, there is a proliferation of novel forms for creating and spreading false content. A Gartner survey with more than 200 consumers between July and August 2023[2] revealed that 53% of consumers believe that the current state of social media has worsened. Furthermore, criminal acts generated from the use of *DeepFake* [37, 41] techniques, in which synthesized videos with audio and voice similar to those of real people, can raise the dissemination of false content to an even more worrying level. For instance during municipal elections in Brazil, that phenomenon can be even more impacting and worthy of concern, as in prior elections [2].

Although the mainstream social media platforms, such as Instagram, X, and others, have included mechanisms for detecting and containment of fake news, doubts can be raised about the interests of the owners of those private companies. Those platforms are considered centralized and monopolized since these companies' owners integrally regulate their operations [14, 27]. Hence, a decentralized solution, i.e., with no central authority and that could gather a diversity of contributors, could overcome such problem. In that sense, blockchain emerges as a suitable solution. Decentralization is a core principle of blockchain technology because it aligns with the idea of creating systems that are open, secure, and resistant to control by any single entity [23]. Based on the concepts of distributed ledger, immutability and consensus, blockchain matches the requirements of a decentralized solution and can reinforce trustability and traceability in a solution for contention of fake news dissemination in social media. Although some other solution already exist [3, 35], they do not explore some resources brought by blockchain, including tokenization.

Given the importance and urgency of the topic, ANATEL (the Brazilian National Telecommunications Agency) and the Federal University of Goiás (UFG) established a Research and Development (R&D) project to develop technologies that support the detection, classification and containment of fake news on social networks [5]. The solutions intend to support the identification of disinformation to inform citizens what is untrue information. In that context, some requirements are essential for the solution, such as security, traceability, persistence and immutability of the information about the fake news analyzed after experts classified it. Blockchain-based approaches can satisfy all those requirements, which makes it a potential option to support the conception of the architecture for the ordered solution.

The *main contribution of this paper* is presenting a software architecture of a solution for fake news detection that, besides including blockchain infrastructure, also accommodates other cutting-edge technologies needed to accordingly deal with the complexity of the problem, as priorly illustrated. The solution advances the state-of-the-art once we are unaware of other architectural proposals that cohabitate blockchain with other technologies in a single solution. To achieve this result, we provide the methodological analysis made to achieve a minimally feasible architecture (MFA) of a solution, conceived by following the canonical principles of Hoffmeister prescriptive process for software architecture design [17]. We discuss the architecturally significant requirements and the decisions that

[1] Henceforth, terms as *fake news* and *misinformation* can be used interchangeably.
[2] https://www.gartner.com/en/newsroom/press-releases/2023-12-14-gartner-predicts-fifty-percent-of-consumers-will-significantly-limit-their-interactions-with-social-media-by-2025

supported the design. A brief architectural evaluation is also provided.

The remainder of the paper is organized as follows: Section 2 presents a brief background on blockchain-based solutions for fake news detection and related work, Section 3 presents the research method, Sections 4, 5 and 6 show, respectively, the steps of Hofmeister's process: Analysis, Synthesis and Evaluation of the architectural design. Section 6 also discusses the results and threats to validity. Finally, Section 7 concludes the paper.

2 FOUNDATIONS ON FAKE NEWS VERIFICATION AND BLOCKCHAIN-BASED SOLUTIONS

Fake News creates propagation bubbles (called *echo chambers*) of untruths that, due to other problems such as the population's low media literacy and low critical sense to analyze the news they receive (in particular on social networks), end up feeding the imagination of its consumers, engaging them in movements that can become devastating. Furthermore, phenomena such as DeepFake [13, 41], in which videos that synthesize audio and voice similar to human people, can increase the dissemination of fake news. As pointed out in our prior tertiary study [13], the population's tendency is to stay in information bubbles and believe in the news and journalistic sources that most align with their worldview. Therefore, the biggest difficulty would be to point out *fake news* associated with the environment in which the individual is inserted on the mainstream media.

In this work, we distinguish the fake news processing steps (which we call *pipeline*) into (i) monitoring, (ii) extraction, (iii) classification, and (iv) containment. These steps are essential because the main architectural elements of a technological solution for fake news address one or more of these concerns. It is worth highlighting that there may be some overlapping between the terms describing the fake news pipeline in the specialized literature, as in Shu, Bernard and Liu (2019) [30]. For all intents and purposes, in this context, the main fake news processing steps are: (i) **monitoring**, which consists of the technical actions necessary to allow access to environments where fake news is often disseminated. Since many of these environments are private and owned by companies (e.g. WhatsApp, Telegram, Tiktok and Facebook), although anyone can freely access them using a free account created, access for analysis purposes is often limited. In this sense, it is necessary to obtain access, as reported by tools such as WhatsApp Monitor [22, 26]. Once you have access, the next step is **information extraction** or detection, that is, using technological resources that allow you to detect potential disseminators of fake news in addition to enabling the next steps to recognize the material produced, such as, for example, not only recognizing fake news in text, but also in audio, video and images. Once you have such information, you can proceed to the **classification** stage, using technical resources to classify news as true, false or biased. Lastly, we have the **containment** stage, in which actions can be taken to prevent or interrupt the spread of news considered false.

In the realm of blockchain-solutions for fake news containment, smart contracts play a crucial role. Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They run on blockchain networks and automatically enforce and execute the terms of a contract when predefined conditions are met. They can enhance the functionality, security, and efficiency of both the consensus (voting) mechanisms, supporting the voting and applying the rules defined for the domain to compute the votes and the result [15].

Related Work. Blockchain has been adopted in solutions of many domains, such as for query and registration of student degree certificates [1], healthcare [20], supply chain [36] and document registration service [31]. The adoption of blockchain in solutions for fake news is also not new in literature, but still a significant concern [8, 21, 29, 42]. Some existing solutions are primarily focused on the voting process to reach a consensus on the degree of fakeness of some news, working on the consensus algorithms to label the news accordingly and persist it in the blockchain. Torky et al. (2019) [33] approaches the Proof of Credibility, which establishes a formula for assessing the credibility of the source that publishes the posts; however, they value the number of followers and similar prior publications, which can be too abstract and inaccurate regarding the provenance of the source of that news. Sengupta et al. (2021) proposes the ProBlock approach [28], also based on consensus algorithms to assess the credibility of the fact-checkers, people and organizations involved in the process of classification named as *fact-checking*.

Duzen et al. (2023) [9], for instance, present a software architecture of a tool to deal with fake news, but focusing on Social Network Analysis (SNA), not including blockchain. Kozik et al. (2023) [21] also proposes an architecture for the same domain, not including blockchain. DiCicco and Agarwal (2020) [8] surveyed the literature to collect Blockchain Technology-Based solutions that fight misinformation. The authors discuss nine solutions proposed by 2020, presenting their pros and cons. However, only one of them (New York Times News Provenance Project) provides architectural details, such as externalizing plug-ins and an API for developers building applications.

