Galactica Whitepaper

Version 1.0
Oct 30, 2022

Executive Summary

Galactica Network is an L1 with unique protocol properties. Powered by zero knowledge cryptography, Galactica aspires to be the first chain with KYC-contingent transactions. This means that accounts and smart contracts can choose to interact only with other accounts fitting a given profile. This also means that sybil resistance is built directly into the protocol.

Protocol level Sybil-resistance enables persistent web3 identities, which allows for a much richer societal substrate to exist on-chain. We refer to this setup as a Cypher State. In layman terms, a Cypher State is a society with all its intricate links and relations existing and interacting directly on a blockchain.

Use cases of Galactica must speak for it better than any jargon heavy elaboration on the tech itself:

1. zkKYC: a user can prove that one is not from prohibited jurisdictions without revealing any more personal data. Same works for age, sex, etc;
2. Medical data records and AI algorithms that can be verifiably used and paid for directly on-chain;
3. MPC-enabled federated learning, anonymous voting with provable results, etc;
4. Undercollateralized DeFi: Only KYC'ed users can interact with a DApp and get a <100% collateral ratio, which dynamically decreases the more one is using the said DApp;
5. Closing the gender wage gap by shielding KYC gender information with zero knowledge;
6. The ultimate use-case, however, is a *Protocol Citizenship.*

Introduction

This paper is intended to give a high level overview of the theoretical framework behind and technological implementation of the Galactica Network, an L1 protocol with heavy focus on account level privacy powered by zero knowledge cryptography and protocol level compliance powered by zkKYC. zkKYC bootstraps the protocol level Sybil resistance. With time, as the number of account and contract interactions increases, the growing Web3 footprint of accounts makes them progressively more heterogeneous, further increasing the cost of Sybil attacks. This setup enables non-trivial societal substrate to exist purely on-chain (i.e. without reliance on Web2) and to transcend the domain of DeFi for on-chain user interactions. A resulting protocol, one that is owned and governed by highly heterogeneous on-chain identities can be referred to as a Cypher State. These identities can be referred to as Protocol Citizens.

The following graph illustrates the conceptual framework underpinning Galactica Network design. It is also instrumental to understanding how this paper is structured.

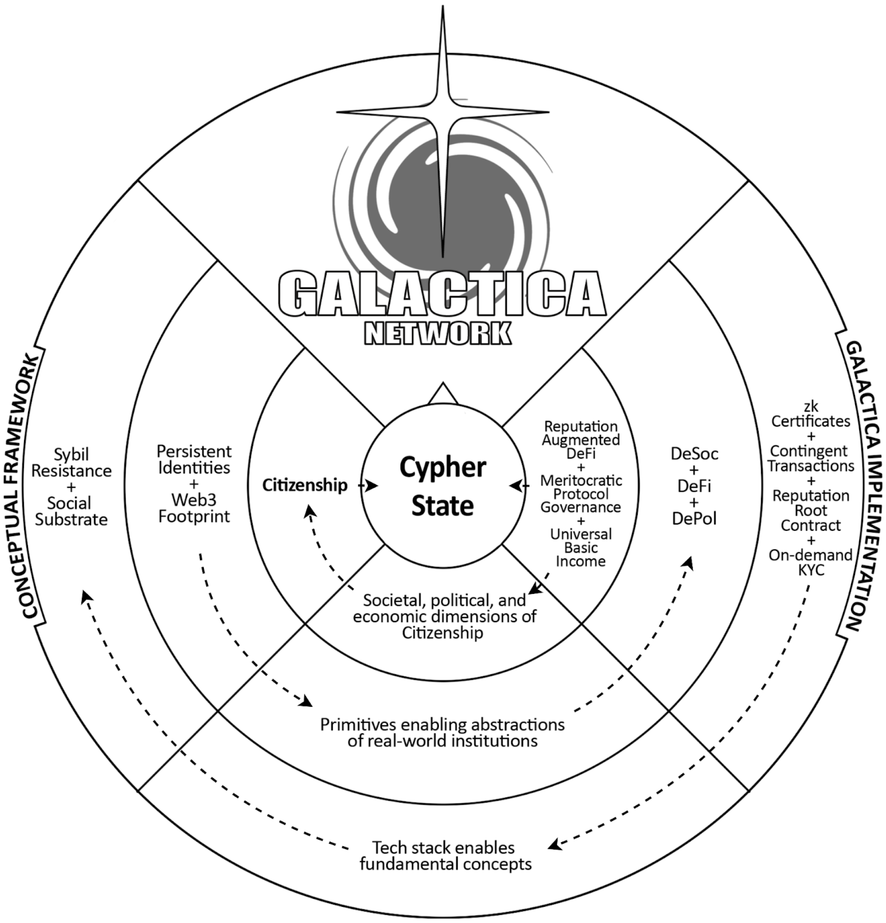

GALACTICA
NETWORK
CONCEPTUAL FRAMEWORK
GALACTICA IMPLEMENTATION
Sybil Resistance + Social Substrate
Persistent Identities + Web3 Footprint
Citizenship
Cypher State
Reputation Augmented DeFi + Meritocratic Protocol Governance + Universal Basic Income
DeSoc + DeFi + DePol
zk Certificates + Contingent Transactions + Reputation Root Contract + On-demand KYC
Societal, political, and economic dimensions of Citizenship
Primitives enabling abstractions of real-world institutions
Tech stack enables fundamental concepts

Figure 1: Galactica Network Concepts at a glance

Figure 1 provides a holistic overview of the crucial concepts that that enabled our notion of a Cypher State. The concepts and technologies mentioned become more nuanced with each successive inner ring until, at the center, the idea of citizenship within a true implementation of a Cypher State becomes a possibility.

Each ring within Figure 1 is representative of a chapter within this paper, which we shall set out below for the reader's convenience.

The outermost ring details the ability of Galactica Network's tech-stack to provide both strong Sybil resistance, in addition to a rich social substrate upon which to build.

Progressing toward the center, the second of the rings attempts to impress upon the reader how the emergence of ‘Persistent Identities’; enable analogues of societal, economic, and political institutions to exist on the Galactica Network.

The third ring describes Galactica Network’s derivative institutions that act as the social, political, and economic pillars of the Cypher State.

At the center of Figure 1 lies the concept of citizenship; enabled by the previously described layers, citizenship is one’s claim to right of governance, wealth distribution, and fundamental ownership of the Galactica Network.

Societal Substrate and Sybil Resistance

Today’s societal building blocks (e.g. celebrities, families, employers, experts, diplomats and ambassadors, and citizens) have proven to be challenging to transcribe into the virtual space (even more so for blockchains). Without a primitive, or a set thereof, that can represent people themselves, the vast number of mutual relationships by which they are interconnected is difficult, if not impossible, to replicate in a decentralized protocol. [1]

In order to understand why this is the case, we have to take a step back and consider the notion of Sybil Resistance. While not being a formal definition, the following will suffice for our purposes: *Sybil resistance is the ability of a protocol to withstand attacks using a large number of pseudonymous identities to gain influence. Galactica achieves high Sybil resistance by enabling a direct mapping between real-world persons and internet identities.*

Web2 applications solved the problem of Sybil resistance by requiring users’ personal data, and imposing draconian compliance standards. An obvious requirement to impose such standards is having access to users’ data (that can be monetized, and as such is both the critical resource of the data economy, and the fuel of big tech business models). Thus, Web2 Sybil resistance came at the expense of extreme centralization and de-facto elimination of users’ privacy.

Most contemporary Web3 protocols record transactions in a pseudonymous fashion; anyone with an internet connection can create a large number of wallets on virtually any blockchain. Pseudonymous by design, cotemporary Web3 is fundamentally unable to model non-trivial societal primitives: that’s why concepts like celebrities, families, employers, experts, diplomats and ambassadors, criminals, and citizens are all meaningless on-chain.

Summarizing the above and without loss of generality, we can posit that Web2 has sacrificed privacy at the altar of Sybil resistance for the benefit of rents extracted from the emerging data economy. Web3 has done the exact opposite. In the case of Web2, the cost of Sybil Resistance is digital dictatorship, censorship, and an adverse status quo in respect to data economy we know all too well from our everyday experience. In the case of Web3, the cost of Sovereignty is Sybil Resistance and, thus, drastically reduced attainable complexity of societal substrates that can be modelled on-chain.

As it stands, people cannot be meaningfully on a pseudonymous blockchain protocol.

But if such representation existed, what would we call it, how would it work, and what would be the implications? In what follows we make an attempt to answer these questions.

Persistent Identities and Web3 Footprint

First, let us introduce some important definitions:

a. A human in the blockchain space could be referred to as a *Persistent Identity*;

b. The multitude of interactions between any such identity and the rest of the protocol could then be called one's *Web3 Footprint*.

Let's unpack the relationships between the two. In this context, "persistent" means that the protocol representation of a human, a private key, or a set thereof, corresponds to a real-world person or identity, that such on-chain identities are costly to duplicate and, ideally, this cost increases over time. This latter property is quite subtle. Why is it desirable? It increases the cost of a Sybil attack as the protocol evolves. Think about a *bitcointalk.org* account. The older and more ingrained into the fabric of the forum it is, the costlier it is to replicate.

It is one's Web3 footprint that defines an on-chain identity and naturally, this footprint increases in size and complexity over time, making it increasingly difficult to replicate or tamper with.

Is there a more intuitive way to define the Web3 footprint, and perhaps bring it closer to something familiar from the off-chain world?

We believe so, and it's the concept of reputation that is semantically closest in our view.

Let us reiterate: the Persistent Identity is defined by its Web3 footprint - the relationships between an account, other accounts, and the system itself. Through one's Web3 footprint, users' impact on the network can be quantified by other users, thus defining a virtual correspondence to a real-world concept of reputation.

Notions of Persistent Identity and Web3 footprint together enable non-trivial societal institutions to be modeled entirely on-chain - in largely the same way as the EVM's Turing completeness has enabled the elaborate transactional logic and ultimately the emergence of complex economic institutions in what's today known as DeFi.

