Journal of COMPUTER AND FORENSIC SCIENCES

CFS 2023, Vol. 2, Issue 1, pp. 29–41
https://doi.org/10.5937/jcfs2-44736
Original research paper

iTrust News Certificate: A Blockchain-Based Solution for News Verification and Reputation Management

Aleksandar Miljković*, Milan Čabarkapa[2], Filip Miljković[1], and Ljubiša Bojić[3]

[1] Ministry of Interior of the Republic of Serbia & University of Criminal and Police Studies, Belgrade, Serbia; aleksandar.miljkovic@mup.gov.rs; filip.miljkovic@mup.gov.rs

[2] Faculty of Engineering, University of Kragujevac, Serbia; mcabarkapa@kg.ac.rs

[3] Institute for Philosophy and Social Theory, University of Belgrade, Serbia; ljubisa.bojic@instifdt.bg.ac.rs

* Corresponding author: aleksandar.miljkovic@mup.gov.rs

Received: May 30, 2023 • Accepted: June 20, 2023 • Published: July 7, 2023

Abstract: The proliferation of fake news and misinformation in the digital era poses a significant challenge to news organizations and content creators. In this paper, we introduce the iTrust News Certificate, the architecture of an online blockchain-based solution designed to combat fake news, enhance news verification, and maintain reputation within the media ecosystem. Unlike previous attempts, iTrust News Certificate focuses on user-friendly features while ensuring transparency and reliability. By leveraging blockchain technology, iTrust News Certificate establishes a decentralized and immutable ledger for storing news-related metadata. This ledger ensures the integrity and traceability of news articles, making it extremely difficult for malicious actors to tamper with or propagate false information.

Keywords: fake news; blockchain; smart contracts.

1. INTRODUCTION

The proliferation of digital misinformation and fake news has raised concerns globally, as highlighted by the 2022 Edelman Trust Barometer [1]. The survey revealed widespread uncertainty regarding the reliability of information in the media, with a significant percentage of respondents expressing doubts about their ability to differentiate factual news from falsehoods. [2] examines the diffusion of true and false news stories on social media and highlights the rapid spread of false information. Additionally, the potential weaponization of fake news further amplifies the need for effective solutions to address this issue. [3, 4, 5, 6] examine the exposure to untrustworthy websites during the 2016 U.S. election and its implications for belief in false information.

Blockchain technology has emerged as a promising tool to authenticate and verify content, including news and videos, as seen in [7, 8, 9, 10, 11]. Avivah Litan, an American analyst and researcher in the field of cybersecurity and fraud prevention, predicts that by

Citation: A. Miljković, M. Čabarkapa, F. Miljković, and Lj. Bojić, "iTrust News Certificate: A Blockchain-Based Solution for News Verification and Reputation Management," *Journal of Computer and Forensic Sciences*, vol. 2, no. 1, pp. 29–41, 2023, https://doi.org/10.5937/jcfs2-44736.

2023, up to 30% of world news and video content will be authenticated using blockchain technology. This development aligns with the concerns expressed in [12], which emphasizes the need for addressing the threats and limitations posed by the misuse of internet technologies, specifically concerning democratic processes and universal freedoms.

However, the absence of widely accepted standards for identifying, labeling, tracking, and responding to digital misinformation presents a significant challenge, as seen in [13, 14, 15, 16]. Without a universally recognized standard, the potential impact of blockchain technology on combating fake news remains limited. Previous initiatives have faced hurdles due to their lack of user-friendliness and the absence of adequate incentives for participation, contributing to their failure.

To address these issues, we propose the iTrust News Certificate, an architecture of a user-friendly online blockchain-based solution designed to provide news organizations and content creators with a reliable and transparent platform. This solution offers a rating tool for users to label potentially fake content, which is then subject to verification by registered users and independent fact-checkers. The incorporation of various post labels based on user perception and the additional feature of media profiling enhance the overall user experience and participation.

iTrust News Certificate revolutionizes the way users interact with news content by introducing a rating tool embedded at the bottom of each post. Unregistered users can easily label posts as potentially fake, triggering further scrutiny by registered users and independent fact-checkers. Only when a post is independently verified as fake, it can affect the post's Score, which is represented by a color-changing system ranging from various shades of green to orange and eventually to red.

