GALACTICA

Powered by SwissBorg & ZAMA

Galactica.com

The Ultimate Identity Stack

Aug 9, 2024

TURNING HASHES INTO SOULS

Table of Contents

Part I

Introduction to Galactica.com

We are here to give meaning to and enable utility for Web3 Identity

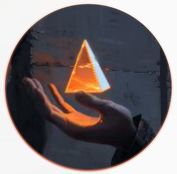
All the core identity use cases emanate from the notion of Web3 Reputation

Universal
Basic Income

Reputation
Augmented DeFi

Hyper Targeted
Attention Economy

Real World
Asset Rails



Undercollate-
ralized Loans

Social Account
Recovery

Data Sovereignty
& Monetization

In order to understand Web3 Reputation we first need to define Web3 Identity a.k.a. Soul

— One way to do it is that **Identity is just a set of data points** generated by an individual as a byproduct of one's online activity

Galactica.com enables users to encrypt, on-ramp and anonymize data points generated in web2 and web3 alike to form private persistent identities - the digital shadows of real people.

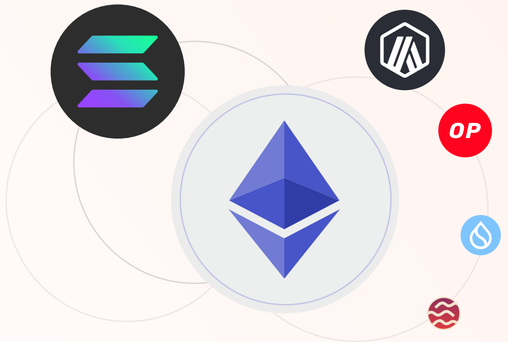
So now, what is Web3 Reputation?

— Reputation is a toolbox enabling the utility for Web3 Identities - i.e. making them functional on a public blockchain.

Web3 Identity Stack

is a set of technological and economic primitives making Web3 Identity practical — i.e giving it utility

In short, Web3 Identity Stack enables the use of Web3 Reputation.
The universe of use-cases it enables is known as DeSoc.



03.

Depending on the architecture, other mixes are possible, yet none maximizes both

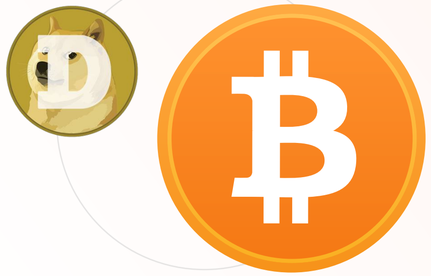
Programmability

04.

Human bound accounts and ZK maximize for both, FHE makes it computationally attainable

Privacy

01.



Standard public blockchains allow for some privacy and some verifiability

02.

One-time addresses and encrypted state allows for full privacy and no verifiability

Galactica.com is the Identity stack

— set of technologies to instill meaning and utility into Web3 Identities.

Galactica.com is Web3's ultimate FHE-powered Identity Layer. Our protocol stack enables concepts far beyond Proofs of Humanity — robust reputation and private data use-cases from DeSoc to user-centric dApp design. It eliminates the gap between off-chain and on-chain identities.

Co-founded by

SwissBorg.com

EU regulated brokerage firm and one of the larger crypto communities of **over 800k KYC'ed users and $1b+ AUM** is at the forefront of the identity revolution Galactica.com enables.

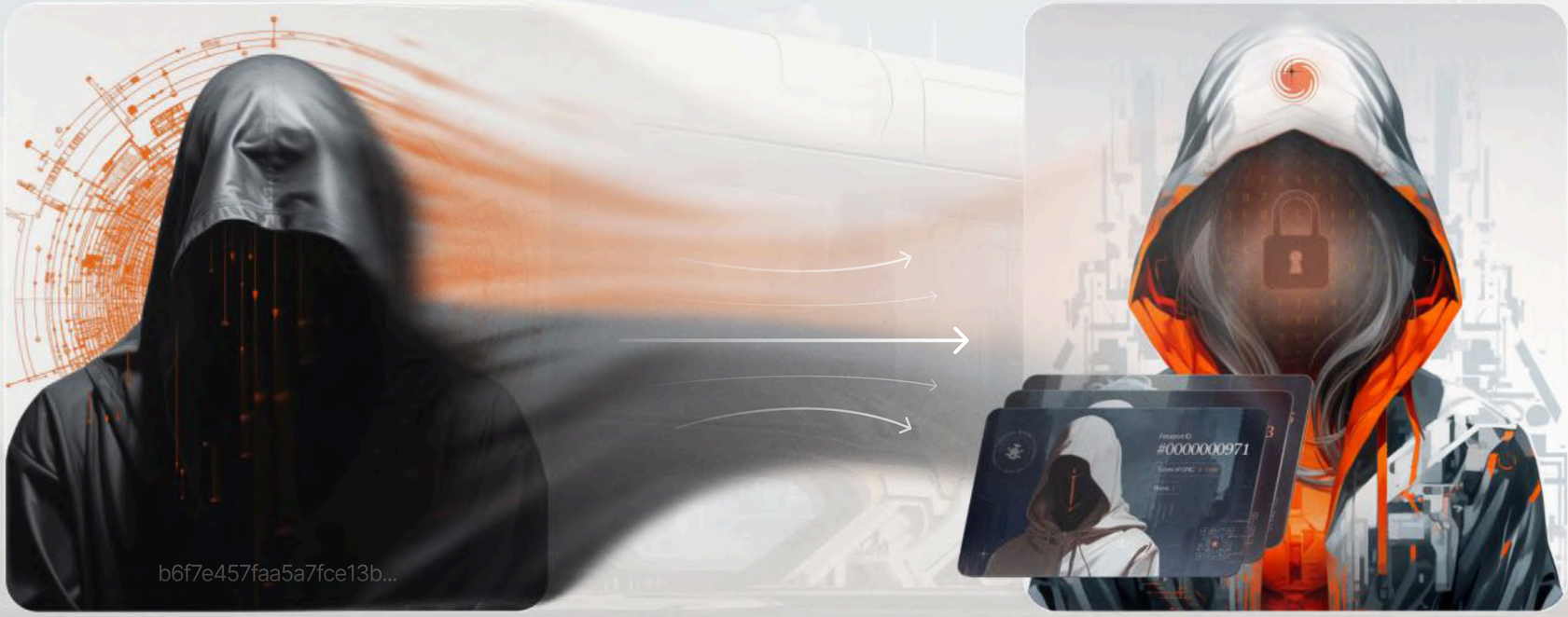
Part II

Tech stack overview

We are now set to explain the 'How?' part

Let's start with private data

Private data is what defines Web3 Identity. It is a link between hashes and souls.



Anonymous Address (Hash)

Encrypted Identity (Soul)

We are turning hashes into souls using

4 core protocol primitives

[Guardians]
Encrypt & Onramp

[zkCertificates]
Store and make private

[Reputation Root Contract]
Compute and verify

[Contingent Transactions]
Enable others to use it

[Guardians]

Encrypt & Onramp

Guardians — a set of whitelisted notaries that serve the purpose of on-ramping data on-chain in a privacy preserving manner.

Data originates, is submitted and verified off-chain. Guardians then issue an on-chain verification hash.

Guardians cannot associate on-chain activity and off-chain records they hold.

[zkCertificates] pt.1

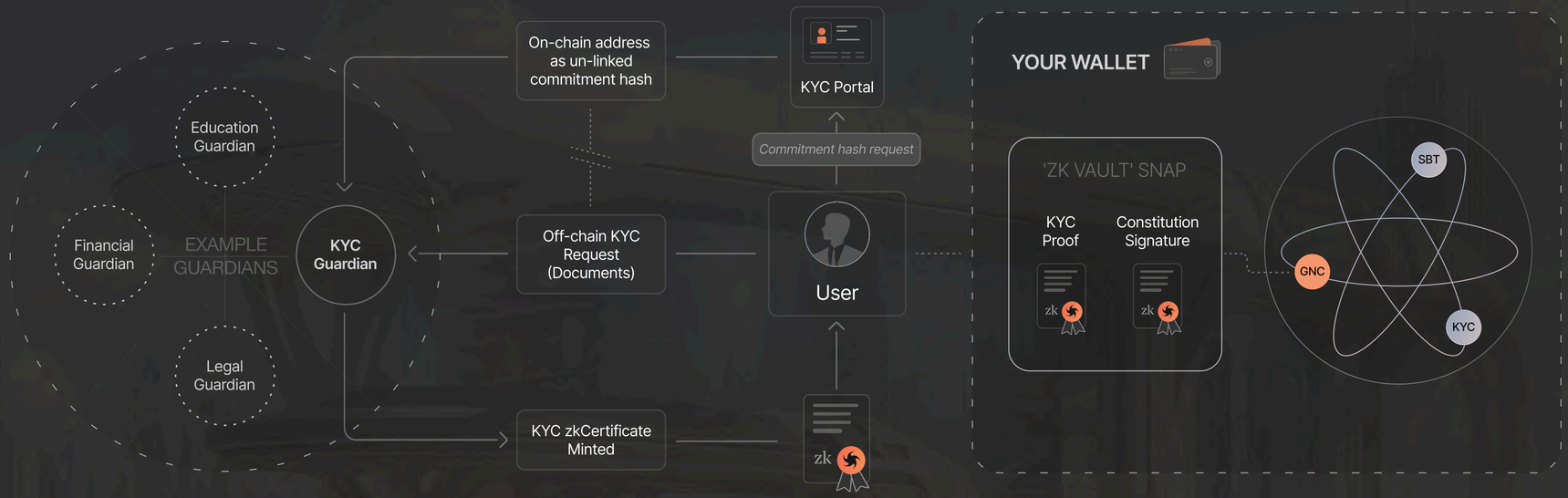
Store and make private

What are zkCertificates:

- On-chain attestations for personal data
- Allow verifying ZK statements about that data

E.g. >18 years old and from a non-sanctioned country without disclosing birthday, name or address or >1m followers in twitter

zkCertificates Core Stack Explained



This technology aims to balance the regulatory requirements for Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) with the privacy and security needs of users in decentralized environments.

