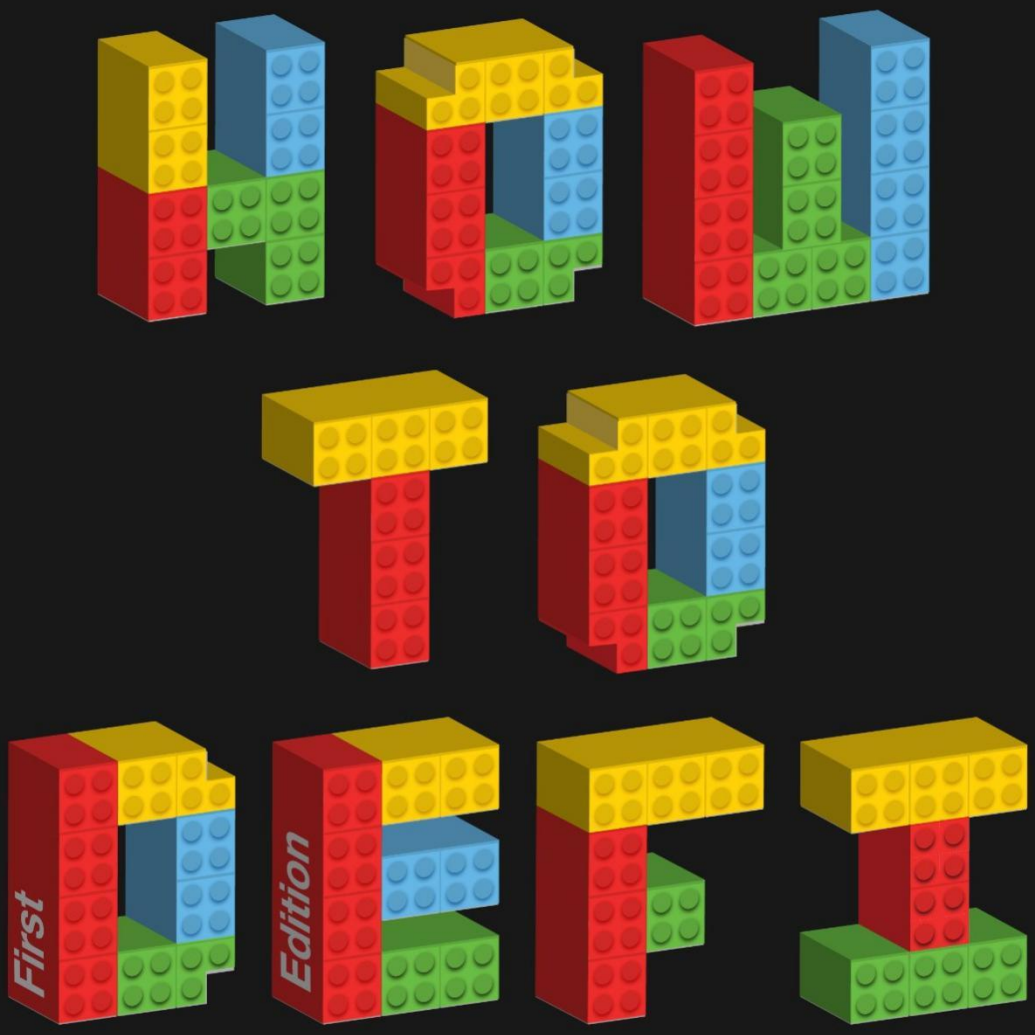
"Probably the most comprehensive DeFi manual out there, a must-read."

Hugh Karp, Founder of Nexus Mutual



ADVANCED

Decentralized Finance is taking over the world.
Learn how to get started and join the revolution.

CoinGecko

How to DeFi:高级

链金投研翻译版

不得用于商业用途

2021年5月

卢修斯·方，本杰明·霍尔，
惠里纳·阿兹米，霍尔·温·温

“可能是最全面的DeFi手册，必读。”

——休·卡普 Nexus Mutual创始人

“教育在DeFi中是至关重要的，像《How to DeFi》这样的读物就显得弥足珍贵。这不仅是一个优秀的续集，更是CoinGecko的团队再次成功地对一个不断快速变化的DeFi世界全面和深入的概述。”

– Ganesh Swami, Covalent首席执行官

这是关于DeFi的最全面的指南，绝无仅有。你应该从头到尾看一遍。”

–Leo Cheng, CREAM Finance联合创始人

“如果你想了解DeFi的最新趋势，这本是市场上最好的书。”

——CREAM Finance联合创始人Yenwen Feng

“这本书是他们第一本书的精彩续集，并提供了对DeFi的更深入的理解，以及如何驾驭DeFi世界的有效指南。”

–Jocelyn Chang，MakerDAO核心单元亚太区负责人

“在2021年阅读《How to DeFi》，就像2015年在Zug的café上偶然遇到Vitalik Buterin并首先发现以太坊。《How to DeFi》将会帮你在构建和使用DeFi协议的未来十年作出改变生命的决定。”

——Molly Wintermute ,Hegic创始人

“新来者相聚在这里确实不容易。但是有了CoinGecko的顶级指南，读者很快就会发现DeFi不仅仅是未来的趋势。DeFi从现在并很快将成为世界各地许多人日常生活的一部分；这可能是目前最好的指南，为任何阶段的DeFi之旅点亮道路。”

——Azeem Ahmed ,Armor联合创始

“这本书汇集了当下你参与和了解DeFi的所有重要概念和项目平台。在未来很长一段时间内，我将把它作为自己和新来者的参考用书。”

——Laurence E. Day，Indexed Finance核心团队

“最深入浅出的前瞻性指南，帮助理解DeFi及其所有可能性”

– DeFi Ted, COVER协议顾问

目录

第一部分：DEFI的状态

疫情与经济双寒冬下，为何中国资本却纷纷入场DeFi领域？

2020年，疫情下的全球经济，可谓是进入了寒冬腊月天。大量公司裁员、削减业务，负债累累，违约事件频发，就连一些国际巨头也不能幸免，有的最终只能向政府求助或是申请破产保护。

与此同时，诸多线下实体行业也都遭受了致命性的打击。据*S&P Global Market Intelligence*统计，在疫情期间，美国零售领域有近百家企业破产，其中包括许多百年老店，破产数量创2009年金融危机以来最高。

而疫情对世界经济的冲击，最引人注目的就是资本市场。2020年3月份，数十个国家的股市相继发生熔断，而美股更是创下两周内四次熔断的教科书式记录，让股神巴菲特都不得不感慨。

巴菲特老爷子感慨美股四次熔断，真是活久见！

然而，在每一轮经济周期的寒冬中，总会孕育着下一波的财富浪潮。就像02年的互联网，08年的电商一样，总一些行业在悄悄异军突起。

当大部分人还在迷茫下一步经济走势的时候，全球投资大佬的资本布局才刚刚开始.....

下一波经济热潮在哪？

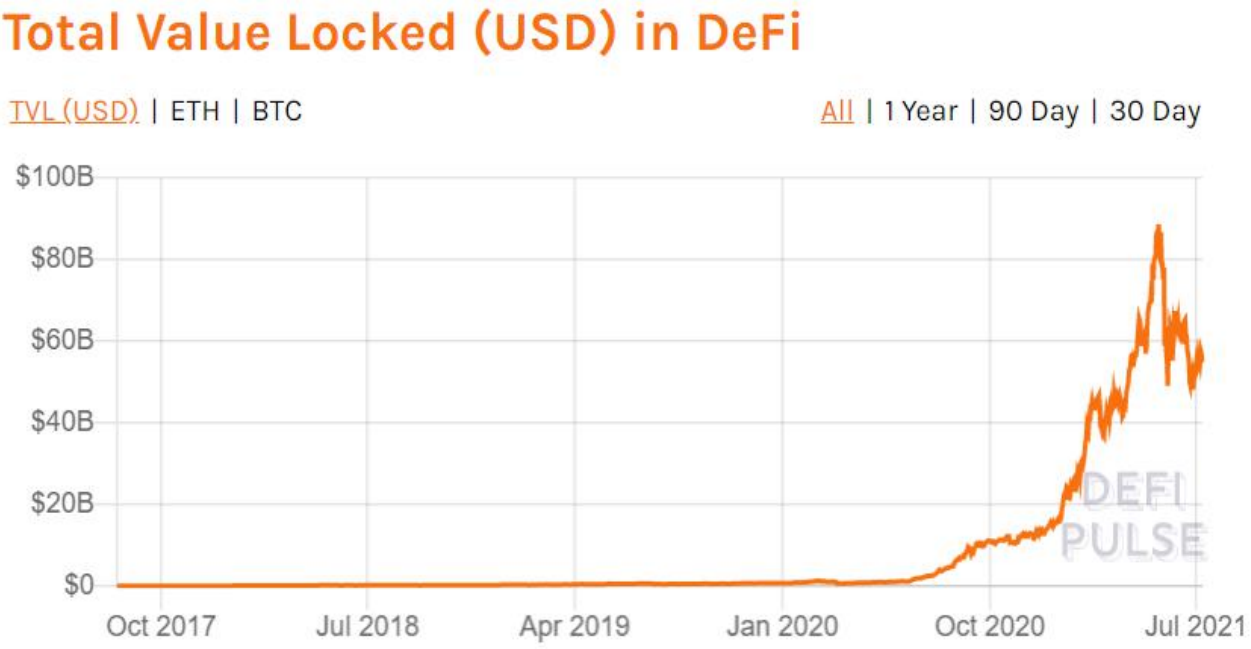
2019年10月24日开始，在中央政治局第十八次集体学习时，习大大特别强调，**“把区块链作为核心技术自主创新的重要突破口”，并且“加快推动区块链技术和产业创新发展”。**

此后，去中心化金融（DeFi）开始逐渐受到加密货币社区广泛关注，并且在2020这一年的时间内取得快速的发展，迎来了加密行业的**“DeFi Summer”**。

回顾这一年取得的成绩，DeFi 生态的发展速度超乎想象，随便举例几个数据都能发现是以百倍计的。

比如，借贷资金量提升了170倍，交易用户数增加了140倍，锁定在DeFi的智能合约中的资产总量增长了140倍等等。

根据DeFi Pulse的数据，在DeFi应用中锁仓的数字资产价值，从2019年的不到10亿美元，增长到2020年的超过100亿美元，并在2021年一度超过800亿美元。



数据来源：DeFi Pulse

去中心化金融（DeFi）正在重新定义金融的未来。而支持传统金融应用的底层基础架构，也正在发生重大转变，改变人们对许可和控制、透明度和风险的看法。

风投基金 Race Capital 联合创始人Chris认为：**「DeFi 的创新速度比传统Fintech应用快10倍。」**

传统金融体系具有不透明特质，运行在部分准备金体系之上，容易受到市场冲击。与其不同的是，DeFi 系统是完全透明的且超额抵押，这使得 DeFi 企业能够更有效地度过市场低迷期。

DeFi的出现，大大优化了传统金融的基础架构

全球有关金融经济的消息不断，眼看加密数字货币的热潮也将再次来临，即使保守如我国，也不得不加快了追赶的脚步。

而DeFi正是这些数字货币的新一局面，作为发展势头最足，代表性最强的前线阵营，DeFi有望成为未来金融科技领域的领头羊。

抓住DeFi所蕴含的财富，就是我们这代人能赶上的最佳机遇。

顶级VC加速布局DeFi赛道

总览整个国际金融大盘，可以发现中国资本在区块链赛道的身影突然多了起来。

近期金沙江创投、光速中国、北极光创投等创投基金都开始纷纷关注DeFi赛道，国内互联网VC也开始入局Crypto。

为何在整体金融低迷的形势下，国内却如此看好DeFi项目呢？

其实，在全球范围的顶级风投公司中，布局加密行业的不在少数——

今年5月，投中Facebook、Twitter的硅谷传奇投资机构a16z，被曝正在筹备第三支加密基金，规模超过22亿美元；
捕获了阿里巴巴、滴滴、Keep的软银也在布局加密行业，投资了巴西一家加密货币基金公司；
在国内投出 360、百度、腾讯、美团、拼多多等 500 多家互联网公司的IDG Capital，在加密行业的攻势也从未断过，Coinbase、imToken、Ripple 等知名加密项目均被其收入囊中

从左到右依次为：
红杉资本沈南鹏；Dragonfly创始人冯波；以太坊创始人V神；美团创始人王兴；大众点评创始人张涛。

更重要的里程碑事件，是今年 4 月美国持牌加密货币交易所 Coinbase 在纳斯达克成功上市，这让一直对加密行业合规性存疑的国内投资人看到了新的可能性。

正如BTX Capital创始人Vanessa所说的：

「Coinbase让传统的投资人看到，加密交易所也可以非常合法地在纳斯达克上市，这意味着投资人有了合法合规的退出机制。」

随着消费互联网野蛮生长时代的落幕，国内互联网行业赖以发展的人口红利也逐渐消失，获客成本增加，流量不再易得，移动互联网市场趋于饱和，习惯了高歌猛进的中国互联网VC们现在不得不将视线转向别处。

当合规通道被打开，Crypto就是一片无法视而不见的诱人蓝海。

普通人如何追赶DeFi浪潮?

实际上，DeFi的范畴很大，包罗万象，所以若想要真的赶上DeFi时代，专业性的学习和针对性的指导是必不可少的。

很多人都想抓住新一波的财富机遇，但是，**大部分人其实连区块链是什么都不知道，而且很难理解这个和传统金融有巨大差异的DeFi，到底有什么独特之处?**

又或者很多人在好奇DeFi是什么，它是一个具体的投资项目？还是这些项目的总称？或者是某金融产品？还是什么新名词？

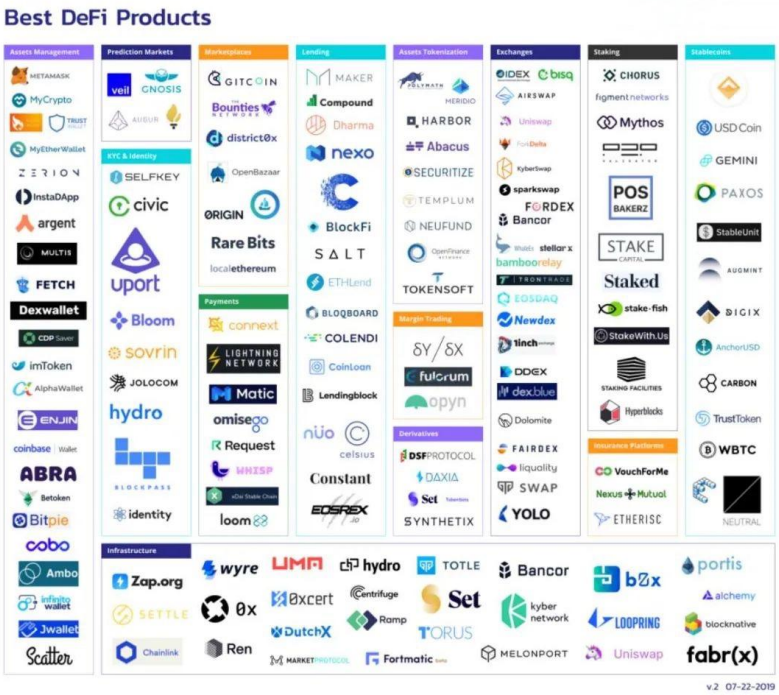
你不知道答案，你只知道DeFi这个词最近好像很火，很多人都在提及：刷微博发现特斯拉创始人马斯克在紧跟它的步伐，而越来越多的金融报道也都在围着它打转...

如果你有类似以上的这种疑惑，这就说明你已经与DeFi的第一波浪潮和第一桶金失之交臂了。

但是现在还不晚，根据链金商学院专业团队的预判，区块链作为一个时代级别的财富机遇，就像当年的互联网一样，至少是一个三十年级别的发展空间。

而DeFi作为基于金融创新的颠覆式产物，最猛烈的浪潮还尚未到来。

然而万事开头难，更何况任何新事物的学习，都是说着简单做着难，更何况DeFi这样门槛还相对较高的领域。



目前DeFi项目众多，巨大的机遇与风险并行

如果你只是在网上空刷文章，然后羡慕别人一年好几倍的收益，其实对自己的生活，不会带来任何的回响和改变。

所以只有真正动身学起来，操作起来，才能跟上财富的步伐，做新机遇的受益者和开拓者。

可是在学习的过程中，一定会遇到各种问题：看不懂、学不会怎么办？能力不足承担不起风险怎么办？入错了门，投错了行怎么办？

其实，这所有问题的答案只有一个：你的方向错了！

跟着报道和笼统无序的文章自学，耗时耗力，开始之路就参杂着各种隐形风险；听亲戚朋友指导，金钱面前无大义，怎能轻易相信他人？

最有效且正规的办法就是寻求专业机构指导。这就像上学时的课外辅导一样，所有人都在同一起跑线，而你却报了课外名师针对性辅导。

不同之处在于，在学生时期你收获的是知识，而现在你获得的是赚钱方法和策略。

链金投研作为区块链行业的专业老牌团队，专门研发、总结出了这套《从0到1学DeFi》小白入门课程，诚意满满。

在课程中，我们会告诉你，**在DeFi大势前如何采取措施，如何持有并管理加密资产，如何借其它产品东风助推自己项目的收益。**

更重要的是，我们的课程导师还会告诉你，在大局势动荡时，紧急措施如何采取，以及带新手鉴别常见的项目风险。

>>明星导师团队

《从0到1学DeFi》小白入门课程的讲师团，由DeFi项目深耕研究者组成。

不仅拥有多年的区块链行业基础，还具备全球名校金融+计算机双学位背景，和丰富的投行研究经验。

虽然课程是解答最常见的小白问题，但却几乎是人人都有的问题。如果仅是靠自学，那必然是要付出点实践代价的。

不仅是新人小白，就连很多资深的传统投资人刚接触DeFi时，也都会在这些问题上栽跟头：

面对牛市，我到底应不应该杀进去，到底什么时候应该进入市场？
我们很喜欢一个DeFi产品，看好项目的发展，那么能不能买它的治理TOKEN？
作为一个普通小白，是持币还是持有稳定币，分散赛道和项目的投资到底有必要么？

这些人人都有的问题，需要更加专业、拥有丰富经验的导师为你做出引导。

在*DeFi*学习的道路上，如果有经验丰富的老师能够带领前行，快速轻松上手参与实操，分析各种热门项目，避免踩坑。

那么不说一定能帮助你实现*DeFi*投资的年化几倍回报，**但是最起码可以获得远高于传统金融的一个稳健收益。**

现在扫描海报二维码，还可以免费领取前4节课程，赶快行动吧！

>>系统完善的课程体系

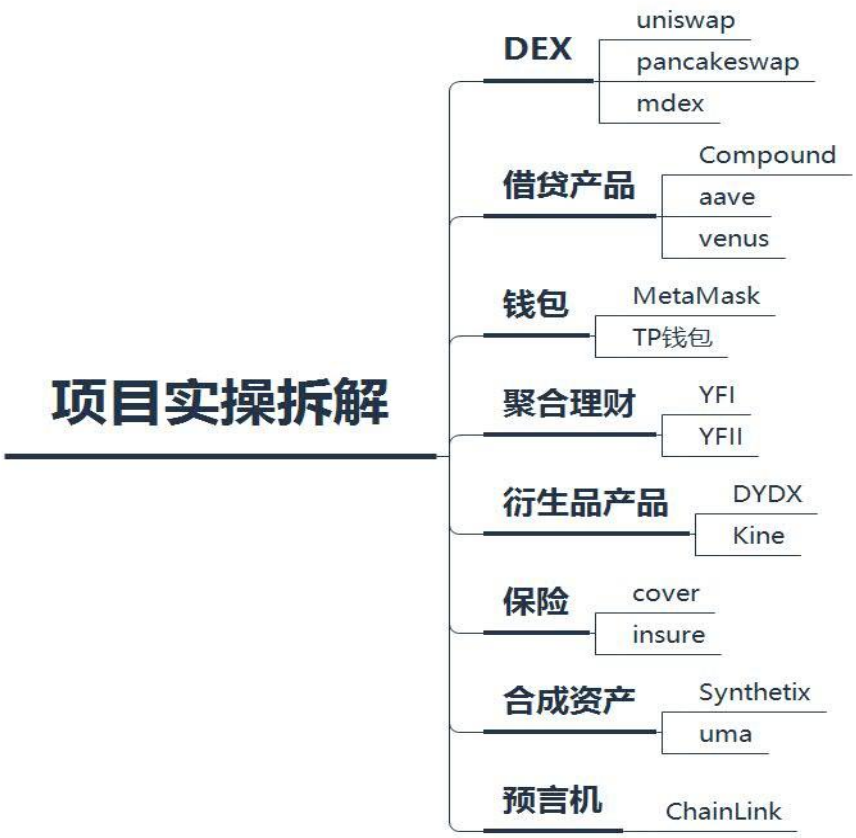
这套《从0到1学DeFi》小白入门课共有60节，**通过讲师精简生动的讲解，化繁为简，把这么一个深奥的领域变得通俗易懂。**

目前课程仍在持续更新中，课程大纲的整体构成，主要包括以下四个部分：

① 体系化学习defi基础理论；
② 小白快速上手实操；
③ 热点项目加餐分析；
④ 掌握在DeFi投资中应该遵守和执行的原则，以便在后续日常中使用。

同时课程大纲也将根据市场热度和用户反馈，随时进行调整。

无论你是学生，在职，还是希望未来投身于区块链行业，通过这套课程，我们会给你传授DeFi加密财富的正确打开方式，相信大家都会有所收获。



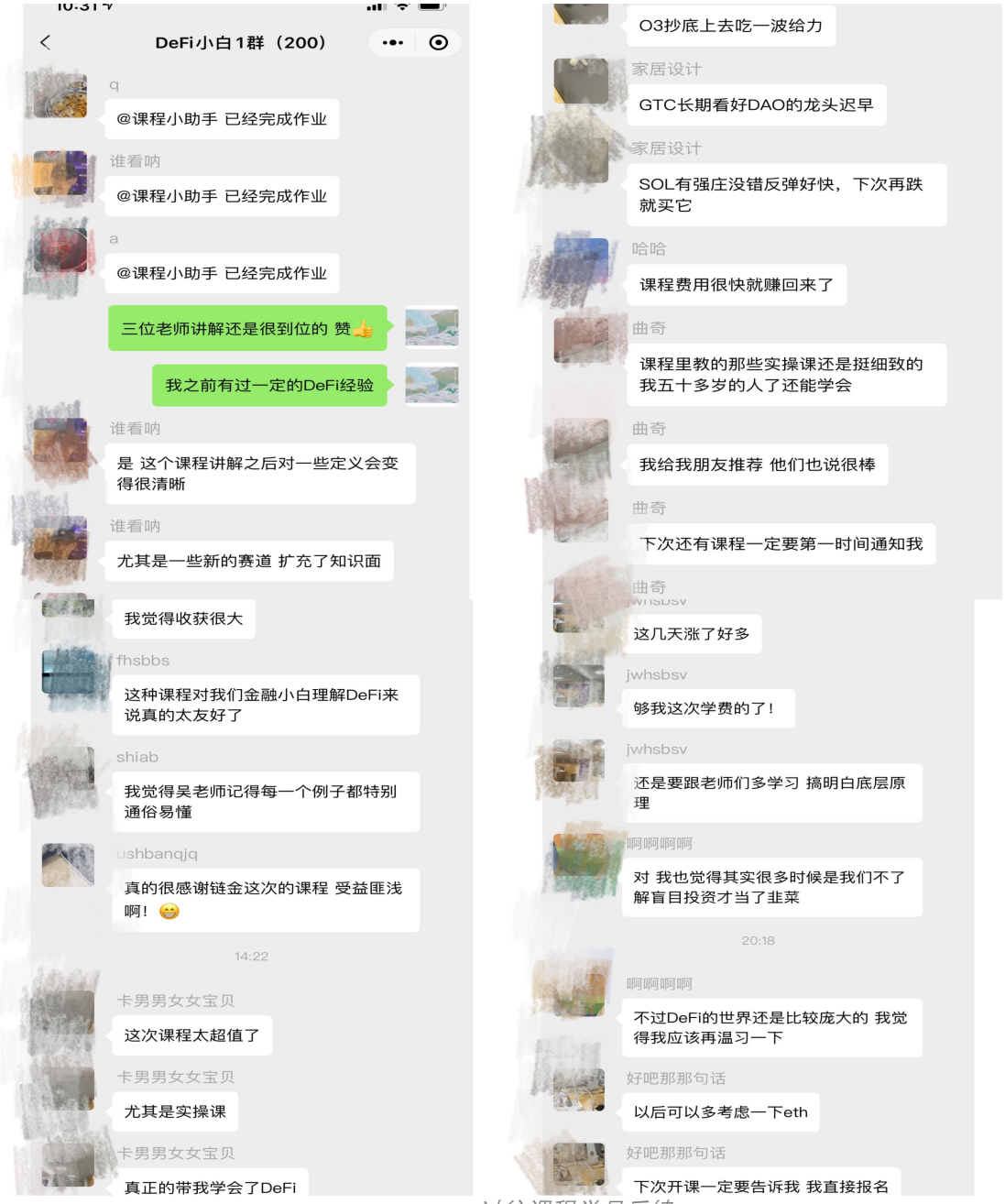
项目实操拆解案例

除了课程，我们的导师还会指导你如何将理论与实操结合，并且还有带班班主任。无论学员基础如何，都能达到一定的高度，这才是最踏实的收获。

>>前期课程反馈

链金投研作为DeFi领域专业的课程研发和培训团队，**之前开设过多次类似课程，并且都获得了学员极高的评价。**

每一次的课程，都可谓是圆满成功。并且有很多学员在课程结束后，还都和我们的导师在群内保持活跃的联系。



过往课程学员反馈

目前，链金投研团队重磅研发的《从0到1学DeFi》小白入门课正在火速招生中。通过60节简易入门课，带你踏上DeFi新征程！

从今天开始，跟专业导师一起打开DeFi新世界的大门，从0到1学起来吧！

学无止境，经济领域发展变化如此之快，时代流行什么，我们就要学会什么，不然就会无情被时代甩在身后。

是否成为先驱者和开拓者，决定权只在你自己手中。每节课只需3块3，不足一顿早餐钱，为什么不用来投资一个更好的未来呢？

希望各位加入的小伙伴，都能深入了解*DeFi*！**一起坚守周期，穿越牛熊，做时间的朋友，领跑市场99%的人！**

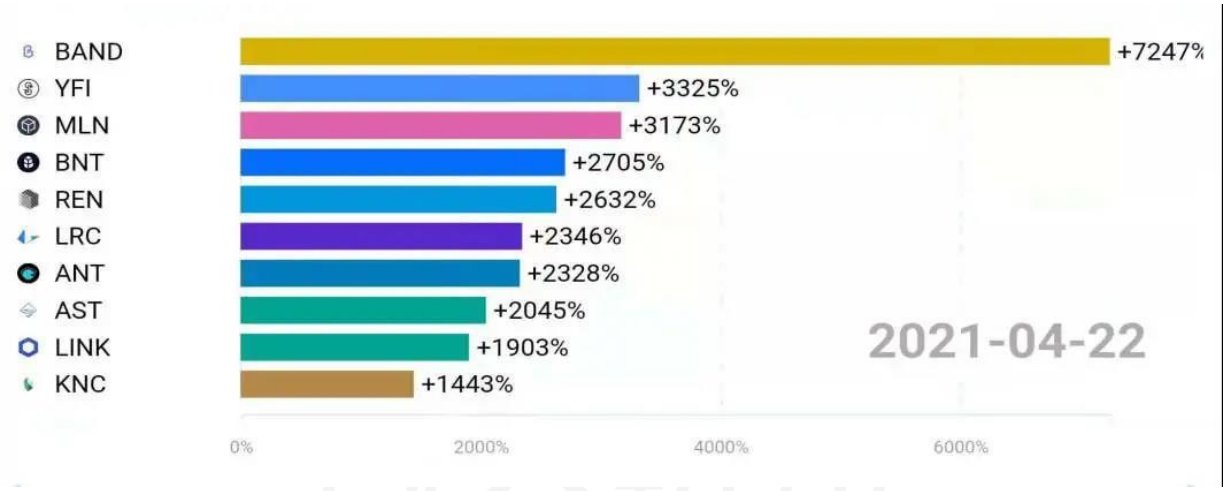
作为普通投资者，如何抓住未来DeFi财富基于的浪潮？

未来十几年，势必是加密数字资产大爆发的时代。如果普通人不懂合理的DeFi资产配置，就像当初错失房产、互联网和比特币一样，注定被甩下时代发展的浪潮。

从去年下半年开始，DeFi（开放式金融）热潮持续高涨，可以说是引发了本轮比特币牛市的最大推手。

在这一年多的时间里，主流加密货币的平均涨幅，基本都在5~10倍左右。在普涨之下，DeFi的表现更加吸引人的眼球。

许多新出的明星项目也纷纷跟涨，十倍币、百倍币又重出江湖，DeFi 板块整体估值的上升。

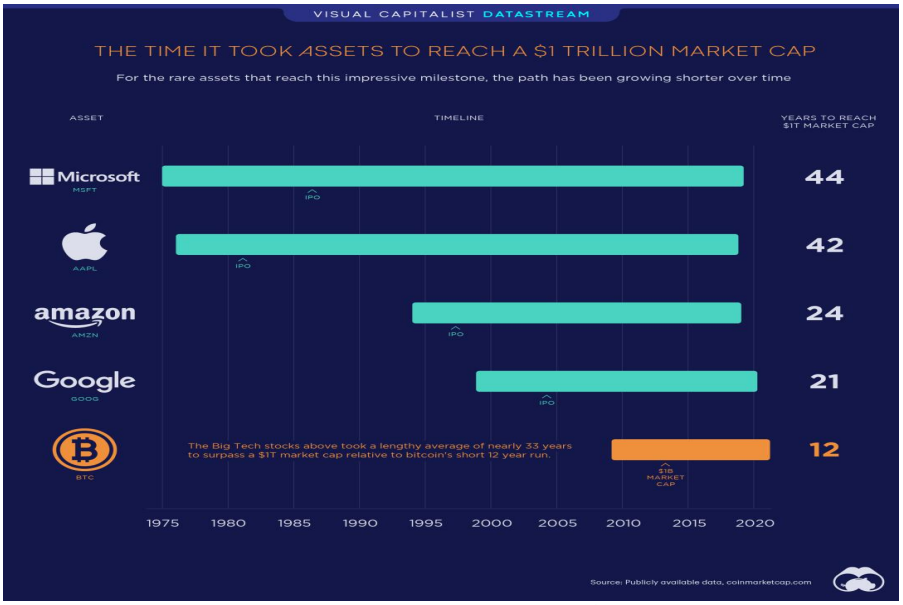


2020年初截至现在，DeFi币种涨幅 Top10

而DeFi生态的爆发，也成功吸引了众多海内外投资机构、行业媒体以及投资者的关注。

传统金融机构纷纷入场，Coinbase上市，马斯克投资BTC，更是体现了传统金融和未来加密世界的全新融合。

从历史上看，公司的市值花了数十年的时间才达到1万亿美元。**而对于比特币，仅用了短短的12年时间，就达到了这一里程碑。**



比特币仅用12年，便达到万亿美元市场

当前，*DeFi*这辆列车正在以高速向前行驶。而且在未来很长一段时间，**可以预见*DeFi*赛道所蕴含的财富机会，还将持续发酵。**

然而，*DeFi*在创造新一轮“造福神话”的同时，也带来了极高的认知门槛。

作为一名普通投资者，你对 *DeFi* 真的了解吗？

目前，*DeFi*已经深入借贷、交易、保险、衍生品等各个领域，那么其行业图谱是什么？下一个赛道又该如何押注呢？

与其看别人在*DeFi*中创造财富神话，不如自己亲身参与到这场“造富运动”的浪潮中。

然而，在现象级浪潮下，大部分人对*DeFi*的认知，其实还停留在最基础的阶段：

到底什么是 DeFi？究竟是未来金融趋势，还是只是庞氏骗局？

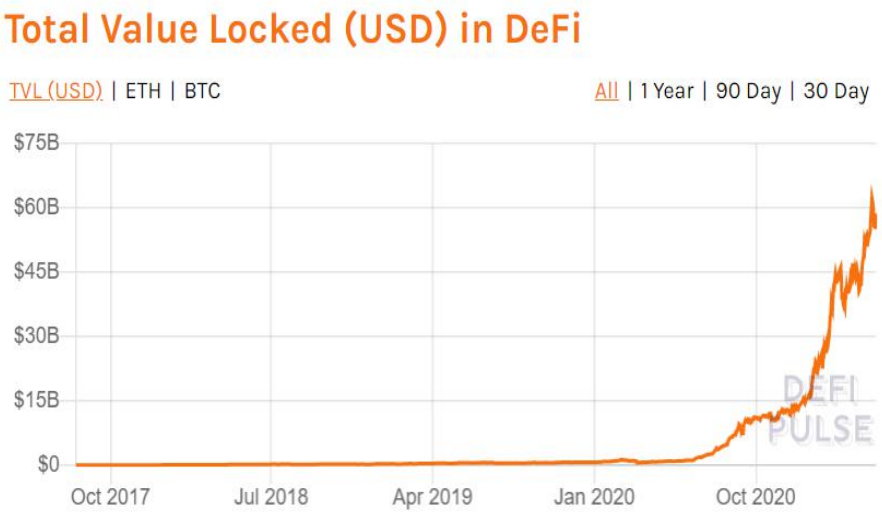
DeFi项目的价值支撑在哪里？估值逻辑是什么，为什么能涨了那么多倍？

流动性挖矿的底层逻辑是什么？如何能通俗易懂的理解，并参与其中？

……

这一系列看似简单的问题，其实都需要专业的解答。

只有透过纷乱的表象，掌握上涨背后的逻辑，用时间置换空间，才是获得财富密码的基本功课。



DeFi总价值在2020下半年，出现爆发式增长

然而，每个人只能赚到他自己认知范围以内的钱。市面上虽然*DeFi*项目众多，但其中不乏各种牛鬼蛇神的项目。

新人在对行业认知不是非常透彻的情况下，就贸然入场。那么往往面临的，便是**“入场即收割”**的惨烈局面。

如果内心又不想错过这次机遇，这时候，加入一个专业靠谱的圈子，**学习基本的投资原则和避坑技巧，并进行项目筛选和风险把控，**是非常有必要的。

看不懂？跟不上？下一波*DeFi*浪潮如何把握？

站在金融历史变革的前夜，*DeFi*一定是历史性的机遇。

普通人如何在未来十年纷繁复杂的加密世界，寻找真正的独角兽，把握住DeFi赛道的产业机会？

链金投研团队**基于对 DeFi 各细分赛道的不断实操，以及对 DeFi 项目的大量调研和分析。**

专门针对希望深入了解DeFi的爱好者，打造了一个兼具理论和实战的知识星球——

链金财富俱乐部

链金财富俱乐部，是由链金投研团队倾尽全力打造的、具有超高含金量的知识星球。

星球内容经过三个月的精心打磨，**集底层理论、小白入门、热点项目和投资分析于一体，邀请了几十位行业人士参与内测，均获得一致好评。**

在链金财富俱乐部中，我们邀请了多位DeFi大咖、老兵、技术白帽、科学家亲自培训答疑，更有币圈资金操盘上亿的大v进行实战分享。

并且，我们还在内测的基础上，不断进行了迭代升级。增加了**挖矿实操，每日空投汇总、薅羊毛攻略、二级市场风险预警**等板块，丰富扩展付费内容和有趣的全新玩法。

在链金财富俱乐部中，我们邀请了多位DeFi大咖、老兵、技术白帽、科学家亲自培训答疑，更有币圈资金操盘上亿的大v进行实战分享。

并且，我们还在内测的基础上，不断进行了迭代升级。**增加了挖矿实操，每日空投汇总、薅羊毛攻略、二级市场风险预警等板块，**丰富扩展付费内容和有趣的全新玩法。

同时，链金投研还邀请具备专业理论知识基础，和丰富实操经验的嘉宾，**为付费会员提供“学习+实操+答疑”的全年陪伴服务，保证学习效果。**

适合人群

如果你是下列之一

· 想要赶上这波DeFi财富机遇，却不知道从哪儿入手；
· 消息滞后且难以判断真假，希望加入圈子共同探讨；
· 想要尝试全新理财投资方式，却对DeFi一知半解；
· 缺乏系统性的技能培训，只能追在热点项目后面跑；
· 想要链接高质量的圈内人士，深入了解这个行业；
· 希望找到一个专业靠谱的团队，做自己的理财顾问；

…… ……

在内容体系设计上，我们**立足新手的认知基础和实践诉求，量身打造体系化学习模式，**从入门到进阶，从理论到实践，涵盖了全维度的内容。

无论你是币圈小白、资深韭菜还是传统行业人员，都希望你能加入我们，一起坚守周期，穿越牛熊，共同创造下一波的*DeFi*财富浪潮。

错过*DeFi*这个机会，你可能要再等*100*年！

任何事物在刚开始发展时，**敢于第一批投身进去的那批人，往往才能获得最大的利益。**

试想一下，如果你是*1992*年第一批彻夜排队购买新股的那些人中的一个，今天会是怎样？

如果你是*2009*年用家用电脑挖比特币的其中一人，而且你坚信去中心化金融的未来，今天又会是怎样？

同样，**今天的*DeFi*就是曾经的股市，曾经的比特币早期挖矿，只是量级更大。**因为它是一个跨国界的多样化金融产品，一个更具深度和广度的新型金融体系。

要知道，**在传统金融领域，衍生品的体量是现货的40到60倍。**

而在加密市场中，衍生品的交易市值还占不到整个数字资产市场体量的一半。对比之下，衍生品的发展仍有巨大的想象空间。

所以，作为一个普通投资者，**如果错过了这次DeFi发展初期的契机，可能100年内都难再有同样的机会了。**

在未来数字时代，如果普通人不懂合理的DeFi资产配置，就像当初错失房产、股市和比特币一样，注定被甩下时代发展的浪潮。

微信扫码加入星球

也许此刻的你，仍看不懂“DeFi”，那么不如加入我们。让专业靠谱的团队助你快速进阶成长，直通未来DeFi财富世界的新大门。

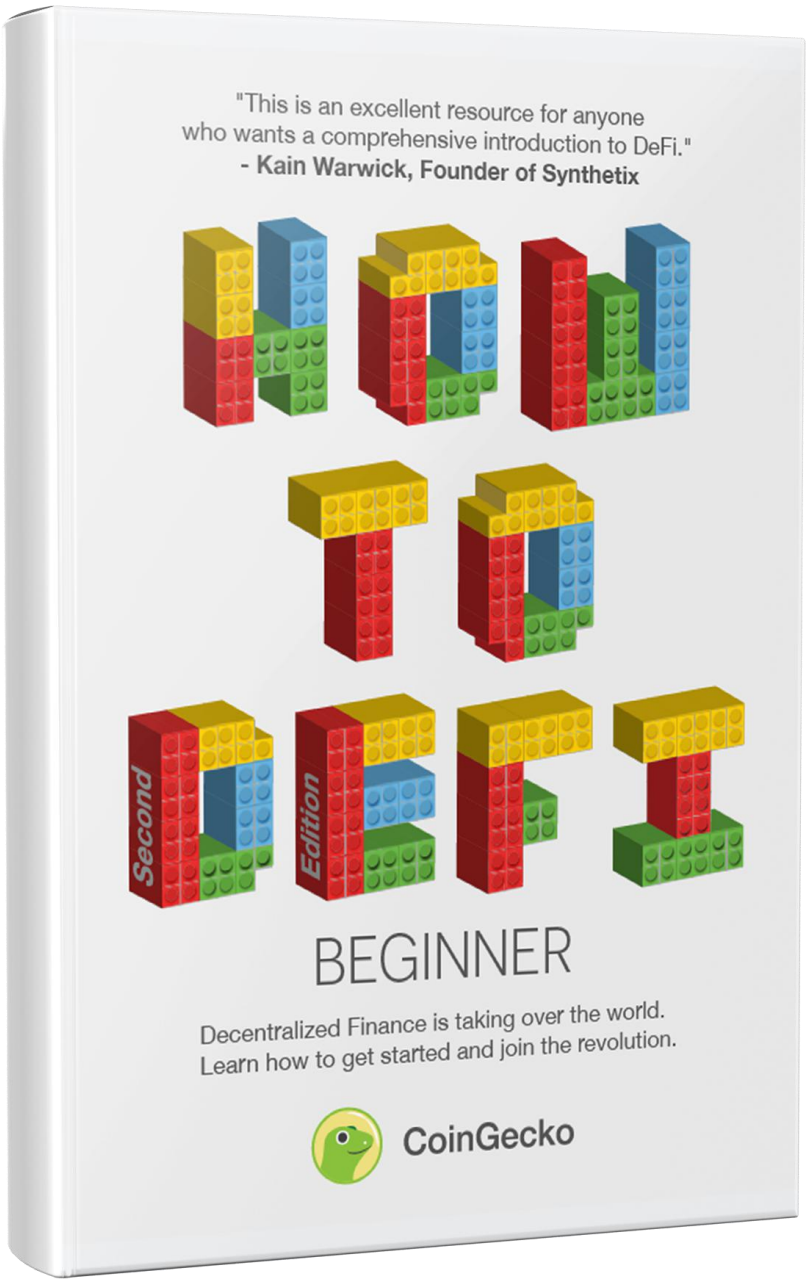
链金投研希望能和你一起，**坚守周期，穿越牛熊，共同创造下一波的DeFi财富浪潮。**

惊喜！《How to DeFi（高级）学习收藏版》全网首发！

Hey，《How to Defi》的小粉丝们，好久不见！

你们迫不及待地进来，一定是看到了我久违而且熟悉的身影吧~
记得2020的那个夏天，你还在寻找进入DeFi世界的系统指南……

为了帮助各位新农民迅速走进DeFi王国，我“爸爸”CoinGecko怀着对新金融世界的理想和渴望把我一字一句地写了出来。



我自诞生之日起就迅速蹿红，成为了当时唯一一本面向初学者的去中心化金融教程。

我问世后就在各个圈内群里迅速传阅，**并一度被誉为DeFi界的圣经级教材**。

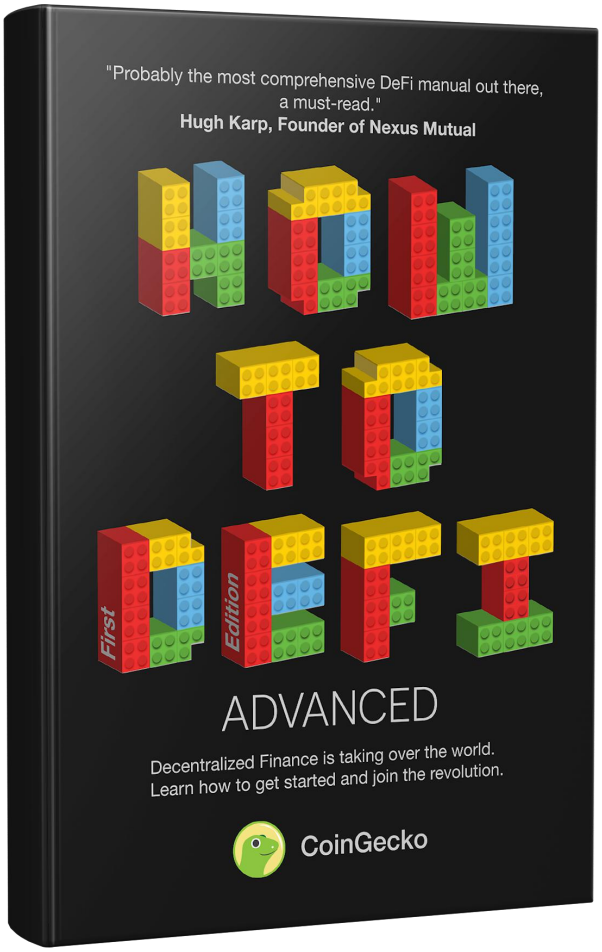
不知不觉一年的时间过去了。在这期间，**我见证着阅读我的DeFi新农民，从菜鸟一步步升级为高手，**对此我感到非常欣慰。

但这一年以来，DeFi协议创新的速度也实在太快了，入门版的我所提供给大家的基础知识越来越不够用了，最近大家来看我的次数越来越少，并且开始逐渐忘记我了。
当我以为已经履行完成了自己的使命并准备悄悄躲进大家手机和电脑文档库的小角落里时，我“爸爸”CoinGecko突然拍拍我说：

“孩子，快起来！大家还需要你！”
“只要传统金融还未完全过渡到去中心化的金融世界，你的使命就还没完成，你还要普渡更多的人，让更多的人觉醒，帮助他们意识到DeFi才是确定的未来。”
CoinGecko爸爸的话霎时间让我意识到我的使命还未完成，必须再次振作起来！

我清楚，很多人要跨越一道很深的知识鸿沟才能跃进这个新金融世界，但我也知道，入门版的我已经不有效的帮大家完成这个任务了。
一番商量之后，爸爸决定立刻下笔，给我做一次大升级！

现在高级版的我和大家见面了！和大家正式打声招呼：

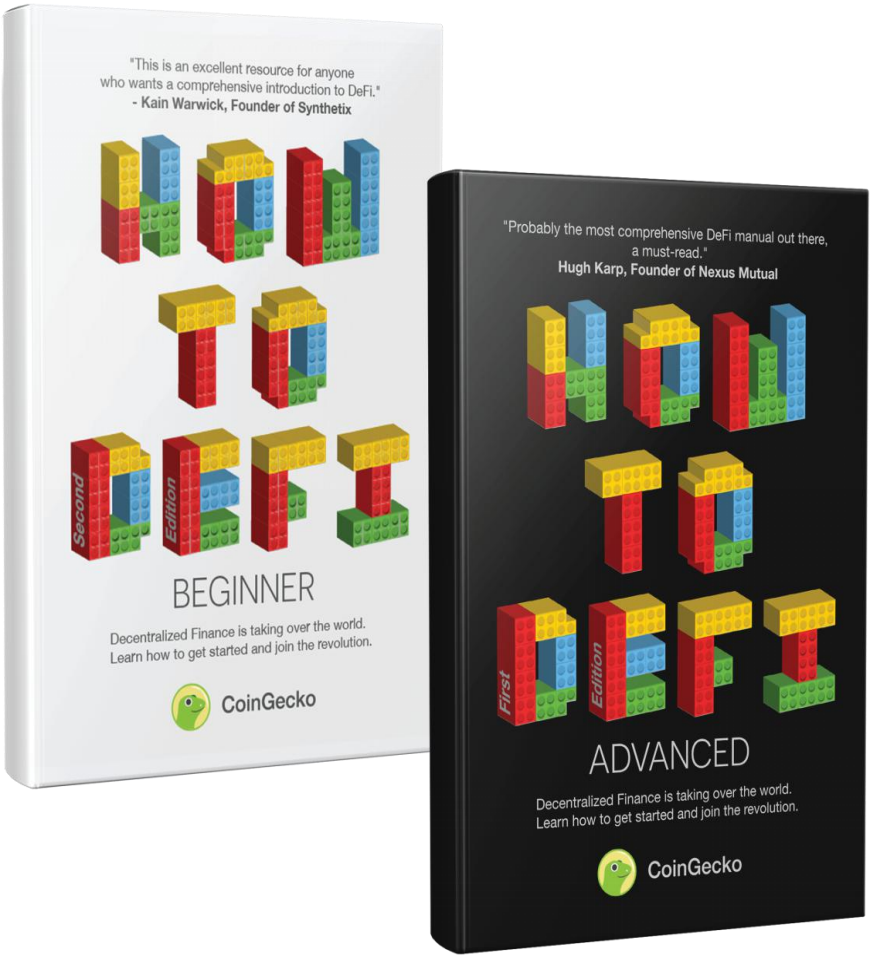


没错，大家可以看到我的封面已经改为了深邃的黑色，意味着这次我将要带各位跨越一段黑暗未知却充满机遇的探索之旅。
悄悄告诉你，当我面世时，知道我的人其实非常少。

因为CoinGecko爸爸是用英文把我写出来的，但我却知道自己最多的粉丝在中国以及其他华语地区。可是因为语言限制没能第一时间来到大家身边。

或许是我的期许被听见了，链金投研，这家知名的区块链投资研究机构，和“爸爸”一样怀着对新金融世界的渴望，履行着自身获得开放式金融机会的便捷途径使命首先发现了我，并把我完整地翻译出来了。

今天我有机会和各位再次相遇，我很感谢他们，是链金让我的生命得到了新生。
我很珍惜这次和各位新旧农民相遇的契机，所以我也对自己进行了自我升级：



我将会提供一个DeFi行业最新状态的概览，涵括所有知名赛道的介绍、行业中优秀协议的分析以及对未来的展望。

我不但会讲DeFi协议的创新，还会指出协议中的不足之处，希望行业内的小伙伴能有所收获。

当然，我还会在每一章的末尾推荐一些阅读资料，帮助大家以后更深入的开拓该领域。

对于初学者，我还是建议你阅读初级版的我，待你对DeFi世界有了基础的认知，再来这里找高级版的我，我会在这里默默地支持你支持你。

虽然这次“爸爸”尽了最的努力来升级我，但是在快速发展着的去中心化金融世界里，仅仅靠我自己还是不可能弥补所有知识的鸿沟。

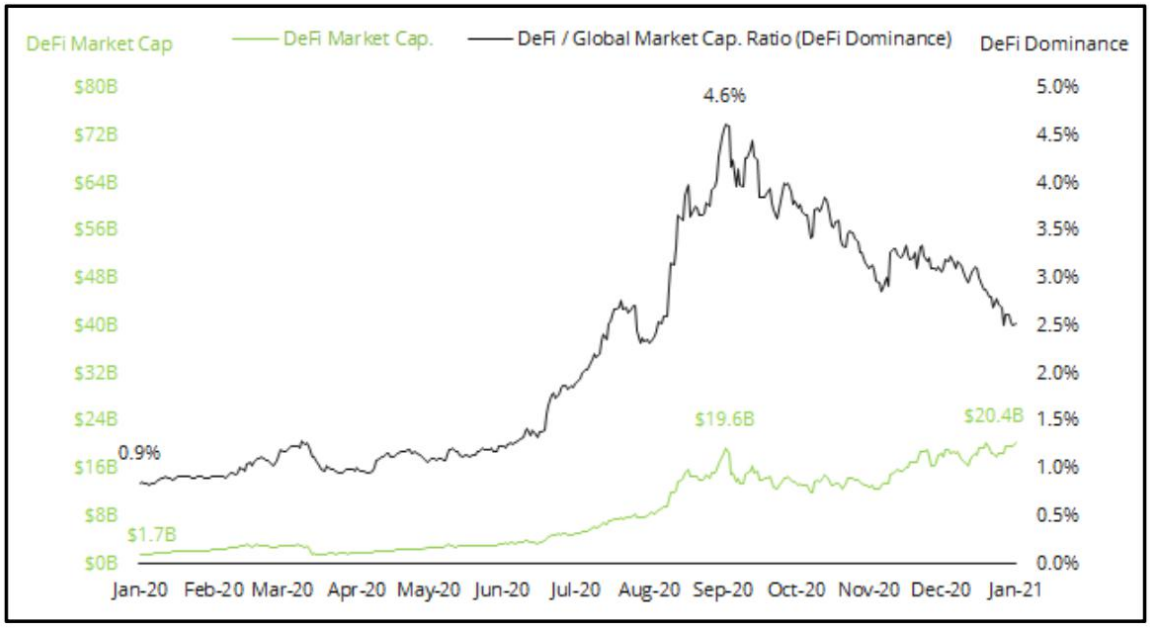
通过链金这次的分享，我相信能让大家吸收到更多有用的DeFi知识，并为选择适合自己的项目提供了额外的经验和认知。
如果你喜欢我，希望你能把我带回家。

公众号DeFi之光回复“高级”二字，让我再次带你开启一段精彩有趣的DeFi学习之旅。

第一章：纵观DEFI

DeFi之夏2020

尤其是在6月份至8月份这一时间段，加密领域一路见证了DeFi行业2020年的迅速崛起。也是在同一个夏天，DeFi协议的总市值在最高点已经翻了12倍，达到 196 亿美元，因此被称为“DeFi之夏2020”。DeFi的市场占比，通过计算DeFi项目的总市值除以加密货币市场总市值的比例，从0.9%迅速上升到4.6%。



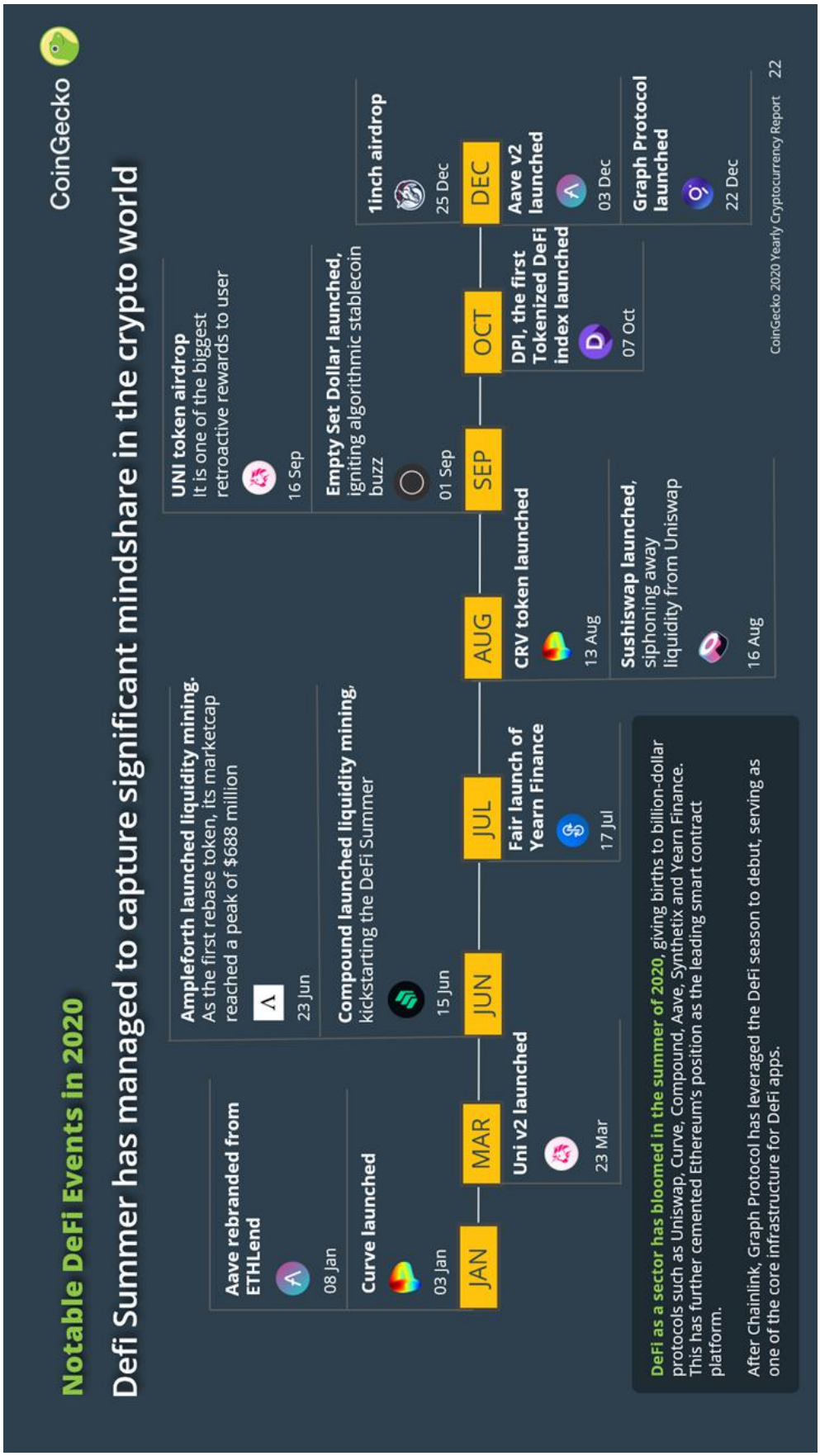
Source:CoinGecko

对于一些2020年没有参与进DeFi的读者们，我们在下一页梳理出了一个2020年主要DeFi事件发生的简短时间线，供您快速了解。

2020年的重点在于许多关键DeFi项目的协议与通证（代币）的发布。在这么多的DeFi协议中，有许多都推出了高收益的流动性挖矿项目，以吸引更多用户去使用这个协议。

