International Journal of Gender, Science and Technology
ISSN: 2040-0748
UGC Care Group I Journal.
Vol-12 Issue-02 Dec 2023
https://ijgst.com.2023.v12.i2.pp169-173

PEER-TO-PEER PLATFORM FOR DATA STORAGE AND EXCHANGE TO STOP DIGITAL FRAUD

Y. YESU BABU [1] G THANUJA [2] G.SIDDHANTH [3] TADIKAMALA VINEELA [4]
[1]ASST.PROFESSOR, DEPARTMENT OF ARTIFICIAL INTELLIGENCE,
[2] PROFESSOR, DEPARTMENT OF ARTIFICIAL INTELLIGENCE,
[3]ASST. PROFESSOR, DEPARTMENT OF ARTIFICIAL INTELLIGENCE,
[4] ASST. PROFESSOR, DEPARTMENT OF ARTIFICIAL INTELLIGENCE,
[1,2,3,4] SRI MITTAPALLI COLLEGE OF ENGINEERING

Abstract- Some have questioned the proper use of the web and social media in contemporary democracies in light of the proliferation of persistently inaccurate and misleading information. The rapid and widespread distribution of digital disappointment has societal and emotional costs, but it also has the potential to create substantial economic losses or even challenges to national security. By creating a safe peer-to-peer platform for data storage and exchange and by providing transparent, immutable, and verifiable data tracking, distributed ledger technologies (DLTs) like blockchain guarantee the authenticity and tracking of data. Examining the possible use of DLTs to forestall digital disappointment, outlining the most pertinent applications, and drawing attention to their key unanswered questions are the overarching goals of this research. Furthermore, some recommendations for researchers in the future are provided on issues that need to be resolved to make modern internet media more resilient to cyber assaults.

Keywords—Block Chain, DLT, deep fakes, fake news, data traceability, decentralization, cyber security.

I. INTRODUCTION

New challenges and possibilities arise with the rise of Distributed Ledger Technologies (DLTs), particularly blockchain, which policymakers may use to combat the spread of disinformation. In a decentralised peer-to-peer (P2P) network [1], these technologies provide privacy, security, and trust in the absence of a central management authority. The input content's legitimacy cannot be adequately assessed by the DLT system on its own. Therefore, in order for other data to be deceptive, a system that can withstand data falsification attacks and use it in the DLT is necessary. To address this problem, it is necessary to include contextual information in order to verify the accuracy of the news. To further our knowledge and gauge confidence, future research may combine DLT with AI and NLP [2]. While building a peer-to-peer platform to share, store, and protect information for fake news, DLT guarantees data provenance and traceability. This article provided an analysis of many existing applications and proposed various novel approaches to content control. We believe that DLT's trust mechanisms are more suited to prove content authenticity and audit and eliminate false news than other technologies, despite the fact that DLT technology has practical and technical limitations in the battle against fake news. Further, it is recommended that researchers in the future develop solutions combining AI and DLT in order to address all aspects of fake news in a more comprehensive and coordinated manner [3-6].

International Journal of Gender, Science and Technology
ISSN: 2040-0748
UGC Care Group I Journal.
Vol-12 Issue-02 Dec 2023
https://ijgst.com.2023.v12.i2.pp169-173

II. RELATEDWORKS

Few articles in the literature use blockchain technology to combat disinformation; those that do tend to focus on tracking down the original sources of news stories [7]. As far as the authors are aware, however, this is the first piece to provide a comprehensive strategy for combating disinformation with DLTs. I have provided a full description of the phenomenon, its prevalence, and the effectiveness of DLTs in dealing with fake news and the major difficulties they raise. This paper aims to foresee and address any issues that DLT may cause to disrupt the media industry [8]. Secure and efficient data storage, processing, sharing, authentication, scalability, transparency, and accounting are all possible with distributed ledger technologies like the Tangle or blockchains [9]. Because transactions cannot be altered once a network consensus has been broadcast, authorised, and confirmed [10] and may be stored in blocks, such features (Figure 1) can be useful in combating misleading information in conjunction with oracle-allowed smart contracts. Furthermore, all parties involved may easily verify the legitimacy of transactions. This article explains how DLT and blockchain work internally, but if you're interested in learning more about how to build a blockchain that fits your company's needs and the environment where it will be deployed, you can find a lot of information in [11, 12]. The use of DLT to detect, prevent, and identify fake news has only been the subject of a small number of studies. As seen in Figure 1, this section delves into the most crucial applications.

