Towards a Location-Aware Blockchain-Based Solution to Distinguish Fake News in Social Media

Chapter · January 2022

DOI: 10.1007/978-981-19-0468-4_9

Wahid Sadique Koly
The University of Asia Pacific
2 PUBLICATIONS **10** CITATIONS
SEE PROFILE

Abu Kaisar Jamil
University of the Ryukyus
5 PUBLICATIONS **72** CITATIONS
SEE PROFILE

Hanif Bhuiyan
Monash University (Australia)
29 PUBLICATIONS **267** CITATIONS
SEE PROFILE

Abdullah Al Omar
University of Alberta
20 PUBLICATIONS **1,015** CITATIONS
SEE PROFILE

Towards a Location-Aware Blockchain-Based Solution to Distinguish Fake News in Social Media

Conference Paper · December 2021

6 authors, including:

Wahid Sadique Koly
The University of Asia Pacific
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Abu Kaisar Jamil
University of Asia Pacific
5 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Shahriar Rahman
University of Liberal Arts Bangladesh (ULAB)
51 PUBLICATIONS **773** CITATIONS
SEE PROFILE

Hanif Bhuiyan
The Commonwealth Scientific and Industrial Research Organisation
20 PUBLICATIONS **86** CITATIONS
SEE PROFILE

Towards a Location-Aware Blockchain-Based Solution to Distinguish Fake News in Social Media

Wahid Sadique Koly[1], Abu Kaisar Jamil[2], Mohammad Shahriar Rahman[3], Hanif Bhuiyan[4], Md Zakirul Alam Bhuiyan[5], and Abdullah Al Omar[6] (✉)

Department of Computer Science and Engineering, University of Asia Pacific, Dhaka, Bangladesh[1,2,6]
United International University, Dhaka, Bangladesh[3]
Data61, CSIRO, Australia[4]
Department of Computer and Information Sciences, Fordham University, New York, NY 10458, USA[5]
wskoly.bp@gmail.com[1], kaisarjamil.cse@gmail.com[2], msr@ieee.org[3]
hanif.bhuiyan@data61.csiro.au[4], bhuiyan3@fordham.edu[5],
omar.cs.bd@gmail.com[6]

Abstract. Nowadays, social media is the main source of all global and local news in this generation. But the propagation of fake news and misleading information through social media has become a major concern. Fake news and misleading information often cause crucial damage to human life and society. Moreover, social media has become a source of news, views, and facts for its user. Through social media, a piece of news or information can reach every corner of the world within seconds. It is quite hard for a general social media user to distinguish fake news from real one. Even sometimes social media users cannot distinguish the fake news while residing in the same location of that real news. Hence, in this paper, we have proposed a location-aware blockchain-based news validation system that can be integrated with social media in order to distinguish fake news and misleading information from real ones.

Keywords: Fake News ; Location-aware ; Blockchain ; Consensus

1 Introduction

In this era of technology, social media has brought everyone closer. We can be more interconnected to each other than before through social media. At present, news of any incident propagates throughout the world within a second through social media. Though it has made our life easier, it has some demerits too.

People tend to believe everything they saw on social media [1]. Generally, we are not in a critical mindset whenever we scroll the news-feed of a social platform. Thus, we do not bother to cross-check the veracity of that particular news and often make it viral by sharing without thinking. Moreover, a survey ran by Pew Research Center in 2020 [2] stated that about 52% of Americans prefer digital platforms as their source of news. So if a piece of misleading information gets viral on social media, it might cause much more damage.

In 2012, a series of assaults conducted by the local mob on Buddhists minority in Ramu, Bangladesh [3, 4]. 22 Buddhist temples along with two Hindu temples and 100 houses were destroyed [5] over a false allegation of posting a photo of burned Quran by a Buddhist male on Facebook. In 2020, a rumor propagated through Facebook that, a certain amount of human heads are needed to be sacrificed for the Padma Bridge Bangladesh [8], and children are being kidnapped for that purpose [9]. This rumor eventually caused some major violent events. There were mob killings of eight people [7] on suspicion of child kidnapping, but none of them were child kidnappers. Later in that year, a clash between police and a religious group caused 4 deaths and several injuries [6, 9]. The violent protest started in the first place when a screenshot containing a hate conversation about the holy prophet of Muslims got viral on Facebook. Later the police confirmed the alleged Facebook account got hacked and, the hacker intentionally made those conversations to create riots between the two religious groups.