流动性挖矿（Liquidity mining）并不是DeFi里一个陌生的概念。这是DeFi协议中为赋予协议流动性的用户，发放协议原生代币作为奖励的激励项目。这种项目于2019年7月份时由Synthetix首次推出，后来在2020年6月因Compound而被大众所熟知。

正因流动性挖矿项目的流行，许多新项目都于2020年夏季诞生，并且许多项目还以食品、蔬菜命名其协议代币，例如“芋头（Yam）”与“腌黄瓜（Pickle）”等。用户作为“农民（Yield Farmer）”度过了一整个忙碌的夏天，积极将资金投入到各式各样的DeFi协议中，试着寻求最高的挖矿收益。



来源：CoinGecko 2020 年度报表

Yearn Finance作为一个收益聚合平台，于2020年7月掀起了“（fair launch）”的浪潮。其治理代币YFI，并没有面向投资者进行任何早期的Private Sales，而是公平地分配给了任何想要参与的用户。随后故事继续以Curve Finance，在2020年8月份“意外”发行了CRV代币而延续着。

同月，Uniswap的对家 - SushiSwap发布了。SushiSwap进行了“吸血鬼挖矿（Vampire Mining）”并推出发行了SUSHI代币，来试图迁移Uniswap的流动性至SushiSwap。

不甘示弱地，Uniswap在2020年9月份举办了一次UNI代币空投，为所有使用过Uniswap协议的用户带来了一笔意外的收益。（注：如果您阅读了我们2020年发布的《How to DeFi：入门》并在空投之前使用了Uniswap，您也会收到UNI代币！）

这引发了另一波加密狂潮，许多项目选择发行代币来达到促进发展和吸引用户的目的。没有代币的项目也随后很快发现自己不得不考虑进一步发行代币来提高自己在市场中的竞争性。

DeFi生态系统

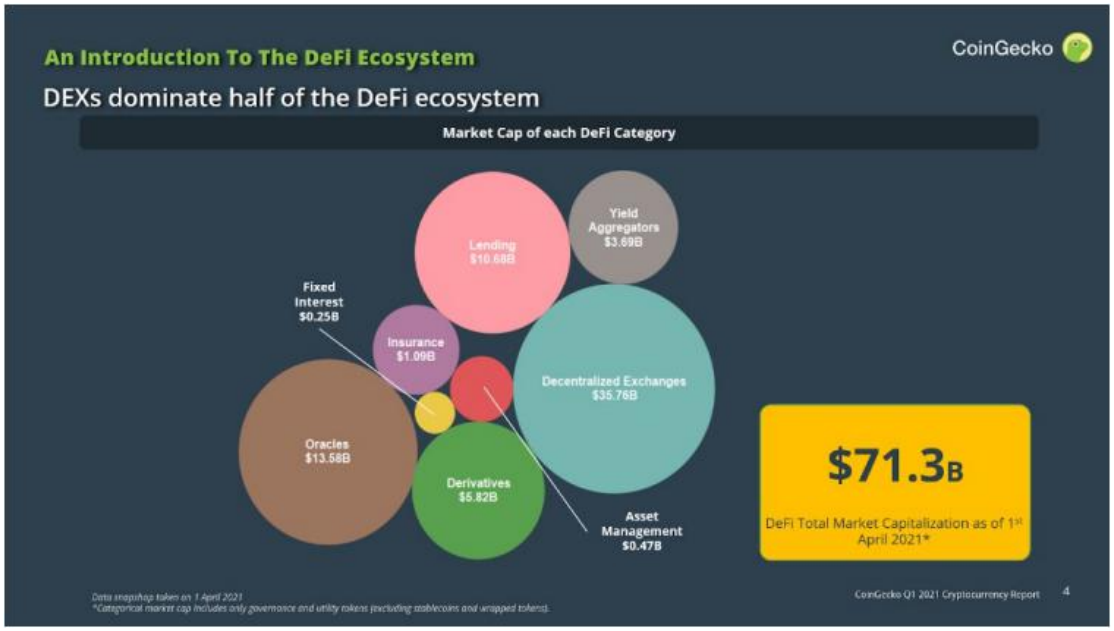
DeFi的总锁仓价值（TVL）在2021年4月份已然突破了860.5 亿美元。TVL是DeFi中最被广泛使用的指标之一，因为它代表了每个协议持有的资产总量。经验之谈：协议中的锁定价值越高，这个协议就越好。

在大多数情况下，锁定的资产会用于整个生态系统中，提供做市、借贷、资产管理和套利等服务，通过这些过程为资产提供者赚取其收益。

然而，TVL并不永远是一个可靠且有效的指标，因为资本可能会受到像流动性挖矿这样的短期激励因素，或像智能合约漏洞这样的外部催化因素的影响，导致TVL波动频率较大。因此，用户有必要跟踪观察一段时间内TVL的变化，以衡量其协议资产的留存率与其用户粘性。

如此大量的资金被锁定在这个领域内，各种DeFi应用（Dapps）应运而生，向传统金融理论的规范和边界发起挑战。新的金融实验每天都在上演着，催生了像算法稳定币这样的新类别。

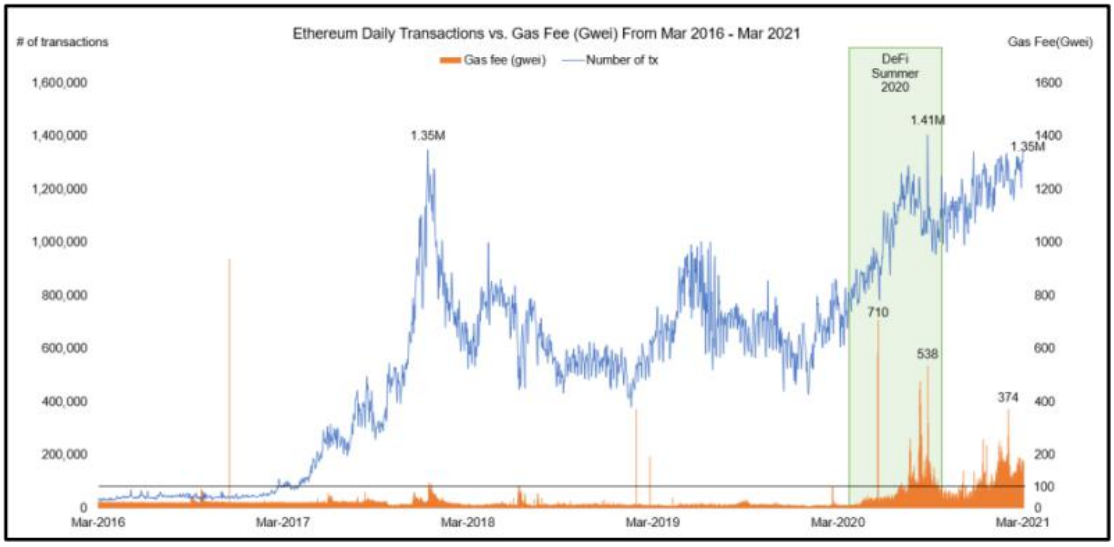
以下是基于市值的新兴 DeFi 生态系统的概述。去中心化交易所类别是价值最高的类别，其次是预言机和借贷类别。



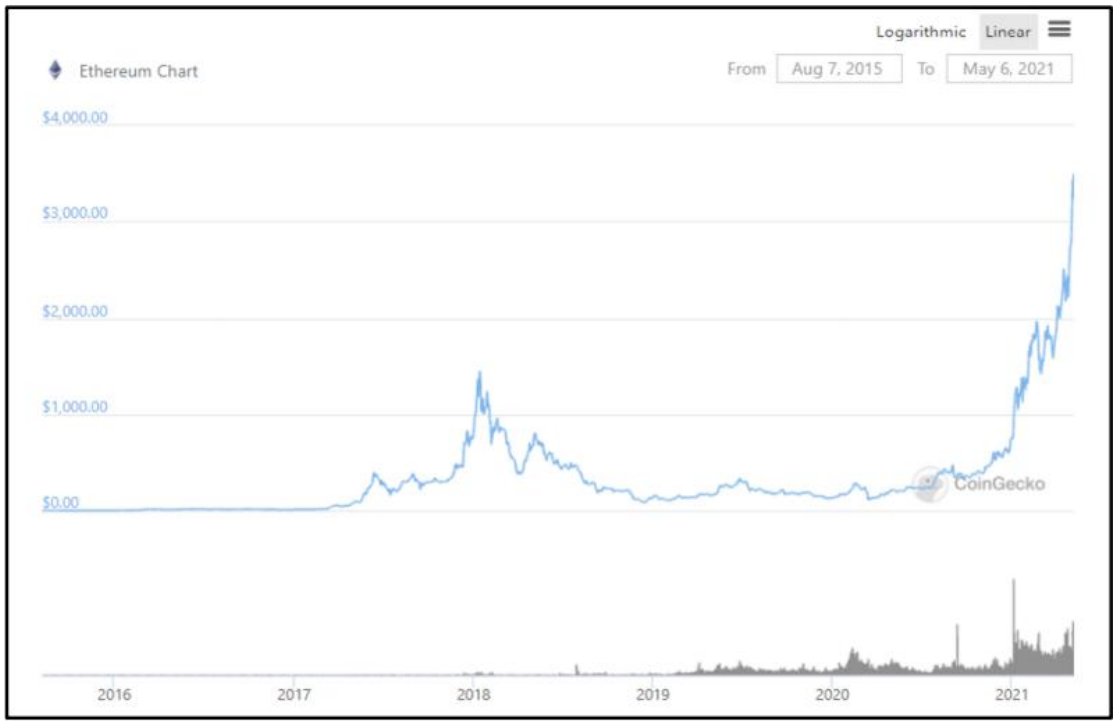
来源：CoinGecko Q1 2021报告

Gas费的上涨

自2020年初以来，以太坊的交易数量持续上升，日均交易超过100万笔。交易水平似乎有望突破2018年的峰值水平。



大量的交易导致了Gas费的上涨，截至2020年8月，每笔交易高达700gwei。虽然2021年Gas费低于2020年DeFi Summer，但2021年ether价格要高得多，导致整体交易费用上涨。以太坊在2021年1月打破了之前的历史高点，并在2021年5月12日创下了4357美元的新高!



来源:CoinGecko

高昂的Gas费和以太坊价格的上涨使得以太坊上的许多DeFi Dapps用户在没有大量资金的情况下使用不再具有经济可行性。在2021年第一季度完成Uniswap上的一个简单的交易，每笔交易可以累积高达100美元的费用，这使得它只适用于大型交易。对于更复杂的交易，如产量种植交易，交易费用甚至会更高。

高昂的交易费用导致许多以太坊DeFi用户在其他地方寻找更便宜的替代品。其他一些选择包括转移到第2层(如，Optimism, Arbitrum和zkrollps)，侧链(如，xDAI和Polygon)，或竞争的第1层链(如，Binance Smart Chain, Solana和Terra)。我们将在第14章更详细地讨论这些内容。

DeFi将成为金融的主流旋律

加密行业在2021年上半年吸引了很多关注。发生在全球各地的重大事件不断登上各大媒体的头条新闻：

1. 特斯拉15亿美元的比特币初始投资

2. 在佳士得拍卖会上，Beeple拍卖了价值6900万美元的NFT（Non-Fungible Token）艺术品(Everydays: the First 5000 Days)

3. Visa支持USDC作为以太坊上的结算选项

4.富达的比特币交易所交易基金计划

5.Coinbase在纳斯达克上市

6.中国对比特币和其他加密资产作为替代投资的积极看法。

在广泛的加密市场中，媒体报道数量不断增加也引起了更多的人关注DeFi。机构投资者尤其开始注意到这一点。例如，在花旗银行(Citibank)的全球视角和解决方案(Citi GPS)报告（货币的未来:加密货币、央行数字货币和21世纪现金）“Future of Money: Crypto, CBDCs and 21st Century Cash”中，这家拥有209年历史的银行强调了DeFi的优势。其中包含了能够跨越第三方中介机构以及提高金融透明度。值得注意的是，该报告还探讨了各种DeFi协议，如Maker, Compound, Uniswap和UMA。圣路易斯联邦储备银行(Federal Reserve Bank of St Louis)的一份深度报告强调：DeFi带来“金融业范式转变的潜力，并可能有助于建立更强健、开放和透明的金融基础设施”。

与此同时，我们也看到投资机构进入DeFi。Grayscale是较为著名的数字投资基金之一，它正通过股票信托积极提供对DeFi资产的敞口。(如Chainlink) Bitwise资产管理基金也有一个DeFi指数基金，提供超过10种DeFi资产的敞口，如Aave和Compound。该基金于2021年3月成立，在短短两周内筹集了3250万美元。

DeFi也不会停在虚拟线上。想象中的DeFi“现实世界”用例已经实现，DeFi协议被认为是传统银行工具的合适替代品。

Centrifuge是首批与MakerDAO整合的“现实世界”公司之一，它正在通过他们的应用Tinlake将非数字资产作为抵押品。2021年4月21日，该公司以房屋作为抵押，成功地执行了其第一笔18.1万美元的MakerDAO贷款，有效地创建了第一批基于区块链的抵押贷款之一。

第二章：DeFi事件

流动性挖矿

流动性挖矿不出意外应该是DeFi领域最具创新性的功能之一，指的是用户将资产分配进各个DeFi协议中，从而获得收益的这一个过程。

大多数的DeFi协议其实就是个点对点金融应用程序。其中，用户分配进协议的资金将会用于为协议的最终用户提供服务。用户使用协议收取的费用随后会被资产提供者和协议本身共享，资产提供者获得的费用将通过真实的收益率呈现。

更口语化地讲，这些资产提供（投资）者被我们统称为“产量农民（yield farmers)”，提供收益率的机会被称之为“农场（farms）”。许多“产量农民”不停地转战至不同的“农场”，以寻找能提供“最高产量”的机会。

以下是一些流动性挖矿的例子，“农民”为协议提供的资金将会用于以下目的：

- 交易——为去中心化交易所的做市环节提供资金，并赚取交易费用作为回报。
- 贷款——向借款人提供贷款，赚取利息。
- 保险 - 保险承保，赚取保费的同时承担在市场灾祸期间支付索赔的风险。
- Insurance - Underwrite insurance, earning premiums while undertaking the risk of paying out claims during disasters.
- 期权 - 通过卖出看涨期权或看跌期权来承销期权，赚取收益。
- 合成资产 - 铸造稳定币或其他合成资产，作为回报可以赚取费用。

空投

空投本质上其实就是项目方自由分发给用户的代币。项目通常将空投作为其市场营销策略的一部分，以为代币发布引起足够多的关注和炒作，尽管会影响到权衡后相对减少的代币所有权。

有部分项目还会对在其协议早期进行交易的用户进行空投。每个协议都有一个成为合格空投接收者的标准，例如与协议交互的时间和使用量方面的限制。

一些曾经比较引人注目的空投如下所示：

Protocol	Token symbol	Date Airdrop	Initial Price	Price as of 1st April 2021	Return
Uniswap	UNI	16 September 2020	$3.44	$28.71	734.59%
1INCH	1INCH	25 December 2020	$2.36	$4.46	88.98%
PoolTogether	POOL	17 February 2021	$11.98	$23.11	92.90%

最著名的空投之一便是 Uniswap 平台进行的空投，当时早期的用户至少都获得了 400UNI。截止 2021 年 4 月 1 日，空投价值高达 11484 美元。（注：如果您在 2020 年阅读过我们的《How to DeFi:入门》，并在空投前使用了 Uniswap，您也会收到 UNI 代币空投！）

首次区块链数字资产发行(IDO)

加密项目必须在其代币发行和分发策略方面具有一定的创造性。随着去中心化交易所 (DEX) 的日益普及，项目方现在有了另一个可行的选择 — 直接面向用户，而不需要遵循传统的方式去支付高额费用，即可在中心化交易所上市。加密项目团队现在可以在不需要这些 DEX 许可的情况下列出他们的代币。

然而，以公平的价格向广大用户无区别化的去分配代币仍然是一项艰巨的任务。项目可以用的 IDO 方式有很多种，我们将带大家来研究一些比较热门的方式。

联合曲线公开发行 (IBCO)

联合曲线公开发行，或 IBCO，是一个防止抢跑交易（Front running）的新概念。基本上来说，随着越来越多的投资者提供资金进入联合曲线模型，代币价格将从其初始价格开始增长。

不过这个方式之下，选择何时提供资金并不重要，因为所有投资者到最后都将根据相同的最终结算价格进行支付。根据 IBCO 结束时的价格，每个投资者将依据其在总投资中所占的份额来获得代币。 Hegic 和 Aavegotchi 等项目都在最初的代币发行中使用了这种分配方法，在最后取得了巨大的成功。

流动性引导池（LBP）

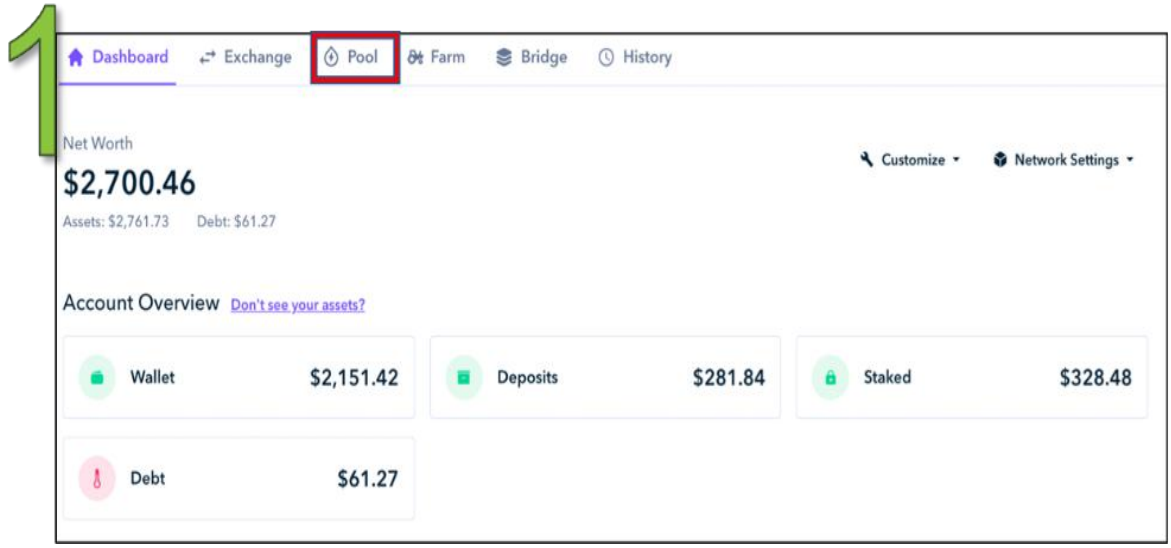
流动性引导池 (LBP) 运用 Balancer 的智能池来托管，是项目使用有配置性的自动做市商（AMM）来出售代币的一种方式。通常，这些池将包含项目代币和抵押代币，通常以稳定币计价。智能池的控制器可以更改其参数并为销售引入各种功能，例如随着时间的推移价格下降以及由于高需求或外部漏洞而暂停任何进一步的掉期。

初始农场产品 (IFO)

PancakeSwap 首次推出的初始农场产品 (IFO) 允许用户质押他们的流动性提供者 (LP) 代币以换取项目的代币。使用溢出机制，用户可以随心所欲地投入多少。在超额认购的情况下，任何多余的代币都将退还给投标人。 PancakeSwap 上的 IFO 使用 CAKE-BNB LP 代币，其中项目接收 BNB 代币以换取其新铸造的协议代币，而剩余的 CAKE 代币则被烧毁。

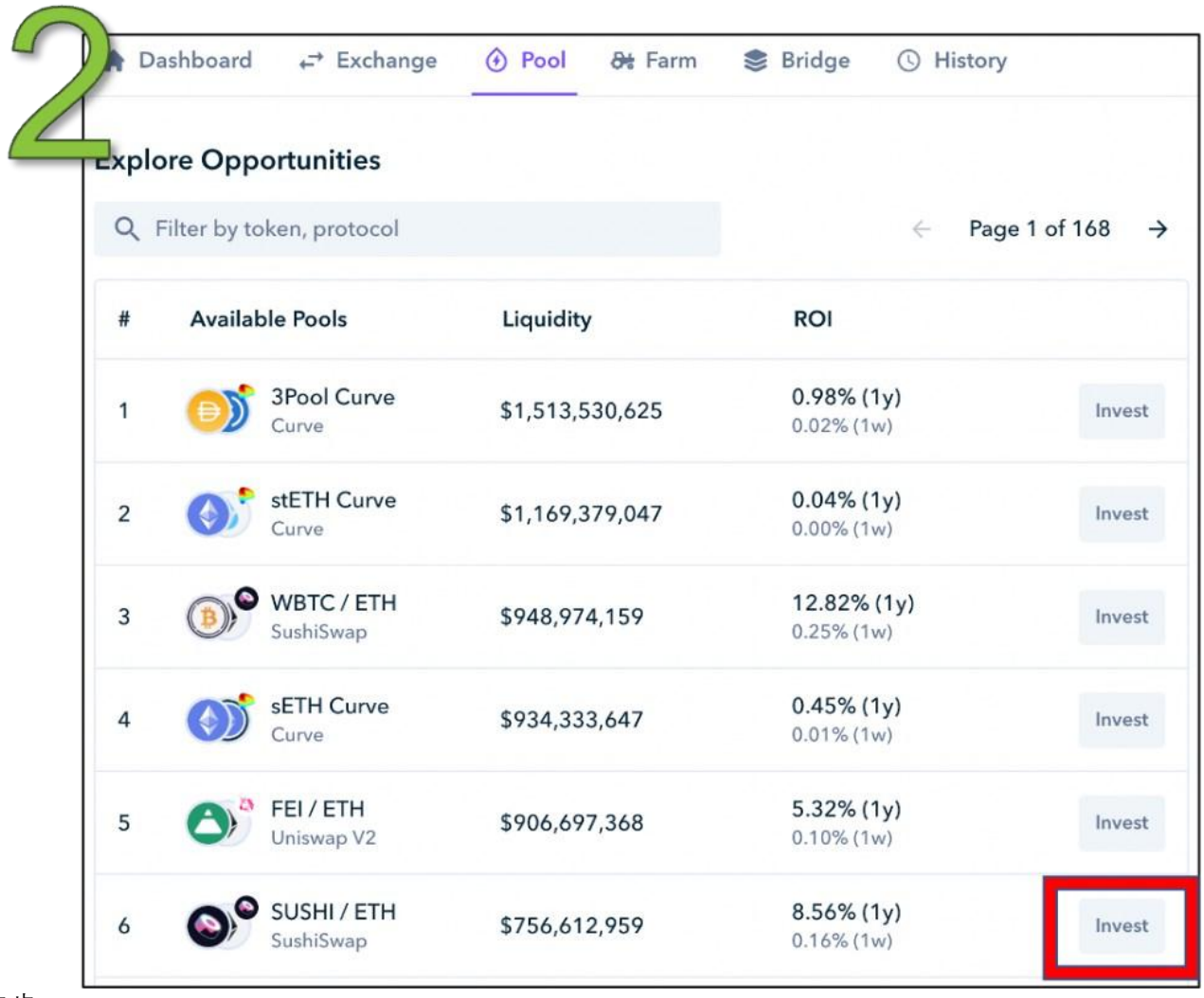
流动性挖矿步骤教学

接下来，我们将为大家展示流动性挖矿的详细步骤教学。通过运用本章之前提到的 SUSHI-ETH 来示例，我们将展示如何使用 Zapper 去提供流动性。



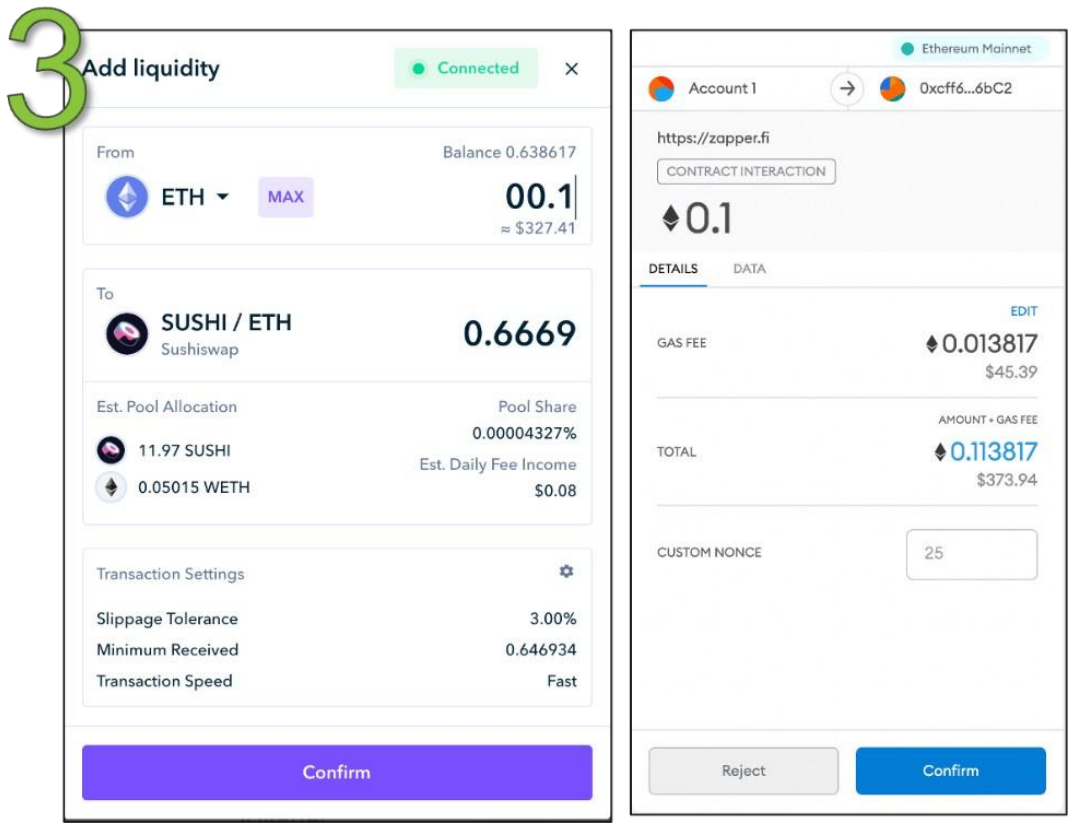
第一步

- 在此网站中连接上您的钱包：https://zapper.fi/dashboard
- 在网站中选择“Pool（流动池）”这个选项。



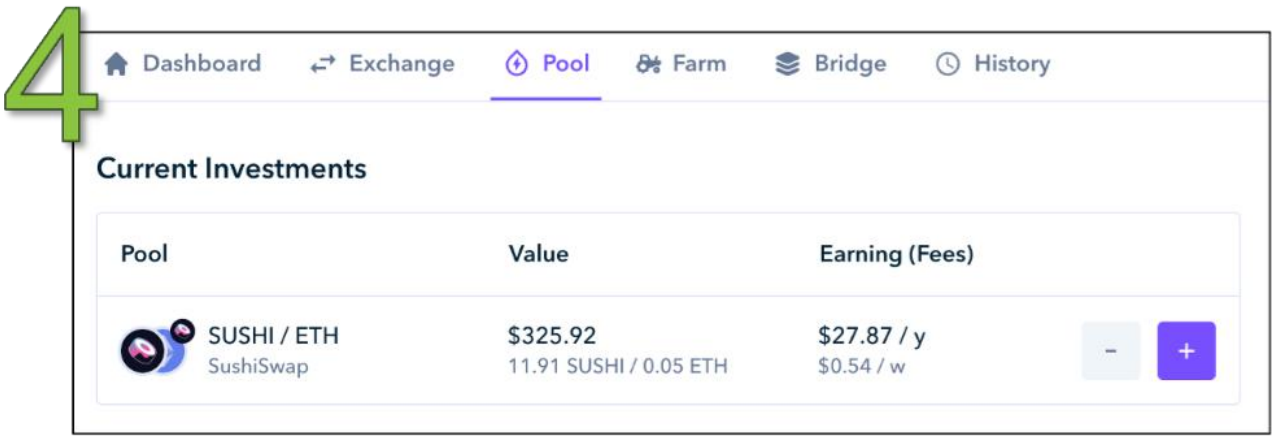
第二步

- 在这篇教学指导中，我们将要为 SUSHI-ETH 提供流动性，从而获得 SUSHI 代币。
- 找到自己想要提供流动性的对子，选择“Invest（投资）”



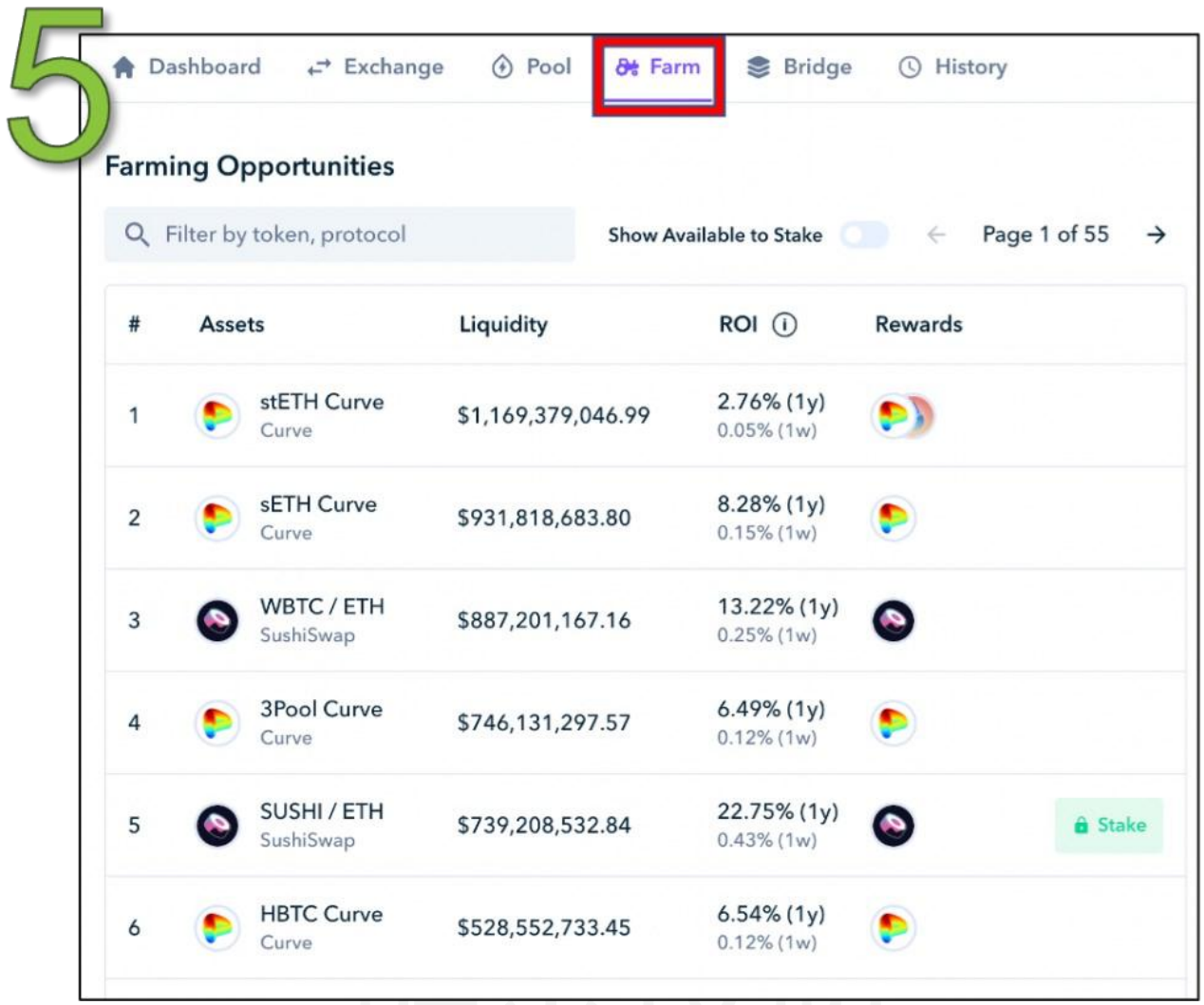
第三步

- 在 Zapper 中，我们可以以任何单一的资产去兑换任何 LP 通证（代币）。在这里我们将使用 SUSHI-ETH 兑换至 ETH。
- 点击“Confirm”来确认交易。



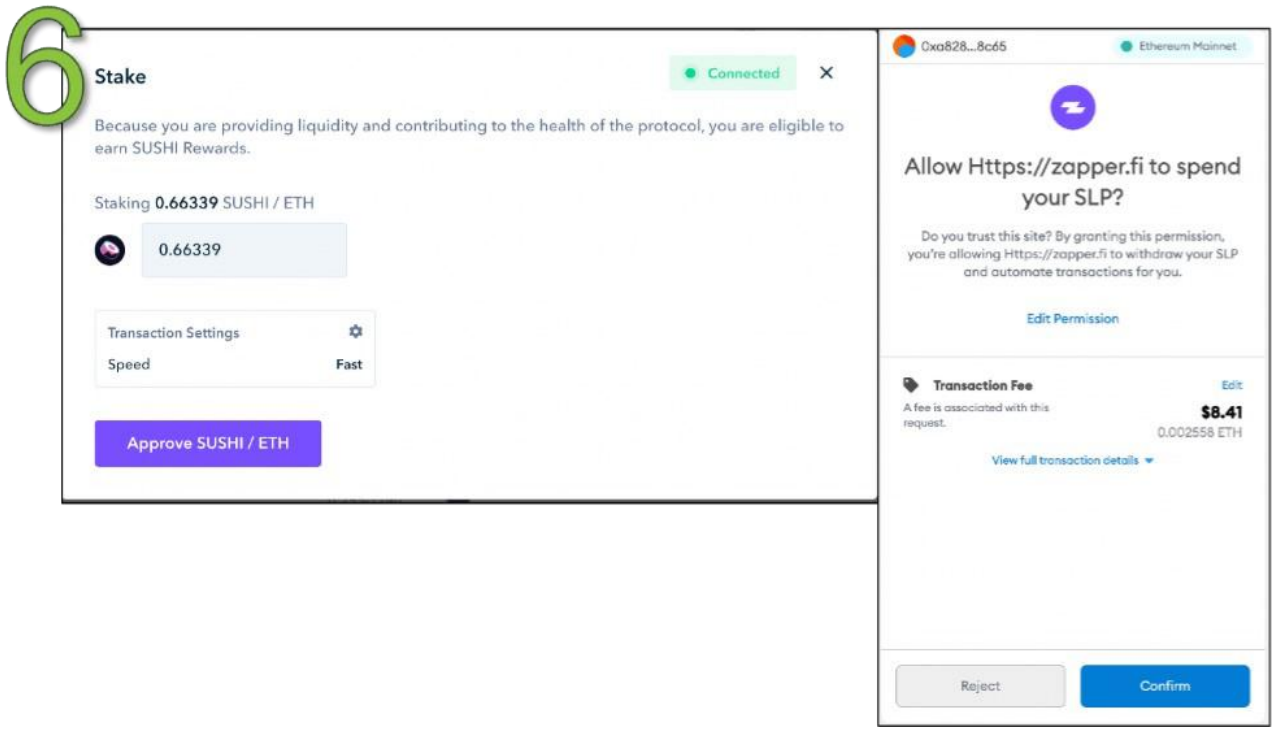
第四步

- 在“Current Investment（现阶段投资）”下面会出现 SUSHI-ETH 这个对子。



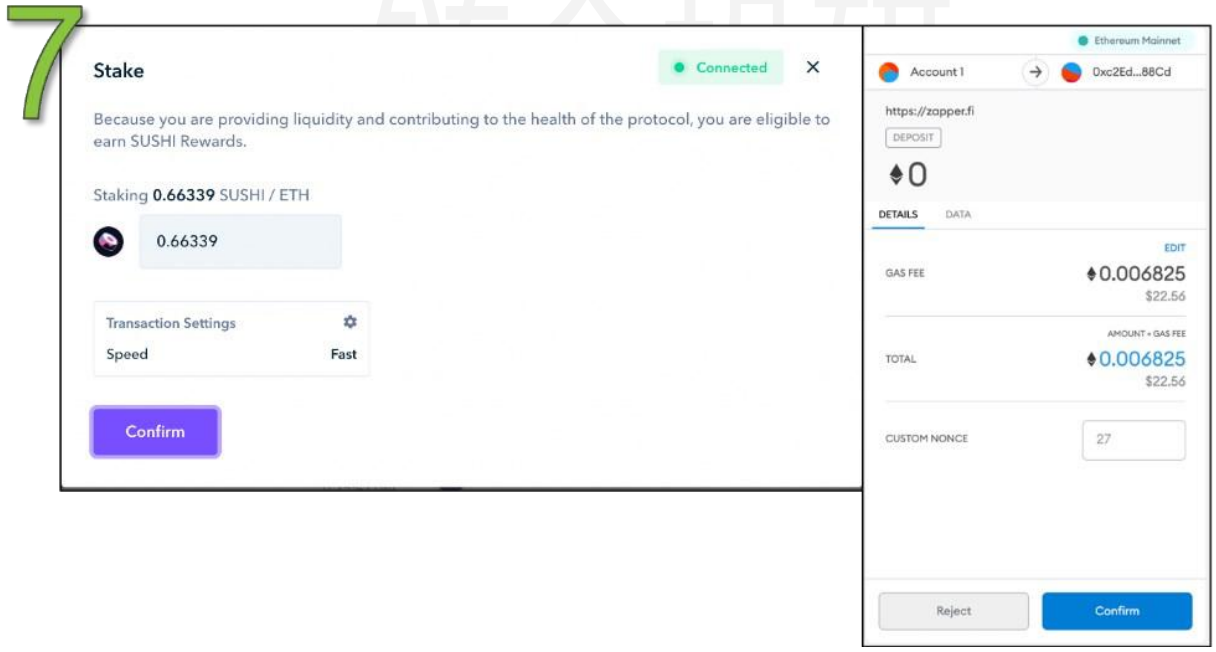
第五步

- “农场”选项卡列出了高产农业机会及其各自的预期回报。
- 如果我们拥有标的资产，则会出现一个绿色的“Stake”按钮为高产农业机会。
- 点击“Stake”来质押。



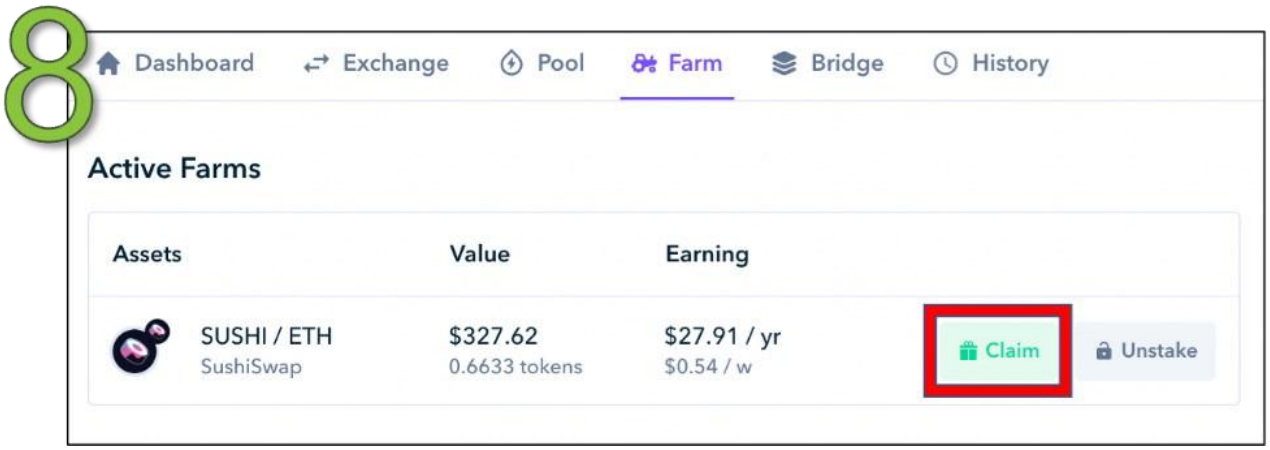
第六步

●“Confirm”准许交易，为 Zapper 对 SUSHI-ETH LP 通证开放权限。



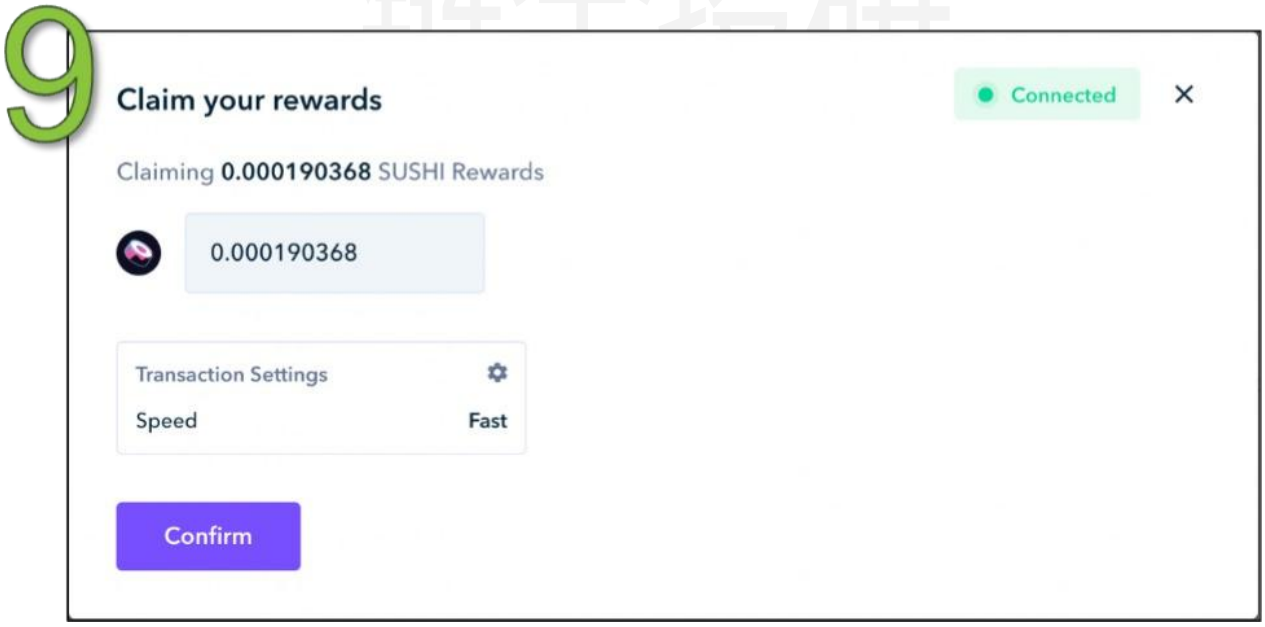
第七步

●“Confirm”来确认交易。



第八步

●现在就有资格获取交易费与流动性挖矿的奖励。
●点击“Claim”来查看获得的奖励



第九步

●点击“Confirm”来确认领取奖励
●如图 8 所示，通过点击右边的“Unstake”可以撤销投资。

相关风险

一旦您熟悉了 DeFi 的生态系统，您将不可避免地看到各种协议提供的令人瞠目结舌的收益率，有时甚至可能超过 1000%的年收益率 (APY)！虽然这么高的收益率听起来很诱人，但这种 APY 通常只是暂时的，一旦其他产量农民开始加入，最终收益率还是会稳定到一个相对低的数字。

鉴于 DeFi 是一个快节奏的世界，关于一个项目是否值得投资，投资者必须要具备快速决定的能力。 其实，投资者对“错过”的恐惧 (FOMO) 是真实存在的，因此不应掉以轻心。

最关键的是，无论您是交易者、投资者还是流动性提供者，都应时刻警惕智能合约风险、无常损失风险和相关常见的系统性风险。无论一个项目在技术上听着多么合理，心存恶意的人总是有可能利用流动性挖矿的漏洞去制造麻烦。

每个 DeFi 用户都需要明白这一点：DeFi 生态系统现在仍处于起步阶段，大多数 DeFi 活动也仍处于实验阶段。在这整本书中，我们将涵盖每个 DeFi 类别会涉及到的不同类型的风险，并将整个第十五章节专门用于讲述智能合约漏洞利用造成的相关风险。

结论

DeFi 是一个极具开创性的新兴加密领域。就现在，我们正在目睹一场金融革命的发生，这场革命使融资渠道变得民主化，同时促进了金融包容性，并保障了用户的金融透明度。尽管当前仍在迭代中的 DeFi 还并未达到其理想状态，但它确实让我们瞥见了未来可以是什么样子。

世界上任何可以访问互联网的人现在都有资格参与到这个盛大的金融实验中，例如成为一名流动性提供者和代币化所有权，允许新组织形式的形成。相信不久后我们就会看到 DeFi 协议的发展，会比世界上的几大公司更有价值。

推荐读物

1.治理代币：对于崭新经济社会一砖一瓦的投资
https://thedefiant.io/governance-tokens-investing-in-the-building- blocks-of-a-new-economy/
2. 关于实用型代币的新模型
https://multicoin.capital/2018/02/13/new-models-utility-tokens/
3. 流动性引导常见问题解答
https://docs.balancer.finance/smart-contracts/smart-pools/liquidity-bootstrapping-faq
4. 什么是流动性挖矿
https://learn.zapper.fi/articles/what-is-yield-farming

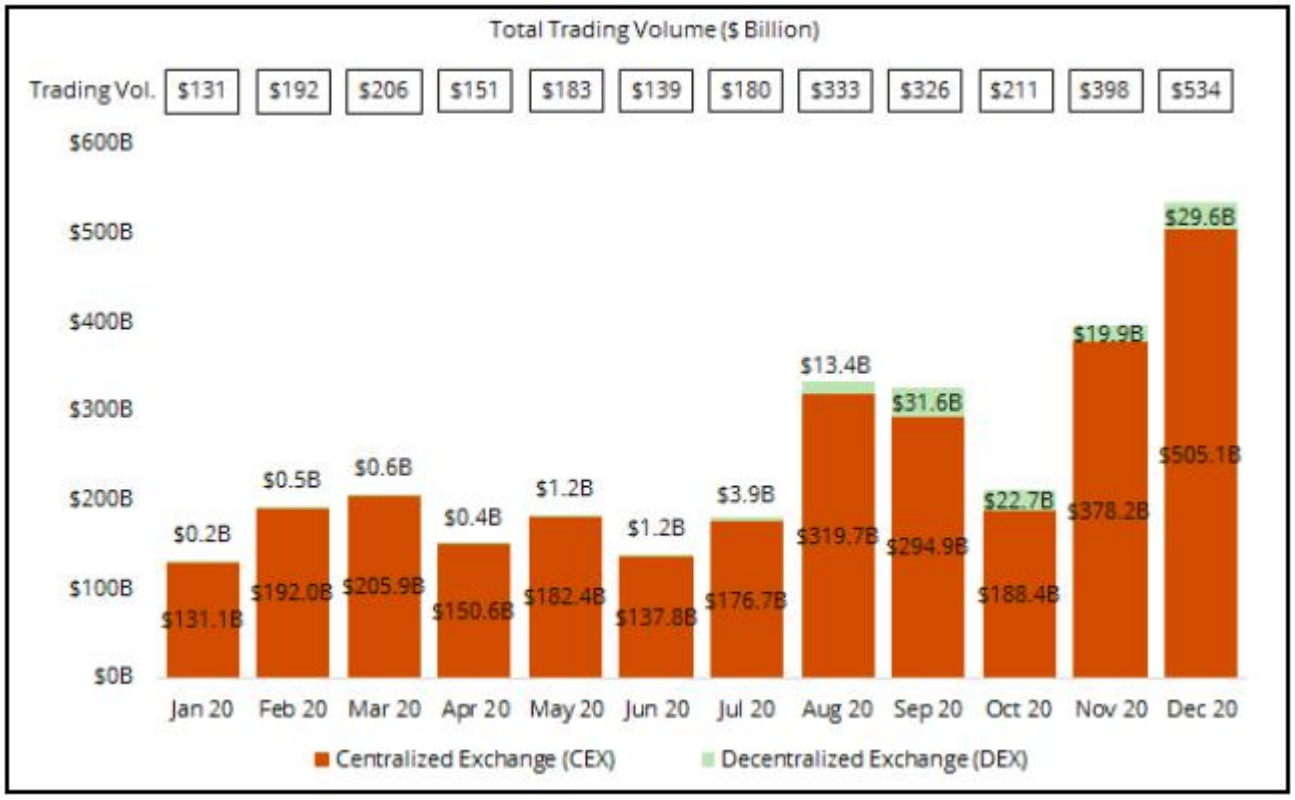
第二部分：评估DeFi部门

第三章：去中心化交易所

无论您是尝试进行简单的掉期交易还是积极交易，您都会需要交易所的服务。 理想情况下，这家交易所必须具有低延迟和深度流动性，以便您拥有最佳价格执行并且不会受到价格滑点的影响。

从历史上看，中心化交易所 (CEXs) 提供了更好的流动性并促成大多数大型交易。 然而，它们有几个弱点——最值得注意的是中心化实体的用户不保管他们的资产。 例如，2020 年 9 月，KuCoin 在安全漏洞后遭受了 2.81 亿美元的黑客攻击。 CEXs 也会随时停止交易并阻止用户提取资金。

2020 年和 2021 年，去中心化交易所 (DEXs) 发展迅速，开始与中心化交易所竞争。 前 9 名 DEX-CEX 比率从 2020 年 1 月的仅 0.2% 提高到 2020 年 12 月的 5.9%。 2020 年，前 9 名 DEX 的交易量呈指数增长 17,989%，达到 300 亿美元。



数据来源：*CoinGecko 2020* 年度报告

但究竟是什么让 DEX 成为……一个 DEX?

DEX 是一个无需中介（即中心化交易所）即可进行代币交易和直接交换的平台。您无需经历了解您的客户 (KYC) 流程的麻烦，也不受司法管辖区的限制。

DEX 的类型

DEX 有两种类型:

1. 基于订单簿的 DEXs

订单簿是特定资产在不同价格水平的买卖订单列表。

dYdX、Deversifi 和 Loopring 等基于订单簿的 DEX 的运作方式与 CEX 类似，用户可以按照他们选择的限价或市场价格设置买卖订单。 主要区别在于，在 CEX 中，交易资产保存在交易所的钱包中，而对于 DEX 来说，交易资产保存在用户的钱包中。

DEX 的订单簿可以是链上的，也可以是链下的。 基于链上订单簿的 DEX 将所有订单记录在区块链上。 然而，由于高油价（gas 费，下同）的影响，这在以太坊上不再可行。 也就是说，对于链上订单簿

方案的 DEX 采用 2 层以太坊（layer 2）解决方案（如 xDai）或者高处理量 1 层区块链（如 Solana）上仍然可行。

基于链下订单簿的 DEX 将交易订单记录在区块链之外。交易订单在匹配之前一直保持链外状态，而交易过程在链上发生。 尽管这种方法具有较低的延迟，但有些人可能会认为，使用这种方式的 DEX是半去中心化的。

2. 基于流动性池的 DEXs

流动性池是基于 DEX 智能合约的代币储备，可供用户交换代币。 大多数基于流动性池的 DEX 会用到自动化做市商 (AMM)，这是一种通过算法预先定义资产价格的数学函数。

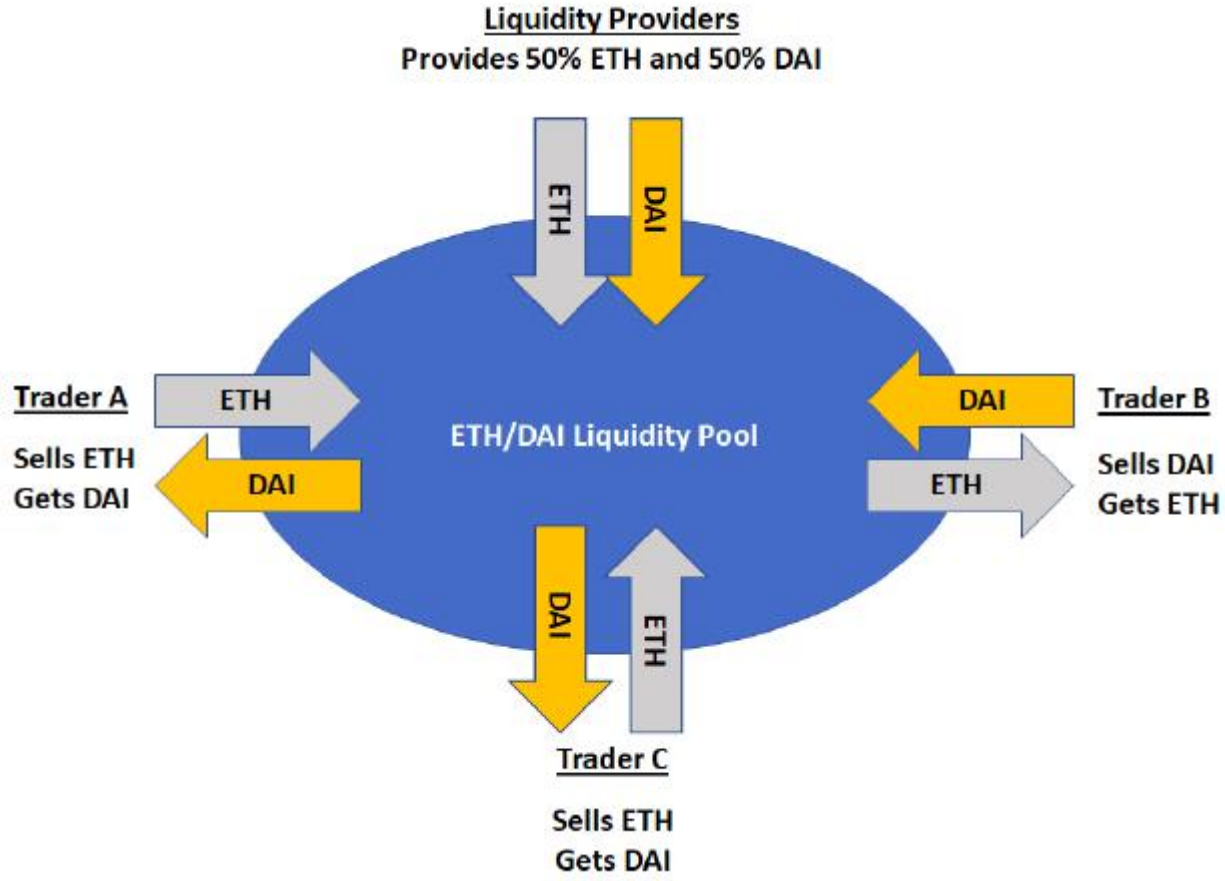
AMM 是 DeFi 近年来最具创新性的发明之一。 它实现了 24/7 的市场时间、提高了资本可及性和效率。 市场上存在多种不同类型的 AMM，这使得的 DEX 实现了各种特征属性。 2020 年 DeFi 夏季期间推出的 DEX 大多是都是基于 AMM 的 DEX，例如 Uniswap、SushiSwap、Curve、Balancer 和 Bancor。

由于多数新出现的 DEX 都是基于 AMM，我们将在本章的其余部分重点介绍一些 AMM 示例。

自动化做市商 (AMM)

在我们的《如何 DeFi：初学者》一书中，我们介绍了最受欢迎的 AMM Uniswap。 以下是 AMM 中流动性池如何运作的回顾。

与在订单簿上放置买卖订单的中心化交易所不同，AMM 没有任何订单簿。 相反，它依赖于流动性池。流动性池本质上是储备，其中包含两个或多个代币，这些代币位于 DEX 的智能合约中，可供用户随时进行交易。



您可以将流动性池视为可以交易的代币池。假设您希望将 ETH 交换为 DAI，您将在 ETH/DAI 流动性池上进行交易，方法是添加 ETH 并从流动性池中减去通过算法确定的 DAI 数量。

存款人，即流动性提供者（LP），为这些流动性池提供保障。LP 根据每个 AMM 的预定义代币权重（在 Uniswap 的情况下 - 每个代币 50%）将他们的代币存入流动性池。

LP 在流动性池中提供资金，因为他们可以从他们的资金中赚取收益，这些收益是从 DEX 上交易用户的交易费用中收取的。 任何人都可以成为 LP， 并通过将他们的资金存入智能合约来自动做市交易对。

有了AMM，交易者可以无缝执行他们的订单，而无需中心化做市商在 Coinbase 或 Binance 等中心化交易所提供流动性。 相反，订单是通过智能合约自动执行的，该合约将通过算法计算交易价格，包括交易执行中的任何滑点。 因此，您可以将基于订单簿的交易视为遵循点对点模型，而 AMM 遵循点对合约模型。

现有的 AMM 类型有哪些?

