Premkumar R, 2022, 10:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology

An Open Access Journal

Blockchain-Based Approach for Detecting Fake News on Social Media Platforms to Ensure Transparency, Credibility, and Secure Information Verification

Premkumar R, Samyuktha J, Jeevitha J, Birundha A
Department of Computer Science and Engineering
Kongunadu College of Engineering and Technology, Tamilnadu, India

Abstract- Detecting fake news as well as recognizing reliable sources of information has become a major issue of conversation inside the news industry and on social media. In the digital age, anybody may create or modify digital content with ease, then post it on social media platforms. These social networking sites facilitate contact in modern times, but they have also created novel challenges regarding their practical use, such as the fraudulent dissemination of deceptive or faux data by contagious channels. This research proposes a primitive blockchain and watermarking-based social media infrastructure to curb the spread of false information. We propose a novel blockchain paradigm to address current issues in this area. Furthermore, by identifying the source of the false information on social media, the innovative approach can aid in slowing its dissemination. Our test findings show our based on the blockchain approach is capable of sending documents instantly over a bloXroute server, which can spread data up to 100 times quicker than traditional solutions.

Keywords- electronic watermarking, distributed networks, overlay networks, scalable blockchain, and fake news

I. INTRODUCTION

Whenever information originates from outlets for news, print media, or digital platforms, its accuracy always has an impact on society. Through social networking sites, television, and other media for the internet, millions of individuals often soak up data that is represented as reliable but lacks valid proof or data. Fake news is the term used when referring to this kind of misinformation. False information shared on social networking sites has a huge impact and has the capacity to destabilize the economy in a matter of hours for millions of users. Propagation of such fake news has the ability to alter election outcomes, incite hatred in the public, influence voting trends, impact stock values, and much more. The greatest tragedy is that it might be challenging to pinpoint the genesis of the disinformation along with come to it from spreading once it goes viral. As a result of improper inquiry into references for verification of regular individuals generally had lost dependence on media organizations, and sometimes also in news . Many types of digital content are being released these days, including blogs, films, pictures, and more. Without doing any fact-checking, anyone can freely publish any type of data on popular social media platforms like Facebook, Instagram, LinkedIn, and Twitter.

People are easily swayed by such fake news and may modify their opinions about the topic, which may include a particular group, socioeconomic patterns, religion, or individual. The impact of counterfeit information is so substantial that it may ruin the credibility of anyone, whether they are well-known or just regular people. It becomes sense to use a central authority that can oversee such digital content and control the flow of details in order to lessen these issues. However, the trust model and privacy of dispersed networks of people are destroyed by the use of such authoritative bodies. Blockchain technology's distributed and modular character [1] has led the research community to firmly think that this technology is appropriate for a number of fields outside finance, encompassing digital right management approaches [7], hospital [4], [5], logistical networks [6], and electronic voting [2], [3]. This study proposes an interpersonal building structure based on watermarking in order and blockchain technology. Our system's capacity to identify the source of false information will aid in halting its spread on social media platforms. Every news item submitted or published on the suggested social networking site is stored on the blockchain in the suggested framework as a transaction completed by registered users. Since blockchain technology is open as well as traceable, it is achievable that one verify the legitimate source of any data distributed on such a platform.

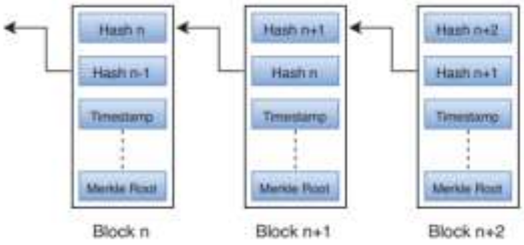

Fig. 1: Basic Blockchain Structure

Timestamping and the chain connection between blocks in blockchain technology make it possible to track the news source. Tracing news items backwards step-by-step is important to determine which user created or deliberately impacts the news in order to determine the breaking news path shared by participants on such internet platforms. A blockchain's block headers include a wealth of data, including timestamps, a new block hash, and the pre-block hashed value. Data tracing may be aided by these block headers. Every exchange that a user uploads to a social media site can be recorded on the blockchain, and each time another person shares or tries to edit the material, a traceable record is created. Timestamps allow anyone to determine the order of these transactions that are recorded in the blockchain.

