去中心化社会：寻找 Web3 灵魂

E. Glen Weyl,2 Puja Ohlhaver,3 Vitalik Buterin4

F. 2022.5 月

“道是万物的灵台和家园”
“善良的灵魂珍惜它，迷失的灵魂在它里面找到庇护”
--老子，#62

摘要

1 引言

Web3 在不到十年的时间里打造了一个具有前所未有的灵活性和创造性的并行金融系统，震惊了世界。密码学和经济原语，也即构建模块，比如公钥密码学、智能合约、工作量证明 (PoW) 和权益证明 (PoS)，已经形成了一个复杂而开放的金融交易生态系统。

然而，金融交易依赖的经济价值是由人及其关系产生的。由于 Web3 缺乏表示这种社会身份的原语，Web3 已经从根本上依赖于它想要超越的非常中心化的 Web2 结构，因此复制了 Web2 的局限性。

这些依赖关系的事例包括：
1. 缺乏 Web3 原生的身份和声誉迫使 NFT 艺术家经常依赖于中心化平台，比如 OpenSea 和 Twitter 来承诺稀缺性和初始来源，并阻止了不完全抵押的贷款形式。
2. 试图超越简单的代币投票的 DAO 通常依赖于 Web2 基础设施 (如社交媒体账户)，以抵抗女巫攻击。
3. 许多 Web3 参与者依赖于由 Coinbase 等中心化机构管理的托管钱包。去中心化密钥管理系统对任何用户都不是友好的，除了那些最老练的人。

此外，由于缺乏原生的 web3 身份，如今的 DeFi 生态系统无法支持实体经济中无处不在的活动，如低抵押贷款或简单的合同，如公寓租赁。在我们的论文中，我们将说明，即使是使用 Web3 原语来表示社会身份的微小而渐进的步骤，也可以解决这些问题，并使生态系统更接近于再生市场及其在原生 Web3 环境中的人际关系基础。

更有希望的是，我们强调具有丰富的社会可组合性的 Web3 原生社会身份，可以在 Web3 中围绕财富集中和治理对金融攻击的脆弱性等更广泛的长期问题上取得巨大进展，同时激发创新政治、经济和社会应用的寒武纪式大爆发。我们将这些用例和它们所支持的更丰富的多元生态系统称为“去中心化社会”(DeSoc)。

2 概述

我们首先解释了 DeSoc 的基本原理，围绕着持有不可转让(最初是公开的)“灵魂绑定”代币的账户(或钱包)，代表承诺、凭证和从属关系。这种代币就像加长版的简历，由其他钱包发行，证明这些社会关系。

然后，我们描述了跨社交堆栈的日益雄心勃勃的应用程序的“阶梯”，这些原语可以赋予权力，包括：

- 确定出处
- 通过声誉打开抵押不足的贷款市场
- 实现分散的密钥管理
- 阻挠和补偿协调的战略行为
- 衡量去中心化
- 创建具有可分解、共享权限和权限的新市场

这种描述以 DeSoc 的愿景达到高潮——一种共同决定的社会性，灵魂和社区自下而上地聚集在一起，作为彼此的新兴属性，在一系列社会尺度上共同创造包括多元智能在内的多元网络商品。

最后，我们回答了几个潜在的担忧和反对意见，并与 web3 空间中熟悉的其他身份范式进行了比较，经常承认我们的愿景只是第一步，但却是可编程隐私和通信方面的进步。然后，我们考虑技术途径来引导我们想象的愿景。在此基础上，我们更哲学地期待着 DeSoc 的潜力，将 web3 重定向到更深刻、更合法、更具有变革意义的道路上。

3 灵魂

我们的关键原语是账户（钱包），其中持有公开可见、不可转让（但可能由发行者撤销）的代币。我们将账户称为“灵魂”，将账户持有的代币称为“灵魂绑定代币”（SBT）。尽管我们对隐私有着浓厚的兴趣，但我们最初假设是公开的，因为它在技术上更容易验证为概念验证，即使受到人们愿意公开分享的代币子集的限制。在本文的后面，我们为更丰富的用例引入了“可编程隐私”的概念。

想象一个世界，在那里大多数参与者都有“灵魂”（即账户），其中存储着对应于一系列从属关系、会员资格和证书的 SBT（灵魂绑定的代币）。例如，一个人拥有的“灵魂”（账户）中可能存储了代表教育证书、他曾经工作过的公司、他所写的艺术作品或书籍的哈希值的 SBT（灵魂绑定的代币）。这些 SBT 最简单的形式是能够“自我认证”，就像我们在简历中分享自己的信息一样。但当一个“灵魂”（账户）持有的 SBT 可以由其他“灵魂”发放或证实时，这种机制的真正力量就显现出来了，这些其他“灵魂”是这些关系的交易对手。这些对手“灵魂”可能是个人、公司或机构。例如，以太坊基金会可以是一个向参加开发者大会的 Souls 发行 SBTs 的“灵魂”。大学可以是一个“灵魂”，向毕业生发放 SBT。一个体育场也可以是一个“灵魂”，向道奇队（Dodgers）的棒球铁杆球迷发放 SBT。

请注意，灵魂不需要与合法名称相关联，也不需要任何协议级别的尝试来确保“每个人一个灵魂”。灵魂可能是一个持久的化名，具有一系列无法轻易链接的 SBT。我们也不假设灵魂在人类之间的不可转移性。相反，我们试图说明这些属性如何在需要时自然地从设计本身中出现。

4 通往 DESOC 的阶梯

4.1 艺术&灵魂

灵魂是艺术家将自己的声誉押在作品上的一种自然方式。 当发行可交易的 NFT 时，艺术家可以从他们的灵魂中发行 NFT。艺术家的灵魂携带的 SBT 越多，买家就越容易识别灵魂属于该艺术家，从而也证实了 NFT 的合法性。艺术家可以更进一步，发行一个存储在他们灵魂中的链接 SBT，证明 NFT 的“ 收藏”成员资格，并保证艺术家希望设置的任何稀缺性限制。因此，Souls 将创建一种可验证的链上方式，以基于对象的出处和稀缺性进行抵押和建立声誉。

应用程序超越了艺术，延伸到服务、租赁以及任何建立在稀缺性、声誉或真实性之上的市场。 后者的一个例子是验证所谓的事实记录的真实性，例如照片和视频。随着深度造假技术的进步，人工和算法的直接检查将越来越无法检测出真实性。虽然区块链包含使我们能够追踪特定作品的制作时间，但 SBT 将使我们能够追踪社会出处，为我们提供丰富的社会背景来了解发布作品的灵魂——他们的成员、隶属关系、证书——以及他们的社会 到主体的距离。“ 深度赝品”很容易被识别为那些起源于时间和社会背景之外的艺术品，而可信的艺术品(如照片)则来自著名摄影师的认证。尽管目前的技术使文化产品（如图片）脱离语境，并使它们容易受到缺乏社会背景的不受限制的病毒式攻击，但 SBT 可以对此类对象进行重新语境化，并使灵魂能够利用社区中已经存在的信任关系作为保护声誉的有意义的支持。

4.2“ 灵魂”的借贷

也许直接建立在声誉上的最大金融价值是信贷和无抵押贷款。目前，web3 生态系统无法复制简单形式的无担保贷款，因为所有资产都是可转让和可出售的——因此只是简单的担保形式。传统的金融生态系统支持多种形式的无抵押贷款，但这些贷款通常是由中心化的信用评分机制调节的——这样做的理由是，信誉较差的借款人几乎没有动力分享有关其信誉的信息。

但这样的信用评分有很多缺陷。在最好的情况下，他们不透明地增加和减少与信誉相关的因素，并对那些没有积累足够数据的人(主要是少数族裔和穷人)构成偏见。在最坏的情况下，他们可能催生“ 黑镜”(Black Mirror) 式不透明的“ 社会信用”体系，从而促成社会结果，加剧歧视。

SBT(灵魂绑定代币) 生态系统可以开启一个抗审查的、自下而上的替代自上而下的商业和“ 社会”信用体系。代表教育证书、以前的工作经历和租赁合同的 SBT 可以作为与信用相关的长期记录，使“ 灵魂”(账户) 能够通过用有意义的声誉来获得贷款，从而避免了抵押品要求。贷款和信贷额度可以表示为不可转让的但可撤销的 SBT，这样贷款额度就可以嵌入到某个“ 灵魂”(账户) 的 SBT 中——作为一种 (不可没收的) 声誉抵押品——直到它们被偿还，并随后被销毁 (或者，更好的是，用“ 偿还证明”来替代，以增加“ 灵魂”的信用历史)。就像信用记录上的便条一样。SBT 提供了有用的安全属性：不可转让性的属性阻止了

转让或隐藏未偿还贷款，同时SBT丰富的生态系统确保了试图逃避贷款(可能通过创建一个新的“灵魂”)的借款人将没有SBT来有意义地抵押他们的声誉。

使用 SBT 来计算公开债务的便利性将催生开源的借贷市场。SBT 和还款风险之间的新的关联将会出现，产生更好的借贷算法来预测信用的可靠性，从而减少中心化的、不透明的信用评分基础设施的作用。更好的是，借贷可能会发生在社会关系中，产生新的社区借贷形式。特别是，SBT 可以为类似于诺贝尔奖得主 Muhammad Yunus 和格莱珉银行 (Grameen Bank) 开创的“团体借贷”的做法提供基础，即某个社交网络的成员同意支撑彼此的债务。因为一个“灵魂”的 SBT 代表了社会团体的成员资格，参与者可以很容易地发现其他“灵魂”，它们可能是团体借贷项目中有价值的共同参与者。商业贷款是一种“借他忘掉他”的还款模式，而社区贷款可能采取“借他并帮他”的方式，将营运资本与人力资本相结合，获得更高的回报率。

