International Journal on Emerging Technologies **11**(3): 158-163(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

The Efficient way to Detect and Stall Fake Articles in Public Media using the Blockchain Technique: Proof of Trustworthiness

S. Phani Praveen[1], Ha Huy Cuong Nguyen[2], D. Swapna[1], K. Koteswara Rao[3] and D. Lokesh Sai Kumar[1]

[1]Assistant Professor, Department of Computer Science and Engineering,
PVPSIT, Vijayawada (Andhra Pradesh), India.
[2]Vietnam-Korea University of Information and Communication Technology, Vietnam.
[3]Associate Professor, Department of Computer Science and Engineering,
PVPSIT, Vijayawada (Andhra Pradesh), India.

(Corresponding author: K. Koteswara Rao)

(Received 28 January 2020, Revised 01 April 2020, Accepted 03 April 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Now a day, "fake articles" have become a worldwide concern that increases exceptional concerns for social culture and democracy. The unrestricted access to make and offer data via web based networking media like Twitter and other advanced social digital environments has cracked out a novel concern of fake data, which made gossips far and wide. With discernible and straightforward feature of blockchain, it tends to be credible to confirm the validity of the data and fabricate belief in articles showed on web. But, the social network's size and the blockchain design constructs add several challenges that delay the deployment of such solutions. In this research paper, we recommend a blockchain design for fake articles avoidance and present an innovative blockchain method termed as (PoT) Proof of Trustworthiness for identifying fake articles and stalling its circulation in societal webs. PoT functionality has been applied over two datasets of article worthy tweets gathered from various sources of reports on Twitter. The outcomes have shown an adequate efficiency of the proposed method in detecting gossips and stalling its dissemination.

Keywords: accuracy, block chain, detect, social media, Trust.

I. INTRODUCTION

Fake article and its Impact?

Fake articles are characterized by data that have no reality at all, but are introduced really as exact and spread by billions of transmissions through TV, radio news, web sites or web based media. The lies can end the status of any person or businesses comprising health, finance, politics, stock and sports.

As an example in the year 2016, an article of Buzz feed categorized that the majority of fake viral articles circulated was that "Obama had issued a command forbidding oath of adherence in all the schools across nation". This article has been circulated to defame position of Obama during 2016 elections in USA.

The lies not fair are restricted to politics, however can disturb more zones such as finance and health. It's not that much easy to identify fake articles, as here are numerous varieties of material everywhere, such as:

(a) Sarcasm – When the lies are shared on websites for entertaining however has no prospective of cheating persons.

(b) Distorted connection – When article materials are not related to its headings, titles, or photographs.

(c) Distorted context – When related materials are exchanged in an incorrect situation.

(d) Pretending material – When real sources are impersonator with fake sources.

(e) Falsified material – When an article is made to either make cash or increase publicity.

The start of 21st century established the reason for present troublesome computerized economy, wherever delivering and displaying digital materials has become helpful and simple.

Digital materials as pictures, videos or online blogs are being made and distributed everywhere today. Nobody who has opportunity to check the credibility of messages or recordings sent on the various platforms of web based media. That is the manner by which persons fall into snare for the fake articles. Hence, it have gotten fundamental to connect out the credibility of the data, i.e., where they have originated from and who made them. Fake articles have genuine significances for our beliefs in vote based systems, freedom, and society [4] since fake articles can be utilized to impact individuals for political resolutions and to satisfy plans that are not really genius social [5]. We understand that fake articles are not just a trouble yet that can prompt incredible damage by noting models, for example, the crowd lynching in India that came about because of the distribution of false communications on social websites and brought about the killing of numerous blameless individuals [6]. There are various comparative models where the fabricated data was transmitted for misdirecting society [22].

Actual life situations in real scenarios: One of huge worries about fake articles is control. Fake materials can fool humanity, particularly for the duration of political occasions.

In 2017, in the course of the Jakarta Gubernatorial Election, in excess of thousand gossips on issues of legislation were confirmed as false.

A fake article about an antagonist Baswedan has been circulated by the occasion that his massacre in elections would result in a Muslim revolt.

Global relations are affected because of fake articles. Articles Organization of Qatar stated that in 2017 its twitter account had been enraged by hackers to circulate fake remarks regarding rules of USA International Arab and Gulf countries towards Iran. Neighbouring nations Bahrain, Saudi Arabia, UAE and Egypt broke political bonds with Qatar because of these fake remarks.

