
# GALACTICA NETWORK FULL DECK

NETWORK FULL DECK GALACTICA NETWORK

# TABLE OF CONTENTS

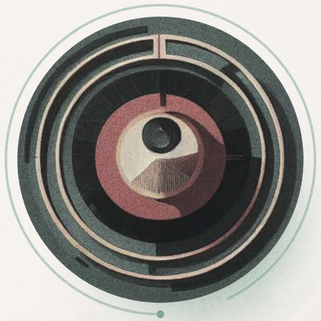
# GALACTICA NETWORK

#SYBIL RESISTANCE

#PROTOCOL CITIZENSHIP

#COMPLIANT PRIVACY

#CYPHER STATE



#SECURITY TOKENS

# REPUTATION AUGMENTED DEFI

# WEB3 FOOTPRINT

# MERITOCRATIC PROTOCOL GOVERNANCE

# ON-CHAIN ROBUST REPUTATION

# PERSISTENT IDENTITIES

# DeSoc

# PROBLEM

## TradFi

1. Democracy is illusory (Opaque DM, Lobbying, Propaganda, Crony Capitalism).
2. Monetary policies are reckless (record high global inflation).
3. Centralized financial system relying on web2 that is opaque, technologically and philosophically outdated.
4. Public goods are funded but benefits are not realized by society at large (VCs, innovation labs, etc.) leading to an ever widening gap between the rich and the poor.
5. Global finance is exclusive - unbanked do not have access to the most basic financial services.

## Web 3.0

1. Lack of Sybil Resistance leads to inability to encode Persistent Identities, that in turn leads to poor Societal Substrate (no DeSoc) and a host of adversarial consequences.
2. Hyper financialization leads to monopolies (DeFi in a purely anarcho-capitalist setup leads to concentration of wealth and power).
3. Necessary overcollateralization in DeFi leads to significant losses in capital efficiency.
4. Meritocracy and quadratic distributional mechanisms can't function without Sybil Resistance.
5. Compliance and privacy are traded off while they can co-exist.

# SOLUTION

1. Galactica Network Oracle Node design enables compliance standards for on-chain transactions similar to those of TradFi.
2. ZKP enables privacy and compliance to exist in symbiotic relationship, instead of being traded off.
3. zkKYC tech generalized into zkCertificates enables privacy preserving proofs of compliance and transactions contingent on data in real world documents.
4. zkKYC-powered Sybil Resistance creates a network of Persistent Identities each characterized with a unique web3 footprint.
5. Galactica Network's contingent transactions and on-chain availability of web3 footprint metrics enable heterogeneous account DApps - the DeSoc and reputation augmented DeFi.
6. Galactica Network's tokenomics built on the principles of meritocracy in distribution, and explicit focus on research, funding of public goods and UBI.

# UVPS

1. Transactions contingent on Web3 footprint and protocol Sybil resistance enable the concept of Protocol Citizenship, DeSoc, Reputation Augmented DeFi and more.
2. Protocol Citizenship through zkKYC bootstraps netowork's Sybil resistance and enables emergence of persistent identities and their web3 footprints;
3. zkKYC, contingent transactions and privacy roll-ups enable full privacy and full compliance guaratees to co-exist and co-evolve;
4. Galactica Network UBI with quadratic meritocratic distribution;