However, zkKYC is just a specific use-case of zkCertificates. They can be used for other instances:

- Social media verification (Twitter followers count)
- Credentials (Proof of user having certain diploma)

[zkCertificates] pt.2

Store and make private

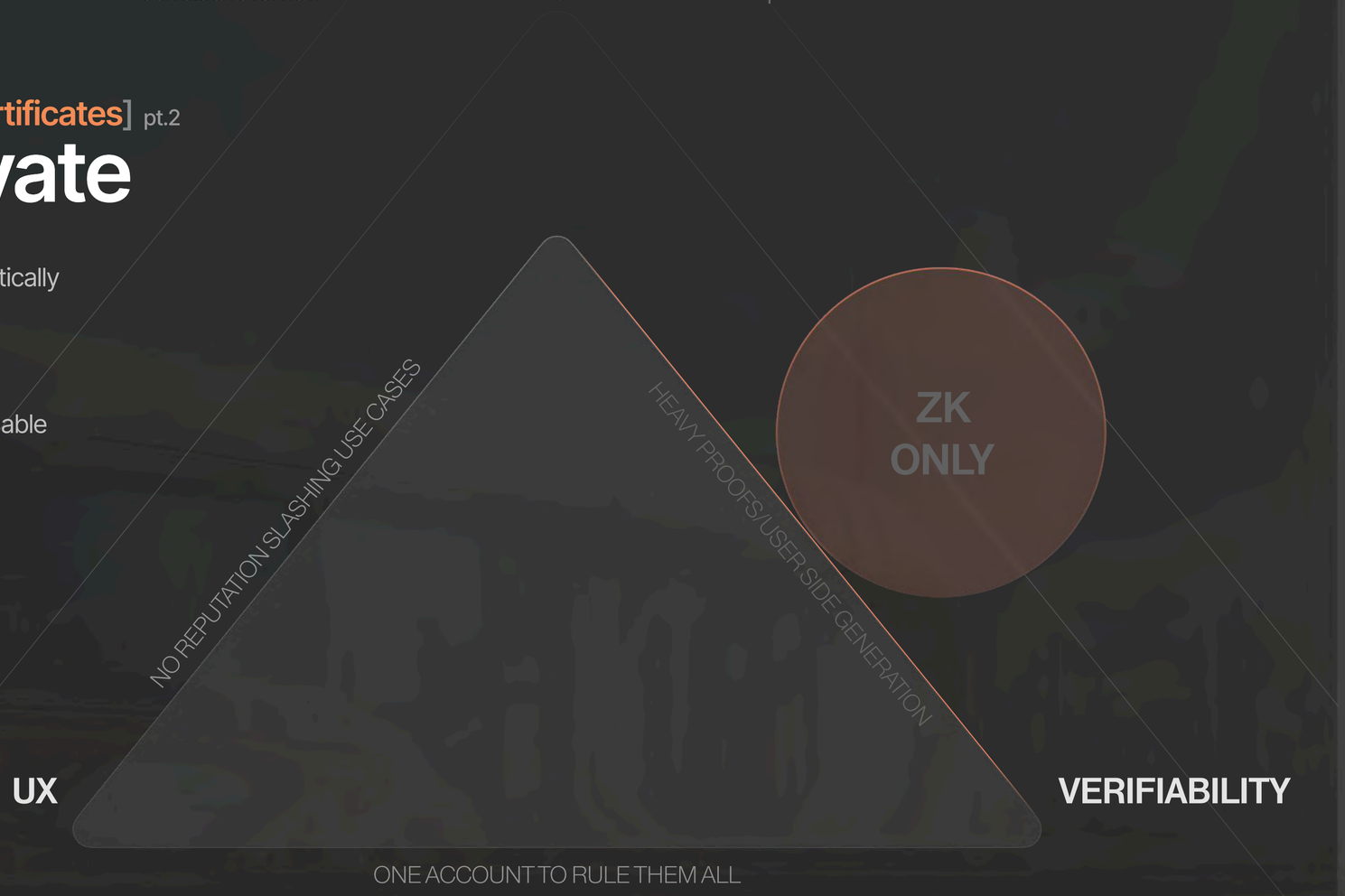
However ZK stack alone is not enough. Reputation slashing is a critically important idea for many use-cases where a user needs to prove absence of adverse behavior, such as private credit ratings.

ZK proofs leak data and allow for profiling. The only solution is to enable one-time accounts to split user activity and user data across many addresses. But then slashing reputation becomes highly non-trivial.

This causes the trilemma:

- Sacrifice Verifiability and lose reputation slashing mechanisms and all its use-cases like undercollateralized lending;
- Sacrifice Privacy and allow for eventual profiling of user activity;
- Sacrifice user expirience by forcing user side generation of ±1 GB proofs for some use-cases.

Up until recently, there has been no way of solving for all three.
Now there is.

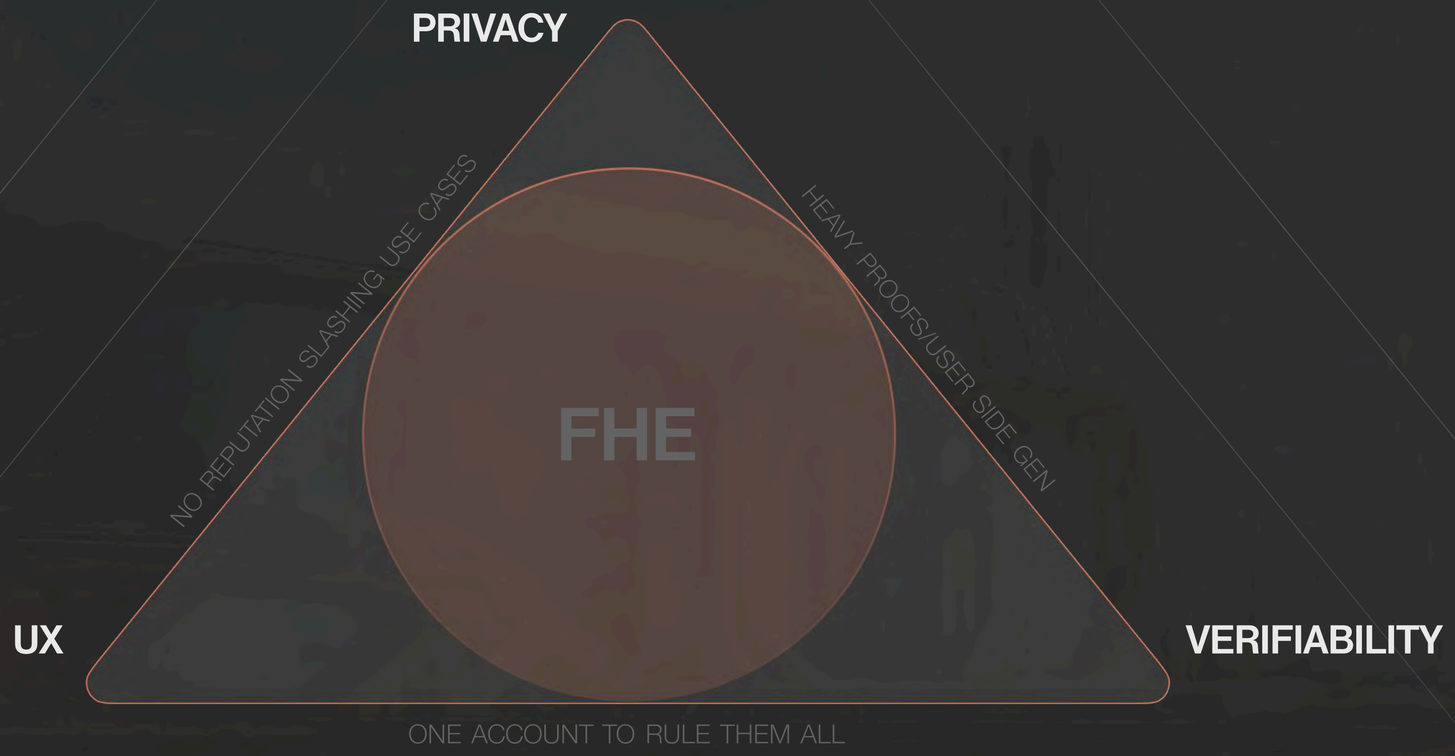


[FHE] pt.3

Store and make private

Integration of Zama's fhEVM can solve this trilemma:

- Integration into CosmosSDK infrastructure with EVM smart contracts
- Confidential reputation processing on-chain
- Moving compute effort to validators
- Maintaining privacy
- Programmable behavior in smart contracts

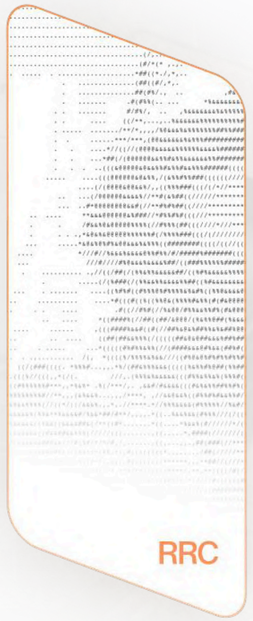


[Reputation Root Contract]

Compute and verify

RRC is a protocol reputation compute framework.

It is essentially an indexer of on-chain activity that computes certain user-defined reputation functions.



Essentially, **RRC allows users to compute arbitrary functions over the data points they have encrypted and on-ramped.** This effectively tokenizes private user data.

This design allows for native protocol usage and robust economics around compute costs of reputation, an approach significantly more robust than using oracles or smart contracts.

[Contingent Transactions]

Enable others to use it

The output of RRC is then used by dApps to fine tune the experience for the user. The mechanism through which they do so is called Contenginent Transactions.

Contingent Transactions enable apps building on Galactica **to create dynamic whitelisting rules** where the outcome of a transaction depends on the Reputation Score of the user (e.g. lower collateral rates for reputable users).

Augmenting smart contracts with private user data is the genesis of user-centric experience in dApp design.

Contingent Transaction

CYPHER BOOK

CypherBook is the interface to zkCertificates that store individual user private data. Only the user can access one's CypherBook.

