GALACTICA
NETWORK

GALACTICA.COM WEBSUMMIT 2023 EXCLUSIVE

TABLE OF CONTENTS

© COPYRIGHT GALACTICA NETWORK 2023

GALACTICA NETWORK

AN L1 WITH THE MOST FLEXIBLE REGTECH STACK AND DESOC PRIMITIVES

[1] RegTech framework for TradFi instruments in DeFi

[2] Regulatory Compliance w/o draconian privacy eroding tools (i.e. CBDCs)

[3] Reputation-contingent primitives (e.g. Souldrops, Meritocracy in DAOs), Cypher State

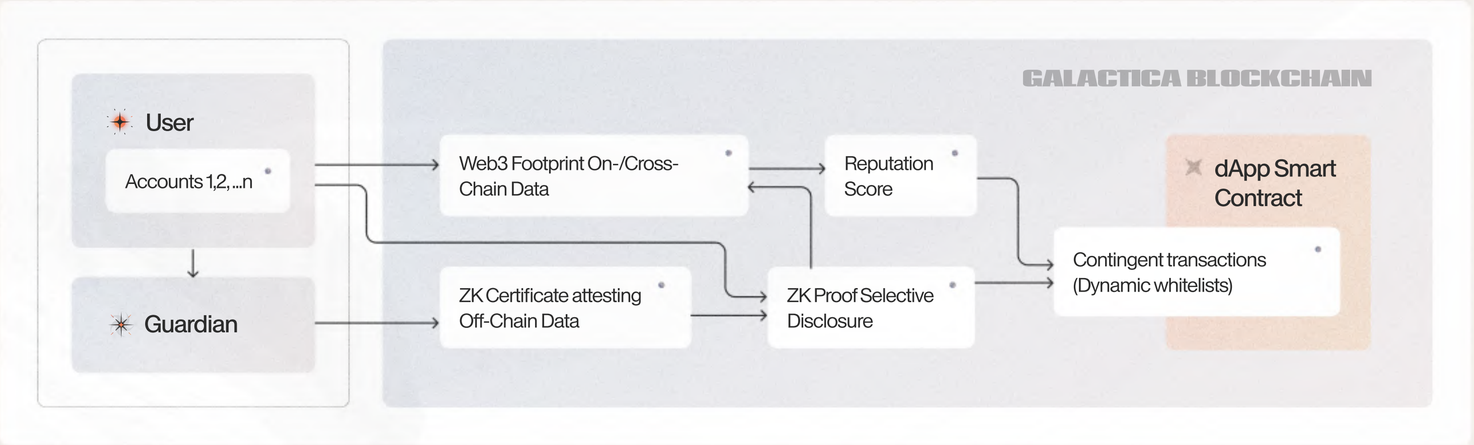
GALACTICA NETWORK

PART I - TECH STACK

TECH OVERVIEW

Galactica Network is an EVM smart contract blockchain built on the CosmosSDK.

It operates as independent layer 1 and leverages zero-knowledge cryptography based on SNARKS and circom.



zkCertificates

- Non-transferable (a.k.a. soulbound) NFTs issued by a Guardian
- Verification hash of personal data
- For selectively proving statements about contained data
- Using ZK cryptography to keep personal data private

Guardians

- Onramp for personal data
- Check user documents
- Issue zkCertificates on-chain
- Example: KYC verification

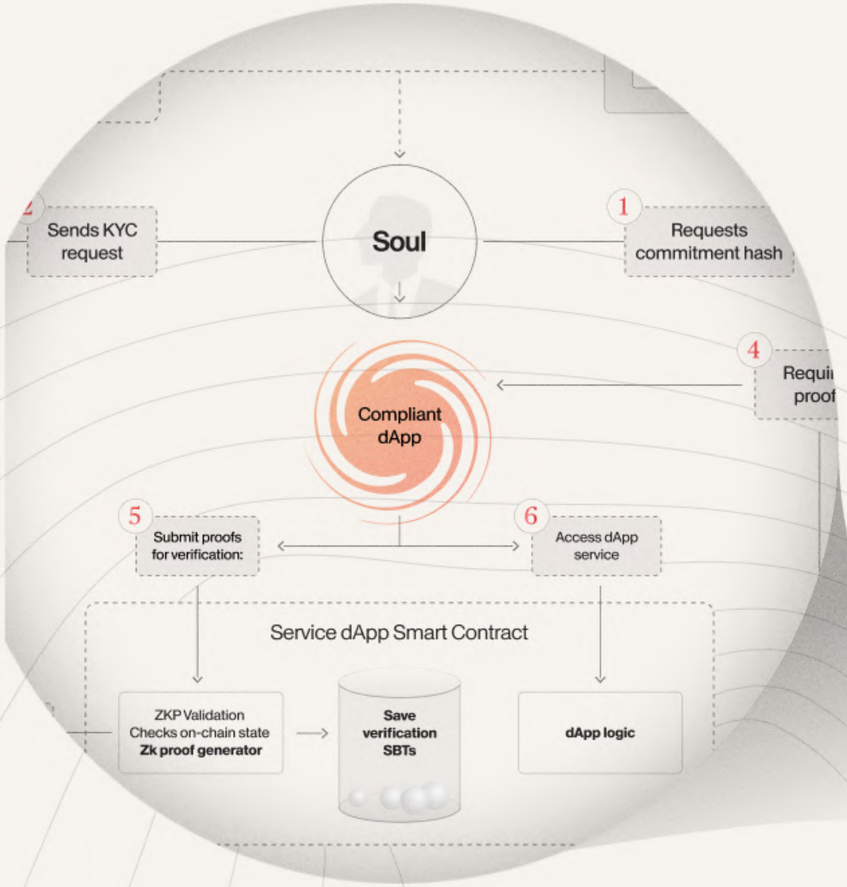
Reputation Root Contract

- Smart contract interface for Reputation calculation system
- Customizable Reputation functions on-chain metrics

Contingent Transactions

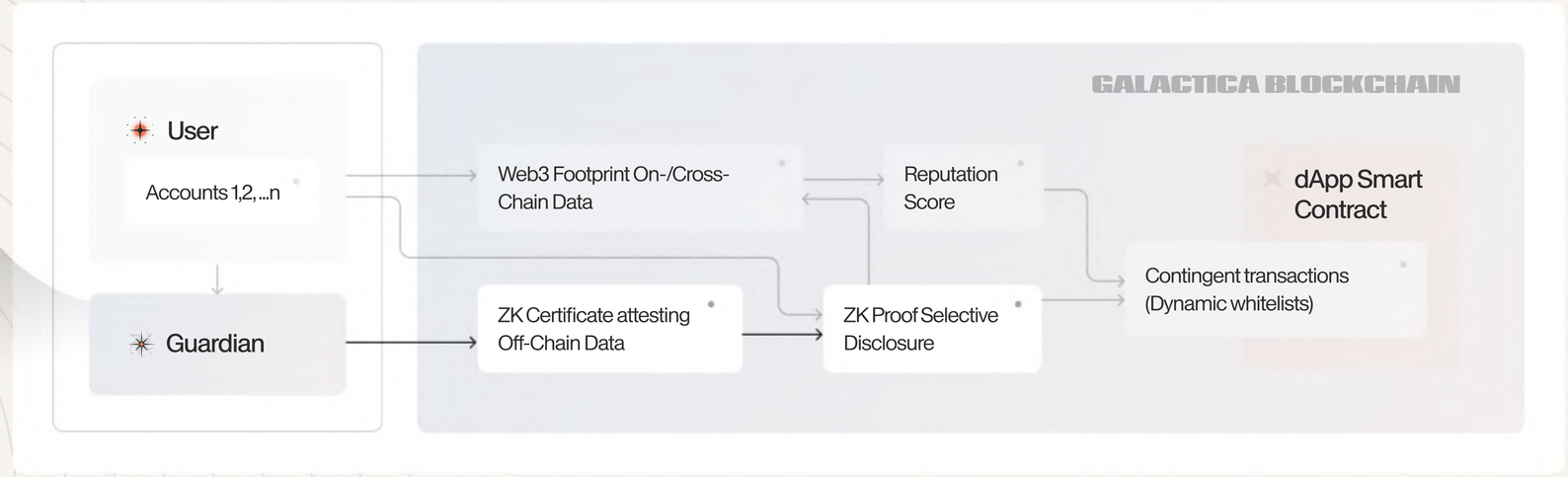
- Dynamic rejection/acceptance rules for smart contract transactions including fund transfers

GUARDIANS

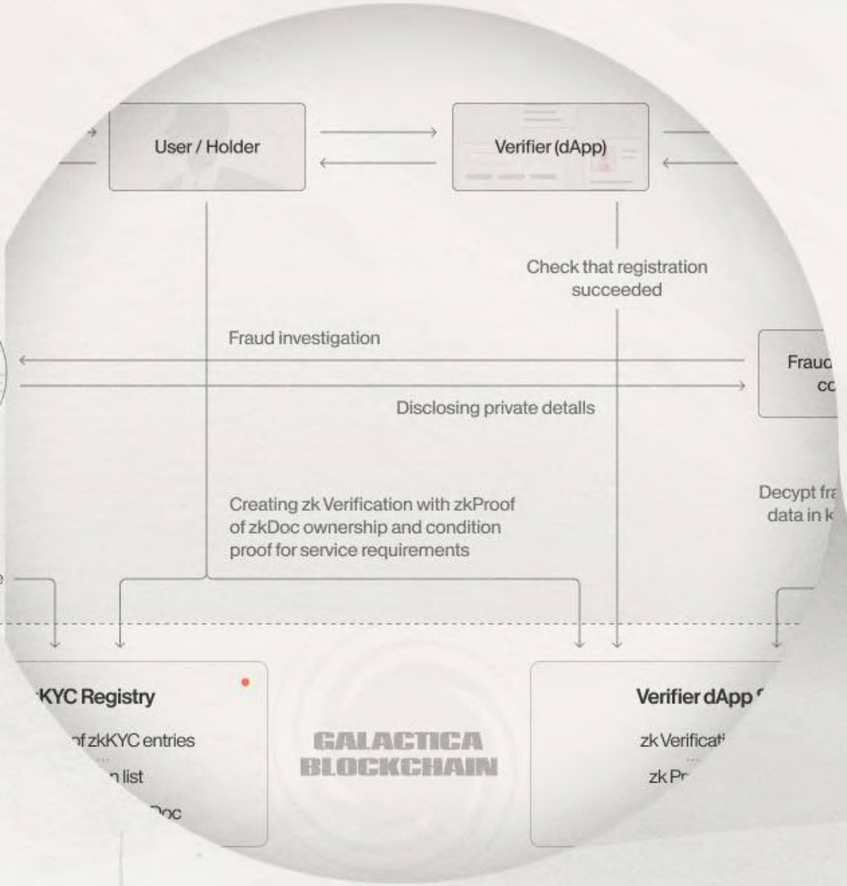


View full version

- Guardians - a whitelist of notaries that serve the purpose of onramping Real World documents on-chain in a privacy preserving manner.
- Documents are submitted and checked off-chain. Guardians then issue an on-chain verification hash.
- 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.