Misleading information often puts risks to public health and security [10]. In 2020, a piece of misleading news got viral that Methanol can cure Covid-19 [12]. Around 700 people in Iran died [11] due to Methanol poisoning after consuming Methanol, believing that information. Sometimes scammers/hackers put fake offers or advertisements with attractive headlines on social media. Naive users often got scammed by responding to those offers.

Nowadays, it is hard to decide whether a news is fake or real. If the task to validate a news is given to any organization, there is no guarantee that the organization will be unbiased. As that certain organization will have the authority and responsibility to certify a news, in some extreme cases, the government or some influential organizations might pressurize them or they can be easily corrupted. In Blockchain, we can build a system where the fake news validation can be done anonymously. In our proposed system, the system will be integrated with social media in such a manner that the users of any social media will act as validators of a particular news. As their identity will be unknown, they can certify any facts or stories without any outside influences. Hence, they can remain unbiased nor forced by any other organization or individual.

Organization of the Paper: The remainder of the paper is organized as follows: Section 2 explains the background study. Related work is described in Section 3. Section 4 explains property comparison between our proposed system and other related work. Section 5 outlines the preliminaries. The working methodology of our system is discussed in Section 6. Section 7 briefly analyses the features of the protocol. In section 8, we have analyzed the blockchain based performance of our proposed system. Lastly, conclusion is included in Section 9.

2 Background

Though our proposed system can be implemented with any other technology, we choosed to implement this idea with blockchain technology which is way more complicated but secure than any other traditional technologies [25], [26].

Blockchain is a chain of blocks that interface with each block through a cryptographic approval called hashing function. Blockchain is also known as distributed ledger as it is customized to record monetary exchanges and to store the record in a decentralized manner [24], [23].

In our proposed architecture, we proposed to store our validation records in a distributed Blockchain. For this, no hacker can harm the system or tamper with the record, as copies of all the transactions will be stored in the computer of every participant node. In order to tamper with information, the hacker will have to recalculate all the hash values and will have to change more than 50% of copies of the chain that are distributed in the network. Also, in this way, decentralization of the database moves trust from the central authority as every node connected with the system has all the records and, if changes are needed, all have to change their record, else the system will not work. In our proposed architecture, we also promised transparency as in this blockchain technology, each and everything is visible to start to end. Also, the decentralized organization makes it an open innovation where nothing is covered up and diminishes the opportunity of discrepancy.

Blockchain technology ensures the freedom of speech as there is no central governing body, and it's completely decentralized [18], [22]. Any individual can reclaim their opportunity. Transfer values and administration only can occur on an overall scale of utilizing a decentralized organization at a worldwide level, which also can eliminate any prerequisites from any administration.

3 Related Works

In [13], T. W. Jing and R. K. Murugesan discussed the likeliness of implementing Blockchain technology and advanced AI in social media to prevent fake news from roaming around social media. Also, they discussed the possible research methodology and the research direction for building a trusted network through Blockchain and AI as well as the research problems and limitations.

In a later study [14], authors elaborately reviewed the impacts of fake news along with the amenities of implementing Blockchain technology with advanced AI algorithms in social media to improve mutual trust and prevent fake news. In that paper, they provided a basic overview of Blockchain in terms of privacy, security, validity, transparency and freedom of speech. In an article [15], A. Qayyum, Et al. proposed a Blockchain-based news publishing framework where news publishers can join and publish their news through a publisher management protocol that registers, updates, and invalidates their identities. The news can be validated by the honest miners using consensus mechanism and upon validation, the news can be added to the chain. In a research [16], I. S. Ochoa, Et al. proposed a system based on centralized Blockchain to detect fake news in social media. In their proposed architecture they defined the news sources as full nodes and the validators as miner nodes. When a piece of news deploys as a block in the chain, the miner nodes can validate the block, and using the PoS algorithm the reliability of that block can be increased or decreased. In another research [17], Paul, Et al. proposed a similar architecture with a decentralized approach. There are several related research based on technologies other than Blockchain. M. Granik, Et al. [20] proposed a model to detect fake news using naive Bayes classifier, in 2017. They used a data set collected by BuzzFeed News to train their model. They split the data set into three parts, the first one for training the classifier model, the second one to calibrate the model, and the third one to test the performance of the model. In 2018 [19], D. Vedova, Et al. proposed a novel machine learning based approach to detect fake news in social media. In another research [21], J. C. S. Reis, Et al proposed a supervised learning based approach to detect fake news in social media. In their method, they explored different attributes extracted from the news content, source, and social media and classified these attributes through various classifiers (i.e., KNN, Random Forests, Naive Bayes).

