A Survey on Fake News Detection Techniques and using a Blockchain based System to Combat Fake News

Akshada Babar  
Department of Computer Science  
Dr.D.Y.Patil Institute of Engineering, Management and Research

Nalini Jagtap  
Assistant Professor  
Department of Computer Science  
Dr.D.Y.Patil Institute of Engineering, Management and Research

Akshata Mithari  
Department of Computer Science  
Dr.D.Y.Patil Institute of Engineering, Management and Research

Aakash Shukla  
Department of Computer Science  
Dr.D.Y.Patil Institute of Engineering, Management and Research

Prachi Chaudhari  
Department of Computer Science  
Dr.D.Y.Patil Institute of Engineering, Management and Research

ABSTRACT
The problem of fake news is getting serious day by day and it has very detrimental impacts in different spheres like that of politics. Due to the availability of social media, it becomes very easy to spread fake news and it becomes difficult to identify the culprit. As the culprit of such actions is not identified, the problem still persists. Hence, there is a need to identify the source or origin of such fake news to take the necessary action. There are several methods to detect fake news but the common people rarely have time to use these detection techniques and they easily fall prey to such pieces of information. In this paper, we review the different methods that are applied to detect fake news and address it's limitations. We propose the flow of a new blockchain based system that can be used by the news agencies to ensure the validity of the news published. With the help of such a system, the news will be entirely traceable and trackable to every single point in the agency and hence, it becomes easy to find the source and identify the culprit in case of any misinformation.

General Terms
Ethereum, Truffle, News Tracing System.

Keywords
Blockchain, Fake News, Fake News Detection using blockchain, Blockchain to curb fake news.

1. INTRODUCTION
The problem of identifying fake news is difficult to tackle because of the dubious nature of the term “fake news”. There are different definitions of the term “fake news”. Fake news can be determined as the news that aims to deceive people by spreading pieces of information that are not true, partially true or represented in such a way so as to create misinformation. There are different types of fake news as explained in [1]. The intention of spreading these types of information can be unknown, maybe the aim is political and financial gain or the aim is to create a parody for entertainment. There are numerous algorithms available to detect fake news but it is very difficult to identify the source or origin of these news articles. Hence, leaving the culprit free. The availability of social media and free access of the public to social media has led to the increase in this problem. Everyone can access the media and hence, the spread of fake news is fast leading to more victims and also as anyone can post on social media, the amount of fake news is increasing at a faster rate. There are some serious effects of the spread of such news. One such example of this long-lasting problem is the pizzagate conspiracy. In the pizzagate conspiracy [2], the fake news, which claimed that many pizza places in Washington DC are the members of a child sex ring that involved Hilary Clinton [2], was spread. This news was retweeted by many of the opponents of Hilary Clinton and clearly it misguided the public and created a problem for the pizza places [2]. One of the accused pizza places called COMET was a victim of these false allegations, as they had to go through severe threat calls and mails [2]. Also, a man from Washington arrived at the place armed with two guns threatening to kill the owner [2]. Although no one got hurt, this can be an example as to how exaggerated a small mislead can become and the victims might face severe consequences [1]. Similar to these, there are many other cases where the spread of fake news leads to some severe problems and now the world has recognised the need to have an efficient solution to this problem. The primary aim of this paper is to review the literature regarding the different techniques and models for fake news detection. Furthermore, we identify its limitations and propose a new model for combating the fake news problem by effectively tracking and tracing the news using blockchain technology. We believe that if the origin of this type of fake news is identified then the necessary actions can be taken on the source and gradually the problem will be solved. Our entire proposed system is inspired by the blog written by [3].

2. LITERATURE SURVEY
There are a number of techniques that have been used to detect the fake news. Some of the techniques that we studied are as follows:

1) Fake News Detection using a Deep Neural Network [4]  
Author: Rohit Kumar Kaliygar

Theory: In this paper the author uses the technologies like machine learning, deep learning and Natural Language
Processing to develop an application that will determine whether the news is fake news or legitimate. This is the most popular model that we came across during the research. He uses the collection of different datasets from Kaggle, the dataset contains both fake and real news.

