REPBASE

THE DECENTRALIZED PROFESSIONAL REPUTATION NETWORK

WHITEPAPER v1.0

SEPTEMBER 2022

BY LUIS ANDRÉS IREGUI AND WESLEY SMITH

Table of Contents

Chapter I: Executive Summary

When people think of a professional network, there is no shortage of examples such as LinkedIn, Indeed, BranchOut, and ZipRecruiter just to name a few. Despite their differences, companies in this space share a common denominator that has them play as matchmakers for employers and talent. The considerable size and growth of this industry indicates that over the last decade these companies have done a fantastic job of delivering on this value proposition and have massively disrupted the way employers and talent find each other. However, by focusing on recruitment and frictionless professional networking, these companies fail in a key component to their value proposition: the accuracy and privacy of professional reputation.

Perhaps the most important component to professional reputation is its accuracy. Under the current centralized paradigm of professional networks, these companies would have to spend billions of dollars getting all their users' experience, education, endorsements, and other components of their profiles properly vetted and verified. This has resulted in professional networks settling for an honor system where they trust that users provide accurate data in their profiles. Although that has worked to a certain degree, it's also meant that profile data is unreliable or incomplete, it doesn't adequately and fairly reflect the skills and accomplishments of its users, and it has left the door wide open for scammers and bots.

Another considerable issue with existing professional networks is how they handle their user's data and the business models they've built around said data. Since they're all Web2 native, they inherit all the issues endemic to these companies, notably those related to privacy, data ownership and centralization. These issues are clearly present in current professional networks and are visible in several ways. First, data privacy is an all or nothing affair. Second, users don't own or get rewarded for their data despite it being the heart and soul of these network's value proposition. Third, the data-selling business model perversely stimulates spam and negatively affects the users' experience. And fourth, the centralized nature of these companies has left users vulnerable to censorship.

To address the problems described above, 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. Additionally, Repbase will have built-in incentives that promote the use of the network by all parties, reward those that add value to it, and significantly improve the user experience for all the good faith network participants while at the same time creating obstacles for bad faith actors like spammers, bots and scammers.

Repbase aims to achieve this by bringing together both employers and employees and 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), which are linked to a Soul Bound Token (SBT). The end result is a unique, non-transferable, reliable, up-to-date, and user-owned professional reputation profile (PRP) for each user.

The Repbase Protocol provides verification of the SBTs and accomplishments that exist on the PRP through smart contracts deployed onto Polygon POS chain and Ethereum L2s. Validation of PRP credentials is done by using zero-knowledge proofs and other privacy preserving techniques. Security is provided through a new social recovery mechanism, defined as Recovery Committees, that allows users to regain control of their PRP in the event they lose access to their wallets or have their private keys compromised.

Regarding governance, as a native Web3 company, the founding team at Repbase is strongly inclined toward the creation of a decentralized structure to oversee the most crucial aspects of the future of the network. In that spirit, we propose that a Decentralized Autonomous Organization is the correct path for Repbase to take. To avoid bots, uncommitted participants, or users that could buy their way to impose their will on the community, only PRPs that have invested in a personhood attestation will be allowed to vote, and each one of these PRPs will have single vote.

Chapter II: The Current State of Affairs

Successes And Shortcomings Of Existing Professional Networks

When one thinks of a professional network, there is no shortage of examples such as LinkedIn, Indeed, BranchOut, and Zip Recruiter just to name a few. Most have different focuses and competitive advantages aimed at getting a slice of a market that is expected to reach USD$ 43.39 billion by 2027, with an impressive annual CAGR of 7.1% between the 2020-2027 and continued growth expected beyond that[1].

Despite their differences, companies in this space share a common denominator that has them play as matchmakers for employers and talent. Their value proposition to employers is that they make talent recruitment easier and cheaper, and they lure talent with the promise of helping them grow as professionals by granting them access to seemingly infinite professional growth and networking opportunities.

