The Past Year with Verite

A Year in Review Suggest Edits

The Past Year with Verite

In 2022 Verite launched, laying a strong foundation for the collaborative work and opportunities ahead. This post highlights milestones reached as well as new discoveries, research directions, and ongoing conversations.

Compliant Membership

We remain laser-focused on solving the use case of Membership Proofs. These proofs attest that a specific blockchain address has undergone a set of compliance requirements and this credential can be verified in a privacy preserving way that limits identifiable data either on-chain or on the open web.

Our research into this use-case uncovered complexity and diversity among on-chain decentralized applications and the varying degrees of credentials needed for these membership proofs. This led us to support parallel technical variations and form-factors.

The original architecture of Verite was modeled as a 3-actor system: 1) issuers of KYC status credentials, 2) end-users who directly choose to whom they want to show those credentials, and 3) dApps which operate their own verification services to receive offchain credentials, which, after validating them, pass decisions off to their frontends or smart contracts.. As part of our user research, we decided to shift from a 3-actor and add support for a 4-actor (see #2 below)

1. Some consumers only wanted to consume membership proofs on-chain, emphasizing the importance of continuing to enable membership proofs on-chain.
2. Other smart-contract-based consumers want to outsource their protocol's policy governance (usually based on roughly defined policies, and expected to be refined over time) to a single service, with an expectation of real-time monitoring and complete separation of concerns. Essentially, "relying parties" wanted a new, fourth actor (which we've been calling "verifier services") to handle verification for them, and hand off decisions rather than data.
3. There was widespread acknowledgement that these services will need to be retooled over time as regulatory requirements and reliance frameworks evolve – policies enforced by verifier services needed to be changeable much more quickly than code deployment, and more often.
4. Nearly everyone we spoke with was concerned about centralization and silos forming, at the new verifier services level in particular. There is a deep, shared desire for services to be interoperable between end-users, meanwhile making the barrier to entry for running these services as low as possible, providing a larger and more decentralized on-chain customer-base.

Previously, Verite's designers assumed that on-chain activity could be gated by on-chain inputs or artifacts containing minimal Personally Identifiable Information (PII), with heavier PII contained in the off-chain Verifiable Credentials (VCs), but the further we delved into the customer requirements of on-chain platforms, the more it became apparent that this approach would not fit into the desired technical or business models better suited to the constraints above. Even if there was no Personally Identifiable Information (PII) in the Verifiable Credentials, there was still too much data, risk of potential liability, and custodianship of "data points" (if not of PII) for the comfort of some relying parties.

Governance and Compliance

The role of governance in the system shifted substantially over the past year. When the work began, we thought Verite would only require a simple feedback loop between relying parties. We constructed a schema design for the contents of the Verite credentials which would be issued and/or validated by verification services. What we discovered, though, was that sometimes verification services were owned by an individual instead of byrelying parties), necessitating more complex governance frameworks for this growing network.

In particular, we worried that on-chain communication would be the hardest to align on given the business model pressures of this new 4-actor model. While "schema design", as we had been calling it, sounded like a relatively simple technical question of data modeling, it turned out to be a far more complex beast across different chains of reliance and architectural variants.

For this reason, less schema design happened in Circle-hosted working groups than we had expected. As end-to-end products continue to evolve, this kind of alignment could perhaps be premature, and many Verite partners have opted to defer this kind of harmonization until after there is significant adoption and traction. The schemas published so far are adequate to geographically-limited launches of the initial use-case, and as the sphere of supported geographies and use-cases expands, or as more players enter the space and demand grows for federation and interoperability, we look forward to truly viable self-governance. In the meantime, we will continue technical research and design work that falls into four categories:

1. On-chain Design
2. Architectural Design & Adoption

3. Technical Standardization
4. Additional Use-Cases

Ongoing On-Chain Research

One of the most active working groups Verite hosted over the last year was the On-Chain Best Practices group, which zoomed in on the "last mile" between the on-chain consumers relying on Verite to deliver safe addresses and the off-chain verifiers handling all the messy details and off-chain data with privacy and nuance. This group focused on the subtle difference between Verification Results (verbose, subject-identifying, necessarily off-chain and archival for reporting and legal reasons) and Verification Records (concise, anonymized, essentially just a log entry or a pointer to archival results documentation). Only the latter can go on-chain, thus requiring enough detail for on-chain relying parties to act. The former, however, enables all the flexibility and nuance needed for a policy engine, a data translation layer, and a federation of competitors.

Two Verite on-chain researchers and a few academics cooperated on a synthetic comparison of architectures represented in today's compliance market. Outlined and discussed at the 2022 Rebooting the Web of Trust (RWoT) conference in The Hague, these researchers produced a functional taxonomy for apples-to-apples and apples-to-oranges comparisons of various products and ecosystems. The result was a thorough lightpaper laying out where Verite fit in the broader landscape of on-chain identity with and without verifiable credentials.