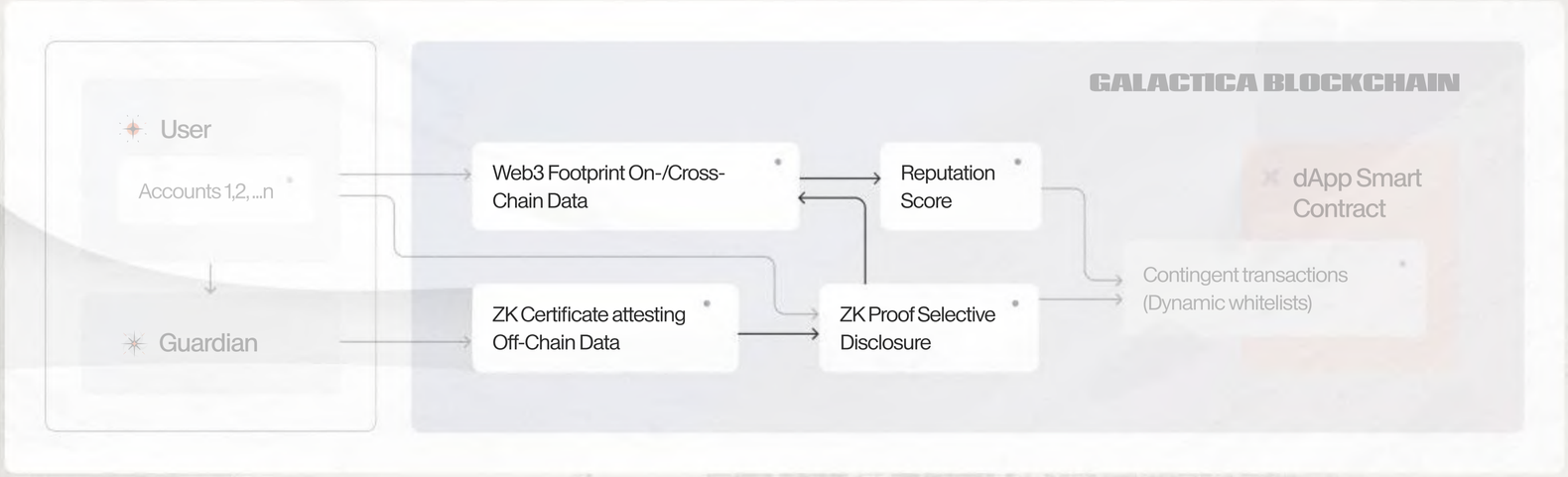


zkCERTIFICATES



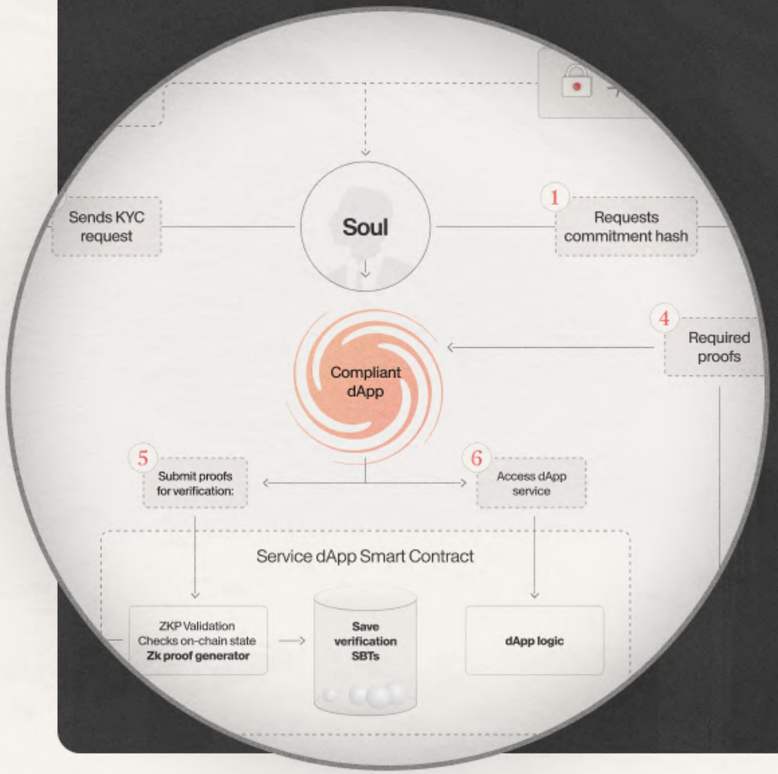
View full version

- 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 assets.
- 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.



GALACTICA NETWORK

zkCERTIFICATES & GUARDIANS FOR zkKYC

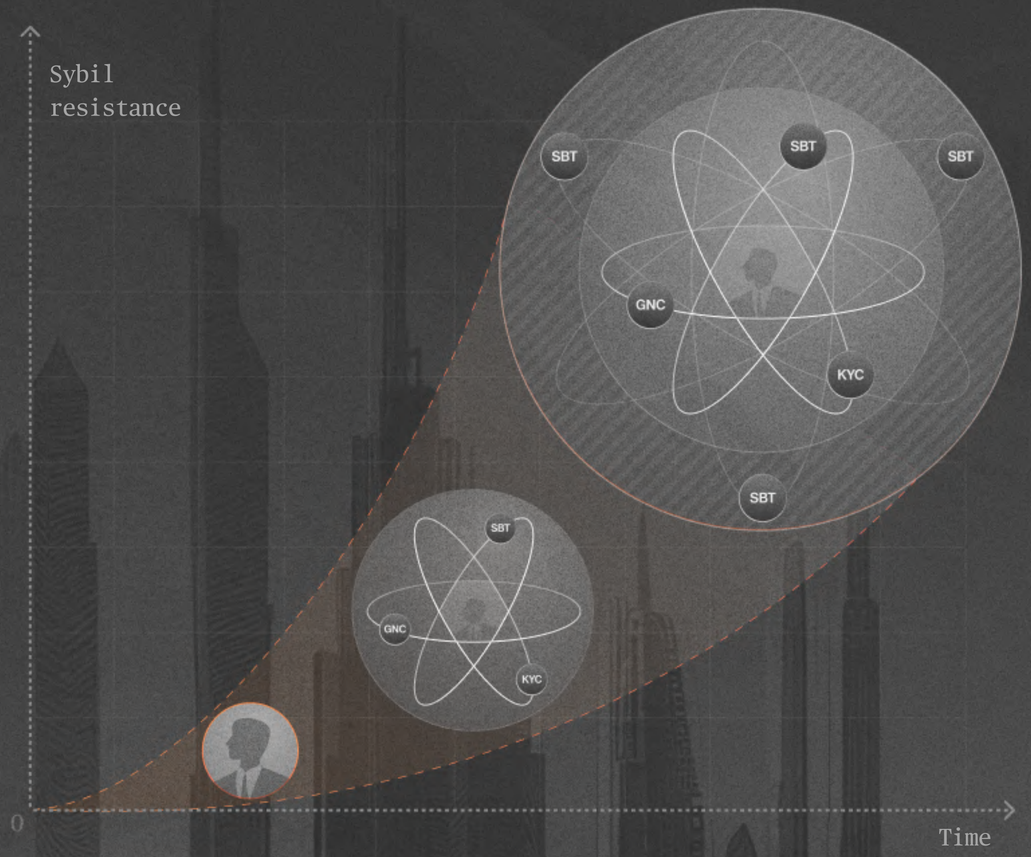


View full version

- **zkCertificates** are a general purpose primitive for migrating on-chain any real world document that can be verified by a notary running a Guardian.
- 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.

GALACTICA NETWORK

SYBIL RESISTANCE

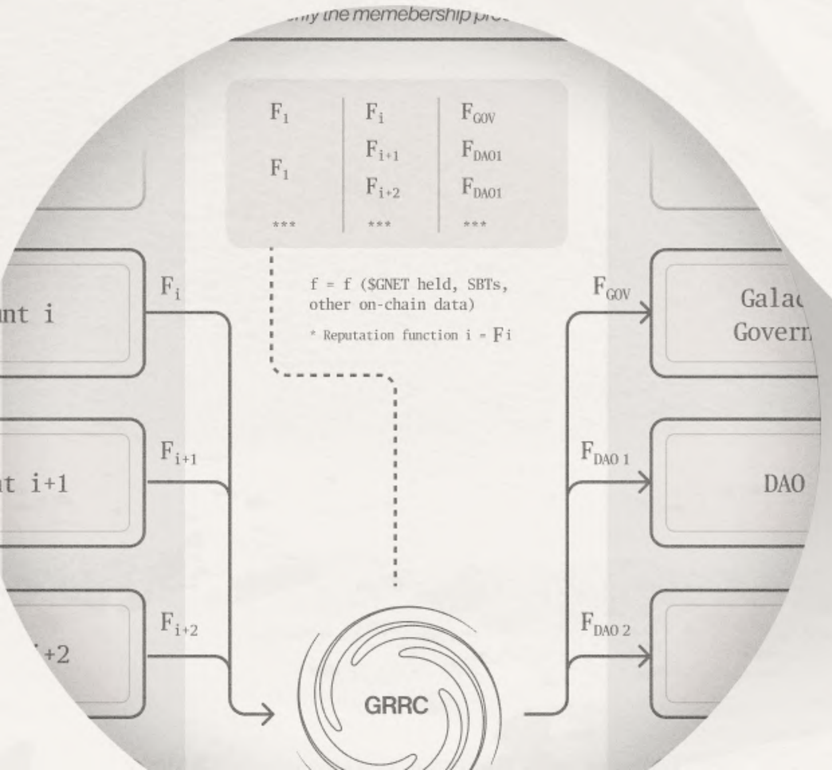


- **Protocol's Sybil resistance is a multitude of mechanisms enabling direct mapping between real world persons and internet identities.** A human in the blockchain space could be referred to as a Persistent Identity. The multitude of interactions between any such identity and the rest of the protocol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

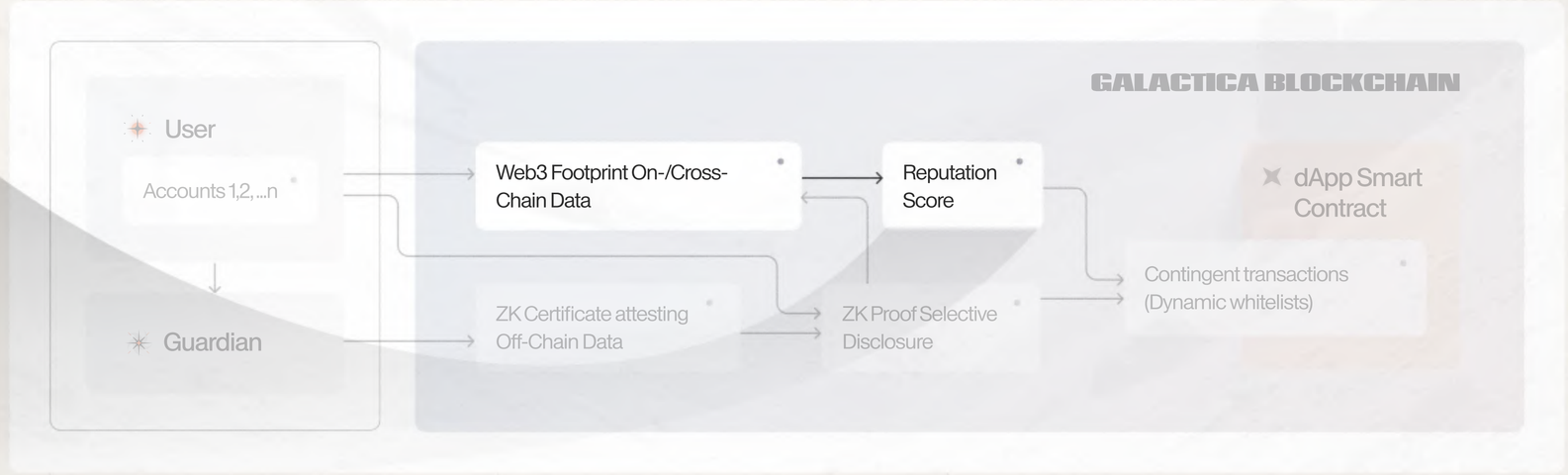
- The notion of zkKYC is arguably one of the most potent ways to bootstrap Sybil resistance on a chain while enabling compliance with many regulations that today prevent the flows of institutional capital from flooding an inherently more technologically advanced web3 space.

REPUTATION ROOT CONTRACT (RRC)

View full version



- RRC is a protocol-level primitive that enables using on-chain data points (including data imported through Guardians as well as on-chain transaction history) to generate scores for user defined Reputation functions.
- It can use both, on, and off-chain sources as inputs. It uses on-chain data as input including transaction history and real-world data onboarded through Guardians. Together, this system allows fusing on-/cross- and off-chain data points to create a Reputation according to a user defined function.
- In summary, RRC allows for evaluating web3 footprint of an account and augmenting it with data sources originating off-chain. An important property of RRC is that dApps can force generating ZKPs about the full set of accounts users control - not a subset (using zkKYC as an id).



CONTINGENT TRANSACTIONS

- The output of RRC is then used by dApps to fine tune the experience for the user. (Lower collateral rates for compliant individuals, for example). The technological primitive that is used for this are so called Contingent Transactions.
- Contingent Transactions enable apps building on Galactica to create dynamic whitelisting rules where the outcome of a transaction depends on the real time Reputation Score of the user.

- **Contingent Transactions enable:**
  - Meritocratic Interactions (where the app fine-tunes the experience it offers depending on the Reputation Score of the user).
  - Compliant Interactions (where the app fine-tunes the compliance profile of users/liquidity that are allowed into the app) and in general enable dApps to benefit from the heterogeneous nature of accounts on Galactica Network.