# COMMUNITY

**Intro agents**

IEO / bounty websites
Advisors
Influencers

**Offchain**

Family Office
Angels

**Whales**

Validators
VC
Crypto funds

**Researchers**

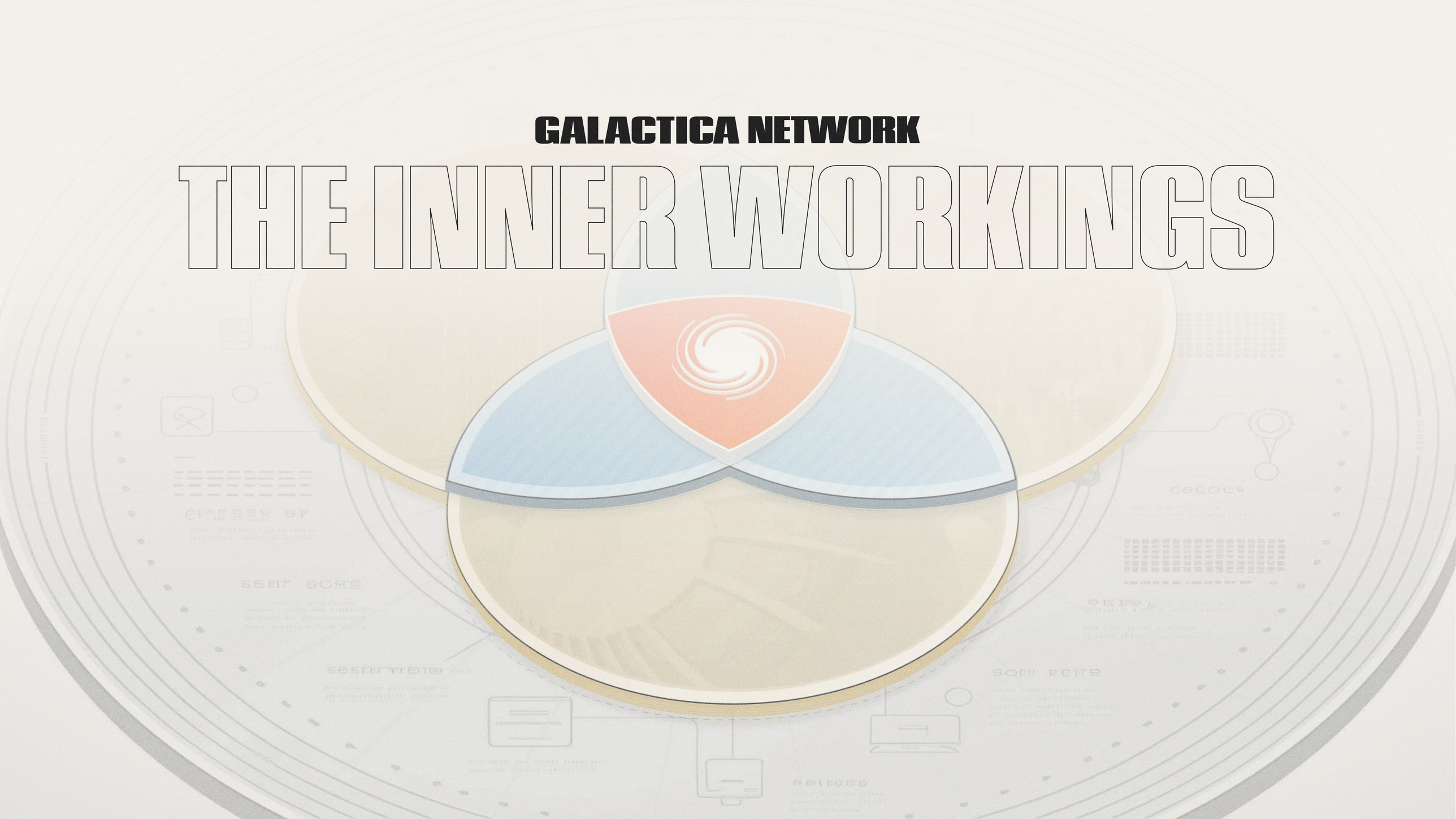
Merit-driven vote weighting

**Governance**

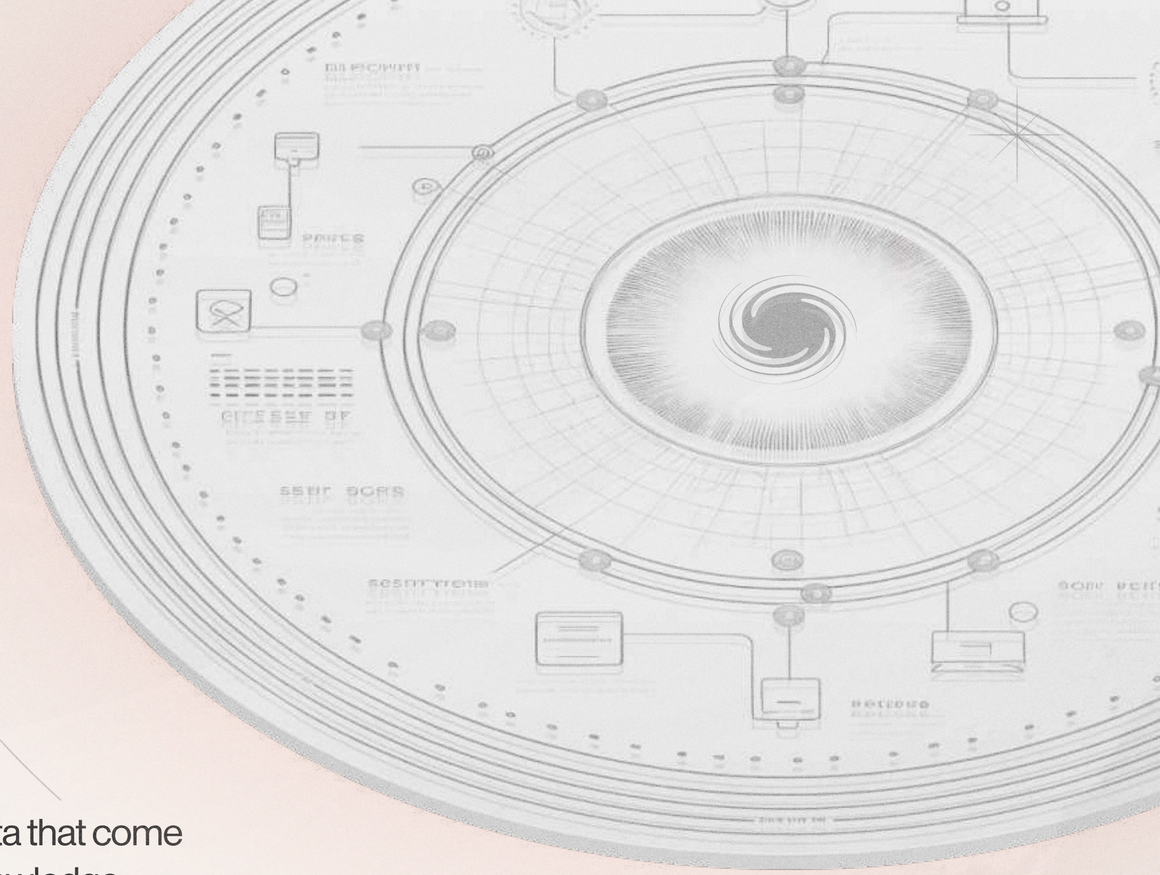
Merit-driven vote weights

# GALACTICA NETWORK

# THE INNER WORKINGS



# TECH OVERVIEW



## Guardians

Guardians power users' ability to submit document verification requests on-chain to a host of verified providers, each of which runs a Galactica Network Guardians. Initial use case of Guardians is that of KYC.

## 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. The zkCertificate containing one's KYC record will be referred to as Human ID.

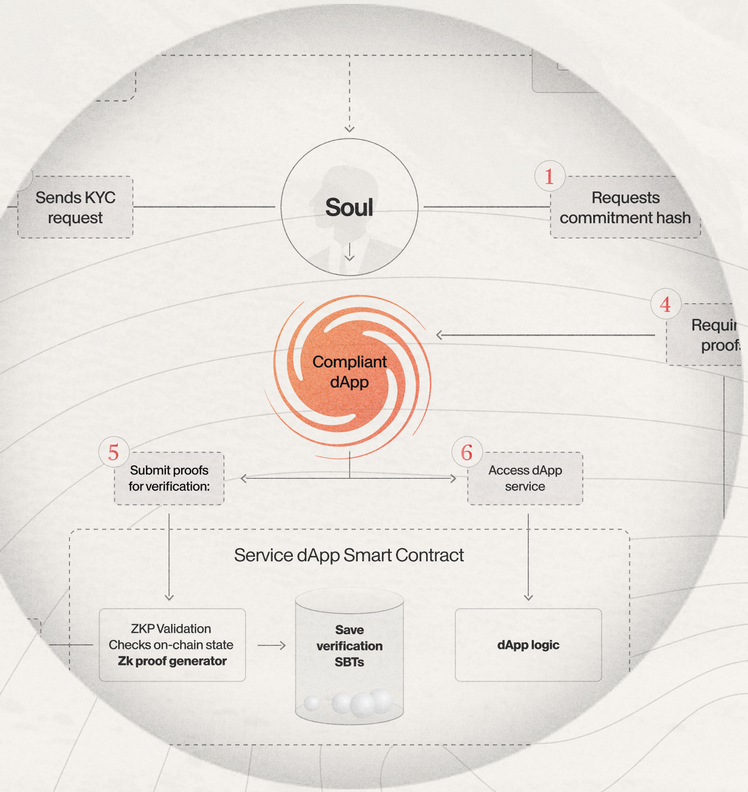
## The Reputation Root Contract

The Reputation Root Contract, or RRC is a system smart contract enabling DApps and users to slice and dice the web3 footprint producing unique score for every Human ID. It is a protocol-wide reputation system. The use of ZKC, however, protects the privacy for every Human ID.

## 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.

# GUARDIANS




- Guardians are basically on-chain notaries that can verify the authenticity of real world documents, such as for example one's KYC docs.
- 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 on-chain.
- At the inception of the protocol, Guardians list is comprised of a curated set of providers. As the protocol evolves, this function will get progressively more decentralized.

