SEEDOM

Seeding the Future of Philanthropy

A Unique FUNdraiser for Altruistic Causes and Their Supporters

Team Palm Tree

April 19, 2018

Abstract

Have you been to a local raffle that supports a cause at some point in your life? At this kind of fundraising event, you have a room full with eager supporters, representatives from the cause, 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. Administrators, after making their rounds, now combine the buckets of ticket duplicates into one bucket in front of the crowd, drawing a ticket at random for each prize. It is a fascinatingly simple and effective fundraising process.

Seedom is a fun Ethereum decentralized application (DAPP) for raising awareness and Ether for altruistic causes 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 altruistic cause is 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 cause, 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 cause.

Contents

1 Introduction

Seedom is an Ethereum decentralized application (DAPP) for raising awareness and Ether for altruistic causes while rewarding a single participant for their contribution and support. The selection of a participant is crowdsourced by the participants, the cause, 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 contracts and the organization changes
- **Infrastructure** temporary systems on our way to full decentralization
- **Events** physical fundraisers to further support and promote the cause

Cause	Participant	Seedom
60%	35%	5%

Table 1: Ether split percentages

1.1 Cause Selection Methodology

Seedom is a fun and entertaining platform for seeding the future of philanthropy through the identification and funding of altruistic causes that can drive the future of decentralization. Decentralization can take many forms outside of the technical interpretation and the underpinnings of Ethereum. It includes, but is not limited to, the decentralization of power, knowledge, money, ownership, and control to as many people as possible. Seedom provides a funding mechanism for these causes to persist, meet their long-term goals, and decentralize our future.

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

- **Decentralizing** believes in the decentralization of power in all forms
- **Legitimate** has a capable team with a clear and effective plan of action
- **Active** is actively working on solving a problem
- **Exacting** is solving an urgent and ongoing problem
- **Cooperative** is willing to work with the Seedom team and accept crypto

1.2 Inherent Advantages

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

- **Philanthropic** a new cause will be chosen bimonthly
- **Trustless** trust in the cause is the only requirement

- **Transparent** all contract transactions publicly visible and immutable
- **Relevant** our team works with legitimate and focused causes benefiting those with an ongoing need for assistance
- **Secure** security provided by the Ethereum platform itself
- **Governed** a polling contract allows participants to suggest future causes to support
- **Anonymous** your personal information is not required
- **Private** your information is never revealed
- **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** payout allocation to the cause and selected participant is immediate

1.3 Trustlessness

The Seedom community relies on our team to choose causes twice a month with the help of participants. After deployment, a user requires no trust in our team or the cause, who are only responsible for administering the begin and end the fundraiser. Users, Seedom, and the cause cannot operate outside of the strict rules of the smart contracts and no Ether stored in these contracts can be extracted before the end of a fundraiser, unless canceled.

The cause and our team have the right to cancel a fundraiser before the end time, which will refund all participants. If the cause or our team fail to end the fundraiser promptly after the end time, a cancel() function opens up to the community, again refunding all participants. Once a fundraiser has ended, the fundraiser contract allocates funds to the cause, a selected participant, and our team, allowing these entities to withdraw while prohibiting all forms of cancellation.

1.4 Comparison to Other Fundraising Methods

Many methods exist for raising funds for causes. 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 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 cause.

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 causes. 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 and 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 experimental Ethereum fundraising DAPPs currently under development. Many of these platforms go beyond fundraising with fund management to control the internal operations of the causes supported. The first three allow donation refunds if the benefiting organization does not meet promised goals by a deadline. 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], with biometric scanners validating fund recipients.

Seedom is a FUNdraising DAPP that brings routine attention to causes, and it is agnostic to the internal operational methodologies employed by the receiving organization. The organization can maintain their autonomy over their funds outside of Seedom or community control. However, we believe in transparent end-to-end philanthropic benefit delivery systems, and we will work to integrate with any organization or platform that increases a user's understanding of exactly where their donation went. See Section 8 for our future plan to integrate with Giveth.

