Detecting fake news in social media using Ethereum Virtual Machine (EVM) approach in Blockchain Technology

Dr.M.Kannan[1]*, Mr.R.Venkadesh[2] and Mr.K.R.Sathish Kumar[3]

[1] Professor, Department of Computer Science and Engineering, Mahendra Engineering College (Autonomous), Namakkal. E mail: kannan@mahendra.info

[2,3] Assistant Professor, Department of Computer Science and Engineering, Mahendra Engineering College (Autonomous), Namakkal.

Article History
Received: **08.04.2024**
Revised and Accepted: **10.05.2024**
Published: **15.06.2024**

https://doi.org/10.56343/STET.116.017.004.003
www.stetjournals.com

ABSTRACT

Social media (SM) has evolved from simply connecting individuals to becoming a platform for sharing ideas, marketing businesses, organizing campaigns, and offering novel career opportunities. However, news disseminated through SM can significantly influence public opinion, both positively and negatively. The prevalence of misinformation makes it difficult for users to discern truth from falsehood, and such false information can harm individuals and communities. Therefore, detecting and halting the spread of fake news on social media is an urgent yet challenging task. This research proposes a blockchain-based approach to address this challenge of fake news detection on SM. Blockchain technology (BT) offers features such as traceability, transparency, confidentiality, tamper-proof security, data control, and monitoring, which our method leverages. In particular, we introduce an Ethereum Virtual Machine (EVM) combined with a Cipher-based Message Authentication Code (CMAC) — denoted as **EVM-CMAC** — within a blockchain environment to authenticate social media accounts. This EVM-CMAC approach verifies the legitimacy of user accounts, thereby increasing the likelihood of identifying the real users behind social media profiles and reducing the spread of fake news. We evaluated the proposed method and compared its outcomes with earlier blockchain-based approaches in social media, which primarily focused on blocking fake news and enhancing data privacy. Our evaluation confirms that the EVM-CMAC model provides an efficient and effective solution for authenticating accounts.

Keywords: Blockchain authentication, Cipher-based Message Authentication Code (CMAC), Ethereum Virtual Machine (EVM), Fake news detection, Social media

Dr. M. Kannan

Professor, Department of Computer Science and Engineering, Mahendra Engineering College (Autonomous), Namakkal.
E mail: kannan@mahendra.info

P-ISSN 0973-9157
E-ISSN 2393-9249

INTRODUCTION

For years now, online social networks (OSNs) such as WhatsApp, Facebook, Instagram, and Twitter have eclipsed traditional social media, becoming indispensable platforms for communication and news sharing (Szczepański *et al.*, 2021). These networks enable users to easily share information, reconnect with friends and former classmates, and form new communities across political, geographical, and cultural boundaries. Social media today connects millions

of people worldwide and facilitates the rapid exchange of knowledge. However, this ubiquity also gives rise to serious concerns regarding user privacy, censorship, and the rampant spread of fake news. To address these challenges, researchers are exploring decentralized social media architectures, with blockchain technology emerging as a promising foundation for next-generation networks (Guidi and Michienzi, 2021).

Fake news has emerged as a significant societal problem, capable of causing serious social, economic, and political consequences (Islam *et al.*, 2020). The term refers to false or fabricated news stories that are typically spread with malicious intent. The proliferation of fake news on social media has been linked to real-world events; for instance, researchers have noted its influence on major political outcomes such as the 2016 United States presidential election and the 2018 Brazilian presidential election (Almeida *et al.*, 2021).

Moreover, OSNs have rapidly transformed from mere platforms for sharing personal updates into primary channels for following news. These platforms now serve as forums where users can receive immediate feedback on global events and readily express their views, emotions, and concerns (Zhang and Ghorbani, 2020). During the COVID-19 pandemic, social media usage surged as individuals sought real-time information amid sudden developments in health, economic, social, and political spheres. In this environment, influential social media users began actively broadcasting news for various purposes. Inevitably, some of this widely shared content has been of questionable accuracy, with certain posts containing misinformation or propaganda (Duda-Chodak *et al.*, 2020).