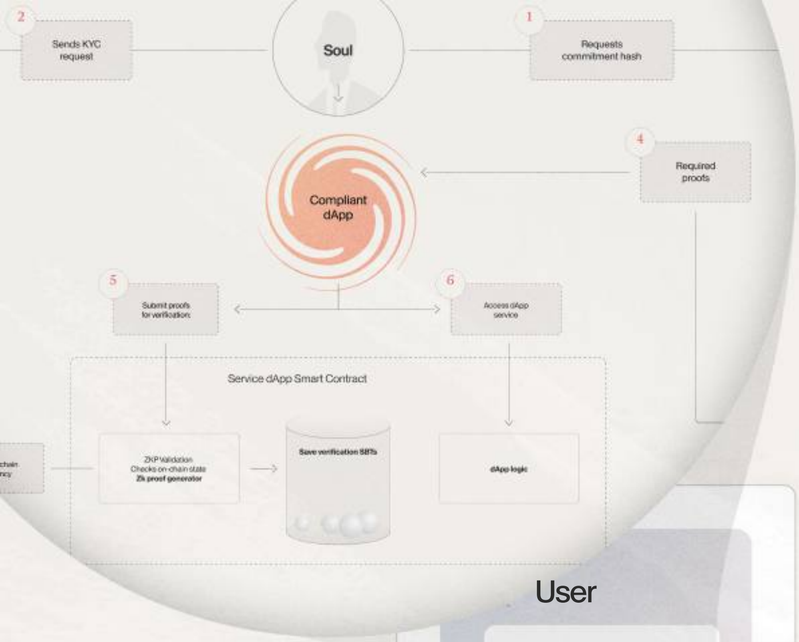
View full version

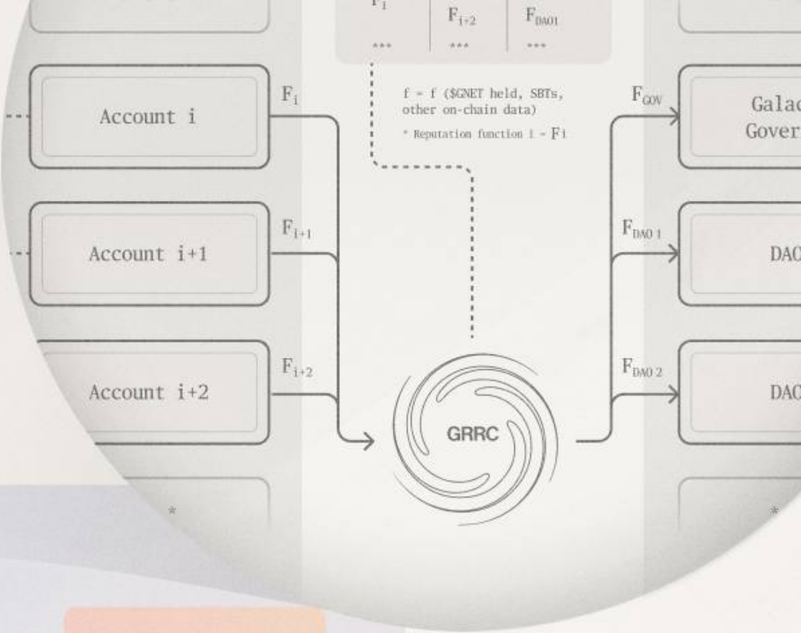
HETEROGENEOUS ACCOUNT TRANSACTIONS

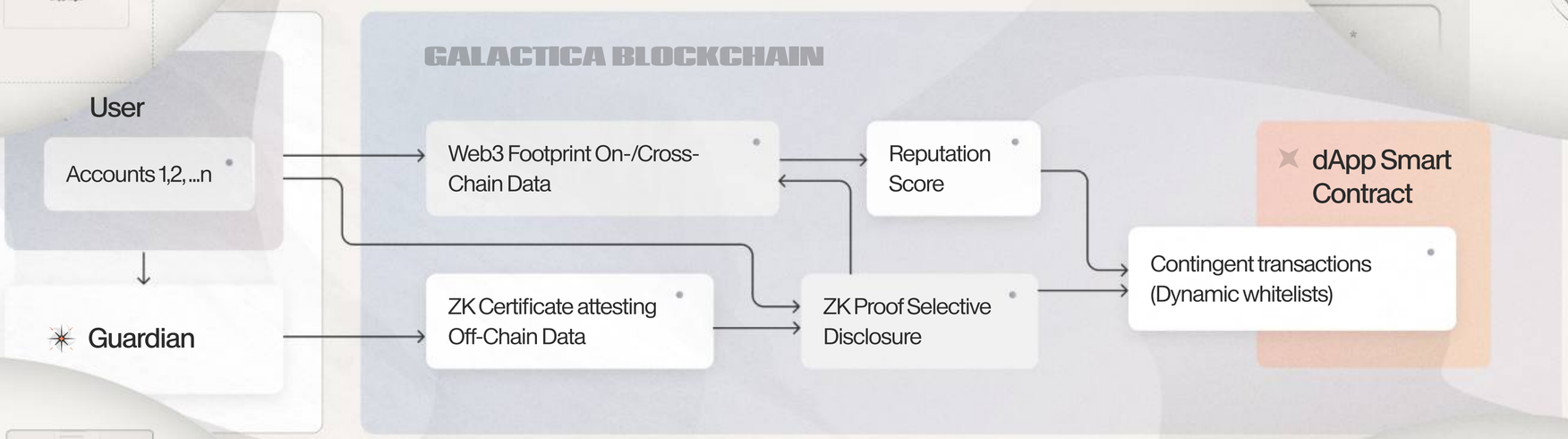
Together RRC and Contingent txs effectively create whitelists with dynamic criteria:

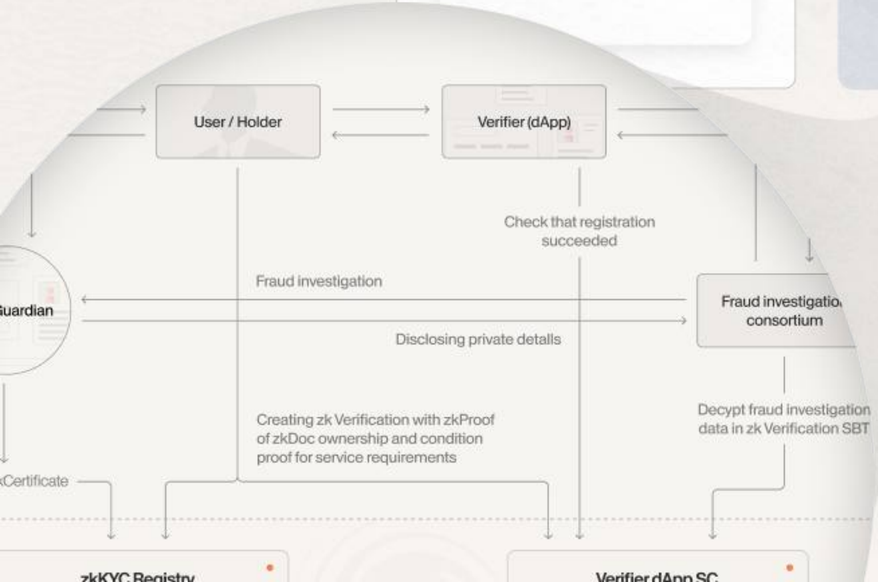
1. The output of RRC can be used to determine whether an account is allowed to submit a transaction to another account (e.g. only users approved through Guardians can interact with a DEX or else the transaction will fail) and enable heterogeneous account (i.e. DeSoc augmented) dApps;
2. The inner logic 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.

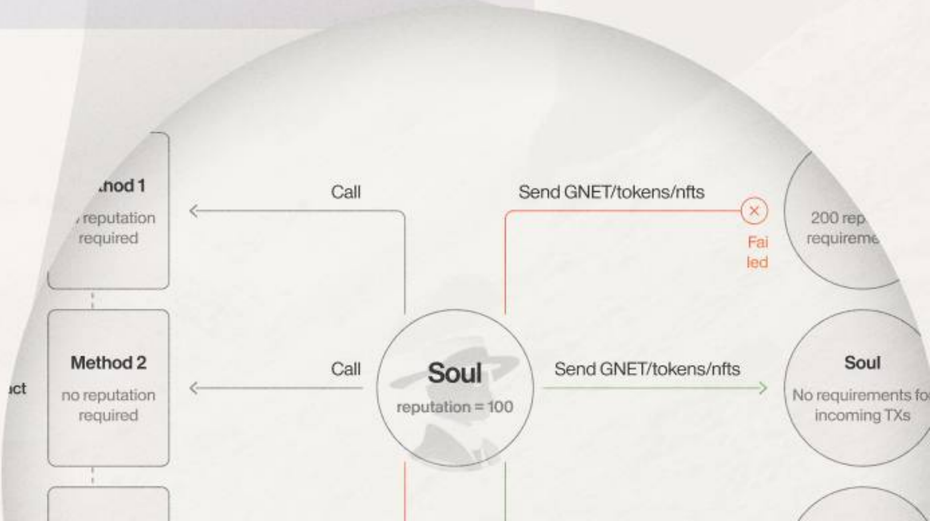
PUTTING IT ALL TOGETHER











GALACTICA NETWORK

PART II – USE CASES

CATEGORIES OF USE CASE LEVERAGING HETEROGENEOUS ACCOUNTS

Compliant Privacy

I

In brief

Privacy preserving on-chain compliance. Libertarian interpretation of fusing TradFi regulatory complex and web3 stack and ethos.

Use cases

1. Platform for DeFi around security tokens:
   - Real world physical assets, such as real estate, cars, etc.
   - Financial assets, such as bonds, stocks, derivative contracts, etc.
   - Various hybrids, such as compliant IDOs and liquid PE.
2. Fusing web3 settlement efficiency and composability and TradFi asset diversity;
3. Automated compliance proofs for a streamlined banking system;
4. Corporate forward financing;
5. Weak form Sybil resistance.

DeSoc and it's various derivatives

II

In brief

Social substrate infused into protocol governance, DAOs and DeFi. Better and more diverse on-chain institutions.

Use cases

1. Social account recovery and other social AA primitives;
2. On-chain creator economy;
3. Sybil resistant governance primitives (QV/QF);
4. Souldrops and incentive allignment;
5. Post DAOs (DePol) [DeSoc + DAOs];
6. Reputation augmented DeFi [DeSoc + DeFi];
7. Cypher States and Protocol Citizenship

Global immutable identity and persistent reputation

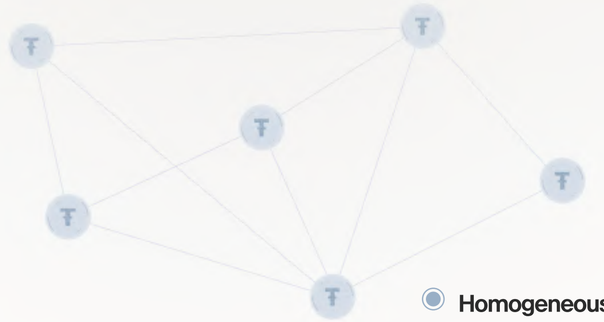
III

In brief

Carrying your full digital self as you traverse the cyber space.
Enabling account heterogeneity.

Use cases

1. Undercollateralized lending and increased capital efficiency;
2. Real time dynamic collateral systems;
3. Meritocratic primitives;
4. Hyper alignment of incentives;
5. Pluralistic network goods;
6. Off-chain persistent reputation;
7. Efficient social matching mechanisms.