Other studies provide insights and highlight the relevance of *blockchain-based* technologies in mitigating the challenges associated with disseminating false information. Paul et al. (2019) [24] addresses the dissemination of *fake news* on social networks, highlighting the importance of security in transactions and the ability of *blockchain* to verify reliable sources. The use of *peer-to-peer* network concepts is proposed as an effective strategy for detecting fake news in social environments. Waghmare and Patnaik (2021) [34] proposes an innovative approach by combining machine learning and *blockchain* in detecting *fake news*. The creation of a *blockchain* environment stands out, integrating mining, smart contracts and *Proof of Work (PoW)*, with a particular emphasis on the reliability of detection through *machine learning* techniques. Qayyum et al. (2019) propose a *framework* based on *blockchain* to prevent *fake news*. Design issues and important considerations are discussed, offering a comprehensive look at the challenges faced in the post-truth era. Dwivedi et al. (2020) [10] focuses on identifying the sources of *fake news* using *blockchain*, presenting a framework based on *blockchain* and watermarking. The ability to track the origin of fake news stands out, providing a solution to reduce its spread. Xiao, Liu and Li (2020) [40] approaches the *Internet of Vehicles* (IoV) and proposes the *framework Quick Fake News Detection* (QcFND). They integrate technologies such as *Software-Defined Networking*

(SDN), *edge computing* and *blockchain*. Jing and Murugesan (2019) [19] implement *blockchain* on social networks to build trust in news content. The integration of *blockchain* technology with advanced artificial intelligence stands out to verify the credibility of news, emphasizing the prevention of negative impacts on society.

The existing solutions are generally not accommodated in a more complex architecture (like ours). Moreover, most solutions cover only one of the steps of the fake news processing pipeline and few relevant functionalities; our solution intends to cover a more robust set of functionalities.

3 RESEARCH METHOD

Before the design of the architecture take place, a scientific workflow was firstly conducted in conformance to the following steps: (i) Exploratory literature review, for acquiring knowledge and expertise in the fake news domain, (ii) Systematic tertiary review, to systematically collect evidence from the literature (which culminated in a publication [13]), (iii) Requirements elicitation meetings with the sponsor, and (iv) brainstorming. All these steps served to collect the requirements that are input for the architectural design reported in this paper, as follows.

The research method of this study was inspired by Abreu et al. (2020) [1] and involves the following steps: (i) Design of the architecture, following the systematic process proposed by Hofmeister et al. (2007) [17], which involves the illustration of the typical user scenario and the assessment of candidate architectures, (ii) Development of a prototype for an application; and (iii) Evaluation, involving the *Technical validation of the prototype*, which maps the prototype characteristics with the criteria defined by Ciccio et al. (2020) [7], *Validation of the prototype for the applicability of the blockchain*, analyzing the viability of using blockchain for that solution through the steps described in Pedersen et al. (2019) [25]; and *Prototype validation with user*, exposing a real typical user to experience the use of the prototype, and conducting interviews, with pre-established questions, aiming to compare the use of the tool with the current usage process.

4 ARCHITECTURE DESIGN

In conformance with the best practices of the state-of-the-art software architecture design (and analogously to what is conducted by Teixeira et al. (2020) [32]), we followed the process proposed by Hofmeister [17] to drive the design of our software architecture. The model consists of three well-defined steps: (i) Analysis, (ii) Synthesis, and (iii) Evaluation, discussed as follows. It is important to emphasize that the requirements (functional and quality requirements) used as input for the architectural design were collected in meetings with the Sponsor in the early moments of the project.

4.1 Step 1: Analysis

This step receives, as inputs, a description of the context and the architectural concerns. As a result, the problems that the architecture solves are then found, also known as Architecturally Significant Requirements (ASR).

4.1.1 Scenario description. Figure 1 illustrates the motivational scenario. Ideally, a solution for fake news should have undeniable access to monitor all the news published in a diversity of social networks (e.g. X, Facebook, Instagram, TikTok), communication platforms (e.g. WhatsApp and Telegram), and portals (e.g. YouTube, News Portals and others) in a diversity of formats (text, audio, video and images) (**Step 1**). Once suspicious content is detected, it should be collected by the tool and made available for analysis (**Step 2**). The analysis (**Step 3**, called as *fact-checking*) can be done under two perspectives: manual (by human fact-checkers, which can be independent freelancers or people of renowned reputation linked to fact-checking agencies) and/or semi-automatic (by AI techniques, such as sentiment analysis, information retrieval, large language models (LLM), natural language processing - NLP, and machine learning - ML). Both approaches can be performed in parallel to double-check the result (true, false or biased) before it is delivered, enhancing the confidence of the final deliberation.

Step 4 is triggered in parallel: the semi-automatic approach endorsed by AI and the human voting supported by blockchain (the reason why there are two 'steps 4' in the figure). In the semi-automatic approach, the first step is a crawling stage (**Step 4**) to search for similar or the same news in public portals (with recognized credibility), repositories of labeled news in public agencies and also in the blockchain of the system, since that publication may have already been previously labeled. Likewise, it triggers the automatic processing mechanism (**Step 5**). This mechanism automatically extracts information from the news, recognizing typical terms and expressions in sensationalist texts. Llama LLM[3] is also used as an oracle for that query[4]. Once many of those attributes are found in a single news, it receives a propensity score of falsehood, ie., a score that varies from 0 to 1; the closer the score is to 1, the more likely the news is false. Once the result is delivered, the news is labeled and persisted in the blockchain (**Step 6**), with the result also being delivered to the fact-checkers in case they are still investigating it. In **Step 7**, which is not focus of this paper, the post labeled with the result is then disseminated in the social networks towards containing/fighting the corresponding fake news dissemination.

In the manual approach, human fact-checkers analyze the suspicious news, searching for evidence that show the news is false. A voting process then takes place according to a consensus mechanism supported by smart contracts. Several consensus mechanisms exist; it can be a simple majority or a more intricate formula that expresses the credibility of the source and the effectiveness of the fact-checkers in prior judgments on fake news. Each available and involved fact-checkers vote on the likely fakeness of that news and explain/rationale that justifies/supports his/her decision. Once the consensus is reached, the decision is registered, the news is labeled and persisted in the blockchain.

In both cases (manual and semi-automatic), the result can be spread on social networks to prevent other people from believing that the news is true. Crypto tokens can also be implemented on top of the blockchain so that fact-checkers can be rewarded for their services in crypto assets.

4.1.2 Architectural concerns. Regarding the blockchain, the main objective of the system is to provide a decentralized Proof of Concept

[3] https://llama.meta.com/

[4] For deciding on Llama, an experiment was performed comparing results with ChatGPT 3.5, which will not be detailed due to space restrictions.