Blockchain have abilities bringing about their reasonableness for deciding credibility and integrity since they are, basically, a changeless database innovation with inbuilt trust procedures [1]. They incorporate cryptographic methods and digital signatures that permit secure electronic association, without requiring any central authority [2]. Block chains likewise can execute smart contracts, which are verifiable materials that mechanize a system's standard set fundamentally, at that point, block chains are a trusted ledger equipped of running application logic [3, 21]. Moreover, they cannot be constrained by any solitary entity.

Those procedures mean we can utilize a blockchain to record information about our media assets and any entity that sees those records will be pleased that data passes are authentic.

However many block chain based solutions exist the first drawback is missing the design of a feasible system which can be deployed easily in the current public networks. Second drawback is it is difficult to maintain a repository on blockchain for every user in the network. No work guarantees testing and evaluating blockchain based solutions in presence of adversarial nodes .Challenges by these drawbacks motivated us to present a paper to stall online fake articles using blockchain.

II. RELATED WORKS

A project funded by Google [7] aims at helping journalists recognize fake articles by investigating connections in enormous, complex articles-based datasets. The project's research team was building up an online-based tool that associates artificial intelligence and machine learning mechanisms to envision those connections. They are targeting to test their items with European-based articles associations, for example the UK's telegraph media group and the Guardian, just as Ireland's national telecaster, RTE [7]. These days, clients don't get their articles exclusively from customary print and communicate media; they additionally get it from online media sources. Subsequently, both Narwal *et al.*, [8] and Jin *et al.*, [9] concentrate on conquering fake articles on platforms, for example Twitter. Jin *et al.*, define a tool that investigates messages and makes a progressive graph enhancement of the connection between articles occasions. By so doing, their application spreads the validity of those events [9]. Narwat *et al.,* have built up a tool called Unbiased Crowd, of which reason for existing is to, first, distinguish bias, second, recognize pictures that are utilized outside of any relevant context to provision a specific opinion, and third, make a call to action, whereby campaigners are urged to depict the inherent bias [8]. Unfortunately, there are generally not many verifiable blockchain methods used for cracking fake articles and false data issue explicitly. In any case, the literature presented some blockchain methods for taking care of determined issues in online webs. For instance, blockchain is designed as a bank of data usable by all public network nodes depending on certain rules and priorities of nodes upon blockchain authorization it facilitates social integrity networking [10]. Some works investigate whether Metcalfe's law has been fulfilled by current blockchain platforms or not in order to model networks for crypto currency protocols [11]. A framework has been proposed in Ethereum Block chain to verify the credibility of contents [12]. The recommended solution adopts preservation metadata implementation strategies (PREMIS) for storing data on blockchain cryptographically [12]. Researchers used the concept that by recording timestamp and establishing chain network between blocks so that the origin of articles can be outlined and therefore a decentralized blockchain based storage approach has been proposed for outlining the news origin [13]. An innovative framework proposed by Yahiatene and Rachedi (2018) [16] depend on 2 important components. Software-Defined Vehicular Networks (SDVN) and Authenticating transactions by ensuring anonymity to data in a decentralised manner across public network using blockchain. A novel framework to eradicate fake article spreading using blockchain [14]. The key idea is to construct an algorithm based on concept of blockchain for raising credibility and clarity of the data disseminating on public networks. The researchers in [15] simulate the capability of using U-share-blockchain concept to make users to trace and manage all the content posted over the public network. An adding contribution of blockchain to public networks is Tweet-chain [17] which works based on protocol called proof of Concept [18] which is used to manage public posts. Fake chain [19] authenticates information shared over the public network based on consensus powered by data mining for recognizing fake articles. Recognizing fake articles can be done by using features of ethereal block chain complied with BFS algorithm [20].

III. PROBLEM METHODOLOGY

Blockchain is stated to be among rising technologies to reform the manner in which data are created and scattered. Because of the detectability, decentralization and transparency feature of blockchain, the issue of fake articles can be efficiently handled. Blockchain provides a trusty way of proving information and source of information to the online readers.

In this research paper, we recommend a Blockchain design model termed Proof of Trust-Worthiness (PoT) for recognizing and preventing fake articles in public networks. PoT re-engineers public networks into decentralised networks, where users will be presented as peers.

An immutable record of detected gossips that is cryptographically secured is shared as a distributed ledger among the peers. Blockchain termed as a distributed ledger is a row of chunks where every chunk holds a newly recognised set of gossips. The PoT chain code which is responsible for detecting fake articles is distributed among all the peers in the platform.

