SEEDOM

Seeding the Future of Philanthropy
An Fundraiser for Charities and Their Supporters

Team Palm Tree

March 27, 2018

Abstract

Have you been to a local raffle that supports a non-profit organization at some point in your life? At this kind of fundraising event, you have a room full with eager supporters, representatives from the non-profit, administrators with rolls of paper tickets with distinct numbers on them, and a set of prizes off in the corner. As the administrators walk around with buckets, they distribute sets of tickets in exchange for the local currency, while retaining a duplicate ticket for each number. Everyone in the room can see these transactions as they occur, giving the audience trust over the process. After the administrators have made their rounds, the buckets of duplicate tickets are combined into one bucket in front of the crowd and a ticket is drawn for each prize. It is a fascinatingly simple and effective fundraising process.

Seedom is an Ethereum decentralized application (DAPP) for raising awareness and Ether for non-profit organizations (NPOs) in need while rewarding a single participant for their contribution and support. It takes the efficiency, security, and transparency of the traditional single-room raffle and re-invents it with trustlessness and crowd-sourced selection into an entirely new type of fundraiser that scales to the entire world. Bimonthly, or roughly every two weeks, a new NPO in need will be chosen, with the help of the community, to receive the majority of funds raised through our smart contract. Most of the remaining portion will go to one of the supporters through a selection process crowd-sourced by the participants, the NPO, and Seedom. A small percentage will be taken by the Seedom team as an administration fee to continuously improve the platform over time and extensively promote each NPO.

Contents

1 Introduction

Seedom is an Ethereum decentralized application (DAPP) for raising awareness and Ether for non-profit organizations (NPOs) in need while rewarding a single participant for their contribution and support. The selection of a participant is crowd-sourced by the participants, the NPO, and Seedom. Ether raised is not tax deductible and will be distributed according to Table 1 at the end of the fundraiser. Administration fees cover Seedom expenses in five operational areas.

- **Staff** sustains our small business, marketing, and development team
- **Legal** 3rd party counsel to protect all forms of private fundraising rights internationally
- **Auditing** 3rd party security and financial audits as changes to the contract and our organization are made
- **Infrastructure** temporary systems on our way to full decentralization
- **Events** physical fundraisers to further support and promote the NPOs we work with

NPO	Participant	Seedom
60%	35%	5%

Table 1: Ether split percentages

1.1 NPO Selection

Well before a Seedom fundraiser begins, our team will accept suggestions from NPOs and our global community of participants. NPOs can suggest themselves for a future fundraiser to Seedom directly by emailing team@seedom.io. Participants can make future NPO suggestions via our polling smart contract, which is deployed alongside each Seedom fundraiser. The Seedom team will have the ultimate discretion of NPO selection, identifying an organization that is legitimate, active, exacting, and cooperative.

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

1.2 Inherent Advantages

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

- **Philanthropic** a new NPO will be chosen bimonthly
- **Trustless** trust in the NPO is all that is required
- **Transparent** all contract transactions publicly visible and immutable
- **Relevant** our team only works with legitimate NPOs working on focused causes that have an ongoing need for assistance
- **Secure** security provided by the Ethereum platform itself
- **Governed** voting contracts allow participants to suggest future NPOs to support

- **Anonymous** a wallet is the only requirement
- **Private** the submission of personally identifying information is optional
- **Inclusive** anyone in the world can participate
- **Affordable** everyone will be able to afford an entry
- **Limitless** there is no limit to the number of obtainable entries
- **Instantaneous** payouts to the NPO and selected participant are immediate

1.3 Trustlessness

The Seedom community relies on our team to choose legitimate, active, exacting, and cooperative NPOs twice a month, with help from the community. No further trust in our team or the NPO is required after the fundraiser has been initiated. While the NPO and our team are responsible for administering the begin and end the fundraiser, neither side can operate outside of the strict bounds of the smart contract. No Ether stored in the contract can be extracted before the end of a fundraiser, unless it is cancelled.

The NPO and our team have the right to cancel a fundraiser before it ends, which will refund all participants. If the NPO or our team fail to end the fundraiser in a timely manner, a cancellation function opens up to the community, again refunding all participants. Once a fundraiser has ended and contract funds are allocated to the NPO, selected participant, and our team, all forms of cancellation are impossible and no transactions can be reverted.

1.4 Comparison to Other Fundraising Methods

Many methods exist for raising funds for NPOs. 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 inherent advantages.

