“Don’t Be Evil or Can’t Be Evil”
——从中心化到去中心化交易平台研究报告

刘轩铭，3180106071

（软件工程 1801）

1 DEX 和 CEX 的区别

1.1 什么是DEX和CEX

自比特币问世以来，数字货币交易逐渐成为了一种新型的金融交易方式。就目前而言，现阶段数字货币更像一种投资产品，因为缺乏强有力的担保机构维护其价格的稳定，其作为价值尺度的作用还未显现，一般而言无法充当支付手段。数字货币作为投资产品，其发展离不开交易平台、运营公司和投资者的参与和运作。

在前段时间，以比特币、以太坊等为先驱的数字货币市场因为各种因素迎来了一波“牛市”，以吸引更多的人投入资金到数字资产交易的热潮中——一些著名的数字资产交易平台也进入了人们的眼帘。

交易所的核心环节一般包括充提、下单、订单撮合、资金结算和提现等。由于数字货币市场可以看作是传统金融交易市场在数字货币领域的拓展，所以最先出现的交易所和交易平台都是我们所熟知的：集传统交易所、券商和投资银行的功能为一体的平台，这类平台以币安、火币等交易所为代表。由于这些平台上的交易由平台撮合完成，中心化程度和受监管程度高，交易平台参与了一笔交易的几乎所有流程，所以这类平台被称为中心化交易平台（Centralized Exchange，以下简称为 CEX）。

由于区块链被发明之初，就是为了解决“中心化”所带来的问题。这样一来，中心化交易所在加密货币这个去中心化的世界里便是一件很讽刺的事情。同时，中心化交易所会把用户的资产和数据储存在中心化的数据库中，这样的做法也会伴随有许多的安全漏洞和流程漏洞。

于是，去中心化交易平台（Decentralized exchange，以下简称为 DEX）便应运而生。在 CEX 中，所有的交易均由交易平台本身撮合完成；而在 DEX 中，上述所有环节都被置于链上，由智能合约执行全部操作，这样用户的交易过程就无需任何第三方介入，用户点对点即可完成交易。

1.2 DEX和CEX交易流程对比

交易所的核心环节一般包括充提、下单、订单撮合、资金结算和提现。对于上述环境，CEX 均由交易平台本身撮合完成；DEX 则是把上述所有环节都置于链上，由智能合约执行全部操作，这样用户的交易过程就无需任何可信任的第三方介入。下面介绍 CEX 和 DEX 对于一次交易流程的执行过程：

CEX（以火币交易所为例）

1. 用户注册用户名并设置密码进入交易所，此过程一般需 KYC（Know Your Customer，即对用户身份进行确认）；

2. 当用户有充值代币需求，可选择“法币交易”菜单进行虚拟货币购买，这一过程一般是用户之间通过第三方资金流通平台（如银行、支付宝等）进行；或使用自己的数字货币钱包地址向自己的交易所地址充值，则钱包内划入的数字货币会自动转入交易所的地址。

3. 当用户有交易需求，需向交易所提出“币币交易”指令，交易所中心化服务器进行交易撮合（中心撮合或者集中撮合），成交后将结果告诉用户。

4. 当用户有提现需求，可向交易所提出提现指令，由上述的步骤可知，所有的币都在交易所的地址里，所以提币的过程是由交易所的地址转向用户钱包地址。

DEX（以 CoinDEX 交易所为例）

1. 用户在 CoinDEX 上，用户创建好钱包和地址后，私钥将会由用户自持，平台方无权限也无能力获取用户私钥。

2. 用户随后通过授权智能合约，进行订单提交，提交的订单将会汇集到 CoinDEX 的订单池中，以供其他用户查看。

3. 当其他用户找对价格适合的订单后，可以选择执行该订单，提交到 CoinDEX 的服务端，确认无误后，相关交易信息将会进行上链，整个交易流程通过智能合约完成。

4. 订单池到用户执行订单通过 P2P 通信，最后提交到服务端，链下执行订单。最后一步执行流程是上链操作，上链成功后，将会由系统通知用户该笔订单已完成的信息。

1.3 DEX和CEX的区别分析

作为两种设计思路和理念、实现方式都不同的交易行为，中心化交易和去中心化交易之间存在着巨大的区别。这些区别体现在安全、效率、控制权等众多角度。以下进行分点分析：

1. 从资产安全角度来看，CEX 的中心数据库（实际上是地址）中存放着所有用户的资金，由于资金量庞大，很容易招来黑客的攻击，一旦出现问题，几乎所有用户都要遭受损失。例如，2019 年 5 月 8 日，币安遭遇黑客攻击，损失 7000 枚稳定币，价值约达 4100 万美元，这是自币安从 2017 年成立至今发生的第一起公开承认被盗事件。

而在 DEX 平台中，用户的资产不是由平台方来储存，而是由智能合约来管理。交易时平台方不触碰用户资产，用户的资产也无需充值到平台中，用户的交易操作都是点对点的交易，订单操作需要交易者用私钥签名，撮合成功后通过智能合约验证，资产直接到账钱包，无需提现，平台只负责交易流动。

2. 从资产控制权角度来看，在 CEX 中，用户资产将由平台掌控，用户需要将自己的资产充值到交易平台的钱包。中心化交易平台的资产托管功能，就像银行一样，用户把钱存在银行，银行给用户一个账号，记录用户资金情况，银行对用户的资金有绝对的控制权；在 DEX，用户的资产完全由自己掌控。DEX 并不提供资金托管服务，所以也就无法控制、转移用户的资金。