AMM 是一种数学函数，可根据流动性池对资产进行算法定价。 目前，有几种 AMM 公式用于满足不同的资产定价策略。

以下是一些比较流行的 AMM 公式:

一、恒定乘积做市

恒定乘积做市商公式首先由Uniswap 和 Bancor 以及市场上其他一些最受欢迎的 AMM 推广。 绘制时，它是一条凸曲线，其中 x 和 y 代表流动性池中两个代币的数量，k 代表乘积。 该公式有助于根据每个代币的可用数量为两个代币创建一系列价格。

为了保持恒定的乘积 k 不变，当 代币x 的供应增加时，y 的代币供应必须减少，反之亦然。 因此，由此产生的价格本质上是不稳定的，因为交易规模可能会影响与池规模相关的价格。 大笔交易导致更高的滑点可能会造成永久性损失。

二、 恒定和做市

恒和做市商公式在绘制时， 创建的是一条直线。 它是零滑点交易的理想模型，但不幸的是，它不能提供无限的流动性。 该模型存在缺陷，因为当报价与其他地方交易的资产的市场价格不同时，它提供了套利机会。 套利者可以耗尽流动性池中的全部储备，从而为其他交易者留下更多可用的流动性。 此模型不适合大多数 AMM 用例。

三、 恒定平均值做市

$$v = \prod_t B_t{}^{w_t}$$

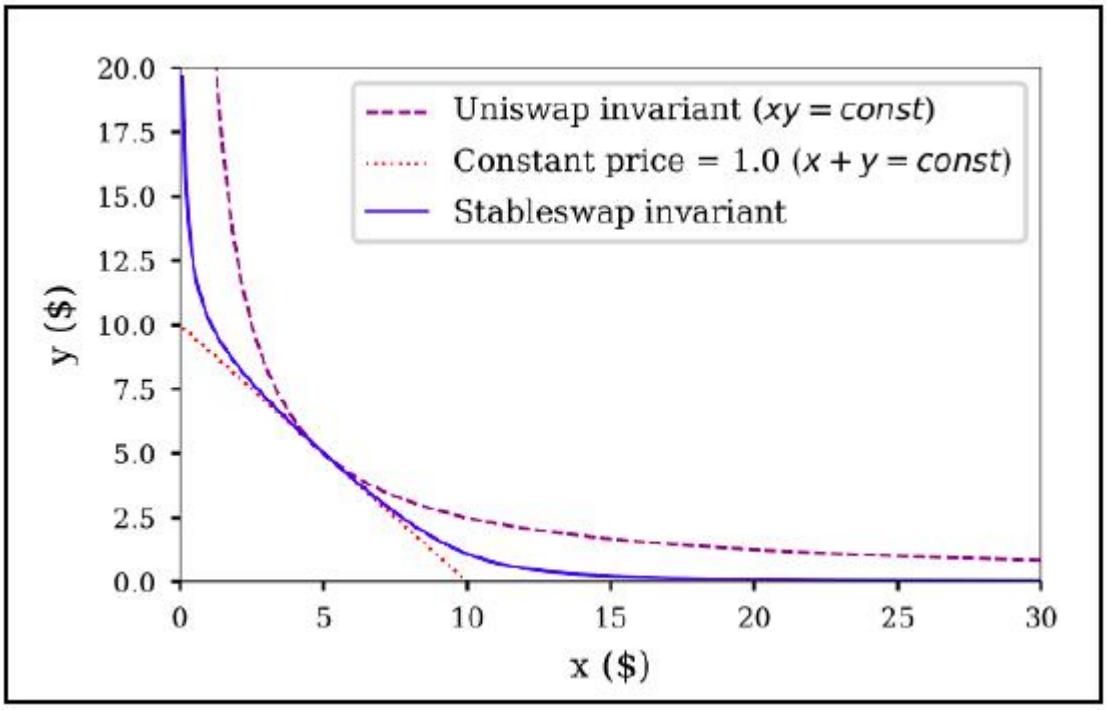
恒均值做市商公式， 又称价值函数，是由 Balancer捧红的。 它允许 拥有两个以上代币的流动性池以及超过标椎50/50分布的不同代币比率。 和乘积不同，这种模型中的加权几何平均值保持不变。 这允许对池中不同资产的可变风险敞口，并允许在流动性池的任何资产之间进行互换。

四、 稳定交换不变量

$$An^n \sum X_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$$

StableSwap Invariant 公式是恒定乘积公式 和恒定总和 公式的混合体。 它由Curve Finance捧红。

当投资组合相对平衡时，交易发生在恒定总和曲线上，当不平衡时切换到恒定乘积曲线。 这允许较低的滑点和无常损失，但仅适用于具有相似价值的资产，因为所需交易范围的价格始终接近 1。例如，这将有助于稳定币（DAI 和USDC）和包裹资产(w BTC 和 sBTC)之间的交易。



数据来源：https://curve.fi/files/stableswap-paper.pdf

此图显示了 Constant Product Market Maker（紫色线）和 Constant Sum（红色线）曲线，中间是 Curve Finance 使用的 Stableswap Invariant 混合曲线（蓝色线）。 我们可以看到 Stableswap Invariant 曲线在 Constant Sum 曲线附近创造了更深的流动性。 结果是一条线，它返回大多数交易的线性汇率和较大交易的指数价格。

恒定 乘积 AMM 的价格是如何确定的?

让我们看一个简单的恒定乘积做市商的例子，看看资产价格是如何通过算法确定的。 它的工作原理是根据池中每种资产的可用流动性数量维持一个恒定的乘积公式。

为了了解它是如何通过受欢迎的AMM工作的，我们将着眼于 Uniswap 推广的恒定乘积做市商：
需要注意的是，AMM 的市场价格只有在池中的准备金率发生变化时才会发生变化。 因此，AMM 上的资产价格可能与其他交易所不同。

例子
基于恒定乘积做市商公式
x * y = k
x = 储备代币 x
y = 储备代币 y
k = 决定流动性池中代币价格的恒定总流动性
例如：
截至 2021 年 4 月 21 日，Uniswap 的 DAI/ETH 流动性池中有 61,404,818 个 DAI 和 26,832 个 ETH。准备金率意味着 ETH 在撰写本文时的价格为 61,404,818 DAI / 26,832 ETH = 2,289 DAI。

假设 1 ETH 现在在 Uniswap 上的价值为 2,289 DAI。 但是当 ETH 的价格在其他地方（例如 Balancer）跌至 2,100 DAI 时，套利机会就会出现。 套利者将通过在 Balancer 上购买便宜的 ETH 并在 Uniswap 上出售以快速获利（为简单起见忽略交易费用）来利用价格差异。 套利者将重复此操作，直到价格达到两个交易所之间的平衡为止。

各种自动化做市商（AMMs)

Uniswap

Uniswap 是以太坊上的去中心化交换协议，它允许直接交换代币而不会放弃您的资金保管权。 要使用 Uniswap，您需要做的就是将您的钱包中的代币发送到 Uniswap 的智能合约，您将在钱包中收到所需的代币作为回报。

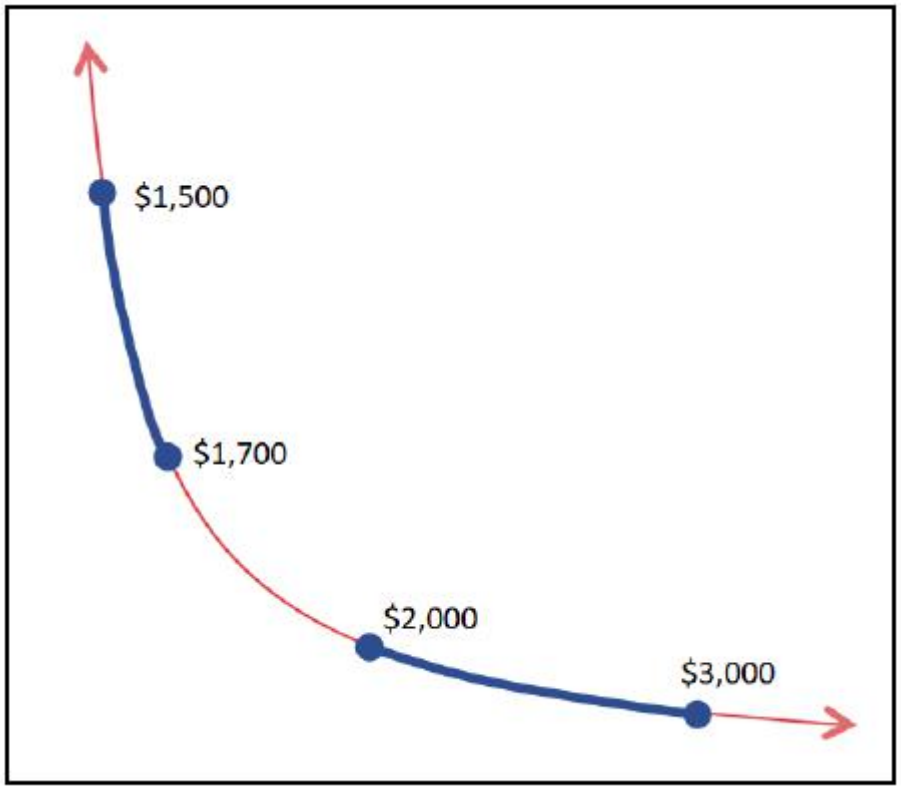
2018 年 11 月，Uniswap 公开上线，当时它推出了第一个版本，Uniswap v1。它是第一个基于 AMM 的 DEX，普及了恒定乘积做市商公式：

2020 年 5 月，Uniswap 增加了功能，将其智能合约升级到 Uniswap v2版本。 新版本增加了交易对来支持任何 ERC-20 代币。

2021 年 5 月 5 日，Uniswap 发布了最新版本 Uniswap v3。在最新版本中，Uniswap 引入了两个主要新功能：

1. 集中流动性

在 Uniswap v 3 中，LP 可以控制他们想要提供流动性的价格范围。例如，ETH/DAI 流动性池的 LP 可以选择将其资本的 30% 分配到 2,000 - 3,000 美元的价格范围，其余 70% 的资金分配到 1,500 - 1,700 美元的价格范围。



现在，在Uniswap v3上对流动性的新的主动管理为 LP带来了更高 的资本效率。 这样做的一个副产品是 LP 将收到不可替代的代币 (NFT)，而不是代表其 LP 头寸的可替代 ERC-20 代币。

2. 费用等级制

Uniswap v3 为流动性提供者提供了三层池费选择：

a. 0.05%

b. 0.30%

c. 1.00%

例如，USDC/DAI 交易对的价格波动性较低，可以保证较低的 0.05% 的池费。 ETH/DAI 交易对具有更高的价格波动性，将保证 0.30% 的池费。 同时，1.00% 的池费可能更适合更多的长尾或异国交易对。

SushiSwap

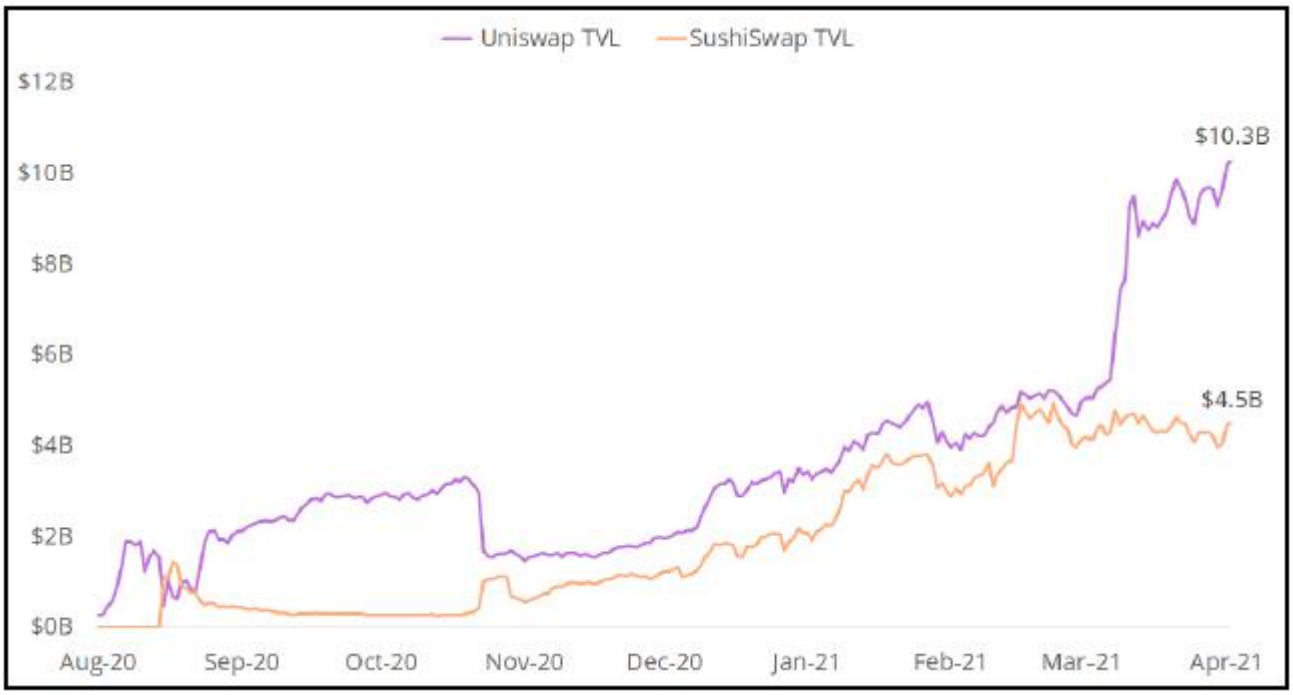
SushiSwap 于 2020 年 8 月 28 日由化名开发者 Chef Nomi 推出。它是 Uniswap v2 源代码的一个分支，并使用了相同的 恒定乘积做市商模型。在 Uniswap 还没有 UNI 代币的时候，SushiSwap 引入了 SUSHI 代币。 SushiSwap 提供的有吸引力的产量农业奖励引起了加密社区中许多人的注意。

2020 年 9 月 9 日，SushiSwap 对 Uniswap 的流动性发起了“吸血鬼攻击”，任何在 SushiSwap 上质押其 Uniswap LP 代币的人都会将其在 Uniswap 上的潜在流动性迁移到 SushiSwap。这次攻击耗尽了 Uniswap 一半以上的流动性，其总价值锁定 (TVL) 从 15.5 亿美元骤减到 4.7 亿美元。同时，SushiSwap 的 TVL 在一夜之间增至 11.3 亿美元。

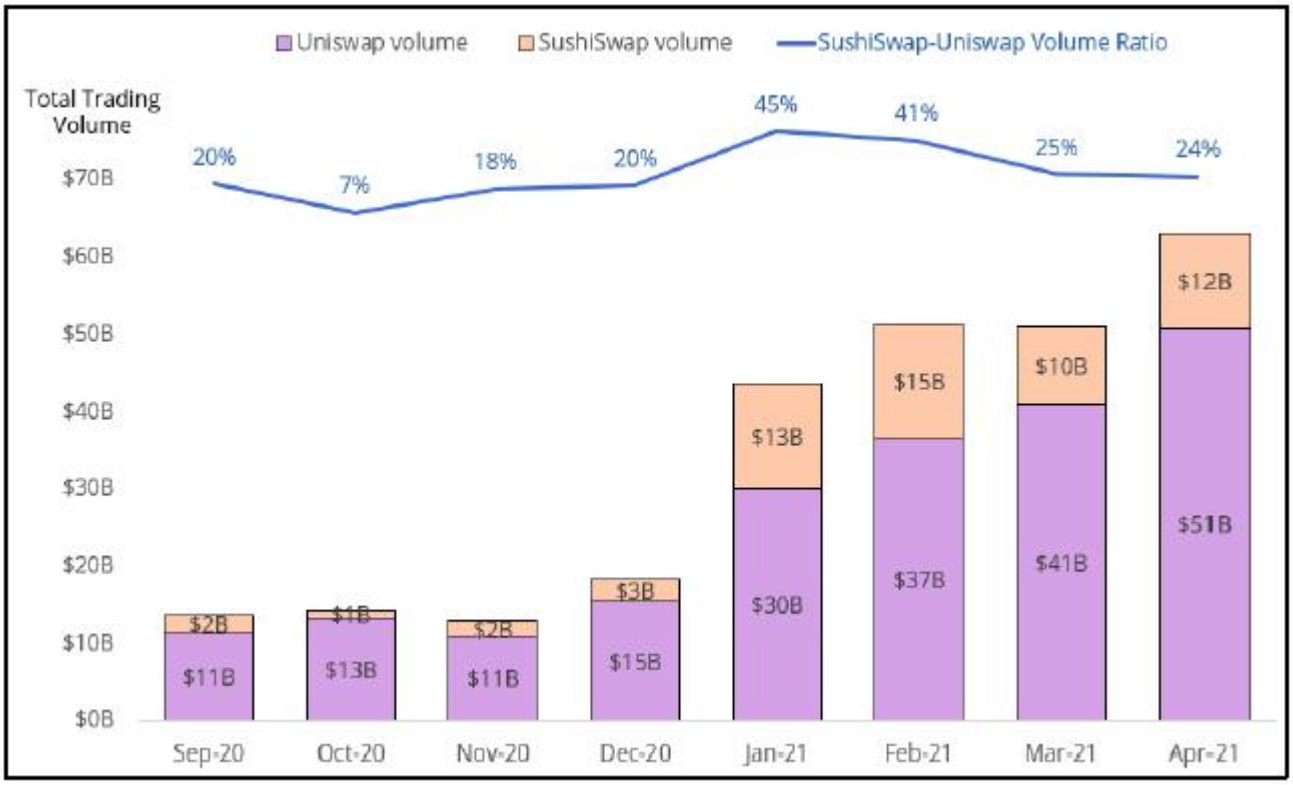
尽管受到“吸血鬼袭击”，Uniswap 仍然保持弹性，并很快恢复了对 SushiSwap 的 TVL 领先优势。截至 2021 年 4 月，SushiSwap 现在拥有 45 亿美元的 TVL，仅为 Uniswap 103 亿美元 TVL 的一半。

SushiSwap 发展迅速，现在是继 Uniswap 之后的第二大 DEX。 截至 2021 年 3 月，Uniswap 的交易量是SushiSwap 的四倍，这表明 Uniswap 在 DEX 市场上的领先地位。 2021 年前两个月，SushiSwap 表现强劲，占 Uniswap 交易量的 45%。

自推出以来，SushiSwap 通过提供更全面的产品系列而脱颖而出。 它还与Yearn Finance --一种挖矿收益聚合协议合作（合并），现在它是Yearn Finance 的AMM 部门。两者之间的主要区别在于池费、可用交易对和支持的区块链。



数据来源:
DeBank



数据来源：CoinCecko

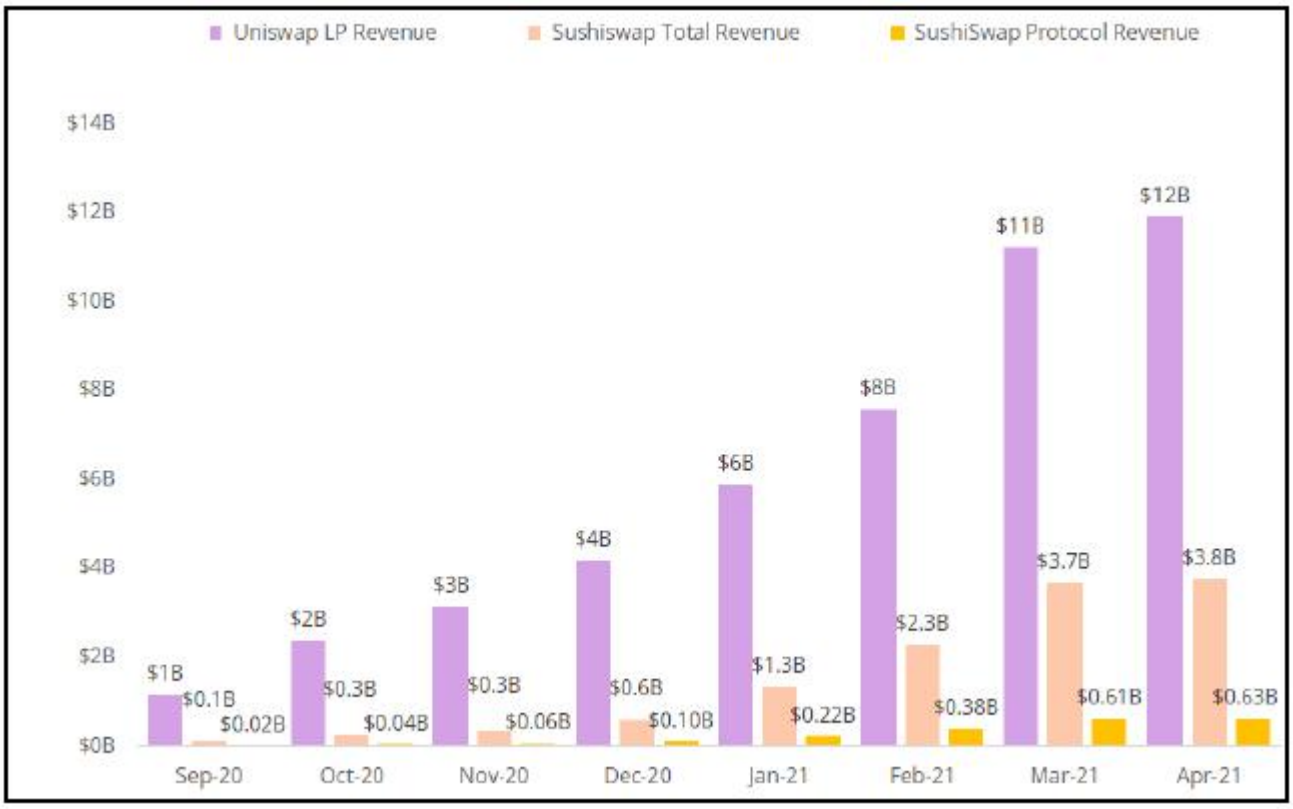
费用类型	Uniswap	SushiSwap
	固定	固定
流动性池费	0.30%	0.30%
协议	0.00%	0.05%
流动性提供者	0.03%	0.25%

*截至 2021 年 4 月 1 日的流动性池费用

从上表我们可以看出 Uniswap 和 SushiSwap 的交易费都是 0.3%。然而，在 SushiSwap 上，0.05% 的交易费用进入协议，然后分配给 SUSHI 代币持有者。

Uniswap 目前不向 UNI 代币持有者分配费用，尽管这可以通过 UNI 治理投票激活。 截至 2021 年 4 月，Uniswap 的 LP 获得的收入份额（0.30%）高于 SushiSwap 的 LP（0.25%）。

从下图我们可以看到，Uniswap 和 Sushiswap 的协议收入在过去一年都有显著增加。



数据来源：Token Terminal

Uniswap 还支持 2,000 多个交易对，大约是 SushiSwap 的五倍——这表明 Uniswap 支持和交易的长尾代币更多。

Uniswap 目前仅支持在以太坊上交易，并计划通过 Optimism 转移到第 2 层。相比之下，SushiSwap 运行在九个不同的区块链上，即以太坊、币安智能链、Polygon、Fantom、火币生态系统、xDAI、Harmony、Avalanche 和 OKExChain。

Balancer

除了基于 AMM 的 DEX，Balancer 将自己定位为投资组合经理。Balancer 池持有者无需支付投资基金的费用，而是向套利流动性池的交易者收取费用。这实质上创建了一个指数基金，该基金在重新平衡时获得支付，为流动性提供者增加了另一个收入来源。

与 Uniswap 仅支持两种资产不同，Balancer 支持多资产池。矿池创建者还可以设置从 0.00001% 到 10% 的自定义费用。这种灵活性为池创作开辟了更多可能性。

流动性池分为三种类型：

1. **公共池**—任何人都可以添加流动性，但池的参数是永久固定的。这是最缺乏信用的池。
2. **私有池**—灵活可变的参数。所有者是唯一可以更改参数和增加流动性的实体。这使得私有池托管和集中。

3. **智能池**—任何人都可以添加流动性。 该池支持固定参数和动态参数，可以持续更改。 这是最灵活的池。

Balancer 2.0 最多支持一个池中的 16 种不同资产，并允许创建智能池。 智能池对于资金管理特别有用，该池可以充当自动代币回购机。此外，它还允许池中的闲置资产借出给借贷协议，从而提高池的收益率。

Balancer 还引入了一种创新的初始 DEX 产品 (IDO) 方法，称为流动性引导池 (LBPs)。 它们是短期的智能池，随着时间的推移具有动态权重。 代币价格设定为高价，预计在整个销售过程中会下跌。 鲸鱼和机器人在一开始就没有动力购买所有代币，从而实现更民主的筹款方式。

Curve Finance

Curve Finance 是一个基于 AMM 的 DEX，主要侧重于促进类似价值资产之间的互换。 这在 DeFi 生态系统中很有用，因为有大量的包装和合成代币旨在模仿基础资产的价格。 Curve Finance 目前支持美元稳定币、欧元稳定币、包裹/合成 BTC 和包裹/合成 ETH 资产。

例如，最大的流动性池之一是 3CRV，这是一个由 DAI、USDT 和 USDC 组成的稳定币池。池中三种稳定币的比例取决于市场的供求关系。以较低的比率存入代币，用户将获得较高比例的池。当这一比率严重倾斜于其中一个代币时，这可能是套利的好机会。

Curve Finance 还支持 Compound、Aave 和 Yearn Finance 上的收益率代币。 Curve 与 Yearn Finance 合作发布了 yUSD 池，该池由收益率代币 yDAI、yUSDT、yUSDC 和 yTUSD 组成。参与该矿池的用户将获得基础收益率代币的收益、Curve 矿池产生的掉期费以及 Curve Finance 提供的 CRV 流动性挖矿奖励。该池的流动性提供者能够从三个收益来源中获利。

为了促进更多长尾代币的流动性，Curve 引入了基础池和元池的概念。元池是一个带有另一个基础池的单一代币池，允许用户无缝交易单个代币。目前，流动性最强的基础池是3CRV池。

例如，有一个带有 UST（在 Terra 区块链上发行的美元稳定币）和 3CRV 基础池的元池。 用户可以在 3CRV 池中交易 UST 和三个美元稳定币。 通过分离基础池和元池，Curve 能够将 UST 的系统性风险与 3CRV 的流动性池分开。

元池的创建在以下方面帮助了 Curve：

- 防止稀释现有池
- 允许 Curve 列出非流动资产
- CRV 代币持有者更高的交易量和交易费用

Bancor

Bancor 于 2017 年推出，是首批基于 AMM 的 DEX 之一。和Uniswap类似， Bancor 使用修改后的恒定乘积做市商曲线，但 Bancor 对此模型的方法不同于 Uniswap 使用的任意两资产曲线公式。

Bancor 没有将基础代币与 Uniswap 等任何目标 ERC-20 代币配对，而是使用其原生代币 Bancor Network Token (BNT) 作为中间货币。 针对 BNT 交易的每个代币都有单独的池。

Bancor v2 引入了多项创新，例如单边抵押和非永久性损失保险。

大多数 AMM 要求 LP 提供池中代表的每种资产的相等比率。 这给可能只想接触单一资产的 LP 带来了不便。 Bancor v2 允许 LP 贡献单一资产并对其保持 100% 的敞口。 LP 可以长期持有单边流动性的单一资产，同时赚取掉期费和流动性挖矿奖励。

非永久性损失是 AMM 上的大多数 LP 所面临的风险。Bancor 通过为 LP 的任何非永久性损失提供补偿来激励流动性。 目前，支出每天增加 1%，并在 100 天后达到 100%。 这种非永久性的损失保障鼓励 LP 在流动性池中停留至少 100 天。 在非永久性损失保护开始之前有一个 30 天的落差。

Bancor 还引入了 vBNT 和 Vortex 来改进 BNT 代币的用例。 用户在列入白名单的 Bancor 池中质押 BNT 时会收到 vBNT。 BNT 对 vBNT 的汇率是 1:1。 vBNT 可用于多种功能：

- 在 Bancor 治理中投票
- 在 vBNT/BNT 池中质押交换费用
- 通过使用 vBNT 作为抵押品 (Vortex) 在 Bancor 上借用其他代币

Vortex 允许 BNT 持有者借入抵押的 BNT。所得款项可用于杠杆或任何其他目的，提高持有 BNT 的资本效率。

AMMs 之间的区别是什么？

既然已经熟悉了市场上各种各样的 AMMs，让我们看一下使它们各不相同的三个特性。 为简单起见，我们将重点介绍 Uniswap v2、Curve、Balancer 和 Bancor。

I. 流动池费用

为了激励用户增加流动性，DEX 允许 LP 在他们的平台上赚取交易费用。 这些费用可以帮助 LP 应对价格波动和非永久性损失风险。

以下是 2021 年 4 月四个 DEX 的矿池费用摘要：

	Uniswap	Curve	Balancer	Bancor
费用类型	固定	固定	浮动	浮动
流动池费用	0.30%	0.04%	0.0001%~10%	最高到5.00%
协议方	0.00%	0.02%	取决于不同协议池	0.00%
流动性提供者	0.30%	0.02%	0.0001%~10%	最高到5.00%

数据来源：Uniswap, Curve, Balancer, Bancor

* 交易费用由矿池创建者控制。 截至 2021 年 4 月 26 日的最高费用为 5%

** 进入协议的应计交易费用用作非永久性损失保险，而不是收入。 一旦从池中取出，它就会被烧毁。

Uniswap 和 Curve 对其平台上的每一次掉期都收取固定的交易费。主要区别在于拆分 - Uniswap 向 LP 提供全部交易费用，而 Curve 在协议和 LP 之间平均分配交易费用。

对于 Balancer 和 Bancor来说，交易费用是可变的，并且由矿池的创建者控制。

II. 流动性挖矿

我们在第 2 章中已经谈到了这个概念。 简而言之，流动性挖矿是指为协议提供流动性，并作为协议的原生代币作为回报的过程。

这是在 DEX 上引导流动性和补偿流动性提供者承担非永久性损失风险的最流行的方法之一。

四个 DEX 中的每一个都有自己的原生代币：

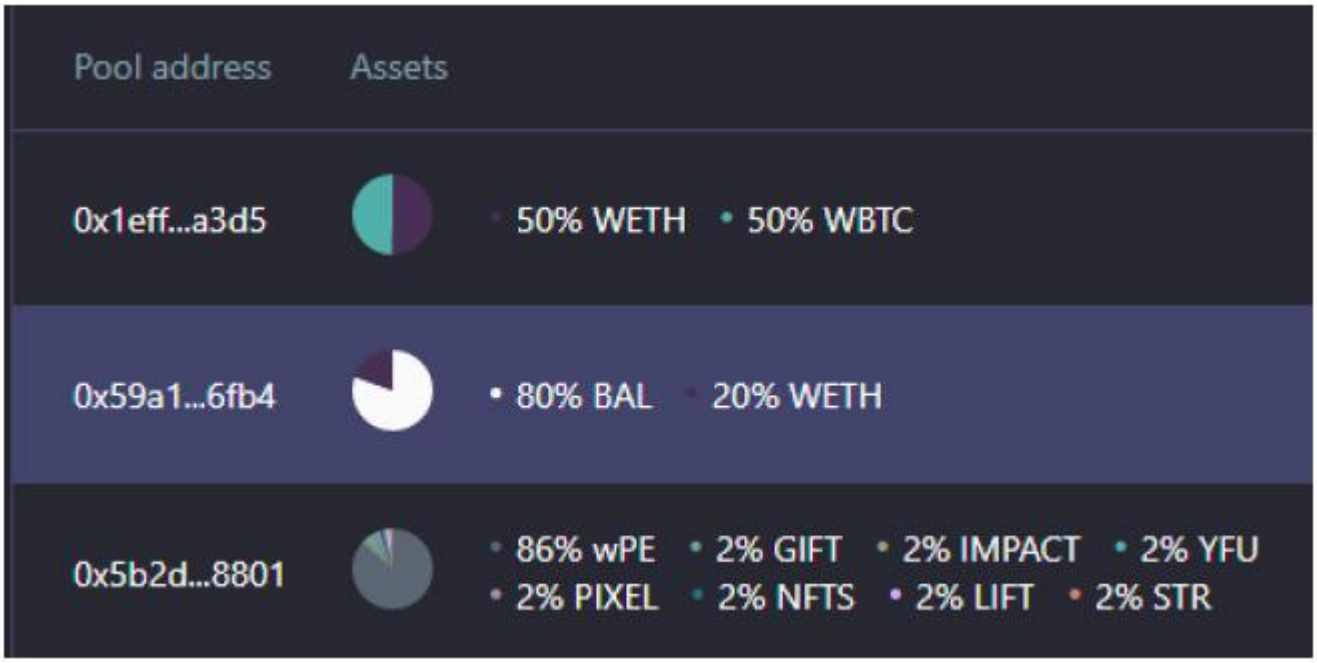
Protocol	Coin name	Ticker
	Uniswap	UNI
	Curve Dao Token	CRV
	Balancer	BAL
	Bancor Network Token	BNT

截至 2021 年 4 月 1 日，Uniswap 是四个 DEX 中唯一一个没有主动流动性挖矿计划的 DEX。

III. 流动池权重

像Uniswap 和 Bancor 等大多数 AMMs 都有标准的 50/50 池权重，因此流动性提供者必须提供两种代币的相等价值。 但是，Balancer 具有可变池供应标准，而 Curve 具有动态池供应标准。

在 Balancer 上，用户可以为每个池设置可变权重。 池会不断重新平衡，以确保它们遵循可变权重集。例如，Balancer 上的 80/20 BAL/WETH 池意味着在向池中提供流动性时，您必须将您的资金分成 80% 的 BAL 代币和 20% 的 WETH 代币。



数据来源：https://pools.balancer.exchange/#/

在 Curve 上，矿池权重是动态的，会根据储备规模的变化而变化。 与其他 AMMs 不同，Curve 不会重新平衡其矿池或将它们保持在平衡的比例。

我们来看一个由 DAI、USDC 和 USDT 组成的 3CRV 矿池的例子。 理想情况下，这个池在三个稳定币之间的权重相等。 然而，下面的快照中 显示USDC 的权重最高（41.98%）， DAI 的权重最低（24.80%）。如果您有兴趣为该池提供流动性，您不需要三个代币，而只需向池中贡献三个代币中的任何一个即可。 通过这样做，您将动态地更改池供应权重。

数据来源：https://curve.fi/3poo **截至 2021 年 4 月 30 日**

使用 AMMs 的相关风险

使用基于 AMM 的交易所并非没有风险。下面我们从交易者和流动性提供者的角度概述了三种风险。

一、价格滑点

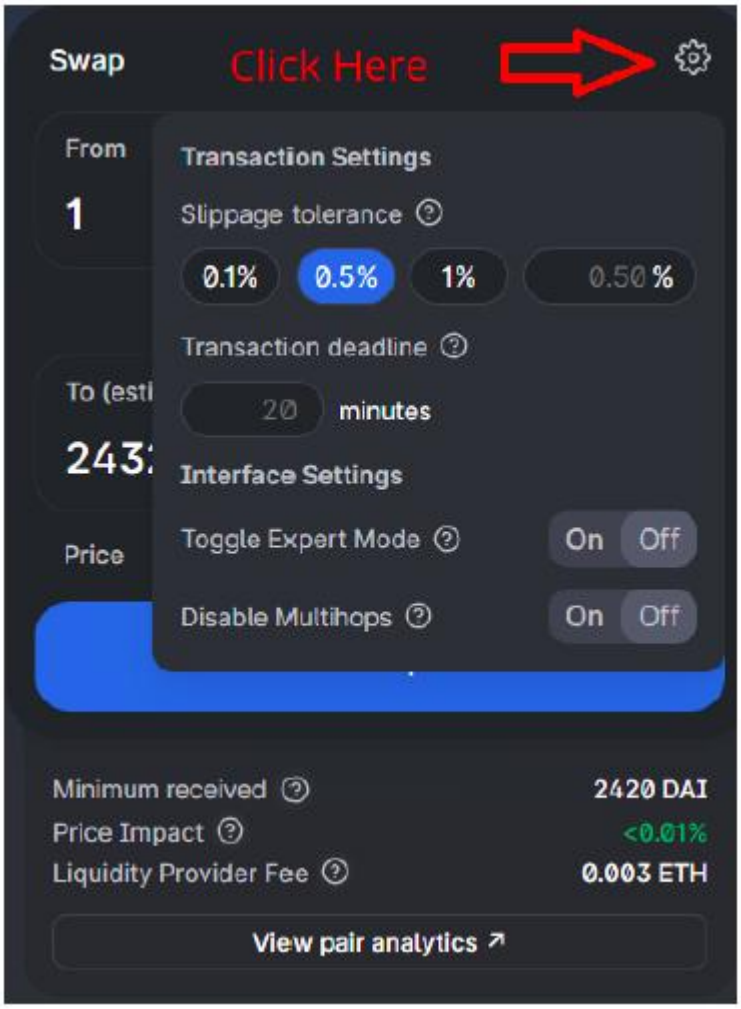
根据 AMM 公式，报价取决于代币储备的比例。

在恒定乘积做市商公式 (x * y = k) 中，订单越大，用户招致的价格滑点越大。这取决于流动性池的大小——流动性较低的池在大订单上会遭受更大的价格滑点。

假设当前 ETH/DAI 价格为 2,000 美元，初始流动性对有 62,500,000 DAI 和 25,000 ETH。这将为您提供 15.6 亿的恒定乘积。下表说明了随着交易规模变大，您必须支付的价格将会发生滑点或溢价。

这是 Uniswap 的另一个价格滑点示例。

例子
基于 Uniswap 上的 ETH/DAI 池，1 ETH 现在价值 ~2,433 DAI
您可以通过转到交易设置来设置您的滑点容忍度。Uniswap 将 0.5% 设置为默认值：



将指示器聚焦在图像底部:

1. 最低可兑换金额 是根据您的滑点容忍度，您将收到的最小代币数量。 如果您的滑点容忍度为 0.5%，那么您将收到的最低金额为 2,433 DAI * 0.95% = 2,420 DAI

2. 交易滑点是您必须支付的溢价，它将反映在显示的价格中。 您的订单越大，交易滑点就越大。

二、抢先交易

由于 AMMs 上的订单被广播到区块链上供所有人查看，任何人都可以监控区块链以获取合适的订单，并通过收取更高的交易费用来提前运行它，以使他们的订单比目标订单的挖掘速度更快。 进行这种无风险套利的领跑者发起了称为“三明治攻击”的攻击。

下面是如何发生这种情况的说明:

下面是在 Uniswap 上使用 Ampleforth 的治理代币 (FORTH) 发生的“三明治攻击”的快照。

三、 无常损失

AMM 的另一个缺点是。当您向 AMMs 提供流动性时，会发生无常损失。 无常损失类似于衡量您在池中持有代币的机会成本和将代币存放在钱包中的机会成本。注意:在您从流动性池中移除您的代币之前，损失不会发生。

持有代币在池中和钱包中的价值之间的差异越大，无常损失就越大。

例子
假设您通过向池提供 10,000 DAI 和 5 ETH 在 Uniswap 上创建了一个 ETH/DAI 池。

- 1 ETH 的价格 = 2,000 DAI
- 矿池由 5 个 ETH 和 10,000 个 DAI 组成
- 池流动性使用恒定产品做市商公式”

(x * y = k) → 5 * 10,000 = 50,000
假设 ETH 的价格翻了一番，达到 4,000 DAI。

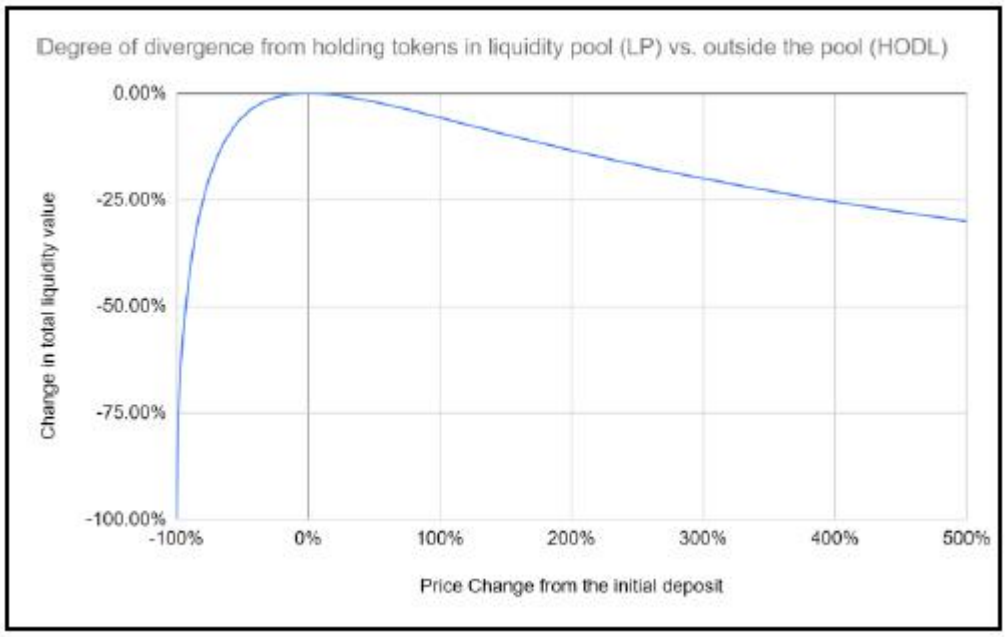
- 套利者将在 Uniswap 中对 ETH 报价的差价进行套利，直到达到 1 ETH = 4,000 DAI
- 矿池将重新平衡准备金率，直到与矿池常数 50,000 匹配
- 新池比例将变为 3.536 ETH 和 14,142 DAI

要计算您的无常损失，您可以减去在池外和池内持有的收益。

在 1 ETH = 2,000 DAI 时，您的原始资本（5 ETH 和 10,000 DAI）的价值为 20,000 DAI。
1 ETH = 4,000 DAI
- 您在池中的持股将是：
  - (3.536 ETH * 4,000 DAI) + 14,142 DAI = 28,286 DAI
  - 投资回报率 = +41%（忽略交易费收益）
- 您在池外的持股将是：
  - (5 ETH * 4,000 DAI) + 10,000 DAI = 30,000 DAI
  - 投资回报率 = +50%
- 你的无常损失是：
  - 30,000 DAI - 28,284 DAI = 1,716 DAI

这种损失只有在您从 Uniswap 提取流动性时才会实现。

下图显示了如果您在池外和池内持有代币，您将获得的机会成本。



- 1.25 倍价格变动 = 相对于 HODL 的 0.6% 损失
- 1.50 倍价格变动 = 相对于 HODL 的 2.0% 损失
- 1.75 倍价格变动 = 相对于 HODL 的 3.8% 损失
- 2 倍价格变动 = 相对于 HODL 的 5.7% 损失
- 3 倍价格变动 = 相对于 HODL 的 13.4% 损失
- 4 倍价格变动 = 相对于 HODL 的 20.0% 损失
- 5 倍价格变动 = 相对于 HODL 的 25.5% 损失

因此，在较小价格范围内交易的交易对（例如稳定币）较少受到无常损失的影响。

值得一提的是

- PancakeSwap

PancakeSwap 是 Uniswap 的一个分支，但它建立在 Binance Smart Chain 区块链之上。 它是币安智能链上最大的 AMM，截至 2021 年 4 月，其交易量甚至高于 Uniswap。

- TerraSwap

TerraSwap 存在于 Terra Chain 上，它是 Terra 区块链上唯一的 DEX 协议。 您可以选择以任何 Terra Chain 资产计价的交易费用。

- 0x Protocol

0x 是一个 DEX 基础设施层，有两个主要产品：一个允许项目启动白标 DEX 的 DEX 聚合 API 和一个名为 Matcha 的面向消费者的 DEX 聚合器。 Tokenlon、Metamask、Zapper 和 Zerion 等项目已经集成了 0x 来推出他们的交换服务。

总结

DEX 在推动 DeFi 领域发挥着至关重要的作用，因为它描绘了当前的市场行为，尤其是加密货币的价格和流动性。 它确定了各种加密货币的相对价值，并说明了交易和资本流动的动态性质。

推荐读物

1. 了解 AMM 基础 https://defiweekly.substack.com/p/understanding-amms-the-basics-f30
2. AMMs 的类型 https://blog.chain.link/challenges-in-defi-how-to-bring-more-capital-and-less-risk-to-automated-market-maker-dexs/
3. 了解价格对 AMM 的影响 https://research.paradigm.xyz/amm-price-impact
4. 以太坊的抢先问题 https://www.coindesk.com/new-research-sheds-light-front-running-bots-ethereum-dark-forest
5. Uniswap V3 https://uniswap.org/blog/uniswap-v3/

第四章：去中心化交易所（DEX）聚合器

流动性对于确保交易能在不被严重影响的市场价格下执行至关重要。 DEX 市场竞争异常激烈，多个 DEXs 之间会争夺用户和流动性。 因此，流动性常常是被分散的，这导致了资金管理效率低下。

虽然对较小交易的影响可能无关紧要，但是较大的DEX交易将很容易出现较高的价格滑点。 这就是 DEX 聚合器帮助交易者在各类 DEX 中获得最佳成交价格的地方。

DEX 聚合器通过汇集不同 DEX 的流动性来寻找最具成本效益的交易方案。 通过在多个流动性池中分别完成单笔交易，进行大宗交易的交易者就可以节省手续费（gas 费），并最大限度地降低因低流动性而导致的价格滑点。

我们已经在《 How to DeFi: Beginner 》中以 1inch 为例简要介绍了 DEX 聚合器。 在下一节中，我们将介绍一些新的 DEX 聚合器，例如 Matcha 和 Paraswap，并对每个聚合器协议进行比较分析。

DEX 聚合器协议

1inch 网络

1inch 网络是一个 DEX 聚合器解决方案，它可以在多个流动性源中搜索更优惠的兑换比例。 初始协议结合了 Pathfinder 算法，该算法能在不同市场之间寻找最佳兑换路径。 自从在以太坊网络上成立以来，1inch 已经扩展到支持币安智能链（BSC） 和 Polygon 网络。 1inch聚合协议也经历了两次重大更新，自2021年3月以来，1inch更新到了第3版。

截至 2021 年 5 月 31 日，以太坊上有 50 多个流动性来源，币安智能链上有 20 多个流动性来源，Polygon 上有 10 多个流动性来源。 值得注意的是，在短短两年内，仅在以太坊网络上，1 英寸 DEX 聚合器的总交易量就超过了 40B 美元。

与其他 DEX 聚合器不同，1inch 有两个原生代币。一个是gas代币（CHI），另一个是治理代币（1INCH）。

CHI 是一种利用以太坊存储退款的 gas 代币。 Gas 代币帮助智能合约在交易过程中消除不必要的存储并降低 Gas 费用。 您可以将 CHI 视为一种可以兑换更便宜的交易的折扣券，它可以让用户节省高达 42% 的汽油费。

2020 年 12 月发布的 1INCH 代币推动该协议成为一个更加去中心化的实体。 1INCH 的持有者允许社区在去中心化自治组织 (DAO) 模型下投票支持特定的协议设置。 治理模型使利益相关者能够控制两个主要方面：
1) **矿池治理**——管理每个矿池的特定参数，例如掉期费、价格影响费和衰减期。
2) **工厂治理**——管理所有矿池的通用参数，例如默认掉期费、默认价格影响费、默认衰减期、推荐奖励和治理奖励。

此外，通过抵押 1INCH 代币，用户可以获得价差盈余（正滑点），这是当执行价格略好于报价时掉期交易之间的净正差额。 值得注意的是，1inch Network 还与其他协议建立了许多合作伙伴关系，在这些协议中，1INCH 交易对的流动性挖掘激励措施是很普遍的。

其他值得注意的功能包括限价单和选择 Pathfinder 路由流程的选项，以及在获得最大回报或最小化汽油费成本之间进行选择的选项。

1inch 网络还包含自己的流动性协议。 自动化做市商保护用户免受抢先攻击，并为流动性提供者提供更多机会。

Matcha

Matcha 是由 0x Labs 构建的去中心化交易所（DEX）聚合器。 Matcha 由 0x 协议提供支持，该协议适用于各种产品，包括用于共享订单的点对点网络（0x 本地流动性）及其专有 API。 Matcha 从 0x API 中提取数据并有效地在所有可用的范围内路由订单 流动性来源（截至 2021 年 5 月 31 日超过 20 个）。

与其他 DEX 聚合器不同，Matcha 在整个交易体验中结合使用链上和链下组件。 报价是通过 0x API 在链下生成的，以在使用链上执行订单之前最小化 gas 成本。 0x API 可以找到最具成本效益的交易路径（包括 gas 成本），如果对交易员更好的话，它甚至可以自动将单个订单拆分为多个流动性来源。

迄今为止，0x 的 API（为 Matcha 提供动力）已经有四次重大更新，最新的是 2021 年 3 月发布的 0x 版本 4。通过此版本 4 更新， Matcha用户应该期待更多的节油订单(报价订单最多节省70%的汽油，限价订单最多节省10%的汽油)和更好的整体价格。

从 0x 版本 3 开始, Matcha 用户需要在 0x 开放订单簿流动性上收取少量协议费用（以 ETH 支付）。费用与填写订单的 gas 成本成正比，并与 gas 价格成线性比例。 这里需要注意的重要一点是，除了原生链或流动性来源所需的必要网络费用外，从技术上讲，Matcha 不收取交易费用。

与 1inch 不同，Matcha 将所有正滑点分享给用户。 其他值得注意的功能包括限价单和 Matcha 最近对 Binance Smart Chain 网络和 Polygon 网络的支持。

Paraswap

ParaSwap 于 2019 年 9 月首次开发，并使用自己的路由算法 Hopper。 ParaSwap 在所有支持的交易所检查给定货币对的汇率，并显示每对货币的有效汇率（考虑滑点）。

ParaSwap 实施了多种解决方案来减少整个平台的 gas 使用量，例如实施 REDUX gas 代币。在分析交换路径时将 Gas 成本考虑在内。

ParaSwap 的最新更新版本 3 于 2021 年 1 月推出。它包括显着的 UI 升级和改进的交换合约。重点放在将总 gas 成本降低 30%，特别是对于仅使用一个 DEX 结算的交易。

协议收入通过两个主要途径产生。 第一个是通过第三方集成商，如果他们对便利掉期收取费用，ParaSwap 将收取 15% 的费用。 第二种是通过正向滑动，其中 50% 用于协议，另外 50% 与用户共享。

ParaSwap 目前有 48 个流动性来源。 这是由私人做市商提供的本地池 (ParaSwapPools) 补充的。ParaSwap 最近还与 Binance Smart Chain 网络和 Polygon 网络集成。

DEX 聚合器的性能因素

DEX 聚合器背后涉及许多错综复杂的问题，因此很难公平地比较它们。 虽然用户可能会关注报价，但它们也不一定可靠。 原因如下：

例子
假设用户想用 1,000 USDC 兑换 1,000 USDT。
聚合器 X 报价 1,000 USDT，预估交易成本为 5 USDT，实现汇率为 1 USDC = 0.995 USDT。 用户兑换 1,000 USDC 后，将获得 995 USDT。
聚合器 Y 报价 1,005 USDT，估计交易成本为 15 USDT，实现汇率为 1 USDC = 0.990 USDT。 用户兑换 1,000 USDC 后，将获得 990 USDT。

在这个例子中，聚合器 X 在考虑交易费用后更具成本效益。 您必须记住，此示例使用 DEX 聚合器在交换之前提供的估计数字。

在现实中，当一个人执行掉期时，批准交换和掉期在链上成功执行之间的时间差将影响最终价格。 在此期间，网络拥堵和选定流动性池的规模等外部市场力量可能会发生变化。协议的路由算法也会影响结果，因为更有效的交易会减少网络使用并最大限度地减少失败的交易。

另一点是交易的规模。 对于较大的交易，DEX 聚合器所节省的成本成比例地更高，因为它们更容易出现更高的价格滑点。 较小的交易可能不需要依赖不同的流动性池，因为单一的流动性池是最佳途径。

如果我们对所有这些指标进行分类，我们将得到四个决定 DEX 聚合器性能的主要因素：
1.路由算法
2. 流动性来源
3. 当前市场状况
4. 交易规模

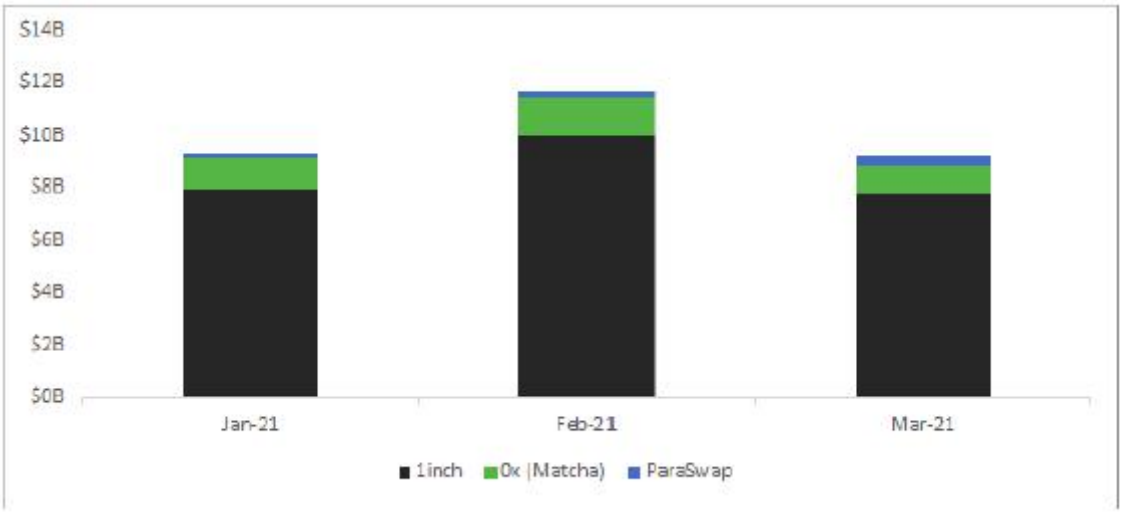
哪个 DEX 聚合器提供的价值最大?

