CS765 Spring 2023-24 Semester, HW3

Vivek Pawar(23M0769), Chiluveru Pranav(23M0787), Jayesh Bangar (23M0805)

A) Describe how your Dapp will handle the following issues?

(1) Sybil attack: A malicious person can create multiple identities and vote to skew the result in any direction

Ans) Proof of Stake (PoS): Implement a Proof of Stake mechanism where users are required to stake a certain amount of cryptocurrency as collateral to participate in the voting process of the news article. This makes it costly for attackers to create multiple identities as they would need to acquire a significant amount of cryptocurrency for each identity. Every user who wants to participate in the consensus procedure should Deposit some stake to classify whether the news article is fake or real.

(2) Method to evaluate or re-evaluate the trustworthiness of voters: The Dapp should evaluate how trustworthy different voters are based on how they vote.

Ans) To evaluate or re-evaluate the trustworthiness of voters in the DApp, a robust method is implemented to mitigate gaming of the system. Here's how it works:

1. Consensus Process: When a user publishes a news article on the DApp, a consensus process is initiated. This involves allowing any user to request fact-checking for the article.
2. Fact-Checking Votes: Users whoever is willing to verify the news article are required to vote on whether they believe the article is fake or real.
3. Verification Outcome: After the consensus process, if the majority vote aligns with the verified truth of the article, the trustworthiness of the voters who voted in accordance with the truth increases.

   voter.domainTrustworthiness[article.category] += trustFactor

   Where trustFactor= $\dfrac{\text{No. of news Articles of a particular Domain correctly voted by voter}}{\text{Total votes voted by Voted in that particular Domain}}$

4. Adjusting Trustworthiness: Conversely, if a user's vote contradicts the verified truth, their trustworthiness rating will decrease.
5. Continuous Evaluation: Trustworthiness evaluations are ongoing and are based on users' voting behavior over time, rather than just one instance. This helps to prevent users from gaming the system with temporary behaviors.

(3) The opinions of more trustworthy voters should be given more weight. However, we must keep in mind that someone may be more trustworthy for certain types of news and not others.For example, someone may give excellent opinions about news related to Physics but is not so trustworthy on topics related to Politics or Economics.
Ans) Users are assigned two types of trustworthiness: overall trustworthiness and domain-wise trustworthiness.

1. When a new article is submitted for fact-checking, users willing to vote can participate in the evaluation process by Depositing some stack
2. If the new article is based on a particular existing domain, then we consider the domain's trustworthiness of the voter. If the new article is of non existing domain then we will consider the overall trustworthiness of the voter.
3. Votes are weighted according to the user's trustworthiness levels, ensuring a more nuanced assessment of the article's credibility.
4. This system aims to incorporate users' expertise and reliability into the fact-checking process, enhancing the accuracy and credibility of the assessments.

(4) Rational voters are to be incentivised to participate and vote truthfully to the best of their Ability.
Ans) The following procedure is followed

1. Users seeking verification for their articles must pay a verification fee.
2. Participants in the consensus process must deposit a certain amount of money before joining.
3. After the consensus, voters whose votes align with the overall consensus receive a reward.
4. Voters whose votes don't align with the consensus do not receive any reward.
5. The reward is distributed equally among voters, consisting of the sum of individual deposits made before participating and the verification fees paid by the user.

   rewardPerVoter = article.totalDeposits / correctlyVotedVoters

(5) Uploading a news item: Some efficient method should be used to identify a news item (which is to be evaluated) in the Dapp.
Ans) Keyword Matching: Develop a database of keywords associated with different categories (e.g., politics, sports, finance) and use keyword matching algorithms to classify articles based on the presence of relevant keywords in the article text.

(**6) Bootstrapping: If the Dapp does not have any trustworthy rating of different initial voters, then how to get started with fact-checking news?**
Ans) To bootstrap fact-checking news on a DApp without any initial trustworthy ratings of different voters, the following approach can be taken:

Initially, during user registration, the DApp prompts users to vote on 5-10 news articles, indicating whether they believe each article to be real or fake. These initial votes help establish a baseline for the user's trustworthiness within the system.

Based on the user's voting patterns and agreement with the known truth of these articles, the DApp assigns an initial trustworthiness rating to the user. Importantly, this rating is assigned without the user's explicit knowledge.