2 Seedom Explained

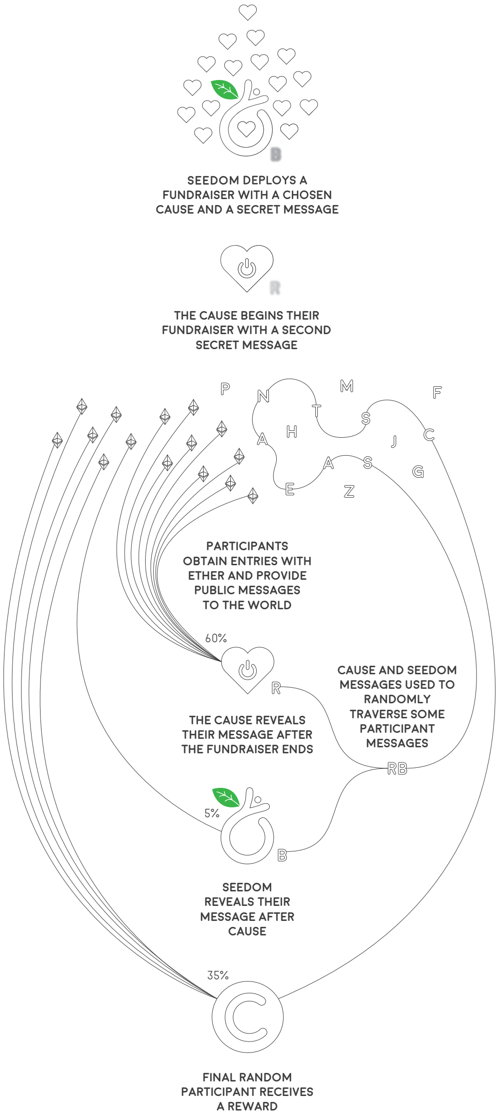
B
SEEDOM DEPLOYS A FUNDRAISER WITH A CHOSEN CAUSE AND A SECRET MESSAGE
R
THE CAUSE BEGINS THEIR FUNDRAISER WITH A SECOND SECRET MESSAGE
P
N
M
F
T
S
A
H
J
C
A
S
G
E
Z
PARTICIPANTS OBTAIN ENTRIES WITH ETHER AND PROVIDE PUBLIC MESSAGES TO THE WORLD
60%
R
CAUSE AND SEEDOM MESSAGES USED TO RANDOMLY TRAVERSE SOME PARTICIPANT MESSAGES
THE CAUSE REVEALS THEIR MESSAGE AFTER THE FUNDRAISER ENDS
RB
5%
B
SEEDOM REVEALS THEIR MESSAGE AFTER CAUSE
35%
FINAL RANDOM PARTICIPANT RECEIVES A REWARD

Figure 1: A visual overview of the Seedom fundraiser

2.1 Seedom Deploys Two Contracts

The Seedom team deploys a new fundraiser for a new cause bimonthly, or roughly every two weeks, on the 1st and 15th of every month. A Seedom fundraiser deployment consists of two new contracts: fundraiser 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.

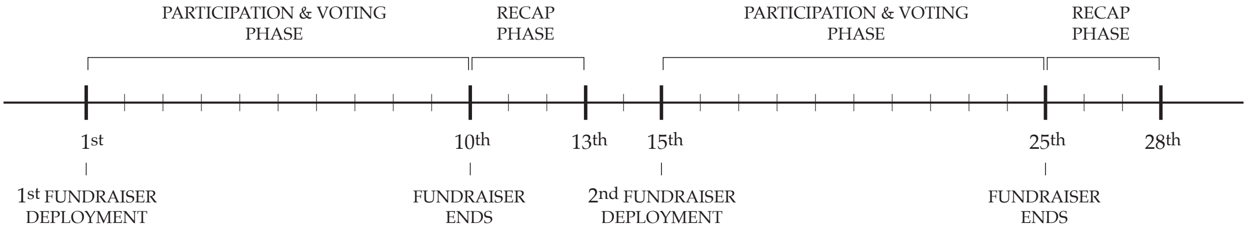
PARTICIPATION & VOTING PHASE
RECAP PHASE
PARTICIPATION & VOTING PHASE
RECAP PHASE
1st
10th
13th
15th
25th
28th
1st FUNDRAISER DEPLOYMENT
FUNDRAISER ENDS
2nd FUNDRAISER DEPLOYMENT
FUNDRAISER ENDS