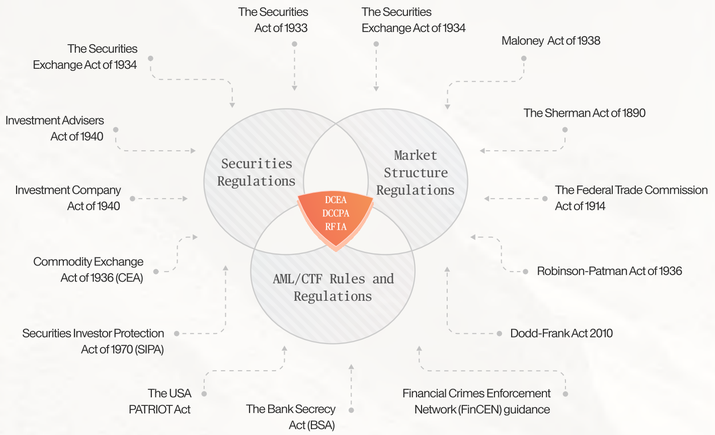
Homogeneous account web3

zkCertificates

Heterogeneous account web3

COMPLIANT PRIVACY

1 **Web3 operates (evolves)** alongside a trinity of regulatory regimes including:



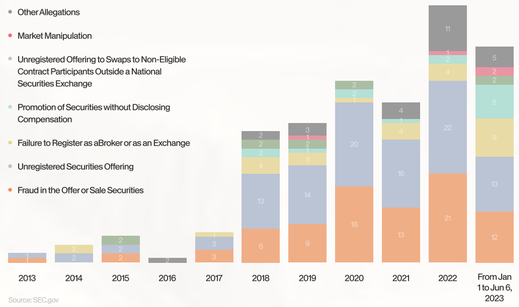
[1] The Digital Commodities Consumer Protection Act of 2022

[2] The Digital Commodity Exchange Act of 2022

[3] The Lummis-Gillibrand Responsible Financial Innovation Act (RFIA).

3 For this reason, the majority of the user issued instruments existing in the permissionless **web3** is limited to the so-called **utility tokens**, **those that require no regulation** other than (in some cases) privacy eroding invasive **AML.**

3.a **This is also why DAO and DeFi** do not mix with the attention of regulators



Source: SEC.gov

3.b This is also why the **ZK revolution** has gone unnoticed

Do we really need Web2/CeFi?

The revolution of zk-enabled primitives has gone largely unnoticed.

ZK-Rollup

is a sufficient UX substitute for CeFi competitors,

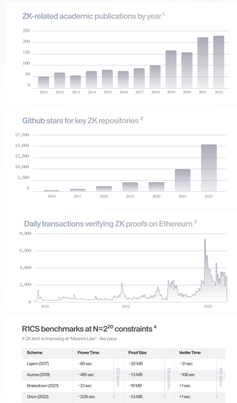
zkKYC

is a superior substitute for CeFi compliance,

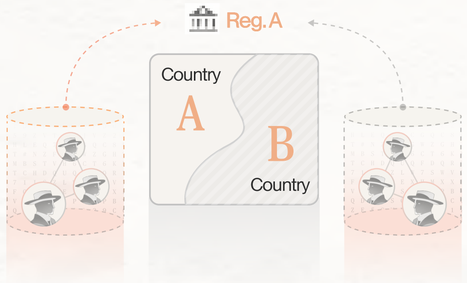
ZKPs

are the ultimate stack for interactive data privacy

We can solve for **privacy, compliance and UX** in the Web3 space.



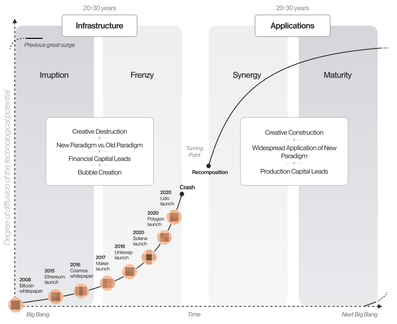
2 Most of the regulations in one way or another are **limited to particular subset of subjects: EU, US, etc.**



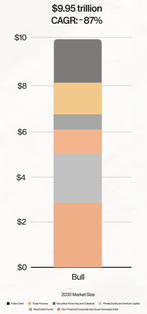
4 When solved for, using **zkKYC** or other such primitives, the ability to identify actual users subjects to regulation will **enable new assets and new markets to flourish on-chain**, taking us as an industry out or a perpetual state of innovation for its own sake and into the domain of genuine use cases and applied value.

	Primary Markets	Secondary Markets
Physical Assets	Vehicles sales, houses sales	Vehicles resales, houses sales
Financial Assets	IPOs, Private Equity, VC	ETFs, Stocks, Bonds, Commodities Exchanges

5 No other arrangement can satisfy both, the privacy requirement of public blockchains and compliance needs of regulators. Thus, there is **no other way to fuse web3 and TradFi.**

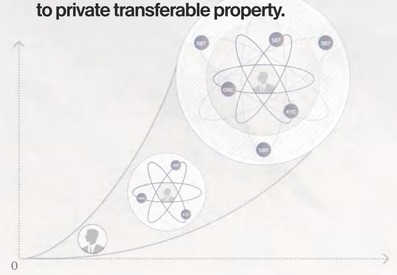


Venue	Network	Type	KYC/AML	Monthly Unique Web Visitors (Jul-Sep 23 Average)	AuM/ Active Loans
Centrifuge	Ethereum	Private Credit	Yes	33,823	$ 244M
Ondo Finance	Ethereum, Polygon	Treasuries	Yes	30,070	$ 188M
Maple	Ethereum, Solana	Private Credit	Yes	11,146	$ 129M
Matrixdock	Ethereum	Treasuries	Yes	<5,000	$ 81M
Backed Finance	Ethereum	Treasuries	Yes	<5,000	$ 47M
WisdomTree Prime	Stellar	Treasuries	Yes	<5,000	$ 11M
OpenEden	Ethereum	Treasuries	Yes	6,182	$ 11M
Securitize	Ethereum, Polygon, Avalanche	Private Credit, Private Equity	Yes	37,398	$ 3.5M*

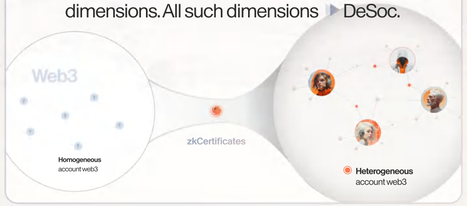


DESOC AND ITS VARIOUS DERIVATIVES

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 governance 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

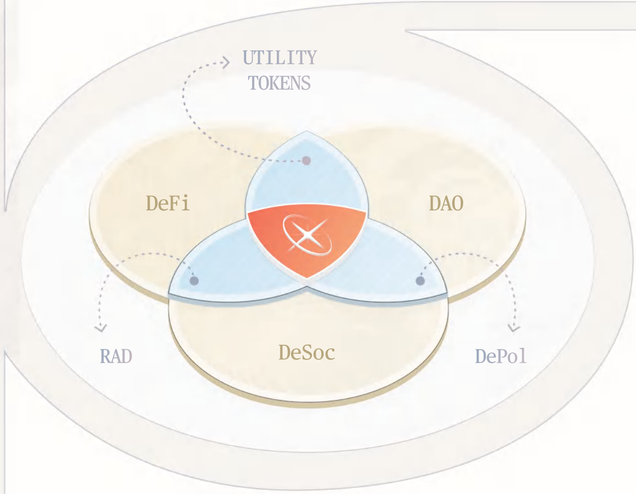
Galactica Network's societal primitives enable complex business models such as undercollateralized DeFi, and offers an unprecedented level of compliance even when compared to TradFi institutions and financial systems

Decentralised Society

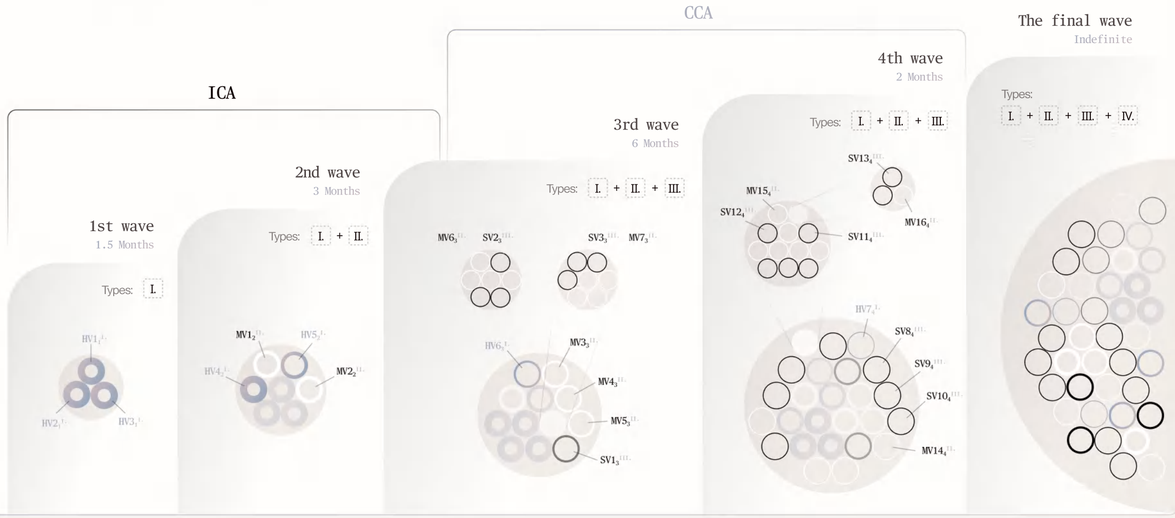
The notions of Persistent Identity and Web3 footprint together enable non-trivial societal institutions to be modeled entirely on-chain

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.

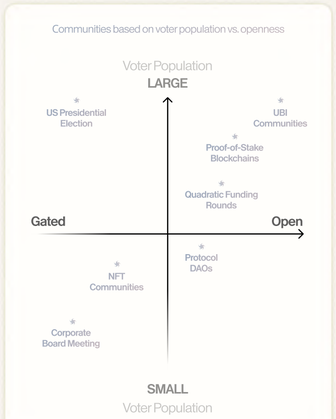


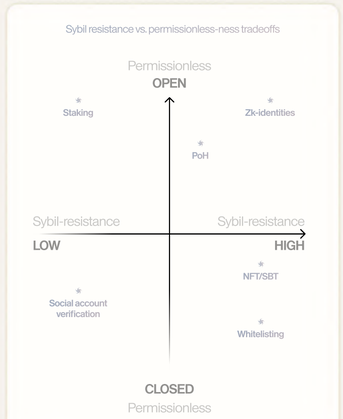
GLOBAL IMMUTABLE IDENTITY AND PERSISTENT REPUTATION

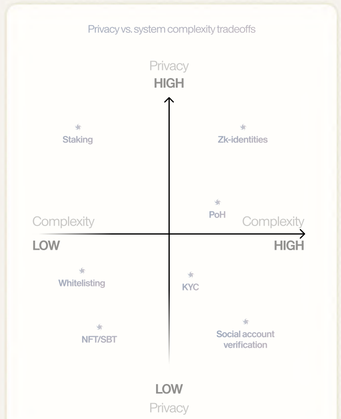
1 **Reliable Identities generate data points** as by-products of their existence, both online and offline. The totality of these data points **forms one's Reputation space**. This space is meaningless if the identities are not reliable; If they are not Persistent.

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;

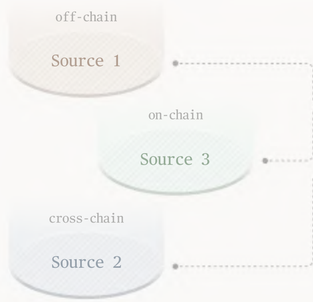
III Meritocratic primitives;

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:

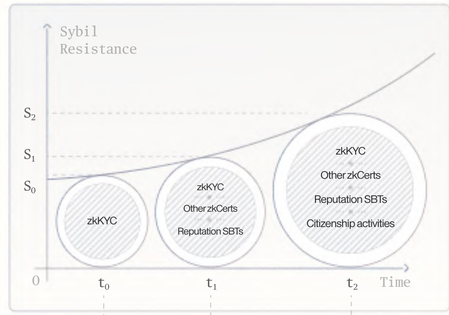
- **Off-chain** (such as one's Twitter account and related data);
- **On-chain** (deduced from one's tx history on Galactica Network);
- **Cross-chain** (deduced from one's tx history on other blockchains).

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:

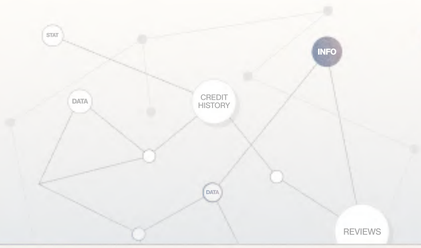
- **Off-chain** (such as surfing the talent networks)
- **On-chain** (an undercollateralized DeFi loan from an app building on Galactica Network)
- **Cross-chain** (same type of loan in another blockchain ecosystem)



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

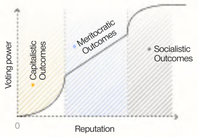
Mapping real world identities into some Voting Power functions

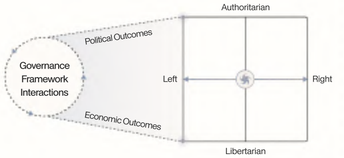
I. 1T1V

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.