1.4.1 Crowdfunding

Crowdfunding is one of the best ways to raise funds for a NPO 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 system, such as GoFundMe, one is relying on it to move funds from donors to a NPO or other beneficiary.

Initially, GoFundMe does not vet fundraisers, relying on fraud prevention specialists to protect their users. Without trustless transaction transparency, it is impossible to know if user contributions ever made it to the cause. Moreover, many crowdfunding companies charge 8% fees or higher for any donation, which includes a hefty payment processing fee. Being reliant on traditional payment processors, GoFundMe is only available in a handful of counties.

1.4.2 Matching, Drives, Sales, and Auctions

Matching, drives, sales, and auctions are also useful fundraising vehicles. Donation matching requires one to work for or know of a company that offers this perk. Donation drives may involve an intermediary that converts non-monetary donations into the monetary type. 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 donations are significant concerns; with intermediaries involved, trust and transparency

are paramount yet not easily demonstrated. Moreover, all three of these methods also lack global participation capability.

1.4.3 Events

Fundraising events are social gatherings that raise funds and awareness for a NPO. Often overlooked, face to face communication is indispensable to furthering a cause. However, these gathers can get expensive when selecting a venue, hiring temporary staff, providing food, creating informative materials, etc. Seedom adopts this face-to-face approach at the end of each fundraiser in the form of fundraising and volunteering events. At this point, the bulk of the funds are raised and distributed, making this final event valuable, but not necessary to the success of the overall fundraiser.

1.4.4 Lotteries & Raffles

Although Seedom is not a lottery and not a raffle, similar organizations exist worldwide, and all of them have administration fees that allow for their existence. In the United States, nearly every state has a lottery, with a national average administration fee of 4.76% according to 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.

1.5 Similar Ethereum Projects

Alice, Charitychain, Giveth, and Hypergive are other experimental non-profit Ethereum fundraising applications currently under development. Many of these systems go beyond fundraising and seek to control the internal operations of the non-profits funded. The first three allow donation refunds if the NPO does not meet their promised goals promptly, however these goals might be defined. Seedom's hands-off approach embraces facilitation, freeing the NPO to manage their internal operations while streamlining their fundraising efforts. This separation of concerns is necessary and maintains the NPO's ability to improve their efforts in their way, outside of Seedom's control.

Hypergive creates a direct and secure funding connection between donators and homeless and hungry individuals globally. This channel is similar to one employed by an aid program run by the United Nations that delivered funds to 10,000 Syrian refugees using the Ethereum blockchain [3]. Seedom will seek to partner with any organization working on these type of trustless end-to-end philanthropic delivery mechanisms as they are a fantastic use-case for the Ethereum platform. Additionally, the Seedom team will offer training services to the NPOs worked with to bring them up to speed on these emerging blockchain technologies.