Scaling of the system is the main obstacles of blockchain technology [8]. Since the first day, scalability has been a key focus for the blockchain research community and is one of the most important issues in the technology. But in the suggested paradigm, we use bloXroute for greater the capacity of networks [9].

We utilize digital watermarking to verify whether the news has been tampered with after the origin has been identified.

1. Associated Work

A strategy for evaluating and identifying false news sources was put forth by Jang et al. [10]. The authors looked into the origins and dissemination of bogus news on social media. The framework analyzes bogus news across the internet system using a dynamic forest modeling strategy. The recommended method has recognized the antecedent tweets and the source of those tweets. The authors also noted how bogus and true news were evaluated. The findings demonstrated that despite bogus news underwent numerous content revisions, genuine news moved swiftly and extensively throughout the network.

Qayyum and collaborators just published a few papers on the topic of applying ethereum to stop propagation of lies [11]. The authors of this study address propagation of false information by employing a smart contract-based blockchain in conjunction with deep learning, also known as DL, and machine learning (ML). In order to stop propagation of false information, they also brought attention to the problems with particular designs led upon the blockchain relies the system. Other studies in the same field of cryptocurrencies with false news study include [12]–[20]. A prototype for demonstrating the provenance of digital media that has been captured was presented by Huckle et al. [21]. The authors suggested a technological fix for the issue of verifying the reliability of media sources used in false information.

Blockchain technology was introduced by Sheikh et al. [22], for instance as an innovative way to stop the spread of false information via social media networks. The writers of the article taking look at the printed word as an interpreter of new that users on social networks might thereafter alter by sharing these news items. Their prototype work has the potential to stop fake news from spreading on social media.

In order to remedy the primary shortcomings in current systems, the scheme put forward within this piece truly travels not clear to a Samuel et al a position by integrating bloXRoute for network flexibility and keyed-watermarking for finding any of the tampering with the initial medium (as identified in the next section). Additionally, the scope has been expanded to include situations that involve everyday users of a web-based platform could produce journalism or content; this particular scenario wasn't addressed in the aforementioned paper.

Current System Drawbacks

- The most difficult aspect of social media networking is identifying the information's original source. It is difficult to find the perpetrator of fake news once it has gone viral.
- Blockchain may be able to track the history of these kinds of business transactions, but social networks cannot use it due to its scalability, which presents another significant problem.
- Once the news's source is identified, it can be challenging to pinpoint the primary offender. if the information proprietor added the breaking news in the first case or if someone else edited it.

II. OUR SYSTEM

1. Establishing a Distributed Distributed Ledger (BDN) Wholly Flexible and Unsecured

The system aims to address the network scalability issue in order to increase the system's throughput. It is necessary that there be a fast internet so that the bricks can spread quickly over the internet and verification of the blocks doesn't take longer. The amount of data transferred will eventually rise as a result of the entire method on boosting network scalability. Distributed high-capacity bloXroute routers are used in our system. The bloXroute addresses the system tier scaling constraint by utilizing a blockchain-based distributed server idea. They suggest a blockchain distributed network, which is an international collection of servers designed to transmit blockchain data rapidly. These BDN servers make advantage of advanced networks technology and over collecting a transmission if the information, an bloXroute client rapidly announces it to everyone else of the network, enabling up to 100 times quicker data propagation. Ledger scaling challenges are handled by the bloXroute server that is which reduces the network bottleneck.There are two kinds of networks that make up the entire system:

- BloXroute servers are high-capacity, low-latency servers designed to swiftly distribute transactions as well as blocks across several blockchain systems.They function similarly to cluster servers that are linked to other clusters. These bloXroute servers reduce latency and bandwidth costs. Keep in mind that these servers oversee similar tiny networks without serve as a central server. BloXroute servers were introduced with the intention of accelerating block propagation.
- Peer networks, and networks of peers which consist by computers or mobile nodes, use bloXroute servers to send blocks and transactions while also monitoring bloXroute's operations. A particular consensus technique is used by these peer networks.Each cluster many these chains is composed of only one network computer and broadcasts transactions as well as blocks for a group many tiny node known as others.

