COMPREHENSIVE STUDY ON DISTRIBUTED LEDGER TECHNOLOGIES AND BLOCK CHAIN BASED SERVICES TO COMBAT FAKE NEWS

Mrs.Sravanthi Sallaram
Assistant Professor,Department of Computer Science and Engineering,
St.Martin's Engineering College,Dhulapally, Near Kompally,Secunderabad-500 100.Telangana,
India

Abstract-

The emergence of ubiquitous, deep-seated fake information, disinformation, and misleading information, commonly dubbed false news, raises challenges about the role of the Internet and social media in contemporary democratic societies. Digital disappointment is not merely an emotional or a social cost because of its swift and broad dissemination but may also generate major economic losses or national security dangers. The block chain and other (DLTs) assure the origin and traceability of data by giving transparent, immutable and verifiable data tracking while building a secure peer-to-peer platform for data storage and exchange. This research aims to evaluate the potential of DLTs to avoid digital disappointment, to describe the most relevant applications and to highlight their major outstanding concerns. In addition, some advice for future investigators are presented on areas which must be addressed in order to strengthen the resistance of today's online media to cyber assaults.

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

I. INTRODUCTION

Today, Distributed Ledger Technologies (DLTs) and notably blockchain, offer new obstacles but also chances for policymakers as a feasible instrument that may help to handle the dilemma of fake news. These technologies guarantee anonymity, safety and trust in a decentralized peer-to-peer (P2P) network [1] without any central management authority being present. The legitimacy of the input content cannot be accurately assessed by the DLT system on its own. Consequently, a system that is resilient to data fabrication attacks that integrates fabricated data in the DLT is essential if other data is to be deceptive. It is essential that contextual information be included into news reporting in order to ensure its accuracy. Additional investigation may entail the use of DLT, in combination with AI and NLP, to construct deep understandings and gauge confidence [2]. DLT enables data provenance and traceability throughout the construction of a P2P platform to share, store and safeguard information for counterfeit news. This article analyzed various existing applications and advocated a number of new content control mechanisms. While DLT technology's technical and practical limits exist in the battle against fake news, our conviction is that DLT's trust mechanisms are better fitted to establish content authenticity and to audit and eliminate fake news than other technologies. In addition, in an extended, coordinated effort to address all parts of fake news, future researchers are urged to produce integrated AI and DLT solutions [3-6].

II. RELATEDWORKS

Most papers in the literature focus on tracking news sources rather than using the block chain to combat false news [7]. Although the authors comprehend DLTs, this is the first article to suggest a comprehensive strategy for combating false news. Therefore, the phenomenon and its ubiquity and the effectiveness of DLTs in dealing with false news and the fundamental concerns they offer are extensively overviewed. The purpose of this paper is to forecast and handle the challenges that DLT could cause to change media industry [8]. It is possible to store, process, and share data in a safe and efficient manner using Distributed Ledger technologies such as the Tangle or block chains [9]. The use of smart contracts permitted by oracles, together with features like those shown in Figure 1, may effectively counter false information by preventing transactions from being changed after a network consensus has been conveyed, accepted, and validated[10]. Auditing transactions is easy for everyone involved. While this article describes the internal workings of DLT and blockchain, interested readers may discover in-depth information on how to build a block chain in line with business needs and the deployment environment in [11, 12]. Only a few studies look at how DLT may be used to identify, avoid, and catch news stories that have been tainted. This section addresses the applications most significant and is summarized in Figure 1.

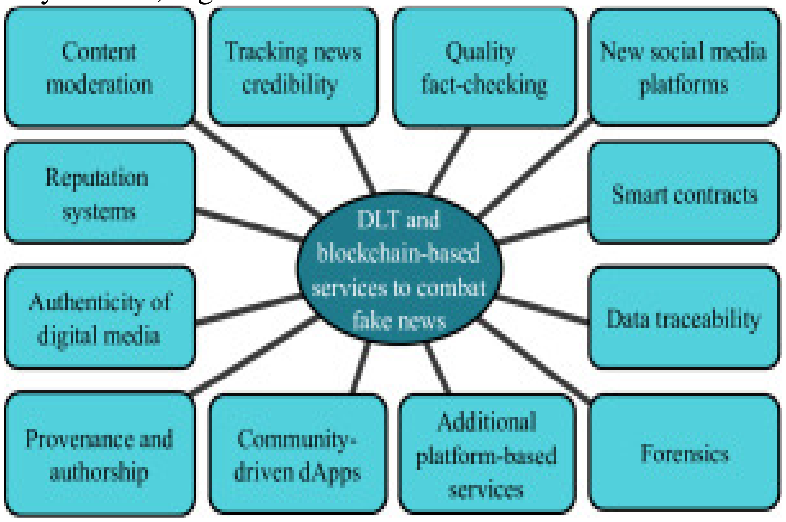
Content moderation
Tracking news credibility
Quality fact-checking
New social media platforms
Reputation systems
Smart contracts
DLT and blockchain-based services to combat fake news
Authenticity of digital media
Data traceability
Provenance and authorship
Community-driven dApps
Additional platform-based services
Forensics

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

Content moderation

Conventional content moderation techniques (for example, flagging, notification and deconstruction) take into consideration the existence of a centralized regulator and the technical capability of promptly eliminating content. This is not necessarily true for DLTs, especially if illegal networks permit everyone to join or become a validator for a transaction and there are no central authority. Further research in this issue is consequently warranted.

