Seedom

The Relevant Charity Fundraiser
with Supporter Rewards

Team Palm Tree

November 15, 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 crowd-sourced 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 Introduction

Seedom is an Ethereum decentralized application for raising awareness and funds for charities in need while rewarding a single supporting participant for their funds contribution. The selection of the winning participant is crowd-sourced from the participants and the selected charity. Funds raised will be distributed according to table 1. Administration fees cover our expenses in four operational areas.

- **Staff** team members, which include the president, founders, software developers, and the marketing team
- **Legal** legal representation to protect private fundraising rights internationally
- **Audits** continuous security and financial audits as organizational and technological changes are made
- **Events** additional physical fundraisers to further raise money for and promote charities

Charity	Winner	Seedom
47.5%	47.5%	5%

Table 1: Fund split percentages

1.1 Charity Selection

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. The Seedom team will have the discretion of charity selection for the first release, identifying an organization that is legitimate, active, demanding, and cooperative, as described below. A future goal is to open up this selection process further to have it be completely community driven.

- **Legitimate** the charity must be a non-profit with a proven record of benefitting the general public
- **Active** the charity must be actively working on a cause
- **Demanding** their should be an urgent or ongoing unresolved need by the charity for assistance
- **Cooperative** the charity must be willing to work with the Seedom team

1.2 Combination of Qualities

Seedom is the first fund raising and rewards platform with all of the following qualities.

- **Philanthropic** a new excellent charity will be chosen bimonthly
- **Trustless** trust in the charity is all that is required
- **Transparent** all contract transactions publicly visible and immutable
- **Relevant** legitimate charities working on focused causes that have an ongoing need for assistance
- **Secure** security is provided by the Ethereum platform itself and MetaMask
- **Anonymous** a wallet is the only requirement
- **Private** any identifying information given is purged after each fundraiser
- **Global** anyone in the world can participate

- **Affordable** everyone will be able to afford an entry
- **Limitless** there is no limit to the number of entries that can be obtained
- **Instantaneous** payouts to the charity and the winning participant are immediate after the fundraiser ends

1.3 Comparison to Other Fundraising Methods

Many methods exist for raising funds for charities. Outside of direct donations, some of the most popular include crowdfunding, matching gifts, drives, sales, auctions, events, lotteries, and raffles. All of these methods lack many of our combined qualities.

1.3.1 Crowdfunding

Crowdfunding is one of the best ways to raise funds for a charity or cause. Unfortunately, most of the popular fundraising platforms are not on Ethereum and therefore receive none of the many benefits native to the platform. When using a centralized website, such as GoFundMe, one is relying on them as to move funds from donors to a charity. Without trustless transaction transparency, it is impossible to know if these funds ever made it to their destination. Moreover, many crowdfunding companies charge 8+% fees for any donation, which includes a hefty payment processing fee. Because of this reliance on payment processors, GoFundMe is only available in a handful of counties.

1.3.2 Matching, Drives, Sales, and Auctions

Matching, drives, sales, and auctions are also effective fundraising vehicles. Donation matching requires one to work for or know a company that offers this perk. Donation drives may involve an intermediary that converts physical donations into monetary ones. Sales of items require the overhead of procuring items to sell in addition to the resale activity. Auctions items must be solicited, hopefully for free, and then sold for donation funds. Because of the various requirements and overheads involved with each of these techniques, the timeliness and relevancy of the ultimate donations might be lacking and with middlemen involved, trust and transparency are still huge issues. All three of these also lack global participation.

1.3.3 Events

Fundraising events are social gatherings that raise funds and awareness for a charity. Face to face communication is indispensable to furthering a cause and should never be overlooked. However, events can get expensive when selecting a venue, hiring temporary staff, providing food, creating informative materials, etc. Seedom adopts this technique at the end of each fundraiser for the mentioned benefits in addition to celebrating the newfound success of the winning supporter. In this way, the bulk of the funds have already been raised and distributed, making this final event important, but not necessary to the success of the chosen charity.