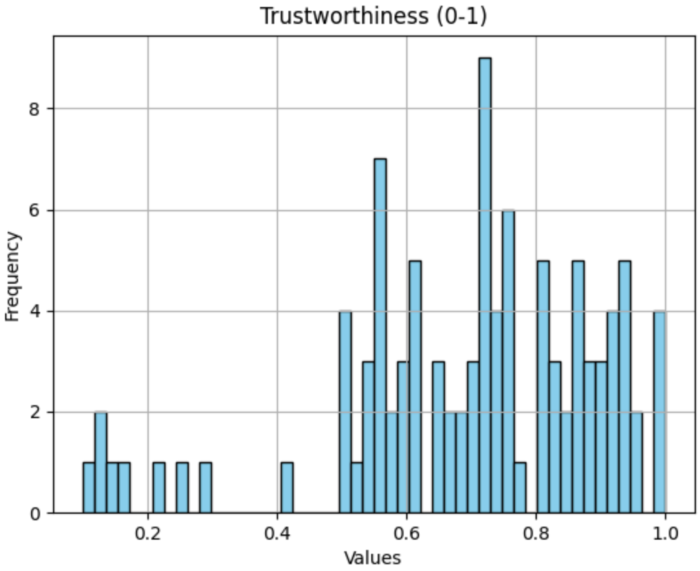
This initial trustworthy rating serves as a starting point for the user's participation in fact-checking news within the DApp. As the user continues to engage with the platform, their actions and contributions further shape their trustworthy rating over time.