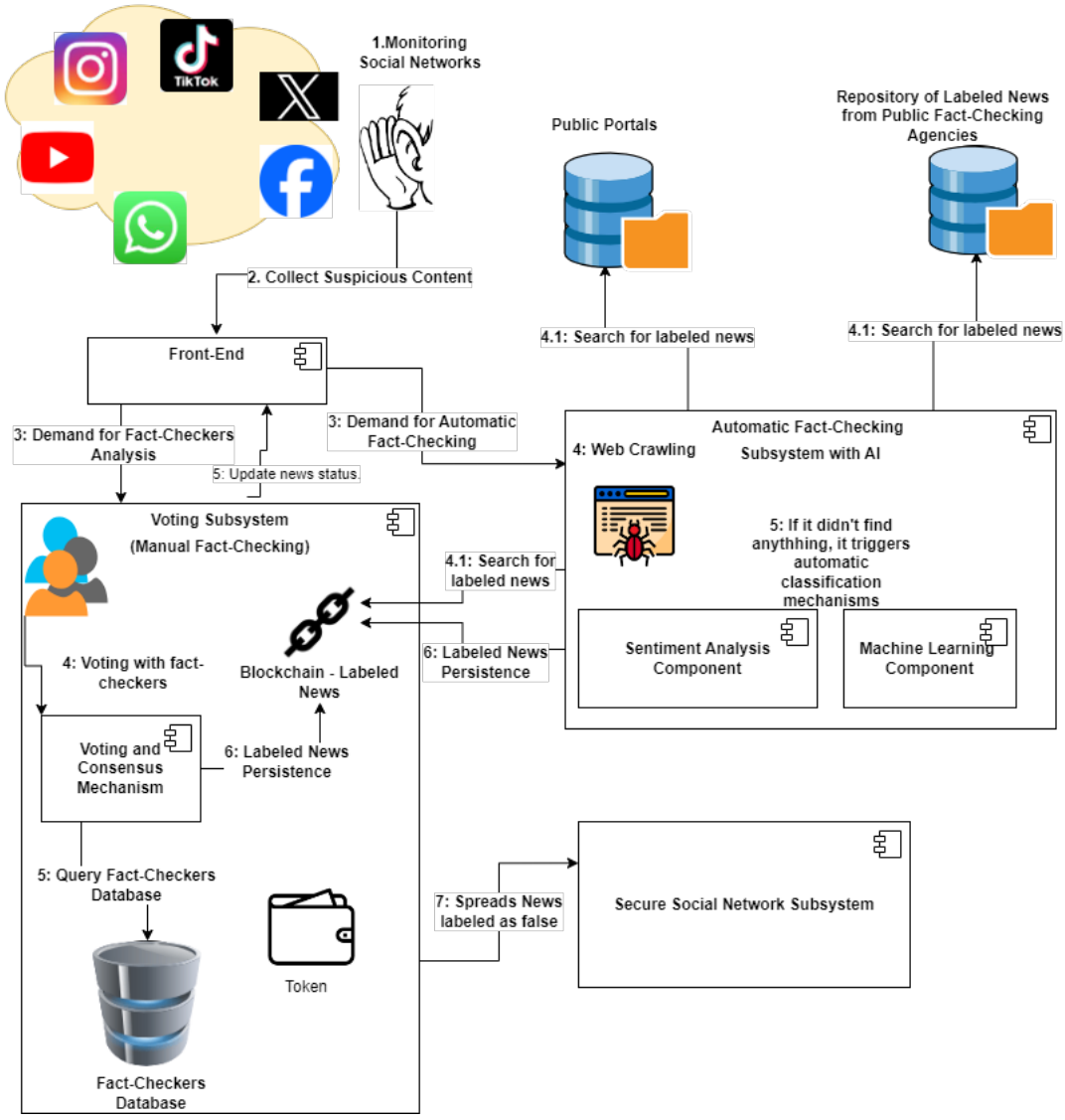

Figure 1: Motivational Scenario on Fake News processing. Extracted from Private Technical Report [5].

(PoC) solution that meets the following main functionalities: **offering a voting mechanism for fact checkers** and support **security, provenance and immutability**.

4.1.3 Architecturally Significant Requirements (ASR). As mentioned earlier, ASR are the problems that the architecture must solve. They are a subset of the requirements that must be met before the architecture can be considered "stable". For each Significant Macro Requirement (SMR), respective ASRs can be derived. Next, we discuss the requirements and their respective ASRs.

[SMR1] Interoperability - It refers to the degree to which two or more systems, products or components can exchange information and use the information that has been exchanged [18]. The consensus/voting mechanism has to be interoperable. The system should externalize an API (as reported in [8]) for invoking services such as querying the base of news labeled as true, suspicious or false. Under this perspective, the system should be able to:

- *[ASR1] Communicate with external agencies and repositories:* The system should be capable of querying public repositories of fact-checking agencies and public portals;
- *[ASR2] Receive request for capabilities/information*: The system should also be capable of providing an interface for queries and for other developers to create solutions, forming an ecosystem;

[SMR2] Performance and Real time - The response time for returning a query to the public blockchain should not exceed a given threshold. Moreover, fact-checking agencies should be able to carry

out their vote as soon as there is novel suspicious news. Consensus should also take no more than a given threshold. Under this perspective, the system should cope with the following ASR:

- *[ASR3] Vote about the news authenticity (True, False, Partial):* The system should support the fact-checkers to vote about the likely fakeness of a publication and also include explanation/decision justification field, mentioning the source, social network analysis, and the type of manipulation, such as a content taken out of context and others. This should happen in a timely manner (couple hours, if feasible), since the impacts of the fake news dissemination increases over time. This imposes a restrict performance threshold, demanding real-time response, if possible;

[SMR3] Scalability: It must be possible to expand the user list to allow access to hundreds or thousands of fact checkers. Public blockchain query users can reach millions of hits and the application should be accordingly adjusted.

[SMR4] Descentralized/Modularity: In a decentralized blockchain network, no one has to know or trust anyone else. If a fake news vote's ledger is altered or corrupted in any way, it will be rejected by the majority of the fact-checkers in the network. The solution architecture must be modular in the sense of allowing functionality to be accordingly accommodated.

[SMR5] Integrity/Immutability and Traceability: All news labeled and persisted on the public blockchain must be backed by those persisted on the private blockchain.

- *[ASR4] List Suspicious News:* The system should be capable of listing emerging publications with suspicious content;
- *[ASR5] Dispatch news classification order*: The system should notify fact-checkers about the need to judge the veracity of one or more news and trigger the classification process in both manual and automatic approaches;
- *[ASR6] Create a unique hash for the news:* The system should receive the news in any format (image, video, text or audio) and generate a correspondent hashing code to uniquely identify it in the system;
- *[ASR7] Obtain news metadata:* The system should collect relevant metadata from the news, such as creation date, content, author, source platform and others;

[SMR6] Security: The system should be secure for all the potential users: fact checkers, news consumers, and agencies.

- *[ASR8] CRUD Fact-Checkers:* It should be possible to Create, Read, Update, and Delete fact-checkers in the system database;
- *[ASR9] Login (for Fact Checker)*: The access to the system should only be granted under credentials;

[SMR7] Rewarding: The system should encourage the participation of fact-checkers (remuneration in crypto or some other asset - currency, social asset, etc. - taking care to make the entity vote responsibly, trying to equalize the accuracy of voting with the desire to do quickly to gain more financial return with each contribution; think about the degree of reliability/credibility, etc.)

