

DeFi初学者指南

去中心化金融，亦称“DeFi”或开放式金融，它的作用是采用自动化的方式取代中间商，重建传统金融系统（例如借贷、衍生产品和交易所）。一旦实现完全自动化，DeFi的金融构件可以生成更复杂的功能。今天，去中心化金融的主要应用在以太坊上，但原则上，DeFi可以应用在所有智能合约平台上。

在本篇DeFi新手指南中，我们将回顾以下内容：

- **稳定币**，是去中心化金融的基础。与以价格波动而出名的比特币或以太坊等加密货币不同，稳定币经过精心设计，在1.00单位法币上保持“稳定”。大多数稳定币都与美元挂钩，但有些稳定币是与其他法币挂钩，例如人民币。
- **去中心化贷款**，以编程的方式在区块链上贷款。无需注册银行帐户。
- **去中心化交易所**，通过区块链而不是像Coinbase这样的中心化交易所买卖加密货币。原则上，计算机可以在区块链上进行交易！
- **抵押**，用数字资产做抵押，借出去中心化贷款，在违约时为贷方提供一些追索权。
- **去中心化身份**，身份在智能合约的语境中用来评估去中心化贷款的信誉度等。
- **可组合性**，将执行不同功能的DeFi功能捆绑在一起，就像软件库一样。例如，如果一个合约获得了加密货币并产生了利息，则第二个合约可以自动将该利息再投资。
- **风险管理**，DeFi的高回报通常伴随着高风险。还好，现在有新的工具来对冲这些风险。

稳定币

如果要在区块链上重新创建传统的金融产品，我们将面临一个紧迫的问题：价格波动。具体来说，以太坊的原生加密货币（即ETH）的USD / ETH汇率日波动率幅度较大，有时一天之内波动大于10%。

这种价格波动下的工具，对许多传统金融产品来说不大完美。例如，如果你借出贷款，一定不想在支付前贷款波动10%。这种程度的波动会使令你对未来难以规划。

稳定币便能解决这个问题，它是经过特殊设计的加密货币，以每枚代币约等于1.00法币的汇率保持“稳定”。稳定币指数（Stablecoin Index）和稳定币统计数据（Stablecoin Stats）上列出了顶级稳定币名单。

稳定币分为三大类：中心化法币抵押、去中心化加密货币抵押和去中心化算法。

1. 法币抵押的稳定币，在银行账户中按1: 1的比例存入法币。例如，Coinbase发行的稳定币USD Coin (USDC) 在银行帐户中有1: 1的美元提供支持。只要你信任发行公司以及他们的基础法币，持有或使用代币的风险就很小。它的另一个优点是，背后有一个中心化公司，如果稳定币出现问题，由公司负责，许多用户和企业都看好这一点。

在美国，联邦存款保险公司的存款保险的保额至少为250,000美元，而其他国家或地区也有自己的存款保险条款。这些听起来似乎很美好，并非每个人都能使用中心化稳定币。例如，USDC的用户协议规定仅在受支持的司法管辖区可用，并且禁止用户在某些活动中交易USDC。

2. 去中心化加密货币抵押的稳定币，没有中心运营商或用户协议。也就是说任何人都可以在未经公司或政府许可的情况下使用稳定币。但是，权衡之下，没有法币来支持稳定币，难以维持稳定性。与简单的USDC模式不同，其1000美元的USDC有1000美元的银行背书，而加密抵押的稳定币是用至少1000美元的加密货币（高波动性）来做背书。

例如，Maker是一个搭建在以太坊上的系统，管理着一种叫作DAI的去中心化稳定币。DAI锚定1美元，挂钩的方式是，Maker系统中的所有人，都能通过锁定代币做抵押（主要是ETH），借出贷款DAI。抵押品的金额要大于借出的金额。因此贷款是超额抵押的。