C) Results of Simulation

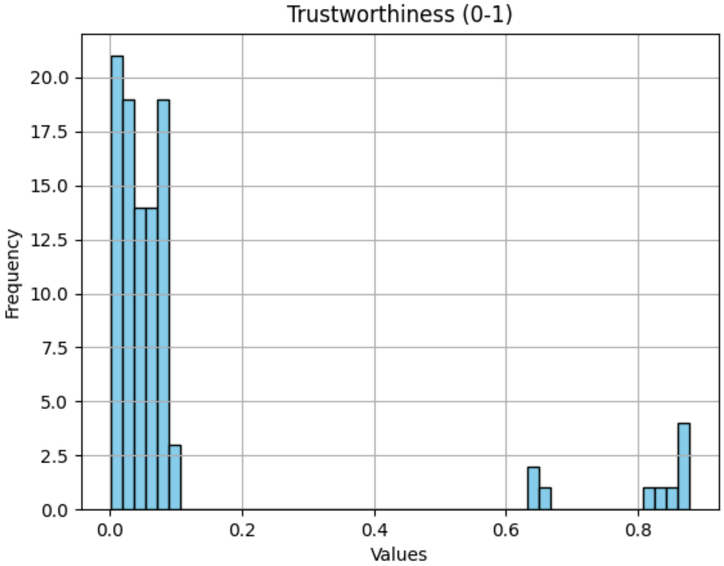
1) N=100, p=0.9,q=0.7

Here the fraction of malicious nodes is very high. The distribution n

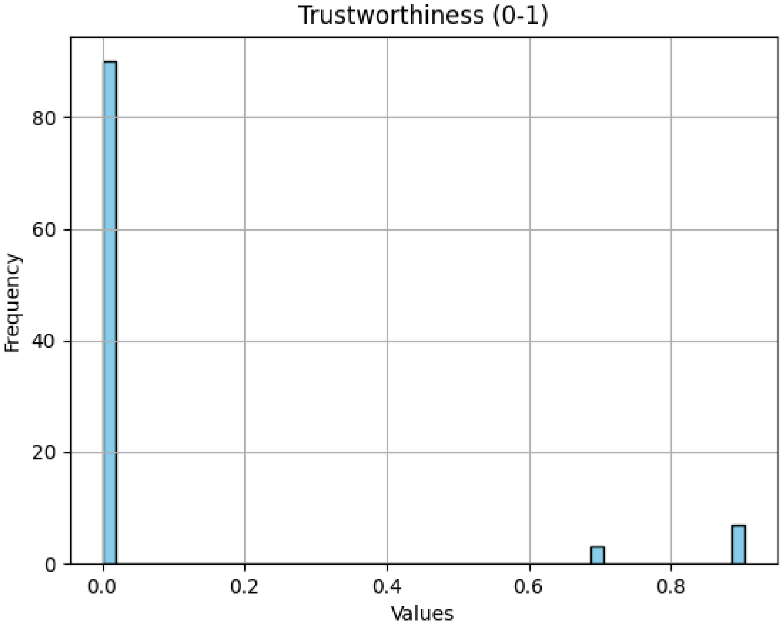
Steps =100



steps=1000



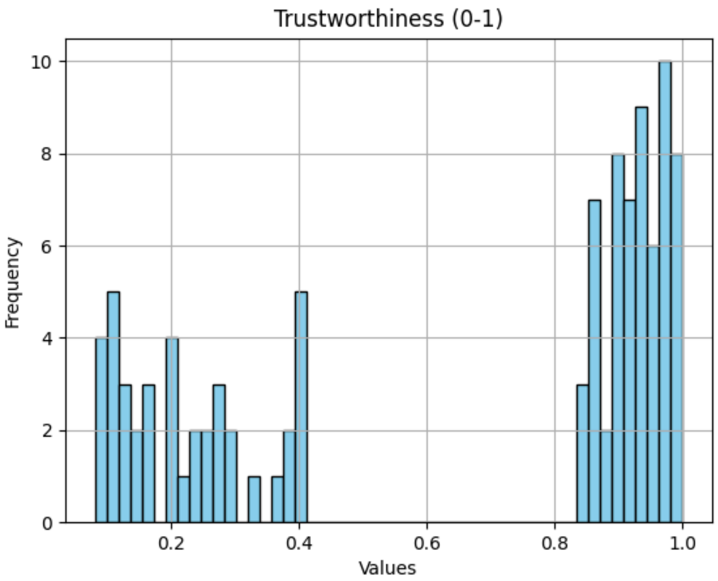
steps=10000



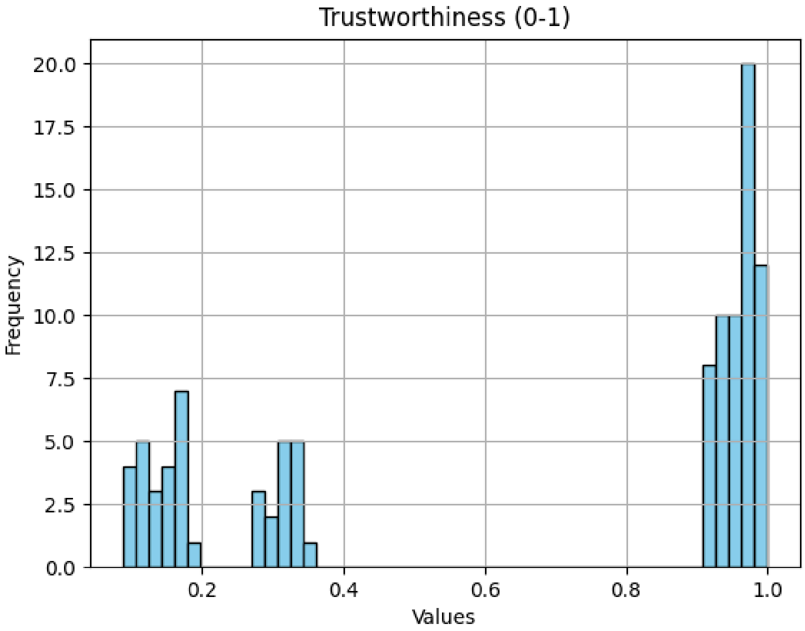
2) N=100, p=0.6,q=0.6

Here, the fraction of malicious nodes is greater than 50%. Here it is very likely that with high probability malicious nodes will take the control of consensus protocol, the trustworthiness of malicious nodes will increase and that of honest nodes will decrease, the histogram below also validates the expected behavior. Here, if the total trustworthiness of honest voters is greater than that of malicious votes then with some probability malicious voters will not succeed in taking the control of the consensus.