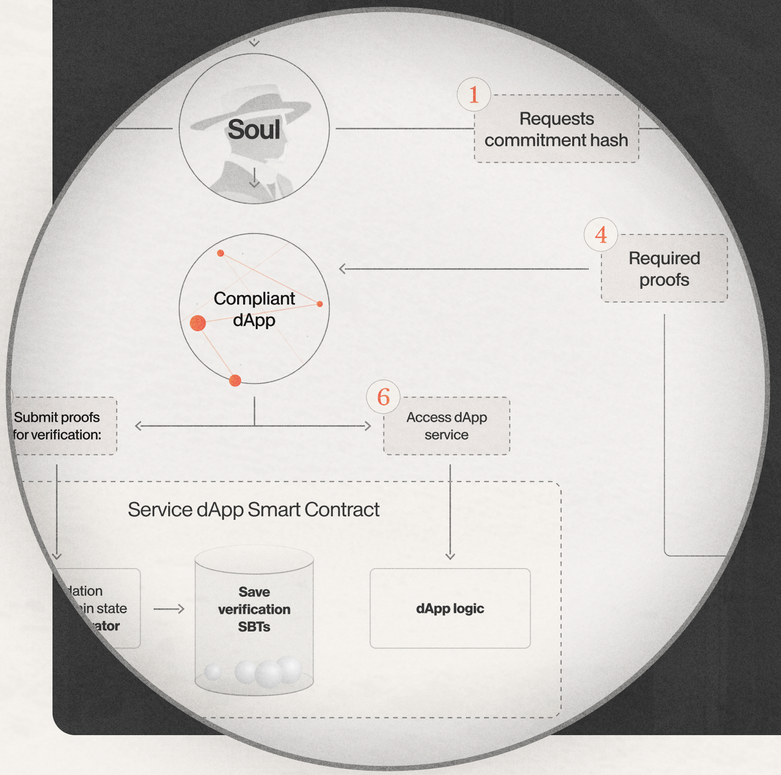
# zkCERTIFICATES

- zkCertificates are non-transferable (soulbound) NFTs with arbitrary metadata that come with an option of selective disclosure through the use of zero-knowledge cryptography.
- zkCertificates are issued by a provider, verifiable on the Galactica blockchain and under self custody of the user. They can have any real world documents as the underlying.
- zkCertificates can be encoded with a range of information about the account they're awarded to, from one's KYC record, property record, university diploma, etc. ZKPs enable proving arbitrary theses about the data stored without revealing it.

Using zero-knowledge technology, users can proof on-chain that they comply with dApp requirements (e.g. being KYC'ed, over 18 years and US residency) while keeping all other details beside this fact private.

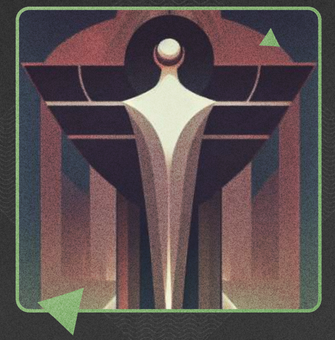
GALACTICA NETWORK

# zkCERTIFICATES & GUARDIANS FOR zkKYC




- **zkCertificates** is a general purpose primitive for migrating on-chain any real world document that can be verified by a notary running an Guardians.
- A peculiar use case is the use of zkCertificates and Guardians for the purposes of zkKYC where real world documents are peoples' PII.
- **zkKYC** is a potent concept as it addresses the issues of compliance for blockchain transactions while not sacrificing user privacy in the process.
- Equally important is the fact that account creation shielded with zkKYC drastically increases the cost of Sybil attacks enabling the universe of use cases that today come under the wider umbrella of DeSoc.

# PERSISTENT IDENTITIES & WEB3 FOOTPRINT



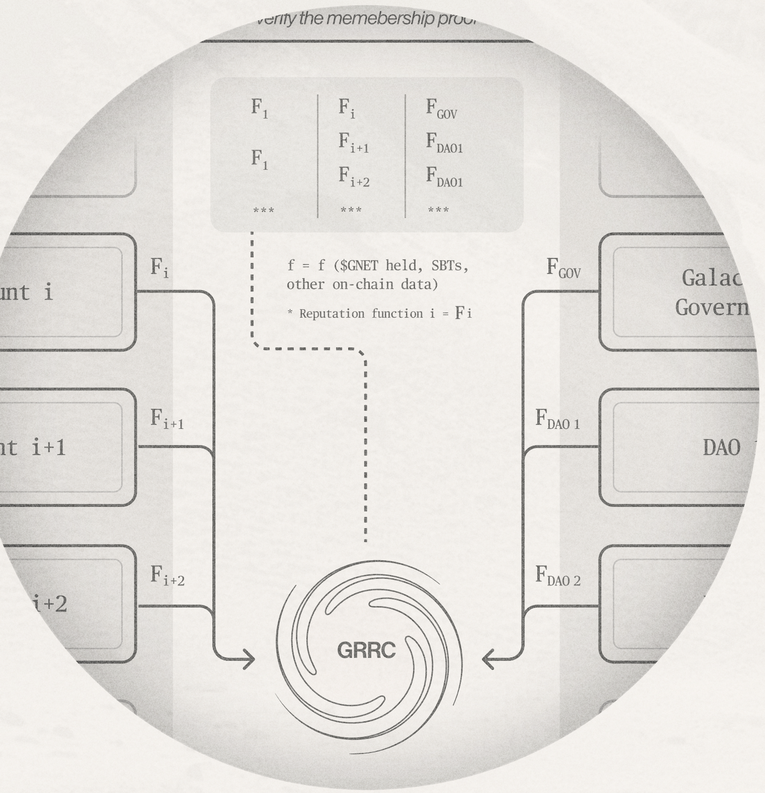
- **Protocol's Sybil resistance is a multitude of mechanisms enabling direct mapping between real world persons and internet identities.** A human in the blockchain space could be referred to as a Persistent Identity. The multitude of interactions between any such identity and the rest of the protocol could then be called one's Web3 footprint.

- 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 real-world concept of reputation.

- The notion of zkKYC is arguably one of the most potent ways to bootstrap Sybil resistance on a chain while enabling compliance with many regulations that today prevent the flows of institutional capital from flooding an inherently more technologically advanced web3 space.