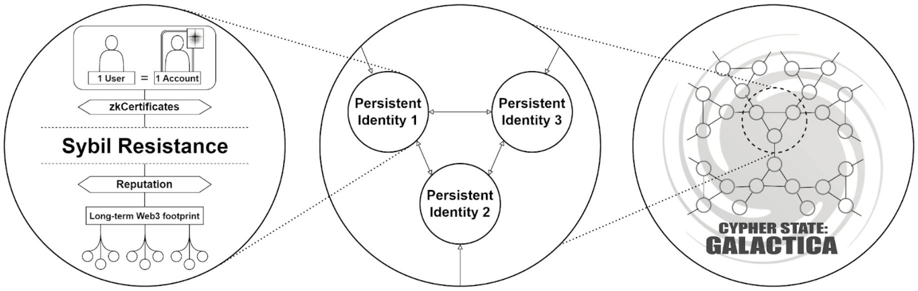


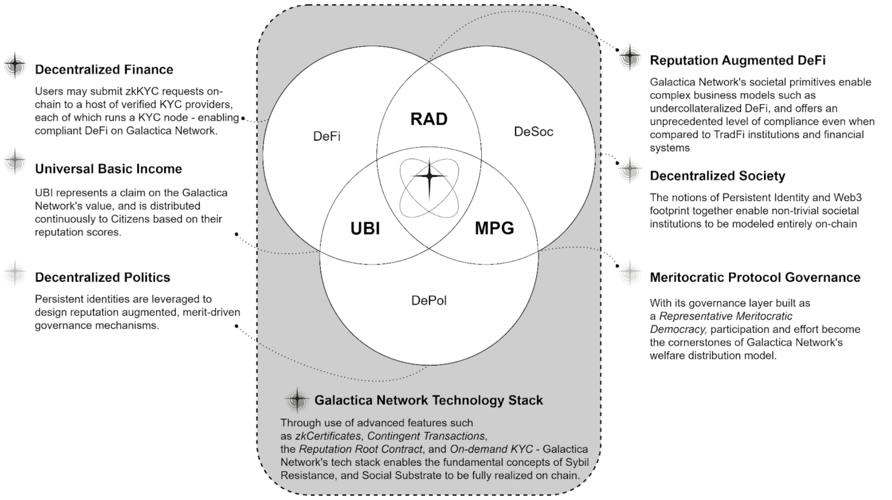
Figure 2: Persistent Identities and the Cypher State

Galactica Network

Galactica Network is designed to be a protocol owned and governed by its Citizens.

Understanding the concept of a Galactica Network Citizenship (henceforth, GNC) as well as that of protocol ownership requires some background knowledge of the technological, economic, and societal primitives that shape the protocol, its incentives, and the interactions of its agents.

Galactica Network Technology



Decentralized Finance

Users may submit zkKYC requests on-chain to a host of verified KYC providers, each of which runs a KYC node - enabling compliant DeFi on Galactica Network.

Universal Basic Income

UBI represents a claim on the Galactica Network's value, and is distributed continuously to Citizens based on their reputation scores.

Decentralized Politics

Persistent identities are leveraged to design reputation augmented, merit-driven governance mechanisms.

Reputation Augmented DeFi

Galactica Network's societal primitives enable complex business models such as undercollateralized DeFi, and offers an unprecedented level of compliance even when compared to TradFi institutions and financial systems

Decentralized Society

The notions of Persistent Identity and Web3 footprint together enable non-trivial societal institutions to be modeled entirely on-chain

Meritocratic Protocol Governance

With its governance layer built as a *Representative Meritocratic Democracy,* participation and effort become the cornerstones of Galactica Network's welfare distribution model.

Galactica Network Technology Stack

Through use of advanced features such as *zkCertificates*, *Contingent Transactions*, the *Reputation Root Contract*, and *On-demand KYC* - Galactica Network's tech stack enables the fundamental concepts of Sybil Resistance, and Social Substrate to be fully realized on chain.

Figure 3: The Galactica Network Technology Stack

Let us begin with technology. We would like to note that the following is not an exhaustive description of the tech that powers Galactica Network.

Instead, it is a brief description of the primitives that make the concept of GNC meaningful. An inquiring reader is directed to Appendix I - Galactica's Zero-Knowledge KYC Design for comprehensive information on other aspects of Galactica Network technology.

Galactica Network Technological stack is a set of protocol primitives that when combined enable strong Sybil resistance, account level privacy and protocol level optional compliance. These properties enable the protocol to be a platform for modeling meaningful and feature rich social and political institutions.

zkCertificates

zkCertificates, are non-transferable (a.k.a. soulbound) NFTs with arbitrary metadata that come with an option of selectively disclosing said metadata through the use of zero-knowledge cryptography. zkCertificates can be implemented in a variety of ways, some vanilla, and some more exotic in nature.

One of the most obvious applications is that of zkKYC, zk-university diplomas, and other forms of attestation. More advanced options are the encrypting of medical data records and other forms of PII/PHI, voting data, government records, and citizen data (think taxes, property titles, etc.). More advanced use cases are machine learning algorithms that can *verifiably* be used and paid for directly on-chain without exposing the data sets used to train the models, nor the models themselves. zkCertificates can also be used to enable Multi-Party-Computation (MPC) powered federated learning routines over user data.

A basic example is a DEX with leveraged instruments that are only available to users over the age of 21. Using zkCertificates one can prove his or her age, satisfying this criterion without revealing the age itself or any more personal information. The same goes for a use case of, say, initiating Initial DEX Offering (IDO) pools that would be non-accessible to citizens from specific jurisdictions.

Reputation Root Contract (RRC)

The Reputation Root Contract, or RRC, is a smart contract available to Citizens (for the time being, think of Citizens as simply a subset of the active user base) of Galactica Network. When used, RRC is fed an arbitrary function that takes on-chain data as input and outputs a unique Reputation score for every account. The reputation score of an account is a measurement of one's Web3 footprint evaluated over a subset of available on-chain data points.

An example of applying RRC would be to generate a score for every account, whereby a 1 or a 0 is granted for the presence or absence of a KYC record respectively, which would then be multiplied by the square root of the age of the account. This function would produce a (perhaps oversimplified) trust score. If the account is not zkKYC'ed, the score is always 0. But if on the other hand, it is, the trust score would increase sublinearly in the age of an account.

A much more elaborate discussion regarding creating an abstraction of reputation on-chain can be found in Appendix II - Galactica's Reputation Framework

Design.

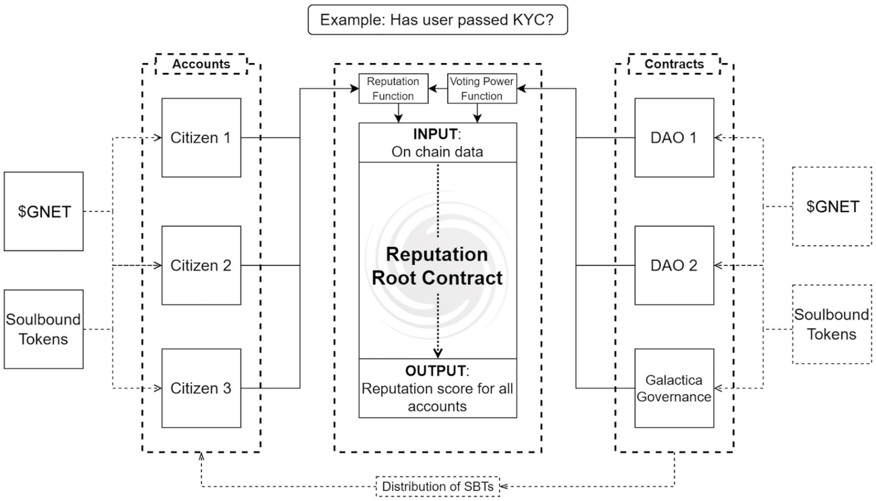


Figure 4: Galactica Network Reputation Framework

Contingent Transactions

Contingent transactions can be created by utilizing the outputs of RRC to create dynamic transaction rejection/acceptance rules (e.g. dynamic whitelists), as well as fine-tuning the rules of interaction. Let us break this down:

1. The output of RRC can be used to determine whether an account is allowed to submit a transaction to another account (e.g. only zkKYC'ed users can interact with a DEX or else the transaction will fail);

2. The inner logic of a decentralized application (DApp) can be conditioned upon the score produced by the RRC (e.g. zkKYC'ed users are allowed to borrow at a 90% collateral ratio, while non-zkKYC'ed users need to post 200% collateral);

3. It shall be noted that contingent transactions can be programmed to combine several RRC outputs creating space for more complex rules of interaction.

While seemingly trivial at the outset, the significance of contingent transactions cannot be understated, especially when combined with other primitives discussed in this section.

For example, when combined with zkCertificates, contingent transactions could create peculiar use cases, such as allowing users who have been active on a cryptography-focused research forum to be granted greater weight when voting for a proposal to which this expertise is relevant. This weight could be further *increased depending on the university they attend, the company they work for, their level of expertise, and other factors that influence their credibility. Importantly, by harnessing the power of zero-knowledge cryptography, voting can be made anonymous.*

Guardians

The fourth primitive powering the technology of Galactica Network is users' ability to submit KYC requests on-chain to a host of verified KYC providers, each of which runs a Galactica Network Guardians (KYC node). Relevant documents are submitted off-chain and are never stored on-chain, however, the KYC nodes - after making a decision to approve the authenticity of the documents submitted - do so by cryptographically signing the issued zkKYC.

All KYC data is stored in two distinct instances: off-chain at KYC providers' back office systems, and off-chain on the user's device (mobile, desktop, or otherwise). More importantly, however, is that by design KYC providers cannot associate a set of documents with the user's on-chain account. In other words, while a KYC provider knows which accounts it has signed (this much is known to anyone as every KYC provider runs its own node), the link associating an account with an off-chain KYC record is encrypted. The only aspect of this process that appears on-chain is the recording of the KYC record encryption event itself, as a verification of its occurrence.

Another important property is that although said link cannot be associated with an account, it can be decrypted using a m of n decryption scheme using Shamir's secret sharing.