The considerable size and growth of this industry indicates that over the last decade these companies have done a fantastic job of delivering on this value proposition and have massively disrupted the way employers and talent find each other. It's a common practice for professionals and corporations of all backgrounds and in every industry to participate in these professional networks.

However, by focusing on recruitment and frictionless professional networking, these companies fail in a key component to their value proposition: the accuracy and privacy of professional reputation. Their centralized nature makes it easy to see why: making sure the data that makes up their users' profiles is accurate would carry a huge cost and making that data private and owned by their users would go against their current, well-oiled and profitable 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, these companies would have to spend billions of dollars getting all their users' experience, education, endorsements, and other components of their profiles properly vetted and verified. This has resulted in professional networks settling for an honor system where they trust that users provide accurate data in their profiles. Although that has worked to a certain degree, it's also meant that profile data is unreliable or incomplete, it doesn't adequately and fairly reflect the skills and accomplishments of its users, and it has left the door wide open for scammers and bots.

The first issue with the data contained in current professional networks is that it's very often unreliable or incomplete. HireRight, a company with a worldwide footprint specialized in employee screening for recruitment processes, found in their 2021 benchmark report that

[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

in Asia, Latin America, and North America up to 60% of employees had "discrepancies" in their work experience, and around 50% of them had the same problem relating to their education[2]. In their own survey of 1,000 professionals in the US, Resumelab found that 45% of the respondents admitted their LinkedIn profiles were incomplete or out of date[3]. These two studies show that people either outright lie or aren't diligent in their professional network profiles, and this is true worldwide.

Another issue lies in the type of data that is displayed in user profiles. Although professional networks today do a great job of showing overall experience and education milestones, the specific skills and accomplishments that can truly distinguish talent are much harder for users to showcase. For example, it's easy to see if someone has worked in a Fortune 500 company, and the years they spent there, but their true performance is far from highlighted. We argue that it is as important to know if someone went to Harvard or worked at Google, as it is to be aware that they earned awards for an incredible graduate thesis and completed their KPIs over 100% every single month they worked for an employer. The devil, or rather the hero, is in the details, but current professional networks encourage their users to coat their profiles with paint guns instead of a precise brush, denying them the huge value that can come from standing out for their accomplishments.

The problem is exacerbated by the few mechanisms that do have a more starring role in user profiles and seek to highlight particular skillsets, like endorsements, because there is no real validation that the endorsements people receive aren't just favors or quid pro quos that do not reflect the true professional ability of members. Some power users really do have very well curated job and education histories, but even if a recruiter has the sharp eye and patience to properly appreciate their efforts and achievements, it's hard for them not to harbor doubts about the veracity of what they are looking at since there is zero objective verification.

Finally, the lack of accuracy in the data contained in professional networks has enabled abuse by unscrupulous and even criminal users. Since anyone can create an account with basically no other verification other than a valid email address, from the earliest days of professional networks scammers have feasted on unsuspecting and trusting individuals. Lately, the scam du jour centers around crypto and it's gotten so bad the FBI has sounded the alarm and called the problem a "significant concern" to these platforms and their users[4]. For instance, a recent CNBC article cites one of their reporters meeting a group of people that lost between USD$ 200,000 and 1.6 million, the entire life savings of some victims.

It's not just criminals that are taking advantage of the lack of data verification in these networks, either. Professional marketing firms that get paid for lead generation are using AI and bots to increase their income by creating entirely fake profiles, as an eye-opening NPR investigation recently revealed[5]. As these kinds of technologies continue to evolve and

---

[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

accelerate their sophistication, the problem will only increase for professional networks and will soon get to the point where it will be unsustainable for everyone involved. It's foreseeable that their users' trust will erode consistently until it directly cuts into the bottom line of these businesses.

