REPBASE

THE DECENTRALIZED PROFESSIONAL REPUTATION NETWORK

WHITEPAPER v1.0

SEPTEMBER 2022

BY LUIS ANDRÉS IREGUI AND WESLEY SMITH

Table of Contents

CHAPTER I: THE REPBASE VISION

What makes blockchains such a game changer for humanity is that they help solve two social problems that are inherent in almost all interhuman relationships: trust and ownership. Since its inception in 2008, blockchain technology has proven to be particularly good at optimizing trust and proof of ownership through decentralization, primarily in the financial realm with DeFi and lately with NFTs in gaming and art.

It's time blockchain technology is applied successfully to the field of reputation, a critical component of human interactions that, due to its traditionally subjective nature, is constantly laden with distrust or suspicion. Such an application, however, must tread carefully or it could be close to dystopic because reputation is one of their most protected and cherished characteristics of a myriad of social actors due to its dramatic impact on most relationships.

One such use case is professional reputations. Currently, there are several professional social networks (ie. LinkedIn, ZipRecruited, etc), but they all suffer from suspicious data accuracy and give users little to no control over their data. Now imagine a professional reputation profile (PRP) where the identity as well as all the academic and professional achievements of an individual are always 100% accurate and up to date. One where users have complete ownership of their data and can easily control who has access to it and under what circumstances. This would solve some of the major problems current professional social networks have such as privacy issues, censorship, unbalanced business models, scammers, bots and spam.

To create a professional reputation profile (PRP) that accomplishes the above, we developed the Repbase Protocol which combines several Web3 technologies, each with a clear purpose that adds value:

- **Soul-Bound Tokens (SBTs)** tie the profile to a single individual.
- **Non-Fungible Tokens (NFTs)** act as verified credentials that guarantee the accuracy of the data contained on each profile.
- **Zero-knowledge proofs** are used to validate credentials without encroaching on privacy.
- **Soul Sharding** allows users to control at a very low level who gets access to what data from their profile.
- **Recovery Committees** are a new social recovery mechanism that allows users to regain control of their profiles in the event they lose access to their wallets or have their private keys compromised.
- **Polygon POS** is the initial blockchain used, but we envision using zero-knowledge proofs and Merkel trees to make protocol cross-chain compatible.
- **Reptokens** are an ERC20 utility token that, through tokenomics, incentivizes network use by all stakeholders.

The next chapters of this document go into much greater detail on why there is a problem with professional reputation (Chapter II), how we see that problem being solved (Chapter III), and the technologies that make our solution viable and how it will likely change in the future (Chapter IV).

CHAPTER II: THE CURRENT STATE OF AFFAIRS

Successes And Shortcomings Of Existing Professional Networks

There is no shortage of professional network examples such as LinkedIn, Indeed, BranchOut, and Zip Recruiter. Their success is expected to create a global market worth USD$ 43.39 billion by 2027, with an impressive annual CAGR of 7.1% between 2020-2027 and continued growth expected beyond that[1].

However, these companies fail in a key component to their value proposition: the accuracy and privacy of professional reputation. Their centralized nature implies that guaranteeing the accuracy of their users' profiles would carry a huge cost and making that data private and owned by their users would go against their business models.

The Data Accuracy Problem

Perhaps the most important component to professional reputation is its accuracy. Under the current centralized paradigm of professional networks, they would have to spend billions of dollars getting all their users' profiles properly vetted and verified. As a result, they settle for an honor system where they trust that users provide accurate data in their profiles, leading to several problems.

- Up to 60% of employees have "discrepancies" in their work experience, and around 50% of them had the same problem relating to their education[2], while 45% of LinkedIn profiles are incomplete or out of date[3].
- The lack of accuracy in the data contained in professional networks has enabled fraud and abuse to the point the FBI calls the problem a "significant concern" to these platforms and their users[4].
- Professional marketing firms that get paid for lead generation are using AI and bots to increase their income by creating entirely fake profiles[5]. As these kinds of technologies continue to evolve, it's foreseeable that their users' trust will erode consistently.