The Step 2 (Synthesis) will be shown in a separate section, since it comprises the conception of the tool itself, as follows. And Step 3 (Evaluation) will be shown in the following section.

5 PROOF OF CONCEPT

This section shows the results of the Step 2, synthesis step, of Hofmeister's process. The output of this activity is an architectural solution to be assessed against the prioritized problems. Thus, it moves from the problem to the solution space [17].

5.1 Architectural Solution based on Hyperledger Fabric

This candidate architecture uses Hyperledger Fabric. Details are shown, as follows.

Rationale for Using Hyperledger Fabric. Hyperledger Fabric is an open-source framework for private blockchains managed by the Hyperledger Foundation. The platform provides a fully-featured and modular architecture, allowing flexibility and expansion depending on the use case. One distinctive characteristic of Fabric is its concept of organizations, which makes it more suitable for enterprise situations. Organizations own components that interact in the network, peers, and orderers (as shown in Figure 2). Each component has its responsibility within the lifecycle of a transaction. [11]

Hyperledger Fabric supports smart contracts, often called chaincodes, written in general purpose languages, namely Go, Java and JavaScript [11]. This lowers the development barrier and allows language-specific resources to be used in implementation, enabling more complex applications to be developed. Many blockchains implement a *Order-Execute* sequence for transactions, whereas Fabric implements a *Execute-Order-Validate* sequence, which enables much more secure and consistent blocks with finality. Hyperledger Fabric implements the concept of channels, where each channel has its own configuration, member organizations and hosts its ledger. Organizations can be part of multiple channels simultaneously, allowing a peer to host multiple ledgers without mixing different data scopes. This means that, unlike most blockchains, a node can be a part of multiple ledger-sharing channels, creating an extensive network [11]. Fabric also implements what are called private data collections (PDCs). PDCs are environments for private data registration in a given chaincode. Only organizations that are members of the collection are given read access to data. The data is shared peer-to-peer via a gossip protocol and is never registered in the ledger. The ledger registers the hash of the private information to allow for proof of registry by parties involved [11].

CC-Tools is a Hyperledger Labs open-source project and part of the toolkit for application development. CC-Tools provides features regarding asset, data type, event and transaction development. CC-Tools allows for more complex chaincodes while decreasing development time. This project supports chaincodes written in Go language and fully compatible with all major Fabric long-term support (LTS) versions. Hence, several features of Hyperledger Fabric can be listed as justifications for its choice, such as (i) Modular architecture, (ii) Smart contract flexibility, (iii) Security, (iv) Consensus, (v) Privacy, (vi) Performance [12], (vii) Scalability, and (viii) Monitoring.

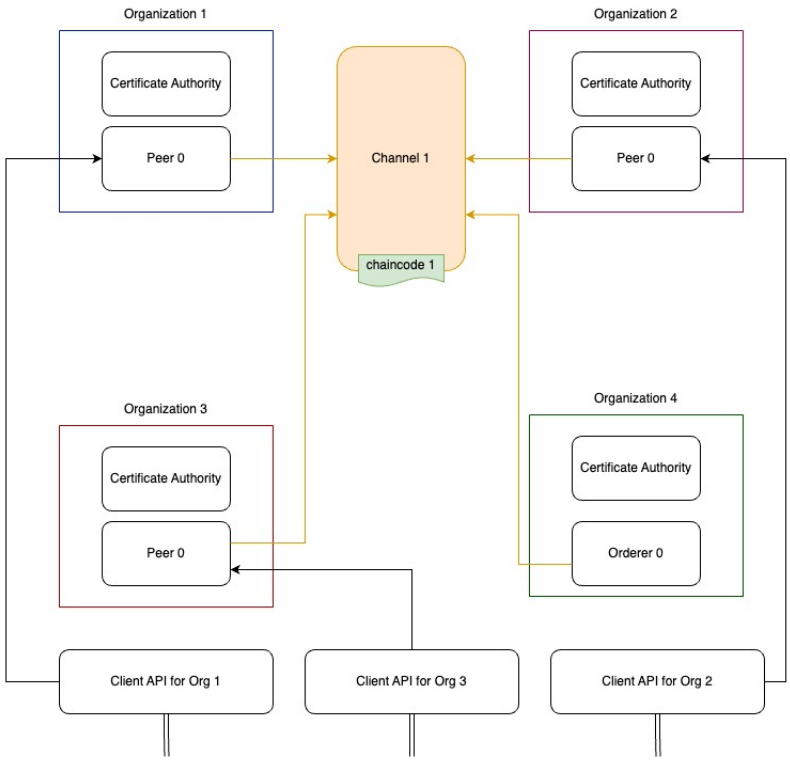

Figure 2: Diagram for the candidate architectural design with Hyperledger Fabric. Extracted from Private Technical Report [5].

Architectural Design. Hyperledger Fabric provides all the features needed to create an entire network architecture for the proposed application. Chaincode implementation was done using the CC-Tools Hyperledger Labs project, where a CC-Tools-Demo repository was used as a base template for the implementation. This repository provides a working test network with three application organizations with one peer each and an ordering organization with one orderer, as shown in Figure 2. The organizations are members of a channel where the chaincode proposed is instantiated. Three client APIs are also provided, tied to identities for each one of the application organizations.

Chaincode implementation. The chaincode is implemented by defining the core assets and transactions within the structure provided by CC-Tools. Assets act as the data mapping that will be registered, that is, the actual properties that will be registered. Transactions implement the business logic that will act on ledger data, either reading from it or writing to it.

API implementation. The client API is implemented in Go using the Fabric SDK package for interaction with the ledger. This API utilizes a certificate and private key issued by the CA of a trusted organization in the channel. These credentials authorize the API to interact with network. The API utilizes the Gin package for creating a REST API that exposes SDK functionality. For compatibility with older and newer versions of Fabric, the API implements endpoints that utilize a legacy SDK for transactions and a newer Gateway SDK that uses the peer Gateway Service, that facilitates transaction submission.

To cope with the raised requirements, we conceived a candidate architectural solution with the following main modules.

Automatic FactChecking Subsystem - This is the subsystem responsible for conducting the web crawling in public portals, to search in the blockchain and conduct automatic analysis based on AI in the selected content. *Matches ASR7.*

Human Fact-Checkers Subsystem - This subsystem involves the management of the database of human fact-checkers, the voting and consensus mechanism (materialized in a smart contract), and the blockchain itself with its interface to interoperate, externalize access and receive persistence demands. *Matches SMR3, ASR4, ASR5, ASR6, ASR8, ASR9 and SMR7.*

Voting and Consensus Mechanism - This component manages the voting and consensus between the human fact-checkers to decide the legitimacy of the content of the news being analyzed. It is a component within the Fact-Checkers Subsystem. *Matches ASR3.*

Secure Social Network - This component will be implemented to support a secure social network. *Matches SMR6.*

Services interface - This part, not explicitly captured in the model of Figure 2, regards to the interfaces externalized for client consumers and software developers that can access and build applications over our public infrastructure, besides the hooks used to consult the external databases of public portals and social networks. *Matches ASR1 and ASR2.*

