V神大作全文精译——去中心化社会：寻找Web3的灵魂

2022-05-15 14:06

去中心化社会：
寻找Web3的灵魂[1]

E.格伦·韦尔[2]，普迦·奥尔哈弗[3]，维塔利克·布特林[4]

2022年5月

“道者，万物之奥。
善人之宝，不善人之所保。”

——《道德经》六十二章

摘要

今天的 Web3多用来表述可转让的金融化资产，而非用于对社会信任关系编码。而诸多核心经济活动，如无抵押贷款和建设个人品牌，都是建立在长期而不可转让的关系之上的。在本文中，我们描述了用以表征“灵魂”的承诺、资历证明和归属关系的不可转让的“合灵”币（“soulbound” tokens, SBT），是如何能将实体经济的信任网络予以编码，并得以建立溯源和声誉的。更

重要的是，SBT 可赋能于其他雄心勃勃的应用，如社区钱包恢复、抗女巫攻击的治理、去中心化机制以及具有可分解可共享权利的新型交易市场。我们将这个更丰饶、多元化的生态系统称为“去中心化社会”（DeSoc）—— 一种共决共定的社交关系，灵魂们和社区自下而上地聚集在一起，以此为彼此的新兴特质，在不同尺度范围内共同创造多元网络物品和智能。这种社交关系的关键是可分解的产权和强化的治理机制，例如按关联度分数进行降权调整的二次方融资，在保护网络不被攻击、抽血和操纵的同时，奖励信任和合作。借助这种强化的社交关系，Web3 可以避开时下过度的金融化，转而支持更具变革性、多元化的未来，超越社交区隔，创造更多回报。

§1 简介

Web3在不到十年的时间里打造了一个具有前所未有灵活性和创新性的平行金融系统，震惊了全世界。密码学和经济的原生组件，如公钥密码学、智能合约、工作量证明和权益证明，已催生出一个复杂而开放的金融交易生态系统。

然而，金融所交易的经济价值是由人类及其关系产生的。由于 Web3 缺乏代表这种社交身份的原生组件，它基本依赖于其原本想超越的中心化Web2架构，复制了后者的局限性。

依赖的例子包括：

1. 大多数NFT艺术家依靠OpenSea和Twitter等中心化平台来表达稀有度和原始**出处**。

2. 想做得比简单的代币投票更好的DAO，常依靠Web2基础设施，如社交媒体上的个人资料，来**对抗女巫攻击**。

3. 许多 Web3 参与者依靠由中心化实体管理的托管钱包，如 Coinbase 或币安。去中心化的**密钥管理系统**对用户不友好，非常专业的人才懂如何使用。

此外，缺乏原生的 Web3 身份认别，使得今天的 DeFi 生态系统无法支持实体经济中那些常见的活动，如**抵押物不足的借贷**或像**公寓租约**那么简单的合同。在本文中我们将阐述，合灵代币代表社交身份识别方面的微小跬步，也能够解决这些问题，并使生态系统得以重建以原生Web3背景下的人际关系为基础的市场。

更值得憧憬的是，我们将重点阐述，具备丰富社交*可组合性*的原生Web3 社交身份，如何在Web3已广泛长期存在的诸多问题上取得巨大进步，包括财富集中和治理组织易受金融攻击的脆弱性等，同时刺激政治、经济和社会应用创新活动的寒武大爆发。我们将这些应用场景及其所支撑的更加丰饶的多元生态系统称为**“去中心化社会”（DeSoc）**。

§2 概览

我们首先阐释 DeSoc 的原生组件，主要是持有代表承诺、资历证明和归属关系的**不可转让（最初是公开的）“合灵”币 (SBT)** 的账户（或钱包）。这种代币就像放大版的简历，由验证这些社会关系的其他钱包发行。

然后，我们将阐述这些原生组件所支撑的在各社会单元中日益兴盛的一系列应用程序，包括：

- 确定来历
- 以声誉为背书，启动抵押不足的贷款市场
- 实现去中心化的密钥管理
- 阻止和抵消协同的策略性行为
- 评估去中心化
- 创建具有可分解、可共享的权利和许可的新型市场

讲述的终点是DeSoc 的愿景——一种共决共定的社交关系，灵魂们和社区自下而上地聚集在一起，以此为彼此的新兴特质，在不同尺度范围内共同创造多元网络物品，包括多元智能。

最后，我们将回应潜在的一些担忧和反对意见，并与 Web3 领域已知的其他身份识别方式进行比较，不得不承认我们所看到的只是第一步，但却是可编程隐私和通信方面的进步。然后，我们将思考实现我们眼中愿景的技术途径。在此之上，我们更多地从哲学的角度，期待 DeSoc 能将 Web3 拉回到更深远、更合理和更具变革力的轨道。

§3 灵魂

我们的核心原生组件是，持有***公开可见***、***不可转让***（**但可*由发行者撤销的***）的代币的账户或钱包[5]。我们将这些账户称之为

“灵魂”，将账户持有的代币称之为“**合灵币**”（**SBT**）。尽管我们对隐私有着浓厚兴趣，我们一开始假设账户是公开的，是因为这在技术上更易实现概念验证，即便人们愿公开的代币持有信息会相当有限。在本文的后面，针对更加丰富的应用场景，我们引入了“可编程隐私”的概念。

想象一下有这么个世界，多数成员都存有SBT，且有一系列的归属关系、成员身份和资历证明与这些币相对应。比如，某人可能一个灵魂，存有代表学历证书、工作履历，或其著作或艺术作品的哈希值。在它最简单的形式中，这些 SBT 可以“自我认证”，类似于我们在简历中分享有关自己的信息。但是，当一个灵魂持有的 SBT 可以由作为对手方的其他灵魂发行或验证时，该机制的威力就会显现出来。这些对手方灵魂可以是个人、公司或机构。例如，以太坊基金会可以是一个灵魂，它向参加开发者大会的灵魂发行 SBT。一所大学可能以一个灵魂，向毕业生发行 SBT。体育馆可以是一个灵魂，向道奇队的长期球迷发行SBT。

请注意，灵魂无需与法定名称关联，也不需要*协议*级别的手段来确保“每个人只有一个灵魂”。[6]灵魂可以是一个不变的假名，拥有一系列无法轻易连接的 SBT。我们也不会假定灵魂在真人之间不可转让。我们将说明，这些特性如何在需要时自然而然地从产品设计中显现出来。

§4 通往 DESOC 的步骤

4.1 艺术与灵魂

灵魂是艺术家将自己的声誉寄托于其作品的一种自然形式。当发行可交易的NFT时，艺术家可以从他们的灵魂中发行其 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，从而也确认 NFT 的真实性。艺术家可以更进一步，发行存储在他们灵魂中的带链接的SBT，可以用来验证 NFT 的“藏品”成员身份，以及艺术家设置的稀有度限制的凭证。因此，灵魂们创建了一种可验真的链上方式，在物品的来历和稀有度之上寄托和累积声誉。

应用程序不局限于艺术方面，还可延伸到服务、租赁以及任何建立在稀缺性、声誉或真实性之上的市场活动。关于后者的一个例子是被主张的事实记录的验真，如照片和视频。随着深度造假技术的进步，通过人工和算法的直接检视，将越来越难以对真实性进行检测。**虽然区块链包罗万象，使我们能追踪特定作品的制作时间，但 SBT 将使我们能追踪其*社会源头***，为我们提供发布该作品的灵魂背后的丰富社会背景，他们的成员身份、归属关系、资历证明之林林总总，以及他们与事件主体的社会距离。“深度赝品”很容易被识别，如果该制品的生产时间和社会背景对不上的话；而知名摄影师的验证则可确认可信制品（如照片）。尽管目前的技术可以移除文化产品（如图片）的背景，使它们易受肆意妄为的病毒攻击而被剥夺社会背景，但 SBT 可对此类物品进行背景重建，使灵魂能够利用社区中已存信任关系，对声誉提供有益的保护网。

4.2 灵魂借贷

也许直接建于声誉的最大金融价值是信用和无抵押借贷。目前，Web3 生态系统无法简单复制无抵押借贷，因为所有资产是可转让和可售卖的，因此徒有抵押品的形式。“传统”金融生态

系统支持多种形式的无抵押贷款，但依靠中心化的信用评级来衡量借款人的信用，而这些借款人几乎没有动力共享其信用记录。这样的评级有诸多缺陷。往好了说，他们至多只能不透明地对信用相关因素进行高估和低估，并对那些未积累足够数据的人抱有偏见，主要是对少数族裔和穷人。往坏了说，他们可以利用电影《黑镜》中的不透明"社会信用"系统，诱导社会结果，并强化歧视。

SBT 的生态系统可以实现抗审查的自上而下的商业和"社会"信用体系，取代自下而上的体系。代表学历证书、工作履历和租约的 SBT 可以作为信用相关历史的不变记录，得以让灵魂通过质押有意义的声誉，免抵押获得贷款。贷款和信用额度可以表示为不可转让但可撤销的 SBT，因此它们嵌套在灵魂的其他 SBT（一种不可扣押的声誉抵押品）中，直到贷款偿还后被烧毁，甚或更好的是，被还款证明所替换。SBT 具备有效的安全性：不可转让性可防止转移或隐匿未偿还贷款，而丰富的 SBT 生态系统惩罚试图逃避贷款（比如新建灵魂账户）的借款人，让他们得不到SBT 来有效质押其声誉。