Figure 2: Fundraiser monthly timeline

2.1.1 Fundraiser Contract

The fundraiser contract deploys with several immutable parameters, including the selected cause, Ether split percentages, Seedom's secret, the cost of an entry, the timing of specific events, and the max number of participants.

Parameter	Data Type	Description
cause	address	The wallet address for the cause must be posted publicly through their social channels for attestation of identity before the cause begins their fundraiser.
causeSplit	uint256	The percentage of funds given to the cause, expressed as an integer out of 1000 (600 is 60.0%).
participantSplit	uint256	The percentage of funds given to a selected participant (350 is 35.0%).
ownerSplit	uint256	The percentage of funds given to the contract owner (Seedom) (50 is 5.0%).
ownerSecret	bytes32	The owner secret is a hash of a 32-byte message from Seedom. This message will be revealed to the world after the fundraiser end time as part of a commit-reveal random number generation method. See Section 2.5.1 for details.
valuePerEntry	uint256	The cost of a single entry, expressed in wei.
endTime	uint256	No participation or raising of entries can occur after the end time, a UNIX timestamp. Instead, the cause and Seedom must reveal their secret messages, selecting a participant to receive the participant reward.
expireTime	uint256	The expire time is a UNIX timestamp set to the end of the recap phase, allowing time for the cause and Seedom to reveal their messages. See Section 2.5 for details.
destructTime	uint256	The destruct time is a UNIX timestamp set well into the future, allowing Seedom to self-destruct legacy contracts and recover abandoned funds. See Section 2.7 for more details.
entropy	uint256	The entropy number is used to increase the participant-generated entropy of the random number generation process. See Section 2.5.1 for details.

Table 2: Fundraiser deployment parameters

2.1.2 Polling Contract

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

Parameter	Data Type	Description
maxScore	uint256	An integer representing the maximum score of a vote.
fundraiser	address	This address links the current polling contract to the current fundraiser contract.

Table 3: Polling deployment parameters

2.2 Cause Begins Their Fundraiser

Shortly after the contracts deploy, the chosen cause must create an additional 32-byte message value and hash it into a secret, using the formula in Figure 3. The cause 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 cause. This message is generated using the secret generation formula in Figure 3 and will be revealed just after the fundraiser end time.

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

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

2.2.1 On the Initial Collection of Secrets

Two secrets, one from Seedom during deployment, and one from the cause through a call to the begin() function, are kept publicly in fundraiser contract storage and allow for the participation and voting phase to begin. These collected secrets, together with some of the public messages provided during the participation and voting phase, are used to generate a random number that selects a participant to reward.

If the cause does not begin() their fundraiser with their secret before the end time, the fundraiser is inoperable, with all participants receiving refunds upon cancellation. See Section 2.8 for more information about the cancellation process. For more details on how the random number generation process works, see Section 2.5.1.

2.3 Participants Obtain Entries and Provide Public Messages

After the cause has submitted their secret to begin(), the fundraiser is considered open, and anyone can now participate and obtain entries with Ether using the participate() function. Participation is the one-time per user contribution of a 32-byte message to the world with enough Ether for at least one entry. These public messages are used after the end time of the fundraiser to provide additional entrop in the random number generation process, detailed in Section 2.5.1.

Each entry costs a fixed value determined by the Seedom team during deployment of the fundraiser 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 is selected to receive the participant split of all of the Ether contributed to the fundraiser contract.

