Tracing the Source of Fake News using a Scalable Blockchain Distributed Network

Dwivedi, Ashutosh Dhar; Singh, Rajani; Dhall, Sakshi; Srivastava, Gautam; Pal, Saibal K.

Published in:
Proceedings of 2020 IEEE International Conference on Mobile Ad Hoc and Sensor Systems

Link to article, DOI:
10.1109/MASS50613.2020.00015

Publication date:
2021

Document Version
Peer reviewed version

Citation (APA):
Dwivedi, A. D., Singh, R., Dhall, S., Srivastava, G., & Pal, S. K. (2021). Tracing the Source of Fake News using a Scalable Blockchain Distributed Network. In *Proceedings of 2020 IEEE International Conference on Mobile Ad Hoc and Sensor Systems* (pp. 38-43). IEEE. https://doi.org/10.1109/MASS50613.2020.00015

Tracing the Source of Fake News using a Scalable Blockchain Distributed Network

Ashutosh Dhar Dwivedi*, Rajani Singh†‡, Sakshi Dhall§, Gautam Srivastava¶, and Saibal K. Pal**

* Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark
† Department of Digitalization, Copenhagen Business School, Denmark
‡ DTU Skylab, Technical University of Denmark, Denmark
§ Department of Mathematics, Jamia Millia Islamia, New Delhi, India
¶ Department of Mathematics and Computer Science, Brandon University, Brandon, Canada
** Defence Research and Development Organization (DRDO), Delhi, India

Abstract—**In the news industry, as well as in social media, fake news detection and identification of news sources has become a central topic of discussion. In the era of digitization, anyone can easily generate or manipulate digital content and publish them on social media websites. On the one hand, these social networking platforms provide ample ease in modern-day communication but on the other hand, using such platforms has posed new challenges to real-world implementation like viral spreading of false/fake information with malicious intentions. In this paper, a naive blockchain and watermarking based social media framework is proposed to control the fake news propagation. We postulate a new blockchain model to mitigate existing challenges in this field. Moreover, the novel solution can help in reducing the spread of fake news by tracing the root or origin of the fake news on social media. Through our experimental results, we show that our blockchain-based solution is able to immediately stream data through a bloXroute server that can propagate data up to 100 times faster than conventional solutions.**

Keywords—**Scalable Blockchain, Distributed Network, Overlay Network, Fake News, Digital Watermarking**

I. Introduction

Information veracity always affects the society, whether it comes from social media, print media or news channels. The information that has no real facts or evidence behind it but is presented in a way that seems accurate and is often consumed by millions through social networking websites, television, and other types of digital media. This type of false information is defined as fake news. The effect of false information spread on social networking websites is significantly high, and it has the potential to cause disorder in society within hours for millions of users. Such fake news propagation has the power to change election results, spread hatred in society, affect voting patterns, stock values and much more. The biggest tragedy is, once the fake news becomes viral, its hard to identify the source of origin and thus, stop its further propagation. As a side effect, the common man today is losing his/her trust in media and sometimes even news channels because of the lack of proper reference checking to verify facts. Nowadays, a lot of digital content is being published in the form of blogs, videos, images, etc. Anyone can freely share any information or news over social networking websites such as Facebook, Twitter, Instagram, LinkedIn, without any actual fact checking. People can easily believe or get influenced by such fake news and change their perception about the subject of such news which could be about a specific community, socio-economic practices, religion, and a given individual. Fake news is so powerful that it can destroy the reputation of anyone, public figure or even an ordinary person. An intuitive solution to mitigate these problems is to use a central authority that can monitor such digital content and regulate information flow. However, using such central authority kills the trust model and privacy of decentralized social networks. Due to the distributed and decentralized nature of blockchain technology [1], it is strongly believed by the research community that this technology is suitable for several areas beyond finance, including e-voting [2], [3], healthcare [4], [5], supply chain [6] and digital right management system [7]. In this paper, a blockchain and watermarking based social networking framework is proposed. Our system has the ability to trace the root or origin of fake news which will help in refraining the propagation of fake news on social networks. In the proposed framework, blockchain stores each news item shared or uploaded on the proposed social networking platform in the form of a transaction performed by registered users. Because of the transparent and traceable nature of blockchain, it is possible to verify the source of any information that is shared on such a platform. Tracing the news source by using blockchain can be achieved with the help of timestamping and the chain connection between blocks. In order to identify the news path shared by users on such social media platform, it is necessary to trace news items by going backwards step-by-step, to identify which user originated or modified the news with malicious intent. Block headers in a blockchain contain lots of information, e.g. a pre-block hash value, current block hash, timestamps etc. These block headers can provide assistance in data tracing. Once the user uploads any information on a social networking website, that transaction can be stored on the blockchain, and every time a new user shares that data or attempts to modify the data, it makes a traceable chain of transactions. With the help of timestamps, anyone can identify the sequence of such transactions stored in the blockchain.

