



本文共5400字，阅读需约7分钟

作者 | MIT蓝莓星人

设计 | UAL宽心星人

排版 | MURPHY星人

全文摘要

加密货币交易所FTX的黑天鹅事件在全球币圈内引发了一场强震。FTX只用10天时间便从世界第二大交易所沦落至破产境地，320亿美元估值直接归零。

作为中心化交易所（CEX），FTX肆无忌惮挪用用户资金的行为更是让币圈对中心化交易所产生巨大的信任危机。

RockFlow研究院认为，在此背景下去中心化交易所（DEX）将迎来其发展的突破点。DEX虽然发展还不够成熟，但由于能避开CEX巨大的中心化风险，将

成为未来交易所的大趋势。



Part 1.FTX暴雷展现出CEX致命漏洞

FTX暴雷事件暴露出CEX中心化的“不透明性”会对用户资金产生极大安全隐患。

1. CEX和DEX的区别

交易所两大类：中心化交易所（Centralized Exchange，即CEX）和去中心化交易所（Decentralized Exchange，即DEX）。

- 中心化交易所CEX

CEX是指基于自己服务器上的中心化交易平台，代表公司有FTX、币安、Coinbase等等。用户将资产充值进交易所的钱包，然后发出交易指令，交易指令会被记在订单簿上，交易所会从订单簿上进行撮合，交易数据记录在交易所自己中心化的服务器上。

- 去中心化交易所DEX

DEX是基于区块链上的交易平台，代表公司有Uniswap、Sushiswap、Curve等等。DEX通过智能合约来匹配买家和卖家，且交易数据保存在区块链上，可以追溯。



购入大量FTT后，Alameda在市场上推高其价格，接着再以高价的FTT作为抵押物来向FTX贷款。FTX将超过100亿美元的客户的资金贷款给Alameda，让其进行高杠杆的交易来扩大收益。根据法庭文件显示，Alameda和FTX在2022年前就已经亏损了约37亿美金。



Part 2. 信任危机下DEX将成为大趋势

FTX暴雷后，加密货币社区对CEX产生信任危机。用户意识到由于DEX拥有更高透明度，所以更安全，用户资金风险更低。更多用户会倾向在DEX交易。因此，RockFlow研究院判断，未来DEX会蚕食更多CEX的市场份额。