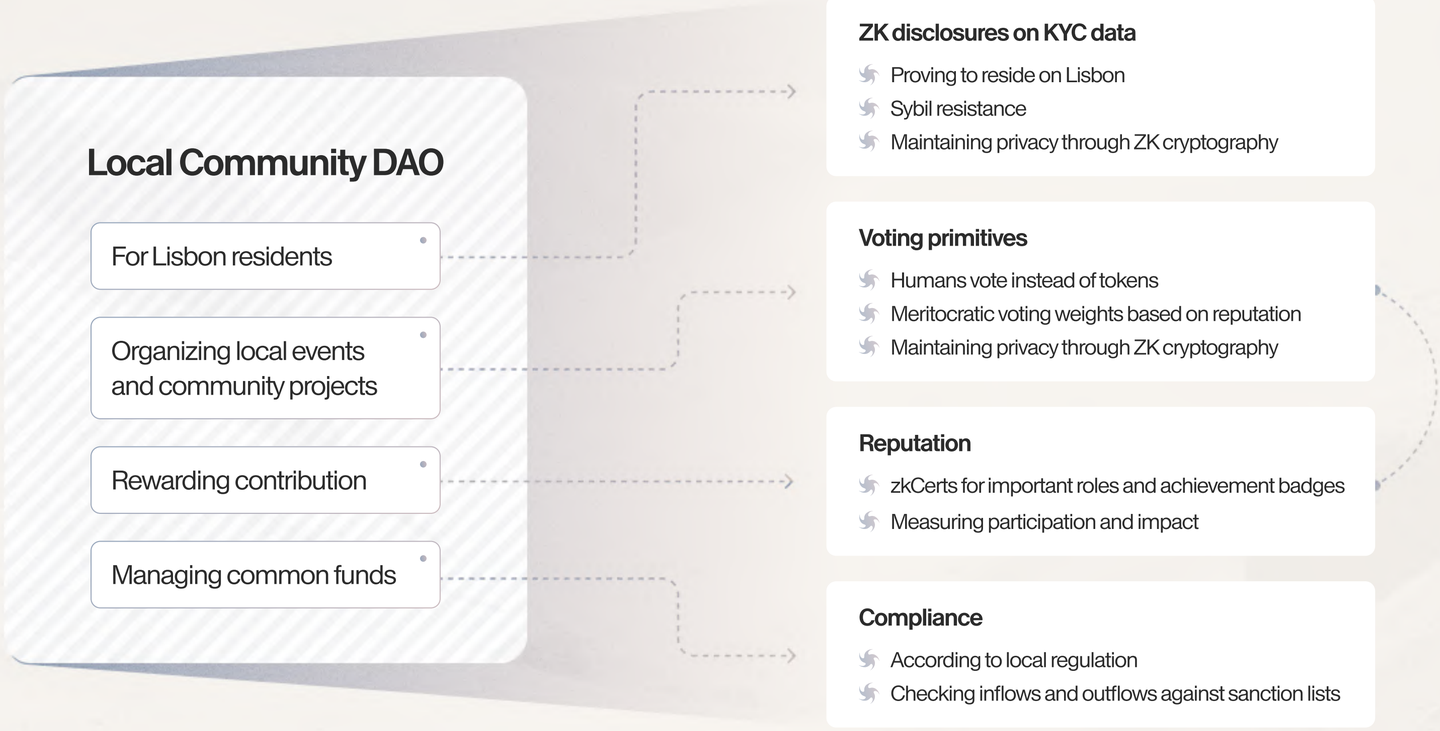
No personal data to build social use cases on-chain

- 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

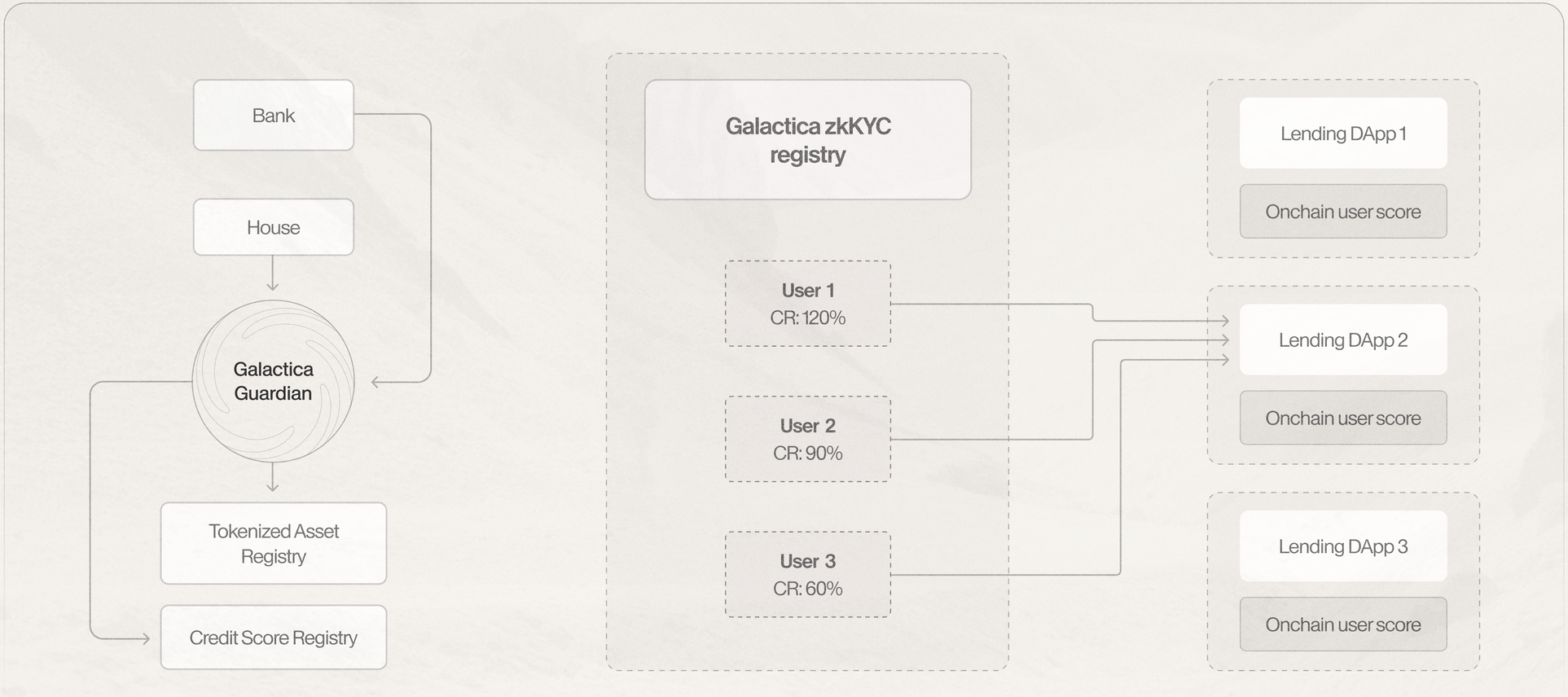
Powered by Galactica Governance Primitives



UNDERCOLLATERALIZED LOANS

The Issues

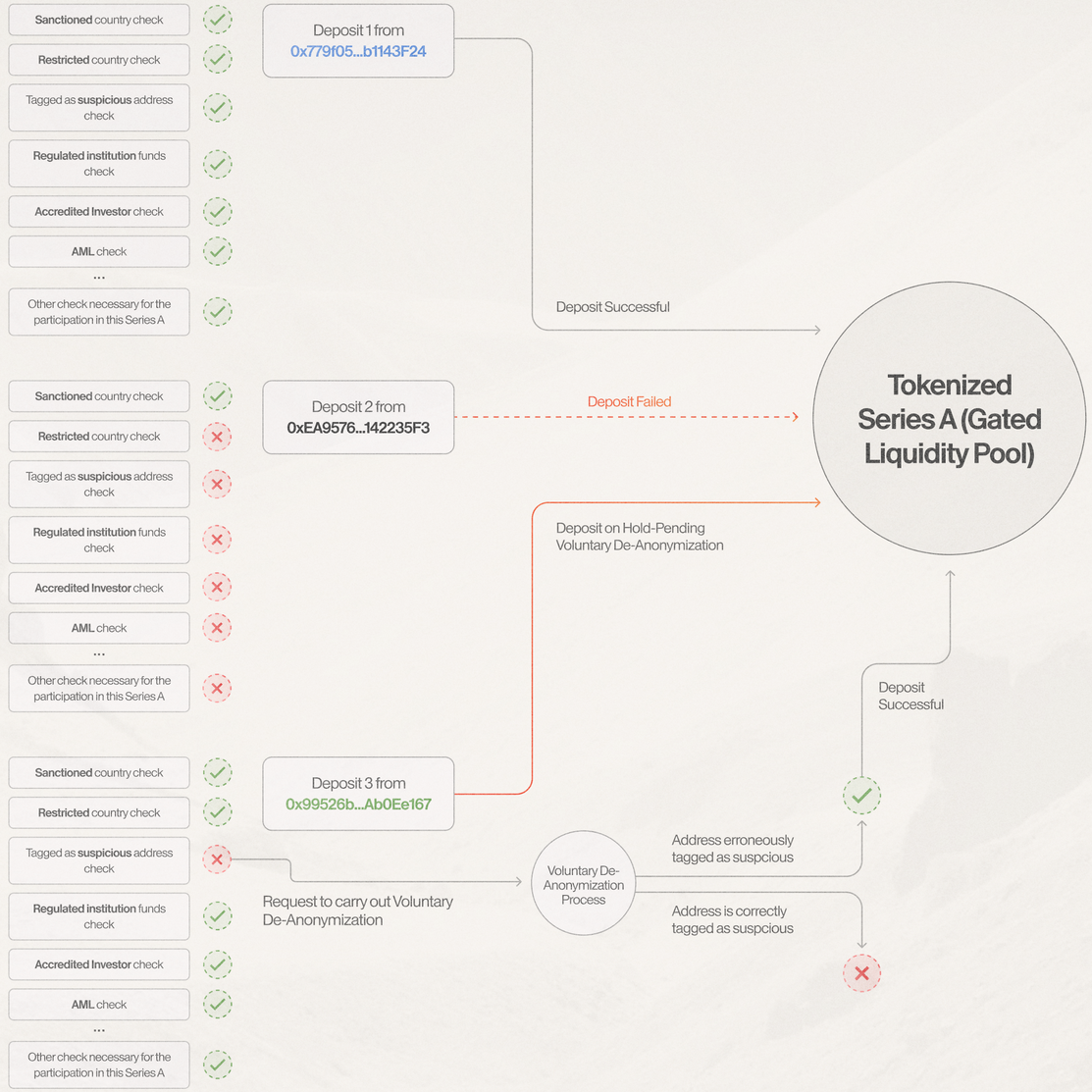
- Most popular lending protocols such as AAVE, Compound, Maker offer overcollaterized loans due to the trustless and anonymous nature of the underlying blockchains.
- Lending protocols on Galactica can take advantage of the zkKYC system to enable lower collateralization ratio or even undercollaterized 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

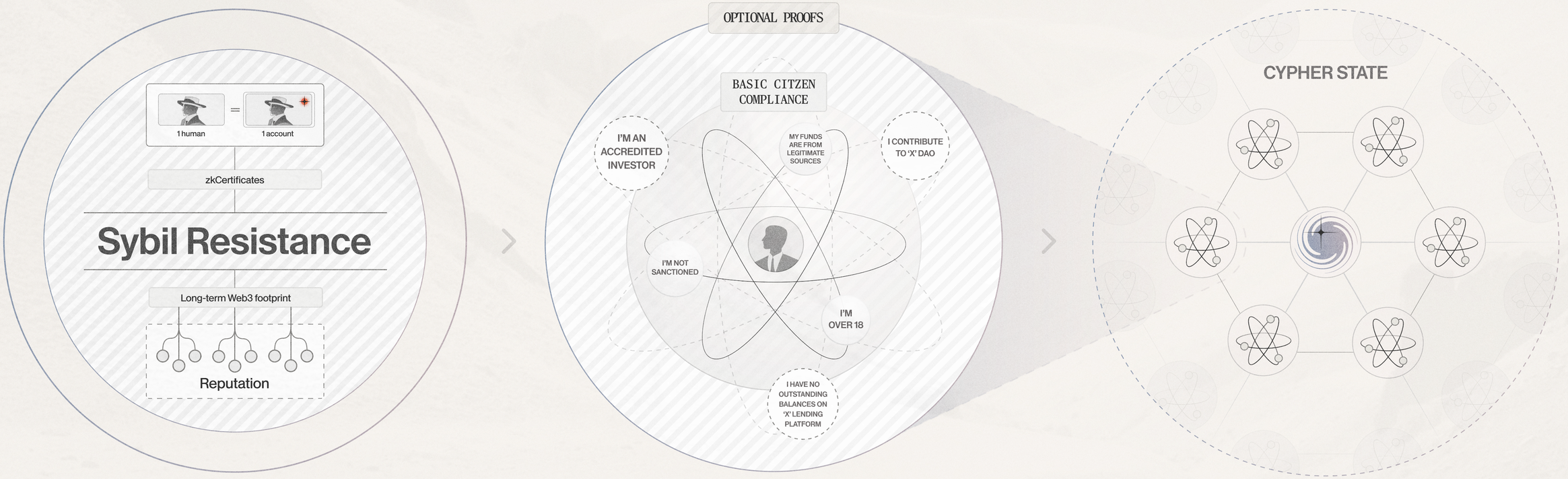
- Scams, hacks, and other types of criminal activities have proliferated and plagued the industry as it has expanded over the past few years.
- $656M lost from crypto hacks, scams and rug pulls in H1 2023 (according to Web3 security firm Beosin).
- In November 2022, the cryptocurrency exchange FTX spiraled 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.