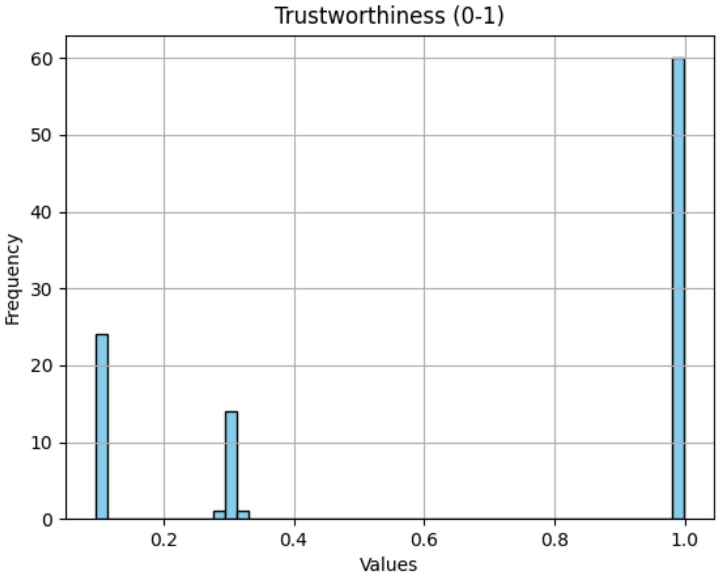
steps=500



Steps =1000



steps=10000

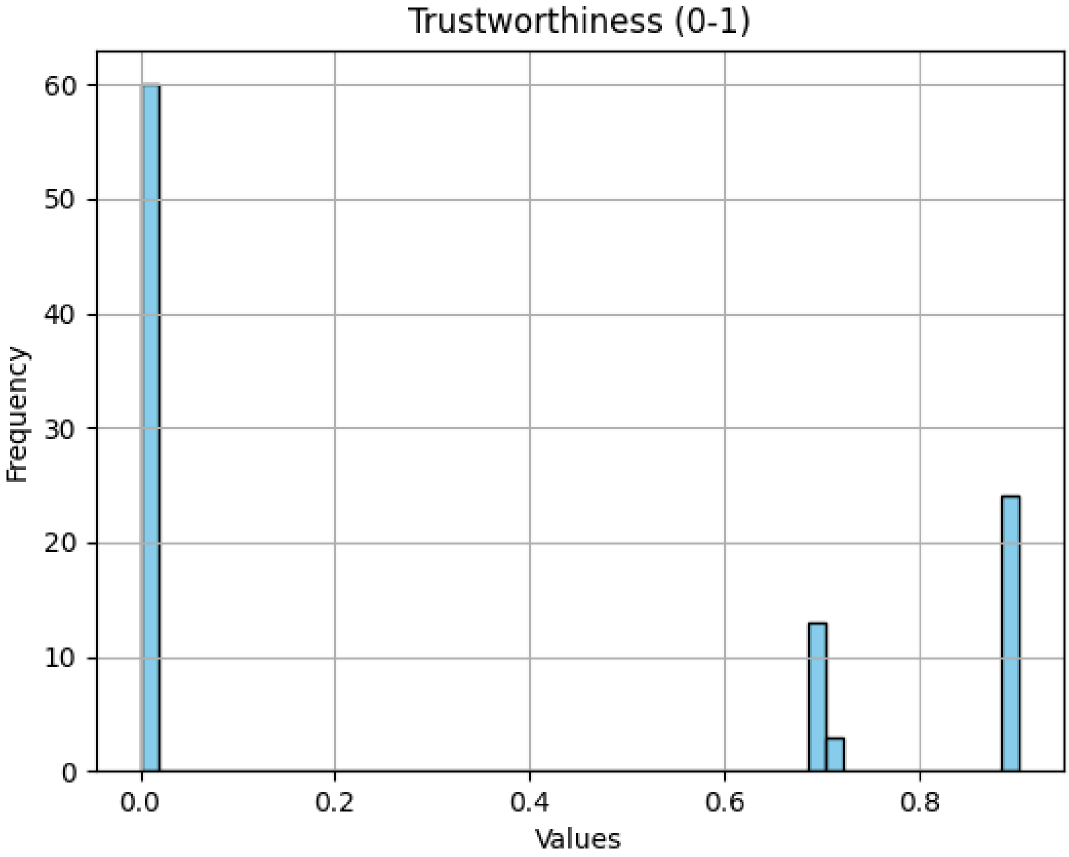


Here, if the total trustworthiness of honest voters is greater than that of malicious votes then with some probability malicious voters will not succeed in taking the control of the consensus.