The major drawback of blockchain technology is scaling

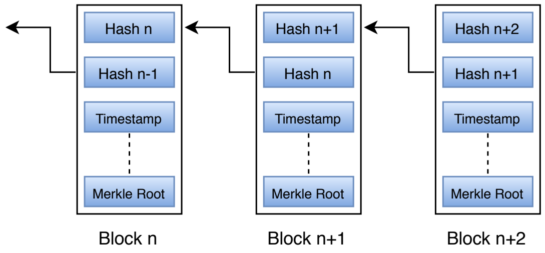

Fig. 1: Basic Blockchain Structure

of the network [8]. Scalability is one the most vital problem in blockchain and has been of key focus in the blockchain research community since its onset. However, in the proposed model, we increase network scalability using *bloXroute* [9]. Once the origin is traced, we need to ensure that if the news is tampered or not by someone and for that, we use digital watermarking.

II. Related work

Jang *et al.* [10] proposed a framework to analyze and identify fake news sources. The authors examined how fake news initiates and transmits through social networks. The framework uses an evolution tree modelling method to examine fake news over the online system. Antecedent tweets and root of those tweets have been identified by the proposed system. Authors also observed the evaluation pattern of fake and real news. The results showed that real news spread quickly and widely to the network while fake news went through many content modifications.

In the context of preventing fake news with blockchain, we have seen some work recently by Qayyum *et al.* [11]. In this paper, the authors use deep learning (DL) and machine learning (ML) along with a smart contract-based blockchain to tackle fake news. They also have highlighted the issues in various designs based on the blockchain-based framework to prevent fake news. Some other works in the same research domain of fake news and blockchain are: [12]–[20]. Huckle *et al.* [21] introduced a prototype for proving the origins of captured digital media. The authors proposed a technological solution to the problem of proving the validity of media resources used in fake news.

Saad *et al.* [22] presented a novel approach of using blockchain to prevent fake news shared by social website network. In this work, the authors considered media as a source of news and later could be modified by users on social media who share these news. Their prototype work can prevent the propagation of fake news in social networks. In fact, the framework proposed in this paper takes the Saad et al. approach further by introducing bloXRoute for network scalability and keyed-watermarking to identify any manipulations with the original media in order to handle the major drawbacks of existing systems (as highlighted in the next section). Also, the scope has been extended to cater to scenarios where the common social media platform user may act as media/news generator while this scenario has not been handled in the said paper.

III. Drawbacks of Current System

- The biggest challenge of social media networking is to trace the source of information. Once a piece of fake news become viral, it is hard to know who created fake news.
- Blockchain could be the solution to track the record of such transactions, but the scalability of blockchain is not suitable for social networks, and it becomes another important issue to solve.
- Once the origin of the news is traced, it is also very difficult to identify who is the main culprit. If the news is modified by someone else or originally uploaded by the content owner.