The author uses different classification models to test the accuracy of the neural network. He uses the Naive Bayes Model, CNN as a classifier model. Also he uses decision trees, Random forest and K-nearest neighbours for testing the accuracy. The accuracy of the model under different conditions was as follows:

1) When CNN was used the model was accurate up to 98% [4].
2) When CNN along with the combination of LTSM was used, the model accuracy was 97.3% [4].
3) For the Naive Bayes model, the precision was 90% [4].
4) When the Decision Tree Regressor was used to classify, the accuracy was reduced to 73% [4].
5) With Random forest Regressor, the accuracy was 72% [4].
6) For the k-nearest neighbour method, the precision was 50% [4].

Hence, the user has explored different Machine Learning models to test the accuracy of the model used to detect fake news [4].

2) Fake News Accuracy using Naive Bayes Classifier [5]: Author: R.J. Poovaraghan, M.V. Keerti Priya, P.V. Sai Surya Vamsi, Mansi Mewara, Sowmya Loganathan

Theory: In this paper the author has described a classification model using the Naive Bayes model to determine the accuracy of the given fake news.

The model works in the following steps:

1) The data is collected from different sources and combined to make a dataset.
2) The dataset is divided into training data and test data.
3) After splitting the data into two, the training data is classified into different groups due to its training.
4) Different vectors are used to keep count of different words and the number of times they appear in the data, the weight is given accordingly and hence, only the most important words are considered.
5) The Naive Bayes algorithm is used to classify the test data into the different groups of the training data to check their accuracy.
6) Hence, whenever the accuracy of the fake news is to be checked, the model can be used to compare it with the previous data and determine its accuracy.

This is the most popular way of detecting the fake news or for classification of news.

3) Fake News on Social Media: A Brief Review on Detection Techniques [10]:

Author: Zaitul Iradah Mahid, Selvakumar Manickam Shankar Karuppayah

Theory: In this paper, the author describes the different methods followed by the different models used to detect fake news. He has classified the models’ approaches into different groups mainly:

1) Content based: Here, the model depends on the type of words that are used in the news to determine whether it is fake or legitimate [10].
2) Knowledge-based: Here the model uses a fact checking mechanism to detect whether the news is fake or not. It highly depends on the human experts to determine the authenticity of the news [10].
3) Hybrid-Models: These models use a combination of content-based and knowledge-based approaches to determine the authenticity of the news [10].

Hence, the paper provides an effective review about the different techniques used to detect the fake news. Also, we get a broad classification of the detection techniques.

4) Fake News: A survey of Research, Detection Methods and Opportunities [11]:

Author: Xinyi Zhou, Reza Zafarani

Theory: In this paper the author describes the different types and the effects of fake news. After describing the different types of fake news, he goes on describing the different techniques used to detect fake news. Below is a short summary of the different techniques used for classification:

1) Knowledge based detection [11]: In this category of detection, the main criteria to classify a news as false or true is fact checking. Fact checking is used to determine the authenticity of the news. Fact checking is of two types, expert based fact checking or crowd sourced fact checking. In expert based fact checking, the fact checking machines are operated that go through thousands of facts to generate the results and compare the given piece of information with the already established facts. Whereas in crowd-sourced checking, the users determine whether the article is true or false by rating the phrases used in the article, the article with the best description gets the highest rate. Although, has good accuracy, this type of classification is based on the expert opinions. The working of Knowledge based detection is as follows:

Fact extraction and Fact checking [11]- First the knowledge is extracted from the open web as raw facts and then a knowledge base is formed, further there is a fact checking process where the news article to be classified is compared with the knowledge base to give a result.

2) Style Based Detection [11]: In style based detection model, different deception theories are used to understand how deception techniques work. Basically in this model, different deceptive keywords or phrases are analyzed depending upon highly researched deception techniques and then the probability of the article being deceptive is determined. Unlike the knowledge based technique which was used to find out the authenticity of the fake news, the style based detection technique is used to find the intention of the news, i.e. whether it is deceptive or not.

