原文：《TheProblemswithDeFiCrypto》bylynalden

由GaryMa吴硕区块链

编译

在Luna、Celsius、Voyager、3AC和FTX/阿拉米达倒闭后，许多加密行业分析师表示，DeFi是一个潜在的解决方案。

本文以此观点为线索进行分析。承认DeFi存在一些机会，但也对整个行业的现状做了相当批判性的评价。

此外，本文还涉及到加密货币行业的其他概念，包括Web3、NFT、通用证券等。以及创造加密货币这一更广泛的问题，这种货币除了让创始人变得富有之外毫无用处。

CeFi:不透明杠杆问题

所谓defi的优势，就是技术可以去中心化，为各种交易和杠杆服务增加透明度。。

因此，在讨论DeFi之前，有必要先分析CeFi。

在加密资产行业，两种主要的集中式公司是交易所和存款/贷款机构。单词&quotCeFi&quot主要指后者，但更广义地说，，可以包含两者，特别是因为这两种商业模式可以交织在一起。

交易所允许交易者交换各种加密资产，通常为交易者提供杠杆。

存款/贷款机构(也称为&quot流动性提供者&quot)允许人们存放加密资产并获得收益，允许人们存放加密资产作为抵押借入稳定货币或法定货币，允许一些机构以无担保的方式借入。

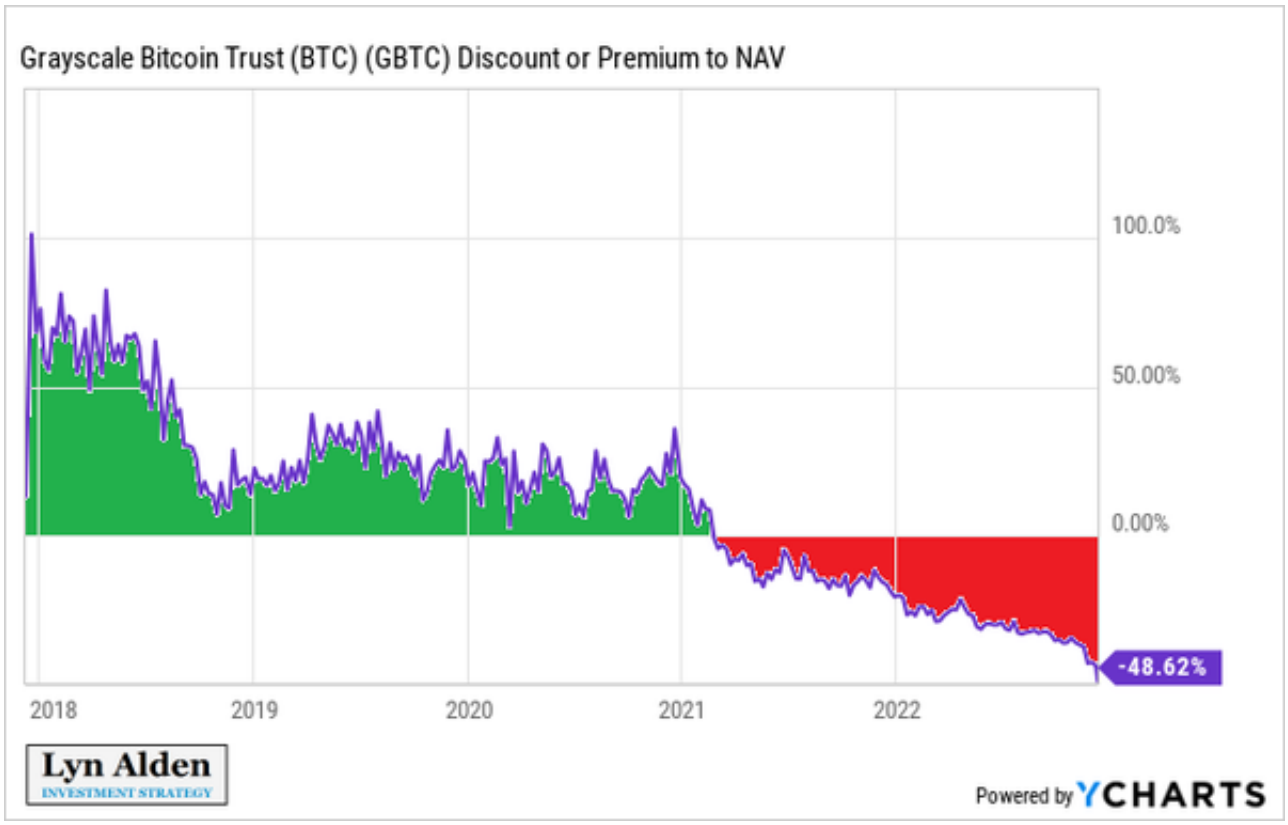
还有其他公司。，比如纯托管，技术开发等。但这两类公司相对与DeFi有关。

遗留金融系统的很大一部分是不透明的。除非公开交易，否则很难确定任何给定实体有多少债务。即便如此，在某种程度上。仍然有可能实施欺诈或使用一些会计技术来混淆细节。

这种趋势一直延续到了CeFi加密货币行业，但势头强劲。各种交易公司和基金经常

利用杠杆来投机加密资产，尤其是假币。。由于这些公司很少公开交易，即使涉及数十亿美元，几乎所有公司都相当不透明。

整个2021年和2022年，行业开始遇到周期问题。。早期的问题始于GBTC从溢价高于资产净值到折价低于资产净值的转变。换句话说，曾经有一段时间。该基金的市场价格是基金中每一美元比特币1.40美元，而现在，基金中每一美元比特币的市场价格不到60美分。



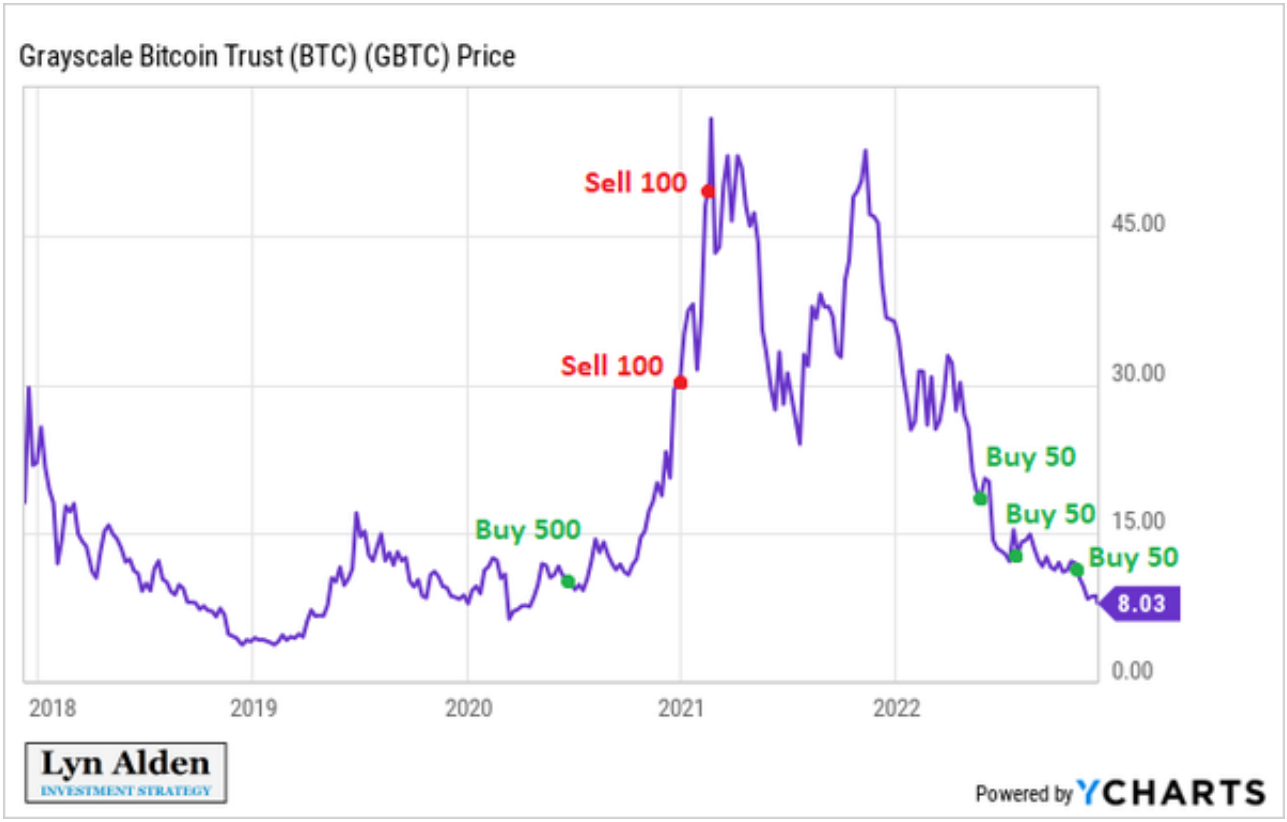
许多交易公司在这一工具上有杠杆敞口，因此这对他们来说是一个比人们可能意识到的更大的问题。

