

# Soulbound Tokens (SBTs) Study Report

*Part 1: Building and Embracing a New Social Identity Layer?*

---



blockchain  
governance  
initiative  
network

**The Global Network for Blockchain Stakeholders™**

This study is a work product of IAM, Key Management and Privacy Working Group of BGIN.

©2022 BGIN (Blockchain Governance Initiative Network) is registered as BN Association, a Japanese general association with its principal place of business at Shiba Building, 704, 4-7-6, Shiba, Minato-ku, Tokyo. All right reserved.

# Abstract

This research paper examines the implications of Soulbound Tokens (SBTs), a novel smart contract primitive introduced by E. Glen Weyl, Puja Ohlhaver, and Vitalik Buterin (2022) “Decentralized Society: Finding Web3’s Soul”, to curb Web3’s “hyper financialisation” and lack of tooling to enable social coordination. Web3 has lacked the facilities for social coordination undermining the potential for rich-social context, permitting a counter-productive cycle of plutocratic governance and superficial pseudonymous interactions. NFTs, despite being considered a possible solution, have also seen problems arising from its anonymous and transferable features. We are intrigued by the implications of a token capable of storing and creating composable non-capital value, which we refer to as “reputation value”. The possible application of soulbound tokens ranges from, community badges, memberships, credentials, accolades, and attestations.

In this research paper, we have constructed a comprehensive overview of SBTs, analyzing SBT’s principle characteristics, features and implications. We discuss the various technical, social, and ethical considerations when tokenizing “reputation value”. We have evaluated the principles and rationale imparted by Weyl et al. (2022), in relation to fundamental academic literature, practical technical examples, and the philosophies of digital identity; ranging from Nick Szabo (1996; 1997), James Cameron (2005), Nat Sakimura (2021), and EIPs relating to SBTs.

While we hope our work catalyzes further research internationally, we equally intend to draw attention to cautionary warnings to ensure SBTs are deployed in a safe and responsible manner, including the discussion on whether they should be deployed at all. Since SBTs are closely related to consequential matters, for one digital identity, a wide range of multi-stakeholders should come together and progress discussions surrounding privacy, ethics, implementations and standards.

This is an early stage discussion and we hope to extend our discussion further in future BGIN works. We welcome diversity of thought, and invite anyone interested to be part of the discussion.

# Introduction

*“The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception which will cumulatively erode public trust in the Internet.”*

*Kim Cameron (2005) “The Laws of Identity”*

In 2005, Kim Cameron published “The Laws of Identity,” where he stated that “[t]he absence of an identity layer is one of the key factors limiting the further settlement of cyberspace”. He explains the difficulty of adding the identity layer in the internet “[m]ainly because there is little agreement on what it should be and how it should be run”.

Over recent decades, the implementation of an identity layer to the internet has become an essential topic for academic research and technical development, achieving progress incrementally.<sup>1</sup> Globally, active discussions and philosophical movements have been established to come to a consensus surrounding the international standardization of digital identity. The classical question of maintaining anonymity but with accountability has yet to be solved but remains vital to the future of the internet. This question is a key pillar to establishing a decentralized society and defines the core foundations of such a plural society.

In this paper, we endeavor to provide a detailed framework for understanding the potentials, design principles, limitations, challenges, problems, and risks associated with soulbound tokens (SBTs), a concept introduced in the “Decentralized Society: Finding Web3’s Soul” (Weyl et al., 2022). We have critically examined SBTs and discussed the consequences of such technology, both at a societal and individual level, evaluating the benefits and detriments of SBTs if they were to be implemented. We believe that SBTs could have significant societal implications and at the same time we also emphasize the need to address various questions in advance, including privacy, global standardization and responsible development. It is essential to continually evaluate the properties that characterize SBTs, understanding potential use cases, and the risks associated.

Throughout our research, we have sought out the key consequences of SBTs, and

---

<sup>1</sup> It remains important to question whether the “missing identity layer” is simply mythical. Sheldrake (2022) argues that “[w]hen the SSI community refers to an ‘identity layer’ its subject is actually a set of algorithms and services designed to ensure the frictionless transmission of incorruptible messages between multiple parties; well, between identifiers. This involves some clever mathematics and neat code that will undoubtedly prove of some value in the world with appropriate tight constraints, and it will certainly impact the operation of various conceptualizations of identity, but I think few people would argue that this is human identity per se, or even the digitalization of human identity. Far from it.”

applied rigor to evaluate whether adopting tokens capable of storing reputation value and social credentials is necessary or desired both individually and socially.

We plan to adapt our report as the market context evolves, to ensure regulatory bodies can address their concerns whilst maintaining SBT innovation grows at a stable pace. We will continue to publish new reports and recommendations on SBTs, to ensure a balance between innovation regulation. This report is based on the information available as of February 2023, but some conditions may have changed since the time of publication. A follow on research paper is being planned for 2023, which takes an extensive analysis of SBTs, contributions are currently open - please contact [bgin-admin@mail.bgin-global.org](mailto:bgin-admin@mail.bgin-global.org).

Lastly, this report is a collaborative effort. In the process of making this paper, we have made it open, allowing anyone to comment and suggest. We thank everyone for their feedback which was all very valuable. Furthermore, in Appendix A. we list all of those involved in authoring, contributing and reviewing this research paper. Again we pay thanks to those and their involvement.

Disclaimer: The views expressed in the document are personal views of the participating members of the BGIN community and should not be seen as the official views or recommendations of the institutions with which they are affiliated.

The technology described in this document was made available from contributions from various sources, including members of the BGIN and others. Although the BGIN has taken steps to help ensure that the technology is available for distribution, it takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any independent effort to identify any such rights. BGIN and the contributors to this document make no (and hereby expressly disclaim any) warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this document, and the entire risk as to implementing this document is assumed by the implementer. The BGIN Intellectual Property Rights policy requires contributors to offer a patent promise not to assert certain patent claims against other contributors and against implementers. BGIN invites any interested party to bring to its attention any copyrights, patents, patent applications, or other proprietary rights that may cover technology that may be required to practice this document.

# Table of contents

# 1. Scope

The intended audience for this document includes developers, businesses, regulatory bodies, academic institutions, and any individual seeking to expand their understanding of soulbound tokens.

This paper aims to provide an overview of the current challenges facing decentralized innovation, specifically soulbound tokens. We then proceed to analyze the defining characteristics of soulbound tokens, the core design considerations and a summary of the broader soulbound token ecosystem. Furthermore, we will examine the potentials and limitations of soulbound tokens, before concluding with recommendations for future research and development, envisioning a decentralized society underpinned by soulbound tokens.

## 2. Normative Reference

This document has no normative reference.

## 3. Terms and Definitions

This document uses the following terms as the shortcut for more complete wording provided as the definition. When the term appears within this document, it should be read as being replaced by the definition.

### 3.1

#### **decentralized autonomous organization**

##### **DAO**

a voluntary association with the operating principles of digital cooperativism. As voluntary associations, they are a cross-jurisdictional way for strangers, friends, or unlikely allies to pseudonymously come together toward common goals, supported by a token model, incentives, and governance. Members of a DAO can have representative ownership of its digital assets through a token, which often simultaneously acts as a governance right and network utility.

[Source: Kei (2021)]

### 3.2

#### **decentralized financial technologies**

technologies that may reduce or eliminate the need for one or more intermediaries or centralized processes in the provision of financial services

[Source: FSB (2019)]

### **3.3**

#### **decentralized financial system**

new financial system that could be the result of decentralized financial technology

[Source: FSB (2019)]

### **3.4**

#### **decentralized finance**

##### **DeFi**

financial application that could consist of a part of a decentralized financial system

[Source: Ushida and James (2021)]

### **3.5**

#### **decentralized society**

##### **DeSoc**

co-determined sociality, where Souls (defined in 3.9) and Communities convene bottom-up, as emergent properties of each other to produce plural network goods across different scales

[Source: Weyl et al. (2022)]

### **3.6**

#### **non-fungible token**

##### **NFT**

tokenized representation of an asset (or anything really) that provides some rights to the owner

[Source: BGIN (2022)]

### **3.7**

#### **privacy enhancing technologies**

##### **PETs**

technologies that covers the broader range of technologies that are designed for supporting privacy and data protection

[Source: ENISA - The European Union Agency for Cybersecurity]

### **3.8**

#### **scarlet letter**

the forced display, and disclosure of a negative sentiment about oneself to others at all times against their will.

[Source: Jain et al. (2022)]

### **3.9**

#### **soul**

account, or wallet, that hold publicly visible, non-transferable (but possibly revocable-by-the-issuer) tokens

[Source: Weyl et al. (2022)]

### **3.10**

#### **soulbound token**

#### **SBT**

publicly visible, non-transferable (but possibly revocable-by-the-issuer) token held by the soul

[Source: Weyl et al. (2022)]

### **3.11**

#### **self sovereign identity**

#### **SSI**

digital movement that recognizes an individual should own and control their identity without the intervening administrative authorities

[Source: Sovrin Foundation (2018)]

### **3.12**

#### **verifiable credential**

#### **VC**

tamper-evident credential that has authorship that can be cryptographically verified

[Source: World Wide Web Consortium (2022 a)]

### **3.13**

#### **decentralized identifier**

#### **DID**

identifier that enables verifiable, decentralized digital identity

[Source: World Wide Web Consortium (2022 b)]

## **4. Abbreviations and Symbols**

In this document, the following abbreviations and symbols are used.

AML: Anti-Money Laundering

BGIN: Blockchain Governance Initiative Network

CDD: Customer Due Diligence

CTF: Counter Terrorism Financing

DAO: Decentralised Autonomous Organisation

DeFi: Decentralised Finance

DeSoc: Decentralised Society

DID: Decentralized Identifiers

EIP: Ethereum Improvement Proposals

ERC: Ethereum Request for Comments

JFSA: Japan Financial Services Agency

KYC: Know-Your-Customer

ML: Money Laundering

NFT: Non-Fungible Token

NTT: Non-Tradable Token

PII: Personal Identifiable Information

SBT: Soulbound Tokens

SDO: Standards Development Organisation

SSI: Self-Sovereign Identity

TF: Terrorist Financing

VASP: Virtual Asset Service Provider

VC: Verifiable Credential

## 5. Current Problems and Risks

In this section, we will examine six major problems that have emerged from decentralized financial systems and NFTs; these include fraud schemes, money laundering and terrorist financing, wash trading, tax evasion, and governance challenges.<sup>2</sup>

In this paper, we will begin by exploring the limitations of NFTs, defined by transferable and non-recoverability attributes, to better illustrate the key distinction between NFTs and SBTs, which are defined by non-transferable and initially revocable traits; SBT recoverability and programmable privacy features are planned post-product maturity.

As outlined in Ethereum's NFT documentation, (<https://ethereum.org/en/nft/>), the primary function of NFT's is to represent distinguishable ownership of unique digital or real-world assets, which can be atomically tracked, similar to a deed; another initially

---

<sup>2</sup> According to BGIN (2022), NFTs “differs from other VAs used as currencies where fungibility is instead a very important and fundamental characteristic of the assets. An easy way to picture an NFT is a blockchain-based asset that has only one indivisible unit available and no possibility for further issuance in the future”.

proposed term for NFTs.<sup>3</sup> The identification of NFT holding is “managed through the unique identifier and metadata that no other token can replicate”.<sup>4</sup> The holder of an NFT (1) “can easily prove you own it”, (2) “no one can manipulate it in any way”, (3) “can sell it, and in some cases this will earn the original creator resale royalties”, and (4) “can hold it forever”.<sup>5</sup>

NFTs were created to address the technical limitations in the Ethereum ERC-20 “Token Standard” contract when attesting distinguishable ownership of a unique digital asset.<sup>6</sup> Early examples of NFTs, such as Cryptopunks and CryptoKitties utilized custom smart contracts based on the standard flexible and multi-purpose ERC-20 contract. These early forms of NFTs served as a catalyst for the development of a new smart contract standard, creating demand for an optimized smart contract capable of attesting to unique assets and their corresponding holder.

Focusing on the core feature of NFTs being the distinguishable connection between owner and digital or real-world asset, there is little room for assets that are non-transferable as an NFT use case. A motivation outlined in the original EIP-721 “Non-Fungible Token Standard”, was to “have a standardized interface that allows for cross-functional asset management and sales platforms”. NFTs, beyond being a technically insufficient standard to represent personal, social or unique reputation value, are equally limited by the financial use case specifications outlined initially. Similarly, to address the deficiencies of the fungible ERC-20 token in expressing distinguishable ownership of unique digital assets, the ERC-721 standard was proposed and approved.

---

<sup>3</sup> Here, “deed” refers to a legal document that is signed and delivered, especially one regarding the ownership of property or legal rights.

<sup>4</sup> Care should be taken in using the word “ownership” in this context when no property rights are recognised with NFTs unlike the general case. According to Reutlaw “NFTs and Property Rights”, “[w]hen buying an NFT, the buyer typically only acquires the right to transfer the NFT to a third party but not the rights to the original work. This means that the holder of the NFT is free to dispose of the token but would not be allowed to reproduce or otherwise exploit the underlying intellectual property” (<https://www.reutlaw.com/en/insights/nfts-and-property-rights>). An NFT, of itself, does not convey or constitute ownership of anything. Ownership is only ever conveyed by a separate legal document. The critical point is “can” i.e. “can represent”, which can be interpreted as “can represent subject to accompanying legislation to support the fact or in the absence of such legislation some separate legal contract that binds ownership of the NFT to ownership of the corresponding real world asset”. This “ownership” is an area for further legal discussion.

<sup>5</sup> See Ethereum “Non-fungible tokens (NFT)” for more. (<https://ethereum.org/en/nft/> )

<sup>6</sup> “ERCs (Ethereum Request for Comments) are technical documents used by smart contract developers at Ethereum. They define a set of rules required to implement tokens for the Ethereum ecosystem. These documents are usually created by developers, and they include information about protocol specifications and contract descriptions. Before becoming an standard, an ERC must be revised, commented and accepted by the community through an EIP (Ethereum Improvement Proposal)” (<https://docs.ethhub.io/built-on-ethereum/erc-token-standards/what-are-erc-tokens/> ).

According to Ethereum, ERC-20 “introduces a standard for Fungible Tokens, in other words, they have a property that makes each Token be exactly the same (in type and value) as another Token. For example, an ERC-20 Token acts just like the ETH, meaning that 1 Token is and will always be equal to all the other Tokens”. (<https://ethereum.org/en/developers/docs/standards/tokens/erc-20/> )

This creates a precedent to address token deficiencies, innovating upon the initial design and creating functionalities that enable a seamless transition..

- “There are many proposed uses of Ethereum smart contracts that depend on tracking distinguishable assets. Examples of existing or planned NFTs are LAND in Decentraland, the eponymous punks in CryptoPunks, and in-game items using systems like DMarket or EnjinCoin. Future uses include tracking real-world assets, like real estate (as envisioned by companies like Ubitquity or Propy). It is critical in each of these cases that these items are not “lumped together” as numbers in a ledger, but instead each asset must have its ownership individually and atomically tracked.”

([EIP-721: Non-Fungible Token Standard \(ethereum.org\)](https://ethereum.org))

The emergence of NFTs whilst providing the blockchain ecosystem with new technical solutions, unfortunately, introduced a variety of new risks and negative use cases as a consequence. The problems associated with NFTs are well-documented in BGIN’s 2022 “NFT Study Report” (BGIN, 2022) and other studies examining NFTs. It is important to recognise that these issues stem from a lack of transparency in the identification of individuals and entities involved in NFT transactions. This is a new example of a common problem that has persisted throughout generations of digital environments, as there is a lack of “a way to know who and what you are connecting to” (Cameron, 2005). Equally, to progress closer to viable identification mechanisms within decentralized environments, NFTs properties of transferability and non-recoverability suggests that it is ill-suited to hold sensitive information such as social credentials, PII, or government-issued identity documents. By design, the described social coordination tools are unsuitable to be transferable or unrecoverable.

Non-transferable NFTs, defined by the smart contract’s singular non-transferable attribute, have emerged as a patchwork solution to NFTs deficiencies in storing reputation value and social credentials. Jain et al. (2022) outlined that non-transferable NFTs are limiting in scope and approach to representing an SBT, as there is no specification nor standard beyond a singular programmable value; non-transferability. If in isolation, this singular value token may not be considered to be an SBT, and could open the non-transferable NFT use cases to “scarlet letters”, which are malicious forms of smart contracts. While non-transferable NFTs are limited and insufficient to hold social credentials, they may serve as a starting point for basic or proto-SBTs, storing non-informing information. A recommendation is for issuing platforms to either embed cautionary warnings to inform issuers or creators or at least monitor token issuance as a case of last resort.

With the exception of “flash loans”, which are a novel financial product native to DeFi, it should be acknowledged that the issues discussed below are not unique to

NFTs. As an example, there are conflicting incentives in the art market in the first place, not just for NFT marketplaces or the greater DeFi market. Simply put, incentives that promote opacity artificially inflate the asset's value through perceived scarcity and provable providence, thereby establishing credibility; leading to value inflation. However, because of NFTs unique features and utility, many of the examples studied pertain specifically to NFTs, and contextualize the potential for SBTs which is covered in clause 8.

## 1 Fraud Scheme (Inauthentic Replicas)

- “There are a number of risks to consumers in the NFT ecosystem, and some NFT marketplaces and digital wallets lack basic features to protect consumers from fraud and misleading or deceptive practices.”  
*(Congressional Research Service. 2022. “Non-Fungible Tokens (NFTs)”)*
- “While anyone can find the NFTs trade history and the address that created the item, NFTs can be difficult to verify if you do not know the owner or the creator.”  
*(BGIN. 2022. “SR 005 NFT Study Report Part 1: Introduction and Use Cases”)*
- The challenge in verifying the true owner or the creator of NFTs stems from the inherent features of decentralized markets, including pseudonymity/anonymity, lack of authentication mechanisms but also from the broader environment of opaque providence and control of the underlying data layer and the utility behind unique high-value transferable assets. Additionally, there are difficulties in establishing a unanimously agreed standard, rather than a system which acts as the de facto custodian of token or the underlying metadata essential to the NFT; which poses significant centralisation risks and undermines the purpose of decentralized markets.
- NFTs present a number of risks to consumers in the form of fraud and deceptive practices. Furthermore, some NFTs, NFT marketplaces and digital wallets lack basic consumer protection features, leading to consumers being vulnerable to fraudulent replicas, phishing scams and similar imperceptible schemes. Therefore, it is imperative to explore authentication mechanisms that provide consumers with clear verification of the NFTs ownership and creator. Further authorisation of the stakeholders will at least enable the consumer to make an informed decision, additional measures can be taken by the marketplace by displaying cautionary warnings or implementing methods of socially agreed proofs of origination and smart contract authorship.

- It is also worth noting that ownership of an NFT does not automatically confer legal or copyright ownership of the digital or physical assets embedded and/or linked with the NFT.

## 2 Wash Trade

- “One can own as many of these wallets as they would like. This means that one can sell an NFT to their own address, with the only loss of value in the network fee. This is a problem because NFT sellers can make their token appear much more valuable than it truly is.”  
[\(BGIN. 2022. “SR 005 NFT Study Report Part 1: Introduction and Use Cases”\)](#)
- “The 110 profitable wash traders have collectively made nearly \$8.9 million in profit from this activity, dwarfing the \$416,984 in losses made by the 152 unprofitable wash traders. Even worse, that \$8.9 million is most likely derived from sales to unsuspecting buyers who believe the NFT they’re purchasing has been growing in value, sold from one distinct collector to another”  
[\(Chainanalysis. 2022. “The Chainalysis 2022 Crypto Crime Report”\)](#)

## 3 Money Laundering (ML) and Terrorist Finance (TF)

- “The US Treasury identified six qualities of the high-value art market that make it enticing for money laundering: high-value, opaque nature, subjective valuation, transportability, law enforcement’s difficulty in monitoring transports, and the use of third-party intermediaries to keep clients anonymous.”  
[\(BGIN. 2022. “SR 005 NFT Study Report Part 1: Introduction and Use Cases”\)](#)
- “NFTs possess the ability to self-launder. Self-laundering is where criminals create an NFT themselves with one address and then buy the NFT with a different address. The NFT is then sold to the open market in exchange for clean funds.”  
[\(BGIN. 2022. “SR 005 NFT Study Report Part 1: Introduction and Use Cases”\)](#)
- “With NFTs and centralized/decentralized exchanges, the transactions are handled not only by the marketplace, but also by the seller of the NFT. This seller has no obligation to ensure the legitimacy of the exchange.”<sup>7</sup>

---

<sup>7</sup> There was a suggestion about the statement in the existing “NFT Study Report”. First, there should be two parts to address decentralized and centralized separately. Second, in a decentralized exchange it is a trustless system. By signing the transaction, you are agreeing that you understand what you are doing. The onus is placed on the wallet User Interface (UI) and subsequently the user. In a centralized exchange the user is signing some end-user license agreements (EULA) or providing a credit card. By doing so they

[\(BGIN. 2022. "SR 005 NFT Study Report Part 1: Introduction and Use Cases"\)](#)

- “NFTs may be particularly susceptible to money laundering since they are easily sent across geographic borders without incurring the financial or regulatory costs of physical shipping. Additionally, the price of digital art is highly variable, which enables money launderers to set the desired value with little historical context in which to compare prices.”  
[\(Congressional Research Service. 2022. "Non-Fungible Tokens \(NFTs\)"\)](#)
- “Cybercriminals have laundered over \$33 billion worth of cryptocurrency since 2017, with most of the total over time moving to centralized exchanges.”<sup>8</sup>  
[\(Chainanalysis. 2022. "The Chainalysis 2022 Crypto Crime Report"\)](#)
- “Value sent to NFT marketplaces by illicit addresses jumped significantly in the third quarter of 2021, crossing \$1 million worth of cryptocurrency. The figure grew again in the fourth quarter, topping out at just under \$1.4 million.”  
[\(Chainanalysis. 2022. "The Chainalysis 2022 Crypto Crime Report"\)](#)

#### 4 Flash Loans

- “Flash loans are a new financial product - "While many of the financial products and services arising from DeFi resemble traditional financial products and services, blockchain technology has supported the creation of entirely new financial products and services, such as "flash loans."”  
[\(OR01/2022 IOSCO Decentralized Finance Report\)](#)
- “Flash loans as a means to obfuscate value by increasing the floor price of an NFT "A seller took out a flash loan – a loan that must be repaid within one block transaction – and purchased their own Cryptopunk #9998 for \$532 million using a new wallet"  
[\(Elliptic. 2022. "NFTs and Financial Crime"\)](#)
- The ability for users to borrow significant sums of money within a short period of time (a block time), to artificially inflate asset prices would disrupt key market metrics such as an NFTs collection floor price or an individual NFTs last sold price. In addition, flash loans, much like traditional loans, are still required to be repaid within the specified time - flash loans are

---

agree they've validated the vendor. Otherwise anyone could claim fraud on every transaction saying they now consider the vendor illegitimate.

<sup>8</sup> There was a suggestion that accurate figure that illustrate the amount that was laundered would be useful for further research. However, it is not easy as the Financial Action Task Force (FATF) states that “[d]ue to the illegal nature of the transactions, precise statistics are not available and it is therefore impossible to produce a definitive estimate of the amount of money that is globally laundered every year. The FATF therefore does not publish any figures in this regard”.

- required to be repaid within the same block time (~15 seconds), which does serve as a mitigant to malicious uses but does not eliminate the risk.
- Flash loans have the potential to undermine trust in a natively trustless environment, therefore it is essential to create accessible and convenient tooling to mitigate the negative externalities that arise from unregulated complex financial tools like Flash loans.