4 Comparison between our architecture and the related works

In this section, we show the results in the eight properties of our architectures. If a particular architecture has the property in it then we marked it with 'Y' otherwise marked with 'N'. Here, Table 1 compares our architecture with other existing architectures. With the careful analogy of the systems, a conclusion can be drawn that our architecture has greater advantages than the other systems in this table.

Table 1. Comparison table

Metric	**Qayyum et al. [15]**	**Ochoa et al. [16]**	**Granik et al. [20]**	**Tee et al. [14]**	**Our Architecture**
Social media integration	N	Y	Y	Y	Y
Anonymity	N	N	N	N	Y
Transparent	N	N	N	Y	Y
Truthfulness indicator	Y	N	Y	N	Y
Reliability indicator	N	Y	N	N	Y
User evaluation	N	Y	N	N	Y
Area factor	N	N	N	N	Y
Blockchain based	Y	Y	N	Y	Y

5 Preliminaries

In this section, we initially discussed each properties shortly that our system achieved. Afterthat, we discussed about the blockchain technology for our proposed system.

5.1 Properties

Our system's key focus points are anonymity, integrity, privacy, and reliability. Some key points of security and privacy are briefly described below:

Anonymity: Anonymity is ensured by generating an unique hash address for each validator of our system. The real identity of each validator will remain hidden.

Integrity: Blockchain ensures the data integrity of our system by storing the validation value of a particular news.

Privacy: In our system, privacy is ensured by keeping the validator's information confidential.

Reliability: The weighting factors and the reliability indicator ensures the reliability during validation process of a particular news in our system.

6 Working methodology

The proposed system is a blockchain based solution to distinguish the widespread of fake news in social media platform. In our system, verified users of any social media platform will act as validators of a particular news. When a news got viral on social media platform, it will be stored in the chain and after that two indicators, and two reaction buttons will be shown under that news on the news-feed of that social media platform. Whenever a verified user validates a news using our reaction button, our system starts generating the validation value of that news through some process. Two indicators will indicate whether the news is true or false after going through some evaluations.

Figure 1 portrays the whole architecture of our proposed system. All the sections and their functionalities of the architecture are briefly described below.

6.1 Validator creation:

As our system will be integrated with a social media platform, every verified user of that platform will be appointed as a validator. Figure 2 shows the validator creation of our proposed system. A social media user(U_s) will be identified with an unique hash address, therefore user's identity will remain hidden. A user(U_s) will have a rank(U_r) on a scale of 1 to 10 and a reliability value on a scale of 50-100. 1 carries the lowest rank and 10 carries the highest rank in this system. Initially, each user(U_s) will be assigned with a rank(U_r) of 1 and a reliability value(U_{rv}) of 50. Upon their evaluation, their Reliability value (U_{rv}) and rank (U_r) will be increased or decreased.