GALACTICA
NETWORK

TLDR Galactica.com Protocol Logic

Data from both Web2 & Web3 is transferred and accumulated in user's Cypher Book (Passport)

zkCertificates are private data silos that allow one to encrypt and on-ramp any off/cross-chain data, securely store it and generate selective disclosures thereof

FHE-powered Reputation Root Contract allows to privately compute dynamic reputation functions over the encrypted data contained in the CypherBook

dApps are able to differentiate their service offering depending on users reputation

(e.g provide <100% loan if user's reputation is >= X)

Putting it all together

Galactica.com protocol design

Your Web2 Data

Big Tech

Social

Finance

On-ramp Data via Oracles

[Guardians]
Encrypt & Onramp

[zkCertificates]
Store and make private

Wrap Data in Encrypted zkCertificates

Form Data into Your On-chain Identity

[Reputation Root Contract]
Compute and verify

[Contingent Transactions]
Enable others to use it

Enter the Cypher State

Real World Asset Rails

Social Account Recovery

Reputation Augmented DeFi

Hyper Targeted Attention Economy

Universal Basic Income

Data Sovereignty & Monetization

Undercollate-ralized Loans

CYPHER BOOK

[1] Fully Homomorphic Encryption
[2] Reputation Root Contract
[3] Zero-knowledge
[3] Contingent Transaction

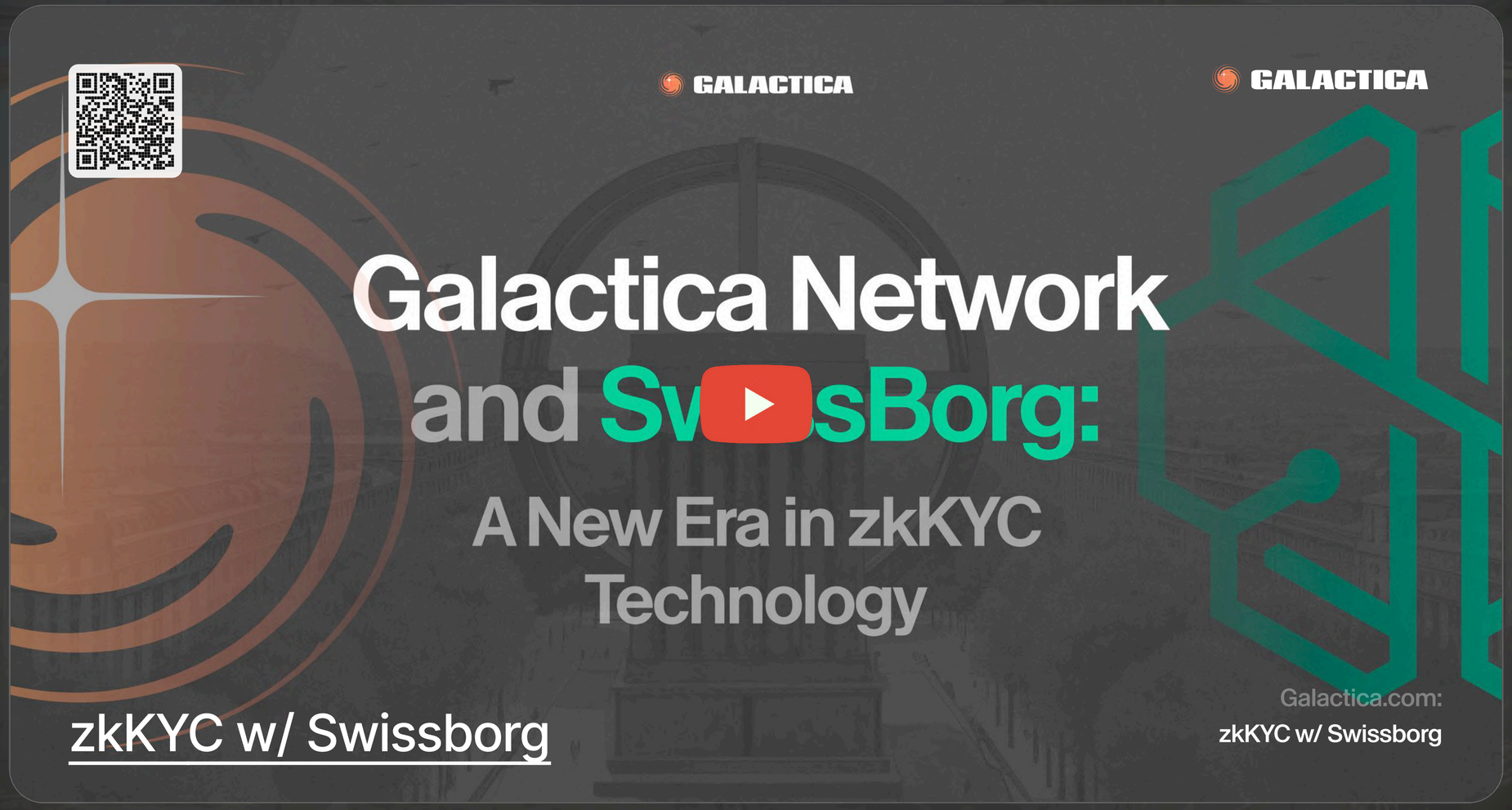
Part III

Success Cases and Roadmap

Galactica.com

Our use-cases

are by now case-studies



zkKYC at a Glance:

Redefining Regtech Landscape

Inspired by series of articles published by a16z and MME case study Galactica.com aims to implement a solution for an everlasting conundrum - a balance between privacy and compliance.

Core Concept:

- **Zero-Knowledge Know Your Customer** (zkKYC) uses zero-knowledge proofs to verify identities without exposing personal data.
- **Balances AML/CTF regulations** with user privacy in decentralized environments.
- **zkKYC is a form of zkCertificate** designed to enable compliant privacy

How it Works:

- **KYC Guardians**, ranked by reputation, issue KYC Records using new or existing data.
- **KYC Process:**
  - Hash added to blockchain as a Merkle leaf.
  - Encrypted data sent to user's machine, stored in a non-custodial wallet.
- **Users provide ZK Proofs** for verification without revealing data.

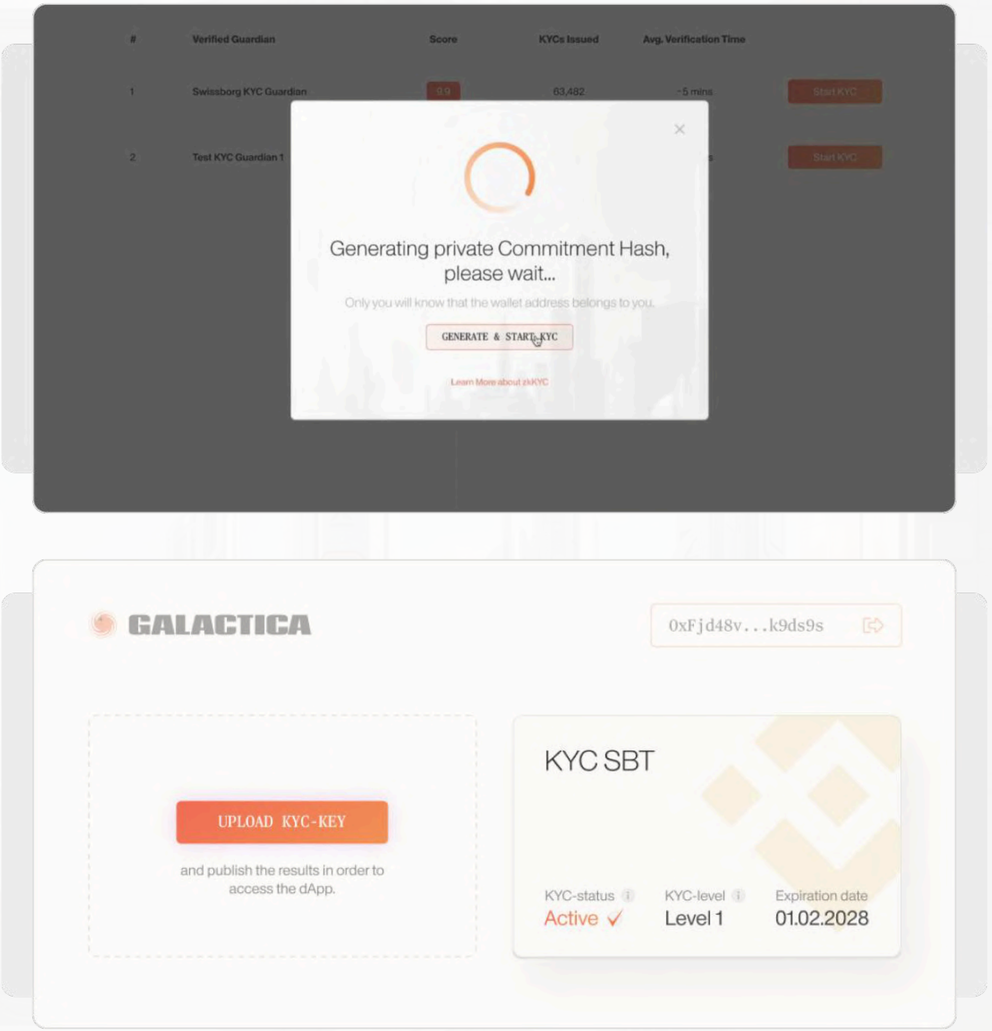
Key Features and Purpose of zkKYC

Key Features:

- Galactica.com deploys a zero-knowledge KYC (zkKYC) technological stack, partnering with a regulated financial institution, SwissBorg.
- This marks the first production zkKYC integration between a permissionless blockchain protocol and a regulated financial institution.
- Galactica's custom MetaMask Snap, the 'Galactica ZK Vault,' enables secure personal data management and storage.
- Enables off-chain proving of conditions without revealing data.
- Protects user privacy by unlinking KYC data from on-chain activity.
- Authorized decryption for verified suspicious activity.

Purpose and Vision:

- Provides a digital, sovereign, compliant identity for financial and social services.
- Single KYC usable across multiple dApps; Guardians ranked by reputation ensure safe service.



Use Cases of zkKYC

DeFi and Beyond:

- **Enables identity verification** for DeFi protocols, DEXs, token sales, and DAO participation.
- **Automates KYC**, reduces costs, and prevents fraud using zero-knowledge proofs.
- **Robust zkKYC system** enables decentralized markets around regulated financial instruments.

