缩小范围并提出一个更广泛的问题是值得的：一般来说，在非金融应用中使用区块链有什么意义？我们是否应该走向这样一个世界：**即使是去中心化的聊天应用程序，每一条消息都是包含加密消息的链上交易？或者，区块链是否只对金融有好处（例如，因为网络效应意味着资金对“全球视野”有着独特的需求），而所有其他应用最好使用中心化或更多本地系统来完成？**

我个人的看法倾向于，就像区块链投票一样，我们要远离“区块链无处不在”的观点，也要远离“区块链极简主义”（blockchain minimalist）。我在很多情况下都看到了区块链的价值，有时是为了真正重要的目标，比如「信任」和「抗审查」，但有时纯粹是为了方便。这篇文章将试图描述区块链可能有用的一些类型情况，特别是身份方面，以及它们不那么有用的地方。这篇文章并不是一个完整的列表，其中故意遗漏了很多东西，文章的目的是阐明一些常见的用例类别。

用户账户密钥更改和恢复

加密帐户系统中最大的挑战之一是密钥更改问题。在以下几种情况下可能会发生：

1、你担心当前密钥可能丢失或被盗，因此希望切换到其他密钥；

2、你想切换到另一种加密算法（例如，因为你担心量子计算机很快就会出现，你想升级到后量子加密算法）；

3、你的密钥丢失，你想重新访问自己的账户；

4、你的密钥被盗，你希望重新获得对自己账户的独占访问权限（你不希望小偷也能访问）；

[1] 和 [2] 相对简单，因为它们可以完全自主的方式完成：你控制密钥 X，你想切换到密钥 Y，所以你发布了一条用 X 签名的消息，上面写着“从现在开始用 Y 验证我”，然后所有人都接受了这一点。

但请注意，即使对于这些较简单的密钥更改场景，你也不能仅仅使用密码学。考虑以下事件顺序：

1、你担心密钥 A 可能被盗，所以你在一条消息上签名说“我现在使用 B”；

2、一年之后，一名黑客确实盗取了密钥 A，其用密钥 A 签署了一则消息，上面写道“我现在使用 C”，其中 C 是黑客自己的密钥；

从后来刚收到这两条消息的人的角度来看，他们看到 A 不再被使用，但他们不知道“用 B 替换的 A”和“用 C 替换 A”的优先级哪个更高。

这相当于设计去中心化货币时会遇到的著名的双花问题，除了目标不是防止以前的 token 持有者能够再次发送它，这里的目标是防止以前控制账户的密钥能够更改密钥。就像创建去中心化的货币一样，以去中心化的方式进行账户管理，也需要像区块链这样的东西。区块链可以为密钥更改消息添加时间戳，提供关于 B 或 C 先出现的共同知识。

而 [3] 和 [4] 会更难。一般来说，我自己首选的解决方案是「多重签名」以及「社交恢复钱包」，如果你的账户丢失或被盗，一群朋友、家人和其他联系人可以将你的账户控制权转移到新的密钥。对于关键操作（例如转移大量资金，或者签署一个重要合约），也可能需要该小组的参与。

而这也需要区块链。使用秘密共享技术进行社交恢复是可能的，但在实践中会更难：如果你不再信任你的某些联系人，或者如果他们想要更改自己的密钥，那么你无法在不更改密钥的情况下撤消访问权限。所以我们又回到了要求某种形式的链上记录。

DeSoc（去中心化社会）论文中的一个微妙但重要的想法是，为了保持不可转让性，个人资料的社交恢复（或“社区恢复”）实际上可能需要强制执行。也就是说，即使你出售自己的账户，你也可以随时使用社区恢复来取回账户。这将解决一些问题，比如没有名气的司机在乘车共享平台上购买经验证的账户。也就是说，这是一个推测性的想法，不必完全实施即可获得基于区块链的身份和声誉系统的其他好处。

请注意，写到这里，这只是区块链的一个有限用例：**在链上拥有账户，但在链下做所有其他的事情，这是完全可以的。**有一个地方可以容纳这种混合愿景，使用以太坊登录是一个很好的简单示例，说明了如何在实践中做到这一点。

