Trutheum

A Network For Rewarding Truth

Whitepaper – Draft Version

Trutheum Network

Abstract: The Trutheum network provides a way to crowdfund large rewards for people that reveal requested truths (truth being: factual proof to an unanswered question). Requests for truths (RFT) are created by anyone and amass tokens from community members. Anyone who transfers tokens to the RFT has a vote in deciding how the tokens are rewarded. The protocol is fully decentralized with no central authority dictating what truths are revealed and uses voting to properly complete rewards.

Note: We do not condone any illegal actions that individuals might take and are not responsible for their actions. Truth should not be considered something that can only be illegally obtained.

Background

Truth is under attack. Intentionally misleading citizens has historically been an effective strategy, not just for governments, but also for many industries and businesses. The only method to combat it is to have an informed population.

Truths are mainly revealed by altruism. A person discovers a truth and decides to release it because they feel it's important to reveal. Sometimes they do this at great peril to themselves and without any reward in return. In an ideal world, this would be the only required motivation for truth to be revealed.

It is easy to imagine that altruism could be insufficient motivation for many people. Some of these people could be incentivized to reveal their truth if it was **extremely beneficial** to do so. This is why we have introduced a **reward system**. The size of the reward also functions as a gauge for what truths are most important for society to discover.

As rewards for a RFT (Request For Truth) grows larger, it also will garner more attention. This will produce a snowballing effect that will increase media coverage of the reward size. As coverage grows, the reward will grow too. This will help find a potential Revealer for the RFT.

A secondary benefit of a decentralized network of truth is it removes the power from organizations to modify or withhold truths that they themselves deem either irrelevant or not beneficial to publish (Quis custodiet ipsos custodes?).

System Overview

All Trutheum smart contracts are **open source** and **verified**. Contracts can only move tokens based on voting rules and Trutheum has no control over token transactions (The only exception is the Trutheum organization wallet, which is separately funded and used to pay for Trutheum related costs).

Request For Truth

Any user can submit a RFT by calling the create method on Trutheum's contract. Trutheum will then create a new contract specifically for the new RFT. At this point the network and other watchers will see the new RFT and can begin transferring tokens to it. RFT contracts have an expiration date. If the contract is never rewarded to anyone, it will return its tokens to the original backers. Contracts also have a minimum time that must pass before any tokens can vote. This defaults to one month to allow adequate time for tokens to be transferred and prevent votes from firing too early. The minimum time does not prevent the truth from being revealed earlier, it just delays the time it takes for the Revealer to receive their tokens.

RFT contracts receive "Reveals", which are proposals for the RFT's tokens for revealing the requested truth.

A Reveal contains:

- A wallet address (for the reward).
- A URL to the supporting media.
- A hash of the URL's supporting media.

To support large files, all Reveal media must be stored elsewhere on the Internet. There are several file drop services, but we may also create a new one to help make the experience easier for Revealers.

The hash of the content ensures that the content was not modified and must be checked by all participants before they vote.

Voting

Each token transferred to an RFT is valid for one vote. A token may not change their vote once it has been cast. To reduce the chance of voting attacks (see Attacks below) the voting

process is more involved than simple majority. After the initial waiting period, tokens can begin casting their votes. When a majority of tokens have casted their votes, a waiting period of two weeks is triggered for any other votes to be submitted. The Reveal with the most votes at the end of the two week period is marked as the winner and triggers another two week period to contest the outcome. Any RFT token may vote to contest, even if they did not initially vote. If more than 10% of tokens contest, the winning Reveal only receives half of the RFT tokens. The other half goes to Trutheum's Match Fund (See Match Fund below). **This method removes the incentive of trying to steal the reward** while still properly rewarding the Revealer in the case of an incorrectly contested vote.

After the vote, the tokens are transferred to the Revealer's wallet that they posted. This can purposely be a different wallet and is up to the Revealer to decide. Users can choose to continue to send to the Revealer's wallet if desired, however the RFT contract will not accept any more tokens after voting is completed.

RFTs can accept fractions of tokens and will be granted a vote with a weight that is equal to the fraction of the token transferred.

Reward After

Another type of contract available is the Reward After contract. This allows a Revealer to publish a truth at the same time as they publish a RFT. No vote is required with this type of contract. It serves as an easy way to reveal a truth without any crowdfunding period and still request rewards from the community.

No Revealer

If no Revealer comes forward or the majority of the tokens in an RFT do not vote, tokens can be requested to be returned. Tokens may also be requested if the RFT reaches its expiration date with no vote.

Potential Attacks

Not having a central authority controlling the release of truths can be problematic, especially when dealing with large sums of tokens.

