KyberNetwork

无须信任的去中心化交易与支付服务

Loi Luu , Yaron Velner
[loiluu, yaron.velner]@kyber.network
(v0.8 版本, 2017 年 8 月 20 日更新)

摘要。我们设计并构建了 KyberNetwork，它是一个具备高流动性的数字资产（例如，各类加密代币）以及加密数字货币（例如以太币，比特币和 ZCash）即时交易和兑换的链上协议。KyberNetwork 将会是第一个实现交易所的理想操作属性的系统，比如无须信任特性、去中心化执行、即时交易和高流动性。除了行使交易所的功能，KyberNetwork 还将提供各类支付 API，以允许以太坊账户轻松地接收以各类加密代币形式呈现的付款。举个例子，任何商家现在都可以使用 KyberNetwork 的 API 来接收任意加密代币形式的用户付款，但商家会以以太币（ETH）或其他首选代币的方式来收到付款。

尽管我们是在以太坊网络上运行，但 KyberNetwork 的路线图包含了使用中继技术和类似于 Polkadot 和 Cosmos 这样的未来协议，以支持不同加密币种之间的跨链交易。通过使用这种无须信任的支付服务，以太坊账户将能够通过我们的支付 API 安全地收到比特币、ZCash 或其他加密货币形式的付款。我们也将引入衍生工具来为用户降低 KyberNetwork Crystal（KNC）及其所选择的其他加密货币的波动风险。通过这种形式，用户可以综合参与价格走势。

目录

1. 项目介绍

新兴加密货币如比特币、以太币近来越来越受到人们的追捧，当中很大的一个原因是它们允许用户在不依赖第三方的情况下以去中心化和无须信任的模式来交易并管理各自的数字资产。更有意思的是，以太坊网络图灵完备的脚本语言和无须信任的智能合约使人们能够更加容易地发行和数字化自己的加密代币。这些代币有的代表了现实世界的资产（例如 Digix Gold 代币），有的则代表了在特定平台上的使用价值（GolemNetwork 代币，Gnosis 代币，Augur 代币等）。到目前为止，最受欢迎的加密资产的总市值为 720 亿美元[1]。这一总市值在过去 5 个月中已经翻了三倍，现今仍处于增长态势。

1.1. 动机

1.1.1. 中心化的风险

随着区块链市场不断增长以及越来越多的加密资产的引入，加密代币间兑换和交易的需求也在不断地增加。例如，ETH 和比特币在各大主要交易所的日交易额高达数亿美元。而在以太坊网络中，ETH 和其他加密代币之间的总交易量（这些加密代币大部分发行时间不足两年）也达到了数百万美元的数量级。然而，尽管加密货币和加密代币具备去中心化和无须信任的特性，但大多数发生在中心化交易所中的交易依旧面临着巨大的内部欺诈和外部黑客攻击的风险。这是一个值得持续关注的问题。我们已经听说过不少关于各类交易所[2]被黑客攻击的报道，这类黑客事件不仅影响数以千计的用户，还造成高达数亿美元的损失。

1.1.2. 即时交易缺乏

现有的交易所，无论是否去中心化，都有一个通病，用户往往需要等待几分钟甚至更长时间才能够提现。

1.1.3. 现有去中心化交易所存在的问题

现已有多个团队开始在以太坊网络上组建去中心化交易所了[3]。尽管他们建立了去中心化和无须信任的交易所，但这些交易所仍然很容易受到外部操纵，因为交易指令从创建到被区块接受的过程中会存在延迟（点击这里获取更多信息）。

现有的去中心化交易所之所以难以达到预期，还有其它的原因。这些交易所保留着链上用户的交易指令集，而一旦用户选择调整或者取消竞价指令，系统的成本将会十分昂贵。交易指令的重复修改会使这个问题变得更加复杂，因为成本会逐步上升直到系统找到匹配的买卖指令。

有一个交易所[4]希望通过中间方进行价格发现和谈判流程来离线解决这个问题，链上的交易只有在交易双方就价格达成一致后才能够实现。但这就引起了一个问题：如何让交易一方相信中间

[1] https://coinmarketcap.com/charts/
[2] 比如， MtGox, Bitfinex, Shapeshift.
[3] 详情请参考 0xProject, OasisIndex and EtherDelta.