无担保社区贷款是如何起步的?一开始，我们希望灵魂只携带反映他们愿意公开分享的信息的 sbt，例如在一个简历。虽然范围有限，但这可能是一个足以启动社区内贷款试验的解决水平，特别是如果 SBT 由声誉良好的机构发行。例如，展示某些编程证书、参加过几次会议和工作历史的 SBTs 组合可能足以让 Soul 为他们的企业贷款(或筹集种子资本)。这种资历和社会关系已经在风险投资等资本配置中非正式地发挥着重要但不透明的作用。

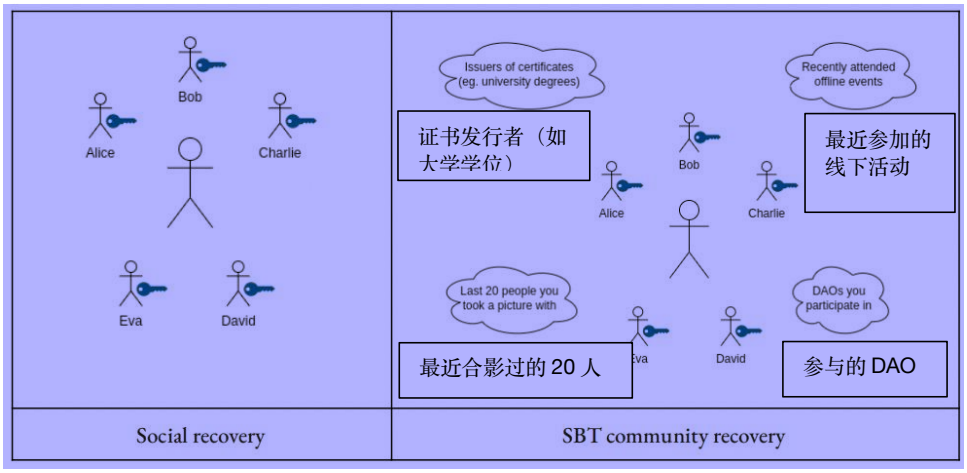
4.3 不要遗失了你的“灵魂”

SBT 的不可转让性——例如一次性颁发的教育证书——提出了一个重要的问题：你如何才能不遗失你的“灵魂”？如今的恢复方法，如多重签名恢复或助记词，在心理负荷、处理的便捷性和安全性方面有不同的权衡。社交恢复 (social recovery) 是一种新兴的选择，它依赖于一个人的信任关系。SBT 允许一个类似的、但更广泛的范式：社区恢复 (community recovery)，其中的“灵魂”是其社交网络的交叉投票。

社交恢复是确保安全性的一个良好起点，但在安全性和可用性方面存在一些缺陷。用户管理一组“监护人”，并赋予他们(基于绝对多数)改变钱包秘钥的权力。这些监护人可以是个人、机构或其他钱包的混合体。问题是用户必须平衡对合理数量的监护人的渴望与监护人来自离散社交圈以避免串通的预防措施。此外，监护人可能会去世，关系恶化或人们只是失去联系，这需要频繁和费力地更新监护人。虽然社交恢复避免了单一故障点，但成功的社交恢复取决于策划和维护与大多数监护人的信任关系。

一个更强大的解决方案是将“灵魂”(账户)的恢复与其所在社区的成员关系联系起来，不是策划监护人，而是利用最大限度地广泛的实时关系来实现安全。回想一下，SBTs 代表不同社区的成员资格，其中一些社区——如雇主、俱乐部、大学或教堂——可能在本质上更多地属于链下社区，而其他社区——如参与协议治理或 DAO——可能更多地属于链上社区。在社区恢复模型中，恢复一个“灵魂”的私钥需要该“灵魂”所在的社区中符合条件的大多数(随机子集)的成员同意。与社交恢复一样，我们假设个人可以获得安全的、比区块链本身更广

泛的链下通信渠道，在那里可以进行“认证”(通过对话和共享秘密)。我们通常可以将这种被 SBT 代币化的关系视为获得这些通信渠道的方式。



社交恢复　　SBT 社区恢复

就像社会恢复一样，我们假设灵魂可以访问安全的链下通信渠道，在这些渠道中，“身份验证”——通过对话、亲自会面或确认共享的秘密——可以发生。与链上机器人或 SBT 本身的计算相比，此类通信渠道将需要更大的带宽（技术上能够承载更丰富的“信息熵”）。事实上，我们可以认为 SBT 从根本上说就是代表参与或访问这种真实的（即高带宽）通信渠道。

完成这项工作的精确细节将需要实验。例如，如何选择监护人以及需要多少监护人的同意是进一步研究的关键安全参数。然而，有了如此丰富的信息库，社区恢复在计算上应该是可能的，随着灵魂加入更多不同的社区并形成更有意义的关系，安全性也会增加。

社区恢复作为一种安全机制，体现了 20 世纪初社会学家、社会网络理论的创始人乔格·西梅尔提出的身份理论，即个性从社会群体的交集中产生，就像社会群体是个体的交集一样。维持和恢复灵魂的密码占有需要灵魂网络的同意。通过在社会性中嵌入安全，一个灵魂总是可以通过社区恢复再生他们的钥匙，这就阻止了灵魂盗窃(或出售):因为卖方需要证明出售恢复关系，任何试图出售灵魂的行为都缺乏可信性

4.4 Souldrop-灵魂投

到目前为止，我们已经解释了灵魂如何能够代表个人并在他们获得反映他们的隶属关系、成员资格和证书的 SBT 时反映他们的独特特征和团结。这种个性化有助于 Souls 建立声誉、确定出处、进入无抵押贷款市场并保护声誉和身份。但反过来也是如此；SBT 还使社区能够在灵魂的独特交汇处召集。到目前为止，web3 主要依靠代币销售或空投来召唤新社区，这几乎没有准确性或精确度。空投，其中代币通过算法免费提供给一组钱包，主要属于现有代币持有者和钱包的某种组合——很容易被女巫攻击，鼓励战略行为和马太效应。SBT 提供了一种根本性的改进，我们称之为“灵魂投”

“Souldrops”是基于灵魂内 SBT 和其他代币计算的空投。例如，想要在特定的第 1 层协议中召集社区的 DAO 可以向持有最近 5 次会议出席 SBT 中的 3 次的开发人员或其他反映出席情况的代币（如 POAP）的开发人员提供帮助。协议还可以在 SBT 组合中以编程方式加权令牌下降。我们可以想象一个非营利组织，其使命是植树造林，将治理代币投放给持有环境行动 SBT、园艺 SBT 和碳封存代币的灵魂——也许向碳封存代币持有者投放更多代币。

Souldrops 还可以引入新的激励措施来鼓励社区参与。丢弃的 SBT 可以设计为在一段时间内受到灵魂约束，但最终随着时间的推移“归属”为可转让的代币。或者反过来可能是正确的。持有一段时间的可转让代币可以解锁 SBT 的权利，从而赋予协议进一步的治理权。SBT 开辟了丰富的可能性空间来试验最大限度地提高社区参与度和其他目标的机制，例如去中心化，我们将在下面进一步讨论。

4.5 Soul 的 DAO

分布式自治组织 (DAO) 是围绕共同目的聚集在一起的虚拟社区，通过公共区块链上的智能合约投票进行协调。虽然 DAO 具有跨距离和不同地协调全球社区的巨大潜力，但它们很容易受到女巫攻击，其中单个用户可以拥有多个钱包来累积投票权——或者在不太复杂的单通证一票式治理中，只需囤积代币即可获得 51% 的投票权，并剥夺其他 49% 的投票权。

DAO 可以通过以下几种方式减轻 SBT 的女巫攻击：

- 计算灵魂的 SBT 星座以区分独特的灵魂和可能的机器人，并拒绝对看似女巫的灵魂有任何投票权。
- 将更多的投票权授予持有更有声望的 SBT（如工作或教育证书、执照或证书）的灵魂。
- 发布专门的“人格证明”SBT，这可以帮助其他 DAO 引导女巫抵抗。
- 检查支持特定投票的灵魂持有的 SBT 之间的相关性，并对高度相关的选民应用较低的投票权重。

后一种相关性检查的想法特别有前途和新颖。由共享相同 SBT 的许多灵魂支持的投票更有可能是女巫攻击，即使不是女巫攻击，这样的投票也更有可能是一群犯同样错误的灵魂 在判断或持有相同偏见的人中，因此应该合理地加权低于具有相同数量支持但来自更多样化的参与者基础的投票。

我们在附录中的二次融资的背景下更详细地探讨了后一种想法，我们在其中引入了一个新的原语，称为“相关分数”。这种相关折扣的概念可以扩展到构建审议对话。例如，容易受到多数控制的 DAO 可以通过 SBT 进行计算，以将最大程度不同的成员聚集在一起进行对话，并确保听到少数派的声音。