Human factors also contribute to the spread of misinformation. Cognitive theories suggest that people are inherently susceptible to believing fake news (Biswas, Vyas and Baskar, 2021). Many individuals tend to accept and propagate information without verification, especially if the content aligns with their preexisting beliefs (Celliers and Hattingh, 2020).

Blockchain technology, originally introduced as the foundation of Bitcoin, is now being applied far beyond the financial sector (Chang *et al.*, 2020). Fundamentally, a blockchain is a decentralized ledger consisting of blocks of data linked together in chronological order, a concept that has garnered considerable attention in both finance and technology (Ozdemir, Ar and Erol, 2020). This technology integrates diverse computing techniques — including distributed data storage, peer-to-peer transmission, consensus algorithms, and cryptography — to ensure security and integrity. Blockchain is widely regarded as an innovative solution for data security, capable of providing a transparent, tamper-proof distributed ledger that fosters digital trust (Ozdemir, Ar and Erol, 2020).

In a blockchain network, each block is cryptographically linked to the previous one via a hash of the prior block's contents, while also containing its own transaction data and timestamp. Proof-of-work schemes (for example, Hashcash) allow new blocks to be added to the chain without the need for a centralized trusted authority (DiNizo, 2018). Blockchain technology has rapidly evolved, particularly in the financial technology domain, and is revolutionizing traditional business processes. It gained widespread attention as the underlying technology for Bitcoin and other cryptocurrencies, introducing a novel foundation for conducting transactions globally. Essentially, a blockchain is a continuously growing, immutable, and distributed database that functions as a decentralized system secured by the longest chain of blocks.

Through strong encryption, blockchain allows users to verify transactions without disclosing personal details. It also eliminates the need for intermediaries, which reduces transaction costs and processing delays. In addition, all recorded transactions on a blockchain are permanent and tamper-proof. With these features, blockchain is poised to drive a new wave of industrial and economic transformation by enabling direct, secure peer-to-peer transactions on a global scale. Underpinning these capabilities are several core design principles of blockchain,

namely computational logic, distributed databases, pseudonymous transparency, irreversibility of records, and peer-to-peer transmission.

Beyond these technical features, researchers have proposed frameworks to harness blockchain for improving trust and governance in online platforms. For example, one such approach — the *Backfeed* framework — demonstrates how blockchain's key elements can support collaborative content creation and value distribution in digital communities (Alkhudary, Brusset and Fenies, 2020). More broadly, decentralizing social media via blockchain is seen as a promising strategy to mitigate issues of privacy breaches, fake news, and censorship. Blockchain is already one of the most prominent decentralization technologies and is being explored as the backbone of next-generation social networking platforms (Guidi and Michienzi, 2021). By leveraging blockchain's tamper-resistant distributed ledger to store critical information, these platforms make it virtually impossible for unauthorized parties to alter or falsify data.

LITERATURE REVIEW

Enhancing security in online social networks (OSNs), which support diverse modes of knowledge sharing, news dissemination, and business transactions, is an area where blockchain technology (BT) plays a pivotal role. The literature demonstrates that advanced BT-based techniques can effectively secure public domains.

Saad *et al.* (2019) introduced BT as a novel approach to mitigating the spread of fake news on social media. They argued that numerous news sources can be manipulated by users and that BT's prototype design can prevent fake news propagation. Building upon this work, the present study integrates *bloXRoute* and keyed-watermarking to improve network scalability and detect media tampering. This also broadens the scope to include cases where regular social media users act as content generators—scenarios not considered in the original work.

Collins *et al.* (2021) classified fake news into categories such as propaganda, clickbait, parody, hoaxes, and satire, along with forms like journalistic fraud and identity theft. Similarly, Medeiros and Braga (2020) proposed a classification that includes hoaxes, conspiracy theories, biased news, satire, and rumours. The complexity of accurately identifying these categories is compounded by the nuances of human language; for instance, satire and parody often rely on sarcasm and humour, which must be accounted for in algorithmic analysis. The prevalence of misinformation on social media has attracted increasing research attention toward developing secure mechanisms for its detection (Birunda and Devi, 2021). Jiang *et al.* (2021) supported Aslam *et al.*'s earlier observation that automated, machine-driven methods are essential for effectively tackling fake news detection.