修改和撤销证明

爱丽丝（Alice）去了 XX 学院并获得了 XX 研究学位，她获得了一个数字记录来证明这一点，上面有 XX 学院的密钥签名。不幸的是，六个月后，XX 学院发现爱丽丝（Alice）存在大量抄袭行为，并撤销了她的学位。但爱丽丝继续使用她的旧数字记录，并到处向不同的人和机构声称她拥有这个学位。潜在地，证明甚至可以带有一些权限（例如，登录学院在线论坛的权利），而爱丽丝也可能试图不恰当地访问它。我们如何防止这种情况发生？

“区块链极简主义”的方法，是让学位成为链上 NFT，这样 XX 学院可以发布链上交易来撤销这个 NFT。但这种方式是昂贵的，也许并不必要（发行很常见，但撤销很少，如果不需要的话，我们不想要求 XX 学院 为发行交易支付费用）。所以我们可以使用一种混合解决方案：**使初始学位成为链外签名消息，并在链上进行撤销，**这是 OpenCerts 使用的方法。

完全链外的解决方案，也是很多链外可验证凭证支持者所提倡的解决方案，即 XX 学院运行一个服务器，他们在其中发布撤销的完整列表（为了改善隐私，每个证明都可以附带一个 nonce，撤销列表可以只是一个 nonce 列表）。

对于一所大学来说，运行服务器并不是一个很大的负担。但对于任何较小的组织或个人来说，管理“另一个服务器脚本”并确保它保持在线对 IT 人员来说是一个巨大的负担。如果我们告诉人们出于对区块链的恐惧而“只使用服务器”，那么可能的结果是每个人都将任务外包给一个集中的供应商。最好保持系统去中心化，只使用区块链，尤其是现在 rollup、分片和其他技术终于开始上线，从而使区块链的成本越来越便宜。

负面声誉（Negative reputation）

链下签名不够用的另一个重要领域是负面声誉，即，你正在对其进行认证的个人或组织可能不希望你看到相关证明。我在这里使用“负面声誉”这个词作为技术术语：最明显的动机用例是证明某人的坏话，比如糟糕的评论或某人在某些情况下滥用行为的报告，但也有一些用例的情况下，“负面”证明并不意味着不良行为，例如，申请贷款并想证明你没有同时申请过太多其他贷款。

对于链外声明，你可以获得正面的声誉，因为让声明的接收者看起来更有信誉（或提供 ZK 证明）符合他们的利益，但你不能获得负面声誉，因为有人总是可选择只展示让他们看起来不错的声明，而忽略其他所有声明。

在这里，在链上进行认证确实可以解决问题。为了保护隐私，我们可以添加加密和零知识证明：证明可以是一个链上记录，数据加密到收件人的公钥，用户可以通过运行遍历链上记录的整个历史的零知识证明来证明缺乏负面声誉。链上的证明以及区块链验证过程可以很容易地验证证明确实遍历了整个历史，并且没有跳过任何记录。为了使这种计算可行，用户可以使用增量可验证计算（如 Halo）来维护和证明已加密的记录树，然后在需要时显示树的某些部分。

负面声誉和撤销证明在某种意义上是等价的问题：你可以通过添加另一个负面声誉证明来撤销一个证明，并说“另一个证明不再重要”，你可以通过背负正面声誉来实施负面声誉撤销：爱丽丝（Alice）在 XX 学院的学位可以被撤销，取而代之的学位是“爱丽丝获得了 XX 研究学位，但她借用了其他人的成果”。

负面声誉是个好主意吗？

我们有时会听到一种对负面声誉的批评：但负面声誉难道不是一种反乌托邦的“红字”计划吗？我们不应该尽最大努力用正面声誉来做事吗？

在这里，虽然我支持避免无限负面声誉的目标，但我并不同意完全避免负面声誉的想法。负面声誉对于很多用例来说都是很重要的。无论是区块链领域，还是非相关领域，「无抵押借贷」对于提高资本效率而言都是非常有价值的，这显然会从负面声誉中受益。Unirep