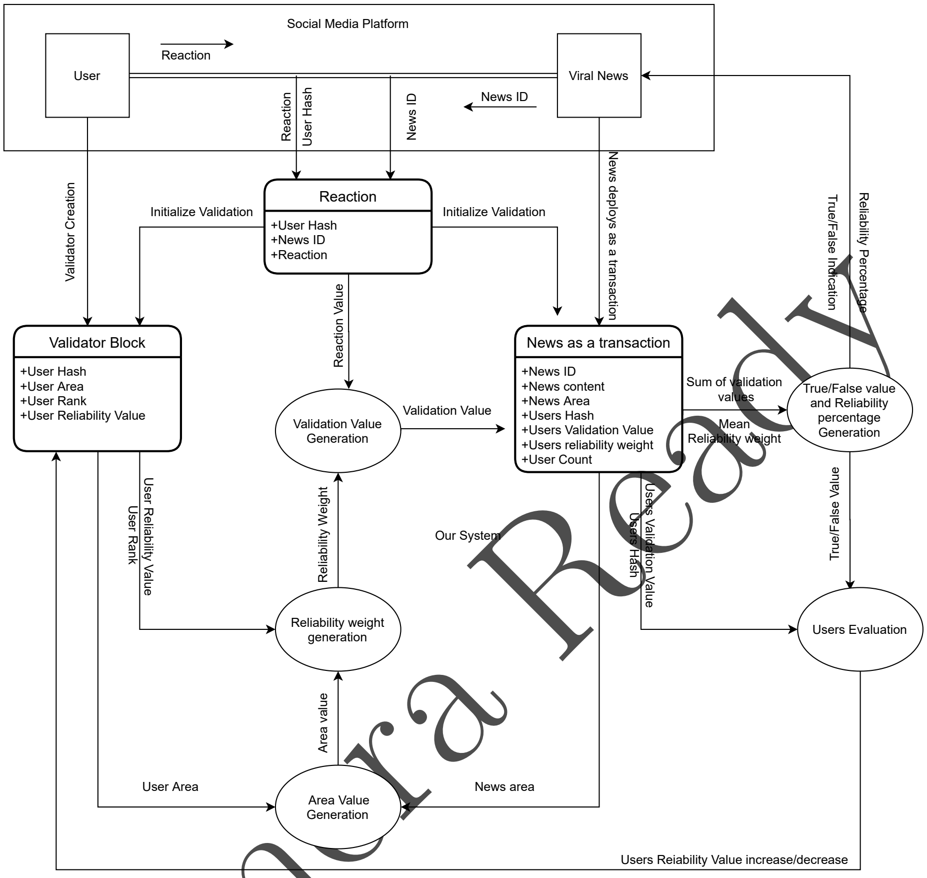

Fig. 1. Architecture of our proposed system.

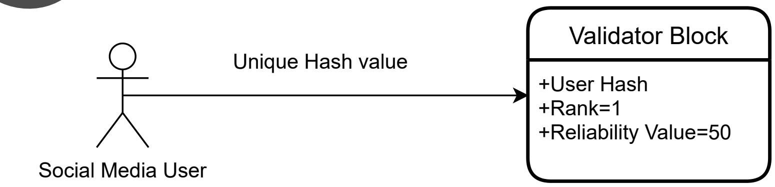

Fig. 2. Validator creation

6.2 News as a transaction(N_w):

If a piece of news or information got viral on that particular social media platform, that means if it reaches a certain amount of shares, it will be added on the chain as a transaction. This transaction shown in figure 3 will contain news id, news area(N_a) information and the news itself. After a news(N_w) has been added to the chain, two indicators, and two reaction buttons will be shown under that news on the news-feed of that particular social media platform. One of the indicators(I_{tf}) will indicate if the news is true or false and another one(I_r) will indicate the reliability percentage of that first indicator. One of the reaction buttons will be marked as true and another one will be marked as false. Therefore, user(U_s) can validate any information without any influences.

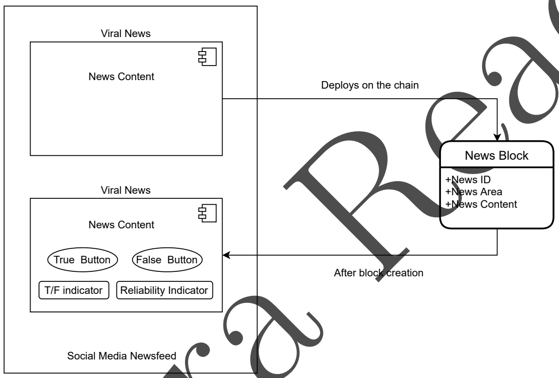

Fig. 3. Creation of news block

6.3 News validation:

The news validation process will start when a user(U_s) gives a reaction to the particular news. The True reaction will have a value of positive one(+1) and the false reaction will have a value of negative one(-1). The reaction block is generated with the user(U_s) hash, news id and the reaction value. To generate a final validation value(U_v) from a user towards a news, system needs to undergo some process.

6.3.1 Area value(A_v) generation:

An area value(A_v) will be generated from the area of the news(N_a) and the area of the verified user(U_a). If the area of any verified user is closest to any particular news, the area value(A_v) will be highest in that case. Figure 4 displays the process of generating the area value(A_v) of this system. As the distance between news and user increases, the area value(A_v) will be proportionally decreased. Thus, the nearest user will have the highest area value(A_v) and the farthest user will have the lowest area value(A_v). After generating the area value(A_v), it will be converted into a value between 1 to 100.

