Seedom

Timely & Relevant Charity Fundraiser
with Supporter Rewards

Team Palm Tree

November 10, 2017

Abstract

There isn't an efficient, transparent, and trustless method to facilitate positive charitable organizations and the members of society they serve in a time of crisis. Fundraisers take time to put together and crowdsourced campaigns often lack transparency and have to spread through word-of-mouth. Seedom is a fundraising and supporter rewards platform that allows anyone to seed fund trustworthy charities that deal directly with afflicted individuals in a trustless fashion, thereby augmenting these individuals' freedom in an otherwise oppressive world. Bimonthly, a new timely and relevant charity will be chosen to receive about half of the funds raised through our smart contract. The other half of the funds will go towards one of the supporters, as selected by the participants at large along with the charity. A small percentage will be taken by the Seedom team as an administration fee in order to continuously improve this product through several phases, advertise with the charity, and celebrate the community-chosen participant.

Contents

1 The Bimonthly Trustless Fundraiser

Seedom will kickoff a new fundraiser for a new charity bimonthly, or roughly every two weeks, on the 1st and 15th of every month. Thirteen days is the span of the entire timeline due to February's 28 total days during standard years. Seedom will go on break on the 13th and 14th of every month in addition to the 29th until the end of any month long enough.

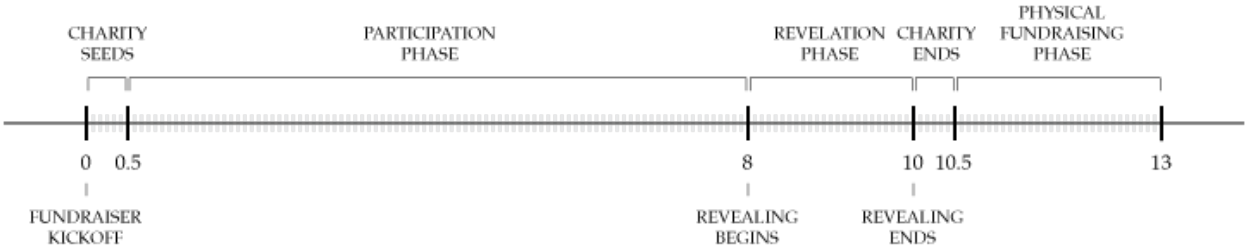

Figure 1: Fundraiser bimonthly timeline

1.1 Charity Selection Before Kickoff

Well before a fundraiser begins, the Seedom team will accept suggestions from various communication sources including email, text messages, chat app messages, and posts to our social media accounts. For phase one, the Seedom team will be the authority for charity selection. A charity will be chosen using several criteria.

- **Legitimacy** the charity must be a non-profit with a proven record of benefitting the general public
- **Relevancy** the charity must be working on a cause that is currently relevant
- **Timeliness** their should be an urgent or ongoing need by the charity for assistance
- **Cooperative** the charity must be willing to work with the Seedom team

1.2 Fundraiser Kickoff

A fundraiser begins with the Seedom team kicking it off through our smart contract by providing several parameters defined in table 1.

parameter	**data type**	**description**
charity	address	the ethereum wallet address of the charity
charitySplit	uint256	the % of funds given to the charity
winnerSplit	uint256	the % of funds given to the winner
ownerSplit	uint256	the % of funds given to the owner
valuePerEntry	uint256	unix timestamp of the start of revelation phase
revealTime	uint256	unix timestamp of the end of revelation phase
expireTime	uint256	unix timestamp of the expiration of the fundraiser

Table 1: Fundraiser kickoff parameters

1.3 Charity Seeds

Shortly after kickoff, the charity must create a 32-byte random number. This hashed random, the address of the charity's wallet, and the address of the active Seedom contract will be posted by the charity and Seedom through our respective social media accounts to guarantee their origin and authenticity. Any user can validate these pieces of data against the contract address state.

The charity will now seed the charity a 32-byte hash of it. Only the charity can provide this hashed number and no one can participate if it is not provided. All hashed randoms are generated using the hashed random formula in figure 2. The charity must safeguard their random number and not reveal it to anyone outside of their organization. It will be used later when the charity ends the fundraiser. If the charity does not seed the fundraiser before the revelation phase, the fundraiser is a dud and all participants will be refunded upon cancellation.

$$hashedRandomNumber = sha3_{keccak256}(randomNumber, ethereumAddress)$$

Figure 2: Hashed random number formula (randomNumber is 32 bytes, ethereumAddress is 20 bytes)

1.4 Participation Phase

After the charity has submitted their hashed random number, the fundraiser is considered open and anyone can now participate and send ether to the contract. Participation is a one-time activity and first, a user must create their own 32-byte random number and hash it using the formula in figure 2. The user must safeguard their random number and not reveal anyone else. It will be used during the revelation phase to confirm their participation in the fundraiser. The participation function also accepts ether funding to obtain entries.

Each entry costs a fixed value determined by the Seedom team at kickoff. The cost of a single entry will be very affordable to those beneath the international poverty line of $1.90 (USD) per day [1]. Each entry increases the likelihood that you will be selected by both the community and the charity to receive a split percentage of all of the ether received by the contract, similar to a raffle. If you are the winner of this ether, you will also be invited to participate in the physical fundraiser event after the end. Entries cannot be refunded and must be confirmed during the revelation phase. Partial entries will be refunded immediately when participating or through additional funding after participation. The owner and the charity are never allowed to participate.