---

[1] https://www.globenewswire.com/en/news-release/2022/02/28/2393171/0/en/USD-43-39-billion-growth-in-Online-Recruitment-Market-by-2027-at-a-CAGR-of-7-1-during-forecast-period-Fortune-Business-Insights.html
[2] https://www.hireright.com/resource-library/view/2021-global-benchmark-report
[3] https://resumelab.com/resume/how-often-to-update
[4] https://www.cnbc.com/2022/06/17/fbi-says-fraud-on-linkedin-a-significant-threat-to-platform-and-consumers.html
[5] https://www.npr.org/2022/03/27/1088140809/fake-linkedin-profiles

The Data Privacy and Ownership Problem

Another considerable issue with existing professional networks is that they're all Web2 native, and thus are weak in issues related to privacy, data ownership and centralization. This weakness is evident in several ways:

- Data privacy is an all or nothing affair, making professional networks vulnerable to data scraping with at least 500 million user profiles being sold in the dark web[6].
- Users don't own or get rewarded for their data despite it being the heart of these network's value proposition. So as the famous expression goes, if you aren't paying for the product, you are the product.
- The data-selling business model has a perverse and negative effect on the user experience. For example, putting certain data behind paywalls is not a justifiable expense for most users, but for scammers and spammers it's an investment with a good return.
- The centralized nature of these companies leaves users vulnerable to censorship. Users lose access to their accounts without explanation or a transparent appeal process[7].

[6] https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/

[7] https://www.vice.com/en/article/dy8m9z/linkedin-social-media-ban-censorship

CHAPTER III: THE REPBASE DECENTRALIZED PROFESSIONAL REPUTATION NETWORK

Overview

To address the problems described, Repbase leverages Web3 technologies that allow people to verify and store their professional reputation on the blockchain while retaining ownership. Something akin to a digital resumé but owned by each individual rather than a centralized corporation and made up of data that is accurate and therefore much more useful to all the stakeholders of the network.

Repbase will bring together employers, employees, academic actors and trusted third-party data sources, then uses tokenomics to incentivize them to participate in a decentralized ecosystem. This network allows for nearly real-time and fully certified information about work experience, academic accomplishments, and identity verification that take the form of non-fungible tokens (NFTs). These NFTs are linked to a unique Soulbound Token (SBT) each user has, which we call the Professional Reputation Profile (PRP).

Work Experience Attestation

Repbase allows employers to attest the professional achievements of their employees directly on to their PRP. For each achievement the employee gets, the employer can also choose to reward the employee with Reptokens, which can be used in the Repbase ecosystem in several ways. This incentivizes employees to perform better and therefore it incentivizes employers to continue using Repbase, creating a virtuous cycle that constantly enriches the network.

The first step is for the employer to set up the achievements and the token rewards they will give out for each achievement. This is done in the Repbase Employer Platform software. These achievements will initially be very general but eventually could get as specific as the employer wants, depending on their business, corporate culture, and what's important to their employees. They can also be based on purely objective metrics or more subjective criteria.

For example, a tech company can decide to award an achievement to developers based on the number of hours worked during a development sprint. Depending on each employee's performance, they will receive an achievement in the form of an NFT that's permanently linked to their PRP. Employers could also attest more subjective metrics, like congeniality, honesty, and proactivity. In other words, pretty much anything that's important to a user or company can be attested and highlighted in the employee's PRP, dramatically enriching the depth of PRPs and adding value to the overall network.

This approach guarantees that the work experience that employees display on their PRPs is accurate and up to date because Repbase integrates directly with employers so that they attest these achievements based on real-world data. This integration can be automatic

or manual, so the data can come directly from software that measures employee performance like Jira, SAP, or Salesforce so that the attestations require very little operation, or if the employer lacks these sophisticated solutions, they can enter it manually in the Repbase Employer Software.

Academic Accomplishments and Identity Attestation

It's also necessary to attest academic achievements of every type as well as acquired and proven skills. In certain cases, it may also be important to know that the owner of the PRP is a real person, or perhaps it's even vital to validate their specific identity.

Academic institutions like universities, online education platforms, standardized testing companies, technical institutes, and other similar academic actors can integrate with Repbase to automatically generate a verified attestation of a degree, skill, test score, award, publication, or other academic achievement the moment the user attains it. That achievement is then linked to a user's PRP via an NFT in the same way work experience is linked.