Entries are non-refundable except in the case of fundraiser cancellation. Partial entries immediately refund at the end of the participate() function. Seedom and cause wallet addresses cannot participate in the fundraiser and polling contracts.

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. Participation 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 is never publicly revealed 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 Seedom mailing list. Opting out protects the user's privacy and keeps the Seedom system compliant with data privacy legislation, such as the European Union's General Data Protection Regulation (GDPR).

Additionally, email addresses provided to Seedom forward to the currently benefitting cause. Users can unsubscribe from the cause's mailing lists at any time.

2.3.2 Raising Additional Entries

A user obtains additional entries, increasing their chances of being selected for reward, by sending more Ether through the fundraiser contract's fallback function after a the user first participates with their public message. 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 fundraiser contract or DAPP at any time.

2.3.3 Suggesting and Voting on Future Causes

After a user participates in the fundraiser contract, the user may now vote once on a future cause through the polling contract. The user can either suggest a new cause, or vote on an existing suggestion, with either counting as their vote. The polling contract is linked to the fundraiser contract, as it uses proof-of-participation to determine if the user is allowed to vote. Currently, proof-of-participation only looks at the running fundraiser contract; however, this will be enhanced in the future as described in Section 4.3.

2.4 Cause 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 cause must reveal() their message to the world provided during begin(). This revealation is the end of part of a commit-reveal random number generation method, detailed in Section 2.5.1. If the cause does not reveal() their message to the world before the expire time, the fundraiser is inoperable, with all participants receiving refunds upon cancellation. See Section 2.8 for more information about the cancellation process.

2.5 Seedom Reveals Their Message and Ends the Fundraiser

The end() function becomes available to Seedom after the cause reveals their message, ending the commit-reveal portion of the random number generation process described in the following section. Within this function, a participant is randomly chosen to receive the participant reward. The contract's value is then split and allocated to the cause, selected participant, and Seedom.

2.5.1 Secure Deterministic Random Participant Selection

Ethereum is a Turing complete deterministic world computer with many mining nodes assisting in its processing. Individual mining nodes cannot generate globally available random numbers as they would never be able to reach consensus. Many Ethereum pseudo-random number generation (PNRG) schemes exist that are resistant to miner tampering, each having various pros and cons [5]. The usage of direct block variables as a source of entropy is usually flawed given a miner's ability to manipulate all of these values; therefore, those methods are not discussed.

Method	On-chain	Single Txn	Global
Future blockhash	X		X
Commit-reveal	X		X
External oracle		X	X
Signidice	X	X	
Sequential PoW		X	X

Table 4: Miner tampering resistant pseudo-random number generation methods

For Seedom, we want a method that is done on-chain, requires only a single participant transaction, and generates a random that is globally available to all participants. On-chain implies that most, if not all, of the calculation of the random number is done transparently within the Ethereum Virtual Machine (EVM). A participant should not have to go through multiple steps when participating, and should only need to submit a single transaction. Finally, the same random number must be globally available to all participants for selection.

The future blockhash method locks the contract to a specific block number in a first transaction and requires a second transaction, within 256 blocks [6], that pulls the blockhash of this block number as a source of entropy. This method is susceptible to miner manipulation of the blockhash of the first block, if a miner has enough computational power to do so.

Commit-reveal implementations, such as the RANDAO [7], collect user-generated secrets, but then require a revelation phase, where many or all of these secrets are revealed on-chain. However, miners can ignore and reorder transactions, and avoid broadcasting blocks entirely. Miners may be able to receive many additional chances of winning, especially towards the end of the revelation phase, even with deincentivization mechanisms.

Any use of an external oracle requires a participant to trust the availability and validity of such service. The participant must trust all of the oracle's underlying infrastructure and trust that the Oracle has not tampered with the results. Moreover, a technique known as front-running allows an attacker to observe pending transactions for a response from an Oracle and insert their own response ahead of the Oracle's response using a higher gas price.