方是寻找最好的交易对手方的合适人选。我们还注意到，零手续费订单更容易受到恶意的女巫攻击或者拒绝服务攻击。

1.1.4. 数字资产种类繁杂所带来的问题

随着 ICO 项目越来越多，新的加密代币也在源源不断地增加。我们可以合理地假设投资者将获得多种所需的加密代币作为其投资策略的一部分。加密代币间的兑换对于投资者和运营者来说都是一个挑战。比如，让已经部署的合约接受新的加密代币类型作为支付方式对于任何一方而言都具有相当的难度。

此外，这一做法还可能带来更多的执行缺陷以及安全漏洞。例如，在最近的 DAO 代币 ICO 中就存在一个重大缺陷——在双方贡献金额一样的情况下，分发给 SNGLS 贡献者的代币要多于 ETH 贡献者。因此，我们有必要对网络中代币持有方、商家以及用户的支付流程进行简化。

1.2.KyberNetwork

在此，我们提出 KyberNetwork。KyberNetwork 是一个链上的去中心化交易所，为用户提供多种有用的应用——包括构建各类实用的交易 API 并将之提供给商家和用户，以便他们能够轻松且“无须信任”地即时兑换代币。这个交易所不存在交易指令集。用户会在发送交易之前获悉各类代币间的兑换率，并收到相应数量的代币。用户也无须支付任何额外的费用（除了交易所消耗的燃料费用）。KyberNetwork 通过合理定价兑换率所产生的利差获取利润。

如果在一笔交易中，某一用户只接受代币 B，我们的用户还可以通过将其现有的代币 A 兑换成另一种类型的代币 B 发送出去。更有趣的是，KyberNetwork 推出了一种新的标准合约钱包，以允许现有的合约（该合约只接受少数种类的代币）接受任意未来的代币作为付款，而无需修改合约代码。这也将允许合约或者商家访问更广泛的用户类别，并接受 KyberNetwork 支持的任何代币作为付款和贡献。

KyberNetwork 的设计中包含了几个新颖的结构来支持这些应用。

- 相比起维护一个全局的交易指令集，我们选择去维护一个储备库。在这个库内保存着适量的加密代币，以维护交易的流动性。储备库中的储备由 Kyber 合约直接控制，合约根据整体储备状况获取每个交易代币对的兑换率。这些比率由储备管理者快速更新，而 Kyber 合约将为用户选择最佳的比率。当把代币 A 兑换为代币 B 的请求到达时，Kyber 合约会检查准确数量的代币 A 是否已被记入合约，然后再将相应数量的代币 B 发送到发送方指定的地址。相应数额的代币 A 在扣除手续费之后，将被记入提供代币 B 的储备中。
- 我们推出一个新的标准合约钱包，来实现一些十分有趣的应用。具体来说，我们的新型标准合约钱包允许 Kyber 合约代表用户将用户新近兑换的代币发送到他/她的目的地址。目的地址在接收已经兑换过的代币时就好像代币是从发送方直接发送过来的，而不是来自 Kyber 合约。
- 我们的长期计划还包括采用 EVM 语言的未来功能在以太坊上构建一个高效的 ZCash-Relay（ZCash 中继链）。以太坊上的 ZCash-Relay 将使我们能够支持 ETH 和 ZEC 之间

[4] Swap.tech 和 0xproject

的跨链交易。我们还使用诸如 Polkadot 和 Cosmos 这样的未来平台，以实现更宽泛的跨链交易和支付功能。

- Kyber 合约在设计上具备高度可扩展性，这种可扩展性体现在其拥有良好的模块化构造。具体而言，我们允许动态添加任意新的代币或将现有代币从兑换列表中移除。因此，未来我们可以与任意代币或数字资产协作。