## 5 Tax Evasion

- “Virtual currencies continue to present a significant risk to tax administration, particularly since one of the attractions to their use is the anonymity of transactions.”  
*(U.S. House of Representatives. 2020. “Understanding The Tax Gap And Taxpayer Noncompliance”)*
- “Cryptocurrency investors are collectively not paying the IRS at least half of the taxes they owe on their virtual-currency trades, according to new analysis from Barclays Plc.”, “[e]xtrapolated from a 2017 IRS calculation to find the current tax gap would be around \$50 billion per year -- accounting for about 10% of all unpaid taxes.”<sup>9</sup>  
*(Bloomberg. May, 2022. “Crypto Investors Likely Paying IRS Less Than Half the Taxes They Owe - Bloomberg”)*

## 6 Governance

- Governance tokens can be bought in the digital asset marketplaces and regularly voting power is bought up by those who have more resources/ the wealthy, leading to an overwhelming number of plutocratic governance systems. In addition, by default, there are no inherent guarantees for the protection of minority interests. Without a system that solicits opinions, the structure goes against the stated goal of many protocols claiming equality and fairness.
- Pseudonymous voting has a positive aspect, for example, independent decision making. It is important to note that since DAOs are an organization, there might be a scenario where holding a participant accountable for a vote is beneficial; as a way to ensure legitimacy.
- Below are the risk factors or possible risk factors in governance that was mentioned in the JFSA (2022) “Report on Distributed Financial Systems in Trust Chains Research on Technology Risk”.
  - Governance Voting Control

---

<sup>9</sup> There was a suggestion that the lack of tooling on the IRS side could be one aspect.

- Voting is dominated by a small number of major governance token holders with enough votes to constitute a quorum for passage.<sup>10</sup>
- Voting is controlled by the community and developers, who hold large amounts of governance tokens, including those for system use.
- Governance tokens are bought and sold on the crypto-asset market, which is structured so that those with the money get more votes (DAO decision-making is not decentralised).
  - Unlimited number of governor tokens.<sup>11</sup>
- Governance Voter Pseudonyms
  - Governance voting is conducted under pseudonyms, which may make it impossible to identify the party to be held accountable for the outcome of the vote.<sup>12</sup>
  - There is a lack of mechanisms to link user account addresses to individuals.<sup>13</sup>
- Quorum to vote is not high
  - Quorum for governance voting is low and decisions are made by a minority opinion (very low quorum of 1 - 4% for major DeFi projects).
  - Low turnout for Governance Vote likely means fewer quorums to pass proposals.<sup>14</sup>
- Low voter turnout<sup>15</sup>
  - Low turnout for governance voting, with decisions being made by a small percentage of voters (extremely low turnout for major DeFi projects, about 2 - 9%).
  - Governance tokens are valuable and speculative in the crypto asset market, so speculative token holders are less willing to vote.

---

<sup>10</sup> This would also apply to Proof-of-Stake (PoS) and most variants. However, Proof-of-Work (PoW) and others address this with computational work. The consensus can still be corrupted, but becomes computationally prohibitive.

<sup>11</sup> In the original text, it is written as “governor tokens” but we assume it to be “governance tokens”. For further research, quantifying the number of governor tokens/governance tokens is important.

<sup>12</sup> This point is on how pseudonymity and the impact of governance decisions made under such identities is a “risk” towards governance. This also applies to anonymity as well.

<sup>13</sup> In other words, it is a lack of mechanism to link user accounts that accurately correlate public address ownership and their legal identity. Services such as Ethereum Name Service (ENS), Proof of Humanity, and Twitter connections provide a means to selectively disclose information. However, these tools are not utilized by the majority of users.

<sup>14</sup> This can be framed as a user experience (UX) and community issue, not a governance problem.

<sup>15</sup> This may not necessarily be true. While many protocols promise rewards, ultimately the motivation to vote is related to your motivation to hold the token in the first place.

- Governance token holders are not motivated to vote (there is no mechanism to motivate them).
- Verification of malicious proposals<sup>16</sup>
  - In the event of a malicious proposal, since verification is dependent on the cooperation of community members, there is a concern that no one will be able to detect a malicious proposal because the role of conducting verification is not clear.
  - In decentralised organisations, communities are free to participate and roles are not specified. It is not clear whether verification of malicious proposals will be ensured.<sup>17</sup>
- Dependency on smart contract modifications
  - When a governance voting proposal modifies a smart contract, most governance voting participants do not understand the content of the smart contract code and assume that it will act correctly according to the proposal.
  - Only a small percentage of governance voting participants are technically capable of interpreting smart contracts; the majority are for profit.
  - Insufficient disclosure of information on smart contract modifications, and no assurance of the validity of comments presented in community forums, etc.<sup>18</sup>
- Organisation of DAOs<sup>19</sup>
  - DAOs have unclear representatives and boards of directors, making it difficult to hold them accountable when problems occur.
  - DAO has no organisation to pursue.
  - The DAO is an organisation of non-trusting participating members and has no representatives.
  - There are no laws and regulations applicable to DAOs, and the shape of the organisation is not yet defined.

<sup>16</sup> It is not important who proposed the change but necessary to know what the change is. People can read their proposal and code alongside it in the new EIP. However, the problem is that many people cannot understand the proposals fully because of complexity, lack of background, lack of time, etc.

<sup>17</sup> As of 2022 it is more accurate to state that “roles are often not specified” as to “roles are not specified”.

<sup>18</sup> In general, smart contracts are immutable in a public network. Therefore they can't be modified. It would be more accurate to describe this “smart contract modifications” in the original text as “add smart contract updates via proxy methods”.

<sup>19</sup> There are cases such as in the State of Wyoming where a DAO can be registered as a legal entity ([DAOs\\_FAQs.pdf \(wyo.gov\)](#)). Additionally, many countries treat undefined organizations as unincorporated associations. There is no limitation of liability for those associations such as in the Commodity Futures Trading Commission (CFTC) v Ooki DAO case (<https://storage.courtlistener.com/recap/gov.uscourts.cand.400807/gov.uscourts.cand.400807.11.1.pdf>).

- Location and membership of DAO
  - The location of the DAO is unclear.<sup>20</sup>
  - DAO members are dispersed throughout the world and cannot be regulated or pursued across national borders.
  - DeFi protocol terms of use (user's own responsibility) are not made available to users before using the service.<sup>21</sup>

(JFSA. 2022. “Report on Distributed Financial Systems in Trust Chains Research on Technology Risk”)

Various ventures are developing and testing solutions to address the lack of identification and social credentials within DeFi. For instance, GoldFinch, a decentralized credit protocol, has transitioned methods of KYC. GoldFinch iterated from an ecosystem-managed incentivised KYC mechanism to now leveraging non-transferable NFTs, that represent the result of users' KYC, Know-Your-Business and/or sophisticated investor accreditation credentials. The issued NFT is labeled as a Unique Identity (UID); no PII is shared on-chain, only the result of the KYC check.<sup>22</sup> While not specific to NFTs, Pauwels et al. (2022) proposed a zkKYC, an off-chain encrypted data object generated by the holder based on elements of the KYC verifiable credential they hold, which can only be revealed to specific parties whose public key signed the token initially. While there are possibilities to patch additional features into NFTs to attempt creating an NFT capable of storing reputation value and social credentials, the standard still falls technically deficient as features of transferability and non-recoverability are ingrained into the NFT standard. In addition, this analysis considers the value proposition of NFTs, understanding the Ethereum community determined the rationale for NFTs stemmed from the desire for a token standard capable of holding unique capital value assets such as property, shares and tradeable-collectables. The previously discussed points on the function and purpose of NFTs form part of the argument to suggest that NFTs are inadequate in storing social credentials and reputation value. However, this has presented the opportunity to

---

<sup>20</sup> The risk to location matters in the case of anonymous on-chain voting for a local impact or law. For example, an individual can post a proposal for a park that anyone in the world could vote on unaffected. That park could be a law. So we need a way in some cases to limit access based on current geo-location. However, this should be approached with caution as it would impact those living abroad with voting rights and could threaten the possibility of a digital sovereign nation/society.

<sup>21</sup> This should be carefully considered since it is not necessarily accurate such as relying on IP geolocation.

<sup>22</sup>GoldFinch presents an intuitive method to tokenize a user's KYC/KYB/sophisticated investor result, however it should be noted the UID is in 'Alpha' (<https://docs.goldfinch.finance/goldfinch/unique-identity-uid/for-developers>) and moreover, the level of KYC/AML needed per jurisdiction may create further complications if other protocol attempt to leverage GoldFinch's UID. <https://docs.goldfinch.finance/goldfinch/unique-identity-uid>

introduce a new smart contract to the blockchain typology that addresses NFTs deficiencies in storing reputation value or social credentials on-chain; the SBT.

Further discussion is warranted to answer questions of “what is reputation value” and “who or what determines reputation value”, which are examined in clause 7.2. These questions should be explored with exceptional caution, and consider the potential dangers of quantifying and digitizing such information, this includes self-issuance, plural determination and especially top-down arbitrated issuance; blockchain’s immutable nature and state of finality shouldn’t be forgotten during this evaluation.

## 6. Characteristics of the SBTs

In this section, we examine the defining characteristics of SBTs as cited in “Decentralized Society: Finding Web3’s Soul” (Weyl et al., 2022), co-authored by Vitalik Buterin, Puja Ohlhaver and E. Glen Weyl, whilst also drawing from insights developed from during our research and discussions with the various contributors listed in Appendix A.

Before defining SBTs, the focus of this paper, it’s essential to define the wallet and means of holding SBTs, the Soul. According to Weyl et al. (2022), “Souls” are “accounts, or wallets, that hold *publicly visible, non-transferable (but possibly revocable-by-the-issuer) tokens*” and “Soulbound Tokens (SBTs)” are “tokens held by the accounts”.<sup>23</sup> The authors also suggest that the SBTs may correspond to a range of affiliations, memberships, and credentials, and users could possibly self-certify and/or be certified by other Souls. Furthermore, “there is no requirement for a Soul to be linked to a legal name, or for there to be any protocol-level attempt to ensure ‘one Soul per human.’” (Weyl et al., 2022).

One way to describe the initial concept of SBTs is to think about them as non-transferable NFTs; this short-hand definition can serve to be limiting when considering the long term vision of SBTs (Jain et al., 2022).<sup>24</sup> While NFTs and SBTs share some similarities, there are several critical features that distinguish SBTs from NFTs, the most significant design feature is NFTs transferability versus SBTs non-transferability. It is essential to recognise that the characteristics of NFTs have led

---

<sup>23</sup> It is important to be cautious when using the term “Souls”. Although it is an intuitive term, It has a risk of introducing an unnecessary lexicon more than it is meant. In general, the “soul” is widely understood to be ephemeral, spiritual, and intangible. There were suggestions that Weyl et al. (2022) focus on sybil resistance i.e. dedication to the corporeality of the human, rather than informational identities and therefore a term such as “wallet tied to an individual” should be appropriate for usage.

<sup>24</sup> “The first caveat is that non-transferable NFTs are the most primitive form of SBTs—which today lack a specifications. In particular, the singular property of non-transferable NFTs is non-transferability, and they lack any of the nuanced socially programmable privacy or community recovery aspirations sketched in the DeSoc paper— pathways which theoretically may enable community mechanisms to counter certain forms of malicious tagging.” (Jain et al., 2022)

to some of the negative consequences and limitations outlined in clause 5, catalyzing the necessary pressure to theorize SBTs.

Another method of determining the characteristics of SBTs is by analyzing the definition prescribed by Weyl et al. (2022), which defines SBTs as “publicly visible, non-transferable (but possibly revocable-by-the-issuer) tokens.” From this definition, four distinct features can be discerned 1) publicly visible; 2) non-transferable; 3) possibly revocable; 4) issuer-arbitrated. These SBT characteristics are further elaborated by Weyl et al. (2022) throughout the aforementioned paper on each features’ individual significance and rationale:

### **The Four Features of Proto-SBT contract design:**

#### **1 Publicly Visible**

- “We initially assume publicity despite our deep interest in privacy because it is technically simpler to validate as a proof-of-concept, even if limited by the subset of tokens people are willing to publicly share.” page 2 (Weyl et al., 2022)

#### **2 Non-transferable**

- “non-transferability prevents transferring or hiding outstanding loans, while a rich ecosystem of SBTs ensures that borrowers who try to escape their loans (perhaps by spinning up a fresh Soul) will lack SBTs to meaningfully stake their reputation.” page 4 (Weyl et al., 2022)
- “the emphasis on transferability has been to web3’s detriment, making it incapable of representing and supporting some of the simplest and ubiquitous property contracts today, such as apartment leases.” page 10 (Weyl et al., 2022).

#### **3 Possibly Revocable**

- “Revocable, transferable tokens are a kind of proto-SBT—serving supportive, placental functions before Soul birth. These tokens buy time both for wallets to gestate secure, community recovery mechanisms and for a person to succinctly accumulate proto-SBTs that can eventually be burned and re-issued into non-transferable SBTs.” page 28 (Weyl et al., 2022)

#### **4 Issuer-Arbitrated**

- “In their simplest form, these SBTs can be “self-certified,” similar to how we share information about ourselves in our CVs... SBTs held

by one Soul can be issued—or attested—by other Souls, who are counterparties to these relationships. These counterparty Souls could be individuals, companies, or institutions.” page 2 (Weyl et al., 2022)

- “A token is revocable if an issuer can burn the token and re-issue it to a new wallet. Burning and re-issuing would make sense when, for example, keys are lost or compromised, and the issuer has an interest in ensuring the tokens are not financialized and sold off to a party—in other words, when the token signals authentic community membership.” page 28 (Weyl et al., 2022)<sup>25</sup>

Whilst feature “4) Issuer-Arbitrated” is not explicitly defined by Weyl et al. (2022), the authors do suggest that the issuer is the authority for the issued-SBTs revocation and re-issuance functions, equally the feasibility for a Soul to also self-issue, ‘self-certify’ an SBT (Weyl et al., 2022).

It is crucial to understand that the definition provided by Weyl et al. (2022), is intended as theoretical and to only guide early proof-of-concept SBTs<sup>26</sup>, and is intended to be limited by technical complexities rather serve as a comprehensive and persistent definition for SBTs. The decision to define SBTs with the four characteristics identified earlier in this section was based on the smart contract functionality available at the time of writing, the ease of development and the potential significance of each feature (Weyl et al., 2022). Weyl et al. (2022), elaborate on this decision in a footnote at the beginning of the paper, quoted below this paragraph. While there is a lack of written or technical examples of SBTs in the market, it is an open question to understand if developers, researchers and other market participants are aware of Weyl et al. (2022) footnote on the rationale behind the prescribed SBT definition and it’s sole purpose for aiding proof-of-concept SBTs.

- “We have chosen this set of properties not because they are clearly the most desirable collection of characteristics, but because they are easy to implement in the current environment and permit significant functionality” - page 2 (Weyl et al., 2022)

Given the absence of a comprehensive SBT definition, it is imperative to continue discussions and establish a working definition that can clearly guide technical

---

<sup>25</sup> We chose to move this quote under ‘4) Issuer-Arbitrated’ rather than ‘3) Possibly Revocable’ because viewed this quote as more specific to the issuer’s ability to revoke by burning, and re-issue - as the quote is primarily defines the relationship between the issuer and the token, extending beyond just revocation qualities but also re-issuance qualities. An additional point to add for this decision, is the ‘arbitration’ illustrated in the Issuers ability to authoritatively decide on core SBT decisions at all points of the SBTs lifecycle.

<sup>26</sup> Also known as proto-SBTs.

implementations and unify market terminology. To inform a broad SBT definition, a subsequent BGIN SBT research paper is planned for 2023, with a section on SBT features, split into: core, expected, potential and avoided features. To differentiate proof-of-concept SBTs from future iterations, it is necessary ‘proto-SBTs’ (refer clause 7.4) are capable of revocation and superseded by SBTs with recoverability features.

- “**Revocable, transferable tokens are a kind of proto-SBT—serving supportive, placental functions before Soul birth.** These tokens buy time both for wallets to gestate secure, community recovery mechanisms and for a person to succinctly accumulate proto-SBTs that can eventually be burned and re-issued into non-transferable SBTs.” page 28 (Weyl et al., 2022)

This section focuses on SBTs in relation to digital identity standards and the design principles behind the digital identity standard. SBTs have the potential to complement digital identity primitives, which is further explained in clause 7.<sup>27</sup> SBTs differ from established forms of digital identity such as DID/VC and serve as a complementary tool to existing digital identity primitives. In this context, digital identity primitives extend the notion of “property rights” to encompass personal data and privacy since it is inherently owned by myself (“I own my data”), not by anyone else or any institution (Weyl et al., 2022).<sup>28</sup> SBTs on the other hand, take a unique approach by treating personal information and privacy as programmable, creating a pluralistic value network instead of a siloed, self-contained privacy asset. SBTs flexible approach provides an opportunity to create composable or permissioned access to the underlying information, which might be social credentials, affiliations or Government-issued identity documents.

- “Rather than privacy-as-transferable-property-right, a more promising approach is to treat privacy as a programmable, loosely coupled bundle of rights to permission access, alter or profit from information. Under such a paradigm, every SBT—such as an SBT that represents a credential or access to a data store—would ideally also have an implied programmable property right specifying access to the underlying information constituting the SBT: the holders, the agreements between them, the shared property (e.g., data), and obligations to 3rd parties. For example, some issuers

---

<sup>27</sup> There was a comment that digital identity would be the soul, not the SBT, and that SBTs provide some form of verification of a "Soul", specifically as stated, verification of: affiliations, memberships, and credentials. This is to be discussed further.

<sup>28</sup> There are discussions limited to grassroots communities on whether to treat personal data and privacy as “private property” but among identity and privacy professionals this question is settled that they should not be viewed as property right.

- would choose to make SBTs wholly public. Some SBTs, such as a passport or health record, would be private in the self-sovereign sense, with unilateral rights to disclose by Souls who carry the SBT.” page 15, (Weyl et al., 2022)<sup>29</sup>
- “Plural intelligences raise important questions about data privacy. Afterall, to build such powerful intelligences requires pooling data across individuals from large data sets (e.g., health data), or capturing data that isn’t interpersonal but shared (e.g., a social graph). “Self-sovereign identity” advocates tend to treat data as private property: data about this interaction is mine and so I should be able to choose when and to whom to reveal it. However, even more than in the physical economy, the data economy is poorly understood in terms of simple private property.” page 15, (Weyl et al., 2022)

In this clause, we will examine the SBTs as a tool for social coordination and apply rigor to understand the characteristics that contribute to this novel utility (See Appendix C for more detail on “social coordination”). SBTs provide a means to optimise aspects of coordination for various social groups and structures, such as local communities, school alumni association, and shared interest groups. It is worth noting that the smallest community unit could be as small as a family or a couple (in sociological terms, a “dyad”). Furthermore, human identity is established within a community, rather than a sudden singular occurrence; concepts of sudden social connection are often popularized by Nietzsche’s concept of the “overhuman” from “Thus Spoke Zarathustra”.<sup>30</sup>

A unique aspect of SBTs lies in its ability to coordinate in a decentralized bottoms-up manner. Why is this so important? The current world order often relies on Government-issued identity documents to achieve complex multi-directional social coordination, generally across millions of individuals. Government-issued identity documents such as driver's licenses, passports or social welfare cards are the incumbent tool for social coordination and proof of legal identity. It is true that in many jurisdictions, Government-issued IDs may have digitally signed data and tamper

---

<sup>29</sup> Nat Sakimura discusses that while Weyl et al posit it as a new concept, contextual and directional identity and selective disclosure actually is pretty much the consensus in the identity and privacy community. What's new is embodying them in the form of Tokens as a multilateral conduit and social coordination tool. In the traditional ways, they are embodied just as a combination of basic human rights, laws, contracts, industry standards, etc. implemented as access control policies at the policy decision endpoint. This comment suggests that further analysis needs to be conducted to establish a fair comparison of the digital identity management community and the SBTs community.

<sup>30</sup> “Self sovereignty is an illusion, we are social creatures and we have a social membership and affiliations. It might not come into the same form for everybody but at a very least we are born into a family and a region. Even language is a social phenomenon. Zarathustra way is not a view of individuality now or ever” (See Appendix C).

proofing design choices, making it effortless to identify a fake ID but not really identify the owner by possession alone nor complex enough to stop the generation of new fake IDs<sup>31</sup>. How would the restaurant serving alcohol know whether the well-made ID they are shown is fake or not? Weatherford et al. (2021) found that “neither length/type of professional experience nor length/type of training experience affected ID verification performance” based on experiments. This suggests that these Government-issued IDs may not be a perfect way for identity proofing, suggesting a need to question topics on “what is your identity?”. Furthermore, what are the attributes that ‘define’ you, as you and equally how could these attributes assist in commercial transactions, social coordination or in simple practical situations like purchasing alcohol.

Given SBT’s function as a flexible plural-purposed social coordination tool, SBTs differ from other forms of social identity in many ways.<sup>32</sup> Jain et al., (2022) compares SBTs to decentralized identifiers (DIDs) and verifiable credentials (VCs). They also examine the trade-off challenge between abstraction and composability when mapping out different digital identity primitives such as SBTs, DIDs, and VCs (Figure 1).<sup>33</sup> They state that “[t]he challenge is to ensure that solutions work across as many platforms as possible while maintaining the composability within each ecosystem”.<sup>34</sup>

---

<sup>31</sup> Nat Sakimura, points out that Government-issued digital I.D. can be fake-safe are trivial to verify and validate it technically though the wide adoption of the verification technique is yet to be seen. He also points out that even if the verification technique become ubiquitous, as the data set that a government issued I.D. can provide is quite limited, it will not be able to meet varying needs of use-cases . For example, a government issued I.D. typically only shows that the person with that name and gender was born at a certain date; limiting the individuals real-context or social value. Further to the point, Nat discusses that in many cases, Biometric binding is extremely weak: in Japan, it is self-attested and that as a society we need much more in our life. A Government I.D. in isolation is incapable of expressing employment status or other rich social context, where the authoritative source varies based on data point and third-party attested information, not always the government.

<sup>32</sup> There were opinions that all social identity exists in our species to assist individual and social sense-making in order that we can in fact socialize. The opinion follows that if SBTs differ from other forms of social identity, it's not because they are designed to form a social coordination tool. SBTs are in some ways biomimetic, and in a good part they are not. SBTs may be biomimetic in some ways, and heuristically where one can match the qualities of a given feature to an analogue equivalent, there is likely less cause for concern than when and where some quality does not correspond to an analogue equivalent. This is to be discussed in future.

<sup>33</sup> Abstraction solutions work across as many platforms (Jain et al., 2022). Composability is “combining distinct components to create new systems or outputs”. It is also explained that “in software development, composability means developers can reuse existing software components to build new applications” ([Smart contract composability | ethereum.org](https://ethereum.org)).

<sup>34</sup> There were opinions concerning the interpretation of Jain et al. (2022). If abstraction and composability are in trade-off, abstraction may be represented with an arrow going left to right and composability with an arrow going right to left. The orthogonal representation offered in Figure 1 indicates that the individual drawing the image has already concluded that they do not necessarily have a trade-off. The authors are saying there are hundreds of DID methods while accepting that there are zero SBT methods (at present), and so claiming the former lacks composability while maintaining the latter is, I guess, because they believe the SBTs idea will ultimately manifest singularly as one method? If so, this seems odd in a paper on pluralism. The authors indicate they argue for a third way between standardizing too early / too late, but it's unclear what that third way is. It is still in an early stage of digitizing identity and should be discussed with caution and care before advocating it.