IV. Our System

A. Building a scalable trustless blockchain distributed network (BDN)

The goal of the system is to improve the throughput of the system by improving the network scalability issue. A fast network is required where blocks can be propagated to the whole network very swiftly, and therefore no delay occurs in verifying the blocks. The overall process of improving network scalability will increase the throughput subsequently. In our system, we use distributed high-capacity *bloXroute* servers. The *bloXroute* uses the blockchain distributed server concept that solves the scalability bottleneck at the network layer. The network proposed by them is a blockchain distributed network – a global network of servers optimized for quickly sending blockchain data. These BDN servers use advanced network techniques – when a bloXroute server receives a packet of data, it immediately streams this data to the rest of the network allowing bloXroute server to propagate data up to 100 times faster. By removing the networking bottleneck, bloXroute server solves the scalability problems of blockchain. The overall system consists of two types of networks:

- *bloXroute* servers – These are low-latency and high capacity servers which are optimized to propagate transactions and blocks for multiple blockchain systems quickly. They work like cluster servers connected with other clusters. These bloXroute servers decrease network overhead and delay. Note that, these servers do not act as any central server and manage other small nodes. The purpose of introducing bloXroute servers is to increase the propagation speed of blocks.
- Peer networks – P2P networks of computer or mobile nodes use bloXroute servers to propagate transactions and blocks, while they also audit the behaviour of bloXroute. These peer networks use specific consensus algorithm. These networks are grouped into clusters and each cluster has one blockchain server that propagates transactions and blocks on behalf of small nodes also called peer.

The blocks from different peers are encrypted and then transferred to the bloXroute servers for further propagation to

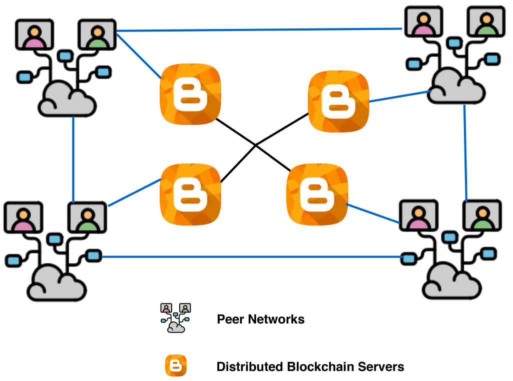

Fig. 2: Distributed bloXroute Servers Connected With Peer Networks.

other networks. Also, peers may either send these encrypted blocks directly to bloXroute servers or they may send it via some other peer nodes. Due to these two properties, the servers cannot be biased or cheat to some particular nodes. The bloXroute servers work blindly without knowing the content of blocks, and once blocks are reached to the destination, the key is revealed. The propagation speed of these bloXroute servers are very fast, and therefore blocks in the network are forwarded quickly to other networks for the verification.

B. Consensus Algorithm

Blockchain uses many consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA) etc. Each protocol has its own positive aspects and negative aspects. However, these protocols are not scalable, and they have low throughput. Therefore, using these consensus protocols in our system is not feasible. On the other hand, Byzantine Fault Tolerance (BFT) based algorithms have low network scalability but high throughput. pBFT thus has extremely high-performance requirements for the network. However, in our case, we increased network scalability by using bloXroute servers, and therefore this consensus algorithm is suitable for our needs. We use a private blockchain (permissioned), where only permitted nodes can participate in the consensus process. There are no anonymous nodes that can validate transactions or nodes that can receive mining rewards. Therefore, no mining cost applies to our system.

C. Fighting Fake News Propagation With Blockchains

Our model involves a platform similar to Facebook, Twitter, LinkedIn etc. that makes use of a blockchain network. A user or news agency can make a profile over the blockchain platform. However, every user has to verify their identity on the blockchain by using an identity card, national identity number, or media credentials. Another method that may be used is through a digital signature that is already registered with a national ID. These pieces of information are hidden from the general public. However, the blockchain-enabled platform can verify information at any time. Note that, in the proposed model we are not identifying the fake news by using some automatic Machine Learning (ML) algorithms; instead the model focuses on identifying the source of news and verify the fake news based on users report on social websites. There are two types of transactions flow in the system:

1) Sharing news already uploaded: Any registered user may share digital news content to the social networking website. Before sharing, the user also needs to mention the type of share, whether the content is news or personal. If the content is news, then its privacy will be public, and anyone can report it as fake or real news among registered users. During this dilemma, i.e. whether the news is fake or real, the news is question marked with an orange sign. Once blockchain members verify the news, the content will be ticked as green if real and crossed as red if fake.

