Decentralized Society (DeSoc): Souls, SBTs & a peek at Tokenized Equities

Enrico Pezzano, 4825087

Thesis. Non-transferable attestations (Soulbound Tokens, SBTs) encode identity & reputation on-chain. We'll discuss the DeSoc vision and briefly see how tokenized equities implement a similar idea for compliance.

Agenda

- What DeSoc/SBTs are and why they matter
- Use cases and key mechanisms
- Bootstrapping DeSoc: standards, privacy, recovery
- Case studies and open problems
- Bridge: tokenized equities (compliance attestations, DvP)

Problem: Assets without Identity

- Blockchains excel at **scarce assets** (fungible tokens, NFTs), but are weak at **social identity** (who, history, trust).
- Missing primitives:
  - under-collateralized lending
  - sybil-resistant governance
  - reputation-based communities

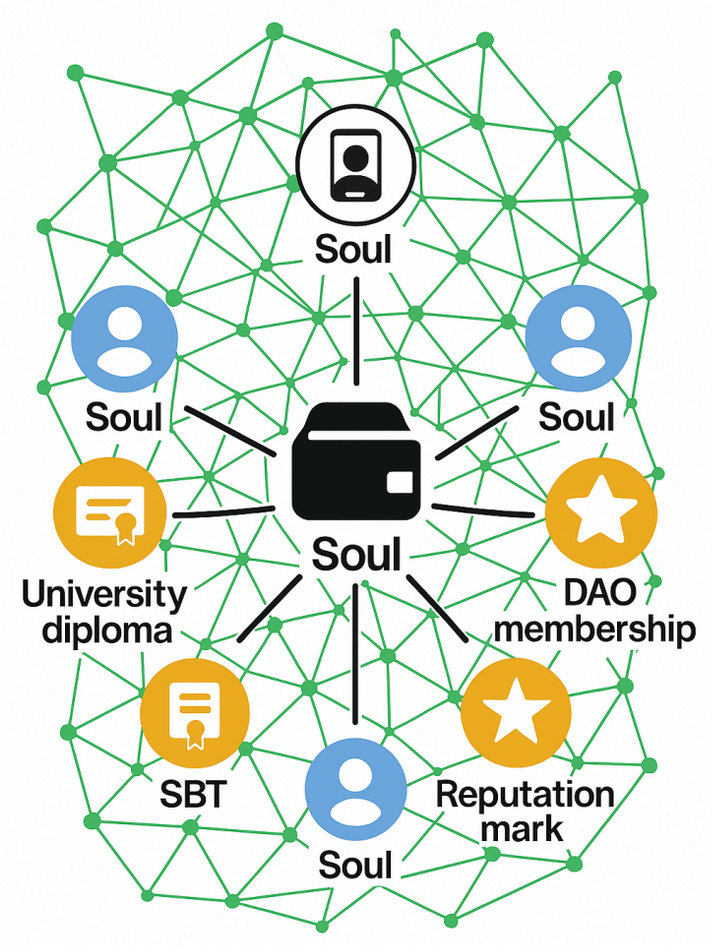
Can we add identity to Web3 without re-centralizing trust?

Core Idea: Souls & Soulbound Tokens

- **Soul**: account/wallet (often pseudonymous) that accumulates relationships over time.
- **SBT**: non-transferable (issuer-revocable, we'll see this later) attestation bound to a Soul; like an on-chain CV entry.