多年来，GBTC是以证券形式接触比特币的少数途径之一。这是许多受监管实体想要的。所以它的交易价格高于NAV，因为它提供了这类证券化组合中难以获得的东西，包括券商账户。

随着越来越多的基金和证券进入市场，为了给这些受监管实体提供比特币价格敞口，GBTC变得不那么独特了，其溢价也消失了。大多数封闭式基金的交易价格相对于资产净值都略有折扣，GBTC也不例外。

我接触比特币的大部分都是直接投资比特币本身(我是通过天鹅比特币买的)。然而，在我的经纪投资组合中，由于缺乏更好的替代品，我使用了少量GBTC头寸来复

制比特币价格敞口。。我不时地重新平衡它的风险敞口，尤其是当它的溢价变得过高时，就像我的无限投资组合：



GBTC不仅是投资组合获取比特币价格敞口的一种方式，也为合格投资者提供了多年的套利交易。他们可以1)做空比特币，2)向GBTC汇款，创建一个带有NAV的新GBTC单位。。他们必须持有这一头寸6个月的锁定期，然后他们可以以高于净值的溢价出售他们的GBTC股票，并平仓他们的比特币空头头寸，以便在不使自己暴露于比特币本身和GBTC价格波动风险的情况下，将高于净值的溢价作为利润。。然后，他们可以一次又一次地重复这个交易。

这种做法持续了很长时间，直到在各种其他受监管的工具中获得比特币敞口变得更加容易。当时，信托没有理由溢价高于资产净值。

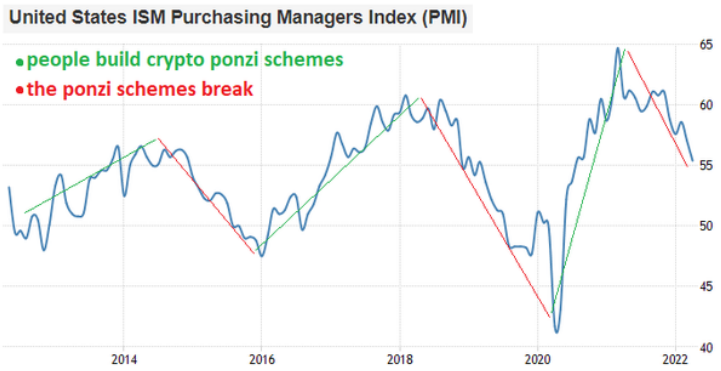
这让许多交易公司措手不及，因为他们被大量的比特币空头头寸和大量的GBTC多头头寸所困，而不是像过去那样溢价交易，而是现在折价交易。换句话说，他们从他们认为的低风险交易中遭受了重大损失。因此，他们的规模和杠杆增加了。

这是第一次打击。

第二次打击是Terra/Luna的雷暴。这从一开始就是一个庞氏骗局。。相关人员以不

可持续的20%收益率人为吸引散户。我在2022年4月和5月高点附近警告过Terra/Luna。然后在2022年5月，他写了一篇题为&quot数字炼金术&quot。

事后分析的主题之一是，当流动性和整体商业环境改善时，加密庞氏骗局往往成立，而当流动性和整体商业环境恶化时。



加密庞氏骗局经常被曝光破：

很多杠杆交易公司都有露娜的曝光，这让加密行业后续的爆发比我当时想象的要严重。对于很多人来说，最大的惊喜是3AC的倒下，这是受GBTC打折的影响。然后受到了Luna崩溃的打击，3AC战队一直特别看好Luna。

三建资本是一家成立十年的大型加密货币交易公司。他们使用的杠杆比大多数人意识到的要高得多，因为它是不透明的。他们悄悄地从许多不同的渠道借钱，其中不&#039；没有必要互相交流。包括Voyager和Genesis在内的许多贷款机构向3AC提供了巨额无担保贷款。BlockFi也有巨额贷款给3AC。但它是抵押的，这减少了对他们的总影响。Celsius和其他数十家公司也向3AC提供了贷款。

所以，3AC的倒闭导致了大量加密贷款行业的倒闭，只有少数几家还站得住脚。。这一领域的总体风险管理很差，尽管有些情况比其他情况好。许多贷款机构只向像3AC这样的少数大型借款人提供贷款。

我在2021年初探索了CeFi平台，了解生态系统。。早在2021年2月，我就在一篇文章中支持BlockFi作为稳定货币收益率、黄金代币收益率等新生事物的一小部分。我强调了它的风险以及存款不受联邦存款保险公司保险的事实。建议一个人最多只放一小部分资产在上面，大部分资产自己保管。然而，一年后的2022年2月，在BlockFi和整个行业还在正常运营的时候，我撤回了我的代言。因为我不再认为风险/回报是值得的。

与许多贷款机构不同的是，BlockFi在2022年5月/6月的加密货币贷款机构倒闭中成功幸存，而其他CeFi存款/贷款机构，比如Celsius和Voyager失败了。BlockFi避免了集中发放无担保贷款，这至少将对其偿付能力的影响降至最低，并为他们提供了

一种继续处理提款的方式。并在投资者的支持下继续运营。

然而，BlockFi随后在2022年6月与FTX/阿拉米达合作，提供流动性供给和要约，决定了他们的命运。。2022年11月FTX/阿拉米达倒闭后，BlockFi不得不停止处理提款，并加入了大多数其他存款/贷款机构。

一般来说，CeFiindustry最大的损失来自1)向资产负债表不透明的杠杆实体提供无担保贷款，或者2)为资产负债表不透明的杠杆实体托管资产。当然，不透明的资产负债表的问题在于，很难确切知道它们有多少杠杆。，尤其是在一些涉及公然欺诈的案件中。