2. KyberNetwork 的设计

2.1. KyberNetwork 的参与者

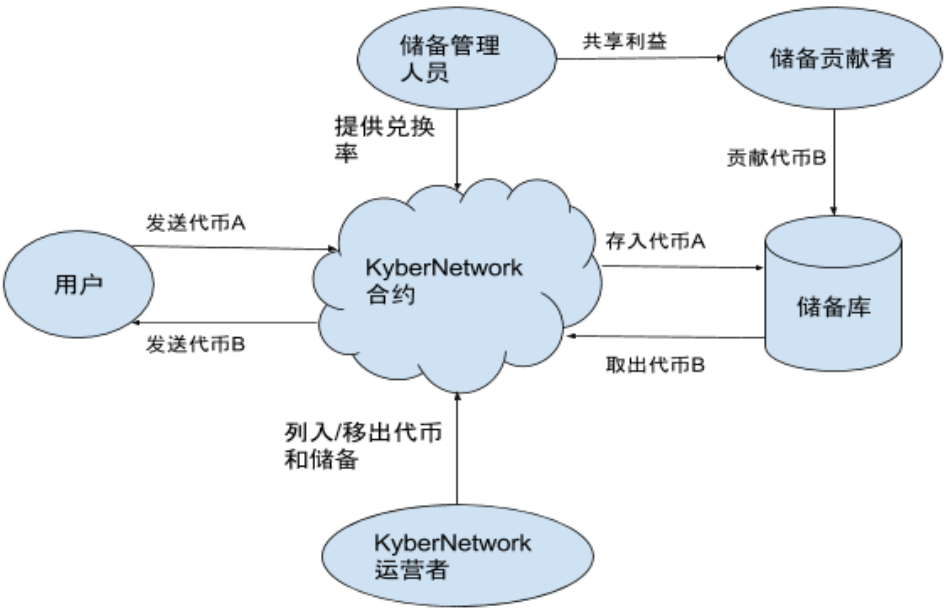
网络中的参与者共分为 5 种角色：

1. 在网络中发送和接收代币[5] 的用户。 KyberNetwork 的用户包括个人用户、智能合约账户和商家。
2. 为平台提供流动性的（一个或多个）储备实体。它可以是平台自己的储备库或者由其他者注册的造市第三方储备库。根据是否从公众那里取得贡献，储备库也被分为公共的和私有的两类。
3. 为储备实体提供资金并分享平台的利润贡献者。这类参与者只存在于公共储备库中，从公众那里接收贡献来创建储备库。
4. 维护储备库、决定兑换率并将该比率反馈给 KyberNetwork 的储备管理者。
5. KyberNetwork 运营者，负责在网络中添加、删除储备实体以及将代币对列入/移出交易列表。Kyber 团队将作为初始运营者引导平台的早期发展。后期将设置去中心化的管理来接替团队的运营者角色。

每一位参与者都以不同的方式独立地与智能合约交互。用户在单个交易中同时发送和接收代币，而无需等待来自储备实体或 KyberNetwork 运营者的任何响应。KyberNetwork 运营者负责添加和删除储备，而储备管理者每经过一个固定的周期（一般而言是几秒钟）决定新的兑换率并将该比率提供给合约。主合约依靠储备实体来保证高流动性。

下图阐述了每一个活动者间的交互过程。

[5] 在本文剩下的章节中，“代币”一词也同时指代以太币。



2.2.动态储备库

KyberNetwork 通过使用网络中现有的储备来保证高流动性。不同的储备由不同的储备管理者直接管理，这一些系列行为不一定与 KyberNetwork 的运营者有关。 KyberNetwork 允许多个储备共存（通过消除储备垄断）以获得更优的价格，（通过利用其他来源）保证更佳的流动性。此外，除了 KyberNetwork 的运营者外，该网络也允许不同的人或者机构来管理自己的储备。这样的话，KyberNetwork 就可以通过将某些低交易量的代币的管理工作转移到相应的储备管理人员身上，来实现对这些代币的支持。通过这种方式，愿意承担低交易量代币交易/兑换风险的各方都可以为自己创建这些代币的储备，并在 KyberNetwork 注册。需要注意的是，KyberNetwork 不持有任何在其上注册的储备资金。他们的资金存储在他们的储备合约中，这些合约将遵循 KyberNetwork 的基本原则。