Moreover, the iTrust News Certificate goes beyond the binary labeling of fake news. Each post is categorized based on user perception, providing labels such as "educational," "fun," "useful," "emotional," "adult," "polarizing," "opinionated," and "negative news." To address the lack of incentives for user participation in previous initiatives, iTrust News Certificate aims to introduce an engaging and interactive element through media profiling. As an additional feature of the platform, media profiling provides information about news organizations to anyone seeking to assess their credibility and trustworthiness. This feature is designed to be enjoyable for users, encouraging their active involvement in the verification process.

The second section presents materials and methods used in researching the defined problem. The third section proposes a solution and gives a broad overview of the architecture. The discussion and limitations of the proposed solution are presented in the fourth section. The fifth section concludes this work.

2. MATERIALS AND METHODS

To investigate the effectiveness of utilizing blockchain technology in combating fake news, we adopted a multi-faceted approach encompassing previous European projects, initiatives, and startup endeavors. In this section, we describe the materials and methods employed in each direction, including AI algorithm training, deep fake detection, incentivizing high-quality content, and maintaining online identity and reputation.

The first direction we explored involved training AI algorithms to recognize fake news. We examined the methodologies employed by previous European projects, such as AI-4Media and Fandango, the recent "AI to fight disinformation (RIA)" call, as well as other approaches [17, 18, 19, 20] that use AI algorithms with NLP approaches. It is important to note that the current challenge lies in the algorithm's inability to decisively determine the authenticity of information. However, it can assess the level of suspicion associated with a piece of content. The algorithms label information as suspicious, providing a valuable indicator for further investigation.

Addressing the issue of manipulated photos and videos, we investigated the utilization of blockchain technology for deep fake detection. One notable initiative in this field is the New York Times News Provenance Project [21], which was launched in 2019. The project aimed to establish a registry of all published images from various media outlets, accompanied by meta information such as captions, locations, consent, and copyright details. This comprehensive dataset was made verifiable by anyone, facilitating the detection of deep fakes. Additionally, Facebook initiated its Deep Fake Detection Challenge [22] to encourage the development of effective deep fake detection tools.

Another avenue we explored was the concept of incentivizing high-quality content creation using blockchain technology. Civil Media [23], a blockchain startup, proposed a new economy for journalism in which users could reward media outlets for their exceptional work. However, this vision faced challenges and failed to attract sufficient buyers. Other startups, including Poet and Nwzer [24], have also explored similar possibilities. It is important to note that the realization of this idea requires several intermediate steps, allowing smaller content providers to participate and be rewarded gradually.

The final direction we investigated involved maintaining online identity and reputation through blockchain technology. Mavin [25], a startup, initiated this endeavor by developing a browser plugin that enables readers to rate each piece of content based on their assessment. This approach empowers readers to discern the trustworthiness of the content they encounter and engage with. Moreover, users are assigned reputation scores based on factors such as their identity and expertise, influencing the weight of their votes and evaluations.

Throughout our exploration, we remained mindful of the ethical implications surrounding the use of AI algorithms, blockchain technology, and reputation systems. We considered issues related to privacy, data security, algorithmic bias, and the potential for unintended consequences. Our analysis acknowledges the importance of a balanced approach that upholds user trust and protects individual rights while addressing the challenges posed by fake news.

In this section, we outlined the materials and methods employed in our investigation of utilizing blockchain technology to combat fake news. We examined the AI algorithm training approaches, deep fake detection initiatives, and the concept of incentivizing high-quality content and maintaining online identity and reputation. Our analysis serves as a foundation for the subsequent sections, where we present our approach and findings as well as discuss the implications.

3. PROPOSED ARCHITECTURE

In this section, we propose an architecture for a blockchain-based smart contract solution for fake news detection iTrust News Certificate.