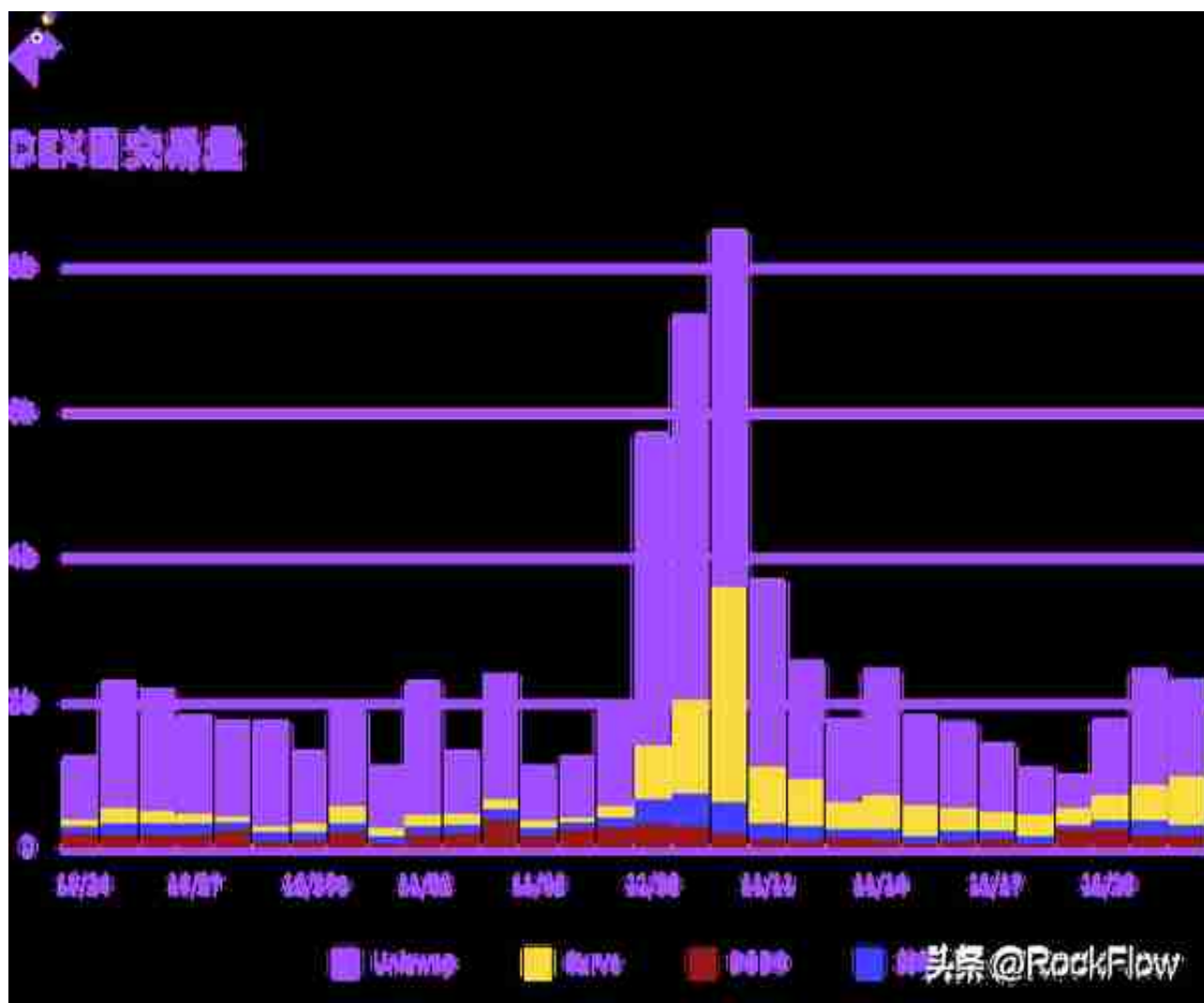
1. 机制决定DEX很难作恶

从上面的案例可以得出，CEX有很经典的委托-代理（Principle-Agency）问题。作为代理人，CEX的利益和作为委托人的用户是很容易冲突的。CEX在巨大的资金利益面前和不透明机制的保护下，被驱使增加自身利益，而不是增加用户的利益。

相反，DEX完全没有委托-代理的问题。回到DEX的定义，DEX是一个完全去中心化的交易平台。DEX本身靠部署在区块链上的智能合约进行运作，背后没有中心化的运营团队。DEX并不拥有用户的帐号、或是资产，仅是提供协议进行交易，因此理论上用户帐号或者钱包不会被DEX禁用，用户的钱完全掌握在用户手中。没有资金掌握权、交易全透明，DEX平台很难作恶。

