What is Popcorn?

Popcorn is a new paradigm for decentralized finance where yield-generating products simultaneously contribute to social impact.

Why create Popcorn?

A tremendous amount of value is being generated in decentralized finance (DeFi). One year ago there was about $500 million of value locked in DeFi contracts - as of today, there is over $35 billion[1] worth of value locked. That's an increase of more than 6,900%, and that number is growing.

During such a transformational time - where decentralized and disintermediated technology has reduced prices, eliminated barriers to entry, and provided unrivaled opportunity to those ushering in the new technology, a question of further directing this opportunity to the public benefit arose. How do we capture the efficiency gains of this new decentralized paradigm and create a better world? The answer is Popcorn.

By creating novel, yield-generating DeFi products, where a small fee is charged to be later shared with public benefit organizations, social good can be baked into the very foundation of a decentralized finance protocol without introducing any additional friction or extraordinary cost to the end user. Users of Popcorn would benefit from unique yield-generating products at a cost comparable to existing solutions all the while contributing to social impact initiatives for the public benefit.

[1] http://defipulse.com - February 5, 2021

Table of Contents

Introduction

The following paper is in an unconventional format. For the reader's convenience, the sections contained are described and summarized for clarity. First the paper begins with a question and answer format to describe the different aspects of Popcorn in a conversational style. This is perhaps the most universally relatable aspect of the paper and addresses most audiences. It then shifts towards describing functional software specifications for implementing a decentralized governance model for the funding of public goods on the Ethereum blockchain. The ensuing Additional Thoughts section, explores theoretical topics and critiques pertaining to the governance model and is followed by a reflection and an outlook towards the future. So let's begin ...

How does Popcorn create social impact?

A percentage of fees (e.g. 20-50%) generated by transacting with the Popcorn smart contracts are shared with social impact organizations elected by the Popcorn governance token holders. These nominated organizations are called beneficiaries.

How does Popcorn create economic opportunity for users?

Popcorn smart contracts allow users to generate yield on their crypto assets through the automation of yield generating strategies. The automation of common yield generating functions such as claiming, staking, re-supplying, leveraging, and swapping of cryptocurrencies, means that users:

1. save time
2. pay less in transaction fees
3. generate yield on their crypto holdings with little overhead or knowledge

Additionally, yield farming and staking incentives for token holders further increase the yield made available to token holders. For instance, by staking or locking tokens, token holders will be able to receive a portion of the fees that are generated by Popcorn.

How can social impact organizations apply?

Popcorn governance token (POP) holders may nominate and elect beneficiaries through a multi-step proposal process. First a beneficiary must be nominated and accepted by POP holders. After a beneficiary is accepted, it may then be awarded a grant through a separate voting process.

A successful nomination will contain financial or impact reports, a mission statement and an Ethereum address proof of ownership. Organizations wishing to apply to become a beneficiary may contact the Popcorn Foundation for guidance at no cost.

Which organizations are eligible to become beneficiaries?

Social impact organizations which provide a public good may be eligible to apply to become a beneficiary. Eligible organizations function to create positive, long-term impact on society.

To become an eligible beneficiary, an organization must first register their Ethereum address on https://sybil.org, or they must otherwise submit substantial proof that they own the address. A Beneficiary Nomination Proposal (BNP) may then be submitted with proof of address ownership along with supplemental application material.

Proof of address ownership is required in order to verify on-chain beneficiary addresses against real-world entities. This step creates transparency and visibility to ensure only addresses belonging to the intended beneficiaries receive funding. Popcorn Foundation may help interested organizations with this process at no cost after submitting a request.

Further eligibility criteria will be determined by the values defined in the Popcorn Foundation charter. The Popcorn Foundation charter will be authored and ratified by the Popcorn Foundation council to define the canonical values governing the election of beneficiaries. It is therefore a collaborative work in progress. As an example, the charter may highlight commitments to secular, environmental, educational, public health and open source initiatives which bring positive, social impact and serve the public benefit in a transparent and quantitatively verifiable way. The Popcorn Foundation charter may be amended in the future with a super majority vote of the Popcorn Foundation council.

What is PopcornDAO?

PopcornDAO is a decentralized autonomous organization of members holding Popcorn governance token (POP). They are able to vote on proposals which influence the parameters of the Popcorn smart contracts. These members are stewards of the Popcorn protocol and share the common goal of fueling the growth of the protocol, decentralizing the organization and nurturing the mission of driving social impact for the public benefit in perpetuity.

What is Popcorn Foundation?

