Galactica's Reputation Framework Design

August 24, 2022
Version: 1.0

Introduction

Since the inception of blockchain systems, now under the nomenclature of *Web3*, they have been almost entirely econo-centric in nature. With Bitcoin and other forerunners conceived out of the collapse of the global housing market in 2008 [1],their mandate has been largely economic in nature.

Following the maturation in the 'store of value' domain, research into new fields intensified, more specifically, effective decentralized governance. Communities have always formed around the many tokens in the industry but they were usually simple, based on systems with a central authority (generally the company or team leading the project) [2]. However as smart contract technology began to mature it enabled communities to move closer to a truly self-governed state [3]. The community now had the capability to create proposals that would change system parameters and characteristics and they would, themselves, accept or decline these proposals - the DAOs emerged [4].

Like in any decentralized governance model, users that participated (by purchasing the token normally) were assigned some voting power and with it they could vote on system changes [5]. In almost every DAO the voting power was a (most often linear) function of the user's staked/held number of tokens - large stakers would have more voting power than smaller less [6]. Naturally, these systems are relatively simple to implement and larger stakers/holders would have more to lose if the system does not operate in the way it was supposed to [7], [8], [9].

Since the discrepancy in investable capital of whales and average retail users is non-negligible, DAOs have traditionally been captured by a few whales, founders or team members [10]. An examination of on-chain voting outcomes confirms that a handful of wallets are the deciding factor in an election [11] thus proving that most DAOs have evolved into power monopolies and run contrary to their founding ideals. This token-based oligarchy [12] is the logical outcome as DAOs (in their current form) are inherently capitalistic systems. These systems will always tend towards highly concentrated power structures: disproportionate distribution of wealth with **one-token-one-unit** of voting power may and will lead to some form of soft dictatorship, since the cost to collude for whales is comparatively small [13].

The oligarchification of DAOs was addressed through various means by protocols and leaders in the industry, but as Vitalik Buterin stated: "Social trust assumptions seem secure and controllable, in the sense that "people" are in charge, but in reality they can be manipulated by economic incentives in all sorts of ways" [14]. While this problem of power concentration affected various DAOs, proposed solutions were simply insufficient. The two most critical vectors were not properly addressed, that of Sybil Resistance and proper user incentivization within governance and DAO systems [14].

For our somewhat narrow context, Sybil resistance shall refer to the ability for DAOs to prevent attacks from actors creating replicas or copies of themselves for malicious intent [15]. With the current technical structure of token based voting systems most DAOs are *Sybil Susceptive*. Malicious actors need only

acquire large amounts of token and populate alternate wallets with said tokens turning a whale account into many smaller sharks that can be socially engineered to come off as real individuals [16].

The answer to the Sybil conundrum lies in *transferability*, wrote Vitalik Buterin, "there are very bad things that can easily happen to governance mechanisms if governance power is easily transferable." [17]. Stripping generic DeFi governance tokens of their ability to participate in voting and instead embedding governance powers in tokens that are *soulbound* [18] permits meaningful governance systems to finally arise. Moreover, soulbound tokens open new opportunities for innovations within DAO governance. Protocol contributors, who lack the deep capital of whales, can be justly rewarded for their efforts and interactions with the community. That is to say, reputation systems can be developed where an actor participating in the DAO is more relevant than any number of tokens they've acquired [19].

The soulbound token concept, as a remedy to DAOs' sybil susceptibility [20], ties into previously proposed solutions particularly the shift from direct token democracies to more representative governance structures. Published in A16z's *Lightspeed Democracy* article: "[representative governance elements] can include explicitly defining the roles of internal units, requiring certain expertise from representatives making decisions regarding those units, and ultimately leaving strategic capital allocation decisions to all voters as a check on the organization itself" [21]. This ultimately allows for more political scalability and organizational effectiveness as more individuals can specialize into the different technical niche's covered by a DAO (see MakerDAO's Core Units [22]).

Moreover, the achievement of sybil resistance by DAOs then supports further governance abstractions; particularly Quadratic Voting and Funding. These quadratic mechanisms are exploitable by Sybil attacks (Gitcoin developed multiple means of maintaining its resistance [23]) but with soulbound tokens and reputations systems in place these systems can be deployed. This equips DAOs with a more reliable and informative voting and funding structure that primarily enhances their effectiveness and social composability [24] [25].