DeFi的目标是什么？

DeFi漏洞的风险无处不在

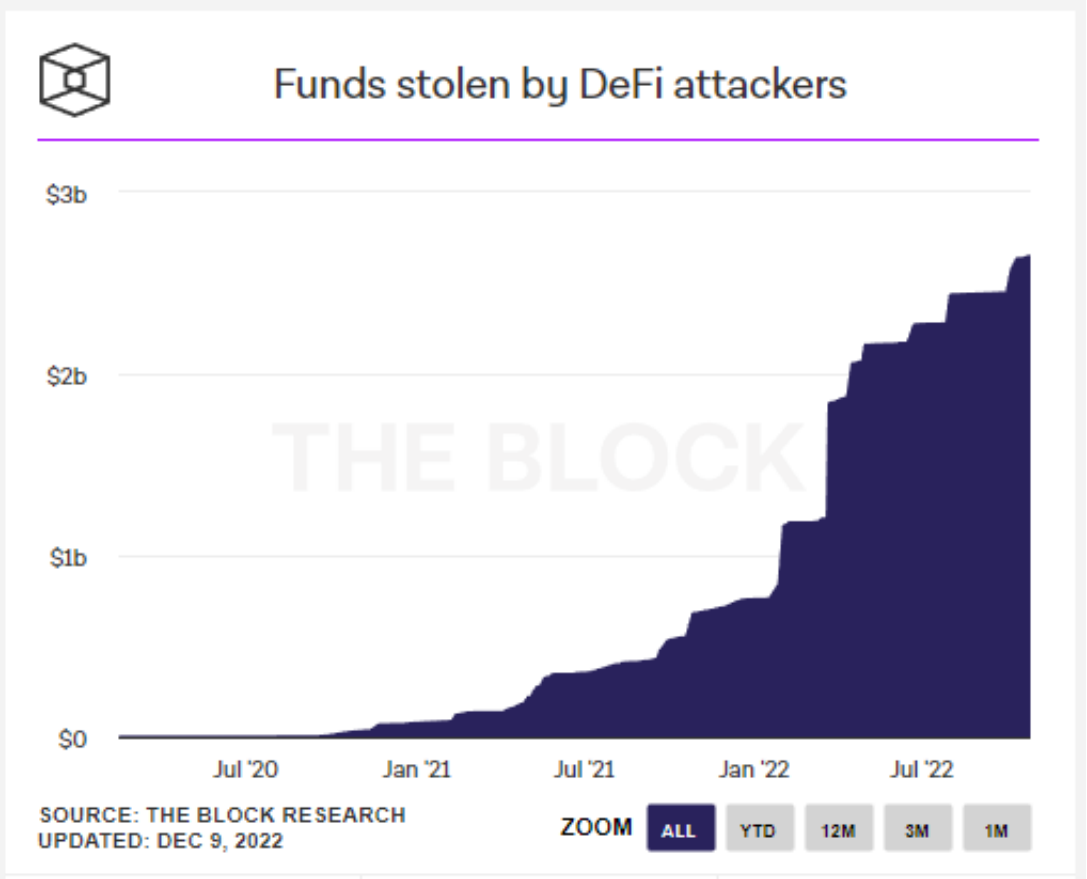
DEFI提供了一些透明的好处，但也为黑客提供了巨大的攻击面。。这些通常被称为&quotDeFi黑客&quot他们中的一些人已经想出了如何从智能合同中偷钱。其实与其说是黑客攻击，不如说是把它们当成剥削或者套利的机会。

&quot；法典就是法律&quot是DeFi&#039早期。如果智能合同存在漏洞，那么就有人可以利用，他们就有可能获得优势，甚至包括在合同中以意想不到的方式获取资产。这类似于一份写得很差的真实合同。聪明的律师可以找到漏洞，帮助客户以书面和无意的方式滥用合同。毕竟，如果代码不是智能合约的最终仲裁者，那么智能合约的意义何在？

比特币网络是最精简的区块链，已有近14年的历史。。就是故意简单，故意慢改，故意抗拒改，除非在压倒性共识的情况下。尽管如此，比特币网络在过去几年中仍然遇到了一些严重的漏洞。

那么，千变万化、高度复杂的智能合约的希望在哪里？？任何持有DeFi或其他智能合约资金的人都应该假设，代码总是有被利用和资金损失的风险。你得到了3%的收益？那&#039；太棒了。将其与一年中任何时候100%亏损的可能性进行权衡。然后年复一年重复这个过程。当来自不同区块链或不同层面的智能合约相互作用时，风险将被放大。

在过去两年半的时间里，超过25亿美元的加密资产从智能合同中被盗：



有抵押vs无抵押：这是关键

许多DeFi支持者指出，2022年大多数CeFi贷款机构破产，DeFi合同继续运作。

虽然这话有一定道理。但是要看根本原因：房贷。提供全额抵押贷款的CeFi贷款机构通常表现良好。如果他们不得不清算客户，破产的是客户，而不是贷方。。当CeFi贷款人向他们认为值得信赖的实体提供无担保或无担保贷款时(这些实体随后押注于DeFi，如LUNA，并且无法偿还贷款)，问题就出现了。

由于DeFi的自动性质，不过度抵押，很难有意义地完成。因此，就其本质而言，DeFi主要由过度抵押的杠杆构成。这里的教训不是DeFi比CeFi好；但是当涉及到不稳定的资产时过度担保贷款比担保不足或无担保贷款更安全。

在DeFi环境下，储户主要面临抵押贷款的风险(就贷款而言这是好事)，但也面临智能合约被盗的持续风险(这是坏事)。。在CeFi环境下，存款人可能会有一些抵押贷款和非抵押贷款的混合风险(这是一件坏事)，但他们对漏洞有更大的保护(这是一件好事)。

我从2022年的加密行业事件得出的结论并不是DeFi比CeFi好。

相反，在我看来，对于这些波动性很大的资产，追逐收益率是不明智的。就审慎贷款而言，你应该选择超额抵押。

比特币为用户提供了自行保管有限流动性资产的能力，可以使用该资产发送或接收未经授权的支付，而无需依赖集中式第三方。在我看来，这是噪音中的信号。它比许多人意识到的更强大。

在难以获得美元的发展中国家，在储蓄和支付中中期使用稳定的货币是另一个很好的公用事业用例。一般来说，他们应该意识到交易对手的风险。我希望看到稳定的货币抵押品越来越透明。

几乎所有其他事情都涉及投机，或在滚筒前捡硬币(收益)(不透明的交易对手风险和/或代码漏洞)。事实上，我花了一年时间，甚至一点钱。我认为在崩盘前就停止投资是一个错误。

DeFi&#039；的集中缺点

除了包括DeFi子行业在内的加密行业的周期性、投机性和有时完全欺诈性之外，这种技术的核心还是有中心化的问题，虽然市场上标榜的是去中心化。

智能合约平台的中心化

与去中心化的比特币网络相比，DeFi技术栈的基础是底层智能合约区块链。，已经从一些集中的方面开始了。

比如以太坊网从2015年成立到2022年PoS转换，代码中有超过7年的难度炸弹。这降低了矿工和单个节点操作员的权力。它强化了头部开发者的权力，这是一种集权的形式。它允许他们推进路线图，并根据他们的愿景修改协议，这基本上使其成为一份投资合同。即使在2022年PoS转换之后。，网络用户仍需等待开发商实施PoS提现。

同时，如果有问题，Bi&#039安几乎可以要求链家停牌，今年10月6日至7日就是这么做的。理论上，BNB链是一个独立于集权公司的分权系统，但实际上：

同样，2022年Solana意外下线5次时，验证者操作员不得不通过Discordmeeting手动重启链。

很多PoS链都是这样工作的。。技术或资本成为验证者的要求相当高，最终导致系统运营的寡头垄断。

与工作量认证协议不同，权限认证协议没有不可伪造的账簿历史，因此如果系统有意或无意地宕机，确定合适的检查点在哪里以及在哪里重启网络是一个相当手动的过程。因为创建几乎无限数量的备选历史是免费的，所以每个历史似乎都是有效的。因此，没有不可伪造和自我验证的方法来确定&quot真实&quot权益认证系统中的账簿历史(这是工作量认证的具体作用)，所以需要信任某个权限或某组权限才能使用权益认证检查点。

这就是为什么像BabylonChain这样的项目允许PoS链在比特币区块链中插入不可伪造的时间戳。它试图通过使用占主导地位的工作量认证制度来缓解权益认证制度固有的一些循环问题。。他们使用比特币网络作为检查点权限。