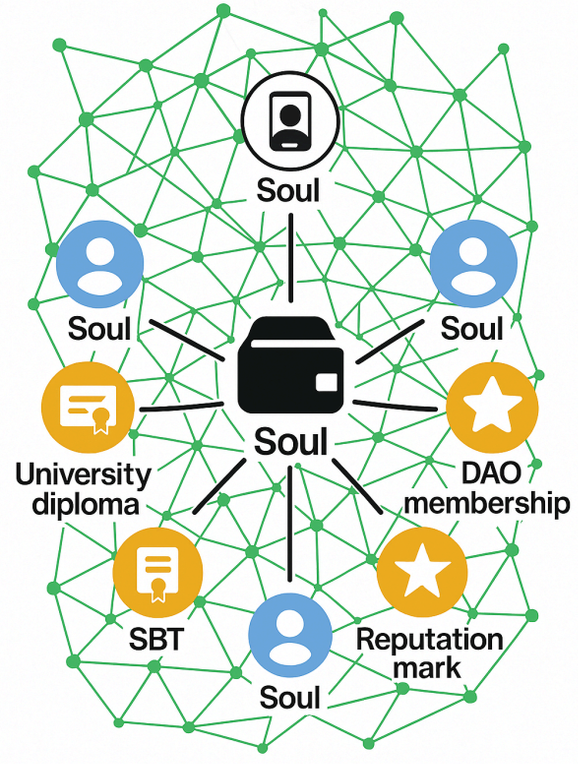
Examples

- Educational credential; employment/affiliation
- DAO membership or contribution badge
- Reputation marks (e.g., on-time repayment)

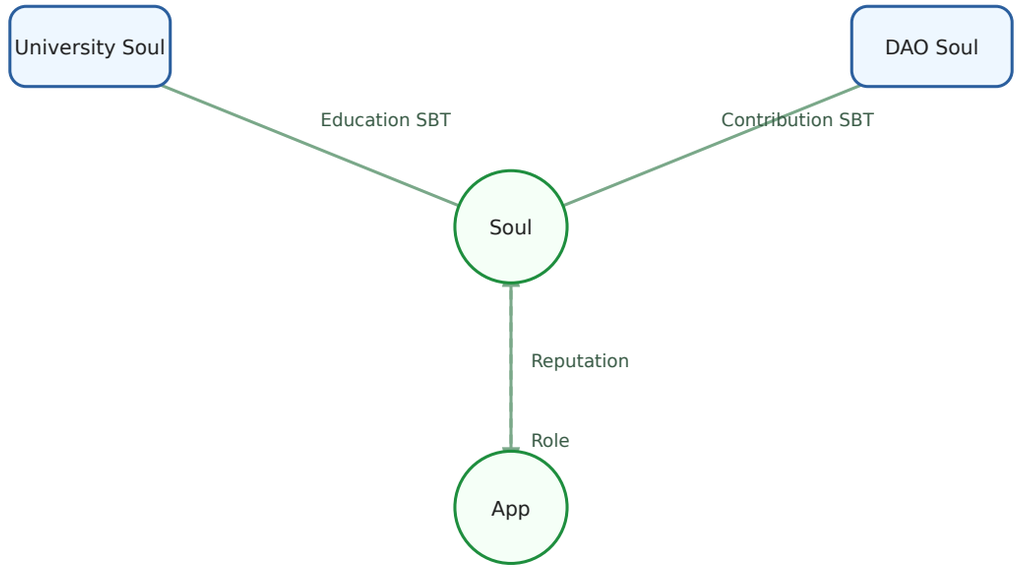


Core Idea: Attestations & Composability

- Self-claimed or, more powerfully, issued by counterpart Souls (people, DAOs, institutions).
- A composable **web of attestations** enabling provenance and reputation directly on-chain.
- Queryable trust graphs that other apps can build on.