Off-Chain Use Cases:

- **Confirms age** for accessing restricted content without revealing birthdate.
- **Verifies eligibility** for services like online gambling while maintaining privacy.
- **Facilitates secure transactions** and asset exchanges with verified identities in gaming and the metaverse.

More can info can be found here: galactica.com/zkkyc_tech_specification.pdf

Meet CT.com — the ultimate launchpad for the influencer economy

Powered by FHE and ZKP, CT.com is a new chapter in SocialFi and DeSoc.

The problems of businesses largely stem from the same sources

1. **Hard to differentiate between great researchers, HQ content creators and 'passengers'** who are there to use their largely fake audience as exit liquidity;

2. **Is there any real way to score engagement?** There is, but it's circumstantial and good diligence takes a lot of resources;

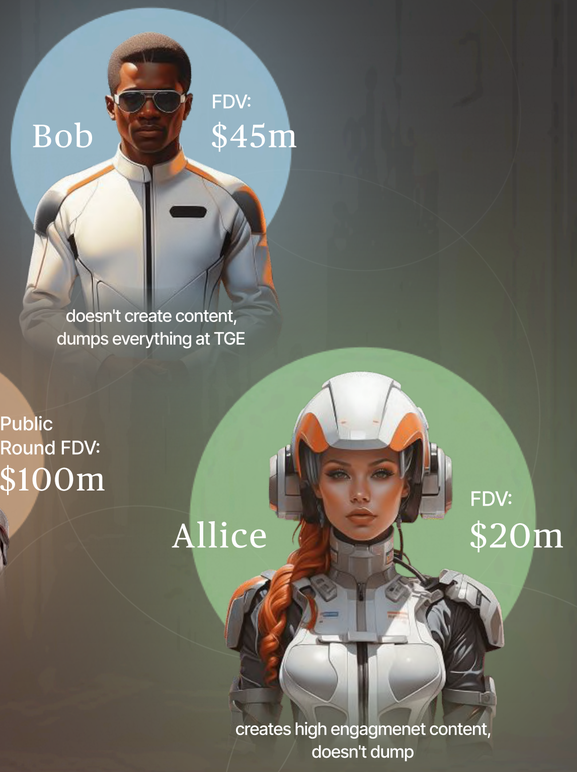
3. **How can one evaluate that influencer's activities drive core metrics for project's success.** Well, referral links.. Right?

4. **How to align incentives** without destroying project's economics. Is it through KOL round? Right?

How does it work?

Galactica.com provides tech stack (FHE & ZKPs) which enables to ensure privacy while aligning influencer reputation with project allocations

1. Anyone can create a private profile attaching one's **social profiles** and web3 addresses carrying all sorts of on-chain metrics.
2. **These data always remains private** – it's encrypted on the device and never makes it's way elsewhere.
3. **For every IDO a project comes up with a function** that relates social or on-chain contributions to the FDV and allocations sizes.
4. An influencer creates a proof of the function score using **FHE cryptography**. The score defines the allocation price, size, etc.
5. What we get is a meritocratic captable where the **worthy ones are rewarded the most**. Others – not so much.



But why has nobody done it before?

Why is Web3 Reputation Still Missing?

- Computational limitation
- Lack of privacy & verifiability
- Composability
- Real-time updates
- Expressive Functional form
- Necessity to rely on centralized surrogates

What Are We Losing Out On?

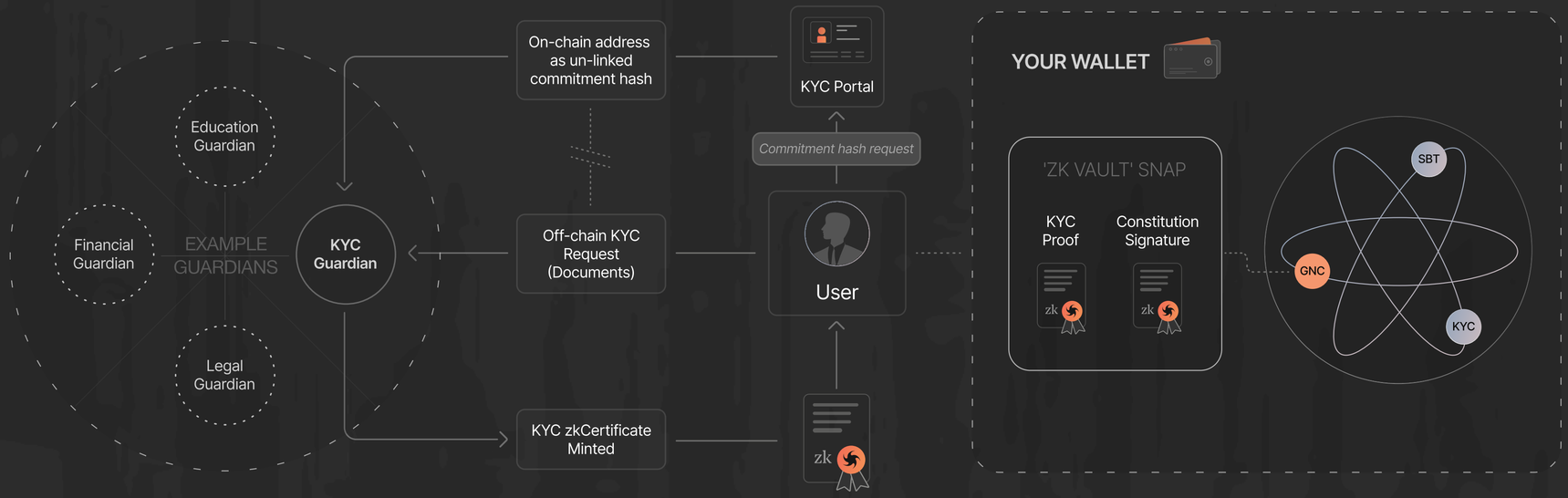
- Social capital
- Sybil Resistance
- Meaningful governance (not 1T1V model)
- Reputation Augmented DeFi
- Merit based distribution
- DeSoc & SocialFi primitives

Enabling Web3 Reputation requires solving the Trilemma.

Galactica.com is uniquely positioned to do so.

Appendix

zkCertificates



This technology aims to balance the regulatory requirements for Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) with the privacy and security needs of users in decentralized environments.

However, zkKYC is just a specific use-case of zkCertificates. They can be used for other instances:

- Social media verification (Twitter followers count)
- Credentials (Proof of user having certain diploma)