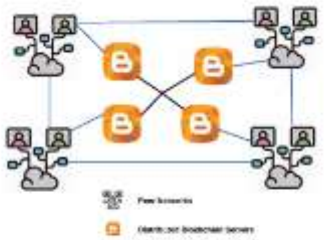

Fig. 2: Distributed bloXroute Servers Connected With Peer Networks.

After being encrypted, the blocks from various peers are sent to the bloXroute servers so they can spread across networks. Additionally, peers have the option of sending these encrypted blocks to bloXroute rs either individually or via other peer nodes. These two characteristics prevent the servers from being biased or deceiving certain nodes. When blocks reach their destination, the key is disclosed by the bloXroute servers, which operate blindly without knowing the content of the blocks. Because of these bloXroute servers' extremely speedy dissemination speeds, internet blocks are swiftly sent to other networks for verification.

2. Consensus Algorithm

Numerous consensus techniques, such as Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA), are used in blockchain. Every protocol has pros and cons entirely particular. Nevertheless, these protocols have a limited bandwidth and cannot be scalable. Consequently, it is not practical to use those consensual approaches in this system. However, methods built around Byzantine Fault Tolerance (BFT) have a high throughput with have poor scaling of networks. As a result, pBFT has very high networking efficiency requirements. But in our situation, we used bloXroute servers to boost network scalability, therefore this consensus technique works well for us.Only authorized nodes are able to take part in the consensus process on our private blockchain, which is permissioned. Nodes that are nameless are unable to validate transactions or obtain mining rewards. As a result, our system has not any mining costs.

3. Using Blockchains to Stop the Spread of False Information

The model uses a website that is comparable to Facebook, Twitter, companies that use blockchain networks, such as LinkedIn. Any individual of press institution may create a blockchain profile platform. Nevertheless, each user must authenticate themselves on the blockchain with a national identification card, number or credentials for the media. An additional technique that could be utilized is through a recognized digital signature using a national identification card. These details are concealed from the masses. But the blockchain-powered Information is able to checked at any moment by the platform. It should be noted that the suggested methodology focuses on determining the news source and validating the disinformation based on user reports on social media platforms as opposed to detect misleading data using autonomous ML (machine learning) techniques. It has multiple types of transaction flows:.

Any registered user is allowed to share digital news content on the social networking platform. Prior to sharing, the user must specify the type of content being shared, indicating whether it is news or personal. If the content is classified as news, its privacy setting will be public, allowing anyone to report it as either fake or real among registered users. During this uncertainty, where the news is being assessed for authenticity, it will be marked with an orange sign. Once the members of the blockchain confirm the accuracy of the news, it will be marked with a green check if it is real and a red cross if it is fake.

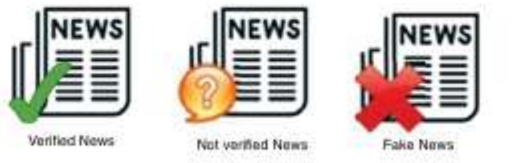

Fig. 3: News Verification

Please note that we are utilizing a private permissioned blockchain, which means that only authorized users can verify it. The transactions include timestamps indicating the individuals who previously shared this information, along with the original source of the content.

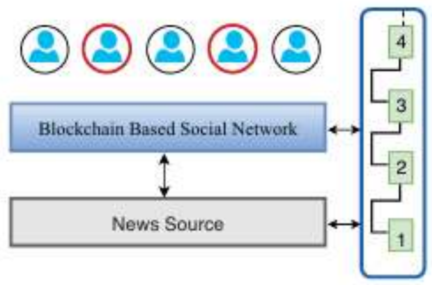

Fig. 4: Transactions chain for sharing of news

When a user generates news, details such as user ID, hash value, and timestamps are recorded as a transaction on the blockchain. If another user shares the same post, the blockchain logs this new transaction with additional information, making it traceable within the blockchain based on the transaction's internal information. If a user changes the content of the post and shares it, the blockchain records this modification transaction as well, making it straightforward to identify who altered the content. In Figure 4, some users are highlighted in red to show those who changed the content.