CYPHER STATES & PROTOCOL CITIZENSHIP

The Issues

- Insufficient Sybil resistance for on-chain social interactions (no identity or reputation).
- Limited 1-token, 1-vote governance paradigm.
- No robust compliance in pseudonymous networks.
- Lack of consequences to action incentivizing fraud.
- Low level of participation in governance.



ZKKYC + REPUTATION = PRIVATE PERSISTENT IDENTITY

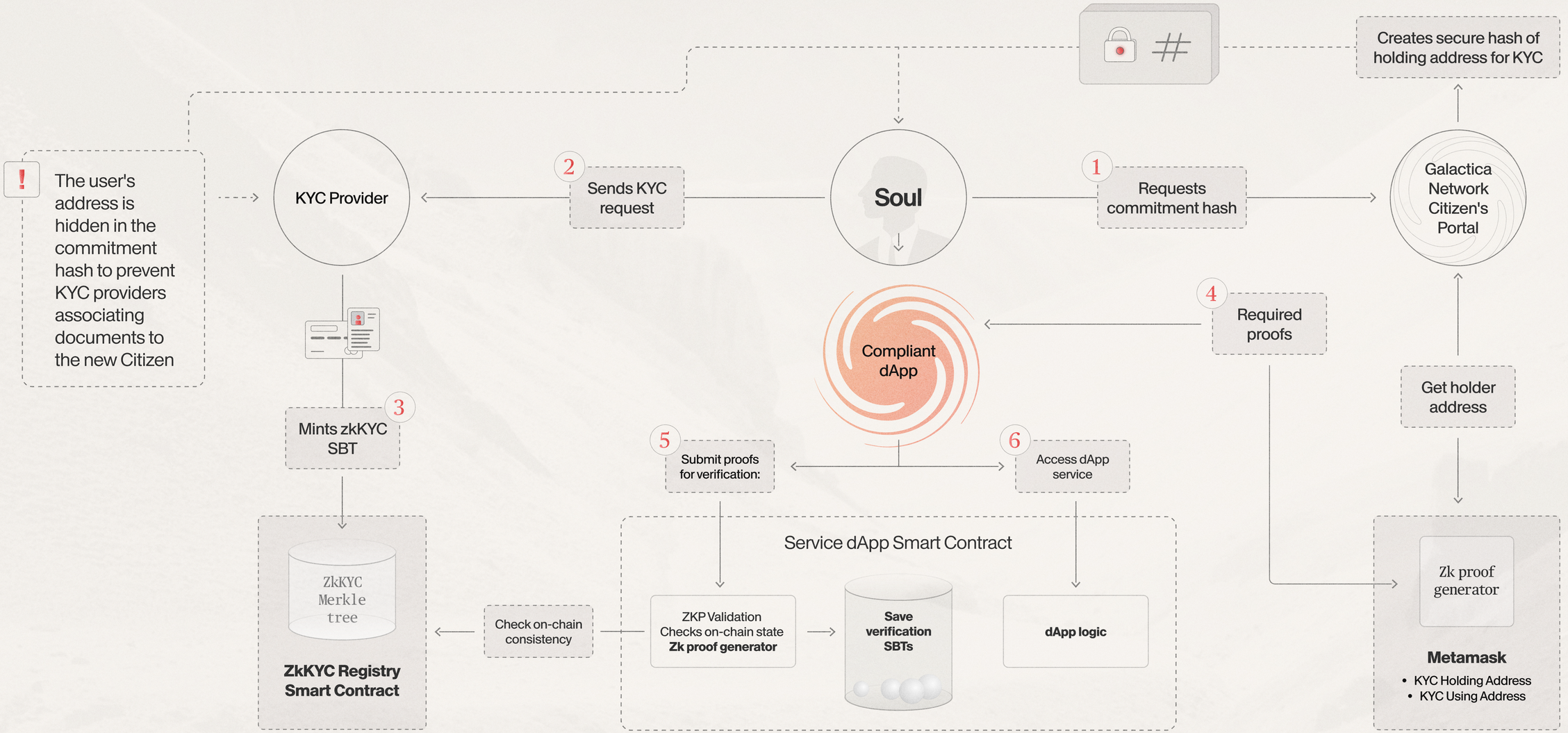
CYPHER STATE OF GALACTICA

THANK YOU FOR YOUR ATTENTION!

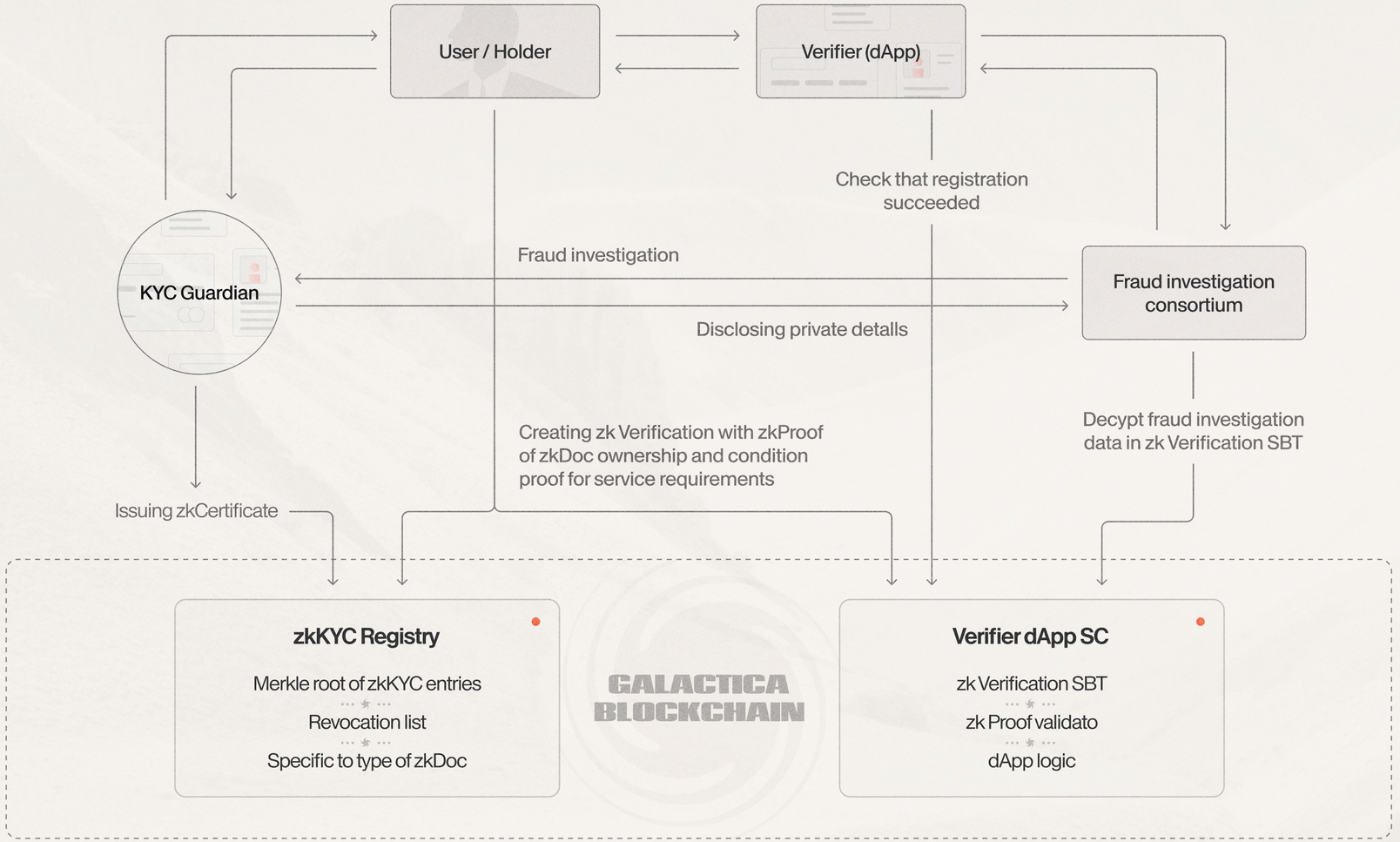
Subscribe to our socials to stay tuned and do check out the research section on Galactica.com website