1.3.4 Lotteries & Raffles

Although Seedom is not a lottery and not a raffle, similar organizations exist worldwide and all of them have administration fees for their existence. In the United States, nearly every state has its own lottery, with a national average administration fee of 4.76% according the the U.S. Census Bureau [1]; however, this does not include commissions paid out to lottery ticket sellers, which equal this same percentage, on average [2]. All expenses considered, 8-10% of every lottery ticket sold in the U.S. goes towards the lottery process itself and not the winner(s) and beneficiaries.

2 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.

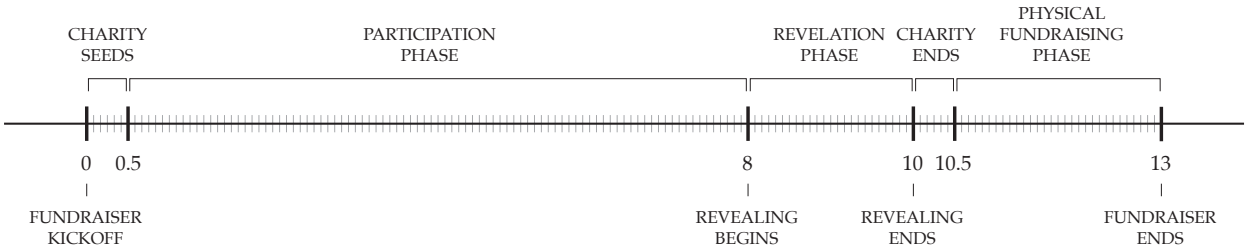

Figure 1: Fundraiser bimonthly timeline

2.1 Fundraiser Kickoff

A fundraiser begins with the Seedom team kicking it off through our smart contract by providing several parameters defined in table 2.

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 2: Fundraiser kickoff parameters

2.2 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)

2.3 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 and during fundraiser end to uniquely identify the winning participant.

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[3]. 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.

Ether can be sent along with participation to obtain initial entries and more can be sent afterwards through the fallback function for the same purpose. 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.

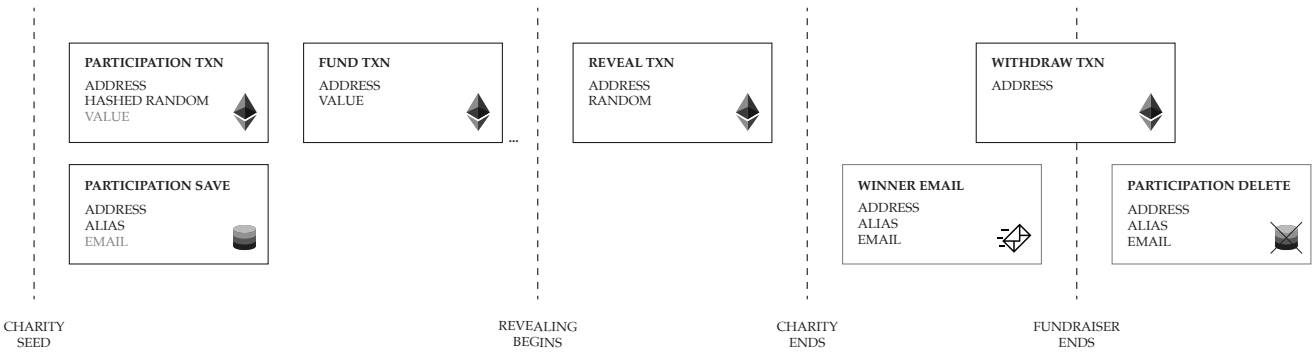

Figure 3: Participant data flow

2.4 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.

2.5 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.

2.5.1 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 [4]. It starts with a hashed random seed 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 crowd-sourced random that will be used to determine the winning participant, as seen in figure 4.