Contributing Digital News to the Blockchain-Based Platform: Users are permitted to upload digital news materials; however, they must indicate whether the data pertains to news or personal information. If the content is classified as news, the transaction is recorded on the blockchain, and our social networking site automatically applies a keyed digital watermark to the material to prevent alteration of digital content. Given the availability of numerous advanced multimedia editing tools, a vast number of manipulated images, videos, audio clips, and news articles circulate on social media, aimed at altering public perception on specific topics. Hence, it is essential to maintain the integrity of such multimedia content.

Watermarking and digital signatures are the most effective tools for ensuring data integrity in digital formats. Digital watermarking is employed for verifying the authenticity of documents, audio, and video content, while digital signatures are utilized for the authentication of documents and images. In the digital signature process, Algorithm 1 computes the hash value of the digital content, allowing the hash value to be used for signature verification at the recipient's end. However, since hash values are unique, any alteration of even a single bit in the input will result in a completely different output from the hash function. Thus, a digital signature can be effective in identifying any changes made to the digital content. In certain cases, modifications may be necessary; for instance, data may be compressed when it is uploaded to various platforms. For example, YouTube provides users with options to view videos in different qualities based on their internet speed. Similarly, data shared on social media often undergo resizing for reduced file size, which can be done for creative purposes as well. Such lossy compressions are part of our model, making digital signatures unsuitable for our specific authentication needs. In our case, the social network compresses data prior to uploading it to servers, so keyed watermarking presents a more suitable method for confirming data integrity. Below is a basic illustration of keyed watermarking (Algorithm 1) applied to image media, and analogous implementations of the proposed platform can establish keyed watermarking for all media types. Additionally, there are two watermarking schemes that may be utilized: invisible watermarking and robust watermarking. Invisible Watermarking is utilized in situations where the level of embedding is too minimal to be detected or noticed, while the Robust Watermarking algorithm is employed to protect digital media content from specific types of transformations, such as image or video manipulation and tampering. It is commonly used for ownership protection. The Robust watermarking algorithm is capable of withstanding not only general operations like compression, noise addition, and filtering, but also geometric attacks such as rotation, scaling, translation, and shearing.

An input image with dimensions of m×n pixels is represented as im(x, y), where x = {0,...,m} indicates the row and y = {0,...,n} indicates the column. We define the functions p(a) and p(b) in the following manner:

$$p(a) = \begin{cases} \frac{1}{\sqrt{m}}, & if\ a = 0 \\ \frac{2}{\sqrt{m}}, & otherwise \end{cases} \text{ and } p(b) = \begin{cases} \frac{1}{\sqrt{n}}, & if\ b = 0 \\ \frac{2}{\sqrt{n}}, & otherwise \end{cases} \quad (1)$$

Algorithm 1 Watermark Embedding

Input: Image, Watermark Output: Watermarked Image

Load the image referred to as Host and transform it into a grayscale format.

- RGB = imread('Host.jpg')
- greyscale-host = rgb2gray(RGB)

Load the encrypted watermark image titled WM, apply the key, and convert it into a binary format.

- watermark = imread('WM.jpg')
- greyscale-wm = rgb2gray(watermark)
- 2d-dct+dwt-coeff-wm = dct2(greyscale-wm)
- 2d-dct+dwt-coeff-WM-keyed = applyKey(2d-dct-coeff-wm, key)
- greyscale-wm-keyed = idct(2d-dct-coeff-WM-keyed)
- binary-wm = im2bw(greyscale-wm-keyed)

Calculate the 2-D DCT-DWT coefficients for the input image.

2d-dct+dwt-coeff-host = dct+dwt2(greyscale-host)

Segment the input image into 8 × 8 blocks and embed the watermark into the first bit of each block.

Merge the blocks back into a single image and compute the inverse DCT-DWT.

Present the Watermarked image.

For the functions p(a) and p(b) defined in (1), the two-dimensional discrete cosine transformation, or DCT, of the image im(x, y) is expressed as

The inverse of the discrete cosine transformation, also known as IDCT, is expressed as follows.

