

# 路印拍卖协议（Oedax）的原理和应用



Daniel Wang  
Mar 9 · 10 min read

今天我们向LRC持有者和路印社区介绍一下我们正在研发的路印拍卖协议：Oedax（是Open-End Dutch Auction eXchange的简称）。相对于原始的荷兰式拍卖，Oedax的一些特性更适用于去中心化交易。我们相信路印拍卖协议和路印交易撮合协议（即路印协议）是互补的。



## 荷兰式拍卖

荷兰式拍卖用来拍卖一定数量的资产。拍卖的初始价格一般设置为比市场公允价格高得多的一个价格，然后随着时间按一个预设的价格曲线逐渐降低到零。当价格曲线降低到实际价格（实际参与金额除以资产数量）的时候，拍卖即可成功结束。

荷兰式拍卖有一些很好的特性。首先是每个拍卖都会保证成交；其次是每个参与者最后交易的价格都相同，与参与顺序和参与金额大小无关。第二个特性避免了基于订单的交易模式面临的抢先交易（Front

Running) 问题。不过这种统一价格的特性也有个缺点：参与者会选择不那么早参与到拍卖当中，而是倾向于选择到拍卖后期，不确定因素更少的时候才加入。

荷兰式拍卖是一个非常好的价格发现机制，尤其是在由区块链赋能的去中心化环境中。荷兰式拍卖还可以为去中心化应用 (dApp) 提供价格预言 (Oracle)。

原始的荷兰式拍卖是为单向卖出某类资产而设计的，一旦拍卖开始，一般不允许更多资产被添加到同一个拍卖中。我们基于荷兰式拍卖，设计了路印自己的拍卖协议Oedax。路印拍卖协议更像是一种双向交易而不是单向拍卖。

## Oedax原理

我们设计Oedax的目标是为买卖双方提供一种新的资产交换方式，尤其是虚拟资产和虚拟货币的交易。因此在本文中，我们会以代币 (Token) 举例说明，但Oedax其实是通用的交易模式，应该可以用来交易任何类型的资产。

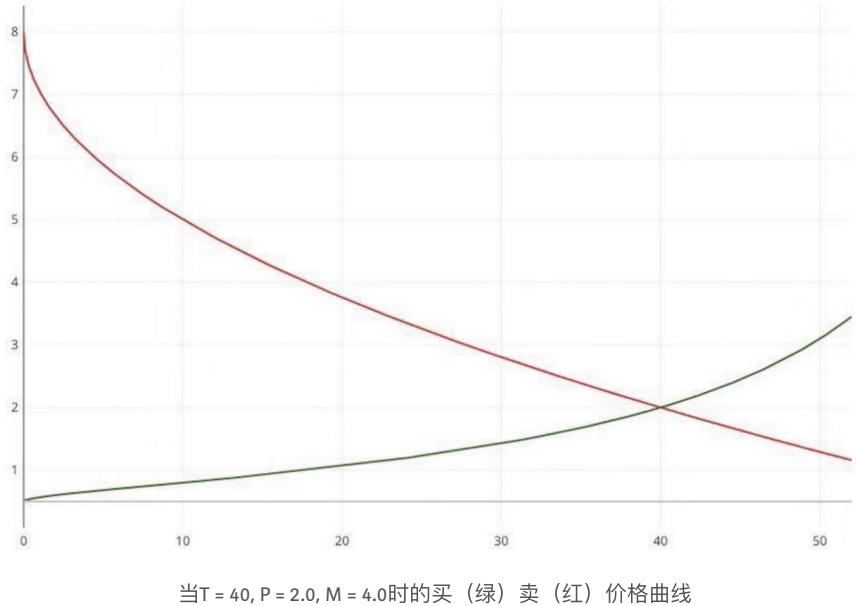
假设卖家想卖出TokenA来换取TokenB；而买家相反，想用TokenB来买入TokenA。Oedax允许卖家将TokenA拍卖成TokenB，并同时在同一个拍卖中，允许买家反向将TokenB拍卖成TokenA。因此我们可以把Oedax看做是共享配置的两个并行荷兰式拍卖的结合体。

