Lyra: 去中心化的场外交易

杨武州 (wuzhou@lyra.live)

摘要

区块链是一项伟大的技术革新，使得去中心化的金融系统成为可能。但是我们所知的各种 DeFi 解决方案只能处理链上数据，对于链下行为，比如场外交易等，却是无能为力。Lyra 发明了去中心化的场外交易系统，解决了 DeFi 无法延伸到线下的不足。

介绍

由于支付方式的进步，全球范围内存在将法币和加密货币互相兑换的巨大需求。目前满足这种需求的主要是各大加密货币交易所的出入金服务，以及基于 P2P 模式的场外交易服务。前者是由交易所和银行系统建立转账协议来实现，后者完全基于点对点模式，客户之间进行场外转账，交易所只提供撮合服务。此外还一批专门面向 OTC 交易的交易所，典型的有 Circle Trade，Cumberland Mining，Koi Trading 等等。虽然多数这类公司不会向外披露具体交易数据，但是业界普遍估计场外交易的额度远超币安这类的场内交易总额。场外交易平台是机构用户投资数字货币最重要的渠道，数字货币行业必备的基础设施。对于个人来说，如果想要在法币和加密货币之间进行兑换，只有交易所的 OTC 服务这个唯一渠道。

现存的所有 OTC 交易都需要一个准入门槛，包括但不仅限于开立账号、严格的 KYC，以及最低交易额限制等。这种相对较高的交易成本限制了 OTC 交易的普及，无法让 OTC 交易成为大众化的服务。Lyra 去中心化 OTC 交易解决了这个问题。Lyra 把 DeFi 的概念引入 OTC 交易，实现了任何人在任何时候、无需注册、无需 KYC、随时随地交易的极端便利性。

在 Lyra OTC 交易中，任何时候，无论是买方还是卖方，都在交易时提供了大于 100%交易价值的 LYR 币作为抵押，该抵押保存在智能合约中，在交易成功之后自动返还交易者的账户中。在交易发生争议后，由 Lyra ODR 争端调解系统进行判定，使用有过错方的抵押来赔付无过错方的损失。因此 Lyra OTC 实现了无前提的安全场外交易，真正让法币和加密货币的兑换变成了像使用现金一样便利。

下图比较了 Lyra 去中心化场外交易和传统中心化场外交易的特点。

	Lyra 去中心化场外交易	传统场外交易
运营方	基于 Lyra 点阵区块链，无中心化	各大加密货币交易所等私营公司
卖家	任何人，无需认证	运营方平台认证 (KYC 等)
买家	任何人，无需认证	运营方平台注册用户 (KYC)
资金安全	基于智能合约的担保交易	运营方平台担保交易
质押方	买卖双方皆需质押	卖方。买方无质押
质押物	LYR 币	运营方平台指定（平台币或者法币）
争端解决	ODR 分布式在线争端解决系统	运营方专有客服
争议仲裁	交易所发生的自治组织 DAO，或者区块链运营者委员会	运营方内部仲裁
交易质量保证	所有数据透明化。不可篡改的交易评价系统。	运营商内部风控机制。通常无评价系统。
用户隐私保障	隐私数据保存在用户所信任的交易服务器上。 任何人可以自由搭建、自由选择交易服务器。买卖双方可以预先设置无争议交易记录自动销毁。	运营商掌握所有人、所有交易的隐私数据，用户无法控制
流动性提供	完全基于用户的 P2P 交易	运营方认证卖家

Lyra 平台上的隐私保护

当人们在线上交易时，总是会面对隐私保护的问题。Lyra 提供了一个 Web3 风格的电商平台，而隐私保护是这个系统的里面最为关键的部分。如何让线上与线下的交易安全可行，同时避免隐私泄露，Lyra 通过去中心化的交易服务器做到了。

交易双方通过交易服务器建立连接，然后交换信息，这其中就包含了对于交易双方来说，至为关键的隐私信息。所以，交易双方都应该信任该交易服务器。那么问题来了，找到一个全体交易者都信任的服务器非常困难，但是找到特定的交易双方共同信任的服务器却是有可能的。所以，在 Lyra 去中心化的架构里面，任何人都可以搭建一个交易服务器，只要获得交易双方的信任，交易就可以发生。最重要的是，交易者的隐私数据仅限于该服务器存储，任何其他方是无法存取。