The Data Privacy and Ownership Problem

Another considerable issue with existing professional networks is how they handle their user's data and the business models they've built around said data. Since they're all Web2 native, they inherit all the issues endemic to these companies, notably those related to privacy, data ownership and centralization. These issues are clearly present in current professional networks and are visible in several ways. First, data privacy is an all or nothing affair. Second, users don't own or get rewarded for their data despite it being the heart and soul of these network's value proposition. Third, the data-selling business model perversely stimulates spam and negatively affects the users' experience. And fourth, the centralized nature of these companies has left users vulnerable to censorship.

Currently, professional networks take an all-or-nothing approach to privacy. In other words, whatever information users put on their profiles is totally public. The most powerful networks don't even have basic privacy filters that allow users to show only certain data to others with whom a connection is shared. This basic privacy feature is something that's available even in social networks (not exactly havens of data protection or privacy, either). This practice has made professional networks particularly vulnerable to data scraping with at least 500 million user profiles being sold in the dark web[6]. Security isn't the only problem since this lack of privacy control can lead to an unconscious bias for those looking at user profiles with a specific aim, like recruitment or workplace research.

The problems caused by this approach are compounded by the current business model most professional networks have because the incentives are not aligned with what's best for the users. These companies need the data of their user profiles to be public, which, as already noted, leads to security problems for users as well as spam issues. As mentioned already, marketing firms are using AI and fake profiles to spam people in search for lead generation, and many users have grown tired of the incessant commercial pitches that constantly flood their message inbox or registered email address. The social aspect of many of these professional networks adds to the spam in the form of seemingly infinite connection requests from complete strangers seeking to pump up their connection count to get more exposure and to seem better connected.

All these examples of problematic user experience have a common denominator: they are rooted in the incentive system that feeds the business model for most of these networks. Historically, users have been willing to share their data despite not having any ownership and very little control over it. In exchange, they don't have to pay to get access to better business opportunities and connections. To be clear, that's a compelling value

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

proposition for users and may have been a fair trade in the early days of this century, but technology and society have moved toward valuing data privacy, ownership, and user control. Users should be rewarded by more than just having access to a not-at-all-exclusive club. As the famous expression goes, if you aren't paying for the product, you are the product.

This is even common in other Web2 companies that have seen the value of user generated content, which is exactly what user profiles in professional networks end up being. Just like videos in YouTube, landscapes on Instagram, and dances on TikTok, user profiles are the blood that gives life to professional networks. Unlike social platforms, however, professional network users don't get a piece of the billions these companies rake in every year by selling their data. To make matters worse, some professional networks monetize profile data by putting it behind a paywall creating perverse incentives. For example, honest users must pay to see who has looked at their data, while scammers can pay to access data of unwilling participants. For normal users, it's not a justifiable expense, but for scammers and spammers it's an investment with a good return.

Finally, as a decentralized network where the data belongs exclusively to its users, the increasingly insidious practice of centralized corporations that ban users from their platforms for saying or acting in ways that go against their business model will not be an issue. This problem is very well known in traditional social media networks, but that public opinion spotlight rarely shines on professional networks. However, it does happen and more often than one might imagine, as a VICE reporter exposed and lived firsthand when he was banned with no concise explanation, but coincidentally (or maybe not so much) after posting about abusive practices by a large Indian company[7]. He lost access to all his data, posts, and other content, not to mention his professional visibility to would-be employers or other professional connections. Such a scenario could never happen to a Repbase user because each user is the sole owner of their data, which is stored safely and censorship-free in the blockchain.

[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 above, 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. Additionally, Repbase will have built-in incentives that promote the use of the network by all parties, reward those that add value to it, and significantly improve the user experience for all the good faith network participants while at the same time creating obstacles for bad faith actors like spammers, bots and scammers.

Repbase aims to achieve this by bringing together both employers and employees and 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), which are linked to a Soul Bound Token (SBT). The end result is a unique, non-transferable, reliable, up-to-date, and user-owned professional reputation profile (PRP) for each user.