Peng *et al.* (2021) investigated privacy risks in blockchain applications, surveying multiple privacy-protection methods such as non-interactive zero-knowledge proofs and their combinations. They also examined blockchain-based platforms designed to preserve privacy in smart contracts. Casino *et al.* (2019) described *Hashcash* as a trusted method for adding blocks to a chain without a third party. They highlighted blockchain's rapid adoption in fintech and its role in revolutionising business transactions. Blockchain's core attributes—immutability, completeness, and decentralisation—ensure robust security through its longest-chain consensus.

Blockchain's intrinsic design features include transparency, adaptability, security, and resilience. It can be conceptualised as a distributed database composed of block sequences, where committed blocks are immutable. This characteristic is especially beneficial in banking, where collaborative blockchain systems can enhance customer transaction speed while maintaining transparency (Ante, 2021).

Steemit, a blockchain-based social media platform, exemplifies decentralisation by building communities and rewarding users with cryptocurrency for positively evaluated content (Bhattacharya *et al.*, 2021). It offers curated news, personalised responses, and a stable cryptocurrency pegged to the US dollar.

To standardise the reporting of systematic reviews, Page *et al.* (2021) developed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, which define methodologies and terminology in recent research. In the context of fake news detection, *Fakechain* data mining algorithms have been employed to authenticate social media content.

Ethereum—a decentralised platform—facilitates smart contracts that efficiently execute, verify, or enforce agreements on the blockchain. Smart contracts combine predefined conditions with promises: once the conditions are met, the system automatically executes the agreement. Paul *et al.* (2019) demonstrated that integrating the Breadth-First Search (BFS) algorithm with Ethereum blockchain can enhance fake news detection capabilities.

RESEARCH METHODOLOGY

In blockchain technology (BT) mapping for security in a big data environment, each node represents a keyword, and each connection indicates the co-occurrence of two words. The weight of the relationship between each pair indicates the frequency with which these terms occur together in online social networks (OSNs). As a result, a co-occurrence network accurately depicts a domain's cumulative knowledge in context, as represented through the weight and patterns of relationships among keywords in socialmedia.

One commonly used cryptocurrency wallet for interacting with the Ethereum blockchain is MetaMask. With MetaMask, each user is provided with a unique Ethereum address, enabling them to send and receive Ethereum. This wallet also facilitates interactions with decentralised applications created on the Ethereum blockchain.