例如，你锁定200美元的ETH作为抵押品，就能借入价值100美元的DAI，然后用这些DAI在交易所进行交易。主要是要做杠杆，如果你相信ETH的价格不会大幅下降，你就能得到“免费”100美元在加密交易所交易。如果果真ETH价格下跌，你价值200美元的ETH低于抵押品金额的要求，Maker算法会扣押你的抵押品并进行清算，返回你100美元。在这种模式下，Maker算法会让贷款避免失去本金的情况。

虽然Maker系统比USDC之类的系统复杂许多，但从理论上讲，DAI没有铸币，终端用户无需了解其中的复杂程序，就像普通美元用户不需要了解货币政策的复杂性。

话虽如此，DAI确实也有它的风险，比如智能合约风险以及DAI打破锚定的风险，交易高于或低于1USD/DAI的水平。

3. 第三类稳定币是去中心化算法稳定币，这种稳定币没有任何抵押品做背书，仅仅依靠算法来稳定价格。

比方说Basis，尚未发布就关闭了。这种模式的稳定币存在一种担忧，资金充裕并有动机的公司会攻击系统，致使人们对钉住的汇率失去信心。导致出现死亡漩涡，稳定币崩溃。

总之，前两种稳定币最受欢迎。无论是用法币或加密货币做抵押，人们似乎都希望价格保持稳定。第三种稳定币正在进行相关实验，希望将加密货币抵押与算法相结合使用。

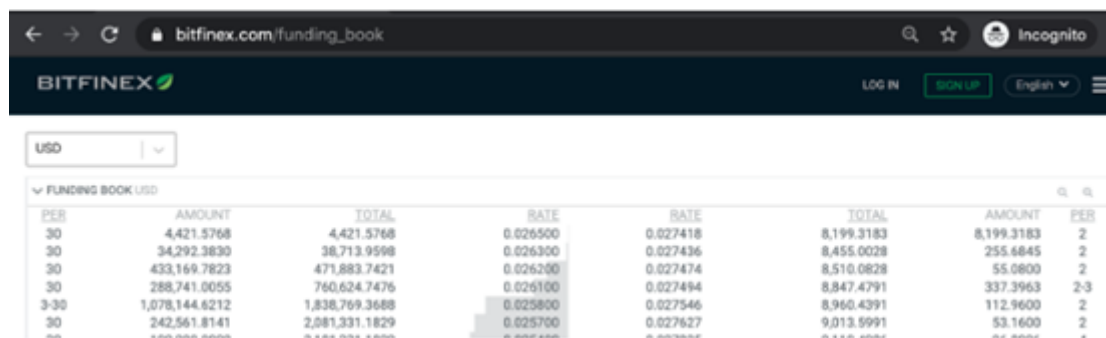
去中心化放贷

有了USDC和DAI等稳定币，就可以着手将传统金融系统各个部分重建为自动化智能合约。金融的一个最基础的概念是借贷。

许多DeFi平台可以直接通过智能合约（例如Compound，dYdX和Dharma）借贷以太坊代币。这些智能合约有一个关键的特征，借款人不用去找贷款人，反之亦然。智能合约代替了中间商，根据供需算法计算利率。

中心化借贷订单簿

在解释中心化借贷订单簿如何工作之前，先来回顾一下中心化交易所如何实现借贷的。下图是Bitfinex的基金订单簿截图：



PER	AMOUNT	TOTAL	RATE	RATE	TOTAL	AMOUNT	PER
30	4,421.5768	4,421.5768	0.026500	0.027418	8,199.3183	8,199.3183	2
30	34,292.3830	38,713.9598	0.026300	0.027436	8,455.0028	255.6845	2
30	433,169.7823	471,883.7421	0.026200	0.027474	8,510.0828	55.0800	2
30	288,741.0055	760,624.7476	0.026100	0.027494	8,847.4791	337.3963	2-3
3-30	1,078,144.6212	1,838,769.3688	0.025800	0.027546	8,960.4391	112.9600	2
30	242,561.8141	2,081,331.1829	0.025700	0.027627	9,013.5991	53.1600	2