Social 展示了一个概念验证社交媒体平台，该平台将高度匿名性与保护隐私的负面声誉系统相结合，以限制滥用行为。

有时，负面声誉可能会增强力量，而正面声誉可能具有排他性。比如一个网络论坛，每个独特的人都有权发帖，直到他们因行为不端而受到太多的“打击”，这比一个首先需要某种“良好品格证明”才能被接纳并允许发言的论坛更为平等。而那些生活在“系统外”的边缘化人群，即使他们实际上品行良好，也很难得到这样的证明。

一些人还可能会考虑性工作者客户匿名声誉系统的案例：你想保护隐私，但你也可能想要一个系统，如果客户虐待性工作者，他们会得到一个“黑印记”，这可以提醒其他工作者更加小心或远离这些客户。这样，难以掩饰的负面声誉实际上可以增强弱势群体的能力，以保护她们的安全。这里的重点不是为负面声誉的某些具体计划辩护，相反，这是为了表明负面声誉释放出的真正价值，一个成功的系统需要以某种方式予以支持。

负面声誉不一定是无限的负面声誉：我想说的是，总是有可能以一定的成本创建一个新的个人资料（可能牺牲很多或所有现有的正面声誉），问责过少与问责过重之间存在一种平衡。**但首先，拥有一些能够让负面声誉成为可能的技术，是打开这个设计空间的先决条件。**

致力于稀缺性

区块链存在价值的另一个例子，是发布数量有限的证明。如果我想为某人做背书（例如，有人可能会想象一家公司正在找工作，或者一个政府签证计划正在查看此类背书），查看背书的第三方会想知道我对背书是否谨慎。

这个问题的理想解决方案是公开背书，这样背书就与动机相一致：如果我背书的人最终被证明做了错事，那么将来每个人都可以对我的背书打折扣。但通常，我们也希望保护隐私。因此，我可以做的是在链上发布每个背书的哈希值，这样任何人都可以看到我给出了多少。

一个更有效的用例是单次多发行（ many-at-a-time issuance）：如果艺术家想要发布 N 份“限量版”NFT，他们可以在链上发布一个包含他们正在发布的 NFT 的 Merkle 根的哈希。单次发布可以防止他们在事后发布更多的 NFT ，你可以将表示数量限制的数字（例如 100）与 Merkle 根一起发布，表示只有最左边的 100 个 Merkle 分支有效。

通过在链上发布单个 Merkle 根和最大计数，你可以提交数量有限的证明。在这个示例中，只有五个可能的有效 Merkle 分支可以满足证明检查。精明的读者可能会注意到，这与 Plasma 链在概念上的相似之处。

共同知识（Common Knowledge）

区块链的一个强大特性是它们创造了共同的知识：如果我在链上发布了一些东西，那么 Alice 可以看到它，Alice 可以知道 Bob 可以看到它，Charlie 可以知道 Alice 知道 Bob 可以看到它，等等。

共同的知识对于协调往往很重要，例如，一群人可能想就一个问题发表意见，但只有当他们有足够多的人同时发表意见，并且他们的人数安全时，他们才会觉得这样做很舒服。一种可能的方法是让一个人围绕特定声明启动一个“承诺池”，并邀请其他人发布表示他们同意的哈希（最初是私有的）。只有在一段时间内有足够多的人参与，所有参与者才会被要求公开他们的下一条链上消息，以表明他们的立场。

这样的设计可以通过零知识证明和区块链的组合来完成（这可以在没有区块链的情况下完成，但需要见证加密（目前尚不可用），或者需要可信硬件（存在严重问题的安全假

设））。围绕这类想法有一个很大的设计空间，目前还没有得到充分的开发，但一旦区块链和加密工具周围的生态系统进一步发展，就很容易开始增长。

与其他区块链应用的互操作性

这很简单：有些东西应该在链上，以便更好地与其他链上的应用互操作。人类证明（Proof of humanity）作为一种链上 NFT，使项目更容易实现自动空投或将治理权授予具有人类证明档案的帐户。链上的预言机数据使 defi 项目更容易读取。在所有这些情况下，区块链并没有消除对信任的需求，尽管它可以容纳管理信任的 DAO 等结构。但是，链上提供的主要价值只是与你正在与之交互的东西在同一个地方，出于其他的原因，这需要区块链。

