Blockchain-Based Source-to-Source News Verification

Blockchain-Based Source-to-Source News Verification

1st Alberto Butera
Dept. of Control and Computer Engineering
Politecnico di Torino
Turin, Italy
alberto.butera@polito.it

2nd Julia Staszczak
Dept. of Computer Science
Norwegian University of Science and Technology
Trondheim, Norway
julia.staszczak@ntnu.no

3rd Patrick Mikalef
Dept. of Computer Science
Norwegian University of Science and Technology
Trondheim, Norway
patrick.mikalef@ntnu.no

4th Valentina Gatteschi
Dept. of Control and Computer Engineering
Politecnico di Torino
Turin, Italy
valentina.gatteschi@polito.it

***Abstract*—As misinformation has become a global phenomenon in the age of digitalization, journalists are expected to provide verified information and prevent the spread of fake news in order to protect the credibility of their profession. This challenge has intensified as conflicts and propaganda became increasingly complex, and in order to stay relevant some may sacrifice reliability for clicks or to serve their own agendas. Therefore, mechanisms that help institutions maintain their reputation and reliability must be implemented. In this study, we propose a solution that enables and automates the verification of sources within the article to enhance the article verification system by enabling the provenance of referenced information. This study helps to lay the groundwork for mechanisms that ensure trustworthiness, enabling the development of solutions for domains where source-to-source is critical. In doing so, it advances the literature on fake news and blockchain applications offering a tool to help institutions preserve their reputation and elevate standards within the news industry.**

***Index Terms*—Source-to-Source, News verification, Blockchain, Smart Contract.**

I. Introduction

In a world where the line between digital and reality has become immensely hard to distinguish, digital misinformation is being strategically deployed for a multitude of purposes and was identified as one of the major threats to human society having become widespread [1]. Scholars generally categorize the effects of misinformation in two broad categories: societal-level impacts (media, politics, science, economics), and individual-level impacts, understood from a psychological perspective (cognitive, behavioral) [2]. Individuals' perceptions of the world, whether accurate or not, play a critical role in shaping their attitudes and behaviors. However, with the growing presence of fake news on modern social networking sites users struggle to determine their origin, which risks diminishing trustworthiness of the information they encounter [3]. Notably, concerns around fake news surpass those related to online fraud or cyberbullying [4]. In August 2024, the case of a reporter at the American newspaper Cody Enterprise using generative AI to produce articles with fabricated quotes emerged. This led to a further discovery of seven cases containing quotes generated by AI - "words that were never spoken, put into stories" [5]. The artificially generated content and fake quotes, not having been identified and corrected by the editor, raised concerns about professional standards - such inability to detect inaccuracies damages the reputation of longstanding institutions as well as jeopardizes the careers of those involved. Moreover, many scientific sources attribute current sociopolitical issues mainly to online misinformation, and therefore declining public trust in media [6]. To respond to challenges of verifying media provenance, there are ongoing attempts of the industry experts and organizations, such as Coalition for Content Provenance and Authenticity, to develop technical specifications for enhancing content authenticity and traceability. In short, provenance refers to metadata that details the origin, history, and transmission [7] of a piece of news content throughout its lifecycle. However, the challenge of characterizing the growing body of knowledge on mitigating misinformation persits, as relevant research is dispersed across multiple disciplines. Consequently, research findings tend to proliferate rather than build upon each other, hence, researchers ought to persist in advancing the understanding of broader misinformation landscape [8].