This scenario is as described as follows:

3) **N=100, p=0.6, q = 0.6**

Steps: 10000

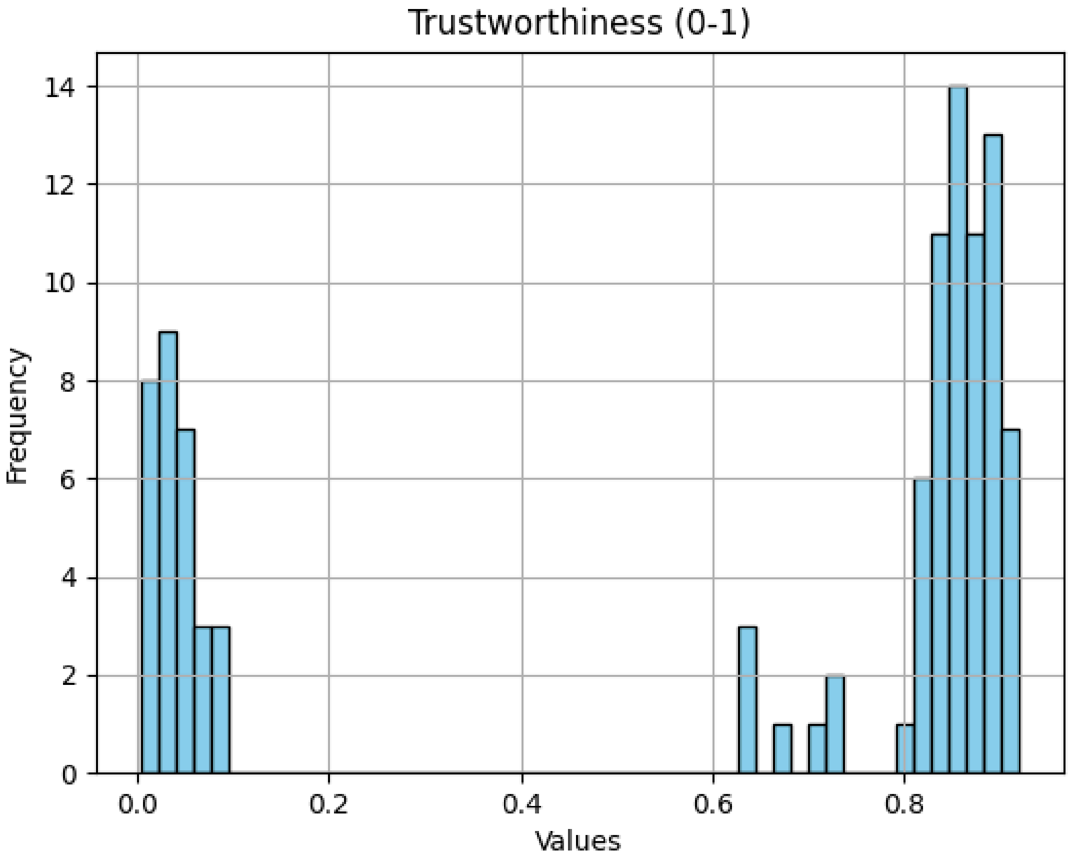


Here, even though the number of malicious voters is greater than 50% the trustworthiness of the malicious voters still decreases.

4) **N = 100, p = 0.3, q = 0.9**

Here, we observe that there will be expected when the number of malicious voters will be less than 50%.

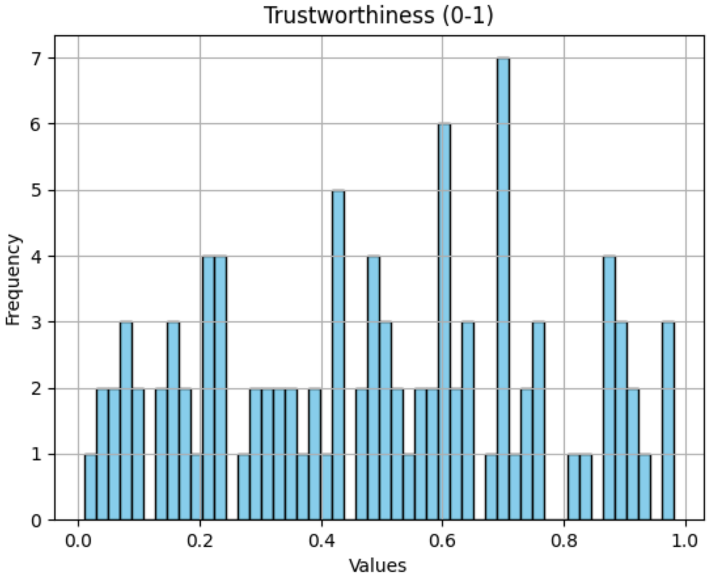
After 1000 steps:



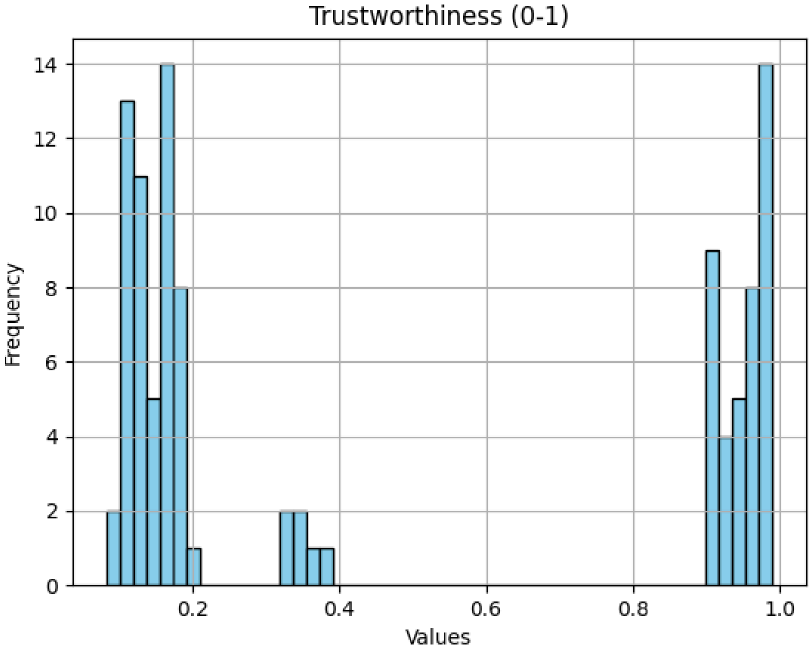
5) N=100, p=0.4,q=0.9

Here we observe that even though the fraction of attackers participating in the consensus is less than 50%, there is still a chance that the attacker will gain control of the consensus. The trustworthiness of the malicious voters will increase while that of honest nodes will decrease, as the output of the consensus will always favor the malicious voters. This may be possible due to the combined bootstrap trustworthiness of malicious voters will be higher than that of honest voters. The distribution of voter's trustworthiness when the malicious nodes take the control is given as follows:

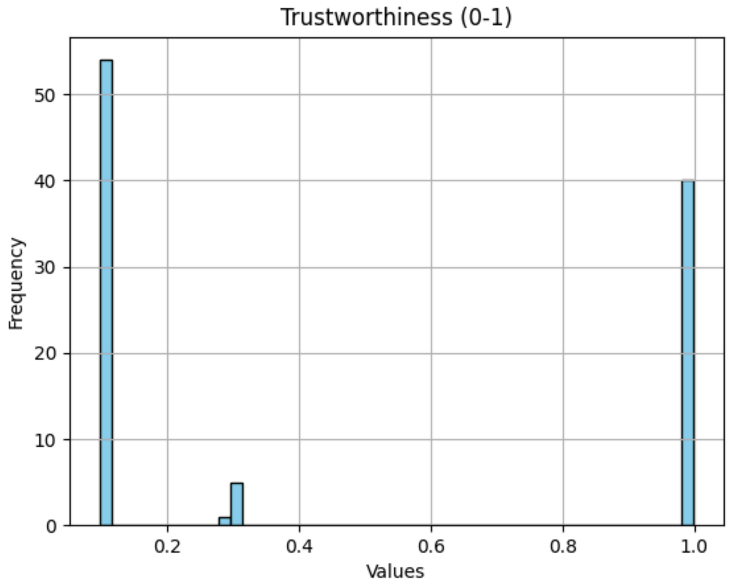
steps=10


Trustworthiness (0-1)
Frequency
0
1
2
3
4
5
6
7
0.0
0.2
0.4
0.6
0.8
1.0
Values

Steps =1000


Trustworthiness (0-1)
Frequency
0
2
4
6
8
10
12
14
0.2
0.4
0.6
0.8
1.0
Values

steps=10000


Trustworthiness (0-1)
Frequency
Values
0
10
20
30
40
50
0.2
0.4
0.6
0.8
1.0