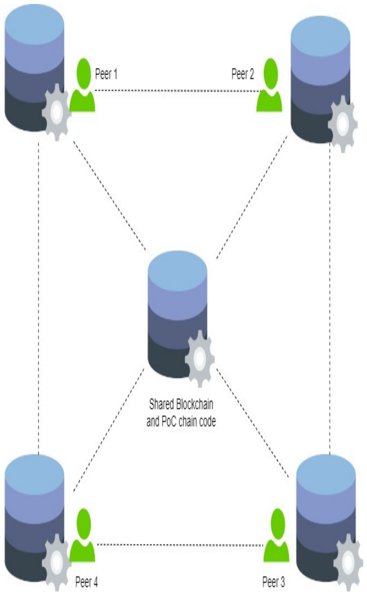

Fig. 1. Conceptual view of block chain depended public network model.

Fig. 1 shows the real vision of social networks based on blockchain where peers over the network execute PoT code through a blockchain web browser. With PoT-based public network schemes there is no necessity for the 3rd party to validate the circulated data and recognizing gossips, such that peers will do this task based on the PoT block chain scheme. PoT enables detection of gossips via shared information on public networks without the intervention of third party. Every block amongst the blockchain consists of a fixed figure of fake articles. The credibility of shared information is assessed by PoT protocol. The source of information may be news, TV, radio, users etc.

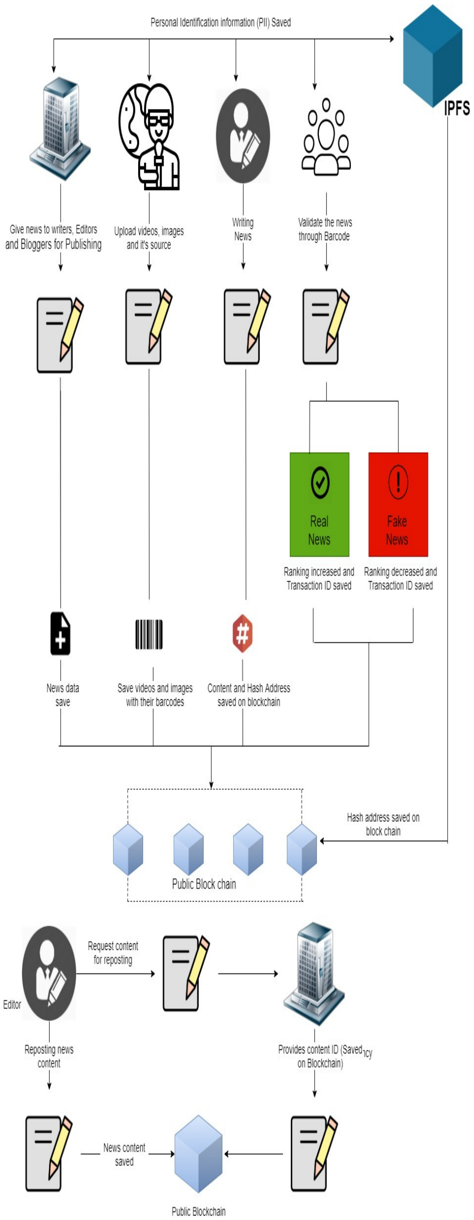
Personal Identification information (PII) Saved
IPFS
Give news to writers, Editors and Bloggers for Publishing
Upload videos, images and it's source
Writing News
Validate the news through Barcode
Real News
Fake News
Ranking increased and Transaction ID saved
Ranking decreased and Transaction ID saved
News data save
Save videos and images with their barcodes
Content and Hash Address saved on blockchain
Hash address saved on block chain
Public Block chain
Editor
Request content for reposting
Reposting news content
Provides content ID (Saved on Blockchain)
News content saved
Public Blockchain

Fig. 2. Design model of the PoT protocol.

Articles organizations: Using blockchain associated applications, official articles organizations can generate their outlines and upload essential records such as:
– Name of organizations
– Certificate of article organizations
– Residence proof
– Name of the domain
– Work license
– Experience

The articles given by article organizations are stored in IPFS which in turn generated hash of IPFS is signed and loaded into blockchain. Articles organizations circulate articles amongst bloggers, publishers, writers through blockchain. Editors check the originality of articles received from organizations and makes a decision on broadcasting of article

Editors create profile: Editor's login to blockchain enabled environment with the essential details like
– Editors designation
– Details of contacts such as phone number, Email id
– Cadre
– License of article organizations, agencies
– Certifications and work experience.