除了集中难度炸弹，集中开发者决策，集中验证和/或集中检查点权限，还有一个简单的问题。在大多数情况下，智能合约区块链节点太大。

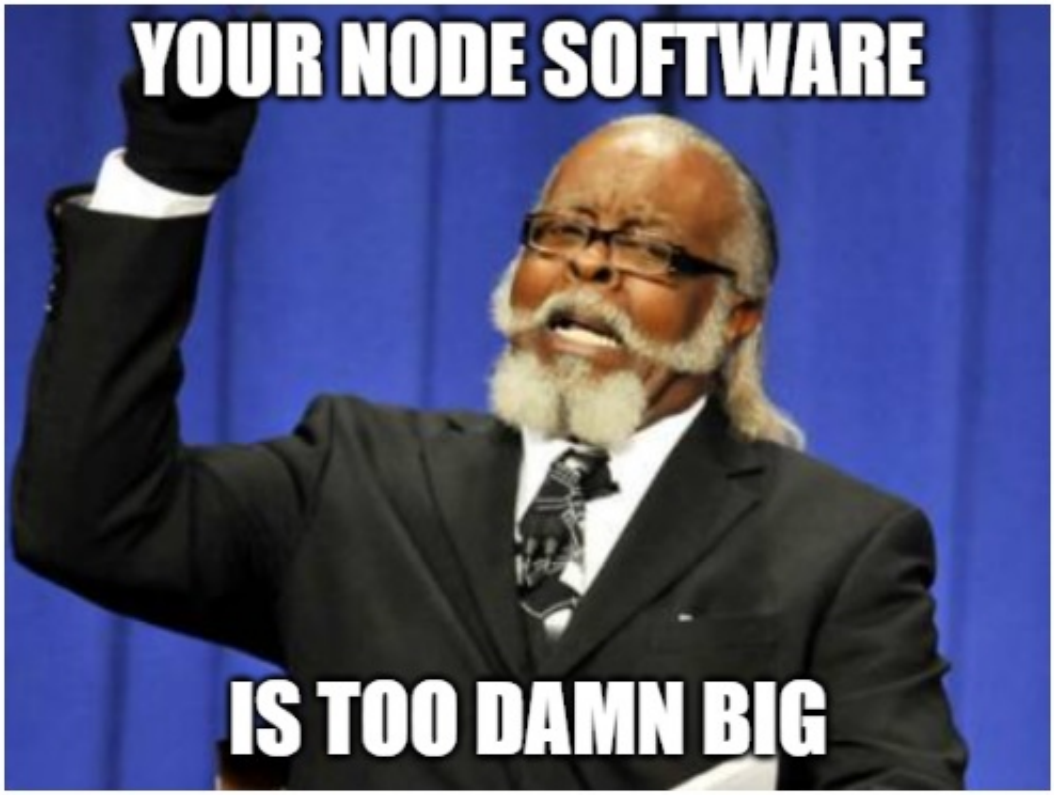
当用户运行他们自己的节点时，或者如果他们需要，至少有实际的选择时，最好的区块链隐私和去中心化出现。这允许他们自己验证网络的所有方面并自己发起交易

，而不是要求第三方为他们发起交易。。

但是，它通过在协议基础层增加更高的吞吐量或更高的代码表达能力，增加了运行节点的处理、存储和带宽要求。例如，运行Solana或BSC节点。，需要企业级设备或者使用云提供商。

以太坊的节点比Solana或者BSC的要轻，但是还是太大了，无法在Tor上运行。根据ethernodes.org&#039s数据目前以太坊节点只有6700个左右。其中，超过4400个由提供商(通常是云服务)托管，其中2700个通过亚马逊托管。非托管节点只有2300个左右。

大多数用户和应用依赖于第三方节点运营商，如Infura和Alchemy(他们自己也大量使用云提供商)。。2022年8月，当美国财政部制裁专注于隐私的智能合约Tornado Cash时，Infura和Alchemy遵守了规定，停止处理与TornadoCash相关的交易。。这意味着许多外国人，包括那些甚至没有受到美国制裁的人，都无法使用TornadoCash，除非他们愿意运行自己的以太网节点，这并不容易做到，也无法通过Tor运行。



恰恰相反，中本聪发明比特币的时候，故意牺牲带宽和复杂度，让它尽可能的小，简单，去中心化。

这使得个人用户可以在正常互联网连接的笔记本电脑上轻松运行比特币节点。。运行节点的需求比处理、存储和互联网带宽的技术提升要慢得多，所以随着时间的推移，运行比特币节点变得更容易而不是更困难。比特币网络从一开始的目标就是去除一切不必要的脂肪，尽可能保持轻量。

托管资产的集中化

除了DeFi行业所依赖的底层智能合同区块链的一些集中化方面之外，实际的DeFi使用案例通常更依赖于集中化的实体。

大多数DeFi的总锁定价值取决于集中托管稳定货币和其他集中托管资产。在伪去中心化的存贷款协议中，稳定币占贷款的很大一部分，稳定币是伪去中心化交易所中常见的交易对。

由法定货币担保的稳定货币，如USDT或USDC，是一种集中发行者，以银行存款、国库券、回购协议、商业票据或类似类型资产的形式持有资产，并发行可在区块链交易的可赎回的象征性负债。换句话说有一个集中的发行人来管理抵押品和处理赎回，但负债是持有人的数字无头资产，因此交易可以在人与人之间有效地自动进行，而无需集中的发行人采取进一步的行动。然而集中式发布者仍然可以根据执法机构的要求或由于各种代码利用而选择主动冻结特定地址。

除了严重依赖稳定币的集中保管，以太坊的DeFi还使用了大量封装的比特币&quot WBTC&quot；。这是被管理产品。比特币是受管理的，其代币债务可以在以太坊区块链进行杠杆交易或交易。以太坊的托管比特币数量可以和最大的密码交易所持有的托管比特币数量相媲美。非常类似于稳定的货币，这是一个中央集权的产物。，其负债是不记名资产。以太坊里可能发生的最糟糕的事情已经发生在索拉纳身上了。Solana上有封装的比特币和以太坊，允许这些资产在Solana生态系统内进行杠杆交易或交易。。但问题是，FTX是这些资产的发行人，而现在FTX已经破产了。因此，这些托管资产与美元脱钩，几乎失去所有价值：

合成稳定币的尝试

一些稳定币开发者试图摆脱对集中发行者和托管者的依赖。毕竟，如果大多数资产的价值在&quot分散财政&quot协议完全集中，这个术语合适吗？

比如前几年马克道推出的阿呆，原本是以太坊担保的合成稳定货币。这意味着戴不能像或那样兑换成实际的美元，而是由过度抵押的以太坊支持。，并用稳定性算法来平衡，来表示一美元。

法币是集中管理的账簿。。试图将伪分散的账本(如加密抵押贷款的稳定货币协议)与主动管理的集中账本(如美联储系统)联系起来，总会带来各种限制和风险。在这种情况下，使用易变资产作为抵押品。意味着抵押物突然出清的可能性相当高。突然平仓很可能发生在市场动荡时期，导致链条拥堵，交易成本极高，因为太多人同时争夺退出，引发太多平仓，网络无法正确处理。

2020年3月，在疫情导致全球市场崩溃，各经济体陷入封锁的时期，以太坊价格暴跌。在紧急情况下，颇具讽刺意味的是，马克尔道投票决定增加中央集权的法定货币抵押稳定货币作为戴的抵押品。这是因为加密抵押贷款的稳定货币(基本上是试图用高波动性资产支持低波动性资产)要么本质上是脆弱的。要么是资金效率低。此后，一直是戴的大比例抵押品。如果政府要求的话，可以冻结戴&#039；的抵押品，并基本上随时结束项目。

为了具有足够低的清算概率，加密抵押的稳定货币需要足够高的超抵押率。简单来说，如果你希望稳定的货币在抵押品减少75%的情况下避免清算，那么你需要4:1的超额抵押品。如果你想在抵押品减少90%的情况下稳定货币以避免清算你需要10:1的超额抵押品。

如果以这种方式处理，这将是极其低效的资本，因此大多数协议都会试图绕过这些，依靠激励机制在需要时从社区引入更多抵押品，而不是一直留在那里。

例如，较新的加密抵押贷款稳定硬币，如Liquity和Zero，旨在通过激励机制实现100%加密抵押贷款。流动性&quotLUSD&quot；是以太坊抵押的。，Zero“ZUSD&quot；是比特币网络RSK的侧链上的一个分支，由RBTC抵押，是RSK开采的比特币的联邦包装版本。

集中式Oracle

将数字资产与真实世界的信息相链接涉及一个集中式的Oracle机器，或多个集中式Oracle机器的法定数量，以试图分散Oracle机器的读数。Oracle是智能合同执行其功能的信息源。例如

