# Shadowgraph: A Hyperdimensional Social Graph for Cryptographically Verifiable Trust and Predictive Identity

Oliver C. Hirst (Steake)
*Shadowgraph Labs*

October 2025

### Abstract

**Shadowgraph** is a decentralized trust fabric that fuses zero-knowledge machine learning, decentralized public key infrastructure (DPKI), and evidence-based subjective logic (EBSL) into a single hyperdimensional reputation substrate. It represents an epistemic re-foundation of digital identity — a network where belief, uncertainty, and reputation are treated as first-class mathematical objects, dynamically updated through cryptographically verifiable interactions.

Through a layered architecture consisting of an overlay network, self-sovereign identity system, decentralized data marketplace, and predictive intelligence layer, Shadowgraph transforms the way humans, agents, and machines reason about trust. It is not merely a social graph, but an *evolving topology of belief* — where every edge encodes evidence, and every node embodies a living hypothesis of integrity.

# Contents

**1 Introduction** **4**

**2 Architectural Overview** **4**

2.1 Design Philosophy . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

2.2 System Layers . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

**3 Overlay Network** **6**

3.1 Reputation-Space Topology . . . . . . . . . . . . . . . . . . . . . . . . 6

3.2 Gossip and Synchronization . . . . . . . . . . . . . . . . . . . . . . . . 6

**4 Decentralized Public Key Infrastructure (DPKI)** **6**

4.1 Social Key Recovery . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

4.2 Zero-Knowledge Attestation . . . . . . . . . . . . . . . . . . . . . . . . 7

**5 Evidence-Based Subjective Logic (EBSL)** **7**

5.1 Opinion Model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

5.2 Fusion Operator . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

5.3 Discounting Operator . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

5.4 ZK-Constraint Enforcement . . . . . . . . . . . . . . . . . . . . . . . . 8

**6 Self-Sovereign Identity (SSI)** **8**

6.1 Belief Tensor Field . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

**7 Data Marketplace** **8**

7.1 ZK-Provenance Exchange . . . . . . . . . . . . . . . . . . . . . . . . . 8

7.2 Privacy-Preserving Valuation . . . . . . . . . . . . . . . . . . . . . . . 9

**8 Predictive Algorithms** **9**

8.1 Trust Propagation Network . . . . . . . . . . . . . . . . . . . . . . . . 9

8.2 Temporal Smoothing . . . . . . . . . . 9
8.3 Anomaly Detection . . . . . . . . . . 9

**9 Applications 10**

9.1 Reputation-Gated Airdrops . . . . . . . . . . 10
9.2 Verifiable Credentials . . . . . . . . . . 10
9.3 P2P Credit and Microfinance . . . . . . . . . . 10

**10 Philosophical Context 10**

**11 Conclusion 11**

# 1 Introduction

In the twenty-first century, *trust* has become the most valuable — and most abused — digital commodity. Platforms centralize it, markets monetize it, and governments attempt to regulate it. Yet in all cases, the mechanism remains brittle: binary, opaque, and coercively custodial.

**Shadowgraph** was conceived as a corrective — a new substrate for digital civilization, where reputation is measurable but not ownable, where privacy is absolute yet participation remains verifiable, and where the mathematical structure of belief itself forms the core of coordination.

At its heart lies an equation:

$$\text{Trust} = f(\text{Evidence}, \text{Uncertainty}, \text{Time})$$

subject to cryptographic constraints, predictive modeling, and social recursion. Shadowgraph operationalizes this function across a distributed peer-to-peer overlay, yielding a *computable epistemology* — a global nervous system of probabilistic trust.

# 2 Architectural Overview

## 2.1 Design Philosophy

Shadowgraph's design is grounded in three axioms:

1. **Evidential Grounding:** Every statement about identity, reputation, or behavior must be backed by evidence, weighted by uncertainty.
2. **Cryptographic Verifiability:** All computations of trust must be provable in zero-knowledge, without revealing private data.
3. **Predictive Continuity:** Trust should evolve according to learnable dynamics, forming the foundation of stable governance and coordination.

These axioms yield a system that is neither social network nor blockchain per se, but a *reflexive trust organism*: a network that continuously learns what it means to trust.