2 Seedom Fundraiser

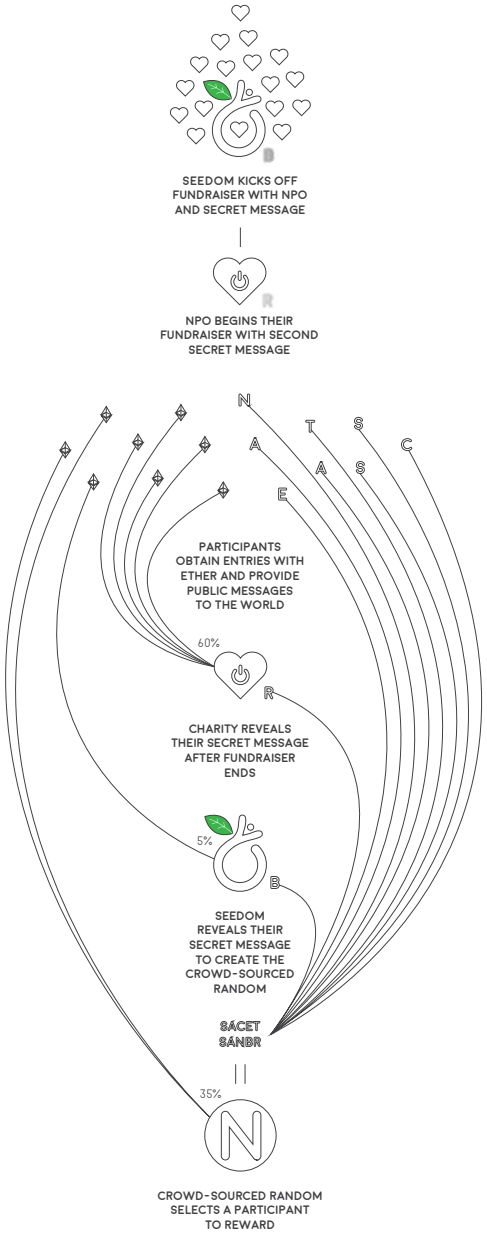

Figure 1: Visual overview of the Seedom fundraiser

2.1 Seedom Deploys a New Fundraiser

Seedom will deployment a new fundraiser for a new NPO bimonthly, or roughly every two weeks, on the 1st and 15th of every month. A fundraiser deployment consists of two newly deployed smart contracts: Seedom and polling. Thirteen days is the span of the entire timeline due to February's 28 total days during standard years. Seedom will go on break the 13th through the 14th of every month in addition to the 29th until the end of the month. Upon deployment, the Seedom DAPP, located at seedom.io, will be updated accordingly.

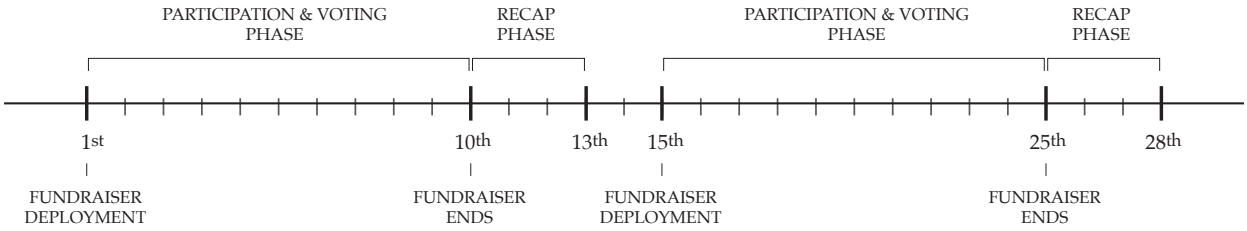

Figure 2: Fundraiser monthly timeline

2.1.1 Seedom Contract

The Seedom contract is deployed with several immutable fundraiser parameters. This includes the selected NPO, Ether split percentages, Seedom's secret, the cost of an entry, the timing of certain events, and the max number of participants.

Parameter	Data type	Description
npo	address	the wallet address of the NPO
npoSplit	uint256	the % of funds given to the NPO
participantSplit	uint256	the % of funds given to a selected participant
ownerSplit	uint256	the % of funds given to the contract owner (Seedom)
ownerSecret	bytes32	an encrypted message from the contract owner (Seedom)
valuePerEntry	uint256	unix timestamp of the start of revelation phase
endTime	uint256	unix timestamp of the end of participation phase
expireTime	uint256	unix timestamp of the expiration of the fundraiser
destructTime	uint256	unix timestamp of when the contract can be destroyed
maxParticipants	uint256	max participants to prevent out-of-gas transactions

Table 2: Fundraiser kickoff parameters

The NPO's wallet address must be posted publicly through their social channels for attestation of identity. The split percentages are numbers out of 1000 to allow the expression of a one decimal place and must sum to 1000. The Seedom owner secret is a hash of a 32-byte message, generated using the secret generation formula in Figure 3. This message will be revealed to the world after the NPO reveals their message after the fundraiser end time.

No participation or raising of entries can occur after the end time. Instead, the NPO and Seedom must reveal their messages to the world, which in turn selects a participant to receive their reward. The expire time is always set to the end of the recap phase, which is 3 days after the end time. If the NPO and Seedom messages are not revealed by the expire time, a participant is not selected, and the cancel() function is opened up to the entire community so that they may receive refunds.

The destruct time is set to 3 months from the beginning of a fundraiser. This allows for 6 sets of live smart contracts and plenty of time for the withdrawal of funds. After the destruct time, Seedom can self-destruct these legacy contracts and any Ether left in the contracts will be transferred to Seedom.

The max participants number is a safeguard against running out of gas during the end() function, which

calculates the crowd-sourced random number and selects a participant to reward.

$$secret = sha3_{keccak256}(message, address)$$

Figure 3: Hashed message (secret) formula (message is 32 bytes, address is 20 bytes)

2.1.2 Polling Contract

A polling contract will be deployed alongside the Seedom contract for the same period, allowing participants of the fundraiser to suggest and vote on future NPOs for us to support. This polling contract is directly linked to the Seedom contract, using it for proof-of-participation, and determining when voting is allowed.