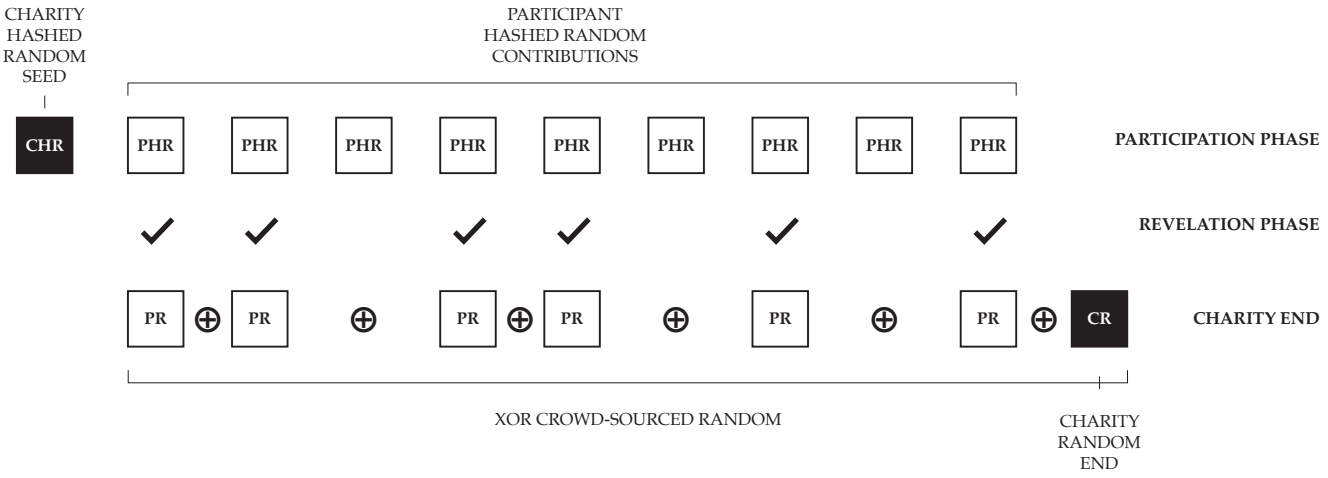

Figure 4: Crowd-sourced random number generation

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 crowd-sourced 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.

2.5.2 Winning Participant Selection

After the crowd-sourced 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 list of revealed entries. A discrete cumulative density function of entries is generated to assist with this process and the participant associated with the entry at this index is the winning supporter. As a last step in this call, a balance map 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 in the Ethereum Virtual Machine. A winner is always guaranteed during each and every bimonthly fundraiser.

After the winning participant is selected during the end call, a contract event will be broadcast that includes the participant's address, the decoded participant's random, and the total reward amounts calculated for the charity, winner, and Seedom. The participant's initially secret generated random from the participation phase serves as the pseudo-unique identifier of the winner. While this uniqueness relies on the uniqueness of participant randoms, which can be the same, the Seedom UI will show both the winning participant's address and their random.

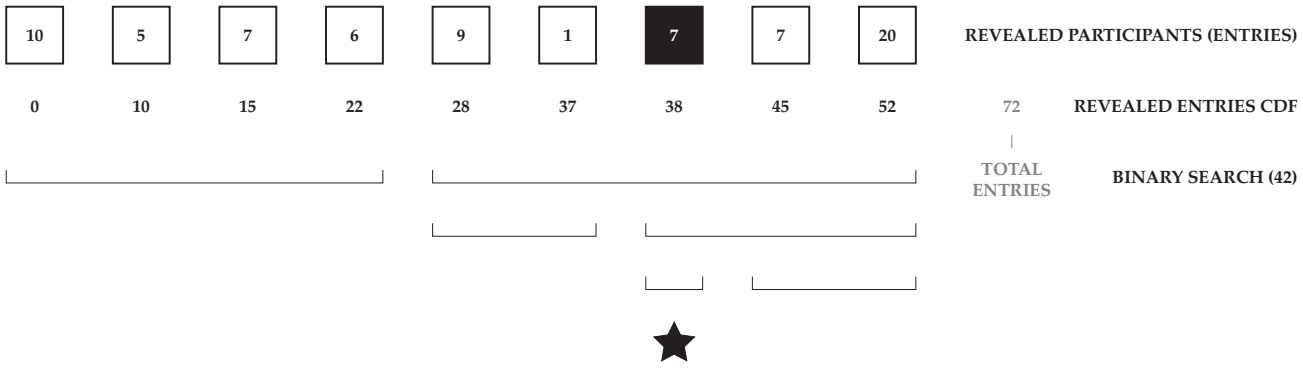

Figure 5: Winning participant selection for entry index 42

2.6 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 in close proximity to the headquarters of the benefitting charity to raise even more funds for them. This event will be open to the public and everyone is welcome to attend. Additional ether can be sent directly to the charity at this event while native fiat funds will also be accepted. Shortly after this event, this process will begin again.