从左侧开始阅读上图中的数据，第一行代表市场中的借款人，他们愿意以0.0265%的日利率借入30天的贷款，借款额为4,421.58美元。在借款人的正下方是另一种借款人，他们愿意以略低的0.0263%的利率获得30天的贷款，借款额为34,292.38美元。右边是放款人。第一行表示愿意以0.027418%的日利率借出2天 8,199.32美元的贷方。第二行是某人愿意以0.027436%的较高利率借出两天255.68美元。











类似种种，这就是中心化贷款订单簿的工作方式。在上面的示例中，借款人愿意接受的最高利率为每日利息0.0265%，而贷方愿意给予的最低利率为每日0.027418%。两方中的一方要么提高，或降低货币价格，达成交易。Bitfinex提供设置订单簿和匹配用户的服务，减少每笔贷款的繁琐步骤。

去中心化借贷订单簿

一些去中心化的借贷服务将借贷提升至一个新的水平。允许用户直接从智能合约借贷，无需建立订单簿和促进匹配，动态地提高或降低匹配的利率。

例如，如果从智能合约借出了大量加密货币，则向借方收取更高的利率。此外，为了借入资金，用户需要向智能合约提供抵押，提供的金额要大于借入的金额，从而使贷款被超额抵押。

前者是一个可扩展的应用程序。从理论上讲，一种比传统银行账户利息更高、风险更低的加密服务，可以吸引数10亿美元的存款。Compound的存款已经达到1.2亿美元，其他服务也在快速增长。主要风险来自智能合约错误和加密货币波动性，但利率也大大高于传统2%或更低的银行利率。下图是LoanScan一张放贷各大平台稳定币可以挣取的利率。

Platform	USDC	SAI	DAI
USD Price	\$1.00	\$1.00	\$1.00
24h change	—	—	—
 Compound v1	•	8.17%	•
 Compound v2	3.94%	2.63%	3.97%
 dYdX	3.55%	•	2.02%
 Dai Savings Rate	•	•	4.00%
 Nuo	2.69%	2.27%	1.01%
 Fulcrum	4.37%	4.81%	4.56%
 Torque	4.37%	4.81%	4.56%
 DDEX	13.81%	•	4.72%
 Dharma	3.94%	2.63%	•
 InstaDApp	3.94%	2.63%	3.97%

去中心化交易所

去中心化交易所试图将Coinbase Pro之类的服务放在区块链上。也就是说，它们的作用是促进拥有不同加密货币的两方达成交易。

要了解去中心化交易所，就要先了解中心化加密货币交易所。这些交易所像Coinbase Pro一样，充当中介和保管人，两方将资产存入Coinbase Pro上来进行交易。虽然中心化交易所能为数十亿美元的交易提供便利，但中心化交易所确实存在单一故障，导致黑客入侵、审查交易或阻止某些人进行交易。

去中心化交易所通过智能合约取代中介，解决了单一故障。让所有资产完全实现点对点交易。

许多项目正在以各种方法，实现去中心化交易基于以太坊的代币（例如Uniswap, 0x和Kyber）。例如，Uniswap利用所谓的自动做市商（AMM）通过算法提供流动性。买卖双方直接从智能合约中获取流动性，根据需要的代币数量和可用流动性接收报价。无论订单大小如何，Uniswap始终跟随订单大小的增加而逐步提高价格。

去中心化交易所目前只能处理一小部分中心化交易，因此无法真正实现来回兑换大量资金。此外，许多去中心化交易所的项目仅限在以太坊上交易基于以太坊的代币，限制了他们使用自己的链访问大型代币的机会。但当前仍然出现一些有前景的技术，例如原子互换和zk-STARK可以解决这个问题。

去中心化身份

去中心化借贷服务离不开一个问题：它们需要大量抵押。这种超额抵押要求可能是对资本的极低效率的使用，许多人一开始就没有多余的资金来提供抵押。

但是，人们正在研究去中心化身份和声誉系统，降低抵押要求。最早的一批应用程序将是构建类似区块链的基于法币的信用机构，例如像Expatrian，TransUnion和Equifax这样的银行机构根据信用评分。