Along with the hashed random and any ether, a user can optionally associate their ethereum address with a short alias and their email address. These three values are stored off-chain in Seedom's secure servers and are forgotten by the time the next fundraiser begins to protect user privacy and keep our system GDPR compliant. For phase one, the alias is used to render a list of recent participants. The email address is only used to invite the community-chosen winning supporter to the physical fundraiser during the last few days.

After initial participation, more ether can be sent to the smart contract directly to obtain more entries. However, additional calls to participate will fail and the participant's hashed random number cannot be altered. There are no limits to the numbers of entries a participant can obtain and the participant can check the number of entries they or any other participant have through the contract at any time.

1.5 Revelation Phase

When the revelation phase begins, calls to participate and fund will fail. Participants may now reveal their secret random numbers, sent hashed in the participation phase, to the rest of the community. All random numbers need not be revealed; however, failing to reveal a random number will result in the forfeiture of funds without the ability to win community selection. Successful revelations may only be performed once per participant and incorrect random revelations, determined using the formula in 2, will be rejected.

1.6 Charity Ends

When the revelation phase ends, participants are no longer allowed to reveal their randoms. Between the end time and expire time, both specified during kickoff, the charity must now reveal their random number provided during seed. If the charity fails to call the end function and reveal their random before the expire time, all entries can be refunded through cancellation.

1.6.1 Secure Deterministic Crowd-sourced Random Number Generation

Because Ethereum is a turing complete deterministic world computer, mining nodes cannot generate individual random numbers as they would never be able to reach consensus. Some decentralized applications decide to use a miner-defined value, such as the blockhash, timestamp, or other value to generate a random number. This technique is flawed because of this and the miner's ability to reorder transactions, not include transactions, and not send out blocks. This gives the miner additional chances of winning.

Seedom's technique in similar to that of the RANDAO [2]. It starts with the seed of a hashed random provided by the charity, a collection of secret hashed randoms in the participation phase, and the revelation of these randoms during the revelation phase. All of these revealed random numbers are XORed together, starting with the participant randoms and ending with the charity random, to produce a final universal random that will be used to determine the winning participant.

If hashed randoms are only collected and revealed from the participants, the last participant has the choice to reveal their random, essentially giving them a double chance of winning. Worse yet, a miner that has participated many times using unique wallet addresses can gain many additional chances by reordering their reveal transactions and choosing which ones to publish. Because the cost of a Seedom entry will be low enough to be affordable by all, transaction gas and entry costs will not deincentivize bad miners from using this method.

To prevent this kind of tampering by the miners, the charity must be used as a trusted third party to provide a random that can alter any manipulation by miners. This charity random is provided hashed before the first user participates so that the charity cannot themselves manipulate the final universal random. Users participating in a fundraiser tied to a specific charity are confirming their trust of the charity and their beneficial work. This trust extends to the charity's ability to seed start the fundraiser with their hashed random and end it with their final random revelation. The charity is incentivized to start and end a fundraiser because of the ether they will receive.

1.6.2 Winning Supporter Selection

After the universal random number is generated as part of the end call from the charity, it will be modded with the total number of revealed entries to determine an index into the global pool of revealed entries with the same call. The participant associated with the entry at this index is the winning supporter. As a last step in this call, a balance mapping is updated with owed funds to the charity, winner, and owner. Ether is not immediately distributed to each individual to prevent invalid or malignant addresses from reverting the end call. A winner is always guaranteed during each and every bimonthly fundraiser.

1.7 Physical Fundraising Phase

After the end function completes, the charity, winner participant, and the owner can now withdraw their funds by calling the withdraw function. These funds will be available for withdraw at any time and will never expire. As a best practice, it is recommended that everyone withdraw their funds as soon as possible.

Now that the Ethereum fundraiser is over, a physical fundraiser will take place near the headquarters of the benefitting charity to celebrate their success. The winning supporter will be invited by email, if provided to Seedom, to an all expenses paid trip to this event, wherever it may be in the world. Seedom will provide staff to work with the charity to throw this final fundraiser. Afterwards, this process begins again.

1.8 Fundraiser Cancellation

At any time after kickoff and before end, both the charity and the owner can cancel the fundraiser. Cancellation is a simple process in which all entries are refunded to the respective participant addresses. This is done by updating the same balances mapping used to distribute charity, winners, and owner funds. After cancellation is complete, users may withdraw their refunds using the withdraw function. Gas costs cannot be refunded.

After the charity issues the end call, cancellation is impossible as funds have already been appropriated into the balances mapping. However, if the charity fails to end a fundraiser before the expire time, the cancel function becomes open to the charity, the owner, and the community. This ensures that even if something catastrophic happens to the owner and the charity, all entries can be refunded.

1.9 Team Members

- Alex Groleau, Founder Software Developer
- Jesse Kuiper, Founder President
- Eric Thomas, Software Developer
- Kyle Graden, Marketing Lead

References

[1] World Bank. *Poverty and Shared Prosperity 2016: Taking on Inequality*. 2016. URL: https://openknowledge.worldbank.org/bitstream/handle/10986/25078/9781464809583.pdf.

[2] *RANDAO: A DAO working as RNG of Ethereum*. URL: https://github.com/randao/randao.

D:20171110011359-05′00′