

# 0x (\$ZRX) 分析和估值

文 Myles Snider, Kyle Samani, and Tushar Jain

2017年12月14日

## 简介

在加密货币生态系统中，中心化交易所可以说是基础设施中最脆弱的一环。这些交易所经常成为负面新闻的主角——它们可能遭到黑客攻击、发行假币、资不抵债，以及经历其他严重的失败。

中心化交易所存在许多问题：

1. **交易对手风险**：用户必须实际将其加密资产发送到交易所。一旦收到，交易所将在其内部分类账上记入用户的账户。中心化交易所维护私有的内部账簿。其中一些交易所被发现一直是以部分准备金的形式运作，之后陷入资不抵债的局面。还有些交易所则涉嫌操纵市场，在其客户之前抢先交易。
2. **速度**：为了将交易对手风险降到最低，用户必须在交易完成后提取加密资产。这是一个缓慢的过程，特别是当用户达到交易所规定的取款限制时。
3. **监管风险**：中心化交易所受到当地监管。这可能导致资产退市，并可能影响价格的流动性问题。监管机构还可能关闭交易所，没收客户资产。

4. **攻击风险**：交易所完全控制用户的资金，并将其保存在有限的钱包地址中，从而成为黑客的首要目标。
5. **成本**：加密货币的交易费用比股票交易所的交易费用高出了一个数量级。例如，Bittrex（交易量最大的交易所之一）[对做单者和吃单者](#)的每笔交易都收取0.25%的费用。

遭受过攻击的中心化交易所的数量太大，因此无法悉数列出。最引人注目的是Mt. Gox，它[损失了850,000个比特币](#)，当时价值4.5亿美元（如今价值超过50亿美元），原因是黑客攻击或者内部操作，这给整个行业带来很大冲击。另一家交易所Bitfinex在2016年的一次黑客攻击中损失了[6,500万美元](#)。Cryptsy在2016年[遭到黑客攻击](#)后宣布关闭。这些事件已经变得非常普遍，所以可以预想它们还会继续发生。加密货币投资的第一条规则便是“永远不要把你的代币交给交易所。”

尽管用户每次使用交易所时都清楚自己面临着风险，但他们会继续这么做，因为交易所是交易的必要基础设施。虽然用户可以通过交易后立即撤出加密资产来降低风险，但这个过程仍然不安全。各交易所的客户经常报告称自己在取出资金时碰到了故障或者经历了时间延迟，而这常常会引发交易所资不抵债的[传言](#)。其他交易所则被怀疑为[洗售\(wash trading\)](#)提供便利。很明显，我们需要另一种解决方案。

## 为什么去中心化的交易所至关重要

去中心化交易所(DEX)是当今加密领域最令人兴奋的创新之一。由于上面列出的问题，大多数行业专家正在寻找中心化交易所的替代方案。中心化交易所相对于DEX的主要结构性优势在于，它支持法定货币，并能够与传统银行体系对接。

我们不能夸大DEX将给生态系统带来的巨大价值。去中心化交易所最重要的特性在于，用户可以随时控制他们的加密资产。这就是所谓的自我监管。在大多数DEX中，交易的实际执行是通过一个开源的智能合约完成的，因此用户永远不必把他们的资产托付给第三方。这是对当前中心化基础设施的重大改进。有史以来第一次，世界各地的人们可以即时交换代币而不必担心任何交易对手风险。

DEX有五个基本好处：

### 1. 安全

- 没有交易对手风险。如果行业参与者永远要为了失去中心化交易所持有的资产而担惊受怕，加密货币就很难成为一种严肃的资产类别。

- 执行交易的智能合同是开源的，可以持续审计。
- 交易所没有部分准备金或资不抵债的风险。

## 2. 速度

- 在中心化交易所存放资产一般需要10-90分钟。经验丰富的加密投资者知道，在发送完整的交易之前先向交易所发送一个小的测试交易，这就会将上述时间延长一倍。使用DEX时这一步不复存在。用户直接用自己的钱包进行交易。

## 3. 抗审查

- DEX既然不存在中央服务器或运营公司，也就不会有被不友好的监管机构关闭的风险。
- DEX是全球性的，这意味着对于所有用户来说，所有的交易可能性和代币对都是可用的。目前，某些国家的用户必须等待本地交易所列出某些加密资产，才能购买它们。DEX将为全球流动性池创造机会，这在以前是不可能的。
- 因为用户可以随时控制自己的资产，所以DEX不受任何资本摆布。没有人喜欢提款上限这种规定。

## 4. 应用程序集成

- DEX提供了与去中心化应用程序(DApp)直接集成的可能性，允许用户在需要代币时进行无缝交易。将来，用户不会关心与服务交互时需要何种代币。集成DEX的支付处理器将利用DEX提供的全球流动性池实时处理资产交易。

## 5. 成本

- 与中心化交易所相比，DEX由于缺少开销，具有结构性成本优势。因为DEX不托管资产，从而大大减少了合规审计等方面的运营开销，这一点是有可能实现的。

## 什么是好的交易所

以下为好交易所的核心要素：

1. 流动性高
2. 费用较低

3. 用户体验设计良好
4. 执行交易迅速
5. 安全保障高（在整个交易过程中，用户应能完全控制自己的资金）
6. 支持不同类型的金融产品（做空、衍生品等）
7. 支持多种不同的交易对
8. 可扩展的API
9. 没有资本管制

