UniRep: A Protocol for Sharing Credibility Across Anonymous Accounts on Social Platforms

Privacy & Scaling Explorations

December 1, 2023

Contents

1 Abstract

A majority of digital platforms and systems do not permit users to engage anonymously while also retaining the ability to prove credibility on the platform. For example, on Reddit, credibility is determined by the karma system. When creating anonymous accounts, users start with zero karma, reducing trustworthiness. UniRep proposes a solution where users can establish

anonymous profiles, yet provide proof of their aggregate reputation without disclosing which profiles are theirs. This is achieved through epoch-based attestations, where the platform confirms account reputation updates, and users validate their account ownership and updated reputations post each epoch.

2 Introduction

In the digital era, the balance between online privacy and maintaining one's reputation on digital platforms is increasingly complex. Privacy, motivated by security, freedom of expression, or the desire for personal anonymity, is a coveted asset. However, digital platforms, designed around the ethos of reputation-building, often pose a conundrum for users. Positive contributions on these platforms translate to reputational gains, which in turn determine a user's credibility and influence within the community.

Despite the benefits of an established reputation, there are moments when even seasoned users wish to act from behind the veil of anonymity, perhaps to share sensitive insights, provide honest reviews, or act as a whistleblower without risk of retaliation. Presently, the choice is stark: use an established identity or create a new anonymous account, starting from ground zero. New accounts frequently face diminished visibility, community skepticism, and potential flagging by automated systems.

Given this dilemma, there's a clear need for a system that marries the two seemingly contrasting ideals of privacy and reputation. UniRep aims to address this gap, proposing a solution that upholds the sanctity of anonymity while allowing users to leverage their hard-earned reputation.

3 Preliminaries

3.1 Terms and definitions

3.1.1 Attesters

Entities or contracts that provide **attestations** to users, aggregating into user data. In typical use cases, like Reddit, the platform acts as the attester.

3.1.2 Users

Entities that acquire data from attesters and **validate received data**.

3.1.3 Epoch

A cycle in the UniRep system marked by updated state and epoch trees. Attesters determine the epoch duration. User epoch keys can accumulate attestations within an epoch.

3.1.4 Epoch Key

Temporary public identifiers for users.

3.1.5 User State Transition (UST)

A process that combines a user's received data in an epoch to yield a new state tree.

3.2 Assumptions

- The proof system is built on a phase 2 trusted setup.
- Network transaction costs for attestations and user registrations are considered moderate.
- Users retain their reputation data to produce User State Transition proofs.

3.3 Proposed Protocol

The UniRep protocol is designed to function on an epoch-based mechanism, facilitating interactions between attestors and users, primarily for the management of reputations and state transitions. The protocol is implemented via a smart contract, which handles essential operations including registrations, attestations, and the maintenance of various cryptographic trees.

Attesters are joined into the system through the 'attesterSignUp' function, which assigns a unique attesterId. Users also enter the system by registering through the 'userSignUp' function and providing a distinct signup proof.

3.3.1 Epoch Keys

Epoch keys serve as temporary identifiers, regenerated per epoch. They're computed using an 'identitySecret', unique to each user. Epoch keys are stored in the format:

```
const field = attesterId + (epoch << 160) + (nonce << 208) + (chainId << 216);
poseidon2([identitySecret, field]);
```

chain id	nonce	epoch	attester id
36 bits	8 bits	48 bits	160 bits

The ‘nonce‘ is a value between ‘0‘ and ‘numEpochKeyNoncePerEpoch - 1‘ so that users may have ‘numEpochKeyNoncePerEpoch‘ epoch keys per epoch.

Although the data is often simplified as a singular value, it's a complex array, managed through ‘$\text{FIELD}_{\text{COUNT}}$‘ fields, and can be amalgamated via addition or replacement mechanisms.

Generally, the data field so far has been considered to be a single value however it is an array of ‘$\text{FIELD}_{\text{COUNT}}$‘ values that can each be combined through either addition or replacement mechanisms.

As suggested, the addition mechanism provides a summation value and includes a modulo of ‘$\text{SNARK}_{\text{SCALARFIELD}}$‘.

```
data[0] = (old_data[0] + new_data[0]) % SNARK_SCALAR_FIELD;
```

Any data fields that do not use the addition mechanism instead use the replacement mechanism. This mechanism stores the data in ‘205‘ upper bits for the data and ‘48‘ lower bits for the nonce so that the protocol may order the attestations.