Signidice uses a cryptographic signature between two parties to generate a secure random number using the signature. BLS threshold signatures would allow a similar method to work with more than two parties [8]; however, the necessary functions for implementation do not yet exist in Solidity. This may be a method used by Seedom in the future.

The current Seedom method involves a combination of some of the methods in Table 4. It begins with receiving two secrets, or hashed messages, guaranteed to be from Seedom and the cause as part of a commit-reveal. Once these secrets store on-chain, the collection of public messages from participants can occur during the participation and voting phase.

After the fundraiser end time, the cause reveals their secret message first, and saves the block number of this revelation transaction on-chain. Seedom then reveals their secret message in a future block, using the future blockhash of the reveal transaction blocknumber as an additional source of entropy. The future blockhash is stored within the fundraiser contract for reference. Both secret messages are verified using the formula in Figure 3.

The two revealed messages and the future blockhash are then used to calculate a first random number using the formula in Figure 4, which is modded with the total number of entires to obtain a random entry number. The entry number is subsequently used to find a first random participant.

$$\boxed{firstRN = sha3_{keccak256}(ownerMessage, causeMessage, futureBlockhash)}$$

Figure 4: First random number formula

Given a random entry number, a participant is found using a binary search into a dynamic array of funding instances constructed during the participation and voting phase. These fund instances represent each participation and raising of entries. This array of funds is structured as a cumulative density function (CDF) of entries by participant, in order of participant contract funding. Figure 5 displays this search process visually.

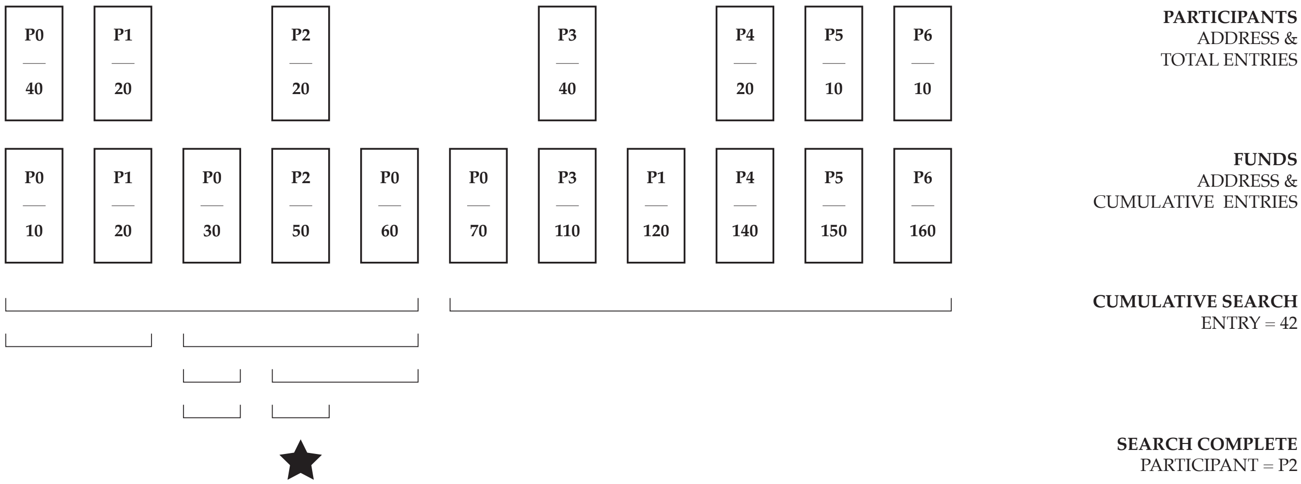

Figure 5: Random participant search on entry number 42

This process loops a set amount of times, as defined by the entropy number supplied during fundraiser contract deployment, using the participant's message at each step as part of the seed for the next random number. This formula is shown in Figure 6.

$$\boxed{nextRN = sha3_{keccak256}(ownerMessage, causeMessage, futureBlockhash, participantMessage)}$$

Figure 6: Next random number formula

The Seedom random number generation method traverses a random path through the immutable set of participants and their corresponding messages to gain additional entropy. The last participant in the path is the selected participant for reward and is stored in the fundraiser contract, completing the fundraiser. Anyone can validate this entire deterministic process using data stored in the contract. The overall method is displayed visually in Figure 7.