DAO 还可以依靠 SBT 来阻止各种形式的战略行为，例如“吸血鬼攻击”。在此类攻击中，DAO（通常具有相关的具有经济价值的 DeFi 协议）通过复制他们的开源代码并随后用代币吸引用户的流动性来搭便车。DAO 可以通过以下方式阻止搭便车者：首先创建一个围绕灵魂投掷的规范（可能授予 SBT），

只针对提供流动性的可能的抗女巫灵魂，然后扣留灵魂投递给在吸血鬼攻击中转移流动性的灵魂。 同样的机制不适用于空投到钱包，因为持有人可以将流动性分散到许多钱包中以混淆他们的流动性轨迹。

DAO 还可以使用 SBT 以编程方式响应其社区的领导和治理。 领导角色可以随着社区组成的变化而动态变化——这反映在 SBT 在成员灵魂中的分布变化中。 根据 DAO 内多个社区的交叉性和覆盖范围，可以将一部分成员提升为潜在的官员角色。 重视社区凝聚力的协议可以使用 SBT 将交叉灵魂保持在中心。或者，DAO 可能会选择比其他更提升某些特征组合的治理，例如邮政编码之间的多样性或特殊爱好 DAO 子集的参与。

4.6 通过多元化衡量去中心化

在分析现实世界的生态系统时，需要衡量生态系统的去中心化程度。 生态系统在多大程度上真正去中心化，去中心化在多大程度上是“假的”，生态系统事实上由一个或一小部分协调实体主导？

两个流行的去中心化指标是 Balaji Srinivasan 提出的 Nakamoto 指数，它衡量需要组合多少不同的实体才能收集 51% 的资源，以及用于衡量反垄断目的的市场集中度的 Herfindahl-Hirschman 指数，通过对市场参与者的市场份额的平方求和计算得出。然而，这些方法留下的关键问题是什么是要衡量的正确资源、如何处理部分协调以及构成“独立实体”的灰色区域。

例如，名义上独立的公司可能有许多共同的大股东，有彼此是朋友的董事，或者受同一政府监管。 在代币协议的背景下，通过查看链上钱包来衡量代币持有量的去中心化是非常不准确的，因为很多人有多个钱包，而一些钱包（例如交易所）代表了很多人。 此外，即使地址可以追溯到独特的个人，这些个人也可能是容易发生意外协调（最好的情况）或故意勾结（最坏的情况）的社会相关群体。 衡量去中心化的更好方法是捕捉社会依赖、弱关联和强大的团结。

矿工和矿池运营商共同组成了 90% 的比特币算力，他们一起坐在一个会议小组中。

SBT 支持一种不同的方法来衡量 DAO、协议或网络中的去中心化（或多元化）水平。

- 第一步，协议可以将代币投票限制为合理抗女巫（或富含 SBT）的灵魂。
- 第二步，协议可以检查不同灵魂持有的 SBT 与灵魂的折扣投票之间的相关性（将它们合并为仅部分分离），如果它们共享大量 SBT。（我们在附录 A 的二次融资背景下更详细地探讨了后一个想法，我们在其中引入了一个新的原语，称为“相关分数”。）
- 第三步，为了缩小并了解整个网络的去中心化，可以测量 Souls 持有的 SBT 在网络堆栈的不同层之间和跨层之间的相关性——测量投票、代币所有权、治理相关的相关性 通信，甚至控制计算资源。

SBT 使我们能够开始衡量当今很难衡量的互操作和分层生态系统的去中心化程度。关于哪些公式最能捕捉我们想要测量的内容并且最不容易受到操纵，仍然存在一个很大的悬而未决的问题。还有很多关于如何检查 SBT 的关系的问题——对某些 SBT 的权重比其他的更高，对嵌套的 SBT 进行折扣，或者还考虑到 Souls 中可转让代币的组成。然而，凭借丰富的 Souls 和 SBT 生态系统，将有大量数据可用于进行这些计算并朝着有意义的去中心化方向发展。

4.7 Plural Property

DAO 通常在虚拟世界和物理世界中拥有或围绕拥有资产进行组织。到目前为止，Web3 的范围很大程度上被限制在一个狭窄的财产类别，其捆绑的权利是完全可转让的:代币、NFTs、艺术品、第一版或罕见的手稿，如美国宪法。但是对可转让性的强调对 web3 是不利的，使得它不能代表和支持今天一些最简单和普遍的财产合同，如公寓租赁。在罗马法律传统中，财产权被定义为使用(“usus”)、消费或破坏(“abusus”)和获利(“fructus”)的捆绑权利。很少有所有这些权利共同归属于同一所有者。例如，公寓租赁赋予出租人有限的使用权(“usus”)，但不赋予出租人破坏公寓(“abusus”)、出售公寓(“fructus”)、甚至转让使用(转租)的不受约束的权利。不动产（土地）的权利通常受到一系列对私人使用的限制、授予公共访问权、对销售权的限制，甚至是征用权的购买权。他们通常还受到抵押贷款的拖累，这些抵押贷款将一些金融价值转移给了贷方。

财产创新的未来不太可能建立在迄今为止想象中的完全可转让的私有财产 web3 之上。相反，创新将取决于分解财产权以匹配现有财产制度特征的能力，并编写更丰富的细节。公司和其他组织形式的演变正是为了以更具创造性的方式重新配置产权——例如，授予员工使用专有设施（“usus”）的权限，但保留管理人员更改或损坏资产的权利（“abusus”），同时支付 股东最大的经济利益（“结果”）。SBT 可以灵活地代表和扩大物理和虚拟资产的细微产权，同时鼓励新的实验。这里只是一些用例：

- 允许访问私人或公共控制的资源（例如，房屋、汽车、博物馆、公园和虚拟等价物）。可转让的 NFT 未能很好地捕捉到这个用例，因为访问权限通

常是有条件的且不可转让的：如果我相信你会进入我的后院并将其用作娱乐空间，这并不意味着我相信你会将该许可转授给 其他人。

- 在数据合作社中，SBTs 向研究人员授予数据访问权，同时实例化成员授予访问权的权利(可能通过二次投票)，并为研究产生的发现和知识产权的经济权利讨价还价。我们将在第四节“ 复数意义解释”中进一步探讨这一点。
- 尝试使用（试验）带有规则的本地货币，让居住在特定地区或属于特定社区的 Souls 更有价值地持有和消费它们。
- 参与实验，其中 SBT 为较少情境化的灵魂（例如移民、青少年）在新颖和更广泛的网络中获得影响力创造了持续的基础。这样的灵魂将从狭窄的 SBT 开始，将他们与家人或当地社区集中在一起。随着他们的从属关系逐渐多样化，他们将获得更广泛的 SBT，以实例化投票权以影响更广泛的网络——本着 Danielle Allen 的多元政治理念的精神——这一过程目前由任意年龄和居住地截止进行调解。
- 市场设计的实验，如 Harberger tax 和 SALSA(在拍卖中出售的自我评估许可证)，资产持有人公布一个自我评估的价格，任何人都可以以这个价格从他们那里购买资产，并且必须定期支付与自我评估价格成比例的税，以保持对资产的控制权。SBTs 可用于创建更细致入微的 salsa 版本——例如，参与权由社区批准，以最大限度地减少社区内外的战略行为。
- 民主机制设计实验，如二次投票。代表社区成员的 SBTs 持有者可以就激励措施和税率等参数进行二次投票。归根结底，“ 市场”和“ 政治”不是独立的设计空间。;sbt 可以是技术栈的主要组成部分，它可以使两类之间的整个空间得到探索。通过二次元资金提供公共产品是另一种交叉。

当然，还有一些反乌托邦场景需要考虑。 移民系统可以通过迁移 SBT 获得许可。 监管捕获可以编入嵌套的社区代币中，其中房主拥有不成比例的投票权并阻碍住房建设。 SBT 可以使红线自动化。 正如我们在下面进一步讨论的那样，应该在当前不透明的自上而下的权限和歧视的背景下考虑这些场景。 SBT 使歧视更加透明，因此可能具有争议性。

4.8 从私人和公共产品到多元网络产品

更普遍地说，SBTs 可以让我们有效地代表和管理在完全私有和完全公开之间的任何范围内的资产和商品。 实际上，几乎所有东西都在范围内：即使是用于个人消费的商品也有积极的溢出效应，例如使消费者能够更好地为他们的家庭或社区做出贡献，甚至全球最容易获得的公共产品（例如气候）也不可避免地更有用 有些人比其他人好（例如塞舌尔诉西伯利亚）。同样，人类的动机很少是完全自私或完全利他的;已有的合作模式有许多，某些社区的合作模式比其他社区的合作模式更多。

然而，今天的机制设计假设原子化、自私的代理没有预先存在的合作，这往往使机制容易受到无害的过度协调，往好了说，是有意合谋，往坏了说，是已经合作的团体之间的勾结。因此，即使是最好的公共融资模式，包括二次融资 (QF)，也无法扩大规模。二次融资通过为少数人的集中行动提供递减的奖励

来鼓励协调，但为多数人的集体行动提供增加的奖励；例如，10 人平均贡献的 1 美元与 99 美元相匹配，总共产生 100 美元，而一个人贡献的 10 美元则没有匹配。 在数学上，这是通过匹配与个人捐款平方根和的平方和成比例的资金来完成的(我们将在附录中进一步阐述)。但是，即使是大型团体（比如大多数中国公民）之间的弱合作（比如向一项事业捐款 1 美元）也会主导系统并吸收所有匹配的资金，因为溢价的二次融资会影响独特贡献者的数量。就目前而言，QF 不会忽视可能淹没 QF 轮次的相关特殊利益之间的协调，而是给予奖励。