Final Technological Considerations. Hyperledger Fabric provides enhanced transaction confidentiality through its architecture, which supports the execution of transactions within a private context. This

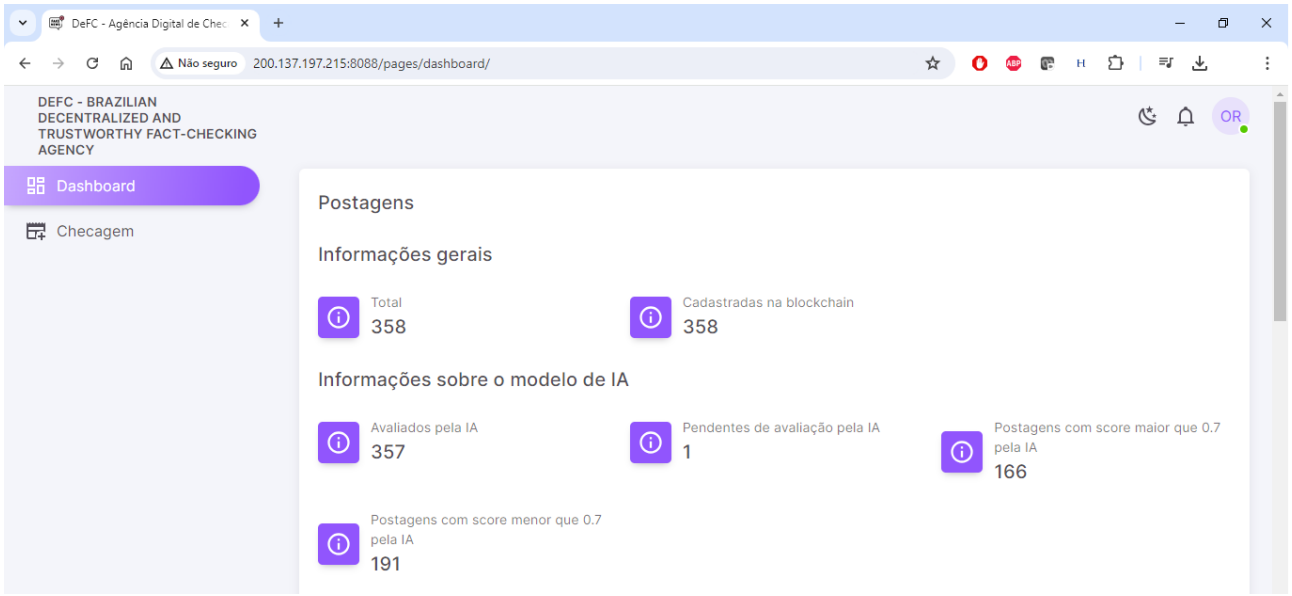

Figure 3: A screenshot of the interface of the tool conceived on the selected architectural design.

is facilitated by its unique approach to channels, where a subset of participants can conduct transactions privately, a particularly appealing feature for applications requiring confidentiality in their operations. An option, Hyperledger Besu, offers privacy features, such as private transactions and privacy groups. However, these are built on top of a platform initially designed for public network compatibility, making Fabric's privacy features more robust for some applications. Additionally, Hyperledger Fabric supports using general-purpose programming languages for crafting smart contracts. Fabric's chaincode can exploit the comprehensive functionalities offered by languages like Go and their extensive libraries. This distinction allows for a broader and more versatile development environment in Fabric, catering to complex enterprise needs beyond the scope of what Solidity and the EVM can provide on other blockchains, such as Besu. Once the candidate architectural solution complies with and satisfies the raised requirements, the proof of concept was then conceived, as follows.

5.2 Prototype

The prototype was named Brazilian Decentralized And Trustworthy Fact-checking Agency (DEFC). The screenshot shows in Figure 3, in Portuguese, one of the main menu items we have (a dashboard). The dashboard displays general strategic information for the public entities that are interested in those results, such as the total of news registered and the total registered in Blockchain, the number of news evaluated by the AI mechanism, those that still demand evaluation, the number of posts under analysis that has a score greater than 0.7 and were evaluated by the AI. The closer the score is to 1, the more likely the news is false, as priorly stated. The another main functionality is the fact-checking, which supports the fact-checker to gather evidence to judge the veracity of one or more posts under analysis, following the pipeline illustrated in Figure 1. Once a established minimum number of fact-checkers decide on the status of a post, this is revealed for all of them, stored in the blockchain, and made available for the competent authorities.

The user can assume two different roles in this tool: (i) a fact-checker, i.e., the human user who will assess the fakeness of the posts under analysis; and (ii) a curator, who will be the gatekeeper that can authorize new fact-checkers to join the board. The latter can also analyze the entire platform in a panoramic perspective.

Step 3 of Hofmeister's Process, Evaluation, is discussed in the next section.

6 EVALUATION AND DISCUSSION

An evaluation of the architecture was performed inspired in the study of Abreu et al. (2020) [1], based on User Validation Scenario, Technical Validation and Viability of the Blockchain Use, as follows. The steps are summarized due to space restriction.

6.1. User Validation Scenario. A typical user of this tool is the fact-checker, i.e., the professional dedicated to the analysis of suspect posts in social media. As such, the credentials of the tools were made available for two fact-checkers of two different agencies: Aos Fatos[5] e Boatos.org[6]. The fact-checkers could register novel news to be analyzed, obtain the score assigned by the AI mechanism and gather evidence and report on their beliefs abou the fakeness of the news just registered in the system. The score delivered by the AI subsystem is accompanied by the explainability, i.e., the reasons that led it to conclude about that post, as shown in Figure 4.

After the use, an interview was conducted with them to assess the usage of the tool when compared to the current process. The participants cleared stated that gains can be obtained from the use of that solution, including (i) **time/productivity**, since the AI mechanism already gather some evidences and scores the news; the fact-checker

[5] https://www.aosfatos.org/
[6] https://www.boatos.org/

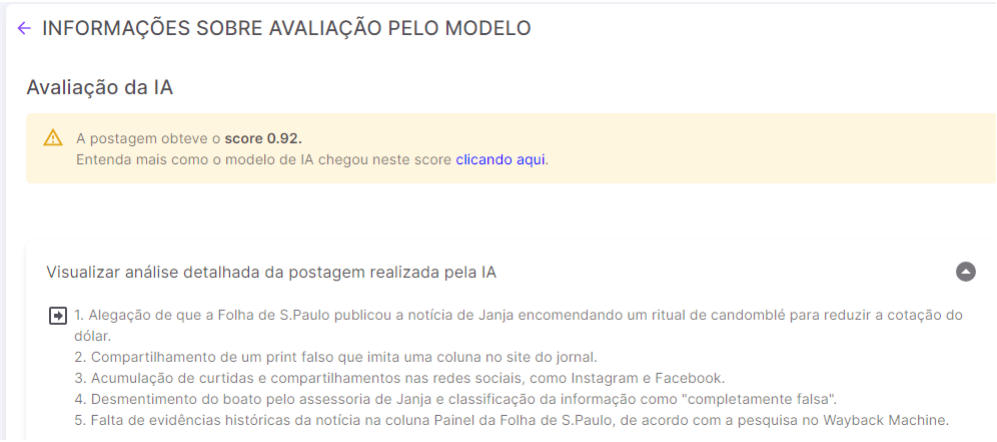

Figure 4: A screenshot of the AI classification for a single news with explainability.

only needs to complement the evidences or even agreeing with the results, accelerating the process. One participant highlighted that this is essential, since the time a fake news is being spread without being classified as such can be determinant for the impacts of it; and (ii) **reliability**, since not only a single fact-checker will work on each suspicious news, but a pool of them, supported by a consensus mechanism and the blockchain infrastructure.