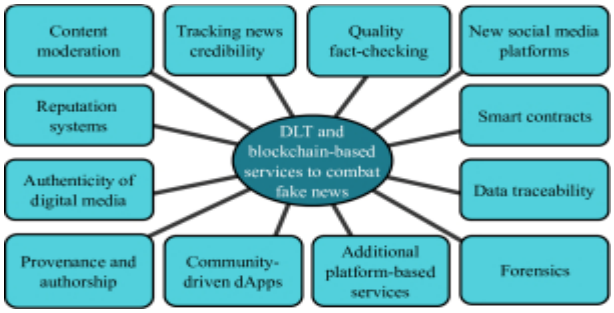

Fig. 1: DLT and block chain-based applications to combat fake news.

Content Moderation Traditional approaches to content moderation, such as flagging, notification, and deconstruction, assume a centralised regulator and the capacity to swiftly remove material via technology. If there are decentralised networks that allow everyone to join or become a transaction validator, this is especially not the case with DLTs. To that end, further research on the topic is required.An open standard for by traversing a single branch of the tree (level 0) all the way to the root. monitoring the reliability of news sources The proof-of-truthfulness (PoT) concept is introduced by Qayyum et al. [13]. It enables any node in the network to verify the inclusion or exclusion of data in a blockchain. The data is stored in a binary tree, which is constructed using hash-pointers. Each node in the tree contains hash-points to the data at level n. With a given piece of material, O(log(n)) can verify its accuracy

Discovering the truth and doing high-quality fact-checking with incentives

https://ijgst.com.2023.v12.i2.pp169-173

A program developed in Latvia, 4Facts.org, is an example of a scalable fact-checking system that uses blockchain technology [14]. You may earn tokens or other forms of monetary reward for confirming the data, and your reputation for high-quality work will grow as a consequence of your efforts. The amount of people who benefit from your fact-checker's work will increase as your reputation is improved. In addition to attracting content providers, the proposed method would encourage them to provide validation materials in an effort to boost their credibility.

Creation of social media platforms that use digital identities

Decentralised applications (dApps) developed by Tim Berners-Lee and the Massachusetts Institute of Technology (MIT) in accordance with the principles of Linked Data have the potential to improve data ownership, access control, location, and privacy. Another instance is the material Blockchain Project, developed by iRights.Lab in Germany. It is a decentralised and open ecosystem that aims to distribute media material that is managed and owned by industry. An essential part of the project was the development of a standard International Standard Content Code (ISCC), which is similar to other well-established identificators like the International Standard Book Number (ISBN) or the International Standard Serial Number, but with improved capabilities to facilitate the creation of an intuitive ISCC application. The program is also making an effort to streamline the licencing process for digital material so that it may be given more easily and faster.

An editor's trustworthiness and any bias-inducing traits in the text may be evaluated using a reputation score. Each unverified media starts with a score of zero in the proposed dynamic reputation system [15], and the score changes as the entity shares more trustworthy verified news [16]. Your identity will be revoked if you fail to achieve a particular reputation level within a certain term. As is the case with BitPress, registered users may provide dependable feedback via the platform [17]. But subjectivity, bias, and the existence of malicious individuals need further investigation.

The authenticity of digital media Automatic Content Management and multi-node content verification may tackle the difficulty of authenticating Big Data News streaming. Data ledger technologies (DLTs) inherently guarantee data integrity due to the storage of transactions. For essential notarial services, the DLT is the backbone infrastructure[18]. But a major obstacle is figuring out how to check data in a block for authenticity before putting it. An important step that service providers may take is to use public key infrastructure (PKI) to notarise the information, for example by creating a digital signature. Provenance and Authorship

In addition to making the source visible and holding the source responsible in the event of a bogus detection, DLT would make content fabrication almost impossible. Even if multimedia content has been heavily altered, knowing where it came from is useful. Huckle et al. [19] proposed an Ethereum architecture with standardised metadatos as a means to validate the authenticity and source of digital material. While this prototype makes use of the P2P content-addressed filesystem (IPFS) [20], it still has a very limited ability to detect fake resources (i.e., it cannot independently verify the legitimacy of an entire story). Apps created by the community

Tokens may be used in crowdfunding to encourage the finding of truths. Using the

https://ijgst.com.2023.v12.i2.pp169-173

same social network, users of DLT-based social networks may simply trade toks or currencies. One use case is the elimination of middlemen from P2P transactions by use of encrypted intelligent contracts, allowing users to deal quickly and securely with one another.