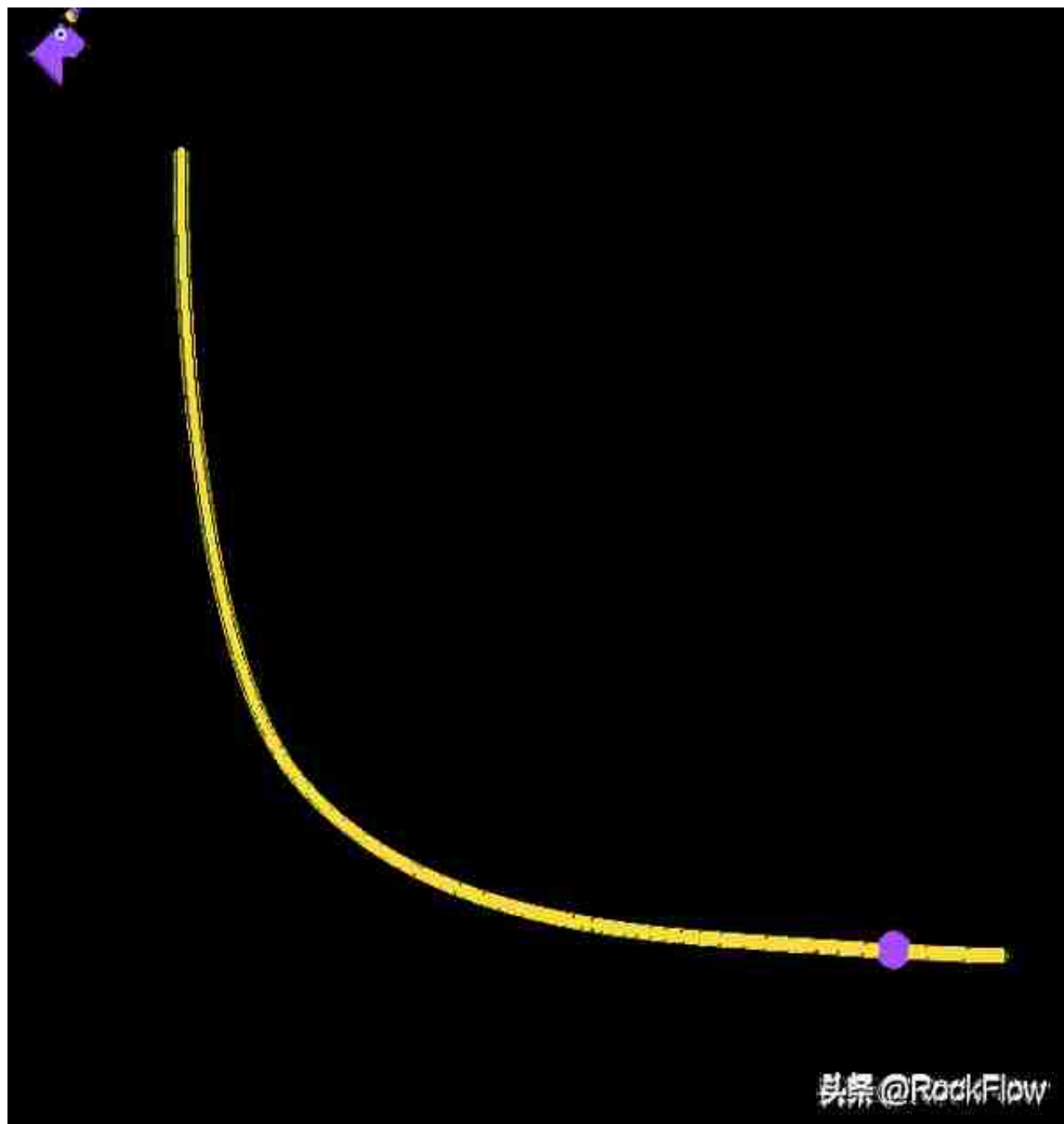
2. FTX暴雷后，DEX交易量增势明显

从链上数据可知，DEX在FTX暴雷后出现明显的增长趋势。用户将资金从CEX中取出存入自己的钱包，并更多使用DEX来进行交易。作为主流加密货币的ETH，从11月初持续流出CEX，数量从11月初近2600万枚到11月21日降至2353万枚，流失占比达到9.5%。



