

FAKE NEWS DETECTION IN SOCIAL MEDIA USING BLOCKCHAIN

KAUSTUBH KATKAR || 3147 0922
SANTOSH KANNAN || 9095 5971
NIKHILESH REDDY TUMMALA || 8350 1593
UF CISE DEPT. • Group 15

1. Introduction

1.1. Problem Statement

Proposing a decentralized blockchain based eco-system for social media applications and validating the authenticity of news articles by integrating user feedback.

- Defining stipulations in smart contract to authenticate the requests from publishers.
- Storage of the published news on the blockchain by hashing the key elements of the news with the hash key.
- Leveraging anonymous user feedback through predefined smart contracts to determine the authenticity of the news.

1.2 Motivation

Although Blockchain has been implemented in a variety of industries, it has still not been able to capture the social media platform. With the growing discontent towards inaccurate and false news reported through this platform, a solution for determining the authenticity of such news is imminent. Many are looking towards blockchain technology to provide a peer to peer network without a central authority, as a potential tool to help combat the false news. By leveraging user feedback through social media applications, we can stride towards solving this problem. Since Blockchain offers anonymity for the users, we can expect an unbiased and unpressurized input from the user. Thus, providing us a robust and trustworthy system to effectively tackle false news.

1.3 Existing Research

To deeply understand the issue regarding fake news, a recent paper [1] has attempted to study the science behind fake news. This answers the questions, what is fake news? how is fake news generated? what are the essential elements in spreading false information?

Various methods across different technologies have been studied to tackle fake news. For instance, authors Youngkyung Seo, Deokjin Seo, Chang-Sung Jeong provided a fake news detection model based on text classifier system [2]. Few creators recently explored the Blockchain route to develop a smart contract based fake news detection model [3]. Another paper demonstrates a model based on leveraging user inputs to verify the authenticity of the news [4]. Although recent researches have proposed few ideas using the Blockchain system, none of the solutions have been implemented in the real-world applications. In this project, we hope to build on the existing research and provide a more robust and practical solution.

2. Scope

- The proposed system should be able to rate news posts for their authenticity so that the end-user will be able to identify the legitimacy of the post.
- The system will generate ratings for each post and based on the performance of the post, each publisher will subsequently be given a separate score to determine his/her legitimacy. As we realize that anonymity is one of the chief aspects of blockchain, we will preserve it by keeping the identity of the scorers anonymous. This has a global use case today, as many platforms are facing this challenge due to the viral nature with which deceptive news propagates.
- Defining smart contracts for various entities across the system.
 - New publisher enrolling into the system

- Acquiring public keys and digital signatures from publishers before publishing their posts
 - Stipulations for validators to rate posts
- Extending the designed model to well-known application in the social media platform. This involves providing a detailed description on the working phases of the model for the application.

3. Potential Challenges

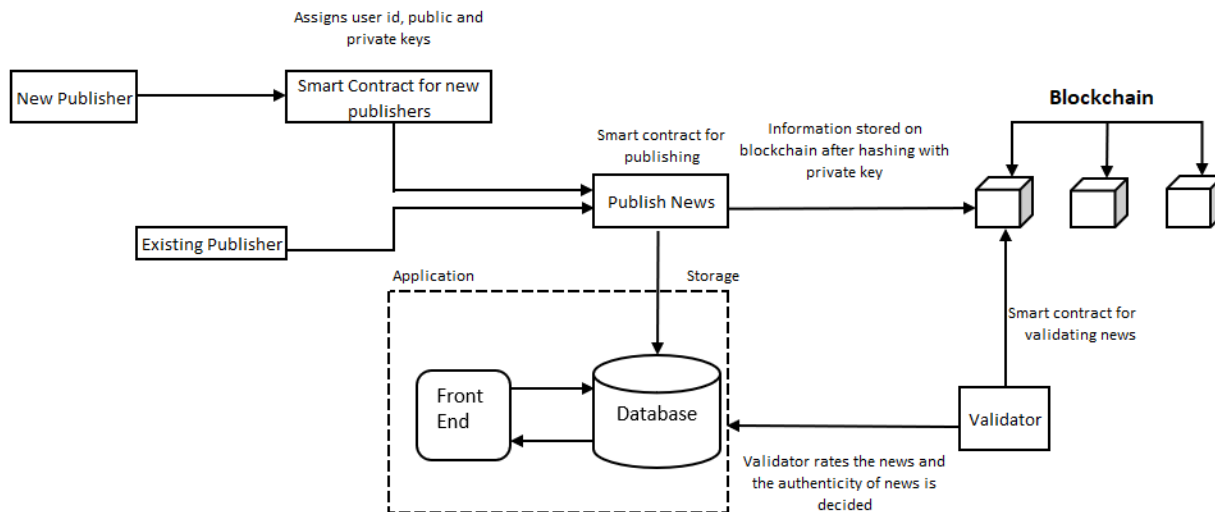
3.1. Challenges

- Since the model is dependent upon user feedback, receiving reviews for as many posts is of utmost importance. An incentive such as ‘X’ number of cryptocurrencies awarded for ‘Y’ number of posts reviewed can encourage validators to review more and more posts.
- Along with this, for the system to remain robust and trustworthy, it is necessary to ensure that the reviews provided by the validators are unbiased and accurate. To examine the reviews and ensure the authenticity of the reviews, we propose a system which analyses the performance of the validators by calculating separate scores for each validator. These scores will be fundamental in prioritizing a validator’s review over another. For example, a validator with a rating of 8/10 will have a greater influence on the reviews than a validator with a score 5/10. A validator’s individual score would be determined by the amount of deviation observed in his / her reviews in comparison with the average ratings for each post.
- Identification of publishers propagating false information and discouraging them. We handle this by flagging each fake post determined through the validation process. Once a certain amount of posts for a publisher are red flagged, their account would be revoked.
- Extending the system architecture to a well-known social media application. Although integrating a blockchain into the existing social media eco-system could be challenging, adding an external layer should be feasible. We propose storing the blockchain separately and providing pipelines for the application interface to communicate with the blockchain.