More can info can be found here: galactica.com/zkkyc_tech_specification.pdf

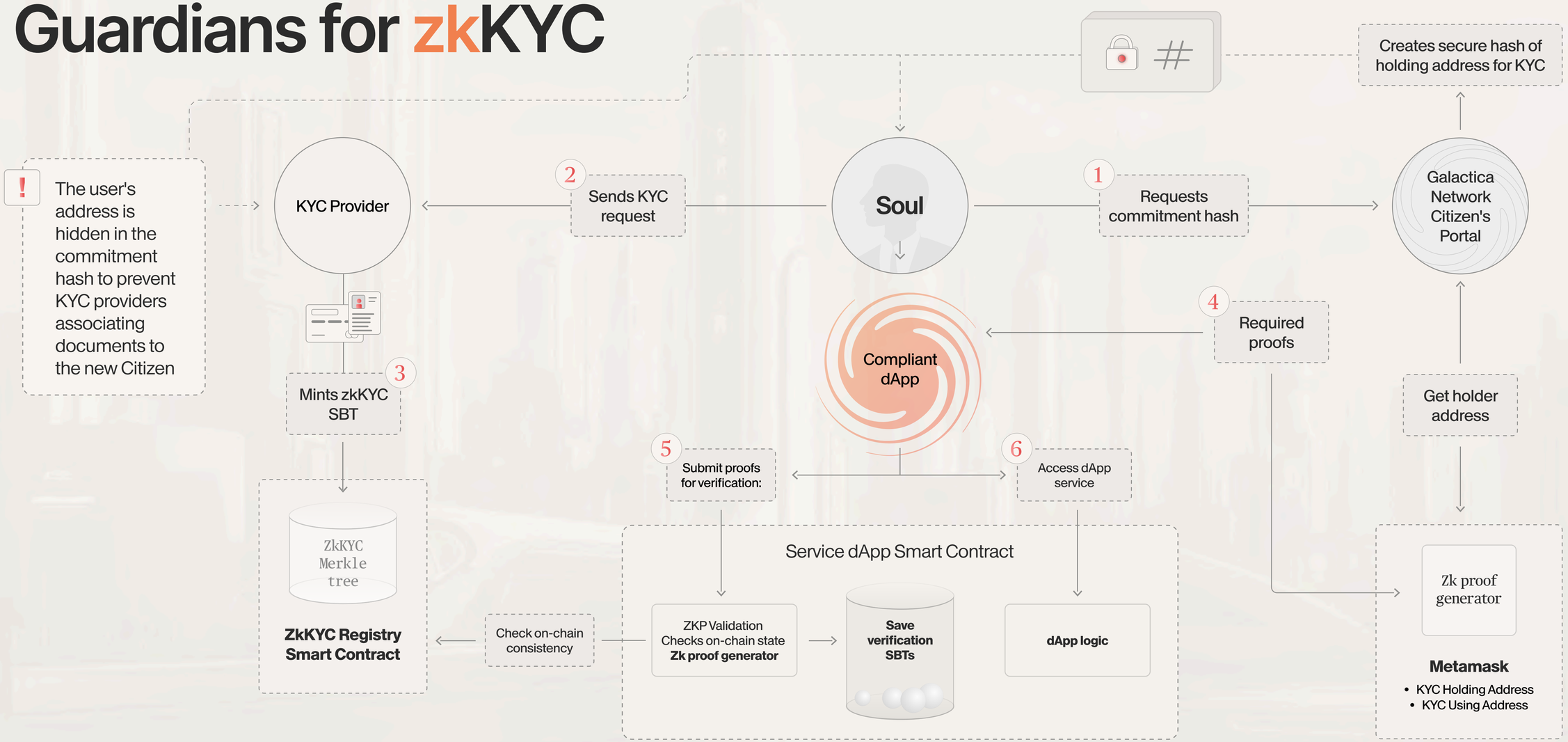
Competitive Analysis

Name	Type	Website	Twitter	Followers	Docs	Github	Description	Privacy Approach	Sybil Res. Approach	Status
Unirep	Reputation	https://about.unirep.social/	https://twitter.com/UniRep_Protocol?s=20	1.1k	https://developer.unirep.io/docs/welcome	https://github.com/Unirep	• UniRep is an anonymous data attestation protocol, providing developers with a pre-built, audited system to create ZK applications that associate data with anonymous users. • Protocol manages user data through anonymous identifiers, known as epoch keys, which promotes non-custodial applications that don't hold user data. • UniRep expands the concept of reputation to include user preferences, activities, alignments, and ownership. • It provides a foundation for developing customized zk apps, offering private data storage, extensible proofs, and trustless interoperability without any forced data sharing. • Attesters in the application layer can customize and manage user data, thereby providing accountability. • The ultimate aim of UniRep is to empower developers to build secure apps while ensuring comprehensive user privacy.	ZK	–	?
Orange	Reputation	https://www.orangeprotocol.io/	https://twitter.com/OrangeProtocol?s=20	12.6k	https://docs.orangeprotocol.io/overview	–	• Orange Protocol is a reputation and trust minting protocol, designed to consolidate on-chain data from multiple decentralized applications. • The protocol generates reputation proofs, Verifiable Credentials, and NFTs by considering various data points. These data points include on-chain transactions, asset balances, smart contract interactions, in-app data, reviews, social network profiles, IoT data, and financial information. • Orange Protocol primarily serves two audiences: dApp builders and Web3 citizens. • For dApp builders, the protocol provides the ability to use existing models or configure their own, integrate reputation into DAO systems, and reward community members with reputation-based NFTs. • For Web3 citizens, the protocol allows them to manage their reputations, link on-chain and off-chain data to their DIDs, and participate in campaigns to claim reputation NFTs.	Encryption (not enough info) Plans to use ZK in the future"	KYC	Live
Quadrata	Identity	https://quadrata.com/	https://twitter.com/QuadrataNetwork	8.5k	https://docs.quadrata.com/integration/introduction/introduction-to-quadrata	https://github.com/QuadrataNetwork	• Quadrata Web3 Passport is a privacy-preserving, sybil-resistant technology that aims to bring identity, compliance, and reputation to DApps built on public blockchains. • The Quadrata Passport is issued as a non-transferrable NFT. • There are following attributes of Quadrata Passport: amount of wallets, country, AML risk score, on-chain reputation.	"Data Encryption"	"KYC, AML checks before issuing SBT"	Live
Privado ID	Identity	https://privado.id/	https://x.com/PrivadoID	31.6k	https://docs.privado.id/	https://github.com/0xPolygonID	• Privado ID is an identity infrastructure based on self-sovereign identity principles, aimed at establishing trusted relationships between applications and users. • It enables organizations to issue VCs about users, which can be verified using tools in the SSI ecosystem. • Users can prove their identity without revealing private information through zero-knowledge proofs. • The core concepts are Verifiable Credentials, Identity Holder. Issuer, and Verifier, forming a “Triangle of Trust”. • Privado ID's achievements include privacy through ZKPs, off-chain and on-chain verification options, self-sovereignty, and transitive trust. • Privado ID includes additional tools such as the Wallet SDK. Issuer Node. Verifier SDK, and JS SDK to support developers in integrating decentralized identity solutions into their applications. • The Schema Builder and Query Builder tools further streamline the creation and management of credential schemas and verification queries. • Privado ID operates on any EVM-compatible blockchain and supports interoperability, making it suitable for a wide range of Web3 applications. • Privado ID is an open-source project, free to use, with plans to generate revenue through additional services and infrastructure support.	ZK	ZK KYC	Live

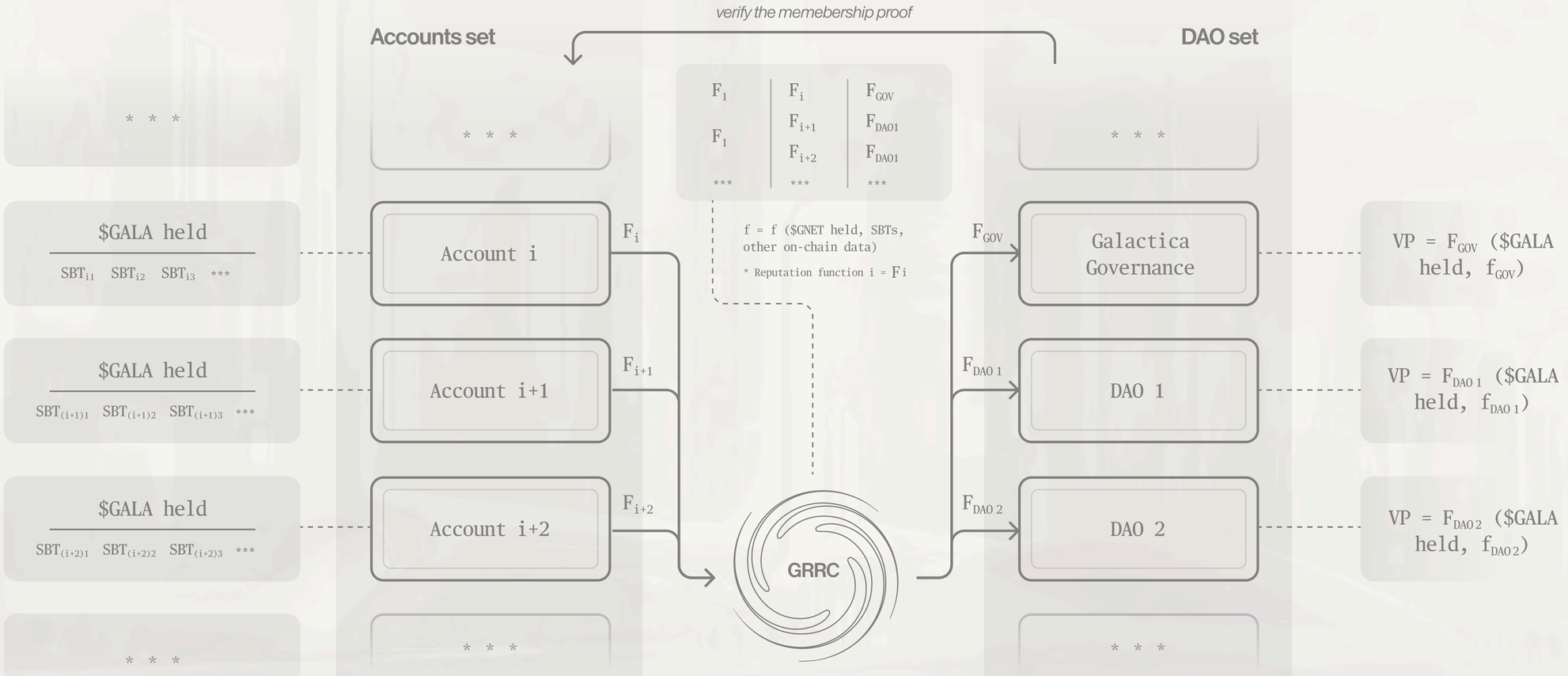
Name	Type	Website	Twitter	Followers	Docs	Github	Description	Privacy Approach	Sybil Res. Approach	Status
Galxe	Identity	https://galxe.com/	https://twitter.com/Galxe	1.4M	https://docs.galxe.com/	https://github.com/GalxeHQ	• Minting of participation SBT based on offchain snapshot, we already do this but better with verification SBT based directly on onchain data. • User usage data is submitted by a network of curators and exposed onchain through Galxe oracle. If we integrate Galxe into Galactica, this can be a way to allow reputation computation from offchain data.	Own technology based on ZK	SBT	Live
Disco	Identity	https://app.disco.xyz/	https://twitter.com/discoxyz	16.4k	https://docs.disco.xyz/disco-docs	https://github.com/discoxyz	• Disco is a platform focused on reforming internet data and identity management which is currently controlled by third-party companies. • Works like a Data Backpack which stores information about a user (identifier cards, licenses, education certificates). • The information can be seen only with a user's permission. • Disco uses Ceramic to store the data.	Encryption	Ceramic DIDs	Live
Humanode	Privacy	https://humanode.io	https://twitter.com/humanode_io	157.1k	https://gitbook.humanode.io/docs	https://github.com/humanode-network	• Humanode is a crypto-biometric blockchain powered by people and is designed to address the Sybil resistance issue with use of private biometrics. • Unique features of Humanode include biometric Sybil resistance, self-sovereignty for users over their digital identities, privacy-preserving capabilities, pseudonymity, inalienability, easy integration into existing protocols, and democratic access. • All nodes are biometricaly verified.	The data is processed automatically by a neural network, never leaving the user's device.	Biometrics Bot Basher	Live
Holonym	Privacy	https://www.holonym.id/	https://twitter.com/0xHolonym	5k	https://docs.holonym.id/introduction/private-credentials	https://github.com/opscientia	• Holonym is a privacy-preserving identity protocol that uses ZKPs. • Holonym serves as a private credential system that simplifies the process of preserving privacy for both on-chain and off-chain identity verification. • The protocol ensures that the party issuing credentials (like a KYC provider) cannot determine the user's wallet address.	ZK Claims that KYC data is deleted from both Holonym and KYC Provider's serves	SBT	Live
WorldCoin	Identity	https://worldcoin.org/find-orb	https://twitter.com/worldcoin	388.3k	https://docs.worldcoin.org	https://github.com/worldcoin/idkit-js	• Worldcoin is a digital identification platform that aims to provide each person on earth with a way to verify that they are a real human and not a bot or an AI algorithm. • The heart of the platform is World ID, which enable users to verify their humanness online while maintaining their privacy. "Proof of Personhood" is created by an iris-scanning device called the Orb. • A user's World ID resides exclusively in their device via an identity wallet like the World App. • Whenever proving uniqueness, the World app creates a ZKP, showing knowledge of an identity commitment's secret without disclosing which one. • One of the potential use cases of World ID is wealth distrubtion e.g. UBI.	ZK	Passport	Live
Silent Protocol	Compliance	https://silentprotocol.org/	https://twitter.com/silentdao_?s=20	14.3k	—	—	• Silent Protocol is a full stack privacy infrastructure. • Silent Protocol grants an application the framework that provides the users of said application with the power to communicate with other network operators, from thei metamask while maintaining complete anonymity • Privacy is ensured by Economical Zero Knowledge Execution Environment (EZEE). • Silent Protocol employs a MPC protocol to create the silent compliance VM. • The Silent Compliance Committee, a decentralized body governed by the Silent DAO, cooperates with regulators to maintain lawful state upgrades and keep bad actors away. • The committee leverages Collective Intelligence to ensure privacy is maintained as the norm and bad actors are deterred.	ZK	Apparently zkKYC	Not launched yet
ENS	Identity	https://ens.domains/	https://twitter.com/ensdomains?s=20	264k	https://docs.ens.domains/	https://github.com/ensdomains	• The Ethereum Name Service (ENS) is a distributed, open, and extensible naming system based on the Ethereum blockchain. • ENS's job is to map human-readable names like 'alice.eth' to machine-readable identifiers such as Ethereum addresses, other cryptocurrency addresses, content hashes, and metadata. • ENS also supports 'reverse resolution', making it possible to associate metadata such as canonical names or interface descriptions with Ethereum addresses.	—	—	Live