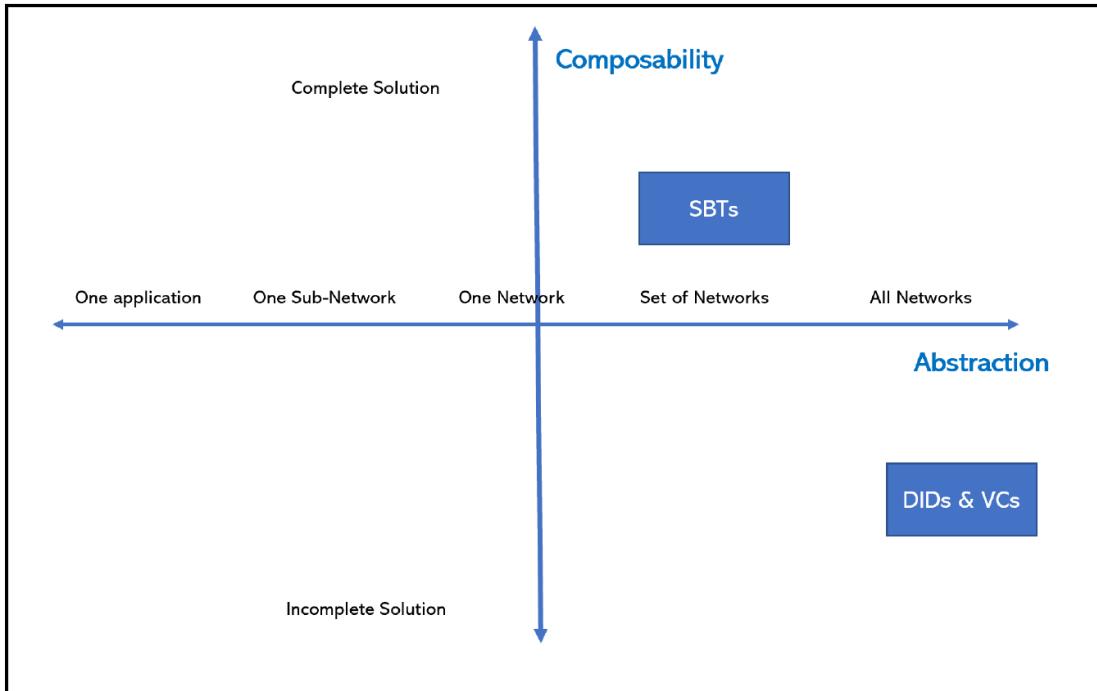


Figure 1 – Current Identity Solutions in the Composability and Abstraction Tradeoff Matrix

(Source) Jain et al. (2022)

In this section, we evaluate fourteen Ethereum Improvement Proposals (EIPs) and Ethereum Request for Comments (ERCs) proposed by the Ethereum development community<sup>35</sup>. We have analyzed these proposals as another set of practical examples to ascertain key features characterizing SBTs. As of January 2023, two ERC standards have reached “Final” status by the Ethereum Foundation, namely ERC-5192 “Minimal Soulbound NFTs” and ERC-5484 “Consensual Soulbound Tokens”.<sup>36</sup> ERC-5192 was the first SBT ERC to achieve “Final” status, marking a historical moment as SBTs officially entered into ERC status. ERC-5484 reached “Final” under a month after ERC-5192. Both standard contracts share the core feature of non-transferability, however, ERC-5192 includes technical parameters to detect the state of transferability, while ERC-5484 focuses on mutual consent between issuer and recipient. Despite two soulbound-centric ERCs achieving final status, further SBT EIPs may inform SBT characteristics, features and standards. A range of proposed ERCs and a diversity of available features would be valuable to formulating distinguishable technical

<sup>35</sup> Nat Sakimura notes that an ERC is not equivalent to a recognised International Standard, but rather shares similarities to a DoC (Disposition of comment) or, in IETF and OIDF, it is a “merged PR” into a draft standard.

<sup>36</sup> According to Ethereum.org, “[a] Final EIP exists in a state of finality and should only be updated to correct errata and add non-normative clarifications”. (<https://eips.ethereum.org/EIPS/eip-1>)

characteristics for SBTs. This aids in mapping a list of viable criteria to define SBTs in comparison to other digital identity primitives, specifically DIDs, VC and possibly NFTs.

Without any universal standard contract, it is valuable to build a framework that could incorporate the features present in the various EIPs listed below.

### List of Soulbound token-related ERC-EIPs:

#### 1 EIP-4671: Non-Tradable Tokens Standard

- Status: Draft (as of January 18th 2023)
- Created: January 13th 2022
- “A non-tradable token, or NTT, represents inherently personal possessions (material or immaterial), such as university diplomas, online training certificates, government issued documents (national id, driving license, visa, wedding, etc.), labels, and so on.”
- “We have seen in the past smart contracts being used to deliver university diplomas or driving licenses, for food labeling or attendance to events, and much more. All of these implementations are different, but they have a common ground: the tokens are non-tradable.”

([EIP-4671: Non-Tradable Tokens Standard \(ethereum.org\)](https://eips.ethereum.org/EIPS/eip-4671))

#### 2 EIP-4973: Account-bound Tokens

- Status: Review (as of January 18th 2023)
- Created: April 1st 2022
- “The Ethereum community has expressed a need for non-transferrable, non-fungible, and socially-priced tokens similar to WoW’s soulbound items. Popular contracts implicitly implement account-bound interaction rights today.”

([EIP-4973: Account-bound Tokens \(ethereum.org\)](https://eips.ethereum.org/EIPS/eip-4973))

#### 3 EIP-5114: Soulbound Badge

- Status: Draft (as of January 18th 2023)
- Created: May 30th 2022
- “Soulbound tokens are meant to be permanent badges/indicators attached to a persona. This means that not only can the user not transfer ownership, but the minter also cannot withdraw/transfer/change ownership as well. This includes mutating or removing any remote content as a means of censoring or manipulating specific users.”

([EIP-5114: Soulbound Badge \(ethereum.org\)](https://eips.ethereum.org/EIPS/eip-5114))

#### 4 EIP-5192: Minimal Soulbound NFTs

- Status: Final (as of January 18th 2023)
  - Created: July 1st 2022
  - “The Ethereum community has expressed a need for non-transferrable, non-fungible, and socially-priced tokens similar to World of Warcraft’s soulbound items. But the lack of a token standard leads many developers to simply throw errors upon a user’s invocation of transfer functionalities.”
- ([EIP-5192: Minimal Soulbound NFTs \(ethereum.org\)](https://ethereum.org))

## 5 EIP-5484: Consensual SBTs

- Status: Final (as of January 18th 2023)
- Created: August 17th 2022
- “This EIP defines an interface extending EIP-721 to create soulbound tokens. Before issuance, both parties (the issuer and the receiver), have to agree on who has the authorization to burn this token. Burn authorization is immutable after declaration. After its issuance, a soulbound token can’t be transferred, but can be burned based on a predetermined immutable burn authorization.”<sup>37</sup>

([EIP-5484: Consensual Soulbound Tokens \(ethereum.org\)](https://ethereum.org))

## 6 EIP-5727: Semi-Fungible Soulbound Token

- Status: Draft (as of January 18th 2023)
- Created: September 28th 2022
- “An interface for soulbound tokens (SBT), which are non-transferable tokens representing a person’s identity, credentials, affiliations, reputation, and private assets. Our interface can handle a combination of fungible and non-fungible tokens in an organized way. It provides a set of core methods that can be used to manage the lifecycle of soulbound tokens, as well as a rich set of extensions that enables DAO governance, privacy protection, token expiration, and account recovery. This interface aims to provide a flexible and extensible framework for the development of soulbound token systems.”

([EIP-5727: Semi-Fungible Soulbound Token \(ethereum.org\)](https://ethereum.org))

## 7 EIP-5516: Soulbound Multi-owner Tokens<sup>38</sup>

- Status: Review (as of January 18th 2023)
- Created: August 19th 2022

---

<sup>37</sup> This would enable key use cases to the expiry revocation discussed above.

<sup>38</sup> How is it different to the current multi-party computation (MPC) wallet implementations or smart contract wallet solutions being built out must be researched further.

- “This EIP proposes a standard interface for non-fungible double signature Soulbound multi-tokens. Previous account-bound token standards face the issue of users losing their account keys or having them rotated, thereby losing their tokens in the process. This EIP provides a solution to this issue that allows for the recycling of SBTs.”

[\(EIP-5516: Soulbound Multi-owner Tokens \(ethereum.org\)\)](https://ethereum.org/en/whitepaper/eip-5516-soulbound-multi-owner-tokens.html)

## 8 EIP-5633: Composable Soulbound NFT, EIP-1155 Extension

- Status: Draft (as of January 18th 2023)
- Created: September 9th 2022
- “This standard is an extension of EIP-1155. It proposes a smart contract interface that can represent any number of soulbound and non-soulbound NFT types. Soulbound is the property of a token that prevents it from being transferred between accounts. This standard allows for each token ID to have its own soulbound property.”

[\(EIP-5633: Composable Soulbound NFT \(ethereum.org\)\)](https://ethereum.org/en/whitepaper/eip-5633-composable-soulbound-nft.html)

## 9 EIP-3525: Semi-Fungible Token

- Status: Final (as of January 18th 2023)
- Created: December 1st 2020
- “This is a standard for semi-fungible tokens. The set of smart contract interfaces described in this document defines an EIP-721 compatible token standard. This standard introduces an <ID, SLOT, VALUE> triple scalar model that represents the semi-fungible structure of a token. It also introduces new transfer models as well as approval models that reflect the semi-fungible nature of the tokens.
- This proposal contains an EIP-721 equivalent ID property to identify itself as a universally unique entity, so that the tokens can be transferred between addresses and approved to be operated in EIP-721 compatible way.”

[\(EIP-3525: Semi-Fungible Token \(ethereum.org\)\)](https://ethereum.org/en/whitepaper/eip-3525-semi-fungible-token.html)

## 10 EIP-5252: Account-bound Finance

- Status: Draft (as of January 18th 2023)
- Created: June 29th 2022
- “This EIP proposes a form of smart contract design pattern and a new type of account abstraction on how one’s finance should be managed, ensuring transparency of managing investments and protection with self-sovereignty even from its financial operators.”

- “This EIP enables greater self-sovereignty of one’s assets using a personal finance contract for each individual. The separation between an investor’s funds and the operation fee is clearly specified in the personal smart contract, so investors can ensure safety from arbitrary loss of funds by the operating team’s control.”
- “This EIP extends EIP-5114 to further enable transferring fund to other accounts for mobility between managing multiple wallets.”

([EIP-5252: Account-bound Finance \(ethereum.org\)](#))

## 11 EIP-4972: Name-Owned Account

- Status: Draft (as of January 18th 2023)
- Created: April 4th 2022
- “This ERC proposes a new type of account - name-owned account (NOA) that is controlled by the owner of the name besides existing externally-owned account (EOA) and contract account (CA). With the new account type, users will be able to transfer/receive tokens using the name-derived address directly instead of the address of the name owner.”
- “A NOA can be used as a social identity with all states on-chain even under 3rd-party or self custody. It also simplifies porting the social identity from one custody to another.”

([EIP-4972: Name-Owned Account \(ethereum.org\)](#))

## 12 EIP-5539: Revocation List Registry

- Status: Draft (as of January 18th 2023)
- Created: August 26th 2022
- “This EIP proposes a set of methods and standards for a role-based registry of indicators aimed for usage in revocations.”

([EIP-5539: Revocation List Registry \(ethereum.org\)](#))

## 13 EIP-5851: On-Chain Verifiable Credentials

- Status: Draft (as of January 18th 2023)
- Created: October 18th 2022
- “This proposal introduces a method of certifying that a particular address meets a claim, and a method of verifying those certifications using on-chain metadata.”
- “Claims are assertions or statements made about a subject having certain properties that may be met conditions (for example: age >= 18), and are certified by issuers using a Soundbound Token (SBT).”

([EIP-5851: On-Chain Verifiable Credentials \(ethereum.org\)](#))

## **14 EIP-6147: Guard of NFT/SBT, an Extension of EIP-721**

- Status: Draft (as of January 18th 2023)
- Created: December 7th 2022
- “This standard is an extension of EIP-721. It separates the holding right and transfer right of non-fungible tokens (NFTs) and Soulbound Tokens (SBTs) and defines a new role, guard. The flexibility of the guard setting enables the design of NFT anti-theft, NFT lending, NFT leasing, SBT, etc.”

[\*\(EIP-6147: Guard of NFT/SBT, an Extension of EIP-721 \(ethereum.org\)\)\*](https://eips.ethereum.org/EIPS/eip-6147)

## **15 EIP-5058: Lockable Non-Fungible Tokens**

- Status: Draft (as of January 23rd 2023)
- Created: April 30th 2022
- “We propose to extend the EIP-721 standard with a secure locking mechanism. The NFT owners approve the operator to lock the NFT through setLockApprovalForAll() or lockApprove(). The approved operator locks the NFT through lock(). The locked NFTs cannot be transferred until the end of the locking period. An immediate use case is to allow NFTs to participate in smart contracts without leaving the wallets of their owners.”

[\*\(EIP-5058: Lockable Non-Fungible Tokens \(ethereum.org\)\)\*](https://eips.ethereum.org/EIPS/eip-5058)

The proposed EIPs and ERCs related to SBTs indicate that non-transferability and a focus on SBTs as stores of social or reputation value are fundamental characteristics; these features consistently appeared throughout our examination of the proposals. While some EIPs may seem disparate or arbitrary to the purpose of this examination, EIPs such as EIP-5539 “Revocation List Registry” were included to provide the reader gestalt visibility of directly relevant and auxiliary proposals. EIP-5539 was included not to overlook the importance of having a revocation registry for SBTs. SBTs defined by revocation features would find a revocation registry complementary and valuable to ensure transparency. A registry has additional significance particularly to early-proof-of-concept SBT’s feature “3) possibly revocable”; features of SBTs are examined earlier in this clause. The exercise of compiling the list of SBT EIPs has proved valuable. As an organization, BGIN will continue to monitor SBT-related EIPs and ERCs, gauging the development community’s perceptions of SBTs and equally surveying prevailing attributes included in SBT proposals. We believe this activity will aid in mapping the capabilities of SBTs and their community-driven purpose.

Our analysis of current SBT EIPs assisted in establishing a framework to evaluate smart contract primitives and draw superficial comparisons to digital identity solutions. Having reviewed the SBT EIPs, we will now proceed to analyze the NFT

standard proposal, followed by an analysis of the original smart contract fundamentals proposed by Nick Szabo (1996). We expect that by examining practical and theoretical documentation on SBTs, NFTs and Smart Contracts, the output will inform distinct characteristics and provide a framework for comparison.

We first examine the EIP-721 “Non-Fungible Token Standard” to understand the rationale and utility behind NFTs.

- “NFTs are distinguishable and you must track the ownership of each one separately.”
- “We considered use cases of NFTs being owned and transacted by individuals as well as consignment to third party brokers/wallets/auctioneers (“operators”). NFTs can represent ownership over digital or physical assets.”
- “It is critical in each of these cases that these items are not “lumped together” as numbers in a ledger, but instead each asset must have its ownership individually and atomically tracked. Regardless of the nature of these assets, the ecosystem will be stronger if we have a standardized interface that allows for cross-functional asset management and sales platforms.”

([EIP-721: Non-Fungible Token Standard \(ethereum.org\)](https://ethereum.org))

We observed in the proposed standards for NFTs in EIP-721, that NFTs are defined by five key characteristics including:

#### Five observed characteristics of NFTs<sup>39</sup>:

- 1 Distinguishable ownership
- 2 Transferability rights
- 3 Indivisible
- 4 Publicly visible
- 5 Store of capital value

Lastly, we examine Nick Szabo’s seminal work “Smart Contracts: Building Blocks for Digital Markets” (1996), which establishes four basic objectives of smart contract design<sup>40</sup>. These principles will serve as a foundation for comparing the various smart contract primitives and have the potential to inform a framework for comparing smart

---

<sup>39</sup> These characteristics should be explored in the BGIN NFT working study paper

[BGIN\\_PWI\\_SR005\\_NFT Study Report Part1 - Google Docs \(bgin-global.org\)](https://bgin-global.org) or in a new paper.

<sup>40</sup> The authors are aware that Nick Szabo’s work on Smart Contracts was primarily theoretical and predates current smart contract applications by 20 years - however, it is important to note the significant impact Nick Szabo has had on the blockchain ecosystem. Revisiting Nick Szabo’s work has been monumental, and can be attributed throughout this paper as playing a significant role in progressing the research established in this paper and hope that presenting Nick Szabo’s concepts in modern context will give his work a second life.

contract-enabled digital identity primitives. These are the following four basic objectives of smart contract design (Szabo, 1996):

### **Four basic objectives of smart contracts:**

#### **1 Observability**

“The first of these is observability, the ability of the principals to observe each others' performance of the contract, or to prove their performance to other principals.”

#### **2 Verifiability**

“A second objective verifiability, the ability of a principal to prove to an arbitrator that a contract has been performed or breached, or the ability of the arbitrator to find this out by other means. The disciplines of auditing and investigation roughly correspond with verification of contract performance. Observability and verifiability can also include the ability to differentiate between intentional violations of the contract and good.”

#### **3 Privity**

“A third objective of contract design is privity, the principle that knowledge and control over the contents and performance of a contract should be distributed among parties only as much as is necessary for the performance of that contract. This is a generalization of the common law principle of contract privity, which states that third parties, other than the designated arbitrators and intermediaries, should have no say in the enforcement of a contract.”

#### **4 Enforceability**

“A fourth objective is enforceability, and at the same time minimizing the need for enforcement. Improved verifiability often also helps meet this fourth objective. Reputation, built-in incentives, "self-enforcing" protocols, and verifiability can all play a strong part in meeting the fourth objective. Computer and network security also can contribute greatly to making smart contracts self-enforcing.”

([Nick Szabo -- Smart Contracts: Building Blocks for Digital Markets \(uva.nl\)](#))

Given the distinction between SBTs, SSI with DIDs and NFTs, we propose a framework for evaluating their relative utility and applicability without implying any inherent superiority or deficiencies. This framework also does not intend to suggest that these concepts are equivalent or easily interchangeable but rather seeks to provide a means for understanding these concepts' relative attributes and affordances. In

addition, this comparison aims to understand SBTs in relation to familiar and well-established concepts. The proposed criteria for comparison is as follows:

**Proposed criteria for comparison:**

- 1 Motivator:** What is the main motivation behind it?
- 2 Transferability:** Can ownership be redesignated via a transfer or other means?
- 3 Fungibility:** Can it replace or be replaced by another alternative and treated exactly the same?
- 4 Privity:** Third parties unless designated, should have no say.
- 5 Social Recovery:** Upon losing the access credential, could it be recovered by the majority of consent from the qualified member of the community?
- 6 Standardized at an SDO:** Is there consensus on the standard?

Using these criteria, we compare the difference between the self-sovereign identity (SSI) with DIDs, NFTs, and SBTs (Table 1).

Table 1– Comparison between the SSI with DIDs, NFTs, and SBTs

	SSI with DIDs	NFTs	SBTs
Motivations	Decouple entity authentication from centralized registries, identity providers, and certificate authorities <sup>41</sup>	Tracking distinguishable assets <sup>42</sup>	Encode real economy trust networks to establish provenance and reputation within decentralized environments. <sup>43</sup>
Transferability	Some custody of the DIDs are transferable	YES	NO
Fungibility	Depends on the DIDs and its ecosystem	NO	Based on the use case, can be both fungible, non-fungible, and semi-fungible <sup>44</sup>
Privity	YES	NO	YES
Social Recovery	Depends on the DIDs and its ecosystem	NO	YES
Standardized at an SDO	DIDs are standardized at W3C	Standardized through Ethereum EIP. However, the implementation of the standard is different across chains and contracts.	Not standardized (In the process of adding standards through Ethereum Improvement Proposal (EIP))

(Source) Prepared by the authors.

It is essential to understand the distinct motivations, which leads to a fundamental difference in their characteristics.

<sup>41</sup> According to the official standard “Decentralized Identifiers (DIDs) v1.0” adopted by the World Wide Web Consortium (W3C), “DIDs have been designed so that identity may be decoupled from centralized registries, identity providers, and certificate authorities” and “the design enables the controller of a DID to prove control over it without requiring permission from any other party” (W3C, 2022).

<sup>42</sup> The Ethereum Improvement Proposals “EIP-721: Non-Fungible Token Standard” states that “NFTs are distinguishable and you must track the ownership of each one separately”.

<sup>43</sup> There was an opinion that it is the decentralized verification of the attributes, i.e. the affiliations, membership, and credentials. These may or may not establish an identity, though they may lend credibility of identity in some part to the soul that holds them.

<sup>44</sup> The fungibility of SBTs remains a question but the true value of SBTs would lie when it is non-fungible.

One of the salient features of future SBTs and Souls, is social recovery mechanisms. While the concept of ‘Soul’ is not explored in great detail within this paper, the authors have decided to use this term to elaborate on the relationship between an SBT being a single data point or token, and the Soul being the container of these data points or tokens. The Soul can be representative of a wallet (as prescribed by Weyl et al., 2022), an individual, an entity or even a group. The authors of this paper are curious to explore souls in greater detail, as it would be valuable to understand why wallets are insufficient in holding both capital value assets and reputation value assets, or to question if the challenge is technical but moreover informative for the holder of the soul and those interacting with the soul; could it be preferential to separate the value dichotomy so that soul interactions are based on merit rather than capital?

Buterin (2021) suggests in the article “Why we need wide adoption of social recovery wallets” and that “the whole point of digital technology, blockchains included, is to make it easier for humans to engage in very complicated tasks without having to exert extreme mental effort or live in constant fear of making mistakes” and therefore a Soul wallet design which satisfies the following three key criteria is necessary:

### Three Soul Wallet Design Objectives:

- 1 **No single point of failure:** there is no single thing (and ideally, no collection of things which travel together) which, if stolen, can give an attacker access to your funds, or if lost, can deny you access to your funds.<sup>45</sup>
- 2 **Low mental overhead:** as much as possible, it should not require users to learn strange new habits or exert mental effort to always remember to follow certain patterns of behavior.
- 3 **Maximum ease of transacting:** most normal activities should not require much more effort than they do in regular wallets (eg. Status, Metamask...)

[\(Why we need wide adoption of social recovery wallets \(vitalik.ca\)\)](https://vitalik.ca/2021/05/20/why-we-need-wide-adoption-of-social-recovery-wallets.html)

Weyl et al. (2022) note that “[b]y embedding security in sociality, a Soul can always regenerate their keys through community recovery, which deters Soul theft (or sale): because a Seller would need to prove selling the recovery relationships, any attempt to sell a Soul lacks credibility”.<sup>46</sup>

Social or communal recovery is not novel to souls/SBTs. In fact, it was leveraged by Facebook as a “Trusted Contact” in 2013 as a way to recover a Facebook account. According to Facebook (2013), it was aimed to “give you more control over your account security, you can now choose and manage your trusted contacts anytime from

---

<sup>45</sup> A single point of failure goes much deeper than the carrying of the wallet.

<sup>46</sup> There was a discussion on whether it is the soul that needs to be socially recoverable, not an SBTs.

your Security Settings, instead of only when you're having trouble accessing your account". It assures that "[w]ith trusted contacts, there's no need to worry about remembering the answer to your security question or filling out long web forms to prove who you are. You can recover your account with help from your friends". The process is as follows.

### **Example of social recovery: Facebook Trusted Contacts:**

- **[Setting Up Facebook Trusted Contacts]**
  - Choose people you trust, like friends you would give a spare key to your house.
  - Choose people you can reach without using Facebook, ideally over the phone or in person, since you'll need to contact them when you cannot log in.
  - Choose more people to help you. The more friends you choose, the more people who can help you when you need it.
- **[Using Facebook Trusted Contacts]**
  - Once you have set up your trusted contacts, if you ever have trouble logging in, you'll have your trusted contacts as an option to help. You just need to call your trusted contacts and let them know you need their help to regain access to your account. Each of them can get a security code for you with instructions on how to help you. Once you get three security codes from your trusted contacts, you can enter them into Facebook to recover your account.