Popcorn Foundation is an organization committed to bootstrapping the development of the Popcorn smart contracts, driving decentralization, onboarding beneficiaries and ensuring the values of the Popcorn Foundation charter are upheld by all beneficiaries.

What is the Popcorn Foundation council?

The council is a group that has been granted the ability to revoke the eligibility status of a beneficiary. They are guardians which function to maintain the integrity of the system and deter malicious actors from gaining beneficiary status. The council may be comprised of experts in education, medicine, public health, open source software, and the environment. Council members are to be nominated by the founding members. New additions and replacements to the council may be added by the existing council, or through a governance vote.

The separation of powers between the council and governance token holders can be considered similar to that of the legislative and judiciary bodies of a democratic government. Token holders elect beneficiaries and modify the parameters of open source smart contracts whereas the council ensures the elected beneficiaries adhere to the values of the charter.

What are hypothetical examples of how Popcorn can serve the public benefit?

Environment

"We do not inherit the Earth from our ancestors; we borrow it from our children."
– Native American Proverb

The current proof of work algorithms powering the Ethereum and Bitcoin blockchains have been widely criticized for their harmful environmental impact. The PopcornDAO model represents a way to offset these harmful side effects through the election of beneficiaries whose role it might be, as an example, to reduce the environmental damage caused by the electrical consumption required to run these networks. Users electing to interact with Popcorn smart contracts, may, at the same time, be contributing to the public benefit by supporting beneficiaries responsible for offsetting carbon emissions.

Free and Open Source Software

"*Only a restoration of open-source culture, and all that it enables across the full spectrum of open source possibilities, can allow humanity to harness the distributed intelligence of the collective and create … a world that works for all." — The Open-Source Everything Manifesto*

The open source software community has led to radical transformation benefiting the public - from privacy-oriented projects protecting the fundamental rights of global citizens and political dissidents, to software powering the operational infrastructure of global NGOs bringing critical medicine and support to needed communities: free and open source software promotes fair and equitable access creating opportunity in underserved and global communities alike. By using Popcorn, users, without any added effort, may be promoting the development of open source projects which create value for the public benefit.

Education, Reduced Inequality and Free Press

"Knowledge is power. Information is liberating. Education is the premise of progress, in every society, in every family" — Kofi Annan

Of late, the world has seen, on one side, the rise of extremism and, on another side, a growing authoritarianism, leading to civil conflict and unrest from continent to continent. Growing inequalities throughout certain populations put communities at a disadvantage and stifles

economic mobility en masse while threatening community and state-wide security. The link between illiteracy rates and crime have also been clearly established[2]. Educational and free press initiatives have the potential to address these issues and create an impact to better communities world-wide. By using Popcorn, users may be contributing to initiatives that make the world a more intelligent and safer place to live.

Voting

Token holders participating in Popcorn governance matters such as beneficiary nominations and grant elections must lock their tokens to receive non-transferable vote escrow tokens. Voting weight will be equal to

$$w = a\frac{t}{t_{\max}}.$$

where a is the amount of tokens locked, t is the time a token is locked, and t_{max} is the maximum amount of time a token can be locked for. The exact implementation details for voting weight may include other mechanisms described by CurveDAO's governance whitepaper[3] such as a decaying vote weight over time. Additionally, in order to introduce Sybil-resistance, a trust score multiplier may be included for accounts which have verified their identity. The multiplier will give the token holder additional voting power.

There may be one of three modes of voting enabled at any one time:

1. Capped - a cap on voting weight will be enforced
2. Unlimited - no cap on voting weight will be enforced
3. Fixed - verified addresses with a minimum trust score will receive voting power proportionally to their trust score.

How does Popcorn prevent against Sybil-attacks, bribery and collusion?

Popcorn will be resilient to Sybil-attacks by implementing privacy-preserving pseudonymous identity verification for on-chain voting with services like BrightID or other specialized oracle solutions. To prevent against bribery and collusion, zero-knowledge cryptographic schemes such as those described by Vocdoni[4] or MACI[5] (Minimal Anti-Collusion Infrastructure Framework) will be implemented.