当交易/兑换请求到达时，KyberNetwork 将从所有可处理该请求的储备中获取兑换率。然后 KyberNetwork 会选择最佳的比率并执行该请求。我们保证储备和用户都是安全的，也就是说，我们不保留任何一方的资金，并且所有的交易都是原子的。

我们注意到，在我们刚开始推出 KyberNetwork 时，它可能只有我们在网络中提供的单一储备。在其它更多的储备在网络中注册之前，该储备将成为系统流动性的主要来源。

为什么其他储备金要加入 KyberNetwork？ KyberNetwork 为储备管理者创建了一个平台，他们可以利用自身的闲置资产在平台中获利。通过为用户的交易请求提供服务，储备实体从利差中获利，而这个利差是由他们自己决定的。当然，储备实体可以随时进行交易，而不必加入 KyberNetwork。但是由于 KyberNetwork 的网络效应，他们将会获得更高的收益。此外，我们还会与钱包提供商以及其它代币项目进行合作，为 KyberNetwork 带来更多的用户。

此外，KyberNetwork 还提供储备信息面板软件，帮助储备管理者管理其储备投资组合。储备信息面板将包含标准的和流行的交易算法/策略，以便储备管理者自动定价并重新调整其投资组合。我们的储备信息面板具有足够的灵活性，储备管理者可以随时随地实施和部署各自的策略。

如何保障储备安全？储备的安全性成为 KyberNetwork 关注的重点，特别是对于由网络中其他成员作出贡献所形成的公共储备。一个最主要的担忧是，恶意的/不道德的储备管理者可能会报出一个极为糟糕的价格并根据该价格进行交易，从而把储备中的代币耗尽。

我们将储备分为两类：（1）不接受他人贡献的私人储备，和（2）接受外部贡献并与贡献者分享利润的公共储备。尽管上述担忧依旧有效，但如果私人储备的储备管理者遵循良好的安全实践，私人储备的风险敞口可以限制在可接受的范围内。尤其是，私人储备是在本地进行处理的，其它各方不能在没有得到许可的情况下进行干预。另一方面，公共储备会因其公开特性面临更大的风险敞口。为了减轻公共储备的安全风险，我们将采用无须信任的基金管理模式，比如 MelonFund（该基金由 MelonPort 开发）。这样的话，储备的贡献者无须信任储备管理者。最重要的是，我们还计划引入限制来保护开放储备。例如，储备资金只能转移到合约中预先定义的地址，例如储备合约本身以及储备与之交互的其它交易所。通过这种方式，未经授权从系统中提取资金的风险就被消除了。当然，为了避免储备管理者故意设定虚假和不合理的兑换率——例如当一个以太币只可以兑换 500 个 Golem 网络代币（GNT）时，管理者想要通过更加便宜的价格来购买到更多的 GNT，于是他设定一个以太币可兑换一百万个 GNT——我们采用链上机制（例如，防止在没有特别授权的情况下，出现不合理的价格变更）和链下机制相结合的方式来进行干预。例如，我们可以采用后台监视器的方式来监控并标记网络中储备管理者的可疑行为。当后台监视器检测到破坏网络健全度的可疑活动时，有权停止当前交易。

2.3.系统的主要构造

KyberNetwork 系统中包含以下主要构造。

- 智能合约：KyberNetwork 包括多个合约。主合约，作为用户和储备管理者进入系统的主要入口。我们也有不同的合约用来维护储备库，以及合约钱包，为 Kyber 支持的所有特点提供方便的交互。
- 用户钱包：具有友好界面的电子钱包应用程序，用于支持用户操作。与现有的钱包应用程序（如 Status，Token，Metamask 等）的结合将有助于吸引更多的用户加入 KyberNetwork。
- 储备管理者门户：通过业绩展示、网络数据统计以及支持不同策略和算法来制定价格/重新协调，从而帮助储备管理者管理储备。储备管理者通过该门户与网络（或 Kyber 合约）进行交互。
- 操作面板：帮助 KyberNetwork 运营者管理整个系统。运营者可以添加新的储备或将之删除，也可以通过该面板来更改网络参数。