当然，你也可以运行一个链外预言机，并要求仅在需要读取数据时才导入数据，但在许多情况下，这实际上会更加昂贵，并且不必要地给开发人员带来复杂性和成本。

开源指标

去中心化社会论文的一个关键目标是，应该能够对证明图进行计算。一个非常重要的问题是衡量去中心化和多样性。例如，很多人似乎都同意，理想的投票机制会以某种方式考虑到多样性，不仅给那些获得最多币甚至最多人支持的项目更大的权重，还赋予那些得到最多不同视角支持的项目更大的权重。

Gitcoin Grants 中实施的二次方融资还包括一些明确的有利于多样性的逻辑，以减轻攻击。

另一个衡量和分数有价值的地方是声誉系统，这已经以评级的集中形式存在，但它可以更加去中心化的方式完成，其中算法是透明的，同时保留更多的用户隐私。

除了像这样的紧密耦合用例，即试图衡量某一组人之间的联系程度并将其直接输入一个机制之外，还有更广泛的用例来帮助社区了解自己。在衡量去中心化的情况下，这可能是一个确定集中度过高的领域的问题，这可能需要一个回应。在所有这些情况下，在大量的证明和承诺上运行计算机化算法，并用输出做真正重要的事情将是不可避免的。

我们不应该试图废除量化指标，而是应该尝试做出更好的指标

Kate Sills 对根据声誉进行计算的目标表示怀疑，这一论点既适用于公共分析，也适用于个人 ZK 证明他们的声誉（如在 Unirep Social 中）：

“对声明进行评估的过程非常主观，并且与上下文相关。人们自然会对他人的可信度产生分歧，而信任取决于环境...[正因为如此] 我们应该对任何“计算”声明以获得客观结果的提议，持极端怀疑态度。”

在这种情况下，我同意主观性和背景的重要性，但我不同意更广泛的主张，即完全避免围绕声誉进行计算是正确的目标。纯粹的个人化分析的规模不会远远超过邓巴数，任何试图支持大规模合作的复杂社会，都必须在一定程度上依赖于聚合和简化。

也就是说，我认为一个开放参与的证明生态系统（与我们今天的中心化证明生态系统相反）可以通过为更好的指标开辟空间来让我们两全其美。以下是此类设计可以遵循的一些原则：

1、主体间性（Inter-subjectivity）：例如，声誉不应该是一个单一的全球分数，相反，它应该是一个更主观的计算，这涉及被评估的人或实体，还包括查看分数的观众，甚至可能涉及当地环境的其他方面。

2、可信的中立性：该计划显然不应该为强大的精英留下空间，让他们不断地为自己的利益而进行操纵。实现这一点的一些可能方法，是最大的透明度以及算法的不频繁更改。

3、开放性：能够做出有意义的输入，并通过自己运行检查来审核他人的输出，这应该对任何人开放，而不仅限于少数强大的群体。

如果我们不创建良好的大规模社会数据聚合体，那我们就有可能将市场份额拱手让给不透明和中心化的社会信用评分系统。

并非所有数据都应该在链上，但以公共知识（Common Knowledge）的方式公开一些数据有助于提高社区自身的易读性，而不会造成可能被滥用以进行集中控制的数据访问悬殊。

作为数据存储

这是一个真正有争议的用例，即使在那些接受大多数其他用例的人当中也是如此。区块链领域有一个共同的观点，即区块链只能在真正需要和不可避免的情况下使用，而对于其他任何地方，我们都应该使用其他工具。

在一个交易费用非常昂贵、区块链效率极其低下的世界里，这种态度是有道理的。但在区块链实现 rollup 和分片技术后（交易费用可以降低到几美分），那这种看法的意义已经不大了，而且区块链和非区块链去中心化存储之间的冗余差异可能只有 100 倍。