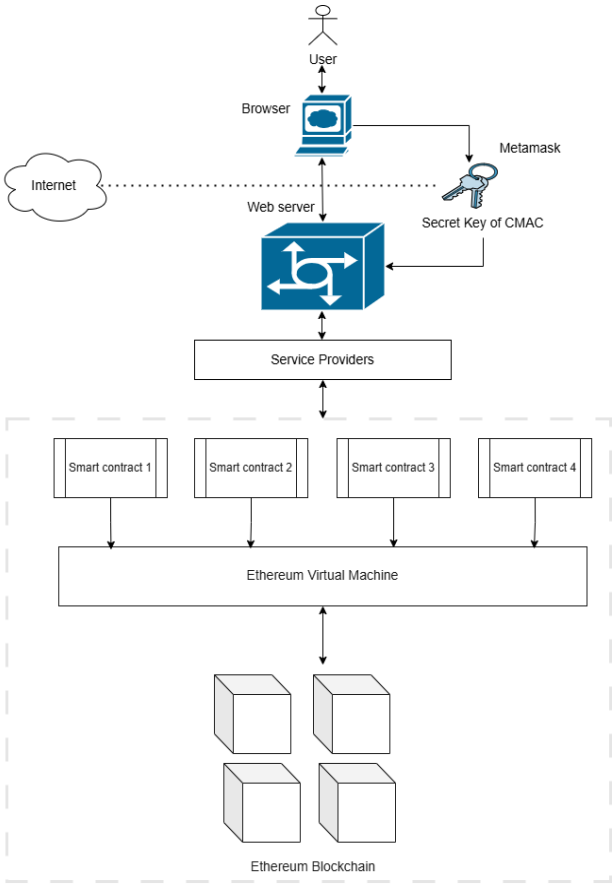

Figure 1 Architecture of EVM-CMAC bockchain model for detecting fake news in SM

Figure 1 illustrates the EVM-CMAC blockchain design, which can identify and address system issues when necessary. An advantage of BT is its traceability. Each user entering the blockchain network is assigned a unique identity linked to their respective account. Security in BT is ensured by a reliable cryptographic hash chain. Once a new block is created, its hash value is computed; the previous hash value becomes the default for the new block. Typically, the hash contains the block type, block ID number, previous hash value, block creation time, user ID number, miner level, and the Merkle root, which includes transaction data and respective hashes.

Working of EVM blockchain mechanism in SM

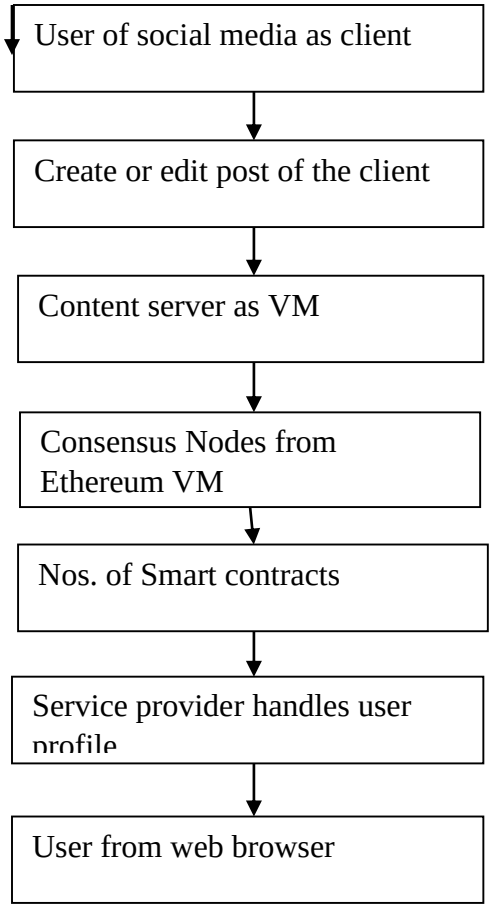

Figure 2 work flow of the Ethereum Virtual Machine EVM Blockchain

The EVM blockchain mechanism in SM involves the following components:

• User Client: The user-facing interface, such as a mobile or web application, allowing users to post, comment, like, and follow content.
• Service Provider: Manages user data, preferences, connections, and profiles, storing them in a decentralised manner to ensure privacy and ownership.
• Blockchain: The core decentralised ledger storing transaction and content server data, ensuring immutability, security, and transparency.
• Content Servers: Store and distribute various content types (posts, photos, videos), ensuring accessibility and efficient retrieval.
• Consensus Nodes: Network participants verifying transactions, adding blocks, and maintaining blockchain integrity via Proof of Stake (PoS) or Proof of Work (PoW) algorithms.
• Smart Contracts: Autonomous blockchain-based programs defining platform rules and automating tasks such as verification, incentives, and content moderation.

This architecture leverages blockchain capabilities to enhance security, data integrity, and user control while maintaining a transparent and decentralised environment.

Ethereum blockchain using CMAC authentication

Data storage in the BT has been enhanced with Ethereum blockchain mechanism whereas the smart contracts provided several benefits namely security, transparency and privacy. Usage of smart contract has capable in creating decentralized system that exclude the requirement for service provider. Hence, the data breaches reduce risk as well as unauthorized accessing. Thus, the proposed EVM based CMAC algorithm mechanism is shown in figure 3. The proposed design flow use the fact that CMAC is cipher-based authentication is used for the implementation of authentication. Therefore, the CMAC algorithm has been altered for utilizing in counter mode to provide the data encryption inclusive of data authentication for providing advanced encryption.