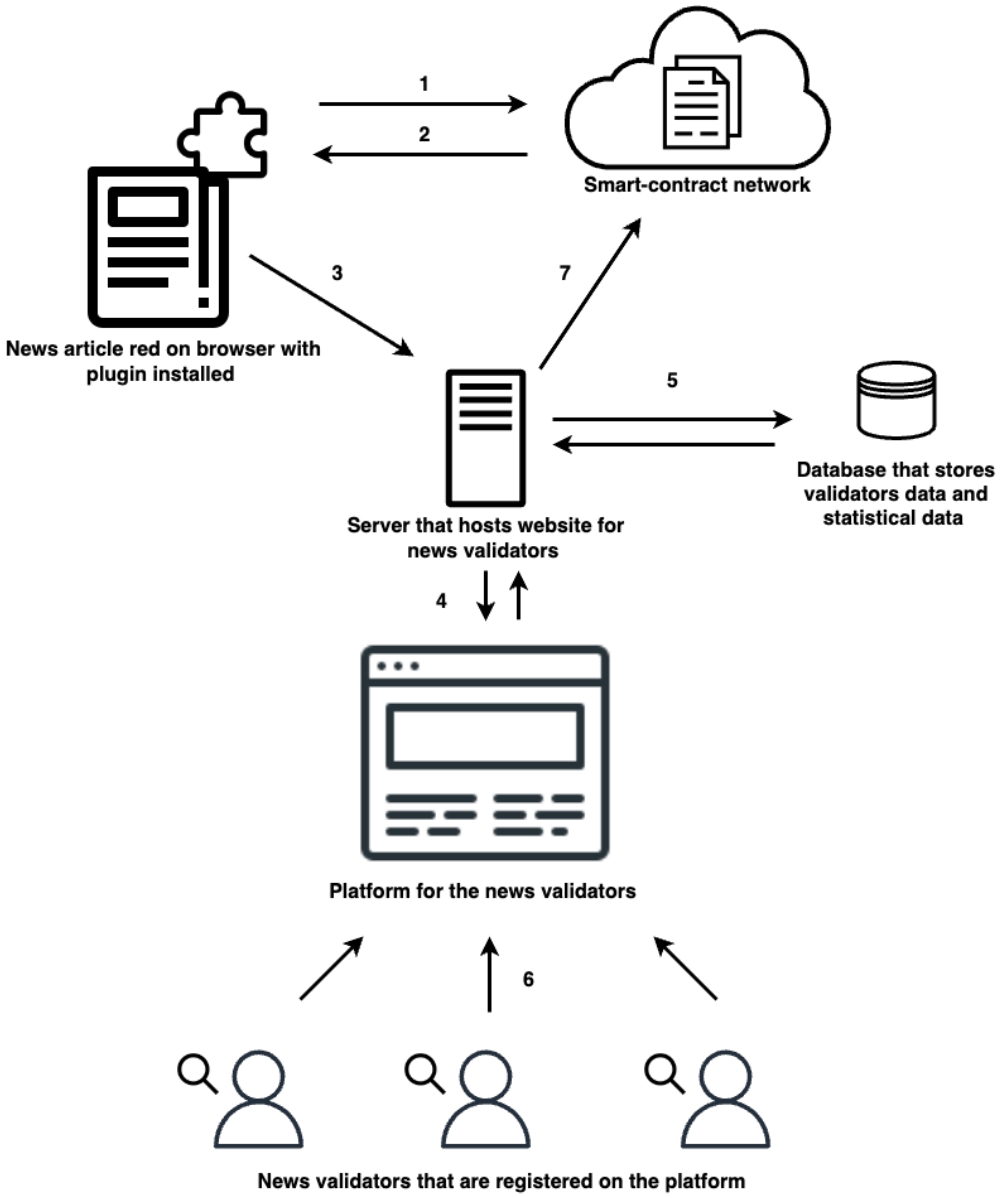

Figure 1. *The architecture of the iTrust platform.*

As we can see in the architectural diagram shown in Figure 1, the proposed platform consists of several components. The first one is a web browser plugin that monitors the web page that the user is visiting and communicating with the smart contract network directly using web3 technologies and with the platform's web server. The next and most important component is a smart contract network that stores information on reviewed news articles. Apart from that, there is a server that hosts part of the platform that enables news vali-

dators to do their part in the system and a database that stores information for registered validators and statistical data.