Work Experience Attestation

As described in Chapter II, the most important aspects of a professional reputation profile (PRP) are that it is composed of data that is accurate. To accomplish this in a work experience context, Repbase allows employers to attest the professional achievements of their employees directly on to their PRP. This attestation takes the form of NFTs that are bound to each employee's SBT, which is the key to access all the data contained in the NFTs that compose the 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, a pharmaceutical

company can decide to give out achievements based on the dollar amount brought in by each of their salespeople, or they could both award an achievement that simply recognizes how much of their monthly KPIs each employee completed. 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 richness 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.

In either case, the data that is entered in the system is attested by the employer and is completely accurate and up to date with the current performance of the employees. If for some reason, like human error or bad faith on behalf of the employee, the data that was originally entered is incorrect, the employer can revoke the NFT, and it will be removed from the employee's PRP entirely or removed and replaced with the NFT that reflects what really happened.

Academic Accomplishments and Identity Attestation

Although work experience is certainly a fundamental part of a PRP, it's not the only important part. It's also crucial to be able to attest academic achievements of every type as well as acquired and proven skills. In certain cases, it may also be necessary to know that the owner of the PRP is a real person, or perhaps it's even vital to validate their specific identity. However, unlike the specific case of work experience, Repbase uses two different solutions to resolve these requirements.

The first method is similar to work experience attestations. 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, course, test score, award, publication, or other educational achievement the moment the user attains said achievement. 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? That can easily be the case for many academic actors that simply have other priorities than this kind of integration, those that feel their doing just fine with old technology, or those that charge for transcripts, test scores, or copies of certain types of certifications. This is even more true for identity attestation, since the certifier is usually the

government, where bureaucracy, legacy tech and other priorities are predominant and incentives for integration much harder to find.

For academic and other types of data sources that are not or cannot be integrated with Repbase, users can use Reptokens to get verification on these achievements or identity attestations. These 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. If the trusted third-party provider confirms the user's claim, Repbase certifies the achievement or identity to be valid and grants the PRP the associated NFT.

Privacy, Ownership, and Control of PRP Data

The Repbase approach to professional reputation not only implies that PRP data is accurate, but by the very nature of the blockchain technology Repbase uses, it's also private, owned and controlled by each user. The technology allows the user 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 they can see it.

For example, users could decide to only make one, some, all or no achievements public. They could 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 or friend, or a person they very much want to show their data to, like a recruiter from a company where they recently applied for a job.

The combination of handing users complete control over who sees what data and when they can see it, as well as empowering them to charge anyone they like for the privilege, creates very powerful obstacles against spam. Furthermore, all users are verified on Repbase at some level. That verification can be based on attested work experience, academic accomplishments, or identity verification found on their PRPs. The accuracy of this data adds a considerable amount of reliability to each user, making it extremely hard for scammers and bots to fool 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. Because Repbase is an open protocol, users can develop new applications and communities that leverage the attestations on their PFPs. For example, proving in a talent marketplace they have a certain experience that grants them access to a premium freelancer contract. It is even possible that existing Web2 juggernauts like LinkedIn and ZipRecruiter in the professional social network and recruitment spaces allow users to use 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. First, by participating in Repbase they create an attested reputation that they own, can monetize and use on their terms and is censorship resistant. This allows them to prove to the world their professional abilities and capacities. Second, they earn tokens that will allow them to further enrich their PRP but can also be seen as financial benefits since these tokens can be exchanged in both centralized and decentralized exchanges for other forms of cryptocurrencies. Finally, these benefits are instantaneous, so they don't have to wait for end of quarter/year to reap the rewards of their work, further incentivizing them to focus on performing well over shorter periods of time, which raises 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. However, due to the great benefits that implementing Repbase gives their employees along with the accuracy of the data that is generated, all employers should at least see increased performance from their current workforce and should have an easier time spotting reliable talent they wish to hire. Companies that don't have sophisticated ways to measure performance of their employees can also leverage the Repbase Employer Platform to see who their top performers are. Similarly, companies that don't have an incentive system in place or do could find in Repbase an automated performance incentive program that is different and possibly cheaper than existing incentive programs.