However, what happens when that integration isn't possible due to legacy systems or the lack of clear incentives? For academic and other types of data sources that are not or cannot be integrated with Repbase, users can exchange Reptokens to get verification on these achievements or identity attestations. The tokens are used to pay a third-party that specializes in this type of task, for example a KYC software provider or a data analytics company, to verify what the user wants to have attested.

Privacy, Ownership, and Control of PRP Data

By the very nature of the blockchain technology Repbase uses, it's also private, owned and controlled by each user. The technology allows users to select exactly what data is viewable and by whom at an extremely granular level, allowing them to pick and choose who sees what from their profile, as well as when and how many times.

There's also an economic component. Users can choose to charge unknown users for the privilege of seeing their data, or to not charge at all if it's someone they know, like a colleague, a friend, or a recruiter from a company where they recently applied for a job.

The combination of handing users complete control over their data, empowering them to charge anyone for the privilege of viewing said data, and that all the information on Repbase is accurate and verified, makes it extremely difficult for spammers, scammers and bots to abuse users.

Additionally, since their data is on a blockchain and owned solely by each user, they can take it with them to other platforms and are in no way chained to Repbase and cannot be censored by anyone. For example, they can prove in a talent marketplace they have the required experience that grants them access to a premium freelancer contract. It is even possible that existing Web2 juggernauts like LinkedIn and ZipRecruiter allow users to connect their PRP data to verify the profiles they have in those platforms.

Incentives For Network Participants

When all the benefits of the Repbase vision are combined, a powerful virtuous cycle emerges where the main participants in the professional reputation network have the right incentives. This incentives system is designed to give the two main actors in Repbase, employers and employees, real world and immediate benefits that stimulate them to continue to use the network.

In the case of employees, there are three clear incentives built into Repbase that will add value to their lives and careers.

1. By participating in Repbase they create an attested reputation that they own, can monetize, use on their terms, and is censorship resistant.
2. They earn tokens that can further enrich their PRP or create additional income by being exchanged for other forms of cryptocurrencies.
3. These instantaneous benefits incentivize them to perform better over shorter periods of time and increase motivation because gratification comes quicker and more consistently.

When it comes to employers, the benefits will vary depending on the type of employer and how sophisticated they are in their incentive programs, but all should at least see some general benefits.

1. Performance from their workforce should increase.
2. They should have an easier time spotting reliable talent they wish to hire.
3. Companies that don't have sophisticated ways to measure performance of their employees can leverage the Repbase Employer Platform for this goal.
4. They will find in Repbase an automated and affordable performance incentive program.

CHAPTER IV: THE TECHNOLOGY THAT POWERS REPBASE

Soulbound Tokens and Attestations

One of the best features of blockchains is the ability to create a near infinite number of new wallets. However, this opens the door for "Sybil Attacks", where an attacker can create as many fake accounts as they wish to impersonate a larger group of people. This is antithetical to the core idea of Repbase, since a personal reputation profile (PRP) is only linked to a single person or entity.

To create sybil resistance we use "Soulbound Tokens" (SBTs) as originally conceived by a group of authors headlined by Vitalik Buterin[8]. SBTs are tokens that are tightly linked to an individual or entity thus making them "soulbound". They solve the sybil problem by providing a verifiable identity for a given wallet on the blockchain.

Within the Repbase protocol, any time an employer wants to issue an achievement to an employee, this is issued as an NFT, and referred to in this chapter from a technical point of view as an Attestation. Attestations share many of the qualities of the SBTs described above, as they are only intended to be issued to a single person.

Problems with SBTs

SBTs are usually envisioned as an NFT that is locked to a specific wallet address. This can be achieved by overriding the transfer function of the NFT. For instance, in the Repbase Protocol, companies would issue their employees Attestations that would then be permanently stuck in their crypto wallet. However, locking tokens at the wallet level creates serious challenges if an employee loses or has their private keys compromised.

Repbase Protocol Solution to SBTs

To overcome these obstacles, Repbase proposes that instead of locking Attestations at the wallet level, they should be locked to an additional NFT with its own special properties. Let's refer to this new NFT type as the "Soul NFT". It is an NFT, but with special recovery characteristics if a user loses access to their wallet. In this way, Attestations are "bound" to this Soul NFT, thus, making them "soul bound". In the event the user's wallet is compromised, they may engage in a social recovery process (described below) that will allow them to transfer their Soul NFT into a new wallet.