The introduction of soulbound tokens, which then forms the foundation for our proposed reputation system, addresses many of the governance exploits, attacks and other failings witnessed since the advent of Web3 governance. It provides substantial increases to sybil resistance and allows for innovations such as quadratic voting to be deployed adding mechanical depth to governance decisions. Put plainly, soulbound tokens and reputation systems in DAOs shifts them away from their hyper financialized nature and refocuses them back on individuals, their social interactions and the very community that comprises the organization.

Reputation

Galactica proposes a new governance system, one that can quantify a user's behavior history and from that decide how much voting power one will accrue, in

a fully decentralized manner. The parameter that would represent this variable is named **Reputation**.

Being involved in the governance process, creating well-accepted proposals, proposing project ideas that bring benefits to the system would be rewarded through reputation. The Reputation function is non-negative and it maps users' addresses with real numbers. System dynamics will change this map in a deterministic manner and always produce a unique value for each user.

Galactica will be governed by merit and actions' impact on the well-being of the whole ecosystem. It will be up to the people to determine what is "good" and "bad". In the long run, because Galactica will become this merit-governed system, the initial discrepancy of wealth distribution will be mitigated and in the future totally neutralized. Galactica's emphasis on a long time frame is one of the factors that guarantees the evolution towards a meritocratic system.

On a more technical note, Reputation in the Galactica system will be managed by the **Galactica Reputation Root Contract (GRRC)** - a protocol-level method that generates an on-chain Reputation score for every existing address using an arbitrary function that is user-defined. In other words, anyone can create a signature metric by which they wish to measure the Reputation of the users they will be interacting with.

This condition also holds if a project wants to work with a subset of users - a good example would be a lending protocol that wishes to allow its user the possibility to take undercollateralized loans. They will have the freedom to choose the parameters and functions they wish to take into account when calculating the user's Reputation. The only condition that is set in stone is that these parameters must have **on-chain data as input**. Going forward any address can set *contingent transactions* upon the sender/receiver Reputation score (that they will be able to calculate in any way they wish using the inputs they have access to).

Generalized reputation function

A generalized formula can be introduced here, but it is important to keep in mind that its primary purpose is to give a good Reputation foundation to the system at protocol start. Nevertheless it can be changed by anyone for personal use and by The Parliament for protocol purposes.

Parameters will be denoted by x_n where n goes over all parameters (on-chain inputs). Let us say that there are N parameters, a generalized formula for Reputation calculation can be defined as:

$$Reputation = \sum_{p=1}^{N} \sum_{i_1=1<i_2<\ldots<i_{p-1}<i_p}^{N} \alpha^{p}_{i_1 i_2 i_3 \ldots i_p} x_{i_1}^{\beta_p^{i_1}} x_{i_2}^{\beta_p^{i_2}} x_{i_3}^{\beta_p^{i_3}} \ldots x_{p-1}^{\beta_p^{i_{p-1}}} x_{i_p}^{\beta_p^{i_p}}$$

The formula presented above is a parametrized sum of all possible parameterized x_n inputs raised to a given power. Furthermore all 2-products, 3-products, ... N-products are also included.

Initial Definition of Voting Power & Reputation

Cautious readers will find a problem with the ideas presented above. In order to change the reputation function by the DAO, the DAO must initially be designed with reputation in mind - the definition is somewhat self-referential. The initial definition of Voting Power (VP) and Reputation must be created and with it the DAO. The exact reputation function is to be defined at a later stage but here we can take a look at the properties it should have and how it contributes to the Voting Power function.

Voting Power function depends on the amount of Galactica tokens held and the Reputation. The ideas described further have been inspired by the recent body of literature on Quadratic Voting/Funding [24], [25], [26].

VP - Tokens Held

VP as a function of Galactica held by an account is an increasing function (first derivative greater than 0) and concave (second derivative smaller than 0). For a small amount of Galactica, a balance will initially increase rapidly but as the amount of tokens becomes larger its ascent will slow (however will always remain rising). In this way it creates strong incentives in the beginning so that new users can acquire a fair amount of tokens in a reasonably short period of time while those users interested in acquiring more outsized amounts will be able to work towards those tokens over longer durations.

Moreover, the amount of tokens required at protocol inception to have sizable voting power is comparatively small thus no favoritism is exercised towards the whales. Galactica maintains this property as voting power will rise at increasingly slower rates meaning that holding large amounts of Galactica yields lower and lower voting benefits (per one Galactica held).