Watermark encryption: In our proposed framework, a watermark image is consistently encrypted prior to being embedded into the original media, which can be any type of digital content. This encryption method proves essential in scenarios where an attacker successfully extracts the watermark from the content. Due to the encryption of the watermark, the attacker will be unable to retrieve the original watermark image. To encrypt the digital media, a lightweight encryption algorithm is employed. Numerous lightweight encryption algorithms have been proposed and showcased in various competitions aimed at encryption algorithms [23], [24], yet many of them are insecure as they have been compromised by specific cryptanalysis techniques. Nevertheless, the ARX family cipher—a lightweight encryption algorithm referenced from [25]—remains secure.fully vulnerable for the complete number of rounds. The ARX family cipher utilizes three basic operations: bitwise rotation, modular addition, and exclusive-OR. As a result, this cipher is ideal for operation on devices with limited capacity. Thus, we employ the ARX family cipher to protect the content from potential attacks. It is resilient against various forms of attack (refer to [26], [27]) for the entire number of rounds.

III. INVESTIGATIVE ANALYSIS

The DCT and DWT algorithms (see Figure 5) are used to insert the watermark into the provided image. We utilized the MATLAB platform to conduct the experiment. The embedding code can be found at github1

We performed encryption (see Figure 6) using a number of minimal cryptography in order to analyze the encryption time appropriate for IoT devices, and we discovered that SPECK is appropriate for our platform. Due to their limited resources, these IoT devices are unable to employ complex ciphers. The US National Security Agency created the SPECK cipher in 2013.Each cipher's encryption algorithm code is readily accessible on the official Github webpages.

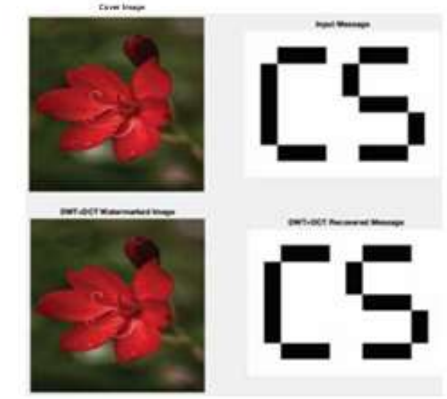

Fig.5: Watermark embedding using DWT and DCT.

To assess both transparency and robustness, bit error is used to assess transparency, while peak signal to noise ratio (PSNR) is used to assess robustness. The discrete cosine transform (DCT) sequence of a block is DCTL, where L = 1, 2, 3,..,63. We choose L=3,4,..,16 in Figure 7.

In order to assess the transparency of the watermark image, we compute the PSNR using the following formula formula:

$$\text{PSNR}=10\log_{10}\left(\frac{(V-1)^2}{MSE}\right)\text{ decibel,} \qquad (2)$$

where MSE is defined as the mean squared error and V−1 is the original image's maximal pixel value.

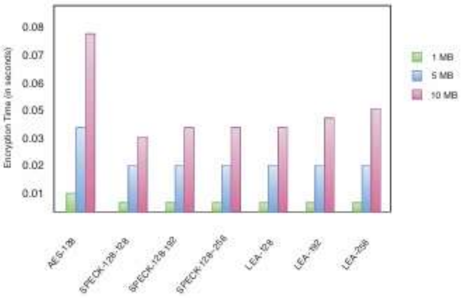

Fig.6: Comparison of encryption time (seconds).

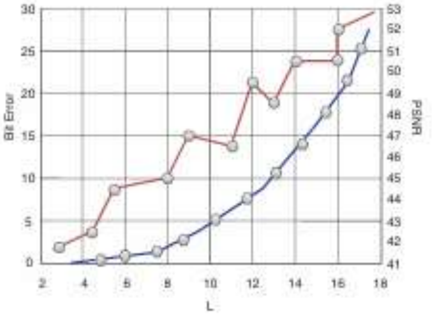

Fig.7: Relationship between DL, PSNR and Biterror

where Wim is the recovered watermark image and Wim is the primary watermark image.

In order to assess the degree of similarity between the original and extracted watermark picture, we use the following formula for computing the Normalized Cross Correlation (NCC):

We used the 21KB JPG image with the name "HOST" for the experiment. We utilize the 1KB bmp image called "WM" for the encrypted watermark image. As for the watermarked image, its NCC is 0.0039 and its PSNR is 44.8887 dB.