Zooming in even more on the relationship between on-chain consumers and identity-enabled on-chain tokens, Keith Kowal from the Hedera-focused research team at Swirlds Labs wrote up another useful primer . It focuses on where on-chain tokens do and don't fit the "soul-bound" model for a "decentralized society," as well as how on-chain artifacts can and cannot meet the requirements of compliance in today's jurisdiction-based and centralized society of laws.

As products launch and evolve in the marketplace, this group remains confident that alignment on incrementally more technologically prescriptive guidance will be valuable, leading to shared interfaces and shared security models as federations form. For this reason, Verite's most active working group plans to keep meeting and designing on-chain registries and smart contracts across multiple languages and blockchain environments.

Ongoing Architectural Design

The RWoT lightpaper linked above implicitly compared the Verite architecture to simpler end-to-end products already active in the DeFi space today, but this comparison only works at a certain level of abstraction. Verite has actually forked into two separate-but-equal architectures over the last year and our collaborative research team works hard to keep feature and use-case parity between the two.

The original Verite design assumed an end-user either using two separate (an identity wallet and a crypto wallet), or a "fat wallet" controlling both a private and portable Decentralized Identifiers (DIDs) and one or more blockchain private keys. This defined our initial schemas, and the original Verite implementation guide imagines multi-chain Crypto wallets adding support for a DID in much the same way they handle adding support for a new blockchain or private-key type to be able to handle private, DID-based off-chain VCs. This "SSI" (self-sovereign identity) and "Crypto" dual-wallet is a cornerstone of the "Web5" approach , allowing SSI for next-gen (and post-cookie!) Web2 use-cases, strong privacy and pseudonymity for Web3 use-cases, and even a few carefully guard-railed bridges between the two. While we fully endorse this approach long-term, we are waiting for more implementation interest and DeFi demand to further prototype technical artifacts for this "fat-wallet" architecture.

In the meantime, a simpler architectural pattern (outlined in detail in a prior blog post) emerged in prototyping work with Circle Engineering: an address-based credential , issued not to a DID controlled by a specific wallet client, but to an address (which might even be controlled from multiple wallet clients). This enables a different path to wallet support, piggybacking on the WalletConnect version 2 upgrade cycle to get wallets implementing lightweight, "minimum-viable" support for verifiable credentials without the need to handle DID keys or complex VC-specific protocols.

In the coming months, expect to see the Wallet Connect instructions on the Verite documentation expanded and entries added to other pages as more wallets roll out support for Verite credentials via Wallet Connect rails. This is a major ongoing research topic with Circle and WalletConnect, testing the hypothesis that thin wallets want to stay thin just as much as dApps wants to stay ignorant of the identities of their users (even in compliant products).

Ongoing Technical Standards Contribution

It bears repeating often that Verite is not a product or a solution, but rather a prototype and a "cookbook" for overlapping DeFi ecosystems. As such, a key design goal for Verite from the beginning was to invent as little new technology as possible and use standards-track building blocks wherever possible to maximize interoperability between competitors and sustainability of technical decisions, two crucial ingredients in any sustainable ecosystem.

Verite might best be described as a "protocol" in the technical sense: a new way for wallets, users, and dApps to communicate directly. Or to be more precise, Verite could be seen as a "profile" and sample implementation of the more general-purpose and open source Presentation Exchange specification at the Decentralized Identity Foundation . The nuts and bolts of crypto-wallet adoption, off-chain VC presentation, and signing involves representing VC use-cases at the Chain-

Agnostic Standards Alliance (CASA).

The bedrockW3C data model specification on which all VC work depends is currently being iterated and Verite plans to take advantage of new features and improvements with time.

Ongoing Research Towards Other Use Cases

While the focus has always been on privacy-preserving exchange of off-chain credentials to enable on-chain reliance, lots of doors are opened by the adoption of Verite building blocks for other credentials. We've discussed:

- "Travel Rule" use-cases
- and the role of VCs in a more open-world version of today's VASP-to-VASP discovery and exchange protocols (led by Nota Bene)
- "Heavier" credentials expressing not just membership but actual personal information for cross-organization de-duplication or identification, or in its more complex formulation, "reusable on-boarding" and "portable identity verification"
- Identity assurance for verifiable credentials, leaning on existing Web2 trust frameworks or "holder-binding" mechanisms for ensuring the actual person identified and onboarded is the same person presenting the credentials later, whether they be "membership" credentials or those categorized as more high-stakes
- Zero-knowledge mechanisms for generating a verification record in the wallet that can be sent to an on-chain relying party, which would bring us back to the fat-wallet, 3-party model

Each of these directions presents new possibilities and venues for future work, technological and otherwise. There are no timelines or commitments in place, as how each of these research directions pans out depends on how the work done thus far finds its way to market and wallet adoption. Updated5 months ago * Table of Contents * * The Past Year with Verite * * * Compliant Membership * * * Governance and Compliance * * * Ongoing On-Chain Research * * * Ongoing Architectural Design * * * Ongoing Technical Standards Contribution * * * Ongoing Research Towards Other Use Cases