---

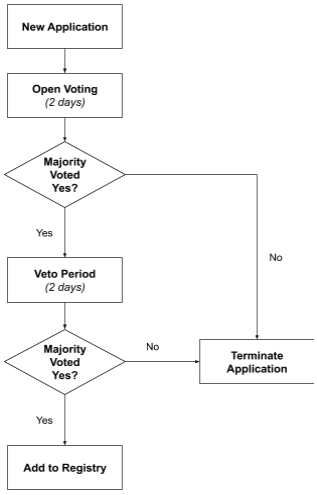
[2] http://www.worldliteracyfoundation.org/The_Economic_&_Social_Cost_of_Illiteracy.pdf
[3] CurveDAO Governance Whitepaper: https://www.curve.fi/curve_whitepapers/CurveDAO.pdf
[4] Vocdoni: https://vocdoni.io/
[5] MACI (Minimal Anti-Collusion Infrastructure Framework): Buterin, Vitalik: https://ethresear.ch/t/minimal-anti-collusion-infrastructure/5413

Beneficiary Nomination and Takedown Functional Specifications

There is a multi-stage process for an organization to become eligible to receive a grant. To summarize, first prospective organizations must be nominated to become eligible beneficiaries through a Beneficiary Nomination Proposal. Only successfully nominated beneficiaries may be considered for grants. Grants are *fixed-term* meaning that they are only awarded for the length of the term defined by the grant. A grant term can be 1 month, 3 months, or 12 months. Grants are awarded to certain top ranking beneficiaries as voted on by the governance token holders. Those beneficiaries awarded a grant will receive a percentage of fees collected by Popcorn smart contracts for the duration of the grant term.

1. Beneficiary Nomination Proposal: For an organization to become an eligible grant recipient, a Beneficiary Nomination Proposal (BNP) must be raised and, the proposal must receive a majority of votes cast towards "Yes" with at least 10% of the available supply of governance tokens voting "Yes". As a spam prevention mechanism, members wishing to nominate a beneficiary through a BNP will be required to lock at least 2000 PopcornDAO governance tokens for the duration of the BNP process.
    a. An organization wishing to apply for eligible beneficiary status may acquire the requisite number of tokens to raise a BNP, or they may reach out to the Popcorn Foundation to seek a nomination at no cost.
    b. Supplementary application materials, such as mission statement, proof of address ownership and links to impact reports will be included as an IPFS content hash.
2. Beneficiary Nomination Challenge Period: If a BNP passes the first phase of voting with a majority of votes, there will be a subsequent 2-day challenge period where users may challenge and veto the BNP. During this phase, users will only be able to vote "No" to veto the BNP. This additional phase in the BNP voting process prevents exploits where a flood of late "Yes" votes swings the results. At the end of the challenge period, if the BNP receives more yes votes than no votes, the elected organization will become eligible to receive grants as an *eligible beneficiary*.

Flowchart [6]:



[6] source: https://medium.com/marbleorg/introducing-humanity-90ddf9ead235

3. **Fixed-term Grant Elections**: Periodically, the governance token holders will elect eligible beneficiaries to receive *fixed-term grants*. Throughout the period of a year, there will be monthly, quarterly and yearly fixed-term grants awarded to beneficiaries through a quasi-quadratic voting process. Of the top ranking beneficiaries, only a certain number of eligible beneficiaries will be awarded a grant. The number of beneficiaries awarded the grant depends on the length of the grant term and the grant parameters defined in the smart contract. The grant may be awarded using some degree of randomness according to the configuration of the smart contract. This hybrid approach acknowledges Arrow's theorem, which highlights the frailty of any ranked voting system, and it further aims to combine merit, popularity and potential randomness to reduce the undue influence of over-represented stakeholders dominating the results of awarded contracts. This configurable approach allows less mainstream projects, or what may be considered to be "entrepreneurial public goods" [7] a chance to receive funding. Further rules and explanations:

    a. Eligible beneficiaries will not be allowed to apply for more than one grant at a time.

    b. An eligible beneficiary may not be awarded a fixed-term grant if that eligible beneficiary has been awarded a grant and the awarded grant term is currently active. For example, if a beneficiary has been awarded a one-year grant, then it is not eligible to be awarded another grant for the duration of the year.

4. **Beneficiary Takedown Proposals** - over the course of time, it may become necessary to remove beneficiaries from the registry. This need may become pressing if beneficiary actions violate the principles and values stated in the Popcorn Foundation charter. In the event that an eligible beneficiary violates the principles and values in the Popcorn Foundation charter, or if allocation of funds is not consistent with the charter's criteria, a Beneficiary Takedown Proposal may be raised, which upon successful execution will remove a beneficiary address from the registry.