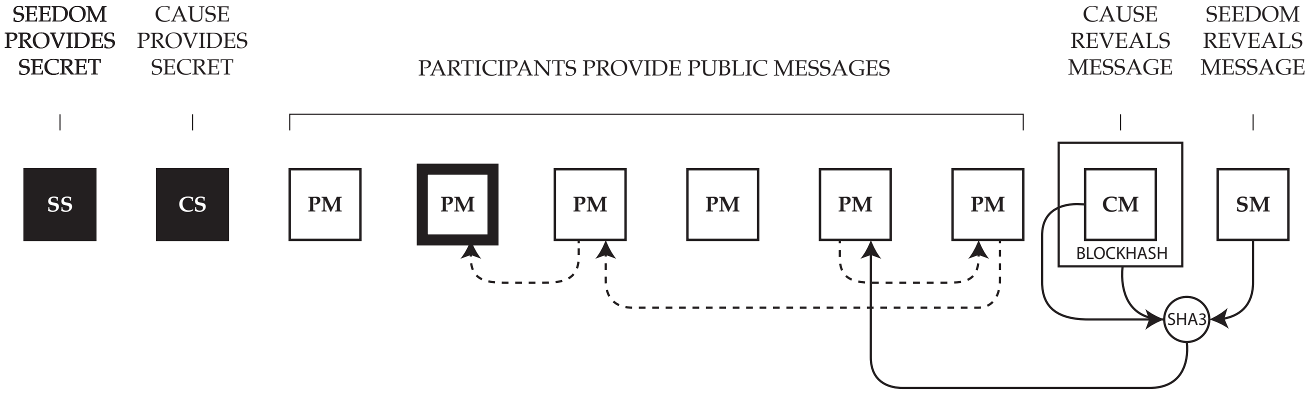

Figure 7: Overall final random participant selection process

2.5.2 Allocation of Ether

In the same end() function, Ether allocates to the cause, selected participant, and Seedom using the split percentages the fundraiser contract is constructed with, defined in Table 2. However, Ether is not distributed to any wallets during the end() function to prevent an invalid or malignant address from reverting the EVM. The withdraw() function in a separate transaction is the only way to pull Ether from the fundraiser contract, for all parties involved.

2.6 Withdrawing Balances

After the end() function completes, the cause, selected participant, and Seedom can now withdraw their respective Ether by calling the withdraw() function. These funds are available for withdrawing until the destruct time of the contract. The withdraw() function uses the checks-effects-interactions pattern [9] to avoid a re-entrancy security issue. As a best practice, Seedom recommends that everyone withdraw their funds as soon as possible.

2.7 Contract Self-destruction

The destruct time for both the fundraiser and polling contracts is set to 3 months from the beginning of a fundraiser. Setting the self-destruct availability time this far into future allows for six more fundraisers to occur and plenty of time for the withdrawal of old contract funds. After the destruct time, Seedom will self-destruct these legacy contracts, and any Ether remaining in them will transfer to Seedom.

2.8 Fundraiser Cancellation

After the fundraiser contracts are deployed, but before the end() function is called, both the cause and Seedom can cancel the contracts using the cancel() function. Cancellation is a simple process that prevents the fundraiser from proceeding further, refunding all participant entries obtained during the participation and voting phase. Once the cancel() function completes, users may check their balance with the balance() function and withdraw their refund with the withdraw() function. Gas costs are non-refundable.