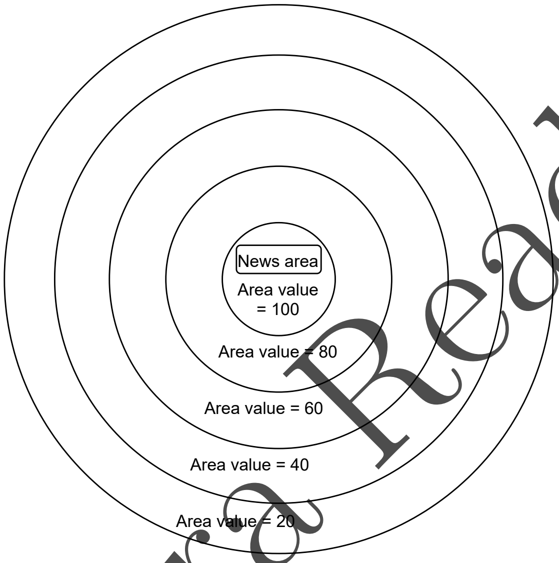

Fig. 4. Area value generation

6.3.2 Reliability weight(R_w) calculation:

Reliability weight(R_w) is very important in our validation process as it indicates, how much reliable is a user to validate a particular news on a scale of 1 to 100. Reliability weight(R_w) will be calculated based on area value(A_v), user rank(U_r), and reliability value(U_{rv}) of a user using the following formula.

$$R_w = \frac{A_v + (U_{rv} \times U_r)}{11}$$

We can see a user with a higher area value(A_v), higher rank(U_r), and higher reliability value(R_w) will generate higher reliability weight(R_w). Besides, user with lower values tends to generate a lower reliability weight(R_w).

6.3.3 Validation value(U_v) generation:

After reliability weight(R_w) generation, it will be multiplied with the reaction value(R_v) to generate the validation value(U_v) towards the particular news.

$$U_v = R_v \times R_w$$

As the true reaction will have a value of +1 and the false reaction will have a value of -1, therefore if a user gives a true reaction to a news(N_w) a positive validation value(U_v) will be added to that news(N_w), and if the user gives false reaction, a negative validation value(U_v) will be added to the news(N_w). User with higher reliability weight(R_w) will contribute a higher value(U_v) and user with lower reliability weight(R_w) will contribute a lower value(U_v) in both cases (Positive or Negative). Therefore, we can see when a user(U_s) gives a reaction to any news, a validation value(U_v) along with a reliability weight(R_w) will be generated and added separately to the news. These two value will contribute to achieve the two indicators(I_{tf} & I_r) which we have mentioned earlier.

6.3.4 True/False indicator(I_{tf}):

Each time a user(U_s) gives a reaction, our system will calculate the sum of all previous user validation value(U_v) of that news(N_w) along with the value generated from that user to generate the news validation value(N_v). That means, if n number of users(U_s) have given reaction to that particular news(N_w), the news validation value(N_v) for that particular news(N_w) will be as follows,

$$N_v = \sum_{k=1}^{n} (V_v)_k$$

If the summation returns a positive value, the indicator(I_{tf}) will show that the news is true, and if it returns a negative value the indicator(I_{tf}) will show that the news is false. On the other hand, summation might also return a zero. In that case, the indicator(I_{tf}) will show that the validation is undefined.

$$I_{tf} = f(N_v) = \begin{cases} \textbf{True,} & N_v > 0 \\ \textbf{False,} & N_v < 0 \\ \textbf{Undefined,} & N_v = 0 \end{cases}$$

6.3.5 Reliability indicator(I_r):

As we have mentioned earlier, there will be an another indicator(I_r) under the news to show the reliability percentage of the True/False indicator. To do so, we need to first calculate the reliability percentage(R_p) of that particular news. Reliability percentage(R_p) will be calculated using the mean reliability weight(R_w) added to that news. As the reliability weight(R_w) is generated on a scale of 1-100, the mean value itself will be the reliability percentage(R_p). That means, if n number of users have given reaction to that particular news, the reliability percentage(R_p) of the True/False indicator(I_{tf}) of that particular news(N_w) will be as follows,

$$R_p = \frac{\sum_{k=1}^{n} (R_w)_k}{n}$$

Here, we can see if any news(N_w) gets reactions mostly from the users(U_s) of higher reliability, the reliability indicator(I_r) will show a higher value. Besides, if the news(N_w) gets most of its reaction from the users(U_s) of lower reliability, the indicator(I_r) will show a lower value.