## 2.2 System Layers

The system architecture is composed of six layers:

[tikz,border=10pt]standalone tikz

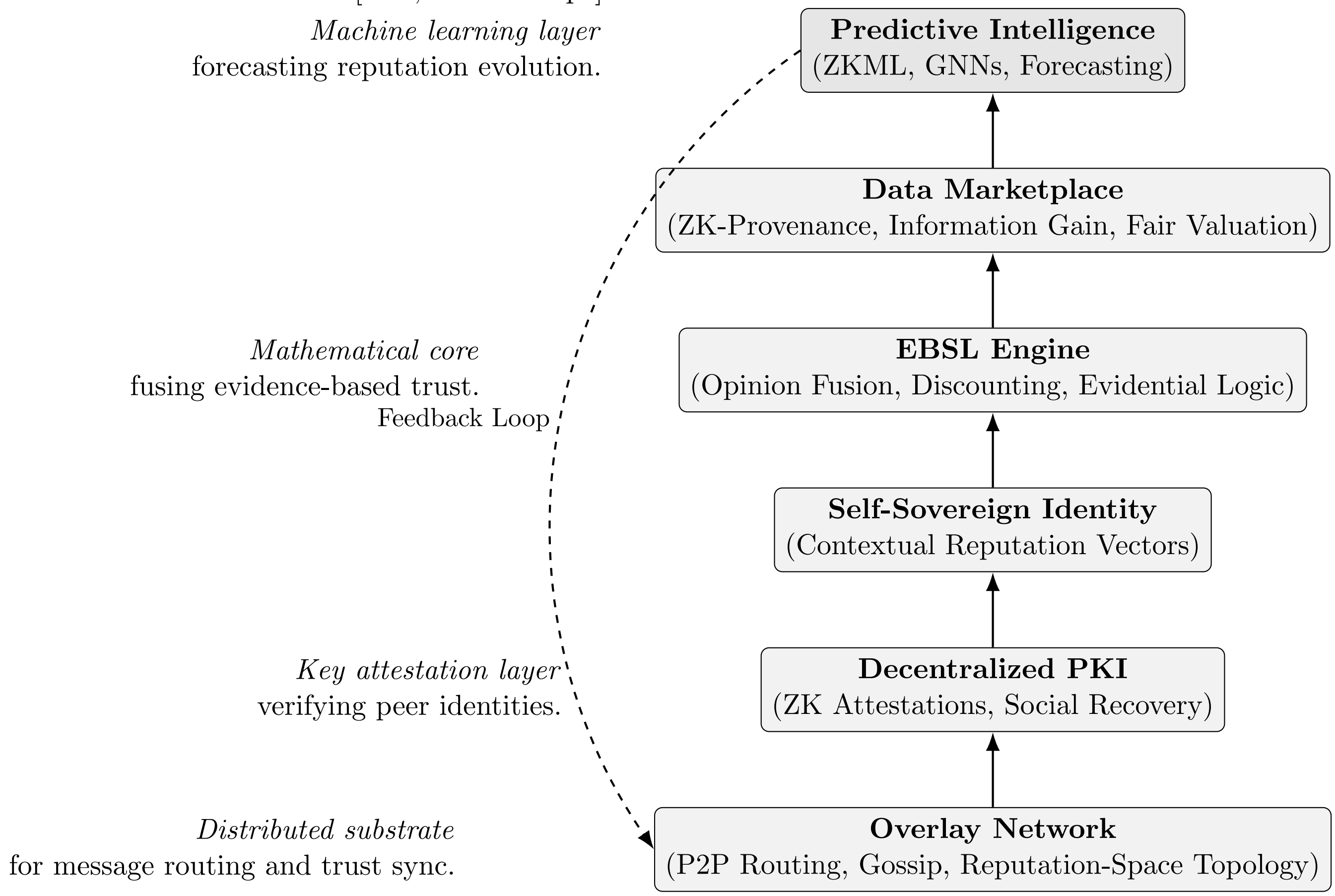
*Machine learning layer*
forecasting reputation evolution.
**Predictive Intelligence**
(ZKML, GNNs, Forecasting)
**Data Marketplace**
(ZK-Provenance, Information Gain, Fair Valuation)
*Mathematical core*
fusing evidence-based trust.
Feedback Loop
**EBSL Engine**
(Opinion Fusion, Discounting, Evidential Logic)
**Self-Sovereign Identity**
(Contextual Reputation Vectors)
*Key attestation layer*
verifying peer identities.
**Decentralized PKI**
(ZK Attestations, Social Recovery)
*Distributed substrate*
for message routing and trust sync.
**Overlay Network**
(P2P Routing, Gossip, Reputation-Space Topology)

Figure 1: Layered architecture of the Shadowgraph system. Each layer feeds its outputs into the next, forming a recursive feedback loop of evidence and inference.

1. **Overlay Network** — The decentralized routing and state layer, organizing agents into a semantically optimized topology.

2. **Decentralized Public Key Infrastructure (DPKI)** — A self-healing, socially verifiable key management system.

3. **Self-Sovereign Identity (SSI)** — Identity represented as an evidential probability distribution rather than a fixed credential.