A transparent procedure for assessing the reliability of news reports

Qayyum et al. [13] proposes the proof-of-truthfulness (PoT) principle, which enables any network node to check whether or not a blockchain contents are included. The contents are preserved in a binary tree, whereby hash-pointers are utilized to form a binary tree, where n−1 nodes carry hash-points to the contents of n level. A single tree branch search from the contents to the root allows O(log(n)) to check its confidence in a given content (level 0).

Incentivized discovery of truth and excellent fact-checking

The scalable blockchain-based Fact Checking system [14] is an example of Latvian platform 4Facts.org. Validating the data allows you to obtain monetary compensation (such as tokens) and enhances your professional reputation as a reliable data controller. As your fact-checker boosts your reputation, the number of receivers will climb. The recommended approach would also entice content producers to contribute their validation material to increase their reputation.

Creation of social media networks that leverage digital identities

A proposed set of tools (dApps) for constructing decentralised social applications based on the principles of Linked Data, spearheaded by Tim Berners-Lee together with the MIT, would promote privacy and true 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. In addition, the project aims to streamline the licensing of digital content so that it may be distributed more swiftly.

Reputation systems

Computing a reputation score may be used to measure an editor's reliability and inform readers if the text contains traits that may imply bias. In [15] a dynamic reputation is proposed: each unverified outlet has a zero beginning score and the score develops as a trustworthy verified news is disseminated by the entity [16]. If you do not gain minimum reputation within a particular duration, your identity will be revoked. Registered customers submit comments on dependability via the platform, as is the case with BitPress[17]. However, it is vital to analyze further the topic of subjektivity, bias and the potential of evil individuals.

Authenticity of digital media

Automatic Content Management and multi-node content verification may help with the difficulty of authenticating Big Data News streaming. DLTs automatically assure data integrity as long as transactions are stored. The DLT is a basic notarial services infrastructure[18]. However, verifying that data in a block is not manufactured before it is put in poses a significant issue. Service providers may play a vital role in guaranteeing that the material is notarized employing a public key infrastructure (e.g., via the production of a digital signature) (PKI) (PKI).

Authorship and chain of custody

DLT would also make content fabrication practically inaccessible by exposing the source, and would make the source responsible if it discovered a fake. The ability to trace the origins of potentially tainted material is an asset. In order to validate digital media legitimacy and provenance, Huckle et al [19] proposed an Ethereum architecture with standardizedmetadatos. This propotypeutilises the P2P content-addressed filesystem (IPFS) [20]. The power of the system is however greatly decreased to discover fraudulent materials (i.e., it is not able to confirm the authenticity of a story as a whole) (i.e., it is not able to prove the authenticity of a storey as a whole).

Community-driven Apps

Crowdfunding may leverage tokens to encourage truth discovery. In DLT-based social networks, users may simply trade toks or currencies inside the same social network. Users may, for example, conduct business with secure and speedy P2P transactions without third-party middlemen using encrypted intelligent contracts.

III. CHALLENGES ANDRECOMMENDATIONS

The following are the most significant open challenges and suggestions in the battle against digital disillusion for future researchers, developers and managers. The current efforts of the research community are largely concentrated on one sort of false news, i.e. validated false material. The bulk of the digital detection options are based on cryptography haze susceptible to noise and may result in a different hash if a changes in a letter, a pixel, or anything in a specific content occur. Although there will be considerably different hazels with a small alteration in two resources, the usage of noticeable hazelnuts results in similar resources. The usage of a semantic zed similarity index of the material supplied by multiple sources is another way of overcoming this difficulty. DLT design should be updated to take into consideration the degree of required decentralization and consensus mechanisms as they impact performance and scalability (e.g. transaction processing) (e.g. transaction processing). Strengthening cybersecurity and safeguarding the privacy and security of social media-shared material is also an essential problem, since the training of an ML/DL model for false content may be applied. Material may be encrypted using DLT systems in such a way that each transaction and interaction's history can be tracked back to its source and provenance. Most present DLT encryption is susceptible to certain quantum computer attacks, which indicates that post-quantum blockchain solutions have to be further investigated. The problem of DLT GDPR compliance remains unclear, particularly when it comes to the role of the controller, the possibility of data anonymization and enabling subject rights. Future platforms must offer security and transparency by assuring a trade-off between moderation of content (e.g. freedom of expression, right to receive information) and protection of personal data. There are additional fears that social interactions and transactions may be governed via untrustworthy technological systems controlled by a few dominant people. Digital disappointment and deception are a rapidly rising problem which necessitates multidisciplinary collaboration (e.g. industry, government and media) (e.g. industry, government and media). In addition, the generic intervention mechanisms cannot be fitted with any cure (e.g., customised remedies) (e.g., personalised solutions).

CONCLUSION

DLT enables data provenance and traceability throughout the construction of a P2P platform to share, store and safeguard information for counterfeit news. This article analyzed various existing applications and advocated a number of new content control mechanisms. While DLT technology's technological and practical limits exist in the battle against fake news, our conviction is that DLT's trust mechanisms are better fitted to establish content authenticity and to audit and eliminate fake news than other technologies. In addition, in an extended, coordinated effort to cover all parts of false news, future researchers are urged to propose integrated 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.