Build Decentralized Identity Apps with Attestations

This guide explains how to build decentralized identity apps using attestations. It will define attestations and review the benefits of using Ethereum Attestation Service for Optimism developers.

About Attestations

Attestations are signed statements about a person, entity, or thing, made by an individual, company, or organization and are one of the building blocks of decentralized identity.

Our journey towards decentralized identity begins with theEthereum Attestation Service(opens in a new tab), a set of smart contracts for creating, verifying, and revoking on/off-chain attestations. You can think of Ethereum Attestation Service as a multiplayer database for streamlining the attestation process and enabling a robust web of trust on any OP Chain in the Superchain.

Benefits of Using Ethereum Attestation Service

EAS makes it easy to sign any piece of data. In addition, here are a few key benefits:

- Permissionless
- : The AttestationStation is a public contract, which means that it is not owned or controlled by any one person or organization. Anyone can use the contract to verify and attest anything.
- Tooling:
- Indexing, various access-management integrations, and more are already available for the AttestationStation.

Privacy

Attestations create log entries that become part of the permanent record of the blockchain. Here are some best practices to avoid violating users' privacy:

- Obtain explicit consent from users forpersonal information(opens in a new tab)
- , which includes a user's legal name and birthdate.
- Clearlyinform users(opens in a new tab)
- what data is being collected, why it is being collected, and how it will be used.
- Sensitive data should not be stored onchain, in any way.
- If you need a smart contract to verify it in the future, you can use the hash of the sensitive data rather than the data itself.
- Even when storing sensitive data offchain, you need to ensure it is stored securely using encryption, proper authentication and authorization, etc.

⚠ You are encouraged to consult a lawyer or other professional advisors if you are uncertain about your obligations. Global data privacy laws are complex and multifaceted, and the violations of user privacy can have meaningful compliance as well as practical implications.

Common Questions

Q: Are attestations replacements for verifiable credentials?

A: Attestations should not be viewed as a replacement for verifiable credentials or decentralized identifiers. Rather developers can use attestations to createdecentralized identifiers(opens in a new tab), credentials, claims, and more.

Q: Are attestations replacements for proof of personhood?

A: Attestations and the associated web of trust are complementary with proof of personhood like WorldID(opens in a new tab) and similar solutions. Without proof of personhood, agents could sybil-attack the web of trust to build their reputation. On the other hand, web of trust extends proof of personhood to confer more information about the person you're interacting with which is critical in governance and other use-cases that require knowledge of the person's reputation.

Q: Why attestations instead of soulbound / non-transferable tokens?

A: Attestations have two key benefits over soulbound / non-transferable tokens: flexibility of whether the attestations is onchain or offchain and composability. While there is a canonicaldecentralized schema registry for attestations(opens in a new tab) , there is no central registry or specification for soulbound / non-transferable tokens which can lead to poor interoperability between systems and protocols.

Next Steps

Are you inspired and don't know what to build? We have a project idea list(opens in a new tab). Do you have a good idea, but you know you're not the right person to build it? Please open a PR on that list and suggest it.

Overview Contracts (EAS)