Principles & Goals

Suggest Edits

First Principles

Verite's decentralized identity standards aim to satisfy the following design principles:

- Decentralized:
- Requires no central issuing agency and functions effectively in DeFi.
- Persistent and portable:
- Inherently persistent and long-lived, not requiring the continued operation of any underlying organization.
- Cryptographically verifiable:
- Based on cryptographic proofs rather than out-of-band trust.
- Resolvable and interoperable:
- Open to any solution that recognizes the common protocols and data model and requires no one specific software vendor implementation, including any that Circle or its members may create.
- Transparent:
- Identity holders know when and how their identity data is being requested and used.
- Private by design:
- No data correlatable to an identity holder is exposed to a public network, including registry mappings and blockchain persistence.

Goals

Interoperability across the ecosystem is an over-arching Verite goal. There has been no previous industry-wide agreement on how products and services might interoperate in key crypto finance use cases, such as how they represent proof of KYC or accredited investor status. Verite aims to provide clarity by defining these standard connections and providing recipes to illustrate their usage.

Verite's specific tactical goals are to: (a) define data models (schemas) that should be shared and exist as common building blocks for all parties as a public good; and (b) define the protocols for requesting and delivering identity claims in a manner that supports crypto finance use cases.

The intent is to enable any member of the broader crypto ecosystem to develop products and solutions that are inherently compliant and interoperable with each other, and to do so in a manner that is open, transparent, and usable by anyone, whether connected to Circle and the USDC ecosystem or not.

A process goal is to maintain transparency and openness in the iteration of the protocols and data models. Anyone is free to use the source code, modify it, and submit improvements to it.

Non-Goals

- Verite standards do not require use of a specific chain, token, consensus algorithm, wallet, storage system, p2p library, or other fundamental infrastructure.
- Verite aims to specify definitions for claims that can be supported by any identity solution, and to specify protocols that can be implemented by any service, wallet, or application.
- Verite does not require use of any specific Decentralized Identifier (DID) method or new attestation format.
- Verite is not intended as a competing decentralized identity standard; it aims to leverage and contribute to existing (and emerging) decentralized identity standards. Updated3 months ago
- Table of Contents
  - First Principles
  - Goals
  - Non-Goals