Utilizing Ledger and Block chain Technologies to fight digital fraud and fake Reality

A Vennela #1, A Jyoshna #2, B Radhika #3, M Deepika #4, R Mounika #5
#1 Asst. Professor, Dept. Of CSE, Qis Institute of Technology,Ongole,Prakasam (Dt)
#2,3,4,5 B.Tech., Scholars, Dept of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)

Abstract- The growth of omnipresent, deep-seated fake information, misinformation, and misleading information, sometimes called false news, raises questions about the role of the Internet and social media in modern democratic countries. Digital disappointment has not just an emotional or a social cost because of its quick and extensive dissemination but may also cause major economic losses or national security threats. The block chain and other distributed ledger technologies (DLTs) ensure the origin and traceability of data by offering transparent, immutable and verifiable data tracking while establishing a secure peer-to-peer platform for data storage and exchange. This study seeks to investigate the potential of DLTs to prevent digital disappointment, describe the applications most relevant and highlight their major open issues. In addition, some guidelines for future investigators are outlined on topics which must be addressed in order to improve the resistance of today's online media to cyber attacks.
Keywords—Block Chain, DLT, deep fakes, fake news, data traceability, decentralization, cyber security.

I. INTRODUCTION

Today, Distributed Ledger Technologies (DLTs) and especially block chain, represent new difficulties but also opportunities for policymaking as a viable tool that may assist to address the challenge of fake news. These technologies provide confidentiality, safety and trust in a decentralized peer-to-peer (P2P) network [1] without any central management authority being present. The DLT system alone cannot properly assess the input content authenticity. Consequently, a system that is robust to data falsification assaults that incorporates falsified data in the DLT is required if other data is to be misleading. In order to deal with this issue, contextual knowledge should be included to confirm the integrity of the news. Additional study may involve the use of DLT, in conjunction with AI and NLP, to create profound understandings and measure confidence [2]. DLT ensures data provenance and traceability throughout the development of a P2P platform to exchange, store and secure information for counterfeit news. This paper evaluated several current applications and recommended a number of new content control methods. While DLT technology's technological and practical constraints exist in the fight against fake news, our belief is that DLT's trust mechanisms are more adapted to demonstrate content authenticity and to audit and eradicate fake news than other technologies. In addition, in an expanded, coordinated effort to cover all elements of false news, future researchers are encouraged to create combined AI and DLT solutions [3-6].

II. RELATEDWORKS

Only a few publications in the literature employ the block chain to fight false news and are mostly concerned with the tracing of news sources [7]. But this is the first article that proposes a holistic method to fighting false news through DLTs, as authors understand. Therefore, the phenomena and its prevalence and the usefulness of DLTs in dealing with false news and the key issues they present are comprehensively overviewed. The objective of this document is to predict and tackle the problems that DLT might make to revolutionize media business [8]. Distributed Ledger technologies such as the Tangle or block chains can enable efficient and secure

identification, data storage, processing and sharing, attack robustness, scalability, transparency and accounting [9]. Such characteristics (Figure 1) can play an effective role in countering false information along with the use of smart contracts allowed by oracles as transactions can be not manipulated once a network consensus has been transmitted, approved, and validated [10] and can be kept in blocks. In addition, all participating parties may readily audit transactions. While this article contains a description of the internal operation of DLT and blockchain, interested readers may find extensive information on how to create a block chain in accordance with business requirements and the deployment environment in [11, 12]. Only a few research evaluate the application of DLT to identify, prevent and detect news falsified. This section examines the applications most important and is summarized in Figure 1.

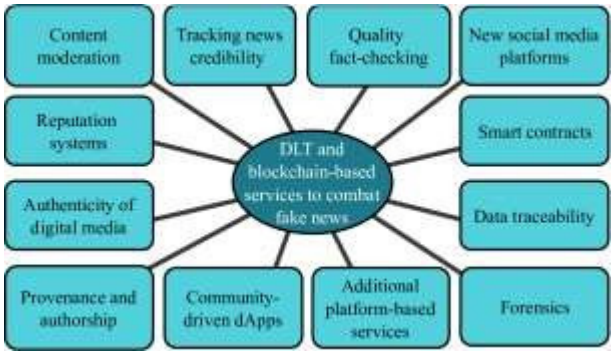

Fig. 1: DLT and block chain-based applications to combat fake news.

Content moderation

Conventional content moderation methods (for example, flagging, notification and decomposition) take into account the presence of a centralized regulator and the technological possibility of quickly removing content. This is not always true for DLTs, particularly if unauthorized networks enable anybody to join or become a validator for a transaction and there are no central authorities. Further study in this subject is thus necessary.

An open protocol for tracking news credibility

Qayyum et al. [13] introduces the proof-of-truthfulness (PoT) idea, which allows any network node to check whether or not a block chain contents are included. The contents are kept in a binary tree, wherein hash-pointers are used to create a binary tree, where n−1 nodes carry hash-points to the contents of n level. Given a certain content, O(log(n)) can check its confidence by searching from contents to the root through a single tree branch (level 0).