Fixed-Term Grant Election Functional Specifications

After calling a smart contract initialization function, a grant election will be created programmatically by selecting beneficiaries that have registered their interest to be included in the grant election for the desired term-length. The initialization logic would *exclude* beneficiaries currently under consideration for another grant election and those with an actively awarded grant. Furthermore, the function would check for the existence of a currently active grant election for the selected term-length to prevent duplicate active grant elections from being created for the same term-length. The invocation of this election initialization function can be incentivized by providing a small reward to the caller of the function funded by a bond or other mechanisms described below.

---

[7] Buterin, Vitalik and Hitzig, Zoë and Weyl, Eric Glen, Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds (December 2018). Available at SSRN: https://ssrn.com/abstract=3243656 or http://dx.doi.org/10.2139/ssrn.3243656

1. Grant Election Registration

a. An eligible beneficiary must register to be included in a grant election.
b. An eligible beneficiary may be required to post a bond to register for a grant election. Details regarding bonds and incentivization mechanisms are detailed in the subsequent section.

2. Grant Election

a. Given a term-length (1 of 3 types: monthly, quarterly, yearly), a grant election initialization function will initiate an election where token holders may vote for the beneficiaries of the grant.
b. The token holders would be able to assign several beneficiaries distinct voting weights based on their voting escrow token balance available for the election.
c. The initialization function will not create multiple active grant elections for the same term. In that sense, the initialization function is to be considered idempotent.
d. The election will be active for a period of 1 week. This contract value may be adjusted by governance.
e. The initialization of each type of fixed-term grant election will be subject to a cooldown period where it will be impossible to create another election during that period of time. This cooldown period is required to space out the creation of elections over time. The cooldown period will be expressed in blocks in the smart contracts, but are described in days here for clarity. Suggested values:
    i. Monthly elections: 21-day cooldown period
    ii. Quarterly elections: 83-day cooldown period
    iii. Yearly elections: 358-day cooldown period
f. Eligible beneficiaries which have registered to be included in a grant election will be included in the election as long as the following conditions have been met:
    i. The eligible beneficiary has registered for the election and submitted the required bond (if such a bond is required by the system parameters).
    ii. The eligible beneficiary has not been awarded a grant for an active grant term.
    iii. The eligible beneficiary has not had their eligibility status revoked.
    iv. The eligible beneficiary is not under consideration for another active grant election.
g. Bonds: an eligible beneficiary may need to post a bond to register for the grant election if governance has voted to require bonds for election registrations.
    i. Under normal circumstances, the value of the bond will always be returned to the beneficiary.
    ii. If the beneficiary is not awarded the grant, the bond will be returned to the beneficiary at the conclusion of the voting period.
    iii. If the beneficiary is awarded the grant, the value of the bond will be repaid over the course of the grant term length.

iv. The bond is used as a payment to incentivize the calling of the grant election initialization function. A well-utilized system would ensure that the entire value of the bond is repaid. The bond amounts are as follows:
    1. Monthly grant: 50 POP
    2. Quarterly grant: 100 POP
    3. Yearly grant: 1000 POP

h. A separate inflationary mechanism may be implemented in place of bonds. The mechanism would mint POP tokens to incentivize the invocation of the election initialization smart contract function. The token minting contract would allow the address of the contract handling election initialization to mint and transfer a predetermined amount of POP tokens to addresses which successfully initialize an election.

i. A third option to be considered in lieu of bonds and inflationary mechanisms to incentivize the invocation of the election initialization function is to transfer a portion of fees collected by a Rewards contract to the election initialization contract. A portion of the fees transferred to the contract could then be used to incentivize the invocation of the initialization function.

3. Grant Election Voting

a. After locking tokens for a configurable period of time, token holders will receive a non-transferable amount of voting escrow tokens in proportion to the length of time they have chosen to lock their tokens. The longer a token holder locks their tokens, the more voting power they will have. The exact ratio is to be defined.

a. Token holders will use their voting escrow balance to indicate the degree of their preference for which beneficiaries should receive the grant.

b. Quadratic voting: a token holder will pay the square of the votes they assign to a given beneficiary.

c. When the voting period expires, the votes for each eligible beneficiary are tallied and then ranked.

d. If the random drawing option is enabled, top ranking eligible beneficiaries will be entered into a random drawing. A Chainlink Verifiable Random Function (VRF) would then be used to determine the awardees of the grant.

e. If the random drawing option has been disabled in the smart contract then only the beneficiaries ranked by the most votes (as determined by the quadratic function) will be awarded the grant according to the number of awardees defined by the election parameters. The following are adjustable parameters of the *grant election* contract and suggested initial values:
    i. Monthly grants:
        1. Awardees: 1
        2. Eligibility: Top 3