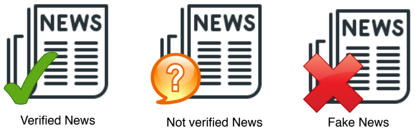

Fig. 3: News Verification

Note that, we are using a private permissioned blockchain and therefore it can be verified only by authorized users. The transactions contains timestamps of sharing data about those who already shared this news earlier including the originator of the content.

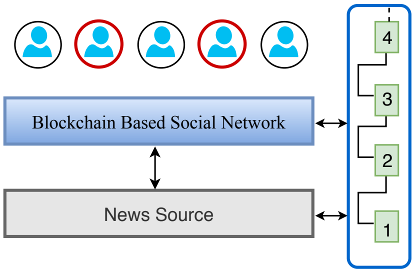

Fig. 4: Transactions chain for sharing of news

Once the news is generated by a user, its details like user ID, hash value, timestamps are saved in the form of a transaction in the blockchain. When a different user shares the same post, the blockchain again stores the transaction with added information, and this makes it traceable inside the blockchain-based on internal information of the transaction. Once a user modifies the content of the post and shares it, the blockchain also stores this modification transaction, and therefore it's easy to know who modified the content. In Figure 4, some users are identified as red who modified the content.

2) Uploading digital news to the blockchain-enabled platform: Any user can upload digital news content; however, the user has to choose if the data is news or some personal information. If the data is a news item, its transaction is saved in the blockchain, and our social networking platform adds a keyed digital watermark to the content automatically to avoid tampering of digital contents. Due to many powerful multimedia editing tools, millions of edited and tampered images, videos, audios and news are seen on social media to change the perception of people regarding particular issues. Therefore, ensuring the integrity of such multimedia content is required.

Watermark based Data Integrity: The best tools available to achieve digital data integrity are watermarking or digital signatures. Digital watermarking is used for the content verification of document, audio and videos while the digital signature is used for documents or images authentication. In the case of digital signature, Algorithm 1 calculates the hash value of the digital content and the given hash value can be used to verify the signature at the receiver end. However, hash values are unique and changing a single bit in the input will change the whole output of the hash function. Therefore, a digital signature can be used to detect any modification in the digital content. In some cases, these modifications are required for some purpose, e.g. data are compressed when uploaded to some platform. In some cases, like YouTube, the user wants to see videos in different video qualities, depending on their internet speed. The data uploaded to social websites are also modified to the smaller size, and therefore in such cases, images are modified for creative reasons. These lossy compressions are also required for our model, and therefore a digital signature is not the solution of authentication suitable for our model. In our model, social network compresses the data before uploading it to servers, and therefore, keyed-watermarking could be the best solution for verifying desired data integrity. Following is an elementary illustration of keyed-watermarking (Algorithm 1) on image media, and similarly, implementations of the proposed platform can define keyed-watermarking for all types of media. Further, two types of watermarking scheme may be used, namely, invisible watermarking and robust watermarking. *Invisible Watermarking* is used in the cases where embedding level is too short to observe or notice while *Robust Watermarking* algorithm is used for securing the digital media contents from the designated class of transformations such as manipulating and tampering of the image or video. It is often used in ownership protection. The Robust watermarking algorithm can survive not only in such general operations like compression, adding noise, filtering, etc., but also in such geometric attacks like rotation, scaling translation, shearing, etc.

We denote an input image of $m \times n$ pixels size by $im(x, y)$, where $x = \{0, \ldots, m\}$ represents the row and $y = \{0, \ldots, n\}$ represents the column. Define a function $p(a)$ and $p(b)$ as follows:

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

Algorithm 1 Watermark Embedding.