### 以太坊DEX生态系统

虽然在以太坊生态系统之外有几个项目也在应对DEX带来的机会（[BitShares](#)、[Waves](#)、[Stellar](#)等），不过本报告将重点关注以太坊生态系统中的DEX，因为其他那些DEX隶属于他们各自的生态系统，而且规模只有以太坊生态系统的一个零头。随着时间的推移，跨链原子交换将支持免信任的跨链DEX。然而，时机还远未出现。

	<a href="#">Ox</a>	<a href="#">Kyber Network</a>	<a href="#">AirSwap</a>	<a href="#">OmiseGo</a>	<a href="#">EtherDelta</a>	<a href="#">ShapeShift</a>
代币	ZRX	KNC	AST	OMG	无	无
链上订单簿？	否	无订单簿	无订单簿	是	否	否
链上结算？	是	是	是	是	是	是
免信任	是	是	是	是	是	否
订单匹配方式	中继器承载链下订单簿	智能合约/储备金	索引	订单簿	吃单者完成提交订单	无
代币效用	费用/治理	储备金必须有KNC的最低余额，并以KNC支付费用	访问索引	费用	无	无

完全稀 释网络 价值	\$376,227,000	\$357,938,079	\$136,052,000	\$1,520,260,114	无	无
项目现状（上线、测试、概念等）	上线	研发中	研发中	研发中	上线	上线

## 综述

### 简介

[0x](#)是交易ERC20代币的去中心化交易所(DEX)协议。ZRX是协议的原生代币。0x从根本上说是一个智能合约系统，任何人都可以使用——它是开源的，完全免费使用。开发人员可以使用0x协议作为基础设施来构建面向用户的去中心化交易平台应用程序。0x是使用[特许经营进入市场策略](#)的早期协议示例之一。

在构建DEX的许多技术手段中，我们认为0x是最出色的一个。0x利用订单的链下匹配和交易的链上执行。这使得大量的单笔交易快速进行，而不会因未完成/取消的订单而使区块链膨胀。

0x通过一种新颖的私钥签名消息实现了这一点。希望进行交易的用户创建一个消息，其中包含关于交易的特定参数——希望交易的代币、价格和订单到期日期。此消息由用户作为授权签名并向网络广播。一旦广播，此订单便是开放的，可以由交易对手方完成。或者用户可以指定一个特定的交易对手方，并将订单直接发送给该方进行填写。订单只能根据生成订单的用户设置的参数来填充。当接受者完成订单时，它被提交到以太坊区块链，在那里，交易由0x智能合约进行免信任执行。这意味着智能合约同时从做单者(maker)和吃单者(taker)那里获取单据，并同时将它们发送给交易对手。无需信任任何第三方。

0x是一个用于订单发现和执行的开源协议。0x团队的目标是通过订单簿和流动性提供一个真正的交易所。因此，协议鼓励第三方创建称为“中继器”(relayers)的通道，以使用户生成和传播这些消息。0x允许中继器对其服务收取以ZRX计价的费用。0x提供去中心化交易所的后端基础设施，中继器将提供前端服务，使得0x能够与现有的中心化服务竞争。

### 背景

0x由[Will Warren](#)和[Amir Bandeali](#)创建，现在他们分任公司CEO和CTO。0x团队主要位于美国加州旧金山。该协议的建立既是为了解决中心化交易所的安全缺陷，也是为了应对以太坊生态系统中对代币到代币日益增长的交易需求。

根据[Etherscan](#)的数据，目前有逾18,000种[ERC20](#)代币，网络总价值达数十亿美元。随着新的应用程序（其中许多都有自己的专用代币）构建在以太坊之上，这个生态系统将继续增长。目前，如果用户希望用一种ERC20代币交易另一种，他们必须通过中心化交易所来完成。尽管用户希望交易的两个代币可能都存在于以太坊生态系统中，但是用户必须先离开以太坊生态系统才能进行交易。0x则为这些交易提供了一种完全在以太坊内进行的方式，消除了第三方摩擦和安全风险。

随着一个多样化的DApp生态系统的出现，用户将需要能够即时交换他们所持有的任何代币，以换取与特定DApp交互所必需的代币。对于用户来说，代币生态系统实在太大了，他们不可能为使用的每种DApp持有相应的代币。0x允许用户将他们的以太币(ETH)按交易时的市场价格转换成DApp上的原生代币。这将允许以太坊用户与以太坊生态系统中的任何DApp无缝交互，而无需离开生态系统。

独立于独立中继器，许多以太坊项目正在将0x直接集成到各自的协议中。[Augur](#)、[Aragon](#)、[Maker](#)和[Melonport](#)都采取这种方法。完整清单可以在[0x的网站](#)上找到。