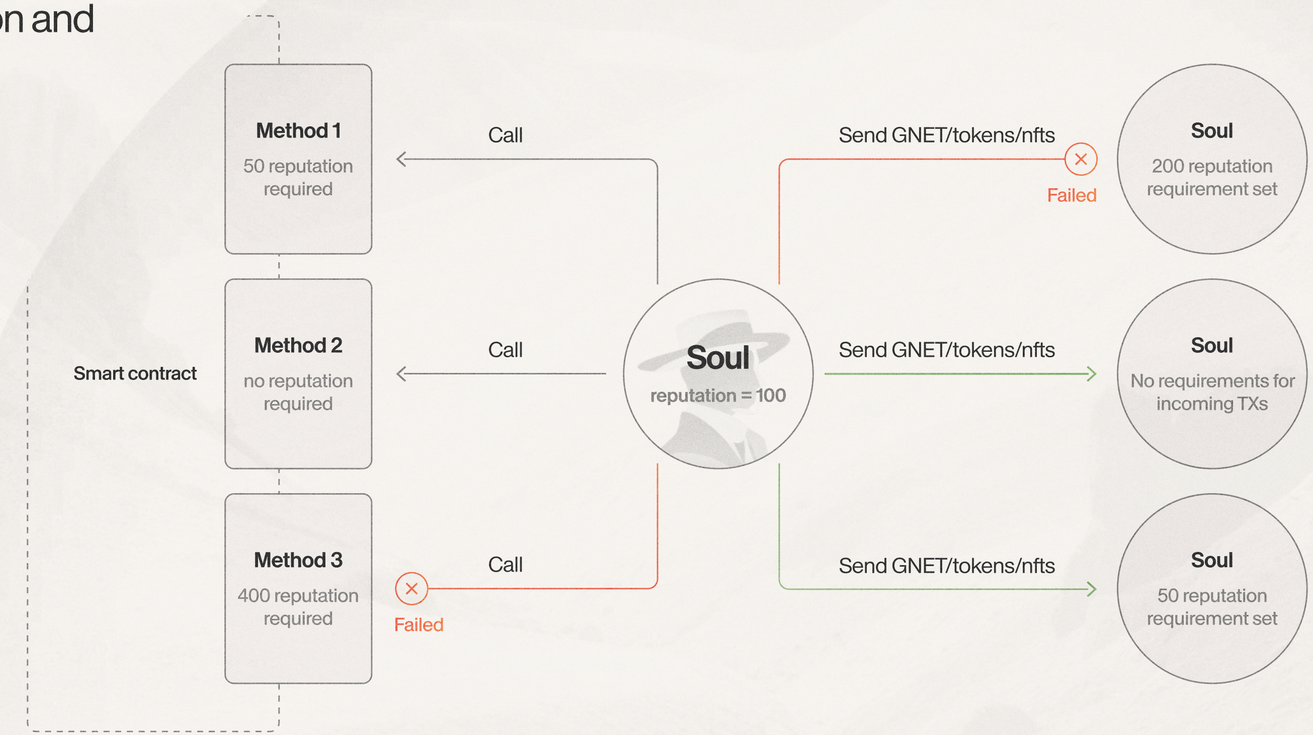
# REPUTATION ROOT CONTRACT (RRC)




- The Galactica Reputation Root Contract (RRC) is a protocol-level method that generates an on-chain Reputation Score for an existing address using an arbitrary function.
- Any user or organization can utilize the RRC, the contract's sole requirement is on-chain data as its inputs.
- Every user's Reputation Score is a metric of their Web3 footprint evaluated over a subset of available on-chain data points.
- In simple terms, on-chain data points are an agglomeration of users' interactions with DApps, DeFi and otherwise, protocol governance and other structures that comprise the Web3 landscape, all of which serve to define who they are.
- The outputs of RRC can be used as inputs by DApps, other users and the protocol governance framework to define rules of interaction.

# CONTINGENT TRANSACTIONS

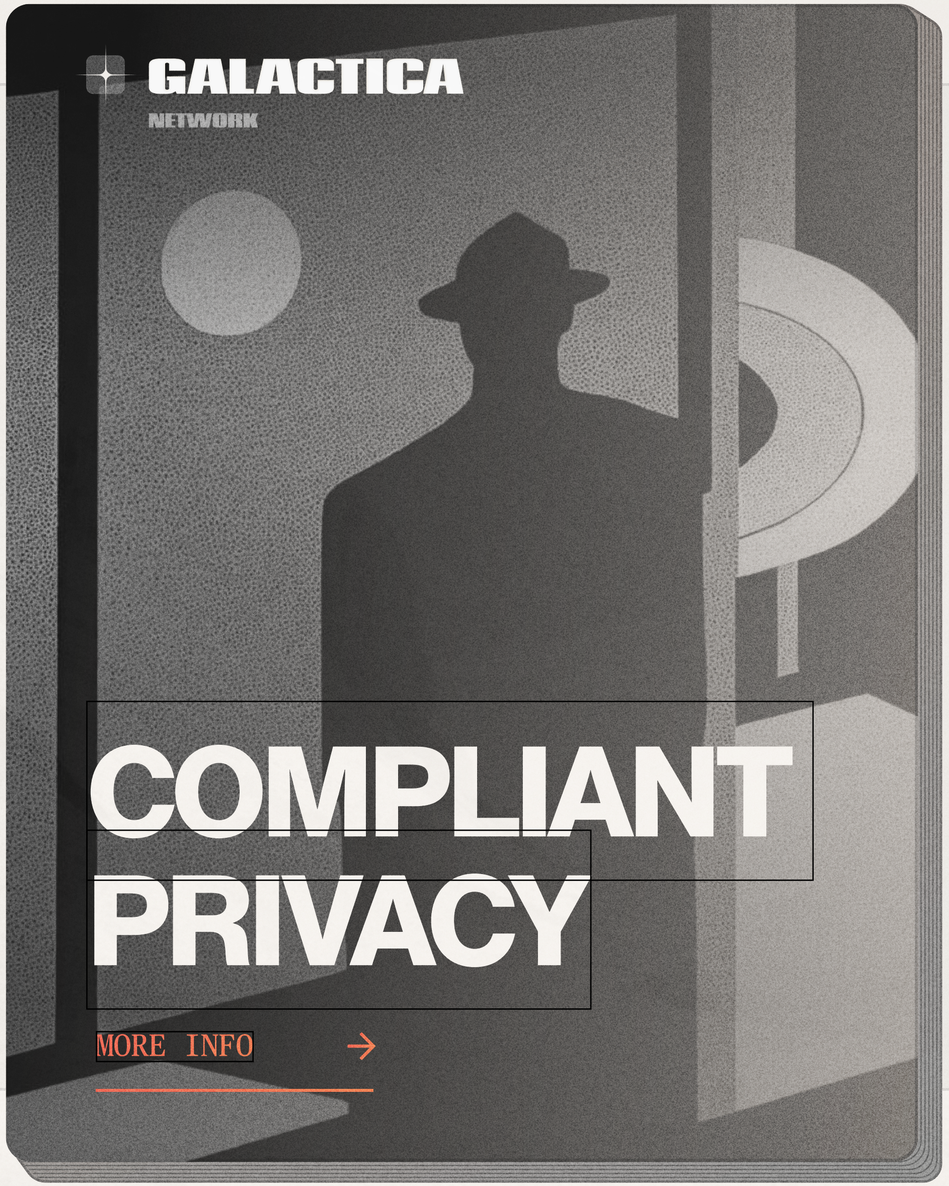
- **Contingent transactions primitive** is an extension of RRC that utilizes it's outputs to create dynamic transaction rejection and acceptance rules.
- Contingent transactions also support added depth for interaction rulesets enabling users **to codify unique interactions** into the baseline of their contracts.
- These programmable transactions **enable meritocratic interactions** (through indexing one's web3 footprint), compliant liquidity pools (through zkKYC) and in general, enable DApps to reflect the heterogeneous nature of accounts on Galactica Network.



# RRC AND CONTINGENT TRANSACTIONS ENABLE MERITOCRACY IN TXS

**Together RRC and Contingent txs** effectively create whitelists with dynamic criteria:

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 users approved through Guardians can interact with a DEX or else the transaction will fail) and enable heterogeneous account (i.e. DeSoc augmented) dApps;
2. The inner logic of a decentralized application (DApp) can be conditioned upon the score produced by the RRC (e.g. only users approved through Guardians are allowed to borrow at a 90% collateral ratio, while non-approved users need to post 200% collateral);
3. Moreover, contingent transactions can be programmed to combine several RRC outputs creating the opportunity for highly complex rules of interaction.