Input: Image, Watermark **Output:** Watermarked Image

```
1) Read the input image named Host and convert it into grayscale format.
     • RGB = imread('Host.jpg')
     • greyscale-host= rgb2gray(RGB)
2) Read the encrypted watermark image named WM, apply key and convert it into 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)
3) Compute the 2-D DCT-DWT coefficients of the input image.
   2d-dct+dwt-coeff-host = dct+dwt2(greyscale-host)

4) Divide the input image into $8 \times 8$ blocks and Insert the watermark into the first bit every block.
5) Recombine the blocks into image and compute inverse DCT-DWT.
6) Display the Watermarked image.
```

For function $p(a)$ and $p(b)$ given by (1), discrete cosine transformation or DCT of two dimensional image $im(x, y)$ is given by

$$D(a, b) = p(a) \cdot p(b) \cdot \left(\sum_{x=0}^{m-1} \sum_{y=0}^{n-1} im(x, y) \cos \frac{(2x+1)\pi a}{2m} \right) \cos \left(\frac{(2y+1)\pi b}{2n} \right) \tag{2}$$

while the inverse of discrete cosine transformation or IDCT is given by

$$im(x, y) = p(a) \cdot p(b) \cdot \left(\sum_{a=0}^{m-1} \sum_{b=0}^{n-1} D(x, y) \cos \frac{(2x+1)\pi a}{2m} \right) \cos \left(\frac{(2y+1)\pi b}{2n} \right) \tag{3}$$

Watermark encryption: In our proposed model, a watermark image is always encrypted before embedding into the original content that could be any digital media. This encryption technique is very useful in the case where the attacker can successfully extract the watermark from the content. Because of watermark encryption; the attacker cannot be able to find the original watermark image. To encrypt the digital content, a lightweight encryption algorithm is used. Various lightweight encryption algorithms are being proposed and presented in different competitions for encryption algorithms [23], [24], but most of them are not secure as they are already broken through some cryptanalysis technique. However, ARX family cipher — a lightweight encryption algorithm, used from [25], is not completely breakable for the full round. ARX family cipher uses three simple ARX operations, namely, bitwise rotation, modular addition, and exclusive-OR. Hence, such cipher is well suited to perform on the devices with low capacity. Therefore, we use ARX family cipher to secure the content from attack. It is secured against various attacks (see [26], [27]) for the full number of rounds.

V. Experimental Analysis

To embed the watermark with given image, DCT and DWT algorithms (see Figure 5) are used. To run the experiment, we used MATLAB platform. The embedding code is available at github [1]

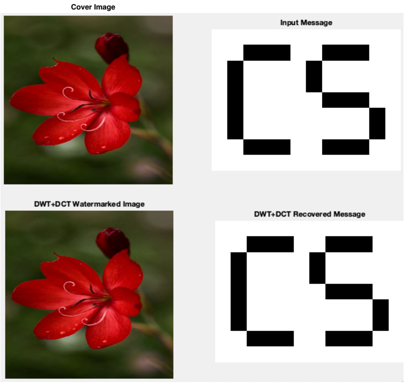

Fig. 5: Watermark embedding using DWT and DCT.

In order to analyse the encryption time suitable for IoT devices, we performed encryption (see Figure 6) with several lightweight ciphers and noticed that SPECK is suitable for our platform. These IoT devices are resource-constrained and therefore, cannot use heavy ciphers. SPECK cipher was designed by the National Security Agency of the US in 2013. Encryption algorithm codes for each ciphers are easily available on Github or official websites.

In order to evaluate robustness and transparency, bit error is used to evaluate robustness and Peak signal to noise ratio (PSNR) is used to measure transparency. The sequence of discrete cosine transform (DCT) of a block is DCT_L, $(L = 1, 2, 3, ...63)$. In the figure 7, we choose $L = 3, 4, ...16$.