Chapter IV: The Technology That Powers Repbase

Basic Technological Concepts

Soul Bound Tokens and Attestations

One of the best features of blockchains is the ability to spin a near infinite number of new wallets. However, this is a double-edged sword when one wants to use public blockchains for identity solution. Because it's so easy to spin up new wallet address, it can be trivial to create as many fake accounts as a user wishes. This type of problem is what is known as a "Sybil Attack", where a single user creates many fake wallets/accounts to impersonate a larger group of people. This is obviously antithetical to the core idea of Repbase, which is a reputation profile that is only linked to a single person or entity.

To solve the sybil attack problem and create sybil resistance, it has been suggested in crypto communities to create what are known as "Soul Bound Tokens" (SBT), as originally conceived by a group of authors headlined by Vitalik Buterin[8]. Soul Bound Tokens are tokens that are tightly linked to an individual or entity thus making them "soul bound". SBTs effectively solve the sybil problem by providing a verifiable identity for a given wallet on the blockchain. For instance, an organization could hold an on-chain vote, but only those members that hold a specific SBT indicating they are a real person are allowed to participate.

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. It may require the employee to use custom wallet software in order to recover access to their SBTs.

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.

---

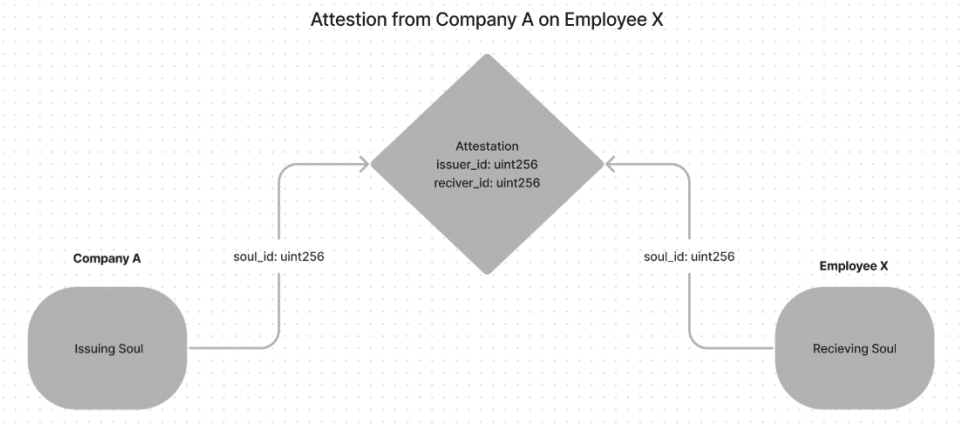
[8] https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4105763_code1186331.pdf?abstractid=4105763&mirid=1

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 wants to use and lets them retain full control over their PRP.

Repbase Primitives

The core of the Repbase Protocol is three constructs: Soul, Attestations, and the PRP. The Soul is an ERC721 NFT that is bound to a specific person or entity. Souls may be transferred between different wallets, but only through the social recovery mechanism. Attestations are NFTs that are bonded to specific souls. Attestations may only be bound to Souls upon their creation, and, most importantly, this bond can never be changed.

A user's PRP is the combination of their Soul and the Attestations they have bound to it. All Attestations are linked to two Souls, the one belonging to the issuer of the Attestation, and the Soul of the receiver of that same Attestation. For instance, if Company A is issuing an Attestation to Employee X, the issuer of the Attestation would be the soul id of Company A, and receiver of the Attestation would be the soul id of 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 3rd parties to confirm and verify information about users' PRPs.

Privacy, data, and Attestation Verification

The main use of having a PRP is its ability to function as a digital CV, where employees can demonstrate different aspects of their professional reputation, whether that's their degree, previous employer, or any special awards they've potentially received.