3) Propagation based deception [11]: According to research conducted by [Vosoughi et al. 2018], there are some patterns through which we can conclude that the spread of fake news is faster compared to the propagation of true news. These propagation patterns of the news can be effectively used to develop models that can help detect the authenticity of news. The propagation patterns are classified and identified and then they are linked to the different types of news.

4) Credibility based news detection [11]: According to
[Silverman 2016], all the fake news in the BuzzFeed resulted from an unreliable source. There is a high chance that the news resulting from an unreliable person or an unreliable source is a fake news. Hence, we can simply identify the fake news depending upon the source of the news. The models deal with finding the source of the news and then classifying it as fake or authentic. Sometimes clickbaitsn are used to attract user attention but the news might be fake, the news that has a clickbait is generally considered to be unreliable. Hence, the paper provides a brief classification and summary of the wide amount of techniques used for classification.

Table -1: A brief Literature Review.

| Name of the paper | Technique/Domain | A Brief Description | Advantages | Limitations |
|--------------------|------------------|---------------------|------------|-------------|
| **Broad Classification Type: Knowledge-Based Detection Model** |
| 1) Fake news detection using deep neural networks[4]. | Machine Learning, Deep Learning, NLP | Algorithms used: 1)Naive Bayes. 2)CNN Classifier 3) Long Short Term Memory 4) CNN + LSTM | 1)Accuracy for the CNN classifier along with LSTM was the highest i.e. 97.3% 2) Works effectively for different datasets. | 1) Can not identify the source of fake news and hence, is not an effective solution to the problem. 2) The accuracy needs to be increased. |
| **Year**: 2019 |
| 2) Fake News Accuracy using Naive Bayes Classifier[5]. | Machine Learning, Deep Learning, Natural Language Processing | Algorithm used: Naive Bayes. Every word is given a certain weight and depending on the weight only the most important word is used for classification. | 1) News can be accurately distinguished into fake and real news. 2) Can not detect the source of the fake news, hence, is not an effective solution to the problem. | 1) It performs detection based on content and not on the news sources |
| **Authors**: R.J. Poovaragh an, M.V. Keerti Priya, P.V. Sai Surya Vamsi, Mansi Mewara, Sowmya Loganathan |

| **Broad Classification Type: Content-Based Detection Model** |
| **Algorithm used**: 1) KNN algorithm Techniques used: Bag of words model | System predicts the tweet/news to be fake with an accuracy of 66.66% |
| 1) Fake News Pattern Recognition using Linguistic Analysis[6]. | Machine Learning |
| **Author**: Amitabha Dey, Rafsan Zani Rafi, Shahriar Hasan Parash, Sauvik Kundu Arko and Amitabh Chakrabarty |
| **Year**: 2018 |
| 2) FAMOUS: Fake News Detection Model based on Unified Key Sentence Information [7]. | Natural language processing |
| **Authors**: Namwon Kim, Deokjin Seo Nuna, Chang-Sung Jeong. |
| **Year**: March 2019 |
| 1) It performs sentence matching between question and article by using key sentence retrieval based on (BiMPM) model which provides better performance for sentence matching by using two directional bidirectional long short term memory. 2) It uses NLP techniques based on deep learning for fake news detection to overcome analysis of complicated sentences, and not reflect contextual information. | 1) It has some limitations for sentence matching in Korean due to different morphological features of Korean language 2) It has some difficulty in finding the contextual relation between two sentences too much apart in the article |
| Broad Classification Type | Credibility Based Detection Model | Base Paper | Review Papers |
|---------------------------|----------------------------------|------------|---------------|
| 1) Using Blockchain to Rein in the New Post-Truth World and check the spread of Fake News [8]. | **Blockhain** | Authors: Adnan Qayyum, Junaid Qadir, Muhammad Umar Janjua, and Falak Sher  
Year: 28 March 2019 | **Blockhain** | Authors: Khaled Salah, Nishara Nizamuddin, Raja Jayaraman, and Mohamma d Omar  
Year: 18 June 2019 |
| The application makes use of Digital signatures and hash codes to ensure the validity of the blocks. Blocks are connected using hashpointers. Hence, it becomes easy to trace the origin of the news publisher.  
1) This system will eliminate the need for a mediator like central trust infrastructure.  
2) The transparency of the blockchain will be helpful in curbing the fake news problem.  
3) Effective use of evolvable reputation set is done to maintain the status of the publisher. | **Survey Paper** | Survey Paper  
Broadly Classified the detection techniques into the following types:  
1) Knowledge-based  
2) Content-based  
3) Hybrid Models | **Review Paper**  
Broadly Classified the detection techniques into the following types:  
1) Knowledge-based  
2) Content-based  
3) Hybrid Models | **Review Paper**  
Provides a broad classification of the detection techniques. |
2) Fake News: A survey of Research, detection Methods and Opportunities [11].