现在，为了避免反对意见，可以肯定的是，征信机构会让某些群体，如国际组织或青年处于不利地位。但是，诸如Lending Club之类的新服务已通过提供其他数据分（如房屋所有权，收入和就业时间）解决了对财务管理分数过分依赖的问题。

去中心化身份和声誉服务可以提供诸如社交媒体信誉，历史贷款的偿还记录，其他信誉良好用户的担保等这样的服务。要对实际财务决策真正起作用，就需要在使用具体数据分和相应的抵押要求上做大量反复实验，而我们才刚刚起步。

从长远来看，带有去中心化身份系统的DeFi可能会成为被传统金融系统拒之门外的另一种选择。例如，有十亿人没有官方身份证，而低收入国家或地区的50%的妇女没有身份证，但其大部分人拥有智能手机。因此，一旦去中心化身份ID在发达国家使用，它们很可能会作为一种跨越式技术迅速出口到发展中国家，就像智能手机本身一样。

可组合性

介绍完去中心化稳定币、借贷、交易所和身份。但是，要在像以太坊这样的智能合约平台上构建去中心化金融构件，最重要的是可组合性。就像软件库一样，不同金融应用的智能合约可以像乐高积木一样即插即用。

例如，如果要在平台上增加交易代币化资产的功能，可以通过集成去中心化交换协议，轻松地使资产可交易。这些乐高积木般的智能合约甚至可以创造全新的概念，而这是传统世界中从未探索过的。

拿一个结合了DeFi与社交媒体，叫作2100的项目来说，它允许用户使用推特账户来挖掘新代币，本质上是从社交资产中生成数字美元。知名账户可以投放只有特定代币持有人可以访问的优质内容，这样一来，就能通过粉丝获利。还可以做一些有趣的事情，例如押注某些推特账户，这一做法正在变得流行。

另一个叫作PoolTogether的项目，将DeFi和彩票相结合，创建“0损失”彩票。用户在链上购买彩票，购票的所有资金都将在Compound上获得利息。在抽奖结束时，每个人都能取回自己的资金，但只有一个人能获得所筹集资金的全部利息。从本质上讲，这是一种利用彩票机制激励储蓄和财富创造的方式！

随着DeFi的成熟，我们希望这些可组合库能在加密社区以外的地方使用，最终，可以添加一行代码，将完整的去中心化市场添加到视频游戏中，或者添加另一行代码允许电子商务商店的商家赚取余额利息。

风险

尽管DeFi令人着迷，但也要认识到它所带来的风险。以下一些风险类别：

- **智能合约风险**，有许多是新系统，需要更多时间进行战斗测试。当协议相互交互时，智能合约会带来风险。如果一个协议具有严重的智能合约错误，则可能导致整个系统遭受攻击。明智的做法是，避免在系统早期投入过多资金。

- **抵押和波动风险**，给贷款做背书的抵押品类型也可能存在风险，超额抵押可以降低波动性，但是，如果抵押资产的价格下跌过快，则无法保证追加保证金能等同全部的借款。但是，采用合理的抵押比率和经过审查的抵押类型，这种风险应该较小。另一个潜在的问题是，许多DeFi平台上的利率波动导致某些人无法参与。可能会有利率掉期或其他方法来锁定溢价利率，但这也增加了复杂性。

- **监管风险**，DeFi平台有不同程度的去中心化，还没有看到检验所有条款的法庭案例，有待观察。

Nexus Mutual和Convexity等去中心化保险是DeFi应用的一个领域，可以对冲DeFi的一些风险。诸如Augur之类的预测市场，押注他们使用的协议存在智能合约漏洞的可能性，来对冲风险。

这些对冲方法还处于起步阶段，它们自身的智能合约还存在风险。但我认为这些方法会慢慢成熟，而且，如果DeFi领域足够大，那么传统的保险公司也可能会提供对冲产品。

总结

DeFi领域涵盖很广，而且在不断扩大。目前DeFi已部署了数亿美元的加密货币，潜力巨大。