Name	Type	Website	Twitter	Followers	Docs	Github	Description	Privacy Approach	Sybil Res. Approach	Status
Privacy Pools	Compliance	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364	—	11.9k downloads 13 citations	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364	—	• Paper envisioning compliance proofs for mixer protocols. • Limited to mixers (transfering funds between accounts in untracable way) • Users prove compliance of withdrawals by proving that their funds originate from a compliant pool of deposits. • Privacy as in existing mixing protocols (e.g. TornadoCash) • More details: https://docs.google.com/document/d/11la7fL60tfmBHfqysKFQZJIZ9aqNx4xx5NS8zh0Q9Y4/edit	ZK	—	Theory paper
Zkpass	Identity	https://zkpass.org/	https://twitter.com/zkPass	234.2k	https://zkpass.gitbook.io/zkpass/	https://github.com/zkPassOfficial	• They seem to build the zkCertificate part of Galactica and offer the selective disclosure/condition proof, but instead of storing the zkCertificate hash in onchain merkle tree and create a proof in relation to that the data are retrieved from a data source (centralized) and to prevent users forge a proof with false data they use MPC in proof creation and interaction with verifier (dApps). • The whole process interactive, i.e. it requires several steps compared to our one step solution. so i think we are clearly better than what they describe in the medium article so far.	ZK	ZK KYC	Live
Dock	Identity	https://dock.io/	https://twitter.com/docknetwork	60.7k	https://docs.api.dock.io/#the-dock-certs-api	https://github.com/docknetwork	• Dock.io offers a secure and scalable infrastructure using Substrate-based blockchain technology, facilitating the creation of Verifiable Credentials and Decentralized Identifiers (DIDs). • The platform enhances privacy through zero-knowledge proofs and supports passwordless Web3 authentication for secure user interactions. • It ensures interoperability with W3C standards, allowing seamless integration with other systems and adherence to global digital identity standards. • Dock.io provides comprehensive tools for issuing, storing, and verifying credentials, maintaining data integrity and privacy. • Integration features include an ID wallet SDK, automated payment systems for verification, and compatibility with Ethereum smart contracts.	ZK	KYC	Live
Gitcoin	Identity	https://www.gitcoin.co/	https://twitter.com/gitcoin	207k	https://docs.passport.gitcoin.co/building-with-passport/introduction	https://github.com/gitcoinco	• Has a feature called Gitcoin Passport, but it linked to an Ethereum address and doesn't contain any identifying information. • Each Gitcoin Passport can be assigned a score, which is the sum of stamps scores. • Examples of stamps: connecting to Gmail, Twitter, Facebook, Github, verified name in ENS, contributed to Gitcoin grants,... • Stamps are verified by Gitcoin with 90 days validity. • Infos are stored in Ceramic network (a ofchain decentralized database), user can also choose to post these info to Ethereum to integrate with other dApp, but the state might not always be up to date. • Only users with passport score higher than 20 will have their contributions matched by Quadratic fundings.	—	—	Mainnet
Kinto	Compliance	https://kinto.xyz/	https://twitter.com/KintoXYZ	147.3k	https://docs.kinto.xyz/kinto-the-safe-l2/general/welcome-to-kinto	https://github.com/kintoxyz	• L2 blockchain of Ethereum built on OP stack. • Focus on safe and compliance to combine DeFi with TradFi. • Compliance by requiring KYC from users and checking AML against OFAC sanction list on every transaction. • Safe by requiring insurance for each smart contract. • Native account abstraction (web2 like, depending on KYC). • more details: https://docs.google.com/document/d/1J5DI-XDPfq7_9sYb1vS4i9yVjJnlFdlY2CUvCkStcA/edit	• KYC data stays at identity provider • User permission for dApps to query data fields off-chain	Enforced KYC at one available identity provider	Live
Ethos	Reputation	https://www.ethos.network	https://x.com/ethos_network	10.3k	https://whitepaper.ethos.network	—	• Ethos is a credibility platform that builds trust in the web3 ecosystem by generating credibility scores through user contributions, reviews, and vouching. • Users earn and build reputation by reviewing others, backing trusted profiles with staked Ethereum, or penalizing bad actors. • Reviews and vouching are key mechanisms that influence the credibility score, reflecting both financial backing and social validation. • The platform integrates with existing web3 interfaces and dApps, ensuring a broad and adaptable application. • Attestation links digital identities and wallets to Ethos profiles, enhancing trust and reducing fraud.	Not enough info	Valid Ethos profile is required	Waitlist

zkCertificates & Guardians for zkKYC

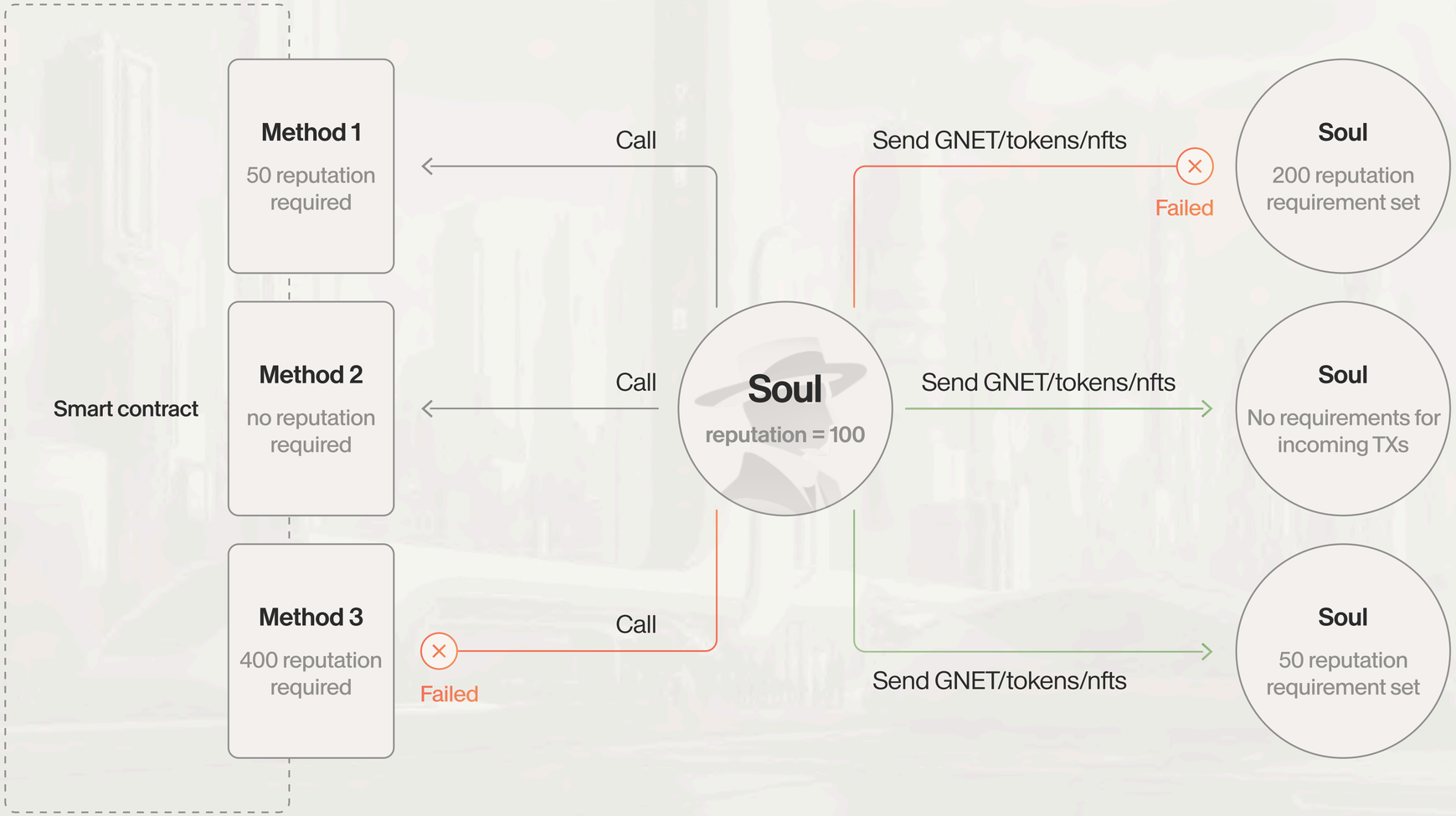


Reputation Root Contract



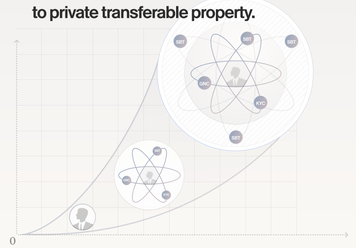
1. 2. 3. 4.

Contingent Transactions

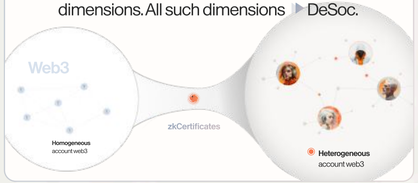


DeSoc and Its Various Derivatives

1 DAOs are primitves, while Defi is skewed toward hyperfinancialization **as it is confined to private transferable property.**



2 When Reputation is used to assign weight to a human in redistributive process ▶ meritocratic dimensions. All such dimensions ▶ DeSoc.



