去中心化金融的承诺与陷阱

如能克服有关挑战，去中心化金融将可支持一种全新的金融基础设施

法比安·沙尔

数字创新为金融体系带来了重大改进。但金融体系的架构基本仍维持不变。它仍然是中心化的。

去中心化金融（DeFi）提供了另一种选择。它使用公共区块链网络进行交易，无需依赖托管机构、中央票据交换所或托管代理等中心化的服务提供商。相反，这些角色由所谓的“智能合约”承担。

智能合约是计算机代码形式的指令。该代码存储在公共区块链上，并作为系统共识规则的一部分被执行。去中心化金融的协议在设计上可以禁止干预和操纵。在所有参与者参与并验证一切得到妥善执行前，他们都可遵守这些规则。状态的改变（如账户余额的更新）会被反映在区块链上，任何人都可以验证。

[illegible]

图片来自ISTOCK/ANNA BLIOKH

性”转让（即这种转让同时发生，不可分割），或是在托管账户中持有抵押品。在这两种情况下，资产都受智能合约规则的约束。只有在满足预定义的条件时，才予以放行。

通过利用这些特性，去中心化金融可以降低交易对手风险并复刻出众多的金融服务，且无需中介机构和中心化平台运营商参与其中。这可降低成本和出错的概率。借贷市场、交易协议、金融衍生品、资产管理协议只是众多例子中的一小部分。

智能合约可将其他智能合约作为参考，并利用它们提供的服务。例如，如果资产管理协议使用去中心化的交易所，则可将传入的资产作为同一交易的一部分进行置换。这种多个智能合约在同一交易中发挥作用的概念，被称为“交易内的可组合性”，其可以有效地降低交易对手风险（也将其他交易方无法完成交易的概率）。

去中心化的好处

在那些通常会被归结于去中心化金融（或更一般的区块链技术）所带来的优势中，有许多也可通过中心化的基础设施来实现。智能合约不仅限于去中心化系统。事实上，相同的标准和执行环境也可用在中心化的分类账上。以太坊虚拟机（它是一个在区块链网络中所有计算机上运行并执行智能合约的虚拟机）与高度中心化的共识协议被一起使用的例子不胜枚举。同样，相同的代币标准和金融协议也可在中心化的平台上使用。这些系统甚至也可以实现“可组合性”。

此外，管理良好的中心化系统比公共区块链的效率要高得多。这可能会得出一个结论，即公共区块链和去中心化金融比不上中心化的系统。

然而，中心化系统建立在一个很强的假设之上，即对很大程度上不透明的中介和机构的信任。但这种信任不应被视为理所当然。历史中存在无数机构内部腐败和发生错误的例子。但当经济学家们讨论金融基础设施，并将公共区块链的特点与中心化账本进行比较时，他们通常会认为中心化实体是好的，因而很难看到去中心化的好处。

公有链是透明的。由于其不受单一实体的控制，它们可以为金融交易提供一种中立、独立和不可改变的基础设施。有关代码在一个开放系统上存储和执行。所有数据都是人人可得且可验证的。这使研究人员和政策制定者能够实时地分析交易、进行实证研究并计算风险指标。

最重要的是，访问不受限制。这有两个影响。

首先，由于不存在访问限制，其能提供一个中立的基础，不会因用例或利益相关方不同而区别对待。这与受许可账本形成了鲜明对比——受许可账本的规则由中心化实体制定。其中心化程度如此之高，很难达成一个各方都普遍接受的标准，且访问和使用这种基础设施的权利很容易被政治化。考虑到这些问题，那些认为中心化基础设施可能对其不利的参与者就不会在一开始使用它们。去中心化系统可以缓解这些阻碍，潜在地避免了合作不足（甚至不合作）的问题。

其次，去中心化金融是建立在分层的基础设施之上的（参见Schär，2021年）。账本的去中心化并不意味着建立在其之上的一切都必须也是去中心化的。可能存在充分的理由对某些代币或金融协议的访问设定限制，或是允许对其进行干预。这些限制可以在智能合约的层面上执行，而不会损害底层基础设施的一般中立性。然而，如果账本本身（结算层面）已经是中心化的，那就不可能可信地实现在其之上的任何东西的去中心化。