但是，与其把已经存在的合作当作一个我们应该“ 掩盖”的错误，不如承认它反映了我们应该利用和弥补的部分合作。毕竟，我们是在鼓励合作。诀窍是让二次机制与预先存在的合作网络一起工作，纠正它们的偏见和过度协调的趋势。SBT 提供了一种自然的方式，使我们能够扭转局面，促进跨差异的合作。正如诺贝尔奖得主埃莉诺•奥斯特罗姆(Elinor Ostrom)所强调的那样，问题不在于协调公共产品本身，而在于帮助由不完全合作但有社会联系的个人组成的社区克服他们的社会差异，在更广泛的网络中进行大规模协调。

如果 SBT 代表了反映灵魂偏向性的社区成员身份，那么支持跨越差异的合作仅仅意味着将合作奖励折扣给类似关联或相关的灵魂——通过他们共享的 SBT 衡量的相似性。假设是，不同附属机构之间的共识更好地表明了更广泛网络中的多种商品，而类似附属机构之间的共识更有可能表明服务于狭隘利益的过度协调（或共谋）商品。

通过揭示 Souls 中的共享成员资格，SBTs 允许我们对现有的合作进行折扣，并以二次比例扩大多个商品，这些商品在新兴网络中广泛地提供利益——由最多样化的成员达成一致——而不是由特殊利益集团无辜地过度协调(或故意串通)的更狭隘的商品。相关折扣“ 最佳”的精确公式取决于模型细节，目前还没有研究，但我们在附录中为进一步的研究提供了实验的第一个途径。

5.0 PLURAL SENSEMAKING

基于用户数据建立的预测模型就是一个例子，在数字世界中越来越引人注目。人工智能 (AI) 和预测市场都试图根据主要从人们那里获得的数据来预测未来事件。但是这两种范式都以不同且几乎相反的方式受到限制。

人工智能中的主导范式避开了激励措施，而是收集（公共或私人监视的）数据，并通过专有的大规模非线性模型将它们合成到预测中——利用 web2 对“ usus”的默认垄断，而没有任何“ 结果”流向数据劳动者。预测市场采取了相反的方法，人们对结果下注，希望获得经济收益，完全依赖金融投机的经济投机(“ 果实”)，而不综合投注者的信念来产生可组合的模型。

与此同时，这两种范式都得出了被称为“ 客观”真理的结论;人工智能模型被描述为“ 通用”或“ 普遍智能”，而预测市场被描述为将市场参与者的所有信念总结为一个数字:均衡价格（平衡价格）。

一个更有效的模式是避开这些极端，而是利用两者的优点，同时弥补它们的弱点，丰富它们的广度。我们深思熟虑地提出，将非线性 AI 模型的复杂性与预测市场的市场激励相结合，将被动的数据劳动者转变为主动的数据创造者。通过这种根植于数据创造者的社会性的来源丰富的信息，我们展示了 DeSoc 如何解锁比任何一种方法都更强大的复数网络(ed)智能。

5.1 预测市场到预测多元化

预测市场的目标是根据愿意下注的人的财富和风险偏好来汇总信念——金钱谈判。但这种“适者生存”并不是聚合信念的理想方式。一名交易员的收益就是另一名交易员的损失，这种零和游戏假设一种普遍的预测能力，这种能力与“聪明人”而不是“傻子”相抗衡。虽然财富可能是某些形式的能力和专业知识的代表，但考虑到其他形式的相对专业知识的预测可能更可靠。在一个特定领域输掉赌注的参与者，可能在另一个领域有更准确的信念。但不幸的是，预测市场会引发那些倾向于赌博的人的信念，这会使赢得赌注的人变得富有，使其他人变得贫穷，并阻碍规避风险的人的普遍参与。

有更好的方法来引出信念。研究表明，虽然预测市场的表现通常优于简单的民意调查，但它们并不优于复杂的团队预测民意调查，因为人们有动力分享和讨论信息。在团队审议模式下，成员可以根据过去的表现和同行评估等因素进行加权，团队参与半结构化的讨论，以汇集无法简单封装在买卖合同中的信息。这种团队审议模型可以通过二次规则进一步改进，以从所有参与者那里获得准确的概率估计（与预测市场相比，预测市场只会引发对当前价格均衡的上下看法）。研究表明，人们有购买动机的合同数量反映了他们的主观概率评估。这样的市场还更加平等地分配参与的收益，奖励准确性而不破坏其余部分，从而使每个人都成为未来轮次的参与者。

SBTs 可以在预测能力和相关专业知识方面解锁一系列丰富的新模型和实验。预测市场只得出一个数字——合约的价格——而二次民意调查则得出每个参与者对事件概率的确切信念。SBT 能够对参与者的教育证书、成员资格和一般社会性的社会背景中的这些信念进行进一步计算，以开发更好的加权（或非线性合成）预测模型，可能会在新的、不可预见的交叉点出现专家预测。这些机制与我们在本文中提倡的机制密切相关。就像被相关分数打折的二次机制可以将协调不佳的自上而下的公共产品转变为强大的、自下而上的多元网络产品一样，它们也可以转变基于零和预测市场的治理系统，以激励参与者隐藏他们的信息（例如，Futarchy）转化为更正和的复数意义构建，可以鼓励新的和更好的信息的揭示和综合。

5.2 人工智能到多元智能

大规模的非线性“神经网络”模型(如 BERT 和 GPT-3)也可以被 SBTs 转换。此类模型会收集大量公共或私人监视的数据源，以生成丰富的模型和预测，例如基于自然语言提示的代码。大多数被监视的数据创建者不知道他们在创建这些模型中所扮演的角色，没有保留任何剩余的权利，并且被视为“附带”而不是关键的参与者。此外，大量收集数据会使模型脱离其社会环境，从而掩盖了它们的偏见和局限性，削弱了我们补偿它们的能力。随着对数据可用性的需求不

断增长，记录数据来源的“数据集数据表”等新举措，以及机器学习的隐私保护方法，这些紧张局势日益凸显。这种方法需要为生成数据的人提供有意义的经济和治理利益，并激励他们合作生产比他们单独构建的模型更强大的模型。

SBT 提供了一种自然的方式来为来源丰富的数据制定经济激励措施，同时赋予数据创建者对其数据的剩余治理权。特别是，SBT 允许根据个人和社区的特征，对个人和社区的数据（和数据质量）进行谨慎和有针对性的激励。同时，模型制作者可以跟踪收集到的数据的特征及其社会背景——正如 SBT 所反映的那样——并找到抵消偏见和弥补限制的贡献者。SBT 还可以为数据创建者设置定制的治理权，允许他们组建合作社来汇集数据并协商使用。数据创建者的这种自下而上的可编程性实现了多元智能的未来，模型制造者可以竞争协商使用相同数据来构建不同的模型。因此，我们摆脱了与人类起源无关的独立的单一“人工智能”范式，将无来源的监视数据集中起来，转而采用合作构建的多元智能的寒武纪大爆发，这些智能植根于社会起源并由灵魂支配。

随着时间的推移，就像 sbt 使一个灵魂个性化一样，它们也使模型个性化——将数据来源、治理和经济权利直接嵌入到模型的代码中。因此，多元智能——就像人类一样——构建了一个嵌入人类社会性的灵魂。或者取决于你如何看待它，人类随着时间的推移而进化，嵌入了多元智能——每个智能都有一个独特的灵魂，与其他灵魂互补和合作。而且，在这方面，我们看到了预测市场和人工智能范式向多元意义的融合，将广泛分布的激励措施和对社会背景的仔细跟踪相结合，创造出多种模型，将两种方法的最佳结合到技术范式中。 比任何一个都强大。

5.3 可编程多重隐私

多元智能提出了有关数据隐私的重要问题。毕竟，要构建如此强大的智能，需要从大型数据集(如健康数据)中汇集个人数据，或捕捉非人际间但共享的数据(如社交图)。“自我主权身份”倡导者倾向于将数据视为私有财产：关于这种交互的数据是我的，因此我应该能够选择何时以及向谁透露它。然而，与实体经济相比，数据经济在简单的私有财产方面的理解甚少。在简单的双向关系中，比如婚外情，披露信息的权利通常是对称的，通常需要双方的许可和同意。正如学者海伦·尼森鲍姆(Helen Nissenbaum)所强调的那样，人们担心的不是“隐私”本身，而是在信息共享中缺乏对上下文的完整性。剑桥分析公（Cambridge Analytica）的丑闻主要是关于人们在未经朋友同意的情况下泄露自己社交图谱的属性和朋友的信息。

与其将隐私视为可转移的财产权，更有希望的方法是**将隐私视为可编程的、松散耦合的权限束**，包括访问权限、修改权限或从信息中获利。在这样的范例下，每个 SBT -例如表示凭据或对数据存储的访问的 SBT -在理想情况下也应该有一个隐含的可编程产权，指定对构成 SBT 的基础信息的访问:持有者、他们之间的协议、共享的属性(例如数据)和对第三方的义务。例如，一些发行人会选择让 SBTs 完全公开。一些 SBT，例如护照或健康记录，在自主权意义上是私人的，拥有 SBT 的灵魂单方面披露的权利。其他的，例如反映数据合作社成