Authorized documents from the editors are placed in IPFS and the hash address of document is loaded into blockchain. Third party APIs does authentication of KYC data of editors. The experience of editors in the journalism industry is verified thoroughly and is granted permission to publish their articles. Smart contracts activate procedures to facilitate rankings based on records uploaded to the editors. Articles written by editors can be chosen by crowd accountants based on provided rankings. After successful registration, materials can be broadcasted by the editors. The hash address of corresponding materials would be signed and loaded on blockchain. As data on blockchain are immutable it is difficult for anyone to change data. The IPFS hash address describes who made it when and where.

Journalist's profile creation: Likewise journalists had to register with necessary details like address, email, mobile number, work license to blockchain platform.

Third party APIs does authentication of KYC data of journalists. Smart contracts activate procedures to facilitate rankings based on reports submitted by journalists. Videos or pictures can be published by journalists after registration. After Publishing data, a smart contract would be activated to store the respective data and its initiation to blockchain.

If at any point, changes are made to videos or pictures by journalists then at that time the item would be placed along with its hash in blockchain. Based on modifications it would help journalists to detect whether uploaded data are genuine or misutilized. Entire things undergone to the published data would be evaluated by peers on Blockchain network. Erasing the information that is videos or pictures is difficult as they are present on blockchain. While making video or picture, smart contracts on blockchain would produce recognisability.

Role of the Crowd Auditors: Group Auditors are active on the network. They should be able to decide whether articles distributed are fake or not by tracing their origin, With required data and needed KYC, group auditors can register to platform. After authentication from third party API auditors can be on permitted blockchain application.

How Group auditors track articles origin and authenticate it?

Based on QR code of articles, group auditors can trace the source of specified articles. The composition, modification, distribution details of articles can be found based on QR code assisted with articles. Regardless of content of article, auditors can mark it as fake or genuine by observing QR code. Activation of smart contract is done to place confirmation status of articles on blockchain. Group auditors can detect articles as spam and get ethers on blockchain. They can rank materials and mark as reliable or unreliable.

Issues for group auditors assessing material's trustworthiness:

Verify a site – Group auditors can check a site, distributed articles in it and mark them as reliable or unreliable

Consider an origin – Domain of sites can be verified by group auditors to check whether it is related to the original articles association or not. Since some domains are made to look like original, but there are chances of duplication.

Check an author – Based on author details available on distributed ledger, group auditors can assess the credibility of them

Subsequent merits of permitted articles in a blockchain environment:

– **Transparency in articles**: Transparency feature of blockchain facilitates option to detect whether articles are spam or not. The validity of articles is dependent on criteria mentioned in smart contracts, which show transparency and trust amongst entire world.

– **Traceability of articles**: Applications permitted by blockchain can trace the validity of articles from the origin to the present**.** It will make readers realize fake articles.

– **Decentralized method**: Distributed nature of a platform enables to crack issues of spam or fake articles. It provides durability and immutability and prevention of single point of failure as it is decentralised.

– **Immutable method**: As information stored on it cannot be modified it provides immutability.

The powerful blockchain technology provides an efficient way to deal with the problem of fake articles. As articles are part and parcel of everyone's life we can fulfil transparency of article by utilizing services of blockchain.

IV. EXPERIMENTAL RESULTS

For researching authenticity and viability of the proposed PoT method, experimentation applied on 2 datasets gathered from Twitter. 2 datasets are depicted as trending concept politifact, and gossipcop from Fake Articles Net database to perform fake articles identification. The experimental results of applying PoT approach on 2 datasets prove that the PoT method could recognize fake articles.

Table 1: Number of fake and real articles of datasets.