2.7 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.

3 Token Sale

Never.

4 Future Work

In between fundraisers, continuous improvements to Seedom's decentralized application will be released. If smart contract changes are involved, this will result in a new Seedom contract address for the next fundraiser; however, due to the immutability of the blockchain and our lack of a self-destruct mechanism, legacy contracts will always be accessible for fund withdraws. The following are some of the improvements the Seedom team would like to implement.

4.1 Efficient Participant Storage

The current dynamic participant storage array in the smart contract will be replaced by an order statistic tree [5]. The participants hash map will remain the same and will be used in conjunction with this tree. This type of balanced binary search tree allows for the efficient rank ordering of participant entries and it is an essential step to providing support for a live participant leaderboard.

4.1.1 Live Participants Leaderboard

As more people enter, a live leaderboard will be available that tracks in descending order each participant's number of entries. If a user does not provide an alias, their sending Ethereum address will be displayed. If the user does provide an alias, that will be used instead. While not encouraged, participants are free to use this as a way of impromptu advertising. So if Company X wants their name to show on the Seedom homepage, they can buy the most entries to display themselves at the top of the leaderboard.

4.2 Enhanced Random Number Generation Security

Miner manipulation of the crowd-sourced random number generation process requires the Seedom team to adapt the random-generation algorithm in figure 4 to stay ahead of potential security issues.

4.2.1 Randomization of the Order of Participant Randoms

In the first release, participant randoms considered in the crowd-sourced random number generation process are XORed in order of time of participation during the participation phase. Randomization of the order of the XORed randoms using the trusted charity's random as a seed would provide additional protection against last minute miner manipulation of the final random.

4.3 Handling Fund Growth

As Seedom's participant base grows, our administration fee and winner selection process may need to be altered.

4.3.1 Administration Fee Reduction

Starting at 5%, our administration fee should be adequate to maintain our decentralized application and protect this idea from any legal involvements that may arise. There are many laws and organizations spanning the local, country, and international jurisdictions that might impede the creation of a fully transparent and trustless private international fundraiser of this magnitude. As those concerns are abated, our administration fee will likely be reduced, at our discretion, to ensure maximal returns to the charity and our community. The administration fee will never be set above 5%.

4.3.2 Multiple Winning Participants

There is an inherent burden that comes with the large influx of funds to any individual. Therefore, as the fund gets larger, we may introduce, at our discretion, the ability for multiple winners. Each successive winner might receive more funds than the last or a pool of winners may equally split the funds. There will only be one benefitting charity for any fundraiser, however.

4.3.3 Volunteer Event & Winner Transportation

As the administration fund grows, the Seedom team will create a volunteer event during the physical fundraising phase to compliment the physical fundraiser. The winning participant(s) will be invited by email, if provided to Seedom, to an all expenses paid trip to both the volunteer and fundraiser events, wherever they may be in the world. Moreover, Seedom will send some of our team members to both of these events to assist the charity directly.

4.4 Crowd-sourced Charity Selection

5 Team Members

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

References

[1] U.S. Census Bureau. *Income and Apportionment of State-Administered Lottery Funds: 2015*. 2015. URL: https://www2.census.gov/govs/state/2015_lottery_table.xls.

[2] Chris Islidore. "We spend billions on lottery tickets. Here's where all that money goes". In: *CNN Money* (2017). URL: http://money.cnn.com/2017/08/24/news/economy/lottery-spending/index.html.

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

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

[5] Wikipedia. *Order statistic tree*. URL: https://en.wikipedia.org/wiki/Order_statistic_tree.

D:20171115152117-05'00'