DEX 聚合器已成为 DEX 经济的重要组成部分。 虽然很难确定哪个 DEX 聚合器提供的价值最大，但下表确实提供了一些清晰的信息：

截至 2021 年 5 月 31 日	1inch	Matcha	ParaSwap
流动资金来源	80+	20+	48
代币	1INCH + CHI	None	None
路径算法	Pathfinder	0x API	Hopper
限价单	是	是	否
抵押功能	是	否	否
协议费用	浮动，在撰写本文时，所有交易的固定费用为 0.25%。	70,000 gwei * 交易的 Gas 价格（如适用）	用户无需支付，但第三方集成商需支付 15% 的便利掉期费用
支持区块链	以太坊和币安智能链，以及 Polygon	以太坊、币安智能链和 Polygon	以太坊、币安智能链和 Polygon
将正滑点转移给用户	变量 - 在撰写本文时（2021 年 5	100%	50%

	月），大约 20% 的正滑点分配给推荐人，80% 给 1INCH 赌注者。		

1inch有很多先发优势。 截至 2021 年 5 月 31 日，该协议拥有最多的流动性来源，超过 80 多个来源。 1inch 也是唯一一个拥有自己的原生代币的 DEX 聚合器，使其比其他协议具有明显的优势，1inch 也允许用户质押 1INCH 代币和赚取协议费用。 1inch 也比其他缺乏 DAO 的协议更加去中心化。 所有这些优势都体现在交易量上，这是最基本的指标：



数据来源：Dune Analytics

2021 年第一季度的总交易量由 1inch 主导。2021 年 3 月，1inch 拥有 84.2% 的总市场份额和 77.6 亿美元的交易额。当然，这可能是由多种原因造成的，包括用户忠诚度和信息不对称。但是，总体而言，高用户保留率表明市场认可1inch 的优势。

相关的风险

最好不要将 DEX 聚合器的报价视为福音。虽然 DEX 聚合器旨在确保执行的交易符合报价，但这并不总是发生。

另一点是交易的规模。尽管 DEX 聚合器为大型交易提供了更好的成本节省，但有时小型交易者直接与 DEX 交互可能更好。

DEX 聚合器通常是可靠的，但也有交易通过小型和流动性差的池进行路由的情况。作为用户，在批准交易之前，您应该始终检查您的滑点是否太高。

值得一提的是

- DEX.AG（更名为 Slingshot）

DEX.AG 是较小的 DEX 聚合器之一，它使用自己的专有路由算法 X Blaster。 该项目于 2020 年 11 月更名为 Slingshot。在撰写本文时（2021 年 4 月 1 日），该协议集成了 18 个流动性来源，不收取任何交易费用，并且尚未发布其更新的实时版本。

- Totle

Totle 是另一个小型 DEX 聚合器，它依赖于他们的原生 API（Totle API）。 在撰写本文时（2021 年 4 月 1 日），有 15 个流动性来源。

总结

DEX 是 DeFi 的命脉。然而，对于许多高级用户（尤其是鲸鱼）来说，DEX 聚合器更为重要，因为 DEX 聚合器可以为大型交易提供更好的成本效率。 DEX 聚合器甚至已经发展到拥有自己的流动性池的地步，这进一步模糊了 DEX 聚合器和 DEXs 之间的界限。

DEX 板块是 DeFi 可组合性的一个主要例子。 DEX 聚合器建立在 DEX 之上，为不同的用户配置文件提供服务。 因此，我们受益于因竞争加剧和互利共赢而产生的更全面的创新产品套件。

推荐读物

1. DEX聚合器概述 https://www.delphidigital.io/reports/defi-aggregators/
2. 比较不同的 DEX 聚合器 https://medium.com/2key/defi-dexes-dex-aggregators-amms-and-built-in-dex-marketplaces-which-is-which-and-which-is-best- fba04ca48534
3. 0x 2020 年 10 月对 Dex 聚合器的研究 https://blog.0xproject.com/a-comprehensive-analysis-on-dex-liquidity-aggregators-performance-dfb9654b0723
4. 1inch v3 升级与其他 Dex 聚合器对比 https://blog.1inch.io/introducing-the-1inch-aggregation-protocol-v3-b02890986547

第五章：去中心化借贷

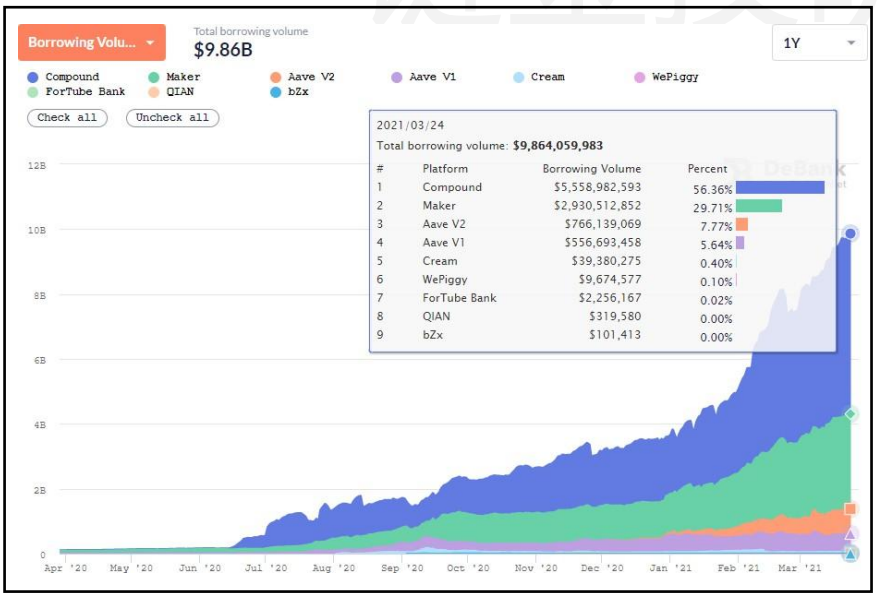
在传统金融体系中的资本市场，其实很多人都无法参与其中，传统市场只属于少部分富人和权势人士。

想象一下，如果你是一个风险投资家，正在为你的下一个企业寻找融资，在DeFi世界里，你可以提供你的资产作为抵押品获得贷款，抵押资本将保持不变，并随着抵押时间不断增长，接着日后赎回。当然，上述并不是一个无风险的策略。如果你不小心逾期拖欠贷款不还，就失去你的抵押品。现在的DeFi的借贷协议带给每个人更公平透明的借贷入口。

使用加密货币作为抵押品，您可以从这些协议中借款并利用。作为最大的DeFi类别之一，去中心化借贷已呈指数级增长，2021年4月借款量达到97亿$。这比前一年增加了102倍!

现在DeFi领先的借贷协议有Compound,Maker,Aave以及Cream。

去中心化借贷



资料来源：DeBank

DeFi借贷协议总览

Compound

Compound Finance是一个由compound实验室建立的货币市场协议。这是一个基于以太坊的开源货币市场协议，任何人都可以轻松地借出或借入加密货币。截至2021年4月1日，在compound平台上有9个不同的通证。

1. 0x (ZRX)
2. Basic Attention Token (BAT)
3. Compound (COMP)
4. Dai (DAI)
5. Ether (ETH)
6. USD Coin (USDC)
7. Tether (USDT)
8. Uniswap (UNI)
9. Wrapped Bitcoin (WBTC)

Compound作为一个建立在以太坊区块链上的流动性池运作。供应商向流动性池提供资产以赚取利息，而借款人则从流动性池中获得贷款，并支付债务利息。本质上，Compound为希望从闲置资金中获得利息的贷款人和希望借款用于生产性或投资使用的借款人之间架起了桥梁。

在Compound中，利率以年化收益率百分比(APY)表示，资产之间的利率不同的。Compound通过考虑资产供求的算法计算出利率。

从本质上说，Compound允许供应商/借款人无需协商贷款条款（如到期日、利率、交易对手、抵押品），降低了借贷的摩擦成本，从而创造一个更有效的货币市场。

Compound是借贷量最大的DeFi存贷款平台，拥有56%的市场份额（DeBank，2021年4月1日）。2020年6月，Compound推出了其治理Token，Compound(COMP)

Maker

Maker是最早的DeFi借贷协议。它通过锁定30多个代币支持的智能合约，铸造与美元挂钩的稳定币Dai。除了作为一个借贷协议，Maker还充当了一个稳定币的发行人(DAI)。

2017年12月19日，Maker最初开始使用单一抵押品DAI(SAI)，它是用以太坊(ETH)作为唯一的抵押品铸造的。2019年11月18日，Maker将SAI升级为DAI，它可以由29种不同的代币作为抵押被铸造。

现在Maker甚至接受了USDC的稳定币方案，以帮助管理DAI的价格不稳定。Maker又通过将第一个真实世界的资产（房屋）作为抵押，Maker在弥合与传统融资之间的差距方面取得了巨大进展。2021年4月21日，该公司成功地以$181k执行了第一笔MakerDAO贷款，并以房屋作为抵押，有效地创建了第一批基于区块链的抵押贷款之一。

与其他贷款协议不同，用户不能将资产借给Maker。他们只能通过存入抵押品来借入DAI。DAI是最大的去中心化稳定币，在DeFi生态系统中得到了越来越多的应用。我们将在第6章更深入地研究DAI。

Aave

Aave 是另一个类似于 Compound 的著名去中心化货币市场协议。 截至 2021 年 4 月，用户可以在 Aave 上借出和借入 24 种不同的资产，与 Compound 相比要多得多。

Compound和Aave的运作方式类似，贷款人可以通过将加密货币存入可用的贷款池来提供流动性并赚取利息。借款人可以利用这些流动性池获得贷款，并支付利息。

Aave与Compound的区别在于，它开创了诸如利率转换、抵押品互换和闪期贷款等新的原始贷款业务。

利率转换:Aave上的借款人可以在可变利率和稳定利率之间切换。

抵押品互换:借款人可以用他们的抵押品交换另一种资产。这有助于防止贷款低于最低担保比率而面临清算。

闪期贷款:借款人可以申请零抵押贷款，前提是借款人在同一笔交易内偿还贷款和任何额外的利息和费用。闪电贷款对套利交易者很有用，因为它们在跨各种DeFi Dapps进行套利交易时具有资本效率。

Cream Finance

Cream Finance(C.R.E.A.M.)是于2020年7月由Jeffrey Huang和Leo Cheng创立。Cream其实是一个Compound的分叉，2020年11月，Cream与Yearn Finance 生态合并部署于以太坊、币安智能链和Fantom。

与Compound和Aave相比，Cream拥有更宽松的资产策略。它采用快速上市的策略，比其他任何借贷协议都更快地上市了更多的资产。并选择专注于长尾资产——流动性较低或属于利基类别的资产。Cream是首批接受收益代币和LP代币作为抵押的借贷协议之一。

Cream还推出了“铁银行”(Iron Bank)，这是一种向白名单合作伙伴提供的无抵押贷款服务。作为合作伙伴之一，Yearn Finance可以利用从Cream借来的资金，进一步提高其流动性挖矿活动所获得的收益。

对于即将发布的ETH 2.0, Cream也在其中提供了ETH2.0质押服务。

用户可以将ETH质押到CRETH2，可以作为抵押物借贷。所有ETH 2.0质押工作由Cream完成，收益由CRETH2持有者分享。从本质上说，CRETH2是一种托管质押服务，对验证者的奖励收取8%的费用。除ETH 2.0外，Cream还为币安Smart Chain和Fantom提供质押服务。

Cream将自己的市场定位是可以承担比Compound和Aave更大风险更的借贷人市场，以促进市场对杠杆利用和做空利基资产的需求。

借贷协议指标对比

(US$ in millions) As of 24th March 2021	Compound	Maker	Aave	Cream
Number of Assets Supported				
Collateral Type	8	29	21	47
Borrowing Type	9	1	25	65
Borrowing Volume	$ 5,559	$ 2,931	$ 1,324	$ 39
Total Value Locked (TVL)	$ 6,910	$ 6,090	$ 5,010	$ 202
Utilization Ratio (Borrowing Vol/TVL)	0.80	0.48	0.26	0.19

资料来源：Maker, Aave, Cream, DeBank, Token Terminal

上表给出了关于4个最大的借贷协议的信息：Compound, Maker, Aave, and Cream.

我们将依次通过每个指标，以评估协议关于借款量和锁定总量(TVL)的资本效率。随后，我们将研究每个风险的相关风险。

所支持的资产

为了确保无信任贷款的发生，借款人需要存放价值高于贷款金额的资产（抵押品）这被称为超额抵押贷款，这支撑了DeFi贷款协议的偿付能力。借款人能借多少钱取决于各种DeFi贷款协议的抵押品比率。

在DeFi贷款协议中，Cream拥有最多受支持的资产

- 45项资产可用作抵押品，65项资产可供借款。

相比之下，Compound支持资产数量最少——只有8个资产可以用作抵押品，9个资产可用于借款;Compound的资产策略更加保守。

营业收入

贷款平台的重要指标之一是它们的借贷量。这个指标很重要，因为借款人为其贷款支付费用，这些协议从而产生收入。以下是每个协议如何获取收入的明细：

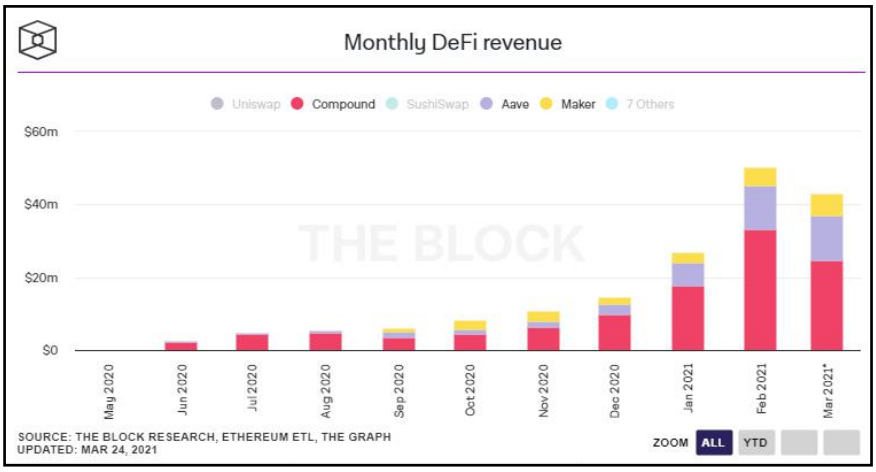
- Compound：借款人支付的部分利息将进入其储备金，作为相应保险，由COMP token持有人控制。每个受支持资产都有一个储备系数可以决定储备金额。

- *Maker*：当借款人偿还贷款时，他们将支付本金和由稳定币确定的利息费。每个受支持的抵押品都有其稳定币费用。

- Aave:该平台有两种费用：
  - 贷款金额的0.00001%在AaveV1贷款收取。
  - 0.09%是从flash贷款金额中收取的-更多关于flash贷款参考第2章 14.

- Cream：借款人支付给供应商的利息有一部分进入Cream的储备协议，并作为奖励分配给Cream token持有人。

截至2021年4月，Compound在贷款协议中产生了最高的收入。数据如下：

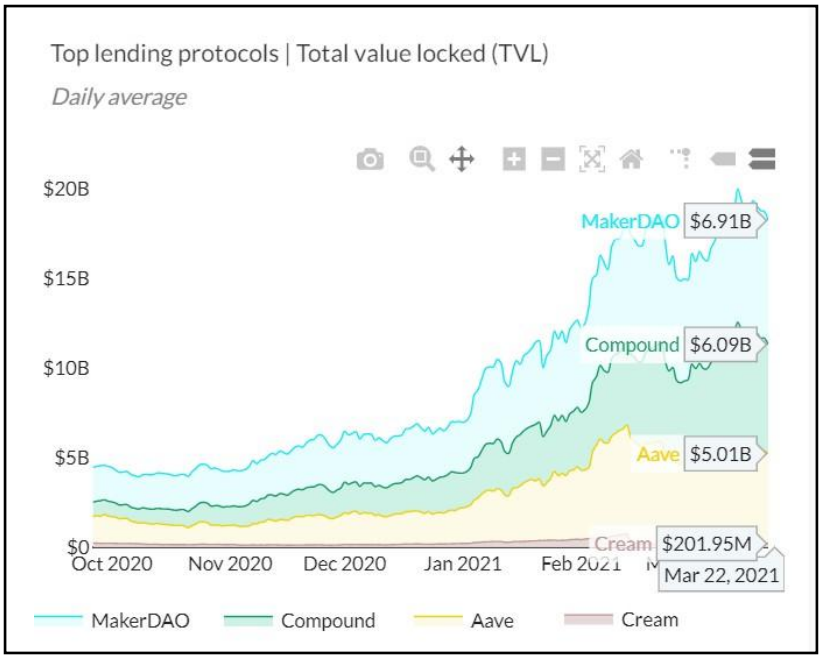


资料来源：TheBlockResearch Data Dashboard

锁仓总值(TVL)

尽管所有的借贷协议自2020年10月以来它们的TVL都在增长，但Aave和Maker的TVL与Compound比起来甚至不值一提。这是因为Compound在其流动性挖掘计划中对借款人和贷款人有持续的激励措施。

注：Aave最近于2021年4月底启动了一个流动性挖掘计划。



资料来源：TokenTerminal

利用率（借款量/TVL）

DeFi借贷协议从其借款中获得协议收入。与此同时，贷款平台上的TVL是由用户存入其资产以赚取收益或作为借贷抵押品所驱动的。

通过除以上述两个数字，我们可以推导出每个协议的利用率——利用率越高，TVL的工作效率就越高。

(US$ in millions) As of 24th March 2021	Compound	Aave	Cream
Number of Assets Supported			
Collateral Type	8	21	47
Borrowing Type	9	25	65
Borrowing Volume	$ 5,559	$ 1,324	$ 39
Total Value Locked (TVL)	$ 6,910	$ 5,010	$ 202
Utilization Ratio (Borrowing Vol/TVL)	0.80	0.26	0.19

**Maker不包括在这个表中，因为与它的同行不同，抵押品不能被借用。*

乍一看，Compound似乎有最高利用率为0.80，
最低的Cream是0.19。然而，Compound的高利用率

可能是由于它的流动性挖矿计划奖励借款人COMP token，而Cream的低比率可能是因为它在过去遭受过几次黑客利用。出于安全考虑，Cream加强了他们的安全保险保障，有150万刀用于Armor.fi/NexusMutual的漏洞奖励保险以及Defi安全的透明度报告。

借贷利率

现在，让我们讨论一下贷款协议的两个主要用户：贷款人和借款人。

贷款人

Supply Market (Snapshot on 24th March 2021)

	Compound	Aave	Cream
USDC	5.51%	7.50%	16.13%
ETH	0.16%	0.33%	1.60%
DAI	7.75%	8.71%	13.50%
WBTC	0.45%	0.18%	2.22%
USDT	2.43%	7.13%	26.11%

资料来源：Compound, Aave, Cream

根据上表，Cream提供最高APY，*Compound*为大多数资产提供最低APY。作为一个贷款人，虽然在Cream上获得最高APY是不错的，但高APY的通常意味着在这些借贷协议中存在更高的潜在风险。

Cream因为它曾多次被黑客攻击，因此必须提供更高的APY来吸引资金。总体来说，Compound相对于同行虽然资产提供最低的APY，但是它更专注于平台的安全性。

借款人

Borrow Market (Snapshot on 24th March 2021)

	Compound	Aave (Variable rate)	Aave (Stable rate)	Cream	Maker
USDC	7.25%	8.23%	15.23%	23.20%	-
ETH	2.76%	2.06%	5.57%	8.02%	-
DAI	10.78%	14.71%	22.71%	21.26%	0% - 9% *
WBTC	4.82%	1.61%	5.01%	9.80%	-
USDT	3.67%	6.80%	14.80%	42.04%	-

* The interest depends on the collateral assets deposited on Maker

资料来源：Compound, Aave, Cream, Maker

若你是借款人，很容易找到提供最低利率的贷款平台，低利率意味着更便宜的借贷成本。与同行相比，Compound提供了最具竞争力的借贷利率。然而，Compound的用户可以借入的资产却很有限。

至于Aave，它为借款人提供了两种利率选择：可变利率和稳定利率。用户可以在任何时候切换利率更便宜的产品，看哪个更便宜就选哪个。

Cream收取最高的借款利率——主要是因为它拥有最多样化的资产列表可供用户借用。Cream的高借贷利率需要补偿贷款机构承担提供资本的高APY风险。

有趣的是，Cream的一些借款人是使用Cream的Iron Bank的机构，如Alpha finance和Yearn finance。Iron Bank提供一种新的无抵押贷款服务，即其他协议不需要提供抵押品就能从Cream贷款。

现在，让我们瞧瞧DAI's的借款人。Maker是DAI的唯一发行人，它的资产比借贷同行提供最便宜的利率。Maker的现在的借款量是仅次于Compound位列第二，主要铸造DAI。

截至2021年4月1日，DAI是世界第四大稳定币。这使得Maker成为DeFi生态系统中一个非常重要的玩家。

相关的风险

在使用去中心化借贷协议时，您必须注意技术风险，如智能合约漏洞。如果开发人员在代码部署上不小心，就可能会被黑客利用。

此外，许多贷款协议依赖于价格预言机(更多信息见第12章)来提供链上价格数据。但价格预言可能失败，也可能被利用。例如2020年11月，Coinbase Pro上的DAI价格上涨了30%，导致价值8900万美元的贷款被清算

然而，作为借款人，主要的风险是由于抵押品比率管理不善而失去抵押品。加密货币以其极端的价格波动而闻名，如果你的贷款低于最低抵押品比率，你的抵押品就有被清算的风险，你将承担相当大的损失，并支付清算费用。因此，不断监控和保持你的贷款的健康指标的抵押品比率是至关重要的。

一些著名借贷协议

●Venus

VenusProtocol是在币安Smart Chain上运行的货币市场和稳定币协议。该协议最初由Binance孵化，是Compound和MarkerDAO的分支。自从被币安收购后，Swipe就接手了Venus Protocol的开发工作。

●Anchor

Anchor Protocol是在Terra区块链上运行的借贷协议。平台上的借贷机制类似于Compound和Aave。Anchor Protocol为Terra区块链上土生土长的美元稳定币UST设定了20%的收益率目标

●Alchemix

alchemix与其他贷款公司的区别在于，它引入了无需清算的自付贷款。简单地说，你的抵押品将被用来赚取利息，利息将被用来偿还你在Alchemix上的贷款。

●Liquity

Liquity是一种定义货币的借贷协议，允许你提取其稳定币，流动性美元(lud)，没有利息费用。你必须使用以太坊作为抵押，并保持最低抵押比率仅为110%。还款将以LUSD支付。这些贷款由一个包含LUSD的稳定池和作为最后担保人的其他借款人共同担保。

结论

DeFi的借贷协议使用率非常高——它们一直在DeFi TVL排行榜上占据主导地位。然而，大多数的DeFi贷款目前仍然是超额抵押的，这意味着资本效率较低。

传统的贷款机构在决定发放贷款之前，会利用来自个人信息的信用评分，比如工作、工资和借贷历史。在DeFi中，很难用假名建立信用记录。

一些协议像TrueFi、Cream和Aave等希望在抵押贷款方面取得进展。在这些协议中，被选为白名单的实体可以在不提交任何抵押品的情况下获得贷款。

低抵押贷款将是DeFi贷款和借款协议发展的下一个阶段。有了低抵押贷款，这样DeFi借贷协议才能更有效地提高资本效率，并有效地与传统贷款机构竞争。

尽管DeFi贷款目前仍主要局限于数字资产领域，与现实资产几乎没有联系，但Maker在2021年4月通过接受房地产等现实资产作为抵押，取得了巨大进展。

推荐的阅读材料

1. Evaluating DeFi Lending Protocols
   https://messari.io/article/a-closer-look-at-defi-lending-valuations
2. How to Assess the Risk of Lending_
   https://newsletter.banklesshq.com/p/how-to-assess-the-risk-of- lending
3. Dashboard on Lending Protocols_
   https://terminal.tokenterminal.com/dashboard/Lending

第六章:去中心化稳定币和稳定资产

在我们的《How to DeFi： Beginner》一书中，我们确定稳定币是加密生态系统的重要组成部分。截至2021年4月1日，稳定币的总市值为645亿美元，比前一年增长了12倍。

随着机构投资者和散户投资者涌入加密货币市场，对稳定币的需求将继续蓬勃发展。这并不奇怪，因为稳定币是能够实现全球价值转移的非波动性资产。

我们的入门书涵盖了集中式稳定币Tether (USDT)和Maker去中心化稳定币Dai 之间的一些关键区别。在本章中，在介绍其他形式的去中心化稳定币之前，我们将先看看Tether和Dai的一些缺点。

中心化稳定币

Tether(USDT)

USDT(原名RealCoin)是一种集中式稳定币，于2015年开始在Bitfinex交易所交易。作为市场上第一个稳定币，它拥有强大的先发优势，一直保持着稳定币市场领导者的地位。截至2021年4月，Tether的市值为400亿美元，占稳定币市场总份额的66%以上。

Tether通过1:1的担保体系维持盯住1美元的汇率。通过持有现金作为储备抵押品，然后发行等量的USDT。理论上，这是确保USDT保持其挂钩的可靠和直接的方法。毕竟，这是在重申金本位制，在上个世纪，美元曾由黄金支持。

但问题在于栓贷的发行过程不透明。由于其发行的集中化本质，加密社区中的许多人对Tether是否拥有其声称拥有的储备持怀疑态度。2019年3月，Tether修改了其政策声明，将向关联公司提供的贷款纳入其担保储备，这在一定程度上证明了怀疑是对的。

多年来，多个政府机构对Tether的行为展开了调查。2021年2月，纽约总检察长对Bitfinex和Tether的内部财务进行了调查，但没有提出正式指控。不过，纽约总检察长确实对Bitfinex将客户和公司资金混在一起的指控处以了1850万美元的罚款。

Tether的故事还在继续，短期内不太可能解决。最近的一些事件进一步证明了它的合法性，比如Coinbase上市Tether。Bitfinex首席技术官Paolo Ardoino也重申，Tether是由FinCEN注册和监管的。

去中心化稳定币

DAI

Maker是DeFi首次尝试去中心化中央银行之一。作为一种借贷协议，当抵押品(通常是ETH)被存入创户金库时，DAI作为借贷需求的副产品被发行。

这些保险库的抵押过高(除稳定币外，一般是150%以上)，这有助于防范抵押资产价值大幅下降的黑天鹅事件。创贷者通过控制贷款利率来影响购买者和借款者的行为，从而帮助调节DAI的供应。

这种设置的问题在于：过度担保限制了资本效率，使得DAI难以随着需求的增长而扩大规模。如果降低DAI价格的套利机制要求更高的资本来赎回更多的DAI。

例如，抵押比率为150%的ETH Vault-A将要求借款人再支付1.5美元来铸造1个DAI。这导致DAI的价格上涨至1美元以上，因为它无法满足需求，比如臭名昭著的黑色星期四运行和Compound的流动性挖掘项目启动。

Maker试图通过多种方法来解决这些问题，例如其Peg Stability Module解决方案。然而，很明显，DAI的需求仍然随着杠杆的需求而扩大，而不是对更分散的交易媒介的需求。

我们如何解决稳定币问题?

每个稳定币都有自己的一套问题，并不严格限于Tether或DAI。问题的核心是如何平衡DeFi的去中心化理念并且创造一种能够可靠地维持其联系汇率的货币。

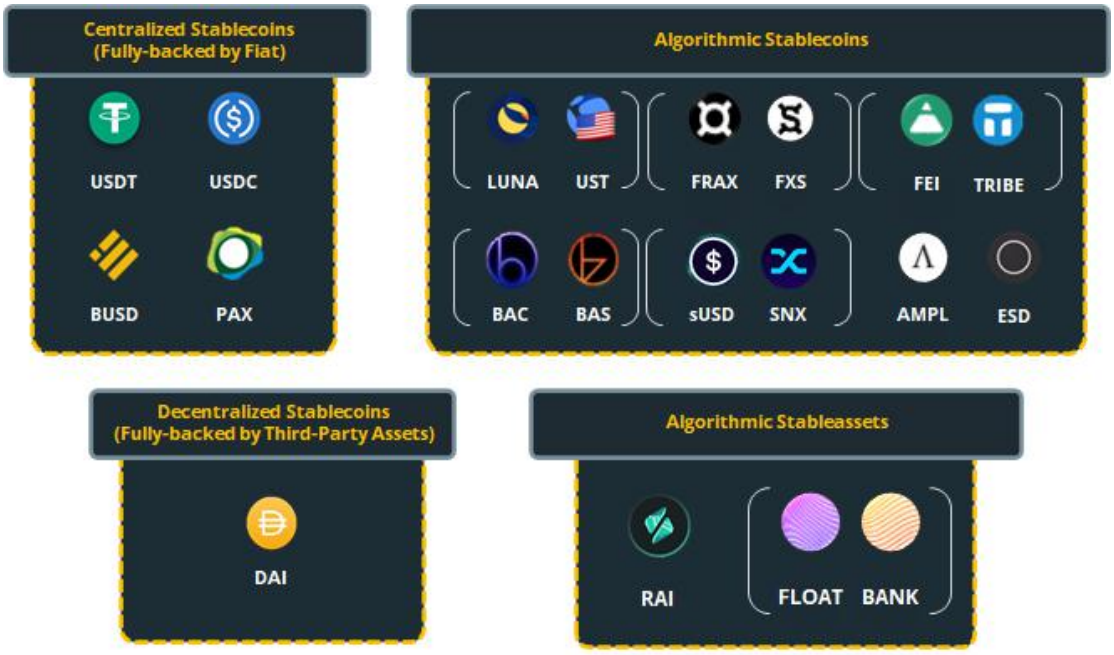
尽管中心化稳定币是可靠的，但它们需要信任一个廉洁的中心实体，并且有着困扰传统金融的同样的系统性风险敞口。另一方面，虽然DAI可能有着去中心化的特性，但它仍然是资本效率低下的，不能满足当前的市场需求。

此后出现了一些去中心化稳定币协议，希望改善去中心化、价格稳定性和资本效率。我们称这些协议为算法稳定币。

什么是算法稳定币和稳定资产?

顾名思义，算法稳定币利用算法来控制稳定币的市场结构和基础经济。你可能会把算法稳定币想象成一个自动化的美联储，在那里，预先编程的代码执行特定的行动来控制和影响价格，无法进行人为干预。

如果我们要在当前状态下对稳定币或稳定资产市场进行分类，下图提供了一个简洁的概述：



来源：CoinGecho 2021年第一季度报告

对于各种分散算法稳定币有两种分类方法：
没有抵押品(ESD、AMPL和BAC)
由他们自己的本地令牌(FRAX, sUSD和UST)部分/完全担保

为了对稳定币进行分类，我们将UST和sUSD作为算法稳定币，因为它由其本地代币支持，而不像DAI，它由第三方资产支持，如ETH和USDC。因为依赖本土发行的资产作为抵押品会产生递归价值，需要算法函数来调节价格。

算法稳定币可以进一步细分为不同类别——主要的子类别是rebase和铸币税模型。

变基模型

rebase模型通过改变稳定币的整个供应来控制价格。根据稳定币的价格是否高于或低于预期挂钩，该协议将自动增加或减少每个持有人钱包中的供应在一个固定的时期。

这样做的原因是，通过强制控制供应，稳定币的价格可以根据简单的通胀/通缩经济理论来影响。
这种模式的先驱协议是Ampleforth (AMPL)，最早可以追溯到2019年。

Ampleforth

每24小时，Ampleforth (AMPL)的整个流通供应都会按比例增加或减少，以确保价格保持在1.31美元。如果AMPL的价格高于1美元的目标价格5%或更多，那么rebase将扩大对持有AMPL的钱包的供应。如果AMPL的价格低于1美元的目标价5%或更多，那么rebase将减少持有AMPL的钱包的单位。

每个钱包持有人都将受到影响，但他们将保持和以前一样的市场份额。这些b变基，无论是正的还是负的，都是非稀释性的，因为它们影响所有AMPL平衡的比例。

由于重置基础发生在固定的时间间隔内，用户可以在重置基础之前为他们的交易设定购买或出售AMPL权利的时间，以增加他们所持资产的价值。

铸币税模型

铸币税模型通过引入影响市场动态的奖励系统来控制价格。如果价格高于挂钩，将铸造新的代币，并提供流动性或持有代币的参与者。

如果价格低于挂钩，代币就会停止铸造，并引入减少供应的机制。用户可以购买烧掉基础代币的优惠券，将其从供应中移除。这些息票可能在未来赎回更多代币，但只有当价格返回或超过预期的挂钩。

这里有三个基本迭代模型:

Empty Set Dollar

空集元(ESD)是一种单代币铸币税模型。顾名思义，在这个模型中只有一个标记。用户通过协议的本地令牌在去中心化自治组织(DAO)中提供流动性或股权——ESD令牌有效地充当稳定币和治理令牌。

在每个时代的开始，系统将测量时间加权平均价格(TWAP)。如果TWAP高于1美元，该协议将进入通货膨胀阶段，并制造代币作为对DAO股东和流动性提供者的奖励。相反地，如果价格低于1美元，协议将进入收缩阶段，用户将无法获得任何奖励。

在收缩阶段，如果协议再次进入扩展阶段，用户可以通过燃烧ESD来购买优惠券，赚取高达45%的溢价。然而，优惠券只能持续30天，这意味着如果系统处于收缩阶段超过30天，买家可能什么都得不到。防静电周期为8小时。

Basis Cash

Basis Cash是一种双代币铸币税模型。顾名思义，还有一个额外的代币称为股票代币。Basis Cash的稳定币是Basis Cash (BAC)，而其股票代币是Basis share (BAS)。

与ESD一样，Basis Cash依赖于TWAP机制，该机制将铸造或停止铸造BAC，取决于BAC的价格是高于还是低于$1。当BAC高于1美元时，协议进入一个扩展阶段，用户可以通过绑定BAS从会议室DAO收到新生成的BAC。

当BAC低于1美元时，该协议进入收缩阶段，在此阶段，没有新的BAC将被生产给在会议室的BAS股东。基础债券(类似于ESD息票)可供购买，定价为(BAC)^2。基础债券的购买者将在协议再次进入扩展阶段时赎回BAC。

Basis Cash周期持续24小时，与ESD息票不同，基础债券没有到期日。

Frax Finance

Frax借用铸币税模型的原则来创建自己的独特模型，其稳定币(Frax)由两种类型的抵押品支持——fiatbacked centralized stablecoin (USDC)和它的本地股票代币Frax share (FXS)。尽管Frax目前使用法定稳定币作为抵押品，但该协议确实打算最终完全多样化为去中心化抵押品。

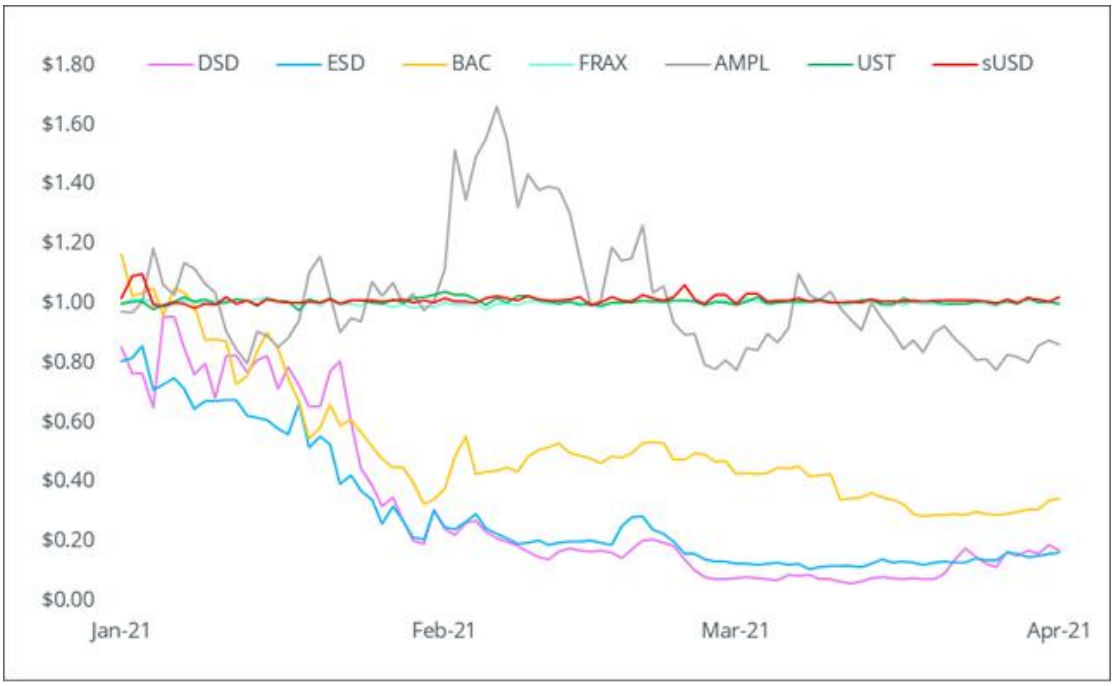
与Basis或ESD不同，Frax采用了分数抵押方法。Frax采用比例积分导数(PID)控制器控制可调的抵押率。抵押品比率是根据增长比率进行调整的，增长比率衡量的是FXS的流动性与FRAX的总体供应之间的比率。

Frax稳定币(Frax)可以被铸造并从协议中赎回，价值为1美元。这刺激了套利者购买或铸造FRAX，使价格回到固定汇率。另一方面，FXS收取费用、铸币税收入和超额抵押品价值。值得注意的是，Frax推出了veFXS，将算法市场运营控制(AMO)的部分利润提供给FXS股东，类似于veCRV从Curve Finance获得部分交易费用的方式。

当FRAX高于$1时，PID将抵押品比率降低一步，当FRAX低于$1时，PID将抵押品比率提高一步。刷新率和步长参数都可以通过FXS治理进行调整。

截至2021年5月8日，FRAX 依靠USDC占比85.25%， FRAX依靠FXS占比 14.75%。

到目前为止，算法稳定币进展如何?



来源：CoinGecko 2021第一季度报告

在2020年的最后一个季度，我们看到市场上推出了许多算法稳定币。许多稳定币使用铸币税模型。

尽管加密社区很兴奋，但大多数协议都失败了。如果我们看看市值排名前7位的算法稳定币的历史价格，只有UST、sUSD和FRAX成功地保持了与美元的挂钩。

虽然每个协议都有自己的设计机制和独特的失败原因，但我们可以对铸币税型稳定币的问题做一些一般性的观察研究。

历史上，法定货币体系更容易实施，因为国家有中央集权。例如，君主和政府垄断铸造硬币和保证其价值。与此形成对比的是，在稳定币市场，新协议必须在一个实验产品的基础上，在一个高度饱和的竞争和现有机构的分散环境中，一夜之间做同样的事情。

为了克服这个问题，算法稳定币以极高的流动性挖掘奖励的形式提供了令人难以置信的激励。这种方法的问题在于，它主要吸引投机者来做一个快速的转手，产生了一种名为Algo-Farmers的新型高产农民。

Algo-Farmers有一个目标——在其他人之前寻找新的算法稳定币协议，通过提供流动性来种植本地稳定币，并在其他Algo-Farmers开始涌入时退出系统。因此，分配集中在第一批AlgoFarmers内部，并向后来

者倾销。算法稳定币的发行实际上变成了一场抢椅子游戏，因为投机商没有什么动力去承诺并积极地为单一社区做出贡献，他们会迅速转向其他算法稳定币的克隆体。

不出所料，供应冲击导致了巨大的价格波动。大多数算法稳定币在设计时都考虑到了某种合作社区，但这未能激励用户在收缩期间支持系统，甚至无法抵消较大参与者的价格操纵。

最重要的是，算法稳定币大多在Uniswap等自动做市商上交易，由于其产品市场特征不变，这放大了波动性。在通缩阶段，由于临时性损失风险，流动性提供者也不愿提供流动性，导致进一步的波动。

为什么FRAX获得成功?

尽管sUSD、UST和FRAX的成功各有各的原因，但我们将重点关注FRAX，因为它迄今为止的钉住率最好，2021年第一季度的平均价格为1.001美元。以下是我们认为他们到目前为止成功的一些原因：

frx部分由USDC担保，这向社会注入了信心，以维持其挂钩制度。截至2021年5月8日，85.25%的FRAX是由USDC支持的。

Frax保持了抵押比率的灵活性，解决了Frax定价为1美元的市场需求。

抵押品被重新配置到其他地方赚取利息。这有助于带来外部收入，并保持协议运行，然后用于回购和烧毁FXS。

由于FXS的回购和焚烧机制，FRAX的价格波动转向了FXS。

虽然这些只是简单的原因，但仍然需要不断重新考虑，特别是在危机时期，FXS的价格大幅下跌，流动性挖掘回报最终停止。

下一代算法稳定币和稳定资产

虽然FRAX在很大程度上是成功的，但有人可能会说它并不是真正的去中心化，因为它仍然部分由USDC担保，而USDC由一个中央实体(CENTRE Consortium - Coinbase和Circle共同创始成员)持有的现金储备支持。

新进入者正试图避免这种困境。它们仍然倾向于抵押系统，但有自己的独特之处，这使得很难在现有算法稳定币的保护伞下进行分类。我们将介绍三个示例。

Fei Protocol

Fei于2021年第一季度末推出。与Frax类似，Fei使用了部分担保系统，但却完全由ETH支持。Fei的稳定币(Fei)与1美元挂钩，这是由创新概念支撑的，以保持其挂钩，并确保协议的整体金融稳定性。

Fei引入了一种称为协议控制值(PCV)的机制，而不是借用抵押品。从本质上讲，Fei通过新创建的Fei向用户购买ETH。然后Fei将使用ETH来支持其抵押担保的流动性池。其他常见的用例包括治理国库和保险基金。在初始启动期间，Fei将ETH bonding曲线所资助的PCV的100%分配给使用ETH交易对的Uniswap池。

当FEI的价格高于1美元时，该协议允许用户使用ETH作为支付方式，以折扣价格(类似于FRAX)直接从系统中铸造新的FEI。

然后，交易者可能会进行套利，直到价格达到1美元的固定汇率。当FEI的价格低于1美元时，协议将向FEI卖家征税(他们的税随后被烧毁并从供应中移除)，并奖励额外的FEI给买家(除了他们最初的购买)。交易

算法确保税款超过买家将收到的金额。

在紧急情况下，FEI的价格在很长一段时间内低于挂钩，FEI可以从Uniswap撤回其pcv支持的流动性，并从市场上购买FEI。与此同时，FEI也被烧了。一旦恢复联系，Fei将向Uniswap重新提供剩余的流动性。

Fei还有一个本地治理令牌(TRIBE)，它最终将成为DAO的基础。未来，TRIBE持有者将能够决定调整PCV分配和增加/调整bonding曲线。

Reflexer

与其他算法稳定币不同，Reflexer的原生代币(RAI)并不是一个固定挂钩的稳定币。RAI于2021年第一季度推出，目的是成为稳定的抵押品，并取代现有的抵押品资产，如ETH或BTC，这些资产自然波动。RAI使用基于eth的过抵押模型，并有一个浮动挂钩，最初设定为3.14美元。

Reflexer采用浮动管理机制原则，类似于中央银行的运作方式由于价格不断波动，Reflexer设计了一个系统，在该系统中，RAI的矿工和交易员(RAI持有者)之间的市场互动被激励去追逐RAI的赎回价格(浮动挂钩)，以保持RAI的价格相对稳定。

为了制造RAI，用户需要将ETH存入抵押物，抵押率最低为145%。然后向用户收取稳定费(借款利率)。截至撰写本报告时(2021年5月)，稳定费为每年2%。然而它是可变的，可以通过治理投票进行修正。

当RAI的价格高于浮动挂钩时，系统就会降低挂钩。这让用户能够赚取更多的RAI，并将其卖回给ETH以获得更高的回报。意大利广播电台的价格低于浮动挂钩时，系统就会提高挂钩。这使得借贷成本更高，并激励RAI的矿工偿还他们的RAI贷款，从而使RAI退出流通，并推高价格。

在紧急情况下(结算)，协议将关闭，只允许RAI的矿工和RAI的持有者以当前的赎回价格从系统中赎回ETH抵押品。

Reflexer还有另一个本地令牌(FLX)，作为最后贷款人，管理某些功能，并允许用户将其置于保护系统的池中。还有债务拍卖，以偿还FLX以换取RAI——通过拍卖获得的RAI将用于消除系统中的坏账。从较长时间来看，FLX旨在成为一个非治理令牌，随着时间的推移逐步实现系统自动化和最小化治理。

Float Protocol

Float与FRAX非常相似，它使用双代币铸币税模型，并部分由ETH担保。然而，与FRAX不同的是，Float的本地资产(Float)有一个浮动汇率，但其初始钉住价格为1.61美元。

Float's share token(BANK)也作为治理通证和监管机制来支持流通股价格。Float使用与Fei的PCV类似的机制，用户只能从协议中获得新创建的Float。然而，Float通过荷兰式拍卖出售Float，在这种拍卖中，价格以可能的最高价格列出，然后向下降到最低价格(保留价)。为了获得FLOAT，用户必须同时使用BANK和ETH支付。资产支付比率取决于对FLOAT的总体需求和ETH在池子中的价值。

如果篮子过量，ETH会在目标价格购买FLOAT, BANK会在目标价格购买FLOAT。从荷兰拍卖中获得的ETH(或任何其他未来交易资产)将作为抵押品存储在协议的担保库(Basket)中。银行被烧毁时，用户铸币浮动。

当FLOAT的价格高于浮动挂钩时，任何用户都可以开始拍卖。最初，它只能在至少24小时后启动，但一旦团队对用户习惯了拍卖功能感到满意，这将被删除。一旦拍卖开始，系统就会制作并出售新的FLOAT，从市场价开始，再加上额外的溢价。价格会随着时间的推移而下降，直到达到目标价格。

当FLOAT的价格低于浮动挂钩时，协议将以反向荷兰拍卖的形式从市场上购买FLOAT。这是指Float以增量价格向买家提供它所能接受的出价。浮动是购买ETH和新铸成的银行。

流通股初始担保比率(一揽子因素)在发行时设定为100%，但可能通过治理投票进行修正。在紧急情况下，如果浮动汇率制低于盯住汇率，则可将储存在货币篮子中的资产用于支撑浮动汇率制的价格。

这些新的算法稳定币和稳定资产将如何运作?

旧的算法稳定币将资本效率置于一切之上。挂钩是固定的，纯粹依赖于个人博弈论机制，而未经测试的自举方法也很流行。

稳定币以其与美元挂钩而闻名，但该领域的最新发展已经改变了这个定义。我们现在有了一种新的资产类别，称为算法稳定资产。

我们认为FLOAT和RAI是算法稳定资产，主要是因为它们有一个浮动挂钩。无论如何，关注的焦点应该是这些资产能否保持价格稳定。为了回答这个问题，我们考虑了三个主要因素:

1. 支链化

较新的稳定算法正在采用一种更为保守的方法，即抵押优先于资本效率。

Fei的PCV方法利用流动性抵押，其中抵押品被自动转移到Fei的Uniswap流动性池。治理投票(通过TRIBE原生代币)将允许用户控制PCV比率，这是有效的抵押品比率。

这类似于浮动篮子系数。然而，Float还有一个额外的优势，即浮动挂钩和股票代币(BANK)，这是收购Float所必需的。这增加了它的价值，并有助于将额外的波动性存入BANK，而不是FLOAT。银行可以被用作抵押品，尽管Fei也可以抵押TRIBE，但由于其拥有较少的效用，其惰性价值较低。换句话说，Float和Fei都让市场力量决定理想的担保比率(类似于FRAX)。

相比之下，Reflexer的RAI是过度担保的，不太容易发生黑天鹅事件。有最低抵押要求，但没有最高要求。的确，人们可以辩称，Reflexer很有可能取得成功，因为它是Maker's Multi-Collateral Dai的分支，并在黑色星期四(Black Thursday)之后成功维持了挂钩(尽管花了很长时间)。此外，RAI并不局限于一个固定的挂钩，因此给了它更大的灵活性。

2. 交易员奖励和惩罚措施

算法稳定币和稳定资产旨在影响市场行为，以帮助维持其固定价格。老一代专注于奖励正确的用户行为(即套利者)。对于较新的算法稳定币和稳定资产，当价格高于挂钩时，这三种货币都拥有类似的铸造奖励机制。然而，在通货紧缩阶段，他们的做法有明显的不同。

较新的协议正在纳入负强化策略。当Fei以低于挂钩的价格出售时，Fei会用交易税惩罚卖方。Reflexer通过提高挂钩间接提高借款利率，鼓励借款人偿还贷款(类似于Maker)。浮动略有不同，因为它让用户在他们的反向荷兰拍卖中战斗。而不是惩罚或奖励用户，浮动让市场力量来决定。

3. 紧急权力

最引人注意的发展是更强大的协议功能的推动。每个协议的系统设计都有内置的功能，以保护其本土资产显著贬值时的市场。人们可以将其与传统金融相提并论，在传统金融危机期间，监管机构或中央金

融机构会介入。

Fei通过将其PCVbacked的流动性从Uniswap池中移除，实质上切断了获取流动性的途径——类似于一个国家可能对银行提款施加限制。然后Fei会卖掉它并提出从市场上回购超额FEI。浮动执行类似的策略，除了购买资金来自篮子。

反射器停止所有借款，只允许偿还贷款。

相关风险

算法稳定币仍处于实验阶段，这一点再怎么强调也不为过。协议仍在试图弄清楚如何在没有巨大价格波动的情况下成功推出。

许多算法稳定币协议也严重依赖有能力的套利者来维持价格挂钩。如果您不确定协议是如何工作的，那么如果您试图与精明的套利者(甚至bot)竞争，您将处于严重的劣势。

算法稳定币需要一个强大的社区，相信项目的基础。通常情况下，短期获利者会利用他们的资本储备来控制和操纵价格。在去中心化的市场中，只有具有强大潜在机制的合作社区才能克服这一困境。

换句话说，您需要投入大量的时间和资源来理解每个项目。只有这样，你才能决定它是否能与许多已经建立了市场地位的替代稳定币/稳定资产竞争。

值得注意的情况

Empty Set Dollar v2 (ESD)

通过引入一种新的代币ESDS, ESD正向双代币稳定币模型迁移。ESD v2(也称为连续ESD)将与Frax非常相似，通过合并由USDC支持的银行储备，获得部分担保的稳定币。这两个新特性与ESDS一起，有望帮助减轻ESD令牌的波动性。

Dynamic Set Dollar v2 (DSD)

虽然大多数稳定币协议专注于部分或完全担保模型，但DSD (ESD的分支)认为这削弱了去中心化的优势。尽管最初失败，但DSD通过引入一个新的代币CDSD更新了它的模型，该代币部分可以1:1兑换DSD代币。其想法是将DSD代币的波动性转移到CDSD上——类似于Frax的模型，但不含任何抵押品。

Gyroscope (GYR)

Gyroscope机制是多种算法稳定币协议的融合，具有自身的扭曲。GYR被过度担保，并由多个资产分成单独的保险库(类似于Maker)支持。与大多数算法稳定币一样，存在套利机制，但添加了一个互补的杠杆贷款机制。在危机时期，用户等待还贷的时间越长，赎回率越高。

TerralUSD(UST)

与DSD v2类似，UST是一种无担保双代币模型(以及LUNA)，完全依赖套利来维持其1美元挂钩。截至撰写本文时，UST是唯一成功维持价格稳定的算法稳定币之一——可能是由于强劲的需求和将采矿网络纳入

其价格稳定机制的繁荣生态系统(Terra)。

结论

算法稳定币有效地取代了中心银行，而算法稳定资产是DeFi模仿金本位制并创建可靠数字抵押品的方式。在传统金融中，一个成功的货币体系需要一个称职和独立的金融当局。在DeFi中，能力来自于被激励合作和理性行动的伪匿名个体。

算法稳定币有效地取代了央行，而算法稳定资产是DeFi模仿金本位制并创建可靠数字抵押品的方式。在传统金融中，一个成功的货币体系需要一个称职和独立的金融当局。在DeFi中，能力来自于被激励合作和理性行动的伪匿名个体。

第七章:去中心化衍生品

数字资产已经广为被接受的当下，逐步发展出为用户和交易员创造复杂的金融产品。目前，加密衍生品的使用在币安期货、衍生品、FTX和Bybit等中心化平台上已经很普遍。

随着去中心化衍生品平台的发展，交易员现在也可以以不同的方式交易加密衍生品。在本章中，我们将分三个不同的部分介绍去中心化的衍生品——去中心化的永续证券、去中心化的期权和合成资产。

去中心化合约

作为加密领域最受欢迎的衍生品之一，永续合约可以让用户在没有到期日的期货合约上建立杠杆头寸。以前，永续证券只能在中心化交易所获得，但是像Perpetual Protocol和dYdX这样的去中心化平台已经为更广泛的DeFi社区在完全控制自己的基金的同时获得杠杆头寸铺平了道路。

Perpetual Protocol

Perpetual Protocol是一种去中心化的协议，提供永续合约交易，允许用户在各种加密资产上开立多达10倍的多头或空头头寸。为了实现这一点，Perpetual Protocol使用了一种独特的虚拟自动做市商(vAMMs)方法。

与Uniswap和Balancer的amm功能类似，交易员可以直接通过vamm执行交易。主要区别在于“虚拟”部分。

在传统的amm中，资产存储在智能合约中，每个资产的交换价格通过特定的数学函数确定。永续协议中的vamm不存储任何资产。

相反，实际资产存储在以USDC计价的智能合约库中，成为用户开立杠杆头寸的抵押品。保险库中的资金总量基本上构成了交易者利润的上限。每个永续合约都有自己特定的vAMM，但是它们都受到协议保险基金的保护。

Perpetual Protocol能够提供更高的交易速度和最小的gas费用，使用xDai链进行交易执行。有了vAMM，用户可以获得高流动性和低滑点，满足他们的交易需求。

与所有形式的永续合约交易一样，资金利率和清算比率是永续协议的关键方面。资金利率是以小时为单位结算的，而清算比率则设定为公布利润率的6.25%。这意味着，持有低于6.25%保证金比率的头寸的交易员将面临被“看门人机器人”平仓的风险。Keeper bots将赚取20%的清算保证金，而剩余部分将存入协议的保险基金。

该协议有自己的PERPtoken ，主要用作平台的治理通证。PERP代币持有者获得与其持有比例的投票权。此外，他们可以在一段固定时间内抵押他们的PERP，以在USDC中获得更多的PERP和协议交易费。

这个固定的时期代币持有者在每个锁定期结束之前都不能提取他们的资金。交易费用可在交易结束后立即获得，而PERP奖励最长可锁定6个月。质押者虽然可以保障本金，但PERP代币价格也是会波动的。

关于永续协议，你知道这些就够了。到2021年4月，在以太坊和xDai主网上都可以玩，所以你可以尝试一下。

dYdX

dYdX是一个去中心化的交易协议，用于借贷、借款、现货交易、保证金交易和永久掉期交易。dYdX是第一个专注于去中心化永续的项目，目前支持三种资产的现货和保证金交易- ETH, USDC和DAI。

对于永续兑换，目前dYdX有11种不同的合约可供交易，包括BTC, ETH, AAVE和LINK。

dYdX与Aave、Compound等其他借贷平台有一些共同特征，允许用户存入资产以赚取利息，或将存入的资产作为抵押进行借贷。然而dYdX也有与众不同的地方，通过在ETH上整合保证金交易，其杠杆率高达5倍，使用DAI或USDC。用户还可以利用高达10倍的杠杆在dYdX上做永续合约交易。

dYdX的贷款非常灵活，自动匹配借款人，所以在你开始赚取存款利息之前无需等待。每次使用该资产进行交易时，利息支付都以复利计算。

利率是根据利用率水平动态更新的——利用率越高，贷款人的利率就越高。对于借款人来说，初始抵押比率需要达到125%，最低抵押比率需要保持在115%，以防止自动清算。

dYdX为现货交易员提供类似于集中交易所的功能，有市场、限价和止损单。保证金或现货仓位的交易费用收取仅限于买方，收取的金额为0.3%或根据当时的gas费，以两者中较高者为准。为了减少天gas成本，交易者应该注意订单大小——平台会对小额的订单收取额外费用，以支付完成交易所需的gas费。