### (Facebook) Introducing Trusted Contacts)

However, Facebook stopped supporting this "Trusted Contact" in 2022 (Facebook, 2022). The case of Facebook's "Trusted Contact" feature highlights the limitations and risks associated to centralised systems in terms of social recovery. Despite this initiative promising greater autonomy and giving users additional control of their account security, it still remained vulnerable to a single point of failure and the centralised authorities arbitrating the revocation of the entire social recovery mechanism. This examples shows that social recovery as a centralised system's promise of "give you more control over your account security" could be easily forfeited and naturally discounted. In contrast, SBTs offer a decentralised approach to social recovery by distributing points of authentication and recovery, removing a single-point centralisation risk.

At the same time, although not publicly stated, the intention behind stopping this "Trusted Contact" system was because of security breaches that could result in the loss

of user's accounts and theft of personal data. Users were easily fooled into setting malicious actors as trusted contacts and thus, entire accounts were taken over by the socially engineered contacts.

Another core SBT feature is "programmable privacy". The programmable privacy feature allows for a flexible and customisable approach to managing data visibility and access controls of the SBT. This feature is meant to supersede the early proof-of-concept SBTs or proto-SBT's first feature "1) publicly visible" mentioned previously in clause 6. Publicly visible features are expected to discontinue, as preference for programmable privacy. Privacy-preserving features such as zero-knowledge proofs may make fixed features such as publicly visible redundant. Currently, it is an idea "to treat privacy as a programmable, loosely coupled bundle of rights to permission access, alter or profit from information" (Weyl et al., 2022). Effective programmable privacy and social recovery are closely intertwined since visible information may vary depending on the sensitivity of the data within the SBT. Practically an SBT could contain the social status of a soul alongside their affiliation to a community, or another soul or not - potentially obfuscating irrelevant or requiring a level of reputation value before composing the SBT (adverse selection is explored in clause 7.2).

The Verifiable Credentials (VCs) are conceptually in a different layer to the SSI with DIDs, NFTs, and SBTs and, therefore, inappropriate to compare side-by-side. VCs do not require to be on a blockchain or decentralized applications, nor do DIDs. Since VCs is an umbrella term which does not define the technical design, they have the potential to be both SSI and SBTs.

## 7. The Design on SBTs and the Ecosystem

### 7.1 Introduction

*"While blockchain inclusion enables us to trace the time a particular work was made, SBTs would enable us to trace the social provenance"* page 3 (Weyl et al., 2022)

This section discusses the detailed design of SBTs and the Soul as a tool for social coordination. The structure of this section is as follows. First, we start by examining SBTs fundamental design for social coordination and the principles essential to consider. Followed by a discussion on the life cycle management of both SBTs and the Soul communities. Lastly, we will reflect on proto-SBT; the early iterations of SBTs.

## 7.2 Fundamental Design for “Social Coordination”

Taking into account the characteristics of the SBTs described in clause 6, this section delves deeper into the practical design features of SBTs with a focus on the properties and principles that contribute to their function for social coordination. It is fundamental to elaborate the “social coordination” aspect of SBTs and equally emphasize the need for appropriate discussion on the safety and governance consequences throughout our research.

Exploring SBT’s essential features, Weyl et al. (2022) outlined that SBTs could be self-certified. Understandably, issues surface and challenges can be made to verify the authenticity of an SBT. The issue compounds if multiple people issue and self-certify the same SBT. If multiple students self-certify a SBT of their bachelors degree, the value of the token may be called into question and without verification from an authoritative source<sup>47</sup>; the university. To address this issue, authoritative sources such as universities may choose to either: 1) attest to the authenticity of a self-certified SBT or; 2) issue an SBT that supersedes any previously held or self-certified SBT.

Expanding upon this example, the University may retrospectively approve an education SBT that a student has self-issued and self-certified. Equally, the University may proactively issue the education SBT to the same student. In both cases, the student has an authenticated University SBT.

Universities can be recognised as ‘high-status’ institutions, so the possible reputation stored in a university issued SBT can be considered to be high or the ‘heavy’. University-issued SBTs have the potential to serve as a foundation to a decentralized society, where recognised intelligence is valued digitally without requiring a superficial capital value. In order for SBTs to effectively aid in social coordination, the authenticity of the SBT should be considered as an essential criterion. Concepts of authenticity are explored and expressed as a key issue “Provenance is established by calling up the 3rd party for a confirmation.” (Weyl et al., 2022). Authenticity is vital if an SBT attests to or implies value that only an authoritative source could verify, with the number of ‘relevant’ authoritative sources attesting exponentially increasing an SBTs integrity<sup>48</sup>. Authenticity is an attribute aligned to the interaction or affiliation between an SBT and another Soul or issuer that proves the relationship or utility. Additionally, the trustworthiness of all stakeholders involved in an SBTs lifecycle should be carefully considered. Relevant

---

<sup>47</sup> Nat Sakimura comments that “in the field of identity management, it is common to introduce the notion of an authoritative source. For university degrees, the university is the authoritative source. For one’s food preference, then the person is the authoritative source, while what Facebook guesses, while it may be a third-party attested claim, is not authoritative. So, the level of trust that can be derived and first-party/third-party is actually orthogonal.”

<sup>48</sup> Nat Sakimura comments that “The hard part is to find if the signer/issuer is actually authoritative. Usually, it is done in Top-down fashion. Trust chain is formed from the root authority in the country - National accreditation agency etc. That obviously is not very decentralized. It is known as PKI. An alternative scheme is through the network of peer evaluations. This is where SBT would potentially shine.”

stakeholders in the ‘soulsystem’<sup>49</sup> could include the issuer, holder, contract creator, verifier, authoritative source and potentially the witnesses or guardians involved in Soul or SBT lifecycles. Authenticity and stakeholder trustworthiness are issues closely related to the early-proof-of-concept SBTs or proto-SBTs. These proto-SBTs underpin the beginning of a decentralized society, which will be explored further in the follow on BGIN SBT part 2 research paper planned for 2023.

In our discussions we have outlined how the value of an SBT could be relative to the attestation by multiple authoritative sources, a single authoritative source or no-authoritative source. Understandably, the value of an SBT could be calculated by  $N$  authoritative sources multiplied by the average trustworthiness of each authoritative source. The authors of this paper plan to explore a reputation formula commonly used in management consulting, called “The Trust Equation”<sup>50</sup> in the following BGIN SBT paper part 2. We found this equation to be effective in peer-to-peer situations, but we have not tested this formula at scale.

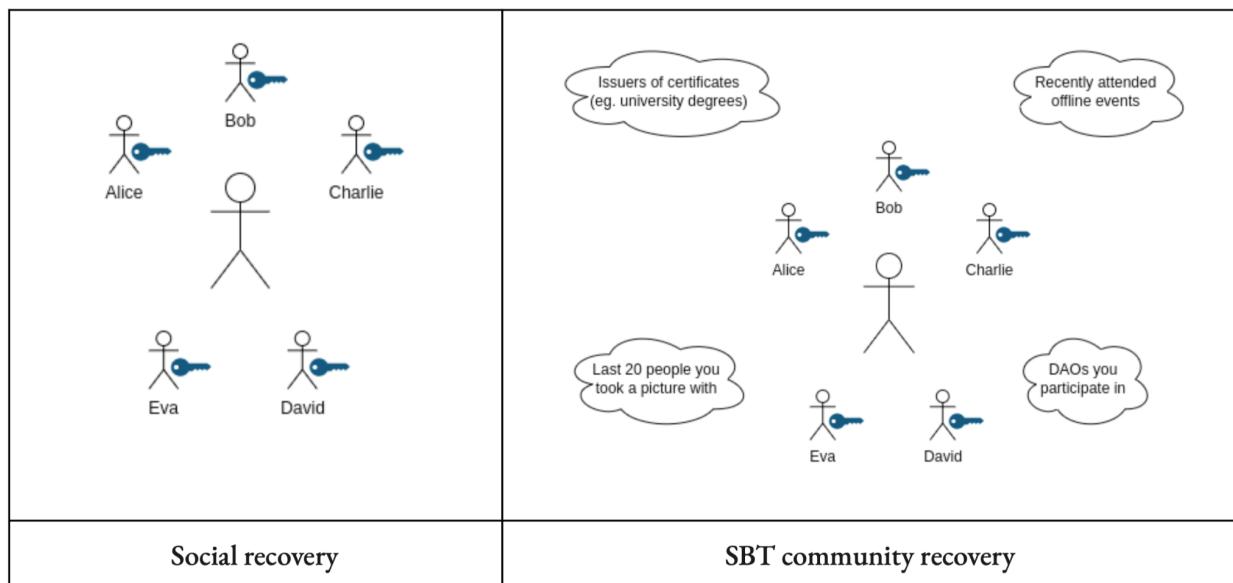
An authentic SBT could be assumed to be a neutral-status SBT that has an implied purpose or reputational value that can only be derived by the issuance or approval by an intermediary, primarily an authoritative source. Self-certified SBTs that lack an authoritative source’s attestation could potentially be labeled as a ‘superficial SBT’ or low-status SBT. This also presents an opportunity to impart high-value to SBTs attested by multiple authoritative sources leading to the SBT to be considered ‘comprehensive’. It is important to recognise the challenges that arise out of “trusted” parties arbitrating authenticity - especially within decentralized ecosystems. One of the issues considered by the authors and suggested by Sakimura in the course of our discussion, is on issues of “one-directional third-party attestation”. The first issue of such a system is determining if a signer or issuer is actually authoritative, which comes with its own issues since the method of determining an authority is top-down and arbitrated by another authority, generally the state. As suggested by Nat Sakimura in footnote 48, exploring networks of peer-evaluation may prove valuable and be an opportunity for SBTs, meeting decentralized requirements and maintaining the integrity of an SBT. The second issue from one-directional third-party attestation, is that the top-down system that initially empowered an authoritative source is generally difficult for an individual to fight against, suggesting that the implementation of these authoritative sources within blockchain may lead to its own demise. The third issue is if an “authoritative source” unilaterally attests reputation value and the receiving party is

---

<sup>49</sup> The authors of this paper have attempted to establish soulbound token and soul-relevant terminology. The authors define Soulsystem, as the collection of stakeholders relevant to the lifecycle of an SBT and Soul. The necessity to create new terminology specific to Soul related activities, stakeholders, token and soul management and categorisation of terms, are to help separate terminology that may prove confusing or diminishing.

<sup>50</sup> The Trust Equation is a commonly used formula in management consulting, created by Charles H. Green (Maister et al., 2001). The trust equation: Trustworthiness = (Credibility + Reliability + Intimacy)/Self-orientation; or  $T=(C+R+I)/S$ .

unable to dispute or challenge the attestation. For example, if an individual is considered high-status because they are a celebrity, or recognised within an industry, a low-ranking university may want to claim affiliation and issue a certificate<sup>51</sup>. If the individual is required to consent to the creation of the certificate, reputation exploitation like this becomes increasingly challenging to attempt. Furthermore, a system of plural peer-determination could disincentive bad actors such as the university in the previous example attempting to inflate their reputation, could have their reputation affected by the plural network voting against the university.



(Source) Weyl et al. (2022)

Another fundamental design choice to aid social coordination is SBTs future recoverability features, specifically through the ability to socially or communally recover credentials (or even authenticate). The recoverability feature still allows the ‘possibly revocable’ feature initially explored in clause 6 and with the aided potential to ‘waning SBTs’, or ‘diminishing SBTs’. Where revocable-based features insinuate centralized arbitration and ‘removal’ or re-issuance of an SBT, recoverability features align to decentralized based values, valuing the distributed mechanism to communally ‘recovery’ an SBT that is out of place (Weyl et al., 2022). Recovery is in principle, nominated by the soul and achieved by a social community (potentially but not

<sup>51</sup> Nat Sakimura suggested that “Another problem of the one-directional third-party attestation in the traditional top-down trust chain is that it is relatively hard for an individual to fight against an organization that tries to unilaterally attest. Suppose you became a celebrity. A low-rank university may want to claim that you are an alumnus and issue a certificate for M.A. or something. If such a "certificate" requires the cooperation of the person to create, then this kind of attack becomes much harder to launch. Also, when such activities are found, the peer review would result in a lower reputation for the university.” This point was further elaborated and a second issue was also added.

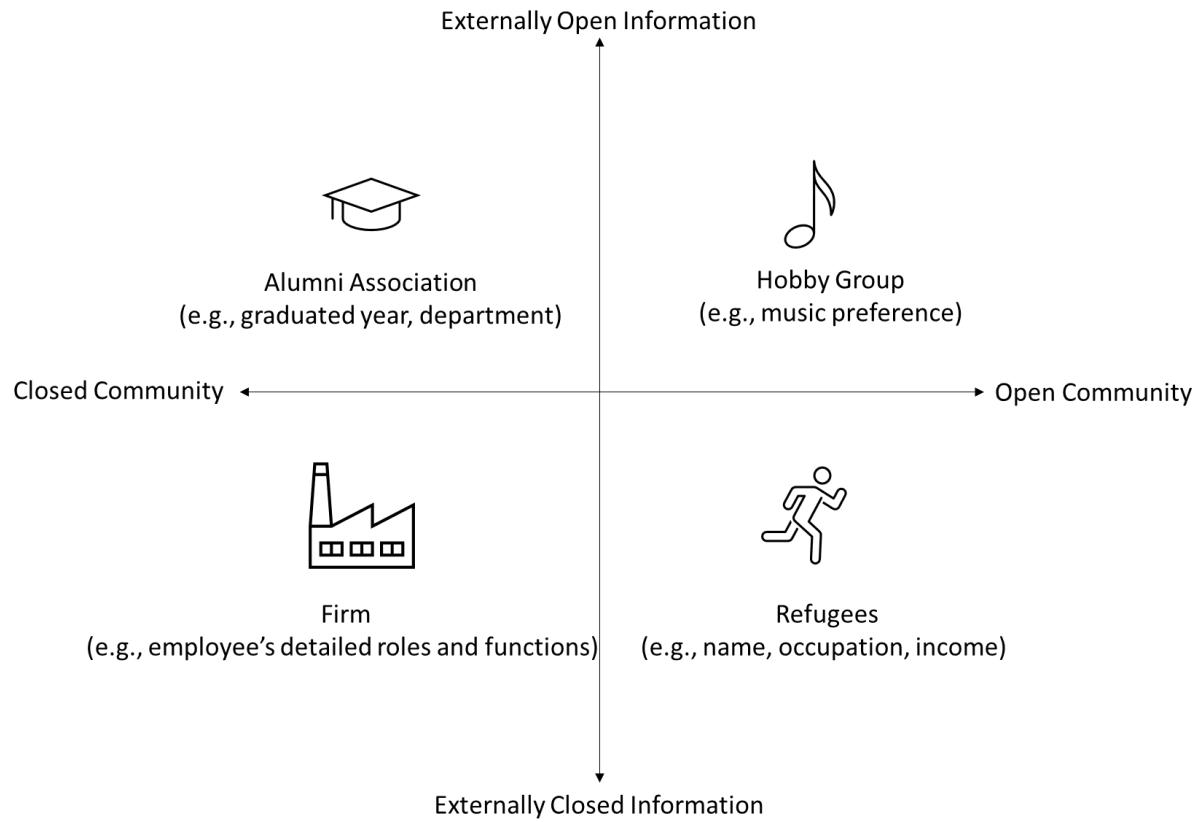
necessarily inclusive of the issuer). In comparison, revoking is requested by the soul or the issuer and arbitrated by the issuer and/or the soul. The distinction between recoverability and revocability lies in decision-making powers and the defined arbitrator. An SBT design that prioritizes only revocability features without recoverability raises concerns about the sovereignty of the soul and the control issuers have over this layer.<sup>52</sup> The difference between recoverability and revocability is where the choice lies, whether with the issuer or both the issuer and the Soul.

In addition, for SBTs, the identifiers are assumed to be initially publicly visible to allow for a proof of concept, with plans to enable programmable privacy for “complex set of expectations and agreements” (Weyl et al., 2022). The level of transparency is co-determined by the community the “Soul” is associated with. This is important as the concept of privacy and tolerance varies between cultures and communities, whereby the rich-context of relationships and communal structures give guidance on the technological affordances available or potentially even visible. Privacy is expected to vary between cultures and communities, and individual's plural affiliations and participation. For example, the level of confidence in privacy differs in a secondary school setting (name and year is open, but grades private) versus to the context of a bar (whether or not you are above age to be allowed entry is apparent, but other information such as names, date of birth, occupation is usually kept private). SBTs allow for “programmable privacy” based on the consensus of the social group that is issuing the token.<sup>53</sup> Figure 2 depicts the image of what kind of choice the community would likely have for the purpose of better understanding.

---

<sup>52</sup> It is worth acknowledging that “recoverability” and “reissuance” are different. SBT community can prevent recoverability for immutability, but reissue a new SBT to supersede the old.

<sup>53</sup> To achieve privacy in the SBTs, Weyl et al. (2022) mentions zero-knowledge proof, but how to technically achieve “programmable privacy” still remains a question.



**Figure 2 – Examples of Community’s Social Group and Preference**  
 (Source) Prepared by the authors.

Although we have mentioned that their privacy preference differs in each social group, there are principles that must be considered. For example, the ISO and IEC have framed “11 Principles of Privacy” as follows in the ISO 29100 (Table 2).

Table 2 The Privacy Principles of ISO/IEC 29100

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10.Information security
11.Privacy compliance

(Source: ISO/IEC(2011))

The basic principles of digital identity should be applied to SBTs (Figure 3). It is important to consider how these principles could be embedded in the design and usage.

<p>“The Laws of Identity” (Cameron, 2005)</p> <ol style="list-style-type: none"> <li>1. User Control and Consent</li> <li>2. Minimal Disclosure for a Constrained Use</li> <li>3. Justifiable Parties</li> <li>4. Directed Identity</li> <li>5. Pluralism of Operators and Technologies</li> <li>6. Human Integration</li> <li>7. Consistent Experience Across Contexts</li> </ol>	<p>“The Seven Principles of Digital Being” (Sakimura, 2021)</p> <ol style="list-style-type: none"> <li>1. Accountable Digital Being</li> <li>2. Expressive Digital Being</li> <li>3. Fair Data Handling</li> <li>4. Right NOT to be Forgotten</li> <li>5. Human Friendly</li> <li>6. Adoption Friendly</li> <li>7. Everyone benefit</li> </ol>
--	--

Figure 3 – Basic Principles

(Source) Cameron (2005), Sakimura (2021)

Cameron (2005) identifies the “The Laws of Identity” which the identity system has to obey as follows.

**1 User Control and Consent:**

Technical identity systems must only reveal information identifying a user with the user's consent

**2 Minimal Disclosure for a Constrained Use:**

The solution which discloses the least amount of identifying information and best limits its use is the most stable long-term solution.

**3 Justifiable Parties:**

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

**4 Directed Identity:**

A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

**5 Pluralism of Operators and Technologies:**

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers

**6 Human Integration:**

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks

**7 Consistent Experience Across Contexts:**

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Sakimura (2021) suggests "The Seven Principles of Digital Being" necessary to make our digital life safe.

**1 Accountable Digital Being:**

Anyone can establish and re-establish a digital presence where they themselves are held accountable for their actions.

## **2 Expressive Digital Being:**

Each person can express themselves through their digital existence, using data attested by others and self-expressed data about their own nature.

## **3 Fair Data Handling:**

Ensure that all participants adhere to the principles of privacy with respect to the handling of data concerning each individual and that the purposes for which the data is handled are not harmful to the individual concerned.

## **4 Right NOT to be Forgotten:**

Technical measures are taken to ensure that digital existence is not pretended or attributes are not rewritten.

## **5 Human Friendly:**

The system shall take into account the asymmetry of information between individuals and legal entities, the limited rationality of individuals, and the socially vulnerable.

## **6 Adoption Friendly:**

Technology is open, leverages existing infrastructure as much as possible, and is continually tested to ensure interoperability.

## **7 Everyone Benefit:**

Individuals, businesses, and governments benefit from this system. Otherwise, the system would not be implemented, for it would not stand as a system.

In relation to the SBTs, it is inseparable from the Soul. With the premise that Soul has the right to reveal SBTs and certain subsets of their data, “4) Right NOT to be Forgotten” and “right to be forgotten” similarities could be drawn that these features originate from the same token. “Right to be forgotten” is about the erasure of any of you’re underlying data, the “Soul” burning the underlying SBT. “Right not to be forgotten” is about not changing the state of the underlying data or duplication to another database. The latter is in conflict of data erasure.<sup>54</sup>

“Les Misérables” a 19-century novel written by Victor Hugo depicts this problem. Jean Valjean is living a respectable and successful life, is suddenly shadowed by

---

<sup>54</sup> The “right NOT to be forgotten” might be implemented for example as an “once-only” policy, in which the state is not allowed to ask citizens for the same information twice. The Estonian government introduced this principle in 2007 ('You can't use 18th century law for a digital world' (euobserver.com)).

Inspecteur Javert who reveals Jean Valjean's past history to the public. As a result, Jean Valjean's life and career are ruined. The novel might have had a different ending much more had Inspecteur Javert or the community "forgot", or in other words, had the past history faded. This is why there are cases in identity where "right to be forgotten" is a principle that should be recognised.

The concepts of "right to be forgotten" and "right not to be forgotten" have parallels in the General Data Protection Regulation (GDPR), specifically in Recital 65 (right of rectification and erasure), Recital 66 (Right to be forgotten), and Article 17 (Right to erasure). In light of these legal considerations, a fundamental design feature for SBTs should reflect the principle of "the right to be forgotten"; ensuring that individuals have the ability to exercise control over their SBTs; especially SBTs containing personal data, to mitigate the negative consequences of data leaks. In addition to the "4) Right NOT to be Forgotten" should be applied as an SBT's design principle.

It is a topic of further research to study the tension between a Soul, and a social group. This paper does not provide a philosophical judgment on SBT use cases nor frame the normative ethics of SBTs. However, to apply rigor in examining the functional relationships that Souls seek or avoid with social groups, (at all scales and vice versa), we have analyzed how a binary value system of SBTs may lead to rich social economics. For simplicity, and with great caution, we will elaborate on this social economic model by presenting the existence of a 1) positive SBT, and a 2) negative SBT, in which the binary value is determined by the Soul holding the SBT but validated by society; either in centralized fashion with an authoritative source or in decentralized fashion with a plural peer evaluation mechanism. Superficially, a positive SBT is beneficial, and desirable, and the Soul desires the SBT to persist infinitely and potentially desires the SBT to be publicly visible. Whereas a negative SBT is detrimental and undesirable, and the Soul desires that the negative-SBT ceases to exist or at the minimum remains hidden. Where these attributes are in the interest of the Soul, potentially oppose the interests of a social group - where context and relevance prevail<sup>55</sup>. A social group may desire for positive SBTs to fade over time to ensure the Soul maintains the SBT to continue being worthy of the positive SBT. A social group may also desire for negative SBTs to persist or, at the minimum, remain publicly visible to inform others of the Soul's negative credentials. While the section does not seek to provide a practical system to define the binary value of SBTs, it does however explore

---

<sup>55</sup> While one group or a soul considers an SBT to be 'positive' another group or soul may consider the same SBT 'negative' - attempts to censor may dismantle decentralized society. Instead, allowing plural networks of social groups to co-determine normative behavior attributes and affiliations considered negative by the wider populace may disincentive owning that specific SBT leading to grassroots social determination. This may be considered slow at first but beneficial in the long term as the decentralized society determines ethics without the need for a single authority to arbitrate a top-down decision.

the possibility of tension that can arise from conflicting interests to evaluate future SBT research and development.