With the growing concern about an increasing prevalence of misinformation in public discourse and politics across many Western democracies [9], it is imperative to recognize it as broad and complex issue. Social media significantly amplify this phenomenon enabling misinformation to spread on a global scale impacting societies beyond just individuals [10], showcasing how easily it can be introduced into mainstream and necessitating the urgent implementation of the enhanced source verification mechanisms. Addressing the problem in its entirety is however a massive undertaking, therefore this study focuses on a more manageable scope. The step we take to address this problem and maintain journalistic integrity, by

preventing the widespread dissemination of misinformation, is the development of a verification system for sources, which would ultimately assist the safeguarding apparatus for the media credibility and professional reputations. By targeting source verification, rather than the broader issue of content accuracy itself, we aim to enhance the development of tools that can improve transparency within established news outlets and institutions already committed to truthfulness. The presented solution seeks to provide a more practical framework for verification on a smaller scale, laying the groundwork for improving the effectiveness of misinformation management. The primary contribution of this paper is therefore the development of a blockchain-based solution designed to enable media outlet publishers to verify the references within the articles they intend to publish. This work lays the foundation for a decentralized application, developed in Solidity and deployed on the Gnosis blockchain. As emphasized, instead of focusing on the identifying of fake news, this study aims to link news and references to create a verified network.

The rest of the paper is organized as follows: Section 2 reviews the relevant literature on blockchain-based solutions for news verification. Section 3 outlines the business logic and technical architecture of the proposed system. Section 4 presents the obtained results, followed by Section 5 and 6, which offer critical reflections on the prototype, discuss its limitations, and propose directions for future research.

II. Background

The topic of fake news has gained a significant public interest, continuously attracting a growing focus from the academic community [11]. Numerous studies have shown that misinformation not only undermines the effectiveness of accurate information but has also been linked to acts of violence and vandalism [9]. What's more, science news and conspiracy rumors both peak within 2 hours but differ in their duration and impact (the former spreading quickly but fading fast, while latter taking longer to spread but having a more lasting influence) [1] - this observation indicates impact of overshadowing important information and leading to the erosion of trust. Realizing these patterns is crucial for creating effective mitigation strategies as for misinformation spreads rapidly and efforts to intervene through early identification and confinement are of foremost importance [11]. To combat this problem, numerous articles have been published proposing various solutions, including blockchain-based. Some studies present systems and frameworks that focus on identifying, analysing and tracking fake news using computational methods on content analysis, URLs, distribution patterns and social networks [12]–[14]. However, to best of our knowledge there is not much work within the existing literature on tracking news' sources for the further reliable dissemination. The solution proposed in this study builds on the use of a public blockchain which ensures transparency and immutability by allowing users to check the history of news themselves, without necessarily relying on third-party platforms. Similar approach has been found in some other studies where a blockchain system for traceability and integrity of news for the journalistic process was proposed focusing on change registration [15]. Although it does not directly address the verification of reference reliability, it provides transparency on primary sources. Furthermore, another framework prevents from fake news spreading by identifying and assessing the reliability of news sources, not by tracking individual news items or checking their references but based on the reputation of the publisher [16]. Finally, another blockchain system was designed for the provenance of scientific data to ensure traceability and integrity of changes through a voting and verification mechanism [17]. With that, the concept of the news provenance proves to be relevant with our solution presenting a novel way of tracking references cited in the news by reporting whether they have been verified or not. It enhances the credibility of information at its origin, helping to prevent the initial spread of misinformation before it escalates - forming a network of source verification with the original article at the center as a series of interconnected references. This process involves tracing and validating each reference to ensure the reliability of the entire article. The current presented approach applies rather to members of the affiliated organizations, which provide accreditation and establish ethical guidelines, to ensure that journalism practices comply with professional standards and verification protocols. Such associations hold publishers and journalists accountable for maintaining truth and integrity in their reporting. Enabling the source-to-source verification, used in crafting news articles, can remarkably strengthen journalism and restore its integrity, allowing for an easier differentiation of professional news outlets from the noise of unreliable content.