对于dYdX的永续市场，所有的合同都以USDC担保。然而，每个合同使用不同的预言机、订单大小和保证金。只要有仓位空缺，融资利率就会持续每秒钟收取一次。费率是每小时重新计算，并以8小时费率表示，类似币安期货，但dYdX的永续合同不让美国居民使用。

在2021年第一季度，dYdX与Starkware合作建立了第二层交易协议，允许更快和更便宜的交易。

使用一个可伸缩性交易将使用零知识卷(zK-Rollup)进行链下匹配，并在以太坊主网进行结算。用户现在可以通过生成Stark密钥进入二层网络，该密钥用于识别你在dYdX上的第二层账户，并发送交易来注册链上的账户。

Perpetual Protocol与dYdX的比较(Layer 1)

项目	Perpetual Protocol	dYdX(layer1)
支持	Btc, eth, yfi, link, dot, SNX	Btc, eth, link, aave, uni, sol, sushi, yfi, 1inch, avax, doge
交易模型	虚拟AMM	订单簿
最大的利用	10倍	10倍
初始保证金	10%	10%
维持保证金	6.25%	7.5%
融资利率	每小时	每一秒
交易费用	0.1%的名义	Maker:-0.025% Taker:高于0.2%或gas成本

在合同规范方面，两个平台为各自的市场提供了高度相似的杠杆选项和保证金要求。Perpetual Protocol提供了更多的资产选项，平均每天6000万美元的交易量比1500万美元的dYdX多几倍。

但我们认为，在引入2层技术以及和更多Dex对接(如Aave和Uni)之后，dYdX可能有潜力以较低的费用与Perpetual Protocol竞争。

其他代表

- Futureswap

Futureswap是一个去中心化的永续交易所，允许用户对任何ERC-20货币对进行高达10倍的杠杆交易。

- MCDEX

MCDEX是一个基于AMM的去中心化永续交换协议，目前使用的是他们的Mai协议的第二次迭代。任何用户都可以创建一个永续的市场，ERC-20代币可以用作抵押品。

- Injective Protocol

在Injective CHAIN的支持下，这个第二层衍生品平台支持完全去中心化的订单簿和到以太坊的双向桥接。到2021年4月为止，它仍在测试网中。

去中心化期权

期权长期以来一直是传统金融的主要产品，为买家提供了押注价格走势的机会，以对冲其资产价值，或以最小的资本放大其回报。随着DeFi继续在加密行业掀起热潮，去中心化期权协议的出现是很自然的。

加密货币用户历来在中心化的(衍生品)交易所进行期权交易，但同时也对去中心化的期权协议有着内在的需求。在本章中，我们将看看两个领先的去中心化期权协议，Hegic和Opyn。

Hegic

Hegic是一个去中心化的链上协议，允许用户购买ETH和WBTC的美式看涨期权和看跌期权。用户也可以通过提供流动性来出售期权来赚取溢价。使用该平台的界面，用户可以自定义他们想购买的期权的条款，如执行价格和到期日。

一旦选择了期权条款，期权价格将自动计算，包括购买期权规模1%的结算费用。虽然这些期权是不可交易的，但由于期权合约的流动性被锁定，用户可以在任何时候行使它们。

Hegic使用的是流动性池模型。换句话说，用户将他们的资金聚集在一起，并将其用作担保所有售出的期权的抵押品。截至2021年4月，ETH和WBTC有两个独立的池。流动性提供者锁定ETH或WBTC，并根据提供的资产接收一定数量的代币。

Write token代表供应商对用户购买期权所支付保费的索赔。尽管任何人都可以从流动性池中购买期权，但每个流动性池的最高购买限额为总标的抵押品的80%。

关于Hegic，值得注意的是，你可以通过使用平台获得奖励。HEGIC有一个流动性挖掘计划，奖励持有其Write代币的用户，并根据购买的期权规模和期限奖励期权买家。

这些奖励的形式是rHEGIC代币。

HEGIC代币也可以下注赚取协议费用，两个池100%的结算费用都分配给HEGIC下注Lot的所有者。要下注lot，你需要88.8万HEGIC。

Hegic已累计锁定总额超过5000万美元，并在一天内结算了超过2200万美元的交易量。

接下来，我们将关注另一个去中心化期权平台Opyn。

Opyn

Opyn是最早推出的去中心化期权平台之一。第一个版本，Opyn V1，允许您通过锁定100%的基础资产作为抵押品，以otoken的形式创建token化的美式期权。

流动性提供者锁定他们的抵押品，Opyn可以提供广泛的资产选择，如ETH, WBTC, UNI和

SNX，尽管有固定的期限和执行价格。otoken可以通过发送稳定币的执行量并烧毁otoken以换取标的资产来行使，或者可以通过Uniswap将其转售给其他方。最重要的是，Opyn不收取任何额外的交易或结算费用。

Opyn V2推出了额外的功能，如auto exercise和闪电铸造，这是对现有的闪电贷款概念的创新。最新版本通过类似于衍生品的订单薄系统提供欧洲期权，但目前仅限于Wrapped Ether (WETH)，执行价格和到期日范围较小。

Hegic和Opyn的比较

这两个协议是如何相互竞争的？在下表中，我们基于几个因素比较了这两个平台。

平台	Hegic	Opyn V1	Opyn V2
选择类型	美式	美式	欧式
流动性模型	单项资产池	Uniswap池	订单
支付类型	现金	现金	现金
抵押资产	ETH,WBTC	Eth wbtc uni SNX	WETH, WBTC
保险费付款	ETH	dai,ETH USDC	USDC
抵押品的要求	100%	100%	100%

在这里，我们可以看到，两个期权平台都需要由期权发行者完全担保，但在流动性模型和支持的资产数量方面有很大不同。

美式结算的选择似乎受到两种协议的青睐，因为它在快节奏的DeFi空间提供了一定程度的灵活性。这与欧洲期权形成了鲜明对比，后者受到衍生品交易所(如Deribit)等中心化式衍生品交易所的青睐。在Opyn V2中，考虑到数字资产的不稳定性，具有较小执行价格选择的薄订单表明，对具有严重时间限制的产品的需求较低。

其他代表

- FinNexus

FinNexus允许用户创建几乎任何资产的期权，只要有可靠的价格馈送。该协议使用了一个多资产单一池(MASP)系统，该系统允许在只使用单一资产类型作为抵押的情况下，对不同的基础资产持有头寸。

- Auctus

Auctus是一个DeFi协议，允许用户执行flash exercises，它们还通过Auctus vault和专门的场外期权交易部门提供本金保护的收益农。

- Premia

Premia为用户提供了一个购买和出售期权的二级市场。用户可以在更少的交易中创造、转移和行使多种选择类型，节省时间和GAS成本。

- Antimatter

Antimatter公司的目标是通过为其永续期权产品提供一个交易所，将自己推销为期权的Uniswap。用户可以通过购买这些期权token获得长期或短期风险敞口，这些期权token可以在不担心到期日期的情况下进行赎回。

- Siren Protocol

通过Siren Protocol，用户可以通过从SirenSwap自动造市商购买特定期权系列的btoken或wtoken来选择成为期权的撰写者或购买者。btoken代表买方一方，允许持有人行使期权，而wtoken代表卖方一方，将用于在行使时提取抵押品或接收付款。

合成资产

合成资产是指与另一资产具有相同价值或效果的资产或资产组合。合成资产跟踪标的资产的价值，允许在不需要持有实际资产本身的情况下对资产进行敞口。

合成资产的例子几乎包括任何可追踪的资产，从真实世界的股票到以太坊gas价格，甚至是CoinGecko网站上的指标。交易这些合成资产的用户可以在不持有任何实际资产的情况下拥有这些资产的风险投资权。

在本章中，我们将比较DeFi合成资产领域中最大的两个协议，即Synthetix和UMA。

Synthetix

在我们的《How to DeFi:Beginner's book》一书中，我们已经广泛地介绍了Synthetix；

Synthetix是一个铸造和交易合成资产的去中心化平台被称为synth，由平台用户提供的抵押品支持。

synth允许用户在不持有实际资产本身的情况下跟踪基础资产的价值。有两种类型的synth - Regular synth(例如sDEFi)和Inverse synth(例如iDEFI)。并不是所有的synth都有一个相反的版本。

synth可以用于各种资产类别，如加密货币、法定货币、大宗商品、股票指数和股票。资产的价格通过Chainlink跟踪，这是一个去中心化的预言机，从多个来源收集价格信息。

Synths是利用超额抵押来创造的，这一概念类似于Maker在铸造Dai时的做法。要制造synth，用户必须持有Synthetix网络令牌(SNX)作为抵押品。由于SNX的价值可以快速向任何方向移动，需要500%的大抵押比率来减少清算风险。

为了保持最低500%的抵押比率，用户可以燃烧低于目标比率的synth，或铸造更多的synth，用户唯一可以铸造的Synth是sUSD。

synth主要在Synthetix交易所交易，这是一个去中心化的交易所，不依赖订单簿，而是依赖用户流动性。Synthetix Exchange允许用户直接针对智能合约进行交易，该合约保持持续充足的流动性，从而降低了下滑的风险。这对于其他交易所可能导致价格大幅下滑的大型交易尤其有用。

为了鼓励抵押和铸造synth，用户有机会获得交易费用和SNX抵押奖励。在Synthetix交易所交易产生的费用被发送到一个池中，在那里SNX的质押者可以手续费的一定比例。

复习了Synthetix，让我们看看UMA

UMA

UMA(Universal Market Access)是一种去中心化协议，用于在以太坊网络上创建和执行合成资产。UMA提供了构建安全金融合同的基础设施，使用其技术的两个核心部分——一个构建和部署衍生品的框架，以及一个被称为数据验证机制(DVM)的预言机来执行它们。

与Synthetix不同的是，这些金融合约被设计为“ priceless”，这意味着它们不需要链上价格馈送来正确估值。相反，这些合同将依赖于对合同对手方的适当担保。这是通过奖励识别虚假抵押头寸的用户来激励的。为了进一步核实不当担保，合同可能会使用DVM。

DVM是一个对这些合同的价格要求做出回应的预言机，仅用于解决与合同清算和结算有关的纠纷。价格请求来自UMA代币持有者，他们在特定时间对最准确的价值进行投票。代币持有者在一个多天的过程中提交并公布他们的投票。

一旦选票被显示出来，拥有最多选票的价格或价值就会被返回到金融合同中。抵押品然后根据这个投票数字分配给代币持有者。DVM是建立在这样一种方式上的。

基本上，这意味着恶意行为者的不良行为受到了抑制。这是通过确保破坏DVM的成本(作为超过一半的UMA投票代币的总成本)总是大于腐败的利润或内部可获得的总抵押品来实现的

除了DVM之外，UMA生态系统中还有其他5个重要的参与者。这些包括:

代币发起人-在智能合约中存入抵押品以制造合成代币的个人。他们有责任保持自己的抵押比率，防止清算。

清算人-监督网络，激励他们通过链下价格反馈来检查头寸是否被适当担保。在清算最终敲定之前，有两个小时的时间供争议方核实清算的准确性。

争议者-争议者是监控合同的激励用户。他们引用链下价格饲料来验证清算事件。如果无效，DVM将被调用。

DVM - 预言机将通过提议对给定时间内资产的最准确价格进行投票来解决争议。

代币持有者——UMA代币持有者在特定时间集体投票决定资产的价格。代币持有者将引用链下数据向DVM提供信息。然后，DVM将统计投票，并报告链上最一致的价格。

如果争论者是正确的，争论者和受影响的令牌发起者将得到奖励。如果清算人是正确的，清算人将获得奖励，而争论者将受到惩罚，代币赞助商将失去他们的资金，因为最终清算。

使用UMA框架构建的一些产品包括合成“收益美元”，这是到期时接近特定价值的代币，以及uGAS代币，可用于投机以太坊天然气价格。UMA还为流行的DeFi代币(如Sushi和Balancer)引入了看涨期权，以及他们自己的UMA KPI期权。

这些KPI期权跟踪UMA的TVL及其价格表现，确定期权持有人在赎回时可以赎回UMA的金额。

现在你对UMA和它的工作原理有了更多的了解，让我们来比较一下
这两个合成资产平台。

Synthetic与UMA的比较

平台	Synthetix	UMA
合成的令牌	Synths	uTokens
标的资产	法币、加密货币、大宗商品、股指、股票	几乎任何东西
预言机	Chainlink	数据验证机制
抵押品比率	500%	取决于token的铸造
能否质押	是的	是的

Synthetix和UMA都提供了超额抵押合成资产，在Synthetix上，synth的价值和抵押比率由链上价格反馈决定。

在UMA中，综合契约的解决是通过激励网络行动者行为来维持的。基于对所有代币发起人的全球担保比率的更灵活的担保要求，我们可以看到UMA可以成为一个更高效的资本平台。但是，Synthetix在选项方面有一个优势，因为它支持目录中超过50个synth。

此外，Synthetix围绕synth建立了一个生态系统，dHEDGE和Curve Finance的交叉资产互换是需求的主要驱动因素。dHEDGE是一个去中心化的资产管理平台

用户可将其投资于不同的投资组合。作为策略的一部分，被选中的投资组合将用其他合成资产交换美元兑美元。另一方面，Curve Finance的跨资产掉期利用Synthetix作为桥梁，允许交易员交换价值高达8位数的资产，且没有任何下滑。

在流动性方面，在没有专门交易这些资产的平台的情况下，UMA能否继续竞争还有待观察。其交易量也很低，日交易量仅为2,000万美元左右。尽管如此，在我们看到大规模零售和机构采用合成资产之前，仍有很长的路要走。

其他代表

- ***Mirror Protocol***

Mirror Protocol部署在以太坊和Terra区块链上，它发行合成资产，称为mAssets，模拟真实世界资产(如股票和指数)的价格。其中一些产品包括mAMZN和mQQQ。

- ***DEUS Finance***

允许用户从预言机获取源数据并将其标记为可交易的dAssets的DeFi协议。dAssets价格使用预言机数据将资产与现实中对应的资产1:1挂钩。

相关的风险

当使用去中心化的衍生品平台时，要注意杠杆交易和衍生品的使用是一个高风险的策略。保持一个健康的抵押比率，并密切关注你的头寸的清盘价格，是安全度过DeFi这一特定部分的关键。

由于合成资产主要依靠预言机作为价格信息的主要来源，数据伪造可能会导致不必要的后果。此外，由于合成资产主要是通过存放抵押品来铸造的，一旦缺乏这些资产可能会出现流动性危机，导致与现实资产相比的定价出现大幅扭曲。

在使用期权时，要确保你能及时行使现金头寸，因为有些平台不提供自动行使功能。由于未平仓头寸持续增加，就应该注意大量期权到期日，因为波动性趋于增加。

结论

去中心化的衍生品和合成资产为普通用户提供了参与以前无法进入或根本不存在的市场的机会。这些产品为方便用户而简化，不再是精英的专属。用户现在也可以在没有中介的情况下参与这些衍生品市场。

这一特定的DeFi子集相对而言仍处于起步阶段，截至2021年4月1日，锁定的总价值不到整个空间的10%。事实上，几乎每一个有前途的DeFi项目都面临着流动性的问题，衍生品也不例外。即使有激励措施，这些波动性较大的产品的本质似乎也超过了承销它们的参与者所获得的回报。

尽管像Charm和Perpetual Protocol这样的协议可以在最低流动性条件下运行，但要与能够提供更大交易量和高达125倍的更高杠杆率的大型集中心化交易所竞争，仍有很长的路要走。

推荐阅读

Decentralized Perpetuals

1. Documentation and Frequently Asked Questions about Perpetual Protocol
   https://docs.perp.fi/
2. Research, Insights, and Announcements from dYdX_
   https://integral.dydx.exchange

3. The latest news from dYdX_
   https://dydx.exchange/blog

Decentralized Options

1. Articles and announcements from Hegic_
   https://medium.com/hegic
2. Hegic Protocol – On-chain Options Trading Protocol_
   https://defipulse.com/blog/hegic-protocol-on-chain-options-trading-protocol/
3. Opyn Review https://defirate.com/opyn/
4. Beginner's Guide to Options: Opyn V2_
   https://medium.com/opyn/a-beginners-guide-to-defi-options-opyn-v2-4d64f91acc84

Synthetic Assets

1. Documentation & System Overview of Synthetix_
   https://docs.synthetix.io/
2. The latest news and announcements about Synthetix_
   https://blog.synthetix.io/
3. What is Synthetix? Everything you need to know about one of the leading DeFi protocols
   https://medium.com/coinmonks/what-is-synthetix-everything-you-need-to-know-about-one-of-the-leading-defi-protocols-bc19bdd2949c
4. UMA Documentation https://docs.umaproject.org/
5. List of Projects using UMA_
   https://umaproject.org/projects.html
6. UMA: Universal Market Access. Interview with Allison Lu_
   https://defiprime.com/uma

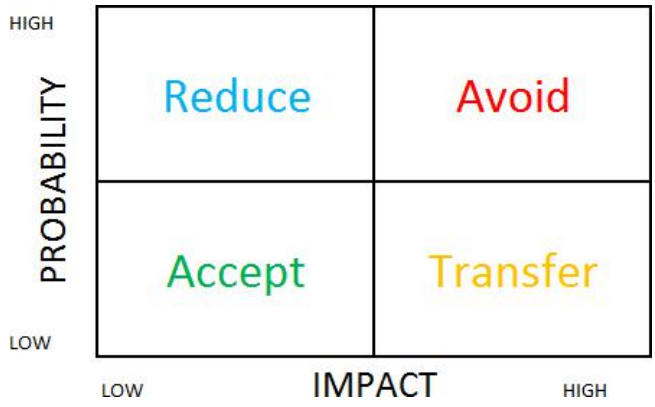
第八章:去中心化保险

随着DeFi项目的快速创新，我们看到越来越多的黑客攻击和项目漏洞被利用，导致重大损失。

如果DeFi生态系统只欢迎高风险偏好的玩家，DeFi的普及将不可避免地停滞。拥有一个健全的保险系统是降低用户在与DeF交互应用程序时承担的风险的关键措施，从而吸引更多用户进入这个领域。

保险是什么?

保险业是一个大行业，2019年全球承保的保费总额达到6.3万亿美元。世界本来就是混乱的，总有发生事故的危险。下面是一个简单的风险管理框架，告诉我们应该如何应对不同类型的风险。



在这一风险管理框架下，应将自然灾害、绝症等影响大但发生频率低的风险转移出去。保险就是用来处理这些类型的风险的。

保险是如何运作的?

保险的运作基于两个主要假设:

1.大数定律
保险承保的损失事件必须是独立的。如果事件重复的足够频繁，结果将收敛到期望值。

2.风险汇聚
损失事件具有频率低、影响大的特点。因此，由一大群人支付的保险费可以补贴几宗大索赔的损失。

从本质上讲，保险是一种汇集资本并将巨额损失社会化的工具，这样参与者就不会因单一的灾难性事件而经历金融崩溃。

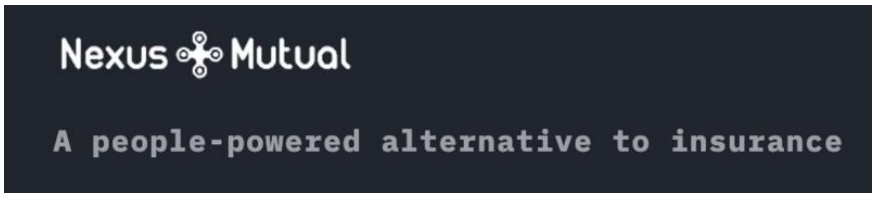
加密货币需要保险吗?

保险通过将任何灾难性事件的成本分散化，使个人能够承担风险。它是一个重要的风险管理工具，DeFi行业需要保险产品，以便拥有大量资本可用于投资的机构投资者相信，参与DeFi是安全的。

DeFi保险协议

我们将在下面详细了解三种DeFi保险协议- Nexus Mutual, Armor Protocol和Cover Protocol。

Nexus Mutual



Nexus Mutual是加密市场上最大的DeFi保险协议。截至2021年5月1日，它的总锁定价值(TVL)为4.5亿美元，相比之下，第二大DeFi保险协议Cover Protocol的锁定价值为700万美元。Nexus Mutual的创始人休•卡普(Hugh Karp)曾担任英国慕尼黑再保险公司(Munich Re)的首席财务官

Nexus Mutual在英国注册为互助银行。与遵循股东模式的公司不同，互助银行由其成员管理，只有成员才能与该互助银行进行业务往来。它类似于一个由成员单独经营的公司。

Armor Protocol

通过加密本地、动态智能保险聚合，Armor使投资DeFi尽可能安全。作为一个去中心化的智能合约经纪公司，Armor的创新为用户资产提供按需、实时覆盖和非托管安全解决方案。

Armor Protocol有四个主要产品:arNXM, arNFT, arCORE和arSHIELD。

arNXM

Nexus Mutual创建了Wrapped NXM (wNXM)，允许投资者在不做KYC的情况下运用NXM。然而，随着创建更多的wNXM，更少的NXM可以用于互助的内部功能，如权益、索赔评估和治理投票。

Armor创造了arNXM来解决这个问题，允许投资者参与Nexus Mutual的运营，而不做KYC。为了得到arNXM，用户可以在Armor中抵押wNXM。Armor打开wNXM, NXM token随后被押注在Nexus Mutual上。通过抵押Nexus Mutual，投资者发出了智能合约是安全的信号，从而开辟了更多可供出售的保险。

arNXM也可以被称为wNXM保险库。将wNXM存入保险库的用户将来可以收到更高数量的wNXM。

arNFT

arNFT是在Nexus Mutual上购买的代币保险形式。arNFTs允许用户购买保险，而不必做KYC。由于这些保险是通证化的，用户现在可以将其转让给其他用户或在二级市场上出售。这些标记化的保险还允许进一步的定义可组合性。

arNFTs可以为所有Nexus Mutual的保险铸造。

arCORE

arCORE是一种现收现付的保险产品。通过使用流支付系统，Armor能够实时追踪用户在不同协议和收费中动态移动的资金数量。基础arCORE是分解并溢价出售的集合arnft。arCORE允许更多创新的产品设计，并展示了DeFi生态系统的可组合性。

arCORE的产品收取更高的溢价，以补偿arNFT的股东，因为他们承担了没有完全卖光保险的风险。到2021年4月，乘数是161.8%，这意味着价格将提高61.8%，而不是直接从Nexus Mutual购买。

对于额外的保费，90%返还给arNFT股东，10%由Armor收取作为管理费。在1.618的溢价乘数和收入的90%的比例下，利用率必须大于69%，才能让arNFT的股东盈利。如果售出的保险少于持有保险池股份的69%，那么这些股东将不得不自己承担保险的成本。

arSHIELD

arSHIELD是流动性提供者(LP)代币的保险存储库，保费会自动从赚取的LP费用中扣除。arSHIELD本质上创建了有保险的LP代币，用户无需支付预付款。

arSHIELD只涵盖流动性池的协议风险。例如，投保的Uniswap LP代币只覆盖了Uniswap智能合约被攻破的风险，但不包括基础资产被黑客攻击的风险。

因此，arSHIELD只是一个重新打包的arCore版本。

索赔

在用户提出索赔后，将触发审查过程并提交到Nexus Mutual进行审核。Armor代币持有者还将参与Nexus Mutual的索赔批准和支付流程。如果支付被确认，金额将被发送到Armor的支付金库，然后分配给受影响的用户。

协议收入

Armor的重点是建立一个互操作协议的生态系统，以确保机构和个人能够大规模采用DeFi。

以下是截至2021年2月更新的利润分享费用表:

产品	Stakers的股票	库存股票
arNXM	90%	10%
arCore	90%	10%
arNFT	0%	100%

来源:https://armorfi.gitbook.io/armor/products/arcore/model-constants

需要注意的是，从Nexus Mutual购买的每一个保单都有10%的保费用于索赔目的。由于理赔费用为保费的5%，所以同一保单每个用户可以理赔两次。如果在保单期结束时没有索赔，10%的保险费将被退还。这是arNFT的利润来源。

Cover Protocol

Cover Protocol由Yearn Finance孵化，最初是提yInsure的安全协议。但由于创始人艾伦(Alan)和著名社区成员阿齐姆·艾哈迈德(Azeem Ahmed)之间的一些内讧，这个项目被取消了。阿齐姆接管了yInsure产品并发布了Armor Protocol，而艾伦则继续发布了Cover Protocol。

Yearn Finance后来宣布与Cover Protocol合并，而Cover Protocol为其所有的yvault提供保险。然而，Yearn Finance于2021年3月5日终止了合作关系

保险的类型

保险协议只提供智能合约的承保。

让我们来看看保险是如何销售的。做市商可以存入1个DAI，他们将能够铸造一个NOCLAIM代币和一个CLAIM代币。这两个token只代表单一协议的风险。Token仅在固定的时间框架下有效，例如半年。

半年后可能会出现两种情况:

- 如果没有有效的索赔事件，*NOCLAIM*令牌持有者可以索赔*1*个*DAI*，而*claim*令牌将归零。
- 如果有一个有效的索赔事件，索赔令牌持有者可以索赔*1*个*DAI*，而*NOCLAIM*令牌将归零。

这类似于一个预测市场，用户可以打赌协议是否会在固定的时间框架内被黑客攻击。

保险协议引入了部分索赔机制，因此在出现有效索赔事件时，索赔代币持有者的支付将由索赔有效期委员会(CVC)决定。

支付购买

用户只需进行一笔以太坊交易，就可以从cover Protocol的网页购买保险，无需注册或进行任何KYC流程。

索赔评估

用户申请索赔有两种选择:

常规索赔:常规索赔费用为10个DAI。COVER代币持有者将首先对索赔的有效性进行投票。验证后，将交由索赔有效性委员会(CVC)做出最终决定。

强制索赔:一次强制索赔需要500 DAI。索赔被直接发送给CVC，由CVC决定。

CVC由外部智能合约审计员组成。如果索赔被批准，保险协议将退还索赔申请费。

风险评估

当用户购买保险时，利用闪贷来降低gas成本和减少用户需要的步骤。在此过程中，CLAIM和NOCLAIM token使用借来的DAI铸造。NOCLAIM代币然后被卖给DAI的平衡器池。

再加上用户支付的保费，DAI随后被用于偿还闪电贷款，用户将只收到CLAIM代币。当用户将CLAIM令牌卖回Cover Protocol时，将发生相反的情况。

在这个系统下有一些好处:

- 由于只有一个平衡器池来进行流动挖矿项目，预计支付成本将会降低。有了正确的激励，做市商将购买更多的*NOCLAIM*代币，以产生农场或赚取交易费用，从而推高*NOCLAIM*代币的价格。因此，当*CLAIM = 1 – NOCLAIM*时，*CLAIM*令牌的价格将会降低。

- 做市商预计将赚取更多的费用，因为每一次购买保险都涉及向平衡器池出售*NOCLAIM*代币。

不像在之前的体系中，做市商只为一个池子而不是两个池子提供流动性。

- *Cover Protocol*预计将获得更高的平台收入，因为每次购买都涉及*CLAIM/NOCLAIM*代币铸造，在赎回期间收取*0.1%*的费用。

保单价格是由供需平衡池决定的。

协议收入

索赔和无索赔代币赎回将收取0.1%费用。COVER代币持有者有权投票决定如何使用金库。截至2021年4月，保单代币赚取股息的担保正在讨论中，但细节尚未最终确定。

Nexus Mutual和Cover协议的比较

	Nexus Mutual	*Cover*
代币模型	相互	股东
产品	保险	预测市场
风险汇聚	是的	没有
资本效率	高	低
交易对手覆盖	*72*	*33*
索赔	投票的成员	通过审计
KYC	不需要(甲)	不是必需的
损失的证明	要求	不是必需的
损失覆盖	完整的	部分
总锁仓值	*4.5*亿美元	*700*万美元

截至2021年4月，Nexus Mutual在保险市场遥遥领先，似乎没有竞争对手。但由于DeFi的保险普及率非常低，竞争对手还有很大的追赶空间，

在一个每天都有创新涌现的领域，保险行业领袖的头衔总是唾手可得。

资本效率

Nexus Mutual允许资金提供者对所持资金拥有15倍的杠杆率。这意味着投资者将获得更高的保费收入。资金提供者确实必须承担更多的风险，但这种方法与传统保险提供者将风险分散到具有不同风险特征的多个不同产品上的方式是一致的。

与此同时，由于每个池都是孤立的，保险协议的资本提供者无法杠杆化他们的资本。因此，由于资金效率较低，Cover Protocol的Cover比Nexus Mutual的Cover更贵。例如，在cover Protocol上购买Origin Dollar的保险每年需要花费12.91%，而在Nexus Mutual上只需要2.6%。有计划将不同的风险捆绑在覆盖协议V2中，但未有详细细节。

我们可以通过活跃担保额除以资金池总额，来定量地计算出资金效率。Nexus Mutual的资本效率比率高达200%，而Cover Protocol在设计上总是低于100%。

Cover Protocol只覆盖22个协议，而Nexus Mutual覆盖72个对手方。Nexus Mutual在保险条款上提供了更大的灵活性，用户可以决定在任何一天开始保险，并有一个直到一年的保险期限。

承保协议只提供截止日期已事先确定的定期保险。例如，对于一个特定的系列，保险期限截止到五月底。不管用户何时购买保险，保单将在5月份结束。因此，随着时间的推移，CLAIM代币将趋近于$0，而NOCLAIM代币将趋近于$1。

用户可以从Nexus Mutual找到更全面的产品，因为它覆盖了大多数主要的DeFi协议。即便如此，由于缺乏赞助者,许多保险已经售罄。Armor Protocol通过吸引更多的wNXM到arNXM来帮助缓解这个问题,因此有更多的保单。

Cover Protocol可以在长尾保险上竞争，项目可以更快地列出，而且不必进行繁琐的风险评估。这是因为每个风险都被隔离并包含在单个池中，这与NXM不同，在NXM中，来自任何单个协议索赔都可能占用资金池。然而，引荐不太知名的项目的保单并不是一件容易的任务。除了受限于有限的能力，保险成本往往过于昂贵。

索赔率

Yearn Finance在2021年2月遭受了1100万美元的黑客攻击。尽管Yearn Finance决定通过他们的基金来弥补损失，但保险协议已经决定支付索赔，以展示他们的产品确实能正常工作。

Nexus Mutual已接受14项索赔，总计索赔支付2410499美元(1351 ETH和129660 DAI)。如果索赔人能证明他们确实损失了至少20%的资金，损失就会得到全额赔偿。

与此同时，由于保险库的损失仅为36%，Cover Protocol决定只支付36%的赔偿率。如果用户持有1000个CLAIM代币，他们只能收到360美元。因为只有价值40.9万美元的索偿代币可用于Yearn Finance，做市商仅损失了14.7240美元。

保险购买者应意识到，保险协议购买并不能保证在发生损失时获得全额赔偿。决定索赔赔付的方式更类似于预测市场。

相关的风险

赔付在很大程度上依赖于保险公司和购买者之间的协议。对协议的解释总是有细微的差别，特别是在涉及大额索赔的高风险场景中。

每一份保险协议都有其决定支付金额的方式，这对所有的买家未必是公平的。买方应了解保险产品目前的限制。

作为保险协议的资金提供者也会面临复杂的事项，用户在决定参与之前应该对风险有全面的了解。如果索赔的可能性高于预期，股东可能会遭受损失。

其他代表

Unslashed Finance

截至2021年4月，unslash Finance处于私人测试模式。unslash Finance为资本提供者提供了桶式风险汇资金池。第一个产品名为Spartan Bucket，涵盖24种不同的风险，涵盖对手方，如托管方、钱包、交易所、智能合约、验证器和预言机。

Lido Finance从unslash Finance购买了价值2亿美元的担保，用于其ETH 2.0担保，以弥补大幅削减罚款的风险。大幅削减是指当权益证明(PoS)网络的验证者不能一致地维护网络时，对其施加的惩罚。

Nsure Network

Nsure Network于2020年9月从Mechanism Capital、Caballeros Capital、3Commas、AU21、Signal Ventures和Genblock筹集了140万美元的种子基金。

Nsure Network是一个交易风险的市场。它依靠对NSURE代币的质押来评估协议的风险，并使用它来为保险定价。截至2021年4月，他们正在以太坊的Kovan测试网中运行一个承销项目，以评估定价在主网中的工作方式。参与者将获得NSURE代币作为奖励。

InsurAce

InsurAce已经从风险投资机构如Alameda Research、DeFiance Capital、ParaFi Capital、Maple Leaf Capital、Wang Qiao和Kerman Kohli筹集了300万至500万美元。它的目标是成为第一个基于投资组合的保险协议，提供投资和保险产品以提高资本效率。

有了InsurAce，如果用户在进行流动性挖矿时使用不同的协议，他们就不必购买多个保险，因为它提供了一个基于投资组合的覆盖上述投资策略中涉及的所有协议的保险。它还声称采用一种基于精算的定价模型，而不是依靠质押来为保险定价。

截至2021年4月，InsurAce尚未宣布其上市日期。由于缺乏索赔历史，InsurAce基于组合的保险协议和定价模型是否适用于DeFi领域还有待观察。

一些衍生协议也提供有趣的保险产品，如:

- Hakka Finance的3F互助-承保DAI脱钩风险。
- Opium Finance——覆盖USDT脱钩风险。

到目前为止，衍生协议所提供的这些保险产品的采用情况并不乐观。

与其他去中心化交易和借贷协议不同，保险协议似乎没有得到太多关注,购买保险的意识在加密领域并不普遍。我们可能会看到更多的用户开始使用保险，更多的保险协议计划在2021年及以后推出。

结论

保险市场仍未得到充分开发。根据Nexus Mutual的活跃保单量，只有约2%的DeFi的锁定总价值被承保。信用违约互换(cds)和期权等衍生品可能会削弱购买保险的必要性。

高风险承担者和零售用户主宰了当前的DeFi市场;他们可能不太强调风险管理，因此不考虑保险的必要性。

随着加密货币领域的成熟和机构资本的介入，保险市场将获得更大的吸引力。

Nexus Mutual的基础业务运作良好，活跃保险金额从2021年1月的6800万美元增长了10倍，到2021年2月达到7.3亿美元。

Armor Protocol的推出对Nexus Mutual是一个巨大的利好，巩固了Nexus Mutual在DeFi保险市场的领先地位。作为wNXM保险库，arNXM旨在取代wNXM。它吸引了如此多的wNXM，现在arNXM贡献了总NXM股份的47%。这有助于打开更多的保险市场。同时，arnts贡献了约70%的活跃覆保险。

Cover Protocol信用违约互换等新产品创新迅速，但业务增长缓慢。保险协议提供的产品较少，保险条款的灵活性也较低。但它允许项目更快地上市，并可以用相对较少的资金提供承保。

推荐阅读

1. Why DeFi insurance needs an Ethereum native claims arbitrator
https://blog.kleros.io/why-defi-insurance-needs-an-ethereum-native-claims-arbitrator/
2. Why insurance is needed for DeFi and what it looks like
https://cryptoslate.com/why-insurance-is-needed-for-defi-and-what-it-looks-like/
3. Nexus Mutual is the most undervalued token in digital assets
https://twitter.com/jdorman81/status/1376920737949184002?s=20

第三部分：DeFi种类的聚集

第九章：去中心化指数

在不持续监控个别货币表现的情况下，在您的投资组合中获得加密货币敞口的一种方法就是投资被动管理的投资组合，例如去中心化指数。去中心化指数的工作方式类似于传统金融市场中的交易所交易基金（ETF)。

ETF 是一种结构化证券，它可以跟踪任何（包括但不限于）指数（例如 S&P500）、商品（例如稀有金属）等资产。它可以在证券交易所购买或出售。

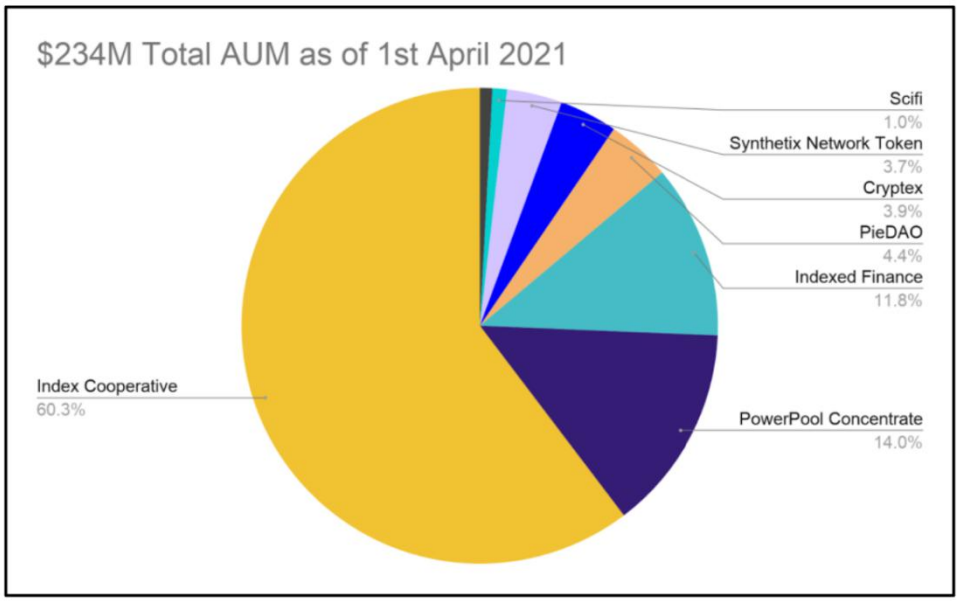
纵观历史，相比较使用主动管理策略的共同基金（Mutual Funds），ETF 给予的回报率会更高。2020 年，全球 ETF 的资产管理规模 （AUM）约为 7.74 万亿美元，交易量达到全球股票交易量的三分之一。

截至 2021 年 4 月 1 日，去中心化指数行业增长迅速，链上 ETF 资产管理规模以极快的速度增长至 2.34 亿美元。不难想象未来几年内这一数字达到数万亿美元。

在本章节中，我们将专注于研究去中心化指数，您可以在其中分散投资组合，而无需花费太多时间和精力来研究、管理和分配您的投资。

指数协议是指资产管理公司，而指数代币是指指数的产品（相当于 ETF）。这些指数代币代表您在指数基金中的份额，并使您有权从相关资产的资本增值中获得利润。此外，还有一些协议的治理代币，赋予您决定指数协议方向的投票权。

首先，我们来看看去中心化指数的市场格局概览：



来源：CoinGecko

DeFi ETF 概览

截至 2021 年 4 月 1 日，合作指数拥有最大的市场份额，是去中心化指数资产管理总额的 60%。紧随其后的是 PowerPool（14%）和 Indexed Finance（12%）。

尽管市场上有 20 多个 DeFi 指数代币，但去中心化指数市场实际上没有看起来这么拥挤和充满竞争力。去中心化指数 AUM 仅占 DeFi 总锁仓量的 0.3%。

让我们来看看前三大的指数协议 — Index Cooperative、PowerPool 集中投票权（Concentrated Voting Power），和 Indexed Finance。

Index Cooperative (INDEX)

Index Cooperative，也被称为 Index Coop ，是一个最有历史的去中心化指数协议。它由 Set Labs Inc. 创立，同时也是构建并推出 Set Protocol 的公司。

Index Coop 使用户能够广泛接触整个加密货币行业内各个主题的各种协议。指数代币持有者可以拥有、并可以直接赎回构成此指数的基础资产。

Index Coop 与各个方法学家合作 — 会有特定的数据提供者负责指数产品发布策略。

直到 2021 年 4 月，Index Coop 下有五个可用的指数:

- DeFiPulse Index (DPI)
- CoinShares Crypto Gold Index (CGI)
- ETH 2x Flexible Leverage Index (ETH2X-FLI)
- BTC 2x Flexible Leverage Index (BTC2X-FLI)
- Metaverse Index Token (MVI)

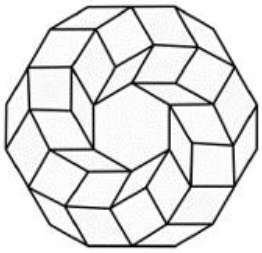
Indexed Finance (NDX)

Indexed Finance 是一种专注于投资组合管理的协议。用户可以铸造、交换或销毁指数代币或是基础资产，并且由 Balancer 分叉出的集成自动做市商 (AMM) 机制会自动重新平衡其指数。Indexed Finance 有由五名团队成员组成，其中一名成员以匿名身份活动。

直至 2021 年 4 月，Indexed Finance 下有七个可用指数:

- DEGEN Index (DEGEN)
- Cryptocurrency Top 10 Tokens Index (CC10)
- Oracle Top 5 Index (ORCL5)
- DEFI Top 5 Tokens Index (DEFI5)
- NFT Platform Index (NFTP)
- 484 Fund (ERROR)
- Future Of Finance Fund (FFF)

PowerPool集中投票权（CVP）



PowerPool

PowerPool的指数带有附加功能，来源于Balancer的自动做市商（AMM）智能池。其主要目的是将治理代币集中在一起，去用于借贷或是用于执行元治理。此外，用户可以直接将一个治理代币交换至另一种。PowerPool正在被一个匿名的团队运营。

目前，PowerPool有四种指数：

- Power Index Pool Token (PIPT)
- Yearn Ecosystem Token Index (YETI)
- ASSY Index (ASSY)
- Yearn Lazy Ape (YLA)

指数协议对比

作为一个协议投资者，这三个基础指标是必不可少的：

1.协议费用
2.协议策略
3.资金权重

协议费用收取

Index Projects	Index Cooperative (INDEX)			Indexed Finance (NDX)						PowerPool Concentrated Voting Power (CVP)			
Index Funds	DPI	CGI	FLI	DEFI5	CC10	DEGEN	ORCL5	NFTP	FFF	PIPT	ASSY	YETI	YLA
Entry fee (mint)	-	-	0.10%	-	-		-	-	-	0.10%	0.10%	0.10%	0.10%
Swap fee*	-	-	-	2.00%	2.00%	2.00%	2.00%	2.00%	2.00%	0.20%	0.20%	0.20%	0.20%
Asset Manager Treasury	-	-	-	-	-	-	-	-	-	0.10%	0.10%	0.10%	0.10%
LP return	-	-	-	2.00%	2.00%	2.00%	2.00%	2.00%	2.00%	0.10%	0.10%	0.10%	0.10%
Management Fee**	0.95%	0.60%	1.95%	-	-	-	-	-	-	-	-	-	-
Asset Manager Treasury	0.65%	0.24%	1.17%	-	-	-	-	-	-	-	-	-	-
Methodologist	0.30%	0.36%	0.78%	-	-	-	-	-	-	-	-	-	-
Exit fees (Burn/Redeem)	-	-	0.10%	0.50%	0.50%	0.50%	0.50%	0.50%	0.50%	0.10%	0.10%	0.10%	0.10%

Source: CoinGecko, Index Cooperation, Indexed Finance, Powerpool, Tokensets. Taken as at 1st April 2021

* When the user swap one of the underlying assets from one to another.

** Annualized

Index Cooperative

每个指数的管理费用由 Index Coop 和相关的方法学家分摊。费用如下 - DPI：0.95%，CGI：0.60%，FLI：1.95%。 DPI 和 CGI 不会产生退出费用，只有 FLI 的退出费用为 0.1%。

Indexed Finance

为了覆盖无常损失，当您将其组成资产铸造或销毁指数代币时，将会被收取 2%的兑换费，并以任何兑换时代币输入的形式分配给流动性池子（LP）持有者。如果您利用的是所有的基础资产进行铸造，或者赎回的是所有的基础资产，那么这 2%的费用将不会被收取。

但是，在销毁任何指数代币时，您将被收取 0.5%的固定费用。该费用会分配回给已质押过原生 NDX 治理代币的协议用户。

PowerPool 集中投票权（Concentrated Voting Power ）

费用分为三种：入场费、兑换费和退场费。如果要铸造一个指数代币，您将被收取 0.1%的入场费。0.2%的兑换费用适用于将一种治理代币交换为另一种的用户。兑换费之后会在指数基金流动性提供者和财政部之间平均分配。如果您退出指数，则需要再额外支付 0.1%的费用。

从上面的费用比较来看，Index Coop 将获得最高的收入，因为收取的费用最高。Indexed Finance 只有一种经济收入来源，那就是 0.5%的退场费。与此同时，Powerpool 可以从铸造、交换和退出费用中，从不同的来源获得更加多的收入。

作为基金投资者，您很可能是一位长期的持有者，因此费用很重要。

在这种情况下，相对于 DPI 和 DEFI5，索引代币 PIPT 将是最便宜的选择。使用 PIPT 和 DEFI5，没有持续成本，不像 DPI 每年 0.95%。

协议策略

我们去了解每个协议的策略，以了解他们对其去中心化指数产品的愿景和方向是非常重要的。

Index Cooperation

以下是团队如何在自己的协议中加入产品的总结:

1. 提出新的产品创意，并与社区成员进行讨论
2.在治理论坛向社区提交产品申请
3.开始第一次快速投票并进行审查
4. 通过的提案由 Index Coop 团队审核
5. 发布第二次投票
6. 产品发布

Index Coop 一直有一个严格的流程，需要两个阶段的社区投票才能获得产品批准。例如，自第一次投票后，推出灵活杠杆指数 (FLI) 还再需要至少三个月的时间。

Indexed Finance

对比 Index Coop，Indexed Finance 进度会更快。

例如，ORCL5，作为第一只进入投票阶段的指数基金，从投票阶段开始到发布总共只用了 18 天。

PowerPool 集中投票权（Concentrated Voting Power ）

Powerpool 最新的指数产品就是 Yearn Lazy Ape，于 2021 年 1 月 17 日开始进行治理投票。它仅在几乎三个月后就于 2021 年 3 月 3 日推出。

目前，Index Coop 和 Powerpool 旗下有四个指数产品。 Indexed Finance 有七个指数。

尽管 Indexed Finance 似乎是推出指数最快的一种，但 Index Coop 和 PowerPool 团队与他们的方法学家合作，以确保他们的产品安全并考虑所有相关因素和风险。

随着 Sigma 计划的推出，Indexed Finance 可能会开始放缓步伐。 Sigma 计划允许 Indexed Finance 与外部合作伙伴合作，这需要更长的时间。例如，与 Redphonecrypto 合作的 DEGEN 指数基金于 2020 年 12 月下旬宣布，仅在三个月后上线。

基金权重

Metrics	Index Cooperative (INDEX)		Index Finance (NDX)				PowerPool Concentrated Voting Power (CVP)			
	DPI	CGI	DEFI5	CC10	ORCL5	DEGEN	PIPT	ASSY	YETI	YLA
Fund Weighting	Market Cap-Weighted	A bi-level approach, accounting historical volatility	Sqrt of Market Cap-weighted	Sqrt of Market Cap-weighted	Sqrt of Market Cap-weighted	Sqrt of Market Cap-weighted	Equal-weighted Market Cap	Market Cap-weighted	Market Cap-Weighted	Adaptive weights proportional to vaults TVL

基本上来说，去中心化治理代币的主要权重方式有三种:

1. 市值加权(如 DPI)

这种方法动态跟踪每种资产的市值，每种资产的配置与它们相对于指数中其他资产的市值成正比。

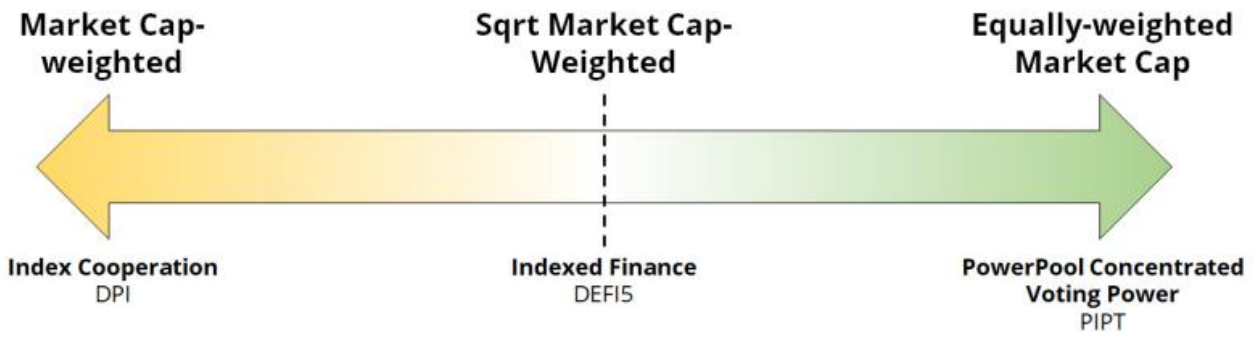
使用这种方法的指数将集中于市值较大的货币,使该指数能够密切模仿实际市场表现。

2. 市值加权的平方根(例如，DeFi5)

指数化金融的所有指数都是基于相对于每项标的资产的市值的平方根。这种方法抑制了市场表现对更大市值币的影响。

3. 加权等权重市值加权(如 PIPT)

这种方法对资产分配进行了平等的设定。例如，PIPT 有 8 个基础资产。因此，每种资产的权重都设置为 12.5%。同等权重的策略受价格动量的驱动，将青睐市值较小的硬币。市值较小的币被赋予与市值较大的币同样的重要性。



相关风险

以下是投资 DeFi 指数协议和基金的三大风险：

1.代码即法律
尽管前 3 个指数协议每一个都经过审计，但投资者需要记住，被审计的协议不是防黑客的。

即使进行了审计，可是加密领域仍发生了大量黑客攻击事件，资金往往是无法恢复的。

2.唯利是图的资本
大多数指数协议都有流动性挖矿项目来激励流动性提供者和引导指数代币的流动性。

然而，这些资本中的大部分通常被称为“唯利是图的资本”。这些资本纯粹是在寻求高回报，一旦出现另一个更高收益的协议，它们就会退出。因此，一旦流动性挖掘回报枯竭，它可能导致大规模取款，导致指数协议的螺旋式下降。

3.系统风险
在 DeFi 中，协议可以像金钱乐高一样堆叠在彼此之上。然而，DeFi 的组合性可能是一把双刃剑，因为它会带来系统性风险。例如，PowerPool 公司的 Yearn Lazy APE (YLA)在其 5 个稳定币库中有 10 种不同的风险敞口。

1. yvCurve-Compound(8.6%) 2. yvCurve-3pool (36%) 3. yCurve-GUSD (17.3%)	4. yUSD(27%) 5. yvCurve-BUSD

这些资产与十种不同的协议相互作用，因此有十种不同的风险。Yearn的稳定币库涉及的十个协议是：

1. Yearn 2. Curve 3. Compound(cDai & cUSD) 4. Maker(DAI) 5. Tether(USDT)	6. Circle(USDC) 7. Gemini(GUSD) 8. Binance(BUSD) 9. TrustToken(TUSD) 10. PowerPool(YLA)

值得注意的事项


BasketDAO-Interest Bearing DPI(BDPI)

BDPI是BasketDAO团队的产品，是DPI的生息版。不同之处在于，标的资产被贷给Aave和Compound等贷款协议，以获得收益。因此，持有该指数基金的收益预计将高于DPI。


Cryptex Finance - Total Crypto Market Cap (TCAP)

由Cryptex Finance创建的TCAP允许你接触整个加密市场。该团队还运营着Prysmatic Labs，这是ETH 2.0的研究团队之一。

结论

我们在去中心化指数领域仍处于非常早期的阶段，我们预计这一领域将在未来几个月或者几年迅速增长。对于长期投资者来说，我们强烈建议您查看基金以往的表现，检查每一笔收费认真考虑所使用的基金策略。你也可以根据风险偏好来选择基金，要全面了解你希望投资的资产类别。

第十章:分散预测市场

预测市场是指参与者对未来事件的结果下注的市场。一个很好的传统的预测市场例子就是我们熟知的体育博彩平台。

去中心化的预测市场利用区块链技术来做其他事物的预测市场。例如，可以预测比特币价格何时会超过 10 万美元或谁是下一任美国总统。

去中心化预测市场的支持者认为，中心化平台会让用户处于不利地位。比如高额交易费用、延迟提款和冻结账户。此外，目前大多数传统投注平台都专注于体育投注，限制了公众可获得的预测市场类型。

建立去中心化的预测市场协议目的是使用户能够创建自己的市场。

预测协议如何工作?

与传统的预测市场不同，预测协议是去中心化的的，必须依靠创新方法才能发挥作用。我们可以粗略地把预测协议流程图分成两个主要部分:

1. Market-Making
2. Resolution

Market-Making

在做市预测协议中，在基本类型市场中有两种类型的股票(结果令牌):YES(长线)股票和 NO(短线)股票。根据行情决定投资方向。

在一个简单的预测市场中，一股 YES 股票(通常以 1 美元计价)在相关事件发生时支付 1 美元，在相关事件没有发生时支付 0 美元。如果事件没有发生，每个 NO 股份支付 1 美元，如果事件发生，支付 0 美元。分类市场利用了这一基本原理，例如，到 2021 年 12 月 31 日比特币会超过 10 万美元吗?

另一个问题是:谁将成为 2025 年的美国总统?在这种情况下，可能有两个以上的选项，例如:

A. Joe Biden
B. Kamala Harris
C. Trump

上述功能类似于一个基础类别类型的市场，除了包含了三个股票来代表三个不同的答案，而不是两个。股票的价格是基于买者愿意支付多少和卖者愿意接受多少。换句话说，该系统是一个自治的赌盘，其利率(即价格)由市场对概率的权衡决定。

另一方面，拥有一系列答案和相关回报的市场将会以不同的方式运作。这被称为标量市场，结果在定义的参数内变化。

设想标量市场的一个好方法是，将其看作是拥有决定谁是最正确/错误的结果，而不是确定谁是绝对正确/错误的结果。

让我们在这里使用一个带有以下假设的例子:

“到 2021 年 11 月 10 日，比特币的价格会是多少?”

精度= $10k
范围= $0 - $200k
通过这种设置，用户可以选择 1 万美元、2 万美元、3 万美元等等。

与 YES/NO 和“多项选择”市场不同，标量市场的收益是分配给所有参与者的。每笔支出都是基于相对于结果的价格在该范围内的下跌情况。所以如果在交易截止日期，比特币的价格是 19.8 万美元，那么比特币将在所有买家之间分配。然而，最接近 20 万美元执行价格的答案将获得与押注规模成比例的最高回报。

对于标量市场，每股价格转化为标的资产的特定执行价格或任何预期价格。

决议

使用与之前相同的例子，如何确定比特币是否在 2021 年 12 月 31 日超过 10 万美元?我是参考 Coinbase，还是参考 CoinGecko 上所有交易所的总价格?在实践中，做市商会在清算源创建之前指定。因此，在这种情况下，可以将 Coinbase 作为解析源。

真正的问题是谁提供这些信息，以及如何验证这些信息?对基于价格的市场，公共 api 可以从在线资源中提取。oracle 也可以使用，但可能不能覆盖所有的市场类型，例如“Vitalik Buterin 会在 2022 年前结婚吗?”