Source	Politifact		Gossipcop	
	Real	**Fake**	**Real**	**Fake**
Articles paper	624	432	1,681	5,323
Tweets	2,498	9555	8,013	2,651
Blogs	119	37	9,119	3,558
Retweets	3,464	10,619	2,495	5,655
Tvchannel	132	56	802	224

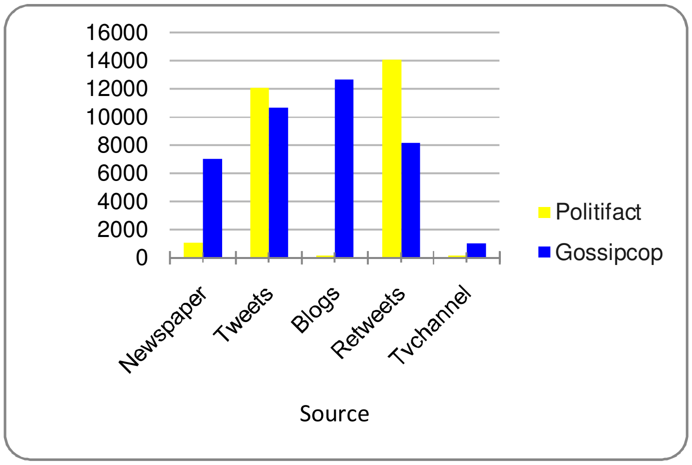

Fig. 3. Sum of real and fake of these data sets.

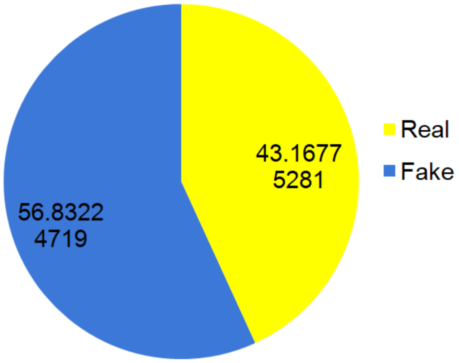

Fig. 4. Percentages of detected fake articles in two studied datasets.

The experimentation proves that tweets are source of fake articles in the politifcat dataset, while retweets are source of fake articles in the the gossipcop dataset.

Metrics: For approving accomplished results, the set of identified fake articles and good articles are deployed to the platform of Xpertin. The feedback and approved results of Xpertin declared that only 91% of identified fake articles is indeed false. Rendering to feedback of Xpertin, PoT method failed to identify 84 tweets as fake tweets and 57 tweets as good tweets.

– Precision evaluates the figure of positive class projections that relate to the class of positives.

– Recall evaluates the figure of positive class projections made among all positive examples in given dataset.

– F-Measure facilitates a single score that balances the both issues of precision and recall in single number .

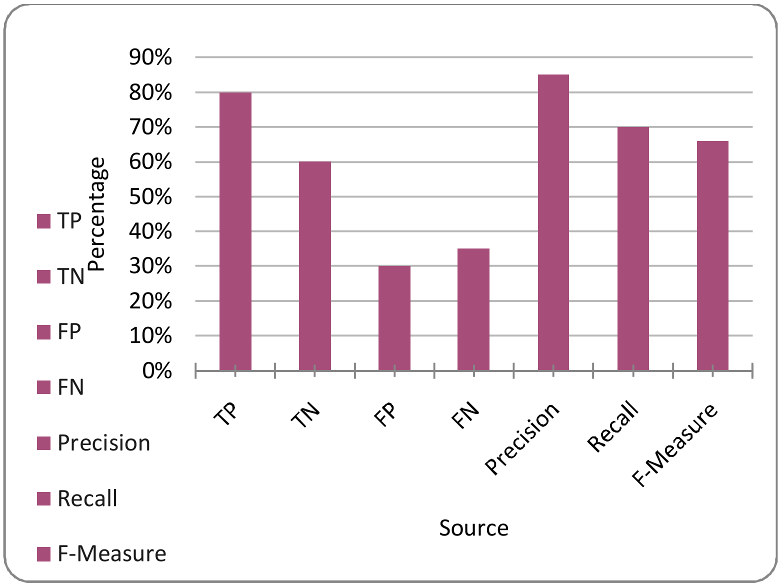

Fig. 5. TP, TN, FP, FN, Precision, Recall, F-Measure Results.

V. CONCLUSION AND FUTURE WORK

The objective of research was to present a design model of proof of trustworthiness protocol for recognizing and obstructing fake articles and misguiding information across public media stages. The work has shown considerable results by simulating projected design model on polifact and gossipcop datasets. Results had shown the effectiveness of PoT in recognizing fake articles with accuracy of 84%. This design can be incorporated beyond social media to various applications such as crowd funding without any loss to the generality. More advancements using other datasets are required for improvement of PoT accuracy in working and detecting gossips and fake articles in further studies

REFERENCES

[1]. Umeh, J. (2016). Blockchain double bubble or double trouble?. *Itnow*, *58*(1), 58-61.