6.4 User(U_s) evaluation:

To make our system more reliable, our system needs to evaluate each user continuously. Through continuous evaluation, rank(U_r) and reliability value(U_{rv}) of a user can be increased or decreased.

6.4.1 Reliability value(U_{rv}):

Each time a user(U_s) gives a reaction to any news(N_w), the system will update the news validation value(N_v) for that particular news(N_w) and will start the evaluation process. Our system will compare the news validation value(N_v) with all the users validation value(U_v) added on that news. If the sign(+/-) of these two value don't match for a particular user, his(U_s) reliability value(U_{rv}) will be decreased. Besides, if the sign of these two values match, the reliability value(U_{rv}) of that particular user(U_s) will be increased. The system will skip evaluation process if the news validation value(N_v) is zero.

$$U_{rv} = f(U_v) = \begin{cases} \textbf{Increments,} & \frac{U_v}{|U_v|} = \frac{N_v}{|N_v|} \\ \textbf{Decrements,} & \frac{U_v}{|U_v|} \neq \frac{N_v}{|N_v|} \\ \textbf{No change,} & N_v = 0 \end{cases}$$

6.4.2 Rank(U_r):

As we have stated earlier, a user will have a rank between 1 to 10 where 1 will be the lowest rank and 10 will be the highest. In each rank, the reliability value(U_{rv}) will be between 50-100. That means the lower reliability limit(L_l) will be 50 and the upper reliability limit(L_u) will be 100. If Reliability value(U_{rv}) of any user decreased lower than the lower reliable limit(L_l), his rank(U_r) will be downgraded. On the other hand, if his reliability value(U_{rv}) increased higher than the upper reliable limit(L_u), his rank(U_r) will be upgraded.

$$U_r = f(U_{rv}) = \begin{cases} \textbf{Upgrade,} & U_{rv} > L_u \\ \textbf{Downgrade,} & U_{rv} < L_l \end{cases}$$

In the continuous evaluation, if the rank of a user is downgraded to 0, then that user will be removed from our system as a validator.

7 Protocol analysis

In this section, our protocols are described in terms of security parameters.

- **Anonymity:** Our system provides anonymity by generating the hash for each validator. As an unique hash address will be used to identify and track each validator, the real identity of each validator will remain hidden in our system. Thus the validators can validate any information anonymously without any influences. Moreover, users who are connected with our system are not capable to identify any user(U_s) during interaction with our system or blockchain transaction which provides pseudonymity too.
- **Data integrity:** Data integrity of our system is ensured by storing data transaction records in the blockchain. When a user(U_s) gives any reaction on a particular news(N_w) a validation value(U_v) will be generated through some process. This validation value(U_v) can not be altered when it once stores into the blockchain.
- **Privacy:** Privacy is provided by keeping the validator's information confidential as validator block contains an unique hash. Moreover, the code is immutable once it gets deployed, and all the data blocks are encrypted which makes the system more secure.
- **Reliability:** Our system ensures the reliability by maintaining the weighting factors and the reliability indicator. The reliability weight(R_w) plays an important role in our validation process as a user's reliability to validate a particular news depends on it. Besides, there will be a reliability indicator(I_r) under the news(N_w) which shows the reliability percentage of the True/False indicator.

8 Experimental analysis

We simulate our proposed system in this section to evaluate the feasibility through graph and proper description.

Experimental setup: To evaluate the effectiveness and performance efficiency of our proposed system, we setup an environment using the following configurations:

- Intel(R) Core(TM) i5-7200U 2.50GHz
- 8.00GB of RAM, Windows 10 (64-bit) OS

In our evaluation, we have written the programs using languages: Solidity, Web3.js, HTML and CSS. Software: atom, browser, Remix-Ethereum IDE to write the smart contract using solidity language to form a simulated Ethereum network locally. Wi-Fi connection is required in the setup.