将加密资产与美元绑定意味着智能合约需要知道加密资产的美元价格，这意味着它需要来自交易所的信息。

同样，智能体育博彩合同需要一个外部真实来源来从现实世界的体育比赛中收集信息。通过这种方式，智能合约可以将利润奖励给获胜的投机者。

这种对一个或多个预测因子的依赖性代表了另一个集中点。谁控制着先知？操纵一个给定的甲骨文或一组甲骨文并侵入合同有多容易？

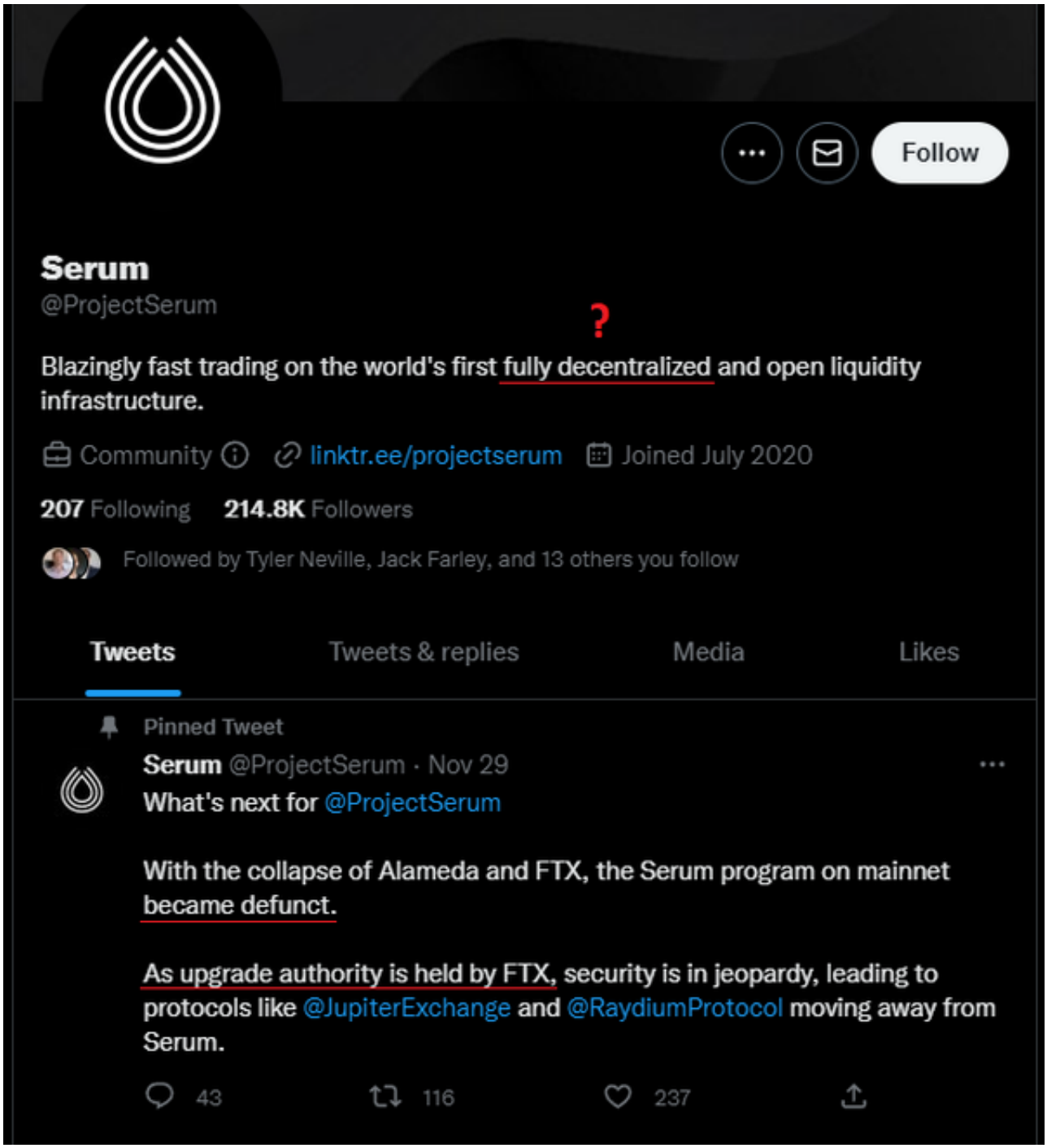
集中治理运营

许多存款/贷款协议和交易协议都有基于web的集中用户界面和支持它们的集中公司。底层技术可能是开源的，没有它们也可以访问(用户需要运行节点)，或技术上的

动手操作)，但对于大多数用户来说，基于web的用户界面是他们访问服务的方式。

这些集中化的公司和界面有从其交易或杠杆环境中删除某些令牌的先例。应政府要求或为了避免违反证券法。

这些系统中有许多比它们看起来更集中的控制。例如，正如詹姆森洛普本月早些时候指出的那样。DeFi协议名为Solana区块链上的血清，在其Twitter个人资料和其他地方宣传自己是完全分散的，但有一条置顶的推文讲述了它如何因其个人资料下的集中控制而失败。



如果一个集中实体有升级权限，怎么会被认为&quot完全分散&quot？

许多协议试图通过使用治理令牌打破对服务的控制来回答这个问题。。无论初始令牌是发放给用户还是空投给用户，这些令牌都可以分发，并允许对与服务操作相关的各种治理操作进行投票。这些同样的令牌也可以从协议产生的利润中分得一杯羹。

虽然这在理论上很有意思，但是从几个问题开始。

首先，与加密领域的大多数事情一样，绝大多数治理令牌由whale公司持有，这意味着少数富裕实体保留了投票权的控制权。第二，投票率往往很低，这使得高度活跃和积极的政党在实践中对协议的治理有更大的控制权。

第三，因为它是匿名的，这些治理模式往往比现实世界的民主更容易被玩弄。。投票支付，实体秘密控制比市场意识到的更大的治理份额，以及其他问题，使其难以以真正分散的方式运作。

以太坊联合创始人VitalikButerin最近提出了与Token治理相关的经济问题，我同意他的观点：

。

因此，经常性利润或许能够支撑Token的价值，但仅靠治理不足以保持Token的可持续发展。无论它们是否盈利，在实践中都可能受到中央控制。

总之，随着时间的推移。DeFi协议可能会面临更严格的审查和监督。由于他们有如

此多的集中攻击面，监管机构不难禁止他们，降低他们的可用性，提高他们的可追溯性。就DeFi生态系统而言，其区块链节点主要运行在集中式云提供商上，其大部分锁定价值严重依赖于集中式托管人。用户主要通过集中式公司维护的集中式web界面与生态系统进行交互。

DeFi没有解决法币存款瓶颈

Defi行业的人倾向于对比特币提出的批评之一是，比特币严重依赖于集中式交易所和经纪人。绝大多数比特币交易是在集中交易所或通过集中经纪商进行的。

&quot；这就是为什么我们需要DeFi&quot；他们中的许多人说。

然而，我们需要在概念上区分1)进场后的投机/交易和2)实际进场和效用。

想交易DeFi，怎么开始？？你是不是神奇地把钱转到了DeFi生态系统？不需要。首先，你通过法定货币进口交易所，如比特币基地或北海巨妖，从银行向交易所转账。或者您可以使用其他集中支付提供商。然后，您可以购买各种加密资产，并将它们转移到DeFi环境中。从那里，您可以在各种智能合约中交易和使用这些加密资产。