Three variables to evaluate reputation economics in pseudonymous environments were proposed by Nick Szabo in “Formalizing and Securing Relationships on Public Networks” (1997), which are: operating value, throw-away value and replacement value. Nick Szabo also cites Peter Swire’s (1997) work that suggests two additional variables that arise from reputation economics concerning loans that are insufficiently secured by capital or reputation: adverse selection, and the endgame problem (Szabo, 1997; Swire, 1997). Together a simple five-point framework is established to evaluate reputation economics, and in the context of this paper, the listed concepts provide a means to evaluate reputation value stored in SBTs in relation to the Soul. These are the five variables of reputation economics:

### **Five variables of reputation economics:**

#### **1 Operating value:**

- Expected future profit, given the reputation

#### **2 Throw-away value:**

- Profit from cheating, which ruins reputation

#### **3 Replacement cost:**

- Cost of recreating reputation
- Combine costs - initial cost, replacement cost, loss of operating value

#### **4 Adverse selection:**

- Entrants without positive reputation can be rejected
- This could also include minimum positive reputation requirements
- From the perspective of other entities

#### **5 The endgame problem:**

- The replacement cost has to be greater than the throw-away value or positive reputation accrued can systematically profit.
- From the perspective of other entities

There are dozens of nuanced variables to consider in evaluating reputation, and for the purpose of this paper, we chose to explore this model in the subsequent BGIN Soulbond Token Paper planned for 2023. In the following paper, we evaluate the value of a bachelor degree SBTs by posing each variable as a question, answered by a low,

medium, or high measure. Examples of reputation models and formulas are of great interest to the authors of this paper and contributions to this controversial side of SBT research is greatly valued.

To build a robust ecosystem that benefits all stakeholders, including individuals, businesses, and governments, it is essential that SBTs and the soulsystem<sup>56</sup> adhere to the principles of “The Laws of Identity” and “The Seven Principles of Digital Being”. These principles serve as the foundation for the function of SBT adopted by social communities and promote positive inter-social-community relationships, facilitating co-determined, positive plural social economies. While individual social communities are empowered to implement additional rules and internal guidelines creating frameworks on socially acceptable behaviors, it will be up to the social communities to govern whether to apply further rules and resolutions beyond these principles, provided that they comply with applicable laws and ordinances. Furthermore, to safeguard the rights and interests of “souls”, it is necessary to develop a system built with programmatic societal guardrails that provide access to these principles. To this point, the mentioned principles are understood, deployed and operated effectively by the community. This recommendation seeks to provide digital communities considering SBTs as a solution for social coordination, a framework that treats each soul with dignity and respect, while equally affording innovation and plural network implementation.

## 7.3 Lifecycle Management

It is without surprise that SBTs do not appear spontaneously, nor evaporate randomly. A comprehensive understanding of SBTs must consider SBTs inherent characteristics and features as discussed in clause 6, but also motivations that facilitate social coordination in decentralized societies. In order to achieve this monumental goal, it is essential to look beyond short-term horizons and adopt long-term perspectives. In this context and direction, considerations around a SBTs lifecycle are critical to the design process. This includes taking into account the various stages, definitions, issuing and depreciation of SBTs that Souls and the Soul communities may encounter during development. Below is the framework mapping the different stages SBTs and SBT communities would have to take into account.

### [The lifecycle of SBTs]

#### 1 Generate:

- SBT is issued and belongs to a social community. SBTs could be self-issued and retrospectively authenticated, or SBTs could be issued by

---

<sup>56</sup> The authors define Soulsystem, as the collection of stakeholders relevant to the lifecycle of an SBT or Soul.

a trusted third party or party whose reputation propagates the value of the issued SBT.

- The trusted third party has to be defined and means of verifying ‘trustworthiness’ or “proof of reputation”. Equally, it is important to consider the potential risks associated with reputation being tied to one’s connections, as being well connected does not necessarily equate to being trustworthy.
- A SBT can potentially “represent” or “express” the affiliation or relationship to a reputational value by the self-determination of the soul or the community, whereby self-determination will generally not hold high-value without the substantiation by another third-party or means that can confirm a proof of reputation; such as an authoritative source.
- A negative reputation could be encompassed within a social community but generally, according to Nick Szabo (1996) "that party would prefer not to reveal a negative credential such as a bad credit rating".<sup>57</sup> From this we can infer that negative SBTs will be difficult to determine on face-value and to the detriment of the Soul would assist a community if the negative SBT was natively publicly visible as discussed briefly in clause 7.2.

## 2 Update:

- Append the information when necessary to account for the current identity.
- Dynamic SBTs may prove to be useful in SBT development to account for the dynamic and multi-dimensional features of social credentials and reputation value
- Digital identity solutions have used offline biometrics localised to users phones to refresh credentials, a similar method could be used to ensure the Soul and the underlying SBTs remain in possession of the intended holder by biometrically unlocking SBTs or initiating composure of the SBT

## 3 Fade:

- The antithesis to “update”. If an SBTs value is correlated to a variable value (potentially timestamp related), the distance between the two values would understandably affect the value of the SBT. Potentially similar to “forgetting”. This is reflecting the “right to be forgotten” design principles. This expiry is similar to a burn mechanism.
- Possible methods of achieving this is as discussed timestamp movement, half-life depreciation or transaction signing.

---

<sup>57</sup> You wouldn't reveal that you have bad or good credit. You would only answer yes or know you have sufficient credit. The requestor or network doesn't need to know the actual score or in reality the act of not providing additional information may inform negative reputation.

- Blockchain's core feature of immutability creates complications for reputation value that fades over time. Potentially negative SBTs could have a half-life until finally the negative SBT is burnt - these features should be considered.

#### **4 Revoke<sup>58</sup>:**

- Revoke the SBTs once unnecessary or inappropriate (e.g., no longer associated with the social community, death of the owner or the issuance of upgraded SBTs).
- Soulbound Tokens (SBTs) are defined by Wyle et al. (2022) as "publicly visible, non-transferable (but possibly revocable-by-the-issuer) tokens held by the soul". They also mention that "[b]urning and re-issuing would make sense ... when the token signals authentic community membership".
- The revoke part of the life cycle may be superseded by recoverability features, although revocability may be grandfathered in with recoverability features
- Emphasis on communal recovery over issuer revocation will occur.

#### **5 Revival:**

- Enable the SBTs to revive using for example community recovery methods.<sup>59</sup>
- This is equally applicable to the Soul containing the SBT

### **[The lifecycle of SBT Community]**

**1 Generate:** SBT community is generated.<sup>60</sup>

**2 Develop and Manage:** Build and manage community guardrails which sets up trust and guidance and measures such as the level of privacy, and develop a community.

**3 Dissolve/Terminate:** The community is dissolved or terminated either by quorum, consensus, or by having nobody left.<sup>61</sup>

<sup>58</sup> In this case, "revoke" is appropriate, not "delete". You could summarize in a Merkle Tree or a zero-knowledge proof but not delete or tamper with data.

<sup>59</sup> If somehow the SBTs could be revived, it would have to overcome a guardrail put in place when the SBTs were revoked. How the revival and recovery is different is not clear yet and is for further discussion.

<sup>60</sup> What would be the minimum number of SBTs to form an SBT community remains a question. The minimum might be one SBTs, or reflecting the fact the smallest unit of a community is a family or a couple as mentioned in the earlier clause, it might be two. It might be an odd number to have quorum. How the SBT community will be generated remains a question.

<sup>61</sup> Whether we need time-bound nobody left remains a question. The community would predefine these rules, i.e. if the community is abandoned for x epochs then revoke all access. In theory the data would still be there, but inaccessible. It could be summarized into a Merkle Tree or zero-knowledge proof to reduce

#### **4 Revival:** Enable the social community to revive using for example, community recovery methods.

The management of SBTs and the corresponding social community must be tailored to the needs and motivations of each community, determining the frequency of updates and renewals of SBTs, potentially new ERCs guide these principles or at least set the framework to create highly accessible interfaces. Before deploying an SBT, governance mechanisms should assist communities in determining the necessary characteristics and requirements of SBT updates. Universal or one-size-fits-all approaches may not be applicable, preferable, or even available. While there is a lack of SBT standards, and clarity on SBT lifecycle management, it is recommended that communities adopting SBTs develop comprehensive guidelines and processes for managing SBTs and the community leveraging these tokens throughout each life cycle stage.<sup>62</sup> Blockchains state of immutability is raised throughout this paper to caveat any deployment of SBTs storing reputation value. All development of this technology should be rigorously tested and interrogated as to avoid any premature or careless implementation of untested SBTs.

### 7.4 Proof of Concept

In addition to the lifecycle of SBTs, it is important to acknowledge that SBTs start from a primitive form, a proof of concept stage. As previously discussed in the subclause (7.2 Fundamental Design for “Social Coordination”), and in clause 6, public visibility of the SBTs is assumed for the SBT in the proof of concept stage for simplicity alongside revocation based features. These initial features start the conversation but do not end it. The ultimate goal is to achieve “programmable privacy” and “Communal Recovery”. The desire to implement these two core features suggests that the features of proto-SBTs are not necessarily expected to continue past product maturity. We expect to see programmable privacy and recoverability features in the long-run. Weyl et al. (2022) differentiate the features of a proto-SBT and future SBTs depicted as follows.

- “We initially assume publicity despite our deep interest in privacy because it is technically simpler to validate as a proof-of-concept, even if limited by the subset of tokens people are willing to publicly share. Later in the

---

space and still provide cryptographic verifiability of the underlying data. It may be worth getting into the revival of the community as well then. Presumably these are historical records that could add value to society. We wouldn't want to encourage that to be locked away. So how do you safely declare a gatekeeper? These could be predefined at the start and become public at a certain date.

<sup>62</sup> Detailed discussion on the guidelines for each lifecycle stages are necessary as a future step.

paper, we introduce the concept of “programmable privacy” for richer use cases.” page 2 (Weyl et al., 2022)

- “Although the hallmark of SBTs is non-transferability, SBTs may also have another property which may prove more useful in bootstrapping: *revocability*. It’s possible that SBTs first gestates as revocable, transferable tokens, before growing into non-transferability. A token is revocable if an issuer can burn the token and re-issue it to a new wallet. Burning and re-issuing would make sense when, for example, keys are lost or compromised, and the issuer has an interest in ensuring the tokens are not financialized and sold off to a party—in other words, when the token signals authentic community membership.” page 28 (Weyl et al., 2022)
- **“Revocable, transferable tokens are a kind of proto-SBT—serving supportive, placental functions before Soul birth.** These tokens buy time both for wallets to gestate secure, community recovery mechanisms and for a person to succinctly accumulate proto-SBTs that can eventually be burned and re-issued into non-transferable SBTs. Under this pathway, the question is not, “what happens first: SBTs or community recovery?” Rather, SBTs and community recovery instantiate simultaneously, birthing a Soul.” page 28 (Weyl et al., 2022)

## 7.5 Coexistence with Other Digital Identities

As we have discussed in clause 6, the purpose and the characteristics of SBTs and other digital identity solutions such as SSI with DIDs are substantially different. Furthermore, non-transferable NFTs do not make them immediately an SBT, nor an effective token for social coordination or decentralized identity. SBTs represent a new option, rather than a replacement of existing forms of SSI, DIDs or NFTs. Therefore, the problem setting is not a question of substituting existing solutions with SBTs, but rather determining the suitability of SBTs for specific use cases; preference may overlay this as well. It is highly likely that SSI with DIDs and NFTs will coexist with SBTs, and that individuals will be the ultimate authority on their use cases.

## 8. SBTs Lead Potentials

Cameron (2005) states that “[t]he absence of an identity layer is one of the key factors limiting the further settlement of cyberspace” and that the difficulty of adding the identity layer in the internet is “[m]ainly because there is little agreement on what it should be and how it should be run”. However, as previously examined in clause 7,

SBTs do not necessitate a universal agreement for novel SBT specific identity principles or to overhaul existing identity standards. Instead, SBTs allow for the replication of existing identity principles and frameworks, with an added focus on “programmable privacy” and “recoverability”; privacy being a core feature of GDPR and digital identity frameworks. “By having these features of being able to know who and what you are connecting to” (Cameron, 2005), with certain privacy each stakeholder will be comfortable with the level of autonomy to express, reject and equally compose SBTs. If future iterations of SBTs are defined by programmable privacy features, Souls and communities could self-determine and co-determine appropriate guidelines to enable a safer and more cohesive plural social network of values.

Weyl et al. (2022), explains that with SBTs, it will “skirt hyper-financialization — yet unlock exponential growth—we propose augmenting and bridging our sociality across virtual and physical realities, empowering souls and communities to encode rich social and economic relationships”.

In this section, we explore the possible implications of SBTs on society by examining five potential outcomes that have the propensity to address and potentially mitigate the financial risks and problems previously outlined in section 5 regarding NFTs.

## 1 Counter Illicit Economic Activities

In clause 5, we have outlined various forms of illicit economic activities, primarily fraud schemes and wash trading. These selected problems are non-exhaustive of the larger range of activities under the umbrella of illicit economic activities, including but not limited to child abuse, darknet market, cybercriminal administrator, ransomware, stolen funds and Sybil attacks (Chainalysis, 2022). While current measures to prevent these activities include investigation and sanctions, the coverage of these activities are minimal, and true value transacted within decentralized permissionless and pseudonymous markets creates an additional smoke screen to dampen law enforcement activities. For comparison, for every \$1,000 of illicit funding, only \$1 is recovered according to Pol (2020) and according to Chainalysis’s 2022 ‘Crypto Crime Report’ (2022), citing UN statistics: criminals using fiat, annually laundered 42.4 times more cash than ‘cybercriminals’ laundered over a five year period using cryptocurrency. This comparison does not seek to diminish the magnitude of money laundered by digital assets, but presents a rational explanation to the lack of incentives in resources allocated to mitigating money laundering using digital assets. This includes the additional challenge of monitoring money laundering in decentralized, permissionless and pseudonymous digital markets. Understandably, addressing these issues requires robust technology and multi-jurisdictional collaboration to accurately identify, measure and mitigate illicit

financial activities within the blockchain. With these issues in mind it becomes clear that current measures, such as investigation and sanction, are insufficient to combat these illicit activities within blockchain environments.

In the context of SBTs, SBTs could serve as an effective tool, adding further functionality to the incumbent regulation technology stack in countering illicit economic activities. SBTs allow “Souls” to create plural social connections, dynamically forming rich on-chain social contexts, and embedding blockchains with reputation-informing tokens and potentially publicly visible affiliations. This novel technology could work as a social mitigant, as Souls correlated to these illicit activities could cause reputation risks in the SBT ecosystem which could inform affiliated communities of their activities; the action's ethical evaluation may vary across different social groups. The reputation risk could generate a strong disincentive making the action undesirable to perform, and undesirable for others to be associated with.

## **2 Promote Regulatory and Tax Compliance**

Regulators face challenges applying AML/CTF to digital assets on Blockchains, primarily due to the lack of available solutions capable of providing accurate identification of the entity transacting on the blockchain network or, at the minimum, evaluating the entity's risk. The current system relies on recording and analyzing on-chain activity such as transactions, addresses association, addresses relationships to the transaction and a plethora of data points publicly available that could create insights on the entity and potentially identify the holders. Additionally, tax compliance is also hindered by lack of entity identification tools to correlate evasive activity on-chain to a specific tax resident. Both regulatory bodies struggle to investigate, prevent and enforce cases. SBTs could provide a blockchain-native solution to meet KYC or CDD obligations, with privacy-preserving SBTs such as zk-SBTs to obfuscate the underlying PII or social credentials. This could provide a two-way access point, as traditional financial institutions could leverage the composability and security of SBTs for customers, and decentralized ecosystems could mature by implementing recognised KYC and CDD requirements. By providing information with past reputation/records, it might make the identification process and risk assessment more sophisticated and reliable. This creates an opportunity to update processes that primarily rely on PII and Government-issued ID in isolation. A range of composable SBTs could build a comprehensive collection of social credentials that go beyond arbitrary Government-issued credentials, expressing rich social context and bridge on/off-chain use cases.

## **3 Diminish Unintentional Information Asymmetry**

SBTs present a potential solution to the challenge of unintentional information asymmetry, in the context of lending and credit systems. Weyl et al. (2022) states that “[a]n ecosystem of SBTs could unlock a censorship-resistant, bottom-up alternative to top-down commercial and “social” credit systems,” which could empower under collateralized lending within DeFi. While access to under collateralized lending would be a monumental advancement for decentralized ecosystems, the paradox of credit provision without available credit scores is essential. Without mechanisms to build credit scores individuals or a community cannot build a reputation/history whether good or bad and the counterparty cannot assess the risk necessary to distribute credit without ascertaining creditworthiness. Even when one is willing to provide their reputation for the other to assess, without a sufficient and credible means of building and expressing the necessary information to be evaluated would only create inefficiencies and market failure risks. The issue of unintentional information asymmetry, presents this paradox clearly, although all parties benefit from sharing information to establish a viable credit relationship, the absence of reputation-building or presenting infrastructure, result in both parties abstracting from the conversation. The lender will not originate borrowable funds without a method of evaluating the borrower nor the business case to rationalize the commercial opportunity without borrowers capable of acquiring credit. Borrowers will not be able to borrow funds without a credit score, nor the opportunity to start building a credit score without borrowing credit. Pushing the lender and borrower back into over-collateralized credit.

To address unintentional information asymmetry, it's important to understand that SBTs are individual data points, the Soul is the database and a collection or ‘constellation’<sup>63</sup> SBTs is a dataset. SBTs could be programmed to represent education, achievements, accolades, income, PII, veteran status and dozens of unique data points. SBTs create the potential to have composable credit scores, where currently fully under collateralized lending is primarily philanthropic or subsidized by governments, future social credit solutions may accept your education SBT, income SBT and a friends Soul to stake their total reputation held to acquire credit. SBTs could enable financial products and market opportunities previously believed to be impossible. There is the potential for any use case within the same structure; where one willingly wants to prove or use their reputation and the other will use that for accurate assessment. The only caveat is that social credit will only be possible overtime, once SBTs are created

---

<sup>63</sup> This is another definition the authors of this paper have included. A constellation of souls or soul constellation is a collection of SBTs related to one another. Similarities can be drawn from NFTs that have a NFT collection, whereas Souls would have a constellation of SBTs. Suggestions on these terms are welcomed.

and distributed and infrastructure is built around formulating scores acceptable by lenders.

#### 4 Fair, Transparent, and Accountable Governance

In clause 5, we examined various risks and limitations in digital asset governance structures, highlighting the potential pitfalls of a majoritarian and plutocratic voting system, whereby voting power is relative to quantity of governance tokens held. This approach may seem archaic, but this boot-strapped governance system enabled complex multi-party coordination, with social, industrial and commercial stakeholders co-determining resolutions across borders and, in most cases, absolutely anonymously. This plutocratic governance system has been sufficient in catalyzing basic governance requirements, and in some circumstances still be considered preferable. However, it lacks the rich-social context that exists natively in traditional governance systems. If these majoritarian systems were to transition or even partly-implement new social coordination tools such as SBTs to improve the decentralization of voting and proposals, would they want to adopt these tools; or could they even pass the proposal to vote for these tools? DAOs are widely recognised as the primary governance system in distributed governance voting structures. The term decentralized is understandably often associated with DAOs, and equally DAOs are selected as the governance system for DeFi dApps for the same reason. However, on closer examination of these organizations, it becomes apparent that there is a significant concentration of voting power within a significantly small minority of token holders. To adequately evaluate the benefits of SBTs for a DAO use case, the authors of this paper struggled to find the appropriate language to accurately illustrate the full extent of centralisation in these so-called “decentralized” autonomous organizations.

Chainalysis published an informative report on the “State of Web 3” (2022), in June of 2022, whereby Chainalysis analyzed the wealth distribution of ten major DAO tokens, finding that “less than 1% of all holders have 90% of voting power.”. The potential impact of this was further illustrated that “if just a small portion of the top 1% of holders worked together, they could theoretically outvote the remaining 99% on any decision” (Chainalysis, 2022). To provide a real-world comparison of web3’s lack in wealth equality, we have used DAOitright.xyz, a public goods calculator that evaluates various DAO governance metrics specifically the Gini-coefficient, a commonly used metric to evaluate a country’s wealth inequality (Zhao, 2022). Lido, the largest Ethereum 2.0 liquid staking provider, an address can stake (deposit) Ether to participate in Ethereum 2.0 consensus mechanism and receive staking rewards without locking staked Ether up. According to DAOitright.xyz, Lido has a Gini-coefficient of 0.931, for

comparison, the country with the highest Gini-coefficient in the world is South Africa, with 0.63 (DAOitright, 2022; World Bank 2023). Lido's score would make it the most inequitable place in the world. So how would SBTs bring the decentralization back into DAOs and distributed governance systems?

SBTs afford DAOs a novel means of securely distributing voting rights and aligning accountability mechanisms when members attempt to act maliciously. Potentially SBTs are used in isolation initially, and only in instances where the outcome has impacted the whole community or its members disproportionately. To ensure these crucial governance votes are conducted in a fair, distributed and unbiased manner, SBTs could represent a single vote and be distributed based on a minimum number of governance tokens to avoid adverse selection as described in clause 7.2. The authors of this paper are also considering an ERC-EIP for an alternative SBT primitive specific for governance voting, this SBT variation is a 'Soulbound Governance Token' (SBGT). We describe a SBGT as a fungible SBT, whereby users are able to generate this token through similar methods used today such as staking and dApp activity. Where the SBGT would differ from standard governance tokens is the SBGTs are non-transferable and have revocability features. Users can generate this token but cannot trade the token for speculative financial returns. Additional fair voting mechanisms such as quadratic-funding would still be possible and afford another layer to equitable voting processes (Weyl et al., 2022). Additionally, transparency will play a crucial role in ensuring that decisions are made in the interests of the community, and where any governance system that allows members to delegate voting power is not pooled to control voting outcomes at the expense of the majority. SBTs could also align ownership, action and relative consequence if members attempt to act maliciously.

The implementation of SBTs holding programmable privacy and communal recovery features, presents a novel method of conducting governance voting. SBTs and variations such as SBGTs could address the 'anonymity but with accountability' problem statement, this paper initially highlighted during the Introduction. SBTs could ensure transparency within the voting process is adequately addressed, to DAO members confidence on voting practices and participants, without needing to expose the underlying PII. SBTs creates accountability, by incentivising fair, honest and purposeful governance voting, whilst making consequences against the DAOs voting guidelines undesirable by layering the five variables of reputation economics outlined in clause 7.2. DAOs could go further by implementing 'one-SBT, one-vote', similar to Satoshi Nakamoto's 'one-CPU, one-vote' a decision that served as part of the foundation to ensuring a fair distribution of network mining for the Bitcoin Blockchain (Nakamoto, 2008). Furthermore, using SBTs as a novel, gamified badge to

impart positive reputation gained by positive work actioned, while no capital value could be derived - tools such as proof-of-attendance protocol (PoAP) have become popular in incentivising participation beyond financial rewards (Weyl et al., 2022). Holding other Souls accountable may be another incentive, and could be a powerful tool when wanting an action; or could sow distrust within communities. Although these features are not recommended to be deployed by default until SBTs are readily accepted, tested and the community has voted - it is, however, recommended for DAOs to plan for future upgrades and the implementation of SBTs to assist in creating fair governance systems. By incorporating SBTs as a new tool for social coordination in governance structures, SBTs have the potential to facilitate fair, transparent and accountable decentralized governance.

## 5 Opportunities for Innovation

SBTs have the potential to transform digital identity infrastructure, both from DID/VC standards and the top-down arbitrated approach conducted by governments and intermediaries. This includes how developers implement different digital identity standards for real-world applications and how developers implement new functionality within decentralized ecosystems. Enabling Souls and communities afford to determine their own digital identities, with additional means of privacy, recovery and utility. Currently, mainstream identity structure, and limited stakeholders can determine which form of digital identity should be implemented, including how the digital identity is managed. SBTs open the possibility for more stakeholders to participate in co-determining standards, features and utilities, and novel innovation in both development and use case. The purpose of SBTs is to aid in creating a decentralized society, so that individuals and communities from all levels compose the digital identity that best represents them in a given context. This shift towards a bottom-up approach to digital identity infrastructures could open up opportunities expanding the range of participants involved in under collateralized lending, social credit systems, equitable governance voting or privacy in highly-integrated global markets. This paper has endeavored to highlight the extent of possibilities so that researchers can progress theory, enabling developers to innovate on the concepts ultimately so that the market can benefit from new technology that addresses real market inefficiencies.

