The Reputation Value Chain

[Simon Brown](#)

[Follow](#)

--

Listen

Share

Introduction

Web3 ecosystems can benefit hugely from establishing a robust and credibly neutral reputation layer. There are a number of ways we can think about what this looks like, but lets start with what an ecosystem needs in terms of what a reputation layer could provide:

- People need a way to find high quality dapps, DAOs and communities that are relevant to them, based on their interests and values.

- Dapps need a way to find product-market-fit, and to do this they need some analytics to tell them what sort of customers are out there, and what those customers want, what communities their customers are members of, where they are based etc.

- Dapps need a way to convince individuals they are trustworthy, and individuals need a way to establish some level of trust in a dapp, without relying on a review system run by a centralized intermediary that will likely develop mis-aligned incentives (as we've seen in web2).

- Dapps and DAOs need a way to prevent sybils and bots, which just end up pushing out real users.

- Dapps and DAOs need a way to reward loyal customers / members without incentivizing airdrop-hunters who aren't going to stick around and who just create noise.

And as well as that:

- We need all of the above without needing someone to store a giant database of people's data, or to to change the order of search results or alter trust scores in return for payment, or to censor results based on requests from the government in some jurisdiction. Basically, it needs to be credibly neutral.

- We also need a way to try to protect people from having their PII put on an immutable public ledger without their consent by unscrupulous actors.

How do we get everything we need from a robust reputation layer without repeating the problems that we've seen with reputation systems in web2? e.g. lack of transparency, mis-aligned incentives, ulterior motives, and mis-information.

The Reputation Value Chain

A reputation layer will likely be composed of a number of different actors in a value chain. A mental model for the value chain for reputation can viewed as thus:

To break down this value chain a bit more:

- Users

are individuals or organizations that derive some value fom their reputation. Reputation can mean many things, but we could think of it like an individual's LinkedIn Profile, a company's Glassdoor profile, a service or product's TrustPilot score etc. There is a wide variety of ways in which reputation can be valuable and many form it can take.

- Issuers

enable data points to be created, so for example, a provider of an online course is an issuer of a certificate that attests to completion of the course. In web3 this can be a dapp that provides proof-of-humanity, a dapp review, a badge for completing a quest etc.

- Reputation Protocols

provide the algorithms that derive some summary data or score from the aggregate of the data created by the issuer's of

attestations. They focus on the inbound logistics of acquiring raw data from many sources. Their "manufacturing process" involves applying custom algorithms to the aggregate data to derive valuable reputational data, and then distributing that reputational data to customers (which sometimes involves them being an issuer).

- Dapps / DAOs

harness the summary reputation data created by RPs to understand their customers and members better, to develop product-market-fit and attract customers that align with them, to improve customer retention and customer loyalty, and to reward members that contribute and add value and to make their UX better.

The following section goes into more detail about the various actors in this value chain and the roles they play in the reputation layer of an ecosystem.

Actors in the Reputation Value Chain

Credential / Attestation issuers

These are the teams that are issuing credentials / claims / attestations. These can be broken down into to broad groups:

Trusted Issuers

These are issuers that attest to something and sign off on it. They do this through the form of a Verifiable Credential, or some sort of SBT or on-chain attestation. I've called them trusted issuers because it usually requires the verifying party to trust the issuer to some degree. An example of this is a KYC service, or it could be as simple as an online course that offers a qualification or certification, for which is issued a credential or attestation.

Trustless Issuers

There are a number of teams that have developed solutions based on sophisticated cryptography, that can create credentials / attestations based on a zero-knowledge proof, usually derived from a TLS session with some other web2 service. They can attest to anything from your Twitter handle, to your bank balance, to the number of Uber rides you've taken. The verifying party doesn't trust the issuer directly, but rather they trust the original datasource and the fact that the technology that the issuer has developed is open-source and peer-reviewed, and leverages MPC or TEEs so that the user is in full control and maintains complete privacy.

Projects that have developed this sort of technology include, Clique, PADO Labs, zkPass, Reclaim Protocol, Chainlink (via DECO), and of course the original TLS Notary by the PSE group in the Ethereum Foundation.

Reputation Protocols (RPs)

These are actors that index data from both on-chain and off-chain sources and compute a reputation score or reputation profile based on some algorithm. These reputation scores are focused on a variety of use cases, ranging from credit scores, to developer profiles, to web3 analytics, to smart contract / dapp trust scores etc. Below are some examples:

- Trusta Labs is an RP that provides very sophisticated reputation management for individuals, and analytics for dapps. Individuals can analyze their on-chain behavior and assess their value score across five dimensions (Monetary, Engagement, Diversity, Identity, Age). They can also visualize your progress on their web3 journey and discover more.