III. Solution Overview

This study adopts action design research (ADR) to develop a blockchain-based source-to-source verification system for the news industry. Research in IS has faced criticism for its limited impact on practical applications [18] therefore our close collaboration with practitioners allowed us to iteratively design and refine a technological artifact (blockchain-based verification system) for this project. ADR approach is applied to the immersive projects within the industry [19] making it suitable for the goal of our study as working with a representative from a company operating in a software space, providing verification solutions, allowed us to develop a prototype extension. This enabled us to access domain knowledge and real-world requirements ensuring the artifact addresses an essential need in the industry. ADR allows researchers to balance the dual mission of advancing theoretical knowledge while also generating insights that help IS practitioners address not only current but also future challenges highlighting the interconnectedness of 'building, intervention, and evaluation' [20]. Feedback loops with the company's representative and other professionals influenced the design of the artifact, providing us with new insights as we progressed.

A. Business Logic

The presented work builds upon and extends an existing digital content verification system, which leverages the cryptographic function to hash the content as well as digital signatures to ensure the authenticity of published material. The existing solution is integrated into a company's Content Management System (CMS) via an API, ensuring that when content is published, it is signed and verified without compromising the security of private keys. The extension we propose introduces source-to-source verification via a smart contract system allowing the journalists and publishers to link and verify the different sources they reference within an article hence creating a transparent and immutable record of the source material used. The smart contract records the provenance of each piece of content, ensuring that every claim or statement can be traced back to its original source. The key components of our enhancement therefore include:

1) Smart Contract: The task of the smart contract is to store new news registration events on the platform with the corresponding reference list. The reference verification process is done off-chain in step 2, as it is not necessary to make it public and would only increase the cost of performing the smart contract functions.
2) Source Verification Loop: The off-chain component performs an automatic loop to check whether or not the sources referenced in the current article have been previously validated. This step does not need to be done on-chain, as it consists of a simple loop of recursive verification of the referenced sources. This step could also be done independently by anyone, since access to on-chain recorded events is free. If all sources are verified, the article is marked as "Verified Proven". Otherwise, the article is marked as "Verified not-proven". "Verified" does not mean that the news is true, but that it has been signed by the author.

Such enhancement adds an important layer of functionality by automating the verification of cited sources at the moment of publication. The variables of the smart contract have been designed to include publisher's public key, the author's public key, the article ID, the content hash, and the cited sources. We outline how the key components work together to achieve the desired outcome as following:

- Content Submission: Author (an accredited individual who has a public/private key pair) submits an article to the CMS of the news outlet. The submitted article is hashed using a cryptographic function to create a unique digital fingerprint of the content.
- Dual-Signature: Publisher Signature (Required) used to sign with the Publisher's private key the hashed content ensuring that the Publisher has reviewed and approved the content before it is submitted to the blockchain. The public key (known and trusted by the system) of the Publisher, can be used by anyone to verify this signature, ensuring the integrity and authenticity. The authors can add their signature to add an extra layer of non-repudiation, but this is not currently required.
- Smart Contract Event-Based Trigger: The smart contract is designed with an event that acts as a trigger point so when certain conditions are met/specific action occurs; in our case: when a new article, along with its metadata (hash, publisher signature, optional author signature), is submitted.
- Sources Verification (Off-Chain): It is responsible for handling the processing which the smart contract cannot efficiently do due to blockchain's limitations, such as high computational cost. This process is initiated to verify if each citation is of a recognized source looping through each citation referenced in the article. Verification Outcome: if all citations are verified, the article is marked as "Proven". If not, it is flagged as "Not-Proven".
- Returning Results to Smart Contract and Storage: The aggregated verification results are returned to the smart contract by calling a function that is designed to receive and store these outcomes. It stores the final verification state of the article, along with details about the citations - which were verified, and which were not. It's an immutable record, which means that once it's stored, it cannot be changed, therefore providing a permanent audit trail.

B. Technical Implementation

As previously stated, our solution was constructed upon an existing system for digital content verification. Consequently, our architectural design incorporates the existing system's infrastructure and augments it with additional components that we have introduced and developed. Specifically, the smart contract responsible for content registration on the blockchain was replaced with an optimized version that enables the registration and tracking of diverse sources referenced in articles. Additionally, a piece of off-chain code was introduced in the back-end section to assess the validity and credibility of all sources within an article.