我们假设TokenA相对于TokenB的市场公允价是  $P$ ，在路印拍卖协议中TokenA的初始价格设定为  $M*P$ ，其中  $M$  是大于1的参数。我们称  $P$  为目标价格， $M$  为价格因子。我们还假设Oedax的时间跨度是  $T$ ，它代表在没有任何人参与的情况下，该Oedax结束所需要的时间。

接下来我们指定两个价格曲线，分别是TokenA的卖出价格曲线，简称  $SC$ ；以及TokenA的买入价格曲线，简称  $BC$ 。这两条曲线满足下列约束条件：

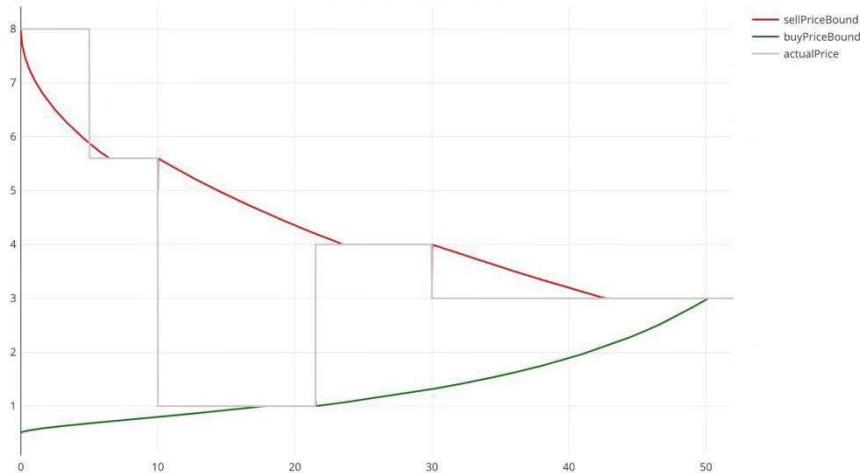
- $SC(0) == P*M$  且  $SC(T) == P/M$  (规则1);
- $BC(0) == P/M$  且  $BC(T) == P*M$  (规则2);
- 存在一个时间点  $t \leq T$ ，使得  $SC(t) == BC(t) == P$  (规则3);

我们进一步假设在拍卖开始后的时间点  $t$ ，TokenA的数量是  $Q_s(t)$ ，TokenB的数量是  $Q_b(t)$ 。那么我们就可以用  $p(t) = Q_b(t)/Q_s(t)$  表示在时间点  $t$  的实际价格，并在坐标轴上面将  $p(t)$  用一系列的线段画出来。我们将这些线段的组合叫做实际价格线（APL）。需要注意的是：更多TokenB参与到Oedax中就会将实际价格线上移；而更多TokenA参与到Oedax中就会将实际价格线下移。



## 价格限定与清结算

- 一旦实际价格  $p$  落入卖出价格曲线  $SC$  和买入价格曲线  $BC$  之间， $p$  就只能在  $SC$  和  $BC$  间移动，即对于任何之后的时间  $t$ ， $BC(t) \leq p(t) \leq SC(t)$  要保持永远成立（规则4）；
- 卖出价格曲线  $SC$  一旦与实际价格线相遇，就必须停止继续向下移动。当实际价格向下移动后， $SC$  可以继续向下移动，但必须从之前停止的值开始。也就是说， $SC$  线必须是连续不间断的。买入价格曲线  $BC$  也遵守同样的规则，只是移动方向相反（规则5）；
- 一旦  $SC$  和  $BC$  相交，就意味着Oedax结束。如果实际价格曲线从未落入  $SC$  和  $BC$  之间，那么拍卖结束后不会进行清算，交易不会发生；否则实际价格曲线与  $SC$ ， $BC$  的值一定相同，这时候交易就按照实际价格进行清算。注意：实际成交价格和目标价格无关。（规则6）；