考虑到预测市场的规模和范围，单纯依靠技术是不可能的。预测协议意识到这个问题：依靠人类来确保信息是最准确的。

然而，如何确保不良行为者不会通过提供虚假信息来操纵市场?与传统的预测市场不同，预测协议是分散的，没有资源来监测和规范每个市场。为了解决这个问题，预测协议提出了不同的解决方案。下面介绍两个例子：

预测市场的协议

Augur

Augur 在以太坊网络上运营，并使用一种决议模型，鼓励用户通过奖励和惩罚准确报告信息。在市场关闭后，它将进入一个报告期，在此期间，市场建立者或其他人(取决于市场创造者指定谁为指定报告者)可提供信息以验证结果。

在报告期间，指定报告人(DR)将有 24 小时提交一份市场结果报告。问题是 DR 在报告他们的发现之前必须先将协议的本地令牌押注。

本机令牌有两个版本:REP 和 REPv2。REPv2 令牌只适用于 Augur v2 协议更新，而 REP 是可迁移和可赎回的 REPv2 令牌。

关键的区别是，代表持有人可能不会参与分叉，如果有实质性的争议的结果。但是，为了简单起见，我们将它们统称为 REP 标记，因为它们在功能上是相似的。

DR 选择的任何一个结果都成为暂定获胜结果(TOR)。一旦 DR 提交 TOR，就可以公开辩论。有争议的结果将开启为期一周的争议期，任何有 REP 的人都可以赌上他们认为正确的答案。一轮持续一周，但最多可达 16 轮。

如果没有争议，部分奖金将用于补偿 dr。该费率是可变的，并根据流通中的所有 REP 代币总总价值确定。

如果出现争议，赌赢结果的用户将获得赌输结果的 REP 份额。这是在记者将收到的酬金之上的。赌输结果的用户将不会收到任何费用，并失去他们所有的 REP 代币。

Omen

Omen 是由 DXdao 开发并由 Gnosis 协议支持的一个预测协议，它在以太坊和 xDai 侧链上运行 Gnosis 允许 Omen 用户使用他们的代币框架，这是一个基于事件的资产类别，包括预测市场的构建模块。

与 Augur 不同，Omen 并不激励社区去报告和解决市场问题。相反，他们依赖于一个被称为“现实.eth”的去中心化的社区，一个为智能合约验证真实世界。

大多数市场将得到解决后通过 Reality.eth 的社区成员将决定基于费用的话题。用户在 Reality.eth 为他们所选择的结果发布债券，他们可能会受到 qitaren 人发布新答案并将债券加倍的挑战。这种情况可能会持续几个周期，直到发行停止，并且答案由最后一个发行债券的人决定。

一旦 Reality.eth 内部决议完成他们的义务,他们将供应结果市场各自的预兆。如果一个 Omen 用户对调查结果不满意，他可以(通过 Reality.eth)向外部仲裁员 Kleros 申诉。

Kleros 从陪审员中随机选择陪审员，并提供基于博弈论的激励，以确保匿名选民达成共识。那些押注于正确结果的人从那些押注于不正确结果的人那里收集信息(很像 Augur)。

值得注意的是，在 Omen 背后的自治组织 DXdao，也可能决定在未来成为一名称职的仲裁者。

Augur 和 Omen 之间的其他关键区别是什么?

正如我们刚才讨论的，Augur 和 Omen 在解决问题的过程中有非常不同的方法。通过建立一个奖惩生态系统来规范报告信息的可靠性，Augur 解决了 oracle 问题。Omen 将他们的报告需求外包给外部 DAO(使用与 Augur 方法类似的原则)。从这个意义上说，Augur 更加自给自足。

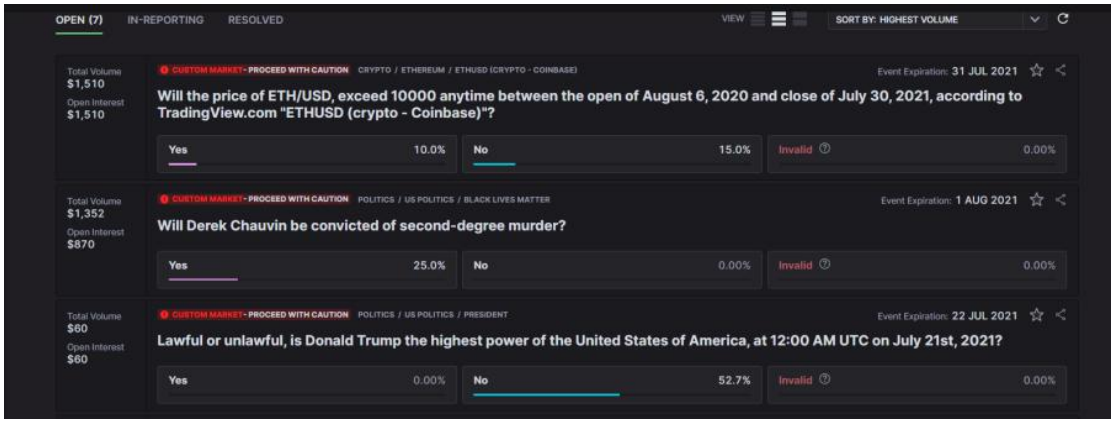
在流动性方面，Augur v2 上的市场使用 0x 的链下订单账本——订单在链下收集，链上结算。相比之下，Omen 的自动造市商的操作类似于 Uniswap 等 DEXs，为代币对创建了大型流动性池。

尽管这两个结果令牌都使用 ERC-1155 标准，但 Omen 的令牌可能被包装在 ERC-20 标准中，并在其网络之外访问-这允许 Omen 访问 DEXs 并利用更大的流动性池。另一方面，Augur 的结果令牌被限制在其协议的内部流动性池。

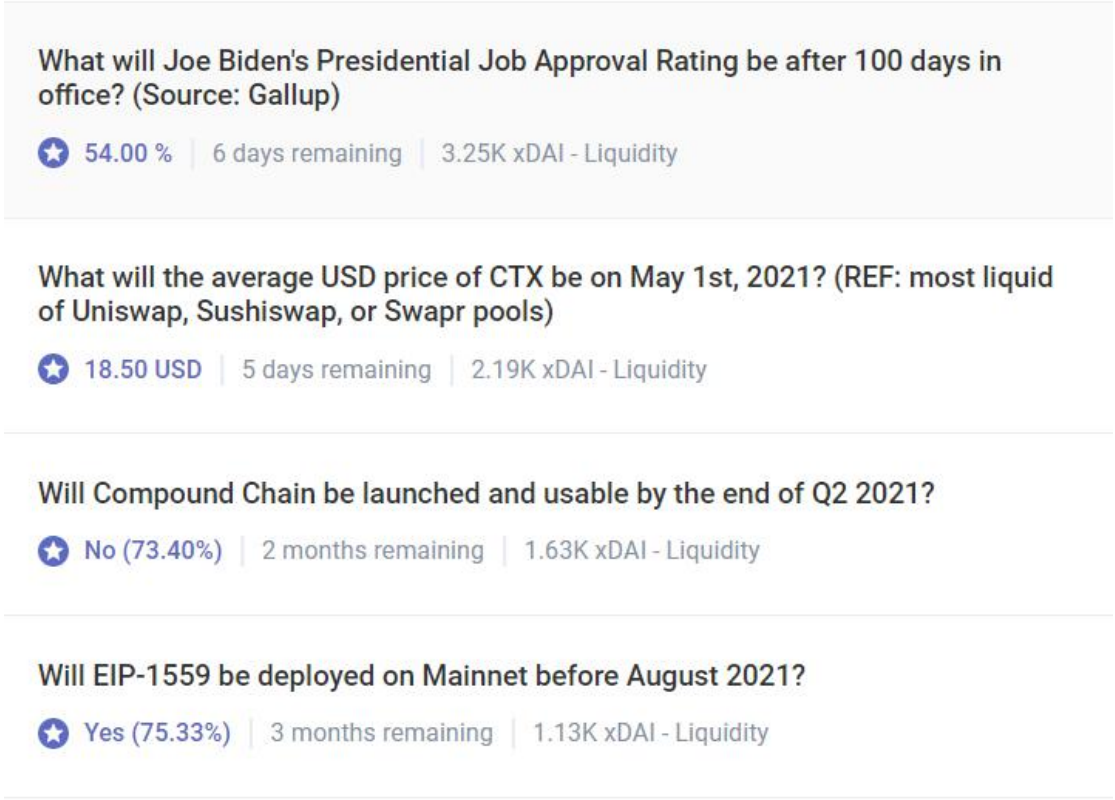
关于 Augur 和 Omen 的简要比较，可以参照下表:

	Augur	Omen
Information Validation System	Uses internal rewards and penalties to control	Outsourced to external DAO-type arbitrators
Liquidity	Traditional order book + 0x protocol for decentralized implementation	Automated Market Maker
Governance	Admin key that are burned means there are no further updates	DAO
Tokens	REP (REP + REPv2)	-
Outcome Tokens	ERC-1155	ERC-1155 but may be wrapped into ERC-20 tokens to access liquidity pools from other DEXs
Market Pairs	DAI	30 pairs
Supported Blockchains	Ethereum	Ethereum and xDai

我们无法获取两种协议的市场数据，但全面扫描(2021 年 4 月 28 日进行)两种协议的网站将显示，几乎没有活动。



对于 Augur 来说，目前只开辟了 7 个市场。只有前三家的实际交易额加起来接近 3000 美元。



至于 Omen 市场，目前只有 4 个市场，但总交易量约为 7200 美元(图中没有反映，但在另一个网页上有显示)。

相关的风险

预测市场最大需要担忧的是数据的可靠性。虽然有多种基于利润的动机来尽量减少数据操纵，但非理性行为者可能会试图危及结果。此外，挑战的结果可能会导致耗时和昂贵的情况

值得注意的相关事宜

Polymarket

截至 2021 年 4 月，Polymarket 有一个在以太坊上运行的 beta 产品。该协议的白皮书尚未发布，但它们似乎是集中式和分散式结构的混合体。该方案似乎比“Augur”或“Omen”更受欢迎——我们在 2021 年 4 月 28 日的快速调研显示，市场活动非常活跃，超过 60 个预测市场。仅最受欢迎的市场的交易量就达到了约 200 万美元。

结论

预测市场是一个有趣的领域，因为它的含义超出了赌博——它允许用户对冲风险。传统的衍生品允许买卖双方通过持有未来以特定价格交易特定商品的权利来对冲特定结果。例如，如果一位稻农预计 2021 年 12 月 31 日价格会更低，他可以签订一份衍生合约，以 5000 美元的价格在 2021 年 12 月 31 日出售 1000 公斤大米。

预测市场可以基于任何东西，而不仅仅是大米。种植水稻的农民可能决定不去对冲大米价格，而是去对冲天气风险。换句话说，预测市场允许用户对冲更具体的风险。

预测协议为任何人提供了一个对冲任何风险的平台。不仅如此，预测市场还可以充当事实上的民意调查。预测协议的参与者有效地分享他们对不同问题的观点，这些观点可以推断出对广泛的见解。

预测协议的未来是令人兴奋的，因为它们是现实生活的基础。我们可以想象使用类似的解决系统将法律合同带到链上，因为仲裁方法的功能与基于陪审员的司法系统非常相似。然而，在短期内，我们预计更

多的协议将利用预测协议的力量，利用它们创建创新的对冲工具。

第十一章：去中心化的固定利率协议

如果我们看一下大多数金融消费者所在的传统金融，会发现受全球化导致了稳定金融生态系统的需求增加。事实上，20多年前，欧洲议会就在其题为《利率的决定》的工作文件中首次承认有必要提高价格稳定性：

"世界金融市场的一体化正在增加外部因素决定国内货币政策方面的压力。此外，尽管世界上主要的中央银行在执行货币政策方面的做法在细节上有所不同，但在基本面上却有着广泛的共识：追求价格稳定和金融市场的稳定。"

这里的关键点是整合。类比于加密货币行业的运作方式，该领域已经成熟到一定程度，DeFi 已经成为协议的行业标准。区块链技术通常被称为金融乐高，它允许开发人员与其他协议整合并构建创新的金融产品。但是这样的进展并没有改变加密行业不可预测和高度不稳定的事实。

稳定的利率是每个金融生态系统的一个重要方面。尽管有大量的借贷协议和收益率聚合器向加密行业的贷方提供利率，但其中提供固定利率的相对较少。

随着收益农业的日益普及和对更稳定的借贷利率的需求，一些 DeFi 协议试图满足对稳定利率不断增长的需求，成为可靠性的标志。 这催生了一类新的协议，称为固定利率协议（FIRP)。

与传统金融相比，传统金融的固定利率是以定期存款（或债券）的形式出现的，而FIRP则是 利用其基础的代币组结构，提供不同的激励措施来维持其利率。 在这一点上，FIRP生态系统可以大致分为两类：

1. 借贷 借出/借入
2. 收益聚合器

即使在这种总的分类下，FIRP 也有许多形状和大小。 每个协议都有其“固定”利率的方法，这导致了不同的用例。 有些提供“固定利率”或“固定利息收益率”。 此外，有些 FIRP 根本不提供固定利率，而是创造一个有利于固定利率的环境。

本章中我们将介绍三个示例。

固定利率协议的概述

Yield

Yield 是一个去中心化的借贷系统，它使用一种名为“fyTokens”的新型代币提供固定利率借贷和利率市场。目前的迭代（版本 1）包括用于 DAI 稳定币的 fyTokens。称为“fyDai”，这种新类别的代币可以在 DAI 中实现完全抵押的固定利率借贷。

fyDai 代币是基于以太坊的代币 (ERC20)，可以在预定的到期日之后兑换 DAI。 fyDai 类似于零息或折扣债券。

要铸造或出售 fyDai，借款人必须提供目前与 MakerDao 相同的抵押率（150%）的 ETH 抵押品。贷方购买 fyDai，其价格通常会低于 DAI。贴现值与 1 DAI（到期值）之间的差值代表贷方的贷款利率或借款人的借款利率。

虽然 fyDai 的价值反映了借贷利率，但它也可以作为一种债券工具在市场上单独交易。这是有可能的，因为 fyDai 有几个“系列”，每个系列都有不同的到期日。

该系统与 Maker 紧密结合，互为补充。 Maker 用户可以将他们的 DAI 金库“迁移”到 fyDai 金库，在一段时期内锁定固定利率，到期后转换回 Maker 金库。

利率由市场对 fyDai 的估值决定（每个系列都有自己的到期日）。对于贷方而言，fyDai 的估值越高，一旦到期，赚取的利率就越低。

相反，fyDai 的估值越高，借款人的借款利率就越低，因为它将被出售以购买相应的稳定币（如 DAI）。这意味着，根据购买 fyDai 代币的时间，借款人和贷方都可以决定他们的借款/贷款利率。

例子:

假设借款人存入 1.5 个 ETH 作为抵押，并打算以 10% 的年借款利率借入 900 个 DAI。 一旦执行，借款人将收到价值 900个 DAI 的 1000 fyDai——这将根据协议自动在市场上出售，并且借款人将收到 900 个DAI。 在一年期限结束时，借款人如果想收回抵押品，就必须偿还 990 个DAI。

对于贷方，假设贷方贷出 1000个 Dai。 作为回报，贷方收到 1000 个 fyDai，随着期限的临近，其价值将逐渐累积。 最初， 1 fyDai 的价值是 1个 DAI，但一年后，1 fyDai的价值是 0.909个 DAI。 然后贷方可以用 1000 fyDai 兑换 1100 Dai。 这实际上意味着贷款利率为 10%。

在实际操作中，用户只能选择由 Yield 预先编程好的 fyDai 系列。 这与常规债券工具的运作方式类似，即有不同的债券利率和到期期限。

在 2021 年第一季度，Yield 已经提议与 MakerDao 协议整合，允许MakerDao 成为 Yield 借款人的固定利率 Dai 贷方。 该提案已被 MakerDao 治理部门接受，并正在整合到 MakerDao 协议中。

Yield 还预计将在 2021 年夏季推出其协议的第 2 版。它将包括新的抵押品类型，并允许借贷 Dai 以外的资产，如 USDC 和 Tether。

你知道吗？

2021 年 1 月，一名匿名的个人在银行还清了抵押贷款，现在正在通过 DeFi 协议 Notional Finance 偿还其再融资的住房贷款。 Notional 具有与 Yield 相似的功能，因为它们还通过引入一种称为 fCash 的新型金融原语来使用零息债券系统。

Saffron.Finance

Saffron Finance 是一个去中心化的，为流动性提供者提供收益聚合器的协议，也是是最早利用基于分期系统的协议之一。 该系统是由流动性池中创建的部分，这些流动性池按风险、到期时间或其他可销售的特征进行划分，以适合不同的投资者。

Saffron Finance的 用户可以根据自己的偏好风险偏好选择不同的投资组合。更重要的是，Saffron Finance 生态系统创建了一个内部保险系统，高风险部分的投资者为低风险部分的投资者提供保险。

Saffron Finance 的原生代币 SFI 主要是作为一种实用代币，用于 访问A 档，即高收益部分。然而，SFI 也可以被用来赚取资金池奖励和对协议管理进行投票。

分期付款系统允许人们对收益进行划分，并为不同芙蓉资金池创造不同的收益率。在 Saffron Finance 的案例中，A 档的收益是 AA 档的 10 倍。S 档提供平衡 A 档和 AA 档的浮动利率；它们始终处于完美的平衡状态，以维持 A 档和 AA 档之间十倍的固定利息收益率。

例子

如果 AA档 赚取 100 DAI：

1) A 档将获得 1,000 DAI

2) S 档将以确保 A档获得偿付的利率获得DAI是 AA 档的 10 倍

但是，如果存在平台风险（如黑天鹅事件），则AA 档将先获得他们的存款资产和收益——这是从 A 档的本金和利息收益中提取的。

Horizon Finance

与传统的收益聚合器不同，Horizon 允许用户根据博弈论原理创建自己的市场。博弈论设想了一个只有理性行为者的环境。 在这种假设情况下，买家和卖家将根据现有的信息做出最佳决策。

Horizon 允许用户向流动性池提交抵押品，然后将抵押品借给诸如 Compound 等的借贷协议。 为了向用户提供固定利率，Horizon 邀请用户在每一轮中提交他们对固定利率（充当收益率上限）或浮动利率的密封投标。

每轮之后都会显示出价，从而形成一个投标订单簿。该协议将从最低利率到最高利率对竞价进行排序。然后，贷款协议的可变收益从最低利率出价到最高利率出价进行分配，任何超额收入都会流入浮动池。

一个值得注意的特点是，所有投标都将显示在 Horizon 的网站上。 显示的出价允许用户积极竞争，并确定哪些利率是最受欢迎的。 最重要的是，用户可以自由修改他们的出价，包括切换到浮动利率。 Horizon 本质上是一种兴趣预测协议。

例子

为了说明这一点，假设 X池 的一轮竞价从 2021 年 5 月 1 日持续到 2021 年 5 月 14 日：

5月1日，

- 参与者 A 存入 10万 DAI 并出价，他将获得 20% 的利率。
- 参与者B 存入10万 DAI 并按浮动利率出价。

5月7日，

- 参与者 C 存入 10万DAI 并出价，他将获得 10% 的利率。

此时，参与者 A 重新考虑他的出价，因为参与者 C 提交了一个低得多的出价。 如果 X 赚的太少，他可能什么也得不到。

5月13日，

- 参与者 A 将其出价修改为 5% 的利率。

本轮结束后，假设 池X 中的 30万DAI 成功赚取了 4% 的利率，总共 是461 DAI，因此：

- 参与者 A 履行其出价并获得 192 DAI，收益率为5%。
- 参与者 C 部分完成了他的出价，获得了剩余的 269 DAI，利率为7%。 如果 X池 获得了足够的利息，那么他最初的 10% 出价，如果完全履行，将在两周内产生 383 DAI。
- 参与者B 出价失败，一无所获。

如您所见，这里面涉及到很多心理的游戏！ 此外，利率在技术上不是固定的。 然而，系统会奖励那些可以衡量他们应该从出价中获得多少利息的用户。 如果用户不确定他们可以赚取的金额，这会激励用户遵守一个“安全”的出价。 出价过高或出价浮动利率过高可能会导致收益减少或根本没有收益。 因此，随着时间的推移，“安全”出价实际上成为“事实上的”固定利率。

应该使用哪个 FIRP?

FIRP 不能被归入一个单一的篮子中并进行并列比较。 首先，贷款协议与收益聚合器非常不同。

在研究利率的竞争力等更多以利润为导向的指标之前，我们应该先看看 FIRP 维持“固定利率”的能力，这实际上就是它们的功能。 而如果我们要细分 FIRP 的运作方式，基本上有三个决定性的特征，围绕着他们对固定利率的承诺：

一、他们在做什么样的承诺？

不同的协议做出了不同的承诺。 例如，Saffron Finance 承诺，如果您参与 A级贷款，您将获得比 AA 级贷款 多 10 倍的收益。 Horizon 甚至不会对您能赚多少钱做出任何承诺。 了解承诺的类型，可以让用户能够决定哪种协议能提供他们喜欢的产品。

二、 他们打算如何保持这一承诺？

每种类型的承诺都需要不同的方法。 例如，Saffron Finance为Tranche AA 用户提供保险，在出现赤字的情况下，优先给他们收益。。 了解每个承诺是如何维持的，可以让用户确定哪个协议更可靠。

三、 他们在多大程度上依赖外部代理来维持这一承诺？

开发影响用户行为的协议机制对于所有 FIRP 都是至关重要的。 例如，Yield要求贷款人和借款人的比例相对平均，以维持固定的利率。 识别这些特征允许用户确定协议的承诺是如何暴露给他们直接控制之外的因素的。

如果我们考虑这些标准，就不可能说哪个是最适合您的。最终，它归结为每个人的首选风险偏好、所需的金融工具类型以及对基础协议机制的信念。也许更重要的是，该行业仍处于起步阶段，因为许多协议仍在建立之中——它们尚未证明自己，尤其是在困难的市场条件下，这威胁到它们提供固定利率的能力。

相关的风险

最重要的风险之一是 FIRP 提供固定利率的能力。这些协议大多依赖外部代理或其他用户积极参与协议，以推动市场功能。

如果存在一个不活跃的社区，或用户资料和流动性不成比例（例如，Yield的贷款人多于借款人，或者 Saffron Finance 的 A部分参与者多于 AA部分），则 FIRP 可能无法支持其固定利息率。

值得一提的是

- Notional

Notional 为加密资产的固定利率、固定期限的借贷提供便利。 与收益率协议非常相似，这两种协议都有非常相似的功能，因为 Notional 通过引入一种名为 fCash 的新型金融原始工具，创建了一个零息债券系统。 但是，也有一些关键的区别。 特别是，Notional 拥有一个不同的自动做市商和不同的抵押品选项。

- BarnBridge

BarnBridge 利用分档系统（类似于 Saffron Finance）来实现基于收益率的产品。 然而，BarnBridge 还有另一种产品（SMART Alpha），它通过分档波动性衍生品提供对市场价格的敞口。

- 88mph

88mph 是一个提供固定利率的收益聚合器。 他们能够通过引入浮动利率债券和有助于影响市场行为的独特代币经济学结构来维持利率。

- Pendle

Pendle 是一项即将推出的协议，它允许用户对未来的收益率进行代币化，然后可以以预付现金的形式出售。从 本质上讲，Pendle 会计算出您的预期收益率，有效地锁定您的利率。

总结

FIRP 是一套新的协议，必将成为 DeFi 领域的主力军。 我们强调了三个例子，因为它们具有创新性，并且能够展示DeFi 在与传统固定收益工具结合时的潜力。

在这个领域有许多令人兴奋的发展，提供独特的产品和服务。 我们已经有了结合价格预测和收益率汇总的协议； 想象一下，如果一家银行对定期存款收益率提供有竞争力的投注服务？ 我们甚至还没有讨论将未来收益代币化的协议，这些协议基本上允许任何人创建自己的债券，并将其出售以获得预付现金。

随着该领域的进一步发展，我们预计会有更多的机构对 FIRP 产品产生更多兴趣。 固定收益工具在传统金融中一直是很常见的。 然而，随着总债务水平和通货膨胀的持续上升，以及美元价值持续下跌，FIRP 可能会提供更可靠的收益率。

推荐读物

1. DeFi 中基于批次的借贷报告

https://consensys.net/blog/codefi/how-tranche-lending-will-bring-fixed-interest-rates-to-defi/

2. 固定利率协议亮点

https://messari.io/article/fixed-income-protocols-the-next-wave-of-defi-innovation

3. 为什么固定利率很重要

https://medium.com/notional-finance/why-fixed-rates-matter-1b03991275d6

第十二章：去中心化的收益聚合器

加密催生了收益农业活动，用户可以通过在 DeFi 协议中分配资金来赚取收益。 许多加密本地人已成为产量农民，寻找提供最具吸引力的产量的农场。

由于每天发布的新产量农场数量庞大，没有人能抓住每一个机会。 随着天价的回报，错失新的高产农场的机会成本越来越高。

收益聚合器的诞生是为了满足用户投资策略自动化的需求，让他们省去监控市场的麻烦，以获得最佳收益农场。 下面我们将研究几个去中心化的收益聚合器协议。

收益聚合器协议

Yearn Finance

Yearn Finance 最初是 Andre Cronje 的一个激情项目，旨在自动化借贷平台之间的资本转换，以寻找 DeFi 借贷平台提供的最佳收益。这是必要的，因为大多数 DeFi 借贷平台提供浮动利率而不是固定利率。随着这些协议之间的利率变化，资金会自动在 dYdX、Aave 和 Compound 之间转移。

该服务包括主要的美元稳定币，如 DAI、USDT、USDC 和 TUSD。例如，如果用户将 DAI 存入 Yearn Finance，则用户将收到一个 yDAI 代币作为回报，一个有收益的 DAI 代币。

后来，Yearn Finance 与 Curve Finance 合作发布了一个名为 yUSD 的有收益的美元代币池。 Curve Finance 是一个去中心化交易所，专注于价值大致相似的资产之间的交易，例如美元稳定币。 yUSD 是一个流动性池，包括四个 y 代币：yDAI、yUSDT、yUSDC 和 yTUSD。

持有 yUSD 可以让用户拥有五种收益来源：

1. DAI 的借贷收益率

2、USDT的借贷收益率
3、USDC的借贷收益率
4、TUSD的借贷收益率
5. 向Curve Finance提供流动性赚取的掉期费

因此，yUSD 被宣传为一种优于仅持有基础稳定币的加密美元稳定币。

保险库

Yearn Finance 代币推出后首次推出金库功能，点燃了自动化产量农业的狂潮，被认为是产量农业聚合器类别的发起者。金库将帮助用户获得流动性挖矿奖励，并为基础资产出售协议的原生代币。

保险库通过将天然气成本社会化、自动化产生收益和重新平衡过程以及在机会出现时自动转移资金来使用户受益。用户也不需要精通所涉及的底层协议。因此，金库代表了用户的被动投资策略。它类似于加密对冲基金，其目标是增加用户存入的资产数量。

除了简单的高产农业，Yearn Finance 还整合了各种新颖的策略来帮助增加金库的回报。例如，它可以使用任何资产作为抵押品借入稳定币，并将稳定币回收到稳定币金库中。然后使用任何后续收益来回购资产。

Yearn 版本 2 于 2021 年 1 月 18 日推出。73 版本 2 保险库可以为每个保险库采用多种策略（最多同时使用 20 个策略），这与版本 1 保险库每个保险库仅采用一种策略不同。

策略

作为收益聚合器，Yearn Finance 最大程度地利用了以太坊的可组合特性。 下面，我们将研究 Curve Finance 的流动性挖掘计划如何在 Yearn Finance 的金库战略中发挥作用。

Curve Finance 是一个去中心化的交易所，专注于稳定币对。 它利用了一个相当复杂的治理系统——veCRV 用于衡量治理投票权，用户可以通过锁定其 CRV 代币来获得该投票权。

- 1 个 CRV 锁定 4 年 = 1 个 veCRV
- 1 个 CRV 锁定 3 年 = 0.75 veCRV
- 1 个 CRV 锁定 2 年 = 0.50 veCRV
- 1 个 CRV 锁定 1 年 = 0.25 veCRV

veCRV 可用于投票招募新配对，并决定每对获得多少 CRV 产量农业奖励。 更重要的是，veCRV 用于确定流动性提供者可获得的高产农业奖励。

通过参考上图，yUSD 是一个收益稳定币池。 用户可以将yUSD存入Yearn Finance以获得yCRV，在那里将收获CRV奖励并出售以获得更多的yUSD。

基本年收益率 (Base APY) 是指作为曲线池的流动性提供者赚取的掉期费。 Rewards APY 是指以 CRV 代币形式的流动性挖矿计划奖励。 通过使用 veCRV，8.68% 的基础奖励可以扩大到 21.69%，或基础奖励的 2.5 倍。 总体而言，预期回报率约为 31.59% 至 44.60%。

通过将您的美元稳定币存入 Yearn Finance，您将受益于最高 2.5 倍的增产农业奖励，而不必锁定您的 CRV 来获得收益。

Yearn Finance 合作伙伴关系

从 2020 年 11 月 24 日到 2020 年 12 月 3 日，Yearn Finance 宣布了多项协议的一系列合作伙伴关系（称为合并和收购），基本上形成了一个围绕 YFI 的联盟。

- SushiSwap 加入其自动化做市商 (AMM) 部门
- Cover 作为其保险部门加入
- CREAM 加入其借贷部门
- Akropolis 作为其保险库和即将推出的借贷产品的机构服务提供商加入。
- Pickle 作为其战略家之一加入。

Yearn Finance 已选择于 2021 年 3 月 5 日终止与 Cover Protocol 的合作关系。

Yearn Finance 的第 2 版还通过向社区战略家分享一定比例的利润来激励社区做出贡献。 Yearn Finance 还与其他愿意形成协同关系的协议建立了一个附属计划，这些协议将获得高达 50% 的收入。 换言之，Yearn Finance 已成为一个大型生态系统，提供一系列高产农业产品和服务。

Alpha Finance

Alpha Finance 通过他们的第一个产品 Alpha Homora 引入了杠杆式高产农业，允许用户使用借入的资金来增加他们在高产农业活动中的曝光度。 从本质上讲，它同时充当贷款和收益聚合器协议。

在 Alpha Homora 版本 2 中，用户可以借出（赚取借贷利率）和借入许多资产（以利用他们的收益耕种头寸），包括 ETH、DAI、USDT 和 USDC、YFI、SNX、sUSD、DPI、UNI、SUSHI 、链接和 WBTC。

例子

使用第 2 章中提到的 SUSHI/ETH 示例，您现在可以选择通过借入价值 1,000 美元的 ETH 来利用 Alpha Homora 的两倍资本，而不是只有 1,000 美元的资本。

通过借入 1,000 美元，您现在将通过提供价值 1,000 美元的 ETH 和价值 1,000 美元的 SUSHI 来参与产量农业，总计 2,000 美元。 只有当掉期费用和产量农业奖励大于 Alpha Homora 的借贷成本时，这种策略才会产生利润。

另请注意，由于 ETH 和 SUSHI 都可以作为可借资产使用，您可以通过同时借入 ETH 和 SUSHI 来利用杠杆产生农场，以最大限度地减少掉期费用。

Alpha Homora 的借贷成本以可变利率计算，受供求关系的影响。如果借贷成本因借贷增加而突然飙升，则杠杆头寸可能会出现亏损。另一个风险是当借入资产的价格与产量农业头寸相比上涨时。使用上面的例子，如果 ETH 价格迅速上涨而 SUSHI 价格下跌，则杠杆头寸可能会被清算。

除了获得更高的回报，在收益农场上拥有杠杆头寸也会使用户面临更高的无常损失。赚取的利润很大程度上受借入农场的资产选择的影响。例如，借入 ETH 与美元稳定币将导致完全不同的回报状况。有关无常损失的更多详细信息，请参阅第 5 章。

Alpha Homora V2 还支持流动性提供者 (LP) 代币作为抵押品。例如，在 Sushiswap 上提供 ETH/SUSHI 池头寸的流动性用户将能够在 Alpha Homora V2 上存入 ETH/SUSHI LP 代币作为抵押品，并借入更多 ETH 和 SUSHI 代币以利用收益农场。

Badger Finance

Badger DAO 旨在创建一个 DeFi 产品生态系统，最终目标是将比特币引入以太坊。这是第一个选择将比特币作为主要储备资产而不是使用以太坊的 DeFi 项目。

Sett 是一个专注于代币化 BTC 的收益农业聚合器。 Sett 可以分为三个主要类别。

a) 代币化的 BTC 金库

- 受Yearn Finance 金库的启发，最初的产品包括支持CRV 代币的比特币金库，如SBTCCURVE、RENBTCCURVE 和TBTC/SBTCCURVE 元池。
- 他们还与 Harvest 协议合作，使用存入 Harvest 的 RENBTCCURVE 来种植 CRV 和 FARM 代币。

b) LP 金库

- 为了吸引更多的用户，WBTC/WETH 有一个集结 SUSHI 奖励的 Sett。
- 除此之外，还创建了四个 Sett 以引导 BADGER 和 DIGG 的流动性。

1) WBTC/BADGER UNI LP
2) WBTC/DIGG UNI LP
3) WBTC/BADGER LP
4) WBTC/DIGG SUSHI LP

c) 协议库

- 用户只需将原生BADGER 和DIGG 代币质押到bBADGER 和bDIGG 金库中，赚取协议费用并获得耕作奖励，就可以选择避免无常损失和代币化BTC 风险。

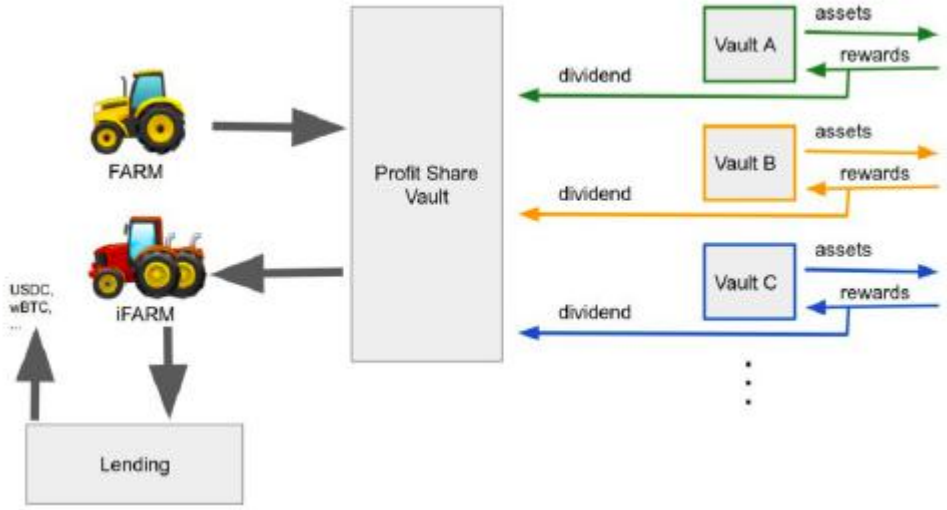
Harvest Finance

Harvest Finance 最初是一个 *Yearn Finance* 分支，此后采用了快速移动策略。 它比其他收益聚合器协议更快地发布新策略，即使那些被认为是高风险的。

截至 2021 年 4 月，它仅在以太坊就支持了令人震惊的 63 个不同的农场，类别涵盖稳定币、SushiSwap、ETH 2.0、BTC、NFT、1inch、算法稳定币和 Mirror Protocol 的 mAssets。

它最近还扩展到 Binance Smart Chain，在 Ellipsis、Venus、Posicle Finance、PancakeSwap、Goose Finance 和 bDollar 上提供农场。

Harvest Finance 团队发布了一种计息 FARM (iFARM) 代币，用户可以在其中抵押 FARM 以赚取协议费用。



资料来源:
https://mbroome02.medium.com/harvest-101-understanding-ifarm-and-its-potential-54d9cfe305e5

收益聚合器的比较

	Yearn Finance	Alpha Finance	Badger DAO	Harvest Finance
Management Fee	2%	-	-	-
Performance Fee	20%	-	20%	30%
Borrowing Fee	-	10%	-	-

在决定使用哪个收益聚合器时，要考虑的重要因素之一就是收取的费用。 Yearn Finance 遵循标准的对冲基金模式，收取 2% 的管理费和 20% 的绩效费。 Badger DAO 和 Harvest Finance 分别只收取 20% 和 30% 的绩效费。 Alpha Finance 在以太坊和 BSC 上的 Alpha Homora v1 根据杠杆借入的金额收取 10% 的利息，并在 Alpha Homora V2 上收取 20%。

费用结构表明，用户可能必须通过使用 Yearn Finance 进行投资来支付最高费用 - 无论所部署的策略是否获得回报，每年都会收回投资金额的 2%。

收取绩效费可以被认为更公平，因为它只是意味着用户的回报较低。 由于其行业领先地位，Yearn Finance 可以收取溢价，它的许多保险库都与 Alchemix、Powerpool 和 Inverse Finance 等其他协议集成。

	Yearn Finance	Alpha Finance	Badger DAO	Harvest Finance
TVL ($ Mil)	2,000	936	1,140	527
Market Cap ($ Mil)	1,305	434	287	113
FDV ($ Mil)	1,348	1,810	975	180
Market Cap/TVL	0.65	0.46	0.25	0.21
FDV/TVL	0.67	1.93	0.86	0.34

* 数据截至 2021 年 4 月 1 日

在总价值锁定 (TVL) 方面，Yearn Finance 仍然保持领先，而 Harvest Finance 似乎是收益聚合器中被低估最严重的。 同时，根据完全稀释估值与锁定总价值（FDV/TVL）的比率，Alpha Finance 的估值最高。

相关的风险

由于收益聚合器从风险较高的协议中寻求高收益的性质，收益聚合器面临着很高的黑客风险。 在四个协议中，只有 Badger DAO 尚未被黑客入侵（截至 2021 年 4 月）。

与保险协议的整合仍然乏善可陈，这可能是该行业锁定总价值进一步增长的最大瓶颈。 随着更多保险协议的推出，我们可能会在未来看到投保收益聚合器产品的推出。

值得一提的是

- Pancake Bunny

Pancake Bunny 是币安智能链生态系统中最大的收益聚合器。 它只提供基于 PancakeSwap 的农场。Binance Smart Chain 的低 gas 费允许更频繁的重新质押策略，从而增加收益率并导致更高的 APY。 所提供的农场始终提供高于 100% 的产量。

- AutoFarm

AutoFarm 是一个跨链产量农业聚合器，支持 Binance Smart Chain 和 Huobi ECO Chain。与 Pancake Bunny 一样，AutoFarm 提供更高的复利频率，因此为其农场提供更高的 APY。 它是币安智能链生态系统中的第二大收益聚合器。

总结

收益聚合器的作用类似于主动管理的基金或对冲基金。他们的工作是寻找最佳投资机会并从中赚取费用。

在 DeFi 中，流动性挖矿计划催生了一种专门的赚取回报的方式。随着 DeFi 可组合性以越来越有创意的方式被利用，我们预测收益聚合器采用的策略将变得更加复杂。

大多数产量农业计划只能维持大约三到四个月，并且可以通过治理随时更改。收益聚合器可帮助用户找到高收益农场，但新农场通常会增加被黑客入侵的风险。在寻求高收益与风险之间取得平衡是一项挑战。

还有人担心收益聚合器提供的高收益可能无法持续。截至 2021 年 4 月，高收益部分受到投机性市场环境的支持。例如，高 CRV 代币价格转化为高产农业奖励。没有人确切知道收益率在熊市中会如何表现，但它很有可能压缩到零。对于收益聚合器来说，这不是一个好景象。

推荐读物

1. Yearn 改进提案 (YIP) 56 - 回购和建设
https://gov.yearn.finance/t/yip-56-buyback-and-build/8929
2. Yearn 改进提案 (YIP) 61：治理 2.0 https://gov.yearn.finance/t/yip-61-governance-2-0/10460
3. Alpha Homora V2 即将重启！ 包括什么？
https://blog.alphafinance.io/upcoming-alpha-homora-v2-relaunch-what-is-included/

第十三章:预言机　和数据聚合器

DeFi 由智能合约支持。有时，我们所需的输入包含没有存储在区块链上的真实数据，例如天气条件、交通信息。因此需要通过将链下数据中继到区块链的协议来弥合差距，以便智能合约与数据交互。

链下信息是 DeFi 的重要组成部分，应该始终保持准确有效。有虚假的数据将完全歪曲一个既定的项目，将给 DeFi 带来重大问题。然而，我们如何确保提供的数据总是准确和可信任的？

一些协议通过在不被操纵或篡改的情况下向区块链传输和广播数据来实现。这通常是通过投票或共识机制完成的，其中验证者对最准确的数据达成一致。如果没有预言机或数据聚合器作为真相的主要来源，坏人就可以利用虚假信息来利用毫无防备的用户。

在本章中，我们将更仔细地研究一些可用的预言机和数据聚合器，如 Chainlink, Band Protocol, Graph Protocol, and Covalent。我们将看到这些预言机和数据聚合器如何在区块链和真实数据之间架起桥梁。

预言机协议

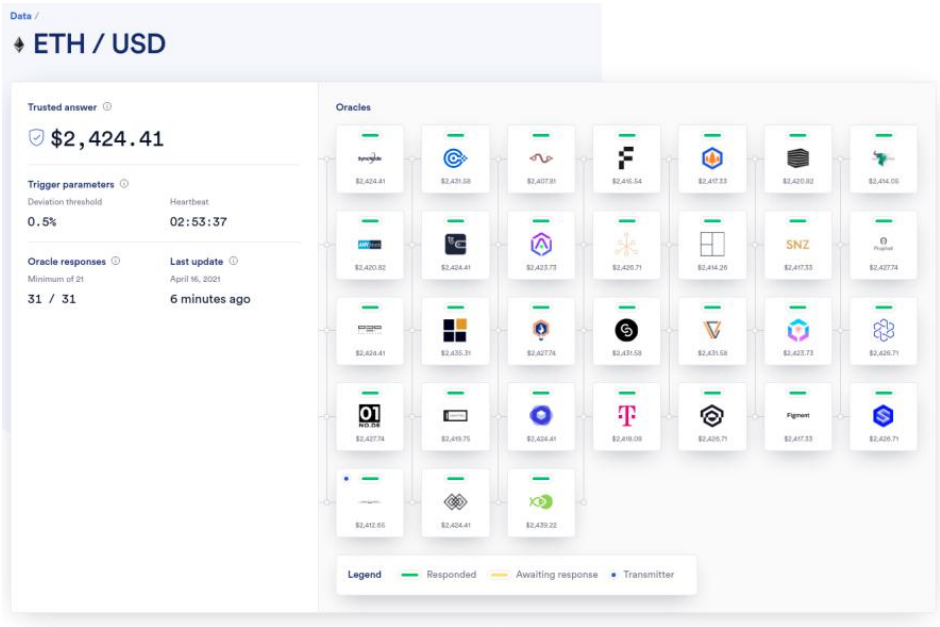
预言机充当了链外数据和区块链之间的桥梁，或者在没有内部数据 feed 来引用链上数据的协议之间的桥梁。这些与一年级寻求将外部信息中继到区块链，由 DeFi 生态系统中的智能合约或 Dapps 进行验证和执行。

Chainlink

Chainlink 是一个用于构建去中心化 oracle 网络的框架和基础设施，可以安全地将任何区块链网络上的智能合约连接到外部数据资源和链下计算。每个 oracle 网络都由独立的、不受 sybil 限制的节点运营商保护，这些节点运营商从多个链下数据提供者获取数据，将信息聚合为单一值，并在链上通过智能合约执行。

Chainlink 的主要功能之一是通过其价格馈源提供最准确的资产价格，这可以集成到区块链协议中用于特定的用例。例如，当到期的期权和期货合约结算时，以及当资产被用作贷款抵押品时，资产价格非常重要。Chainlink 的服务还包括一个用于跨链代币的储备证明参考 feed 和一个用于链上游戏应用的可验证随机函数。

为了更深入地了解 Chainlink 如何与数据交互和处理数据，我们将看看 Chainlink oracle 使用的一些方法来连接真实世界的数据到区块链。



Chainlink oracle 用来将外部数据带到链上的最常用方法是去中心化数据模型，这是一个持续更新的链上智能合约，代表一个特定的数据(例如，ETH 对 BTC 的价格)，可以在单笔交易中按需查询。

基本请求和接收模型是另一种方法，用户的智能合约直接从一个或多个 Chainlink 节点请求数据，并在下一个交易中接收报告的值。这个模型用于获取随机值或更多唯一的数据集。在这两种 oracle 网络模型中，Chainlink 节点都以 LINK 令牌作为其服务的费用。

任何人都可以成为 Chainlink 节点操作员，并开始向网络提供数据。Chainlink 价格馈送网络由传统企业(如德国电信的 T-systems、数据提供商和专业的 DevOps 公司)联合运营的节点来保证安全。数据提供商在其自身的 Chainlink 节点上直接对其数据进行加密签名，为智能合约提供更大的安全保障。

2021 年 4 月，Chainlink 2.0 白皮书发布，介绍了去中心化 Oracle 网络的新架构。去中心化 Oracle Networks 的功能类似于第二层解决方案，极大地提高了数据传输的速度并提高了安全性。此外，Chainlink 还引入了超线性押注模型，这是一种加密经济安全机制，可以激励节点提供准确的 oracle 报告，并显著增加恶意行为者的攻击成本。

这是一个关于 Chainlink 和去中心化 oracle 网络的快速概述。您可能已经注意到:本书中介绍的一些顶级 DeFi 协议，如 Synthetix 和 Aave，也由 Chainlink 提供支持。

Band Protocol

Band Protocol

与 Chainlink 类似，Band Protocol 是一个跨链 oracle 平台，将智能合约与外部数据和 api 连接起来。与 Band 协议集成的去中心化应用程序通过 Band 协议的智能合约数据点接收数据，而不是直接从链下的 oracle。

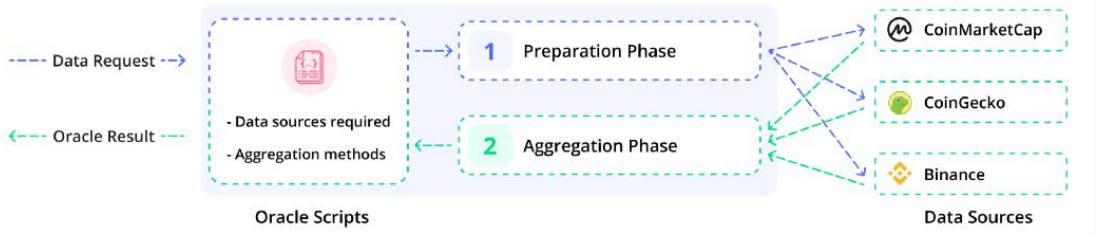
Band 协议的一个独特的方面是，他们利用 BandChain，一个单独的区块链来处理和中继信息，可以处理数千个事务。数据可以通过宇宙区块链间通信(IBC)协议发送到其他区块链。

来自 Band Protocol 的数据由社区管理和验证，确保它们足够可靠，可以被 Dapp 用户和开发者引用。这些数据源可以使用不同的统计方法(如平均值、中值或模式)从不同的链上提要和数据聚合器中聚合，也可以使用任何额外的数据清理方法(如标准化或时间加权平均数)。

要从 Band Protocol 检索数据，请求者需要指定几个参数:请求者想要调用的 oracle 脚本 ID，oracle 脚本的参数，以及所需的验证器数量。在 BandChain 上发出请求并验证后，oracle 脚本将开始执行的第一阶段，即准备阶段，通过发送满足请求所需的数据源。

验证器将根据随机加权算法来处理请求。验证器将尝试从所有指定的数据源中检索请求的数据，并将带有检索结果的原始数据报告提交给 BandChain 进行确认。

一旦最小数量的验证器成功提交了他们的报告，BandChain 将继续进行第二个阶段，也称为聚合阶段。所有收集到的报告都被汇编成存储在 BandChain 上的单个结果，可以访问并发送给其他区块链供未来使用。



BandChain 网络依赖于多个参与者，其中最重要的是验证者和委托者。持有最多 BAND 令牌的前 100 名验证者负责在 BandChain 网络上创建和确认新区块。另一方面，委托者可以将他们的 BAND 令牌委托给任何验证者以获得块奖励。

无论何时请求，BandChain 上的验证器都有从指定的数据提供者获取数据的职责。从经济上讲，验证者会被鼓励提供准确的数据，因为虚假数据的提供将导致被押注的 BAND 代币被大幅削减或没收。后续的错误信息计数将导致更低的信任分数和用户计数，进一步降低所押代币的价值，并增加损失。

在此基础上，所有人都可以公开查看和验证数据请求过程以及验证器的执行，进一步降低了传输错误或篡改数据的风险。自 2020 年 10 月 oracle 功能在 BandChain 主网上线以来，在前 6 个月里，验证器已经服务了大约 430 万个数据请求。

要成为 BandChain 上的验证官，你需要拥有一些 BAND 令牌或让其他用户委托给你 BAND 令牌。验证器是使用基于其所占 token 份额的权重算法随机选择的。比例越大，被选中的机会就越大。

数据聚合器

如果 oracle 将真实世界的数据连接到区块链，那么数据聚合器就可以帮助用户读取数据。这些协议将区块链数据编译成一种简化的格式，使项目和个人用户更容易创建他们的分析仪表板。

The Graph Protocol

Graph 是一个去中心化的协议，用于从以太坊、Polkadot 和 Solana 等区块链查询和接收数据。虽然通过读取区块链上的合约地址直接检索查询更简单，但具有更高特异性和粒度的数据更难找到。Graph 通过将区块链数据索引为子图或使用标准 GraphQL API 查询的开放 API 来解决这个问题。

Well 根据子图的描述(也称为子图清单)对不同类型的数据进行索引。清单定义了相关的智能合约和合约的关键事件。它还指出了如何将事件数据映射到 the Graph 数据库中存储的数据。

一旦创建了子图清单，Graph CLI 将其存储在星际文件系统(IPFS)中，这是一个分散的存储解决方案，并开始为该子图建立索引信息。

下面是一个关于图节点如何检测和存储数据的基本流程:

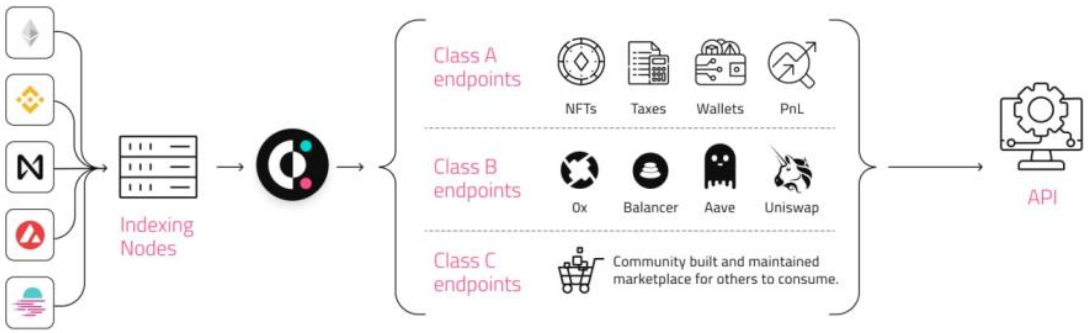
1. 去中心化应用程序(Dapps)将智能合约交易中的数据添加到区块链。
2. 智能合约在处理事务时发出事件。
3. 图节点不断扫描区块链以寻找新的块和子图显示的数据。
4. 图形节点查找事件并运行提供的映射处理程序。WASM 模块生成并更新存储在节点中的数据。
5. Dapps 使用 GraphQL 端点查询 Graph node 的索引数据。
6. GraphQL 查询在被 dApp 检索之前由节点进行翻译。
7. dApp 通过其用户界面显示这些数据，以便在区块链上发布新事务时用作参考。

在 DeFi 和 Web3 空间中，许多 dApps 都使用该图形，包括 Uniswap、Aave、Balancer 和 Synthetix。它为数据密集型协议提供了适当的基础设施。截至 2021 年第一季度，约 16000 名开发人员部署了超过 10000 个子图，在不到一年的时间里处理了超过 1000 亿个查询。

Covalent

Covalent 是一个区块链数据提供者，它提供了一个统一的 API 来访问看似无穷无尽的链上数据行。可以使用单一 API 检索来自不同区块链的代币余额和钱包活动的详细信息，这使得开发人员更容易创建分析仪表板或收集区块链活动的洞察。

Covalent 的功能可能看起来很相似的图表，但它区别自己在几个方面。例如，Graph 需要将数据的子集转换成子图，然后才能查询。同时，共价将对区块链进行整体索引，为用户提供更大数量的粒度数据。此外，共价已经扩展到以太坊之外。截至 2021 年 4 月，Covelant 支持其他四个区块链的数据，包括 Fantom、币安智能链、Polygon 和 Avalanche。



来源： https://www.covalenthq.com/blog/beginners-guide-to-covalent/要访问 Covalent API，您将需

要首先通过在 Covalent 上创建一个帐户获得一个免费的 API 密钥。有两类共价 API - A 类和 B 类。

您可以使用 A 类端点来检索区块链数据，这些数据与网络无关。简而言之，这是适用于所有网络的一般数据，如余额、交易和令牌持有者。另一方面，您可以使用 B 类端点从区块链上的特定协议返回值。例如，您可以从 Uniswap 或 PancakeSwap 查询数据，这两种去中心化的交换都隔离在各自的网络上。

值得注意的情况

DIA

DIA 是去中心化信息资产(Decentralized Information Asset)的缩写，是一个开源 oracle，为许多 DeFi 应用程序提供数据。他们在币安 Smart Chain 和 Polygon 等其他链上为 Uniswap 和 Sushiswap 等流行的 DEXs 提供价格反馈。

API3

API3 通过分散的 api 或 dAPI 向项目提供信息。数据提要由一个包括项目合作伙伴和行业专家的 DAO 监督。它们还允许 dAPI 用户在 API 不能正常工作的情况下获得链上保险。

相关风险

随着越来越多的协议开始依赖于长期存在的产品，这些产品已经在最恶劣的环境中进行了竞争完善。但与此同时，我们也应该警惕这些产品可能不是完全安全的。如果黑天鹅事件发生，预言机可能无法有效地提供数据，导致做出不准确的决定。

在 2020 年 3 月，也就是所谓的“黑色星期四”，Chainlink 和 MakerDAO 的 Medianizer 等甲骨文未能足够快地更新它们的价格信息，导致了严重的价格错误。MakerDAO 的价格故障引发了一系列灾难性事件，导致 CDP 所有者损失了超过 800 万美元的 ETH 抵押品。

结论

预言机和数据聚合器构成了许多 DeFi 协议的骨干。对于寻求改变数据提供游戏的未来项目来说，在查询和中继数据时对极快的速度和准确性的需求是至关重要的。目前，链链以超过 400 个集成项目主导着这个领域，其中包括超过 200 个 DeFi 项目。然而，随着更好的 oracle 和数据收集机制的定期发挥作用，DeFi 场景一直处于创新的前沿。最终，DeFi 的目标是拥有一个可靠的、内部安全的、免受负面外部影响的 oracle 服务。此外，已经建立并不断改进的健壮的索引协议将为区块链上的用户行为带来更多的清晰度和洞察力，允许项目提供更适合产品市场的更好的产品和服务。

第十四章:多链协议以及跨链桥

毫无疑问，以太坊是许多DeFi项目的归宿。然而，正是由于高使用率，导致gas费用飙升，为用户和开发者敲响了警钟，并迫使让他们去探索交易费用更低的其他区块链。

许多DeFi项目在其他区块链网络中找到了第二个家，并为更多用户提供服务，更有效地扩大规模。虽然交易所也提供用户在各种区块链网络之间轻松转换，但却可以限制资金的移动。

从这种困境中，Ren、THORChain和anyswap等几个项目已经成长为允许用户以不同方式在区块链之间无缝连接和转移资金的项目。币安等中心化交易所也试图通过引入币安桥来桥接以太坊和其他区块链。