用 SBT来计算公共债务十分便利，这将开源借贷市场。SBT 与还款风险之间将出现新的相关性，从而催生更好的贷款算法来预测信用，从而减少中心化、不透明的信用评级基础设施所起的作用。甚或更好的是，借贷可发生于社交网络内部。特别地，SBT 将为类似于穆罕默德·尤努斯（Muhammad Yunus）和格莱珉银行（Grameen Bank）开创的社区借贷实践提供土壤，其间社交网络成员同意担保彼此的债务。因为一个灵魂的 SBT 组合代表了跨社会群体的成员身份，参与者可以很容易地在一个团体借贷项目中发现可当作有价值的共同参与者的其他灵魂。商业借贷是一种"先贷后忘"直止还款的模式，而社区借贷可

能会采取“先贷后助”的方式，将营运资本与人力资本结合起来，从而获得更高的回报率。

无抵押的社区借贷如何落地？一开始，我们预料灵魂们只持有反映他们愿意公开分享的信息的 SBT，例如简历中的信息。虽然范围有限，但足以启动社区内的借贷实验，尤其当SBT是由信誉良好的机构发行的时候。例如，用以展示某些编程证书、参加过几场会议和工作履历的一组SBT，可能足以让灵魂为他们的事业获得贷款（或种子轮投资）。这种资历和社会关系，已经非正式地在风险投资等资本配置活动中发挥了重要但模糊的作用。

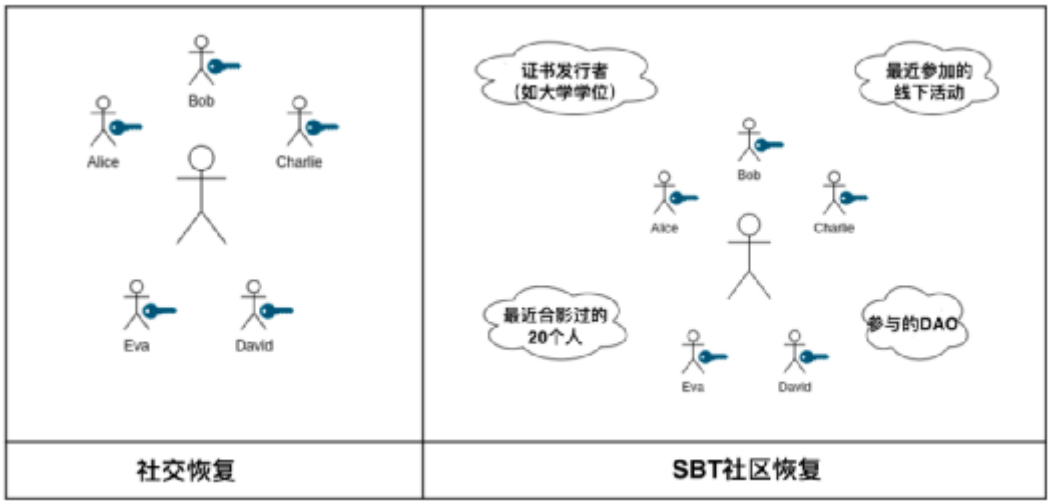
4.3 保管好你的灵魂

重要SBT 不可转让，比如只发一次的学历证书，这产生了一个重要问题：你如何不丢失灵魂？目前的恢复方法，如多签恢复或助记词，在心理压力、交易便利性和安全性方面不得不做出取舍。社交恢复是一种新兴的手段，它依赖于个人的信任关系。SBT 允许类似的但范围更广的方式：社区恢复，在这里，灵魂是其社交网络交集的投票表决。

社交恢复是保护安全的良好起点，但在安全性和可用性方面存在一些缺陷。用户生成一组“监护人”，授权他们按多数人的决定修改钱包密钥。监护人可以是个人、机构或其他钱包的混合体。问题是，一方面希望监护人数量足够多，另一方面得让监护人来自不同社交圈以预防串通，用户在这两者之间得做出权衡。此外，监护人可能会去世，关系可能恶化，或者只是失去联系，因此需要繁复费力的替换。虽然社交恢复避免了单点故

障，但成功的恢复仍然取决于与大多数监护人建立维持信任关系。

一个更强大的解决方案是，将灵魂恢复绑定于灵魂的多社区成员身份，不是生成，而是利用一组广度最大的实时社交关系，来确保安全。回想一下，SBT 代表不同社区的成员身份。其中一些社区，如雇主、俱乐部、大学或教堂，在本质上可能更接近链下，而其他社区，如参与协议治理或DAO，可能更接近链上。在社区恢复模型中，灵魂私钥的恢复需要来自灵魂所在的（随机挑选的一组）社区的合格多数成员的同意。



与社交恢复一样，我们假设灵魂可以访问安全的链上通信渠道，其中“身份验真”可通过对话、面谈或确认共同的秘密等实现。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验真的（即高带宽）通信渠道。

这些是否行得通，其细节需要实验来验证。例如，如何选择监护人，以及需要多少监护人的同意，这些关键安全参数需要进一步的研究。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，且随着灵魂加入更多不同的社区，并形成更多有意义的关系，安全性也会增强。

社区恢复作为一种安全机制，体现了20世纪初社会学家GeorgSimmel（社交网络理论的创始人）的身份理论，该理论认为，个性从社会群体的交汇中显现而出，就像社会群体作为个体的交汇显现而出一样。维护和恢复灵魂的加密财产需要灵魂网络的同意。**通过在社交关系中嵌入安全性**，灵魂总是可以通过社区恢复来重新生成他们的密钥，从而阻嚇灵魂的被盗（或出售）：因为卖家需要证明恢复关系的出售，任何出售灵魂的尝试都将缺少信用。

4.4 灵魂空投

到目前为止，我们已阐释灵魂们如何能代表个人，并反映他们的独特特征和纽带，因为他们拥有反映其归属关系、成员身份和资历证明的 SBT。这种形式的个性化，有助于灵魂们建立声誉、追溯来源、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 还使社区能在灵魂们的独特交汇处汇集**。到目前为止，Web3 主要依靠代币销售或空投来召集新社区，但准确性或精确度很低。空投，是指通过算法将代币免费投送给一组钱包，大多数落于已有特定代币的持有者和钱包，其很容易受到女巫攻击，诱发策略性行为和马太效应。SBT提供了一种彻底的改进，我们称之为“灵魂空投”。

“灵魂空投”是基于灵魂内 SBT 和其他代币而计算的空投。例如，想要在特定的第 1 层协议中召集社区 DAO ，可以向持有出席最近 5 次会议中的3 次的SBT 开发者，或其他反映参会情况的代币（如 POAP）的开发者，给予灵魂空投。协议还可在不同

的 SBT 组合之间以编程方式处理代币空投的权重。我们可以设想一个非盈利组织，其使命是植树，将治理代币空投给持有环保SBT、园艺 SBT 和碳封存代币的灵魂，可以向碳封存代币持有者投放更多的代币。

灵魂空投还可以引入新的激励措施来鼓励社区参与。空投的SBT可以设计为在一段时间内与灵魂绑定，但随着时间的推移最终“归属”为可转让的代币。或者反过来。持有一段时间可转让代币可以赋予SBT的权利，给予更多的协议治理权。SBT 为试验最大化社区参与度和其他目标（如去中心化）的机制，提供了丰富的可能性，我们将在下面进一步讨论。

4.5 灵魂之DAO

去中心化自治组织 (DAO) 是为了共同目的而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来运作。虽然 DAO 在跨距离和差异化的全球社区协调方面具有巨大潜力，但它们容易受到女巫攻击，其中单个用户可以凭多个钱包来累积投票权，或者在不太复杂的一币一票式治理中，只需囤积代币获得 51% 的投票权就可剥夺其他 49% 的投票权。

DAO 可以通过以下几种方式应对SBT的女巫攻击：

- 通过计算灵魂持有的SBT组合，**辨识独特的灵魂和可能的机器人**，并拒绝给予看似女巫的灵魂以投票权。

- 对持有更多声誉 SBT 的**灵魂给予更多的投票权，**如工作或学历资质、执照或证书

- 发行**专门的"人格证明"SBT**，以帮助其他 DAO 对抗女巫攻击。

- **检查**支持特定投票的灵魂所持有的**SBT 之间的*关联度***，以及对高度关联的投票者给予较低的投票权重。

关联度检查的前景特别好，也特别新颖。由持有相同的 SBT 的灵魂所投的票，更有可能是女巫攻击，即使不是女巫攻击，这样的票也更有可能来自*一群犯同样决策错误或同样偏见*的灵魂，因此其权重应适当地低于数量相同但参与者更分散的票。[7]

在本文附录中，我们用数学方法对这一做法在二次方融资的情形下的运用进行了更细致的探讨，我们在其中引入了一个新的原生组件，称为"**关联度分数**"。这种按关联度进行降权调整的概念可以扩展到会商机制的构建。例如，易受多数派操纵的 DAO，通过SBT计算，将参加商议的成员分散度予以最大化，确保少数派的声音能被听到。

DAO 还可以靠 SBT 来阻止各种形式的策略性行为，如"吸血鬼攻击"。在此类攻击中，DAO（常与具有经济价值的 DeFi 协议相关联）通过复制别的DAO的开源代码并随后用代币吸引用户的流动性，来搭便车。DAO们可以阻止搭便车者，首先制定规范，只对那些能反抗女巫攻击的流动性提供者给予灵魂空投（如授予SBT），而扣留对在吸血鬼攻击中转移流动性的灵魂的空投。同样的机制不适用于对钱包的空投，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，让领导层和治理机构程式化地回应社区诉求。领导角色可以随着社区组成的变化而动态变化，反映 SBT 在灵魂成员间分布的变化。根据 DAO 内多个社区的交叉和覆盖范围，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用 SBT 将跨多个社区的灵魂放在中心位置。或者，DAO 可以选择对某些特征组合给予优先照顾的治理机制，例如基于邮政编码的多样性或参与某些特殊爱好的 DAO 。

4.6 以多元化衡量去中心化

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”，生态系统事实上是由一个或一小撮协同实体来主导的?