# 9. Further Considerations of SBTs

In the previous section, we presented the potential for SBTs, outlining how SBTs can counter financial crime, meet regulatory requirements, address market failures, improve governance systems and create opportunities for innovation. In this section, we want to discuss SBTs limitations, risks, challenges, and open up on questions for the future of SBTs and Souls. It is important to understand that SBTs are not a silver bullet and if not cautiously analyzed and carefully implemented, new risks are bound to rise. As it is important to examine the advantages and use cases of SBTs, we must equally discuss the potential limitations and carefully calculated aspects to consider the extent of these possibilities. Among the key considerations to safely, and effectively implement SBTs, includes concerns surrounding the storage and management of PII on-chain; one of the exasperating concerns. Blockchain's core feature of immutability does not allow for PII concerns to be addressed retrospectively, and will have to be discussed far before the development stage of SBTs. Any SBTs looking to interact with PII, will require solutions that meet privacy requirements and reassure Souls that identity standards are sincerely addressed.

All stakeholders participating in SBT-related discussion should be mindful and consider the questions we raise as follows; Innovation, Design, Privacy and Transparency, Responsibility, and Implementation.

## 1 Further Innovation

- Innovation in communal authentication, attestation, and recovery in a safe and sound way is necessary.
- There will be at least a need for creating a platform to issue proto-SBTs / proto-soul issuers as another layer before rolling out.
- How can research communities, developers and commercial entities align for the benefit of creating public-good social coordination use cases?
- How do you commercialize non-transferable assets in a natively hyper financialised decentralized market?
- In what ways can definitions surrounding non-transferable NFTs and SBTs be clearly outlined and decided?
- How can we avoid using the term ‘web3’ to define the ecosystem that leverages both blockchain and smart contracts? A proposed term by an author of this paper is “decentralized innovation”, “decentralized technology” or “decentralized ecosystems”.

## 2 Design

- Programmable privacy reflects the general view of privacy in the community. However, even in the same community, confidence for

disclosure varies between the “souls”. How do we ensure individual confidence while maintaining a functioning mechanism as a community?

- What are the mechanisms necessary to eliminate improper usage of SBTs?
- How to ensure that the SBTs and its ecosystem function efficiently and effectively? What is necessary to maintain credibility and trust in the SBTs other than the initial agreement?
- Reputation works because it is relatively compared and enables assessment simply if it is good or bad. Even with programmable features, one might need to unintentionally disclose reputation or association perceived negatively. This is as efficient as AML/CTF and other regulatory measures. But it might be used for assessing credit scores when applying for a loan. To some extent, this is necessary to reduce unintentional information asymmetry. However, we must keep in mind the possibility that it might lead to social exclusion or stigma. How do we deal with these cases of negative characteristics or outcomes?
- Sakimura (2021) has framed that “Trust” is to “answer to expectation” and “Brand” is to “promise to answer expectations”. SBTs and SBT communities will each build their own trust and brand. They should consider and have an agreement within the community to build trust and branding, regardless of whether or not they will actually adopt it.
- Even with SBTs, it will not fully be a solution to governance voting problems as mentioned in clause 5. For the problems that are not addressed by SBTs alone, could it be solved in combination with other solutions? Potentially quadratic funding, as proposed by E. Glen Weyl.
- Community recovery and revocability is closely related. That is, recovery has its value because it is revocable. How could it be aligned with the community recovery system?
- For some communities it is easier to revoke a soul. Those examples are communities for current employees in an organization, current students, etc. On what basis does revocability function and how to ensure governance remains a question. Burning one’s soul, even if it could be restored, will have great consequences on the holder and the community. How would revocability work as aimed in less apparent cases.
- Without a good design on the revocability, it could lessen the trust and functionality of the whole SBT ecosystem or the SBT community. Szabo (1997) has nailed down that “[t]here is an important conundrum in an ID-based key system: the conflict between the ability to get a new key when the old one is or could be abused by another (key revocation), and the ability of another to be sure they are dealing with the same person

again. This may also provide an opportunity for parties to selectively reveal positive credentials and hide negative ones”.

### 3 Privacy and Transparency

- Although the features of SBTs is programmable privacy, it should not be a lawless zone. Preventing evasive usage of privacy regulation must be considered.
- Privacy concepts and protections differ between various jurisdictions and regions. Given the difference, how do we bridge or create a framework given the different policy aims of the privacy policy? For example there is General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the California Consumer Privacy Act of 2018 (CCPA) which aims to ensure strong protection on personal data and regulates business's activity to collect, use, and share data. GDPR and CCPA have overlaps as well as differences in many ways such as the definition and rights it ensures (Future of Privacy Forums, 2018). In the current system, there are inconsistencies.
- SBTs community includes cross-border communities, the “souls” spread across regions. On what standards should these rules be applied and how should they be complied? Even with the programmability, should there be a common ground for the SBT community to have a baseline on the collection, usage, and sharing of SBT data? This may apply to both the SBT community as well as other third parties.
- ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) “provides a high-level framework for the protection of personally identifiable information (PII) within information and communication technology (ICT) systems” (ISO/IEC, 2011). ISO and IEC have framed “11 Principles of Privacy” as follows in the ISO 29100 (Table 2). The question is should SBTs be applied to these principles. If so, how to embed these principles in the SBTs and how to ensure them? Should there be further standards and principles added or amended specifically for SBTs?
- How do we balance privacy with regulatory/tax compliance? What is the best way for the SBT community and the regulators or tax authorities to cooperate?
- How do we ensure a balance between privacy and transparency for off-chain data? What technologies can be used to balance privacy and transparency? Are there ways other than the zero-knowledge proof? If so, what are the merits and limitations? Can designated verifier proofs which

allow “authenticated but private conversations to take place” (Jakobsson, et al., 1996) be applied for SBTs?

#### 4 Responsibility

- Who will be held accountable for building and running the SBT community (e.g., accountable for vulnerabilities in protocols, dispute resolution)? Too much responsibility might lure away those willing to contribute to the community. It is a question that should be discussed in each community, but there should be some kind of an incentive mechanism linked to the burden and responsibility.
- Who are the stakeholders and what do they do?
- How do the legal rules, enforcement, and judiciary apply to the SBTs? In that case, which jurisdiction should it be applied to?

#### 5 Implementation

- What are the risk as a consequence of having SBTs?
- Would the benefit of having SBTs outweigh the cost?
- A large population or services need to adopt SBTs in order to lead to outcomes as we have described in clause 8. Given this, how much scalability do we need to make a social impact? How to promote adoption and scalability in an early stage?
- We have stated in clause 7 that SBTs do not eliminate other digital identity forms. What is an ideal form of existence?
- How to bridge, if any, between SBTs or SBTs and other forms of digital identity? How would different SBTs or SBT communities interact with each other effectively while ensuring safety and soundness?
- There would be no meaning of SBTs if the SBTs were just shown on a smartphone screen and no infrastructure which uses SBTs as a proof of the “Soul”. Therefore, social infrastructure beyond the SBT community must be considered.

## 10. Conclusion

The application of Blockchain and smart contract technology has enabled a variety of technology, Bitcoin, Altcoins, ICOs, NFTs, DAOs with added layers of complexity at each new development, ultimately pushing real demand towards SBTs, a compatible on-chain social coordination tool. This is particularly necessary for the safety and convenience of individuals and communities, interacting within plutocratic anonymous, decentralized markets. Understandably, this relays back-bottoms-up pressure for new tooling that can afford features of programmable privacy and

recoverability, ensured by authentic and honest third-party verification; either by authoritative sources or plural peer evaluation. In this report, we have discussed the emergence of SBTs, examining SBTs potential to bring a whole new means of social coordination within decentralized markets not previously possible. Within this report we have explored the context, opportunity, use cases, methodology, lifecycle and limitations of SBTs, aiming to assist readers in understanding this novel technology and evaluate how SBTs might afford previously impossible use cases.

In our discussion, we explored the opportunities and challenges of SBTs. Throughout this paper we have outlined that SBTs have the potential to enable plural social networks and provide rich-social context behind previously plutocratic anonymous governance systems. If SBTs were to be adopted and implemented, individuals and social groups at all scales would be able to co-determine levels of utility and privacy, creating flexible tooling for expansive functionality. However, it is important to acknowledge that SBTs are still in an early stage of development and theory. A serious number of risks, malicious usages, challenges and limitations still need to be explored and at the minimum highlighted to serve as a cautionary warning. Numerous questions need to be answered to provide the market with confidence on the safety and value behind SBTs, and create a forum to further multi-stakeholder discussions through this exploration, to understand the implications of SBTs both technically and socially. Since SBTs are closely related to personal information, these conversations must be handled with the utmost care given the consequences. It is vital that SBTs should not be promoted for SBT's sake but understood and inspected from various perspectives, including should SBTs even exist. Through the process of building this report, different stakeholders sat together and discussed these issues, not just the advantages of SBTs, but also serious discussions on the risks, dangers, and challenges.

Given its social implications, before advocating/promoting or denying SBTs, we think that further multi-stakeholder discussion is essential and its surrounding environment as well as the technical development. There should be a continuous debate on the existence, design and management, usage, social impact and meaning, applications, problems, and risks between academia, government, developers, lawyers and commercial sectors.

Publishing this report is the first step in this process, and we hope that it will serve as a catalyst for an open and ongoing discussion. We are currently in the planning stages of a subsequent paper on SBTs to ensure research and theory stays ahead to provide a clear direction and vision for developers, academia, the commercial sector and market participants. As BGIN is neutral, we have and will continue to welcome diverse perspectives and feedback for past, present and future discussions.

# Appendix A – Acknowledgement

(Informative)

(Note) The views expressed in this report are based on the personal views of the authors and not the views of the organizations to which they belong.

## A.1 Editors and Co-editors

- Michi Kakebayashi (University of California, Berkeley) - ([LinkedIn](#))
- Joseph Beverley (Soulbis) - ([Joey@soulbis.com](mailto:Joey@soulbis.com) | [LinkedIn](#))

## A.2 Contributors (Alphabetical)

- E. Glen Weyl (Microsoft Research; RadicalxChange Foundation)
- Hugh Harsono (University of California, Berkeley)
- Kazue Sako (Waseda University)
- Ken Katayama (Nomura Research Institute, Ltd.)
- Louisa Choe (Nansen)
- Mitchell Travers (Soulbis)
- Nat Sakimura (OpenID Foundation)
- Pablo Pejlatowicz (Independent Researcher)
- Puja Ohlhaver (Flashbots Ltd.)
- Ryan Kris (Verida)
- Shai Perednik (Amazon Web Service)
- Shin'ichiro Matsuo (Georgetown University)
- Shinji Sato (Independent Researcher)
- Shrey Jain (Microsoft, University of Toronto)
- Stephanie Bazley (AirTree Ventures)
- Testu Kurumisawa (Yale University)
- Tomonori Yuyama (Georgetown University)

## A.3 Reviewers (Alphabetical)

- Ash van der Spuy (Jubi.io)
- Philip Sheldrake (Euler Partners)

Blockchain Governance Initiative Network (BGIN) aims at providing an open and neutral sphere for all stakeholders to deepen common understanding and to collaborate to address issues they face in order to attain sustainable development of the blockchain community. As an open network, we are now actively and widely seeking interested

parties to join this initiative, so as to accommodate diverse opinions from a wider range of blockchain stakeholders. This paper was discussed in [Block #6](#), Block #7 and during our bi-weekly IKP Working Group (co-chair: Nat Sakimura; co-chair: Mitchell Travers). For those who are interested, please contact us via [bgin-admin@mail.bgin-global.org](mailto:bgin-admin@mail.bgin-global.org).

## Appendix B – Informative reference

(Informative)

- 5660-eth, Wizard Wang, "EIP-6147: Guard of NFT/SBT, an Extension of EIP-721 [DRAFT]," Ethereum Improvement Proposals, no. 6147, December 2022. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-6147>. (last viewed on January 18 2023)
- Omar Aflak, Omar, Pol-Malo Le Bris, Marvin Martin, January 2022. "EIP-4671: Non-Tradable Tokens Standard [DRAFT]," Ethereum Improvement Proposals, no. 4671., January 2022. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-4671> (last viewed on November 22, 2022)
- BGIN. March, 2022. "SR 005 NFT Study Report Part 1: Introduction and Use Cases." Available: <https://bgin-global.org/pdf/NFTReport.pdf>
- Bloomberg. May 11, 2022. "Crypto Investors Likely Paying IRS Less Than Half the Taxes They Owe." Available: <https://www.bloomberg.com/news/articles/2022-05-11/crypto-investors-likely-paying-less-than-half-the-taxes-they-owe>.
- Buterin, Vitalik. 2021. "Why we need wide adoption of social recovery wallets." Available: <https://vitalik.ca/general/2021/01/11/recovery.html> (last viewed on November 22, 2022)
- Cai, Buzz. August, 2022. "EIP-5484: Consensual Soulbound Tokens [Final]." Ethereum Improvement Proposals, no. 5484,. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-5484> (last viewed on November 22, 2022)
- Cameron, Kim. 2005. "The Laws of Identity." Kim Cameron's Identity Weblog. Available: <https://www.identityblog.com/?p=352> (last viewed on November 22, 2022)
- Chainalysis. February, 2022. "The 2022 Crypto Crime Report." Available: <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>

- Chainalysis. June, 2022. “The Chainalysis State of Web3 Report” Available: <https://go.chainalysis.com/2022-web3-report.html> (last viewed on January 22, 2023)
- Congressional Research Service. July, 2022. “Non-Fungible Tokens (NFTs).” Available: <https://crsreports.congress.gov/product/pdf/R/R47189>
- DAOitright.xyz Available: <https://www.daoitright.xyz/> (last viewed on January 22, 2023)
- Daubenschütz, Tim, Raphael Roullet. April, 2022. “EIP-4973: Account-bound Tokens [Review].” Ethereum Improvement Proposals, no. 4973. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-4973> (last viewed on November 22, 2022)
- Daubenschütz, Tim, Anders. July, 2022. "EIP-5192: Minimal Soulbound NFTs [Final]." Ethereum Improvement Proposals, no. 5192. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-5192> (last viewed on November 22, 2022)
- Elliptic. 2022. “NFTs and Financial Crime -Money Laundering, Market Manipulation, Scams & Sanctions Risks in Non-Fungible Tokens.” Available: <https://www.elliptic.co/hubfs/NFT%20Report%202022%20-full.pdf>
- Entriken, William, Dieter Shirley, Jacob Evans, Nastassia Sachs. January, 2018. “EIP-721: Non-Fungible Token Standard [Final].” Ethereum Improvement Proposals, no. 721 [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-721>. (last viewed on November 22, 2022)
- Financial Action Task Force (FATF). “Frequently asked questions - Money Laundering.” Available: <https://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223>. (last viewed on December 7, 2022)
- Goldfinch. “Unique Identity (UID).” Available: <https://docs.goldfinch.finance/goldfinch/unique-identity-uid>. (last viewed on December 14, 2022)
- HonorLabs, "EIP-5633: Composable Soulbound NFT, EIP-1155 Extension [DRAFT]," Ethereum Improvement Proposals, no. 5633, September 2022.

[Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-5633> (last viewed on January 18, 2023)

- Hyungsuk Kang, Viktor Pernjek, "EIP-5252: Account-bound Finance [DRAFT]," Ethereum Improvement Proposals, no. 5252, June 2022. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-5252>. (last viewed on January 18, 2023)
- Martin Becze, Hudson Jameson, et al., "EIP-1: EIP Purpose and Guidelines," Ethereum Improvement Proposals, no. 1, October 2015. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-1>. (last viewed on November 22, 2022)
- Ethereum.org. August, 2022. "ERC-20 Token Standard." Available: <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/> (last viewed on November 22, 2022)
- Ethereum.org. "Non-fungible tokens (NFT)." Available: <https://ethereum.org/en/nft/> (last viewed on November 22, 2022)
- EthHub. "ERC Token Standards." Available: <https://docs.ethhub.io/built-on-ethereum/erc-token-standards/what-are-erc-tokens/> (last viewed on November 22, 2022)
- European Union (EU). 2016. "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ." *Official Journal of the European Union*. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (last viewed on November 22, 2022)
- Facebook. 2013. "Introducing Trusted Contacts." Available: <https://www.facebook.com/notes/10157814523321886/> (last viewed on November 22, 2022)
- Facebook. "How can I contact the friends I've chosen as trusted contacts to get back in to my Facebook account?" Available: <https://www.facebook.com/help/213343062033160> (last viewed on November 22, 2022)

- Future of Privacy Forums. 2018. “Comparing privacy laws: GDPR v. CCPA.” Available: [https://fpf.org/wp-content/uploads/2018/11/GDPR\\_CCPA\\_Comparison-Guide.pdf](https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf)
- Goldfinch. “Goldfinch Documentation.” Available: <https://docs.goldfinch.finance/goldfinch/unique-identity-uid> (last viewed on November 22, 2022)
- ISO/IEC. 2011. “ISO/IEC 29100:2011(En), Information Technology — Security Techniques — Privacy Framework.” Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en> (last viewed on November 22, 2022)
- Jain, Shrey, Leon Erichsen, and Glen Weyl. 2022. “A Plural Decentralized Identity Frontier: Abstraction v. Composability Tradeoffs in Web3.” Available: <https://arxiv.org/abs/2208.11443>
- Jakobsson, Markus, Kazue Sako, and Russell Impagliazzo. “Designated Verifier Proofs and Their Applications.” In Advances in Cryptology — EUROCRYPT ’96, edited by Ueli Maurer, 1070:143–54. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996. Available: [https://doi.org/10.1007/3-540-68339-9\\_13](https://doi.org/10.1007/3-540-68339-9_13)
- JFSA. June, 2022. “Report on Distributed Financial Systems in Trust Chains Research on Technology Risk.” Available: [https://www.fsa.go.jp/policy/bgin/ResearchPaper\\_qunie\\_en.pdf](https://www.fsa.go.jp/policy/bgin/ResearchPaper_qunie_en.pdf)
- Kei. July 21st, 2021. “A Prehistory of DAOs.” Available: <https://gnosisguild.mirror.xyz/t4F5rltMw4-mlpLZf5JQhElbDfQ2JRVKAzEpanyxW1Q>. (last viewed on January 15, 2023)
- Maister, D. H., Galford, R. M., Green, C. H. 2001. The Trusted Advisor: 20th Anniversary Edition. United Kingdom: Free Press.
- Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System” Available: <https://bitcoin.org/bitcoin.pdf> (last viewed on January 18, 2023)

- Pauwels, Pieter, Joni Pirovich, Peter Braunz and Jack Deeb. 2022. "zkKYC in DeFi: An approach for implementing the zkKYC solution concept in Decentralized Finance." Available: <https://eprint.iacr.org/2022/321.pdf>
- Philipp Bolte, Lauritz Leifermann, Dennis von der Bey, "EIP-5539: Revocation List Registry [DRAFT]," Ethereum Improvement Proposals, no. 5539, August 2022. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-5539>. (last viewed on January 18, 2023)
- Pol, Ronald F. (2020): Anti-money laundering: The world's least effective policy experiment? Together, we can fix it, Policy Design and Practice, DOI:10.1080/25741292.2020.1725366
- Pop, Valentina. February 26, 2015. "[Interview] 'You Can't Use 18th Century Law for a Digital World.'" EUobserver. Available: <https://euobserver.com/economic/127800>. (last viewed on December 7, 2022)
- Reutlaw. "NFTs and Property Rights." Available: <https://www.reutlaw.com/en/insights/nfts-and-property-rights>. (last viewed on December 8, 2022)
- Sakimura, Nat. 2021. "Digital Identity The Essence of Cyber Business that Management Does Not Know. (Digital Identity Keieisha ga Shiranai Cyber Business no Kakushin)" (In Japanese). *Nikkei BP*.
- Sheldrake, Philip. October 21st, 2022. "The number one challenge in computer science." Available: <https://medium.com/decentralized-web/the-number-one-challenge-in-computer-science-43b26c27f079>. (last viewed on December 7, 2022)
- Shu Dong, Qi Zhou, "EIP-4972: Name-Owned Account [DRAFT]," Ethereum Improvement Proposals, no. 4972, April 2022. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-4972>. (last viewed on January 18, 2023)

- Sovrin Foundation. December 6, 2018. "What is self-sovereign Identity?" Available: <https://sovrin.org/faq/what-is-self-sovereign-identity/> (last viewed on December 8, 2022)
- Peter Swire, 1997. "The Uses and Limits of Financial Cryptography: A Law Professor's Perspective." Available: <http://www.peterswire.net/archive/pscrypto.html> (last viewed on January 20, 2023)
- Szabo, Nick. 1996. "Smart Contracts: Building Blocks for Digital Markets." Available: [https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smarty\\_contracts\\_2.html](https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smarty_contracts_2.html). (last viewed on November 22, 2022)
- Szabo, Nick. 1997. "Formalizing and Securing Relationships on Public Networks." Available: <https://nakamotoinstitute.org/formalizing-securig-relationships/> (last viewed on November 22, 2022)
- The Board of the International Organization of Securities Commissions. March 2022. "IOSCO Decentralized Finance Report." Available: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf>
- The National Law Review. April 23, 2021. "Thinking Beyond the Law: What Is the ISO 29100 Privacy Framework?" Available: <https://www.natlawreview.com/article/thinking-beyond-law-what-iso-29100-privacy-framework> (last viewed on November 22, 2022)
- Ushida, Ryosuke and James Angel. 2021. "Regulatory Considerations on Centralized Aspects of DeFi managed by DAOs." Available: [https://drive.google.com/file/d/14XkrwGI\\_8fFRFtfkePAH2OkIZI-kIOKB/view](https://drive.google.com/file/d/14XkrwGI_8fFRFtfkePAH2OkIZI-kIOKB/view)
- U.S. House of Representatives. September, 2020. "Understanding The Tax Gap And Taxpayer Noncompliance." Available: <https://www.treasury.gov/tigta/auditreports/2020reports/202030066fr.pdf>

- Commodity Futures Trading Commission (CFTC) v Ooki DAO (formerly d/b/a bZx DAO), No. 3:22-cv-5416 (N.D. Cal. September 22, 2022) "COMPLAINT FOR INJUNCTIVE AND OTHER EQUITABLE RELIEF AND CIVIL MONETARY PENALTIES UNDER THE COMMODITY EXCHANGE ACT AND COMMISSION REGULATIONS". Available:  
<https://storage.courtlistener.com/recap/gov.uscourts.cand.400807/gov.uscourts.cand.400807.1.0.pdf> .
- Weyl, Eric Glen and Ohlhaver, Puja and Buterin, Vitalik, 2022. "Decentralized Society: Finding Web3's Soul." Available at SSRN:  
<https://ssrn.com/abstract=4105763>
- Wang, Will, Mike Meng, Ethan Y. Tsai, Ryan Chow, Zhongxin Wu, and AlvisDu. December, 2020. "EIP-3525: Semi-Fungible Token [Final]." Ethereum Improvement Proposals, no. 3525. [Online serial]. Available:  
<https://eips.ethereum.org/EIPS/eip-3525> (last viewed on November 22, 2022)
- World Wide Web Consortium (W3C). March, 2022 a. "World Wide Web Consortium (W3C)." Available: <https://www.w3.org/TR/vc-data-model/> (last viewed on November 22, 2022)
- World Wide Web Consortium (W3C). July, 2022 b. "Decentralized Identifiers (DIDs) v1.0" Available: <https://www.w3.org/TR/did-core/> (last viewed on November 22, 2022)
- Wyoming Secretary of State. "Decentralized Autonomous Organization (DAO): Frequently Asked Questions."  
[https://sos.wyo.gov/Business/Docs/DAOs\\_FAQs.pdf](https://sos.wyo.gov/Business/Docs/DAOs_FAQs.pdf). (last viewed on December 7, 2022)
- Weatherford, Dawn R., Devin Roberson, and William Blake Erickson. 2021. "When experience does not promote expertise: security professionals fail to detect low prevalence fake IDs." Cogn. Research 6, 25. Available:  
<https://doi.org/10.1186/s41235-021-00288-z>.