4. **EBSL Engine** — The mathematical substrate of belief fusion and uncertainty propagation.

5. **Data Marketplace** — A ZK-verified incentive layer for exchanging provable information.

6. **Predictive Intelligence** — The network's emergent reasoning layer, forecasting reputation trajectories and detecting anomalies.

# 3 Overlay Network

The overlay network functions as the topological foundation of Shadowgraph, maintaining a distributed graph of nodes that exist in *reputation space* rather than physical or IP space.

## 3.1 Reputation-Space Topology

Nodes $V = \{v_1, v_2, \ldots, v_n\}$ form a directed weighted hypergraph $G = (V, E, W)$, where edges represent evidential assertions:

$$E_{ij} = (\text{opinion}_{ij}, t, \text{context})$$

and $W_{ij} \in [0, 1]$ encodes the credibility weight of the link. Routing is governed by a probabilistic distance metric:

$$P(u, v) \propto \frac{1}{1 + d_{rep}(u, v)}$$

where $d_{rep}$ is the semantic distance in reputation vector space.

## 3.2 Gossip and Synchronization

The overlay employs a consensus-free synchronization model (inspired by CRDTs and probabilistic gossip), ensuring eventual consistency of reputational data even under partial connectivity or censorship.

# 4 Decentralized Public Key Infrastructure (DPKI)

Traditional PKI centralizes authority in certificate issuers. Shadowgraph redefines this model as a decentralized, self-verifying trust web.

Each entity $i$ holds a keypair:

$$(k_{pub,i}, k_{priv,i}) \in \mathbb{G}_1 \times \mathbb{G}_2$$

anchored to a decentralized identifier (DID) and maintained through peer attestations:

$$A_{ij} = \text{Sign}_{k_i}(\text{Trust}(i \rightarrow j, \omega))$$

where $\omega$ is an evidential opinion tuple.

### 4.1 Social Key Recovery

Keys can be regenerated by quorum-weighted recovery:

$$k_i' = f(k_{rec}, \{S_j\}_{j \in T_i}) \quad \text{s.t.} \quad \sum_{j \in T_i} R_j \geq \tau$$

where $R_j$ is the reputation weight of trustee $j$ and $\tau$ a minimum credibility threshold.

### 4.2 Zero-Knowledge Attestation

Each attestation is verifiable in zero-knowledge:

$$\text{VerifyZK}(A_{ij}, \pi) = 1$$

without exposing raw trust values or identity attributes.

## 5 Evidence-Based Subjective Logic (EBSL)

### 5.1 Opinion Model

Each opinion $\omega$ about proposition $X$ is a quadruple:

$$\omega = (b, d, u, a)$$

with belief $b$, disbelief $d$, uncertainty $u$, and base rate $a$, satisfying:

$$b + d + u = 1, \quad b, d, u \in [0, 1].$$

Expected probability:

$$E(\omega) = b + a \cdot u.$$

### 5.2 Fusion Operator

Opinions from independent sources combine via:

$$\omega_1 \oplus \omega_2 = \left( \frac{b_1 u_2 + b_2 u_1}{k}, \frac{d_1 u_2 + d_2 u_1}{k}, \frac{u_1 u_2}{k} \right), \quad k = u_1 + u_2 - u_1 u_2.$$

### 5.3 Discounting Operator

Trust propagation across multiple hops employs a discounting operator:

$$\omega_{ik} = \omega_{ij} \otimes \omega_{jk}, \quad b_{ik} = b_{ij} b_{jk}, \ u_{ik} = 1 - b_{ik}.$$

### 5.4 ZK-Constraint Enforcement

ZK circuits enforce:

$$b + d + u = 1, \quad 0 \leq b, d, u \leq 1,$$

allowing verifiers to confirm opinion integrity without disclosing data.

This ensures the *mathematical honesty* of the trust graph.

## 6 Self-Sovereign Identity (SSI)

In Shadowgraph, identity is not a document or token — it is a *state of belief*. An agent $i$ is represented by a dynamic reputation vector:

$$R_i = [r_{i,1}, r_{i,2}, \ldots, r_{i,n}]$$

where each dimension corresponds to a trust context (e.g., technical reliability, social integrity, temporal consistency).

The identity space evolves as:

$$R_i^{(t+1)} = \beta R_i^{(t)} + (1 - \beta) f(E_i^{(t)}),$$

where $E_i^{(t)}$ denotes accumulated evidence and $\beta$ controls memory persistence.

### 6.1 Belief Tensor Field

The Web of Trust thus becomes a tensor field:

$$\mathcal{T}_{ijk} = P(\omega_{ij} | C_k),$$

where $C_k$ represents context (financial, social, or epistemic domain).

This forms the foundation for self-sovereign, adaptive, and portable digital identity.

