

# Soulbound Tokens: Building a Decentralized Society

Based on the paper "Decentralized Society: Finding Web3's Soul" by Weyl, Ohlhaver, and Buterin

**Presenter:** Mahdi Mirzahosseini (s5436927)

**Date:** September 16, 2025

# The Problem: Web3's "Trust Gap"

Today's Web3 is "**hyper-financialized**". It excels at financial transactions but struggles to represent complex social relationships, identity, and trust. This reliance on purely financial primitives creates a significant "trust gap" in the decentralized ecosystem.

This gap often leads to a dependency on centralized Web2 systems (like social media for verification) to establish reputation, counter-intuitively centralizing aspects of identity in a decentralized space.

# The Solution: Souls & Soulbound Tokens (SBTs)



## Soul

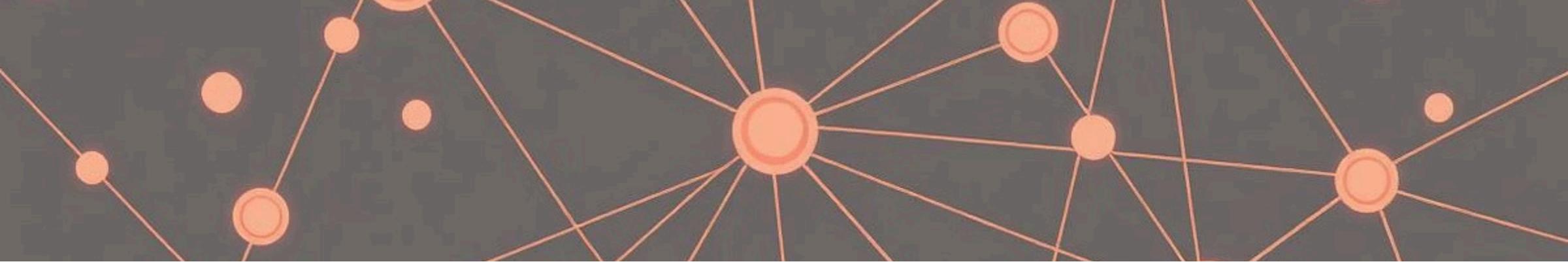
A **Soul** is a wallet or account that acts as the persistent locus of identity within a Decentralized Society. It's designed to accumulate and hold Soulbound Tokens.



## Soulbound Token (SBT)

An **SBT** is a non-transferable digital token representing a commitment, credential, or affiliation. Unlike NFTs, SBTs cannot be sold or transferred, making them intrinsically tied to a Soul.

SBTs are foundational to building a rich, verifiable, and decentralized digital identity for individuals and entities.



# How It Works: The "Web of Trust"

SBTs are issued by one Soul (e.g., a community, an institution, or another individual) to another Soul to attest to a specific relationship, skill, or achievement. This creates a rich, interconnected graph of verifiable claims.

A Soul's reputation doesn't come from a single score, but emerges from the **constellation** of all its SBTs, forming a dynamic and nuanced digital identity.

This "Web of Trust" moves beyond simplistic reputation systems, allowing for a more granular and context-aware understanding of identity.

# Use Case 1: Community Wallet Recovery

1

## Problem with Seed Phrases

Traditional seed phrases are a single point of failure; loss means total loss of assets, and compromise means total theft. It's a major barrier to broader Web3 adoption.

2

## SBT Solution: Social Recovery

Instead of a single seed phrase, a Soul can designate a qualified majority of its SBT-holding communities as guardians. These guardians (e.g., your university, your DAO, your sports club) can collectively help recover a lost or compromised private key.

3

## Decentralized Security

This method leverages existing social ties and community trust, distributing the risk and making recovery more resilient than centralized or single-point solutions.

# Use Case 2: Fairer Governance for DAOs

1

## Problem: DAO Vulnerabilities

DAOs are susceptible to Sybil attacks (one entity controlling multiple identities) and collusion, where malicious actors can manipulate voting outcomes to their benefit, undermining decentralization.

2

## SBT Solution: Correlation Discounting

SBTs can enable "correlation discounting." If multiple Souls with highly correlated SBTs (e.g., all holding "Employee of Company X" SBT) vote identically, their collective vote weight can be proportionately reduced.

3

## Enhancing DAO Resilience

This mechanism helps prevent concentrated power and encourages more diverse, independent voting, leading to more robust and decentralized governance outcomes for DAOs.

# The Big Vision: "Decentralized Society" (DeSoc)

A "co-determined sociality, where Souls and Communities convene bottom-up... to produce plural network goods across different scales".

DeSoc envisions a future where individuals and communities can form self-sovereign, trust-based relationships, fostering collective action and producing shared resources and value without relying on centralized intermediaries. It's about building a more cooperative and inclusive digital future.

# The Risks & Challenges (A Balanced View)

## Dystopian Futures

SBTs, if misused, could lead to social control: automating red-lining, predatory lending based on social scores, or creating oppressive credit systems, potentially exacerbating existing inequalities.

## Privacy Concerns

Making sensitive relationships and credentials publicly visible is dangerous. "Programmable privacy" using advanced cryptography (like zero-knowledge proofs) is essential to control who sees what data.

## Cheating & Bootstrapping

The system is vulnerable to fake SBTs and sybil attacks, especially in its early stages. It requires bootstrapping from authentic communities and careful design to prevent manipulation and ensure genuine trust.

# Conclusion & Key Takeaways

- 1 SBTs are non-transferable tokens that represent social identity.
- 2 They aim to solve Web3's critical lack of trust and reputation.
- 3 They unlock powerful applications like community recovery and fairer governance.
- 4 The ultimate vision is a more cooperative Decentralized Society (DeSoc).
- 5 Significant privacy and ethical challenges must be addressed for responsible implementation.

# Thank You

## Questions?