6.2.Technical Validation. As shown in Figure 3, more than 300 posts were analyzed by the AI, labeled and stored in the blockchain. Abreu et al. (2020) [1] mentions the technical challenges posed by the use of blockchain in a commercial solution, as listed by Ciccio et al. (2020) [7]. The technical challenges include smart contracts (reflecting monitoring capabilities), oracles (identifying data sources) and data monitoring (balancing between data inside and outside the chain). Several other related challenges exist for each of these categories.

Abreu et al. (2020) [1], citing Ciccio et al. (2020) [7], mentions that the challenges related to smart contracts are (i) Monitoring Transparency: anybody can see the logic and data behind monitoring, data required for smart contracts must be provided and confidential data should not be shared or be protected; (ii) Observability: to access monitoring data, smart contracts must implement mechanisms to expose them, for instance, private variables can not be easily accessed; and (iii) Lack of reactivity: smart contracts can not directly invoke external services. For challenges on oracles: (i) Time management: the blockchain lacks the notion of time, and timers can not expire by themselves, an external triggering event is always required; (ii) Reliability: oracle breaks the decentralizsed trust and to compensate, several oracles should be used; and (iii) Flexibility: oracles are bound to smart contracts because a compromised oracle can not be replaced during execution, nor new capabilities can be introduced. Finally, as challenges for data management: (i) Data quality: the quality of the data influences the monitoring results, for example, poor quality data sources compromise the monitoring and once stored, incorrect data cannot be changed; (ii) Data size: the cost of the blockchain is proportional to the amount of data stored, for example, in public blockchains, monetary cost (cryptocurrency), in private blockchains, overhead on the platform, and also storing data off-chain; and (iii) Side effects: most blockchains are prone to forks, and this may cause contradictory information or interoperability issues.

Regarding those issues, about transparency, only the fact-checkers identities are confidential data that should not be shared or be protected; about observability, there is an additional layer that restricts the access only to the data that should be accessed by others, i.e., the labeled news and their history during the process; and analogously to the prior justification, the smart contracts do not directly invoke external services (Lack of reactivity); an additional layer was conceived for that purpose. About oracles, we did not have resources in the blockchain infrastructure to measure the exact time of a transaction. The approximate time of transactions was measured without the need for a policy trust between nodes. Finally, as about data management, (i) about data quality, the news were only labeled after the consensus run by the smart contracts and with results from the fact-checkers; then, the prototype has quality and correct data; (ii) about data size, only textual information was stored in the blockchain; the other information was replicated in ElasticSearch; and (iii) side effects are avoided, since the infrastructure was outsourced, and they implement mechanisms to avoid that.

6.3. Viability of the Blockchain Use. For a viability analysis, the ten steps proposed in [25] were used the Ten-step Path for Blockchain Validation, which support to decide whether or not to use blockchain technology in our prototype, as perfomed by [1]. The ten steps consist of questions that must be made before deciding to use blockchain. As a general rule, Pedersen et al. (2020) [25] recommends a blockchain is feasible to use if five questions of the applied questionnaire are answered as "Yes". We discuss each one, as follows.

Currently, the process of fact-checking is often questioned because it is performed by single fact-checkers in their agencies. Fact-checkers can have bias in their judgement and the results should be stored in a single shared space. Multiple fact-checkers from a diversity of opinions and agencies should be involved to check each news. Then, this brings Yes for the questions: **Need for a shared common database?; Multiple parties involved? Involved parties**

have conflicting interests/trust issues? If the tool is owned by the government and the fact-checkers are also from the same entity, this can be target of doubts and attacks. Then, this is a Yes for **Parties can/want to avoid a trusted third parties?** Finally, all the history of processing and analyzing each news should be stored indefinetively, allowing traceability and auditing, which poses a Yes for **Need for an objective immutable log?**[7]

6.4. Brief Discussion and Threats to Validity. Other blockchain technologies could have been considered as candidates for our Proof of Concept (PoC). However, Hyperledger Fabric presented desirable characteristics that weighted the decision towards them. Hyperledger Fabric offers a modular and configurable architecture that enables a high degree of privacy, scalability, and flexibility in transaction management, essential for meeting enterprise-level applications' diverse needs. Its support for smart contracts, known as chaincode, allows for developing complex business logic that can be securely executed within the blockchain network.

While blockchain offers potential benefits for creating a transparent and immutable record of news articles, its application in fighting fake news can face important challenges, particularly regarding feasibility, scalability, and cost. About feasibility, the success of a blockchain-based system depends some important technical concerns, including its large-scale adoption, the hardware infrastructure to deploy it with elastic capabilities to respond to the increase of resource demands and even a pool of fact-checkers that could contribute to the voting process. All these concerns lead to other two important issues: scalability and costs. About scalability, such a system should be prepared to support a large degree of transaction throughput, data storage, and network load. Since the system is still a proof-of-concept, this is not a concern. Once it is made available to the population, a load balance is need both to receive the queries and to process them, maybe in a queue. Services redundance is also needed, which is supported due to the technology stack used even in the PoC version. Moreover, by the blockchain nature, more nodes can be created to accordingly support an increasing demand in the services, splitting the demands in groups of nodes inside the blockchain. Finally, about costs, we could consider three types: (i) infrastructure, (ii) transactions and (iii) fact-checkers payment. In all the cases, this would not be a considerable problem, since this is a government initiative. Then, the government could (i) acquire the necessary hardware to deploy the blockchain network accordingly, (ii) pay for the gas eventually needed to emit the tokens and (iii) pay the fact-checkers, converting tokens into currency, as in other already existing initiatives, such as the bases for educational institution assessment.

Threats to Validity. This research could have been affected by different factors [38], and we discuss them, as follows.

Internal Validity. Internal validity concerns to the validity within the given environment and the reliability of the results. As stated by Abreu et al. (2020), The network environment can fluctuate in terms of latency, execution time for queries and transactions, block validation, disk space, and other factors. This variability can be problematic if the application requires immediate results. To address this, extensive testing of the application can be conducted to evaluate quality attributes and ensure compatibility with the environment. Another issue is that even if data is correctly registered on the blockchain, it can still be incorrect. Since the blockchain is immutable, this erroneous data remains recorded. To rectify this, a new correction record must be added, and the application must be designed to manage such cases.

External Validity. External validity concerns the extent to which the results of a case study can be generalized. This study involved only two fact-checkers, raising questions about scalability. Additional research is needed to test the prototype in broader contexts, involving more fact-checkers and processing a larger number of posts for registration and labeling.