跨链协议概述

Ren Project

Ren Project是一个无需许可的协议，允许用户匿名地在区块链之间进行交互和转移token。Ren协议通过由Ren虚拟机(RenVM)提供的RenBridge实现了这一点。

RenBridge允许在其他网络上轻松转换加密货币。例如，比特币可以在以太坊网络上表示为ERC-20代币，将其包装成renBTC。使用RenVM，资产根据其目标网络的格式以1:1的比例进行转换，确保包装的版本总是完全由基础资产支持。

当您使用新包装的代币探索其他区块链时，RenVM充当您原始资产的去中心化托管者，通过铸造和燃烧，保税REN的价值保持在锁定资产总价值的三倍。为了维持RenVM的平稳运行，Darknodes会不断进行重组。还有额外的安全级别，如RPZ MPC算法的实施和算法调整费用，使得黑客攻击变得极为困难。在不太可能发生的攻击事件中，RenVM可以恢复被盗资金。

RenVM运行在一个被称为“暗黑节点”(Darknodes)的去中心化计算机网络上，这有助于验证交易并维护Ren网络的安全性。为了运营Darknode，用户需要押注10万个REN代币作为抵押，总额约为103,000美元(2021年5月7日)。

Darknodes以打包资产的形式从RenVM交易中收取部分交易费用。

Ren虚拟机支持三种类型的跨链交易—锁定和铸造（Lock-and-mint）、烧毁和释放（Burn-and-release）以及烧毁和铸造（Burn-and-mint）。

Lock-and-mint

当用户将资金从原始链发送到目的地链时，就会发生锁定和造币。发送给RenVM的令牌被“锁定”保管中。一旦资产被确认锁定，RenVM将向用户释放铸币签名，允许用户在目的链上铸币资产的1:1令牌化版本。铸币资产可在任何时间赎回，没有最低数量。

Burn-and-release

为了补充第一个交易，烧毁和释放允许用户通过烧毁目标链上资产的令牌化版本并接收选定地址上锁定的资产，将他们的代币从目标链发送回原始链。顾名思义，挂钩的令牌被“烧毁”，而RenVM在原始链上“释放”等量的基础资产。

Burn-and-mint

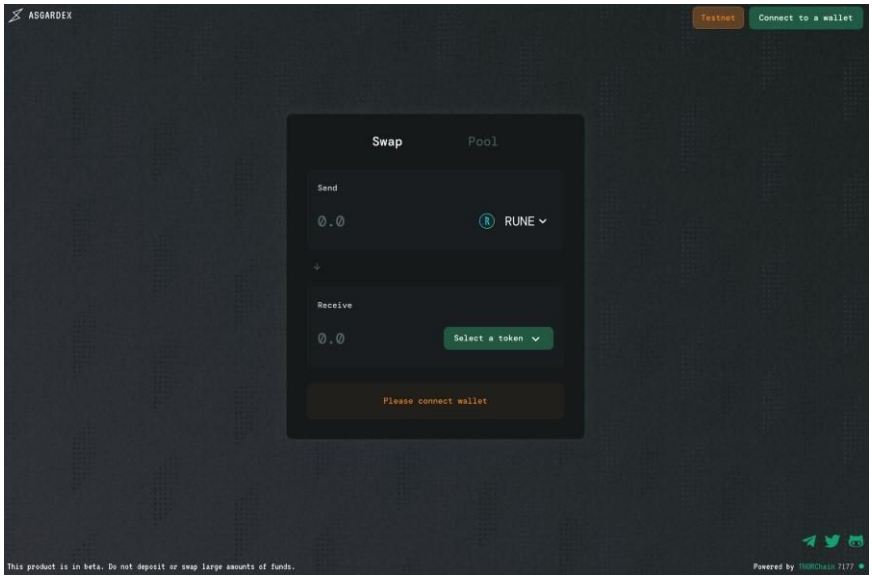
Burn-and-mint结合了上述两种交易。用户可以通过烧毁一个主机链上的固定资产，并在另一个主链上铸造相同数量的固定资产，从而直接在主链之间移动资产。然而，这将需要通过RenVM进行多次付款和确认，这是一个缓慢而昂贵的过程。

ThorChain

ThorChain是一个去中心化的流动性网络，具有可互操作的区块链；允许以非托管方式进行跨链token互换。它不固定或包装资产，但允许用户在不同的第一层区块链上交换代币。例如，ThorChain上的玩家可以无缝地将他们的资产从比特币转移到以太坊，而无需注册或通过中心化交易所的KYC流程。

ThorChain的吸引力在于它的链允许它无需进行某种形式的转换就可以交换资产。不想Ren,没有1:1锁定的比特币(renBTC)被创建的。相反，我们可以用ETH交换真正的比特币。和以前一样，这是一个里程碑，因此，ThorChain让比特币更接近DeFi生态系统的核心。

此外，随着Solana和Polkadot等新的智能合约平台用户数量的增长，这些区块链上各种项目也继续以抛物线速度扩张。链的多样性导致需要一种信任最小化和去中心化的方式来在不同的链上交换token。



ThorChain使用权益证明共识机制。它建立在Tendermint上，网络验证器或节点需要绑定本地token“RUNE”。RUNE有一个token模型，它的价值随着网络利用率的增长而增加。这意味着，随着更多的流动性存入ThorChain流动性池，RUNE将变得更有价值。

RUNE被需求有两个根本原因:

I. 在流动性池中，RUNE作为一个资产对，其中的资产比例为1:1:符文需要进行担保(例如，bnb-RUNE或ETH-RUNE)。ThorChain不是通过直接的资产转换;相反，它需要RUNE从一个资产转移到另一个资产。RUNE也被需要激活ThorChain的彩虹桥协议，它作为桥梁，使多链连接。该协议还跟踪了符文与其连续流动性池(CLP)中的资产的比率，这意味着它们也继承了不需信任的链上数字资产价格喂价，而无需依赖第三方预言机。

II. RUNE由节点运营商作为抵押品担保，其债券与股份比例为2:1。RUNE不打算成为治理token;

T

ThorChain更像比特币，节点运营商可以决定其未来的方向。这也意味着ThorChain不仅限于交易员，还被流动性提供者和节点运营商使用。

如果是2:1的债券:股权比例，再加上1:1的池质押比例，需要的RUNE数量将是锁定的非RUNE资产数量的三倍。换句话说，这个3:1的比例代表了协议操作所需的RUNEtoken的最小值。

使用ThorChain跨链服务的用户将需要支付固定的网络费用和可变的流水单费用，以支付外部服务和快速执行的gas费用。除了为交易员提供无缝服务外，用户还可以成为ThorChain上的流动性提供者。

ThorChain上的流动性提供者可以向不同的池添加流动性，这些池与单独的保险库中的RUNE绑定。流动性池鼓励任何ThorChain参与者提供流动性以换取RUNE奖励。

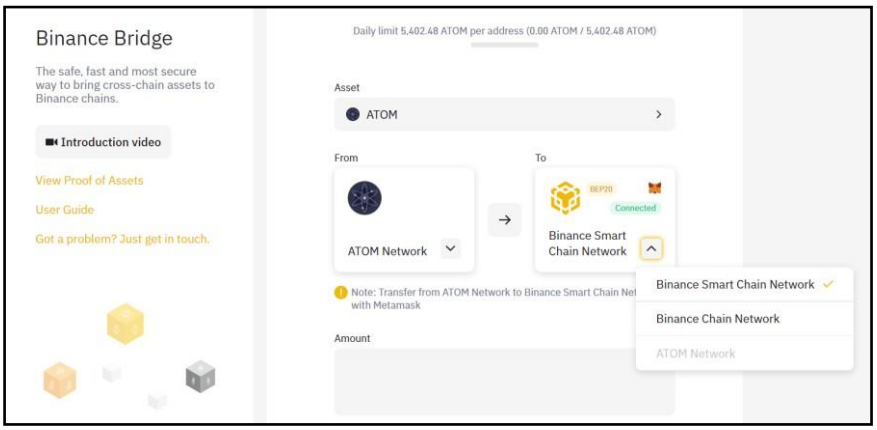
正如ThorChain网站上提到的，“流动性是由在掉期交易中赚取费用的质押提供的，这些质押以非托管的方式将其非生产性资产转化为生产性资产。”市场价格是通过池子中的资产比率来维持的，交易员可以通过套利来恢复正确的市场价格”。

ThorChain与众不同的是它的跨链功能——它允许用户交换任何资产，并创建一个流动性池，为DeFi生态系统打开了一个全新的可能性世界。

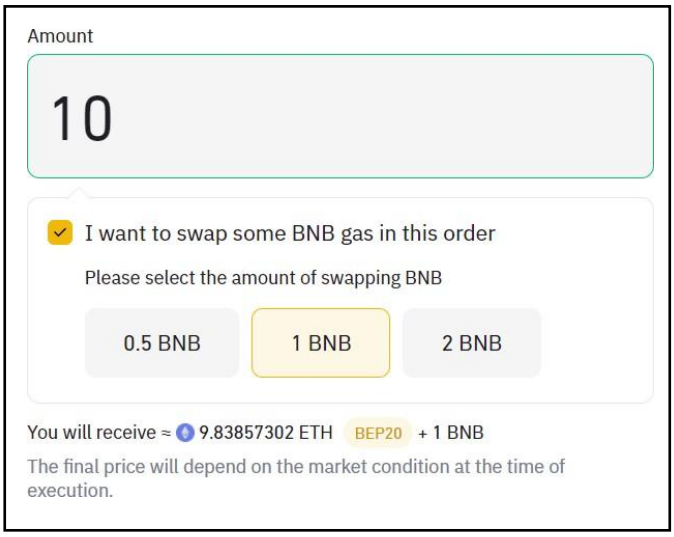
截至2021年4月13日，THORChain多链Chaosnet以及其去中心化交易所Asgardex已经上线。用户可以在五个活跃的区块链网络上进行交易——比特币、比特币现金、莱特币、以太坊和币安链。

币安桥

使用币安桥，用户可以在以太坊、Tron或币安智能链(BSC)网络等各种区块链之间转账。每个特定资产只支持特定的区块链。例如，其他区块链(如Cosmos (ATOM)和Ontology (ONT))的原生代币只能在币安智能链、币安链或其原生网络之间传输。对于每个资产，你每天可以转移多少是有限制的。

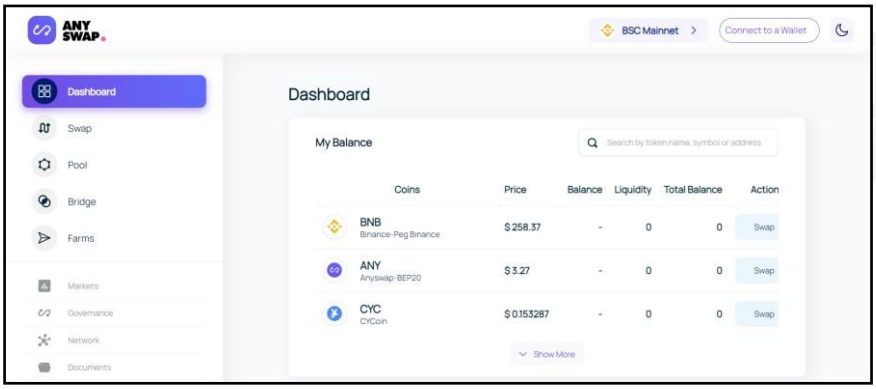


如果你正在将资产转移到币安智能链网络，你也可以选择兑换一些币安币(BNB)。与以太坊网络上使用Ether支付交易费用的方式类似，BNB被用于支付币安智能链网络上的交易费用。因此，建议您兑换一些BNB，特别是如果您是币安智能链的新手。



Anyswap

answap是一个去中心化的跨链交易所，支持8种不同的区块链，如以太坊、币安智能链和Fantom。它为用户提供了一个一体化的平台，以交换或转换他们的资产到其他区块链。用户可以选择将其资产存入再mint token的传统方法，或直接执行跨链互换，将其代币交易为不同区块链上的另一个代币。



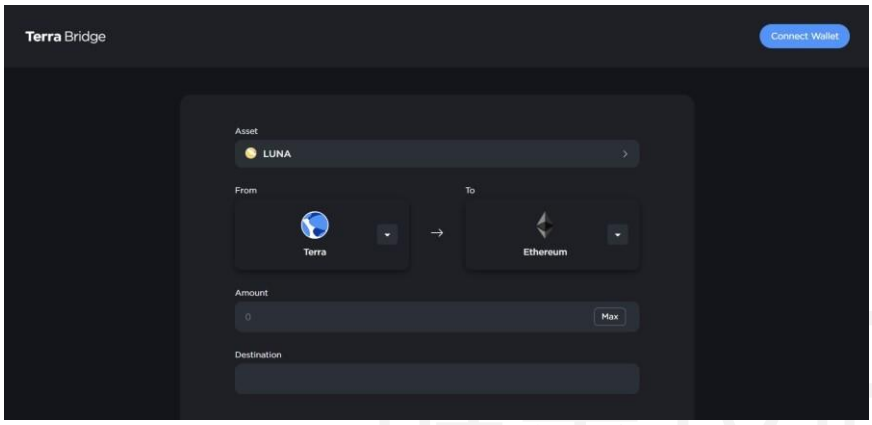
对于每个区块链，answap DEX支持不同的代币对，从版本1开始，这些代币总是与网络的原生代币配对。例如，在Fantom网络中，Tokens与FTM代币配对。

该交易所收取的费用根据gas的使用量和互换中使用的资产类型而有所不同。本质上，用户除了支付网络交易费用外，还必须支付0.4%的交易费。75%的费用给流动性提供者，其余的费用给answap。用户在任意两个非本地资产之间进行交易时，都会收取两次0.4%的费用。

自从Andre Cronje分享了他对跨链项目的兴趣之后，answap项目就越来越受欢迎。随着answap支持的区块链总价值超过6.2亿美元(截至2021年5月)，越来越多的用户愿意接受它和探索其他网络，该协议仍有很大的增长空间。受answap的启发，Andre Cronje也发布了multichain.Xyz跨链协议。

Terra桥

Terra Bridge是一个应用程序，用户可以在Terra区块链上向以太坊和币安智能链网络发送受支持的Terra资产。这些资产包括LUNA (Terra的原生代币)、UST (Terra USD)等Terra稳定币，以及mTSLA(特斯拉)和mAAPL(苹果公司)等镜像资产。



其他项目

-  Multichain.xyz

  支持10种不同的区块链，多链。xyz允许你交换各种资产，如BNB, ETH和USDC。截至2021年5月24日，其总价值锁定超过2亿美元，支持超过280个代币。

-  Matic bridge

  Matic的Web钱包桥允许用户使用Plasma或PoS桥将资金转移到Polygon网络。根据使用的情况，只有某些资产可以转移。反向取回时间可能会有所不同。

-  **APYSwap**

  APYSwap是一个用于在不同区块链之间交换资产的去中心化协议，它有一个独特的功能——它也适用于非EVM兼容的区块链，允许用户将资金从以太坊、币安智能链和Huobi 生态链转移到Solana，反之亦然。

相关风险

尽管跨链桥和跨链协议正在成为改善不同区块链网络之间的连接的关键步骤，用户也应该意识到在与这些协议交互时可能发生不同的问题。

除了智能合约的本身所带来的内在风险，例如它们暴露于错误代码和漏洞之中，用户必须确保他们的原始资产在其他链上创造挂钩资产之前真正锁定在本地链上。如果原始的代币可以自由解锁

并被他人使用，铸成的资产将变得一文不值，因为它们不能在原始链上用于赎回。

用户还需要了解不同网络的代币的不同智能合约。尽管大多数代币在多个区块链中具有相同的合约地址，但在尝试执行转账或跨链存款时，检查您确实获得了相同版本的代币或挂钩的资产仍然很重要。

结论

随着侧链开始受到越来越多的关注，跨链桥和多链协议将比以往任何时候都更加重要。无论是通过代理代币还是原生代币之间的无缝交换；很明显，更多的用户将继续尝试进入可能提供不同服务或更低费用的区块链。因此，改善这些协议的安全性和用户体验对于确保DeFi真正适用于每个网络中的每个人都至关重要。

推荐阅读

1. Ren Protocol Review https://defirate.com/ren-protocol/
2. An In-depth Guide to Thorchain's Liquidity Pools https://medium.com/thorchain/an-in-depth-guide-to-thorchains- liquidity-pools-c4ea7829e1bf
3. Documentation on Binance Bridge v2 https://docs.binance.org/smart-chain/guides/bridge-v2.html
4. Anyswap DEX User Guide
   https://anyswap-faq.readthedocs.io/en/latest/
5. User Guide for Interchain Transfers on Terra's Shuttle Bridge
   https://docs.anchorprotocol.com/user-guide/interchain-transfers
6. Guide to use Matic Bridge by Matic Network https://blog.matic.network/deposits-and-withdrawals-on-pos- bridge/
7. How to Add Networks Using Chainlist.org https://metamask.zendesk.com/hc/en-us/articles/360058992772- Add-Network-Custom-RPC-using-Chainlist-in-the-browser- extension

第十五章:探索DeFi

探索 DeFi 是极具风险的，黑客攻击智能合约的事情时有发生。仅仅是在 2020 年，就有至少 12 起备受瞩目的黑客入侵事件，从各个 DeFi 协议中盗取了不少于 1.21 亿美元的资金。

来源：CoinGecko 2020 年报

哪怕是最好的智能合约审计人员也不能够完全预测已经被部署智能合约何去何从。当数十亿美元的资金在智能合约上流动时，毋庸置疑，最聪明的黑客将一直寻找安全漏洞来从中获利。

DeFi 项目利用可组合的特点构建在彼此之上，DeFi 应用程序的复杂程度也呈几何倍数增加，这也使得智能合约的审计人员更难检测到安全漏洞。这也是 DeFi 面临的最大风险。DeFi 应用程序开发者必须确保网络安全监测人员不断检查他们的代码，以减少任何被利用的可能性，因为不经意间的一个漏洞将会导致巨大的经济损失。

在本章中，我们将着眼于黑客入侵的原因、闪电贷、减少黑客入侵损失的可能解决方案，以及为个人提供一些在使用 DeFi 时避免损失的建议。

漏洞利用的诱因

下面我们将了解一些常见的漏洞原因。这份清单并非详尽无遗。

经济漏洞/闪电贷

只要借贷人在同一笔交易内偿还贷款，闪电贷就可以给用户提供无限的资金进行金融交易。闪电贷是一项强有力的工具，它可以使过去受到资本制约而无法实现的经济攻击都可以被实现。有了闪电贷作为手段，仅仅需要找到合适的策略就可以利用无限机会。

几乎所有的 DeFi 黑客都利用了闪电贷。我们将在下一个部分详细研究它。

产品文化中的代码漏洞

在 Yearn Finance 创始人 Andre Cronje 的领导下，DeFi 的许多项目都遵循在生产中测试的精神，而不是最大限度提高安全性以及通过更多的测试来加快产品开发。若对每个版本都进行完备的审核将延长新一代产品推向市场所需的时间。

DeFi 的主要竞争优势之一是，开发者可以更快地迭代产品，不断拓展金融创新的边界。然而，并不是每个项目都可以接受审计，特别是当项目尚未取得任何进展时。尽管经过了多次审计，但是黑客仍然会设法利用一些项目漏洞。这表明审计可能不足以防范所有的黑客攻击。

草率的编码和不充分的审核

在牛市中，许多项目团队因同行竞争压力需要快速发行推进产品，甚至有时候采取捷径。有些项目可能决定完全跳过审核，以获得先发优势，只有在产品上线几个月后才进行审核。

还有很多分叉——新项目使用与其他已建立的项目相同的代码。在没有完全理解代码如何工作的情况下，它们就被当作快速捞钱的工具，导致了许多漏洞。

Rug Pull（inside Jobs）

在 DeFi 空间中，匿名团队启动的项目并不罕见。因为当下不确定的监管环境，有些人这样做是为了逃避监管机构的审查。然而，其他人选择匿名是因为他们另有所图。例如有很多匿名小组通过内部工作之便故意留下一个漏洞，加以利用从不知情的用户手中偷取利益。

加密社区不会疏远由匿名创始人发起的项目，正如我们看到的第一个加密货币——比特币也是由一个不知名的人创立的。用户往往基于所生成的代码来评价项目，而不是开发人员是谁或在哪里。这与开放软件的去中心化思潮是一致的。

撇开理想不提，如果一个攻击发生在一个匿名团队发起的协议上，由于很难找到开发人员的真实身份，因此没有追索权的可能性很高。

Oracle 攻击

DeFi 协议需要了解资产价格才能正常运行。例如，贷款协议需要知道资产价格来决定是否清算借款人的头寸。

因此，作为 DeFi 基础设施不可缺少的一部分，oracle 可能会受到严重的操纵。例如，我们在第 12 章中提到，利用 MakerDao 的金库漏洞造成不必要的金库清算，使致 ETH 损失总计超过 800 万美元。

Metamask 攻击

Metamask 作为每个以太坊应用程序的主接口，成为主要攻击目标也就不足为奇了。Consensys 团队的安全措施非常周全，到目前为止，还没有大规模的攻击。

然而，也有一些备受关注的被入侵事件：
EasyFi 项目的 MetaMask 管理钱包损失了 5900 万美元
Nexus Mutual 创始人的钱包损失了 800 万美元

闪电贷

什么是闪电贷?

闪电贷是指只要用户在同一笔交易中偿还贷款，即可无需任何担保获得资金。如果用户在此

次交易中不偿还贷款，那么交易的费用就会丢失，保证了闪电贷不会发生，交易也就自动取消了。有各种 DeFi 协议能够提供闪电贷，例如 Aave 和 dYdX。

与普通贷款相比，闪电贷有三个突出的特点：

无违约风险：闪电贷需在同一交易内偿还，因此没有违约的风险。

没有抵押品：只要他们能在一次交易内偿还贷款，借款人就可以在不公布任何抵押品或信用检查的情况下获得贷款。

无限制的贷款规模：用户可以从 DeFi 协议的借款额度不能超过可获得的总流动性。

截至 2021 年 4 月，闪电贷的应用不是很亲民。因为你必须通过编写智能合约代码来应用闪电贷。所以，软件程序员比一般人更容易理解它。

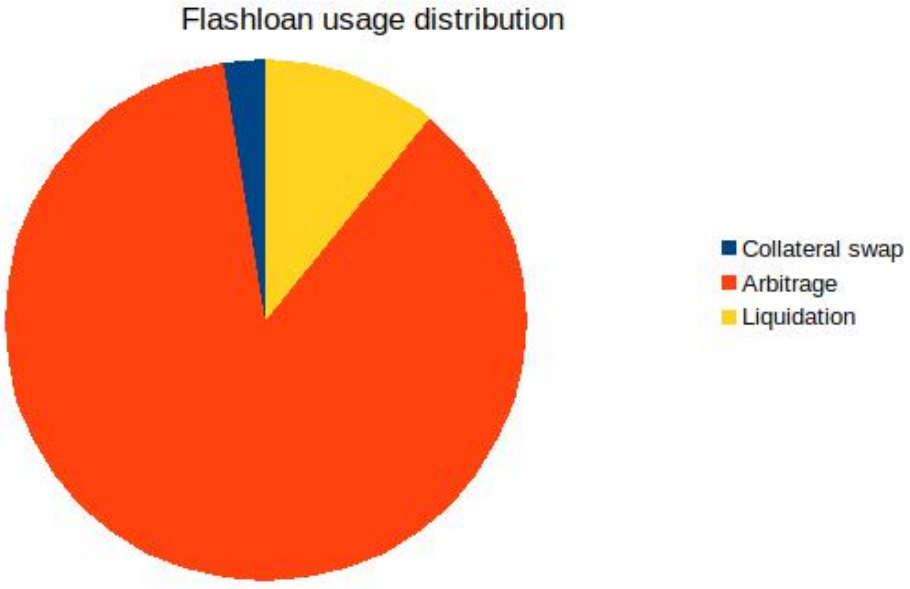
事实上，一些程序员经常利用不需要抵押品的这一因素，发起我们所说的"闪电贷款攻击"(flash loan attack)。最著名的一次闪电贷款攻击发生在 Harvest Finance，造成了 2400 万美元的损失。

下表显示了提供闪期贷款的主要协议所产生的费用：

Protocols	Flash Loan Fee
Aave	0.09%
dYdX	1 Wei (10^{-18}) ETH
bZx	None
Uniswap v2	0.3%

闪电贷的用途

下面的图表显示了所有闪电贷的使用情况：



来源：Aave

我们可以看到，闪电贷主要用于套利目的。套利是利用市场之间的价差来获利的行为。例如，假设我们发现 WBTC 在两个不同的去中心化交易所有相当大的价格差异。我们可以使用闪电贷，在没有任何担保的情况下借入大量 WBTC，从差价中获利。

闪电贷的第二种用途是用于贷款清算。如果借款者被协议清算，他们通常会受到惩罚。当市场出现重大价格波动时，借款人可以选择获得闪电贷款并自行平仓，从而避免了罚款费用。

让我们看一个例子，我们从 Maker 那里借 DAI，以 ETH 作为抵押。当 ETH 价格大幅下跌时，

可能会接近我们 DAI 贷款的清算水平。我们可能没有 ETH 来增加我们的抵押品，也没有 DAI 来偿还贷款。我们所能做的就是用 DAI 闪电贷来偿还 Maker 贷款。然后，我们可以将部分已提取的 ETH 抵押品交换给 DAI，来立即偿还闪电贷。使用这种方法，我们将保留剩余的 ETH 不支付清算罚款。

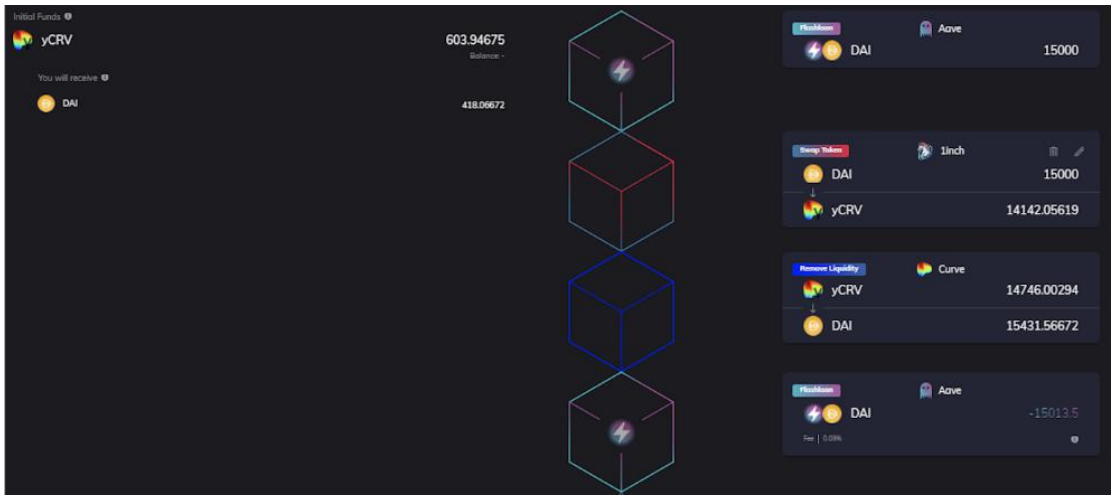
最后，闪电贷还可以用来执行抵押品互换。例如，如果我们在 Compound 中有一笔 DAI 贷款，以 ETH 作为抵押，我们可以使用闪电贷款将 ETH 抵押换成 WBTC 抵押。这使我们可以轻松地降低我们的风险，而不必进行多次交易。

使用闪电贷仍然需要大量的技术知识，对于那些不知道如何编程的人来说门槛很高。然而，有一个第三方应用程序可以帮助普通用户执行闪电贷，这个平台被称为 Furucombo。

闪电贷协议：Furucombo

Furucombo 是一个任何人都可以利用闪电贷来实现套利策略的平台。由于它的拖放工具允许终端用户能够创建和定制不同的 DeFi 组合，组装金钱乐高的门槛降低了。其重要注意的是 Furucombo 并没有寻找套利机会。

为了使用 Furucombo，用户需要设置输入/输出和交易的顺序，它将把所有多维数据集捆绑到一个交易中执行。下面展示了一个如何执行套利交易的示例：



1. 向 Aave 申请 15,000 DAI 闪贷。
2. 使用 1nch 交换 DAI 到 yCRV。
3. 交换 yCRV 回 DAI 使用曲线。由于价格差异，你最终得到 15,431 个 DAI，比以前更多。
4. 15,013 个 DAI 的贷款金额(包括 Aave 的闪电贷费用)已偿还给 Aave。

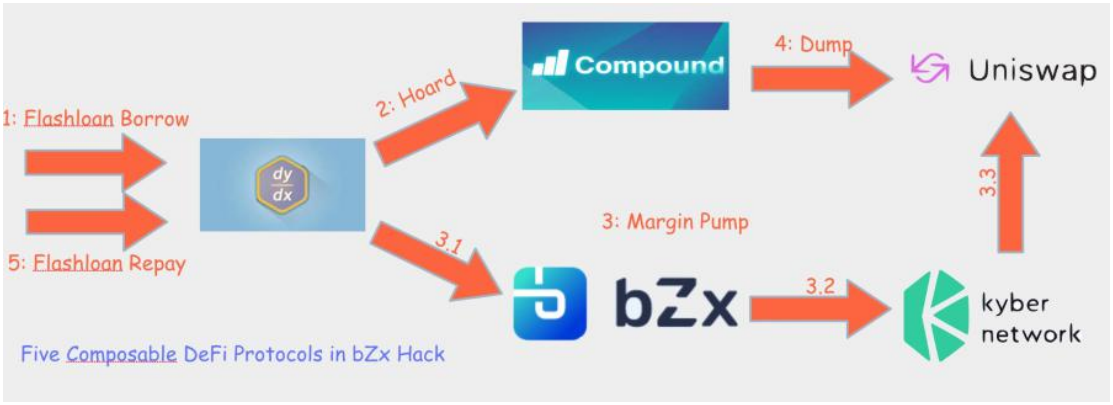
用户的利润为 418 DAI。所有这些步骤都在一个事务中执行。

Furucombo 不需要任何预付资金，也不收取任何费用，用户可以在平台上使用闪电贷建立组合和套利交易。你所需要的只是钱包里的 ETH 来支付 gas 费。

建议用户自行承担交易风险，因为 Furucombo 上并不总是存在套利机会，如果价差不再存在，组合可能会失败。无论结果如何，用户都要承担支付交易费用的风险。

案例研究：bZx 闪电贷遭遇黑客入侵

2020 年 2 月 15 日，以太坊区块链上发生了一笔交易，当时被认为是独一无二的。在不到一分钟的时间里，一个区块和一笔交易就实现了大约 36 万美元的利润。这一交易引起了加密社区的关注，经过深入分析后发现这一收益是通过一种最初几乎无风险的闪电贷形式获得的，随后在不同去中心化的交易所之间进行一系列套利。



来源：Peckshield

1. 借出闪电贷

首先，从 dXdY 利用闪电贷借出 10000ETH。

2. 存入

其中一半的 ETH (5500 ETH)作为抵押在 Compound 中借 112 WBTC。

3. 保证金买入

将 1300 个 ETH 存入 bZx，利用 5 倍杠杆做空 ETH，以提供 WBTC。从 bZx 借的 5637 个 ETH 使用 KyberSwap 交换 51 个 BTC。根据 KyberSwap 算法，Uniswap 提供了最优价格。然而，由于流动性较低，该交易将 1 WBTC 的汇率推高至 109.8 WETH 左右，大约是同期正常兑换率的三倍。

4. 卖出

攻击者在价格上涨后将借来的 112 WBTC 卖给 Uniswap，得到 6871 ETH，此时兑换率是 1WBTC = 61.2 WETH

5. 闪电贷收益

通过出售一个未使用的 3200 ETH 和 6871 ETH，攻击者偿还了 10000 ETH flash 贷款，收益为 71 ETH。

Protocol	Amount	Asset	Type
dYdX	-10,000	ETH/WETH	Debt
Compound	+5,500	ETH/WETH	Collateral
Compound	-112	WBTC	Debt
bZx	+1,300	ETH/WETH	Collateral
bZx	-5,637	ETH/WETH	Debt
bZx	+51	WBTC	Collateral

Accounts	Amount	Asset	Type
-	+3,200	ETH/WETH	Balance
-	+6,871	ETH/WETH	Balance

6. 总利润

Compound 公司仍然盈利。由于 1 个 WBTC 的市场平均价格为 38.5 WETH，那么攻击者可以用大约 4300 个 ETH 得到 112 个 WBTC。总的来说，攻击者获得了 71 WETH + 5,500 WETH - 4,300

ETH = 1,271 ETH，大约$355,880(假设 ETH 价格为$280)。

上述事件不仅表明了通过操纵其他资产价格而获得极端资本利得的可能性，而且还表明除了相对较低的协议费用外，借款人没有其他成本。借款人只需要满足贷款必须在同一笔交易内偿还。因此，无抵押贷款的概念本身在这个领域开辟了新的天地，提供了广泛的机会。

闪电贷总结

闪电贷款可能是一把双刃剑。一方面，它对智能合约的创新使用为 DeFi 生态系统带来了便利和进步——没有太多资金的交易者可以利用闪电贷推出套利和清算策略，而不需要大量资金基础。

另一方面，因为不需要抵押品黑客可以利用闪电贷发动闪电贷攻击，这大大提高了他们的利润。就像任何工具一样，闪电贷既可以“造福人类”，也可以“害人害己”。

在我们看来，由于项目改善了基础设施，以防止未来发生攻击，用于不良目的的闪电贷款攻击强化了整个 DeFi 生态系统。由于闪电贷仍处于初期阶段，这些攻击可以被视为提高 DeFi 生态系统抗脆弱性的一线希望。

解决方案

仅仅进行智能合约审计是不足以防止漏洞的。项目方需要做更多努力。他们正在寻找替代方案，以确保在协议中的资金安全。下面是一些可能的解决方案：

内部保险基金

几个项目已经决定使用他们的原生代币来对冲风险：
Maker 在黑色星期四重新发行 MKR，以弥补 DAI 的清算缺口。
Aave 推出了 stAAVE 以填补储户的潜在差额。
YFI 抵押了他们的代币并借了 DAI 来偿还被窃取的资金。

保险

作为区块上的新兴项目之一，unslash Finance 为其用户提供 LIDO 和 Paraswap 的协议级覆盖。This opens up the possibility for protocols to buy covers for their users.

漏洞奖励

项目正越来越多地利用 Immunefi 来列出漏洞赏金，鼓励黑客发现漏洞而不是利用它们来索取奖励。最高赏金可达 150 万美元。然而，由于黑客行为有更高的潜在回报，这是否能阻止黑客还有待观察。

其他的可能解决方案

行业保险池

可以有一个行业范围内的保险池，每个 DeFi 协议项目的部分收入或支付固定的费用。当其中一个成员遭遇黑客攻击时，该池预计将支付索赔。这与联邦存款保险公司(Federal Deposit Insurance Corporation, FDIC)的想法类似。

审计员也要参与其中

这一想法建议审计机构入股 Nexus Mutual 等 DeFi 保险平台。作为利益相关者，如果协议被黑客入侵，审计人员将遭受损失。这种方法将使审计人员和项目的利益保持一致。

给个人的建议

除了智能合约黑客攻击，您还可能面临各种各样的入侵意图。你可以采取一些步骤，可以降低风险和被黑客攻击的几率。

不要给智能合约无限制的授权

与 DeFi 协议交互通常需要你允许智能合约访问并同意使用你钱包中的资金通常，为了方便起见，DeFi 协议要求将默认批准设置为无限，这意味着该协议对您钱包中已批准的资产有无限访问权。

无限制地授权在你的钱包上花费已批准的资产通常是一个坏事，恶性智能合约可能会利用这一点从你的钱包中偷走资金。

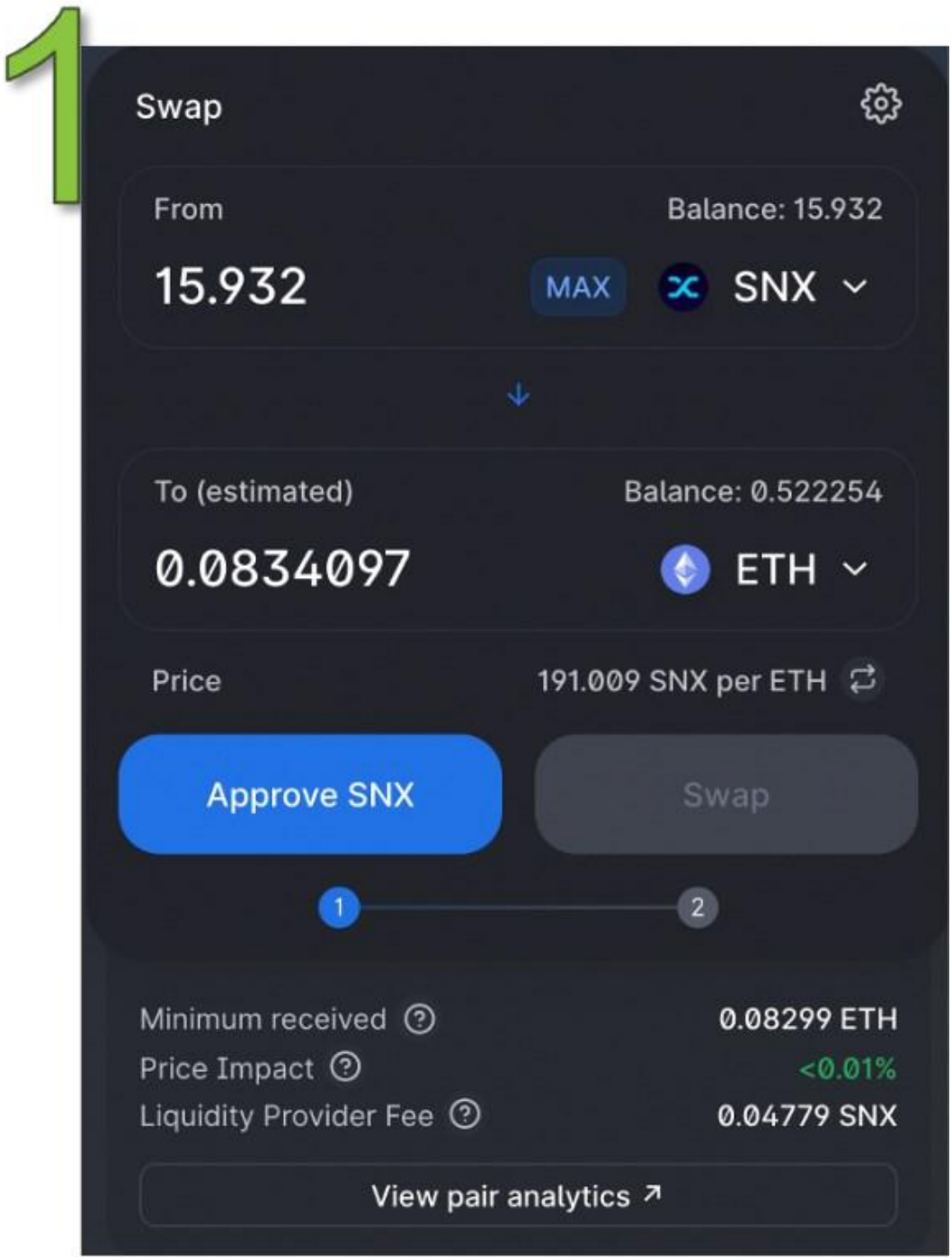
无限制地批准在你的钱包上花费已批准的资产通常是一个坏主意，因为恶性智能合约可能会利用这一点从你的钱包中抽走资金。

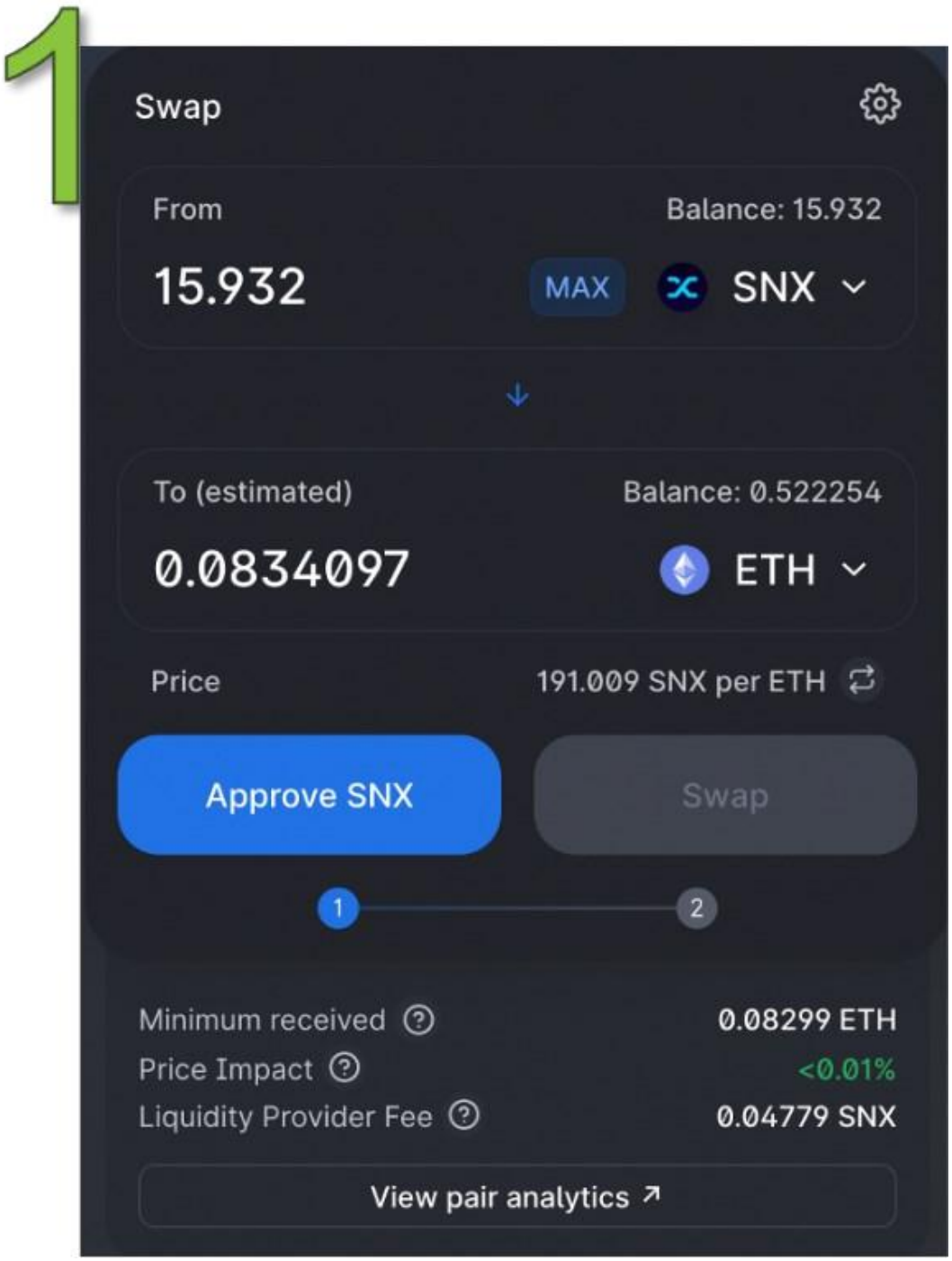
2021 年 2 月 27 日，一名黑客使用虚假智能合约欺骗 Furucombo，让其误以为 Aave v2 有了新的突破。该攻击利用了拥有无限代币许可的大型钱包，通过将资金转移到黑客控制的地址来耗尽这些资金。

这次攻击给 Furucombo 用户造成的损失总计达 1500 万美元。就连借贷协议 Cream Finance 也犯了没有限制的错误，在这次袭击中损失了 110 万美元。

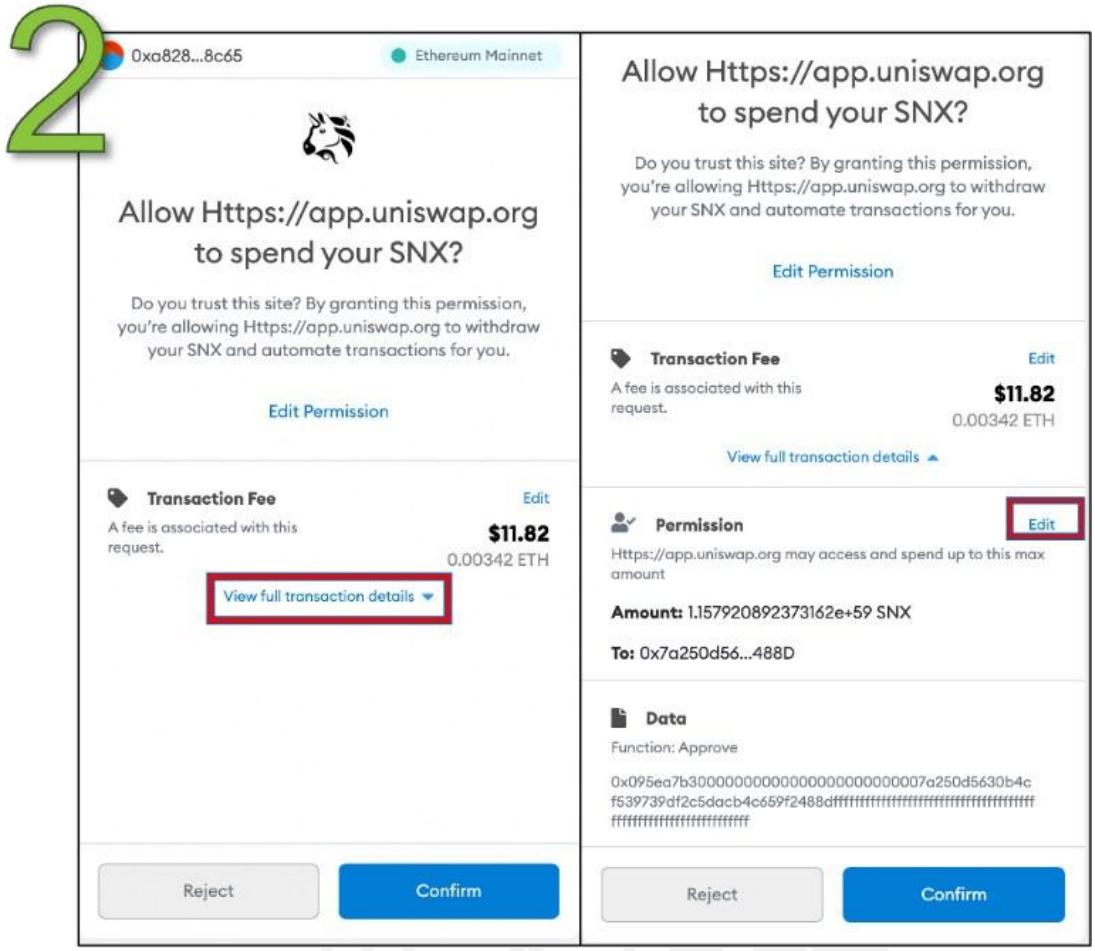
因此，手动更改每笔交易的批准金额是一个好习惯，以防止在代币授权期间给予 DeFi 协议无限的消费许可。尽管这将导致后续的 DeFi 交互产生额外的交易，并导致更高的交易费用，但您可以减少智能合约攻击耗尽钱包里面资产的风险。

要手动更改已批准的数量，请遵循下面的逐步指导。


1
Swap
From
Balance: 15.932
15.932
MAX
SNX
To (estimated)
Balance: 0.522254
0.0834097
ETH
Price
191.009 SNX per ETH
Approve SNX
Swap
1
2
Minimum received
0.08299 ETH
Price Impact
<0.01%
Liquidity Provider Fee
0.04779 SNX
View pair analytics ↗



步骤 1
最常见的需要批准的例子之一是“交换”
我们计划在 Uniswap 上将 15.932 SNX 交换为 0.0834 ETH
点击批准 SNX

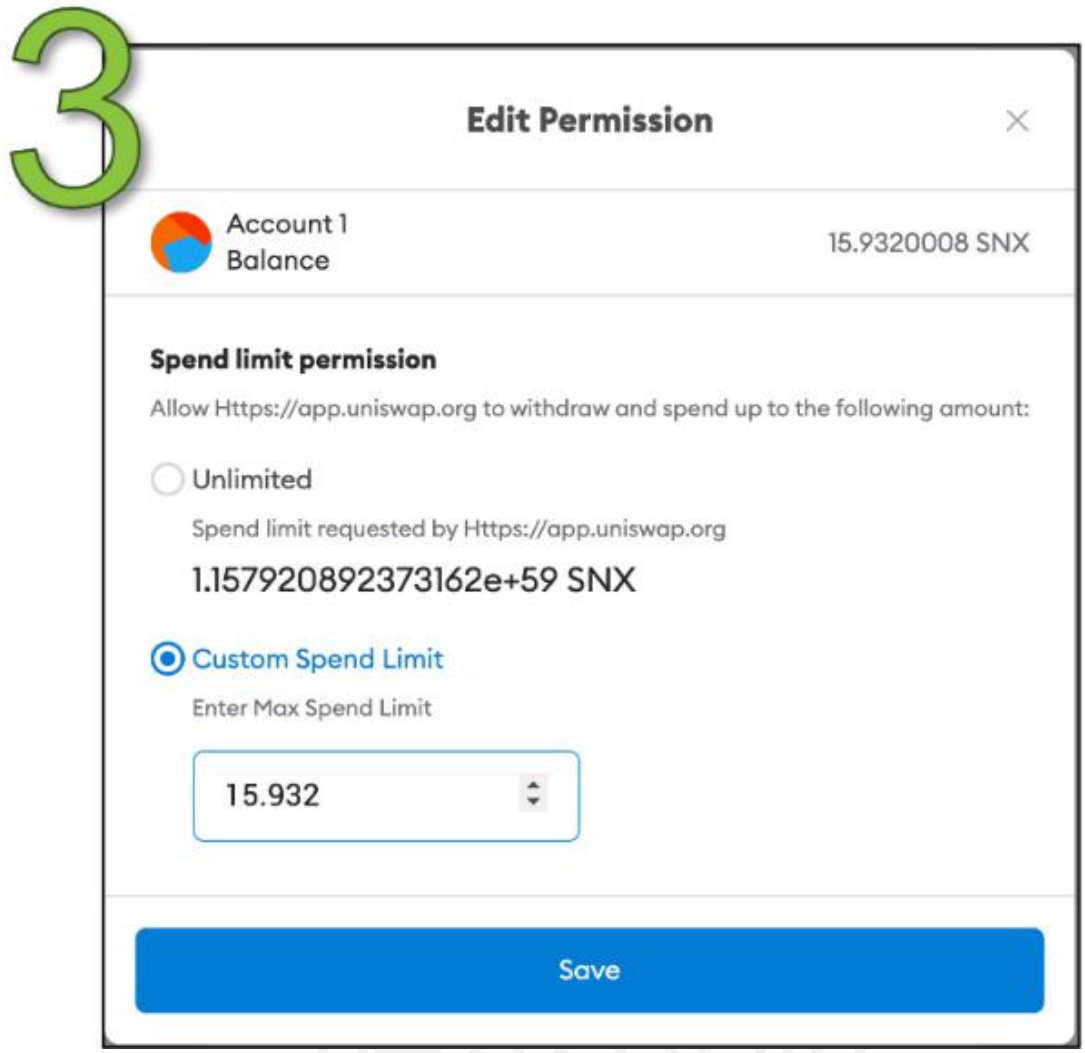


步骤 2

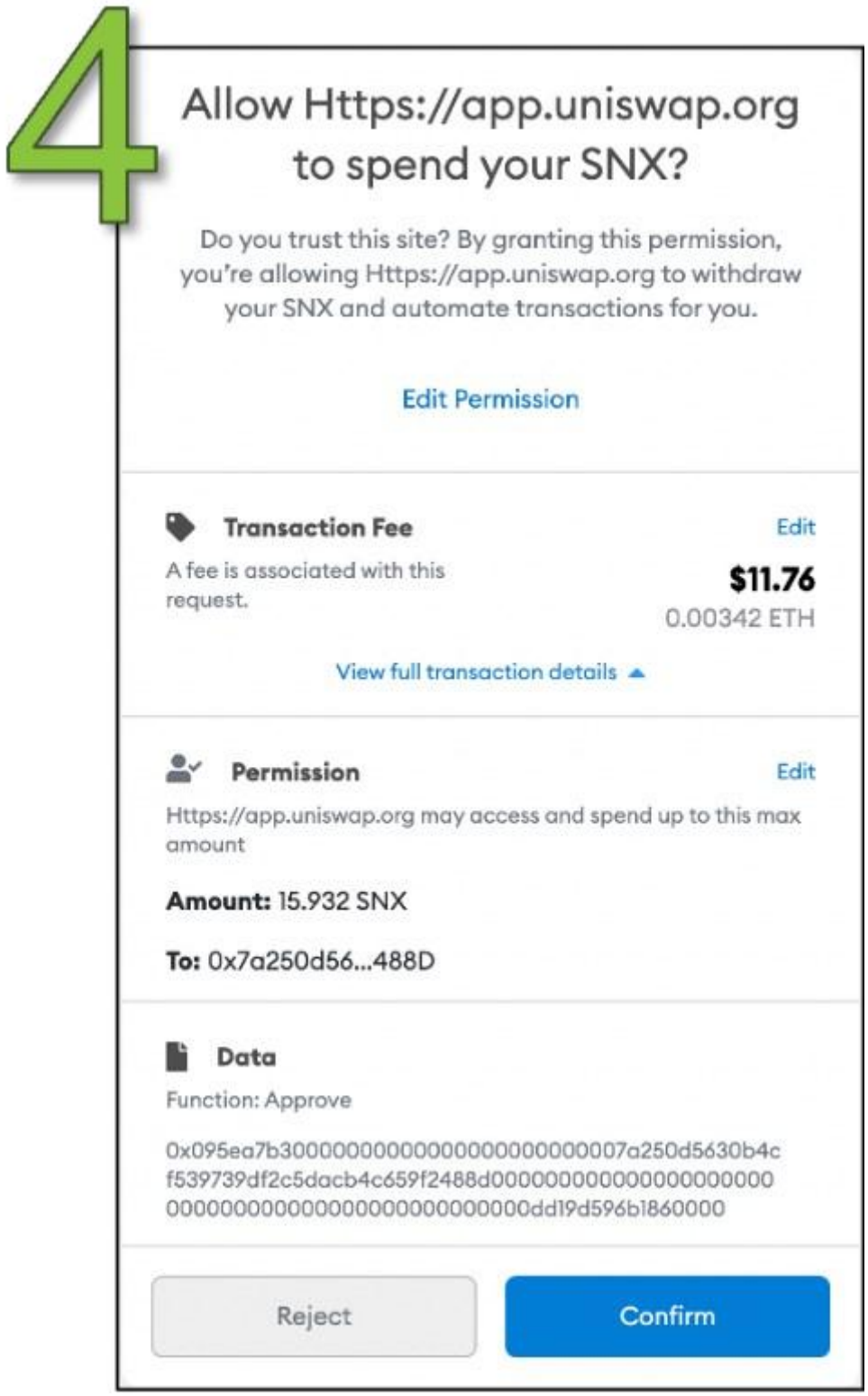
左边的图像是我们将看到的默认窗口

点击查看完整的交易详情（View full transaction details）

我们将看到正确的图像。单击编辑（Edit）



步骤 3
选择“自定义开销限制”（Custom Spend Limit）
很多应用程序默认选择“无限”（Unlimited）选项
输入我们想要花费的金额，在这个例子中，是 15.932 SNX