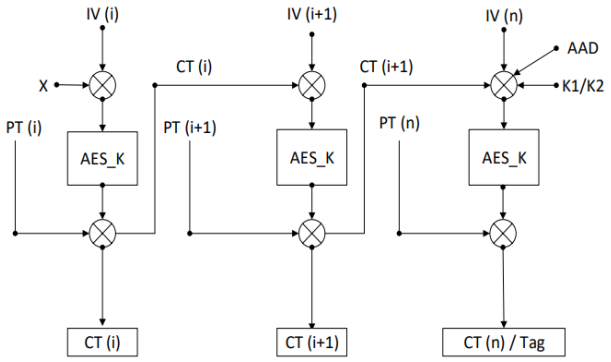

Figure 3 CMAC for authentication

Algorithm for CMAC

Input: Authenticated Message (AM), Secret key (K), Block size of the cipher (n)
Output: Authentication tag (T)

- **Step 1:** If message length < n bytes, append '1' bit and pad with '0' bits to reach n bytes. If equal to n bytes, append '1' bit and pad with '0' bits
- **Step 2:** Divide the padded message into n-byte blocks. Pad the final block with '0' bits if required.
- **Step 3:** Generate subkeys K1 and K2 by encrypting an all-zero block with the secret key using the MAC cipher.
- **Step 4:** Set the initial MAC value M0 as an all-zero block.
- **Step 5:** For each block Mi, XOR it with the previous MAC value Mi-1, then encrypt using the secret key to produce a new MAC value.
- **Step 6:** For the last block, XOR with K1 if complete, or with K2 if incomplete, then encrypt to produce the final tag T.

By integrating CMAC encryption into the Ethereum blockchain, the proposed model ensures secure content server protection and robust authentication between the service provider and user client in SM environments.

RESULT AND DISCUSSION

This section presents potential scenarios for applying blockchain technology (BT) to authenticate social media (SM) pages. The authentication process begins with the creation of a block containing all personal details, and concludes with the generation of a hash code and trust logo displayed on the user's account. The procedure is straightforward: a block is generated and linked to the account, enabling the immediate acquisition of the trust logo without delays. There is no possibility of rejecting the application for the trust logo unless personal data in the block is altered or the same hash code is reused across multiple accounts. If a hash code is detected on multiple accounts, the remaining blockchain nodes reject the action and flag it as a violation, thereby helping followers identify fraudulent accounts and raising awareness of fake pages.

The proposed Ethereum Virtual Machine–Cipher-based Message Authentication Code (EVM-CMAC) model demonstrates superior performance in detecting fake news on SM. Performance evaluation was conducted using cryptographic metrics such as network throughput and encryption execution time. Simulations were implemented in C++ (Visual Studio 2019), with network nodes distributed in a circular area of 2000 metres radius. The EVM-CMAC blockchain model was compared with EVM blockchain and EVM-Hash blockchain models. Simulation parameters were optimised with k and M values set to 3 and 4, respectively. Cooperative transmission was permitted only when the maximum data rate of direct transmission from source to destination was below 2 Mbps, and the link distance was limited to 67.1–100 m. IEEE 802.11b standard settings were used for RTS, CTS, and ACK, with the HTS value matching CTS and ACK parameters in different CMAC protocol scenarios.

