CS 765 Assignment - 3

B.S.S.R. Saran **K. Sree Nikhil** **V. Mahanth Naidu**

1 Introduction

In this report, we will discuss about the challenge of preventing Sybil attacks running on the permissionless blockchain, using `Decentralized-App(DApp)` without relying on `Proof-of-Work(PoW)` or `Proof-of-Stake(PoS)`. `DApp` is implemented as a smart contract. A smart contract is essentially a program whose code is on the blockchain. The code is initially put on the blockchain in a transaction. The smart contract can have many functions. Different functions can be invoked by other transactions later on, provided the person invoking the function(s) has permission to do so as specified by the smart contract. When different functions are executed, the state of the smart contract is modified.

2 Explanation

2.1 The Problem: Divide and Conquer Approach

One of the main incentive motive of the Sybil attack is to manipulate the data request for fact-checking a news article or item. Consensus decisions within a Decentralized Network results in single data points, which are then reutilized by other protocols. As a result, the benefits of performing a Sybil attack might take the form of assets other than those used to execute the attack. Thus, even with a loss of confidence in a network, a Sybil attack might still be profitable. In this way, an attacker may manipulate the data request.

2.2 Proposing a New Alternative

We are going to create a reputation system based on algorithms. Its main aim is to encourage people to handle data requests honestly. Our system operates by shifting reputation points away from attackers and dishonest members towards honest and active network members. Participants receive tasks based on their reputation score, reflecting their past behavior. Reputation cannot be traded and is redistributed automatically and algorithmically by a protocol. Therefore, if an attacker intends to execute a Sybil attack on the network, each Sybil identity must initially engage in tasks with integrity (and attain adequate reputation scores).

2.3 Performance Based Data Request Committees

To ensure efficient data request handling, our protocol employs a system of performance-based committees. This involves:

- Our system tracks active participants through the Active Reputation Set (ARS). Then it monitors individuals who are involved in making data requests. To determine active participation, it looks at a metric that includes the identities chosen for committees within a specific period of time.
- Our system employs a `Committee Selection Mechanism`, which selects committees based on their reputation scores. To determine eligibility for committee selection, each identity uses a `Verifiable Random Function(VRF)` while considering its current reputation score. If the identity is considered eligible, it then takes on the responsibility of handling the data request.

3 Issues Covered

- **Sybil attack:** As mentioned above, we prevented Sybil attacks by implementing a reputation system based on algorithms. This system discourages dishonest behavior by shifting reputation points away from attackers and towards honest network members. Participants' reputation scores reflect their past behavior, making it challenging for attackers to execute Sybil attacks without first engaging in tasks with integrity.
- **Method to evaluate or re-evaluate the trustworthiness of voters:** Our protocol evaluates and re-evaluates the trustworthiness of voters through a reputation system. Reputation scores are algorithmically redistributed based on their behavior, ensuring that those who consistently engage honestly are rewarded with higher reputation scores. Here, we are taking the final result as the weighted average given by the committee (which is selected based on trustworthiness and registration for the committee).
- **More trustworthy voters should be given more weight:** In our system, more trustworthy voters are indeed given more weight through their reputation scores. Participants with higher reputation scores are selected for committees and given tasks reflecting their past behavior. This incentivizes honesty and active participation within the network.
- **Rational voters are to be incentivized:** Rational voters are incentivized to engage honestly and actively within the network to increase their reputation scores. Higher reputation scores lead to increased opportunities for participation in committees and data request handling, ultimately benefiting the network as a whole.
- **Final answer determination and Trustworthiness adjustment:** We determine the final answer by calculating the weighted average given by

the committee, where each member's vote is weighted by their trustworthiness. If the final result is greater than 0.5, the article is considered true; otherwise, it is false. Additionally, we check each individual's vote against the final answer to adjust their trustworthiness. If a voter's guess is correct, their trustworthiness increases by 1%, and if it's wrong, it decreases by 1%, with a cap at 0% and 100%.

$$\text{final result} = \frac{\sum_{i=1}^{n} w_i v_i}{\sum_{i=1}^{n} w_i}$$

- **Uploading a news item:** In our system, all the news articles are stored in a list named `articles`. On uploading a news item, we append it to the articles list.
- **Bootstrapping:** Bootstrapping in our DApp involves initializing trustworthiness ratings for voters without prior data. We initially set the trustworthiness for each voter to be 50%. After the evaluation of each article, their trustworthiness either increases or decreases accordingly. It begins by categorizing voters based on their probabilities of providing truthful votes. Initially, the DApp randomly selects fact-checkers and evaluates news articles through committee voting. Trustworthiness ratings evolve iteratively based on voting outcomes, refining the system's ability to identify reliable fact-checkers over time. This process enables the DApp to start fact-checking even without initial trustworthy ratings.