- {r}elinkd is an RP that has developed a sophisticated blockchain addresses scoring protocol and dapp, that has been built for creating a trustworthy digital identity layer. They also issue these reputation scores as both Verifiable Credentials and SBTs.

- Aspecta is an RP that allows individuals to link their valuable data across GitHub, Twitter, Stack Overflow, MetaMask, etc. and to unlock a unique Aspecta ID. This allows individuals to aggregate Web2 & Web3 footprints into an AI-generated reputation profile. They are one of the few RPs to leverage AI, and are arguably the leader in this regard.

- HAPI is an RP (and much more) specializing in security and risk profiling. Their decentralized security protocol that detects and prevents malicious activity in the blockchain space. It utilizes external and on-chain data to provide accurate information on compromised wallets and malicious activities and can be integrated into DEXes and DeFi protocols to prevent money laundering and enhance cybersecurity.

- dappSheriff is an innovative RP that provides trust scores to dapps based on user feedback and reviews. Each review incorporates the number of transactions and number of contracts that the reviewing wallet has interacted with, with respect to the dapp being reviewed.

- ReputeX — web3 analytics platform that helps developers to understand users and user behavior based on on-chain activity, as well as aggregating reputation data from other RPs.

- RociFi is an RP and issuer of credit score attestations as NFCS (non-fungible credit scores).

- [Masa](#) are issuers of the Masa Credit Score Soulbound Tokens (MCS SBTs, in and uses Cred Protocol's web3 credit scoring technology as it's RP.

- [Morfyus](#) are both an RP and an issuer . They issue attestations called "Kreds", which have a reputation score that grows as users connect, complete work, and receive recommendations.

- [Kleoverse](#) is a similar RP and issuer. They provide "Skill Scores" which aggregate a user's relevant achievements, including GitHub contributions, courses taken, and projects built. Kleoverse then issues attestations called [Badges](#) which are issued as SBTs.

- [SOURC3](#) is a decentralized, on-chain platform for reputation management, that allows developers to build on-chain reputation by giving provenance to GitHub contributions.

- [Nomis](#) is a multichain identity protocol that helps users build, manage, and leverage their on-chain reputation and web3 projects to make data-driven decisions. Nomis scores are derived from a wallet's on-chain activity and are issued as attestation via NFTs. Nomis enables users to leverage their on-chain reputation to get personalized web3 experiences. It also helps dapp developers to offer custom terms, rates and powers to their end-users based on the reputation scores.

- [digitalsocial.id](#) is building trust through non-transferable reputation profiles for digital identities in web3. Individuals initiate some activity such as checking out in a store, making a donation, or undertaking some work. They then connect their wallet before they check out or before making a donation etc., and the protocol issues an attestation as an SBT.

The methods that these RPs use to generate scores or profiles is also quite diverse, from classical reputation algorithms such as [Eigentrust](#) to newer machine learning algorithms.

The sources can also be quite diverse, ranging from on-chain to off-chain data, for example,[Omnid lists 78 different sources](#) for the reputation score. This is an area where registries can complement the data pipelines that reputation protocols build, and can allow them to derive even more powerful reputation data.

Attestation Registries

Attestation registries play an important role in the reputation ecosystem as[verifiable data registries](#), but are well suited for use in web3 because they are decentralized. Furthermore, on-chain attestation registries are directly interoperable with other dapps via smart contracts.

Public attestation registries allow for reputation protocols to build powerful models by being able to discover and index more data faster. They allow for recursive reputation, whereby reputation profiles and scores can be issued as attestations that can be consumed by other RPs.

Currently RPs index data from various on-chain and off-chain data sources. This is quite an overhead considering every on-chain data source has its own idiomatic smart contract with its own specific data structures and function calls. Off-chain data is even more of an overhead, with API authentication and limits and different protocols. Many reputation protocols either maintain their own database of data points or scrape the data on-demand, but developing an integration for every data point requires development effort. This is where being able to retrieve data from consolidated attestation registries makes things much easier, and leads to more powerful reputation algorithms.

Whether a credential / attestation should be on-chain or off-chain is a tricky question.[See below for more details](#).

Dapps, DAOs, Users

In the end, issuers and RPs exist to serve the needs of both individuals and of dapps, DAOs, and protocols, as described at the start of this post. The issuers and RPs create a flywheel of self-reinforcing reputational value, whereby attestation issuers can create data points that help individuals and organizations to find each other, and establish trust using credibly neutral mechanisms.

Using these credibly neutral mechanisms such as on-chain registries, RPs can compose claims / credentials / attestations from an ever increasing number of sources via issuers, and can create more robust and sophisticated reputation profiles and scores. Reputation Protocols can themselves become issuers as they feed back reputation scores as attestations into the registries, creating meta-attestations. Issuers can themselves have reputation profiles / scores, which can help discern the quality of attestations, which in turn makes the reputation protocols stronger.