1) Smart Contract Part: The smart contract has been developed for the Gnosis blockchain, an Ethereum sidechain, with the objective of ensuring compatibility and straightforward integration into the existing system, which also relies on the Gnosis blockchain. Given that Gnosis is an Ethereum Virtual Machine (EVM)-compatible blockchain, the smart contract was programmed using Solidity, the primary language utilized for the development of smart contracts on EVM-compatible blockchains. The role of the smart contract is to provide a function that, upon execution, stores all the metadata associated with a given piece of content that is to be validated on the blockchain. Given that no specific operation is required other than storage, we have opted for an event-based solution, leveraging the smart contract event log, which has provided multiple advantages to our implementation:

- Event log storage is a more cost-effective option than smart contract account storage. The cost per byte of data stored on the event log is 8 units of gas, whereas the

cost per byte on account storage is 625 units of gas, a significant discrepancy in costs.

- Data stored in the event log are immutable as opposed to data stored in any smart contract variable that could be overwritten.
- Storing data directly in the event log allowed for simpler and leaner code to be written, thereby reducing the cost of smart contract deployment and function execution and minimizing the presence of bugs within the code.
- Data retrieval during the read phase from the blockchain is optimized, as one of the primary functions of the event log is to return contract values to an off-chain application.

In terms of limitations, the data stored in the event log is not accessible to the smart contract itself. However, given the specific use case and the design of the solution, this drawback can be considered marginal. Figure 1 depicts the code for the smart contract. The definition of the "Article" event, which is stored on the blockchain, contains metadata that is useful for tracking and searching content. These include the public keys of the author (optional) and publisher of the content, which are used both to identify them and to verify the content's integrity. Additionally, the hash of the content signed by the private keys of the author (optional) and publisher, and the list of referenced resources within the content is also included. The content ID is unique and has been declared with the keyword "indexed" to facilitate searching and reading the content within the event log. Finally, the last metadata is a boolean value that is set to "True" if all referenced resources are themselves proven; otherwise, it takes the value "False". The "storeArticle" function accepts the requisite metadata for each piece of content to be stored on the blockchain as input parameters and generates the "Article" event, which is then passed the same input parameters. This function is invoked by the off-chain application in response to a request for the validation of new content.

2) Off-chain Part: The off-chain part of our solution is responsible for verifying the validity of the resources cited within the new news to be stored on the blockchain, structuring the metadata required by the smart contract, and finally uploading the news on-chain. Initially, authors submitting a new news using our platform upload both the text of the news and the list of references cited within the news. We reiterate that our solution is not designed to verify the veracity of a news story (a task that can be accomplished by integrating one of the most advanced systems), but to assign ownership and responsibility for what is written to the authors themselves, and to verify that all references cited within the news story are themselves signed and approved by the publishers and authors. The off-chain verification process reads from the smart contract the events associated with the identifiers (IDs) of the references taken from the provided list, and recursively checks that all the references are present in the smart contract's list of events, and that they themselves are "Verified Proven" (i.e. composed of signed and approved references). The publisher (obligatory) and the author (optional at this point) must have a key pair (public and private) to ensure ownership and non-repudiation of the uploaded messages. The private key is used to sign the news text (including references), while the public key is inserted into the metadata of the structure stored on-chain and can be used by anyone to verify who wrote the news and that the text has not been altered. Finally, the structure is created containing the signature of the message text, the public key of the publisher, the public key of the author (optional), the message ID, the list of IDs of the references cited within it, and a Boolean value indicating whether the news is "Proven" or "not-proven". The whole structure is registered on-chain by calling the smart contract function described in the previous section, which issues the new event associated with the newly inserted news. Figure 2 summarises the pipeline of steps covered by the off-chain part of our solution.