Core Idea: Web of Attestations



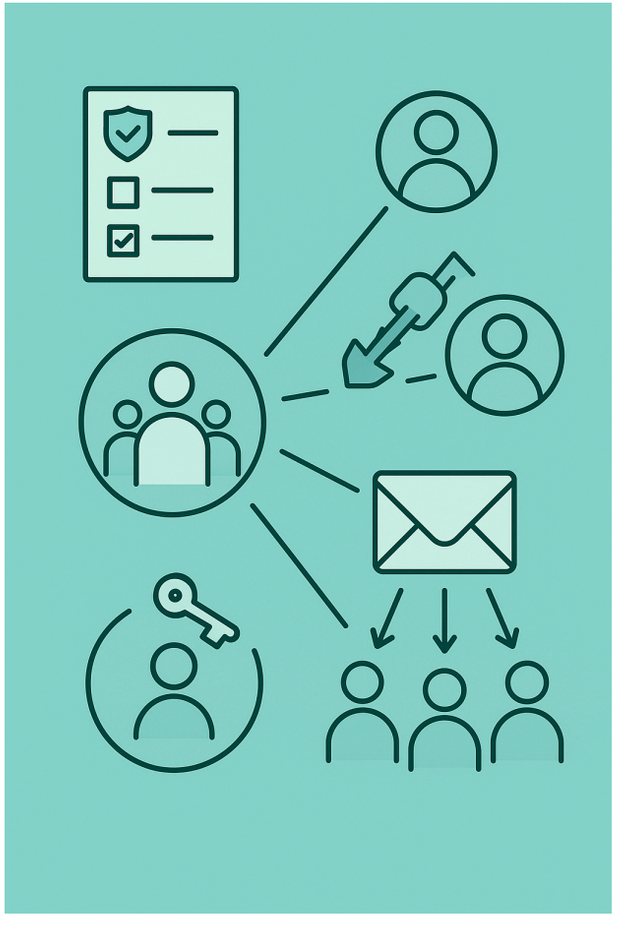
Issuers attest to Souls; apps read and write roles, composing a web of trust.

Stairway to DeSoc: provenance → soul lending → community recovery → measuring decentralization (correlation-aware)

Use Cases I: Finance & Reputation

- **Soul lending**: under-collateralized credit using attestations (e.g., repayment history, affiliations).
- **Provenance**: creators/artists stake identity; collections and scarcity attested as SBTs.
- **Reputation graphs**: cross-issuer attestations compose into richer, queryable trust signals.

Use Cases II: Governance & Communities



- **Sybil resistance**: voting/participation weighted by diverse attestations, not just coin holdings.
- **Correlation discounts**: reduce influence of tightly correlated clusters to deter capture.
- **Community recovery**: social key recovery via trusted circles when a Soul loses access.
- **Souldrops**: targeted distributions to Souls with relevant, verifiable contributions.

Mechanisms: Privacy & Plurality

- **Programmable plural privacy**: commit on-chain, keep data off-chain, prove properties via ZK without revealing PII (personally identifiable information).
- **Plural sensemaking**: combine attestations, AI, and markets for contestable collective judgments.
- **Revocation/expiry**: issuers can revoke or time-limit SBTs; clients verify freshness at use-time.
- **Measuring decentralization**: use correlation-aware metrics built from SBT graphs.
- **Quadratic funding/voting with discounts**: account for correlation to resist plutocratic capture.