GALACTICA
NETWORK
COMPLIANT
PRIVACY
MORE INFO

# THE INNER WORKINGS

## OF GALACTICA NETWORK

### Decentralised Finance

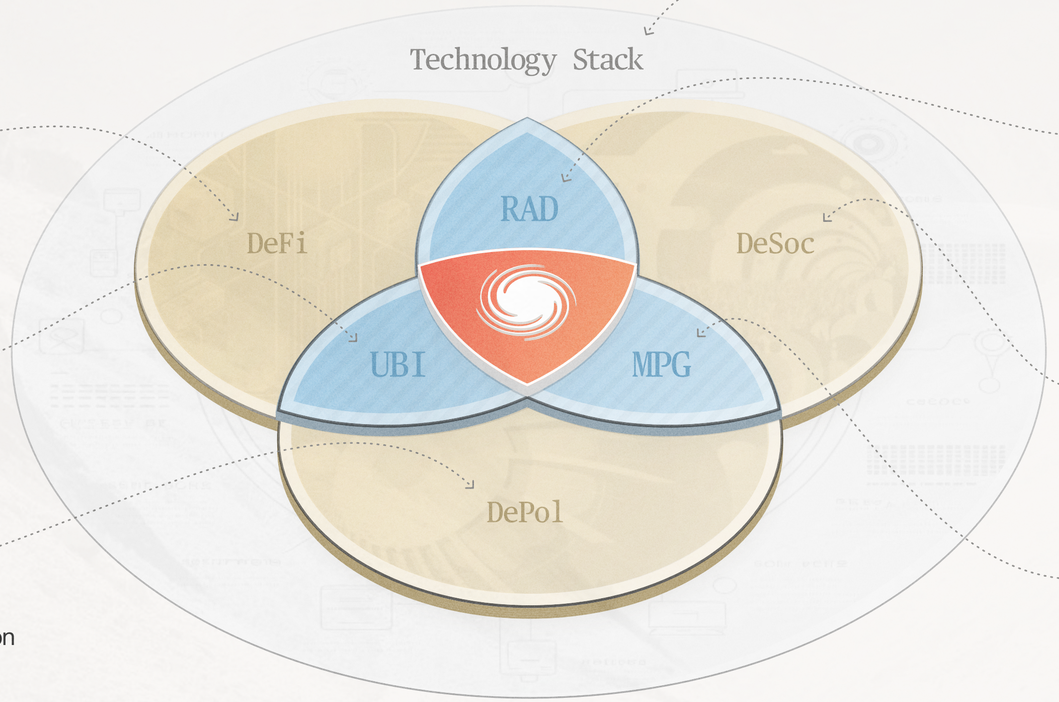
Users may submit zkKYC requests on-chain to a host of verified KYC providers, each of which runs a KYC node — enabling compliant DeFi on Galactica Network.

### Universal Basic Income

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

### Decentralised Politics

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




### 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.

### 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

### Decentralised Society

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

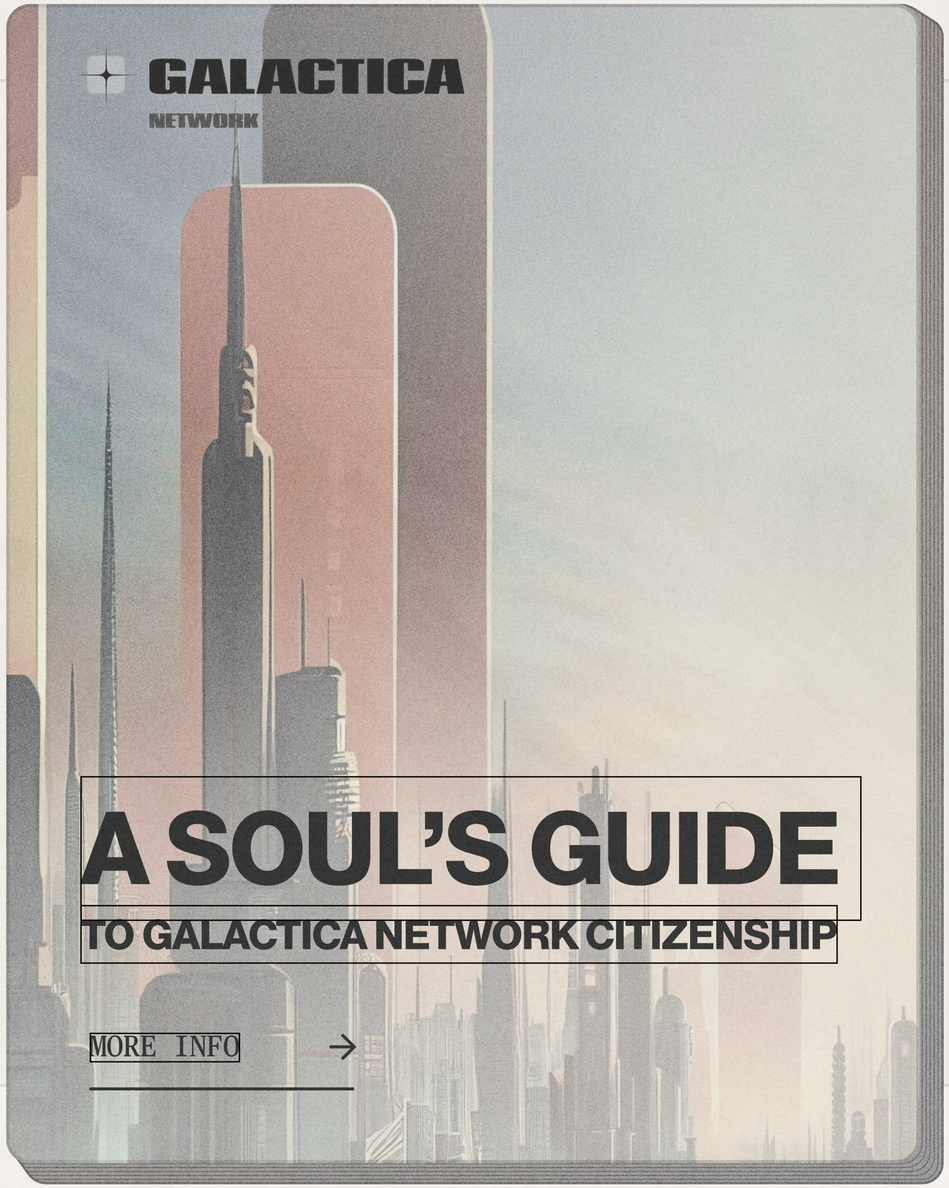
### Meritocratic Protocol Governance

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

**Galactic 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.

**The Derivative Institutions** are protocol mechanisms at the mutual intersections of DeFi, DeSoc, and DePol. Together they instill meaning in the concept of Galactica Citizenship providing a forum and a framework for wealth and power distribution within the network.