员身份的 SBT，将拥有多重签名或更复杂的社区投票权限，所有或符合条件的大多数 SBT 持有者必须同意披露。

虽然目前存在技术问题（SBT 可以以这种方式编程吗？）和围绕激励兼容性的重要问题（在第 7 节中进一步探讨）——但我们认为可编程多重隐私值得进一步研究，并提供优于替代范式的关键优势。在我们的方法下，SBT 有可能将隐私作为一种可编程的、可组合的权利来映射我们今天拥有的一系列复杂的期望和协议。此外，这种可编程性可以帮助我们重新构想新的配置，因为隐私（作为对信息的访问权限的权利）有无数种方式可以由“ usus”、“ abusus”和“ fructus”组成，以创建一个微妙的访问权利组合。 例如，SBT 可以使用特定的隐私保护技术对数据存储(可能由多个 souls 拥有和管理)上的计算进行授权。一些 sbt 甚至可能以某种方式允许访问数据，以便进行某些计算，但结果无法向第三方证明。一个简单的例子是投票：投票机制需要统计每个灵魂的投票，但投票不应向其他任何人证明，以防止购买选票（贿选）。

通信可能是最规范的共享数据形式。然而，今天的沟通渠道缺乏用户控制和治理（“ usus”和“ abusus”），同时将用户的注意力（“ fructus”）拍卖给出价最高的人——即使是机器人。SBT 有可能管理更健康的“ 注意力经济”形式，使 Souls 能够过滤来自其社交图谱之外的可能机器人的入站垃圾邮件，同时提升来自真实社区和所需交叉点的沟通。听众可以更清楚地知道他们在听谁地演讲，并且能够更好地将功劳分配给激发洞察力的作品。这样的经济体可以优化正和合作和有价值的共同创造，而不是优化最大参与度。这种通信渠道对安全也很重要;如上所述，“ 高带宽”通信通道对于建立社区恢复的安全基础至关重要。

6.0 去中心化社会

Web3 渴望广泛地改变社会，而不仅仅是金融系统。然而，今天的社会结构——家庭、教堂、团队、公司、公民社会、名人、民主——在没有代表人类灵魂的原始人和他们所支持的更广泛关系的虚拟世界（通常称为“ 元界”）中毫无意义。如果 web3 避开持久性身份、信任和合作模式以及可组合的权利和许可，我们将分别看到女巫攻击、勾结和完全可转让的私有财产的有限经济领域——所有这些都趋向于超金融化。

为了避免过度金融化——同时释放指数级增长——我们建议在虚拟和物理现实中增强和连接我们的社交性，赋予灵魂和社区以编码丰富的社会和经济关系的能力。但仅仅建立在信任与合作之上是不够的。 纠正信任网络之间的偏见和过度协调（或勾结）的倾向对于鼓励比以前跨越更大社会距离的更复杂、更多样化的关系至关重要。我们称之为“ 去中心化社会（DeSoc）”：一种共同决定的社会性，灵魂和社区自下而上地聚集在一起，作为彼此的新兴属性，以产生不同规模的多种网络商品。

我们强调多元网络商品是 DeSoc 的一个特征，因为网络是经济增长最强大的引擎，但最容易被私人参与者（例如 web2）和强大的政府（例如中国共产党）

所俘获。最显着的经济增长来自网络回报的增加，其中每增加一个输入单位就会产生更多的输出。简单的物理网络的例子包括道路、电网、城市和其他形式的基础设施，这些基础设施是建立在劳动力和其他资本投入之上的。强大的数字网络的例子包括市场、预测模型和基于数据构建的多元智能。强大的数字网络的例子包括市场、预测模型和基于数据构建的多元智能。在这两种情况下，网络经济学都背离了新古典经济学，新古典经济学教授的是回报递减——每增加一单位的投入产生的产出逐渐减少——以及私人财产产生最高效的结果。在收益递增的情况下，私有财产会产生相反的效果——通过提取租金来抑制网络增长。两个城市之间的道路可以从贸易收益中获得越来越多的回报。但是，如果业主选择收取租金至两个城市之间交易的价值，私人拥有的同一条道路可能会抑制增长。网络的公共所有权也有其自身的风险，容易受到监管或资金不足的影响。

当既不被视为纯粹的公共产品，也不被视为纯粹的私人产品，而是被视为部分和多个共享产品时，回报不断增加的网络效率最高。DeSoc 为分解和重新配置权利提供了社会基础——使用权（“ usus”）、消费或破坏权（“ abusus”）和利润权（“ fructus”）——并在这些权利中启用有效的治理机制， 在检查合谋和俘虏的同时增强信任和合作。在本文中，我们已经探索了几种机制，如基于社区的 SALSA 和二次融资(和投票)，通过相关性得分贴现。第三种部分所有权和复数所有权的方式避免了收取私人租金的“ 卡律布迪斯”(Charybdis)和获取公共监管的“ 锡拉”(Scylla)。在许多方面，今天的 DeFi 是一种收益递减的私有财产范式，被改造成收益递增的网络。 DeFi 建立在无需信任的前提下，本质上仅限于完全可转让的私有财产（例如可转让代币）领域，主要捆绑了“ usus”、“ abusus”和“ fructus”。往好了说，DeFi 有可能通过提取租金来限制网络增长，而在最坏的情况下，可能会迎来由“ 鲸鱼”主导的反乌托邦监视垄断，这些“ 鲸鱼”在逐底竞争中收集和吸食数据——就像 web2 一样。

DeSoc 将 DeFi 对网络价值的控制和推测的竞赛转变为自下而上的协作来建立、参与和管理它们。至少，DeSoc 的社会基础可以使 DeFi 抗女巫（支持社区治理）、抗吸血鬼（内化正外部性以构建开源网络）和抗共谋（保持网络的去中心化）。通过 DeSoc 的结构修正，DeFi 可以支持和扩展多元化的网络，这些网络可以广泛地赋予利益——只要最多样化的成员同意——而不是进一步巩固被狭隘利益所占据的网络。

然而，DeSoc 最大的优点是它的网络可组合性。持续增加的回报和网络增长不仅避免了租金抽取的风险，而且还鼓励了嵌套网络的扩散和交叉。一条道路可以在两个城市之间形成路网。但是，如果两个合作的城市被切断了更广泛的合作，它们的收益将会逐渐减少，要么是因为拥堵（道路和住房），要么是因为疲惫（达到他们可以服务的人群的极限）。只有通过技术创新和扩大(如果更宽松的话)与邻近网络的合作，以获得新的收益来源，价值才能继续呈指数级增长。一些合作将是实体的，逐步扩展跨空间的实体贸易。但更多的连接将是信息化和数字化的。随着时间的推移，我们将看到物理和数字网络之间的新合作矩阵，依赖并扩展它们所建立的社会互连。
通过构建网络和协调，DeSoc 出现在政治和市场的交汇处，增强了二者的社会性。DeSoc 赋予了 JCR Licklider（创造互联网的 ARPANET 的创始人）在“ 星

际计算机网络”中“ 人机共生”的愿景，并在信任的基础上显着增加了社会活力。DeSoc 不是建立在 DeFi 的去信任前提之上，而是对支撑当今实体经济的信任网络进行编码，并使我们能够利用它们来生成多种网络商品，以抵御捕获、提取或支配。借助这种增强的社交性，web3 可以避免短期的超金融化，从而获得跨越社会距离的无限回报。

6.1 灵魂可以去天堂，或地狱

虽然我们选择性地强调了 DeSoc 释放的潜力，我们认为有希望，但重要的是要记住，几乎任何具有这种变革潜力的技术都会有类似的破坏性变革的潜力:火焰燃烧;车轮粉碎;电视洗脑;汽车污染;信用卡陷入债务，等等。在这里，可以用来弥补群体内动态和实现跨差异合作的 SBTs 也可以用来自动划定不受欢迎的社会群体的红线，甚至针对他们进行网络或物理攻击，执行限制性移民政策，或进行掠夺性贷款。在当前的 web3 生态系统中，这些可能性中的许多都不那么突出，因为在当前的基础上，它们并不是有意义的概念。启用 DeSoc 的优点也启用了这些缺点。正如拥有一颗心的缺点是一颗心可能会破碎一样，拥有一颗灵魂的缺点是它可能下地狱，而拥有一个社会的缺点是社会经常被仇恨、偏见、暴力和恐惧所激发。 人性是一场伟大而又常常是悲剧的实验。

当我们思考 DeSoc 可能的反乌托邦时，我们也应该将这些可能性置于其他技术支持的反乌托邦之中。Web2 是用于不透明的权威监控和社会控制的架构。web2 经常依赖自上而下的人为官僚机构来授予身份(“ 驾照”)，而 DeSoc 则依赖水平的(“ 点对点”)社会认证。 DeSoc 使 Souls 能够对自己的关系进行编码并共同创建多元财产，而 web2 则通过可能极化、分裂和误导的不透明算法来中介社会联系或将其货币化。DeSoc 避开了自上而下、不透明的社会信用体系。 DeSoc 避开了自上而下、不透明的社会信用体系。Web2 构成了它们的基础。DeSoc 将灵魂视为代理，而 web2 将灵魂视为对象。