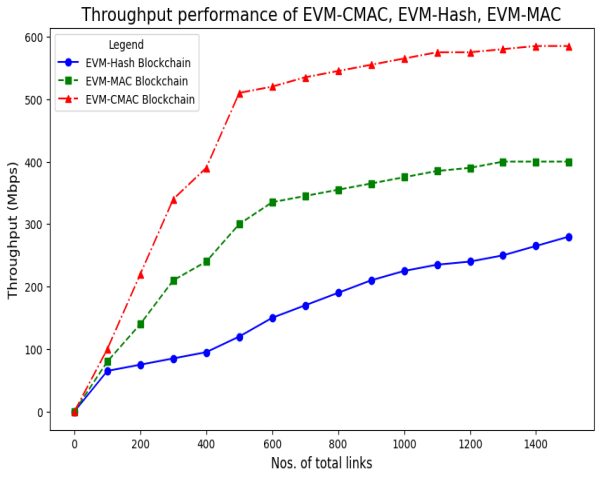

Figure 4 Comparison of throughput performance of EVM-CMAC, EVM-MAC and EVM-Hash

As shown in Figure 4, network throughput varies with the total number of links

in the network across different link distances. Throughput is defined as the total data packet time delivered over successful links and the total number of successful links. Given a specific link distance, effective throughput increases as the number of links grows, eventually reaching saturation when the network is dense. The EVM-CMAC model consistently demonstrates higher throughput compared with the EVM-MAC and EVM-Hash blockchain models, indicating improved data transmission efficiency between nodes.

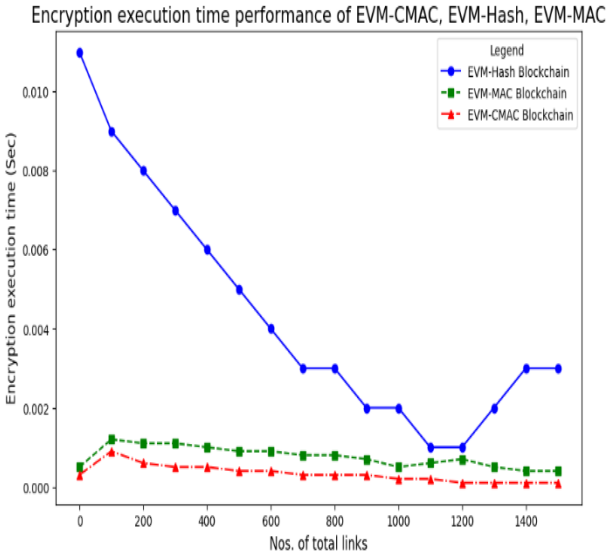

Figure 5 Comparison of encryption execution time performance of EVM-CMAC, EVM-MAC and EVM-Hash

Figure 5 compares encryption execution times for the three models. The EVM-CMAC model achieves better execution time performance than EVM-MAC and EVM-Hash. As the number of links increases, encryption execution time initially rises until around 100 links, after which it decreases. Overall, the EVM-CMAC model offers superior encryption efficiency, contributing to more effective fake news detection in SM environments.

CONCLUSION

Fake news has been identified by cryptography model developed on top of BT whereas the proposed model incorporates cipher based cryptography method that determined in current systems. Based on this research, the simplest way to process an application is to use a customized blockchain using ethereum. The system's framework is in place, but it need to be implemented. Using BT empowered by Ethereum smart contracts offers various benefits for storing data. This proposed EVM-CMAC blockchain has better security and detection of fake news in SM BY its decentralized and secure nature for storing and managing information in OSNs. Employing smart contracts reduces the requirement for intermediaries, lowering the possibility of data breaches as well as unauthorized access. Furthermore, the adoption of EVM-CMAC increases security. As a result, creating system will give an effective and secure method for storing and retrieving data.

REFERENCE

Alkhudary, R. , X. Brusset, and P. Fenies. (2020). "Blockchain in general management and economics: a systematic literature review," Eur. Bus. Rev., vol. 32, no. 4, pp. 765–783, 2020, doi: 10.1108/EBR-11-2019-0297.

Almeida, L. , Fuzaro, V. Nieto, F., & Santana, A.L.M. (2021). Identificação de "Fake News" no contexto político brasileiro: uma abordagem computacional. In: Proceedings Workshop sobre as Implicações da Computação na Sociedade (WICS), Porto Alegre, Brasil, pp. 78-89.

Ante, L. . (2021). "Smart contracts on the blockchain – A bibliometric analysis and review," Telemat. Informatics, vol. 57, no. 10, pp. 1–48.