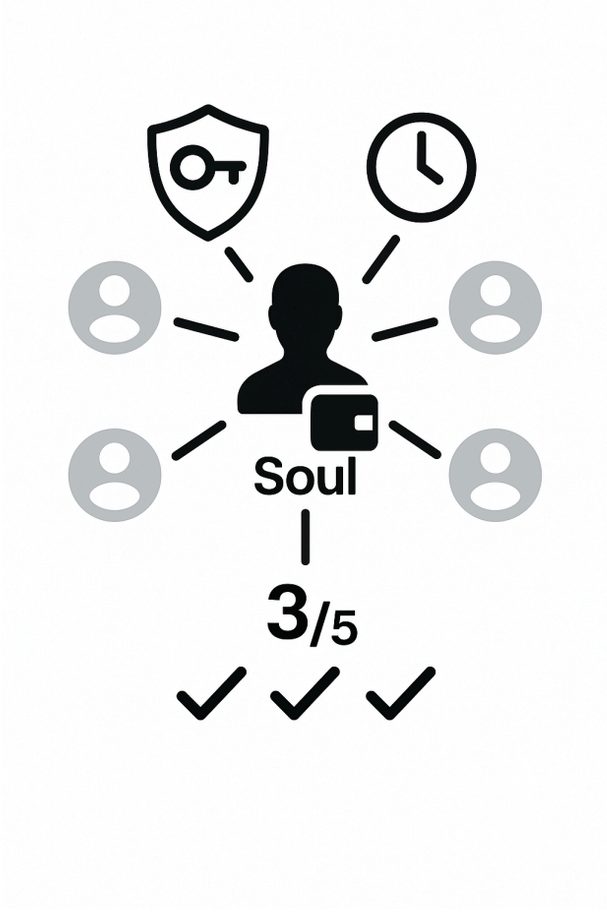
Limitations & Risks

- **Privacy leakage & coercion**: public SBTs may expose sensitive affiliations; + coercive demands.
- **Issuer collusion & low-quality attestations**: requires governance and audits.
- **Harassment & exclusion**: potential misuse for BlackMirror-style “social credit” systems, blacklisting, or targeted harassment.
- **Recovery abuse**: community recovery can be exploited by colluding or malicious guardians.
- **Bootstrapping**: …

…Bootstrapping DeSoc: What Exists Today

- Early building blocks (§5, §7):
  - **On-chain** attestations/POAPs/registries.
  - **Off-chain** VCs with on-chain anchors.
- Design principles:
  - Start public, then add privacy (commitments/ZK).
  - Prefer **issuer** attestations; check revocation/freshness.
  - Iterate issuers & revocation norms toward stronger privacy.

Community Recovery



- **Guardians**: nominate trusted peers or institutions as recovery guardians (SBTs).
- **Threshold**: t-of-n approvals, with a timelock to deter abuse.
- **Scope**: rotate keys and rebind identity only; no asset moves.
- **Auditability**: public intent, delay, and revocation path.
- **Role**: mid-step in the stairway to DeSoc.

Case Studies

- **EAS**: generic attestations; schemas, revocation, on-chain queries.
- **Gitcoin Passport**: sybil-resistance from multi-source stamps; early correlation-aware scoring.
- **POAP badges**: event attendance attestations; simple, transferable format evolving toward non-transferable use.
- **DAO badges/roles**: governance gated by non-transferable credentials and contribution history.

Bridge: From Souls to Securities

- In real finance, **tokenized equities** (security tokens) already rely on **attestations**.
- **Compliance as code** …
- **Wallet as credential holder**: attestations + expiry/ revocation decide transferability.
- Atomic **Delivery-versus-Payment** → avoid settlement risk.
- **Parallel to SBTs**: non-transferable credentials gate actions.

Tokenized Equities: Standards

- **ERC-1400 family**
  - Partitions (e.g., restricted vs public tranches)
  - Operator roles (registrar/transfer agent)
  - Document links & error signaling
- **ERC-3643 (T-REX)**
  - Compliance contract per transfer: `canTransfer(from, to, amount)`
  - ONCHAINID identity; off-chain credentials, on-chain refs

Both enable programmable compliance on public chains.

Tokenized Equities: Compliance as Code

```
fn _update(address from, address to, uint256 value) internal override{
  if (from != address(0) && to != address(0)) {
    (bool ok, string memory reason) = comp.canTransfer(from, to, value);
    if (!ok) revert ComplianceViolation(reason);
  }
  super._update(from, to, value);
}
```

- It transfers check eligibility (KYC, jurisdiction, investor type, lockups, sanctions).
- If attestations are valid → transfer settles.
- If expired / revoked / jurisdiction fails → transaction **reverts**.
- This embeds **permissioned rules** on **permissionless rails**.

Tokenized Equities: Benefits & Trade-Offs

Benefits

- **Atomic DvP**: cash & stock settle in one transaction → no principal risk.
- **Cross-border distribution**: global cap table, local rules in code.
- **Corporate actions as code**: dividends, voting, cap-table updates.
- **Machine-auditability**: regulators verify events, not PDFs.

Trade-offs

- **Liquidity fragmentation**: whitelists constrain venues.
- **Legal overhang**: shareholder rights remain off-chain.
- **Privacy vs auditability**: data minimization vs supervision.
- **Retail benefit limited**: post T+1, marginal gains for typical investors.

