Introduction

Verana Whitepaper: Verifiable Trust and Public Registries

Abstract

The internet today faces critical issues related to trust, identity fraud, phishing, and privacy violations due to reliance on centralized, non-verifiable identity systems. This whitepaper introduces **Verifiable Trust (VT)**, underpinned by the **Verana Verifiable Trust Network**, providing decentralized, secure mechanisms to establish trust between users, services, and AI agents.

Problem Statement

Traditional internet services utilize **public identifiers** such as emails or usernames, which are inherently vulnerable to misuse. Users **lack reliable methods** to verify service identities, exposing them to **fraud** and **phishing attacks**. Centralized authentication processes empower large intermediaries, limit user control, and compromise privacy. Additionally, direct service-to-service interactions, including AI-to-AI communications, lack standardized authentication mechanisms, resulting in **fragmented and insecure trust models**.

Solution: Verifiable Trust

Verifiable Trust provides an open, **decentralized trust** layer using cryptographic verification via Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). VT replaces **implicit trust with explicit**, **verifiable cryptographic proofs**, creating **secure**, **interoperable connections** across users, services, and decentralized AI agents. It also enables content provenance by integrating with the C2PA standard, allowing content signed by DIDs to reveal ownership upon trust resolution.

Components of Verifiable Trust

- **Verifiable Services (VS):** Decentralized services, including AI agents, identified by resolvable DIDs, providing verifiable credentials in their DID Documents for proving claims to peers, serving as the basis for identifying providers and establishing connections.
- **Verifiable User Agents (VUA):** User-facing software (e.g., browsers, wallets) establishing connections with peers (VSs or other VUAs) and presenting verifiable credentials upon peer requests after establishing a trusted communication channel. VUAs themselves verify peer credentials and perform trust resolution.
- **Proof-of-Trust:** A verification summary evaluated directly by VSs or presented visually by VUAs, detailing peer legitimacy, ownership, and credentials.

Verifiable Public Registry (VPR)

The first implementation of a VPR is the **Verana Verifiable Trust Network**. The VPR serves as a decentralized "registry of registries," providing foundational support to Verifiable Trust ecosystems by offering:

- **Trust Registry Management:** Enables ecosystems to define credential schemas, roles (Issuer Grantors, Verifier Grantors, Issuers, Verifiers), and permission policies.
- **Standardized APIs:** Facilitate real-time trust resolution queries by VSs and VUAs.
- **DID Directories:** Allow decentralized service discoverability, essential for indexing and querying services.

Trust Registry and Credential Schemas

Each trust registry maintains:

- **Credential schemas** for structured data and permissions management.
- Defined roles and governance structures, facilitating autonomous yet interoperable ecosystems within the broader VPR network.

The **Verana Foundation** will create a trust registry within the Verana Verifiable Trust Network, defining Essential Credential Schemas required for basic trust resolution. Specifically, the Foundation will select trusted issuers for the **Organization**, **Person**, **UserAgent**, and **Service** schemas, laying the groundwork for robust trust resolution.

Economic Model

The VPR employs a tokenized model comprising:

- **Trust Deposits:** Financial guarantees backing participant integrity, generating yields, and subject to penalties for non-compliance.
- **Transaction Fees:** Covering operations including credential issuance, verification, and registry management.
- **Economic Incentives:** Rewards for ecosystem participants, user agents, and trust deposit holders to encourage participation and compliance.

Governance

Verana features a dual-layer governance system:

- **Global Governance Framework (GF):** Governs overarching network rules, fee allocations, penalties, and operational policies.
- **Ecosystem Governance Frameworks (EGFs):** Allow ecosystems to independently define and enforce their specific governance rules, enhancing autonomy while ensuring global interoperability.

Use Case Example

A user employs a VUA-based social browser, establishing a trusted connection with a VS, such as an influencer channel. The VUA resolves the DID of the VS, performs trust resolution by checking the VS credentials presented in the DID Document and performing VPR queries, and presents a Proof-of-Trust to users so they can verify channel owner identity and its reputation. Similarly, decentralized AI agents operating as VSs authenticate each other through essential credential verification, enabling secure inter-agent collaboration.

Roadmap

- **Phase 1 (completed):** Deploy testnet of the Verana Verifiable Trust Network, including DID Directory and foundational credential schemas.
- **Phase 2:** Verana Foundation establishes a trust registry for Essential Credential Schemas (Organization, Person, UserAgent, Service), selects trusted issuers, and develops SDKs, VS libraries, and standardized query APIs.
- **Phase 3:** Mainnet launch of the Verana Verifiable Trust Network, accelerated ecosystem onboarding, decentralized governance, and expanded support for decentralized AI, content provenance, and advanced user-to-user trust scenarios.

Conclusion

Verifiable Trust, underpinned by the Verana Verifiable Trust Network, represents a paradigm shift in internet security, enabling secure, transparent, and privacy-preserving digital interactions across users, decentralized services, and AI agents. By leveraging cryptographic verification and decentralized governance, Verana delivers scalable trust, verifiable ownership, and robust infrastructure for a trusted digital ecosystem.