在 Lyra 平台上，建立一个新的交易服务器的成本极低。交易服务器建立买卖双方的消息传递通道，同时作为公证，使用区块链技术，保存每一条消息的哈希值，在每次交易状态发生改变时，把最新的哈希值作为见证永久存储在 Lyra 的区块数据库里。因此，只要交易服务器存续，所有人都可以验证交易数据的完整性和真实性。

借助于私有和独享的交易服务器，交易双方拥有了场外交易完全的隐私权。这一点是其他任何中心化的场外交易服务商无法做到的。

DAO

DAO：分布式自治组织

对于 OTC 业务来说，有一些关键的参数需要根据不同情况设置，比如买家和卖家抵押价值的比例，分配给 Lyra 区块链运营者的利润比例，以及争端交易的处理等。基于去中心化的理念，Lyra 不会设置全平台统一的参数，而是把这些参数的设置放置在 DAO 里面。简单地说，卖单必须基于某一个 DAO 而创建，这个卖单也相应的接受 DAO 的预设参数。因此，Lyra 把 DAO 变成了一个盈利单位。我们鼓励创业者根据市场，或者其选定的某一方向特定用户的需求，设置特定的交易参数。只要这些设定能够促进交易，繁荣市场，那么 DAO 就可以获得更多盈利。

ODR

ODR：在线争端解决系统

在一个完全去中心化的交易平台，处理交易争端是至为重要的。Lyra 目前提供支持三个级别争端解决 ODR 系统。

第一个级别，买卖双方的一方会发起一个正式的争议，对方会看到这个信号并且有机会主动来解决冲突。如果对方能够回应并且主动解决争议，这一级别的争端不会记入交易历史。

第二个级别，买卖双方的协商不能够解决争议，那么一方将会申请 DAO 介入。DAO 的运营者必须根据双方提供的证据来提出调解方案。如果 DAO 是一个股份制的结构，那么 DAO 的决议必须由 DAO 的所有者们进行投票才能生效。生效后的调解方案如果被发生争议的双方共同接受，那么争端获得解决。这一级别的争端会记录在区块链上。

第三个级别，如果争议双方有一方不接受 DAO 的调解方案，那么该争议上升至 Lyra 委员会上进行仲裁。Lyra 委员会由 Lyra 区块链网络的验证节点的所有者组成，按照 2/3 多数的原则形成最终决议，而且 Lyra 委员会的决议有强制性，不管争议双方是否接受，决议都会被强制执行。这一级别的争端会被 Lyra 记录并且可能会公开包括双方的证据在内的详细信息。另外，由于 DAO 不能够解决争端，最终 DAO 将支付 Lyra 委员会的调解费用，以及争议交易损失价值比例 30%~100%的罚金。

Lyra ODR 系统将会确保任何争议都会被最终解决，从而保证了交易的顺利进行。

信用系统

对于一个金融交易系统来说，信用是至关重要的。那么，如何在没有 KYC 的情况下来保证交易者的信用呢？Lyra 通过建立口碑系统来实现这一点。

在 Lyra OTC 系统中，用户可以对每一笔交易进行评价，而该评价使用区块链技术使得其不可篡改、不可删除。因此该系统鼓励用户通过合规诚实的交易历史，累积而建立良好的、社区公开的信用。对于不可避免的争议交易，Lyra ODR，在线争端调解系统会引导双方解决纠纷。

所以，尽管 Lyra OTC 没有 KYC，但是真实的交易数据、可信的交易评价，让客户拥有比 KYC 更加可靠的参考。

市场前景

去中心化的 OTC 交易彻底把交易成本（包括时间成本、金钱成本）降到了最低，让任何人拥有了随时随地兑换任何货币的可能。历史的来看，成功的商业模式全部都是降低交易成本的模式。

结论

去中心化的 OTC 交易彻底去除了机构对于客户的控制，让每一个交易者拥有隐私方面完全的控制权。随着人们对于隐私保护越来越重视的时代的到来，Lyra OTC 将会发挥不可替代的作用，创造出巨大的市场需求。

Reference

[1] Lyra 公链白皮书

https://github.com/LYRA-Block-Lattice/LYRA-Docs/blob/master/LYRA-BLock-Lattice-White-Paper.md

[2] Lyra Unify App

https://app.lyra.live/