**Galactica Network Technology** stack is a set of primitives that enable strong Sybil resistance, account level privacy and zkKYC compliance. These properties enable the protocol to be a platform for modelling non-trivial social and political primitives and institutions.

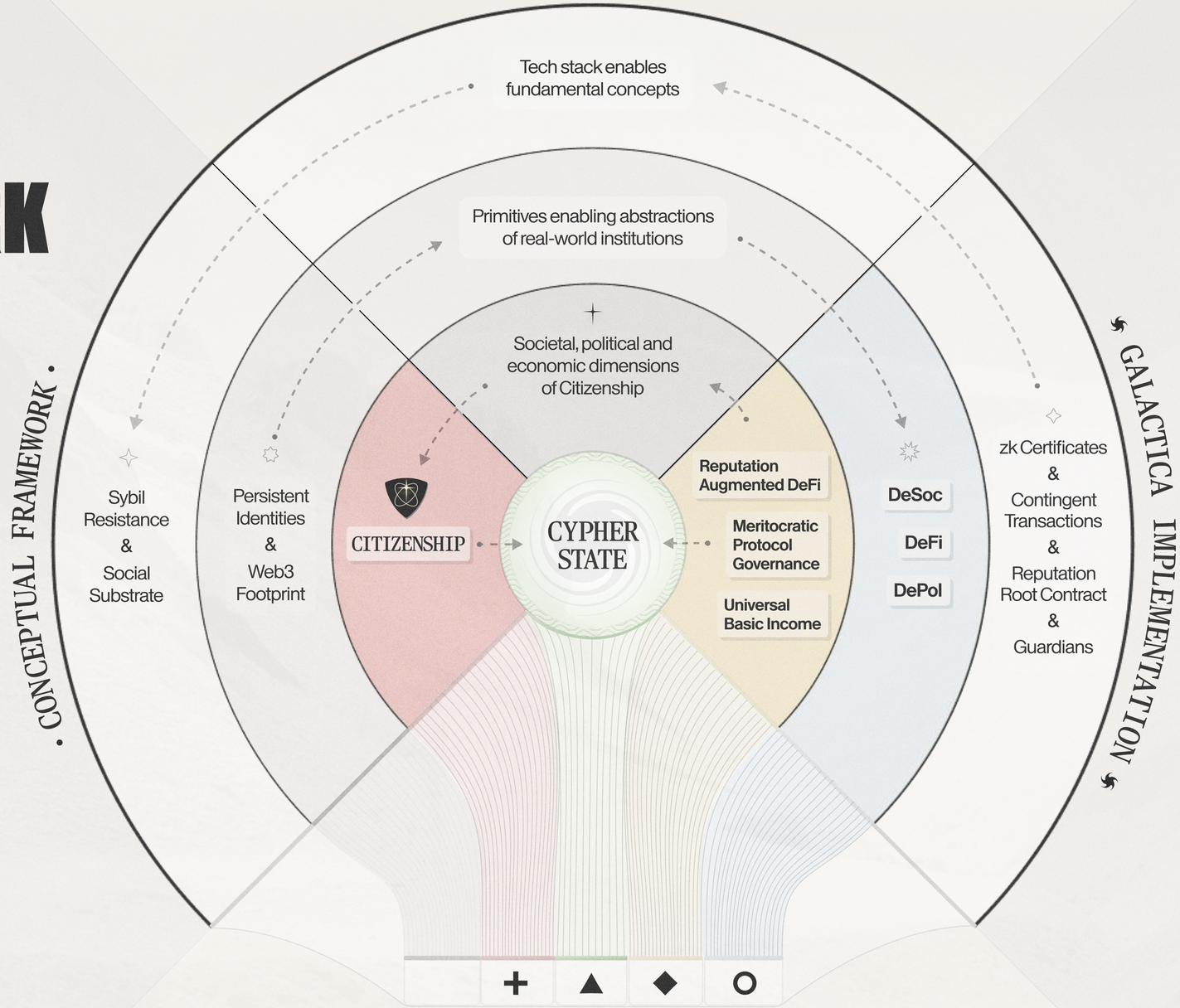



# OTHER USE CASES

MORE INFO

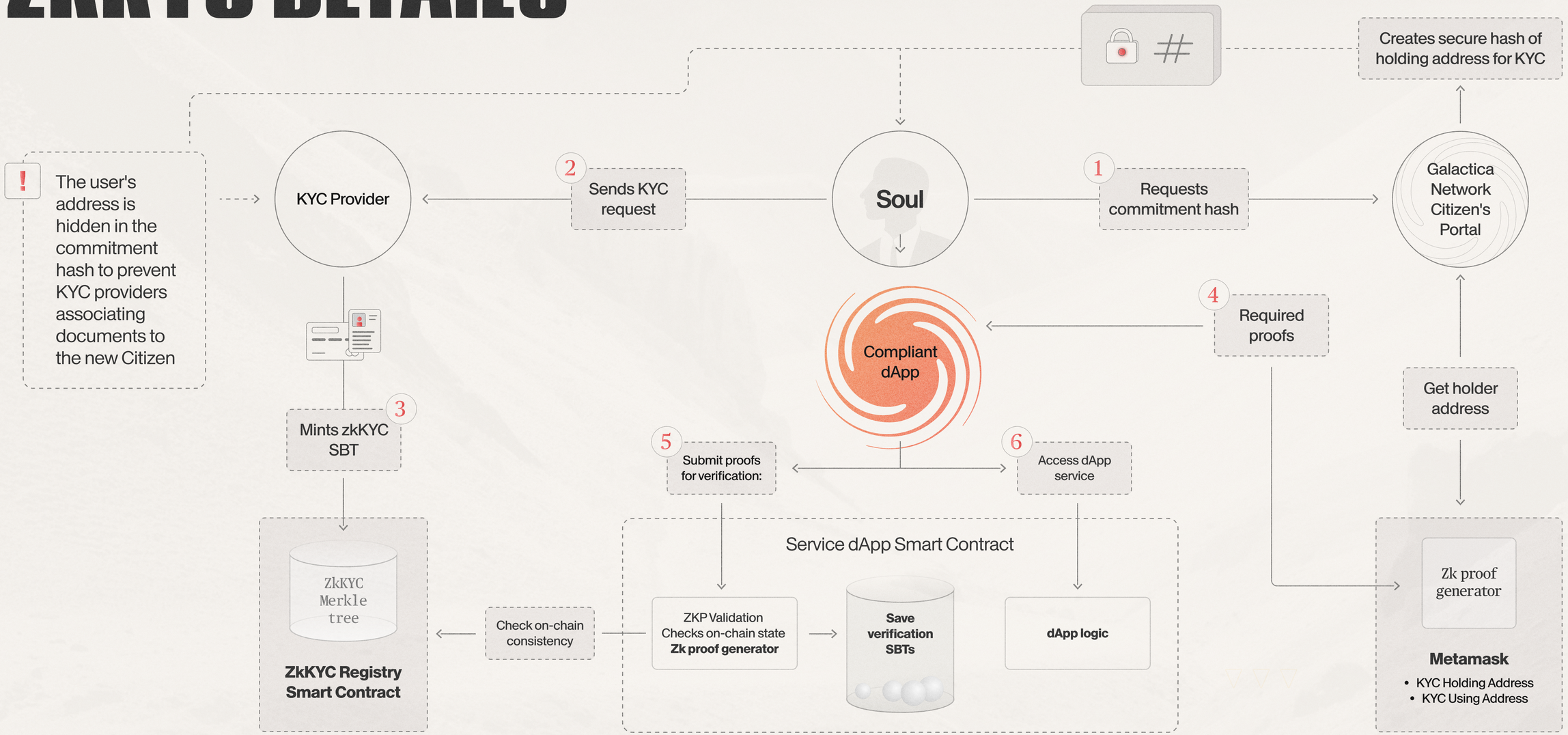
# APPENDIX

# GALACTICA CONCEPT FRAMEWORK

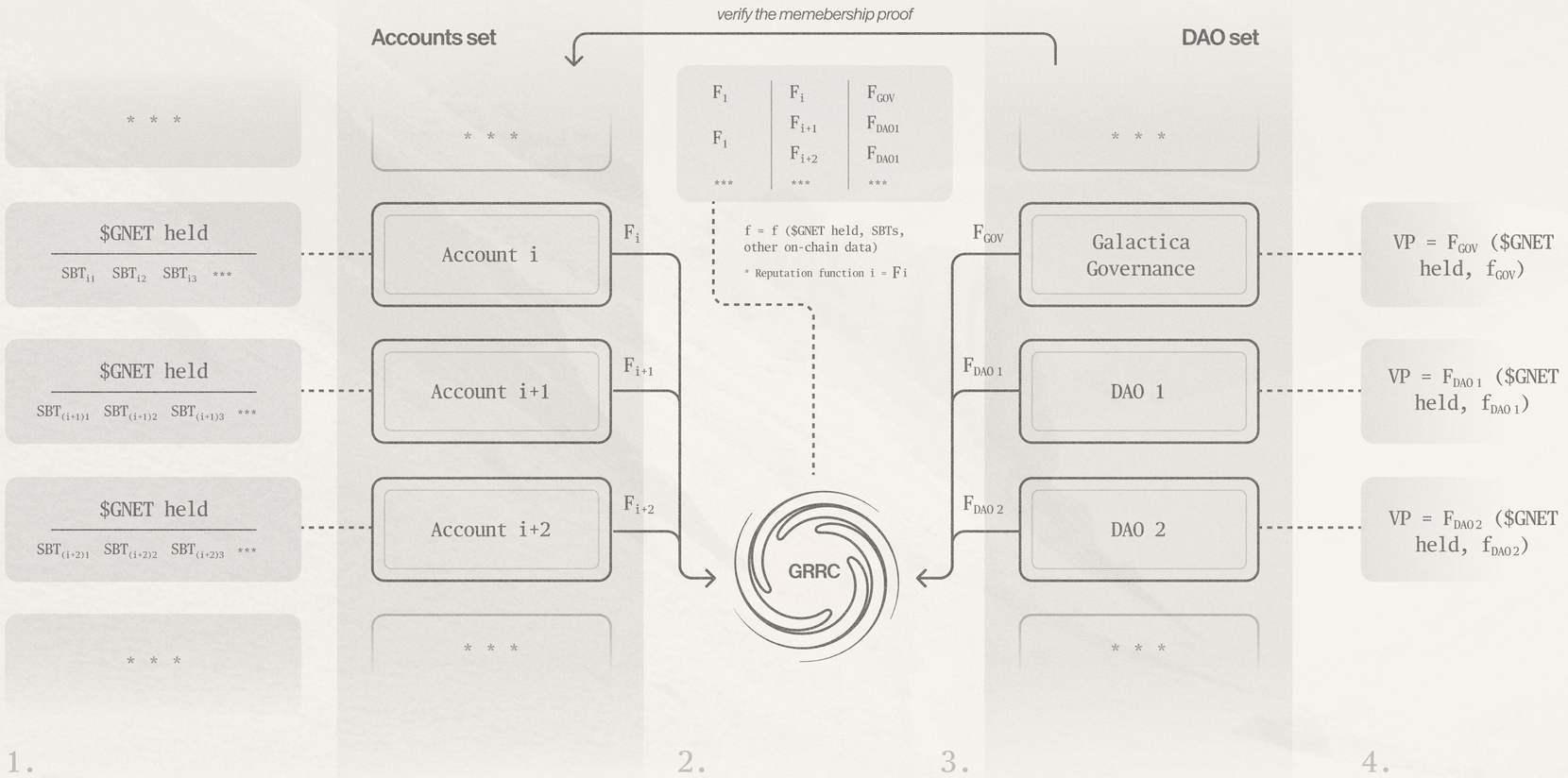


# ZKKYC DETAILS

## KYC RECORD CREATION AND VERIFICATION



# ROBUST ON-CHAIN REPUTATION THROUGH RRC



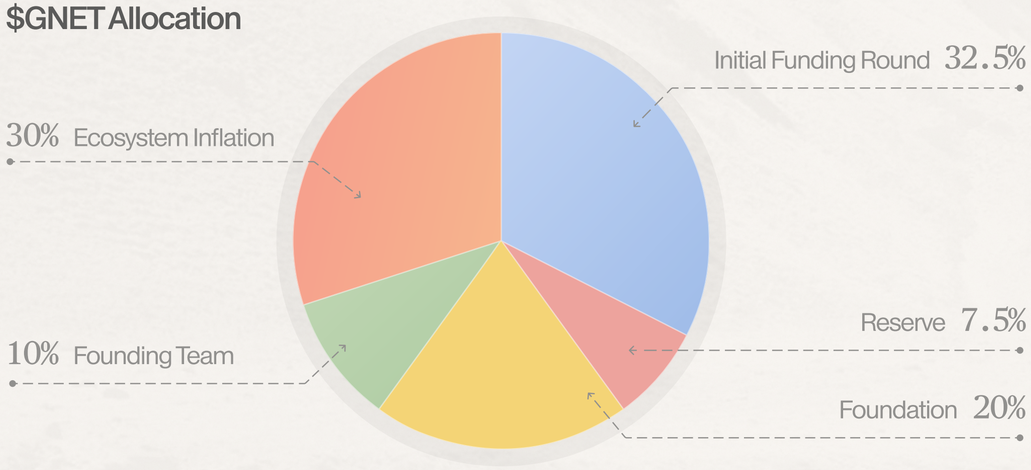

- Native onchain Reputation Scoring introduces a dimension of interaction where users' trustworthiness can be quantified, where contracts, accounts and Citizens can make Reputation contingent interactions.
- Reputation mitigates the wealth distribution-induced ecosystem asymmetry.

1. Every Citizen or contract has $GNET stake (or delegate) and a list of SBTs that are granted by other Citizens or contracts.
2. Each Citizen can specify the Reputation function f - a function with SBTs, $GNET held, staked or delegated and other on-chain data as inputs.
3. Every Citizen or contract (Governance DAO included) can specify the reputation function f through GRRC.
4. Every Contract (incl. DAOs) can specify the Voting Power F function.