When a human user of a web browser plugin visits a news article, the dedicated plugin checks whether the article is present in the network. This is done by using the URL of the news article (step 1 in Figure 1). If the URL of the news article is present in the network, the data from that article are retrieved and its rating is displayed (step 2). When the URL is not present, a notification is sent to news validators that there is a new article that is yet to be verified (step 3). The news validator uses the platform's website to access the article by using its credential that is stored in the database and rate the article (steps 4, 5, and 6). An article review is then stored on the smart contract network for future usage.

3.1. Smart Contract

The first component of the architecture involves the creation of a smart contract using the Solidity programming language and the Remix development environment. The smart contract establishes the rules and conditions for user validation and the storage of relevant information, such as news URLs, ratings, user identities, and publishers. Creating a smart contract using the Solidity programming language and the Remix development environment involves several steps, has various use cases, and comes with certain limitations. Let's explore each aspect in detail:

3.1.1 Steps to Create a Smart Contract Using Solidity and Remix

This subsection presents a guide for setting up the Remix IDE, creating and writing Solidity code, compiling the smart contract, deploying it on a blockchain network, and interacting with the deployed smart contract. The Remix IDE is utilized as an integrated development environment to streamline the development process and facilitate the deployment of the smart contract. This subsection serves as a practical resource for researchers and developers aiming to implement and deploy their smart contracts.

To initiate the development process, the Remix IDE is launched through a web browser. This step establishes the foundation for creating, editing, compiling, and deploying smart contracts. Within the Remix IDE, a new Solidity file is generated by clicking on the "+" button and assigning it a .sol extension. This file serves as the container for the smart contract code. Leveraging the Solidity programming language, the structure, functions, and variables of the smart contract are outlined within the newly created Solidity file. Remix's built-in editor enhances the coding experience by providing syntax highlighting and auto-completion functionalities. Navigating to the "Solidity Compiler" tab within the Remix IDE, the desired version of Solidity is selected. Subsequently, the "Compile" button is clicked to initiate the compilation process, which includes error checking and bytecode generation. Within the "Deploy & Run Transactions" tab, the target blockchain network for deploying the smart contract is chosen. Options range from local development environments to various testnets. By clicking the "Deploy" button, the compiled smart contract is deployed onto the selected blockchain network. Successful deployment necessitates the

presence of a connected Ethereum wallet. Once the smart contract is deployed, Remix provides an intuitive interface for interacting with its functions and variables. Researchers and developers can conveniently invoke functions, send transactions, and observe state changes within the contract. By leveraging Remix's capabilities, researchers and developers can streamline the implementation of their smart contracts and leverage the Ethereum blockchain's potential.

It is important to note that Solidity and Remix are just two options for creating smart contracts. There are other programming languages (e.g., Vyper) and development environments available as well.

3.1.2 Use Cases of Smart Contracts

Smart contracts play a pivotal role in powering a diverse range of decentralized applications (DApps), eliminating the need for intermediaries, and enabling transparent and trustless interactions among users, as shown in [26]. Beyond their application in DApps, smart contracts offer extensive capabilities in various domains. They facilitate tokenization and crowdfunding efforts, providing a seamless mechanism for the creation and management of tokens, enabling processes such as Initial Coin Offerings (ICOs), crowdfunding campaigns, and the tokenization of assets. Moreover, in supply chain management, smart contracts offer invaluable benefits by tracking and validating the movement of goods throughout the supply chain, thereby enhancing transparency and mitigating the risks of fraud, as shown in [27]. Another practical use case for smart contracts is their ability to function as automated escrow services [28]. By holding funds until predetermined conditions are met, they ensure secure and equitable transactions. Furthermore, smart contracts offer a robust solution for voting systems, enabling the development of transparent and auditable voting mechanisms [29, 30]. By leveraging smart contracts, the possibility of tampering or manipulation within voting systems can be significantly reduced, reinforcing the integrity of democratic processes.

3.1.3 Limitations of Smart Contracts

There are some limitations when developing smart contracts:

- Immutability: A smart contract's code cannot be modified once deployed, which means any bugs or vulnerabilities discovered after deployment may be difficult to rectify.
- Lack of External Data Sources: Smart contracts have limited access to external data sources, making it challenging to incorporate real-time data or interact with external APIs directly.
- Scalability: Ethereum, the most popular blockchain for smart contracts, has scalability limitations, leading to potential congestion and higher transaction fees during periods of high network usage.