即使在这样的世界中，将所有数据都存储在链上也没有意义。但如果是小的本文记录呢？绝对是有必要的，为什么？因为区块链是一个非常实用的存储东西的地方。我在 IPFS 上保留了一份这篇博文的副本，但上传到 IPFS 通常需要一个小时，它需要中心化网关让用户以接近网站延迟水平的任何东西访问它，并且有时文件会丢失并且不再可见。另一方面，将整个博客转储到链上，将完全解决这个问题。当然，博客太大了，实际上无法在链上转储，即使是实施分片后，也是如此，但同样的原则也适用于较小的记录。

将数据存储上链可能是正确决定的一些小例子包括：

1、增强的秘密共享：将你的密码分成 N 个片段，其中任何 M = N–R 个片段都可以用于恢复密码，但你可以选择所有 N 个片段的内容。例如，这些片段可能都是密码的哈希值、通过其他工具生成的秘密或安全问题的答案。这是通过在链上发布额外的 R 个片段（看起来是随机的），并在整个集合上进行 N–of–(N+R) 秘密共享来完成的。

2、ENS 优化。通过将所有记录组合成一个哈希，只在链上发布哈希，并要求任何访问数据的人从 IPFS 中获取完整数据，从而可以提高 ENS 的效率。但这将显著增加复杂性，并增加另一种软件依赖性。因此，即使数据长度超过 32 字节，ENS 也能将数据保存在链上。

3、**社交元数据。**连接到你的帐户的数据（例如，用于以太坊登录目的），这是你希望公开且长度非常短的数据。对于更大的数据（例如头像图片），这通常是不正确的（尽管如果图片恰好是一个小的 SVG 文件，那它可能是！），但对于文本记录来说，情况确实如此。

4、**证明和访问权限。**特别是如果要存储的数据长度小于几百字节，将数据存储在链上可能比将哈希放在链上和将数据放在链下更方便。

在很多这样的情况下，权衡的不仅仅是成本，还有那些密钥或密码学被破坏的边缘情况下的隐私。有时，隐私只是有点重要（偶尔会因为泄露密钥或遥远的量子计算幽灵而失去隐私），这与高度确定数据将保持可访问性相比没有那么重要。毕竟，存储在“数据钱包”中的链外数据也可能遭到黑客攻击。

但有时，数据会特别敏感，这可能是反对将其置于链上并将其作为第二层防御存储在本地的另一个论据。但请注意，在这些情况下，隐私需求不仅是反对区块链的理由，也是反对所有去中心化存储的理由。

结论

在上面的列表中，我个人迄今最有信心的两个用例是**与其他区块链应用的互操作性**以及**账户管理。**第一个已经在链上了，而第二个会相对更便宜（每个用户只需要与链交互 1 次，而不是每个操作交互 1 次），情况是很清楚的，并且确实没有一个好的基于非区块链的解决方案。

负面声誉和撤销也很重要，尽管它们仍然是相对早期的用例。通过仅仅依靠链外正面声誉，我们可以在声誉方面做很多事情，但我预计，随着时间的推移，撤销和负面声誉的用例会变得更加明显。我预计会有人尝试使用中心化服务器来做到这一点，但随着时间的推移，人们应该清楚地看到，区块链是避免在不便和中心化之间做出艰难选择的唯一途径。

区块链作为短文本记录的数据存储用例可能是微不足道的，也可能是重要的，但我确实希望至少有一些这样的使用会继续发生。区块链对于廉价和可靠的数据检索确实非常方便，无论应用有 2 个用户还是 200 万用户，都可以继续检索数据。**开源指标**仍然是一个非常早期的想法，它仍然需要看看在不被利用的情况下可以做多少事情并使之公开（例如在线评论、

社交媒体等一直在被利用）。**共同知识（Common Knowledge）**游戏需要说服人们接受社会重要事物的全新工作流，所以这当然也是一个早期想法。

我在很大程度上不确定这些类别中非金融区块链的使用水平到底有多大意义，但很明显，区块链作为这些领域的支持工具不应该被忽视。

NFT数字藏品热度居高不下，
对NFT的监管也逐步落实。
在国内发售及购买数字藏品，
哪些环节会涉及法律风险？

明晚8点，
听行业知名法律人肖飒律师怎么讲，
详情戳下方海报~