This idea of linking the Attestation to the Soul NFT creates considerable advantages. The Repbase protocol can be agnostic about whatever private key management solution the user prefers and lets them retain full control over their PRP.

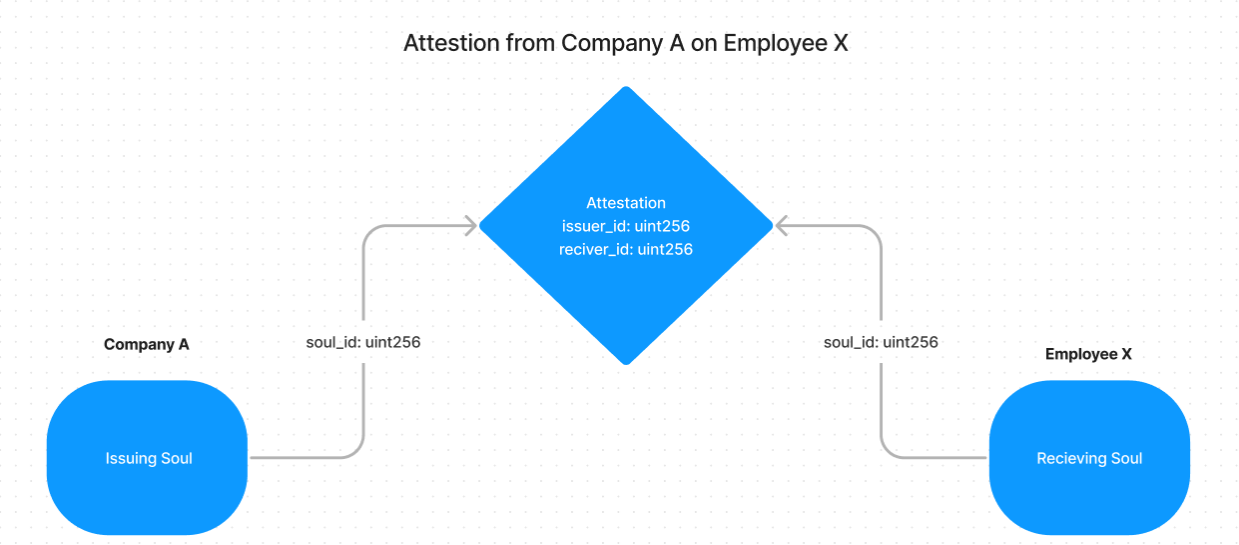
[8] https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4105763_code1186331.pdf?abstractid=4105763&mirid=1

Repbase Primitives

The core of the Repbase Protocol is three constructs: Souls, Attestations, and the PRP.

- **The Soul** is an ERC721 NFT that is bound to a specific person or entity.
- **Attestations** are NFTs that are bonded to Souls when created and this bond can't be changed.
- A user's **Professional Reputation Profile (PRP)** is the combination of their Soul and the Attestations they have bound to it.

All Attestations are linked to two Souls, the Soul of the issuer of the Attestation, and the Soul of the receiver. For instance, if Company A is issuing an Attestation to Employee X, the issuer of the Attestation would be Company A, and receiver of the Attestation would be Employee X.



1. An example Attestation, where the NFT IDs of the issuing and receiving souls are stored immutably. This is the foundation of the PRP.

Finally, Repbase is powered by validator smart contracts that live on the blockchain. These have an API that can be called by other contracts or referenced externally to validate users' Attestations. Validator contracts allow third parties to confirm and verify information about users' PRPs.

Privacy, data, and Attestation Verification

For an employee to demonstrate that they have received a certain Attestation, they must create a proof using the wallet that holds their Soul. For any of the Attestations connected to this Soul, they may generate a corresponding proof. Once this proof is generated, it can be submitted to the validator contract to ensure its validity.

There are several ways a user may generate one of these proofs, the simplest being that a user must sign a message from the wallet that is currently registered as the soul-owner.

While this is functional, it doesn't completely preserve the users' privacy. An improved approach is to use a zero-knowledge proof.