- Complexity and Security Risks: Writing secure smart contracts requires expertise, as incorrect code can lead to unintended consequences or vulnerabilities that may be exploited.
- Legal and Regulatory Concerns: The legal and regulatory frameworks surrounding smart contracts are still evolving, which may pose challenges in certain jurisdictions.

3.2. Testing Smart Contract Using Truffle

To ensure the reliability and integrity of the developed smart contract, a comprehensive testing phase is essential. This section explores the utilization of Truffle tools for testing smart contracts, emphasizing the significance of thorough testing before deployment to the network.

Truffle is a popular development framework and a suite of tools used for testing, compiling, and deploying smart contracts on the Ethereum blockchain. It provides a comprehensive environment for building decentralized applications (DApps) and simplifies the process of testing smart contracts. The Truffle Framework offers a development environment with built-in capabilities for smart contract compilation, deployment, and testing. It streamlines the workflow by providing a standardized structure for organizing one's project and managing dependencies. Truffle integrates the Mocha testing framework and the Chai assertion library to facilitate writing and executing tests for smart contracts. Mocha provides a testing framework structure, and Chai offers various assertion styles to make test assertions more expressive and readable. Truffle follows a specific directory structure for organizing test files. By default, test files are stored in the test directory within one's Truffle project. Truffle automatically discovers and runs the tests defined in these files. Truffle allows one to write tests for smart contracts using JavaScript. One can use the Truffle API and web3.js (a JavaScript library for interacting with Ethereum) to interact with deployed contracts, simulate transactions, and verify contract behavior. Truffle provides a migration system that helps manage the deployment of smart contracts to various Ethereum networks. Migrations are written in JavaScript and enable one to specify the sequence of contract deployments and any required initialization steps. Truffle supports automated testing through scripts. One can define scripts that set up the testing environment, deploy contracts, and run tests automatically. This is particularly useful for continuous integration (CI) and continuous deployment (CD) workflows. Truffle can generate code coverage reports to assess the extent to which one's tests cover the smart contract code. This feature helps identify areas of the codebase that lack test coverage and ensures a higher degree of reliability and security. Truffle facilitates testing contracts on different Ethereum networks, such as development, testnet, or mainnet. It provides network configuration options, allowing one to define multiple networks and switch between them easily during testing. Truffle integrates seamlessly with Ganache, a personal Ethereum blockchain for development and testing purposes. Ganache provides a local blockchain environment, allowing one to run tests quickly and simulate various scenarios.

Truffle's testing tools and features greatly simplify the process of writing and executing tests for smart contracts. They enable developers to ensure their contracts' correctness, reliability, and security before deploying them to production networks.

3.3. Deploying Smart Contract to the Ethereum Network

Once the smart contract has been thoroughly tested, it is deployed on the Ethereum network, enabling decentralized and immutable execution of the application. The deployment process, including gas optimization and contract address management, is discussed in this section.

Deployment of the contract can be done directly from the Remix IDE by connecting it to an Ethereum network. To deploy a contract, an Ethereum wallet is needed. The wallet holds the necessary funds to pay for the deployment transaction fees. There is a need for wallets like MetaMask, Mist, or any other Ethereum wallet that supports interacting with smart contracts. We should determine the Ethereum network on which one wants to deploy their contract. One can choose the Ethereum mainnet, a testnet like Ropsten, Rinkeby, or Kovan, or even a local development network like Ganache. In addition, the network may be selected and the contract bytecode and constructor arguments may be specified.

Once the contract is successfully deployed, it can be accessed via its contract address. One can send transactions to execute contract functions, read the contract state, and interact with the contract's public interface. After the deployment of the contract, the deployment transaction needs to be confirmed by the Ethereum network. The confirmation time varies depending on the network's congestion and the gas price one set for the transaction. It is important to note that deploying a smart contract incurs transaction fees (gas costs) for the deployment transaction and any subsequent contract interactions. The gas cost is paid in Ether (ETH) and depends on the complexity of the contract and the network conditions.