## 7 Data Marketplace

### 7.1 ZK-Provenance Exchange

Every dataset or contribution $D_i$ is registered by its provenance hash:

$$H_i = \text{Hash}(D_i || \text{metadata} || t).$$

Value is assigned according to *information gain*:

$$\Delta I = I(D_i; G) = H(G) - H(G|D_i),$$

weighted by contributor reputation $R_i$:

$$p_i = \alpha \cdot \Delta I \cdot R_i.$$

### 7.2 Privacy-Preserving Valuation

Buyers can verify model validity via ZKML proofs:

$$\text{VerifyZK}(\text{Model}, \pi) = 1$$

without accessing raw data or model weights, ensuring both privacy and fairness.

## 8 Predictive Algorithms

### 8.1 Trust Propagation Network

A graph neural network (GNN) operates over the EBSL graph:

$$h_v^{(l+1)} = \sigma\left(\sum_{u \in N(v)} W^{(l)} h_u^{(l)} + B^{(l)}\right),$$

yielding latent embeddings that encode belief flow and opinion dynamics.

### 8.2 Temporal Smoothing

Reputation volatility is stabilized via exponential smoothing:

$$R_i^{(t+1)} = \beta R_i^{(t)} + (1-\beta) E(\omega_i^{(t)}),$$

reducing susceptibility to short-term manipulation or Sybil bursts.

### 8.3 Anomaly Detection

Deviation is detected using Z-score metrics:

$$z_i = \frac{R_i - \mu_R}{\sigma_R}, \quad |z_i| > \theta \Rightarrow \text{flagged as anomaly.}$$

**Algorithm 1** Dynamic Reputation Update Procedure

```
Require: Prior state $R_i^{(t)}$, Evidence set $E_i^{(t)}$
Compute local opinion: $\omega_i \leftarrow \mathrm{EBSL}(E_i^{(t)})$
Fuse neighbor opinions: $\omega_i' \leftarrow \bigoplus_{j \in N(i)} \omega_j$
Compute expected belief: $E(\omega_i')$
Update trust: $R_i^{(t+1)} \leftarrow \beta R_i^{(t)} + (1 - \beta) E(\omega_i')$
if $|R_i^{(t+1)} - R_i^{(t)}| > \epsilon$ then
    Flag node as anomalous
end if
```

# 9 Applications

## 9.1 Reputation-Gated Airdrops

Eligibility is determined by EBSL-weighted reputation rather than raw wallet metrics:

$$\mathrm{Eligible}(i) = \begin{cases} 1, & R_i \geq \tau, \\ 0, & \text{otherwise.} \end{cases}$$

This prevents Sybil farming and aligns token issuance with authentic contribution.

## 9.2 Verifiable Credentials

Credentials are privately provable via ZK attestations:

$$\mathrm{VerifyZK}(\mathrm{Claim}, \pi) = 1,$$

eliminating the need for trusted intermediaries.

## 9.3 P2P Credit and Microfinance

Trust vectors function as decentralized credit scores:

$$r_i = r_0(1 - \lambda R_i),$$

enabling adaptive loan rates, staking requirements, and cooperative risk sharing.

# 10 Philosophical Context

Shadowgraph reimagines identity as an *epistemic waveform* — a superposition of trust states constrained by cryptographic reality. It is an inversion of the surveillance paradigm: where traditional systems extract identity, Shadowgraph *emits verifiable uncertainty*.

By combining symbolic reasoning (EBSL), statistical inference (ML), and cryptographic verifiability (ZK), it manifests a new category of network: a *computational epistemology* that learns from its own trust dynamics.

In doing so, it transforms the social graph from a static map of relationships into an evolving field of belief, continuously recalibrating what it means to be known, to be credible, and to be human.

## 11 Conclusion

**Shadowgraph** is not merely infrastructure — it is a living theorem. It proposes that digital society can self-organize around verifiable belief, predictive reputation, and consent-driven identity.

Where blockchains made history immutable, Shadowgraph makes trust computable. It is, ultimately, a map of faith rendered in math — a hyperdimensional mirror of our collective epistemic state.

## Acknowledgements

The author acknowledges the foundational work of Audun Jøsang on Subjective Logic, the EZKL team for their contributions to ZKML, and the wider decentralized identity community for providing the intellectual ecosystem from which Shadowgraph emerged.

## References

[1] Jøsang, A. (2001). A Logic for Uncertain Probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3), 279–311.

[2] EZKL Team. (2024). *Zero-Knowledge Machine Learning Framework*. GitHub Repository.

[3] Hirst, O. C. (2025). *Evidence-Based Subjective Logic in ZKML Identity Systems*. Shadowgraph Technical Report.