After Seedom calls the end() function, early cancellation is impossible; however, if Seedom or the cause fail to reveal their messages before the expire time, the same cancel() function become available to the cause, Seedom, and the entire community. This time-based expiration ensures that every entry is refundable in the improbable event that something catastrophic happens to Seedom, the cause, or both.

3 Token Sale

Never.

4 Future Work

The fundraiser and polling contracts will be re-deployed for every fundraiser, resulting in new contract addresses for each. Seedom is an agile project continuously improved from user feedback with a release cadence aligned with these deployments. The following are some of the improvements the Seedom team would like to implement going forward.

4.1 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 for participation, their sending address will be 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 within Seedom DAPP, they can buy many entries to display themselves at the top of the leaderboard. This feature requires the implementation of an order statistic tree.

4.1.1 Order Statistic Tree Participants Storage

An order statistic tree [10] may be added to the contract to allow for the live participants leaderboard. A balanced and ordered statistic binary search tree augments the participants mapping, allowing for the efficient rank ordering of participant total entries.

4.2 Handling Fund Growth

As Seedom's participant base grows, our administration fee and participant selection process will evolve.

4.2.1 Administration Fee Reduction

The 5% administration fee is adequate to maintain our DAPP 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 fundraising system of this magnitude. As those concerns dwindle, our administration fee should follow in tandem, at our discretion, to ensure maximum funds for the cause and our community. The Seedom team fully intends to keep the administration fee at or under 5%.

4.2.2 Multiple Rewarded Participants

There is an inherent burden that comes with a sizable influx of funds to any individual. Therefore, as the popularity of Seedom grows, we may introduce, at our discretion, the ability for multiple rewarded participants. Each additionally selected participant might receive more or fewer funds than the previous, or a pool of participants may equally split the reward Ether. However, there is only one benefiting cause per fundraiser.

4.3 Enhanced Proof-of-Participation in the Polling Contract

The initial release of Seedom uses a proof-of-participation routine that only looks at the currently running fundraiser contract for evidence of user participation. This proof will be enhanced to include all fundraiser contracts that have not self-destructed. Each participant will receive a single vote per fundraiser, independent of the number of entries obtained, allowing engaged Seedom participants an increased effect on the future of Seedom and the causes the team ultimately choose.

4.4 Giveth Integration

Seedom is a FUNdraising platform at its core, ensuring Ether is transferred transparently from participants to the organization backing a cause. Giveth is a platform that extends this transparency into the management of this receiving organization, a collection of people referred to as a Decentralized Altruistic Community (DAC). Funds raised from Seedom or through donations are collected and stored in a vault and become available for withdrawal after various milestones complete [11]. Figure 8 is a visual explanation of this optional integration.