有两个流行的去中心化指标，一个是 Balaji Srinivasan 提出的 Nakamoto 系数，用以衡量需要汇总多少不同实体才能聚集 51% 的资源，另一个是Herndahl-Hirschman 指数，用于为了反垄断的目的而衡量市场集中度，以市场参与者市场份额的平方之和计算得出。然而，这些方法的关键问题是，什么才是需衡量的正确资源、如何处理局部协同，以及 “不同实体”的界定这一灰色区域。

例如，名义上独立的不同企业可能有许多共同的大股东，董事是新朋好友，或者受同一政府监管。就代币协议而言，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，即使地址可以溯及到特定个人，这些人也可能是

容易发生无意的过度协同（往好了说）或故意串谋（往坏了说）的社会亲缘群体。**更好的衡量去中心化的方法，要能捕捉社会依从度、弱归属和强关联。**

矿工和矿池运营商共同组成了 90% 的比特币算力，他们一起坐在一场会议的讨论小组中。

SBT 支持以一种不同的方式来衡量 DAO、协议或网络的去中心化（或多元化）水平。

- 作为第一步，协议可将代币投票权限于能适当反抗女巫攻击（或持有很多SBT）的灵魂。

- 作为第二步，协议可以检查不同灵魂持有的 SBT之间的关联度，如果它们共同拥有大量 SBT，则对其投票权进行调整（将它们当作一个整体，仅将他们的部分投票权分开计算）。（在附录 A，我们用数学方法对这一做法在二次方融资的情形下的运用进行了更细致的探讨，我们在其中引入了一个新的原生组件，称为**"关联度分数"**。）

- 作为第三步，为了从更广的范围来看，并对跨网络的去中心化有所了解，可以测量灵魂持有的 SBT 在网络堆栈的不同层级之间和跨越层级的关联度，也就是测量其在投票、代币所有权、治理相关的通信，甚至计算资源控制等诸多方面的关联度。

SBT 使我们能够衡量互操作的分层生态系统的去中心化水平，这在今天是非常难以实现的。什么样的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，仍然是一个悬而未决的大问题。还有很多关于如何检查 SBT之间关系的问题，哪些SBT权重大些，哪些SBT权重少些，对嵌套的SBT降权调整，或者还要考虑灵魂们内部可转让代币的组成。然而，随着灵魂和 SBT 生态系统日渐丰富，大量数据可用于进行这些计算，并朝着真实的去中心化迈进。

4.7 产权多元化

DAO 通常在虚拟世界和现实世界中拥有资产，或组织于这些资产的所有权之上。目前Web3 的范畴主要局限于一小部分财产类别，其权利可以完全转让：代币、NFT、艺术品、初版或像美国宪法这样的稀有手稿。但是，强调可转让性对 Web3 并不利，使其无法代表和支持当今一些常见的简单财产合同，例如公寓租约。财产权在罗马法传统中被定义为使用（“usus”）、处分（“abusus”）和收益（“fructus”）的权利的组合。所有这些权利很少共同归属于同一所有者。例如，公寓租约授予出租人有限的使用权（“usus”），但没有无限制地处分（“abusus”）、出售（“fructus”） 公寓甚至转让其使用权（转租）的权利。不动产（土地）的权利通常受制于一系列私人使用限制、公共使用权

授予、出售权限制，甚至国家征用购买权。他们通常还负担着抵押，其将一些金融价值转移给贷方。

与目前想象的Web3不同，未来的产权创新不太可能建立在完全可转让的私有财产之上。相反，**创新将取决于能否分解产权，以与现有财产制度的特征相匹配，并对更丰富的细节予以编码**。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设定产权。 例如，授予员工使用专有设施的权利（“usus”），但保留经理修改或销毁资产的权利（“abusus”），同时向股东支付大部分财务利益（“fructus”）。SBT 可以灵活地代表实物和虚拟资产的这种细微产权并使之增殖，同时鼓励新的实验。这里有一些应用场景：

- **允许访问**私人或公共控制的资源（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应用场景，因为访问权通常是有条件的，且不可转让的：如果我信任你，让你进入我的后院用作娱乐空间，这并不意味着我允许你将该许可转让给其他人。

- **数据合作社**，SBT 给研究人员授予数据访问权限，同时将成员的权利实体化，如对研究成果及其知识产权的访问许可（可通过二次方投票）和经济谈判权。我们在第4节多元意义建构中进一步探讨此点。

- **当地货币的实验**，规则是让居住在特定地区或隶属于特定社区的灵魂更有价值地持有和消费当地货币。

- **社会参与的实验**，其间 SBT 为有较少社会背景的灵魂（例如移民、青少年）创造一个持续的平台，帮助其在陌生的

大网络中获得影响力。这些灵魂刚开始持有较小范围的SBT，能将其家人和当地社会归集在一起。随着他们加入的团体越来越多，他们将获得更大范围的SBT，获得投票权，施展对更广网络的影响力。这是DanielleAllen多元政治思想的主旨，不过目前主导这一过程的是一些随意的年龄和居住地标准。

- **市场设计的实验**，如哈伯格税制和 SALSA（自行评授并拍卖出售的许可证），资产持有人发布自行评估的价格，任何他人都以此价格向其购买资产，并且须定期缴纳占该估价一定比例的税费以维持其对资产的控制权。SBT 可用于创建更细小的 SALSA 版本，例如，社区要对参与权进行批准，以尽量减少来自社区内外的策略性行为。

- 二次方投票等**民主机制设计的实验**。代表社区成员身份的 SBT 的持有者可以对激励额和税率等参数进行二次方投票。最后，“市场”和“政治”不是割裂的制度领域；在那些探索两个领域之间广阔天地的技术方案中， SBT 可扮演主要角色。通过二次方融资来提供公共物品，就是另一个这样的市场和政治交汇点。

当然，还有一些地狱乌托邦情形需要考虑。可以有移民系统，让SBT可以迁移。监管者被收买也可以被编码进嵌套的社区代币中，在这种情形下，业主拥有不成比例的投票权阻碍住房建设。SBT 可以使拒贷自动化。下面会进一步讨论，这些情形要放在当前自上而下的不透明许可和歧视的社会背景下考虑。SBT 让歧视无所遁形，人们得以与之抗争。

4.8 从私人和公共物品到多元网络物品

更宽泛地说，SBT 得以让我们有效呈现和管理**介于完全私有和完全公共的中间地带**的任何资产和物品。在现实生活中，几乎所有东西都在这个中间地带：即使用于个人消费的物品也有积极的副作用，如消费之后能更好地为其家庭或社区做贡献；即使是地球上无处不在的公共物品（如气候），对某些人也必然比对另一些人更有益（如塞舌尔比西伯利亚）。同样，*人类的动机*很少是完全利己或完全利他的。许多类型的先验存在的协作，在某些社区比在另一些社区更常见到。

然而，今天的制度设计是假定存在原子化的、自私的代理人，他们之间没有先验存在的协作，制度因而常常被已有协作的群体无意的过度协同[8]（往好了说）和故意串谋（往坏了说）攻击。因此，即使是最好的公共融资模型，包括二次方融资 (Quadratic Funding,QF)，也无法规模化增长。QF 通过减少对少数人集中行动的奖励，增加对多数人集体行动的奖励，来鼓励协作；例如，10 人各出资1 美元，会有99 美元之相匹配，总共筹集100 美元；而一个人出资10 美元，则没有匹配。其数学实现方法是，按个人出资的平方根之和的平方，给予相应比例的资金匹配（我们在附录中进一步详细说明）。但是，有些大型群体（比如大多数中国公民），即使他们之间的*协作很弱*（比如向一项事业出资1 美元），也会垄断系统，并吸走所有匹配的资金，原因是QF 对独特出资者数量所加的权重。照此，QF 不但不对关联的特殊利益体之间的协同行为予以降权，反而会*奖励*它，即使其会吸干QF。

但是，与其将先验存在的协作视为应予"改写"的漏洞，不如承认它，有些协作可以被利用和抵消。毕竟，我们从事的是鼓励协作的事业。关键是让二次方机制能与先验存在的协作网络一起运作，纠正其过度协同的偏好和倾向。SBT 提供了一种自然的

方式，使得我们调整天平，支持*跨越差异*的协作。正如诺贝尔奖获得者埃莉诺·奥斯特罗姆（Elinor Ostrom）所强调的那样，问题不在于协同公共物品*本身*，而在于帮助由不完全协作但具有社会联系的个人组成的社区*克服*他们的社会差异，在更广的网络中进行大规模协同。

如果 SBT 代表反映灵魂偏向性的社区成员身份，那么**支持跨差异的协作，就意味着归属关系相似的灵魂或关联的灵魂所得的协作奖励应予降权调整**，其相似度以他们都有的 SBT来测量。其中的假设是，*归属关系不同的灵魂之间的*共识，能更好地代表横跨*更广*网络的多元物品，而归属关系*相似*的灵魂之间的共识，更可能代表服务于狭隘利益的过度协同（或串谋）物品。