- Word Bank. 2023. “Gini Index” Available:  
<https://data.worldbank.org/indicator/SI.POV.GINI> (last viewed on January 22, 2023)
- Yu Liu, Junyi Zhong, "EIP-5851: On-Chain Verifiable Credentials [DRAFT]," Ethereum Improvement Proposals, no. 5851, October 2022. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-5851>. (last viewed on January 18, 2023)
- Sicong Zhao. May 2022 “How to evaluate the “Fairness” of DAO Governance?” Available:  
<https://medium.com/@luo9137/how-to-evaluate-the-fairness-of-dao-governance-82bde68c01b9> (last viewed on January 22, 2023)
- Zoltu, Micah. May, 2022. “EIP-5114: Soulbound Badge [DRAFT].” Ethereum Improvement Proposals, no. 5114. [Online serial]. Available:  
<https://eips.ethereum.org/EIPS/eip-5114> (last viewed on November 22, 2022)

# Appendix C – BGIN Block #6 Session Notes

## (With E. Glen Weyl, Puja Ohlhaver, Shrey Jain)

[Blockchain Governance Initiative Network \(BGIN Block #6\) @Zurich \[Hybrid\] – UZH Blockchain Center](#)

IKP Working Group Editing Session - Soul Bound Token (SBT)

<https://tube.switch.ch/videos/n7aPlsHzkj>

Panel Speakers (Glen, Puja, Shrey):

- SBTs are still preliminary in terms of social incentive design. The ideas raised are ambitious and we won't have clarity on most of the implications raised until more innovations and experiments.
- If you regard SBTs as representing just membership to social groups, those groups have a socially determined set of rules, rights, and privacy controls (particularly programmable privacy). Starting from there, you can think of a person being a constellation of their social memberships.
- The level of publicity is programmably private by the social groups themselves. Initial publicity was just a starting point for other conversations and a way to bootstrap the idea. As we expect social groups to have their customs and norms around conversation/communications, we expect those privacy expectations to be encoded in social communication channels as well.
- All of that being said, if you think of an individual as being a constellation of social membership, when we think as people to have a social identity, what the SBTs to the extent that they are public (not everything is going to be public), what they may need to do is to surface social coordination for fraud to the extent that there are multiple players in the fraudulent schemes.
- It also enables you to have rather than government to individual, have an intermediate layer of communities for enforcement and cooperation between communities.
- We talked a lot about the community recovery of wallets and you can think of that also for community assets held by social groups, DAOs. It really adds an interesting spin to why recovery methods for say stolen funds.
- The idea of governance token and DAO is native to web3 and the problem is that you don't have civil resistance. Somebody could split holdings between different wallets and actually say that he/she is 51% control of a protocol to benefit them. For the same reason that the democracy does not become majoritarian direct democracies, a lot of DAOs don't want to do that because their assets will be eluded from those who own the majority of that stake.
- VCs (verifiable credentials) = Meant to prove properties but not to show commitment as there is a lack of accountability/transparency (no public trace

unless you choose to present them). To prove property but not to facilitate accountability. VCs are oriented towards proving property (claim or statements) but not primarily to facilitate accountability.

SBTs = Commitment that you present publicly, at least partially, with transparency, which means accountability. When you have memberships, commitments and roles come along. SBTs are oriented towards rights of various kinds. SBTs enable social coordination. The transparency (within the group and between the group) of the SBTs is dependent on the social group. SBTs represent social membership and when you have social membership, there are rights, responsibilities, permissions, access controls etc., which are social coordination tools.

- The distinction between VCs and SBTs is subtle but an important distinction.
- NFTs = Represent private property which is very distinct from both VCs and SBTs.
- For the tables, the rows could be added for credibility and trackability.
- For SBTs led potential, SBTs broadly enables social coordination, for example plural network goods or what people think as traditionally public goods, and doing that in a sybil resistant way. As well as rethinking how we plurally concrete future AI and intelligences in a way that the technology is transparent and based in the legitimacy of data creators rather than data coders and make technologies more accountable to the users. So when you think of SBTs as representing membership to social groups seeking social coordination around technology, data, and communications.

Audience:

- When reading the paper, it was really about creating credentials, memberships, and legitimacy so I was curious why the reference was more about social network theory as opposed to social capital. Is there space for discussion on social capital might be applied to SBTs?

### Soul Bound Token (Interviewing)

<https://tube.switch.ch/videos/mP1TnEarQj>

- What was it that really motivated you to publish the paper “Decentralized Society: Finding Web3's Soul”?
  - Our motivation was how we can achieve network coordination we need in the 21st century both globally and locally, and bottom up key decentralized ways. When we say decentralized, we mean a set of social groups where the powerful company doesn't dominate the network and the network power is limited to solving problems at its social scale and not necessarily on the social scale underneath it. Bottom up coordination of individuals co

creating their communities to compose into larger networks in a decentralized way was really the animating goal.

- Concerned that you couldn't really do stuff that sophisticated using blockchain was the starting point. You needed base level data structures. The combination of Vitalik's paper and working with the gitcoin community on quadratic funding and trying to move towards a more plural direction, web3 as a primitive starting point, and showing people the pathway.
- What is in your opinion the biggest challenge or your concern? Is it NFTs or more broad on the Web2 or Web3 ecosystem?
  - It was both. In Web3, there is the problem of hyper-financialization and also DOAs struggling with governance and sybil resistance.
  - I don't think it is the problem of NFTs per se, but it was an interesting point to see that unlock so much success that highlighted the potential for the space to be very innovative. The amount of innovations we saw in NFTs was incredible in the past few years so I took that as an inspiration for innovations.
  - I had an ambivalent relationship with Web3, on the other hand it is exciting that there have been so many cool experiments happening there. At the same time, there are activities that are awfully speculative and not producing much value in the lives of people and so forth. I was pessimistic about it. But the paper was triggered by my seeing that there may be a way to build from what exists in the Web3 world as to what we were aiming at.
- Do you have other ideas on the application (or steps to DeSoc) of the SBTs? (We think that it has benefits on government policies such as AML/CTF)
  - The idea of representing signatures to petitions or otherwise putting your name to some form of social principles. These are natural applications.
  - Others are more promotional affiliations. If you give a donation and receive a receipt, or a fan of a sports team and want to make a commitment could be used. These aren't amazing, transformative, long-term but near-term applications.
  - There are explosions of experiments happening with SBTs. There is a potential for social coordinations in a decentralized way. Excited to look at different communities looking at SBTs as a coordination tool and in particular communities that have had a difficult time coordinating in the past or are subject to monopolist extractors. In the scientific community, there is a lot of innovation happening there in the DeScie space where innovators are really trying hard to form what today we call "science" into

“open-science”. Solve the problem of reproducibility of science and at the same time achieve traceability. Unlock the renaissance in science. The ability of the SBTs (the ability to show the membership to the social groups) and then the social groups to coordinate is very profound. We will see these open-source communities having different problems of poor ways of representing status or encouraging more contributions.

- Innovation in protocols that do not necessarily have a token but have open-source research protocols or communities and a way to govern themselves or ways of communicating is exciting too.
- What do you see as potential from a government side, such as AML issues?
  - See a different framework coming into existence. The basic principles of KYCs and AML are that there is one authoritative notion of who you are and traceable in state. That is a limited and simplistic way to think about traceability.
  - Alternatively, people could hold a whole set of SBTs that shows affiliations to communities and each community at least have some capacity to trace their members and have authorities over their assets for community recovery.
  - The governments could also set standards of SBTs that you have to collect to do certain kinds of activities with certain entities. So there would be different collections of SBTs that might be sufficient to give you accountability for different activities. But it wouldn't be traceable through legal naming, it would have to be affiliated with enough communities diversely and jointly, to have enough credibility that you will reach the threshold. That is much more secure because you can play with legal names, but it is much more flexible and pluralistic. I hope we could get to regimes that would be a little more like that.
  - In Bogota, Columbia, they have stronger AML measures and you have to give a legal document number in order to do a transaction, even buying food on the street with a credit card. That is not desirable and there are much more thoughtful ways to achieve traceability to transactions than requiring a passport number. You can have different thresholds for different transactions and contexts.
  - Eventually, you would have to change the framework, laws, many people would have to be able to access these technologies, would have to be one of many options so that you don't exclude people.
- What would be the necessary and sufficient conditions for a working decentralized society? What would be the necessary elements?

- It is useful to know the contributions. That enables individuals to coordinate with others in an open-source much more easily. Especially the scientific community.
  - Different institutions would be governed democratically to a certain extent and even the most democratically governed society is nowhere near what could be possible. So it is an ambition, aim, goal, not a threshold.
  - It is not an end state, it is a north star. The key goal of the north star is just retain governance and critique technology (rather than technology govern us). Active engagement with the tools of technology is one of the primary values.
- What is the important aspect when we have to think about when we are trying to integrate SBTs in different cultures and norms we have?
  - Hopefully, the SBTs should capture social groups, norms, expectations (including privacy), and not righting it over. It should enable people to express their norms which Web2 was not good at doing.
  - What is the interaction between the systems is an interesting game theory question.
  - A lot of traditional corporations would want to use them as a way to give access to services that gate native Web3 people. A lot of the aim depends on the aims, needs, cultures, and values.
- How would SBTs coexist with other identities? How would large populations adopt SBTs?
  - Whether it is DID, VC, or SBTs, you need to have a wallet (custodial or non-custodial), being the way to benefit from these tools.
  - In the same way you scale traditional identity, you will scale them the same way as you would to tokens, creating access to tools/wallets that would enable people to showcase their distributed shares of these tokens.
  - The way that they would coexist is having wallets of different identity, experiments are yet to come.
  - All of these are going to end up being messy processes. Hope that there will be public institutions trying both the experimentation and when there are clear patterns, make a standardization.
- How to balance privacy and publicity?
  - With the SBTs, you can preserve the privacy while still being interoperable in the blockchain and smart contracts. There has been enough proof of concept out there to present that the SBTs have the ability of selective disclosures, as well as preserving tradeoffs between privacy and publicity.

- We are only starting to understand what we mean by privacy and publicity. The reality is, privacy is conceived as almost binary, which is not helpful. What actually matters is what communities of people have access and in what way, what ability to disclose on what terms, collectively or individually to other parties. This is why we call it socially programmable privacy.
  - The publicity idea has been dramatically misunderstood. Something could be available somewhere but extremely hard to discover and not widely understood, and that is a very thin version of publicity. What we usually mean publicity is simultaneously/close to simultaneously gets into the minds of a very large number of people.
  - We use these terms without richness or precedent. Actually what we want to get at is a rich range of programmability in both the notion of privacy and publicity. Things could be mixed; something could be extremely public to a very limited within the community but extremely secure externally (e.g. military operation).
  - We have to get through the notion of privacy and publicity, and socially meaning of privacy and publicity.
- In your opinion, who do you think are the key stakeholders and what are their different roles? As we have multiple stakeholders here today, could you share some of the benefits you imagine that SBTs can bring to each of them? (Government/policy, business, users, academia)
  - Communities which will be using these. DAO Star is a consortium of DAOs focused on governance. Representation from there would be very valuable.
  - Ministers of Digital Transformation who are interested in experimenting in the public sector.
  - People who are concerned about potential harms which includes people involved in tech ethics.
  - Large and established institutions that are considering going into space. It could be a blockchain team from large corporations.
  - Social, entertainment, culture communities that have been seen in the NFTs could be interested in adopting this.
  - Anyone experimenting with SBTs. They are the heart of the problem of programmable social privacy.
- Message to the audience.
  - RadicalXChange hosts a blog which introduces what is going on and definitely keeps track of that.

- SBTs are great social coordination tools and if you are part of a community that is seeking better coordination, think about how SBTs could help.
- Working through the tradeoffs is what every community is trying to answer.

## Round Table on NFT, SBT

<https://tube.switch.ch/videos/eYrLfjB4r6>

- From what we have understood, SBTs primarily fall in 3 categories. i.e. Affiliation SBTs, Credential SBTs and Commitment SBTs. What are the fundamental properties that differentiate these SBTs?
  - SBTs can be thought of as right to various things (e.g., the right to access the document, purchase assets at some price).
  - All of these could be in the larger umbrella category of social groups. The social groups have different levels of rights, responsibilities, permissions, access controls etc.
- How possible is it to establish a voting system through soulbound tokens instead of a voting system based on market mechanisms such as quadratic voting? If you have ideas about it, can you share some of your insights?
  - Ecosystems that use SBTs to interpret quadratic voting/funding in ways that are partially but not completely clustered together. Separation of quadratic voting roots is dependent on the pattern of affiliations that you have. The most simplistic example is suppose that everyone has just one affiliation, you could put all of the funds in the quadratic funding route given by the same affiliation then give the matching fund only applied to those cooperation of social groups. There are infinitely more elaborate things than that.
  - It is not a prefilter and in the process itself. Prefilter could be one part but that is just one piece. The main use of that is to condition the ways votes are tallied.
- There is a focus on social network theory in the paper. However, memberships and credentials seem to be a big part of the paper. What do you think about the perspective of social capital?
  - SBTs are not a great way to represent broader conditions and formation of social relations. They can represent social networks and cooperation on them.
  - Social Capital is embedded in the social network and at the end of the paper we start to gesture towards alternative ways to think about trust relationships and in the ways that eschews the status in SBTs and capture it even better to bring equality and bring in social capital formation.

- What are your thoughts about transferability and non-transferability of souls?
  - The pattern that is created by all those things linked to the wallet makes these transfers challenging at least once the system gets on going.
  - It is unclear why you transfer your soul if they also have the rights and permissions associated with them to other communities that you participate in. It would have to be for a large sum of money, but for a large sum of money it is not a credible sale because of the community recovery (what we propose is a community recovery mechanism). And all the subsequent actions would be tracked.
  - There are cases where transferable makes sense. When somebody dies, their soul is at least partially passed on to the children.
  - We want the social norms of personhood to be governed for transfers. (Privacy Death.)
- Do you have specific use cases for governments in mind?
  - Other than the AML/KYC, another would be the way to prove that you are above the age of 21 and eligible for action by having some drivers license or government issued ID. These are extremely easy to fake and they are also based on bureaucrat processing. When there is so much information that you are above the age of 21 or not, it would make much more sense if you have secure implementation, to have patterns of information rather than one document.
  - In order to earn rights for voting/participation, there are arbitrary tests for immigrants. When you think of rights as an accumulation of community granting more permissions and rights eventually, would be an alternative way to determine citizenship which is a more social and pluralistic way to view citizens. You could change the whole nature of citizenship.
- Examples of elective disclosure protocols that have been used in SBTs added in the report would be great.
- In the near future, we are not going to get a single credential format and live with multiple credentials.
- As opposed to using community, how about using such as biometrics data for recovery?
  - Critique of the proof of personhood is that you lose the social differentiation on both the security of the properties and pluralistic properties of social incentive design.

- In an attempt to build decentralized networks, biometrics fails to capture the richness of sociality which is critical when you want to decentralize systems.
- Soulbound tokens define the individual as a very social component, dependent a lot on community. That is true but that could have a handicap on people that are not much connected even if they could influence society like Nietzsche. How could this slow down the mechanism of the future?
  - Self sovereignty is an illusion, we are social creatures and we have a social membership and affiliations. It might not come into the same form for everybody but at a very least we are born into a family and a region. Even language is a social phenomenon. Zarathustra way is not a view of individuality now or ever.
  - Issuance of multiple SBTs makes it rich and enables social coordination.
- How about the people who are left behind? What could potentially happen to those cases?
  - It also applies to vulnerable communities too.
  - SBTs is a tool and it makes it explicit what decisions of choices we make with our relationship with technology. Currently we are having these decisions made from a Web2 company or nation states for us. SBTs empower us to protect minorities and choose mechanisms like consensus across differences, but we have to be intentional about it.
- How about the right to be forgotten on negative information in the context of SBTs?
  - SBTs give you a right to participate and are not public to the world which makes it programmable privacy based on the decision of the social group that is issuing.
  - Negative reputation depends on the rules social groups are agreeing to.
  - The idea of making claims about someone else publicly whether they would be positive or negative is inevitable and there would be only a few ways that we can control that. That is consistent with the VC and DID as well as SBTs. What matters more is how to manage negative information, more client facing solutions we could think about. We could look into only signed or approved SBTs which give consent. There are ways to go around filtering this as we do today with NFT protocols that integrate with wallets, but there is no way yet today to inhibit making negative claims about some individuals.

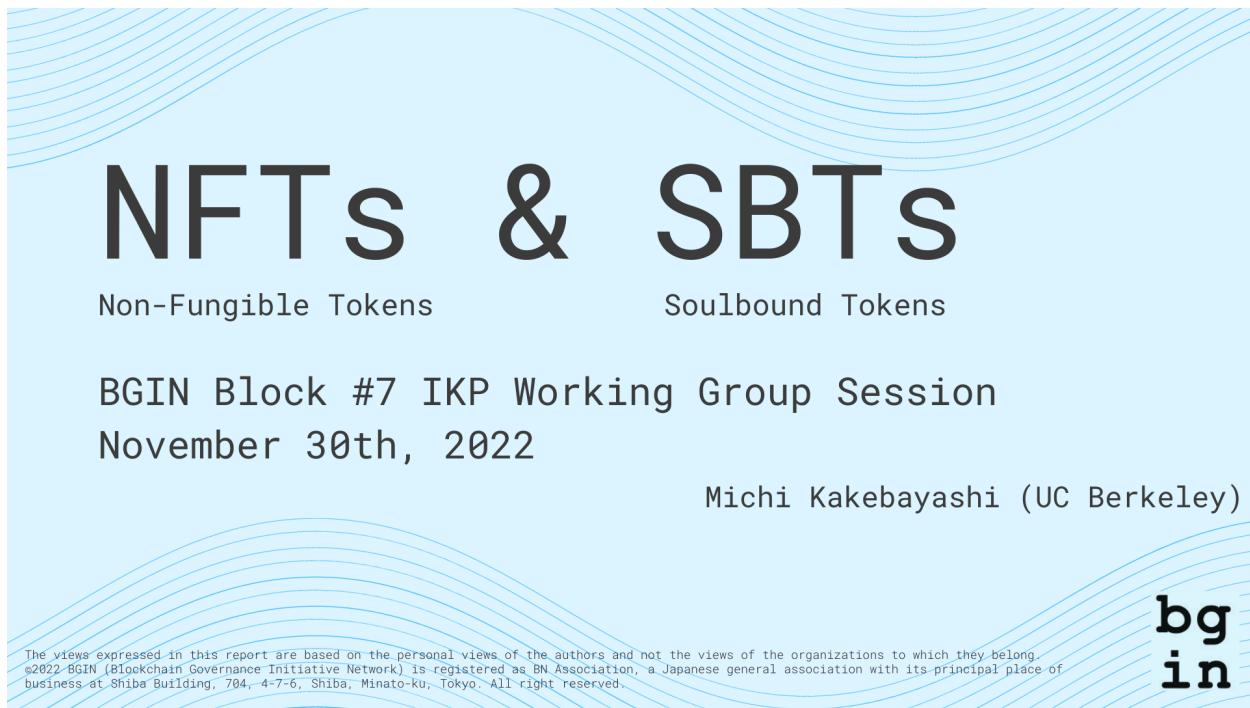
- What are your thoughts on data ownership?
  - We are going more towards social data (capturing social) that needs to be determined and programmed by the set of contributors to that data.
  - SBTs can be seen as a tool to let social groups come together and determine the data.

# Appendix D – BGIN Block #7 Session Slides

The slides that has been presented by Michi Kakebayashi and Joseph Beverley can be found in the following link. Videos are available too [BGIN Media - YouTube](#).

Part 1: [https://drive.google.com/file/d/1P\\_fXOvomHqVBbALK1amaeXtii5r0rLb2/view](https://drive.google.com/file/d/1P_fXOvomHqVBbALK1amaeXtii5r0rLb2/view)

Part 2: [https://drive.google.com/file/d/1EyhVjAee1r4CXj1PWER1Pdyld-Y\\_E93u/view](https://drive.google.com/file/d/1EyhVjAee1r4CXj1PWER1Pdyld-Y_E93u/view)



## 1. NFT STUDY REPORT

PART 1: INTRODUCTION AND USE CASES

(JUNE, 2022)

## 2. SOULBOUND TOKENS (SBTS) STUDY REPORT

PART 1: BUILDING AND EMBRACING A NEW  
SOCIAL IDENTITY LAYER

(NOVEMBER, 2022)

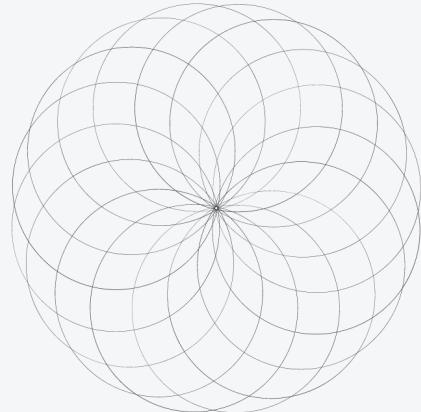
**bg  
in**

# NFT Study Report

## Part 1:

### Introduction and Use Cases

Claudio Levini (Seven Labs / Liquid federation)  
Henry Hobin (Georgetown University)  
[BGIN\\_PWI\\_SR005\\_NFT\\_Study\\_Report\\_Part1](#)



**bg  
in**

This report is based on the information available as of March 1, 2022

## 1-1 Overview of NFTs

- “Ownership” in the virtual world
- Key difference to cryptocurrencies: Fungibility and Non-fungibility
- Marketplaces for NFTs: LooksRare, OpenSea
- Use Cases: Digital Art, Digital Goods, Physical Goods

**bg  
in**

# 1-2 Key Considerations

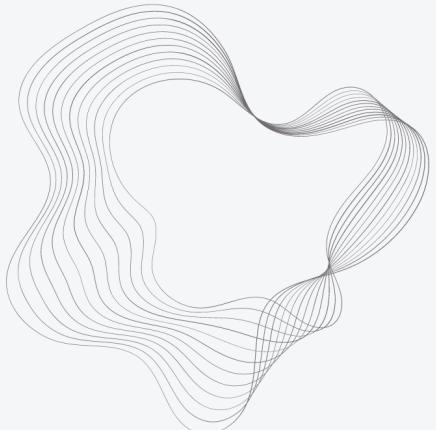
- Authenticity
- Off Chain File Storage
- Money Laundering
- Wash Trading
- Regulatory and Tax Implications
- Fractionalization

**bg  
in**

## Soulbound Tokens (SBTs) Study Report

### Part 1: Building and Embracing a New Social Identity Layer

Michi Kakebayashi (UC Berkeley)  
Joseph Beverley (Soulbis)  
[BGIN\\_WD\\_SR008\\_Soulbound\\_Tokens\\_\(SBTs\)\\_Part\\_1](#)



**bg  
in**

## 2-1 Identity in the Internet

"The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception which will cumulatively erode public trust in the Internet."

Kim Cameron (2005) "The Laws of Identity"

**bg  
in**

## 2-2 What are SBTs?

"Decentralized Society: Finding Web3's Soul" (Weyl et al., 2022)

1. Publicly visible
2. Non-transferable
3. Possibly revocable
4. Issuer arbitrated

(self-certified/certified by other related Souls)

- ✓ No requirement for a Soul to be linked to a legal name
- ✓ No requirement to be a "one Soul per human"
- ✓ The definition of SBTs provided by the authors were to limit the technical complexities of SBTs for an initial proof of concept, and was never meant to be all-encompassing.