## 中继器

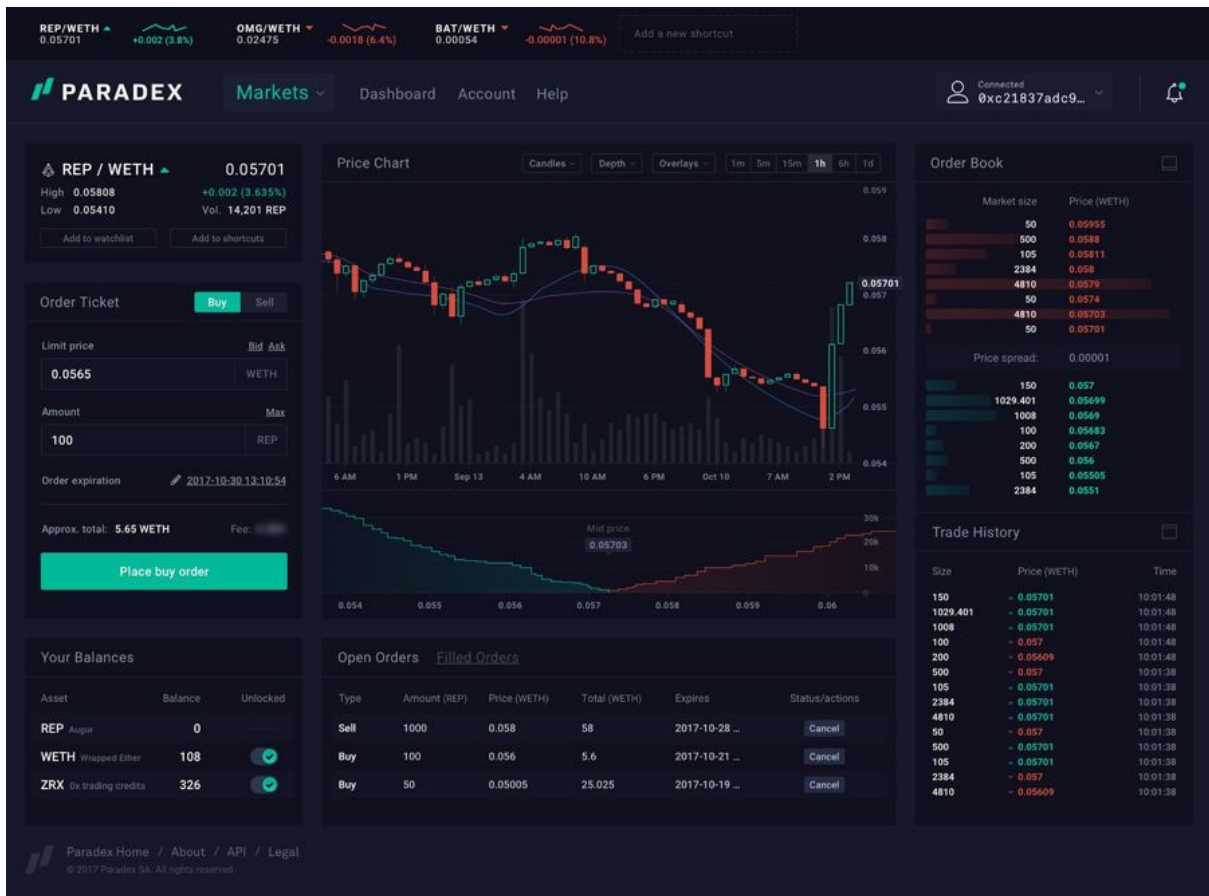
除了促进现有DApps内的交易所外，0x协议还允许任何第三方运行直接构建在0x之上的专用去中心化交易所。这些团体被称为中继器；他们运行自己的订单簿和用户界面，但使用0x合约进行交易。[雷达中继\(Radar Relay\)](#)、[The Ocean](#)、[Kin Alpha](#)、[Paradex](#)和[EthFinex](#)都是正在建造0x中继器的独立公司。其他项目如[dYdX](#)、[Dharma](#)和[Market](#)正在构建衍生品和使用0x协议的其他金融产品。

中继器是0x生态系统中最重要的一部分，可能对协议的成功至关重要。通过创建一组任何中继器都可以使用的智能合约，0x将从不同中继器之间出现的自然竞争中获益。目前有超过9个中继器建立在0x上，还会有更多出现在市场中。每个中继器都将竞相争夺客户，也都会独立地营销其服务，并将新用户引入0x生态系统。

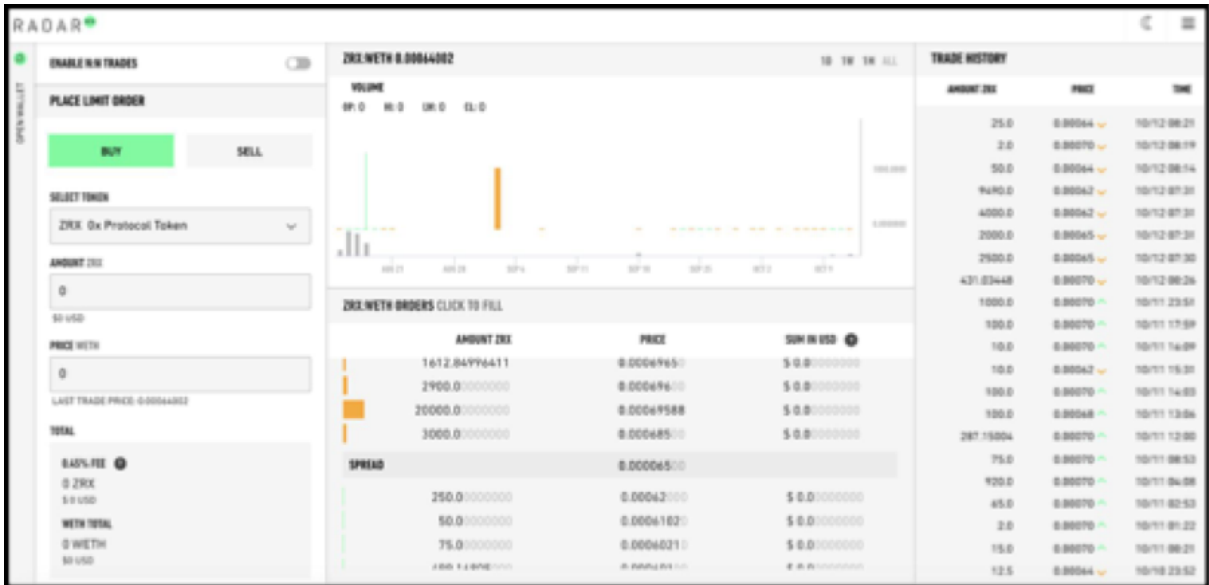
中继器同时能提供中心化交易所模型和去中心化交易所模型的最佳特性。中继器可以投资于高质量的用户界面，并为其专门化的服务收取额外费用，但它们永远无法控制用户的资金。此外，建立中继器的门槛是远低于构建中心化交易所的门槛的（主要是因为不用去维护一个客户余额的内部账户，不必建立结算基础设施，最重要的是由于不需要开展资产托管业务，不用进行