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.26;

contract Test {

    event Article(
        string publisher_public_key,
        string author_public_key,
        uint256 indexed article_id,
        string content_hash,
        uint256[] sources,
        bool has_proven_sources
    );

    function storeArticle(
        string memory publisher_public_key,
        string memory author_public_key,
        uint256 article_id,
        string memory content_hash,
        uint256[] memory sources,
        bool has_proven_sources
    ) public {
        emit Article(publisher_public_key,
        ↪  author_public_key, article_id,
        ↪  content_hash, sources,
        ↪  has_proven_sources);
    }
}
```

Fig. 1. Smart contract code written in Solidity and deployed on the Gnosis blockchain

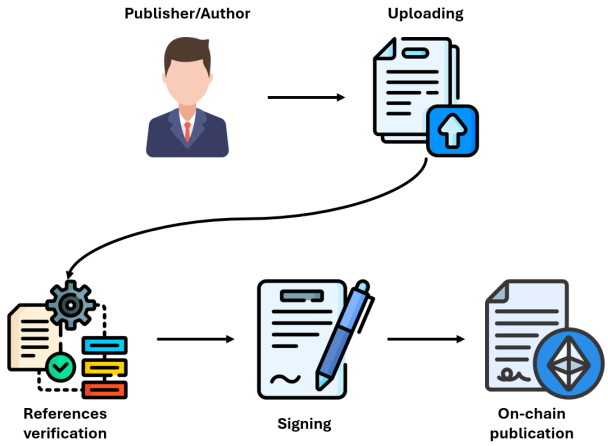

Fig. 2. Off-chain steps before the publication on the smart contract

IV. Testing and results

The proposed solution was tested to evaluate the cost of running the function that uploads the metadata of a new news item to the blockchain, and to verify its operation. When using a public blockchain to store data, it is crucial to carry out a cost analysis, as all transactions to write to the blockchain usually involve the payment of fees proportional to the amount of data to be written and the complexity of the code to be executed (in the case of blockchains that allow code execution). Another factor that negatively affects the cost of a transaction is network congestion: the more the network is used, the higher the cost that must be paid to store data on the blockchain. As anticipated in the previous sections, our solution was developed from an existing solution using the Gnosis blockchain. For compatibility reasons, we also chose to use the same blockchain. Gnosis is a relatively new blockchain with very low transaction costs. Nevertheless, we tried to optimise the cost of our solution as much as possible. Choosing the event log for storage, rather than EVM account storage, reduced the cost by a factor of 100 (8 gas units per byte vs. 625 gas units per byte). In addition, using the event log kept the smart contract code extremely simple, reducing the cost of deploying the smart contract on the chain. The metadata stored on the blockchain by our solution is small and limited in size because it is fixed and small data, with the exception of the reference list, which could potentially be large, but it is unlikely that a news article would ever have a very large number of citations. As a result, the cost of running the storage function will not be very different from what was found in the tests. In terms of numbers, the average cost of running the function was 0.00006778 xDAI, equivalent to $0.000068 (values on 15/4/24). All test transactions are accessible via the Blockchain Explorer[1]. Performing the same function with the same metadata on Ethereum (notoriously expensive) would cost 238,918 gwei, equivalent to $0.6367 (value on 15/4/24). While much more expensive, this is still less than $1. Although the solution works and has low transaction costs, the proposed code currently has a security problem due to the lack of an access control system, i.e. a system that restricts the execution of the storage function to authorised accounts. If execution were not restricted to all users, there would be a risk that incorrect metadata would be loaded, corrupting the event history and making it difficult to read and verify. This problem could be solved by adding a modifier to the code of the smart contract function that prohibits it from being called by all unauthorised addresses. In any case, further thorough security testing should be done before putting our solution into production.

V. Discussion