In order 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 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 are a relatively new cryptographic tool. They allow for a user to "prove" that a 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 gain entry into 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 in order to generate Attestation proofs, users must be 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 on a daily basis 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. In order to verify to recruiters that they have this certification, they must submit a proof of the scum master Attestation with each of their job applications. Since they are applying to many jobs throughout the week, 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 be connecting and signing 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.

For instance, let's say a company wants to leverage Repbase' s identification system to allow access to their company headquarters. It's not sufficiently secure to generate a single proof for entry to the building, because if an attacker got a copy of this proof, they could also use it to gain access using what is known as a replay attack. As a result, a new proof needs to

be generated every day for security purposes. An employee could generate a soul shard that only has the required Attestation for entry to building attached to it. This could then live in a hot wallet on their phone and allow them to generate a proof when they need to enter the building. Since there are no other attestations attached to this Soul Shard, if their wallet is compromised the attacker won't gain access to any of the other data in their PRP, and the user can reject the soul shards permissions using parent Soul NFT.

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, only a hash of the attestation details is actually published onto the chain. This allows the protocol to preserve privacy, but also allow for on-chain verification of attestation claims.

Since this data is stored off chain, one may wonder why the use of a blockchain is necessary. After all, there are already off-chain identity specifications that have been defined, such as the W3C verified credential specification.

The reason the Souls and Attestations must be published on-chain is to show the origin of the Attestations. While specs such as verified credentials do partly solve the problem, they don't create a compelling solution to how we can know with certainty that a given key belongs to a specific entity. By publishing part of the data on-chain, this lets us leverage what blockchains are really good at, which is an immutable ledger that shows history of provenance.

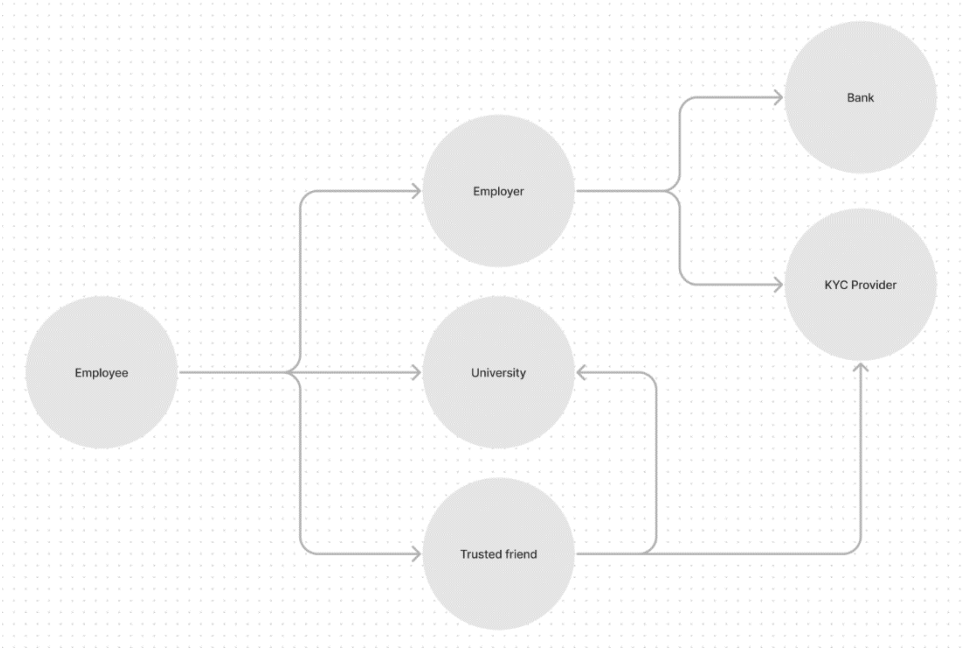
Wallets and Attestation Ownership

Since the Soul is the core aspect of the Repbase Protocol, being able to recover the Soul in the event of hacks or lost private keys is an essential protocol feature. 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.