**Author:** Xinyi Zhou, Reza Zafarani

**Year:** 2 December 2018

Classification of the detection techniques in the following types:

1) Knowledge based
2) Style based
3) Propagation based
4) Credibility

A detailed classification of the detection techniques is provided.

3) Challenges and opportunities in Blockchain [12].

**Author:** Zibin Zheng, Hong-Ning Dai, Shaoan Xie, Xiangping Chen

**Year:** October 2018

The author gave the key characteristic of Blockchain

1) Decentralisation
2) Persistency
3) Anonymity
4) Auditability

Blockchain Categorised into three types:

1) Public blockchain
2) Private Blockchain
3) Consortium blockchain

The authors compares these from different perspectives

As blockchain is open to world wide many users attracted therefore

Hyperledger is developing the business and several companies in blockchain frameworks.

1) Advances on consensus algorithms.
2) Blockchain can potentially solve the problems of Academics and Web Community.

Also provides the application domain of blockchain and its help in current technology like IOT.

### 3. LIMITATIONS

The most popular model to detect the fake news was “The Naive Bayes Classifier [5]”, which has been implemented successfully. Although these detection techniques are very accurate, they are not a successful solution to combat fake news. The model can effectively detect whether the news is fake or not but after the news is classified as “Fake”, there are no steps taken to identify the source and eliminate it. The fake news can be stopped from propagating further but it can not be eradicated from its root because the Machine Learning Algorithms are incapable of identifying the source of the news. As the source of such news is not eradicated or as there is no action taken on such news providers, the problem of fake news still persists. Before publishing the news, it goes through various editing processes and there is a possibility that one of these editing processes is the source or cause of the fake news. If this source is identified and stopped then there is a possibility that only authentic news providers will exist and the news hence produced will be authentic. The Credibility based news detection model identifies the source as reliable or unreliable, based on these sources the news is further classified, hence, this model can be extended to further eliminate these unreliable sources of news.

### 4. PROPOSED MODEL

![Figure-1: Features of News tracking and Tracing System Using Blockchain](image)

We are proposing a blockchain based news tracking and tracing system through the integration of big data to curb the problem of fake news as inspired from [3]. Our system can be used by news agencies to trace the origin and find the culprit. The system will consist of four main entities:

1) News Agency [3]: Responsible for publishing the news or providing it to the audience.
2) Journalists [3]: Responsible for collecting the news.
3) Editors [3]: Responsible for editing the news to make it presentable.
4) Crowd Auditors [3]: Responsible for validating the news.

Each of these different entities will be connected through a blockchain which will make the news traceable. The system will work as follows:
1) The journalist will be responsible for creating the first block. The news collected by the journalist will be stored in this block along with the timestamp, hash value and the hash pointer. Timestamp is the time when the block is created. Hash value is the hash value of the block. Hash pointer is used to store the pointer to the next block in the chain.

2) The News Agency will contain the next block. This block will contain the data that is received from the journalist and passed to the editor.