The intensification of competition in the news industry enlivened the production of sensational false news to serve each economic interest [21]. This study set out to adress the issue of news outlets' diminishing credibility by developing a solution for source-to-source verification using blockchain. The immutable nature of blockchain technology ensures that once recorded data cannot be altered or deleted, providing a permanent record and allowing consumers to independently verify the sources. In addition, our system requires authors/publishers to pay more attention to the truthfulness of news, as its content is signed (non-repudiation), cannot be changed, and the exact date of publication is known. This increases the reputation and reliability of authors who publish true and well-referenced news, which is an important gain for those who do this work. The fact that some of the code is off-chain might lead some to believe that our solution is less transparent. In reality, the loop and reference verification operation that is performed off-chain is a verification that can be performed by any user reading the data from the blockchain, as the metadata contains all the information needed to replicate the verification loop without necessarily relying on our system. Keeping this part of the code off-chain does not affect transparency, but it allows us to drastically reduce the cost of executing transactions, as loop operations tend to be very expensive. In domains where source-to-source verification is critical, we believe this solution establishes a foundational approach to addressing the challenges of data manipulation and the spread of misinformation. Further applicability may be recognized within academia or the financial sector. In order to prevent data frauds such as fabrication, under-reporting, and manipulating results to reach and align with research objectives, it's vital to maintain provenance of data in research [17]. Assessing and validating references is a key process for ensuring the authenticity of academic research [22]. Moreover, numerous efforts have been made to adopt international financial reporting standards over a country's domestic ones [23], as improved financial reporting quality leads to greater advantages for both investors and users of financial statements [24]. Blockchain could help achieve international buy-in and enforcement for such standards. Furthermore, teaching individuals to be media-literate is among the most crucial skills that shall be provided, empowering consumers to critically evaluate sources, navigate misinformation, and making informed decisions [25]. This competence is essential for effectively understanding, managing, and utilizing information in an increasingly complex and digital world.

VI. Conclusions

As misinformation and propaganda efforts continue to spread, and tactics used are becoming more sophisticated, the urgency to combat them is increasing. These activities are expanding on an unimaginable scale, as demonstrated by the U.S. Department of Justice's takedown of a covert social media bot farm operated by the Russian government, which utilized AI to generate fake social media profiles - often posing as U.S. citizens - disseminating misinformation and promoting narratives aligned with Russian government interests [26]. This underscores the multidimensional nature of the phenomenon which requires comprehensive tackling.

[1] https://gnosisscan.io/address/0xb8155f09c4cdaf9c0ec0924c27f85c7304a14b55

The solution we proposed in this paper offers a way to help combat the spread of misinformation, with the potential to expand into additional areas by leveraging the cryptographic features of blockchain technology, potentially also targeting the growing illicit use of AI in the future. With our work we aimed to take the initial steps in establishing a ground beam, which should be explored in more detail moving forward. The ADR methodology holds potential for further refinement and practical application of the artifact. Therefore, we propose that future research would benefit from an extended study duration allowing for more in-depth exploration and analysis. Further employment of an iterative approach when developing the solution could focus on continuous testing to refine the solution over time. Blockchain can enhance transparency and traceability, however it is not a cure-all solution. The vast problem of misinformation requires collaborative efforts on a global scale. To more effectively deal with the problem of misinformation spread, blockchain must be integrated with robust fact-checking mechanisms, international standards, and cross-sector partnerships.

REFERENCES

[1] Michela Del Vicario, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H. Eugene Stanley, and Walter Quattrociocchi. The spreading of misinformation online. Proceedings of the National Academy of Sciences, 113(3):554–559, January 2016.