[2]. Huckle, S., & White, M. (2016). Socialism and the Blockchain. *Future Internet*, *8*(4), 1-15.

[3]. Eris Industries (2016). Explainer | Smart Contracts [Internet]. Eris Industries Documentation. 2016 [cited 2016 Mar 19]. Available from: https://docs.erisindustries.com/explainers/smart_contracts/

[4]. Cass R. Sunstein (2018). Republic: Divided democracy in the age of socialmedia. Princeton University Press.

[5]. Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of economic perspectives*, *31*(2), 211-236.

[6]. Gowen, A. (2018). As mob lynchings fueled by WhatsApp messages sweep India, authorities struggle to combat fake news. *Washington Post.*

[7]. Ed Grover. City journalism academics to lead European big data and fake articles project [Internet]. City, University of London. 7th July 2017 Available from: https://www.city.ac.uk/articles/2017/june/google-digital-articlesinitiative-dminr

[8]. Narwal, V., Salih, M. H., Lopez, J. A., Ortega, A., O'Donovan, J., Höllerer, T., & Savage, S. (2017). Automated assistants to identify and prompt action on visual news bias. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 2796-2801.

[9]. Jin, Z., Cao, J., Jiang, Y. G., & Zhang, Y. (2014). News credibility evaluation on microblog with a hierarchical propagation model. In *2014 IEEE International Conference on Data Mining*, 230-239.

[10]. Shah, S. N. (2019). *U.S. Patent No. 10,490,304*. Washington, DC: U.S. Patent and Trademark Office.

[11]. Alabi, K. (2017). Digital blockchain networks appear to be following Metcalfe's Law. *Electronic Commerce Research and Applications*, *24*, 23-29.

[12]. Huckle, S., & White, M. (2017). Fake news: A technological approach to proving the origins of content, using blockchains. *Big data*, *5*(4), 356-371.

[13]. Shang, W., Liu, M., Lin, W., & Jia, M. (2018). Tracing the source of articles based on blockchain. In2018 IEEE/ACIS 17th *International Conference on Computer and Information Science (ICIS)*, 377–381.

[14]. Jing, T. W., & Murugesan, R. K. (2018). A theoretical framework to build trust and prevent fake news in social media using blockchain. In *International Conference of Reliable Information and Communication Technology,* 955-962. Springer, Cham.

[15]. Chakravorty, A., & Rong, C. (2017). Ushare: user controlled social media based on blockchain. In *Proceedings of the 11th international conference on*

ubiquitous information management and communication, 1-6.

[16]. Yahiatene, Y., & Rachedi, A. (2018). Towards a blockchain and software-defined vehicular networks approaches to secure vehicular social network. In *2018 IEEE Conference on Standards for Communications and Networking (CSCN)*, 1-7.

[17]. Buccafurri, F., Lax, G., Nicolazzo, S., & Nocera, A. (2017, June). Tweetchain: An alternative to blockchain for crowd-based applications. In *International Conference on Web Engineering*, 386-393.

[18]. Song, G., Kim, S., Hwang, H., & Lee, K. (2019). Blockchain-based notarization for social media. In *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 1-2.

[19]. Ochoa, I. S., de Mello, G., Silva, L. A., Gomes, A. J., Fernandes, A. M., & Leithardt, V. R. Q. (2019). FakeChain: A Blockchain Architecture to Ensure Trust in Social Media Networks. In *International Conference on the Quality of Information and Communications Technology*, 105-118.

[20]. Paul, S., Joy, J. I., Sarker, S., Ahmed, S., & Das, A. K. (2019). Fake News Detection in Social Media using Blockchain. In *2019 7th International Conference on Smart Computing & Communications (ICSCC)*, 1-5.

[21]. Swapna, D., & Praveen, S. P. (2020). An Exploration of Distributed Access Control Mechanism using Blockchain. In *Smart Intelligent Computing and Applications*, 13-20.

[22]. Sudha, M. V., & Narayana, M. V. (2019). An Efficient Distributive Framework for Preserving Data Privacy Through Block Chain. *Journal of Innovation in Computer Science and Engineering*, *8*(2), 32-36.

How to cite this article: Praveen, S. P. Nguyen, H. H. C., Swapna, D., Rao, K. K. and Kumar, D. L. S. (2020). The Efficient way to Detect and Stall Fake Articles in Public Media using the Blockchain Technique: Proof of Trustworthiness. *International Journal on Emerging Technologies*, *11*(3): 158–163.