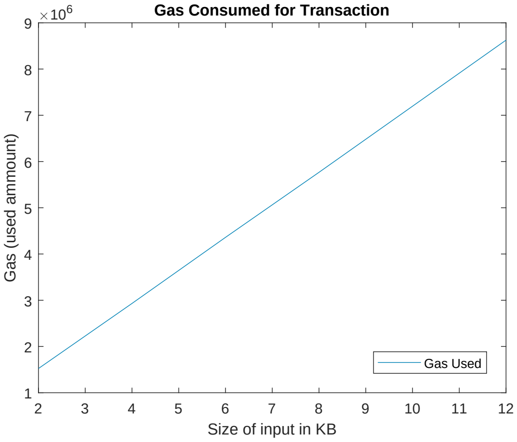

Fig. 5. Gas used for transaction in blockchain

8.1 Gas used for transaction in blockchain

The amount of computational effort required to perform any operations in the Ethereum blockchain network is referred to as Gas. Here, we've calculated the amount of Gas used to complete transactions with different data sizes for our system. Figure 5 depicts the trends of gas used for each transaction occurs in our proposed system. In order to analyze the consumption of Gas of different size of data, we have taken 2 to 12KB of data. In the resulting graph, we find that with the increase size of input data, Gas increases. As a result, the graph shows a linear trend.

8.2 Transaction time

Here, we have observed the transaction time taken in seconds to complete the transaction of varying data sizes of our proposed system. The time required to complete any transaction in blockchain is considered as transaction time. Our system's transactions show the tends in figure 6 with regards to time. Initially the transaction time increases from 2KB to 4KB data and then suddenly starts decreasing with the data from 4KB to 8KB. We notice that transaction time again starts increasing with the increase of data sizes from 8KB. From the resultant graph, the highest transaction time was found for 4KB data due to inconsistencies in the testing environment.

9 Conclusion

In our proposed method, we tried our best to utilize the core benefits of Blockchain technology (immutability, decentralization, security, ease of use) to

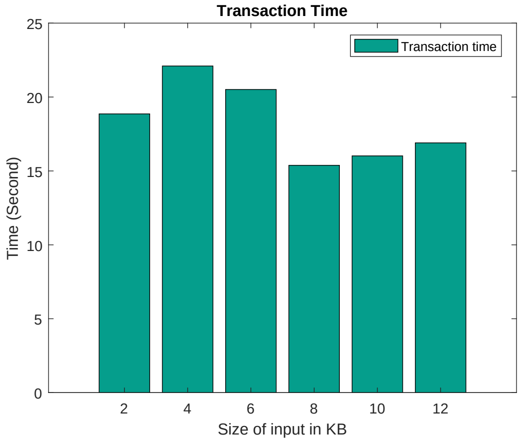

Fig. 6. Blockchain transaction time

reduce the widespread of fake news in social media. As fake news in social media often mislead people and turn them against each other and often result in violent incidents, it is a concerning issue. Individuals or organizations often deceive people by propagating fake or misleading information to gather profits. Hackers often propagate fake or misleading information over social media and convince a gullible user to click on harmful links or install harmful programs in their system and stole their personal data. Moreover, in a traditional validation system, users might not validate news freely because of the pressure created by some influential organizations. To address the problems, we proposed a location-aware blockchain based solution to reduce fake news in social media platform. In our system, any verified user of a particular social media platform can play the validator role for a particular news. Whenever a user validates a news which got viral in social media platform using our reaction button, our system starts generating the validation value of that news through some process. We introduced two indicators which will indicate whether the news is true or false after going through some evaluations. There may be some limitations. Being biased, some or a major portion of the validators may validate a fake news as real one during validation. Yet we hope if we can integrate this system into mainstream social media, all or some of the issues can be reduced.

References

1. "Social Media And The Need To Believe", https://www.forbes.com/sites/petersuciu/2019/11/11/social-media-and-the-need-to-believe/
2. "More than eight-in-ten Americans get news from digital devices", https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/
3. "2012 Ramu violence", https://en.wikipedia.org/wiki/2012_Ramu_violence/