To evaluate the quality of watermark image in terms of transparency, we calculate the PSNR by the folllowing formula:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{(\bar{V}-1)^2}{\mathrm{MSE}}\right)\text{decibel,} \tag{4}$$

where $\bar{V} - 1$ is the maximal pixel value of the original image and MSE is the mean squared error and defined as

$$\frac{1}{m\times n}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}\left(\mathrm{Wim}(x,y)-\overline{\mathrm{Wim}}(x,y)\right)^2, \tag{5}$$

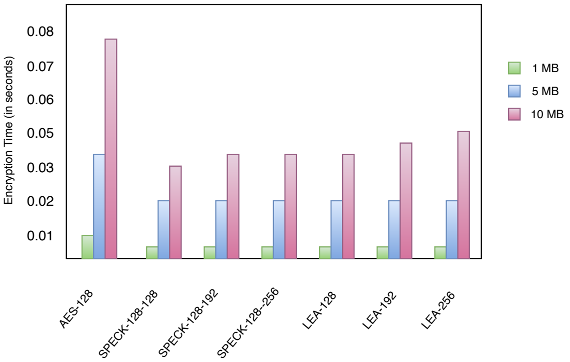

Fig. 6: Comparison of encryption time (seconds).

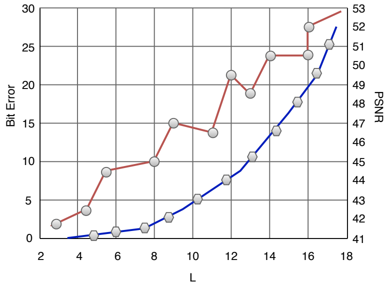

Fig. 7: Relationship between D_L, PSNR and Bit error.

where Wim is the original watermark image while $\overline{\mathrm{Wim}}$ is the extracted watermark image.

To evaluate the similarity level between the original and extracted watermark image, we calculate the Normalized cross correlation (NCC) by using the following formula:

$$NCC = \frac{\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}\mathrm{Wim}(x,y)\times\overline{\mathrm{Wim}}(x,y)}{\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}(\mathrm{Wim}(x,y))^2} \tag{6}$$

In the experiment, we took the jpg image of size 21 KB name 'HOST'. For the encrypted watermark image we use bmp image of size 1 KB named 'WM'. The PSNR of the watermarked image is 44.8887 decibel, while the NCC of the watermarked image is 0.0039.

VI. Conclusion

In this paper, we present a novel blockchain-based social networking system to mitigate the growing problem of fake news. Our proposed system is scalable, secure and provides high throughput. The majority of blockchain solutions face the problem of scalability. To address the scalability issue, we use Blockchain Distributed Network (BDN) with bloXroute servers which substantially improves the scalability in our case. These BDN servers use advanced network techniques

[1] https://github.com/earthat/Digital-Image-Watermarking-Using-Optimized-DWT-DCT

– when a bloXroute server receives a packet of data, it immediately streams this data to the rest of the network allowing bloXroute server to propagate data up to 100 times faster. We also performed watermark experiment using MATLAB, and used DCT and DWT algorithm to embed the watermark with image and presented a relationship graph for PSNR and bit-error by choosing mid-frequency coefficients that directly affects the transparency and robustness of watermark. Thus, using the proposed scalable blockchain distributed network and keyed-watermarking schemes, our platform addresses the major drawbacks in existing systems and is found suitable to identify the source of fake news on blockchain-based social websites which can be helpful to reduce the fake news propagation. Additionally, by solving the bottleneck issue of the network, any cryptocurrency community, as well as IoT based systems, can adjust their protocol to our network. We performed an experiment related to cryptanalysis of lightweight ciphers and based on security margin and encryption time we choose most efficient cipher. Therefore, the proposed model is suitable for resource-constrained devices, as we have selected an efficient, lightweight encryption algorithm.

Funding:

The work of Rajani Singh is funded by the Danish Ministry of Education and Science, Digital Pilot Hub and Skylab Digital. This research was partially funded by the Natural Sciences and Engineering Research Council of Canada held by Dr. Gautam Srivastava.

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.2019.8861828

[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_41

[3] G. Srivastava., A. D. Dwivedi, and R. Singh., "Crypto-democracy: A decentralized voting scheme using blockchain technology," in *Proceedings 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. 117 266–117 277, 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. 5 4, 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, Applicability, 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 cryptanalysis of round-reduced speck suitable for internet of things devices," *IEEE Access*, vol. 7, pp. 16 476–16 486, 2019.

[27] A. D. Dwivedi, P. Morawiecki, and S. Wójtowicz, "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.