3 **DeSoc** is the societal substrate that **enables a new dimension of web3 use cases**, the most important one being the Cypher State

- The state of the art in web3 is hyper-financialization across the spectrum of DeFi institutions and primitive governance frameworks that more often than not boil down to variations of 1T1V or reliance on web2 for Sybil resistance.
- DeSoc is the human dimension a.k.a. societal substrate infused into existing web3 financial and governance primitives. It is on the intersections of DeFi, DAO, and DeSoc where the next wave of economic, financial and political innovation will emerge.
- As has been said better elsewhere, "…native web3 social identity, with rich social composability, could yield great progress on broader long-standing problems in web3 around wealth concentration and vulnerability of governance to financial attacks, while spurring a Cambrian explosion of innovative political, economic, and social applications." [Decentralized society: Finding web3's soul - Weyl, Ohlhaver, Buterin 2022]

4.1 DeSoc: In it's purest form, DeSoc itself allows for use cases such as Social account recovery, Sybil resistant governnace primitives, such as QF and QV, Souldrops as a way to more accurately fine tune incentives.

Pluralism & Plural Property

- Permissioning access to resources like homes or cars, where SBTs can manage conditional and non-transferable access rights.
- Data Cooperatives, where SBTs manage data access for researchers and handle members' rights and economic benefits from research discoveries.
- Market design innovations, such as Harberger taxation and self-assessed licenses sold at auction, with SBTs enabling more nuanced versions of these concepts.
- Democratic mechanism design, like quadratic voting, where SBTs enable community members to vote on parameters such as incentives and tax rates, exploring the space between markets and politics.
- Participation, where SBTs help integrate less contextualized individuals (e.g., immigrants, adolescents) into broader networks, offering them voting rights and influence

Plural Nertwork Goods

- DeSoc improves prediction markets with team-based voting, making predictions more equitable and less biased.
- DeSoc enhances AI by respecting data origins and creators' rights, resulting in more balanced, context-aware AI models.
- DeSoc innovates in data privacy, offering adaptable, rights-based privacy settings that balance individual and community needs.

4.2 **DeSci, DePol and Reputation Augmented DeFi** are all clusters of applications leveraging the identity aspects that **DeSoc enables.**

Identity is the substrate from which the institute of reputation can emerge. Persistent reputation, in turn, is key for finance, academic endeavours and politics.

	Reputation-based governance	Token-based governance
Voting power	**Tied to value of contributions:** Has the aim of creating a meritocratic system	**Tied to token ownership:** Potentially leads to a plutocratic system
Access / entry	**Anyone who contributes non-monetary value:** Where value is measured by work, ideas, etc.; latecomers may be at a disadvantage as reputation builds over time	**Those who own tokens:** Potentially limiting access to those with low capital; latecomers are not necessarily disadvantaged
Incentive alignment	**Incentivizes increasing reputation scores:** Hypothetically can encourage people to act in the best interest of the community	**Incentivizes increasing value of tokens:** May or may not align with long-term community goals
Liquidity / speculation	**Non-transferable:** Prevents market-based selling of reputation and market-based exit	**Transferable:** Creates potential temptations to exit
Longevity	**Long-term:** Reputation is built over time	**Variable:** Governance tokens can be quickly acquired and liquidated
Scalability	**Hard:** Measuring the value of contributions can be complex, time-consuming, and context-specific	**Easy:** Tokens can be easily transferred and divided
Sybil resistance	**More resilient:** Reputation may be tied to unique personhood, although there are concerns about selling proof of personhood	**Vulnerable:** Token acquisition can be botted, as has been widely observed in airdrop farming
Privacy	**Less private:** Potential privacy concerns when verifying identity	**More private:** Pseudonymous token-ownership preserves privacy

4.0 **Definitions**

Reputation Augmented DeFi

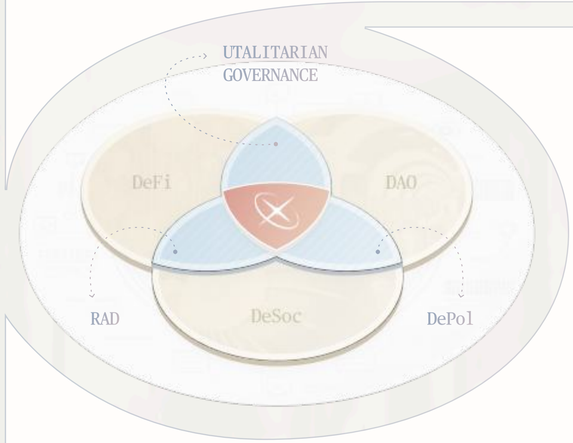
Galactica Network's societal primitives enable complex business models such as undercollateralized DeFi, and offers an unprecedented level of compliance even when compared to TradFi institutions and financial systems

Decentralised Society

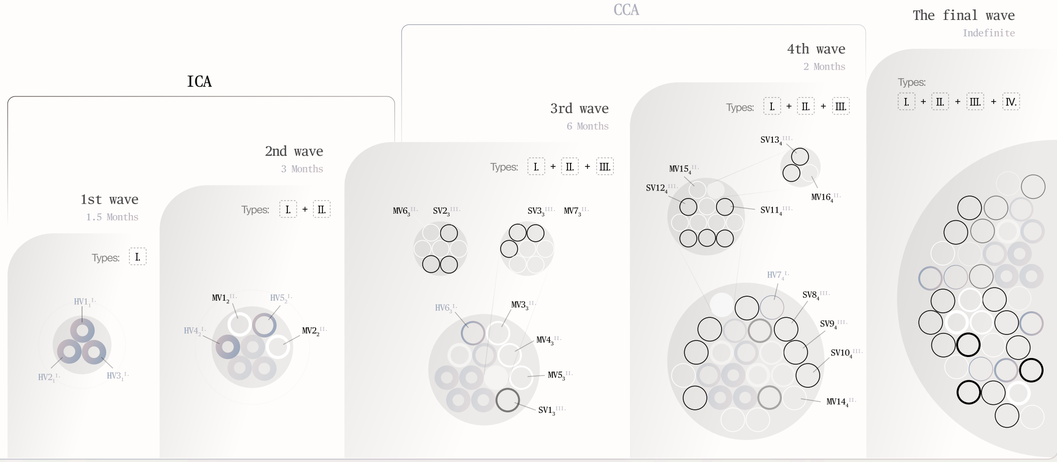
The notions of Persistent Identity and Web3 footprint together enable non-trivial societal institutions to be modeled entirely on-chain

Decentralised Politics

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



4.3 **Cypher States and Protocol Citizenship:** a holistic toolkit for building permissionless social institutions is set to become a key piece of the infrastructure of political sovereignty in the cypher space.

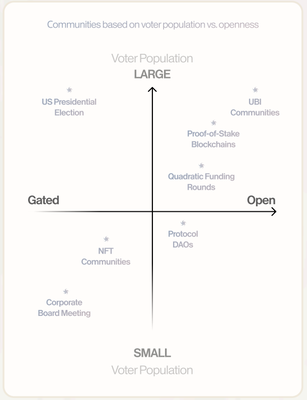


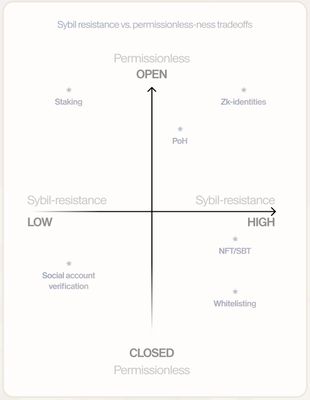
Global Immutable Identity and Persistent Reputation

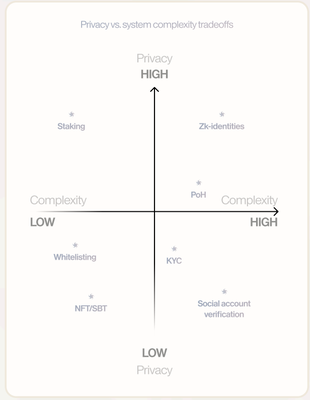
1 **Reliable Identities generate data points** as by-products of their existence, both online and offline. The totality of these data points **forms one's Reputation space.** This space is meaningless if the identities are not reliable; If they are not Persistent.

2 **These data points are used in risk management** and situations that require signalling of merit broadly for:

- Risk Mitigation
- Association
- Redistribution







4 Mapping off-chain, cross-chain, and importantly on-chain data points into a privacy preserving persistent and unique identity **will open a variety of use cases:**

I Undercollateralized lending and increased capital efficiency;

II Real time dynamic collateral systems;

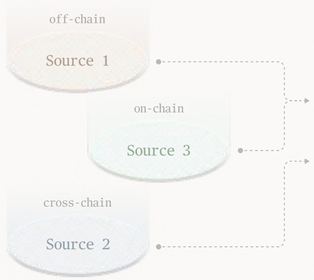
III Meritocratic primitives;

IV Hyper allignment of incentives;

V Pluralistic network goods;

VI Off-chain persistent reputation;

VII Efficient social matching mechanisms.



I **Data points can be imported from various sources,** broadly falling into the following categories:

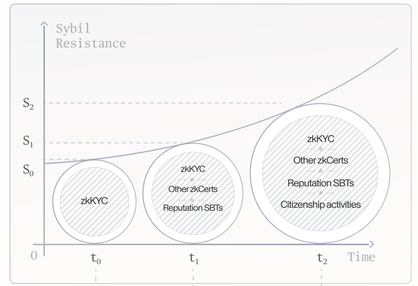
- **Off-chain** (such as one's Twitter account and related data);
- **On-chain** (deduced from one's tx history on Galactica Network);
- **Cross-chain** (deduced from one's tx history on other blockchains).