至少在短期内，使用 DeFi（没有任何身份基础）进行社会控制的风险较小。但 DeFi 也有自己的反乌托邦。尽管 DeFi 克服了明显的中心化形式——特定参与者在系统中拥有超大的正式权力——但它没有通过共谋和市场力量克服隐性的中央集权的内置方法。垄断企业并不总是像过去的标准石油那样浮出水面。串通（勾结）甚至可以发生在一个生态系统的更高和更远的级别。今天，随着一批机构资产管理公司（如先锋、贝莱德、道富、富达等）的崛起，我们看到了这一点，它们是所有最大银行、航空公司、汽车公司和其他主要行业的最大股东。由于这样的资产管理公司持有一个行业内所有竞争对手的股份(例如，每一家主要航空公司的股份)，他们的动机是使他们持有的公司看起来像一个竞争行业，但行为却像一个垄断者，最大限度地提高整个行业的利润和以消费者和一般公共费用为代价的加固。

在 DeFi 中，同样的“ 鲸鱼”和风投在堆栈的每一层和堆栈中的竞争对手之间积累了更大的份额，可能在代币治理中投票，或将其委托给同样在网络中相互关联的同一类代表。由于没有任何社会基础来支持“ 希比尔阻力”和“ 相关性折扣”来强制功能去中心化，我们还应该期待看到更多由“ 鲸鱼”资助的垄断，因为垄断者越来越多地成为可用投资资本的最大池。如果没有任何抗女巫的社

会基础和力功能去中心化的相关折扣，我们还应该期待看到更多由鲸鱼资助的垄断企业，因为垄断企业越来越成为最大的可用投资资本池。随着“ 金钱阶层”和用户的分化，我们应该会看到(而且已经看到)越来越严重的激励失调和租金榨取。如果处理私人数据的 DeFi 应用程序出现，我们很可能会看到类似的动态，例如应用程序鼓励多个“ 拥有”实际人际数据(例如，他们的社交图谱)的人之间的竞价战争，以构建与人类竞争的单一私人 AI，避免未来竞争增强人类的多元 AI。

因此，DeSoc 不需要是完美的，以通过可接受的非反乌托邦测试;要成为一个值得探索的范例，它只需要比可用的替代方案更好。尽管 DeSoc 有可能需要防范的反乌托邦情景，但 web2 和现有的 DeFi 正陷入不可避免的反乌托邦模式，将权力集中在决定社会结果或拥有大部分财富的精英手中。Web2 的方向是决定性的权威主义，加速了自上而下的监视和行为操纵的能力。如今的 DeFi 的方向名义上是无政府资本主义，但已经陷入网络效应和垄断压力，这可能会使其中期路径以同样的方式变成威权主义。

相比之下，DeSoc 是随机的社会多元主义——一个由个人和社区组成的网络，作为彼此的新兴属性，共同决定自己的未来。从 Web2 来看，DeSoc 的发展可以类比为几个世纪君主制中大众参与政府的兴起。参与式政府并非必然带来民主;它还导致了共产主义和法西斯主义的兴起。同样，SBT 不会使数字基础设施本质上民主，而是民主兼容，具体取决于灵魂和社区共同决定的内容。开放这种可能性空间是对 web2 的威权主义和 DeFi 的无政府资本主义的显著改进。

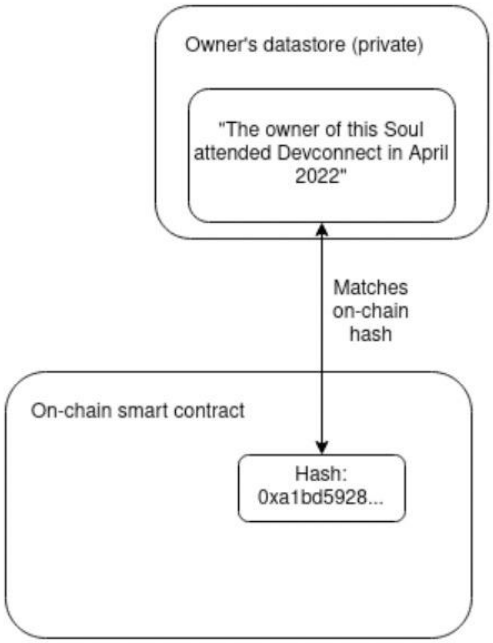
7. 执行挑战

隐私对 DeSoc 来说是一个关键挑战。一方面，太多的公共 SBT 可能会泄露太多关于一个灵魂的信息，使他们容易受到社会控制。另一方面，过多的纯私人 SBT 也可能导致私人沟通渠道避开治理和社会协调的相关性折扣——这提出了重要的激励相容性问题。与隐私问题密切相关的是欺骗问题:灵魂可能会歪曲他们的社会团结，同时通过私人或次要渠道进行协调。我们不能渴望知道所有的可能性和答案，而是在这里探索挑战的本质，并为未来的研究勾勒出一些有希望的路径。

7.1 私人灵魂

基于区块链的系统默认是公开的。记录在链上的任何关系不仅对参与者，而且对全世界的任何人都是立即可见的。使用多个假名可以保留一些隐私:家庭灵魂、医疗灵魂、职业灵魂、政治灵魂，每个人都携带不同的 SBT。但是如果天真（质朴）地完成，很容易将这些灵魂相互关联起来。这种缺乏隐私的后果是严重的。事实上，如果没有采取明确的措施来保护隐私，简单地将所有 SBT 上链的“ 幼稚”愿景很可能会使许多应用程序公开太多信息。

为了应对过度公开，有许多具有不同技术复杂性和功能级别的解决方案。最简单的方法是 SBT 可以在链下存储数据，只留下链上数据的哈希值。

	
链上数据（完全公开）	链下数据，链上哈希链接（拥有者选择何时显示）

如何存储链下数据由个人选择；可能的解决方案包括(i)他们自己的设备，(ii)他们信任的云服务，或(iii)去中心化的网络，如星际文件系统(IPFS)。将数据存储在链下让我们继续拥有有权写入 SBT 数据的智能合约，但同时拥有读取该数据的单独权限。Bob 只有在愿意的时候才可以选择显示他的任何 sbt(或其允许的数据存储)的内容。这已经让我们走得很远，并且具有提高技术可扩展性的进一步好处，因为大多数数据只需要由极少数各方处理。但要完全实现多元隐私等属性，以及更细粒度的披露形式，我们还需要更进一步。幸运的是，许多加密技术让我们能够做到这一点。

一套强大的构建模块能够以新的方式部分揭示数据，它是密码学的一个分支，称为“零知识证明”。虽然如今零知识证明最常用于保护隐私的资产转移，但它们也可以让人们证明任意陈述，而无需透露陈述本身之外的任何更多信息。例如，在一个政府文件和其他证明都可以用密码证明的世界里，有人可以证明这样的声明:“我是加拿大公民，18 岁以上，拥有经济学大学学位，有 5 万多 Twitter 粉丝，但还没有在这个系统中申请账户。”

零知识证明可以通过 sbt 计算来证明一个灵魂的特征(例如，它有某些会员)。通过引入多方计算技术（例如乱码电路）可以进一步扩展该技术，这可以使此类测试具有双重私密性：证明者不会向验证者透露他们是谁，而验证者不会向证明者透露他们的验证机制。相反，双方一起进行计算，只学习输出结果。

另一个强大的技术是指定验证者证明。一般来说，“数据”是不可靠的:如果我向你发送一部电影，我无法从技术上阻止你记录下来并将其发送给第三方。数字版权管理 (DRM) 之类的变通办法充其量只能起到有限的作用，而且通常会

给用户带来巨大的成本。然而，证明并不会以同样的方式狡猾。如果 Amma 想向 Bob 证明她的 sbt 的某些属性 X，她可以对以下语句进行零知识证明:“我持有满足属性 X 的 sbt，或者我有 Bob 的灵魂的访问密钥。”Bob 会觉得这个陈述很有说服力：他知道他没有做出证明，因此 Amma 实际上必须有满足性质 X 的 SBT。但如果 Bob 将证明传递给 Cuifen，Cuifen 不会被说服：据他所知，Bob 可以用他自己的密钥制作证明。这可以通过可验证的延迟函数 (VDF) 变得更加强大：Amma 可以制作并展示目前只能使用所需的 SBT 制作的证明，但其他任何人都可以在五分钟后制作。这意味着尽管不可能对原始数据本身（可能只是简单地复制和粘贴）进行相同类型的选择性权限，但可以表示对有关数据的可信证明的复杂访问权限。尽管如此，这可能会让我们走得很远。正如区块链在交易中提供可追溯性以防止某人右键单击复制并粘贴有价值的 NFT（以及女巫攻击原始所有者）一样，SBT 可以提供社会传播的可追溯性，这至少可以降低复制的价值，并粘贴来源未经证实的数据。

这些链下数据和零知识技术与负面声誉兼容——即使持有者不希望它们可见，SBT 也会变得可见。负面声誉的重要示例包括信用记录、未付贷款数据、负面评论和业务合作伙伴的投诉，以及证明与协调相关的社会关系的 SBT。与相同密码学相结合的区块链可以提供一个潜在的解决方案：灵魂可能会被智能合约逻辑强制将负 SBT 合并到数据结构中，例如存储在链外的 Merkle 树，并且任何零知识证明或乱码电路计算都需要他们引入该信息，因为否则会出现验证者可以识别的所提供数据中的可见“漏洞”。Unirep 协议就是如何实现这一点的例子。

这些示例的重点并不是说明如何使用加密技术来解决 sbt 的所有隐私和数据权限问题。更确切地说这是为了勾勒出几个例子来展示这些技术的力量。一个重要的未来研究方向是确定不同类型数据许可的确切限制以及最适合实现所需许可级别的技术的特定组合。另一个问题是需要什么样的多元财产制度来管理数据，以及如何正确地拆分访问（“usus”）、编辑（“abusus”）和现金流（“fructus”）权利。

7.2 灵魂欺骗

如果 SBT 是多种财产、网络商品和智能在其上协调的社会基础，人们可能会担心灵魂会试图欺骗或欺骗他们进入社区以获得我们想象 SBT 允许的治理或财产权。例如，如果许多应用程序依赖于代表会议出席的 SBT，则不道德的会议可能会提供此类 SBT 以换取贿赂。只要贿赂足够多的人，人类(和机器人)就可以生成一个虚假的社交图，让账户看起来像一个真正的人类灵魂，被(虚假)SBTs 大量区分开来。就像 DAO 可以被贿赂一样，Souls 和他们使用的链上投票机制也可以。相反，如果使用 SBT 来降低协调性，Souls 可能会避免 SBT 以最大化其影响力。为什么我们要相信灵魂所拥有的 SBTs 准确地反映了他们真实的社会承诺，而不是他们选择如何玩这个游戏?