3) The Editor will contain the next block, which will contain the data that was received from the News Agency. The editor can also backtrace to get the information about the journalist who provided this information to the agency.

5. CHALLENGES AND FUTURE SCOPE

We have several challenges that need to be resolved while building this system. The very first challenge is that of ensuring the hashpointer is calculated correctly. Due to the introduction of noise, the hash values can be altered and it will be difficult to verify the block if the hash value is invalid. The entire system should be built on a decentralized database and this is another challenge that needs to be resolved. The blockchain system used for cryptocurrencies cannot be used as it is, it needs to be changed to suit this project. In the future, this model can be integrated with Big Data to detect fake news and identify its origin. Let us consider a news agency, if the editor modifies the news sent by the journalist, there are two ways how the publishing of this news will be prevented:

1) The block will not be created for this modified news as the hash value will be modified and it will become invalid.

2) If the hash value is valid, then a new block will be added in the chain. Hence, the crowd auditor will be able to trace back to the origin of this news and he can verify if it is fake by considering the reliability of the source.
6. CONCLUSIONS
Overall, the system will help the News Agencies in maintaining a transparent and reliable system to track the news. The origin of the news can be identified easily. News will be validated before publishing. Hence, the problem of fake news will be solved. The system will be strong and hence, difficult to hack. This will keep the news secure and make sure that the information published is original. In the future, this application can be implemented using Hyperledger.

7. REFERENCES
[1] G. Kumar. “What is Fake News and its different types”. April 3, 2018. [Online]. Available: https://www.jagranjosh.com/general-knowledge/what-is-fake-news-and-its-different-types-1522761961-1

[2] Wikipedia. “The PizzaGate Conspiracy Theory” Available:https://en.wikipedia.org/wiki/Pizzagate_conspiracy_theory

[3] A. Takyar. “Blockchain in fake news - Transforming News Industry”. [Online] Available: https://www.leewayhertz.com/blockchain-fake-news/

[4] R. Kaliyar. “Fake News Detection using Deep Neural Network (ICCCA 2018)”. [Online]. Available: https://ieeexplore.ieee.org/document/8777343

[5] R. Poovaragham, M. Keerti Priya, P. Sai Surya Vamsi, M. Mewara, S. Loganathan. “Fake News accuracy using Naive Bayes Classifier (May 2019)”; [Online]. Available: https://www.ija.org/wpcontent/uploads/papers/v8i1C2/A11660581C219.pdf

[6] A. Dey, R Zani Rafi, S. Hasan Parash, S. Kundu Arko and A. Chakraborty. “Fake News Pattern Recognition using Linguistic Analysis”. 14 February 2019. [Online]. Available:https://ieeexplore.ieee.org/document/8641018/authors#authors

[7] N. Kim, D. S. Nuua, Chang-Sung Jeong. “FAMOUS: Fake News Detection Model based on Unified Key Sentence Information”. 11 March 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8663864

[8] Adnan Qayyum, Junaid Qadir, Muhammad Umar Janjua, and Falak Sher. “Using Blockchain to Rein in the New Post-Truth World and check the spread of Fake News”. 28 March 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8764081

[9] Khaled Salah, Nishara Nizamuddin, Raja Jayaraman, Mohammad Omar. “Blockchain based Soyabean Traceability in Agricultural Supply Chain”. 18 June 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8718621

[10] Zaitul Iradah Mahid, Selvakumar Manickam Shankar Karuppayah. “Fake news on social media: Review on detection techniques”. 29 July 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8776689.

[11] Xinyi Zhou, Reza Zafarani. “Fake News: A survey of Research, detection Methods and Opportunities”. 2 December 2018. [Online]. Available: https://arxiv.org/abs/1812.00315

[12] Zibin Zheng, Hong-Ning Dai, Shaoan Xie, Xiangping Chen. “Blockchain :Challenges and opportunities.” October 2018. [Online]. Available: https://www.researchgate.net/publication/328338366_Blockchain_challenges_and_opportunities_A_survey