

# Design of Realtime Fake News Detection using Blockchain

Yash Ghodake<sup>1</sup>, Mayur Dhanawade<sup>2</sup>, Pratik Patil<sup>3</sup>, Dhanashri Deore<sup>4</sup>

<sup>1</sup>UG. Student, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India

<sup>2</sup>UG. Student, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India

<sup>3</sup>UG. Student, Sandip Institute of Technology and Research Centre Nashik, Maharashtra, India

<sup>4</sup>UG. Student, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India

**Abstract** - Social Networking is one of the important outlets for exchanging news between social groups. Using social media, not only real news but also rumors and fake news are spread on a wide scale. This may have serious adverse effects on society.

Blockchain is used to limit the spread of rumors, to overcome this problem. The proposed system tracks and analyzes the news that is shared, thus restricting where it is fake or user-manipulated. The system also proposes a real-time alert panel that aims to find out the reality of the news by taking user's votes. The news status is constantly tracked and then eventually modified once the threshold value is reached. The fake word data set can be used to spot misleading terms and prevent the fake news.

**Key Words:** Block Chain, Rumour Transmission patterns, Security, Decentralize technology.

## 1. INTRODUCTION

The social media has been the most successful information-sharing site in recent years. As the amount of information increases, reading the right news becomes more important, and detecting fake news that provides inaccurate information and lack of accuracy becomes more necessary [3]. It takes long time if people try to verify the truthfulness of news. In fake news, users with malicious intent spread false information by altering content of a genuine news feed.

To encounter this problem, it is necessary to use decentralize technology. Such capability is readily available in blockchain technology. Blockchain can be used to track and control the information flow. We use trusted news outlets such as Times Now news website in our model. Blockchain technology maintains the credibility of such news as people post news in social media. In the real-time alert panel, users can post news to receive feedback from other users and trusted sources. This approach helps to assess the truthfulness of the news with real-time synchronization. Fake word data set helps identify trends of spam in news.

## 2. Rumor Iterative Spreading Process

To detect fake news the dynamics of rumor spreading need to be understand. In the typical SIR model [4] people have to immediately judge the rumor and determine whether or not

to spread it. Nevertheless, it is hard to easily draw decision and right choice without careful analysis. There's no time for people to gather more information or do reasoning. Additionally, once the rumor resists, the user becomes stiffer and never changes. Facing the same event, people may have distinct opinions i.e. positive, dubious and negative [5] [6]. However, the people with dubious opinions have few descriptions.

The dubious state represents those who keep suspecting the rumor and decide to not spread it until having received more information about it. The rumor may be disappointed here, while it could success deceiving other people who may be a friend of the dubious. Therefore, the dubious will receive the rumor again from other friends. On the contrary, the spreaders (both the malicious and the deceived) want to share and exchange the topic about the rumor and make more people to believe the rumor and to be active to spread it. When founded that someone would not accept the rumor, more friends would be sponsored to persuade him. In this way, the dubious would be shaken and possibly turned to convince the rumor and began to spread it as spreaders when an increasing number of people told them about the rumor.

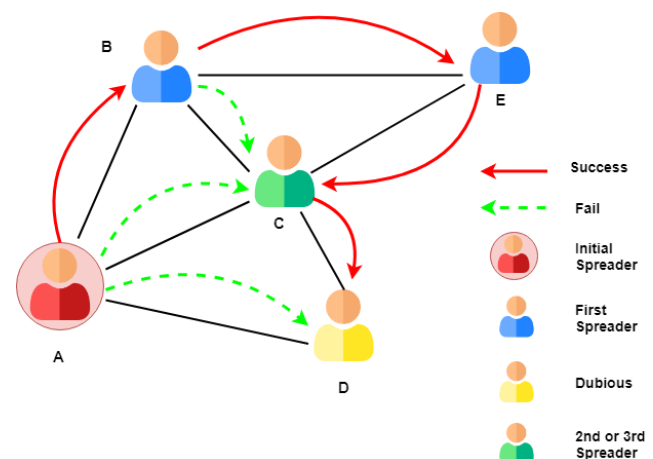


Fig -1: Rumor Iterative Spreading Process

As shown in Fig. 1, a malicious user A initiated a rumor spreading [1]. User B, C and D received the rumor, but user C and D didn't believe it at first time. However, user B became a spreader and spread this rumor to his friends C and E. User C ignored it again, but user E turned to spread it to C the third time. User C had heard the rumor three times and was persuaded to become a spreader at last. Then user C spread

this rumor to D, user D received this rumor twice and became a spreader. Finally, every user was a spreader, where user B and E became spreaders at first time, user D and E became spreaders at twice and three times respectively.