III. CHALLENGES AND RECOMMENDATIONS

To help future academics, developers, and managers in their battle against digital disillusion, we have compiled a list of the most pressing open challenges and suggestions. Currently, researchers are mostly concentrating on validated fake content, a specific kind of misleading news. The bulk of digital detection solutions rely on cryptography, which is noise-sensitive and may produce a new hash if a character, pixel, or content element is changed. Using noticeable hazelnuts yields comparable resources, even if there will be drastically different hazels with a little change in two resources. One alternative approach to this problem is to use a semantic similarity index on the data made public by various sources. Since decentralisation and consensus techniques impact performance and scalability, DLT design should account for the amount of decentralisation and consensus methods that are essential, for example, for transaction processing. Another pressing issue is the potential use of ML/DL models trained on fraudulent information in order to strengthen cyber defences while simultaneously protecting the privacy and security of content published on social media. With distributed ledger technology (DLT), data may be encrypted in a manner that makes it possible to track every interaction and transaction. Previous distributed ledger technology (DLT) cryptography is susceptible to certain quantum computer assaults; so, post-quantum blockchain solutions need more investigation. Unresolved issues with DLT GDPR compliance include the controller's role, data anonymization's feasibility, and the facilitation of subject rights. Platforms of the future will need to strike a balance between content filtering (such as free speech and the right to receive information) and data protection in order to provide users with both security and transparency. There is also concern that a small number of powerful players may use unreliable technological systems to govern people's social interactions and financial activities. A multi-sectoral response is necessary to the rapidly expanding issue of digital deception and misinformation, which includes sectors such as business, government, and the media. Furthermore, no fix (such as customised solutions) can be fitted to the generic intervention methods.

IV. FUTURE SCOPE AND CONCLUSION

While building a peer-to-peer platform to share, store, and protect information for fake news, DLT guarantees data provenance and traceability. This article provided an analysis of many existing applications and proposed various novel approaches to content control. We believe that DLT's trust mechanisms are more suited to prove content authenticity and audit and eliminate false news than other technologies, despite the fact that DLT technology has practical and technical limitations in the battle against fake news. Also, academics in the future are urged to use AI and DLT to find answers for all aspects of fake news in a larger, more coordinated effort.

REFERENCES

[1] K. Panetta, Gartner Top Strategic Predictions for 2018 and Beyond. Gartner, 2017.
[2] Disinformation and propaganda – impact on the functioning of the rule of law in the EU

and its Member State. Directorate General for Internal Policies of the Union, PE 608.864, 2019.

[3] C. Wardle and H. Derakhshan, "Information disorder: Toward an interdisciplinary framework for research and policy making," Council of Europe policy report DGI(2017)09, 2017.

[4] V. Bakir and A. McStay, "Fake news and the economy of emotions: Problems, causes, solutions," Digital Journalism, 6(2), 154-175, 2018.

[5] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," Science, 359 (6380), 1146-1151, 2018.

[6] H. Rainie, J. Q. Anderson and J. Albright, "The future of free speech, trolls, anonymity and fake news online," Washington, DC: Pew Research Center, 2017.

[7] H. Kim, P. Garrido, A. Tewari, W. Xu, J. Thies, M. Niessner, P. Pérez, C. Richardt, M. Zollhöfer, and C. Theobalt, "Deep video portraits," ACM Transactions on Graphics (TOG), 37(4), 163, 2018.

[8] A. Andorfer, "Spreading like Wildfire: Solutions for Abating the Fake News Problem on Social Media via Technology Controls and Government Regulation," Hastings LJ, 69, 1409, 2017.

[9] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, "Fake news detection on social media: A data mining perspective," ACM SIGKDD Explorations Newsletter, 19(1), pp. 22-36.

[10] A. Shahaab, B. Lidgey, C. Hewage and I. Khan, "Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review," in IEEE Access.

[11] P. Fraga-Lamas and T. M. Fernández-Caramés, "A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry," IEEE Access, vol. 7, pp. 17578-17598, 2019.

[12] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories," IEEE Access.

[13] A. Qayyum, J. Qadir, M. U.Janjua, F. Sher, "Using Blockchain to Rein in The New Post-Truth World and Check The Spread of Fake News," arXiv preprint arXiv:1903.11899, 2019.

[14] 4Facts.org official webpage. Online: https://www.4facts.org/

[15] Solid official webpage. Online:https://solid.mit.edu/

[16] Content Blockchain Project official webpage. Online:https://irights-lab.de/en/launch-of-the-content-blockchain-project/

[17] BitPress official webpage. Online:https://bitpress.news/

[18] G. Song, S. Kim, H. Hwang and K. Lee, "Blockchain-based Notarization for Social Media," 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, pp. 1-2.

[19] S. Huckle, and M. White, "Fake news: a technological approach to proving the origins of content, using blockchains," Big data, 5(4), 356-371, 2017.

[20] IPFS official webpage. Online:https://ipfs.io/

[21] First results of the EU Code of Practice against disinformation. Online: https://ec.europa.eu/digital-single-market/en/news/first-results-eu-code-practice-against-disinformation

[22] Vivek, Kolla, et al. "An Efficient Triple-Layered and Double Secured Cryptography Technique in Wireless Sensor Networks." *2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*. IEEE, 2021.

[23]Anusha, Pureti, T. Sunitha, and Mastan Rao Kale. "Detecting and Analyzing Emotions using Text stream messages." *ECS Transactions* 107.1 (2022): 16913.