KYC/ AML合规审查)。到时将出现一个多样化的生态系统，中继器彼此争夺客户、迎合不同的利基市场。

Ox还为中继器提供了一种共享订单簿的方法，创建了一个全球流动性交易池，形成的网络效应将使Ox生态系统中的所有利益相关者受益。



Paradex截图



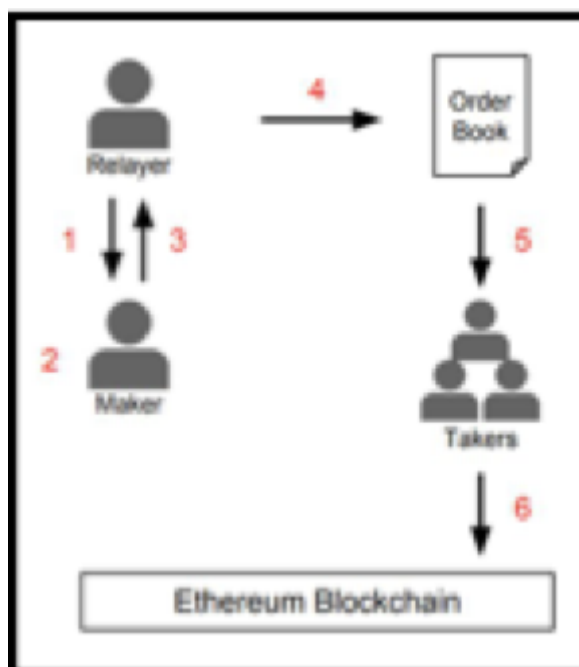
[Radar Relay](#)测试版截图

## 协议机制

Ox协议包含以下组件：

- **做单者**是发起订单的人。
- **吃单者**是履行订单的交易对手。
- **中继器**组织订单簿，撮合做单者和吃单者。
- **Ox智能合约**是运行在区块链上，免信任地执行订单的以太坊帐户。





### 如何运作：

1. 中继器提供一个前端接口，允许用户与0x协议交互。他们可以为服务指定所需的费用。
  - 0x系统的所有费用必须以ZRX的形式支付。
  - 中继器可以提供任何他们想要的收费结构；中继器很可能具有价格竞争力。
2. 用户生成带有特定参数集的订单（用私钥签名）并将其发送给中继器。参数包括：
  - 他们想要交易的代币对和金额。
  - 他们愿意交易的价格。
  - 向中继器支付的费用。
  - 订单到期的时间。
3. 只要该订单有效并包含中继器的（可选）费用，中继器便可将订单添加到其订单簿中。
4. 吃单者扫描订单簿，找到他们想要完成的订单。一旦他们发现了一个订单，便可以通过将其发送到0x智能合约上来执行该订单。
  - 另一种选择是，一些中继器将提供“自动匹配”服务，让吃单者自动与交易对手匹配，而无需扫描订单簿。

5. 以太坊智能合约在链上执行订单。做单者和吃单者收到他们的新代币，中继器收到他们的费用。

- 0x用户直接用自己的钱包进行交易。智能合约从做单者和吃单者双方获取余额，并在完全相同的时间执行交换。

## ZRX代币效用

0x的原生代币[ZRX](#)有两个主要的功能：

1. ZRX用于向中继器支付费用。
2. ZRX将用于代币持有者为0x协议建立某种形式的去中心化治理。

一个或许让人难以接受的事实是，ZRX代币对于协议的当前功能来说并非是必需的。

因为0x是开源的，所以第三方当然有可能分叉0x源代码，删除ZRX代币，并用ETH来取而代之。这种情况发生的可能性，是一个重要的讨论话题。

ZRX中的计价费用对协议的首次用户造成了轻微的摩擦，他们必须在使用0x中继器进行交易之前获得ZRX代币。[雷达中继](#)试图解决这种摩擦，允许用户免费用ETH交换ZRX。由于在0x生态系统中不断增长的网络效应，我们相信用户不会切换到一个不使用ZRX的“非官方”分叉版本上去。更有可能出现的情况是，中继器找到了其他方法来规避这种摩擦，例如完全不收取交易费用，而是通过其他渠道获利（例如：[Robinhood](#)虽然提供的是免费股票交易，但其支持的杠杆交易和其他产品需要收费），或者充当做市商从而获得利差。

中继器的开销比中心化交易所要小得多，所以我们认为基于0x的中继器能够提供更低的费用。随着中继器之间竞争的加剧，费用可能会进一步降低——甚至可能降至零。我们认为这种情况极有可能导致ZRX代币的价格持续下跌，前提是不存在投机价格行为。然而，ZRX代币的价值可能来自它的第二种效用——作为协议的治理工具。

到目前为止，去中心化治理问题一直是加密货币领域中讨论得最广泛的问题之一。许多项目都将治理作为其平台的核心功能，当中包括通过代币销售筹集了2.32亿美元的[Tezos](#)。目前比特币生态系统中关于区块大小的争论凸显了这一担忧。以太坊的[Vlad Zamfir](#)和[Fred Ehrsam](#)（此前他在Coinbase就职）公开表达了对这个问题的反对意见。目前正在探讨以下几种不同的治理制度：