通过揭示灵魂们共有的成员身份，SBT得以让我们对先验存在的协作给予*降权调整*，并**基于最富多样性的成员同意**，以二次方的方式增加在新兴网络中广泛赋利的多元物品规模， 而不局限于受特殊利益集团无意的过度协同（或故意串谋）影响的更狭隘的物品。相关度降权调整的精确公式，“其最佳效果”取决于模型细节，这方面的研究尚未开展，但我们在附录中为实验起了个头，以方便进一步研究。

§5 多元的意义建构

数字世界中日益突出的多元网络物品的一个例子，是基于用户数据构建的预测模型。人工智能 (AI) 和预测市场，都试图根据主要来源于人的数据预测未来事件。但是这两种方法都有局限性，原因不同甚至近乎相反。AI 中的主导方式避开了激励措施，它收集（公共或私人监控获得的）数据馈送，并使用私有的大规模非线性模型，将数据合成为预测，它利用了Web2固有

的对“usus”（使用权）的垄断，而没有给数据工作者任何“fructus”（收益权）。预测市场采取了相反的方法，人们押注结果以期获得财务收益，完全依赖金融投机的经济激励(“fructus”收益权），不需对投注者的看法作合成处理并产生组合模型。同时，这两种方法都得出了所谓“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看法概括为单个数字：均衡价格。

一种更富成效的方法，是避开这些极端，取而代之以利用两者的优点，同时弥补它们的弱点且丰富它们的广度。我们建议，将复杂的非线性 AI 模型与预测市场的市场激励相结合，把被动的数据工作者转变为主动的数据创造者。有了这些植根于数据创建者社交关系的丰富信息源， DeSoc 能实现比这两种方法强大得多的多元网络智能，让我们来看看这是怎么做到的。

5.1 预测市场到预测多元性

预测市场的目标是，根据愿意下注的人的财富和风险偏好，汇总他们的看法，即用钱来说话。但是这种“适者生存”并不是汇集看法的理想方式。一个交易者的收益是另一个交易者的损失，这种零和游戏假设了一种能预测在与“聪明人”还是“愚蠢人”搏斗的一般性能力。虽然财富可能代表某些形式的能力和专业知识，但基于别样的专业比较优势的预测可能更可靠。在特定领域输掉赌注的参与者可能对另一个领域有更准确的看法。但预测市场不好的是，它提取那些有赌性的人的看法，这会使赢得赌注的人变得富有，使其他人变得贫穷，并阻碍风险厌恶型的人的普遍参与。

有更好的方法来提取看法。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*高级的团队预测调查*，那里人们更有动力分享和讨论信息。在团队会商模式下，可以根据过去的表现和同行评价等因素对成员进行评估，团队参加半结构化的讨论以汇集未能在买卖合约中涵盖的信息。这种团队会商模型可以通过**二次方规则**进一步改进，**从所有参与者提取确切的概率估计**（与之相比，预测市场只能提取对当前均衡价格的自上而下的看法）。[9]已经证明，人们有动机购买的合约数量，反映了他们的主观概率评估。[10]这样的市场也更平等地分配从参与中获得的收益，奖励准确性，而不至于让其他人破产，从而让每个人都成为未来轮次的参与者。

SBT 可以在预测能力和专业比较优势方面带来一类新的丰富模型和实验。预测市场只得出一个数字，即合约的价格，而二次方投票可得出每个参与者对事件概率的*确切*看法。SBT 能够代入参与者的学历证书、成员身份和一般社交关系等***社会背景*对这些看法作进一步运算**，以获得更好的加权（或非线性合成）预测模型，这可能会导致在新的、意料之外的交汇区出现专家级预测者。进而，即使一次投票没能很好地汇总看法，也可以追溯研究过往投票，揭示“更正确”参与者的特征，并在未来的投票中召集更适合的“专家”，这或许会在团队会商的情形下出现。这些机制与我们在本文中倡导的机制密切相关。就像按关联度分数进行降权调整的二次方机制可以将协调不佳的自上而下的公共物品转变为强大的、自下而上的多元网络物品一样，这些机制也可以将基于零和预测市场、鼓励参与者隐匿自身信息（如Futarchy）的治理系统，转变为正和的、多元的意义构建，以鼓励新的优质信息的披露和合成。

5.2 人工智能到多元智能

大规模非线性“神经网络”模型（例如BERT和 GPT-3）也可以被SBT改变。此类模型会收集大量公共或私人监控的数据流，以生成丰富的模型和预测，如基于自然语言提示符的代码。大多数监控数据创建者不知道他们在创建这些模型中的作用，不保留任何追索权，并且被视为“偶然的”而不是关键的参与者。此外，数据收集使模型脱离了它们的社会背景，这掩盖了它们的偏好和局限，并削弱我们修补的能力。随着对数据可用性的需求不断增长、记录数据来源的“数据集的数据表”等新举措以及机器学习的隐私保护方法的出现，这种矛盾日益凸显。这些方法需要为生成数据的人提供实在的经济和治理利益，并激励他们协作创造比他们单打独斗所能做出的强大得多的模型。

SBT 提供了一种自然的方式，**为来源丰富的数据编制经济激励措施，同时赋予数据创建者对其数据的追索治理权**。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（及数据质量）进行谨慎而相称的有的放矢的激励。同时，模型制作者可以跟踪所收集的数据的特征及其社会背景（被SBT反映），并找到抵消偏好和弥补局限的因素。SBT 还可以为数据创建者设置定制化的治理权，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，就是多元智能的未来，模型制作者可以通过竞争及协商，使用相同数据来构建不同的模型。因此，我们抛弃了脱离人类源头、从来源不可溯的监视数据归集而来的、分离的单体“人工智能”模式，转向通过协作构建的、植根于社会源头并由灵魂们治理的多元智能的寒武大爆发。

随着时间的推移，就像 SBT 使灵魂个性化一样，它们也使让模型个性化，即把数据来源、治理和经济权利直接嵌入模型的代码中。因此，多元智能像人类一样，构建的灵魂嵌入了人类社

交关系。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，与其他灵魂互补和协作。而且，在这方面，我们看到预测市场和人工智能两种方法在多元意义建构方向上的融合，综合普遍采用的激励措施和对社会背景的仔细跟踪，创造出多种多样的模型，将两种方法的优点揉合在一起，获得青出于蓝而胜于蓝的技术方法。

5.3 可编程的多元隐私

多元智能引发了数据隐私方面的重要问题。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，或者捕获非人际但共享的数据（如社交图谱）。“自我主权身份”倡导者倾向于将数据视为私有财产：这次交互产生的数据是*我的*，*因此我*应能选择何时以及向谁披露。不过，与实体经济相比，人们对数据经济的简单私有产权知之甚少。在简单的双向关系中，例如婚外出轨，披露信息的权利通常是对称的，通常需要双方许可和同意。正如学者海伦·尼森鲍姆（Helen Nissenbaum）所强调的那样，关注点不在于“隐私”本身，而是在特定社会下背景披露某些信息是不正当的。剑桥分析数据丑闻 (Cambridge Analytica Scandal)就主要是在未经他人同意的情况下透露他们的社交图谱属性和朋友信息。

与将隐私作为可转让产权不同，一种更有前途的方法是将隐私视为***一组可编程的、松散耦合的、许可对信息访问、更改或从中获利的权利***。在这种范式下，每个 SBT（例如代表资历证明或数据存储访问权的 SBT）理想的话也将具有可编程的隐性财产权，指代对构成 SBT基础信息的访问权，基础信息包括：持有者及其之间的协议、共享财产（例如数据）以及对第三方的

义务。比如，某些发行人会选择将 SBT 完全公开。一些SBT，比如护照或医疗记录，在自主权意义上是私有的，持有SBT的灵魂才有单方面披露的权利。其他的，例如反映数据合作社成员身份的 SBT，拥有多签或更高级的社区投票权，在所有或大部分 SBT 持有者同意时才可以披露。

尽管目前存在技术问题（SBT 可以以这种方式编程吗？），以及激励兼容性方面的重要问题（在第 7 节中进一步探讨），我们认为可编程的多元隐私值得进一步研究，并且与其他方法相比具有关键优势。 在我们的方法下，SBT 有潜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约定。此外，这种可编程性可以帮助我们重构新的配置，因为可以***有无数种方式将隐私（作为许可访问信息的权利）解构为"usus"（使用）、"abusus"（处分）和"fructus"（收益）***，从而创设出一簇簇细小的访问权。例如，SBT 可以使用特定的隐私保护技术，允许对数据存储（可能由多个灵魂拥有和管理）进行计算。一些 SBT 甚至可能允许以可进行某些计算但结果不得向第三方证明的方式访问数据。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，但投票不应向他人证明，以防止购买选票。

通信可能是最正统的共享数据形式。然而，今天的通信渠道缺乏用户控制和治理（"usus使用"和 "abusus处分"），而将用户的注意力（"fructus收益"）拍卖给了出价最高的人，即使是机器人。SBT 有可能实现更健康的"注意力经济"形式，使灵魂能够对来自其社交图谱之外可能是机器人的信息进行垃圾过滤，同时提升来自于真实社区和青睐的社会交汇区的信息。听众可以更加了解他们在听谁，并能更好地给激发洞察力的作品点赞。这样的经济体可以优化正和协同，以及有价值的共同创造，而不