APPENDIX

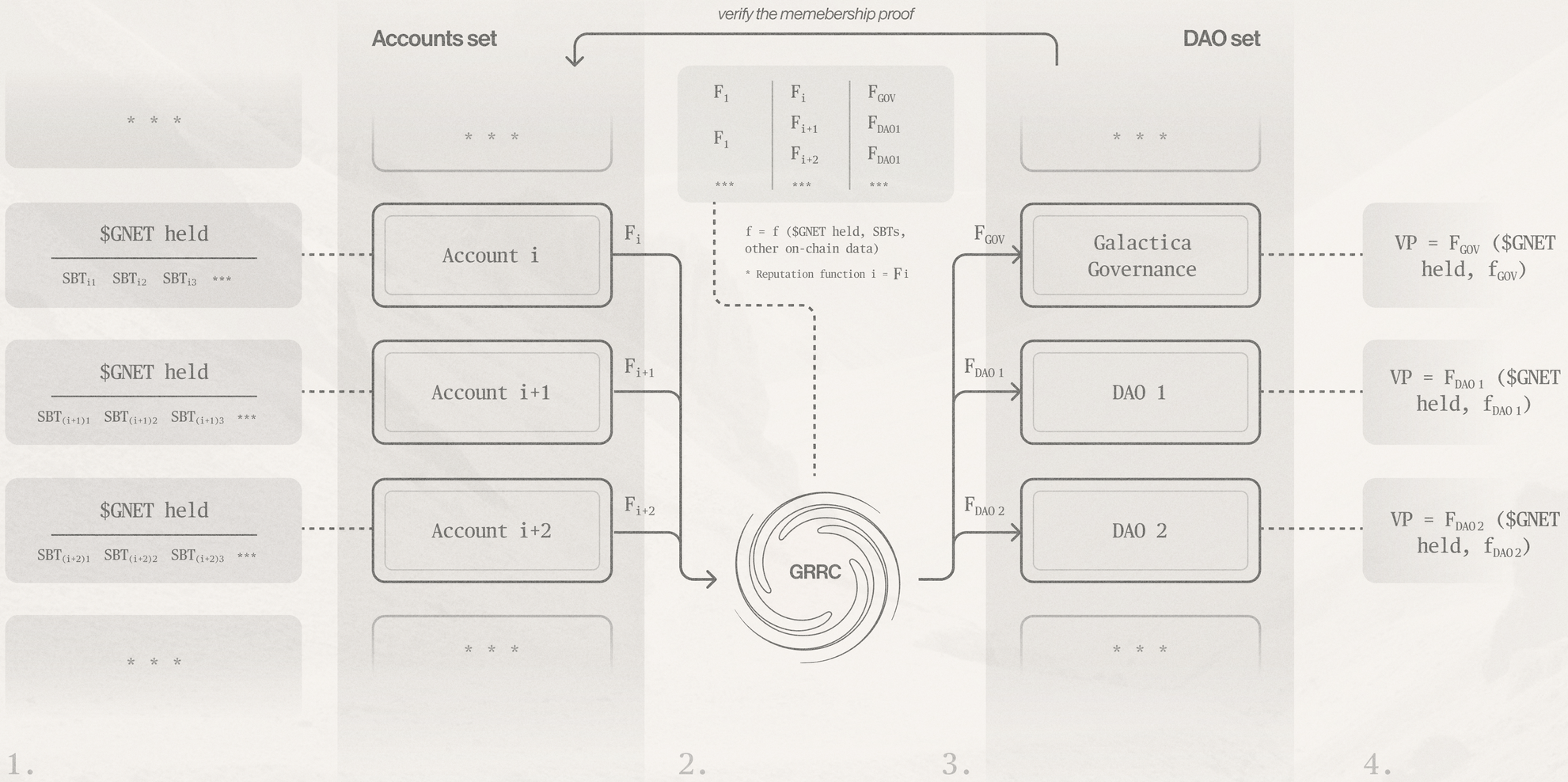
zkCERTIFICATES & GUARDIANS FOR zkKYC



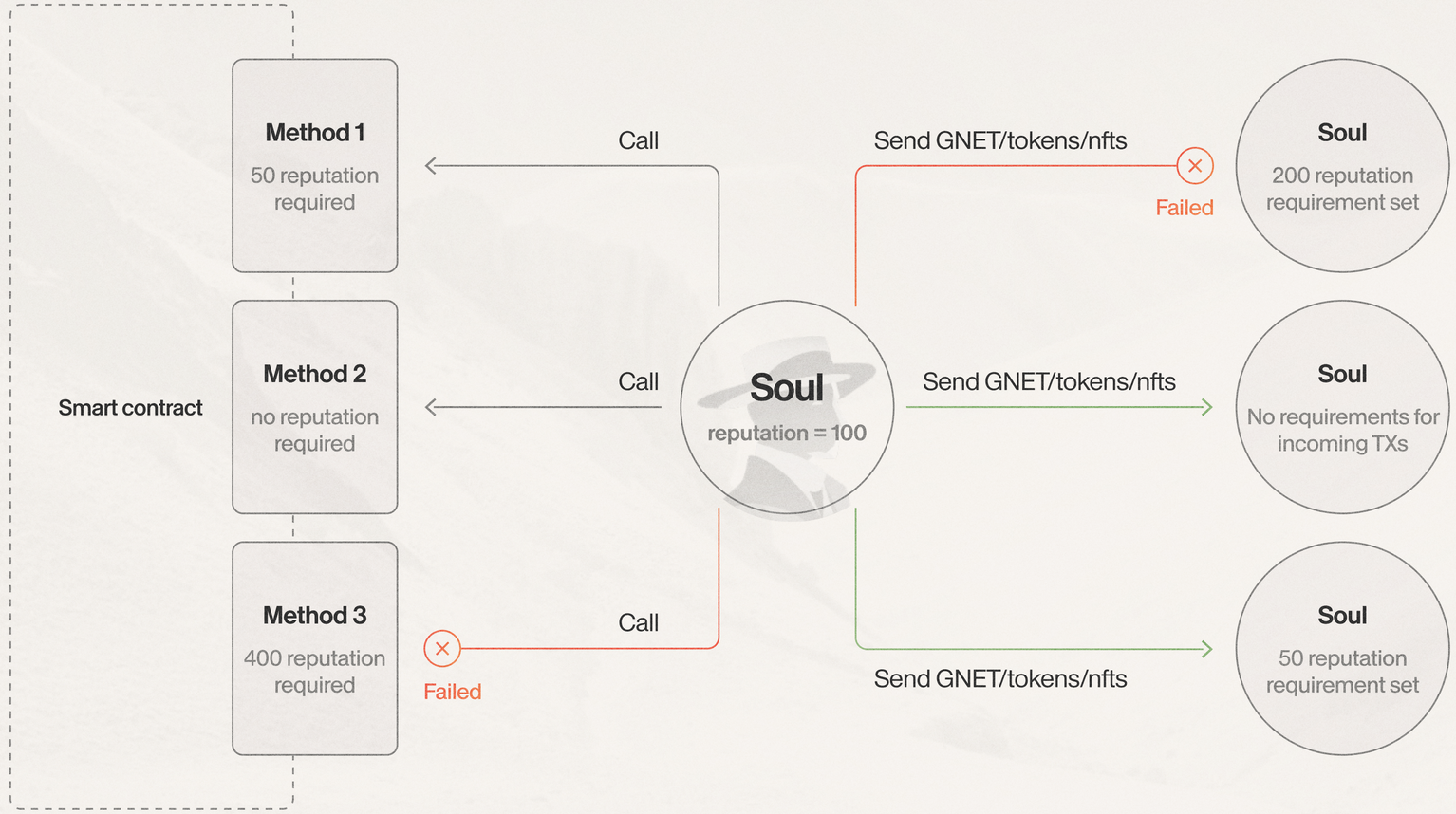
zkCERTIFICATES



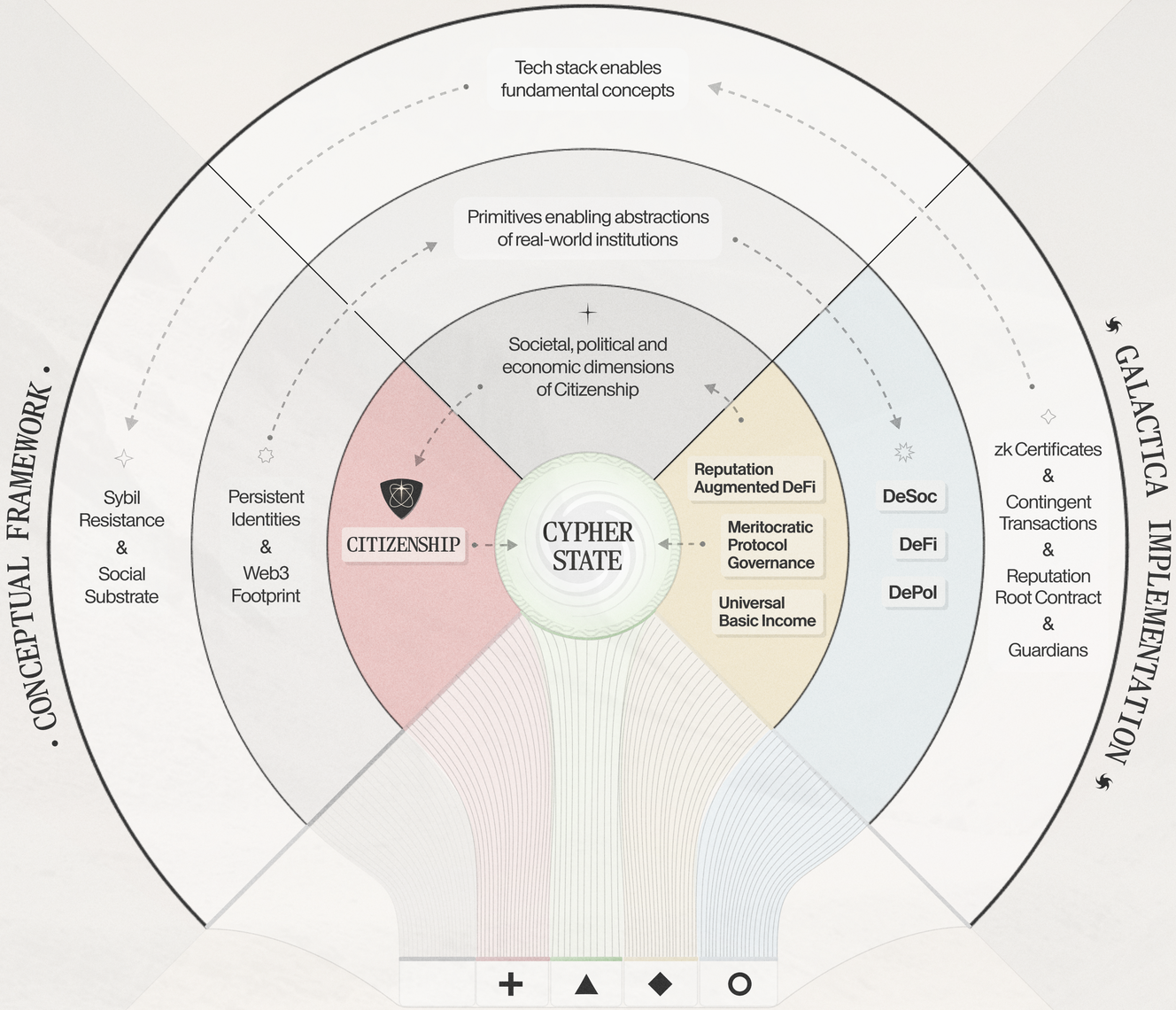
REPUTATION ROOT CONTRACT



CONTINGENT TRANSACTIONS



GALACTICA CONCEPT FRAMEWORK



TOKENOMICS

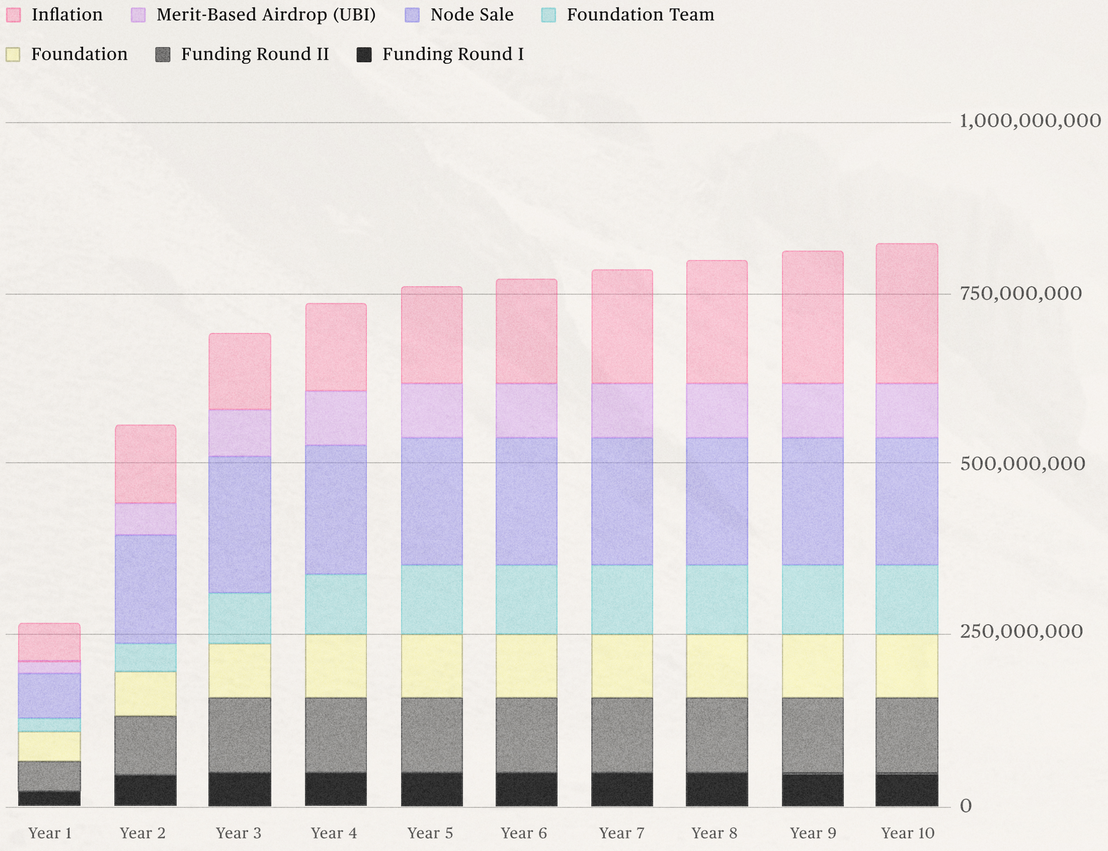
Total Supply:
1,000,000,000 GNET

	% of Total Supply	in $GNET	Unlock at TGE	in $GNET	Cliff (months)	Vesting (years)
Funding Round I	5.00%	50,000,000	7.50%	3,750,000	3	2
Funding Round II	10.00%	100,000,000	7.50%	7,500,000	3	2
Reserve	11.40%	114,000,000	20.00%	22,800,000	0	1
Foundation	20.00%	200,000,000	30.00%	60,000,000	1	2
Founding Team	10.00%	100,000,000	0.00%	0	4	4
Node Sale	13.60%	136,000,000	5.00%	6,800,000	3	2
Merit-Based Airdrop	6.00%	60,000,000	0.00%	0	-	3
Inflation: Validation Rewards	11.08%	110,769,231	0.00%	0	-	36
Inflation: Guardians	4.15%	41,538,462	0.00%	0	-	36
Inflation: AoS	8.77%	87,692,308	0.00%	0	-	36
Total	100%	1,000,000,000	10.09%	100,850,000		