- 代币持有者基于权益进行投票
- 主节点(Masternode)投票（例如[达世币\[Dash\]](#)）

- 基于权益投票选举决策者（例如[EOS](#)和[Tezos](#)）
- 基于权益投票给任何将代币锁定较长时间的人（例如[Dfinity](#)）
- 购买投票“彩票”的代币持有人进行伪随机投票（例如[Decred](#)）

0x团队还没有详细描述他们计划如何实现去中心化治理。考虑到去中心化治理仍处于试验阶段，这堪称谨慎之举。0x团队表示，他们将积极关注形势发展，并研究自己的方法。虽然我们不知道在0x中会实现怎样的治理，但为了防止分叉和流动性池破裂，协议治理的必要性是显而易见的。

如果0x成功，该协议很可能在短期内占以太坊网络总交易量的很大比例。相比之下，以德（EtherDelta）是以太坊生态系统中使用最广泛的DApp之一，经常包含以太坊网络交易的[重要部分](#)。以太坊协议本身仍在积极发展中，并将随着时间的推移继续发生重大变化。其中一些已经由核心开发团队做出了简要介绍，未来还可能出现其他不可预见的变化。随着这些变化的发生，0x协议将需要不断随之发展和改变。0x还提出了一些主要功能，比如将来将构建的跨链原子交换。这些特性将大大提高0x协议的实用性，用户需要找到一种方法来决定何时以及如何技术上准备好集成这些更改。

我们预计最有可能出现的情况是，大部分投票将由严重依赖0x的中继器运营商和DApp完成。中继器和DApp作为建立在0x之上的企业，对确保协议的持续成功和发展有着浓厚的兴趣。不难想象这样一种场景：哪怕中继器没有将ZRX用于支付费用，也仍然保留着ZRX的大量余额，以便参与协议的治理。如果这种情况成为现实，ZRX的所有权很可能高度集中，并且交易速度可能极低。遗憾的是，目前基本上是不可能对治理进行量化评估。去中心化治理太不成熟、太抽象，而且没有经过量化价值的检验。许多传统的公共股票缺乏投票权，股票分析师试图为缺乏投票权设定一个贴现率。然而，这两种场景并不类似，因为协议治理与选举董事会有本质的不同。

## ZRX估值

为ZRX代币确定价格目标是一项很艰难的工作，因为有很多因素在当中起作用。我们不仅要交易量、费用、流通速度和代币作为投资所占百分比（相对于代币的实际效用）等变量进行估计，还必须考虑ZRX的代币经济学，适用于这个市场上几乎所有加密资产的投机溢价。

我们看好0x项目的终极原因在于，0x拥有一支极具才华的团队，他们利用最佳的技术方案（链下中继、链上结算），结合强大的市场验证，解决了加密生态系统中最紧迫的需求之一。围绕0x出现了一个令人难以置信的生态系统——不仅有中继器在0x上构建传统的交易所，还

有其他人正在使用该协议提供别的金融工具，此外，以太坊生态系统中的许多大型项目正在直接集成0x。

我们预计ZRX的价格将在短期内大幅上升，原因有两个：

其一是实际效用。随着中继器陆续上线，用户为了使用它们将需要获得ZRX代币。雷达中继和Paradex都将很快推出，我们预计，它们的体量至少将很快超过以德(EtherDelta)。新用户将必须购买ZRX代币才能进行交易，而交易频繁的用户可能会持有ZRX的余额，以避免在每笔交易中都经历购买代币的摩擦。资本的涌入可能会导致短期价格上涨。

其二是投机。0x驱动的中继器将很快投入使用，这些中继器将强有力地证明0x协议的潜力。加密资产市场还不够成熟，不能仅凭效用价值进行交易，炒作和投机仍是价格走势的主要因素。当用户开始使用0x中继器进行交易时，我们相信他们会认识到这一潜力，购买并持有ZRX。去中心化交易所是所有加密技术中最大的机会之一，我们预计，随着投资者押注于他们预期会胜出的协议，市场将对这一垂直行业进行大举投机。0x团队一直在证明其执行能力，他们的新进展可能会助长这种投机。

而从中期来看，我们相信ZRX的代币机制将成为更重要的因素。随着新的中继器进入这一领域并争夺客户，费用将大幅下降。一些中继器可能会完全取消以ZRX计价的费用，以提供更流畅的交易体验。随着费用下跌、[流通速度](#)加快，支撑ZRX经济所需的货币基础将变得非常小。这可能意味着ZRX代币的价格将持续下跌。

然而在同一时期，我们将看到0x推出一个正式的治理系统。大型代币持有者（中继器、投资基金、DApp开发人员和投机者）将力争保护他们的投资，会创造一个程序来影响项目的方向。这令人兴奋，因为它意味着0x将继续进化。该项目尚处在生命周期的早期阶段，而且它将继续顺应市场力量和其底层区块链以太坊的变化而不断发生改变。最终，0x的愿景是成为一个区块链不可知(blockchain-agnostic)的平台，促进跨链代币交换。拥有一个治理系统对于支持这种演进是至关重要的。