是将优先级放在最大参与度上。这种通信渠道对安全也很重要；如上所述，“高带宽”通信渠道对于建立社区恢复的安全基础至关重要。

§6 去中心化社会

Web3 立志于改变广泛的社会，而不仅仅是金融系统。然而今天的社会结构，家庭、教堂、球队、公司、市民社会、名人、民主政体，缺了代表人类灵魂及其支撑的更广泛关系的原生组件，这些在虚拟世界（通常称为“元宇宙”）中都毫无意义。如果 Web3 离开了不变身份、信任和协作模式以及可组合的权利和许可，我们将渐次看到女巫攻击、策略性行为和完全可转让私有产权经济领域的局限性，所有这些都将引致过度金融化。

为了避免过度金融化，又能实现指数级增长，我们建议将虚拟和现实世界中的社交关系*放大和桥接起来*，赋能灵魂和社区，对丰富的社会和经济关系进行编码。但仅仅在信任与协作之上建设是不够的。纠正信任网络之间的偏好和过度协同（或串谋）倾向，对于促进比以往更复杂、更多元且社交跨度更大的社会关系，至关重要。我们称之为“去中心化社会（DeSoc）”：**一种共决共定的社交关系，灵魂们和社区自下而上地聚集在一起，以此为彼此的新兴特质，跨越不同尺度生产*多元网络物品***。

我们多元网络物品当作DeSoc 的一个功能来强调，因为网络是经济增长最强大的引擎，但最容易被私营企业（例如 Web2）和强权政府所恶意俘获。最显着的经济增长来自*网络回报的增加*，其中每增加一个单位投入就会产生递增的产出。简单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

些基础设施是投入劳动力和其他资本建设的。强大的数字网络的例子包括交易市场、预测模型和基于数据的多元智能。在这两类情况下，网络经济学都不同于新古典经济学，后者教导收益*递减*，每增加一个单位的投入产出就会逐渐*减少*，而私有产权会产生最有效的结果。收益递增背景下的私有产权具有相反的效果，收取租金会抑制网络增长。两座城市之间的道路可以从贸易收益中实现越来越多的回报。但如果该道路是私人拥有的，而业主选择按两个城市之间的贸易价值收取过路费，就会抑制增长。网络的公共所有权也有其自身的危险，容易受到监管者被收买或资金不足的影响。

在既不被视为纯粹的公共物品也不是纯粹的私人物品，而是被视为*局部的多元的共享物品*时，收益递增的网络最有效。DeSoc提供了社会土壤，得以分解和重新设定权利，即使用（“usus”）、处分（“abusus”）和收益（“fructus”）的权利，并在这些权利中启用有效的治理机制，在制衡串谋和收买的同时，增强信任和协作。在本文中我们已探讨了几种机制，例如基于社区的 SALSA 和根据关联度分数作降权调整的二方次融资（和投票）。作为第三种机制的局部和多元所有权，避免了Charybdis式的私人收租和Scylla式的公共监管者收买。

在许多方面，**今天的 DeFi 只不过是将收益递减私有产权模式老瓶装新酒，放到了收益递增网络上。**建立在无需信任的基础上， DeFi 天然地局限于完全可转让的私有产权（如可转让代币）领域，大多将“usus使用”、“abusus处分”和“fructus收益”捆绑在一起。往好了说，DeFi 只不过可以收租而限制网络增长，往坏了说，有可能面临由“鲸鱼”操纵的地狱乌托邦式监控垄断，这些鲸鱼竞相无底线收割吸食数据，就跟Web2 一样。

DeSoc 将 DeFi 的网络价值控制和投机的竞赛转变为自下而上的协同，建设、参与和治理网络。至少，DeSoc 的社会土壤可以让 DeFi对抗女巫攻击（赋能社区治理）、对抗吸血鬼攻击（将积极的外部性予以内化，以建设开源网络）并对抗策略性行为（维持网络的去中心化）。通过 DeSoc 的结构化纠偏措施，DeFi 可以支持和扩展多元网络，这些网络可以广泛地赋利，只要获得极为分散的成员的同意，而不是进一步巩固被狭隘利益集团挟持的网络。

然而，**DeSoc 的最大优势在于其*网络可组合性***。持续递增的回报和网络增长不仅避免了收租的危险，而且还促成嵌套网络的扩张和交汇。一条道路可以形成两个城市之间的网络。但是，如果缺乏更广泛的协作，仅仅是两个城市间的协作，有朝一日也会达到收益递减的天花板，要么因为*堵塞*（道路和住房），要么因为*疲劳*（达到可服务人群的极限）。只有通过技术创新和更广泛（也可以是更松散）地与邻近网络开展协作，获得新的收益增长来源，价值才能继续呈指数级增长。一些协作将是实体的，跨区域的实体贸易逐步扩展。但更多的连接将是信息的和数字的。随着时间的推移，我们将看到实体网络和数字网络之间新的协作矩阵，依赖于并扩展它们所建立的社会互连。DeSoc 所要赋能的，正是这种彼此交汇的、局部嵌套的跨数字和现实世界的不断增长的网络协作结构 。

通过组成网络和协同，DeSoc出现在政治生活和市场上，通过社交关系来增强两者。DeSoc 实现了 JCR Licklider（孕育了互联网的 ARPANET 的创始人）的愿景，在“星际计算机网络”中“人机共生”， 社会活力在*信任的基础上*显著增强。DeSoc 并非建立在 DeFi *不需信任*的基础之上，而是对支撑当今实体经济的信任网络进行编码，使得我们对之加以利用，生成多元网络物品，

并对抗挟持、抽血或操纵。借助这种增强的社交关系，Web3 可以避免短期的过度金融化，迈向跨越社交距离的回报递增的无限未来。

6.1 灵魂可以去天堂……或地狱

虽然我们选择性地强调了我们看好的 DeSoc可释放的潜力，但要记住，任何具有这种变革力的技术，几乎都将具有相同的破坏力：化石燃料；车轮滚滚；电视洗脑；汽车污染；信用卡债务陷阱，等等。在这里，可用于解决群体内部问题和实现跨差异协作的同种 SBT，也可用于对不受欢迎的社会群体自动拒贷，甚至针对他们进行网络或实体攻击，实施限制性移民政策，或进行掠夺式贷款。诸多类似的可能性，在当前的 Web3 生态系统中还不太突出，因为在当前的土壤里它们还不是有意义的概念。落实 DeSoc 的好处，也会带来这些害处。就像拥有一颗心的缺点是这颗心可能会破碎一样，拥有一个灵魂的缺点是它会下地狱，而拥有一个社会的缺点是社会常常被仇恨、偏见、暴力和恐惧所裹挟。人类就是一场伟大而往往结局可悲的实验。

当我们思忖DeSoc 可能陷入地狱乌托邦时，我们还应将这些可能性与其他技术所导致的地狱乌托邦作比较。Web2设施被用于不透明的威权监控和社会控制。Web2 常依赖自上而下的人为官僚机构来授予身份（“驾驶执照”）， DeSoc 则依赖横向（“点对点”）社会证明。DeSoc 使灵魂们能对自己的关系进行编码并共同创建多元财产，而 Web2 则采用可极化、分裂和误导的不透明算法，扮演社会联系的中介人甚或将其变现。DeSoc 摒弃自上而下、不透明的社会信用体系。 而Web2是这些信用体系的基础。DeSoc 将灵魂视为代理人，而 Web2 将灵魂视为客体。

使用 DeFi进行社会控制的风险较小（因为缺少身份识别这一基石），至少在短期内是这样。但 DeFi 自身有其地狱乌托邦属性。**虽然 DeFi 克服了*显性*的中心化形式（即特定行为人在系统中拥有超大的正式权力），但它缺少内嵌的机制，来克服串谋和滥用市场力量这类*隐性*中心化。**垄断并不总是像过往的标准石油公司那样浮在水面上。串谋甚至可能发生在生态系统高远的层面。今天，随着一众资产管理机构（如先锋、贝莱德、道富、富达等）的崛起，我们看到了端倪，它们是所有大型银行、航空公司、汽车公司和其他主要行业的最大股东。由于此类资产管理机构持有一个行业内所有竞争参与者的股份（如每家主要航空公司的股份），他们就有动机让他们持股的公司*看起来*像一个竞争性的行业，但却按垄断者那样*行事*，牺牲消费者和公众利益，最大化行业利润。[11]

在 DeFi 中也是如此，同类“鲸鱼”和风投机构在系统各个层级以及系统内的竞争参与者中积攒了很大份额，可在代币治理中操纵投票，或者将其委托给同类的代表，这些代表在网络中相互关联。如果没有对抗女巫及按关联度降权调整作为社会基石，以强力推行去中心化，我们就会看到更多由鲸鱼支持的垄断，而垄断者逐渐成为可用投资资本的最大来源。随着“金钱阶级”和用户的分化，我们将看到（并且已经目睹）越来越多的激励错位和收租行为。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发展，例如应用程序鼓励“拥有”实则为人际关系数据（例如其社交图谱）的多个人之间的竞标战，以组建单体私人 AI，与人类竞争，而不是组建相互竞争的多元AI来造福人类。