3.4. User-friendly Site for News Verification

Creating a user-friendly site is crucial for promoting the widespread adoption of the application. This section focuses on the implementation of a web interface using web3 technology, allowing validated users to view and rate news articles. User authentication and access control mechanisms are integrated to ensure the integrity of the rating system.

To enhance accessibility and engagement, a browser plugin is developed, enabling users to register, rate news articles, and receive notifications for validating new users. The storage of relevant information, such as news URLs, providers, ratings, and user identities, is needed, along with the potential use of hash values for efficient data storage.

3.5. Browser Plugin for Users

Design and development of the user interface for components of the plugin are made using HTML, CSS, and JavaScript. This includes creating the popup when the article exists in the smart contract network, the options page, and other UI elements that the plugin requires. A script runs in the background of the browser and handles the core functionality and interactions of the plugin. This script communicates with the browser's extension APIs and manages events and data. Asynchronous API calls are made to allow the user to browse the page until all the data has been retrieved.

3.6. Analytics Tools for Validators and Users

Beyond user validation, the proposed application incorporates NLP techniques to provide insights into the evaluated news articles. This section explores the generation of basic NLP statistics, such as word frequency analysis, to identify commonly used words and their impact on the overall rating. The potential for creating a valuable dataset for future scientific research is highlighted. There are several natural language processing (NLP) techniques that can be used to provide insights into evaluated news articles.

Text classification is a fundamental NLP technique used to categorize text into predefined categories. It can be applied to news articles to identify the topic or subject matter of the article, such as politics, sports, finance, or entertainment. This classification can provide insights into the distribution of news topics and help in organizing and filtering articles based on their relevance to specific categories.

Sentiment analysis aims to determine the sentiment or opinion expressed in a piece of text. By applying sentiment analysis to news articles, one can gain insights into the overall sentiment towards specific topics, individuals, companies, or events. This information can be useful for understanding public opinion, analyzing market sentiment, or detecting trends.

Named Entity Recognition (NER) is a technique used to identify and classify named entities such as persons, organizations, locations, or dates within a text. By applying NER to news articles, key entities and gain insights into the entities mentioned in the news, their relationships, and their prominence, can be extracted. This can help in identifying important individuals, organizations, or locations associated with specific news topics.

Topic modeling is a statistical technique used to discover abstract topics or themes within a collection of documents. By applying topic modeling to a set of news articles, the underlying topics or themes present in the articles cane be identified. This can provide insights into the distribution of different topics, the emergence of new trends, or the prevalence of certain subjects within the news.

Text summarization techniques can be used to automatically generate concise summaries of news articles. These summaries can provide a quick overview of the main points or key information in the article, allowing users to quickly grasp the content without reading the entire article. This can be particularly useful for news aggregators or applications that provide curated news content.

Information extraction techniques aim to identify and extract structured information from unstructured text. By applying information extraction to news articles, specific pieces of information, such as events, dates, locations, or relationships between entities, can be extracted. This can provide insights into the factual information contained within the articles.

These NLP techniques can be applied individually or in combination to analyze and gain insights from news articles. They enable automated processing, organization, and understanding of large volumes of textual data, facilitating effective information retrieval and analysis in the field of news and media.

4. DISCUSSION

To validate the effectiveness of the iTrust News Certificate, we propose the development of a working prototype that will undergo rigorous testing within the media ecosystem in South East Europe. Furthermore, we invite other media organizations interested in utilizing the iTrust News Solution free of charge to participate in the testing phase. The successful implementation of this prototype will serve as a catalyst to attract additional funding and expand our reach, with the ultimate goal of establishing iTrust News as a European standard for reputation management and the fight against fake news.

By developing a prototype that will be tested within the media ecosystem in South East Europe, as well as inviting other media organizations from other parts of Europe and the whole world to utilize the iTrust News Solution, we aim to establish a robust and effective standard for maintaining the reputation and combating fake news. The successful implementation of the iTrust News Certificate has the potential to attract further funding and grow into a European benchmark, contributing to the restoration of trust and accuracy in news reporting while safeguarding democratic processes and universal freedoms in the digital era.