我们认识到当前ZRX代币机制从长远来看的缺点。用ZRX形式进行的支付，如果使用ETH会更容易，而且这种费用很可能被很快抽象出来，即以其他代币支付。0x经济体的参与者完全有可能寻求实施一些机制，比如押注或焚烧代币，以降低代币流通速度和供应。我们将0x当前的形式视为协议的蓝图，随着时间的推移，该协议将经历重大变化。带领它度过早期阶段的核心团队是整个以太坊系统中最有才华的团队之一。围绕0x出现的生态系统，包括中继器、DApp和其他项目都非常令人印象深刻，它已经显示出自己是以太坊堆栈的一个关键基础设施组件。我们相信，0x协议为以太坊和整个加密领域带来了可观的价值，我们也相信，从这种价值创造中获利的机会将是巨大的。

## ZRX的目标价格

我们创建了一个[模型](#)来估计ZRX代币在几种不同场景下的未来价值。这是一个框架，我们可以在其中插入关于数量、费用和增长的各种假设。我们强烈鼓励读者也这么做。

关于流通代币数量的数据，我们直接从0x的官方声明中获得。总供应量的50%在众筹中售出，另外10%流向了早期投资者。这些代币目前是流动的。创始人获得10%的供应量，行权期为4年，锁定期1年。另外15%分配给外部发展基金，还有15%由0x组织预留用于未来的员工薪酬以及维持协议发展。

我们将ZRX代币分为三个部分：用于效用（支付费用）的代币、作为投资持有的代币和用于治理的代币。随着使用0x启动中继器和DApp，我们怀疑用于效用的ZRX代币数量将会增加，而作为投资持有的代币数量可能会减少。我们还发现，为参与未来治理而持有的代币数量可能会增加。这不仅与0x团队关于治理将如何运作的基本想法相对应，还与构建在0x之上的越来越多的项目相对应，这些项目将寻求在协议的未来方向上拥有发言权。根据我们与中继器和其他基金的初步交流，我们设定了25%的基数。

我们对费用的估计是根据中继器公布的费用结构计算的。我们保守估计，起初费用将占总额的0.65%，随着更多中继器提供更具竞争力的费率，费用占比将随着时间的推移而下降。

最后，我们对交易量的估计是基于ERC20代币的每日交易量。我们预计，随着时间的推移，由于围绕着流动性池的强大网络效应，这种交易活动的绝大部分将迁移到0x，我们还相信，随着整个加密行业的增长，这种活动将在未来几年经历持续增长。尽管以太DEX的数据当前主要由EtherDelta来贡献（目前[隐含年交易量](#)约为30亿美元），但我们相信，诸多因素将推动0x的交易量较EtherDelta有数量级的提升。

首先是易用性。Beta阶段的中继器已经优于EtherDelta；这个差距将会扩大。第二点则在于，0x协议将不仅仅用于像在EtherDelta上那样交易ERC20代币。0x还将被用于去中心化衍生品，为Augur预测市场赋能，用于代币化证券的交易等。在未来，0x很可能被用于跨链交易，而这将使各种种类的用例成为可能。可供参照的一个数字是：[NASDAQ](#)的股票日交易量超过720亿美元。0x还处于起步阶段，但其总目标市场是巨大的。

基于这些变量，根据ZRX的[当前价值](#)（0.37美元左右），我们分别提出了基本行情、牛市行情和熊市行情下的ZRX的价格目标。

（注：在我们初次撰写该份分析时，ZRX的价格为0.20美元。出版之日价格升至0.37美元左右）。

- 熊市行情：隐含价值0.51美元

- 基本行情：隐含价值1.19美元
- 牛市行情：隐含价值2.57美元

[该模型可在此处下载](#)。我们还提供了一个[谷歌表格](#)文档。如果想要使用，请单击“文件→复制”选项。在当中也能看到一些评论，对某些假设给出了解释。

## 风险

目前，对0x的投资是押注于以太坊生态系统内部需要去中心化交易所。虽然对去中心化交易所的需求超出了以太坊生态系统的范畴，但0x只支持ETH和ERC20代币之间的交易。因此，0x的潜在市场仅限于以太坊生态系统内部。0x团队表示，希望最终使0x成为一个不可知区块链(blockchain-agnostic)的系统，但在可预见的未来这种机会尚不可能出现。如果在不久的将来出现其他平台，开发出一种与以太坊竞争或超越以太坊的代币经济，那么0x的市场机会将是有限的。

同样重要的是要认识到，虽然0x解决了中心化交易所带来的许多问题，但它并不是一个完美的解决方案。0x[安全审计报告](#)《ConsenSys Diligence》和康奈尔大学一个研究区块链技术的团队发表的题为《Hacking Distributed》(分布攻击)的[文章](#)都指出了0x存在的几个问题。

这两份报告都强调了矿工预先交易的问题，在这种情况下，矿工、中继器或吃单者可以抢在其他人之前进入订单，以获得价格优势。可以采取以下几种手段。

- 最终决定交易顺序的矿工，可以吃下任何他们希望完成的任何广播订单，即使另一个吃单者已经打算完成该订单。
- 矿工可以在交易取消之前完成订单，哪怕做单者试图取消订单。
- 做单者可以在看到一个订单已经被完成后完成同样的订单，支付更高的gas成本以期优先处理自己的交易。

0x为这个问题提供了一些不同的解决方案。协议被设计成通用类型，允许不同的中继器执行不同的策略。中继器可以提供的一种策略是[匹配](#)，即做单者自动指定某个中继器作为其订单的吃单者。然后中继器在内部匹配订单，并将它们发送到区块链以批量执行。用户仍然完全控制他们的资金和订单参数。这也可以防止提前交易，并使得实时交易、限制交易和异步交易等选项成为可能。[Paradex](#)中继器已经宣布打算使用这一策略。