因此，DeSoc 不需要很完美，就可通过可接受的非地狱乌托邦测试。要成为一个值得探索的模式，它只需要比可得的其他选

项更好。尽管 DeSoc 有需防范的地狱乌托邦情形，但 Web2 和现有 DeFi正在陷入*必然*的地狱乌托邦模式，将权力集中在精英手里，由他们来决定社会成果或拥有大多数财富。Web2 命中注定是要迈向威权主义的，自上而下的监控和行为操纵的能力会日渐强化。今日的 DeFi 名义上是无政府资本主义，但正在落入网络效应和垄断压力的桎梏，中期来看可能会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，共决共定自己的未来。看看Web2，DeSoc 的诞生可以类比从诸多世纪的君主统治中生长出来的大众参与型政府。参与型政府并非*必然*会产生民主。它也导致了GC主义和法西斯主义的兴起。同样，SBT 并不*必然*使数字基础设施民主，而是具有民主兼容性，具体取决于灵魂和社区共决共定的内容。打开这个可能性空间，是对 Web2 的威权主义和 DeFi 的无政府资本主义的显著改进。

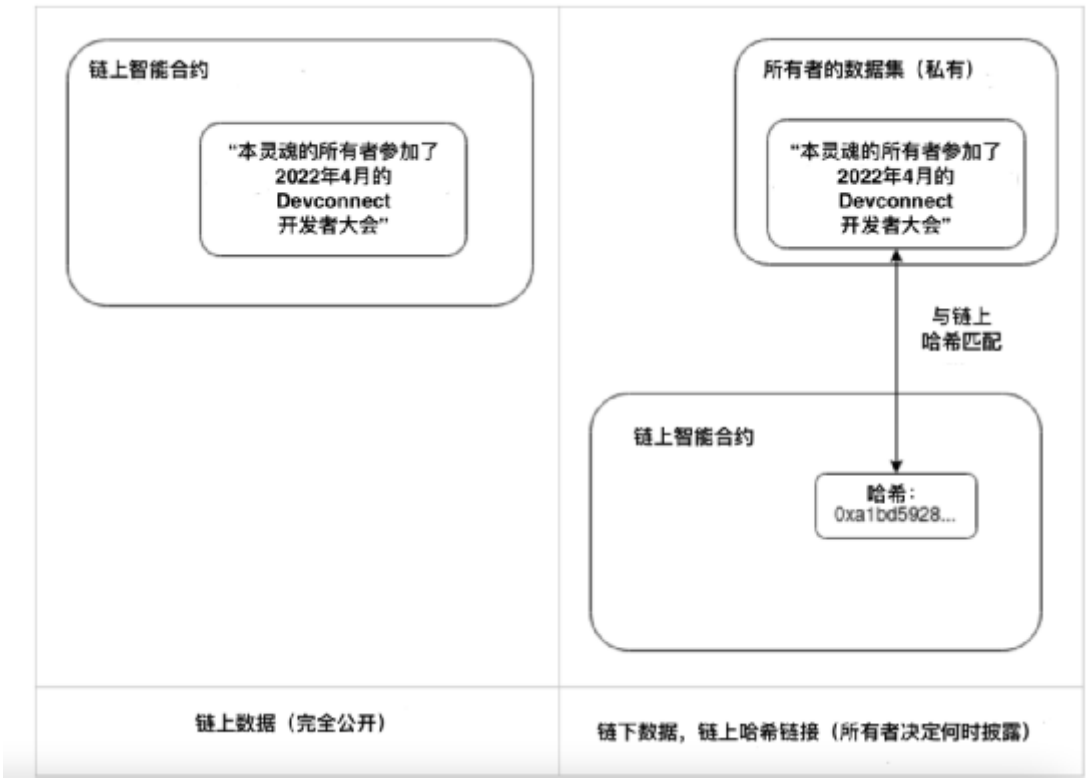
§7 实施的挑战

隐私对 DeSoc 来说是一个关键挑战。一方面，太多的公开SBT可能泄露灵魂的过多信息，使他们面临社会控制的危险。另一方面，过多的纯私有SBT 也可能使私人通信渠道得以规避治理和社会协作中的关联度降权调整，这就带来了激励兼容性的重要问题。与隐私问题密切相关的是欺骗问题：灵魂们可能虚假陈述他们的社会联结，同时以私下或旁路渠道进行协同。我们不能指望穷尽所有的可能性和答案，而只能在本文中探讨这些挑战的性质，并为未来的研究勾勒出一些有前景的路径。

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，而且对全世界的所有人都是立即可见的。使用多个假名可以让某些隐私得以保留：一个家庭灵魂、一个医学灵魂、一个专业灵魂、一个政治灵魂，每个灵魂都持有不同的SBT。但这有些幼稚，因为很容易将这些灵魂相互关联起来。这种隐私缺失的后果是严重的。事实上，**如不采取明确的措施来保护隐私，简单地将所有 SBT 上链的“幼稚”想法，很可能会让许多应用程序暴露过多的信息。**

针对过度信息暴露问题，有几个解决方案，其技术复杂度和功能有所不同。最简单的方法是 SBT 可以在链下存储数据，链上只保留数据的哈希值。



如何存储链下数据完全由个人选择；可能的解决方案包括（i）其自己的设备，（ii）其信任的云服务，或（iii）去中心化网络，如星际文件系统（IPFS）。链下数据存储让我们在拥有许可*写入*SBT 数据的智能合约的同时，保留*读取*该数据的单独许

可。Bob 可以选择仅在他愿意时透露他的 SBT内容（或其许可的数据集）。这已让我们走得相当远了，并且具有提高技术可扩展性的更多好处，因为大多数数据只需由极少数人处理。但要完全实现多元隐私等属性，以及更细粒度的披露形式，我们还有更多路要走。还好的是，许多加密技术能让我们做到这一点。

其中一组强大的构建模块，能以新的方式实现局部数据披露，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主要用于资产转移中的隐私保护，但它也允许人们证明任意陈述的同时，无需透露陈述本身之外的任何更多信息。例如，在可以通过加密技术证明政府文件和其他验证的地方，有人可以证明这样的陈述：“我是加拿大公民，18 岁，拥有大学经济学学位，在 Twitter 上有超过 50,000 名粉丝，尚未在本系统中申请账户。”

零知识证明通过对 SBT进行计算来证明灵魂的特征（例如，它有特定的成员身份）。该技术可以引入**多方计算技术**（例如混淆电路）予以进一步扩展，从而使此类测试具有*双重私密性*：求证者不用向验证者透露他们是谁，而验证者不会向求证者透露其验证机制。而是，双方一起进行计算，只知道输出的结果。

另一种强大的技术是**指定验证者证明**。一般来说，“数据”是滑的：如果我发给你一部电影，我无法从技术上阻止你转录和转发给第三人。数字版权管理 (DRM) 之类的变通办法最多也只起有限的作用，且常给用户带来巨大的成本。然而，证明却不一样地滑。如果 Amma 想向 Bob 证明她的 SBT的某个特性X，她可以对“我持有符合特性X 的 SBT，或者我有Bob灵魂的访问密

钥"这一陈述进行零知识证明。Bob 会认为这个陈述是可信的：他知道他没有作证，因此 Amma 实际上必须有符合特性 X 的 SBT。但是如果 Bob 将证明传递给Cuifen，Cuifen不会认为可信：据他所知，Bob 原本可以用他自己的密钥来作证。***可验证延迟函数 (VDF)***可以将此变得更加强大：Amma 可以制作并展示目前只能用该 SBT 制作的证明，而其他人只可以在*五分钟后*制作。**这意味着，代表*对数据的可信证明*的高级访问许可是可能的，尽管不可能对原始数据本身（可能只是简单地复制和粘贴）予以同类选择性许可。**不过，这可能会让我们走得很远。正如区块链在交易中可提供可追溯性以防止某人右键单击复制粘贴有价值的 NFT（以及对原始所有者进行女巫攻击）一样，SBT 可以提供社会来历方面的可追溯性，这起码可以降低那些来源未经验证、复制粘贴而来的数据的价值。

这些链下数据和零知识技术能兼容***负面声誉***，即使持有者不*希望*它们可见，SBT 也可见。负面声誉的重要例子包括信用记录、未还贷款数据、负面评论和业务合作伙伴的投诉，以及能证明牵涉到协同的社会关系的 SBT。与这一密码技术相结合的区块链，可以提供一个潜在解决方案：智能合约逻辑可以强制灵魂将负面SBT 合并到数据结构中，例如存储在链下的 Merkle 树，并且任何零知识证明或混淆电路计算都需要引入这些信息，否则在提供的数据中会有一个可见的"漏洞"，验证者会识别出来。Unirep 协议就是这点如何实现的一个例子。

以上举例的目的，并非要确切说明如何使用密码技术解决 SBT 的全部隐私和数据许可问题。我们只勾勒出几个例子来展示这些技术的力量。未来重要的研究方向是，明确不同类型数据许可的具体局限，用最优的特定技术组合来实现想要的许可水平。另一个问题是需要什么样的多元产权制度来管理数据，以

及如何妥善拆分访问（“usus使用”）、编辑（“abusus处分”）和现金流（“fructus收益”）的权利。

7.2 作弊的灵魂

如果 SBT 是多元财产、网络物品和智能得以协同的社会基石，人们可能会担心灵魂会试图耍花招或作弊，以攫取我们让SBT许可的社区治理权或产权。例如，如果许多应用程序靠 SBT来代表参会记录，无良会议组织者就可能提供此类 SBT 以换取贿赂。有了足够多的贿赂，人类（和机器人）就可以生成一个虚假的社交图谱，使该帐户看起来像一个真实的人类灵魂，因其（假的）SBT 而与众不同。就像DAO 可以被贿赂一样，灵魂及其使用的链上投票机制也可以。相反，如果用 SBT 来对协同行为作降权处理，灵魂就可避免 SBT被利用来提高影响力。为什么我们该相信灵魂拥有的 SBT 能准确反映其真实的社会承诺，而不仅仅是他们选择的游戏玩法?