VP - Reputation

VP as a function of Reputation held by some account should be an increasing function (first derivative greater than 0) and convex (second derivative greater than 0). These properties imply that a relatively small initial Reputation score will have a minor impact on VP. However, as users gain more and more reputation the effect will be disproportionately larger, and at some point a unit of reputation will be worth more (in terms of contribution to VP) than one unit of Galactica held.

VP - Functional Form

Besides the aforementioned properties, the VP function (by itself) must be expanded. If a user has either 0 Reputation or 0 Galactica tokens held the total VP must be equal to 0. This property inevitably leads to the following condition: if a user wishes to possess non-zero VP with either of the two equal to 0 then that user must have an infinite of the other one. In graphical terms this means that the VP a equals non-zero constant - the VP curve will never cross

the X and Y axes.

The following VP function is defined:

$$VotingPower^{User} = (Galactica_{held}^{User} * p)^{\alpha} * (Reputation^{User} * q)^{\beta}$$

where:
$\alpha = 0.5$
$\beta = 2$
p, q - amplification parameters (to be defined)

Reputation System Augmentation - SBTs

To bring about an explicit meritocracy Reputation by itself would be insufficient. Consider the following thought experiment:

> *A novel topic within the Galactica system is introduced as a proposal and the proposal originator believes that its consequences (if accepted) would bring significant benefits to the ecosystem in the form of some Public Good.*

The system presented above would not be of a meritocratic nature since the users that have earned their Reputation over time and would hold the strongest votes may know nothing about the topic that had been presented. One should have a representation of their real-world knowledge on the blockchain, since the topics can correspond to something outside of the blockchain domain, trivially.

Reputation by itself cannot make this distinction between users, therefore another mechanism must be introduced here - **Soul Bound Tokens (SBTs)** . SBTs are non-transferable, revocable tokens that represent commitments, credentials, affiliations and participation - accounts that possess SBTs are henceforth denoted as **Souls** [17], [18].

One can look, naively, at SBTs as a condition that defines a set - in mathematical terms. Every inequivalent SBT defines itself as an inequivalent set - that is, if a user possesses some specific SBT then that user belongs to a set defined by the said SBT. Following this line of reasoning, every user is an intersection of SBT sets and is characterized by them (by the SBTs one possesses) – a realization of *individuality* and *humanity* on a blockchain.

Like-minded individuals are more likely to have large overlaps between the SBTs they possess and those that do not belong to the same social circle, or are with the same interest, would have close to no overlap.

Within the same ecosystem multiple “societies” can emerge and the SBT mechanism would create a less granular picture of the ecosystem as a whole. A user that has a PhD in the field of Nuclear Fusion should have VP with a larger weight if such a project was brought up in the Galactica ecosystem. On

the other hand, projects can specifically target some SBT-defined social circles or specific users and distribute some rewards across them only.

SBTs have no quantitative value per se, they represent whether a user belongs to a set. Emerging societies, as coined in Weyl, Ohlhaver, Buterin (2022) [18] would have their own substructures (sub societies) and would thus create a metric, which may be, among others, utilized to:

1. Gauge system decentralization (e.g. Nakamoto Coefficient);
2. Determine how and to who of Universal Basic Income (UBI) should be distributed;
3. Unlock undercollateralized lending markets through reputation and SBTs;
4. Enable decentralized key management;
5. Compensate for coordinated strategic behavior;
6. Create novel markets with decomposable, shared rights and permissions;
7. Promote interdisciplinary expert research;
8. Create a meritocratic governance system in the long term.

Sybil Resistance - SBTs

Decentralized Autonomous Organizations (DAOs) are blockchain-specific communities that organize themselves around a common purpose with the use of smart contracts as public means of decentralized decision making. The value embedded in the DAO concept is immense - community-built projects inherit sovereignty and self-governance. However, the Web3 paradigm, being centered around anonymity and economy, implies some blockchain-native vulnerabilities, one of which is the **Sybil attack**.

A Sybil attack is defined as an attack on computer network service (in this case blockchain) in which an attacker subverts the service's reputation system by creating a large number of pseudonymous identities and uses them to gain a dominant position. A single user can create multiple wallets to collect immense amounts of voting power. In one-token-one-vote DAO governance systems, a user can simply accumulate tokens, in multiple accounts, until which eventually represent 51% of the system's total VP. If that is to happen in systems that require at least 51% VP then a transition into dictatorship is inevitable.