Conclusion Validity. Conclusion validity pertains to the relationship between the treatment and the outcome. The evaluation conducted involved a small number of participants and relied on subjective questions. Additional research involving a larger group of fact-checkers is necessary for more robust results.

Construct Validity. Construct validity focuses on the link between theory and observation. In this work, we only considered opinions from individuals at two fact-checking agencies. These individuals lacked technical expertise in blockchain, limiting the depth of their responses to their knowledge of the fact-checking process. The data used were sourced from actual news portals. Moreover, the application was not deployed for production use but was only utilized for this research. There is a need to evaluate the application with real, large-scale data, considering impacts on quality attributes and involving multiple users, to truly demonstrate its effectiveness and determine whether investing in blockchain is worthwhile.

7 FINAL REMARKS AND FUTURE WORK

The main contribution of this paper was to report the creation of a blockchain-based software architecture of a solution to fight fake news dissemination, within the project scope of a dApp PoC [5]. The architecture was systematically conceived following the canonical architectural framework of Hofmeister [17]. We assessed a candidate architecture and evaluated it using simulation. This study brings insights and lets the concerns be accordingly recorded so that iterations over the architecture can enhance the satisfaction of other requirements. This work demonstrates a practical approach to creating local blockchain development environments. Possible extensions include incorporating authentication and authorization mechanisms, deeper analysis of communication between nodes, and exploring advanced features of other blockchains, for instance, Hyperledger Besu.

Nevertheless the focus of the architecture proposed herein was not on the availability of the services for the public or other entities, we already have an evolved proposal of it to provide an external endpoint exposed as an API for news agencies, social media platforms and even a service for the population to use and collect information regarding the validity of the information they want to check [14]. Agencies and social media platforms could use the API to award badges to verified information, giving their users more transparency about the news they consume whilst the population could use the service to check suspicious content they find in their daily lives. We expect the advances achieved here can be reproduced/replicated in

[7] The other questions are more technical than business-oriented. Since we already have the Yes for 5 of them here, the others will not be shown due to space restrictions.

several countries to combat fake news dissemination or even in other domains, such as Smart cities [16].

ACKNOWLEDGEMENTS

We thank ANATEL (the Brazilian National Telecommunications Agency) and FAPEG (the Research Support Foundation of the State of Goiás) for funding this research.

REFERENCES

[1] Antonio Welligton S. Abreu, Emanuel F. Coutinho, and Carla I. M. Bezerra. 2020. A Blockchain-based Architecture for Query and Registration of Student Degree Certificates. In *14th SBCARS*. ACM, Natal, Brazil, 151–160.

[2] João Guilherme Bastos dos Santos, Arthur Ituassu, Sérgio Lifschitz, Yago Cury, Thayane Guimarães, Diego Cerqueira, Debora Albu, Redson Fernando, Julia Hellen Ferreira, and Maria Luiza Mondelli. 2022. Regional patterns and networked behavior: interdisciplinary methods for identifying bots in the 2020 elections in Brazil. *iSys - Brazilian Journal of Information Systems* 15, 1 (Dec. 2022), 26:1–26:12. https://doi.org/10.5753/isys.2022.2415

[3] Cristian Nicolae Buțincu and Adrian Alexandrescu. 2023. Blockchain-Based Platform to Fight Disinformation Using Crowd Wisdom and Artificial Intelligence. *Applied Sciences* 13, 10 (2023). https://doi.org/10.3390/app13106088

[4] Argus Antonio Barbosa Cavalcante, Paulo Márcio Souza Freire, Ronaldo Ribeiro Goldschmidt, and Cláudia Marcela Justel. 2024. Improving Implicit Crowd Signals Based Fake News Detection on Social Media: A Time-Aware Method for Early Detection. In *SBSI 2024*. ACM, Juiz de Fora, Brazil, 7:1–7:9. https://doi.org/10.1145/3658271.3658278

[5] Eliomar Araújo de Lima et al. 2024. *Projeto Web 3.0 - Avaliação de Impacto da Web 3.0: Descentralizada, Imersiva, Semântica, Centrada no Usuário e Conectada com o Mundo Ciberfísico; Relatório Técnico - Fake News – Etapa 4 – Relatório 2 – PoC dApp*. Technical Report 02-2024. Universidade Federal de Goiás. TechReport In Portuguese (Under Development) Restricted Access.

[6] Janaína Ignacio de Morais, Hugo Queiroz Abonizio, Gabriel Marques Tavares, André Azevedo da Fonseca, and Sylvio Barbon Jr. 2020. A Multi-label Classification System to Distinguish among Fake, Satirical, Objective and Legitimate News in Brazilian Portuguese. *iSys - Brazilian Journal of Information Systems* 13, 4 (Jul. 2020), 126–149. https://doi.org/10.5753/isys.2020.833

[7] Claudio Di Ciccio, Giovanni Meroni, and Pierluigi Plebani. 2020. Business process monitoring on blockchains: Potentials and challenges. In *BPMDS at CAiSE*. Springer, Grenoble, France, 36–51.

[8] Karen Watts DiCicco and Nitin Agarwal. 2020. *Blockchain Technology-Based Solutions to Fight Misinformation: A Survey*. Springer, 267–281.

[9] Zafer Duzen, Mirela Riveni, and Mehmet S. Aktas. 2023. Analyzing the Spread of Misinformation on Social Networks: A Process and Software Architecture for Detection and Analysis. *Computers* 12, 11 (2023).

[10] A. D. Dwivedi, R. Singh, S. Dhall, G. Srivastava, and S. K. Pal. 2020. Tracing the Source of Fake News using a Scalable Blockchain Distributed Network. In *Proc. of IEEE 17th MASS*. 38–43.

[11] Elli Androulaki et al. 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains *(EuroSys '18)*. ACM, Porto, Portugal, Article 30, 15 pages.

[12] Hyperledger Foundation. 2023. Benchmarking Hyperledger Fabric 2.5 Performance. https://www.hyperledger.org/blog/2023/02/16/benchmarking-hyperledger-fabric-2-5-performance. Accessed: [February 10th, 2024].

[13] Juliana Gomes, Valdemar Vicente Graciano Neto, Jacson Barbosa, and Eliomar Araújo de Lima. 2023. A Rapid Tertiary Review at the Fake News Domain. In *Proceedings of the XI Escola Regional de Informática de Goiás*. SBC, Goiânia, Brazil, 1–10. https://doi.org/10.5753/erigo.2023.237391

[14] Valdemar Vicente Graciano-Neto, Jacson Barbosa, Eliomar Lima, Sérgio Carvalho, and Samuel Venzi. 2024. A Blockchain-based and AI-Endorsed Mechanism to Support Social Networks on Fake News Containment. In *XIII BraSNAM*. SBC, Brasília/DF, 207–213. https://doi.org/10.5753/brasnam.2024.2255

[15] Valdemar V. Graciano-Neto, Vinícius Borges, Luiza Cintra, Pedro Henrique Campos, Jacson Rodrigues, and Eliomar Araújo de Lima. 2024. Avaliando um Mecanismo de Consenso no Processo de Perícia de Desinformação através de Simulação. In *6th MSSiS*. SBC, Curitiba, Brazil, 1–10.