To support our recommendations, we will conduct statistical analyses on relevant datasets, including the performance of AI algorithms in identifying suspicious content, the detection accuracy of deep fake detection tools, and the impact of reputation scores on content evaluation. These analyses aim to provide quantitative insights into the strengths and weaknesses of the proposed solution.

The development of an adequate UI/UX design poses challenges in ensuring user satisfaction and engagement. The testing phase requires careful organization and precision to guarantee the reliability of the application. Furthermore, real-time monitoring of news updates and the accurate detection of meaningful changes present additional challenges.

It is important to acknowledge certain limitations in our work. The rapidly evolving nature of technology and the limited availability of comprehensive datasets posed challenges in conducting a comprehensive evaluation. Moreover, the feasibility and scalability of implementing blockchain-based solutions require further exploration and real-world testing.

Implementing and maintaining a distributed blockchain system requires significant technical expertise. Developing secure and robust smart contracts, setting up the necessary infrastructure, and ensuring network consensus can be complex and costly. The need for ongoing updates and improvements to address emerging vulnerabilities further adds to the technical complexity.

While blockchain technology ensures transparency and immutability of the recorded reviews, it may pose challenges to reviewers' privacy. The public nature of the blockchain means that reviews can be traced back to individual reviewers, potentially compromising their anonymity. Ensuring the confidentiality of reviewers while maintaining the integrity of the blockchain is a complex task.

5. CONCLUSIONS

This paper presents a comprehensive architectural design overview of an innovative application for user-validated news rating and analysis. By leveraging smart contracts, blockchain technology, and NLP techniques, the application aims to enhance the credibility and evaluation of news articles. The proposed architecture provides a foundation for developing a reliable and user-friendly solution that addresses the challenges associated with misinformation in the digital age.

By leveraging blockchain technology, user ratings, and independent fact-checking processes, iTrust News Certificate presents a user-friendly solution that empowers individuals to effectively identify and combat fake news. With the potential to reshape the media landscape, this innovative platform holds promise for fostering trust, transparency, and accuracy within the realm of news reporting.

The successful implementation of the iTrust News Certificate will contribute to the ongoing efforts to combat fake news and improve the quality of news dissemination. Moreover, it has the potential to encourage media organizations and journalists to prioritize accuracy and accountability in their reporting practices. Ultimately, this innovative platform can significantly foster a more trustworthy and reliable news ecosystem. To the best knowledge of the authors, this is the pioneering architectural blockchain design work in this direction and could be expanded and applicable in different contexts of this topic.

The next step in our future work will be the full implementation of the iTrust News Certificate platform designed during our previous work, deploying it on the real blockchain network and/or blockchain cloud, and putting it into real-life operation.

FUNDING:

This research received no external funding.

INSTITUTIONAL REVIEW BOARD STATEMENT:

Not applicable.

INFORMED CONSENT STATEMENT:

Not applicable.

CONFLICTS OF INTEREST:

The authors declare no conflict of interest.

REFERENCES

[1] Edelman. (2022). Edelman Trust Barometer 2022 [Online]. Available: https://www.edelman.com/trust/2022-trust-barometer [Accessed: June 20, 2023].

[2] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," *Science*, vol. 359, no. 6380, Mar., pp. 1146–1151, 2018.

[3] H. Allcott and M. Gentzkow, "Social media and fake news in the 2016 election," *Journal of Economic Perspectives*, vol. 31, no. 2, Spring, pp. 211–236, 2017.

[4] S. Lewandowsky, U. K. H. Ecker, and J. Cook, "Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era," *Journal of Applied Research in Memory and Cognition*, vol. 6, no. 4, Dec., pp. 353–369, 2017.

[5] G. Pennycook and D. G. Rand, "The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Stories Increases Perceived Accuracy of Stories Without Warnings," Management Science, vol. 67, no. 11, Nov., pp. 4944–4957, 2019.

[6] A. Guess, B. Nyhan, and J. Reifler, "Exposure to Untrustworthy Websites in the 2016 U.S. Election," *Nature Human Behaviour*, vol. 4, no. 5, May, pp. 472–480, 2020.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, Nov., pp. 352–375, 2018.