2.2 NPO Begins their Fundraiser

Shortly after the Seedom contract is deployed, the chosen NPO must create an additional 32-byte message value and hash it into a secret, using the formula in Figure 3. The NPO sends this secret to the begin() function, and, upon confirmation, the community may now participate. The begin() function will only accept secrets from the chosen NPO. This message is generated using the secret generation formula in Figure 3 and will be revealed just after the fundraiser end time.

2.2.1 On the Initial Collection of Secrets

Two secrets, one from Seedom during construction of the Seedom contract, and one from the NPO through a call to the begin() function, are kept publicly in Seedom contract storage and allow for the participation and voting phase to begin. These secrets are collected prior to participation and, together with public messages collected during the participation phase, are used to generate a crowd-sourced random number that selects a participant to be rewarded.

The NPO and Seedom must both safeguard their messages to the world as they would their Ethereum wallet private key by not revealing it to anyone outside of their organization. Both messages are revealed to the world after the end time of the fundraiser with the reveal() and end() functions to override any form of miner manipulation during the collection of public messages during the participation phase. If the NPO does not begin() their fundraiser with their secret before the end time, the fundraiser is inoperable, with all participants receiving refunds upon cancellation.

For more details on how the crowd-sourced random number generation process works, see Section 2.4.1.

2.3 Participation Phase

After the NPO has submitted their secret to begin(), the fundraiser is considered open, and anyone can now participate and obtain entries with Ether. Participation is the one-time per user contribution of a 32-byte message to the world with enough Ether for at least one entry.

Each entry costs a fixed value determined by the Seedom team during deployment of the Seedom contract. The cost of a single entry, including Ethereum transaction fees, will be globally affordable to allow those beneath the international poverty line of $1.90 (USD) per day [4] to participate, with a minimum entry being less than the Ether equivalent of this amount. Each entry obtained by a participant increases the likelihood that the participant will be selected by all participants, the NPO, and Seedom to receive the participant split percentage of all of the Ether contributed to the Seedom contract.

Entries are non-refundable except in the case of fundraiser cancellation. Partial entries are immediately refunded during immediately participation. The owner and NPO addresses are prohibited from participation in the Seedom and polling contract.

2.3.1 Email Addresses

While participating within the Seedom DAPP, a user can optionally provide their email address, which is securely passed to MailChimp by the DAPP along with their Ethereum public wallet address for storage. This will sign the user up to the Seedom mailing list. This mailing list is used to notify users of the results of all fundraisers, to announce upcoming fundraisers, and to congratulate selected participants that receive the reward.

The email address associated with a rewarded participant's wallet address will never be publicly revealed in order to protect the privacy of the selected participant. A user's email address, and their associated Ethereum wallet address, are forgotten immediately after the user opt-outs out of the mailing list. This protects the user's privacy and keep the Seedom system compliant of data privacy legislation, such as the European Union's General Data Protection Regulation (GDPR). EMAILS GET FORWARDED TO THE CHARITY

2.3.2 Raising Additional Entries

After a user participates in the Seedom contract, additional entries can be obtained by sending additional Ether through the contract's fallback function. There is no limit to the number of entries a participant can acquire during the participation and voting phase. A participant can check the number of entries they or any other participant has through the Seedom contract or DAPP at any time.

2.4 NPO Reveals Their Message

After the fundraiser end time, users can no longer participate or raise additional entries. Between the end time and expire time, the NPO must reveal() their message to the world provided during begin(). If the NPO does not reveal() their message to the world before the expire time, the fundraiser is inoperable, with all participants receiving refunds upon cancellation.

2.4.1 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. Many decentralized applications decide to use a miner-defined value, such as the block-hash, timestamp, or other value to generate a random number. This technique is flawed given the miner's ability to ignore or reorder transactions and avoid broadcasting blocks entirely. It opens up the potential for the miner to receive additional chances of winning, even with deincentivization enhancements. Other method of random number generation include the usage of an external oracle, which requires a participant to trust the availability and validity of a such service.