Bridge: From Theory to Practice

DeSoc (“theory”)

- Identity: Soul + non-transferable tokens
- Use: governance, reputation, recovery
- Privacy: ZK proofs & correlation-aware metrics

Tokenized equities (“practice”)

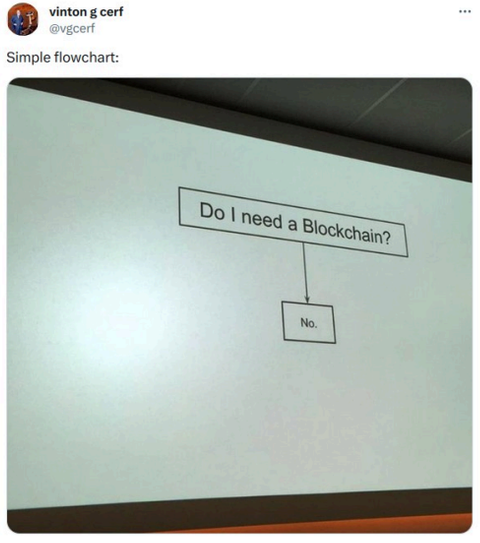
- Identity: wallet + eligibility credentials
- Enforcement: compliance checks at transfer
- Operations: DvP; corporate actions as code

Both on public, permissionless blockchains

DeSoc - Critical Reflections :)

- **User tendency to centralization**
- Sybil attacks vs. democracy
- **Red flags** and **scams**

- **DeSoc downsides**
  - Stigmatization and exclusion
  - Attestation quality and issuer bias
  - Collusion and correlation in governance
  - Cross-chain linkability of identities
  - Privacy leakage and revocation usability



Latest News 📰

September Developments (2025)

- **Nasdaq pushes to launch trading** of tokenized securities Reuters, Sept 8
- **Figure raises $787.5M in US IPO** - blockchain lender goes public Reuters, Sept 11
- **BlackRock seeks to tokenize ETFs** after Bitcoin fund breakthrough Bloomberg, Sept 11

Impact & Implications

- Traditional finance embracing tokenization at scale
- Infrastructure providers (Nasdaq) building rails
- Institutional adoption accelerating beyond crypto

Takeaways

- Attestations are only as strong as issuers and revocation.
- Non-transferable ≠ risk-free: design for privacy, coercion, correlation.
- Compliance gates can work on public chains; law and operations still rule.
- Code is not law: test, audit, monitor; contracts do what we wrote.
- No one seems to care about tokenized stocks, despite their benefits [6][SEC].

Stairway to DeSoc: provenance → soul lending → community recovery → decentralization metrics (correlation-aware)

Thanks for the attention

Questions?

References

[1] Buterin, V., Hitzig, Z., Weyl, E. (2022). *Decentralized Society: Finding Web3's Soul*. papers.ssrn.com

[2] Lecture 21: Are Blockchains Any Good? - Prof. MDA & Prof. MR

[3] ERC-1400 Security Token Standard (Partitions, Operators, Documents). github.com/SecurityTokenStandard.

[4] ERC-3643 (T-REX) and ONCHAINID documentation. erc3643.org · github.com/onchain-id/documentation

[5] Atomic Delivery-versus-Payment (DvP) patterns for tokenized assets. CPMI (BIS) report: bis.org/cpmi/publ/d163.htm · PDF

References (2)

[6] Zero-knowledge KYC / Verifiable Credentials on public chains (surveys and implementations). Spec: w3.org/TR/vc-data-model · Impl: Polygon ID docs

[7] r/DeFi. “Why does no one seem to care about tokenized stocks, despite all of their benefits?” reddit.com/r/defi

[8] Finance Magnates. “Could Tokenized Stocks Bring Volume to the Market?” financemagnates.com

[9] YouTube. “Tokenized equities explained: How xStocks are changing the digital economy.” youtube.com/watch?v=OpiyVve5URM

[10] SEC (United States Securities and Exchange Commission). “Framework for ‘Investment Contract’ Analysis of Digital Assets.” sec.gov