Incentivized discovery of truth and quality fact-checking

The scalable block chain-based Fact Checking system [14] is an example of Latvian platform 4Facts.org. Reliable data controls are discovered to let you receive cash compensation (for example, tokens) and improve your reputation for high quality work as a result of your interest in validating the material. As your fact-checker enhances your reputation, the number of recipients will rise. The suggested approach will also interest content providers to submit their validation material to enhance their reputation.

Creation of social media platforms that use digital identities

A proposed set of tools (dApps) for creating decentralised social apps based on the concepts of Linked Data, led by Tim Berners-Lee jointly with the MIT, would increase privacy and real data ownership, access control and location. Another example is the Content Blockchain Project (iRights.Lab, Germany), a blockchain ecosystem open and decentralised for distribution of

media content controlled and owned by industry. A standard International Standard Content Code (ISCC), which is comparable to established identificators, such as International Standard Book Number (ISBN) or the International Standard Serial Number, have been developed as a key element of the project, but with enhanced functionality for the creation of an easy-to-use ISCC application. The initiative also works to simplify the licencing of digital content to allow it to be issued more simply and quickly.

Reputation systems

Computing a reputation score may be used to assess an editor's credibility and notify readers if the text has characteristics that may suggest bias. In [15] a dynamic reputation is proposed: each unverified medium has a zero starting score and the score evolves as a reliable verified news is shared by the entity [16]. If you do not acquire minimum reputation within a certain timeframe, your identification shall be cancelled. Registered consumers offer feedback on reliability through the platform, as is the case with BitPress[17]. However, it is necessary to examine further the question of subjektivity, partiality and the possibility of malevolent actors.

Authenticity of digital media

The challenge of validating Big Data News streaming can be solved by Automatic Content Management and multi-node content verification. As long as transactions are stored, DLT's naturally ensure data integrity. The DLT is a fundamental notarial services infrastructure[18]. However, a fundamental challenge is how to verify that data is not fabricated in a block before it is put. Service providers can take an essential part in ensures that the material is notarized utilising a public key infrastructure (e.g., by the generation of a digital signature) (PKI).

Provenance and authorship

DLT would also make content falsification nearly unavailable by showing the source, and would make the source accountable if it detected a fake. Provenance of multimedia material is helpful that may be deeply forged. In order to verify digital media validity and origins, Huckle et al [19] suggested an Ethereum architecture with standardized metadatos. This propotype utilises the P2P content-addressed filesystem (IPFS) [20]. The capacity of the system is nonetheless considerably reduced to find bogus resources (i.e., it is not able to prove the authenticity of a storey as a whole).

Community-driven Apps

Crowdfunding may employ tokens to stimulate truth discovery. Users may easily swap toks or currencies in DLT based social networks over the same social network. Users may, for example, do business with safe and quick P2P transactions without third-party intermediaries using encrypted intelligent contracts.

III. CHALLENGES AND RECOMMENDATIONS

The following are the most important open problems and recommendations in the fight against digital disillusion for future researchers, developers and managers. The present efforts of the research community are mostly focused on one form of false news, i.e. verified false material. The majority of the digital detection offers are based on cryptography haze sensitive to noise and can result in a different hash if a changes in a character, a pixel, or something in a particular content occur. Although there will be significantly different hazels with a minimum modification in two resources, the usage of perceptible hazelnuts results in equivalent resources. The usage of a semanticized similarity index of the information released by several sources is another way of solving this challenge. DLT design should be adjusted to take into account the amount of necessary decentralisation and consensus methods since they affect performance and

scalability (e.g. transaction processing). Strengthening cyber security and maintaining the privacy and security of social media-shared material is also an important problem, as the training of an ML/DL model for false content may be employed. DLT-based systems can encrypt material in a way that traceability can be established for each transaction and interaction. Most existing DLT encryption is vulnerable to some quantum computer attacks, which means that post-quantum blockchain solutions have to be further examined. The problem of DLT GDPR compliance remains unresolved, especially when it comes to the position of the controller, the viability of data anonymization and facilitating subject rights. Future platforms must provide security and transparency by ensuring a trade-off between moderation of content (e.g. freedom of speech, right to receive information) and protection of personal data. There are further worries that social relationships and transactions might be managed through untrustworthy technology systems controlled by a few dominating actors. Digital disappointment and falsification are a fast growing problem which demands interdisciplinary cooperation (e.g. industry, government and media). In addition, the general intervention mechanisms cannot be fitted with any remedy (e.g., personalised solutions).

IV. FUTURE SCOPE AND CONCLUSION

DLT ensures data provenance and traceability throughout the development of a P2P platform to exchange, store and secure information for counterfeit news. This paper evaluated several current applications and recommended a number of new content control methods. While DLT technology's technological and practical constraints exist in the fight against fake news, our belief is that DLT's trust mechanisms are more adapted to demonstrate content authenticity and to audit and eradicate fake news than other technologies. In addition, in an expanded, coordinated effort to cover all elements of false news, future researchers are encouraged to create combined AI and DLT solutions.

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] W. Shang, M. Liu, W. Lin, and M. Jia, "Tracing the Source of News Based on Blockchain," 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS), Singapore, 2018, pp. 377-381.
[23] "Blockchain and the GDPR," Thematic report. European Union Blockchain Observatory and Forum, 2018.