Rewards for Node Holders

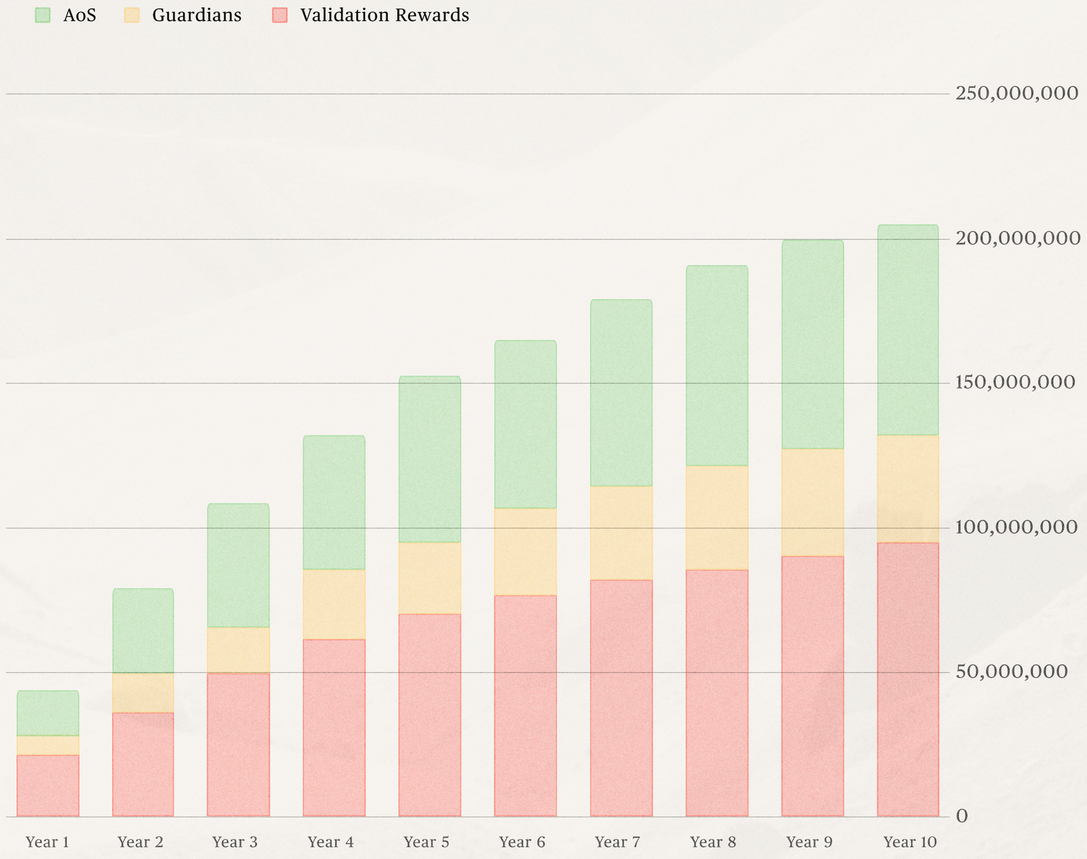
GNET VESTING SCHEDULE

First 10 of 36 years



INFLATION RELEASE SCHEDULE

First 10 of 36 years



IN FOCUS: WEB3 REGULATION AND RWA TOKENIZATION

In 2023, the cryptocurrency market faced significant regulatory developments in both the United States and Europe.

In the United States, the Securities and Exchange Commission (SEC) filed lawsuits against two major cryptocurrency exchanges, Coinbase and Binance [1].

These lawsuits represent a significant escalation in the SEC's efforts to assert its jurisdiction over the cryptocurrency industry, which has largely operated outside of traditional regulation. If successful, these lawsuits could potentially transform the cryptocurrency market, marking a shift towards more significant regulatory oversight.

In Europe, the European Council approved the Regulation on Markets in Crypto-Assets (MiCA) in May 2023, marking a substantial change to the EU regulatory landscape. MiCA, which is the EU's first legal framework for crypto, aims to create a harmonized regime for the issuance and provision of services related to crypto-assets [2].

The regulatory developments in the US and Europe will have significant impact on the tokenization industry. Though Europe was exploring the tokenization even before the approval of MiCA [3], such regulatory developments could speed up the process of crypto adoption.

[1] Reuters (2023), US tightens crackdown on crypto with lawsuit against Coinbase, Binance

[2] Baker Mckenzie (2023), European Union: EU MiCA final approval - Europe adopts comprehensive crypto legal framework

[3] DLNews (2023), EU regulators just launched a programme that will have massive implications for tokenisation

IN FOCUS: RAPID ADVANCES IN AI AND DEVELOPMENT OF ZKML

1. AI Advancements: Significant progress has been made in AI, with increasing capabilities of LLMs like GPT-4, LaMDA, LLaMA, etc. This advancement has broadened AI's application across various industries. More companies are looking into the ways of integrating AI into their products.

2. Zero-Knowledge Machine Learning: Zero-Knowledge Machine Learning (ZKML) is an emerging area within AI that allows data to be processed without revealing sensitive information. It's a part of privacy-preserving machine learning techniques and it's attracting increasing attention due to the growing concern for data privacy [4].

3. Why ZKML is important: ZKML protects the privacy of data during machine learning processes. It can be utilized in areas where sensitive data is involved, such as healthcare, finance, and personal services, ensuring that privacy is maintained while still benefitting from AI's capabilities.

4. Recent Developments: Various research and advancements are being made in the field of ZKML, including the development of new algorithms and techniques [5].

[4] Worldcoin (2023), An Introduction to Zero-Knowledge Machine Learning (ZKML)

[5] a16z (2023), Checks and balances: Machine learning and zero-knowledge proofs

IN FOCUS: ZKP-ENABLED SCALABILITY IMPROVEMENTS

As blockchains have attracted millions of users, and the complexity of applications they host continues to grow more advanced, two key demands around privacy and scalability have emerged.

With the development of zkSNARK protocol in 2014 ZKPs gained significant attention in the crypto space. zkSNARKs essentially made it possible to efficiently scale the number of polynomials that can be gated, unlocking speed and more complex potential applications for zero-knowledge proofs [6].

Here are some of the possible use cases of ZKPs [7]:

1. Privacy-Preserving Transactions
2. Decentralized Identity Management
3. Voting Systems

Application	Bytes in rollup	Gas cost on layer 1	Max scalability gain
ETH transfer	**12**	21,000	105x
ERC20 transfer	**16** (4 more bytes to specify which token)	~50,000	187x
Uniswap trade	**~14** (4 bytes sender + 4 bytes recipient + 3 bytes value + 1 byte max price + 1 byte misc)	~100,000	428x
Privacy-preserving withdrawal (Optimistic rollup)	**296** (4 bytes index of root + 32 bytes nullifier + 4 bytes recipient + 256 bytes ZK-SNARK proof)	~380,000	77x
Privacy-preserving withdrawal (ZK rollup)	**40** (4 bytes index of root + 32 bytes nullifier + 4 bytes recipient)	~380,000	570x

[6] a16z (2022), Decentralized Speed: Advances in Zero-Knowledge Proofs

[7] Chain, Chain Insights: How Zero-Knowledge Proofs Can Enhance Blockchain's Privacy and Scalability

Opportunities	Challenges	Nature	Remedy	Comment
Reduced friction and transaction cost for creation, distribution, trading and settlement of financial assets.	**Scalability, throughput, and transaction fees** for blockchain settlement platforms are significant limiting factors. Energy usage raises concerns about contributing to climate change.	**Tech (ZK)**	Roll-ups, app-chains and on-chain settlement of off-chain computations through ZKPs.	Though it is clearly outside of scope of this report, it's nice to see how all remedies will boil down to clever applications of ZKPs.
Increased standartization and functional interoperability, allowing reuse and recomposition of financial primitives.	**Limited interoperability** accross blockchains and with traditional financial services.	**Reg/Tech (ZK)**	Interoperability with TradFi requires regulatory clarity on the side of watchdogs and RegTech stack sufficiently rich to address it.	Cross-chain messaging and other technological aspects of interoperability are out of scope, but interoperability with traditional finance and real-world assets depends on developing a robust RegTech stack.
Increased auditability and transparency of transactions through blockchain-based records.	**Privacy considerations** may be in tension with transaction transparency.	**Reg/Tech (ZK)**	Zero-knowledge proofs will play a pivotal role in addressing compliance in public networks.	The opaque nature of traditional finance led to corporate scandals such as Enron and Lehman Brothers. Web3's transparency can prevent these issues in future, but to fully realize its potential, the segment needs appropriate regulation.
Improved accountability for decisions through software-based governance systems.	**Immature governance** as high-stakes decisions are made by small, inexperienced teams. Lack of accountability when developers are anonymous.	**Reg/Sybil (ZK)**	On-chain reputation through Sybil Resistant protocols and robust regulation through identity centric solutions	Lack of accountability is perhaps the single greatest adverse factor limiting the adoption of web3. It has turned it from a vehicle for financial liberation into a glorified casino. On-chain reputation will solve the current lack of merit-based incentives in the web3 stack.
Greater stakeholder control through non-custodial, disintermediated service provision.	**Hidden centralization of control** and low thresholds for governance rights may give certain actors disproportionate power.	**Reg/Sybil (ZK)**	Sybil resistance networks lend themselves to much more sophisticated political primitives than traditional DAOs	"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."
Improved market access by providing global, 24/7 availability of services and removing barriers such as a bank account requirements.	**Regulatory questions** and enforcement challenges in applying national legal requirements to decentralized global networks.	**Reg**	A developed RegTech stack would offer a meaningful solution, allowing the industry to respond swiftly to the emerging regulatory landscape.	From the standpoint of securities regulation, digital assets do not have a standardized form or definition. Therefore, they can take any shape, structure, or form. This can make it challenging for regulators to classify and regulate them appropriately, and eventually leads to regulatory adoption with different speed across different jurisdictions.
Faster settlement, reducing counterparty risks and freeing up capital.	**Immature technology** is being used to manage high-value assets. Poor design choices and implementations have led to significant losses.	**Tech**	A robust reputation system for developers is essential to promote accountability, trust, and high-quality work in decentralized technologies.	As Web3 matures, it has become clear that the stack would benefit from a reputation framework. This is due to the unique nature of digital assets, and the specificities that underlie decentralized ecosystems.
Greater inclusivity of financial services by making automated tools available to all, with transparent and non-discriminatory execution.	**Extreme short-term returns** during DeFi's early growth stage attract unscrupulous actors and warp user expectations. Limited usability impedes large-scale adoption.	**Reg/Tech**	To create something valuable, prioritize the user and ensure consumer protection. Design intuitive UX/UI for user-friendliness and adoption.	In many ways, the web3 industry today resembles a glorified casino; a parody of its own ideals. This has resulted in a paradoxical situation where the industry has burned more of its supposed "next billion users" than it has elevated from poverty. Without effective regulation, the industry risks losing its potential to bring about positive change in the world.
Permissionless innovation, allowing the creation of novel products and services.	**Potential for facilitation of financial crime** such as money laundering.	**Reg/Tech**	In order to promote effective regulatory compliance, Web3 requires both regulatory clarity and a RegTech stack.	The Web3 ecosystem enables permissionless innovation, but has also led to the proliferation of financial crimes. Regulatory clarity and the development of a robust RegTech stack are crucial in the fight to combat opportunistic bad actors motivated by greed.