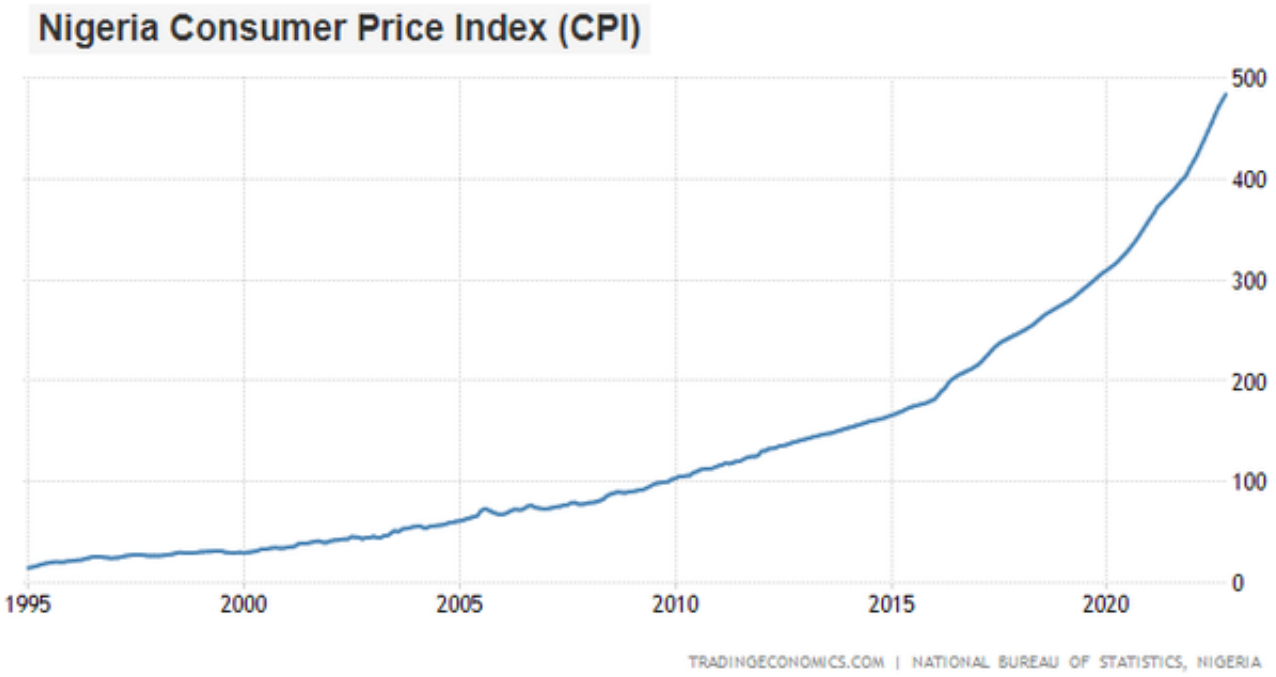
因此，DeFi并没有消除依靠集中兑换或集中银行连接实现法币入口的瓶颈。DeFi只是提供了一个在存款后交易或使用加密资产的智能合约环境，作为竞争对手留在这些交易所交易和利用加密资产。

但实际上，有多少人应该交易或利用加密资产呢？这些不是&quot银行业&quot服务；这些服务主要是针对投机者的。

另一方面，比特币网络也有类似的进入瓶颈。你把钱汇给交易所或经纪人。，购买比特币，然后从那里你可以从交易所或经纪人那里提取比特币。从那以后，你在经济上&quot自我主权&quot，这意味着你可以保留自己的比特币，并使用去中心化的网络在世界各地发送或接收未经授权的比特币支付。。另外，如果因为某种原因，你想在用比特币做抵押的同时获得贷款(法币或稳定货币)，可以使用一些多签名托管服务。如果集中交易所被完全排除在银行系统之外，那么唯一绕过入口瓶颈的方法就是点对点购买。除了挖矿，这也是在交易所存在之前，人们开始接触比特币的方式。

有些方法，如Bisq、RoboSats、HodlHodl、Paxful或Azteco，适用于那些没有&#039；t不想通过集中交易所购买比特币，有时需要匿名。。缺点是流动性有限；这些类型的服务只适合买卖少量的比特币。然而，如果集中交易所被排除在银行系

统之外，这种服务的数量和规模可能会大大增加。作为一个实际的例子，近两年前，尼日利亚将加密资产从其银行系统中剔除。尼日利亚的银行被禁止让客户向加密货币交易所汇款。然而，尼日利亚是世界上人均比特币/加密货币采用率最高的国家之一。比特币/加密货币在这个国家的采用率远高于数字货币eNaira，这个国家的中央银行。这怎么可能呢？因为他们使用各种点对点的方法来获取比特币。他们甚至可以做远程工作，如编程或图形设计。并且直接把国外客户的比特币支付给自己的托管人，然后就可以用比特币进行全球支付了。有志者事竟成。自2010年以来，由于货币供应量不断扩大，官方消费者价格普遍上涨了约5倍。当当局拥有冻结抗议者银行账户的专断权力时，肯定会有这样的意愿。



比特币&#039；s&quot杀手级应用&quot仅用于其最初的设计目的：在迄今为止最分散、安全和防篡改的加密资产中自托管和发送/接收未经授权的支付。

交易/杠杆是一些比特币持有者可能会选择做的事情，但这并不意味着这个世界迫切需要更多的方法来投机一万种加密资产，尤其是当DeFi只与存款过程有关，与现有的合法银行体系无关的时候。

章节摘要

简而言之，DeFi环境试图解决真实的交易/杠杆问题，但它通常由多层中心化组成，如智能合约平台的中心化、资产的中心化和治理的中心化。任意铸币税的问题

当创始人和早期风险投资家成立一家科技初创公司时，他们通常会将自己的命运与

这个想法的成败联系在一起。他们投资流动性差的股票，解锁这些股票，成功退出流动性的主要途径不是上市就是被收购。

为了上市，他们必须经过一个昂贵的披露过程，在这个过程中，他们必须披露他们的账目，披露他们的主要所有权，并详细讨论风险。创业公司上市的平均时间超过8年。

如果你想被收购，他们需要创造一些足够吸引其他公司的东西来购买他们。换句话说，拥有MBA或其他商业经验/教育的专业人士会对他们的企业进行评估，然后决定收购。

因此，初创公司的创始人和早期投资者的财富通常与他们创建和融资的公司的潜在基本面密切相关。该公司需要一些收入、一些用例以及一定程度的尽职调查。他们必须花费数年时间来建立一家公司。要么让另一家公司愿意收购，要么让这家公司大到足以存在足够长的时间，上市并进行所有必要的披露。

在加密的世界里，事情就不一样了。创始人和早期投资者可以创建一个项目。，公开出售Token(通常是向合格投资者或海外投资者出售，以规避现行的公开证券法，因为Token的首次公开发行受到打击)，为其工作一年、两年或三年，并大力营销其在加密交易所上市。然后将炒作的代币(可能是未注册的证券)倾销给公众散户投机者，夸大或完全谎称项目的去中心化和效用水平。换句话说，创始人和早期投资者可以从项目的基本原则的实际成功中区分自己的利润。他们不&#039；他们不需要花10年时间来建立一家好到足以让另一家公司想要收购的公司，而且他们也不会这么做。不需要通过美国证券交易委员会的程序进入公开市场。。为了迅速摆脱流动性，他们可以大肆炒作，向散户投资者出售自己的货币。

&quot；铸币税&quot是政府通过发行本币获得的利润，尤其与生产成本(接近于零)和市场价值的差额有关。。区块链技术使私人实体能够从铸币税中受益。他们可以以非常低的成本创建一个加密的半流动/同质资产，对其进行广告宣传，并试图从中获利。因为这个过程中创造的价值很少，基本上是零和博弈。Token的创造者和推广者赚钱，散户投机者赔钱。

比特币因为从来没有募集过资金，所以不符合证券的定义。相反，开源软件被创造出来，然后放在那里。基于链式分析显然，中本聪没有&#039；也不卖他的比特币；早在2010年，他就在没有任何明显经济利益的情况下离开了比特币网络，比特币网络在没有他的情况下继续以一种相当分散的方式运行。

然而中本聪创造的实现点对点支付和储蓄的技术也被其他人重新用于点对点欺诈、欺诈和加密货币行业的广泛销售。

随着这种情况不断发生，我认为会发生两件事。

首先，更多国家的监管机构可能会加大打击这种做法的力度。美国限制了向在岸公众出售未注册初始代币发行的能力，他们可能会进一步限制在岸交易所在发行后向公众出售代币的能力。