Zero knowledge proofs

Zero knowledge proofs are a relatively new cryptographic tool. They allow for a user to "prove" that something is true, without revealing more than the bare minimum amount of data that is required. The most famous example is if someone wants to enter a bar where the drinking age is 21. Currently, customers are required to show their ID, which reveals their entire birthdate, name, gender, and other private information. With a zero-knowledge proof, a customer could simply show a proof that returns true/false when they are asked if they have the minimum age required, with no further information being given away.

The concept is the same within the Repbase Protocol. Instead of a user having to reveal their entire work history, they could simply submit a proof that confirms that they worked a specific company, nothing more. By leveraging zero-knowledge proofs, the protocol can maximally preserve users' privacy while giving them fine grained control over when and with whom they want to share their PRP information.

Soul Shards

One challenge of this system is that to generate Attestation proofs, users must frequently sign messages with their Soul owner wallet. This may not be ideal for many users, who would prefer to keep their Soul in a cold-storage wallet that is accessed less frequently.

To solve this problem, the Repbase Protocol allows users to create "Soul Shards". Soul Shards are temporary Souls that may be approved for a subset of the parent Soul's Attestations. This allows a user to place a Soul Shard in a hot wallet that they can use to generate Attestation proofs daily while keeping their Soul secure in cold storage. Soul Shards may be revoked with a signature from the parent Soul, or after their expiration date has passed. This allows the Repbase Protocol to prioritize security and convenience equally.

For instance, an employee has just received a scrum master certification, and is currently searching for a new job. For recruiters to verify this certification, the user must submit a proof of the scum master Attestation with each job application. Since they are applying to many jobs, they must generate a lot of proofs. By creating a Soul Shard that has permissions to generate proofs for the scrum master Attestation, they can easily generate these proofs on the fly, without having to constantly sign messages from their cold wallet. Since there are no other Attestations attached to this Soul Shard, if the employee's wallet is compromised, the attacker won't gain access to any of the other data in the PRP, and the user can reject the Soul Shard's permissions using the parent Soul.

Social Recovery and Security

Off-chain data

Because one of the core value-adds of the Repbase Protocol is privacy protection, users would not want their Attestations and work history stored on a public blockchain in

unencrypted plaintext. As a result, the Attestation metadata is stored off-chain and only a hash of the Attestation details is published onto the chain. This allows the protocol to preserve privacy and allow for on-chain verification of Attestation claims.

Since the sensitive data of Attestations is stored off-chain and there are already off-chain identity specifications that have been defined, such as the W3C verified credential specification, it's valid to question why the use of a blockchain is necessary.

Souls and Attestations must be published on-chain to show the origin of the Attestations. Although specs such as verified credentials partly solve this, they can't truly certify that a given key belongs to a specific entity. By publishing part of the data on-chain, the Repbase Protocol leverages one of blockchains best use-cases: an immutable ledger with a history of provenance.