该Oedax 在时间点50以3.0的价格成交—灰色横线表示不同时间点的实际价格。

理想情况下，Oedax的初始条件应该使得实际价格在拍卖开始后很快便落入买卖价格曲线之间，这样就可以保证拍卖结束后一定会有成功的交易和清算，进而鼓励参与者尽早参与到该拍卖中。

## 拍卖的不同阶段

Oedax最终成交的前提是在某个时间点  $T'$ ，实际价格落入买卖价格曲线之间。我们称从拍卖开始到  $T'$  这个阶段叫阶段A。阶段A具有最大的不确定性。在时间点  $T'$  之后，拍卖进入阶段B，意味着成交是有保障的。

我们可以引入另外一个参数  $N$ ，一旦买卖曲线在某个时间点的价差小于  $P*N$ ，我们即进入阶段C， $N$  越小，阶段C的价格不确定性也就越小。

当然也可以引入其它的机制来衡量是否成交以及成交价格的不确定性（风险），并以此来收取不同的交易手续费，甚至为早期参与者提供交易手续费的返佣。这种灵活的费用机制和基于订单交易模式中的做市商奖励是类似的。

## 参与和撤销

在阶段A，参与者可以成功充值任意额度的TokenA或（和）TokenB。如果提现也被允许，那么参与者也可以提取任何额度的TokenA或（和）TokenB。

进入阶段B之后，充值和提现的数额就将受到上述价格绑定规则的限制。在时间点  $t$ ，这些充值提现的上限分别是：

- $TokenA$ 的充值上限为:  $Qb(t)/BC(t) - Qs(t)$
- $TokenB$ 的充值上限为:  $Qs(t)*SC(t) - Qb(t)$
- $TokenA$ 的提现上限为:  $Qs(t) - Qb(t)/SC(t)$
- $TokenB$ 的提现上限为:  $Qb(t) - Qs(t)*BC(t)$

为了能帮助后来的参与者进行较大额度的买卖, Oedax可以为买方或卖方设置一个充值等待队列 (*Deposit Waiting List*), 用以暂时托管超出充值上限的资产。一旦有对手方也进行大额充值, 就可以随同对手方的参与, 将充值等待队列里的部分或者全部资产参与到Oedax当中。值得注意的是, 在任何一个时间点, 只会有卖方充值等待队列或者买方充值等待队列。在Oedax结束后, 充值等待队列中的资产会自动返还给参与者。

## 价格曲线

Oedax中的买卖价格曲线可以完全独立定义和配置。比如一条曲线实际上可以是一条直线, 而另一条可以是一条多项式曲线。不过我们倾向于把它们的配置做的更具有相关性, 毕竟在 $TokenA$ 和 $TokenB$ 之间, 哪个商品属性更强, 哪个货币属性更强完全是主观的, 换句话说 $TokenA$ 到 $Token$ 的Oedax与 $TokenB$ 到 $TokenB$ 的Oedax是完全等价和对称的。因此我们更倾向于将买卖曲线定义成具有一样的变化“速度”或者“形状”。基于这个概念, 我们进一步约定在任何时间点:

- $BC(t)*SC(t) == P*P$  (规则7);

有了这个规则, 我们只需要定义一条价格曲线, 另一条曲线就可以被计算出来。我们也称遵守规则7的Oedax为对称的Oedax。[1]

[1]其实路印协议的订单也是遵循类似的对称性原则, 一个 $TokenA$ 到 $TokenB$ 的卖单就是一个 $TokenB$ 到 $TokenA$ 的卖单, 反之亦然。在之前的博客中, 我们称这种模型为“单向订单模型” (*unidirectional order modeling*)”。

## Oedax的特点

相对于其它交易模式, Oedax有下列优点:

- 它不依赖于其它平台或交易模式来提供价格参考;

- 拍卖开始后买卖双方都可以进一步参与，而无需把拍卖固定为初始大小；它甚至允许取消参与（提现）；
- 相比于uniswap，它没有资金池要求，因此适用于流通量小的资产买卖；同时它对大额买卖也十分友好；
- Oedax的充值等待队列使得在拍卖后期依然有可能接收较大的买卖双方参与到即将结束的拍卖中。

Oedax也有继承自荷兰式拍卖的不足之处：

- 交易不是实时的，拍卖可能耗时几个小时甚至很多天；
- 最终交易价格的合理性取决于参与者的参与程度，小范围内的拍卖价格不具代表性。



## 滚动式Oedax交易

对于任意交易对，我们可以生成一系列自动化的，有固定时间间隔的Oedax拍卖。当最早的一个拍卖结束后，新的拍卖便自动被触发[2]—其目标价设定为上一个结束的拍卖的成交价。这样就会保证在一个时间段内，总有固定数量的拍卖在持续进行。我们称这样一个Oedax系列拍卖叫“滚动式Oedex交易（Rolling Oedax）”。

[2]: 实际在区块链上这种自动化需要用户来触发。

当用户参与滚动式Oedax交易的时候，资金先被充值到最先开始的那个拍卖中，剩余部分参与到开始时间次长的拍卖，以此类推。如果参与这个系列所有在运行的拍卖后，充值金额依然有剩余，剩余部分就会被放到一个被所有拍卖共享的充值等待队列里。如果在下一个新的拍卖开始前，充值等待队列里依然有未被消化的额度，那么这部分额度就会被当成下一个拍卖初始充值的一部分全部消化掉。

滚动式Oedax交易还可以把每个oedax当做是它之前所有oedax拍卖的充值等待队列。这种特殊设计会使得交易量更加聚集在下一个即将结束的Oedax中，而不是相对均匀地分散到多个拍卖里。

滚动式Oedax交易使得去中心化交易也可以接收市价单，并保证市价单的成交在不使用任何外部价格预言机的情况下，具有较高的公平性和透明性。



## Oedax在路印协议中的应用

路印协议将使用Oedax来完成协议2.0中引入的燃烧机制。该机制保障当路印协议被更多人使用后，有更多的LRC被自动燃烧掉，进而使LRC变成一个越来越通缩的代币。这个燃烧过程将是完全去中心化的，即

任何人后续都可以触发LRC的燃烧，而不是由路印基金会完成这个操作。我们相信这是去中心化治理的一个重要的组成部分。

另外路印拍卖协议收取的费用也会通过同样的机制，拍卖成LRC，燃烧掉。

## 研发和激励

我们的目标是开发出一款和路印协议互补，完全去中心化，无需授权的Oedax拍卖协议。任何人，在任何时间，都可以发起任意数量，任意大小，在任意两个代币间的拍卖。“上币”无需经过路印基金会，项目团队自己就可以零成本完成。

我们后续会在GitHub上开源基于以太坊的Oedax代码库，并在UpWallet中提供普通用户可以使用的UI界面。同时我们还计划从路印生态发展基金（LEAF）中拿出LRC作为Oedax开发奖励资金。如果您想参与我们在以太坊生态中Oedax的开发，或者想把Oedax落地于其它公有链生态，请与我们联系。

我们很希望听听您对Oedax的意见和建议。请发电子邮件给我们分享您的想法。

获取路印协议更多最新的动态，请访问我们的社区帐号：

- ★ Twitter: [twitter.com/loopringorg](https://twitter.com/loopringorg)
- ★ Reddit: [reddit.com/r/loopringorg](https://reddit.com/r/loopringorg)
- ★ 电报: [t.me/loopringfans](https://t.me/loopringfans) (中文)
- ★ 微博: <https://weibo.com/loopringfoundation>
- ★ 路印官方小秘书微信: loopring999