一种观点认为，不同的作弊动机可以“平衡”。灵魂们可能会在适当的规模上对对他们重要的网络进行分类和自我识别，就像哈伯格税(Harberger tax)如何平衡高估和低估资产的动机，以获得接近准确的市场估值一样。Souls 将希望持

有更多的 SBT 以在他们的社区中获得影响力，但另一方面，他们会避开他们不太关心的社区中的 SBT，从而在相关性指标上得分较低，并增加他们在更广泛网络治理中的影响力。

但如果认为这两种动机——获得访问权和最大化影响力——总是势均力平，甚至接近于势均力平，就像魔法一样，那就太天真了。可能有许多社区使用 SBT 以外的系统来控制访问和治理。或者，社区可能——与我们关于公开性的主要假设相反——发放私人 sbt 来反映治理权利，但诱导社区成员在更广泛的决策中对这些 sbt 保密。

我们不应该低估“游戏”的问题。这是一个具有重大意义的问题，解决这一问题是未来研究的重点之一。确实，这是开源许多为人类用户优先或过滤的现有算法非常具有挑战性的原因。为了减轻和阻止 SBT 游戏，我们建议了几个规范和加密方向：

1. SBT 的生态系统可以从“密集”的社区渠道中启动，在这些渠道中，SBT 通过强大的社会纽带和重复互动表明真正的链下社区成员身份。这将使社区更容易过滤和撤销模仿者和机器人的 SBT。如此密集的渠道——我们经常在教堂、工作场所、学校、聚会小组和公民社会的组织中找到——将为在更“薄”的社交渠道中的警察游戏（例如，通过机器人、贿赂、冒充）提供更抗女巫攻击的社交基础。
2. 嵌套社区可能需要 SBT 对“正下方”的潜在共谋向量施加上下文。例如，如果一个州正在举行一轮融资或投票，该州可能会要求每个参与的公民也持有一个确定的县和市的 SBT。
3. SBT 生态系统的开放性和密码学可证明性本身可用于主动检测合谋模式并惩罚不真实的行为——也许会降低共谋之魂的投票权，或者迫使之魂接受代表负面证明的 SBT。例如，如果一个灵魂证明了另一个灵魂的人性，而这个灵魂被证明是一个机器人，这个案件可以升级并公开验证，导致那个灵魂有大量的负面证明。这在一定程度上已经发生在 GitCoin QF 生态系统中，其中使用了一系列信号来检测“合谋团体”。
4. ZK 技术（例如 MACI）可以通过加密方式防止灵魂做出的某些证明是可证明的。这将使出售某些类型的证明的尝试变得不可信，因为行贿者将无法判断受贿者是否遵守了他们的交易。已经有大量关于使用这种技术进行投票的研究，但最终任何非金融化的社会机制都可能最终受益于类似的想法。
5. 我们可以鼓励举报人，以此来使大规模的串通变得不稳定。我们不是检测和惩罚不正确或滥用行为，而是检测和惩罚共谋的滥用模式。由于存在虚假贿赂的可能性，这种技术有过度使用的风险，但它仍然是工具包的一部分。
6. 我们可以使用来自同行预测理论的机制，鼓励在所有情况下如实报告，除非勾结极其严重。与会议证明参与者的出席不同，参与者可以证明彼此的出席，因此，需要贿赂以证明虚假声明的参与者数量变得非常大。奖励不一定是金钱上的，但可以是 SBT，这使得奖励对真正的社区成员比对攻击者更有用。
7. 如果一群灵魂有共同的兴趣，我们可以使用专注于相关性的相关性分数。例如，有界成对二次融资中使用的相关评分技术使用二次融资捐赠本身来确定两个参与者的相关性，从而确定他们的交集的折扣程度。如果两个参与者有许

多共同利益，他们向 QF 机制表达这一事实的动机肯定会随着相关性折扣而减少，但它永远不会变成零或负数。

8.0 比较与局限性

虽然提出的身份框架的范围几乎是无限的，但在 web3 空间中有四个特别突出和相邻的范式被广泛讨论，值得比较：占主导地位的“传统”身份生态系统、假名经济、人格证明和可验证的凭证。每一种范式都强调了我们所倡导的社会认同范式对未来发展的重要贡献和挑战，我们将这些局限性作为探索未来方向的跳板。考虑到所有这些，我们还解释了为什么我们相信我们的灵魂和灵魂令牌的社会身份原语是隐私制度的一条更有希望的前进道路。

8.1 遗产

传统身份系统依赖于由第三方（政府、大学、雇主等）发行和调解的文件或身份证。通过致电第三方进行确认来确定出处。虽然遗产系统有一组有趣的属性，我们应该更深入地理解，但这样的系统非常低效，不适合用于快速、高效协调的可组合性或计算。此外，这些系统缺乏社交环境，使得 Souls 依赖于一个集中的第三方来确认社区成员，而不是嵌入社区。例如，大多数政府颁发的身份证明最终都可以追溯到医生和家庭成员授权签发的出生证明，他们是真相的最终来源，并遗漏了许多同样有意义的社会联系，这些联系在一起提供了更强大的验证。事实上，当权力集中的中心寻求强有力的身份证明(例如，从主要政府获得安全许可)时，他们很少依赖这些文件，而是转向社交网络上的采访。因此，这种遗留身份系统往往会将权力集中在发行人身上，集中在那些能够承担尽职调查以获得更有力核查的人身上，而这些人反过来又会变成僵化和不可靠的官僚机构。DeSoc 的一个关键设计目标是确保能够满足和超过政府 ID 的安全要求，允许横向网络通过一系列社交基础为所有用户提供更高的安全性。

8.2 匿名经济

巴拉吉·斯里尼瓦桑(Balaji Srinivasan)创造并推广了“匿名经济”一词，他提出了一个将名誉系统与零知识证明机制结合起来以保护隐私的社会愿景。他的早期版本强调使用化名来避免歧视和逃避社会暴民的“取消文化”，这些暴民试图损害一个人的声誉和打破他们的社会关系。它设想人们在他们的钱包中积累可转移的零知识 (ZK) 证明，并通过将证明子集转移到新钱包或将证明拆分到多个钱包中来逃避声誉攻击，这可能是没有可追溯性的。在挑选要移植的证明时，一个人选择新帐户中所需的假名级别，权衡更多匿名性（移植较少的证明）或更多分布到他们的社交网络（移植更多的证明）之间的权衡。

典型的匿名经济提案和 DeSoc 之间的实际区别在于，我们不再强调身份隔离是保护参与者免受虐待和取消文化的主要方式。某种程度的分离（例如，家庭、工作、政治等之间的不同灵魂）可能是健康的，但一般来说，依靠建立新身份的能力作为抵御攻击的主要拐杖存在很大的缺点。它使贷款和出处的声誉

赌注变得更加困难，并且它与试图纠正相关性或女巫攻击攻击的治理机制的组合很差。

DeSoc 将允许其他方法，例如将攻击者置于情境中，而不是通过让他们以一种新的(如果被削弱)身份重新出现来保护受害者。“取消”经常出现，因为当一个人或机器人与受害者几乎没有社交联系或背景时，声明和行动是脱离上下文并且病毒信号通过非上下文网络传播的。与 SBT 提供出处以防止深度伪造的方式相同，SBT 的地图在社交上绘制了“热门作品”的起源。“热门作品”本质上是在受害者社区之外产生的人工制品（如共享的 SBT 成员资格所反映），或者缺乏来自受害者社区的 SBT 证明——这应该会让人怀疑该作品的真实性。SBT 还使受害者能够发起防御性反应，以抵消从他们的信任网络中策划和传播的打击（此处以共同持有 SBT 的模式为代表）。通过保持社交环境，人们可以保持信任，即使他们面临被取消的威胁，并追究攻击者的责任。改善来源，就改善了真理的社会基础。

8.3 人格证明

人格证明协议 (PoP) 旨在提供个人唯一性的代币，以防止女巫攻击并允许非金融化应用程序。为此，他们依赖于社交图谱的全局分析、生物识别、同步的全球关键方或它们的某种组合等方法。然而，由于 PoP 协议寻求代表个人身份——专注于实现全球唯一性——而不是映射关系和团结的社会身份，所以 PoP 协议仅限于对所有人一视同仁的应用程序。我们感兴趣的大多数应用程序（例如质押声誉）都是相关的，并且超越了成为一个独特的人，成为一个与众不同的人。