最小可行产品（MVP）已经于 2017 年八月份发布，更多信息请参阅我们的博客 6。

[6] https://blog.kyber.network/kybernetwork-mvp-release-e8440a79346f

2.4.KyberNetwork 的 API 类型

KyberNetwork 支持多种适用于用户、储备实体以及储备贡献者的不同的 API 命令。

2.4.1. 用户 API

用户 API 可以由任意以太坊帐户调用，包括普通帐户和合约帐户。

Transfer（数量，源代币，目的代币名称，目的地址）

传输函数将相应数量的源代币（代币 A）兑换为目标代币（代币 B），并将 B 类代币发送到目的地址。例如，用户可以通过调用 Transfer（100,"DGD","Melon","0xb794f5ea0ba39494ce839613fffba74279579268"）将 100 个 DigixDao 代币兑换为 Melonport 代币，并将所有兑换得到的 Melonport 代币发送到地址“0xb794f5ea0ba39494ce839613fffba74279579268”。

GetExchangeRate（代币 A，代币 B）

该函数返回代币 A 和代币 B 之间的兑换率。未来我们可以支持基于交易量差异实现不同兑换率的功能。

2.4.2.储备贡献者 API

储备贡献者 API 可以被以太坊网络中的任何帐户调用，但某些 API 仅在帐户已经作出贡献时才能被调用。KyberNetwork 将有两种不同的储备类型：不允许接受公共贡献的私人储备和允许他人贡献资金的公共储备。公共储备的 API 非常类似于 MelonFund（由 MelonPort 构建的去中心化对冲基金平台）中的 API。在这里，我们只列出主要的函数。

ContributeReserve（代币类型，数量）

为公共储备贡献一定数量的某一类型的代币。在每一次贡献中，贡献者都将收到一定数量的储备代币/份额来表示他们对平台的贡献。更多技术细节，我们推荐阅读 Melonport 的绿皮书。

WithdrawProfits()

利润根据贡献者的贡献大小按比例分配。平台利润分配的确切公式将取决于储备的实施情况。

WithdrawContribution（KNC 数量，代币类型）

现有的贡献者可以从储备中赎回他们所贡献的代币。贡献者可以指定他赎回贡献时所希望收到的代币类型，我们将在后台进行兑换。

2.4.3.储备管理者 API

SetRate（代币 A，代币 B，兑换率）

设置现有的代币 A 和代币 B 交易对的兑换率。在实际部署中，此 API 会被替换为另一个不同的 API，该 API 可在单次交易中更新所有已有代币对的兑换率。批量更新的目的主要是为了降低燃料成本。

2.4.4.KyberNetwork 运营者 API

ListPair（代币 A，代币 B，初始兑换率）
添加 KyberNetwork 支持的新代币对。

DelistPair（代币 A，代币 B）
停止接收某一代币对间的交易。

AddReserve (储备地址)
在网络中添加新的储备，该储备由其本身的管理者进行管理。

RemoveReserve (储备地址)
从 KyberNetwork 中移除现有储备。移除的原因有很多，比如流动性低，价格不佳等。

2.5.支持无须信任的跨链交易

链中继技术（比如 BTCRlay）可实现不同区块链之间的通信。像 Polkadot 和 Cosmos 这样的协议在发布后将使得跨链交互变得更加容易。 KyberNetwork 将使用这些技术来实现以太坊账户接收不同加密币种付款的功能。

3. 系统属性

3.1.无须信任与安全性

KyberNetwork 运营者不持有用户的代币。因此，在我们的设计模式中，用户无须担心承受代币被平台盗窃损失的风险。由于智能合约强制/保证了运营者的诚实性，因此用户不需要相信储备实体和 KNC 代币持有者的意图。

3.2.即时交易

在单个交易中某一交易或兑换的请求会立即被执行。用户在转出自有原始代币的那一瞬间即可获取他们所要兑换的代币，无需保证金、无需确认，也无需等待时间。这种高效和用户友好型的功能将使 KyberNetwork 在现有和未来的交易所中脱颖而出。