3. AMM技术推动DEX崛起

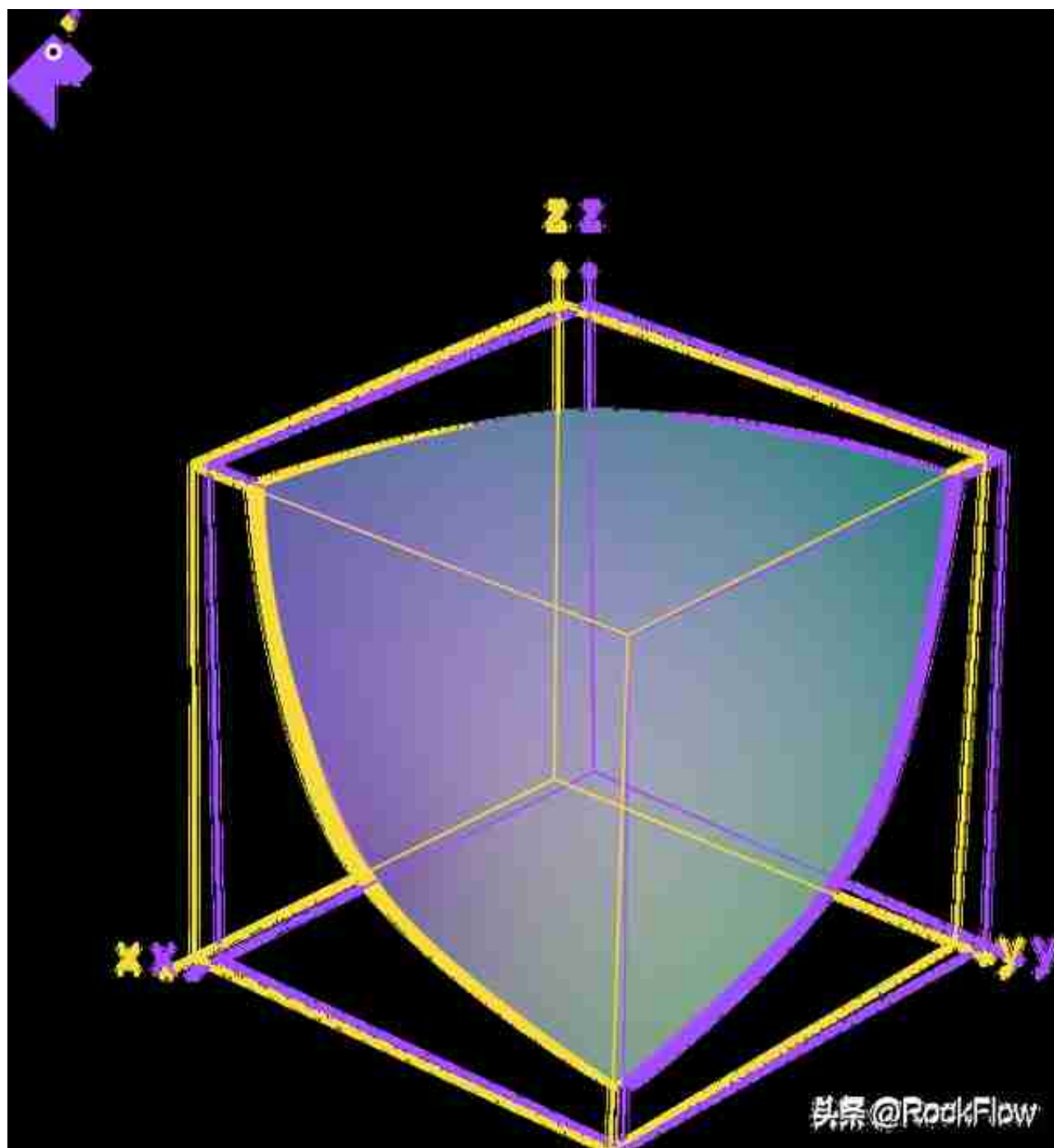
AMM技术是目前主流DEX使用的做市机制，其技术发展推动DEX崛起。AMM (Automated Market Maker) 是自动做市商。AMM能根据简单的定价算法自动计算出买卖价格，类似于一个进行买卖交易的机器人。它将代币汇聚到一个流动性池中，并根据预定义的算法来提供报价。做市商向交易池中注入代币，交易者据此可以直接在该池中根据特定的算法进行交易，不需要挂单、吃单。



恒定和做市商 (CSMM)