While the actual implementation of the decryption procedure is clear, it is to be decided the set of entities that will participate and will likely vary by jurisdiction; we can speculate on the possible designs of such implementation using the following example:

1. *There are two keys with an account, one key with a regional enforcement agency (police department or similar), and one key with the KYC provider;*

2. *There could be an account with three keys, the first two the same as in the previous example and the third with the Galactica foundation;*

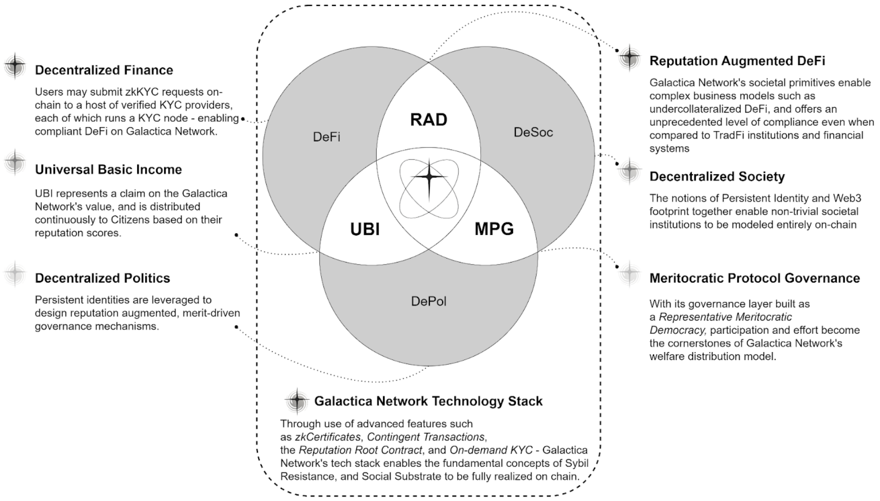
3. *The example can be expanded with additional keys located elsewhere, say the Galactica High Council (a body consisting of user representatives).*

The details on the cryptography used as well as the technical implementation of the zkKYC procedure can be found in Appendix I - Galactica's Zero-Knowledge KYC Design.

The Institutional Setup

Galactica Network Institutions are abstractions modeling social, political and financial institutions that can be leveraged when building DApps on Galactica

Network and interacting with the protocol itself. These are substrates that can be leveraged to frame agent interactions within the network.



Decentralized Finance

Users may submit zkKYC requests on-chain to a host of verified KYC providers, each of which runs a KYC node - enabling compliant DeFi on Galactica Network.

Universal Basic Income

UBI represents a claim on the Galactica Network's value, and is distributed continuously to Citizens based on their reputation scores.

Decentralized Politics

Persistent identities are leveraged to design reputation augmented, merit-driven governance mechanisms.

Reputation Augmented DeFi

Galactica Network's societal primitives enable complex business models such as undercollateralized DeFi, and offers an unprecedented level of compliance even when compared to TradFi institutions and financial systems

Decentralized Society

The notions of Persistent Identity and Web3 footprint together enable non-trivial societal institutions to be modeled entirely on-chain

Meritocratic Protocol Governance

With its governance layer built as a *Representative Meritocratic Democracy,* participation and effort become the cornerstones of Galactica Network's welfare distribution model.

Galactica Network Technology Stack

Through use of advanced features such as *zkCertificates*, *Contingent Transactions*, the *Reputation Root Contract*, and *On-demand KYC* - Galactica Network's tech stack enables the fundamental concepts of Sybil Resistance, and Social Substrate to be fully realized on chain.

Figure 5: The Galactica Network Technology Stack

DeFi

We begin with the financial aspect of Galactica's institutional setup. We expect that the basic set of DeFi primitives built on Galactica Network will resemble that of any other smart contract enabled permissionless blockchain. The models of agent interaction, however, will be massively altered when augmented with selective disclosures and Web3 footprint contingent interactions.

1. Enabling transactions contingent on one's Web3 footprint implies making accounts heterogeneous. Heterogeneous accounts will be the basis for enabling meritocratic finance and *reputation-augmented DeFi*. Reputation-augmented DeFi is a set of societal primitives that enable business models of, say, undercollateralized DeFi;

2. Compliant privacy preserving DeFi. zkCertificates enable a variety of use cases for on-chain compliance, without compromising user privacy. Every DApp and account can be inspected with mathematical certainty and at any time for its interaction with non-KYC'ed accounts or liquidity pools. This means that Galactica Network offers an unprecedented level of compliance even when compared to some of the TradFi institutions and financial systems. At the same time, no KYC data exists in any form other than a cryptographic hash, on-chain, and cannot be associated with the real-world person even in the case of the KYC center being compromised.

An important note on regulation: at the outset of the protocol, regulation will be confined to the code-is-law mantra. As time goes by, however, we will expect the emergence of Web3 footprint-augmented regulation. In other words, in the presence of persistent identities and selective disclosures, regulatory statutes and compliance can be meaningfully represented on-chain.

Decentralized Society (DeSoc)

As has been well put in a paper that has been among the primary sources of our inspiration:

> *"Web3 today centers around expressing transferable, financialized assets, rather than encoding social relationships of trust. Yet many core economic activities—such as uncollateralized lending and building personal brands—are built on persistent, non-transferable relationships. [...] non-transferable "soulbound" tokens (SBTs) representing the commitments, credentials, and aliations of "Souls" can encode the trust networks of the real economy to establish provenance and reputation. "*[1]

In a broad sense, reputation is the fabric that holds human society as we know it together. Another way to define a Cypher State is a blockchain protocol that allows for reputation-centric primitives and composability thereof.

In other words, the DeSoc dimension of a Cypher State is built around the institute of reputation.

As has been mentioned above, reputation is a pre-web counterpart to the notion of Web3 footprint. Meaningful Web3 footprint can only exist following the emergence of primitives enabling persistent identities. zkCertificates in general and zkKYC in particular as well as RRC are such primitives within the Galactica Protocol.

> *"Web3 aspires to transform societies broadly, rather than merely financial systems. Yet today's social fabric—families, churches, teams, companies, civil society, celebrity, democracy—is meaningless in virtual worlds [...] without primitives representing human souls and the broader relationships they support. If Web3 eschews persistent identities, their patterns of trust and cooperation, and their composable rights and permissions, we see, respectively, Sybil attacks, collusion, and a limited economic realm of wholly transferable private property—all of which trends towards hyper-financialization."*[1]

Some of the important notions that are hardly implementable without this deeper societal substrate are meritocratic governance and economic mechanisms, emerging social networks, celebrity-centric content networks, new security models, and far beyond that. Strictly speaking, the reputation-augmented DeFi mentioned above is the product of the intersection of DeFi and DeSoc dimensions of Galactica's institutional fabric.

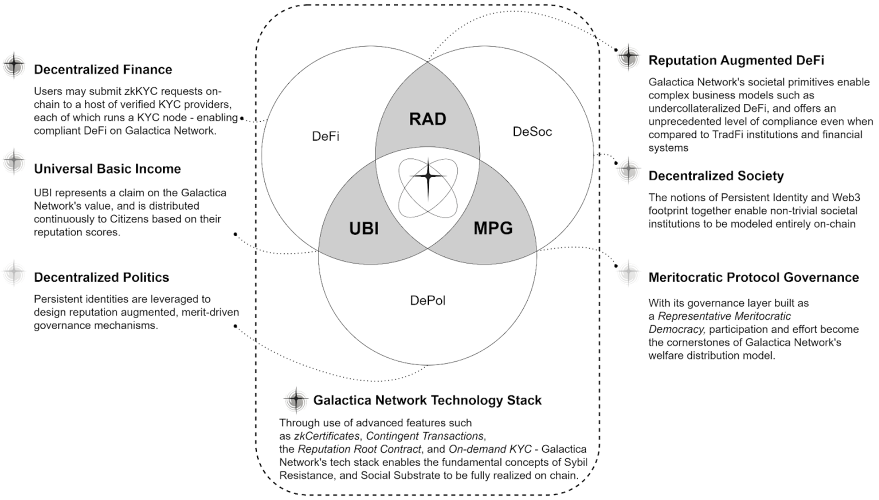
Decentralized Politics (DePol)

Persistent identities and the broader notion of DeSoc can be leveraged to design reputation-augmented or merit-driven governance mechanisms far more elaborate than those possible without explicit modeling of primitives enabling the protocol's societal substrate. These governance mechanisms can exist on the level of any given DApp, however, there is nothing preventing the same principles to be applied to the protocol itself. The distribution of power and economic resources of the protocol itself can be institutionalized to replicate the framework of any state governance or, better yet, *any* alternative distributional logic expressible through a Turing complete language.

The notion of meritocratic distribution of power and wealth as applied to a decentralized protocol and the actual mechanisms of doing so is the DePol dimension of the Galactica Protocol. Of course, DePol can be built around principles other than meritocracy.

Other Derivative Institutions

The derivative institutions are protocol-level mechanisms that are enabled by its institutions. Together they instill meaning in the concept of Galactica Citizenship providing a forum and a framework for wealth and power distribution within the network.



Decentralized Finance

Users may submit zkKYC requests on-chain to a host of verified KYC providers, each of which runs a KYC node - enabling compliant DeFi on Galactica Network.

Universal Basic Income

UBI represents a claim on the Galactica Network's value, and is distributed continuously to Citizens based on their reputation scores.

Decentralized Politics

Persistent identities are leveraged to design reputation augmented, merit-driven governance mechanisms.

Reputation Augmented DeFi

Galactica Network's societal primitives enable complex business models such as undercollateralized DeFi, and offers an unprecedented level of compliance even when compared to TradFi institutions and financial systems

Decentralized Society

The notions of Persistent Identity and Web3 footprint together enable non-trivial societal institutions to be modeled entirely on-chain

Meritocratic Protocol Governance

With its governance layer built as a *Representative Meritocratic Democracy,* participation and effort become the cornerstones of Galactica Network's welfare distribution model.

Galactica Network Technology Stack

Through use of advanced features such as *zkCertificates*, *Contingent Transactions*, the *Reputation Root Contract*, and *On-demand KYC* - Galactica Network's tech stack enables the fundamental concepts of Sybil Resistance, and Social Substrate to be fully realized on chain.

Figure 6: The Galactica Network Technology Stack

Leveraging the above concepts, Galactica Protocol introduces a number of derivative mechanisms that together instill practical meaning into the concept of protocol Citizenship.

Merit-Driven Universal Basic Income (UBI)

The first one is merit-driven UBI.