3.3.链上交易

交易在链上进行，适用于所有账户，包括普通账户和智能合约。这种方式使得智能合约可直接与交易所进行交互，无需第三方干预，并达到以原生不支持的各类代币的形式来进行接收/支付业务的目的。此功能使我们的 KyberNetwork 可以成为适用于所有帐户的代理支付平台，包括普通账户和智能合约。

3.4.兼容性

KyberNetwork 的运行不需要对以太坊的基础协议和现有的智能合约进行任何修改。我们的支付 API 可以与现有合约进行通信，而不会对其进行任何更改。

即便如此，我们还推出了一个新的合约钱包，该钱包持有所有用户的以太币和其它代币。这个钱包允许用户把代币 A 支付给期望收取代币 B 的合约。其中，从 A 到 B 的兑换由 KyberNetwork 无缝完成。接收方收到付款时就像该款项是从原始发送方发送的一样。

3.5.与现有系统的对比

KyberNetwork 与现有系统的对比如表格所示。我们特意没有列出 Bancor，因为他们声称（私下交流）将专注于社区的代币平台，而不是通用的交易所。

交易所	交易成本[6]	无须信任	即时交易	链上	保证流动性	有效抵御攻击
Kraken/Poloniex	低	否	否	否	是	否
Shapeshift	低	否	是	否	是	否
Coinbase	低	否	是	否	是	否
EtherDelta Oasis Index	高	是	否	是	否	是
Swap.tech 0xProject	低	有点[7]	否	混合	否	不确定[8]
KyberNetwork	低	是	是	是	是	是

[7] 除了交易费用，该成本还包含执行交易的成本。
[8] 用户需要相信中间方会为他们匹配最佳的对手方。
[9] 攻击者可以创建假的订单，还无需承担任何成本。无法保证交易可以达成。

4. 应用

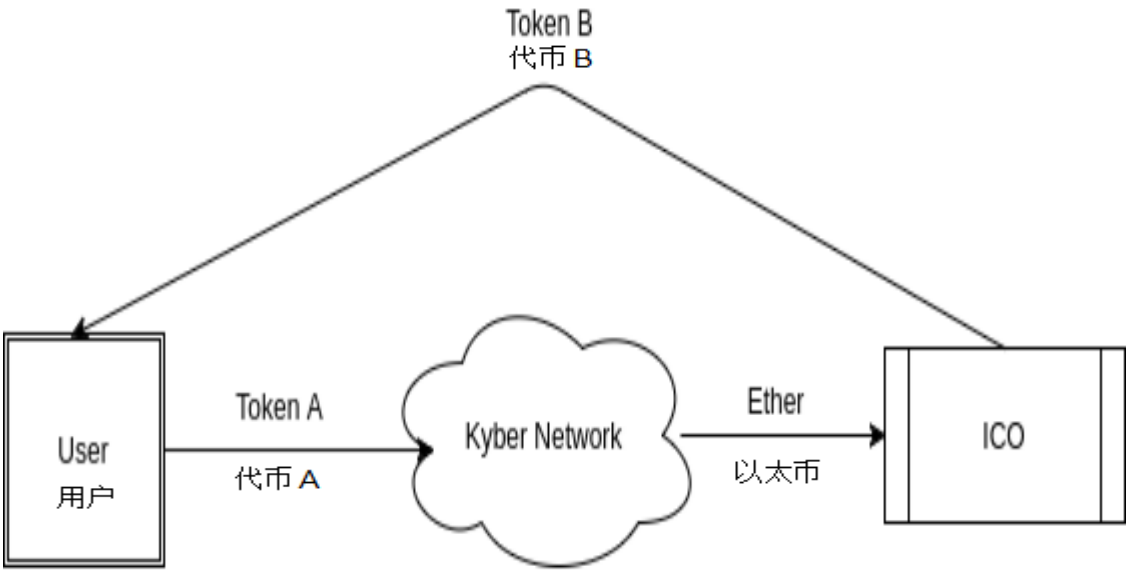
4.1.即时安全交易

首先，也是最重要的一点，KyberNetwork 是一个交易所。然而，不同于大多数交易所，KyberNetwork 能即时执行交易请求。此外，KyberNetwork 不会持有用户的代币，因此在设计上可以避免代币被盗用或丢失的情况。