### 3. Blockchain

Block chain is a chain where several blocks are connected together block forming a logical chain. Block-chain is a distributed, decentralized network that conducts peer-to-peer transactions, meaning that it does not have a main or central entity to operate. No third-party system is required for the transaction to take place within the nodes or peers themselves.

Block-chain operates by connecting new blocks to existing blocks, and the chain continues. A gossip protocol is executed when inserting a new transaction or blocking which validates the new block. A node must be checked across several blocks or nodes. Upon validation of the node, it is connected to the block chain.

### 4. Distributed vs Centralize Architecture

Centralized software systems [7], the components are located around and connected with one central component. In contrast, the components of distributed systems form a network of connected components without having any central element of coordination or control.

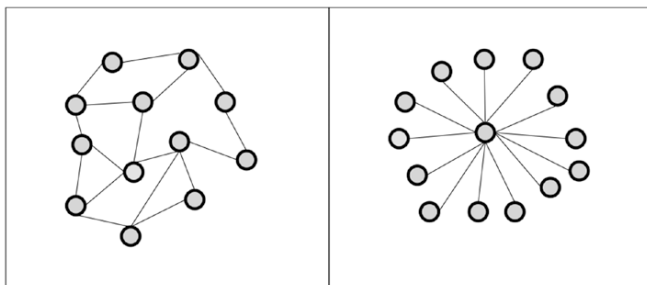


Fig -2: Distributed (left) vs. centralized (right) system architecture

Figure 2 depicts these two contrary architectures. The circles in the figure represent system components, also called nodes, and the lines represent connections between them. The right-hand side of Figure 2 illustrates a decentralized architecture. It is important to see that none of the components is directly connected with all other components. However, all components are connected with one another at least indirectly. The right-hand side of Figure 2 illustrates a centralized architecture where each component is connected to one central component. The components are not connected with one another directly. They only have one direct connection to the central component.

### 5. Detection of Fake News.

Our program includes trustworthy information sources, social media platform and users. News publishers such as CNN, Times Now and BBC media groups can be reliable sources of information. We use Times Now publishers in our case which can be considered as trusted information source. We can use social media sites such as Instagram, Facebook and Twitter. For ease of purpose we built our own social media platform where user can post news. Users are the ones who can exchange information on social media platform. Here we have reduced the number of users to system more efficient.

To detect fake news, it is important to identify the malicious entities in information propagation over social network. First news is published by the Times Now and posted on their website. As shown in fig 3, A, B, C, D, E and F are the social network users. B obtains news from Times Now website and shares with A and C through social media platform. As A is malicious user, manipulates information and forwards it to D.

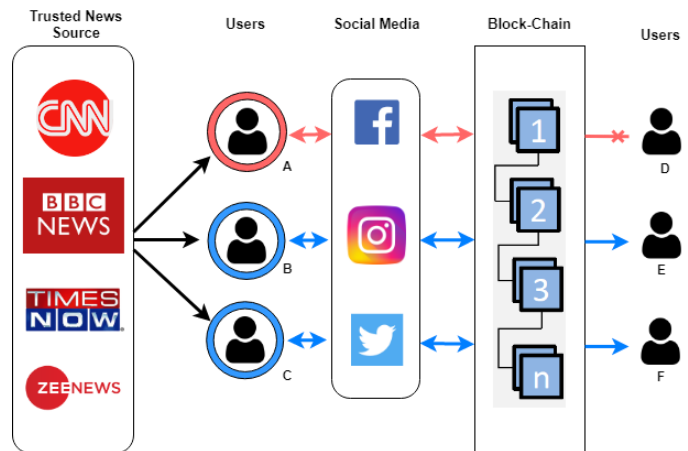


Fig -3: Detection of fake news and malicious user. Thus, preventing spread of fake news.

Here blockchain plays important role. Blockchains involves a ledger maintained by each entity, including every user on a social network. When news is generated, each entity is required to validate its authenticity.

When user manipulates the information, the hash key generated by the blockchain gets changed. Thus, it blocks the news before it is shared on social media platform. Moreover, if a tries to spread fake news more than three times, system will block the account of user A.

## 6. Real Time Alert Panel

To verify the live news content that is not yet published by reputable news outlets, more details and feedback from different users is required [9].

RTAP (Real Time Alert Panel), fig 4, is designed to collect live feedback from users about live news posted in panel. Status of the news is updated dynamically by the system. Users can post the live news to get input from other users on social media sites, as shown in the figure. There are three states of news true, false and pending. The initial news status is 'pending' by default. As the vote count exceeds the threshold value the news status turns to 'true, news otherwise it becomes 'fake'.