Seedom's method is similar to that of the RANDAO [5]. The Seedom contract receives two hashed messages, from Seedom and the NPO. Once these secrets are stored and confirmed on-chain, the collection of public messages from participants can occur during the participation and voting phase. After the fundraiser end time, Seedom and the NPO reveal their hashed messages, which are again stored and confirmed on-chain. All of the participant messages are XORed together and this result is XORed again with the NPO and Seedom revealed messages to produce a crowd-sourced random number used to select a participant to reward, as seen in figure 4.

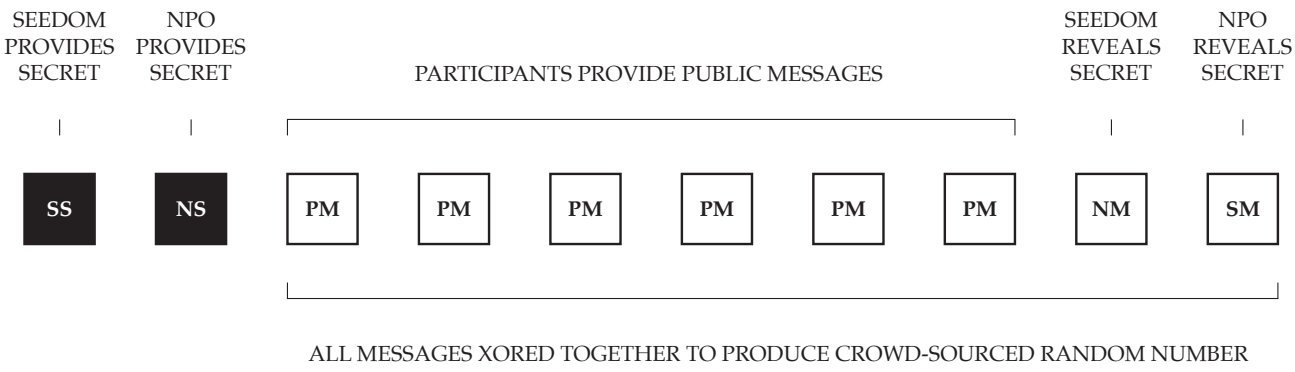

Figure 4: Crowd-sourced random number generation

Due to miner transaction and block flexibility, the miner is always able to choose to participate just before the end time of the fundraiser and affect the participant-generated portion of the crowd-sourced random. The cost of a Seedom entry combined with Ethereum transaction fees will not be high enough to deincentivize miners from attempting this manipulation.

However, because the NPO and Seedom have provided additional sources of randomization with their revealed messages, such efforts will be in vain. It is important, however, to prevent miner manipulation of the participant-generated portion of the crowd-sourced random and these future efforts are discussed in Section 4.2.1. An attacker trying to rig the selection of a participant has to know the secret messages of both Seedom and the NPO and has to be able to manipulate the participant-generated portion of the crowd-sourced random.

2.4.2 Winning Participant Selection

After crowd-sourced random generation, but as part of the end call from the NPO, the resulting number 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. Ether is not immediately distributed to these wallets as to prevent invalid or malignant addresses from reverting the end function in the Ethereum Virtual Machine. The contract guarantees a winner during every bimonthly fundraiser unless canceled. The participant's random and address serve as the pseudo-unique identifier of the winner.
After the end function completes, the NPO, winning participant, and Seedom can now withdraw their funds by calling the withdraw function. These funds are available for withdraw until the destruct time of the contract, six fundraisers later. Value left int the contract after it is destroyed will be sent to Seedom. As a best practice, Seedom recommends that everyone withdraw their funds as soon as possible.