**bg  
in**

## 2-3 Social Coordination

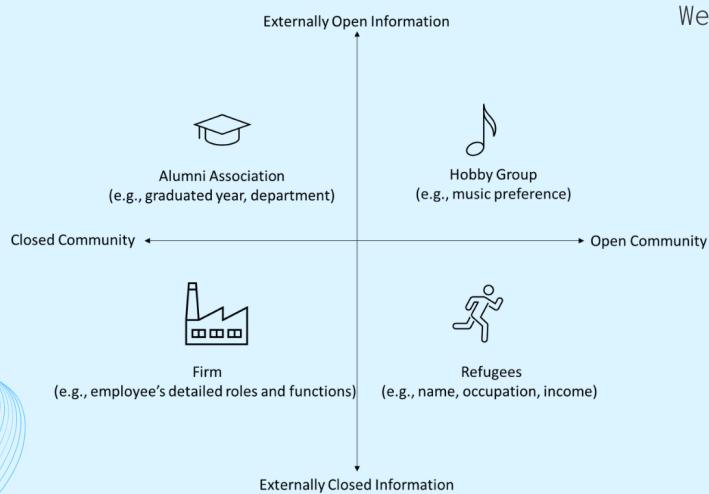
- Trust, reputation, personally identifiable information (PII), etc.
- Social coordination in a bottom-up and decentralized manner.
- There are many existing forms of social coordination such as local community, school alumni associations, interest groups, etc. The smallest community unit could be a family or a couple.
- Identity is only established in a community. It does not suddenly get established like the "overhuman" from Nietzsche's "Thus Spoke Zarathustra".

**bg  
in**

## 2-4 Programmable Privacy

"Rather than privacy-as-transferable-property-right, a more promising approach is to treat privacy as a programmable, loosely coupled bundle of rights to permission access, alter or profit from information."

Weyl et al. (2022)



**bg  
in**

## 2-5 Community Recovery

"By embedding security in sociality, a Soul can always regenerate their keys through community recovery, which deters Soul theft (or sale): because a Seller would need to prove selling the recovery relationships, any attempt to sell a Soul lacks credibility."

Weyl et al. (2022)

- ✓ If it is recoverable, it can still be able to be revoked and/or lost by the Soul who may even **choose for it not to be found** (even temporarily).
- ✓ Recovery is in principle nominated by the Soul and achieved by a social community. If an SBT design has only revocability without recoverability, that would raise concern for the **sovereignty of the soul**.
- ✓ Social recovery in a centralized system as a promise of "give you more control over your account security" could be easily forfeited. (**Single point of failure**)

**bg  
in**

## 2-6 How are SBTs different?

	SSI with DIDs	NFTs	SBTs
General Aim	Decouple entity authentication from centralized registries, identity providers, and certificate authorities	Tracking distinguishable assets	Social coordination
Transferability	Some DIDs are transferable	YES	NO
Fungibility	Depends on the DIDs and its ecosystem	NO	Based on the use case, can be both fungible, non-fungible, and semi-fungible
Priority	YES	NO	YES
Social Recovery	Depends on the DIDs and its ecosystem	NO	YES
Standardized at an SDO	DIDs are standardized at W3C	Generally not standardized. However, for Ethereum, is standardized.	Not standardized (In the process of being standardized through Ethereum Improvement Proposal (EIP))

**bg  
in**

## 2-7 Basic Principles

### "The Laws of Identity"

(Cameron, 2005)

1. User Control and Consent
2. Minimal Disclosure for a Constrained Use
3. Justifiable Parties
4. Directed Identity
5. Pluralism of Operators and Technologies
6. Human Integration
7. Consistent Experience Across Contexts

### "The Seven Principles of Digital Being"

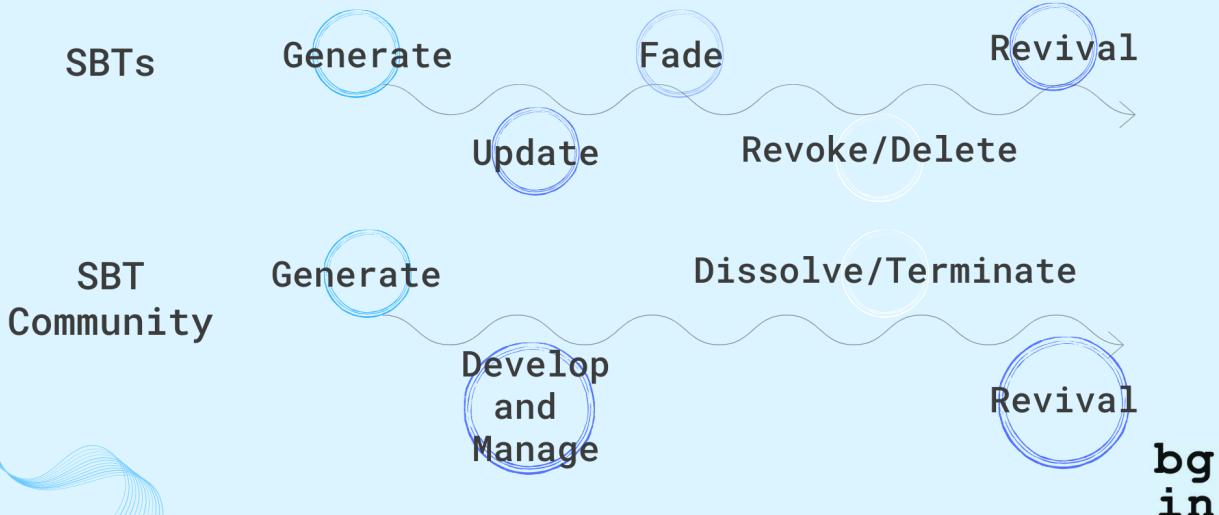
(Sakimura, 2021)

1. Accountable Digital Being
2. Expressive Digital Being
3. Fair Data Handling
4. Right NOT to be Forgotten
5. Human Friendly
6. Adoption Friendly
7. Everyone benefit

"right to be forgotten"  
(GDPR)

**bg  
in**

## 2-8 Lifecycle Management



## 2-9 Development

*Non-transferability and a Store of Social or Reputational Value*

1. EIP-4671: Non-Tradable Tokens Standard
2. EIP-4973: Account-bound Tokens
3. EIP-5114: Soulbound Badge
4. EIP-5192: Minimal Soulbound NFTs
5. EIP-5484: Consensual SBTs
6. EIP-5727: Semi-Fungible Soulbound Token
7. EIP-5516: Soulbound Multi-owner Tokens
8. EIP-5633: Composable Soulbound NFT, EIP-1155 Extension
9. EIP-3525: Semi-Fungible Token



## 2-10 SBTs Lead Potentials

1. Counter Illicit Economic Activities
2. Promote Regulatory and Tax Compliance
3. Diminish Unintentional Information Asymmetry
4. Fair, Transparent, and Accountable Governance
5. Opportunities for Innovation

and much more...



# 2-11 Limitations & Questions

Introducing some from the paper...

- **Further Innovation:** There will be at least a need for creating a platform to issue proto-SBTs/proto-soul issuers as another layer before rolling out.
- **Design:** Without a good design on the revocability, it could lessen the trust and functionality of the whole SBT ecosystem or the SBT community.
- **Privacy and Transparency:** How to prevent evasive usage of privacy regulations must be considered. What are the mechanisms necessary to eliminate improper usage of SBTs?
- **Responsibility:** How do the legal rules, enforcement, and judiciary apply to the SBTs?
- **Implementation:** How to promote adoption and scalability in an early stage?

**bg  
in**

## Thank you!

We will further explore at Part 2.

Join us and be part of the BGIN multi-stakeholder discussion!

IKP WG/SGIP bi-weekly call:  
on every other Thursday at 14:00-15:00 PM UTC  
Register for the mailing list to join the discussion.  
[BGIN-IPKM\\_Info\\_Page\\_\(blockchain-discussions.org\).](http://BGIN-IPKM_Info_Page_(blockchain-discussions.org).)

**bg  
in**

# Soulbound Tokens Paper Part 2

BGIN Block #7 IKP Working Group Session  
November 30th, 2022

Joseph Beverley (Soulbis)

The views expressed in this report are based on the personal views of the authors and not the views of the organizations to which they belong. BGIN (Blockchain Governance Initiative Network) is registered as BN Association, a Japanese general association with its principal place of business at Shiba Building, 704, 4-7-6, Shiba, Minato-ku, Tokyo.



Introduction - Table of Contents

Slide 2/23

## What I Will Discuss:

- |                                   |                               |
|-----------------------------------|-------------------------------|
| 3. Introduction                   | 20. BGIN + Paper Coordination |
| 8. Soulbound Token Paper: Part 1  | 22. Q&A + Contact             |
| 11. Soulbound Token Paper: Part 2 | 23. Soulbound Token Panel     |
| 17. Topic Research                |                               |



# Introduction

Overview / Who am I / What I've Seen / SBT Background



## Overview

### What we've accomplished

- The first SBT Research paper
- Successful multi-industry co-ordination
- Amplified voice for BGIN

### What we're doing

- Starting the follow on paper
- Involving a larger cohort across complementary sectors
- Expanding the influence of BGIN

### What you should expect

- SBT paper part 2 (~6 months)
- Dozens of individuals across the world to contribute
- BGIN to provide the backbone behind SBT research



# Who Am I?



**Joseph Beverley**  
Partner & Co-Founder of Soulbis

Joseph is a Strategic Advisor & Researcher in Web3, covering theoretical decentralised concepts, foundational protocol level mechanisms and web3 venture methodology.

## Areas Involved:

- CBDCs
- KYC/AML Technology
- Decentralized Innovation
- Web3 Ventures
- Soulbound Tokens

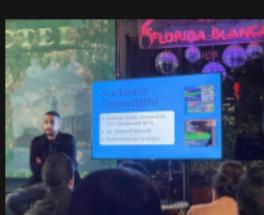


bg  
in Soulbis  
© Soulbis Pty Ltd, 2022

# What I've Seen...



The Metaverse Overview, Cryptomera Capital  
(September, 2022)



Presentation at Nearcon, Verano (September, 2022)



Report for 'Decentralized Society: Analysing Web3's Use' and 'Recommendations for Shaping Purpose Built Decentralized Digital Identity Infrastructure'

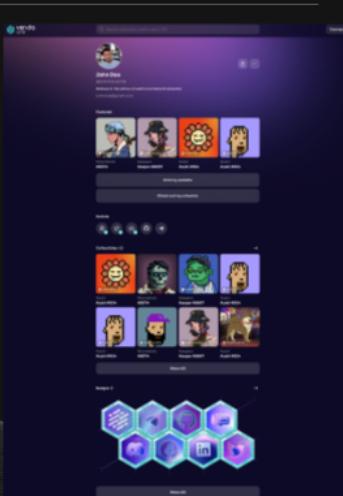


Binance to Launch Binance Account Bound (BNFT) Token, the First-ever Soulbound Token on Binance Chain  
(September, 2022)

Presentation in Australian DeFi Association (September, 2022)



How to Mint NFTs (Soulbis)



Verida One Profile (November 2022)

bg  
in Soulbis  
© Soulbis Pty Ltd, 2022

# Soulbound Token Background

## Context

- Initial blog post published in January 2022 'Soulbound' by Vitalik Buterin [1]
- Discussion paper published in May 2022 titled 'Decentralized Society: Finding Web3's Soul' by Vitalik Buterin, Puja Ohlhaven and E. Glen Weyl [2]
- Soulbound tokens as defined in the discussion paper was for a proof of concept - not an all encompassing definition
- Debate on which feature is more essential: 1) 'Revoke' or; 2) 'Recover'

## Key quotes

*"While blockchain inclusion enables us to trace the time a particular work was made, SBTs would enable us to trace the social provenance"*

*"An ecosystem of SBTs could unlock a censorship-resistant, bottom-up alternative to top-down commercial and "social" credit systems."*

*"privacy as a programmable, loosely coupled bundle of rights to permission access, alter or profit from information"*

*"favoring cooperation across differences simply means discounting cooperative rewards to similarly affiliated or correlated Souls—similarity measured by their shared SBTs."*

[1] Soulbound, Buterin, Vitalik (2022)  
[2] Decentralized Society: Finding Web3's Soul, Weyl, Eric Glen et al (2022)

bg  
in Soulbis  
© Soulbis Pty Ltd, 2022

# Soulbound Token Paper: Part 1

## Key Discussions / Contributions

bg  
in Soulbis  
© Soulbis Pty Ltd, 2022

## Key Discussions

### Topics

- Market Failures leading to SBTs
- NFT deficiencies
- SBT Design choices
- SBT Ecosystem
- SBTs in relation to VCs/DID
- SBT Lifecycle

### Questions

1. What market failures catalysed the need for SBTs?
2. What literature and resources point towards soulbound token use cases?
3. What models can be used to fairly compare SBTs to other digital identity primitives?

 Soulbis  
© Soulbis Pty Ltd, 2022

## Contributions

### Summary

**Words:** ~16,659 words

**References:** 39 references

**Pages:** 56 pages

**Timeline:** 5 Months

**Status:** Open for Public Comment

### Authors & Contributors

2 editors / co-editors

14 contributors

Academics / Corporate / Consultants / Researchers

 Soulbis  
© Soulbis Pty Ltd, 2022

# Soulbound Token Paper Part 2

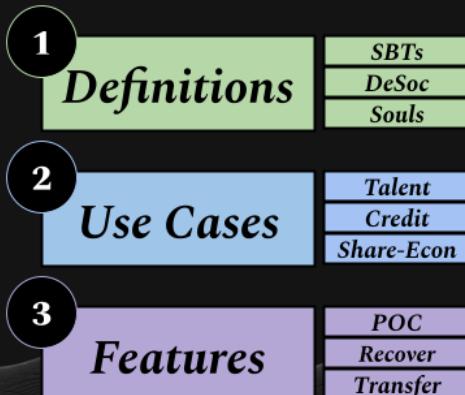
Rationale / SBT POC Definition / Decentralized Society Definition / As Is - To Be

 Soulbis  
© Soulbis Pty Ltd, 2022

## Rationale

### SBT Challenges

- No Clear Definitions
- Evolving Space
- Lack of commercial models
- Limited discussion on technical aspects
- Institutions are particularly interested
- Opportunity to shape innovation



 Soulbis  
© Soulbis Pty Ltd, 2022

## Soulbound Token POC Definition

### 1 Publicly Visible

"We initially assume publicity despite our deep interest in privacy because it is technically simpler to validate as a proof-of-concept, even if limited by the subset of tokens people are willing to publicly share." - (3) Souls, Page 2

### 3 Possibly Revocable

"Revocable, transferable tokens are a kind of proto-SBT—serving supportive, placental functions before Soul birth. These tokens buy time both for wallets to gestate secure, community recovery mechanisms and for a person to sufficiently accumulate proto-SBTs that can eventually be burned and re-issued into non-transferable SBTs." - (9.1) Proto SBTs, Page 28

"publicly visible, non-transferable (but possibly revocable-by-the-issuer) tokens."

[2] (3) Souls Page 2

### 2 Non-Transferable

"non-transferability prevents transferring or hiding outstanding loans, while a rich ecosystem of SBTs ensures that borrowers who try to escape their loans (perhaps by spinning up a fresh Soul) will lack SBTs to meaningfully stake their reputation." - (4.2) Soul Lending, Page 4

### 4 Issuer Arbitrated

"In their simplest form, these SBTs can be "self-certified," similar to how we share information about ourselves in our CVs... SBTs held by one Soul can be issued—or attested—by other Souls, who are counterparties to these relationships. These counterparty Souls could be individuals, companies, or institutions." - (3) Souls, Page 2

[2] Decentralized Society: Finding Web3's Soul, Weyl, Eric Glen et al (2022)

**bg**  
**in** Soulbis  
© Soulbis Pty Ltd, 2022

## Redefining Soulbound Tokens

Interested in future terms expanding on recursive issuance to show providence and authenticity - the weight of current soul issuing a new soul is carried through... Potentially a scale of 'soul printing'.

We believe it's important to emphasise 'recoverability' over 'revocability' - understanding that the authors chose 'possibly revocable' because of the complex infrastructure required to recover an immutable tokens in a permissionless network.

It might be in our interest to scope out a derivative of Soulbound Token that meets initial definitions - a "Smart Lien" [3]. Where a 'smart lien' or 'lienbound token', could lead to meeting issuers looking to have enhanced revocable permissions or atomic compositability.

"Non-transferable - equally recoverable tokens." **publicly visible**

At the same rate an SBT is intended to be non-transferable, it should at the same rate be recoverable. Elements of transfer/destruction will exist even in a non-transferable environment, but determining the ability to recover a soul that is out of place (stolen, soul wallet sold, exploits).

Omitted this citing Nick Szabo (1996) "knowledge and control over the contents and performance of a contract should be distributed among parties only as much as is necessary for the performance of that contract" [3]

A blockchain's transparency enables a superficial level of transparency, any smart contract using ZKP or layering or atomised information could break this definition. We should prepare for the soulbound token ecosystems end-state over the primordial stages.

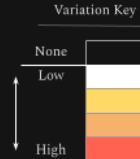
[3] Smart Contracts: Building Blocks for Digital Markets, Nick Szabo (1996)

**bg**  
**in** Soulbis  
© Soulbis Pty Ltd, 2022

# What is Decentralized Society?

## Comparative Definitions

"—a co-determined sociality, where Souls and communities come together bottom-up, as emergent properties of each other to co-create plural network goods and intelligences, at a range of scales." » Abstract, Cover Page



"a co-determined sociality, where Souls and Communities convene bottom-up, as emergent properties of each other to produce plural network goods across different scales." - (6) Decentralized Society, Page 17

"—a co-determined sociality, where Souls and communities come together bottom-up, as emergent properties of each other to co-create plural network goods, including plural intelligences, at a range of social scales." - (2) Outline, Page 2

## Use Case Definitions

"DeSoc encodes trust networks that underpin the real economy today and enables us to harness them to generate plural network goods resilient to capture, extraction, or domination." - (6) Decentralized Society, Page 18

bg  
in Soulbis  
© Soulbis Pty Ltd, 2022

# As is - To Be

## Current State

- Lack of an overarching definition of SBTs, only proof of concept SBTs are defined
- Definition of Decentralized Society is fractured
- Features for future iterations of SBTs are conceptual and require further exploration
- Lack of referenceable material
- Lack of content diversity
- No standards in place

## Ideal outcomes

- Clear definitions
- Delineate between proof of concept & futures
- Strong, peer reviewed research and industry analysis to base future studies & technology
- Cover a range of topics: design, commercials, technicalities, use cases
- Peer-reviewed standards
- Clarify value mechanisms

bg  
in Soulbis  
© Soulbis Pty Ltd, 2022

# Topic Research

Topics (non-exhaustive) / Example: Revoke vs Recover



## Topics (non-exhaustive)

- **Reputational Value:** How is reputational value informed, and what models are compatible with blockchain immutability
- **Analogues in Classical Writing:** How is the Soul & social value codified throughout history in classical writing - Les Miserables, The Republic (non-exhaustive)
- **Clear Definitions:** How can DeSoc / SBTs / Souls / Soul Guardians / Soul issuers be accurately defined for consumption by a plurality of individuals and groups?
- **Use Cases:** How can soulbound tokens overhaul recruiting processes, enhance credit scoring (includes social credit scores) and provide further confidence in the share economy applications
- **Soulbound Token Innovation:** What projects are in the development and how can BGIN provide the necessary research to reduce tech debt and leaner products?



## Example: To **Revoke** or to **Recover**

### Revocable

**Revocable** - Oxford Dictionary  
/rɪ'vəkəbl/ adjective

capable of being revoked or cancelled.

Times **revocable\*** appeared within the DeSoc paper:  
Pages appeared: 4 pages  
Mentioned times: 8 times

Denotes authority, centralisation and is permissioned

The revoking of a credential is generally rare and imposed rather than agreed or substantiated by multiple parties. Potentially limiting agreed use cases or leading to a autocratic use cases.

\*Includes all derivations & inflections

### Recoverable

**Recoverable** - Oxford Dictionary  
/rɪ'kʌvərəbl/ adjective

(of something lost) able to be regained or retrieved.  
(of compensation or money spent or lost) able to be regained or secured by means of a legal process or subsequent profits.

Times **recoverable\*** appeared within the DeSoc paper:  
Pages appeared: 7 pages  
Mentioned times: 36 times

Denotes pluralism, decentralisation and is permissionless

Soulbound tokens express reputational value, either superficially or by self-sovereign compositability. To recover is to restore what is misplaced, whilst the possibility of revoking/revocability is still possible

**bg**  
**in** Soulbis  
© Soulbis Pty Ltd, 2022

## BGIN + Paper Coordination

Opportunity / Next Steps

**bg**  
**in** Soulbis  
© Soulbis Pty Ltd, 2022

# Opportunity

Overhaul BGIN Processes	Recommend new tooling	Expand sphere of influence
Update the means to conduct outreach	Utilise tools such as Notion, Mailchimp	Increase awareness of SBT paper
Look beyond SBT paper, and coordinate as a group	Improve how we coordinate and how we can be found	Involve a range of individuals, industries and working groups
Potential fork of SBT working group	Give time back to other working groups	Apply regular updates to followers and contributors



## Q&A (5 minutes)

# Soulbis

Blockchain research and advisory firm specialised in soulbound tokens and decentralized innovation.

### Contact Us:

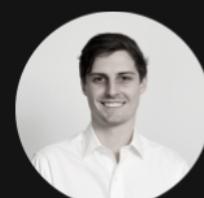
[Joey@Soulbis.com](mailto:Joey@Soulbis.com) / Telegram: JoeyNB\_COS / LinkedIn: [Joseph Beverley](#)  
[Mitchell@soulbis.com](mailto:Mitchell@soulbis.com) / Telegram: Mitchuski / LinkedIn: [Mitchell Travers](#)



**Joseph Beverley**  
Partner & Co-Founder

Joseph started in 2012 mining bitcoin out of the family garage, and grew up surrounded by blockchain technology. Joseph is a Strategic Advisor & Researcher in Web3 covering theoretical decentralised concepts, foundational protocol level mechanisms and web3 venture methodology.

Alongside his advisory experience and research, Joseph has spoken across the globe – including Monaco, Paris, London, Sydney, Melbourne and Stockholm on DeSoc, DAOs, DeFi, SBTs and smart contract technology.



**Mitchell Travers**  
Partner & Co-Founder

Mitchell is passionate about transforming society through the utilisation of blockchain technology and promotion of decentralised governance systems. He has worked in the industry for over 6 years.

At Soulbis Mitchell leverages experience and knowledge in decentralised innovation, tokenomics, CBDCs, stablecoins, payments, digital identity, soulbound tokens, web3 go-to-market and product strategies.



## Panel (20 min) - Soulbound Tokens



**Nat Sakimura**  
(Moderator)  
**OpenID Foundations**  
Chairman



**Joseph Beverley**  
**Soulbis**  
Partner & Co-Founder



**Michi Kakebayashi**  
**UC Berkeley**  
MPP Candidate



**Shai Perednik**  
**Amazon Web Services**  
Global Tech Lead  
Web3/Blockchain



**Mitchell Travers**  
**Soulbis**  
Partner & Co-Founder

**bg in Soulbis**  
© Soulbis Pty Ltd, 2022

## References

### References

- [1] Buterin, Vitalik, 2022. "Soulbound". Available at <https://vitalik.ca/general/2022/01/26/soulbound.html>
- [2] Weyl, Eric Glen and Ohlhaver, Puja and Buterin, Vitalik, 2022. "Decentralized Society: Finding Web3's Soul." Available at SSRN: <https://ssrn.com/abstract=4105763>
- [3] Szabo, Nick. 1996. "Smart Contracts: Building Blocks for Digital Markets." Available at [https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.bestvwh.net/smart\\_contracts\\_2.html](https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.bestvwh.net/smart_contracts_2.html)

Soulbis

**Soulbis**  
© Soulbis Pty Ltd, 2022