IV. CONCLUSION

In this paper, we propose a new community management platform based on blockchain technology to address the growing issue of fake news. Fast throughput, security, and development are characteristics that distinguish our designed solution. Durability is an obstacle for most blockchain systems. We employ bloXroute routers alongside with the Blockchain Decentralized Network (BDN) to solve our scaling problem, which significantly increases scalability in our situation. By using cutting-edge network techniques, these BDN servers may disseminate data as much as 100 times more quickly. Once a bloXroute server gets a packet of info, it quickly streams it to everyone else of the network. By selecting mid-frequency coefficients that directly impact the transparency and durability of the watermarking, we also conducted an engraving test using MATLAB. We subsequently embedded the logo with a picture using both DCT and DWT algorithms and presented a relationship diagram for PSNR and bit-error. Consequently, our platform addresses the main shortcomings of present ones by utilizing proposed adaptable blockchain distributed network and keyed-watermarking schemes. It has also been determined to be perfect for knowing the source of trolling on based on blockchain technology social websites and to which may assist with reducing the propagation of counterfeit information. Every cryptocurrency community and IoT-based system can adapt its rules to our web by fixing their network's bottleneck problem. We conducted a lightweight cypher cryptography experiment and selected the best effective cypher based on encoding time and protection margin. Therefore, because we have chosen a lightweight, effective encryption skills, the recommended configuration is appropriate for platforms with limited resources.

Funding
The Danish Ministry of Education and Science, Digital Pilot Hub, and Skylab Digital are providing funding for Rajani Singh's work. Dr. Gautam Srivastava of the Natural Sciences and Engineering Research Council of Canada provided some funding for this study.

REFERENCES

1. G. Srivastava, S. Dhar, A. D. Dwivedi, and J. Crichigno, "Blockchain education," in 2019 IEEE Canadian Conference of Electrical and Computer Engineering, CCECE 2019, Edmonton, AB, Canada, May 5-8, 2019. IEEE, 2019, pp. 1–5. [Online]. Available: https://doi.org/10.1109/CCECE.2019.8861828J.
2. G. Srivastava, A. D. Dwivedi, and R. Singh, "PHANTOM protocol as the new crypto-democracy," in Computer Information Systems and Industrial Management- 17th International Conference, CISIM 2018, Olomouc, Czech Republic, September 27-29, 2018, Proceedings, ser. Lecture Notes in Computer Science, K. Saeed and W. Homenda, Eds., vol. 11127. Springer, 2018, pp. 499–509. [Online]. Available: https://doi.org/10.1007/978-3-319-99954-8 41K. Elissa, "Title of paper if known," unpublished.
3. G. Srivastava., A. D. Dwivedi, and R. Singh., "Crypto-democracy: A decentralized voting scheme using blockchain technology," in Pro ceedings of the 15th International Joint Conference on e-Business and Telecommunications- Volume 2 SECRYPT: SECRYPT,, INSTICC. SciTePress, 2018, pp. 508–513.
4. G. Srivastava, A. D. Dwivedi, and R. Singh, "Automated remote patient monitoring: Data sharing and privacy using blockchain," CoRR, vol. abs/1811.03417, 2018. [Online]. Available: http://arxiv.org/abs/1811.03417.
5. A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," Sensors, vol. 19, no. 2, p. 326, 2019. [Online]. Available: https://doi.org/10.3390/s19020326.
6. R. Singh, A. D. Dwivedi, and G. Srivastava, "Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention," Sensors, vol. 20, no. 14, p. 3951, 2020. [Online]. Available: https://doi.org/10.3390/s20143951
7. A.D. Dwivedi, "A scalable blockchain based digital rights management system," IACR Cryptol. ePrint Arch., vol. 2019, p. 1217, 2019. [Online]. Available: https://eprint.iacr.org/2019/1217
8. D. K. D. Im, "The blockchain trilemma," 2018.
9. K. Uri, B. Soumya, K. Aleksandar, and S. E. Gun, "bloxroute: A scalable trustless blockchain distribution network," Available at https://bloxroute.com/, 2019.
10. S. M. Jang, T. Geng, J.-Y. Q. Li, R. Xia, C.-T. Huang, H. Kim, and J. Tang, "A computational approach for examining the roots and spreading patterns of fake news: Evolution tree analysis," Computers in Human Behavior, vol. 84, pp. 103–113, 2018.
11. A.Qayyum, J. Qadir, M. U. Janjua, and F. Sher, "Using blockchain to rein in the new post-truth world and check the spread of fake news," IT Professional, vol. 21, no. 4, pp. 16–24, 2019.
12. Q. Chen, G. Srivastava, R. M. Parizi, M. Aloqaily, and I. A. Ridhawi, "An incentive-aware blockchain-based solution for internet of fake media things," Information Processing and Management, p. 102370, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0306457320308657
13. G. Shrivastava, P. Kumar, R. P. Ojha, P. K. Srivastava, S. Mohan, and G. Srivastava, "Defensive modeling of fake news through online social networks," IEEE Transactions on Computational Social Systems, pp. 1 9, 2020.
14. N. Deepa, Q. Pham, D. C. Nguyen, S. Bhattacharya, P. B, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, and P. N. Pathirana, "A survey on blockchain for big data: Approaches, opportunities, and future directions," CoRR, vol. abs/2009.00858, 2020. [Online]. Available: https://arxiv.org/abs/2009.00858
15. H. Liang, J. Wu, S. Mumtaz, J. Li, X. Lin, and M. Wen, "MBID: micro-blockchain-based