4 Simulations

- From the first graph, after evaluating 100 articles, we obtain a basic idea of the trustworthiness of people. We can distinguish the voters between those who are more trustworthy, those who are less trustworthy, and those who are malicious voters. Following this, we recalculate trustworthiness at the end of the simulation.
- From the second graph, we can observe that the performance of the committee, represented by $\frac{\sum_{i=1}^{n} w_i v_i}{\sum_{i=1}^{n} w_i}$, is approaching the truth value of the articles as the number of articles it evaluates increases. This suggests that our DApp successfully selects members who are more trustworthy, resulting in final results that closely align with the true value of the articles.

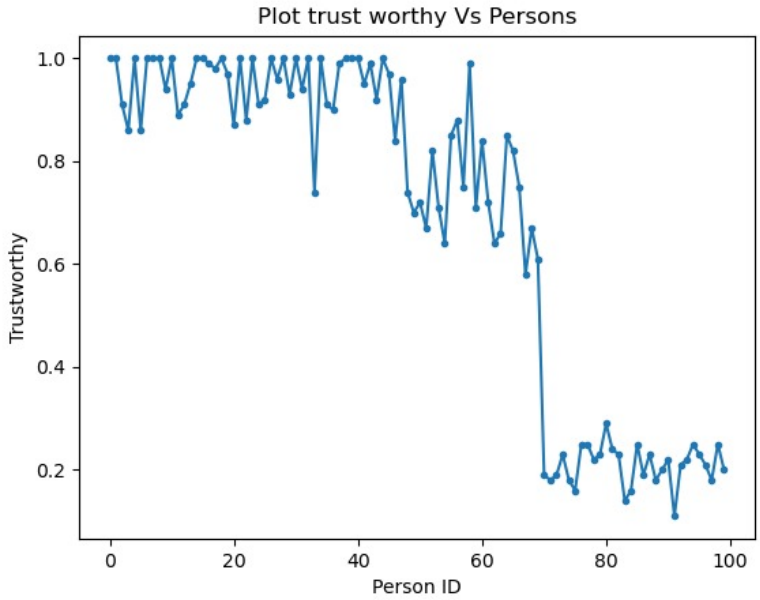

Figure 1: Trusthworthiness of individuals after evaluating 100 articles.

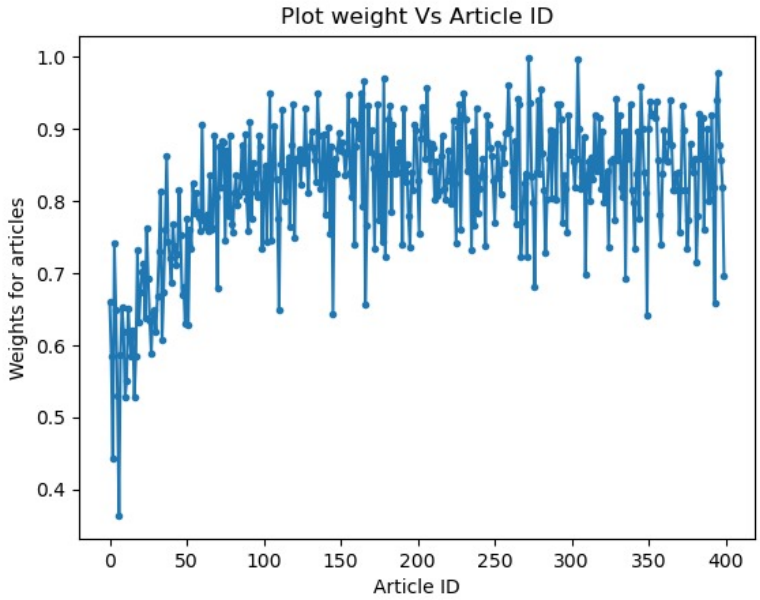

Figure 2: Weighted sum results given by the committee for all articles.