Sybil attacks can be at least mitigated in through the implementation of SBTs:

1. Unique SBTs are hard to obtain. If an account is relatively old and holds only SBTs that can be easily obtained, it can be tagged as one that is Sybil attack prone and its VP can be reduced;

2. Accounts holding rare, unique and reputable SBTs can be considered as low risk when it comes to Sybil attacks and therefore their voting power does not need to be reduced. Some examples would be education credentials, designations, work-related credentials, licenses and other;

3. Calculating correlation between votes over different SBT sets as proposed by Weyl, Ohlhaver, Buterin (2022) [18].

Human behavior is rarely purely altruistic or purely selfish, yet mechanism design today assumes atomized, selfish agents without pre-existing cooperation [18]. These funding mechanisms are vulnerable if one accounts for user (or social circle) collusion. Even Quadratic Funding experiences issues since it assigns more weight to the number of people that voted for some option rather than the total amount deposited. If one does not exclude the possibility of Sybil attacks, then these funding mechanisms can be exploited.

SBT systems can only mitigate the consequences of these problems rather than attend to the cause itself. A16z aptly pointed out that "designers could require some sort of user authentication for participating in votes, such as a KYC (know your customer) check or reputation score threshold" [20]. Vitalik Buterin further explains this in his Quadratic Primer article: "Quadratic payments in any form require a model of identity where individuals cannot easily get as many identities as they want" [25]. So SBT mechanics can assist in Sybil attack mitigation, KYC and identity features must be incorporated to ensure that there is a guaranteed resistance.

Sybil Resistance - Galactica

The main differentiator between Galactica and other networks is its built-in strictly optional Zero-Knowledge KYC (zkKYC) process. For technical details see Galactica's zkKYC Design paper.

Designated KYC centers would confirm user credentials and post the ZK proof of that information on-chain. To all others the information would be hidden, however with the use of ZK proofs a user can selectively disclose their personal information. The KYC process will be used for translating users' achievements and certificates in the form of SBTs. The zkKYC system maintains **anonymity** and ensures **one-person-one-account** correspondence. In this line of reasoning, it mitigates the issues described, by increasing the cost of Sybil attacks, and over time, with the use of SBTs and aggregate Reputation more and more precise sets will emerge.

Societies built around these **persistent identities** [18] are transformed to purely decentralized ones, interconnected between themselves into a global net of such networks that will be henceforth named **Web4**.

With Sybil resistance in place, pure DAOs can be achieved, quadratic funding can be implemented, the free-riding problem solved, and much more.

References

[1] Bitcoin: The Final Movement to Come Out of the 2008 Financial Crash, (2018)

[2] J.Duncan (2021). Four Paradigms of Tokenized Communities

[3] A.Garcia, D.Cameron, N.E.Chavez, A.Ruckes, E.Betanzos, S.Savage (2020). Using Smart Contracts for Governance and Identity

[4] K.Kreutler (2021). A Prehistory of DAOs

[5] Governance Token

[6] V.Buterin (2017). Notes on Blockchain Governance

[7] Uniswap Documentation

[8] MakerDAO Governance

[9] Compound Governance

[10] I.Alisson (2022). Is MakerDAO Becoming 'a Company Run by Politics'?

[11] Marcus (2022). [Part 2] Talk About MakerDAO's Controversial Governance Vote

[12] Ed.Z (2022). Kleptocracy, Oligarchy and Cryptocurrency

[13] T.Hu (2021). Vitalik: Token voting should not be the only legal form of governance decentralization

[14] V.Buterin (2018). Governance, Part 2: Plutocracy Is Still Bad

[15] Binance Academy (2018). Sybil Attacks Explained

[16] A.Akamo (2022). Typo moves $36 million in seized JUNO Tokens to wrong wallet

[17] V.Buterin (2022). Soulbound

[18] E.Glen Weyl, P.Ohlhaver, V.Buterin (2022). Decentralized Society: Finding Web3's Soul

[19] D.Dive. WHY Soulbound Token?

[20] P.Garimidi, S.D.Kominers, T.Roughgarden (2022). DAO governance attacks, and how to avoid them

[21] A.Hall, P.Smith (2022). Lightspeed Democracy: What web3 organizations can learn from the history of governance

[22] B.Dale (2021). MakerDAO Moves to Full Decentralization; Maker Foundation to Close in 'Months'

[23] Owock (2022). Characterizing the Sybil Resistance Problem

[24] V.Buterin, Z.Hitzig, E. Glen Weyl (2018). Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds

[25] V.Buterin (2019). Quadratic Payments: A Primer

[26] V.Buterin, Z.Hitzig, E. Glen Weyl (2020). A Flexible Design for Funding Public Goods