一个论点是，不同的作弊动机可能会“相互抵消”。灵魂们会分门别类，加入自我认同的规模称心的重要网络中，就像哈伯格税制中高估和低估资产的动机可相互抵消，从而能得出大致准确的市场估值那样。 灵魂想要持有更多 SBT 以在其社区中获得影响力，但另一方面，会回避不太关心的社区的 SBT，从而降低关联度指标上的得分，并增加他们在更大网络的治理中的影响力。

但如果认为这两种动机，即获得许可和增加影响力，总能均匀地抵消，甚或只是接近于抵消，像变戏法一样，这就显得幼稚了。可能有许多社区使用 SBT 外的系统来调节许可和治理。或者社区可能（与我们关于信息暴露的主要假设相反）发行一点

儿私人 SBT 以代表治理权，但诱使社区成员在更广泛的决策中为这些 SBT 保密。

“博弈”的问题不容小觑。这是一个重要的问题，解决它是未来研究最重要的焦点之一。事实上，为什么把人类用户排序或过滤的诸多现有算法予以开源将非常困难，这就是一个主要原因。为了减轻和阻嚇 SBT的博弈，我们提议几条规范和加密指南：

1. SBT 的生态系统可以**发展“紧密”社区渠道**，其中SBT代表真实的链下社区成员身份，其具有强大的社会纽带和重复的互动行为。这将使社区更容易过滤和撤销冒充者和机器人的 SBT。这种紧密渠道，我们经常在教堂、工作场所、学校、聚会团体和民间社会组织中看到，将为在更“稀薄”的社交渠道中的警察博弈（如通过机器人、贿赂、冒充）提供一种更能抵抗女巫攻击的社会基石。

2. 嵌套型社区可对有串谋可能性的SPT施加“紧接于其下” 的矢量要求。例如，如果一个州正在举行一轮融资或投票，该州可要求每位参与的公民持有某个县和市的 SBT。

3. SBT 生态系统的开放性和加密可证明性，本身可用于**主动检测串谋行为模式，并惩罚不真实的行为**，如降低串谋灵魂的投票权重，或要求灵魂接受代表负面验证的 SBT。例如，如果一个灵魂证明另一灵魂是真人，而其后来被发现是机器人，那么案件可以升级为公开认证，导致该灵魂持有大量负面验证。这在 GitCoin QF 生态系统中已在一定程度上发生了，其使用一系列信号来检测“串谋团伙”。

4. 零知识技术（例如MACI）可**通过加密方式阻止灵魂做出的某些验证不可被证明**。这将使出售某类验证的行为变得不可信，因为行贿者无法判断受贿者是否遵守了他们的交易约定。已有大量关于将这种技术运用于投票的研究，不过任何非金融化的社会机制最终都可受益于类似想法。

5. 我们可以**鼓励举报人**，以此使大规模串通变得难以落地。不是检测和惩罚错误或滥权*行为*，而是检测和惩罚滥权的*串谋模式*。由于存在假旗贿赂的可能性，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，**鼓励在所有情况下都提交验证报告，而在串通范围变得极大时则不需要。和会议组织者验证不同，参会者可以互相验证已参会，因此得贿赂大量的参会者来以验证一份虚假的参会证明。奖励不必是金钱上的，也可以是 SBT，这种奖励对真正的社区成员的价值，比对攻击者更大。

7. 我们可使用关联度分数，**其关注点在于**有共同的利益的一群灵魂的**关联关系，**其**有很大动机诚实行事**。例如，有上限的配对二次方融资中所用的关联度评分技术，采用二次方融资捐赠本身来确定两个参与者的关联度，从而确定如何按其交集做降权调整。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因关联度降权调整的适用而减少，但它永远不会变成*零*或*负数*。

§8 对比和局限

虽然已提出的身份识别方案无比众多，但Web3 领域有四个特别突出和相近的方法广为讨论，值得对比：占主导地位的“传统”身份生态系统、假名经济、人格证明和可验证资质文件。每个方法都突现了我们所倡导的社交身份识别方法的重要贡献和未来需解决的问题，我们将这些局限作为探索未来方向的跳板。有鉴于此，我们也阐释了为什么我们相信我们的灵魂和合灵代币所提供的社会身份识别原生组件，是隐私制度一条更富前景的前进道路。

8.1 传统

传统身份识别系统依赖第三方签发和规管的文件或身份证件（政府、大学、雇主等）。可以联系第三方来确认其来源的真实性。虽然传统系统具有我们应深入理解的一组有趣特性，但这些系统非常低效，并且不适合用于快速有效协同所需的可组合性或计算。此外，这些系统脱离社会背景，使灵魂依赖一个中心化的第三方来确认社区成员身份，而不是依赖其所加入的社区。例如，大多数政府签发的身份证最终都可以追溯到医生和家庭成员授权签发的出生证明，他们是事实的最终来源，更不用说许多同样有用的社会联结，这些社会联结合起来能提供更强大的验证。事实上，当集权中心寻求强有力的身份认证（例如，主要政府部门颁发安全许可）时，他们很少依赖此类文件，而是转向社交网络中的访谈。因此，**此类传统身份识别系统倾向于将权力集中在签发者和那些能够进行尽职调查以获得更强验证的人身上，而这些人反过来又会成为僵化和不可靠的官僚机构。** DeSoc 的一个关键设计目标是，确保能够满足和超越政府 ID 的安全要求，使得各个横向网络能跨越各类社会基础为用户提供更高的安全性。

8.2 假名经济

Balaji Srinivasan 创造并普及了“假名经济”一词，他推广了将声誉系统与零知识证明机制相结合以保护隐私的社会愿景。他的早期版本强调使用假名以避免歧视、防范社会暴徒的“取消文化”，免于被这些暴徒损害声誉和破坏社会关系。它设想人们在其钱包中积累*可转移的*零知识 (ZK) 验证，并通过将验证的子集转移到新钱包，或将验证拆分到多个无法追溯的钱包中，来防范声誉攻击。在挑选要转移的验证时，要选择新帐户中所需的匿名级别，在更多匿名性（转移更少的认证）或更广地分布到其社交网络中（转移更多验证）作出权衡。

典型的假名经济方案和 DeSoc 的实际区别在于，我们不再强调身份分离是保护参与者免受网暴和取消文化的主要方式。一定程度的分离（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，将建立新身份作为抵御攻击的主要手段，存在很大的弊端。它使声誉质押贷款和追踪来历变得更加困难，并且它难以与旨在纠正关联度或女巫攻击的治理机制相组合。

DeSoc 不是通过允许受害者使用新的身份（如旧身份消失）而免受攻击，而是允许使用其他方法，例如将攻击者**放在社会背景中比对**。“取消行为”经常出现在攻击者或机器人与受害者几乎没有社交联系或背景时，且其陈述和行动是*脱离社会背景的*，而病毒信号是通过脱离社会背景的网络传播的。这种方式与SBT能够追踪来历以防止深度伪造相同，SBT 的社交图谱描绘了“热门作品”的源头。“热门作品”本质上是在受害者社区（反映为共享的 SBT 成员身份）之外产生的制品，或者没有受害者社区的 SBT来验证，这足以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击，以反制在其信任网络（为共同持有 SBT 的模式所代表）中策划和传播的攻击。通过维持社会背景，人们可以保持信任，即使他们面临取消文化的威胁，并可追究攻击者的责任。真相的社会基石，也就随着可溯源度的提高而改善。

8.3 人格证明（PoP）

人格证明协议 (PoP) 的目标是，提供具有个人唯一性的代币，以防止女巫攻击，并赋能非金融的应用程序。为此，其依赖社交图谱的全局分析、生物识别、同步的全球关键当事人及其不同组合的方法。然而，由于 PoP 协议寻求代表*个人身份识别*，专注于实现*全球唯一性*，而不是反映社会关系和联结的*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（例如声誉质押）都是要求关联的，并且不是要成为一个具有唯一性的人，而是成为一个*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 系统都实际上地对女巫攻击开放，只是成本略高。除非地球上的大多数人都注册 PoP 服务并参与特定的认证活动，否则攻击者总是可以招募尚未参与的无利害关系人充当女巫。虽然这样的雇佣兵并不完全是机器人，但差别只是表面的，除了可能增加的一小部分费用。

许多 PoP 协议旨在为无条件基本收入或全球民主建立基础。尽管我们没有相同的野心，但这些协议促使我们考虑，如何分步建设，促成多元网络产品的协同。与 PoP 的二元、个人主义和全球性相比，我们的方法旨在为自下而上的声誉、财产和治理

构建一个丰饶的、与社会背景相关的和分层的基础，使得人们能参与各种规模的社区和网络。

8.4 可验证的资质证明

可验证的资质证明 (VC) 是 一种W3C 标准，其中资质证明（或认证）是可以零知识共享的，共享与否由持有人自行决定。VC 突出了我们底线隐私方法的主要局限性，并启发了我们在上面对隐私外延的讨论。在 SBT 具有能缩小曝光范围的隐私外延之前，VC 和SBT可以被自然而然地视为有互补性：特别是，SBT 最初是公开的，因此它们不适用于政府颁发的身份证明等敏感信息，而 VC 一直在努力寻找一种现在可由社区恢复来解决的恢复方案。在短期内，将这两种方法结合起来可能比单独使用任何一种方法要强大得多。但是VC也有一个重要局限：起码按它们的标准化形式，VC 不支持我们列举的大多数应用程序，原因是它们的*单方面*隐私性。