geographical dynamic intrusion detection for V2X," IEEE Commun. Mag., vol. 57, no. 10, pp. 77–83, 2019. [Online]. Available: https://doi.org/10.1109/MCOM.001.1900143

16. X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-ai enabled iot: A consortium blockchain-based efficient and incentive approach," IEEE Trans. Ind. Informatics, vol. 15, no. 12, pp. 6367–6378, 2019. [Online]. Available: https://doi.org/10.1109/TII.2019.2917307
17. R. Singh, A. D. Dwivedi, G. Srivastava, A. Wiszniewska-Matyszkiel, and X. Cheng, "A game theoretic analysis of resource mining in blockchain," Clust. Comput., vol. 23, no. 3, pp. 2035–2046, 2020. [Online]. Available: https://doi.org/10.1007/s10586-020-03046-w
18. A. S. M. S. Hosen, S. Singh, P. K. Sharma, U. Ghosh, J. Wang, I. Ra, and G. H. Cho, "Blockchain-based transaction validation protocol for a secure distributed iot network," IEEE Access, vol. 8, pp. 117266–117277, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3004486
19. A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, "Optimized blockchain model for internet of things based healthcare applications," in 42nd International Conference on Telecommunications and Signal Processing, TSP 2019, Budapest, Hungary, July 1-3, 2019, N. Herencsar, Ed. IEEE, 2019, pp. 135–139. [Online]. Available: https://doi.org/10.1109/TSP.2019.8769060
20. P. Singh, A. Nayyar, A. Kaur, and U. Ghosh, "Blockchain and fog based architecture for internet of everything in smart cities," Future Internet, vol. 12, no. 4, p. 61, 2020. [Online]. Available: https://doi.org/10.3390/fi12040061
21. S. Huckle and M. White, "Fake news: A technological approach to proving the origins of content, using blockchains," Big data, vol. 54, pp. 356–371, 2017.
22. M. Saad, A. Ahmad, and A. Mohaisen, "Fighting fake news propagation with blockchains," in 2019 IEEE Conference on Communications and Network Security (CNS), 2019, pp. 1–4.
23. "NIST: National Institute of Standards and Technology," 2018, https://csrc.nist.gov/Projects/Lightweight-Cryptography.
24. "CAESAR: Competition for Authenticated Encryption: Security, Appli cability, and Robustness," 2013, http://competitions.cr.yp.to/caesar.html.
25. R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers, "The simon and speck lightweight block ciphers," in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015, pp. 1–6.
26. A. D. Dwivedi, P. Morawiecki, and G. Srivastava, "Differential crypt analysis of round-reduced speck suitable for internet of things devices," IEEE Access, vol. 7, pp. 16476–16486, 2019.
27. A. D. Dwivedi, P. Morawiecki, and S. W´ ojtowicz, "Finding differential paths in arx ciphers through nested monte-carlo search," International Journal of electronics and telecommunications, vol. 64, no. 2, pp. 147 150, 2018