UBI represents a claim on the protocol value and is distributed continuously across Citizens based on their reputation scores as proxied by RRC.

One way to define reputation (in a sense of an RRC indexer) is to represent a quantitative impact an individual has had on protocol prosperity - put in simpler terms Reputation quantifies contribution merit. Hence, when modeled this way, UBI distribution is merit-driven. Galactica is intended to work like a self-organized machine, every part has its role and is rewarded its share (proportional to merit) in the form of UBI.

We shall attempt to keep this paper light and won't go into the details of implementation that are destined to change a number of times before settling on their final design. Nevertheless, let us specify the aspects of UBI design that will remain unchanged:

1. UBI is distributed in the form of a basket token;
2. The basket token has value as it is backed by a pool of tokens/coins;
3. The composition of the pool will be defined by:
    a. $GNET inflation ($GNET is Galactica Protocol coin);
    b. Tokenized Intellectual Property (IP) of innovation produced within the realm of Galactica Protocol;
    c. Tokens are funded through grants and other investments;
    d. Other.
4. The distribution of UBI is linear in merit and sublinear in $GNET stake.

Reputation-Augmented DeFi

The second one is Reputation-augmented DeFi (or DApps, in general).

The integration of Galactica's financial and societal primitives allows for Reputation-augmented DeFi. This enables a myriad of use cases, including, importantly, undercollateralized lending. Project-specific DAOs can integrate new features in their economic and governance designs: DAO-defined reputation voting mechanisms, Souldrops, etc.

The general premise of reputation augmentation, however, remains unchanged - it's a way of leveraging merit, rather than stake, for alternative wealth and power distributions.

Representative Meritocratic Democracy

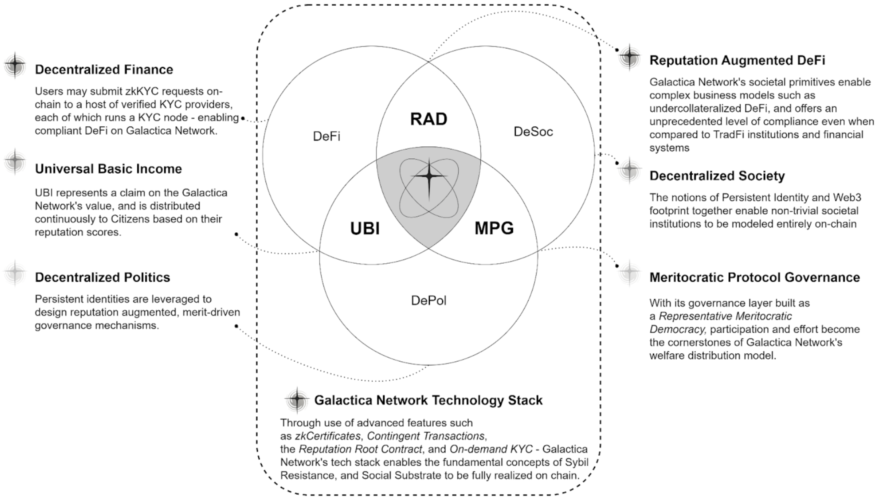
The final derivative institution is that of Representative Meritocratic Democracy.

Meritocratic protocol governance, the intersection of DeSoc and DePol, is a way to leverage merit to shape the interaction of agents on a protocol level. Curious readers shall explore the design of Galactica Protocol's political system in Appendix III - Galactica's Governance Framework Design.

These derivative institutions make up the foundation that enables the concept of Protocol Citizenship.

Citizenship and the Cypher State

Galactica Network Citizenship is a way for persistent identities to have merit-driven claims on the value generated on the network by the agents using it. It is a primitive defining rights and responsibilities to persistent identities, subject to the political process.



Decentralized Finance

Users may submit zkKYC requests on-chain to a host of verified KYC providers, each of which runs a KYC node - enabling compliant DeFi on Galactica Network.

Universal Basic Income

UBI represents a claim on the Galactica Network's value, and is distributed continuously to Citizens based on their reputation scores.

Decentralized Politics

Persistent identities are leveraged to design reputation augmented, merit-driven governance mechanisms.

Reputation Augmented DeFi

Galactica Network's societal primitives enable complex business models such as undercollateralized DeFi, and offers an unprecedented level of compliance even when compared to TradFi institutions and financial systems

Decentralized Society

The notions of Persistent Identity and Web3 footprint together enable non-trivial societal institutions to be modeled entirely on-chain

Meritocratic Protocol Governance

With its governance layer built as a *Representative Meritocratic Democracy,* participation and effort become the cornerstones of Galactica Network's welfare distribution model.

Galactica Network Technology Stack

Through use of advanced features such as *zkCertificates*, *Contingent Transactions*, the *Reputation Root Contract*, and *On-demand KYC* - Galactica Network's tech stack enables the fundamental concepts of Sybil Resistance, and Social Substrate to be fully realized on chain.

Figure 7: The Galactica Network Technology Stack

When there are rights and responsibilities to enjoy and honor respectively, that come as a result of explicitly modeled institutions defining the distribution of power and wealth within a crypto-economic protocol, we can speak of the notion of Protocol Citizenship.

As we have established above, Sybil resistance of a protocol enables complex societal concepts to be meaningfully represented on-chain. Historically, the most notable societal primitive defining a meaningful and rich set of a person's rights and responsibilities is that of citizenship. A protocol sufficiently feature-rich to instill meaning into the concept of Protocol Citizenship can be called a Cypher State.

At least this is one of the definitions.

In order to give a more exhaustive definition to the concept of Cypher State, we shall introduce a set of definitions and principles.

Definitions

1. **Cypher Capital** is the aggregate economic and political capital generated within and available to the decentralized techno-economic ecosystem (think, all the value secured by a protocol and the power to distribute that value);

2. **Cypher State** is a decentralized techno-economic ecosystem defined by a set of persistent identities, smart contracts, and their endowments where the distribution of Cypher Capital follows an explicitly modeled political process;

3. **Cypher State Citizens** are persistent identities within the Cypher State that have contingent claims on the Cypher Capital generated therein;

4. **Galactica Network** is a Capitalistic Cypher State, characterized by a capitalistic economic setup and a laissez-faire representative meritocratic political framework, optional citizenship, and hybrid (capitalistic/socialistic) rules of distribution of economic Cypher Capital.

Galactica Network Cypher State Principles

1. Economic Cypher Capital distribution process integrated into a tiered inflation schedule where Citizen's ultimate inflation-induced wealth dilution is a function of one's endowment (i.e. stake) and merit, as proxied by reputation;

2. Political Cypher Capital of a Citizen is driven by merit and endowment. It's linear in merit and sublinear in endowment;

3. Reputation is not and cannot be homogeneous, and neither can it be constant in time. It is an evolving metric for every Citizen of Galactica network, both accumulating in time and evolving within the cross-section of disciplines. Being an input into one's ultimate voting power on various matters, reputation is a form of Cypher Capital (both, social and political) within the Galactica Network;

4. Inflation-funded public goods with an explicitly modeled generation of on-chain IP and non-alienation of IP created as a result of developing public goods. Those creating the innovation (read, IP) ought to have a disproportionate allocation of its fruits;

5. Explicit segregation of public and private goods, and explicit modeling of public/private goods transition. The process of opaque transition of the fruits of publicly financed innovation within traditional economies into the pockets of the few without awareness of the many is among the most disproportionate acts of adverse wealth redistribution in the Web2-governed world we live in today. Innovation produces Cypher Capital. Galactica Citizens have a claim on it through UBI;

6. Quadratic reputation-augmented UBI, where UBI's composition is a diversified innovation portfolio. Galactic Cypher Capital is strictly increasing in value long term the more innovation is produced within the network. This innovation, however, needs to remain, at least partially, as the economic capital of its Citizens, young or old, reputable or otherwise. Anything invented within Galactica ends up fueling the innovation portfolio, and every citizen has a claim on economic capital sitting therein. This claim itself, however, is heterogeneous depending on Citizen's merit, and endowment;

7. Citizenship is optional and manifests institutionalized persistent identity. Zero-knowledge and MPC cryptography shields sensitive information and choices of any Citizen;

8. Long-term deflationary token supply, with deterministic token emission schedule. The value of a unit of system economic Cypher Capital is increasing in economic activity through network effects and deflation and effective publicly financed innovation. It decreases through inflation. Inflation and innovation are the only systematic drivers of capital redistribution;

9. Code is the only law. Citizens are the only judges.

Enjoying the fruits of being a Citizen of a Cypher State can be as valuable as that of a nation state with all the benefits that come along with it. Building upon the concepts of reputation and merit enabled by protocol's Sybil resistance, a Cypher State can benefit from unique incentives and bootstrapping procedures: a basic example would be to give more voting power to Citizens with particular expertise relevant to a subject that's being voted for. A more sophisticated example would be to give a higher dividend to those who have contributed the most to research and IP generation. Targeting particular social profiles in Souldrops, enabling protocol-wide quadratic funding, and voting mechanisms are all on the table as well.

Citizenship

The Galactica Citizenship is an SBT that once obtained grants the *owner rights and responsibilities* within the Galactica Network. In particular, being a Galactica Citizen entitles one to the following rights:

1. Universal Basic Income (UBI) represents a stake in the ecosystem's innovative projects and consists of a share of the Inflation Rewards;
2. Royalties for Intellectual Property generated within the ecosystem;
3. Proceeds from Grants;
4. Become a Validator;
5. Access to certain DApps.

Besides these economic benefits, with Citizenship, one has a right to participate in Galactica's meritocratic governance, create new proposals that will bring prosperity to the system itself, and vote out the malicious actors in a democratic and transparent manner. At times voting for certain protocol changes will be obligatory, hence the Citizenship responsibilities. Citizens have the right to participate in the Governance Process by:

1. Voting;
2. Taking part in the proposal generation process in the High Council;
3. Taking part in Parliamentary activities;
4. Forming Common Interest Groups & Special Interest Groups.

The only condition that is needed to be eligible for Citizenship is obtaining a zkCertificate by passing Galactica's zkKYC process. One will be able to obtain Citizenship in various ways which are to be described in a dedicated document.