II **These data points can be imported onto Galactica Network accounts** (public addresses) generated by the same real world uniquely identifiable entity, such as:

- Humans
- Legal entities
- AI entities

III **Zero knowledge proofs can be thereafter used in real time** to prove statements about the data points imported for various use-cases, such as:

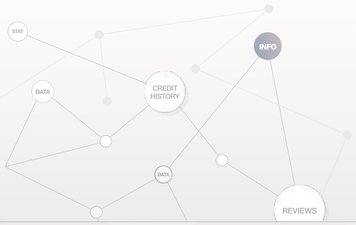
- **Off-chain** (such as surfing the talent networks)
- **On-chain** (an undercollateralized DeFi loan from an app building on Galactica Network)
- **Cross-chain** (same type of loan in another blockchain ecosystem)



The cost of Sybil Attack grows due to requirements to have **zkKYC.** It's the bootstrap phase.

Sybil Resistance further grows as individuals trust the platform and import off/cross chain data points and generate on-chain reputation as a result of activities.

The true Sybil Resistance emerges alongside self-aware intelligent citizenry who involve themselves with the governance framework of the protocol.

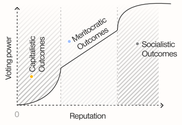


3 In short, **these data point form the basis for human heterogeneity** - the basic building blocks of human-centric institutions

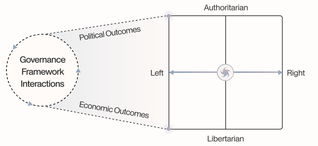
Off-chain

- Mapping real world identities into some Voting Power functions

I. 1T1V
II. 1H1V
III. Hybrids



On-chain



- Rules by which political process design translates human inputs into political and economic outcomes - it's redistributive function - can span from purely socialistic, the one where excellence is taxed, to that of hyper capitalism, where there are increasing returns to one's excellence.
- Assuming a human centric political process design, we can map a function relating one's reputaiton to one's voting power (or any other political/economic output for that matter).
- It's linear domain would correspond to the notion of meritocracy, the superlinear - to that of hyper capitalism where the winner takes it all, while the sublinear domain would be that of socialism where there are decreasing returns to excellence.

DAOs on Ethereum

— The Issues

Hyper-financialized

- Token cost as a workaround for Sybil resistance.
- Hard to build fair voting systems.
- Alternative is centralization and permissioned access.

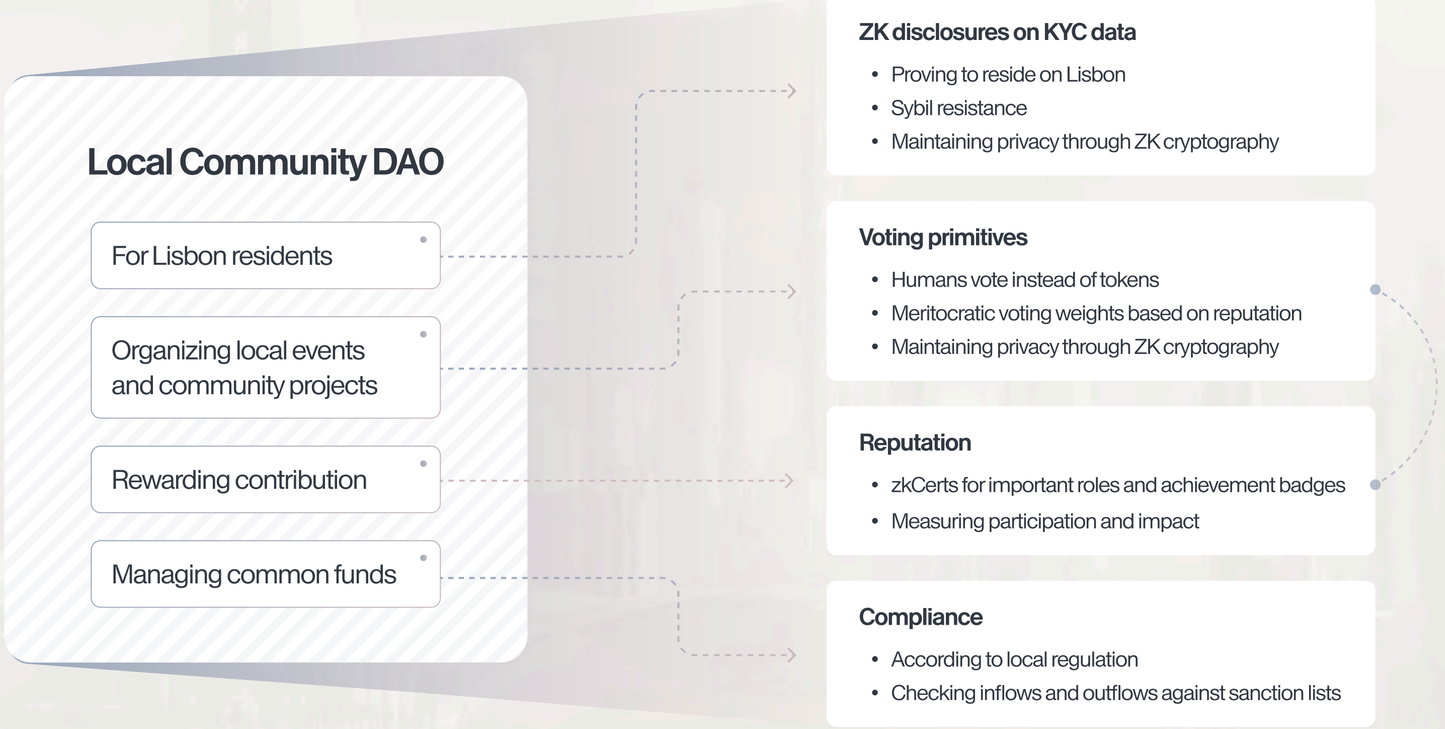
No personal data to build social use cases on-chain

- Missing privacy means people don't use personal data on-chain
- Data missing to prove regulatory compliance.

No established system for Reputation

High transaction costs

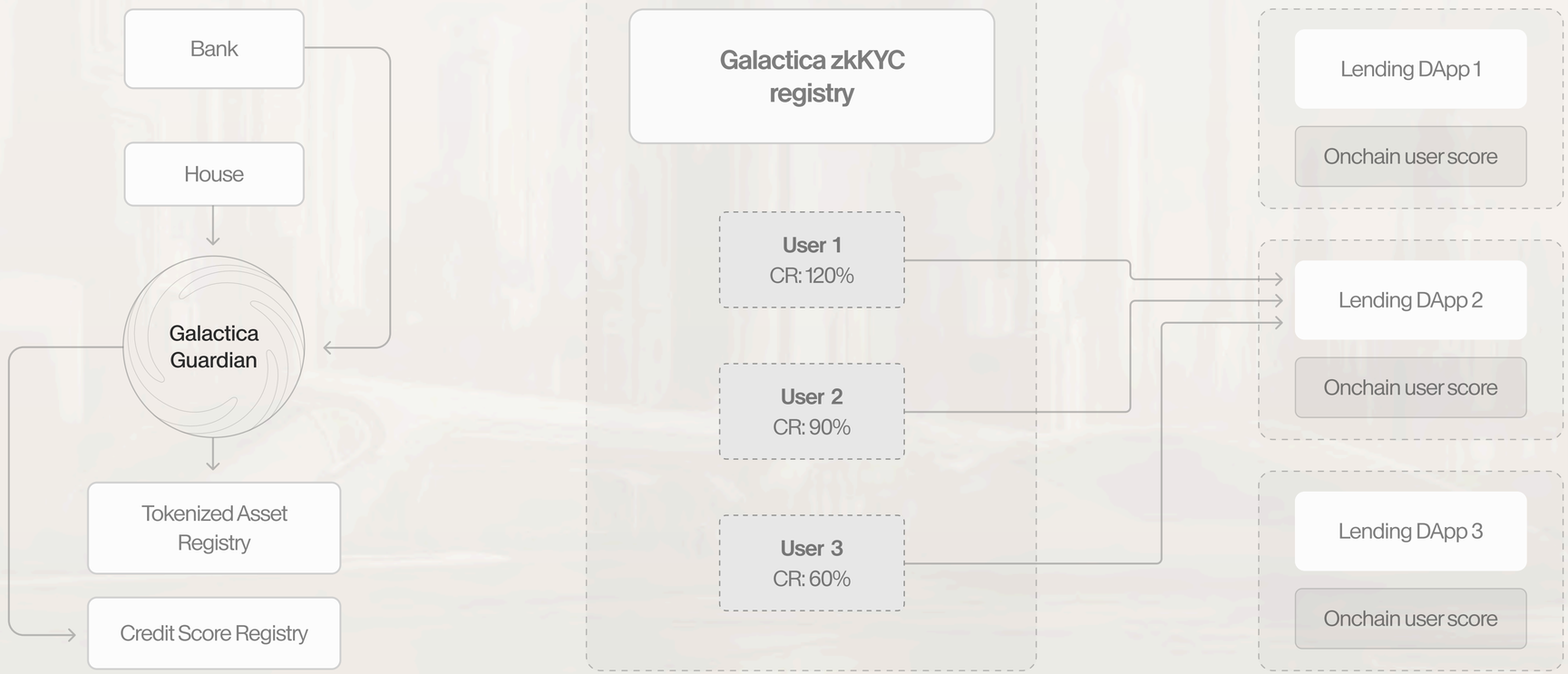
Powered by Galactica Governance Primitives



Undercollateralized Loans

— THE ISSUES

- Most popular lending such as AAVE, Compound, Maker offer overcollaterized loans due to the trustless and anonymous nature of the underlying blockchains.
- Lending protocols on Galactica can take advantage of the zkKYC system to enable lower collateralization ratio or even undercollaterized loans.
- Borrowers would be able to access credit through their reputation, thus providing opportunities and lowering barriers for well-trusted but still anonymous entities.



Compliant Privacy [Use Case]

— The Issues

- Scams, hacks, and other types of criminal activities have proliferated and plagued the industry as it has expanded over the past few years.
- $656M lost from crypto hacks, scams and rug pulls in H1 2023 (according to Web3 security firm Beosin).
- In November 2022, the cryptocurrency exchange FTX spiraled into bankruptcy, creating a wave of crypto crime. Its users were subjected to a scam offering a refund, $415 million of crypto was stolen in a series of cyber attacks, and another $3.1 billion was wiped from the market.
- In the first half of 2023, the Web3 domain witnessed a total of 110 major rug pull events, involving approximately $75.87 million.