代表DEX : 无

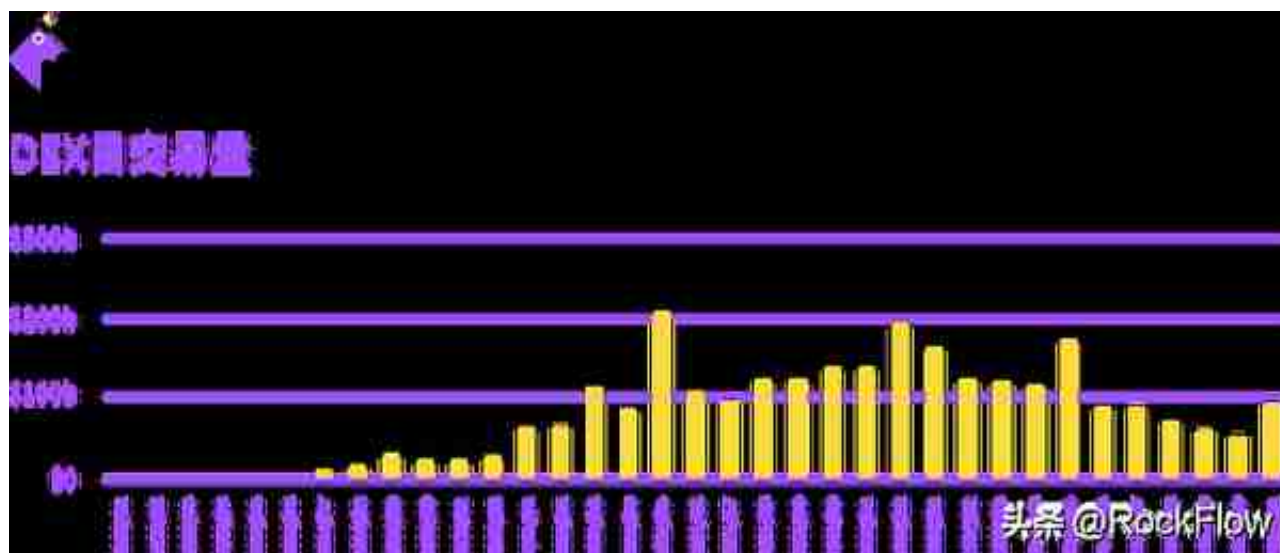
它是零滑动交易的理想选择，但它不能提供无限的流动性。恒定和做市商（CSMM）遵循公式 $x + y = k$ ，在绘制它时，创建的是一条直线。不幸的是，如果代币之间的链外参考价格不是1:1，那么这种设计允许套利者耗尽其中一种储备资产。这种情况将摧毁流动性池的一方，迫使流动性提供者承受损失，并使得交易者不再有流动性。因此，恒定和做市商（CSMM）并不是一个常见的AMM模型。