3. Pure LR[8]: false

ii. Quarterly grants:
    1. Awardees: 2
    2. Eligibility: Top 5
    3. Pure LR: false

iii. Yearly grants:
    1. Awardees: 3
    2. Eligibility: Top 7
    3. Pure LR: false

Additional Thoughts

The theoretical discourse surrounding governance structures, voting and welfare economics, suggest it is difficult if not impossible to implement an infallible system where the desires of the many are represented and carried out in an equitable way without the possibility of bribery, collusion, under-funding, over-funding or other failures of governance. Without a privacy-preserving voting mechanism (by using zero-knowledge proofs as an example), a system may be prone to bribery. Without a registry of eligible voters to enforce a one-person-one-vote constraint, the benefits of a quadratic voting mechanism can be partially circumvented by voting with new addresses. While the implementation of the quasi-quadratic voting mechanism with an optional selective random function as described in this paper may lead to an imperfect solution, it may be considered a sufficiently practical way to fund public goods on a public blockchain at scale, as the mechanisms described contain deterrent properties that make the system resistant to bribery, collusion, and underfunding, while at the same time it effectuates the will of voting participants. There are further considerations to examine about the governance structure of Popcorn, and they are explored in brief detail below.

The existence of guardians or a council with veto power may be considered an undesirable trait for a couple of reasons. The first is that the neutrality of the guardians may come into question and allows for subjectivity in the beneficiary revocation process. A second argument can be made that the guardians represent a point of centralization. While these arguments may be true, the existence of a council presents a practical safeguard and deterrent against the threat of collusion and elections in which malicious actors are awarded grants. A malicious actor can be defined as an organization which is awarded a grant, but does not meet the basic criteria for receiving a grant such as providing a public good. The council is a practical and necessary compromise which balances the shortcomings of a system that is not entirely Sybil-resistant and one in which the economic incentives for fraudulently winning an election may become greater as the system generates more value.

There does exist a distinct yet unlikely scenario where a malicious actor can somehow pass the nomination process and be awarded a grant without a veto because of a bribery or collusion scheme. Such a scenario

[8] If enabled, the Pure LR parameter would award the grant to all beneficiaries registered for the grant and provision the funds according to the quadratic voting function formula. In the case this parameter is enabled, governance might choose to also disable all but one or two grant term elections for simplicity.

may involve collusion or bribery to the extent that a requisite amount of voting power is obtained and the council is bribed or involved in such a scheme to prevent the removal of a beneficiary. In the event that such a scenario were to occur, the reputation of a system purporting to generate positive social impact might be severely harmed and thus the value generated by the system would be negatively impacted to the extent that an attack may not be economically justified in the long term. The likelihood of such a potential occurrence might be rare, but with a diverse array of council members, the issue is mitigated to a certain extent.

Another attack vector presents itself with a wide array of diverse, publically elected council members. Council members may revoke legitimate beneficiaries to the extent that their preferred beneficiary is promoted and has an increased chance of being awarded a grant. This attack vector can be mitigated in a few ways. As an example, there could be a limit imposed on the amount of revocations made available to any one council member. Additionally, governance and council members may be granted the ability to remove or penalize a council member. Lastly, third-party decentralized solutions like Aragon Govern and Kleros may provide drop-in solutions where disputes about beneficiaries may be sent for arbitration. These mitigation options may provide solutions to further decentralize governance and are worthy of exploration in the future.

There are several ways to configure the governance parameters of the Popcorn smart contracts. Each variation of the configuration provides certain benefits while assuming trade-offs. The system described affords governance an opportunity to configure system parameters to respond to different levels of volume, participation, and market conditions. The flexibility in configuration also allows the system to be dynamically resistant to attacks to a certain extent by discouraging certain types of deleterious behavior such as collusion and bribery. Overall, Popcorn is designed to be flexible and resilient considering a number of potential future scenarios, but a long-term effort will be required in order to further decentralize governance and bring greater protections to the voting process.

Summary

Through the development of yield-generating DeFi products, and the implementation of participation incentives, it is possible to create a sustainable system which generates and shares value among different classes of participants. The implementation of a quasi-quadratic voting mechanism, leads to a practical way of funding beneficiaries which may lead to social impact at a large scale. Ultimately, the success of the system described in this paper relies on innovative DeFi products, and a community which believes and adopts the mission.

Popcorn fundamentally is an experiment. At a minimum, it might provoke curiosity and inquiry into alternative forms of governance and social impact methodologies. At best, within the context of the Popcorn DeFi products, it will remove all barriers to creating positive social impact for the public benefit in perpetuity.