Governance

The one-token-one-vote (OTOV) governance scheme has proven an ineffective governance mechanism that lacks means of preventing the agglomeration of Voting Power (VP), due to the relative ease of obtaining the units (tokens) representing it.

Galactica Network incorporates a translation of the Swiss model of governance, as a more effective alternative to legacy (e.g. OTOV and its extensions) governance schemes. This Swiss model represents a semi-direct democratic federal republic. Furthermore, the VP each account in the Galactica Network holds is a function of their Reputation and tokens held.

Integrating merit into Galactica's governance framework addresses many of the common pitfalls that afflict democracies and enables all users to have an equal chance to apply themselves and be rewarded for their efforts.

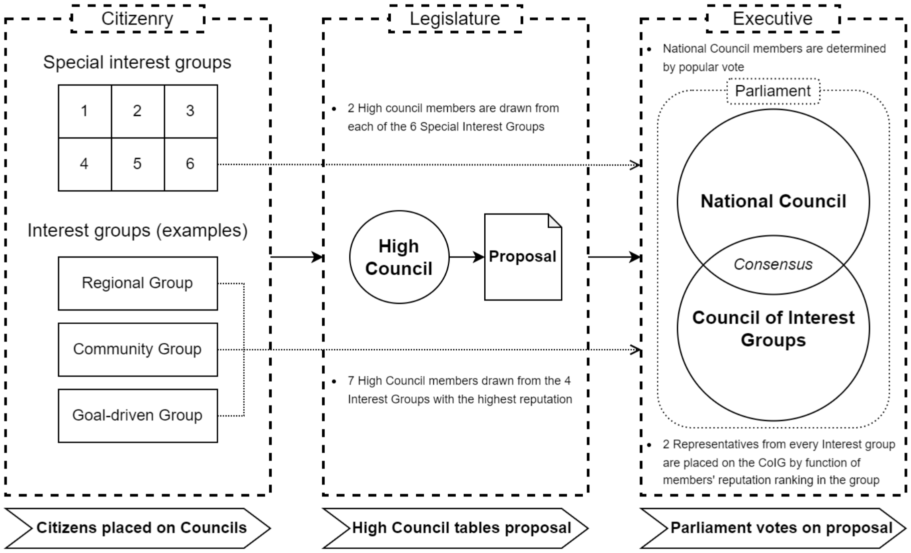

Citizenry
Special interest groups
1
2
3
4
5
6
Interest groups (examples)
Regional Group
Community Group
Goal-driven Group
Legislature
2 High council members are drawn from each of the 6 Special Interest Groups
High Council
Proposal
7 High Council members drawn from the 4 Interest Groups with the highest reputation
Executive
National Council members are determined by popular vote
Parliament
National Council
Consensus
Council of Interest Groups
2 Representatives from every Interest group are placed on the CoIG by function of members' reputation ranking in the group
Citizens placed on Councils
High Council tables proposal
Parliament votes on proposal

Figure 8: Galactica Governance Framework

Accounts holding citizenship within the Galactica Network may choose to join various 'Interest Groups' at their discretion; this structure is described in more detail in Appendix III - Galactica's Governance Framework Design, however, for clarity we shall now describe it in brief:

1. Citizens organize themselves into various Interest Groups - these groups can be formed for any number of reasons, but generally have some well-defined goal or ideal acting as a social adhesive;

2. Galactica Network's government is composed of 2 governing entities:

   a. The High Council (Legislature);

      i 2 High Council Members from 6 Special Interest Groups;

      ii 1 High Council Member from each of 7 top-ranking Interest Groups determined by popular vote;

      iii The High Council is responsible for the creation of proposals to be tabled in *Parliament*;

   b. Parliament (Executive);

      i Consists of two entities; the National Council, and the Council of Interest Groups;

      ii Parliament's sole purpose is to find consensus on proposals tabled by the High Council; passing or rejecting them as necessary.

The $GNET Token

Galactica Network's native currency ($GNET) is utilized across the Galactica Network for various purposes, including, but not limited to:

1. Validator revenue (for ensuring Galactica Network's security);
2. Governance (The more $GNET you hold, the greater your weight within Galactica Network's governance system);
3. Value distribution (In the form of UBI, which represents a claim on the Galactica Network's value, and is distributed continuously to Citizens based on their reputation scores.);
4. The funding of Public goods;
5. Distribution of Grants.

More detailed information regarding the $GNET token, its distribution, and tokenomics can be found in our public deck (Galactica Network Deck).

Appendix

Appendix I - Galactica's Zero-Knowledge KYC Design

Abstract

Current cryptocurrency industry trends more often than not place AML/CTF regulations on the opposing side of the aisle under the guise that efforts towards KYC mechanism improvements detract from the trustless environments being developed. By and large the absence of such flexible solutions has created a significant blindspot for all cryptocurrencies. However, with the growing wealth of research behind zero-knowledge proofs, a solution with minimal compromises can be achieved. One that satisfies both the institutional demands on the AML/CTF side and consumer demands for privacy and security of personally identifiable information (PII). This concept; zkKYC, is the basic unit of provable identity for what is termed a *Decentralized Society* [1], which expresses identity attributes that can privately interface with dApps, smart contracts, and other Web3 entities. zkKYC [2] enables the true development of reputation systems and meaningful social composability in Decentralized Autonomous Organizations and other Web3 governance systems. This innovation is vital to the preservation of user privacy and PII, while also ensuring trustless systems maintain their integrity from the ever-increasing threats of malicious actors. These social and governance systems can be deployed completely on-chain. This reaffirms the fact that cryptosystems, while preserving transparency, can also adhere to compliance standards at the same level as those in TradFi.

Introduction

In the last few years decentralized applications (e.g. DeFi ecosystems, NFTs, GameFi) as well as their governance layers have gone through multiple stages of evolution. The mechanics underpinning the long-term growth of these dApps have been constantly being reformulated, adapted, and improved with the goal of facilitating adoption. However, most developments have failed to address a more controversial but necessary component, which shares an outsized level of importance for securing institutional adoption - via zkKYC [3].

The term KYC is generally mentioned in reference to trading on centralized exchanges [4], participating in investment rounds [5], and in more contentious cases, dealing with regulatory requirements. For many Americans or residents of jurisdictions [6] that are not so amiable to the concept of cryptocurrencies, KYC is something that is often dreaded. It means that certain users will likely be left out of a major part or all of the functionality of a platform. KYC does not have a positive relationship [7] with the majority of industry participants as many believe that the notion of KYC runs contrary to the very founding ideals of crypto.

The misplaced animosity towards KYC has an unintended by-product: a divorcing of much of the innovative energies that pervade other realms of cryptocurrencies so that KYC as a domain of technologies (in the context of its applications to crypto) hasn't evolved as much compared to its counterparts like DeFi [8][9]. Performing KYC procedures hasn't changed much from the time of the ICO (to the chagrin of many smaller investors [10]) and while improving the technology underneath KYC may not immediately appear to benefit users like the outgrowths of DeFi managed to do, its development is monumentally important.

The Layer-2 and roll-up technology race [11][12] that erupted on Ethereum has given way to a rejuvenation in other domains of knowledge being applied to cryptocurrencies. New emphasis was placed on privacy [13], crypto-focused applications of AI [14], and federated learning [15][16]. This additional effort gave an impetus to the rapid development of Zero-Knowledge proofs [17] and with this reapplication of thought and creative energies, KYC has found a new crop of support [18].

By extension, zkKYC accounts can contain other data apart from that pertaining to the KYC process such as ownership of private Soulbound tokens (SBTs), educational YouTube channel, reputable Medium account, Summa Cum Laude designation of their Master's Degree, et cetera. This is important as naturally, this data can be used in a multi-party computation setting and selectively proven or revealed.

This paper will go on to provide the technical basis of KYC's integration with Zero-Knowledge proofs and more importantly it will demonstrate how valuable *zkKYC* [2] technology can be in reputation-based, governance, and general smart contract environments [19]. To unlock the next stage of secure, identity-based user interaction and social composability on the road to a *Decentralized Society*, this paper will explain how and why zkKYC is that technical foundation.

Overview of the Technical Design

Schematic Overview

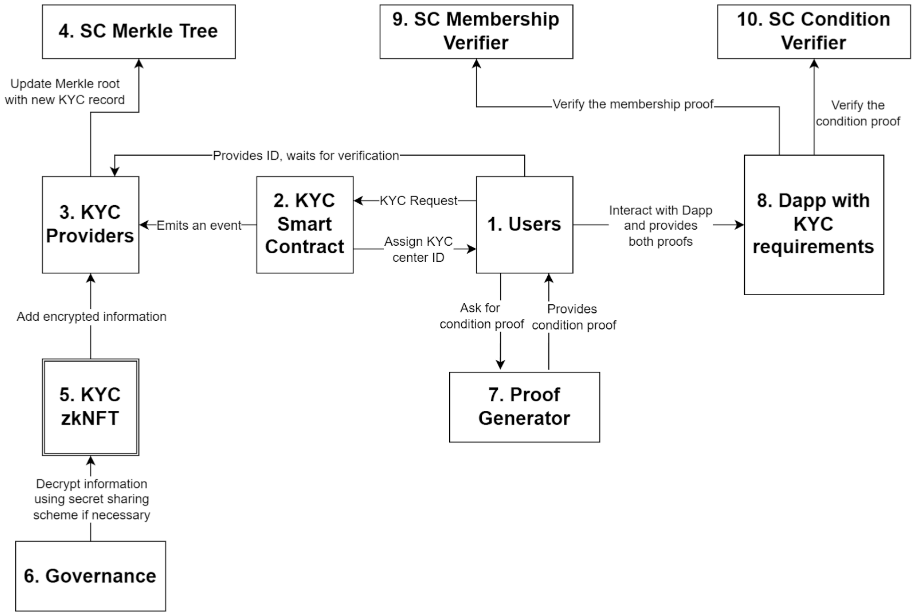

4. SC Merkle Tree
9. SC Membership Verifier
10. SC Condition Verifier
Update Merkle root with new KYC record
Verify the membership proof
Verify the condition proof
Provides ID, waits for verification
3. KYC Providers
2. KYC Smart Contract
1. Users
8. Dapp with KYC requirements
KYC Request
Emits an event
Assign KYC center ID
Interact with Dapp and provides both proofs
Add encrypted information
Ask for condition proof
Provides condition proof
5. KYC zkNFT
7. Proof Generator
Decrypt information using secret sharing scheme if necessary
6. Governance

Figure 9: Galactica's zkKYC Overview

Diagram description

1. User: a physical person when interacting with off-chain entities, an address when interacting with on-chain smart contracts.