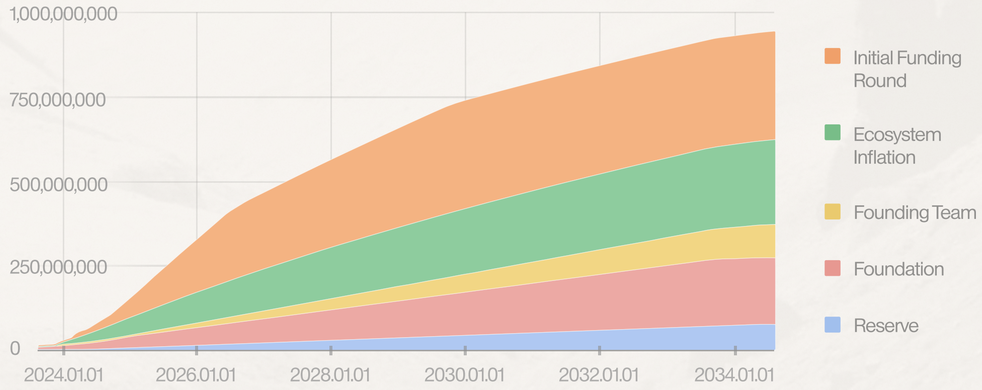
# COIN ALLOCATION & DISTRIBUTION SCHEDULE

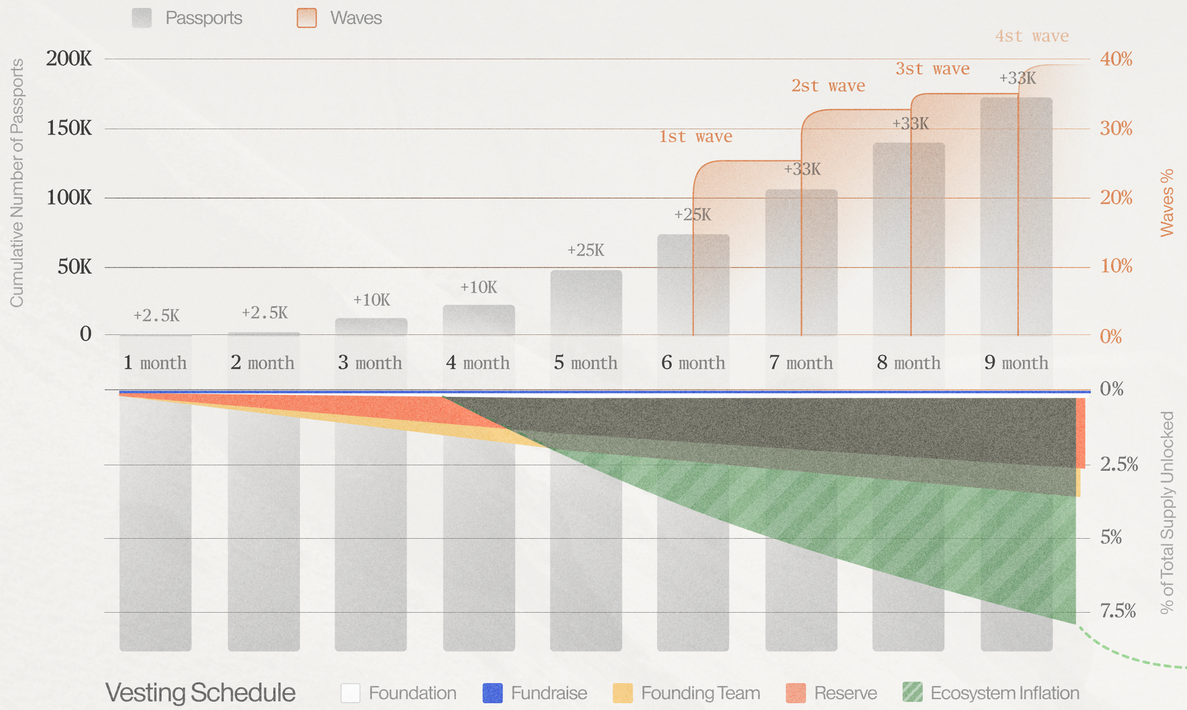
| | % of Total Supply | in Coins | Initial Unlock | in Coins | Lock | Vesting | Unlock Scheme |
|---|---|---|---|---|---|---|---|
| **Initial Funding Reserve** | 32.50% | 325,000,000 | To be determined | | | | Linear |
| **Reserve** | 7.50% | 75,000,000 | 0.00% | 0 | - | 10 years | Linear |
| **Foundation** | 20.00% | 200,000,000 | 5.00% | 10,000,000 | - | 10 years | Linear |
| **Founding Team** | 10.00% | 100,000,000 | 0.00% | 0 | 1 year | 10 years | Linear |
| **Ecosystem Inflation** | 30.00% | 300,000,000 | 0.00% | 0 | - | 36 years | x^-n |

## $GNET Allocation



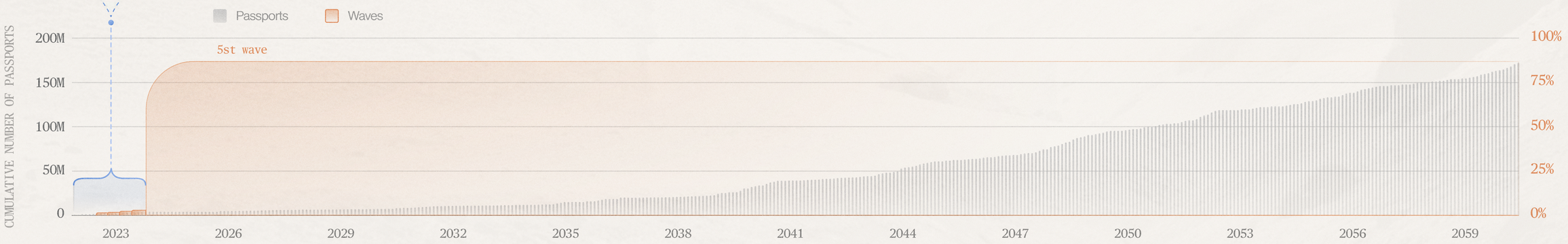

## $GNET Unlock Schedule (first 11 years)






| | % of Total Supply | Initial Unlock | Lock | Vesting |
|---|---|---|---|---|
| Initial Funding Reserve | 32.50% | | To be determined | |
| Reserve | 7.50% | 0.00% | - | 10 years |
| Foundation | 20.00% | 5.00% | - | 10 years |
| Founding Team | 10.00% | 0.00% | 1 year | 10 years |
| Ecosystem Inflation | 30.00% | 0.00% | - | 36 years |


1. Inflation distribution is subject to Galactica High Council vote. The weights can be altered once in several months.
2. Initially, there are 4 streams that inflation is channeled into:
   - A. UBI (reputation incentives),
   - B. Academy of Sciences (grants),
   - C. Validators (sec/decentralization incentives),
   - D. KYC centers (aka Guardians - user growth incentives).
3. The weights indicated are for illustrative purposes only. The weight of every stream is set by the High Council prior to new epoch beginning.



# THE CYPHER STATE