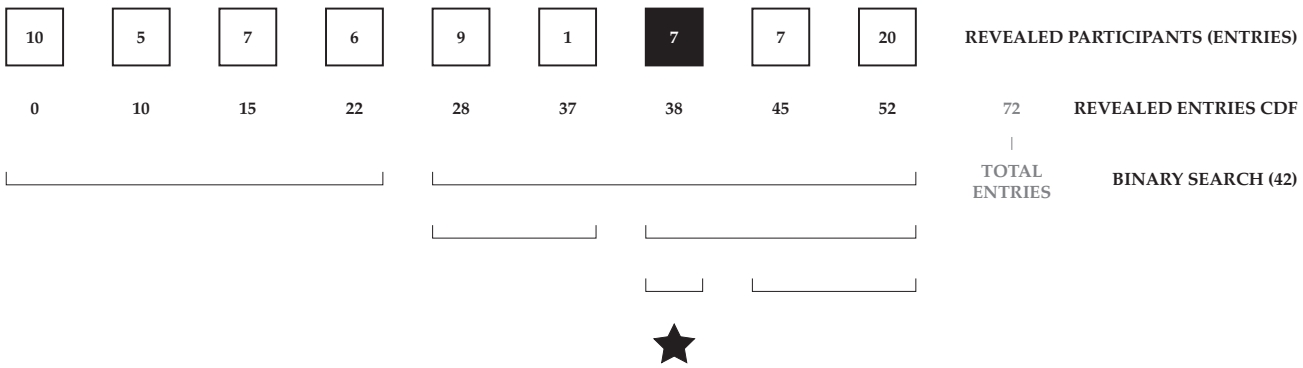

Figure 5: Winning participant selection for entry index 42

2.5 Fundraiser Cancellation

At any time after kickoff, but before NPO seed, both the NPO and the owner can cancel the fundraiser. Cancellation is a simple process that refunds all participant entries obtained during the participation phase. After the cancellation function is complete, users may check their balance with the balance function and withdraw the entirety of their balance with the withdraw function. Gas costs are non-refundable.
After the NPO calls the end function, cancellation is impossible; however, if the NPO fails to end a fundraiser before the expiration time, the cancel function becomes open to the NPO, the owner, and the entire community. This time-sensitive command ensures that every entry is refundable in the improbable event that something catastrophic happens to the owner, the NPO, or both.

3 Token Sale

Never.

4 Future Work

In between fundraisers, Seedom releases updates to our decentralized application as part of our continuous improvement process. If 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

An order statistic tree [6] will replace the dynamic participant storage array in the contract to facilitate future features of the application. The participants hash map remains the same, used in conjunction with this tree. A balanced and ordered statistic 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 users participate, a live leaderboard will be available that tracks, in descending order, each participant's number of entries. To allow for a leaderboard, an alias will be captured during participation. If a user

does not provide an alias during participation, their sending address is displayed. 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 **??** 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 NPO'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 will evolve.

4.3.1 Administration Fee Reduction

The 5% administration fee is adequate to maintain our decentralized application and protect the concept from any legal involvements that may arise. Many laws and organizations span the local and international jurisdictions that might impede the creation of a thoroughly transparent and trustless private global fundraiser of this magnitude. As those concerns dwindle, our administration fee should follow in tandem, at our discretion, to ensure maximal returns to the NPO and our community. It it the intention of the Seedom team that administration fees never exceed 5%.

4.3.2 Multiple Winning Participants

There is an inherent burden that comes with a sizable influx of funds to any individual. Therefore, as the contribution fund grows immense, we may introduce, at our discretion, the ability for multiple winning participants. Each successive winner might receive more funds than the last one, or a pool of winners may equally split the ether. However, there will only be one benefiting NPO for any fundraiser.

4.3.3 Physical Fundraiser Phase

After the end of an fundraiser, a physical fundraiser can take place near the headquarters of the benefiting NPO to continue bringing awareness and contribution to their cause. This event will be open to the public, and everyone is welcome to attend. During the event, the Seedom team will assist the NPO in their ability to accept direct ether donations and native fiat funds as well. Shortly after, the timeline will begin again with a different NPO.
As the administration fund grows, the Seedom team will create a volunteer event during the physical fundraising phase to complement the NPO fundraiser. The winning participant or participants will be invited by email, if provided to Seedom, to a trip to both the volunteer and fundraising events, wherever they may be in the world. Moreover, Seedom will send some of our team members along to assist the NPO directly.

4.4 Crowd-sourced Charity Selection

After the first initial events, we will consider opening up the NPO selection to a voting process. This will involve pre-selecting up to five NPOs that have expressed interest to work with Seedom and a one week voting period open to previous participants.

5 Team Members

The Seedom team is comprised of philanthropic entrepreneurs and enthusiasts from various sectors of the technology industry. The current employers of all team members have no affiliation with Seedom.

- Jesse Kuiper, Founder & President
- Alex Groleau, Founder & CTO
- Eric Thomas, Software Developer
- Kyle Graden, Strategic Advisor

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] Michael del Castillo. "United Nations Sends Aid to 10,000 Syrian Refugees Using Ethereum Blockchain". In: *CoinDesk* (2017). URL: https://www.coindesk.com/united-nations-sends-aid-to-10000-syrian-refugees-using-ethereum-blockchain/.

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

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

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

D:20180327022421-04'00'