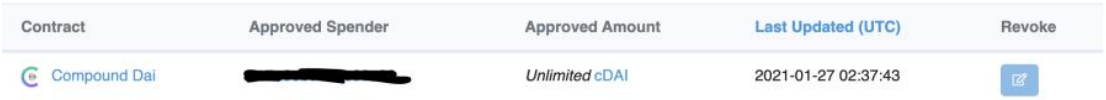
步骤 4
在“许可”（Permission）部分，我们可以看到数字被更新了
单击“确认”（Confirm），支付交易费用

撤销智能合约的无限授权

如果我们之前已经给了 DeFi 协议无限制的支付授权，那么有两个选择：

其中更便捷的选择是将我们的所有资金转移到一个新的以太坊地址，而无需承担与我们以前的以太坊地址相关的任何风险。

但是，如果无法将资金转移出我们现有的以太坊地址，可以使用 Etherscan 提供的代币授权工具查看所有之前的授权信息。



在此页面上，可以看到之前授予智能合约的所有授权。应该撤销所有不受限制的授权数量，尤其是那些不再接触的协议。注意，撤销每个授权本身需要智能合约交互，并将产生交易费用。

使用硬件钱包

硬件钱包是一种单独用于存储加密货币的物理设备。硬件钱包将私钥与联网设备分开保存，降低了钱包被入侵的可能性。

在硬件钱包中，即使硬件钱包感染了恶意软件病毒，私钥也是在安全的离线环境中维护。虽然硬件钱包可以被偷，但如果小偷不知道你的密码，它是无法访问的。最不幸的情况下，你的硬件钱包被损坏或被盗，如果你在丢失之前创建了一个秘密的备份代码，你仍然可以找回你的资金。

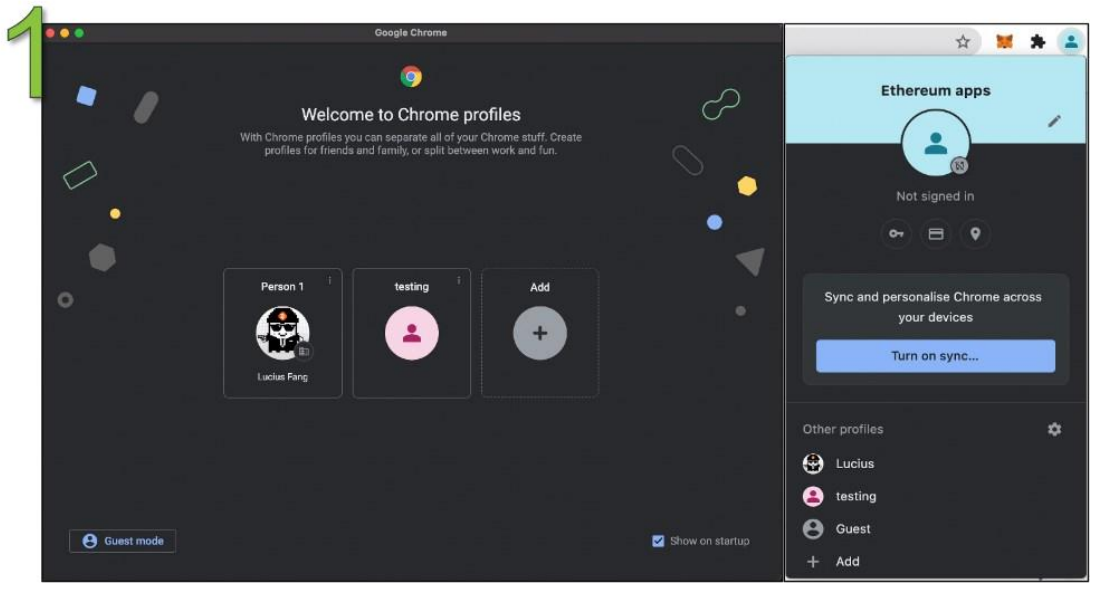
尽管越来越多的制造商已经进入这个行业，但最好的硬件钱包制造商是 Ledger 和 Trezor。

使用单独的浏览器配置文件

尽管浏览器扩展很有帮助，而且在工作中更高效，但始终担心恶意浏览器扩展会给用户加密货币交易带来麻烦。

如果不小心安装一个恶意的浏览器扩展，它可能会窥探 Metamask 密钥，并攻击你的账户资金。有一个方法可以让账户变得相对安全：在谷歌 Chrome 或 Brave 浏览器上创建一个单独的浏览器配置文件。在这个新的浏览器配置文件中，只安装 Metamask 扩展。这样可以减少风险的恶意浏览器扩展坞从钱包窃取资金。

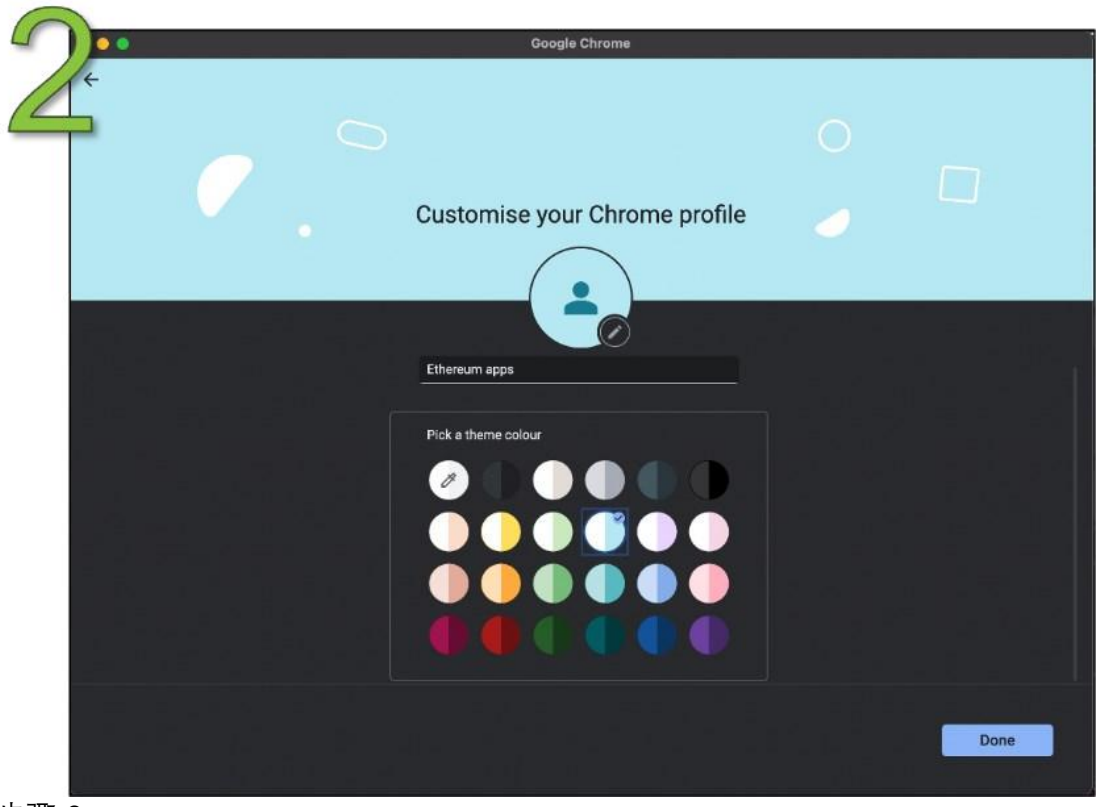
下面是一个在谷歌 Chrome 上安装浏览器配置文件的指南：



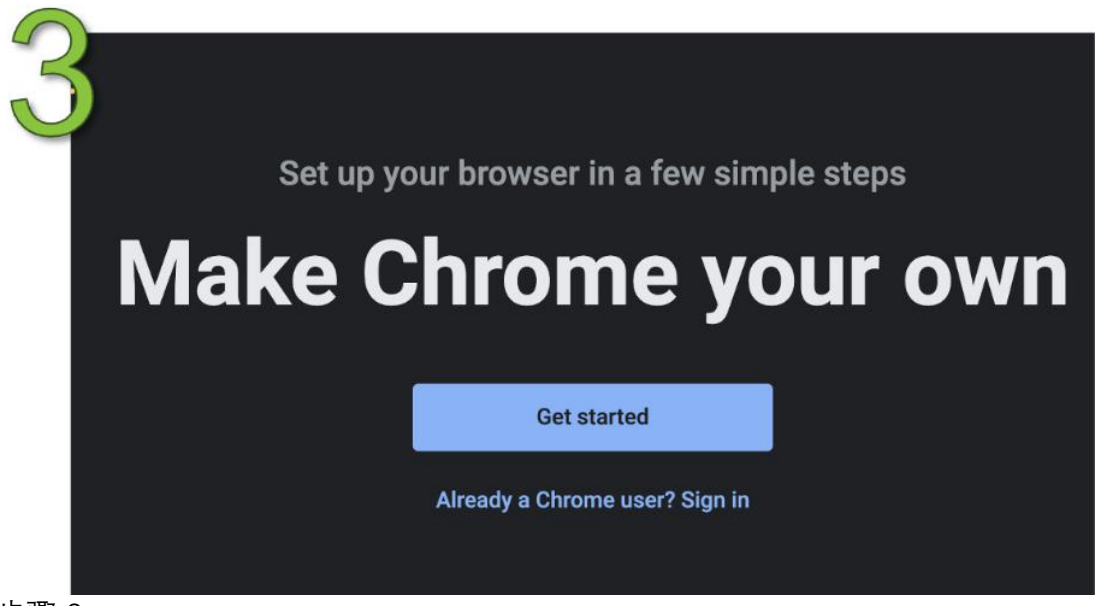
步骤 1

打开 Chrome 浏览器会进入上述页面。单击“Add”

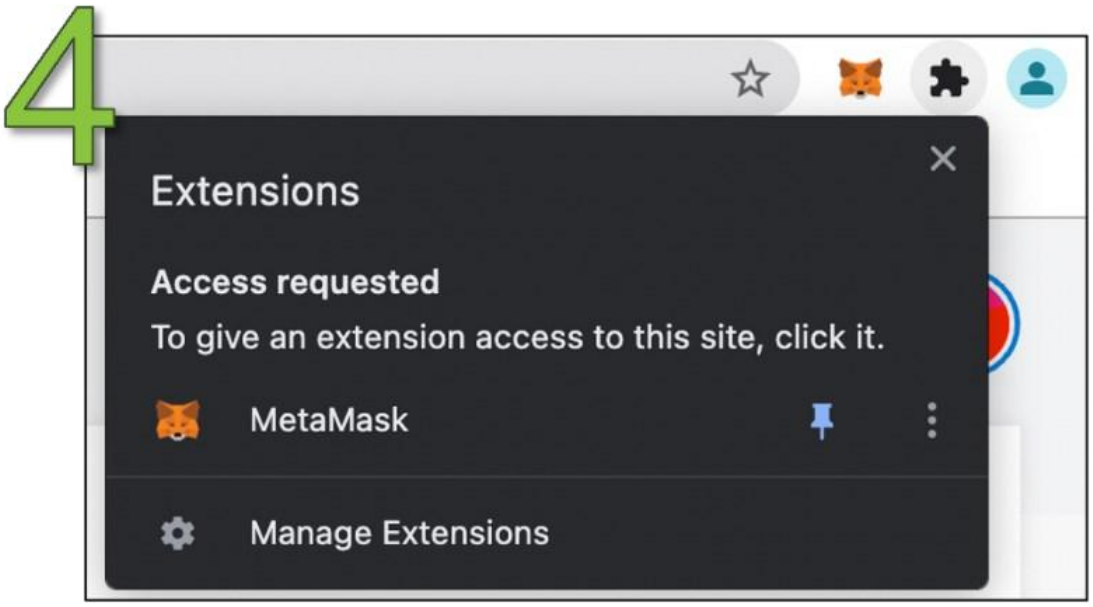
或者，你可以到右上角，点击配置文件图标。点击最底部的“+添加”（+Add）



步骤 2
选择名称和颜色，然后单击完成



步骤 3
登录不同的 Chrome 帐户(如果有的话)
如果没有，请单击“Get started”



步骤 4

下载 Metamask 扩展，并将其作为该配置文件中的唯一扩展。

结论

DeFi 项目在很大程度上仍是各金融项目创新的试验田。因此，万事也有可能出错。一定要注意使用新的 DeFi 应用程序的风险，尤其是那些没有经过实战测试的。

在使用任何 DeFi 协议之前一定要做研究。大多数情况下，一旦出现问题，所造成的损失基本没有追责方式。即使按照协议给予报酬，损失通常也超过所得到的赔偿。

尽管如此，由于涉及的风险较高，参与 DeFi 活动的回报也很高。为了不错失 DeFi 提供的高回报，你可以选择购买保险或看跌期权来对冲一些风险。

DeFi 领域仍在不断成熟。随着我们的探索，我们预计将推出更多的 DeFi 协议，将更好的保障措施和保险资金纳入其运营模式。

第十六章：金融的未来——DeFi

DeFi 的使命是明确的：通过更高的透明度、更强的可访问性、更高效、更便利、更好的互通性，重塑传统金融基础设施和接口。

截至2021年4月，在DeFi领域的总锁定价值 (TVL) 已经到达860亿美元——自我们于2020年三月出版的How to DeFi: Beginner(第一版)至今，总锁定价值已增长了86倍。那时候DeFi的总锁定价值刚刚打破10亿美元。以下是DeFi里程碑的简介摘要：

- 2018年，总锁定价值从5000万美元到2.75亿美元增长了5倍
- 2019年，总锁定价值增长了2.4倍达到了6.67亿美元
- 2020年，总锁定价值增长了23.5倍达到了150.7亿美元
- 2021年，总锁定价值增长了5.5倍达到了860.05亿美元（截至2021年4月）

通过我们“How to DeFi”的两本书，你可以看到DeFi本身正在重新构想全球金融体系的运作方式。正如我们前面所有章节所涵盖的，各种金融原始模型已经存在，如分散的交易所、贷款、保险和衍生品。无论地理位置和社会地位如何，只要他们能够访问互联网，DeFi 都将使世界上的任何人都有可能获得金融服务。

虽然我们涵盖的大多数DeFi协议是基于以太坊上的协议，但是我们已经看到其他区块链上的项目和用户呈指数级增长，比如BSC,Solana,Polygon,Fantom等区块链。
重塑传统金融将不仅局限于科技，还有文化。从本质上说，DeFi代表着一个透明和开源的运动，有着极其强大的文化，继续其创造数万亿美元价值的使命。这种文化是有助于DeFi的塑造与合法化。

人们思维交织碰撞，试图解决困扰传统金融的一些最紧迫的问题。得到的结果结合了传统的金融准则、创新能力和区块链技术，与此同时提供优越的金融产品和服务

还有多久机构才能建立在这些网络上?

我们已经看到了一些基于DeFi成立的机构。例如，Visa在2021年第一季度宣布，它将很快开始在以太坊上与USDC进行交易结算。2021年5月，在进军DeFi生态前，Aave为机构建造了一个私域矿池作为练习场所。它们都是两个金融体系之间合作学习的优秀范例，是机构直接参与DeFi的先驱

接下来的5-10年，DeFi会把世界带到什么样的地步?

很难说未来会是什么样子，但我们愿意把DeFi看作是一种挑战传统金融现状的技术运动。互联网通过彻底改变我们沟通和分享信息的方式，淘汰了许多发明，DeFi将在金融领域利用全球网络创建一个更加透明和高效的金融系统。

新行业的开发需要时间，但DeFi的创新步伐一直在以惊人的速度前进。截至2021年4月，DeFi总锁定价值比四年前（2018年）增长了1700多倍。

我们之所以能走到这一步，最主要的原因之一就是要感谢DeFi的开发者和社区。尽管这个领域的竞争非常激烈，但他们一直在坚持不懈地开发探索，开天辟地。为此，我们想说，感谢你们让开放金融成为可能。

闭幕词

恭喜你走了这么远!从当前的DeFi概览到去中心化交易所再到开发，我们在本书中的DeFi旅程已经结束。然而，这并不是真的结束，因为总会有新的东西需要学习，新的协议需要探索。

到目前为止，您应该对DeFi及其工作原理有了更深层次的理解。你应该知道，DeFi发展非常迅速，而且又是相对复杂的。当我们出版这本书的时候，一些信息可能已经过时了!

不过，我们希望《How to DeFi:Advanced》这本书能成为您正式DeFi之旅的一个核心参考。愿它指引你探索DeFi无数的未知。

附录

CoinGecko's 推荐的DeFi 资源

分析

DefiLlama - https://defillama.com/home
DeBank - https://debank.com/
DeFi Prime - https://defiprime.com/
DeFi Pulse - https://defipulse.com/
Dune Analytics - https://duneanalytics.com/home
LoanScan - http://loanscan.io/
Nansen - https://www.nansen.ai/
Token Terminal - https://www.tokenterminal.com/
The Block Dashboard - https://www.theblockcrypto.com/data

新闻网站

CoinDesk - https://www.coindesk.com/
CoinTelegraph - https://cointelegraph.com/
Decrypt - https://decrypt.co/
The Block - https://www.theblockcrypto.com/
Crypto Briefing - https://cryptobriefing.com/*How to DeFi: Advanced*

时事通讯

CoinGecko - https://landing.coingecko.com/newsletter/
Bankless - https://bankless.substack.com/
DeFi Tutorials - https://defitutorials.substack.com/
DeFi Weekly - https://defiweekly.substack.com/
DeFi Pulse Farmer - https://yieldfarmer.substack.com/
Delphi Digital - https://www.delphidigital.io/research/
Dose of DeFi - https://doseofdefi.substack.com/
Ethhub - https://ethhub.substack.com/
Deribit Insight - https://insights.deribit.com/
My Two Gwei - https://mytwogwei.substack.com/

Messari - https://messari.io/
The Defiant - https://thedefiant.substack.com/
Week in Ethereum News - https://www.weekinethereumnews.com/

播客

CoinGecko - https://podcast.coingecko.com/
BlockCrunch - https://castbox.fm/channel/Blockcrunch%3A-Crypto Deep-Dives-id1182347
Chain Reaction - https://fiftyonepercent.podbean.com/
Into the Ether - Ethhub - https://podcast.ethhub.io/
PoV Crypto - https://povcryptopod.libsyn.com/
Uncommon Core - http://uncommoncore.co/podcast/
Unchained Podcast - https://unchainedpodcast.com/
Wyre Podcast - https://blog.sendwyre.com/wyretalks/home

Youtube

Bankless - https://www.youtube.com/channel/UCAl9Ld79qaZxp9JzEOwd3aA
Chris Blec - https://www.youtube.com/c/chrisblec
DeFi Dad - https://www.youtube.com/channel/UCatItI6C7wJp9txFMbXbSTg
Economics Design - https://www.youtube.com/c/EconomicsDesign
The Defiant - https://www.youtube.com/channel/UCL0J4MLEdLP0-UyLu0hCktg
Yield TV by Zapper - https://www.youtube.com/channel/UCYq3ZxBx7P2ckJyWVDC597g

Bankless 升级指南

https://bankless.substack.com/p/bankless-level-up-guide

我们也喜欢的项目

Dashboard Interfaces
Zapper - https://zapper.fi/dashboard
Frontier - https://frontierwallet.com/
InstaDapp - https://instadapp.io/
Zerion - https://zerion.io/
Debank - https://debank.com/
Decentralized Exchanges

Uniswap - https://uniswap.org/
SushiSwap - https://sushi.com/
Balancer - https://balancer.exchange/
Bancor - https://www.bancor.network/
Curve Finance - https://www.curve.fi/
Kyber Network - https://kyberswap.com/swap
Dodo - https://dodoex.io/

Exchange Aggregators

1inch - https://1inch.exchange/
Paraswap - https://paraswap.io/
Matcha - https://matcha.xyz/

Lending and Borrowing

Maker - https://oasis.app/
Compound - https://compound.finance/
Aave - https://aave.com/
Cream - https://cream.finance/

Oracle and Data Aggregrator

Covalent - https://www.covalenthq.com/
The Graph - https://thegraph.com/

Prediction Markets

Augur - https://www.augur.net/

Taxes

TokenTax - https://tokentax.co/

Wallet

Metamask - https://metamask.io/
Argent - https://argent.link/coingecko
Dharma - https://www.dharma.io/
GnosisSafe - https://safe.gnosis.io/
Monolith - https://monolith.xyz/

Yield Optimizers

APY Finance - https://apy.finance/
Yearn - https://yearn.finance/
Alpha Finance - https://alphafinance.io/

参考文献

Chapter 1: DeFi Snapshot

Bambysheva, N. (2021, March 29). *Visa Will Start Settling Transactions With*
Crypto Partners In USDC On Ethereum. Forbes.
https://www.forbes.com/sites/ninabambysheva/2021/03/29/visa-to start-settling-transactions-with-bitcoin-partners-in-usdc/.
Emmanuel, O. (2021, April 16). Citibank Demystifies MakerDAO and DeFi for Fund Managers. BTCManager.
https://btcmanager.com/citibank-makerdao-defi-fund-managers/.
Franck, T. (2021, March 26). *Fidelity to launch bitcoin ETF as investment giant*
builds its digital asset business. CNBC.
https://www.cnbc.com/2021/03/24/fidelity-to-launch-bitcoin-etf-as investment-giant-builds-its-digital-asset-business-.html.
Kharpal, A. (2021, April 19). *After a bitcoin crackdown, China now calls it an*
'investment alternative' in a significant shift in tone. After a bitcoin crackdown,
China now calls it an ‘investment alternative’ in a significant shift in tone. https://www.cnbc.com/2021/04/19/china-calls-bitcoin-an investment-alternative-marking-shift-in-tone.html.
Manning, L. (2021, April 19). *Coinbase IPO Exceeds All Expectations, Showing*
More Promise For Bitcoin. Nasdaq.
https://www.nasdaq.com/articles/coinbase-ipo-exceeds-all expectations-showing-more-promise-for-bitcoin-2021-04-19.
Schär, F. (2021, February 5). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets.
https://research.stlouisfed.org/publications/review/2021/02/05/dece ntralized-finance-on-blockchain-and-smart-contract-based-financial markets.
Schmitt, L. (2021, April 22). *DeFi 2.0-First Real World Loan is Financed on Maker*. Medium. https://medium.com/centrifuge/defi-2-0-first-real

world-loan-is-financed-on-maker-fbe24675428f.

Chapter 2: DeFi Activities

Cryptopedia, S. (2021, April 17). Airdrops: Crypto Airdrops and Blockchain
Airdrops. Gemini. https://www.gemini.com/cryptopedia/airdrop crypto-giveaway-uniswap.
Etherscan. (n.d.). Airdrops List. https://etherscan.io/airdrops.
Etherscan (n.d) Ethereum Activities Stats. https://etherscan.io/charts.
How to add tokens to SushiSwap Exchange as an LP. SushiSwap. (n.d.). https://help.sushidocs.com/guides/how-to-add-tokens-to-sushiswap exchange-as-an-lp.
Liquidity Bootstrapping FAQ. Balancer. (n.d.). https://docs.balancer.finance/smart-contracts/smart-pools/liquidity bootstrapping-faq.
Xie, L. (2021, March 13). A beginner's guide to DAOs. Mirror. https://linda.mirror.xyz/Vh8K4leCGEO06_qSGx vS5lvgUqhqkCz9ut81WwCP2o.
Zapper: Dashboard for DeFi. (n.d.). https://zapper.fi/dashboard.

Chapter 3: Decentralized Exchanges

Balancer Whitepaper. (2019, September 19). https://balancer.fi/whitepaper.pdf.
Bancor. (2021, February 17). Using Bancor Vortex. Medium https://blog.bancor.network/using-bancor-vortex-46974a1c14f9.
Chainlink. (2020, June 29). DeFi Series: More Capital & Less Risk in Automated Market Makers. Chainlink. https://blog.chain.link/challenges-in-defi-how-to-bring-more-capital and-less-risk-to-automated-market-maker-dexs/.

FAQ. Balancer. (n.d.). https://docs.balancer.finance/getting-started/faq.
Hasu. (2021, April 19). Understanding Automated Market-Makers, Part 1: Price Impact. Paradigm Research. https://research.paradigm.xyz/amm-price-impact.
Kohli, K. (2020, June 1). How AMMs Work (Explainer Video). DeFi Weekly. https://defiweekly.substack.com/p/how-amms-work explainer-video.
Kohli, K. (2020, June 25). The State of AMMs. DeFi Weekly.

https://defiweekly.substack.com/p/the-state-of-amms-3ad.
Kozlovski, S. (2021, March 31). Balancer V2-A One-Stop-Shop. Medium. https://medium.com/balancer-protocol/balancer-v2-a-one-stop-shop-6af1678003f7.
Krishnamachari, B., Feng, Q., & Grippo, E. (2021). Dynamic Curves for Decentralized Autonomous Cryptocurrency Exchanges.
Martinelli, F. (2021, April 19). Balancer V2: Generalizing AMMs. Medium. https://medium.com/balancer-protocol/balancer-v2-generalizing amms-16343c4563ff.
Naz. (2020, February 24). Crypto Front Running for Dummies. Medium. https://nazariyv.medium.com/crypto-front-running-for-dummies bed2d4682db0.
Pintail. (2020, August 30). Uniswap: A Good Deal for Liquidity Providers? Medium. https://pintail.medium.com/uniswap-a-good-deal-for liquidity-providers-104c0b6816f2.
Powers, B. (2020, December 30). New Research Sheds Light on the Front Running Bots in Ethereum's Dark Forest. CoinDesk. https://www.coindesk.com/new-research-sheds-light-front-running bots-ethereum-dark-forest.

Understanding Returns on Uniswap. Uniswap Blog RSS. (n.d.). https://uniswap.org/docs/v2/advanced-topics/understanding returns/.
Uniswap Info DAI/ETH. Uniswap Info. (n.d.). https://info.uniswap.org/pair/0xa478c2975ab1ea89e8196811f51a7b7a de33eb11.
Uniswap. Uniswap Blog RSS. (n.d.). https://uniswap.org/blog/uniswap v3/.
Xu, J., Vavryk, N., Paruch, K., & Cousaert, S. (2021). SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols.
Younessi, C. (2019, March 7). Uniswap-A Unique Exchange. Medium. https://medium.com/scalar-capital/uniswap-a-unique-exchange f4ef44f807bf.

Chapter 4: DEX Aggregators

1inch Network, (2021, March 16). *Introducing the 1inch Aggregation Protocol v3*.

Medium. https://blog.1inch.io/introducing-the-1inch-aggregation protocol-v3-b02890986547.
1inch Network. (2020, December 25). *1INCH token is released*. Medium. https://blog.1inch.io/1inch-token-is-released-e69ad69cf3ee.
Balakrishnan, A. (2021, March 22). *DeFi Aggregators*. Delphi Digital. https://www.delphidigital.io/reports/defi-aggregators/.
Gonella, T. (2021, January 27). *Say hello to 0x v4*. Medium. https://blog.0xproject.com/say-hello-to-0x-v4-ce87ca38e3ac.

Hemricourt, P. de. (2020, August 24). *DeFi, DEXes, DEX Aggregators, AMMs, and Built-In DEX Marketplaces, Which is Which and Which is Best?*
Medium. https://medium.com/2key/defi-dexes-dex-aggregators amms-and-built-in-dex-marketplaces-which-is-which-and-which-is best-fba04ca48534.
Kalani, C. (2020, June 30). *Say hello to Matcha!* Matcha. https://matcha.xyz/blog/say-hello-to-matcha.
Kalani, C. (2020, October 2). *How Matcha is taking DEX aggregation to a whole*
new level. Matcha. https://matcha.xyz/blog/trading-on-matcha-keeps getting-better.
Paraswap. (2021, January 28). *Introducing ParaSwap's new UI & a significant*
upgrade for our contracts. Medium. https://medium.com/paraswap/introducing-paraswaps-new-ui-a significant-upgrade-for-our-contracts-ed15d632e1d0.
Paraswap. (2020, September 17). *Towards a community-owned & driven DeFi*
middleware. Medium. https://medium.com/paraswap/towards-a community-owned-driven-defi-middleware b7860c55d6a6?source=collection_home---6------1----------------------.

Chapter 5: Decentralized Lending & Borrowing

Aave: Open Source DeFi Protocol. Aave. (n.d.). https://aave.com/.
Compound Markets. Compound. (n.d.). https://compound.finance/markets.
Cream: DeFi Lending Protocol. cream. (n.d.). https://cream.finance/.

DeBank | DeFi Wallet for Ethereum Users. DeBank. (n.d.). https://debank.com/ranking/lending?chain=eth&date=1Y&select=borrow.

Lending Protocol Revenue. The Block. (n.d.). https://www.theblockcrypto.com/data/decentralized finance/protocol-revenue.
Maker Market. Oasis.app. (n.d.). https://oasis.app/borrow/markets.
Maker: An Unbiased Global Financial System. MakerDAO. (n.d.). https://makerdao.com/en/.
Protocol Revenue. The Block. (n.d.). https://www.theblockcrypto.com/data/decentralized finance/protocol-revenue.
Token Terminal Dashboard on Lending Protocols. Token Terminal. (n.d.). https://terminal.tokenterminal.com/dashboard/Lending.

Chapter 6: Decentralized Stablecoins and Stableassets

Tether's Credibility And Its Impact On Bitcoin (Cryptocurrency:BTC-USD). SeekingAlpha. (n.d.). https://seekingalpha.com/article/4403640-tethers-credibility-and-impact-on-bitcoin.
Eva, Matti, Koh, N., & Wangarian. (2021, March 20). *Stability, Elasticity, and*
Reflexivity: A Deep Dive into Algorithmic Stablecoins. Deribit Insights. https://insights.deribit.com/market-research/stability-elasticity-and reflexivity-a-deep-dive-into-algorithmic-stablecoins/.
Empty Set Dollar. (n.d.). *Empty Set Dollar - ESD*. Empty Set Dollar - ESD –
Empty Set Dollar. https://docs.emptyset.finance/.
Fei Protocol. (2021, January 11). *Introducing Fei Protocol*. Medium. https://medium.com/fei-protocol/introducing-fei-protocol-2db79bd7a82b.
Float Protocol. (2021, March 22). *Announcing Float Protocol and its democratic*
launch. Medium. https://medium.com/float-protocol/announcing float-protocol-and-its-democratic-launch-d1c27bc21230.

Float Protocol. (2021, March 22). *FLOAT and the Money Gods*. Medium. https://medium.com/float-protocol/float-and-the-money-gods-

5509d41c9b3a.
Frax Finance. *Frax: Fractional-Algorithmic Stablecoin Protocol*. Frax ¤ Finance.
(n.d.). https://docs.frax.finance/.
Ionescu, S. (2020, October 29). *Introducing Proto RAI*. Medium. https://medium.com/reflexer-labs/introducing-proto-rai-c4cf1f013ef.
McKeon, S. (2020, August 12). *The Rise and Fall (and Rise and Fall) of Ampleforth-Part I*. Medium. https://medium.com/collab-currency/the rise-and-fall-and-rise-and-fall-of-ampleforth-part-i-cda716dea663.
Schloss , D., & McKeon, S. (2020, August 12). *The Rise and Fall (and Rise and*
Fall) of Ampleforth-Part II. Medium. https://medium.com/collab currency/the-rise-and-fall-and-rise-and-fall-of-ampleforth-part-ii-6c0f438e8129.
Stably. (2021, February 19). *What Uniswap's Liquidity Plunge Reveals about*
Stablecoins. Medium. https://medium.com/stably-blog/what-uniswaps liquidity-plunge-reveals-about-stablecoins-4fcbee8d210c.
Watkins, R. (2021, March 3). The Art of Central Banking on Blockchains: Algorithmic Stablecoins. https://messari.io/article/the-art-of-central banking-on-blockchains-algorithmic-stablecoins.

Chapter 7: Decentralized Derivatives

dYdX: Leverage, decentralized. (n.d.) https://dydx.exchange/
Hegic: On-chain options trading protocol on Ethereum. (n.d.) https://www.hegic.co/
Opyn: Trade Options on Ethereum. (n.d.) https://www.opyn.co/#/

Perpetual Protocol: Decentralized Perpetual Contract for every asset. (n.d.)
https://perp.fi/.
Perpetual Protocol Exchange. (n.d.) https://perp.exchange/.
Synthetix: The Derivatives Liquidity Protocol. (n.d.) https://synthetix.io/.
Synthetix Staking Page. (n.d.) https://staking.synthetix.io/.
UMA: UMA enables DeFi developers to build synthetic assets. (n.d.) https://umaproject.org/.
UMA KPI Options. (n.d.) https://claim.umaproject.org/.

Chapter 8: Decentralized Insurance

Armor.Fi: Smart DeFi Asset Coverage. (n.d.). https://armor.fi/.
Cover Protocol: A peer-to-peer coverage market. (n.d.).
https://www.coverprotocol.com/.
InsurAce DeFi Insurance. (n.d.). https://landing.insurace.io/.
Nexus Mutual Tracker. (n.d.). https://nexustracker.io/.
Nexus Mutual: A decentralised alternative to insurance. (n.d.).
https://nexusmutual.io/.
Nsure.Network: Experience DeFi, Risk Free. (n.d.).
https://nsure.network/#/home.
Unslashed Finance: The Insurance Products that crypto needs. (n.d.).
https://www.unslashed.finance/.

Chapter 9: Decentralized Indices

Campbell, L. (2020, November 11). The best DeFi indices for your crypto portfolio. Bankless. https://newsletter.banklesshq.com/p/the-best defi-indices-for-your-crypto.
Dune Analytics. (n.d.). https://duneanalytics.com/0xBoxer/indices products.
Governance on Index Coop. Snapshot. (n.d.).
https://snapshot.org/#/index.
Governance on Indexed Finance. Snapshot. (n.d.).
https://gov.indexed.finance/#/ndx.eth/proposal/QmdVmMefXUA UqU1xgfjeUie4o4Ud4cqFKwyABaQSBnQNG9.
Inc., M. S. C. I. (2010). Update on Msci Equal Weighted Indices. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1729770.
Index Cooperative Website. Index. (n.d.). https://www.indexcoop.com/.
Indexed Finance Official Documentation. Indexed Finance. (n.d.).
https://docs.indexed.finance/.
Indexed Finance Official Website. Indexed. (n.d.).
https://indexed.finance/.
McKee, S. L. (2016, July 18). Cap Weighted Versus Equal Weighted, Which
Approach Is Better? Forbes.
https://www.forbes.com/sites/investor/2016/07/18/cap-weighted versus-equal-weighted-which-approach-is-better/?sh=727e63e847c3.

PowerPool Official Blog. Medium. (n.d.).
https://medium.com/@powerpoolcvp.
PowerPool Official Website. PowerPool. (n.d.).
https://powerpool.finance/.

PowerPool. (2021, January 24). PowerIndex v2: Unlimited ETFs & Automated Portfolio Strategies. Medium.
https://medium.com/powerpool/powerindex-v2-unlimited-etfs automated-portfolio-strategies-6086917e6348.
pr0, G2theM, Norsefire, Tai, John, RickieJean, … Noice. (2021, January 30). Oracle Top 5 Token Index proposal. Indexed Finance.
https://forum.indexed.finance/t/oracle-top-5-token-index-proposal/89.

Chapter 10: Decentralized Prediction Markets

Augur. *The Ultimate Guide to Decentralized Prediction Markets*. Augur. (n.d.).
https://augur.net/blog/prediction-markets.
Beneš, N. (2018, April 6). *How manipulation-resistant are Prediction Markets?*
Medium. https://blog.gnosis.pm/how-manipulation-resistant-are prediction-markets-710e14033d62.
Fletcher-Hill, P. (2019, February 7). *A guide to Augur market economics*.
Medium. https://medium.com/veil-blog/a-guide-to-augur-market economics-16c66d956b6c.
Gnosis. (2020, July 5). *Omen and the Next Generation of Prediction Markets*.
Medium. https://blog.gnosis.pm/omen-and-the-next-generation-of prediction-markets-2e7a2dd604e.
Omen Prediction Markets. Omen. (n.d.). https://omen.eth.link/.
The World's Most Accessible, No-Limit Betting Platform. Augur. (n.d.).
https://augur.net/.*Appendix*

Chapter 11: Decentralized Fixed-Interest Rate Protocols

Horizon. (n.d.). https://horizon.finance/#/.
How Tranche Lending Will Bring Fixed Interest Rates to DeFi. ConsenSys. (2021,
February 4). https://consensys.net/blog/codefi/how-tranche-lending

will-bring-fixed-interest-rates-to-defi/.
Introduction. Introduction · GitBook. (n.d.). https://docs.yield.is/.
Rai, R. (n.d.). *Fixed Income Protocols: The Next Wave of DeFi Innovation*. Messari
Crypto News. https://messari.io/article/fixed-income-protocols-the next-wave-of-defi-innovation.
saffron.finance. Saffron. (n.d.). https://saffron.finance/.
Woodward, T. (2020, November 19). *Why Fixed Rates Matter*. Medium. https://medium.com/notional-finance/why-fixed-rates-matter-1b03991275d6.

Chapter 12: Decentralized Yield Aggregators

Alpha Finance Lab. (2021, April 19). https://alphafinance.io/.
Badger Finance: Community Rules Everything. (2020, December 27). https://badger.finance/.
Defi Lego connects as Yearn Finance announces five mergers in a week. Brave New Coin. (n.d.). https://bravenewcoin.com/insights/defi-lego connects-as-yearn-finance-announces-five-mergers-in-a-week.
Harvest Finance. (n.d.). https://harvest.finance/.
yearn.finance. (n.d.). https://yearn.finance/.

Yearn.finance. (2021, March 5). We have decided to end the previously announced merger process of Yearn and Cover. Both protocols will continue to operate independently. yVault depositors who have previously purchased Cover protection are unaffected by this. Twitter. https://twitter.com/iearnfinance/status/1367796331507552258.
Yearn Finance Launches v2 Vaults, YFI Token Jumps 15%. BeInCrypto. https://beincrypto.com/yearn-finance-v2-vaults-yfi-token/.

Chapter 13: Oracles and Data Aggregators

Band Protocol: Secure, Scalable Blockchain-Agnostic Decentralized Oracle.
(n.d.) https://bandprotocol.com/.
BandChain. (n.d.) https://bandprotocol.com/bandchain.
Chainlink: Connect your smart contract to the outside world. (n.d.) https://chain.link/.
Chainlink. (2021, April 30). Chainlink 2.0 Lays Foundation for Adoption of Hybrid Smart Contracts.Chainlink. https://blog.chain.link/chainlink-2-

0-lays-foundation-for-adoption-of-hybrid-smart-contracts/.
Covalent: One unified API. One billion possibilities. (n.d.).
https://www.covalenthq.com/.
The Graph: APIs for a vibrant decentralized future. (n.d.)
https://thegraph.com/.

Chapter 14: Multi-Chain Protocols & Cross-Chain Bridges

An Introduction to Binance Bridge. (n.d.)
https://academy.binance.com/en/articles/an-Introduction-to-binance bridge.
AnySwap Dashboard. (n.d.) https://anyswap.exchange/dashboard.

Binance Bridge. (n.d.) https://www.binance.org/en/bridge.
Chainlist: Helping Users Connect to EVM powered networks. (n.d.)
https://chainlist.org/.
Documentation on Terra Bridge. (n.d.) https://docs.mirror.finance/user guide/terra-bridge.
Terra Bridge. (n.d.) https://bridge.terra.money/.
ThorChain Technology. (n.d.). https://thorchain.org/technology#how does-it-work.

Chapter 15: DeFi Exploits

Etherscan Information Center. (n.d.). https://info.etherscan.com/.
Flash Loans. Aave FAQ. (n.d.). https://docs.aave.com/faq/flash-loans.
Furucombo: Create all kinds of DeFi combo. (n.d.).
https://furucombo.app/.
Immunefi: DeFi's leading bug bounty platform. (n.d.).
https://immunefi.com/.
rekt. (n.d.). https://www.rekt.news/.

Chapter 16: DeFi will be the New Normal

Bambysheva, N. (2021, March 29). Visa Will Start Settling Transactions With Crypto Partners In USDC On Ethereum. Forbes.
https://www.forbes.com/sites/ninabambysheva/2021/03/29/visa-to start-settling-transactions-with-bitcoin-partners-in-usdc.
Bitcoin Headlines. (2021, March 21) Documentation Bitcoin:
https://twitter.com/DocumentingBTC/status/1372919635083923460

Buterin, V. (2020, December 28). *Endnotes on 2020: Crypto and Beyond.*

https://vitalik.ca/general/2020/12/28/endnotes.html.
Cronje, A. (2021, January 12). *Building in defi sucks (part 2)*. Medium. https://andrecronje.medium.com/building-in-defi-sucks-part-2-75df9ee7871b.
stani.eth (2021, May 17). Aave Pro for institutions pic.twitter.com/sUWOFDWcxd. Twitter. https://twitter.com/StaniKulechov/status/1394390461968633859.
Thurman, A. (2021, May 12). DeFi lending platform Aave reveals 'permissioned pool' for institutions. Cointelegraph. https://cointelegraph.com/news/defi-lending-platform-aave-reveals private-pool-for-institutions.

术语表

索引	术语	描述
A	空投	空投是指分配一部分储备代币，通常分配给已经完成某种任务或满足某种标准的用户。
	年收益率(APY)	它指储蓄或投资的年化收益，以一年期为基础计算利息。
	管理员私钥风险	它指的是协议的主私钥可能被破坏的风险。
	算法稳定币	算法稳定币利用算法来控制稳定币的市场结构和经济基础。
	算法稳定资产	与算法稳定币不同，算法稳定资产可以被视为另一种形式的抵押品，而不是账户单位

索引	术语	描述
	自动做市商(AMM)	自动做市商无需人工在订单簿中报价和询价，而是用一种算法代替。
	审计	审计是一个系统的审核过程过程，检查一个代表该组织的记录，以确保公平和信息准确。智能合约审计是指审查智能合约代码，以发现漏洞，以便在被黑客利用之前将其修复。
	应用程序接口(API)	一种充当桥梁的接口，允许两个应用程序相互交互。例如，您可以使用CoinGecko的API在您的网站上获取加密货币的当前市场价格。
B	后台操作	它是指攻击者抢在受害者的交易之前出售代币，从而进行无风险套利的行为。
	买入并持有	这指的是TokenSets交易策略，该策略重新调整其目标配置，以防止对一种货币的过度敞口，并将风险分散到多个代币上。
	桥	一种将两个区块链连接在一起的协议，允许用户在它们之间转移资产。

索引	术语	描述
	债券曲线	债券曲线是定义价格和代币供应之间动态关系的数学曲线。债券曲线起到了自动做市商的作用，当代币供应量减少时，代币价格会上升。它之所以有用，是因为它帮助买卖双方在不需要中介的情况下进入即时市场。
C	加密货币交易所(Cryptoexchange)	它是一个帮助用户交易加密货币的数字交易所。对于一些交易所来说，它们还帮助用户将法定货币交易为加密货币。
	托管人	托管人是指对您的资产拥有控制权的第三方。
	法币抵押型稳定币	一种由法定货币支持的稳定币。例如，1 Tether与1美元挂钩。
	加密货币抵押型稳定币	由另一种加密货币支持的稳定币。例如，代币由Ether按照约定的担保比率提供担保。
	中心化交易所(CEX)	中心化交易所(CEX)是一种以集中式方式运作的交易所，需要对用户的资金进行全面托管。
	抵押品	抵押品是你为了借到另一项资产而必须向贷方锁定的一种资产。它是你偿还贷款的担保。

索引	术语	描述
	抵押比率	抵押品比率是指在将抵押品放入DeFi去中心化应用程序后，您可以借到的最大资产数额。
	cTokens	ctoken是你向Compound的流动性池提供token的证明。
	加密资产	加密资产指区块链上的数字资产。加密资产和加密货币通常指的是同一件事。
	保额	它是指保险公司在提出索赔时应支付的最高赔款。
	索赔评估过程	保险人有义务审查保险人提出的索赔。办理后，保险公司将按投保金额退还被保险人。
	可组合性	可组合性是一种系统设计原则，它允许从组件创建应用程序。
	跨链	发生在不同区块链之间的交易。
D	去中心化金融DeFi)	DeFi是一个生态系统，允许利用金融服务，如借款、贷款、交易、获得保险等，而不需要依赖于一个中心化的实体。

索引	术语	描述
	去中心化应用程序(Dapps)	运行在去中心化点对点网络(如以太坊)上的应用程序。
	去中心化自治组织(DAO)	去中心化自治组织是由区块链上的智能合约编码规则的组织。DAO的规则和交易是透明的，并由DAO代币持有者决定。
	去中心化交易所(DEX)	去中心化交易所(DEX)允许交易和直接交换代币，而不需要使用中心化的交易所。
	衍生品	衍生品来自于派生一词，因为它是一种从基础实体/产品中获得价值的合约。一些基础资产可以是商品、货币、债券或加密货币。
	Dai 储蓄利率(DSR)	Dai Savings Rate (DSR)是长期持有Dai所获得的利率。它也是影响Dai需求的货币工具。
	可视化工具dashboard	Dashboard是一个简单的平台，它将所有的DeFi活动聚集在一个地方。它是一个有用的工具，以可视化和跟踪您的在不同的DeFi协议的资产。
	数据聚合器	索引和聚合数据以便其他去中心化应用程序查询数据的服务提供者

索引	术语	描述
E	Ethereum	以太坊是一个基于区块链技术的开源、可编程、去中心化平台。与比特币相比，以太坊允许使用脚本语言进行应用开发。
	Ether	以太是为以太坊区块链提供动力的加密货币。它也充当去中心化以太坊网络上应用程序的gas
	ERC-20	ERC是以太坊请求评论(Request for Comment)的缩写，20是提议标识符。这是一个官方协议，用于提议改进以太坊网络。ERC-20是指以太坊上用于创建代币的常用标准。
	敞口	敞口指的是你可能面临的投资损失的潜在风险。例如，价格风险是指当价格变动时你可能面临的投资损失风险。
F	期货合约	它指你在未来的某一天以某一价格购买或出售某一特定资产的合约。
	工厂合约	它是一个能够产生其他新的智能合约的智能合约。
	固定利率协议(FIRP)	一种新的具有固定利率元素的协议。

索引	术语	描述
	快速贷款	如果借款人在同一笔交易中偿还了贷款和任何额外的利息和费用，借款人可以接受零担保的贷款。
	领跑单	在加密行业的语境,frontrun（领先单）是尝区块链挑选合适的订单区间,并投入足够的费用来确保订单被执行。
	融资利率	交易员根据资产的永续合约价格和现货价格之间的差额进行的定期支付。
G	燃料费	燃料费（Gas）是指以太坊上执行智能合约操作所需计算工作量的度量单位。
	治理	为了引导DeFi协议的方向，引入了治理机制，可以由项目社区集体决定。为了使这成为可能，最初由Compound开创治理代币，允许代币持有者对任何社区成员提交的协议提议进行投票。

索引	术语	描述
H	硬分叉	区块链的强制分叉，通常在网络的软件代码中实现相当显著的变化时表示。它会导致住区块链永久分裂为两个区块链。原来的区块链不能识别新版本。
I	IDO	IDO是Initial Decentralized Exchange Offering或Initial DEX Offering的缩写。这是代币首次使用DEXs流动性池向公众出售的地方。
	IBCO	IBCO代表初始键合曲线供给。代币价格基于曲线，随后的投资者将推高代币的价格。
	IFO	IFO代表首次农场发行(Initial Farm Offering)。通常，用户用他们的资产换取项目的代币。然后项目收到用户的资产并分发代币。
	IMAP	IMAP是Internet Message Access Protocol的缩写。它是一种Internet协议，允许电子邮件应用程序访问TCP/IP服务器上的电子邮件。
	无常的损失	由于流动性提供者提供的代币对之间的价格差异导致的波动造成的资金暂时损失。
	指数	指数衡量一篮子标的资产的表现。当一篮子标的资产的整体表现变动时，指数也随之变动。

索引	术语	描述
	保险	补偿协议损失提供补偿以换取预付款项的协议。
	反向（Inverse）	Synthetix策略是为那些希望“做空”基准的人设计的。当交易员认为基准价格将下跌时，他们可以购买。
J		-
K	了解你的客户(KYC)	了解你的客户(KYC)是企业实体验证和评估其客户的合规流程。
l	Layer1	每笔交易都在网络上进行结算和验证的区块链。
	Layer2	第2层是建立在基链之上的一个链，以在不损害安全性和去中心化的情况下提高交易可伸缩性。
	清算罚款	当抵押资产的价值低于最低抵押价值时，借款人必须连同清算的抵押物一起支付费用。
	清算率	担保品与债务的比率，在这个比率下，如果你的担保品低于这个比率，就会被清算。
	引导流动性池	项目可以通过可配置的AMM出售代币的流动性池。它们主要用于提高价格发现和减少波动。

索引	术语	描述
	流动性池	流动性池是智能合约上的代币储备池，用户可用于交换代币。目前，这些池主要用于交换、借贷和保险。
	流动性挖矿	是一种奖励计划，发放协议的本地代币以换取资本投入。这是一种新颖的挖矿方式来吸大家参与DeFi协议。
	流动性风险	当像Compound这样的协议可能耗尽流动性时，这是一个流动性风险。
	流动性提供者	流动性提供者是那些把自己的资产借给流动性池的人。随着代币数量的增加，流动性池将会增加。
	资金池聚合器	它是一个从不同的交易所汇集流动性池的系统，并且能够在一个地方看到所有可用的汇率。它可以提供你比较最好的交易价格。
	杠杆	它是一种利用借来的钱来获得更高潜在投资回报的投资策略。
M	MakerDAO	MakerDAO是Maker平台的创造者，DAO代表去中心化自治组织。MakerDAO的原生令牌是MKR，它是稳定币SAI和DAI背后的协议。

索引	术语	描述
	做市商机制	做市商机制(Market Maker Mechanism)是一种利用债券曲线同时给出买入和卖出价格的算法。在加密领域，做市商机制主要被Uniswap或Kyber用于交换代币。
	保证金交易	它是一种通过向经纪人借钱进行交易的投资方式。在DeFi中，借款需要你对资产进行抵押。
	MKR	Maker的治理代币。用户可以使用它对Maker分散自治组织(DAO)的改进建议进行投票。
	铸造	它指的是发行新硬币/代币的过程。
	多链	通常指存在于一个或多个区块链上的协议或代币。
N	节点	在区块链网络中，节点是连接到网络并拥有区块链更新副本的计算机。他们和矿工一起都是网络正常工作的保证。比特币中的节点非常重要，因为它们有助于保持网络去中心化。
O	订单	它是指某一特定资产在不同价格水平上的买卖清单。

索引	术语	描述
	超额抵押	超额抵押是指抵押资产的价值必须高于借入资产的价值。
	期权	期权是一种权利，而不是某人的义务，以商定的价格在到期日或到期日之前购买或出售特定的资产。
	预言机	收集和验证将提供给区块链智能合约的链下数据的服务提供商。
P	远期兑换	允许用户在没有到期日的期货合约上开立杠杆头寸。
	预测市场	预测市场是让参与者对未来事件的结果下注的市场。
	价格发现	价格发现是指通过市场需求和供应等几个因素确定资产合理价格的行为。
	协议	协议是一个底层的代码，它告诉显示数据运作层面的东西。例如，比特币和以太坊区块链有不同的协议。

索引	术语	描述
	点对点	在区块链中，“peer”是指分散网络上的计算机系统或节点。点对点(Peer-to-Peer, P2P)是一种网络，其中每个节点对验证数据具有相同的权限，它允许两个个体直接相互交互。
	永续	它指的是永续期货，是一种没有明确日期的未来购买或出售资产的协议。
Q		-
R	范围约束	该TokenSets策略自动在指定范围内买卖，仅用于熊市或中性市场。
	平衡	它是通过购买和出售投资组合中的资产来维持投资组合中理想的资产配置的过程。
	风险评估员	一个在Nexus Mutual中智能合约做价值质押的人。他/她这样做是为了获得NXM代币的奖励，因为其他用户购买了利害关系与之相反的智能合约保险。

索引	术语	描述
	Rug-Pull	指在加密货币和去中心化金融(DeFi)中，中心化交易所(DEX)流动性池被移除导致了抛售死亡螺旋，因为其他流动性提供者、持有者和交易员纷纷抛售以挽救其持有的资产。通常，这是一种新的退出欺诈形式，有人会耗尽DEX的资金池，让代币持有者无法交易。
S	三明治的攻击	这是一front-running and back-running的组合攻击。“三明治”受害者的交易进行无风险套利。
	智能合约	智能合约是一种可编程合约，允许两方设置交易条件，而不需要信任另一个第三方来执行交易。
	稳定币	稳定币是一种与美元等另一种稳定资产挂钩的加密货币。
	质押	在加密世界中，质押可以意味着各种各样的东西。通常是指在dApp中锁定你的加密资产，或者它也可以指参与PoS(PoS)系统，将你的代币放入区块链，作为区块链的验证者并接受奖励。

索引	术语	描述
	软分叉	由于点对点加密货币网络的去中心化特性，任何更新或更改必须得到所有参与节点的同意。区块链中的这种代码变化通过链分叉发生，当网络实际上分成2个时，每个都遵循不同的规则集。软分叉指的是发生了分叉但旧节点仍然可以参与网络的情况。
	现货市场	现货市场是指资产的买卖和即时交割。
	投机活动	这是一种买卖行为，同时拥有未来获利的预期。
	掉期盈余	当执行价格略好于报价时，掉期交易之间的净正差
	稳定费用	它相当于“利率”，你需要支付连同保险库的主要债务。
	滑点	滑移是订单填写时的预期价格和实际价格之间的差异。它通常是由低流动性造成的。
	Synths	Synths代表合成资产。Synth是具有/具有与另一资产相同价值或效果的资产或资产组合。

索引	术语	描述
	智能合约保险	Nexus Mutal提供的保险，保护用户在存储价值的智能合约中免受黑客攻击。
T	TCP / IP	它代表传输控制协议/互联网协议。它是一种用于互连互联网上的网络设备的通信协议。
	总锁仓值	锁定总价值是指所有DeFi协议的累积抵押品总价值。
	Token	它是数字资产的一个单位。代币通常是指在现有区块链上发行的通证。
	标记	它指的是将事物转换为数字可交易资产的过程
	技术风险	它是指智能合约上的漏洞，可能会被黑客利用，造成意想不到的后果。
	交易对	交易组合是指交易市场上与目标资产配对的基础资产。例如，对于ETH/DAI交易组合，基础资产是ETH，其目标资产是DAI。
	趋势交易	该策略使用技术分析指标，根据已实施的策略，从100%的目标资产转移到100%的稳定资产。

索引	术语	描述
U	利用率	利用率是在传统金融中使用的一个常见指标，在该指标中，您要衡量您的借款额度与借款限额之间的差额。类似地，我们也可以通过度量借款量与贷款dApp中锁定的价值来计算去中心化的贷款应用程序利用率。
V	质押值	它指的是保险公司将对目标风险投入多少价值。如果保险公司持有的价值低于目标风险，则该风险不属于承保范围。
	验证器	与在工作量证明区块链网络上挖掘不同，权益证明区块链网络由专门分布式的验证者的共识保护，这些验证者在验证者节点运行时，就已经在网络中投入了大量的代币。 根据共识算法的设计，验证器根据随机选择、数量(权重)和时间长度(年龄)等组合排队进行块签名。
W	钱包	钱包是区块链网络中可以用作用户和区块链之间的资产存储、交易和交互桥梁。

索引	术语	描述
	包装资产	表示除了本地区块链之外存在于其他网络上的资产。例如，WBTC是存在于以太坊区块链上的比特币的ERC-20版本。
X		-
Y	流动性挖矿	它指的是将数字资产质押或出借以产生回报的行为，通常是其他代币的形式。
	收益聚合器	收益聚合器的诞生是为了满足用户自动化投资策略的需要，免去了他们寻找最佳收益农场的麻烦。
Z	ZK Rollup	第二层扩展解决方案，它让交易捆绑在一起，并在基础链下单独执行。这些解决方案还包括Starkware和Loopring。