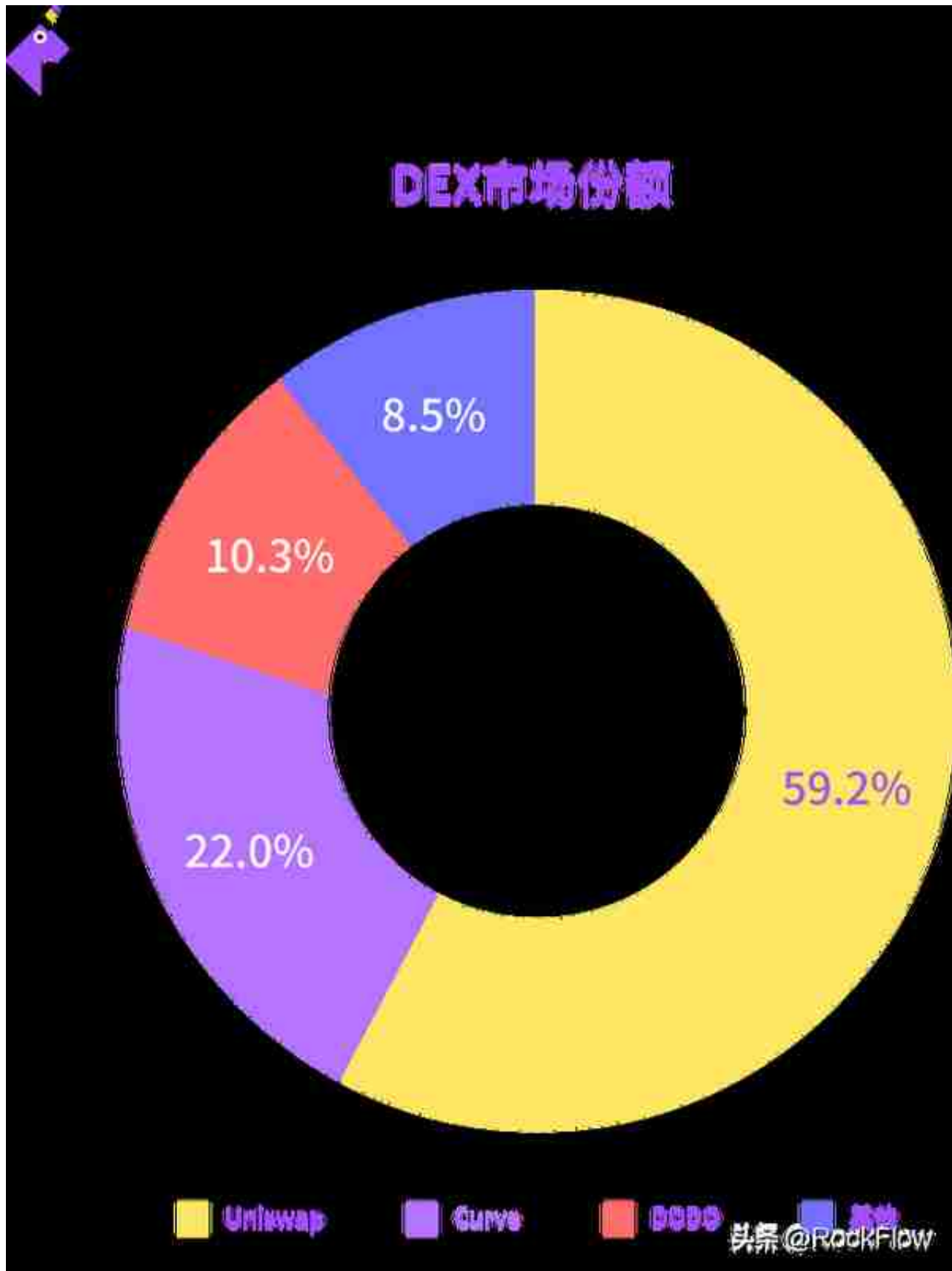
在AMM技术兴起之前，DEX也是用和CEX相同的订单簿模式，然而由于订单簿交易模式对性能和市场深度的要求很高，DEX由于流动性比较低，并不占优势。

因为当代币市场流动性不佳，即代币的挂单很少时，买家会面临巨大的价差，此时小额的资金就有可能对市场价格造成很大的影响；因此，订单很难得以成交。而AMM很好地解决了这个问题，因此AMM技术的发展极大地推动了DEX崛起。