另一种可能的攻击向量叫作做单者恶意攻击(griefing)，如果做单者创建一个广播订单，将其发送出去，然后将原本打算交易的代币移动到另一个地址，就可能发生这种攻击。该订单将由一个吃单者完成，发送到区块链，然后作为失败事务返回。而且，吃单者仍需支付与之相关的

gas费用。0x提供了一个解决方案，中继器可以“修剪”(prune)他们的订单簿，在有效删除无效订单后再完成交易。中继器可以监控以太坊区块链，寻找可能使未决订单失效的新交易（例如，如果做单者按照他们的发布顺序移动了将要交易的代币），然后从订单簿中删除这些订单。中继器还可以选择要求做单者在使用他们的服务之前先支付一小笔保证金，以此来抑制人们的恶意攻击行为。被抓到有攻击行为的做单者，其保证金将被没收。

最终，0x灵活的通用设计允许不同的中继器使用许多不同的策略，其中一些策略可能需要进行细微的权衡，以避免上面讨论的一些问题。然而，不论采用何种中继器，用户都能保持对其资金的完全控制，这是去中心化交易所迄今最重要的特点。

到目前为止，0x生态系统面临的<sup>最大</sup>风险是缺乏对专有代币的需求。让用户以ZRX的形式付费并不能直接给用户带来任何好处，而该代币的付费功能可以通过ETH来实现。虽然去中心化治理将在未来实现，但治理结构尚未成文的事实意味着它还没有向系统添加任何实际效用。

尽管如此，我们认为短期内不太可能出现不使用ZRX的分叉版本0x。协议仍在积极开发中，已有的中继器都计划使用ZRX收取费用。许多这类中继器都是直接与0x团队合作。出现分叉版本0x的可能性是一个长期的风险，但通过0x团队开发出稳健的治理功能可以得到缓解。0x团队在代币销售之前发布了一个功能良好的产品，并持续改进软件、推出更新，这已经证明了他们的执行力。我们相信他们有能力提供包括去中心化治理在内的新功能。

和所有其他在以太坊上构建的项目一样，0x面临着以太坊特有的风险。如果以太坊不能扩展事务吞吐量，0x交易可能会变得过于昂贵。即使使用链下订单匹配，事务的链上执行也会使区块链膨胀。gas费用将变得更加昂贵，用户可能只在大型交易和结算中使用0x。如果费用过高，价差过大，即使存在安全缺陷，用户也可能转向中心化交易所。以太坊的可伸缩性路线图——包括Casper、PoS（权益证明）、分片和最终的Plasma——正在积极开发和改进。我们相信在未来几年内，以太坊的规模将扩大几个数量级。

## 竞争对手

如上面的图表显示，0x在以太坊生态系统中有几个竞争者。每种的方法各不相同，但我们相信0x最有可能成功。

[AirSwap](#)是[Swap协议](#)的一种实现。它在许多方面类似于0x，不过使用的是索引而不是中继器。协议本身不需要代币（事实上，Swap白皮书甚至从未提及代币）。AirSwap是第一个建立在协议之上的索引，它集成了自己的代币，也就是AST。AST并不是用于支付费用，而是用于发布在索引上的交易意向。在0x，做单者发布包括价格这类特定参数的订单。而在AirSwap上，做单者只需在索引下发一个帖子，说明他们希望交易哪些代币对。吃单者可以看到这些帖子，然后做单者和吃单者可以在完成区块链上的订单之前直接协商价格。

为了发布到索引中，做单者必须锁定特定数量的AST，这样用户就可以在一段时间内发布一定数量的帖子。AST代币持有者还可以在平台上对价格整合预言机进行投票。这个代币模型很有趣，但它确实有一个主要缺陷。由于AST代币是专门用于索引的，因此对于Swap协议而言并不具有广泛的实用性，竞争对手可以在Swap协议之上建立自己的索引，并采用种种方式破坏AirSwap——比如将ETH用作实用代币，完全取消AST的应用，或者用他们自己的代币提供更好的服务，以期取而代之。这对AST的投资者来说是一个重大风险。0x能为中继器提供与Swap协议索引相同的服务，而且不止于此。中继器可以使用称为“[报价提供商](#)”的策略模拟AirSwap的索引功能。用户在提交交易被执行前，通过链下通道连接，发出交易意向和价格谈判的信号。AirSwap或基于Swap协议构建的其他索引可能很难与这种灵活性竞争。

[Kyber Network](#)是另一个基于以太坊的去中心化交易平台，设计完全不同。Kyber的主要优势在于它便于交易快速进行。用户可以在单个事务中提交交易请求并接收他们的新代币。Kyber通过第三方托管不同的代币来实现这一点。用户通过请求特定的交易与Kyber智能合约进行交互。智能合约扫描各种储备库，选择价格最优的储备库，然后执行代币的原子交换。

Kyber依赖于愿意建立储备库的第三方——这需要预先配置大量资金，然后必须将这些资金保留在储备库中，以完成订单。储备库从他们的订单价差中获利。这不是对资金最有效的运用手段，所赚取的利润可能不足以激励第三方经营储备库。Kyber曾表示，可以建立公共储备，让贡献者共享利润，但问题仍然是一样的：不收取高额价差就不会产生足够的动力，而这将抑制用户实际使用Kyber的积极性。

Kyber的代币动力也有些问题。其原生代币KNC主要供储备库使用。储备库必须确保达到KNC下限才能参与协议，而且它们还必须为每笔交易支付以KNC计价的费用。这些费用中，有一部分支付给了该行业的其他参与者，比如钱包运营商，其余的则被烧掉。用户不需要直接支付费用，但这些成本可能会通过更广泛的利差转嫁到他们身上。