[16] Valdemar Vicente Graciano Neto and Mohamad Kassab. 2023. *What Every Engineer Should Know About Smart Cities*. CRC Press - Taylor & Francis. 1st Edition. 254 p..

[17] Christine Hofmeister, Philippe Kruchten, Robert L. Nord, Henk Obbink, Alexander Ran, and Pierre America. 2007. A general model of software architecture design derived from five industrial approaches. *JSS* 80, 1 (2007), 106–126.

[18] ISO/IEC. 2010. *ISO/IEC 25010 System and software quality models*. Technical Report.

[19] T.W. Jing and R.K. Murugesan. 2019. A Theoretical Framework to Build Trust and Prevent Fake News in Social Media Using Blockchain. In *Recent Trends in Data Science and Soft Computing (Advances in Intelligent Systems and Computing, Vol. 843)*. Springer, Cham.

[20] Mohamad Kassab, Joanna F. DeFranco, Tarek Malas, Phillip A. Laplante, Giuseppe Destefanis, and Valdemar Vicente Graciano Neto. 2021. Exploring Research in Blockchain for Healthcare and a Roadmap for the Future. *IEEE Trans. Emerg. Top. Comput.* 9, 4 (2021), 1835–1852. https://doi.org/10.1109/TETC.2019.2936881

[21] Rafał Kozik, Wojciech Mazurczyk, Krzysztof Cabaj, Aleksandra Pawlicka, Marek Pawlicki, and Michał Choraś. 2023. Combating Disinformation with Holistic Architecture, Neuro-symbolic AI and NLU Models. In *2023 IEEE 10th DSAA*. 1–9.

[22] Philipe Melo, Johnnatan Messias, Gustavo Resende, Kiran Garimella, Jussara Almeida, and Fabrício Benevenuto. 2019. WhatsApp Monitor: A Fact-Checking System for WhatsApp. *Proc. of the International AAAI Conference on Web and Social Media* 13, 01 (Jul. 2019), 676–677.

[23] Suyel Namasudra and Kemal Akkaya. 2023. Introduction to blockchain technology. In *Blockchain and its Applications in Industry 4.0*. Springer, 1–28.

[24] Shovon Paul, Jubair Islam Joy, Shaila Sarker, Abdullah Al Haris Shakib, Sharif Ahmed, and Amit Kumar Das. 2019. Fake News Detection in Social Media using Blockchain. In *Proc. of 7th ICSCC*. 1–5.

[25] Asger B Pedersen, Marten Risius, Roman Beck, et al. 2019. A ten-step decision path to determine when to use blockchain technologies. *MIS Quarterly Executive* 18, 2 (2019), 99–115.

[26] Julio C. S. Reis, Philipe Melo, Fabiano Belém, Fabricio Murai, Jussara M. Almeida, and Fabricio Benevenuto. 2023. Helping Fact-Checkers Identify Fake News Stories Shared through Images on WhatsApp *(WebMedia '23)*. ACM, Ribeirão Preto, Brazil, 159–167.

[27] Christiane Santana, Daniela Barreiro Claro, and Marlo Souza. 2022. Fake News Detection in Tweets: Challenges and Adaptations imposed by the COVID-19. *iSys - Brazilian Journal of Information Systems* 15, 1 (Oct. 2022), 11:1–11:26. https://doi.org/10.5753/isys.2022.2286

[28] Eishvak Sengupta, Renuka Nagpal, Deepti Mehrotra, and Gautam Srivastava. 2021. ProBlock: a novel approach for fake news detection. *Cluster Computing* 24 (2021), 3779–3795.

[29] Wajiha Shahid, Bahman Jamshidi, Saqib Hakak, Haruna Isah, Wazir Zada Khan, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. 2022. Detecting and Mitigating the Dissemination of Fake News: Challenges and Future Research Opportunities. *IEEE Transactions on Computational Social Systems* (2022), 1–14. https://doi.org/10.1109/TCSS.2022.3177359

[30] Kai Shu, H. Russell Bernard, and Huan Liu. 2019. *Studying Fake News via Network Analysis: Detection and Mitigation*. Springer, 43–65.

[31] Pamella Soares, Raphael Saraiva, Iago Fernandes, Jerffeson Souza, and Ricardo Loiola. 2022. DocStone: A Blockchain-Based Architecture for a Customizable Document Registration Service. In *16th SBCARS*. SBC, Uberlândia, Brazil, 1–10.

[32] Paulo Gabriel Teixeira, Bruno Gabriel Araújo Lebtag, Rodrigo Pereira dos Santos, Juliana Fernandes, Ahmad Mohsin, Mohamad Kassab, and Valdemar Vicente Graciano Neto. 2020. Constituent System Design: A Software Architecture Approach. In *2020 IEEE ICSA Companion 2020, Salvador, Brazil*. IEEE, 218–225.

[33] Mohamed Torky, Emad Nabil, and Wael Said. 2019. Proof of credibility: A blockchain approach for detecting and blocking fake news in social networks. *International Journal of Advanced Computer Science and Applications* 10, 12 (2019).

[34] Akash D. Waghmare and Girish Kumar Patnaik. 2021. Fake News Detection Of Social Media News In Blockchain Framework. *IJCSE* (2021).

[35] Abhishek Wahane and Balaji Patil. 2022. Blockchains to curb Fake News in an Online World. In *2022 International Conference for Advancement in Technology (ICONAT)*. 1–6. https://doi.org/10.1109/ICONAT53423.2022.9725933

[36] Yihang Wei. 2020. Blockchain-based data traceability platform architecture for supply chain management. In *IEEE 6th BigDataSecurity*. IEEE, 77–85.

[37] Mika Westerlund. 2019. The emergence of deepfake technology: A review. *Technology innovation management review* 9, 11 (2019).

[38] Claes Wohlin, Per Runeson, Martin Höst, Magnus C Ohlsson, Björn Regnell, Anders Wesslén, et al. 2012. *Experimentation in software engineering*. Vol. 236. Springer.

[39] World Economic Forum. 2024. Global Risks 2024: Disinformation Tops Global Risks 2024 as Environmental Threats Intensify. https://www.weforum.org/press/2024/01/global-risks-report-2024-press-release/. Accessed: [June, 2024].

[40] Y. Xiao, Y. Liu, and T. Li. 2020. Edge Computing and Blockchain for Quick Fake News Detection in IoV. *Sensors* 20, 16 (2020), 4360. https://doi.org/10.3390/s20164360

[41] Peipeng Yu, Zhihua Xia, Jianwei Fei, and Yujiang Lu. 2021. A survey on deepfake video detection. *Iet Biometrics* 10, 6 (2021), 607–624.

[42] Xinyi Zhou and Reza Zafarani. 2020. A survey of fake news: Fundamental theories, detection methods, and opportunities. *ACM Computing Surveys (CSUR)* 53, 5 (2020), 1–40.