此外，PoP 协议也不能免受女巫攻击。在几乎所有近期可预见的应用中，PoP 系统都有效地对 Sybil 攻击开放，只是成本略高。除非地球上的大多数人都注册了 PoP 服务并且正在参与特定的验证活动，否则攻击者总是可以招募尚未参与的不感兴趣的人充当 Sybils。虽然这样的雇佣兵并不完全是机器人，但区别只是表面的，可能只是增加了一点点费用。

许多 PoP 协议旨在为普遍基本收入或全球民主建立基础。虽然我们没有相同的野心，但这样的协议已经促使我们考虑如何逐步构建协调多元网络商品。与 PoP 的二元、个人主义和全球性质相比，我们的方法旨在构建一个丰富的、上下文相关的、分层的基础，自下而上地建立声誉、财产和治理，允许参与各种社区和网络，无论大小。

8.4 可验证凭证

可验证凭据(VCs)是一个 W3C 标准，凭据(或认证)可以由持有人自行决定 zk 共享。VC 强调了我们基线隐私范式的主要局限性，并激发了我们对上述隐私扩展的讨论。除非 SBTs 有隐私扩展来缩小公开范围，否则 VC 和 STs 可以被视为自然的补充: 特别是，SBT 最初是公开的，因此不适用于政府颁发的身份证明等敏感信息，而 VC 的实施一直在努力解决可以通过社区恢复来解决的恢复范式。在短期内，这两种方法结合起来可能比单独任何一种都更有效（强

大）。但是 VC 也有一个关键的限制：至少在它们的标准化形式上，VC 不支持我们列举的大多数应用程序，因为它们具有单方面的隐私性。

单方面的 zk 共享与我们的用例不兼容，也不反映我们关于隐私的规范。我们的大多数应用都依赖于一定程度的宣传。但是在 zk-sharing 下，Souls 无法知道另一个 Soul 拥有 SBT，除非它被共享给他们——这使得声誉赌注、可信承诺、抗女巫治理和简单的租赁合同（例如公寓租赁）无法摆脱其他承诺和产权负担不一定是可见的。更深入地说，我们怀疑单方面的可共享性通常是正确的隐私范式。多方关系中的一方很少有未经另一方同意而单方面披露关系的权利。正如单方面可转让的私有财产不是丰富的财产制度一样，简单的单方面可共享性也不是非常丰富的隐私制度。如果两方共同拥有一项资产并选择通过 VC 代表他们的关系，则这种凭证不允许相互同意和相互许可。这个问题涉及到更复杂的复数财产和复杂的组织形式和权限的情况，这是 DeSoc 的一个特点。

9.0 灵魂诞生

从当前的 web3 生态系统到由 SBT 介导的增强社交的路径面临着典型的冷启动挑战。一方面，SBT 不可转让。另一方面，今天的钱包组合可能不是 SBT 的最终归宿，因为它们缺乏社区恢复机制。但为了让社区恢复钱包发挥作用，它们需要在分散的社区中提供各种各样的 SBTs 来确保安全。首先是什么：SBT 还是社区恢复？谁是社区早期应用者？不同链上的 sbt 如何互操作?我们不能期望知道所有的可能性和答案，而是为读者勾勒出一些有希望的路径，以便在当前的 web3 甚至 web2 架构中进一步探索。

9.1 典型 SBTs

尽管 SBT 的标志是不可转让性，但 SBT 可能还具有另一个可能被证明在引导中更有用的属性：可撤销性。在成长为不可转让性之前，sbt 有可能首先孕育为可撤销、可转让的代币。如果发行者可以销毁令牌并将其重新发行到新钱包，则令牌是可撤销的。例如，当密钥丢失或受损，而发行者有兴趣确保代币不被金融化并出售给一方时——换句话说，当代币标志着真正的社区成员身份时，销毁和重新发行是有意义的。具有重复链下互动的雇主、教堂、聚会团体、俱乐部很容易销毁和重新发行代币，因为它们与人有关系，并且可以通过电话、视频会议或 简单的会面。 单一的互动，如出席音乐会或会议不太适合因为社区纽带较弱。

可撤销、可转让的代币是一种原型 SBT——在灵魂出生之前提供支持性的胎盘功能。这些代币为钱包争取时间来孕育安全的社区恢复机制，以及让人们充分积累最终可以被烧毁并重新发行为不可转让的 SBT 的原始 SBT。在这条路径下，问题不是“ 首先发生什么：SBT 还是社区恢复？”相反，SBT 和社区恢复同时实例化，产生了一个灵魂。

9.2 社区恢复钱包

尽管今天的钱包缺乏社区恢复能力，但它们在成为 SBT 的家——或者可能是妊娠子宫——方面都有相对的优势和劣势。人格证明 (PoP) 协议的优势在于已经在尝试社会争议解决机制，这是社区恢复的基础。此外，许多 DAO 使用 PoP 来促进治理，使其自然成为 SBT 的第一发行者。然而，尽管 PoP 自然领先，但 PoP 协议尚未赢得广泛信任来存放有价值的代币资产，而托管钱包则有。

托管钱包——尽管存在中心化缺陷——可能因此为不太成熟的零售用户提供了一个自然的入口。此类托管钱包还可以为零售社区构建工具，以发行可撤销的代币，这些代币随后会转换（或销毁和重新发行）为 SBT，甚至可以为更多“ 企业”发行人提供工具——其中许多人正在寻找在 web3 中建立忠诚客户群的方法，但缺乏监管方面的专业知识。一旦社区恢复机制正式确定并经过实战考验，这些托管钱包可以分散到社区恢复中，而托管人则继续在 DeSoc 中提供其他有价值的服务（如社区管理、SBT 发行等）。

对于更成熟的 web3 用户，去中心化的非托管钱包（或像 Argent 和 Loopring 这样的非托管社交恢复钱包）是引导社区恢复机制的自然起点。非托管钱包具有原生 web3 开源的优势，并且可以灵活地预先宣布和逐步试验机制，让一部分自愿的、成熟的用户对激励和混合机制（例如多重签名）进行战斗测试。所有这些方法（PoP、托管和非托管）在试验和入职具有不同复杂程度和风险承受能力的用户方面发挥着重要作用。

9.3 典型（原型）灵魂

规范也可以引导灵魂存在。当我们重新考虑代币和钱包时，我们还可以重新定义我们对某些类别的 NFT 和旨在表明会员资格的代币的看法。特别是，我们可以引入不转让由知名机构颁发的反映出席会议、工作经验或教育证书的 NFT 和 POAP 的规范。这种会员代币的转移——如果进行价值交易——可能会降低钱包的声誉，并可能阻止发行人进一步向该钱包发行会员或 POAP 代币。在非托管生态系统中，相当多的用户已经获得了显著的财务声誉，并在他们的钱包中持有股份，这可以作为他们不滥用不可转移预期的有效抵押品。

虽然所有这些途径都有各自的挑战，但我们希望各种方法能够通过一小部分步骤增加在中期收敛到我们的准平衡状态的机会。

10. 结论

尽管我们一直在想象 DeSoc 可以实现什么，但在许多方面，上述只是第一步。通往 DeSoc 的道路不止一条，包括许多基于非区块链的框架，例如 Spritely、ACDC 和 Backchannel，它们依赖于与本地机器而不是全局分类帐相关的数据存储。这些框架最终可能会在社交距离上提供更大的信任，因为它们可以利用信任关系的传递性——比如受信任的介绍——而不是依赖于知名的高地位机构（如大学或 DAO）发布的 SBT。此外，我们上面描述的应用程序只是 DeSoc 能够实现的一个开端，并不涉及虚拟世界:它们的物理、社会以及它们与物理世界的复杂交集。所有这些都表明，即使我们上面描绘的远大抱负，也只是 DeSoc 最终可能成为的一个开始。

然而，在这条道路上，仍然存在许多挑战和悬而未决的问题。上述草图需要大量的红色团队，其中许多草图更多的是暗示性的，而不是完全规定性的。DAO 如何在仔细比较 SBT 中的灵魂模式和相关性以执行 Sybil 保护和去中心化的同时保持其状态宣传？面对各种相关贴现方案，获得 SBT 的激励兼容性如何？隐私与相关折扣和其他 DeSoc 机制设计有多少冲突？我们如何以一种社会性的但又适当的私人（语境整合）方式来衡量不平等？遗产（继承）在社区恢复框架中应该如何工作？是否可以在协议中划出或甚至嵌入红线，以避免反乌托邦的场景?还是我们应该首先竞相构建最佳场景？这些问题只是我们期望的跨年研究议程的开始，该议程将与 DeSoc 生态系统共同发展。

然而，DeSoc 提供的潜力似乎不仅值得为应对这些棘手的挑战付出代价，而且可能是确保我们生存所必需的。阿尔伯特·爱因斯坦(Albert Einstein)在 1932 年的裁军会议上说，“人类的组织力量”未能跟上“他的技术进步”，这让“一个 3 岁的孩子手里拿着一把剃刀”。在一个他的观察似乎比以往任何时候都更有先见之明的世界里，学习如何编程编码社会性的未来——而不是写在信任之上——似乎是人类在这个星球上生存下去的必修课。