0x还可以令中继器像Kyber储备库一样运作。中继器和大型代币持有者可以使用“[储备库管理器](#)”策略，该策略允许中继器提供自己的流动性。虽然Kyber和AirSwap这两个项目都很有趣，但0x功能极其灵活，与这两个协议相比都颇具竞争力，而且还能提供更多的好处。

[EtherDelta](#)是一个建立在以太坊之上的实时去中心化交易平台，已经运行了一年多。

EtherDelta缓慢且笨重，有时难以使用。和0x一样，EtherDelta使用链下匹配服务和链上执行，但是它只有一个接口。EtherDelta是一个DApp，而不是协议，因此它的灵活性远远低于0x。我们初步使用了第一批中继器beta版本，体验比用EtherDelta容易得多，也更流畅。

最后，[OmiseGo](#)正在着手开发一个去中心化交易所，将实现链上订单簿。尽管OmiseGo最终计划作为一系列独立的[等离子体链](#)运行，但它将在未来几个月作为Cosmos的一个区域上线。Cosmos提供的吞吐量比目前的以太坊要高几个数量级；OmiseGo打算利用Cosmos带来的吞



吐量以及Ethermint的贡献，在不久的将来交易ERC20代币。这是一个非常迂回的过程，需要从以太坊到Ethermint的多次跳跃，通过Cosmos网络进入OmiseGo区域，然后按顺序完成交易。我们怀疑这么一个复杂的系统是否能正常运作，或者即使它能正常运作，又是否能提供一个可接受的用户体验。

OmiseGo白皮书还指出，OmiseGo去中心化交易所将不会专注于高交易量、低价值的交易，这在链上实现起来要困难得多。他们的重点将放在更大规模的交易和结算上，这就为0x占据大部分市场份额留下了大量空间。OmiseGo的交易价格约为0x估值的10倍，因此经风险调整后的回报率要低得多。

## 结论

去中心化交换是加密货币基础设施的一个关键部分，它将从根本上改善加密经济的功能。0x正在成为以太坊生态系统中领先的DEX平台。这不仅是因为0x核心协议设计良好且功能齐全，也是因为它还激励了第三方中继器的完整生态系统，有了这些中继器后，使用0x将比使用中心化交易所更加简便。在0x上建立的DEX将比其中中心化的竞争对手费用更低廉、准入门槛也更低。0x能够直接集成到各种DApp中，这将意味着基于以太坊的应用程序之间具有更大的流动性和互操作性。0x代表着以太坊生态系统向前迈出了一大步。

0x的ZRX代币最初将只用于向中继器支付费用。这可能导致ZRX的网络价值在中短期内出现增长；我们预计，随着0x在ETH和ERC20交易所市场占据较大份额，ZRX的需求将显著增长。随着更多中继器的出现、价格更具竞争力，以ZRX计价的费用可能会大幅下降。然而，0x团队若能实施基于代币的去中心化治理，将为ZRX代币增添额外的效用价值。在实现治理功能之前，我们不可能对这种效用进行评估。基于代币的治理很可能对构建在0x之上的中继器和DApp最有用，而他们可能会为了投票而持有大量ZRX。治理功能还将促使ZRX代币持有者积极参与协议的发展。0x正处于早期阶段，并将随着时间的推移继续变化和演进。去中心化交易所是加密领域最重要的发展之一，0x提供了我们所见过的最好的框架。我们希望0x最终成为一个区块链不可知的跨链去中心化交易平台，我们期待着0x在各个方面都能取得进一步的发展。

如有任何评论或疑问，欢迎致信research@multico.in.capital。

### 披露

截至本报告出版之日，Multico.in资本管理有限公司及其附属公司（统称“Multico.in”）、对本报告做出贡献的其他人以及我们与之分享研究成果的其余人士（统称为“投资者”）可能持有本报告所涉及项目的多头或空头头寸，或拥有相关代币期权，在代币价格上涨或下跌的情况下实现收益。本报告发布后，投资者可就本报告所述项目的代币进行交易。本报告所有内容均代表Multico.in的意见。Multico.in获取的所有信息均来自其认为准确可靠的来源。但是，此类信息“按原样”呈现，不作任何形式的保证，无论是明示还是暗示。

本文件仅供参考之用，不作为任何交易的正式确认。所有市场价格、数据和其他信息均不保证其完整性或准确性，它们都基于选定的公开市场数据，并反映截至发表之日的普遍情况和Multicoïn的观点，上述所有信息都可能发生变化，恕不另行通知。

Multicoïn没有义务继续提供有关该项目的报告。报告是按所标明的日期编制的，可能因随后的市场或经济情况而不再精准可靠。

任何投资都存在相当的风险，包括但不限于价格波动、流动性不足和潜在的本金完全损失。本报告的基本价值估计值仅代表对特定代币潜在基本价值的最佳努力估计值，并不明示或暗示为对代币质量的评估、对过往业绩的总结或对投资者提供的可操作投资策略。

本文件不以任何方式构成以下任何投资的要约或邀请，包括：买卖本文件中所述的任何投资或代币；或任何根据该司法管辖区的法律将此类要约视为非法的司法管辖区内的任何代币；或Multicoïn的任何附属机构。

本文件所含信息可包括或引用前瞻性陈述，其中包括任何非历史事实陈述。这些前瞻性陈述可能被证明是错误的，可能受到不准确的假设、已知或未知风险、不确定性和其他因素的影响，其中大多数超出了Multicoïn的可控范围。投资者应在专业财务、法律和税务专家的协助下，对本文件中讨论的所有代币进行独立的尽职调查，并在作出任何投资决策前对相关市场做出独立判断。