单边零知识共享与我们所举的应用场景的激励机制并不兼容，也不符合我们提出的隐私规范。我们的大多数应用程序都依赖于一定程度的信息披露。但是在零知识共享下，灵魂无法知道另一个灵魂拥有 SBT，除非其被共享予他们，这使得声誉抵押、可信承诺、抗女巫治理和简单租约（如公寓租约）无法实现，因为该灵魂做出的其他承诺和产权负担是不一定可见的。更深入地说，我们怀疑单边零知识共享并非合适的隐私方案。多方关系中的一方很少有未经另一方同意而单方面披露其关系的权利。正如单方面可转让的私有产权并不是丰富的产权制度一样，简单的单边共享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，则这种资质证明将无法实现相互同意和相互许可。这个问题涉及到更复杂

的多元产权以及复杂组织形式和许可的情形，而这正是DeSoc的一项特点。

§9 灵魂诞生

从当前的 Web3 生态系统迈向由 SBT调整的增强社交关系之路，面临着常见的冷启动困难。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，他们需要跨不同社区的多种 SBT 来保证安全。**哪个会最先到来：SBT 还是社区恢复**？早期采用者社区会是谁？不同链上的 SBT 如何互操作？我们不能指望穷尽所有的可能性和答案，而是为读者勾勒出一些有前景的路径，方便其在当前的 Web3 甚至 Web2设施中进一步探索。

9.1 SBT原型

尽管 SBT 的标志是不可转让性，但 SBT 也可能具有另一个属性，在冷启动中可能更有用：*可撤销性*。 有可能初代SBT是可撤销、可转让的代币，其后才发展出不可转让性。如果发行者可以销毁代币，并将其重新发行到新钱包，则代币就是可撤销的。例如，当密钥丢失或泄露时，烧毁和重新发行是有意义的，并且发行人有利益确保代币不会被金融化及出售给别人，比如当代币表明真正的社区成员身份时。具有重复链下互动关系的雇主、教堂、聚会团体、俱乐部很容易销毁和重新发行代币，因为它们与这人有关系，并且很容易可以通过电话、视频会议或亲自见面来排除冒充。单一的互动，例如参加一次音乐会或会议，则不太适合，因为社区纽带较弱。

可撤销、可转让的代币是一种SBT原型，在灵魂出生之前提供给养性的胎盘功能。这些代币为钱包争取时间来孕育安全的社区恢复机制，并让人们充分累积SBT原型，这些原型最终可被烧毁并重新发行为不可转让的SBT 。在这条路径下，问题不是"哪个会最先发生：SBT 还是社区恢复？"而是，SBT 和社区恢复同时落地，生出了一个灵魂。

9.2 社区恢复钱包

尽管今天的钱包缺乏社区恢复能力，但它们各有优劣，可以成为 SBT 的家，或者孕育它的子宫。人格证明 (PoP) 协议的优势在于已经在社会争议解决机制方面先行先试，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 的第一个发行者。不过，尽管 PoP 有先发优势，PoP 协议尚未赢得广泛信任来存放有价代币资产，而托管钱包则有这些信任。

托管钱包，尽管它们有中心化的缺点，会以更少的成本为不专业的散户提供一个顺滑的入口。此类托管钱包还可以为散户社区提供工具，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，其中许多企业正在寻找在 Web3 建立忠诚客户群的方法，但缺乏托管方面的专业知识。一旦社区恢复机制正式确立，并经过实战考验，这些托管钱包可以去中心化到社区恢复中，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）。

对于更专业的 Web3 用户，去中心化的非托管钱包（或非托管的社交恢复钱包如 Argent和 Loopring ）是启动社区恢复机制的

自然起点。非托管钱包具有原生 Web3 开源的优势，以及可以灵活地将机制予以预先公布并分步试验，让自愿参与的专业用户对激励机制和混合机制（如多签名）进行实战测试。所有这些方法（PoP、托管和非托管），在测试和启动不同专业度和风险承受能力的用户方面，发挥着重要作用。

9.3 灵魂原型

规范也可以引领灵魂的诞生。在审视代币和钱包时，我们还可重塑对用以表明成员身份的某类NFT和代币的看法。特别是，我们可以引入规范，规定由信誉良好的机构颁发的，反映参会记录、工作经验或学历证书的 NFT和POA不得转让。成员身份代币的转让，如果是有价交易，会降低钱包的声誉，并可阻碍发行人进一步向该钱包发行成员身份或 POAP代币。非托管生态系统中的大量用户，其钱包已获得了可观的财务声誉和利益，可引导他们将其作为有效的抵押品，避免遭致他们对不可转让性的反抗。

虽然这些路径都有各自的困难，但方法越多，通过一些小步骤达成中期的准平衡状态的机会就越大。

§10 结论

尽管我们一直在想象 DeSoc 可以实现什么，但不管怎样，以上都只是第一步。条条大路通DeSoc，包括许多基于非区块链的框架，如Spritely、 ACDC和Backchannel ，其依赖本地机器上而不是全球帐本中的数据集。这些框架最终可提供跨社交距离的更多信任，因为它们可以利用信任关系的可传递性，比如受信任的介绍，而不是依赖知名的、地位高的机构（如大学或

DAO）发行的 SBT。此外，我们上面描述的应用，只是 DeSoc 能够实现的东西的发端，而虚拟世界还尚未涉及：它们的物理、社会以及它们与现实世界的复杂交汇。所有这些都表明，即使是我们在上面描绘的勃勃雄心，也只不过是 DeSoc 终极面貌的端倪而已。

然而，在这条道路上，仍然存在许多挑战和悬而未决的问题。上面的草图需要大量的红队测试，其中许多方案只是建议，并非规定。DAO 如何在保持其状态信息公开的同时，详细比较各灵魂的行为模式和各SBT的关联度，以执行抗女巫攻击保护措施和去中心化？在各种关联度降权方案下，如何获取SBT 的激励兼容性？隐私与关联度降权和其他 DeSoc 机制有多少冲突？我们如何以一种既社交又私人（统一于社会背景下）的适当方式来衡量不平等？继承权在社区恢复框架中如何有效？协议中是否划定甚至融入一些红线，以避免出现地狱乌托邦情形？还是我们只应该把最好的场景先建起来再说？这些问题只是我们研究议程的开始，这些研究将跨越数年，与 DeSoc 生态系统共同发展。

不过，DeSoc 有如此的潜力，似乎不仅值得我们枕戈待旦未雨绸缪，更可能是我们生存所必不可少的保证。阿尔伯特·爱因斯坦在 1932 年裁军会议上说，“人类组织能力”跟不上“其技术进步”的步伐，就如同让“一个 3 岁小孩手持一把剃刀”。在这一论断貌似比以往任何时候都更有先见之明的世界里，学习如何通过编程把*社交关系*编码进未来，而不是纸上谈兵讲信任，似乎是人类在这个星球上生存下去的必修课。

附录：先验协作的二次方调整机制（从略）

尾注：

[1]我们感谢 Audrey Tang、Phil Daian、Danielle Allen、Leon Erichsen、Matthew Prewitt、Divya Siddarth、JaronLanier 和 Robert Miller 的深思熟虑的反馈和评论。所有的错误和观点都是我们自己的。

[2]E. Glen Weyl，微软公司和 RadicalXChange基金会，glen@radicalxchange.org。格伦将本文链接到他的灵魂。

[3]Puja Ohlhaver, Flashbots有限公司， puja@ashbots.net。Puja将这篇论文献给她的祖母 Satya，她的爱和光将永远照耀着许多灵魂。

[4]Vitalik Buterin, 以太坊基金会，vitalik.buterin@ethereum.org。

[5]我们选择这组属性不是因为它们明显是最理想的特性，而是因为它们易于在当前环境中实施，并实现重要的功能。我们在第 5.3 节将探讨可编程的私有 SBT。

[6]但是请注意，原则上法定名称可以表示为 SBT：姓可以是家族的成员SBT，而名可以是父母给孩子的礼物SBT。事实上，更丰富的名称概念也很容易表示，比如，其他宗亲或亲缘关系可将成员SBT 授予给新生儿。

[7]参见 https://twitter.com/VitalikButerin/status/1264948490834247 6

81 和 https://twitter.com/VitalikButerin/status/1265252184813420544中的非正式Twitter 民意调查证据，表明人们已经发现，在决策机制中引入多样性考量的想法是很自然的。

[8]我们谓之“无意”，是因为高度合作的群体会自然而然地寻求增进利益，且很可能是为了*他们的*集体福祉。

[9]根据二次方规则，团队成员可以购买一份合约，该合约在特定事件发生时支付 $X，但成本为 $(X^2)/2。例如，某人设定 X=0.5 ，在事件发生时，其将获得 0.5 美元（由设注者支付），但其支付的成本无论如何都只有 0.125 美元。

[10]如某人评估概率为 p，其预期收益是 pX，成本是 X^2/2。取关于 X 的导数，假设风险中性，最优条件是 p=X，这对于小额赌注是合适的（收益和成本都可以任意缩小或放大，都同样成立）。