Bhattacharya, R. ; White, M.; Beloff, N. (2021). An Exploration of Blockchain in Social Networking Applications. In Proceedings of the Intelligent Computing; Springer International

Publishing: Cham, Switzerland, pp. 858–868. [CrossRef]

Birunda, S. , & Devi, R.K. (2021). A Novel Score-Based Multi-Source Fake News Detection using Gradient Boosting Algorithm. Proceedings of International Conference on Ar-tificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, pp. 406–414.

Biswas, R. , N. Vyas, and M. Baskar. (2021). "Sentiment Analysis on National Education Policy Change 2020," Turkish Journal of Computer and Mathematics Education, vol. 12, no. 11, pp. 1480–1488.

Casino, F. , T. K. Dasaklis, and C. Patsakis. (2019). "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics and Informatics, vol. 36. Elsevier Ltd, pp. 55–81.

Celliers, M. and M. Hattingh. (2020). A Systematic Review on Fake News Themes Reported in Literature, vol. 12067, Springer International Publishing, LNCS.

Chang, V. , P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami. (2020) "How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees Victor".

Collins, B. , Hoang, D.T., Nguyen, N.T., & Hwang, D. (2021). Trends in combating fake news on social media–a survey. Journal of Information and Telecommunication, 5,2:247-266.

DiNizo, A. , "From Alice to Bob: The Patent Eligibility of Blockchain in a Post-CLS Bank World," J. Law, Technol. Internet, vol. 9, no. 1, Jan. 2018, Accessed: Jun. 26, 2021. [Online].

Duda-Chodak, A. , Lukasiewicz, M., Zięć, G., Florkiewicz, A. & Filipiak-Florkiewicz, A. (2020). COVID-19 pandemic and food: present knowledge, risks, consumers fears and safety. Trends Food Sci. Technol. 105, 145–160.

Guidi, B. ; Michienzi, A. (2021), The Decentralization of Social Media through the Blockchain Technology. In Proceedings of the 13th ACM Web Science Conference 2021, Virtual Event, 21–25 June 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 138–139.

Ozdemir, I, A. . I. M. Ar, and I. Erol. (2020). "Assessment of blockchain applications in travel and tourism industry," Qual. Quant., vol. 54, no. 5–6, pp. 1549–1563. doi: 10.1007/s11135-019-00901-w.

Islam, M. , Liu, S., Wang, X., & Xu, G. (2020). Deep learn-ing for misinformation detection on online social networks: a survey and new perspectives. Social Network Analysis and Mining, 10,1:1-20.

Jiang, T. , Li, J.P., Haq, A.U., Saboor, A. & Ali, A. (2021). A novel stacking approach for accurate detection of fake news. IEEE Access, 9:22626-22639.

Medeiros, H. , & Braga, R. B. (2020). Fake News detection in social media: a systematic review. Proceedings 16th Simpó-sio Brasileiro de Sistemas de Informação (SBSI), Porto Ale-gre, Brasil, pp. 1-8.

Page, M. ; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ 2021, 372, 89.

Paul, S. & Joy, Jubair & Sarker, Shaila & Shakib, Abdullah & Ahmed, Sharif & Das, Amit. (2019). Fake News Detection in Social Media using Blockchain. 1-5. 10.1109/ICSCC.2019.8843597.

Peng, L. , W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu. (2021). "Privacy preservation in permissionless blockchain: A survey," Digital Communications and Networks, vol. 7, no. 3, pp. 295–307.

Saad, M. , A. Ahmad, and A. Mohaisen. (2019). "Fighting fake news propagation with blockchains," in 2019 IEEE Conference on Communications and Network Security (CNS), 2019, pp. 1–4.

Szczepański, M., Pawlicki, M., Kozik, R. & Choraś, M. (2021). New explainability method for BERT-based model in fake news detection. Sci. Rep. 11, 23705.

Zhang, X. & Ghorbani, A. A. (2020). An overview of online fake news: characterization, detection, and discussion. Inf. Process. Manag. 57, 102025.