[8] S. Zannettou, T. Caulfield, E. De Cristofaro, and M. Sirivianos, "Disinformation warfare: Understanding state-sponsored trolls on Twitter and their influence on the web," *ACM Transactions on the Web*, vol. 13, no. 3, Aug., Article 17, 2019.

[9] D. O'Loughlin, P. Matthews, and I. U. Rehman, "An exploration of blockchain-based anti-fake news systems," *Information Processing and Management*, vol. 57, no. 2, Mar., Article 102082, 2020.

[10] Y. Zhang, E. Chang, and G. Li, "Blockchain-based trust management for fake news detection in social media," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 1, Mar., pp. 51–63, 2020.

[11] Y. Zhang, H. Gao, X. Fan, and E. Chang, "BlockFake: Towards blockchain-based automated fake news detection model for social media," *Future Generation Computer Systems*, vol. 115, May, pp. 495–505, 2021.

[12] Next Generation Internet. (2017, October). HUB4NGI D2.1: NGI Architecture Definition – Version 1.0. [Online]. Available: https://www.ngi.eu/wp-content/uploads/sites/48/2017/10/hub4ngi_d2.1_v1.0.pdf [Accessed: June 20, 2023].

[13] D.M.J. Lazer, et al., "The science of fake news," *Science*, vol. 359, no. 6380, Mar., pp. 1094–1096, 2018.

[14] Y. Benkler, R. Faris, and H. Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, Oxford University Press, 2018.

[15] L.M. Neudert, et al., "A Longitudinal Measurement Study of 4chan's Politically Incorrect Forum and its Effect on the Web," ArXiv preprint arXiv:1908.08313, Aug. 2019.

[16] G. Pennycook and D.G. Rand, "The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Stories Increases Perceived Accuracy of Stories Without Warnings," *Management Science*, vol. 66, no. 11, Nov., pp. 4944–4957, 2019.

[17] N. Ruchansky, et al., "CsiNet: A Convolutional Neural Network Approach for Fake News Detection," arXiv preprint arXiv:1709.09064, Sept. 2017.

[18] K. Popat, et al., "Deception Detection in News Articles Using Headline Features," In Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing (EMNLP), Brussels, Belgium, 2018, pp. 3057–3067.

[19] D.T. Vo, et al., "Combining Graph Convolutional Networks and LSTMs for Fake News Detection," In Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP), Online, 2020, pp. 3442–3452.

[20] M. Potthast, et al., "A Stylometric Inquiry into Hyperpartisan and Fake News," In Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing (EMNLP), Copenhagen, Denmark, 2017, pp. 2319–2324.

[21] News Provenance Project. [Online]. Available: https://www.newsprovenanceproject.com/ [Accessed: June 20, 2023].

[22] AI Research at Facebook. (n.d.). DFDC – Deepfake Detection Challenge Dataset. [Online]. Available: https://ai.facebook.com/datasets/dfdc/ [Accessed: June 20, 2023].

[23] Civil. [Online]. Available: https://civil.co/ [Accessed: June 20, 2023].

[24] NWZER. [Online]. Available: https://nwzer.com/ [Accessed: June 20, 2023].

[25] Fundsup. "Featured on Fundsup: Mavin.org – Content Integrity Movement," Fundsup.co [Online]. Available: https://fundsup.co/featured-on-fundsup-mavin-org-content-integrity-movement/ [Accessed: June 20, 2023].

[26] C. Li, et al., "Smart Contract-Based Crowdfunding for Decentralized Applications," In Proceedings of the 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Prague, Czech Republic, 2017, pp. 456–459.

[27] K. Wang, et al., "Smart Contract-Based Supply Chain Traceability System," In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 3531–3536.

[28] J. Li, et al., "Smart Contract-Based Escrow Service for Secure and Trustworthy E-Commerce Transactions," In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 5120–5125.

[29] A. Kiayias, et al., "On Blockchain and Voting," In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 2017, pp. 839–847.

[30] M. -V. Vladucu, Z. Dong, J. Medina and R. Rojas-Cessa, "E-Voting Meets Blockchain: A Survey," *IEEE Access*, vol. 11, pp. 23293–23308, 2023, DOI 10.1109/ACCESS.2023.3253682