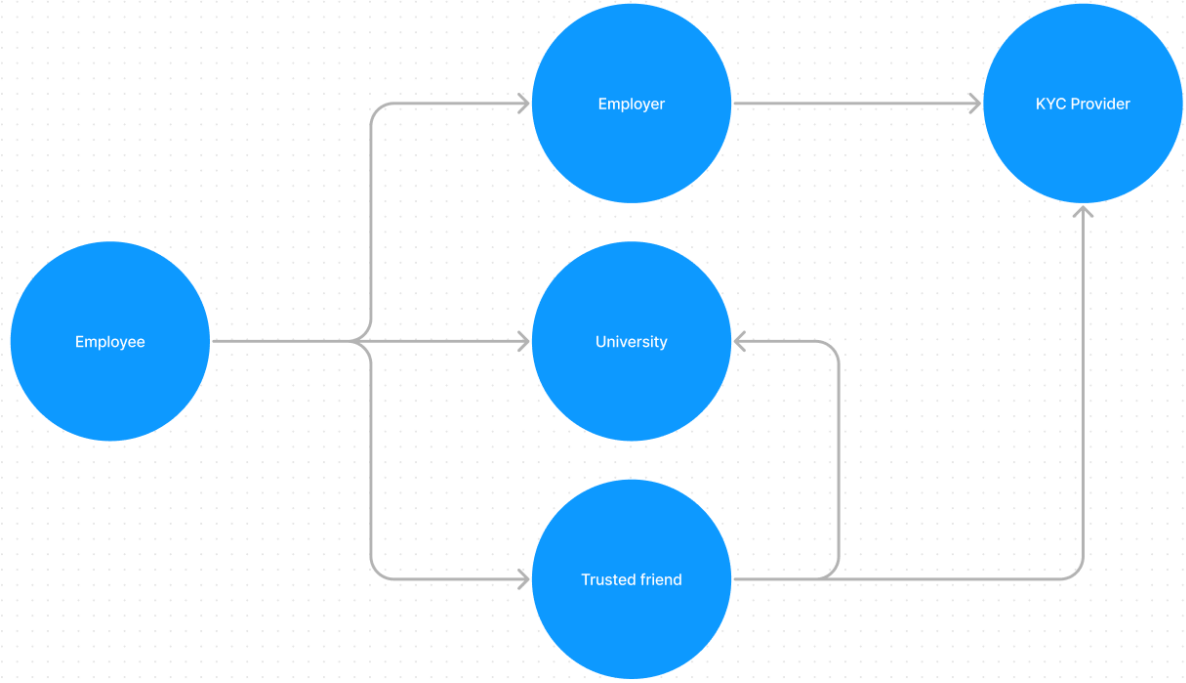
Wallets and Attestation Ownership

The Soul is the core of the Repbase Protocol, so recovering it in the event of hacks or lost private keys is essential. Repbase solves the recovery problem by requiring that all Souls create a Recovery Committee. A Recovery Committee is a group of Souls that must all submit valid signatures to recover a Soul. Once a Soul has been recovered, its ownership is updated to a new wallet controlled by the rightful owner. In the context of Repbase, a Recovery Committee can be comprised of a collection of PRPs that the owner can appeal to so they can recover their Soul.

This is similar to the concept of an N-of-M multisig. A N-of-M multisig is a wallet where a certain number of the owner's signatures are required to approve a transaction. For instance, in a 2-of-3 multisig wallet, at least two of the three members must sign the message for it to be valid. In the same way an N-of-M multisig functions, users may decide that only a partial majority of their Recovery Committee is required to approve a transfer of a Soul to a new wallet. This allows the user to have fine grained control over their security settings.

The result of this is a social recovery web, where Souls are all interlinked to one another providing different types of social recovery. Employers can provide recovery for their current employees, while identity solutions can provide recovery mechanisms through traditional KYC verification.

Ultimately, it's up to the Soul's owner how broad they want their social recovery committee to be and who participates in it. This intertwined social recovery web is a core value add of the Repbase protocol. It benefits from strong network effects where the usefulness, robustness, and security of the social recovery mechanism grows stronger with the more participants it has.



2. An example of how the social recovery web might grow over time, with different entities and users all providing social recovery for each other.