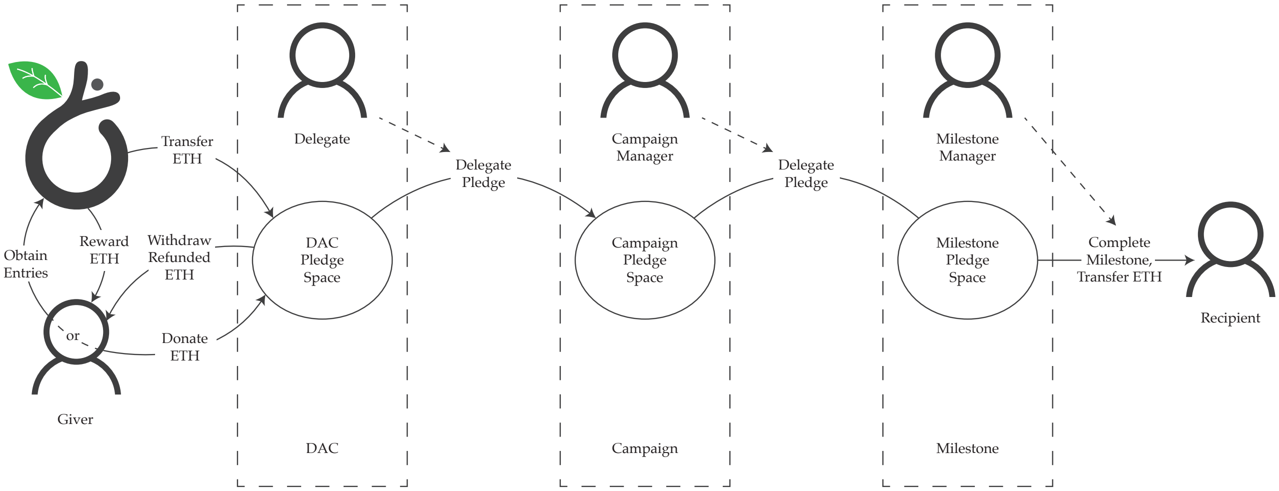

Figure 8: Giveth integration [11]

4.5 Reducing Volatility with Maker Dai

Most crypto-currencies, including Bitcoin and Ether, can be quite volatile assets. The value of a Bitcoin often experiences sizable fluctuations, rising or falling by as much as 25% in a single day and 3x in a month [12]. Over the period of a Seedom fundraiser, the price of Ether, compared to fiat currencies such as the U.S. dollar, might change significantly.

Seedom will likely switch to a more stable crypto-currency, such as Maker Dai, for all smart contract transactions. The Maker platform is decentralized and stabilizes the value of Dai to one U.S. dollar using external market mechanisms and economic incentives. Once generated, Dai transacts in the same manner as any other crypto-currency: it can be freely sent to others, used as payments for goods and services, or held as long-term savings [13].

4.6 Physical Fundraiser and Volunteering Events

During the recap phase, a physical fundraiser and volunteering event can take place near the headquarters of the benefiting cause to continue bringing awareness, contributions, and volunteers to their cause. This event will be open to the public, and any participant is welcome to attend.

The rewarded participant or participants will be invited by email if provided to Seedom during participation, 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 cause with these endeavors.

5 Team Members

The Seedom team is diverse, geographically decentralized, and 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.

5.0.1 Alexander Groleau

LinkedIn https://www.linkedin.com/in/jesse-kuiper-cpa-771a2111
Role Founder, Chief Technology Officer (CTO)

5.0.2 Eric Thomas

LinkedIn https://www.linkedin.com/in/awgneo
Role Founder, Chief Information Officer (CIO)

5.0.3 Jesse Kuiper

LinkedIn https://www.linkedin.com/in/eric-l-m-thomas
Role Founder, Chief Executive Officer (CEO)

5.0.4 Kyle Graden

LinkedIn https://www.linkedin.com/in/kylegraden
Role Founder, Chief Marketing Officer (CMO)

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] Arseny Reutov. "Predicting Random Numbers in Ethereum Smart Contracts". In: (2018). URL: https://blog.positive.com/predicting-random-numbers-in-ethereum-smart-contracts-e5358c6b8620.

[6] *Solidity: Units and Globally Available Variables: Block and Transaction Properties*. URL: http://solidity.readthedocs.io/en/v0.4.21/units-and-global-variables.html#block-and-transaction-properties.

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

[8] Antonio Salazar Cardozo. "Threshold Signatures". In: (Dec. 2017). URL: https://blog.keep.network/threshold-signatures-ff2c2b98d9c7.

[9] *Security Considerations*. URL: http://solidity.readthedocs.io/en/develop/security-considerations.html.

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

[11] Kris Decoodt. "What is the Giveth DApp?" In: (2017). URL: https://medium.com/giveth/what-is-the-future-of-giving-d50446b0a0e4.

[12] David Ernst. "Hard Problems in Cryptocurrency". In: (2017). URL: https://github.com/ethereum/wiki/wiki/Problems.

[13] The Maker Team. "The Dai Stablecoin System". In: (2017). URL: https://makerdao.com/whitepaper/DaiDec17WP.pdf.

D:20180419213814-04′00′