Within the crypto industry, many are familiar with 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 end 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.



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.

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 strong with the more participants it has.

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. This allows the owners to have an added protection mechanism against identity theft. After their Soul has been frozen, they may only un-freeze it by going through the social recovery process.

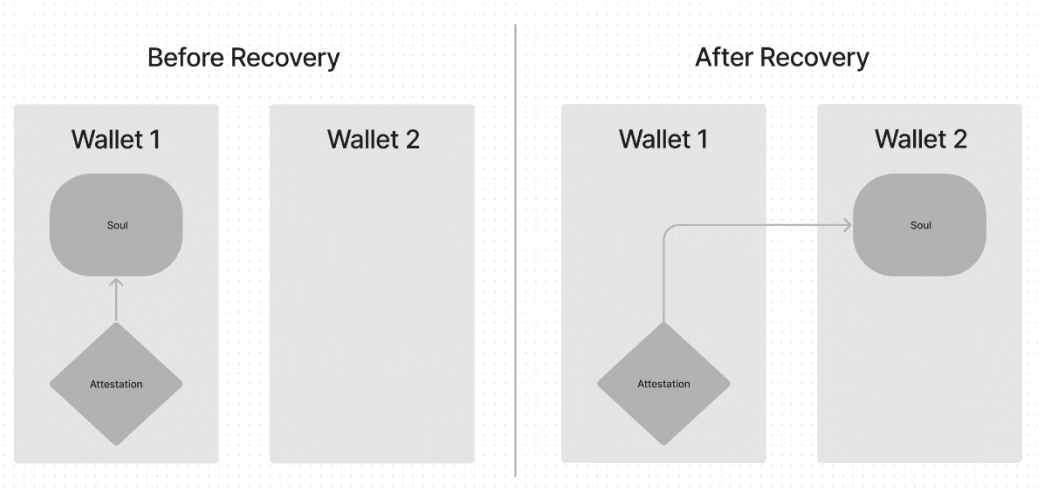
The social recovery steps would be as follows:

1. A user freezes their Soul.
2. The user reaches out to their Recovery Committee to begin the recovery process. This can be an automated process or an interpersonal one depending on the user and how their Recovery Committee was built.

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 a sufficient number of 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. Somewhat counterintuitively, 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 that a user is the owner of a specific Attestation is the bond between that Attestation and the ID of a Soul that they own.

This is an essential feature, as there are a wide variety of 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 compossibility. 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 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 through 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. To this day, many DAOs and other blockchain organizations struggle to solve on-chain voting problems due to sybil attacks. Web2 KYC is often onerous, repetitive, and vulnerable to fraud. Deepfakes and AI generated profiles are increasingly difficult to detect. Current anti-fraud solutions 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.

Chapter V: Governance

Repbase DAO Overview

As a native Web3 company, the founding team at Repbase is strongly inclined toward the creation of a decentralized structure to oversee the most crucial aspects of the future of the network. In that spirit, we propose that a Decentralized Autonomous Organization is the correct path for Repbase to take. To avoid bots, uncommitted participants, or users that could just buy their way to impose their will on the community, only PRPs that have invested in a personhood attestation will be allowed to vote, and each one of these PRPs will have single vote.

Our technological and product visions allow us to avert such a fate. In the Repbase DAO, votes will not be counted based on a user's Reptoken count, nor will every PRP have a vote. To avoid bots, uncommitted participants, or users that could just buy their way to impose their will on the community, only PRPs that have invested in a personhood attestation will be allowed to vote, and each one of these PRPs will have single vote. This allows us to guarantee that the PRPs participating in the most crucial decisions for the DAO are actual (i) a single individual, (ii) actual humans, and (iii) users that have invested into verifying their personhood, thus proving their commitment and belief in the Repbase vision.