2. KYC smart contract: on-chain smart contract with a list of KYC providers which randomly assigns to each KYC request a KYC provider to process it.

3. KYC providers: off-chain entities to verify physical ID documents and submit KYC records on-chain.

4. SC Merkle tree: on-chain smart contract to store KYC Merkle root and other related data.

5. KYC zkNFT: on-chain smart contract to mint zkNFT storing encrypted information of each KYC record.

6. Governance: Using Shamir's secret sharing, private key can be reconstructed from k out of n pieces and this private key can be used to decrypt zkNFT.

7. Proof-generator: off-chain program to generate zk proofs.

8. Dapp: on-chain protocols which require KYC records or certain conditions on them from users.

9. Membership verifier: on-chain smart contract to verify that a certain KYC record exists in the Merkle tree SC.

10. Condition verifier: on-chain smart contract to verify that the KYC record satisfies certain conditions.

KYC Record Creation

1. A hash is stored in a leaf of the Merkle tree: Each KYC user record will contain at least some of the following information: Date of birth, Country of Origin, Name, Verification Level, Random Salt, and others.

2. The Merkle leaf can also be considered a "soulbound" [20] NFT - that is, it is a non-transferable NFT. Throughout the remainder of this text and in other documents we will refer to such tokens as SBT (soulbound tokens) [1].

3. At the moment, two methods of constructing the Merkle trees are investigated:

   a) Method 1: Only store the Merkle root on-chain, and both the root transition and KYC record validity are verified by a ZK-proof;

   b) Method 2: Using Incremental Merkle tree [21], where alongside the Merkle root a filled subtree is also stored on-chain, which makes appending a new leaf independent of the current Merkle root possible. We still use a ZK-proof to verify the KYC record validity;

4. In this current version of the implementation we opt for the second method, as it allows more KYC providers to work on the same Merkle tree at the same time, whereas the first method might create concurrency issues;

5. Encrypted token: Alongside the Merkle tree, the KYC provider will also post the encrypted KYC record on-chain. This information can be decrypted using k out of n governance keys if necessary;

6. In the Merkle tree smart contract a nullifier mapping will be used to record the valid hash of the KYC record, as the KYC record can be revoked, changed, etc. In that case, the old KYC record is still in the Merkle tree, however, it is marked as false in the nullifier mapping.

Membership Proof

1. This proof demonstrates that the user has a valid record in the Merkle tree;
2. The *public inputs* are the Merkle root stored on-chain;
3. The *private inputs* are the Merkle path and the KYC record information that along with the user's address hashes to the corresponding Merkle leaf;
4. It has to be verified that the user's address is owning the KYC record and that the Merkle path is valid - that is, it subsequently hashes towards the Merkle root stored on-chain;
5. It also has to be checked that this KYC record has not expired.

Proof Generator and Condition Proof

1. The proof generator can be created from the public circom code, so it does not have to rely on one centralized identity;
2. The proof generation requires the user's private inputs, therefore it can be done on the user's computer in the browser - the user's information remains private and secure;
3. Various condition verifies will exist such as Age thresholds, Country restrictions, and KYC level restrictions;
4. Anyone can deploy a new verifier depending on the condition that has to be checked.

Selective Information Disclosure

1. Users can publicly disclose any part of information (e.g. being over the age threshold) in a ZK proof. All other information (the concrete age, name, etc.) stays private and is only processed locally in order to demonstrate that the disclosed information is indeed the one contained in the hash stored on-chain. In this case, users reveal this piece of information to everybody;
2. If a user only wants to reveal the information to a certain entity, then that user can encrypt the information with that entity's public key. The proof will be more complicated in this case.

Interaction with dApps

1. To interact with any protocol requiring KYC users will need to supply two proofs:
   a) The Membership Proof;

   b) The Condition Proof.

2. The protocol will then verify these proofs through respective verifiers and only proceed when the proofs pass.

3. As mentioned earlier, the protocols can deploy the verifiers themselves if they require custom conditions - they need to publish the circom code, so that anyone can create the prover.

Further Considerations

Generalization into zkCertificate

1. In the discussion above we have mentioned information related to the KYC process, however, it can be generalized to any metadata;

2. Any information can be encoded as a normal field like country or date of birth;

3. The disclosure or encryption is the same as the process described earlier.

Secret Sharing Scheme

1. We propose a Secret Sharing scheme based on Pauwels (2021) [2].

2. The Merkle tree of Galactica acts as a Verifiable Data Registry and is the storage used for:

   a) Public identifier DIDs (Decentralized Identifiers) - representing IDs of issuers, holders, verifiers, governments, and the relationships between them. For example, each time a holder registers at a verifier a new DID for this holder-verifier relation is created to make the zkKYC independent of other registrations;

   b) Revocation lists - Cryptographic list of verifiable credentials revoked by the issuer - e.g. expired credentials;

   c) zkKYC verification tokens encrypting information about:

      - Issuers for certificate/KYC;
      - Holder-Verifier combination.

      Government investigations (e.g. fraud) require decryption of the zkKYC token to:

      - Find the issuer of the KYC and obtain the information;
      - Verify that the fraud claim is valid - that is, the holder interacted with the verifier.

3. Following the aforementioned, the zkKYC token is naturally encrypted. The decryption keys are shared between members of the DAO (further details are to be provided separately) with Shamir's Secret Sharing scheme [22] as follows:

   a) If there are m keys and a minimum of n are required to decrypt the secret, a polynomial of degree n is created with the secret being one coefficient and n-1 random coefficients. Every one of the m participants receives a point on this polynomial. With n points, the polynomial can be reconstructed.
   b) Each point is encrypted with the government entity's public key on-chain.

Decryption of KYC Token

1. Process in case of government investigations:

   a) A government regulatory body approaches the DAO (more on the mechanics will be disclosed in a dedicated document);
   b) The DAO processes the request through voting;
   c) At least n members need to agree on the request to be able to decrypt the zkKYC token using Shamir's secret sharing scheme;
   d) The decrypted zkKYC token reveals the holder and issuer DID;
   e) The government regulatory body can then request the actual KYC data from the issuer;
   f) The issuer discloses the KYC data to the government regulatory body as long as the DAO vote is successful.

2. When DAO members change they need to pass their Shamir secret sharing data to the next member.

Negative reputation prevention

1. In the beginning, there will be only chosen trusted KYC providers;

2. Later on, in order for the leaf addition to the Merkle tree to be valid, the leaf needs to be approved by the owner. The approval can be submitted by anyone and it contains the zk proof that the user corresponding to the zkKYC record/account has signed a certain message. There will be a zk verifier to check that the signer is indeed the owner of the zkKYC record/account. The fact that a zkKYC leaf is approved by its owner is then stored in a mapping;

3. Likewise later on any newly minted zkKYC NFT will not be immediately sent to the owner but stays firstly in the issuance smart contract and its owner can claim it only if he wants to.

Data storage

ZkCertificate data is stored for different purposes in the following ways:

1. Data for verification is stored on-chain, so that verifiers can check if a zero-knowledge proof is consistent with the on-chain state. The most prominent part is the Merkle root representing the set of hashed zkCertificates added by providers. Furthermore the data includes the list of authorized providers and verification SBTs that mark the verification of the zkCertificate between a user and a dApp as complete until some expiration date.

2. Data including private zkCertificate details need to be stored to be available to the holder for when he or she wants to create a ZK proof. The data can be stored off-chain in the holder's responsibility using an encrypted file or wallet software. It can also be stored on-chain in encrypted logs, so that only the holder's private key can decrypt the data. This on-chain storage has the advantage that only the private key is needed for accessing the data, leading to a simplified user experience and device interoperability. We plan to support both on- and off-chain storage to give the user a choice and redundancy.

3. Data for eventual fraud investigation is stored on-chain in the multi party encryption scheme mentioned above. Each of the m data pieces are encrypted for the responsible entity and saved in event logs. Individual pieces are useless until at least k pieces from different entities are combined to decrypt the fraud investigation data. It does not hold zkCertificate data directly. Instead it holds the IDs of the provider and zkCertificate, so that the fraud investigation team can query the details from the provider.

One more important point is that even though the KYC providers submit the zkKYC records on-chain and update the Merkle root accordingly, they don't know which on-chain address this record belongs to. On the other hand for simplicity, we want to associate each KYC record with one address only. To achieve this we can use the approval step of the record Merkle leaf described in the negative reputation prevention section. In this step, the user will also specify an address associated with the Merkle leaf, which will be stored in a mapping (or even a second Merkle tree, if we don't want to reveal the hash of the record Merkle leaf). The address will not be public but stored on-chain as a hash combined with some random number (to make it more difficult to guess).

Conclusion

What has been outlined in the above discourse on zkKYC encapsulates a paradigm shift for the entire industry, an industry that has, from its inception, treated any form of KYC as antagonistic towards the ideals of cryptocurrency. This paper began the discussion with a high-level schematic overview of zkKYC's technical underpinnings to introduce readers to the components of KYC's technological evolution. The discussion transitioned into a step-by-step explanation of how a record is created and how it is then proven valid within the ecosystem. The membership proof is the mathematical notation by which said record is proved within the Merkle tree and thus proves the user as real and valid.

The proof generator was introduced alongside the notion that individuals and organizations will be able to deploy their own verifiers which check specific conditions existing in a user's record. Guarantees to user privacy were also included via the explanation of how users are able to selectively disclose information on their records. Additional information was provided on how users will interact with KYC smart contract dApps, particularly, how to supply proper information to the respective dApps. An excerpt on zkCertificate generalization, the secret sharing scheme, and the decryption of KYC tokens were included to close out the discussion on zkKYC.

With rather minor modifications, the efforts outlined in this paper can be readily applied to a host of dApps and Web3 interactions. This results in these zkKYC developments being more rapidly deployable to production-ready and live environments. Moreover, this paper also addressed the straightforwardness and customizability of the entire zkKYC procedure. KYC should not exist in an unapproachable state in which it is painted as a monolithic *enemy* of Web3. zkKYC has been elucidated in its entirety, it is ready to be integrated into Web3 and it is what is needed to provide the technical foundation for the development of highly complex reputation-based, governance, and social systems.