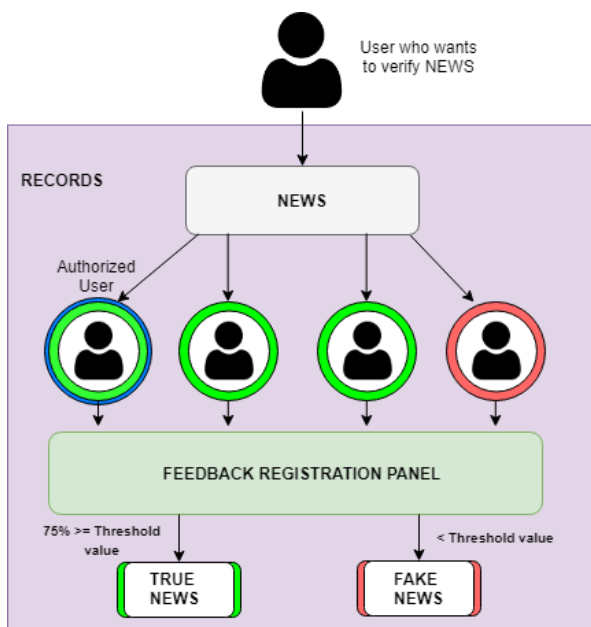


Fig -4: Architecture of RTAP

## 7. Fake Keyword Data Set

Fake news and spams have similar properties [2] such as:

1. They are often emotionally coloured.
2. They often try to affect reader's opinion on some topics in manipulative way.
3. They often use similar limited set of words.

So, one can see, that fake news articles and spam messages indeed share a lot of important properties. Therefore, it makes sense to use similar approaches for spam filtering and fake news detection. Hence use of fake keyword dataset can be found more useful.

Here we have used fake news dataset consisting of words which are common fake words used in fake web-based news. Such databases have a high probability of removing plenty of false news. Our program's first step is to eliminate all stop words [8] through stemming and conflation and we are left

with multiple-word plain text now. Fake dataset recognizes the fake keywords by analysing each plain text. Here we have used Boyer-Moore algorithm to make process of pattern matching effectively. Fake word dataset is an efficient way to minimize the spread of fake news and to apply additional filters to the information to make it more reliable to verify whether it is fake or not.

## 8. Future Scope

As the social media expands, it also enables information to be shared in different forms, such as images and audio. Given that our system focuses only on text-based content, methods for detecting fake images as well as audio need to be researched and detected. The Real Time Alert Panel system works fine until the users are honest with their votes. By finding new methods, more security can be achieved.

## 9. CONCLUSION

A new system is proposed to detect and avoid further spreading of fake news and validate the information from origin. The proposed systems make use of block-chain technology for verifying the source and content of the news. Using blockchain makes it secure and efficient as it identifies the user's malicious intent and hence prevents it from spreading fake news. This prevents the iterative spreading of fake news. RTPA (Real Time Alert Panel) keeps track of the live news and constantly updates news status. Fake dataset helps to identify fake nature of the news.

## REFERENCES

- [1] Q. Han, F. Miao and L. You, "Rumor Spreading Model Considering Iterative Spread on Social Networks," 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, 2018, pp. 1363-1367.
- [2] M. Granik and V. Mesyura, "Fake news detection using naive Bayes classifier," 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), Kiev, 2017, pp. 900-903.
- [3] E. Kiely and L. Robertson, "How to Spot Fake News - FactCheck.org", FactCheck.org, 2016. [Online]. Available: <https://www.factcheck.org/2016/11/how-to-spot-fake-news/>. [Accessed: 19- Apr- 2020].
- [4] Daley D J, Kendall D G. Epidemics and rumors. Nature, 1964, 204(4963):1118-1118.
- [5] Daley D J, Kendal D G. Stochastic rumors. J. Inst. Math., Appl.1, 1965.
- [6] Daley D J, Gani J. Epidemic Modelling. Cambridge University Press, Cambridge, UK, 2000

[7] Imran Bashir Mastering Blockchain Second Edition, Packt Publishing, Birmingham, UK, 2018.

[8] Wikipedia contributors. (2020, April 16). Stop words. In Wikipedia, The Free Encyclopedia. Retrieved 14:20, April 19, 2020, from [https://en.wikipedia.org/w/index.php?title=Stop\\_words&oldid=951205436](https://en.wikipedia.org/w/index.php?title=Stop_words&oldid=951205436)

[9] M. Granik and V. Mesyura, "Fake news detection using naive Bayes classifier," 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), Kiev, 2017, pp. 900-903.