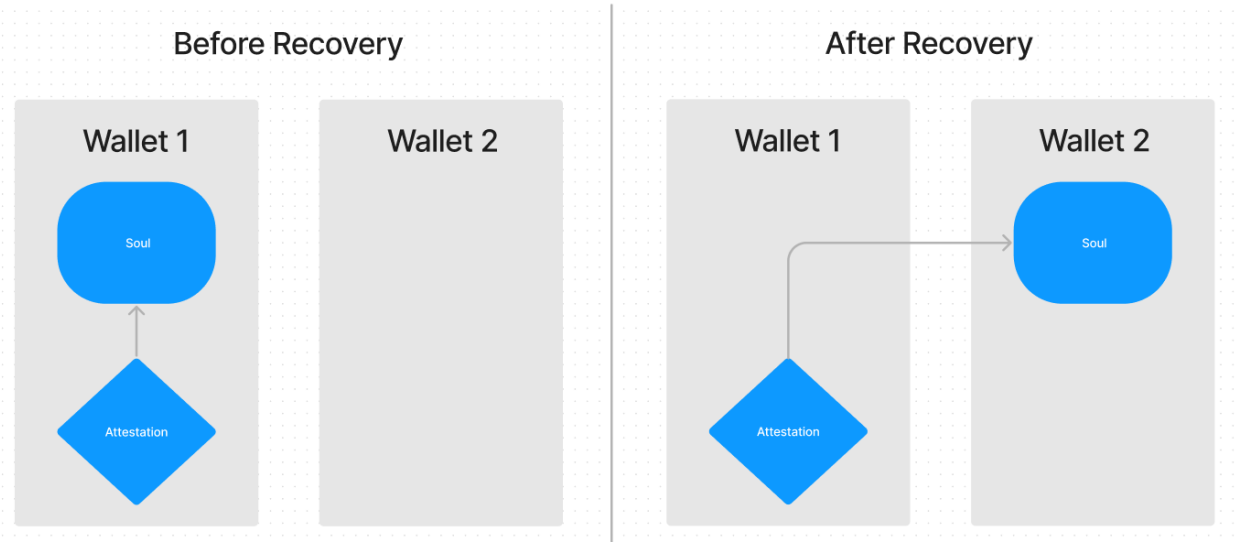
In addition to the Recovery Committee, a user can freeze their Soul at any time. Soul freezing is an added security feature in the event an owner's private keys have been compromised. Because a user will still have access to their private keys, they can submit a transaction to the validator contract that marks their Soul as "Frozen". Once a Soul has been frozen, the validator contract will return false for all Attestation proofs that are submitted to it. After their Soul has been frozen, they may only un-freeze it by going through the social recovery process.

The social recovery steps would be as follows:

1. A user freezes their Soul.
2. The user contacts their Recovery Committee. This can be an automated or interpersonal depending on the user and their Recovery Committee preference.
3. Each committee member sends a signed message to the user approving the transfer of the Soul to a new wallet.
4. When the user has enough signed messages from the committee members, they submit the messages in a transaction to recover their Soul.

At this point, the Soul is transferred to a new wallet, but the Attestations are not transferred with the Soul. This is permissible because the only significant part of the Attestation is the bond to a specific Soul, not which wallet the Attestation currently resides in. In fact, it's not necessary that the users hold **any** of their attestations in their wallet. The only requirement for verifying the owner of a specific Attestation is its bond between that Attestation and the ID of a Soul that they own.

This is an essential feature, as there are several security and privacy reasons that a user may want to change wallets. Additionally, if someone wants to change wallets for any reason, they do not need to transfer all their Attestations into a new wallet.



3. After social recovery, Souls are transferred to a new wallet, but Attestations remain behind.

The Future of the Repbase Protocol

A core component of blockchain systems is the concept of composability . Composability allows for smart contracts to re-use and integrate with other smart contracts that live on the chain.

The Repbase Protocol will initially launch on the Polygon POS chain due to low network fees and a strong community. However, the future of Ethereum is likely to be multi-chain and rollup centric. While rollups allow Ethereum to scale through Layer 2 solutions, one of their biggest weaknesses is that they break composability.

Therefore, it's highly likely that Repbase will eventually have validator contracts that live on all the popular L2 solutions. Using zero-knowledge proofs or Merkle trees, it can be possible for users to export Attestation proofs from one chain and submit them for validation on other chains.

This is an area within the Ethereum ecosystem that is developing rapidly, and as a result the Repbase Protocol must remain flexible enough to adapt. However, the objective remains the same: allowing users to export their proofs of Attestation and use them anywhere throughout the Web3 ecosystem.

The Repbase Protocol may also evolve to encompass far more than just professional attestations. This same technology could be used to power a wide range of identity and verification systems throughout the blockchain ecosystem. Some examples of problems Repbase could solve include the following:

1. DAOs and other blockchain organizations could solve on-chain voting problems due to sybil attacks.
2. Reduce the need for Web2 KYC, which is often onerous, repetitive, and vulnerable to fraud.
3. Add protection from deepfakes and AI generated profiles, which are increasingly difficult to detect.
4. Aid current anti-fraud solutions that are engaged in a race to the bottom where fraudsters and bot creators will inevitably become indistinguishable from honest actors.

The realistic long-term solution to these problems is that real people will have verifiable IDs that they can use to show their "proof of humanity", proving to internet systems that they are not a bot or fake account. In the spirit of this, we aim to make it so that Repbase can become a cornerstone technology that helps create the next generation of identity and verification solutions.