Appendix II - Galactica's Reputation Framework Design

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, the 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 of 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 tokens 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 in the different technical niches 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 reputation 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 shift them away from their hyper-financialized nature and refocus 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, and 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 guarantee the evolution toward a meritocratic system.

On a more technical note, Reputation in the Galactica system will be managed by the **Galactica Reputation Root Contract (RRC)** - 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).

Initial Definition of Voting Power & Reputation

Cautious readers will find a problem with the ideas presented above. In order to change the reputation function of 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 number 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:

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

where:
$\alpha = 0.2$
$\beta = 2$
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** [18], [17].

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 Ph.D. 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 whom the 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 a 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 using 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, 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 others;

3. Calculating the 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 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 into purely decentralized ones, interconnected between themselves into a global aggregation 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.

Appendix III - Galactica's Governance Framework Design

Introduction

Governance and its application to cryptocurrencies is embodied by the Decentralized Autonomous Organization (DAO). The management and systems of DAOs are concerned with enacting the will of the people that make up the DAO. Whether the discussion of the intricacies of DAOs concerns the management of the DAO, the leadership, or the mechanics of the dApp underlying the DAO, all fall under the Web3 umbrella term of *Governance* [1].

Currently, the governance of DAOs is executed through a variety of platforms; Snapshot, forums, and Discord most notably. Governance generally begins with discussions being held on a DAO Discord channel or forum; a topic or issue affecting the DAO is acknowledged and DAO members start proposing and debating solutions [2]. After sufficient solutions have been developed and a soft consensus within a community is reached, an official proposal is created, voted on either within the channel or forum and then proceeds to a snapshot vote where (more often than not) direct token voting occurs [3].

Assuming the proposal passes the vote, the team behind the DAO is then obligated to enact the consequences of the proposal. This process is widely used but is by no means the most effective means of governing a DAO. Furthermore, DAO governance has been observed to devolve into either non-negligible voter apathy amongst the DAO participants or voting power captured by a minority of token-holders [4].

Since the birth of DAOs in 2016 with *The DAO*, the communities that formed around them have been working on solutions to effectively manage them and some of their issues [3] [5]. Progress is being made as discussion continues to be held concerning governance systems other than the traditional one-token-one-vote (OTOV) scheme [3]. The OTOV scheme has a direct analog to an *Athenian Democracy* [6] but in the case where the functional unit for conveying a vote is an economic unit that can be acquired with practically no limits, this presents a systematic flaw.

Many different participants in the DAO space have proposed alternatives to the Athenian Token Democracy, A16z outlined the value of a representative system: "While web3 governance should be different from older archetypes, it can also incorporate well-designed representative elements from traditional frameworks to build more inclusive and efficient organizations." [4].

What this paper presents is the translation of the Swiss Model of Governance as a more effective alternative to the OTOV scheme.

The Swiss Model is a semi-direct democratic federal republic. The federal legislative power is vested in the two chambers of the Federal Assembly: the National Council and the Council of States. The Federal Council holds executive power and is composed of seven power-sharing Federal Councilors elected by the Federal Assembly. [7].

For users to participate in the governance of the Galactica protocol, they will need to join *Interest Groups*. This is similar to voters joining a political party or Swiss citizens in a Canton [8]. Within the Galactica structure, there are the following entities, the *Parliament*, composed of the *National Council* and the *Council of Interest Groups*, and the *High Council*. Galactica's unique system of governance combines characteristics of modern-day democracies with a meritocratic focus. Integrating merit into Galactica's governance framework addresses many of the common pitfalls that afflict democracies and enables all users to have an equal chance to apply themselves and be rewarded for their efforts.

Voting Power

Within Galactica's governance framework the basic functional unit is an agent's *Voting Power* and is a byproduct of the user's Galactica tokens they hold and the Reputation they've earned specifically to their field of expertise. The definition of Reputation is to be addressed separately, nonetheless one does not necessarily have to perform KYC in order to be eligible for Reputation accumulation. To earn Reputation it is best to understand that actions involving active participation in the DAO, with the assumption that those actions are positive, will reward users with reputation.

The Voting Power (VP) of a given user in the Galactica network is defined as:

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

$\alpha = 0.5$
$\beta = 2$
p, q – amplification parameters

In the future these parameters may be changed, within certain bounds, by the community via the voting process. It should also be noted that the specific means of acquiring Reputation is not defined as of yet but users can assume that they will be rewarded should they participate in voting, propose a good project to invest in, if their proposal is accepted by the *High Council* and other net benefits for Galactica.

Parliament

The Parliament is designed to represent the vote of the majority of the participants in the network. The Parliament is the overarching mechanism that formalizes the will of the participants. It consists of two entities - the National Council (NC) and the Council of Interest Groups (CoIG), both made up of various representatives from the Interest Groups.

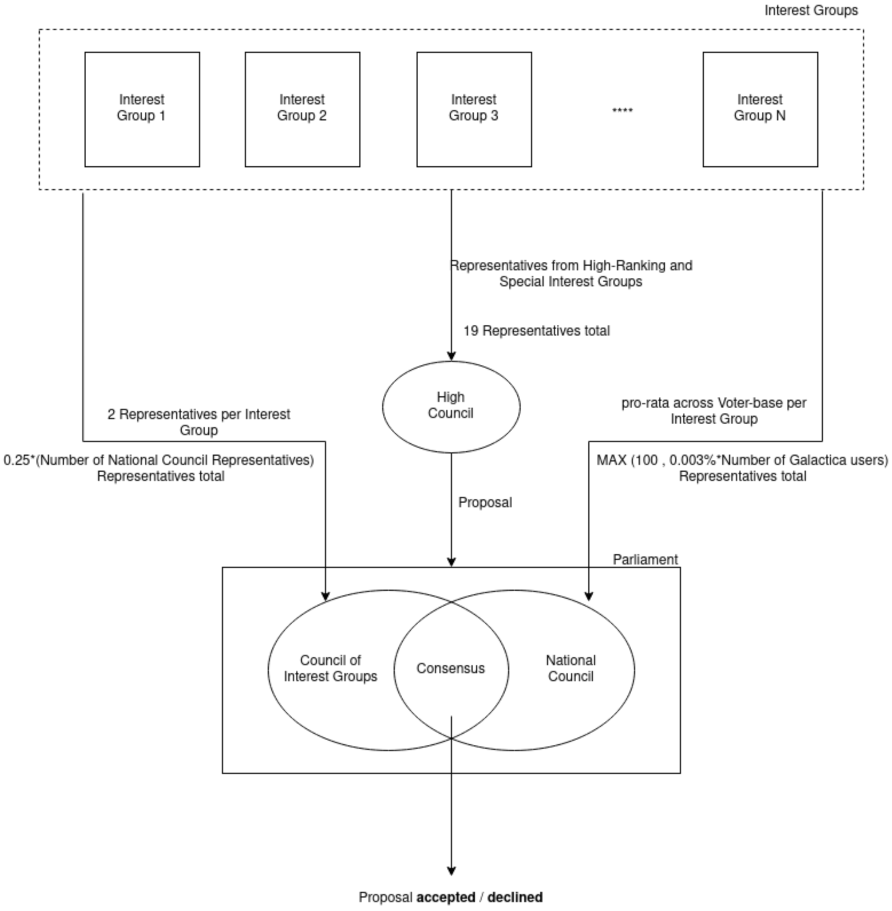

Interest Groups
Interest Group 1
Interest Group 2
Interest Group 3
****
Interest Group N
Representatives from High-Ranking and Special Interest Groups
19 Representatives total
High Council
2 Representatives per Interest Group
0.25*(Number of National Council Representatives) Representatives total
pro-rata across Voter-base per Interest Group
MAX (100 , 0.003%*Number of Galactica users) Representatives total
Proposal
Parliament
Council of Interest Groups
Consensus
National Council
Proposal **accepted** / **declined**

Figure 10: The Galactica's Parliament At-a-Glance

National Council

1. Number of Representatives in the NC:

$$NC^{Representatives} = MAX(100, 0.003\% * NumberofUsers)$$[1]

[1] Depending on the number of different Interest Groups these numbers can be changed but their ratio should roughly remain the same

2. Every Interest Group will be represented by a proportional number of Representatives as the number of votes placed upon them

Council of Interest Groups (CoIGs)

1. Number of Interest Groups in the CoIG (*Rounded to the first higher odd integer*):

$$CoIG^{NumberofIGs} = 0.5 * 0.25 * NC^{Representatives}$$

2. Every Interest Group is represented by 2 participants irrespective of their populations

As a note:

1. If we have more CoIG Representatives than what is needed, then IGs are ranked by votes given to them and the needed number of Representatives are picked from the top ones ranked by VP.

   a. Example: if the CoIG has 50% of the Voting Power overall then they will have 50% of the seats in the NC.

2. Minimum number of users inside of an IG should be at least = $NC^{Representatives}$

High Council

The High Council sits above the Interest Groups and the group's function is to allow for discussion of proposals and issues faced amongst the component Interest Groups that all comprise the High Council. The High Council, at a minimum, will contain two representatives from the following **Special Interest Groups**:

a. Validator Interest Group

b. KYC Interest Group

c. Tech Interest Group

d. DeFi/GameFi/NFT Interest Group

e. TradFi Interest Group

f. Galactica Foundation

Furthermore, the remaining Interest Groups are ranked by their Total Voting Power and the top four can have Representatives in the High Council as follows:

a. Top 3 Interest Groups are represented by 2 representatives each (total of 6)

b. 4th Interest Group is represented by only 1 representative (total of 1)

There is a rotation (Voting for Key Interest Groups and Top Four Interest Groups) that is currently set for every twelve months (a Mandate) with each interest group having the ability to be chosen only for two consecutive Mandates (twenty-four months). Key Interest Groups can not be kicked out of the High Council, but IGs that are not Key ones can be voted out with maximum attendance and $\frac{2}{3}$ vote. Absence is penalized and if one misses a voting session they will be warned (on their first offense). Continued absences (two or more) will be penalized in the form of reduction of Reputation points or the rewarding of negative Soulbound Tokens (SBTs).