。



和CEX对比，2020年DEX只有CEX交易量的1%。今年FTX暴雷事件后，这一数字从9月的10%攀升到11月的16%，呈明显的上升趋势。



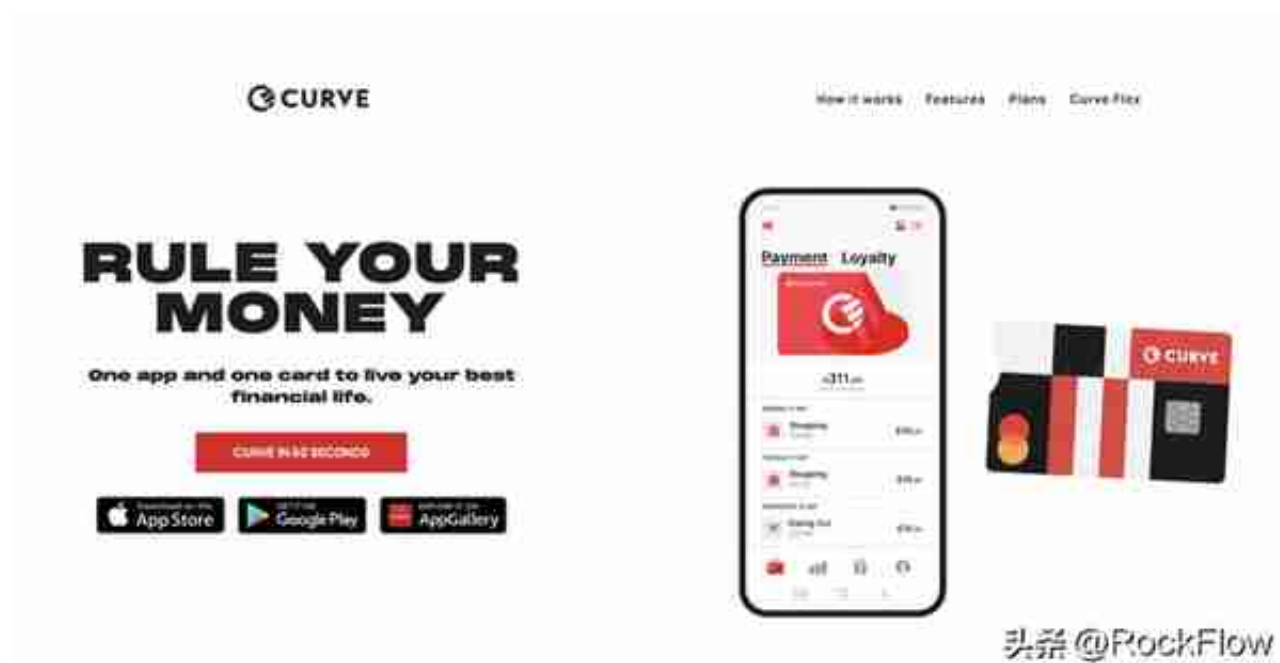
Uniswap - 最大最全面的去中心化交易所

成立时间：2018

市场份额：59.2%

交易机制：AMM

Uniswap专注于成为所有加密资产的通用型DEX，是目前DEX中上架代币最多、用户最多、交易量最大的平台。Uniswap作为领头羊将AMM模型引入DEX，并且对AMM进行了创新性的改变。在新推出的V3版本中，Uniswap从恒定乘积流动性曲线转移到更动态的模型。在该模型中，流动性提供者可以决定在哪一价格范围提供流动性。这一概念被称为“集中流动性”，它将流动性汇聚在更精确的价格区间内。



2. DEX的成长难题

虽然RockFlow研究院对DEX的增长持乐观态度，但目前CEX仍占领加密货币交易所主流。我们可以看到，尽管DEX从2019年起迅速增长，其总体交易量和CEX相比还是较小。这是因为DEX目前存在两大痛点：交易速度低和交易成本高，而这两个痛点的深层原因是以太坊现在的吞吐量太小。

- 交易速度低

DEX的交易通常比CEX慢得多。这是因为在DEX上的每一个交易订单，每一个状态的变化都将作为交易记录在区块链网路中，都需要矿工验证。当需要在短时间

内对不断变化对市场情况做出反应时，DEX还不适合作为一个快速的交易平台。相比之下，CEX由于交易数据不上链，只要有匹配的对手单就能成交，因此成交速度极快，币安的服务器每秒可以处理140万订单。

- 交易成本高

DEX的交易费用波动，可能比CEX高很多。当链上交易拥挤时，gas fee会陡升，那么在DEX便可能产生较高的交易费用。而CEX由于不走链上交易，所以交易费用是交易所自己设置的固定值。

这两个痛点目前很难解决，但是随着技术的升级和以太坊的扩容，相信这些问题会被逐渐得到改善。

在以太坊升级的路线图中，共分为四个阶段：

- Merge – 从PoW过渡至PoS。
- Surge – 透过分片增加Rollup的可扩展性。
- Verge – 添加能够使网路更加分散的无状态客户端。
- Purge – 删除历史数据以简化区块链网路。

这一路线图的终点，以太坊将成为一个更具可扩展性的系统。完成升级后，以太坊将能够每秒处理100万笔交易。RockFlow研究院相信，随着以太坊扩容顺利进行，DEX的痛点将自然而然地解决。因此，只要以太坊能成功扩容，DEX的前途无可限量，未来将成为大趋所势。