Voting Attack

The most obvious voting attack is trying to control the majority of an RFT with a Sybil attack. Since anyone can transfer tokens to an RFT and each token represents one vote, a single entity can try to build up a majority of votes. Since the Revealer has already revealed their truth openly, this attack does not prevent the truth from being discovered. This attack would only be used to try and divert the reward away from the proper Revealer to their own bad Reveal (and wallet).

We solve for this attack in two ways. The first is to allow the minority a chance to contest the vote. By setting the threshold to 10%, an attacker would need to control over 90% of the votes to prevent a contested vote. With popular RFTs this would be an unrealistic percentage to obtain against the community. The second way we solve this is by cutting the reward in half if a vote is contested.

For example, let's say the community controls 49% (49 tokens) and an attacker controls 51% (51 tokens). The attacker votes for an invalid Reveal, but the community contests the vote. The attacker is rewarded with half of the tokens (50 tokens). The attack fails as they lost 1 token. Any higher percentage attained by the attacker just results in more lost tokens for them.

The downside to this method is if a Revealer genuinely revealed a truth and 10% of the tokens vote for it to be contested. This worst case still rewards the Revealer with half of the tokens, which will still be a large reward. There is little incentive to do this and offers no reward to the attackers.

Non-voting Attack

An attacker can possibly attain 51% of all tokens for an RFT and refuse to vote even if a Revealer has properly revealed a truth. Unfortunately there is no way around this without introducing a higher voting authority (which we do not want to create).

If this situation occurs, the community can decide to reward the Revealer from the Match Fund. Tokens from the RFT will then eventually be returned when the RFT expires.

URL Copying Attack

A URL Copy attack is a Revealer submits their URL to a RFT and immediately is copied by an attacker who submits the same information either with the same URL or a different URL. This attack turns into a timing issue and is mitigated by ensuring a high gas price is paid by the Revealer.

We may launch with a change that removes this issue. First a Revealer would submit a hash of the URL and a hash of the content. Once it has been included, they would then submit their unhashed URL and it would not matter how long it takes to be included.

How to Properly Reveal

The Reveal process can be complex as it involves using ethereum contracts. We don't want it to dissuade people that want to submit a Reveal and collect the reward. We will be providing some open source tools that make this process easy so that anyone can do it. Ideally this will take the form of very simple instructions to follow and involve a direct download of the source code instead of 3rd party installations or hosting, which could potentially hijack the Revealer's information.

Example

Joe suspects that his town's mayor, Rob, is using government funds for personal trips. Joe submits an RFT that asks for any proof of this. He mentions this to other community members, who also want to know the truth and begin submitting to the RFT. The RFT grows to 500 tokens and makes headlines in the local newspaper. Patrick reads the article and knows for a fact that this is exactly what Rob is doing. Rob has bragged to Patrick multiple times over text messages about it and he has even sent photos of some of those trips. Patrick decides that it's worth revealing the truth and he could use the money. He submits to the RFT a bunch of screenshots from his phone. With the truth revealed, token holders vote and Patrick receives the token reward. Since Patrick did this anonymously, nobody (except for maybe Rob) knows who submitted the screenshots. Rob is recalled and faces charges for his misuse of government funds.

Trutheum Network Tokens (TNT)

The objective of the Trutheum crowdfund is to create our initial tokens of TNT and to raise funds for two distinct parts of Trutheum, described below.

Match Fund

70% of funds raised will be inaccessible by the Trutheum organization and solely controlled by the voting block of all TNT owners. Votes can be held to divert funds from the Match Fund to successful RFTs. This allows the community to have a reserve of tokens that they can collectively reward to important RFTs. By design, the Trutheum organization cannot withdraw from the Match Fund, but will have the power to freeze and unfreeze the Match Fund to avoid any unintended exploits.

The Match Fund also serves as a bucket for any contested RFTs.

Organization Fund

30% of funds raised will be reserved for the Trutheum organization. The main areas are for employees, legal, and improvements.

Employees

Trutheum requires a large amount of programming and audits from both the community and internally to ensure that deployed contracts work as desired. We hope to also employ as much of the community as possible so that their time spent on building Trutheum is also rewarded.

Legal

Trutheum is simply an idea. It will be completely up to the community on how it gets used and moderated. We realize that there is always potential that both our organization and Revealers may get brought into legal battles. We want to make sure that we have funding available to cover legal costs.

Summary

Trutheum is building a powerful new incentive structure that aligns people's self interest with the greater interest of the group. As truths become more desirable to be discovered, its reward will grow, which will create a cycle between exposure and reward. The larger the reward grows, the more coverage it will get and the more likely someone will come forward to reveal the truth. We must strive to always become a more informed society and reject false information and its spread.

Truth is not subjective.