Choosing Representatives

Within every Interest Group users are sorted accordingly by their respective Voting Power. The top two users by Voting Power are automatically selected as representatives for the High Council (assuming the Interest Group satisfies the conditions to have a representative in the High Council). The third highest-ranking user by Voting Power will represent the Interest Group in the Council of Interest Groups. The fourth representative is determined by Popular Vote (see Non-Referendum Decisions section), and National Council representatives are chosen by Popular Vote. The user that has the highest voting power earned overall (from the entirety of the DAO) is the 4th representative in the Council of Interest Groups. Lastly, the Mandate (the term to be served) for each Representative is 1 year. Each Representative may hold the position for a maximum of 2 years in a row.

Proposal to Vote Process

The process for the drafting and voting of a proposal is as follows:

1. A Proposal is created by the High Council
2. The proposal is passed down to Parliament
3. The National Council and Council of Interest Groups hold discussions on the topic
4. If a consensus is reached the Proposal is passed
5. If a consensus cannot be reached, the Proposal is set for a Mandatory Referendum

Mandatory Referendum

Lack of consensus leads to a Mandatory Referendum where all users in the system will be obliged to vote with their respective voting power on the Proposal. Only YES or NO is accepted during such a voting. All users that participate in the referendum by voting will be rewarded with a portion of Reputation points.

Referendum Mechanics

For referendums created by the parliament, at least 40% attendance needs to be reached for the votes to be counted. The general public can create a referendum independent of all governance bodies, before the referendum is created at least 1% of users need to sign it, and if successful, a system-wide referendum will be created. The same attendance conditions must be met for the referendums created by the Parliament.

If the referendum is mandatory and the user failed to participate they will receive a SBT that will reflect this and it will have a negative impact on their reputation. The referendum would be a success if at least 50% + 1 users had voted for the same option. Protocol referendums (and governance) need at least $\frac{2}{3}$ of the users to vote for the same option. The voting process in a referendum is different from the standard voting process as it does not get calculated with voting power but on the 1-user-1-vote principle.

Non-Referendum Decisions

The process by which non-referendum decisions are made is through a popular vote. Users vote with their Voting Power on the options pertaining to a particular proposal. Minimal requirements are defined in the **Parliament Consensus** Definition section.

Parliament Consensus Definition

Consensus has to be reached within the Parliament entities.

1. Council of Interest Groups: If M representatives (and $\frac{M}{2}$ IGs) exist at least $50\% + 1$ IGs need to attend ($> \frac{M}{4}$), they trivially need to have at least 1 attending representative but at least half of them need to have 2 thus at least $\frac{3M}{8}$ representatives need to attend in total. Consensus limit is $50\% + 1$. This holds for the most common proposals. Those proposals that concern the protocol itself and the governance system must have at least $\frac{2}{3}$ attendance. Consensus is reached after $\frac{2}{3}$ of users have voted on the same option.

2. National Council: At least 50% of the users need to attend. A problem arises if an IG has enough users to reach 50% by itself. It is a minor issue as Galactica has two governance entities that must reach consensus thus the ultimatum rule is impossible. It is not a direct problem but it can bring instability into the system thus it should be addressed, though the system will work only with the basic 50% condition.

The problem of an Interest Group being capable of reaching the 50% vote threshold by itself can be addressed by at least 2 ways:

1. Put a hard cap on the number of representatives some IG has (this is an inflexible option but sufficient)

2. Ascribe some weights on the IGs so that the total attendance will work out to 50% but every IG needs to be represented by at least some precalculated portion of their NC representative set. The weight associated with the smallest should be the biggest and the rest follow the same principle of weighting.

Parliamentary consensus is reached only if consensus in the National Council and the Council of Interest Groups is reached separately and on the parliament scale it is in favor of the same option. If the second step (global parliament consensus) is not reached the vote is postponed and discussion starts. After some time (1 week) the voting is held once again. If the consensus is not yet again reached because of low attendance, round 3 begins, and the votes will be counted irrespective of attendance.

If the consensus is not reached because the NC and CIGs opinions differ, then a system-wide referendum is held This referendum is mandatory for protocol and governance-specific proposals, but not mandatory for others.

One vs Many IGs problem (and what to expect) - Unification of IGs
If the representation is being done using the Popular Vote then it is not important if we have one or many IGs regarding the same thing. The only thing that must not be forgotten is the communication channels used within the said interest. They must be made in a way that anyone can express their opinion and that opinion can be seen by anyone. In the end, the proposal is to have one IG per topic (1 validator IG, 1 KYC IG, and so on).

Intra-IG process of choosing the Representatives
Both the High Council and the Council of Interest Groups are each allotted two representatives chosen by Popular Vote. The National Council has sorted Voting Power and following the census, the IGs and Coalitions that meet or surpass the threshold will be granted representation on the NC. Representatives will be proportionally awarded based on the sum of voting powers of the IG and Coalition members (groups with higher total Voting Powers will be awarded more representation).

For the National Council Representative selection process:

1. Popular vote to determine which IGs are in the NC
2. We define some census ($\sim 3\%$), every IG that has more then the census limit is in the NC
3. In a proportional way to the total VP placed upon them, the number of Representatives is found for every IG that will comprise the NC
    a. Coalition formation is permitted, for IGs that fail to meet the census limits (thus wouldn't be granted any Representation in the NC) they are permitted to form coalitions together in order to acquire representation within the NC

b. The stipulation for coalitions is that the total population of the coalition must not exceed two times the census limit as specified above

c. Any number of IGs can comprise a coalition so long as they don't surpass the two-times census limit

4. Sort each IG by Voting Power and pick the top five users that should represent them in the NC (that is if they are to be represented by five people)

Mandate duration and spec

A Representative's mandate length is one year, any user can have at least two mandates in total irrespective of being on the High Council or CIGs. With the IG-specific referendum, the people can remove someone from the position of power. The attendance condition is the same as the one defined for referendums. In order to remove him at least $\frac{2}{3}$ users must vote for him.

Universal Basic Income (UBI)

As a quick refresher, traditionally UBI is enacted as a sociopolitical financial transfer policy proposal in which all citizens (in our case, governance participants of Galactica) of a given population regularly receive a legally stipulated and equally set financial grant paid by the government. In Galactica for participants to be eligible to receive UBI the user must satisfy the following conditions:

1. Must have non-zero Voting Power
2. Must have SBTs that will confirm that the user frequently applies their Voting Power; they participated in governance either directly (being a member of the governing bodies) or indirectly (voting on a referendum)

The UBI distribution function is the function of the user's Reputation primarily and the SBTs they possess.

Examples of Proposals for Protocol Changes

This section provides some examples of what governance participants can propose and vote on within the Galactica system; this list is not intended to be exhaustive.

1. Voters could vote on what the share of Inflation Rewards (for example in the next 2 years) would be for:

   a. Validators' share of token inflation.

   b. Public Goods Fund (PGF) - At the beginning of every quarter the Parliament votes on how much % of the Inflation Rewards is allocated to the Public Goods Fund and at the end of the quarter the Parliament must vote towards which Public Goods projects they must be invested in.

c. DAO Ecosystem Fund - Similar to the Public Goods Fund, the voting process for funding of non-public good projects requires the Parliament to cast their vote twice a quarter - once for the size of the fund and once towards which projects it is channeled. Interest Groups propose research topics and the top 10% (of projects based on Voting Power placed upon them) will receive funding based on a quadratic voting basis.

2. Changes to the UBI criteria

3. Changes to the mechanism of Representative's rotations

4. Changes to the number of Representatives within the High Council and Parliament

5. Redefining the Reputation function

6. Redefining the Voting Power parameters

Academy of Sciences (AoS)

The AoS provides necessary venues for Galactica participant specialization with the express purpose of developing innovative features which would ultimately be deployed on Galactica. The AoS is structured as follows:

1. The Academy of Sciences consists of disjunct Sectors

2. These Sectors are populated by the users that hold skill-specific SBTs that are predefined for said Sector

3. Every Sector is represented by 3 representatives in the Council

4. Council (as an Entity) does not have any voting power, it can give its opinion on the topics discussed within the parliament and it can veto the proposals that are malicious with absolute attendance and $\frac{2}{3}$ vote

5. It is the responsibility of the HC and Parliament to distribute inflation streams to different substreams that go to Public Goods Funding, Private Goods Funding, UBI and Validators rewards.

6. It is the responsibility of the Council to divide the stream designated for Public Goods Funding to sub-streams that go to specific Sectors. This is done in a Quadratic manner

7. Once the inflation reaches some specific Sector the decision is placed upon them to determine the projects that will receive the rewards, in a quadratic manner also

8. Academy of Sciences can not create proposals, they can only consult the High Council and the Parliament on the topics that require AoS expertise

a. An example topic would be: “Galactica wants to invest in an external project that is concerned with electric vehicles, there are 5 projects that Galactica could invest in.” This would then be brought to the attention of the AoS where sectors within the AoS would perform necessary due diligence and come up with a conclusion. The AoS would then provide this conclusion for Galactica to make the final decision.

9. Sector that proposes a project that benefits the whole ecosystem (by consultation with the High Council) will receive that project’s tokens in a Retroactive manner. The vote will be passed within the Council, and if they vote that the project is good the Sector will be rewarded. (High Council will also be rewarded with the project tokens if the project is a success - if not the members of the High Council will be penalized either with reduced UBI for some time or reputation-diminishing SBTs. This mechanism is used to prevent spam and simple acceptance and funding of all projects that are introduced in the system)

10. Additionally, the AoS has a leader, the Chief Scientist, who is elected in a popular vote by all members of the AoS. The Chief Scientist has no direct power but is the delegating authority for all proposals. The Chief Scientist does have an indirect impact on sectors as the sector which the Chief Scientist delegates a proposal to receives retroactive tokens as a reward for their efforts. The position receives a salary in reputation, and a retroactive distribution of tokens, the position’s mandate follows the standard term length and can be removed following an AoS-specific referendum (also by popular vote).

The AoS is a unique and important structure within Galactica that encourages community members to contribute their skills and knowledge in a manner that is not typically found in other cryptocurrency projects.