我们很可能会看到一种向结合了支付、代币化资产和金融协议的账本的转变，如交易所和借贷市场。去中心化金融是这种趋势的第一个例子，但中心化的基础设施也会出现类似的趋势。其基本原理在于，“交易内的可组合性”只有在资产和金融协议位于同一分类账上时才是可行的。网络效应是十分强大的，而且，如果加密资产和央行数字货币被部署在缺乏其他资

中心化系统建立在一个很强的假设之上，即对中介和机构的信任。

产或金融协议的分类账上，它们就不会特别令人信服。使用额外的资产和金融协议来建立一个“可组合”的中心化基础设施是可能的，但考虑到受许可账本的相关挑战，这将是有风险且难以管理的。这为去中心化提供了一个有力的理由。

挑战与风险

去中心化金融具有多种优势，但存在一些挑战和权衡取舍问题需要考虑。

首先，存在出现骗局的风险（即“去中心化剧场”，指表面去中心化，但实际上为中心化）。实际上，一些被称为去中心化金融的事物往往是高度中心化的。在许多情况下，区中心化金融的协议受需要满足中心化的数据馈送，且可能受到具有“管理员密钥”或高度中心化的治理令牌分配（投票权）的人的影响。虽然部分中心化不一定是坏事，但重要的是要严格区分真正的去中心化企业和声称自己去中心化、实际上却提供中心化基础设施的企业。

其次，不可改变性会带来新的风险。实施投资者保护可能变得更难，智能合约的编程错误也可能带来毁灭性的后果。“可组合性类”以及类似于抵押品再抵押的复杂的代币包装方案（Nadler和Schär，待发布）能促进系统中冲击的传播，并可能影响实体经济。

再次，从隐私角度来看，区块链的透明性和去中心化的区块创建可能存在问题。此外，它允许通过一般化的提前运行来提取租金——这种现象被称为“矿工/最大可提取价值”（MEV）。那些在去中心化交易所中观察到某一交易包含了交换资产订单的人，可以尝试通过发起自己的交易来抢先行动，这被称为“三明治套利交易”。先行者将获利，而原始交易的发起人将承受损失。有一些潜在的方案至少可以部分缓解这一问题，但这需要做出权衡取舍。

最后，在不损害其一些独特属性的情况下，是无法轻松实现公共区块链的扩展的。创建去中心化区块会带来高昂的成本，这在一定程度上是由高额的交易费来支付的。确保每个人都可验证交易，会导致运行节点所需的硬件存在一定的上限，而这会限制链上可扩展性并导致高昂的交易费用。这种在安全性、去中心化和可扩展性之间的权衡取舍关系，通常被描述为一种“三难选择”。一个潜在的解决方法是所谓“第二层解决方案”（Layer 2）。其旨在将一些负担从区块链中移开，同时允许参与者在出现错误时在区块链上行使其权利。这是一种前景良好的方法，但其在许多情况下仍需要信任和各种形式的中心化基础设施。

去中心化金融仍然面临着许多挑战，但其仍可创建独立的基础设施，减轻传统金融的一些风险，并在过高程度的中心化之外提供另一种选择。去中心化金融的开源特性能鼓励创新，且有许多才华横溢的人（包括学者和从业人士）都在致力于应对这些挑战。如果他们能够在不破坏去中心化金融的独特核心属性的情况下找到解决方案，其就可能成为未来金融的一个重要组成部分。 FD

法比安·沙尔（FABIAN SCHÄR）是巴塞尔大学研究分布式账本技术和金融科技的教授兼创新金融中心的总经理。

参考文献：

Schär, Fabian. 2021. “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets.” *Federal Reserve Bank of St. Louis Review* 103 (2): 153–74. https://doi.org/10.20955/r.103.153-74.

Nadler, Matthias, and Fabian Schär. Forthcoming. “Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution.” *Journal of Blockchain Research*. https://arxiv.org/abs/2012.09306.