Governance Overview

Overview of Verite Network Governance

The design of Verite was optimized for the privacy at various levels, but it was also optimized for flexibility for each actor in the system, to support many different kinds of business arrangements and infrastructural investments. Fundamentally, Verite only thrives (and justifies its complexity) if an organic and resilient ecosystem arises where actors can specialize, discriminate, and profit. Like all ecosystems, we need governance to balance flexibility against liability and reach against fairness. This overviews components of the governance we see as necessary.

Why do we need governance?

In a network with multiple issuers, every VC issued should be on equal footing. This means a VC can be presented across the network with the same level of confidence and veracity, regardless of who issued it and who verifies it

Without common ground about the meaning and value of each VC, the Verite ecosystem will only be as strong as its weakest Issuer or Verifier:

- The network will fragment, i.e., verifiers will only accept VCs from certain issuers
- Fragmentation of reliance means VCs become less portable – which is one of the most important factors aspects of their value proposition
- This will also be a huge barrier to adoption, as widespread acceptance of VCs will be difficult to achieve (or the network will centralize around a single Issuer)

Current State: Boot-strapping an Ecosystem

Verite is currently orchestrated by Circle in close collaboration with its initial implementers, and grounded in feedback from early evaluators who commit seriously to considering our work to date. This is "strategically centralized," in the sense that Circle is currently the hub at the center of major technical and business planning with implementers, but the multi-lateral collaboration has already started in Working Groups, bound by multi-lateral IP/NDA agreements. One such working group is actually focused on roadmapping and elaborating everything that follows; to get involved, reach out to Circle.

Target-State: Three Interlocking Governance Mechanisms

In a scaled ecosystem with multiple issuers and verifiers of differing scales and foci, Verite needs an explicit, detailed governance framework and rulebook that defines how to create, update, and enforce rules and standards that bind the network together legally and technically. These can be thought of as "by-laws" that structure how Verite expands, as community-driven governance gets formalized.

This rule-based governance will be key to making Verifiable Credentials, and the business relationships they represent, portable and interoperable, and thus to achieving mass adoption.

Verite governance will have three primary components: (1) the Governance Framework, (2) the Rulebook, and (3) the Network Utilities.

The Governance Framework

TheGovernance Framework refers to a standing body of humans representing organizations (companies, non-profits, and/or DAOs), who together make decisions about Verite. This includes an authoritative Verite Governance Board and the more dynamic Verite Working Groups that spin up and wind down on a "project basis" to add technical, business, product, and/or legal features to Verite as a whole.

The Verite Governance Board should authorize new Working Groups, which produce standards and technical artefact. One such working group is already working on a Rulebook (detailed below) that governs and binds key ecosystem participants. When Working Groups present upgrades to an already-functioning Verite system in production, this can create breakage (technical and economic) for participants; for this reason, the Governance Board's primary duty is to make decisions about these changes. Specifically, the Governance Board votes to accept changes to standards and rules that protect the technical and regulatory integrity of the Verite ecosystem.

Detailed Remit

The governance framework will define (not exhaustive):

- The legal structure of the Verite consortium
- The eligibility criteria for participating in the Verite consortium
- How IP / CLAs / open source is managed

- How working groups are structured, who can participate, and what do they do
- How standards are created and agreed on
- How updates and extensions to the standards are agreed on
- How the rulebook is created and agreed on
- How the rulebook is updated and agreed on over time
- How decisions are made, what decisions are made, who can make decisions
- Onboarding and offboarding policies and procedures
- The consortium's business model – pricing, fees, expenses etc

Network Utilities

The "Network Utilities " that power Verite provide common services to all participants and end-users in the Verite ecosystem.

The first and most structural network utility is theTrusted Identity Registry . The Trusted Identity Registry defines which Issuers and Verifiers can be trusted to adhere to Circle Verite Standards. It functions as an "key directory" providing authoritative key material to prevent phishing or impersonation within the system. As Verite scales up, it will also include up-to-date information on conformance testing, to facilitate real-time decision making about the trustworthiness and roadworthiness of each actor's implementation and credentials. Circle reserves the right to remove actors from the Registry if they have not signed the Rulebook or have been judged by the community not to be honoring it.

Detailed Remit: Trusted Identity Registry

Circle will build, maintain, and publish the Trusted Identity Registry that includes Issuers and Verifiers which have applied for and been approved by the Verite Governance Board to join the registry. Entities in the registry adhere to technical, operational, legal, regulatory, and compliance standards defined by Verite Governance Board. Verifiers and Issuers in the registry must sign a Verite Rulebook which defines the rights, obligations, standards, reps & warranties, etc that they must adhere to. The rulebook dictates the conditions under which a VC can be issued, verified, and or/revoked The Verite Governance Board can elect to remove entities from the registry if they fall out of compliance with the rulebook. Each one is identified by a Decentralized Identity (DID) from a supported DID method, that is listed in a machine-readable registry published on Github and in an Ethereum smart-contract for on-chain use-cases.

Verite Rulebook

As the network expands and hits the market "in production", all of this will have to be formalized: not just the governance between issuers and verifiers, but also the liabilities and obligations from issuer to end-user to consumer/relying party. These various kinds of relationships will be circumscribed and specified by rules, the sum of which can be periodically published as a versionedVerite Rulebook .

This rulebook structures the relationships, expectations, and limits of all the actors in the system. Most crucially, however, it governs and bindsIssuers andVerifiers , who must sign a contract to uphold it and stay within its limits to stay in the Trusted Identity Registry over time.

Detailed Remit

The Verite Rulebook will cover a number of different topics, including but not limited to:

- Definitions of who can and cannot be issued a verifiable credential
- Regulatory standards that must be adhered to for issuing different types of VCs
- Standards/rules for the processes an Issuer must follow to perform KYC/B and Accredited Investor checks
- Standards/rules for the processes an Issuer must follow to perform to issue other VC types
- Standard/rules for the processes a Verifier must follow to verify VCs
- Rules for how long should VCs be valid for and for how often should KYC/B be redone on an existing holder.
- Standards/rules for when a VC should be revoked, the process and SLA for revoking it, and how others are notified
- Defines manager(s) of the Trusted Identity Registry, the eligibility criteria for inclusion, criteria and processes for removal for the registry, etc.
- Defines how liability is allocated across various participants and network utilities
- Define who has recourse and whom do they have recourse against and the terms of that recourse
- Representations and warranties of participants that signers commit to uphold
- Technical standards which, in being adhered to, sustain and protect the integrity of the ecosystem
- Financial requirements of the issuers/verifiers
- SLAs for the network utilities (e.g. uptime, resiliency, latency, etc) Updated3 months ago
- Table of Contents
-
    - Why do we need governance?
-
    - Current State: Boot-strapping an Ecosystem
-