其次，不管是否意识到监管风险，人们都会一次次被加密货币行业灼伤，直到开始将加密货币与骗局联系起来。

需要代币吗？

加密行业的问题与密码学无关。。没有人会责怪任何一个开发者去研究有趣的技术，构建有趣的项目。只有当他们试图在这项工作取得根本成功之前从这项工作中赚取数百万美元时，道德问题才会出现。

在评估任何加密货币或邻近项目时，如果它有自己的令牌，请始终询问&quot它真的需要代币吗？"通常答案是否定的。它有一个令牌。，以便让创作者/创始人从快速退出流动性中受益，而不管基础项目是否提供了任何长期的实际价值。

举个例子，假设有人发明了一个叫Rebu的拼车应用。，但此应用程序被标记为&quot分散&quot"Web3&quot项目。创始团队和早期投资人自己创造了RebuToken，把大部分给了自己，然后卖掉一部分来筹集资金。。他们花了两年时间开发应用并宣传，在一些加密交易所上市了Rebu。很多散户都买了这些硬币(虽然已经向公众出售，但可能是未注册的证券)。热布的开发商和早期投资者利用这一机会，以热布货币的形式退出头寸，获利数百万美元。然后人们意识到，&quot等等。不是&#039；用美元购买Rebu的使用权不是比先把美元兑换成RebuToken更容易吗？韩元&#039；这不会增加不必要的摩擦吗？当然，这个项目毫无进展，最终土崩瓦解，热布令牌的价值也随之崩塌。但开发商和早期投资者已经退出并变得富有。

Web2是一个行业营销术语，指的是加密货币的一个子集，试图提供比我们所习惯的更加去中心化的互联网体验。虽然目标令人钦佩。但问题是，这些项目当然大多是想发行自己的代币，大部分并没有真正去中心化，大部分都会失败(虽然很多创作者反正会因为快速退出流动性而变得富有)。

有些发展提供了另一种选择。例如，布洛克公司(SQ)有一个名为TBD的业务部门，该部门一直在研究他们所谓的&quotWeb5&quot，一种允许去中心化交互的技术。而不需要新的令牌。Block的首席执行官杰克多西对与Web3及其相关令牌相关的可疑财务激励非常不满。与此同时，人们承认，建立一个更加分散的互联网是一个重要的目标。

另一个例子是，许多开发人员一直在使用Hypercore协议构建技术堆栈。。例如Slashtags和Holepunch。随着这些技术的成熟，它们有可能实现去中心化的身份和去中心化的应用，这涵盖了Web3技术的大部分目标。。这些Slashtags和Holepunch协议没有令牌，因为它们不是必需的。

我一直在测试和使用Keet，Holepunch的第一个应用。这是一款点对点加密视频、文件共享和聊天应用。它还内置了闪电支付。目前还在alpha的开发阶段，但是到目前为止效果非常好。如果视频通话只涉及几个人，则分辨率更高，延迟更低。而且比Zoom等基于服务器的产品更私密。

这些组织使用的另一项技术Hypercore协议称为PearCredit，这是一种点对点会计系统。如果成功，，将允许以非常有效的方式进行稳定的货币转移和其他集中的无记名资产转移，而无需附加单独的令牌。

这还是一个很有活力的领域，未来3-5年的情况我们会看到。但是它&#039；记住这一点很重要大多数被创造出来的加密货币都无法持续积累长期价值。他们中的许多人是&quot推波助澜&quot计划，通常只允许创作者从项目中获得经济利益，而不考虑项目的基本原则最终是否成功。

这个行业历史上两万多种代币中，只有三种在比特币定价的第二个加密牛市周期达到了更高的价格。如果你环顾四周，没有&#039；如果你不知道退出流动性在哪里，那么你就是在退出流动性。

更新技术栈

多年来，我一直对比特币和稳定币感兴趣，并将继续做下去。

通过比特币，一个相当去中心化的系统，让全世界的用户都可以在没有许可的情况下进行支付，并自行保留有限的匿名资产。。它伴随着波动和风险，却是实实在在的创新。在我看来，从长远来看，它将继续提供巨大的前景。环顾世界，很难低估有多少人存在储蓄或支付问题，要么是因为发展中国家持续的通货膨胀，要么是因为货币失灵。要么是威权主义，要么是金融审查。

有了稳定的货币，一个集中的发行者就以无记名资产的形式创造了一种美元负债，以抵押品为后盾，从而让人们在世界各地的管辖区获得美元，否则很难获得美元。。稳定的货币带有交易对手风险，通过提高抵押品的透明度可以在一定程度上缓解这种风险。我对发展中国家富人杠杆化/交易的稳定货币不太感兴趣，但我对发展中国家人民用于小额支付和储蓄的稳定货币非常感兴趣。。这也可以用黄金等其他货币资产来实现，而且已经实现了。

区块链技术或类似类型的分布式图书还有其他使用案例吗？当然是理论上的。

以下两种的共同点是，它们就像稳定的硬币一样。它们有一个集中的发行人，但债务可以作为无记名资产自动交易。这可以提供很大的效用。换句话说，这代表了升级技术/分配轨道的潜力，以集中证券的交易、结算和保管。

通用认证货币和证券

美股正常的交易窗口是32.5小时，从早上9:30到下午4:00，一周五天。由于一周有168个小时，这意味着美国股票只有19.3%的时间可以交易。在此基础上扣除部分节假日，可能会降到19%左右。

期望他们在剩下的81%的时间里交易合理吗？比如比特币等加密资产？我也这么认为

另外，股票和其他证券的交易需要几天时间才能完全结算。这些年来，时间缩短了，但它仍然运行在遗留的技术架构上。如果每笔交易都可以在几分钟内完全结算，会怎么样？

最后对于发展中国家的大多数人(至少是上层阶级以外的人)来说，整体投资股票是相当困难的。这适用于他们的国内股票和美国股票。

如果传统证券，比如世界各地的股票、债券，，以及所有商品和货币都可以认证，世界上任何人都可以通过智能手机访问它，全天候交易，并在几分钟内完全结算。会发生什么？就像稳定币一样，还是会集中发行，只是债务人会是数字注册资产。而且是相当有效的数字注册资产。