[2] Zoë Adams, Magda Osman, Christos Bechlivanidis, and Björn Meder. (Why) Is Misinformation a Problem? 18:1463–1463, November 2023.

[3] Russell R Torres, Natalie Gerhart, and Arash Negahban. Combating Fake News: An Investigation of Information Verification Behaviors on Social Networking Sites.

[4] Lloyd's Register Foundation. World risk poll press release cyber risk, oct 2020.

[5] The Associated Press. Reporter caught using artificial intelligence to create fake quotes and stories, August 2024. Section: National.

[6] Sacha Altay, Manon Berriche, and Alberto Acerbi. Misinformation on Misinformation: Conceptual and Methodological Challenges.

[7] Bofeng Pan, Natalia Stakhanova, and Suprio Ray. Data Provenance in Security and Privacy. ACM Computing Surveys, 55(14).

[8] Jennifer Jerit and Yangzi Zhao. Political Misinformation. Annual Review of Political Science, 23(Volume 23, 2020):77–94, May 2020. Publisher: Annual Reviews.

[9] Stephan Lewandowsky and Sander Van Der Linden. Countering Misinformation and Fake News Through Inoculation and Prebunking. European Review of Social Psychology, 32(2):348–384, July 2021.

[10] Panayiotis Christodoulou and Klitos Christodoulou. Developing more Reliable News Sources by utilizing the Blockchain technology to combat Fake News. In 2020 Second International Conference on Blockchain Computing and Applications (BCCA), pages 135–139, November 2020.

[11] Karishma Sharma, Feng Qian, He Jiang, Natali Ruchansky, Ming Zhang, and Yan Liu. Combating Fake News: A Survey on Identification and Mitigation Techniques. ACM Transactions on Intelligent Systems and Technology, 10(3):1–42, May 2019.

[12] Chun-Ming Lai and Yi-Hua Guo. Tracking of Disinformation Sources: Examining Pages and URLs. IEEE Transactions on Computational Social Systems, 11(5):6242–6253, October 2024.

[13] Zhouhan Chen, Kevin Aslett, Jen Rosiere Reynolds, Juliana Freire, Joshua A Tucker, and Richard Bonneau. An Automatic Framework to Continuously Monitor Multi-Platform Information Spread.

[14] Liang Wu and Huan Liu. Tracing Fake-News Footprints: Characterizing Social Media Messages by How They Propagate. In Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining, WSDM '18, pages 637–645, New York, NY, USA, February 2018. Association for Computing Machinery.

[15] Francisco Jurado, Oscar Delgado, and Álvaro Ortigosa. Tracking News Stories Using Blockchain to Guarantee their Traceability and Information Analysis. International Journal of Interactive Multimedia and Artificial Intelligence, 6(3):39, 2020.

[16] Adnan Qayyum, Junaid Qadir, Muhammad Umar Janjua, and Falak Sher. Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News. IT Professional, 21(4):16–24, July 2019.

[17] Aravind Ramachandran and Murat Kantarcioglu. SmartProvenance: A Distributed, Blockchain Based Data Provenance System. 2018.

[18] Robert Cole, Sandeep Purao, Matti Rossi, and Maung K Sein. Running Head: PROACTIVE RESEARCH APPROACHES.

[19] Matthew T. Mullarkey, , and Alan R. Hevner. An elaborated action design research process model. European Journal of Information Systems, 28(1):6–20, January 2019. Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/0960085X.2018.1451811.

[20] Maung K. Sein, Ola Henfridsson, Sandeep Purao, Matti Rossi, and Rikard Lindgren. Action Design Research. MIS Quarterly, 35(1):37–56, 2011. Publisher: Management Information Systems Research Center, University of Minnesota.

[21] Zhang Xin and Wei Shiyao. Internet News Traceability Solution Based on Blockchain. In 2019 IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS), pages 236–240, June 2019.

[22] Abdullah Umar Nasib. References validation in scholarly articles using RoBERTa. May 2023. Accepted: 2023-09-25T06:25:45Z Publisher: Brac University.

[23] Philip Brown. International Financial Reporting Standards: what are the benefits? Accounting and Business Research, 41(3):269–285, August 2011. Publisher: Routledge _eprint: https://doi.org/10.1080/00014788.2011.569054.

[24] Dr Siriyama Kanthi Herath. Financial Reporting Quality: A Literature Review. 2(2), 2017.

[25] Joanna M Burkhardt. Library Technology Reports vol. 53, no. 8, "Combating Fake News in the Digital Age".

[26] Chainalysis. Malign interference and crypto. how crypto transaction tracing can expose and disrupt malign influence efforts, 2024.