4. “Bangladesh rampage over Facebook Koran image”, https://www.bbc.com/news/world-asia-19780692
5. “24 Buddhist and Hindu temples burnt in Bangladesh - India and UN urged to intervene”, https://web.archive.org/web/20121004004231/http://www.achrweb.org/press/2012/IND08-2012.html
6. “Police-protesters clash in Bhola over hate spread through facebook id: 4 Killed, 100 Injured”, https://www.thedailystar.net/frontpage/clash-in-bhola-4-killed-100-injured-1816540
7. “Children being sacrificed, heads used for bridge project: Social media rumour sparks spate of Bangladesh lynchings”, https://www.straitstimes.com/asia/south-asia/children-being-sacrificed-heads-used-for-bridge-project-social-media-rumour-sparks
8. “Padma Bridge”, https://en.wikipedia.org/wiki/Padma_Bridge
9. “Bangladesh: Fake news on Facebook fuels communal violence”, https://www.dw.com/en/bangladesh-fake-news-on-facebook-fuels-communal-violence/a-51083787
10. S. B. Naeem, R. Bhatti and A. Khan: “An exploration of how fake news is taking over social media and putting public health at risk”. In: *Health Information & Libraries Journal*, https://doi.org/10.1111/hir.12320
11. “Iran: Over 700 dead after drinking alcohol to cure coronavirus”, https://www.aljazeera.com/news/2020/4/27/iran-over-700-dead-after-drinking-alcohol-to-cure-coronavirus
12. “A syndemic of COVID-19 and methanol poisoning in Iran: Time for Iran to consider alcohol use as a public health challenge?”, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7272173/
13. W. J. Tee and R. K. Murugesan: “Trust Network, Blockchain and Evolution in Social Media to Build Trust and Prevent Fake News”. In: *2018, Fourth International Conference on Advances in Computing, Communication Automation (ICACCA)*, pp.1–6, https://doi.org/10.1109/ICACCAF.2018.8776822
14. W. J. Tee and R. K. Murugesan: “A Theoretical Framework to Build Trust and Prevent Fake News in Social Media Using Blockchain”. In: *2019, Recent Trends in Data Science and Soft Computing*, vol. 843, pp. 955–962, Springer(2019), https://doi.org/10.1007/978-3-319-99007-1_88
15. A. Qayyum, J. Qadir, M. Janjua and F. S. Vira: “Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News”. In: *2019, IT Professional*, LNCS, vol. 21, pp. 16–24, https://doi.org/10.1109/MITP.2019.2910503
16. I. S. Ochôa, G. Mello, L. Silva, A. Gomes, A. Fernandes and V. Leithardt: “FakeChain: A Blockchain Architecture to Ensure Trust in Social Media Networks”, In: *2019, Quality of Information and Communications Technology*, pp. 105–118. Springer (2019), https://doi.org/10.1007/978-3-030-29238-6_8
17. S. Paul, J. Joy, S. Sarker, A. Shakib, S. Ahmed and A. Das: “Fake News Detection in Social Media using Blockchain”, In: *2019, 7th International Conference on Smart Computing Communications (ICSCC)*, pp. 1–5, https://doi.org/10.1109/ICSCC.2019.8843597
18. Al Omar, Abdullah, et al. ”Towards A Transparent and Privacy-preserving Healthcare Platform with Blockchain for Smart Cities.” In: *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2020.*
19. M. L. D. Vedova, E. Tacchini, S. Moret, G. Ballarin, M. DiPierro, and L. D. Alfaro: “Automatic Online Fake News Detection Combining Content and Social Signals”, In: *2018, 22nd Conference of Open Innovations Association (FRUCT)*, pp.272–279, https://doi.org/10.23919/FRUCT.2018.8468301

20. M. Granik and V. Mesyura: "Fake news detection using naive Bayes classifier", In: *2017, IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, pp. 900–903, https://doi.org/10.1109/UKRCON.2017.8100379
21. J. C. S. Reis, A. Correia, F. Murai, A. Veloso and F. Benevenuto: "Supervised Learning for Fake News Detection", In: *2019, IEEE Intelligent Systems*, vol. 34, no. 2, pp. 76-81, https://doi.org/10.1109/MIS.2019.2899143.
22. Al Omar, Abdullah, et al. "A Transparent and Privacy-Preserving Healthcare Platform With Novel Smart Contract for Smart Cities." In: *IEEE Access 9 (2021)*, https://doi.org/90738-90749
23. Bosri, R., Rahman, M. S., et al. "Integrating Blockchain With Artificial Intelligence for Privacy-Preserving Recommender Systems" In: *IEEE Transactions on Network Science and Engineering (2020)*, https://doi.org/10.1109/TNSE.2020.3031179
24. Al Omar, Abdullah, et al. "Towards Privacy-preserving Recommender System with Blockchains" In: *International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications. Springer, Singapore, 2019*, https://doi.org/10.1007/978-981-15-1304-6_9
25. Bosri, R., Uzzal, A. R., et al. "HIDEchain: A User-Centric Secure Edge Computing Architecture for Healthcare IoT Devices" In: *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162729
26. Bosri, R., Uzzal, A. R., et al. "Towards a Privacy-Preserving Voting System Through Blockchain Technologies" In: *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp. 602-608. IEEE, 2019.*, https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00116