3.3.2 User State Transitions

For each epoch, Attesters submit attestations in epoch trees, containing the data changes for each epoch key. While attesters are trusted to provide accurate updates, the protocol ensures user anonymity is preserved making it difficult to provide biased data toward any user.

Users engage in a User State Transition (UST), wherein the proof of several values is required, including a proof of a state tree leaf's presence in the previous epoch's tree, the validity of the epoch tree root, and the state tree root in the history tree. The UST process then requires users to aggregate data from each valid epoch key, outputting the combined data to be added to the new state tree and new epoch keys to be used for the following epoch. If an epoch key is not found in the epoch tree, it will expire.

Following the generation of the UST proof, the proof is submitted on-chain where validations are made to confirm the validity of the proof and check the merkle tree root. The uniqueness of the nullifier is to prevent duplicate USTs.

3.3.3 Data Storage

The data required for the protocol operations is stored in three main trees: The State Tree, the Epoch Tree, and the History Tree.

The State Tree stores the user's state values after signing up and after a UST is performed. Leaves contain the user's 'identitySecret' and starting data in the format:

```
H(H(identitySecret, attesterId + (epoch << 160) + (chainId << 208)), H(data))
```

chain id	epoch	attester id
36 bits	48 bits	160 bits

The Epoch Tree contains the data transitions received by the epoch key in the epoch in each leaf stored in the format:

```
H(epochKey, H(data[0]), H(data[1]), ...H(data[n]));
```

The History tree contains valid combinations of state and epoch tree roots in each leaf stored in the format:

```
H(stateTreeRoot, epochTreeRoot);
```

3.4 Discussion

UniRep's introduction to the digital ecosystem offers a transformative solution to a long-standing issue plaguing social platforms: the challenge of creating anonymous accounts without losing previously accrued reputational capital. In platforms such as Reddit, where reputation (or karma) directly influences the perceived credibility of a user, starting from scratch isn't just an inconvenience but a significant impediment. Anonymity often comes at the cost of trust, leading users to face skepticism and undermining their contributions.

In this report, UniRep has mainly been described as a reputation system. However, since the attestation values can be any chosen data, utility isn't just confined to platforms with explicit reputation metrics like Reddit. Consider GitHub, a platform where user contributions (in the form of code submissions or PRs) significantly benefit from the trust earned by contributors through consistent and quality submissions. By integrating UniRep, maintainers of a repository might be more inclined to trust and accept contributions from anonymous accounts. These contributors, through UniRep, can demonstrate

a track record of credibility from other accounts, ensuring their contributions aren't dismissed outright due to the lack of an attached reputation.

Extending this thought further, an online marketplace could also derive significant benefits from the UniRep framework. Such platforms, such as Etsy or eBay, rely heavily on user reviews and reputations to build trust between sellers and buyers. An experienced seller, looking to branch into a new niche under an anonymous identity, could face challenges convincing potential buyers of their credibility without a visible track record. UniRep can bridge this gap. By allowing sellers to prove a positive history from other accounts without disclosing their identity, buyers can be reassured about the quality and reliability of a product. This approach could revitalize how trust is established and maintained in online marketplaces, granting sellers more flexibility in their operations while ensuring buyers remain confident in their purchasing decisions.

However, while UniRep's potential applications are promising, there are challenges to consider. A primary concern arises from the inherent on-chain actions integral to the system. Depending on the blockchain's transaction fees, costs associated with attestations and user registrations might become prohibitive. This potential economic barrier could deter users and platforms from adopting the system. Hence, it's worth investigating alternative approaches, such as transitioning to a layer 2 solution, which could circumvent these cost-related challenges and make the protocol more accessible.

In summary, while UniRep introduces a compelling solution to the dichotomy of privacy and reputation on digital platforms, its widespread adoption and success will depend on addressing the economic and technical challenges inherent in its design.

3.5 Conclusion

UniRep introduces a novel approach to address the longstanding issue of balancing online privacy with the preservation of reputation on digital platforms. By enabling users to aggregate their reputation across anonymous accounts, the protocol fosters trustworthiness without compromising privacy. As digital interactions continue to evolve, protocols like UniRep are poised to redefine online credibility paradigms.