3. 从交易速度角度，在 CEX 中，由于交易数据不上链，所以只要有匹配的对手单，成交速度极快；DEX 则是完全由区块链支持的，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络中，往往会导致流动性差、成本高、速度慢等问题。

2 DEX 的设计理念：Can’t Be Evil

2.1 Don’t or Can’t Be Evil

通过上述分析和对比可以看出，传统的中心化交易所，一定是建立在宣称“不要作恶（Don’t Be Evil）”的基础上的。只有这样，用户才会选择使用你的应用。但是，这样的宣称往往是无法担保的，因为如前所述的恶意攻击，或者监守自盗的情况是无法避免的。

而 DEX 的宣言则是“不能做恶（Can’t Be Evil）”，也就是从源头上防止作恶的发生，这其实是价值互联网时代的一种趋势。如何实现这样的需求？那就是依靠区块链的衍生物——智能合约。智能合约把卖家和买家之间，交易执行的过程和规则写到智能合约里，然后将该合约上链——没有人能够篡改这个合约，因为没有人可以篡改区块链上的数据。

智能合约可以做到，在钱包到钱包之前进行交易。用户自己掌握这个钱包的私钥，没有别人知道。当卖家 A 用 A 货币，吃掉卖家 B 的 B 货币卖单，等值的 A 货币和 B 货币在链上进行交换，资产直接打入到双方交易的钱包地址里，而没有中间人插手。撰写智能合约是以太坊区块链的主要功能。目前的去中心化交易所主要是以太坊上的交易所，支持以太坊上的 ERC20 币币交易。

去中心化交易是目前的趋势，不仅很多中心化交易的项目在大力研发去中心化的交易所、交易协议和衍生品，中心化交易所巨头也在入局和布局。比如 Coinbase 收购了 Trust、传闻币安在研发去中心化交易所等等。

目前去中心化交易所还有几个痛点：

- 交易流动性和深度不足：目前有 0x Protocol 等协议提出去中心化交易所之间共享流动性池的方案
- 跨链交易：目前 Kyber 和 DDEX 在合作研发 WBTC，支持 ERC20 标准的 BTC 交易
- 移动端 App 也是一个趋势，随时随地交易。去中心化交易所可以同时提供钱包功能，比如我们上文提到的 DDEX 交易所已经有海外移动版 App。

2.2 杭州鲸交所：国内的DEX代表

目前世界上有超过 100 家的去中心化交易所。而在我国，这样的 DEX 还是较少的。其中比较著名的就是位于杭州的鲸交所。

图 1 鲸交所图标

事实上，鲸交所的企业宣言就是：Can't Be Evil（无法作恶）。而其愿景则是：Everything exchange。

从技术上说，鲸交所要建立一个集体见证不可篡改的可信价值交换网络，坚持用区块链技术做去中心化交易所。鲸交所基于 EOS 主链开发，用经过第三方安全审计的智能合约进行资产托管，并且用 1+1+3 的多重签名机制对智能合约进行防护，智能合约或资产的任何改变，都需经过鲸交所私钥签名、慢雾安全第三方审计通过、8 个 EOS 超级节点中的 3 个共同签名，多方共同授权同意后才能执行。即使交易所私钥泄露，黑客也无法盗取用户资产，交易所自身也无法作恶。

可以说，它是国内在 DEX 领域的先行者。但是，近段时间以来，不断有消息曝出：鲸交所提出的 FIL 云挖矿等交易和项目，实际是一种骗局。而鲸交所本身也并不是一家完全“去中心”的交易所。它在众多用户心目中的可靠性发生了极大的动摇。

这让我们开始思考一个问题：许多鼓吹的“去中心化交易所”本身是否真的完全去中心化？例如，2018 年 7 月 9 日一家去中心化交易所 Bancor 遭受黑客攻击事件后，它便被认为其实是个“伪去中心化平台”。当时，24,984 个以太坊（约合 1200 万美元），以及 30 万 Pundi X（价值约 100 万美元）和价值约 1000 万美元的 BNT 被窃。之后，Bancor 公告“已经识别出黑客地址，并使用 Bancor 协议内置机制冻结了被盗的 BNT”。这说明 Bancor 可以随意篡改智能合约，冻结用户钱包的资产。没有一家去中心化交易所有能力并且应该这样做。

非常讽刺的是：比特币这类的加密数字货币打着去中心化的旗号来对抗审查和大机构腐败，但一次次比特币交易所的监守自盗却一次次重创比特币的价值。

3 总结

综合来看，DEX 相对于 CEX 有明显的安全优势，能够大幅降低人为因素导致的各种风险，不过目前底层公链的性能严重制约 DEX 的发展，导致用户体验远低于 CEX。但随着 DeFi 项目逐渐活跃，市场上各类去中心化交易所正不断突破，试图多的市场份额。DEX 和 CEX 的竞争不仅仅只是技术的竞争，更多的是经济模式、高性能的竞争。

而 DEX 目前也遇到了较大的挑战，其中比较明显的方面在于：交易速度和效率低，同时也存在着信任危机的问题。关于效率低问题的解决方案，目前已经有技术上的运量方案；而信任危机的问题，则是一个难以解决的问题。或许企业背书会是这一问题解决的良方。