3.2. Limitations:

- Since social media is a ever growing ecosystem, providing a bound on the resources required for implementing the system is out of scope for this research.
- Restricting the users from posting sensitive or controversial news is not feasible for the proposed model. This could be handled through other methods such text classifier algorithms.
- Since the system is dependent on the user feedback, certain cases may exist where the news is still inaccurately rated. The system is limited in its capability to interfere in such cases.
- Since Blockchain plays a major role in this application, all the problems that blockchain faces from adversaries like eclipse attacks, partitioning attacks, etc. will still be applicable.

4. System Architecture



Publisher – Every entity which requests a user id for publishing news would be assigned a user id, private key and public key based on the stipulations in the smart contract.

Publishing news – Each news posted by a publisher would be subject to terms in the ‘news publishing’ smart contract. Once a news is published, it will be stored in the application database. Simultaneously, the information such as title of the news, publisher, timestamp etc would be hashed using the private key of the publisher and stored on the blockchain.

Validators – Validators would be able to access the information through the application portal and rate every news article. These ratings are then recorded in the blockchain. Validators for our application are classified into two categories.

- Field Experts – These would typically be journalists, reporters etc
- General Audience

Smart Contract for Validators – Each validation would be controlled by terms in the smart contract for validations.

Application – This is the end user social media application. The database would store all the news and associated ratings provided by the validators.

5. Methodology

- **Public Key/Private Key**

Every publisher / validator will be given a pair of public and private keys which are generated through the system. Once the keys are assigned, the address obtained by hashing the public key can be used in each post for the publisher. Whenever the publisher posts a news, the software would sign the transaction with the private key of the publisher. This would help in authenticating each post. The validators can send the ratings for the posts based on the public key address of these posts.

- **Voting mechanism**

Scoring will be handled in two phases and categorized based on the validators.

- In the first phase each validator will be rated based on a score bracket that our architecture will determine. We will be exploring various other possibilities to come up with a range for the score bracket which helps us to find a noticeable discrepancy between the average score and validator’s score and this could be because of one of the two possibilities:

- 1) The validator has certain prejudices regarding the subject
- 2) It was a genuine point of view.

We will investigate further and come up with the best possible scoring behavior that will maintain a rating for the validator themselves, based on their scoring behavior which will be elucidated in our mid-term paper.

- Our second phase will be to establish a framework for the audience of the post to rate the post that has been published. This can serve two purposes:
 - 1) provide the audience with geographical relevance to the published story to have more impact on the scoring
 - 2) understand the pattern of inclination of the general audience i.e. what types of stories get the most or least responses.
- **Smart contracts**

In our mechanism we plan to utilize smart contracts for 3 instances:

 - To validate the publisher and determine if it is a verified or not verified account.
 - When a user publishes a post, the smart contract would be essential for acquiring the publisher's digital signature.
 - To record scoring for validators and audiences.
 - To incentivize validators

We will be determining novel approaches to identify effective implementation in this context through our research.
- **Anonymity**
 - Validators would be able to rate the news through the public key address of each post on the blockchain. These ratings will be recorded over the blockchain network as transactions and the scores will be computed through the system. This will preserve the anonymity of the validators and the voting audiences over the blockchain network.
- **Actions Against False Information Propagators**

This will be another important aspect of our research. We will conduct analysis to identify how to establish a fair threshold to distinguish between malicious and honest activity.

6. Road Map

- **Midterm paper**

The midterm report would consist of a detailed design of the end to end blockchain model along with the illustration of smart contracts and rating mechanism. This report would cover provide the below mentioned milestones:

 - Detailed architecture of the model along with the step by step mechanism.
 - Step by step working mechanism of the private / public keys for publishers and validators
 - Role of smart contracts in the model
 - Proposal for rating scheme
- **End Term Paper**

The final research paper would integrate the proposed blockchain model into a well-known social media application. Following areas would be covered in the final paper

 - Architecture and mechanism proposed in the midterm paper
 - Methodology of implementing the model on social media platform with an example
 - Future scope and scalability challenges

7. References

- [1] David MJ Lazer, Matthew A Baum, Yochai Benkler, Adam J Berinsky, Kelly M Greenhill, Filippo Menczer, Miriam J Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, et al. The science of fake news. *Science*, 359(6380):1094–1096, 2018.
- [2] FaNDeR: Fake News Detection Model Using Media Reliability -IEEE Conference Publication. [Accessed 22 Mar. 2019].
- [3] 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. Information Technology University (ITU), Lahore, Pakistan, 2019
- [4] Shovon Paul, Jubair Islam Joy, Shaila Sarker, Amit Kumar Das, Sharif Ahmed, Abdullah - Al - Haris Shakib. Fake News Detection in Social Media using Blockchain. 7th International Conference on Smart Computing & Communications (ICSCC), 2019.