传统资产获得认证似乎是一个合理的预期，这只代表了现有证券运作技术框架的升级。

数字收藏

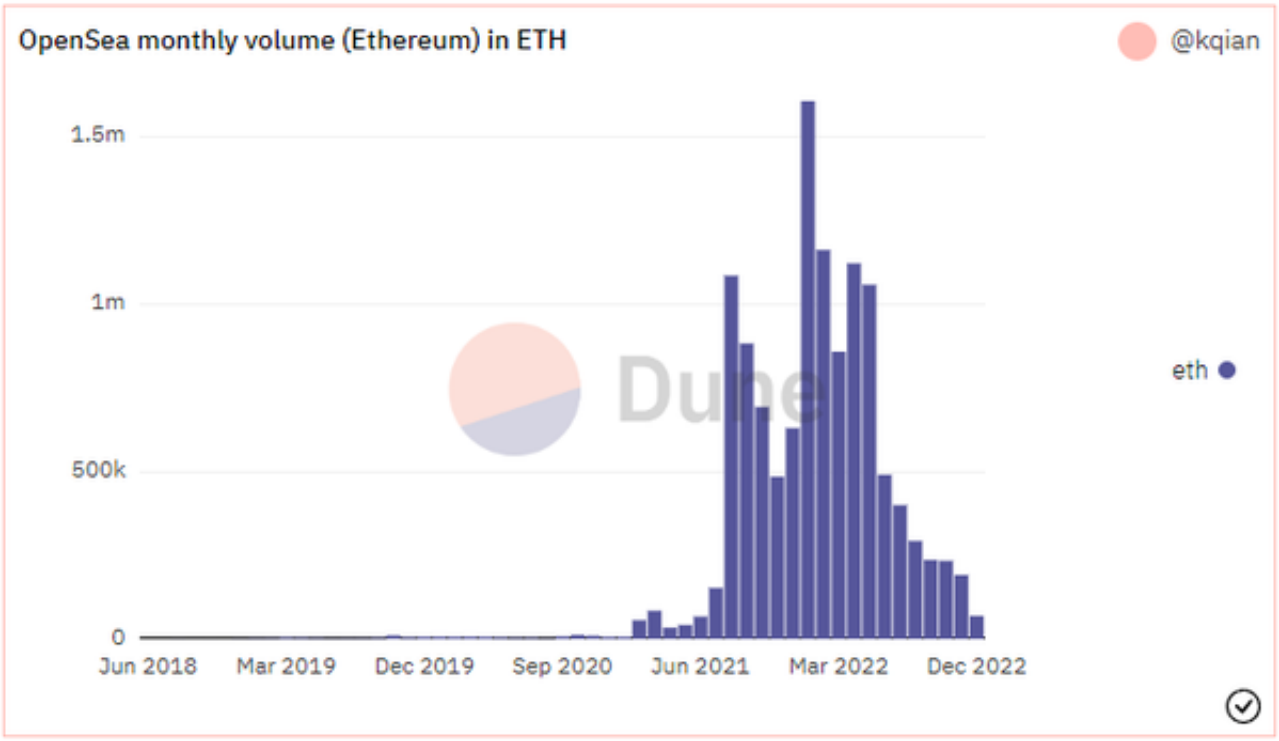
NFT或数字收藏。或者我更愿意称之为&quot第一版收据&quot，这继续吸引着一些人&#039；的兴趣。

这些可以是数字艺术作品的形式，也可以是其他方面的再现。，但基本上有&#039；第一版收据&#039；与之相关。此外，它们还可以是电子游戏物品的形式，可以转移到其他游戏中，或者在游戏之外的公开市场上交易。它们也可以是像音乐会门票这样的东西，可以作为数字无记名资产进行转移。。有些人可能会用它们来直接

支持他们喜欢的音乐家或艺术家。我不知道。我不太喜欢艺术或消费主义，所以这些趋势不适合我，但我不&#039；不排除它们是一个潜在的市场，可能以更大的规模出现。我真的不&#039；我不知道。

然而在实际操作中，无论是数字艺术、数字游戏项目、实体与数字项目的匹配，还是其他方面，目前的NFTs迭代一直都是高度投机的，充满了有目的的价格操纵(对于非同质资产，这比高流动性和同质化资产更容易做到)。开发者往往会创造出一些毫无趣味的游戏然后插上Token或者NFT，而不是创造出一个本来就很有趣的游戏，然后在任何小范围内看。一些可转让的价值是否能在一定程度上提高游戏的趣味性。

在过去一年半的保费报告中，到目前为止，我对整个行业的热情并不高。事实上，在过去的一年里，NFT的数量和价格都急剧下降。



结论：潘多拉&#039；盒子已经打开

中本聪&#039；美国在2008年的发明本身结合了之前几十年的密码学和计算机科学工作，并打开了潘多拉&#039；的盒子。

在国际上持有和转移货币或类似货币的资产。不经过现有的银行体系，突然就有了可能。这个技术是不能取消的。做到这一点的能力是开源的，广泛分布的，现在是已知的。一个加拿大人可以付钱给一个尼日利亚人做一些平面设计工作。这样一来，这两个国家的银行系统都是移动的。普京&#039；美国的政治对手可以筹集捐款

，即使普京政府将他们排除在俄罗斯银行系统之外。委内瑞拉人可以自己保留比特币或美元稳定的硬币，以防恶性通货膨胀，如果他们离开，也可以随身携带。有180种法定货币在近200个国家流通。这些国家大多极其脆弱，容易出现反复的大幅贬值。各自在当地都有垄断，但大部分都没用，在自己国家管辖范围之外很难卖出去。。许多发展中国家的人民很难在几年甚至几十年内保持流动性的价值，更不用说美元自离开最初的锚定金本位制度以来已经贬值了98%以上。

上个月，我在Twitter上问了一个问题。作为思维实验和讨论的开始：

假设你生活在一个发展中国家，这个国家正面临着严重的货币贬值问题。

你想卖掉现有的房子，让它保持稳定的现值。然后两年后可能会买不同的房子。

为什么要转换资产/货币？

答案的范围令人惊讶。发达国家的许多人不&#039；不理解这个问题，说他们只会持有美元。而我不&#039；我似乎不明白为什么有人会问这个问题。

当然，问题是发展中国家很多上层阶级之外的人在开外国银行账户时遇到了困难。他们中的许多人不&#039；我甚至没有国内银行账户。例如在拥有1亿人口的埃及，74%的人没有银行账户。尼日利亚是55%，印度尼西亚是50%，印度是23%。那些有银行账户的人通常不容易获得公平汇率的外汇。那些有幸拥有外国银行账户的人。，通常为此支付相当高的费用；外资银行的业务既不快速也不高效。

在货币贬值问题严重的国家，通常要么1)难以获得美元，要么2)只能以虚假汇率获得美元。，或者3)在国内银行存美元是有风险的，因为可能会被没收，强行换回当地货币。

有些人&#039；答案是他们会持有现金、美元或黄金。想象你在一个发展中国家的公寓里。某处有一栋价值美元或黄金的房子。每次你离开家去工作或购物，你们中的一些人会意识到你可能会因为盗窃、火灾或类似的问题而失去一生的积蓄。我也收到了许多来自发展中国家的人的回复。他们更了解这个问题的挑战，因为他们中的许多人经常处理这些问题。他们中的许多人说，他们只是持有大量实物美元，尽管这有风险。其他银行说会持有汽车或者其他实物资产，效率很低。。其他人说，&quot我就是不能&#039；不要这样做；"我可以&#039；不要卖掉房子，在一段有意义的时间内以流动资金的形式持有。"

因此，在2022年的今天，世界上很大一部分人&#039；美国的人口仍然挑战着&quot储蓄&quot。

出售具有巨大价值的东西，并以流动和安全的形式持有几年，直到这些价值被重新配置，这应该是微不足道的。这不是一个微不足道的事实，它表明了全球金融体系的问题有多严重，尤其是对发展中国家的人民而言。。法币是集中管理的弹性账本，由特定辖区内的地方政府垄断，多数管理不善。

还有财务审核的问题。非营利组织自由之家将国家分类为&quot免费&quot，&quot部分免费&quot或者&quot不自由&quot。与2005年的46%相比，只有20%的国家符合他们对自由的定义。在许多国家，银行账户会被任意冻结。如上所述，在许多情况下，甚至银行账户对发展中国家的工人阶级来说也是一个挑战。因为银行不值得为这么小的余额操心。对于在人生某个阶段成为难民的数百万人来说，他们通常很难携带大部分或全部财富。

所以，加强世界与金钱的关系，还有很多工作要做。2022年。存储和转移价值不应该是火箭科学。全球拥有智能手机的人口比例已经超过拥有银行账户的人口比例，而且还在以更快的速度增长。没有理由说每个有智能手机的人都可以&#039；得不到基本的金融服务，包括现金。。即使是功能手机也可以在一定程度上使用其中的一些技术。

交易和杠杆不是基本的金融服务；它们主要是为已经拥有大量资本的人提供的次级服务。第一个也是更大的机会是提高全球许多人的支付和储蓄。，包括发展中国家和发达国家的人民。这就是比特币和稳定货币所提供的，在不同的时间框架内进行各种权衡。

&quot；获得更好的交易渠道&quot是一个值得努力的合理目标。但这并不是一个像&quot以支付和储蓄的形式获得更多的钱&quot。

该行业的技术随着时间的推移而发展，并将继续发展。这对各个行业会有不同的影响，目前影响有多大还不好说。

在探索这个新的复杂领域时，每个人都会犯错误，但前进的方向是将错误控制在小范围内，强调实用性而不是猜测性，并专注于找到需要解决的最大问题。