这一点与大多数交易所形成了鲜明对比，因为那些交易所往往需要几分钟的确认时间。在此期间的任何故障都可能会给用户带来不便，或更有甚者，造成资金损失。

4.2.适用于任意代币的通用支付 API

通过利用智能合约来执行交易，用户可以使用任何他们喜欢的加密代币来支付任意服务或产品。合约将提供即时兑换服务，将其代币转换为以太币，并代表用户安全地将代币支付给任意他所期望的合约。下图描述了用户如何使用任意代币参与仅接收以太币的 ICO。整个过程发生在单个交易中，并且 KyberNetwork 自始至终都未持有用户代币（既不持有代币 A，也不持有代币 B）。



4.3.可信的汇率报价链上来源

其他智能合约可以看到 KyberNetwork 的兑换率。因此，网络可以引入掉期合约等高级金融工具。 KyberNetwork 提供的报价是安全的，因为它们反映了用于在两个代币之间进行交易的实际兑换率。

4.4.降低价格波动的风险

由于加密资产的流动性不足，加之供需不规则，代币间的兑换率通常波动比较大。一旦缺乏愿意把代币存入储备库的人，那么这个问题将会进一步恶化。现今加密资产的用户几乎不可能基于未来的需求进行对冲操作。KyberNetwork 将以期货和期权形式引入衍生工具来解决这一挑战，为用户提供更多的替代方案。

4.5.期货

期货是指各方同意在未来某一天以当前指定的价格交易资产的合约。 随着 ICO 逐渐成为主流，一个常见的问题是一些用户需要将代币进行兑换——比如，从 Melon 兑换为 ETH——以准备参加即将到来的 ICO。用户可以以目前的市场价格来购买 ETH，也可以把购买期货合约来抵消 ETH 价格波动的风险作为可行的替代方案。

4.6.期权

期权合约允许用户支付一定的费用（我们称之为期权费）来对冲不利的价格变动。看涨期权可以让合约的所有者以商定的价格购买加密资产，看跌期权则刚好相反。期权费是根据潜在加密资产的隐含波动率计算的。

未来准备购买或出售加密资产的用户可以通过支付期权费来购买看涨或者看跌期权。举个例子，被冻结的代币的持有人可以买入看涨期权，并在价格上涨时以约定的行权价格购入以赚取溢价。

5. 路线图

KyberNetwork 的路线图包含几个阶段。

5.1.阶段 0: 测试网部署

预计交付：2017 年 8 月（美东时间）

开发我们平台的 MVP 版本，包括 KyberNetwork 钱包，主要的 KyberNetwork 合约和我们的储备信息面板。此阶段的目的是要创建一个具备所有主要功能和应用的 KyberNetwork 的基本功能版本。 MVP 将公开发布，相关合约将在以太坊测试网上进行部署和测试。

5.2.阶段 1: 基础主网部署

预计交付：2018 年第一季度（美东时间）

此阶段我们会在主网上部署第一个版本的 KyberNetwork。我们首先着手开发支持任意代币与以太币之间进行交易和代理支付的功能。虽然我们计划与多个大型代币持有方以及其他做市商进

行合作，让他们在 KyberNetwork 上推出自己的储备，但我们的储备可能是服务于所有交易的主要储备。我们支持的代币将成为市场中高需求、高交易量的流行代币。

我们还将与 MyEtherWallet，Status，Jaxx 等电子钱包提供商合作，实现 KyberNetwork 的核心功能。由于大多数用户对自己喜欢的钱包会具有黏性，将我们的功能融入钱包会是提高 KyberNetwork 使用率的最佳方式。

5.3.阶段 2: 支持任意代币对

预计交付：2018 年第二季度（美东时间）

在阶段 1 顺利实施以后，这个阶段的目标很容易就能够实现。届时，我们预计有更多的储备（即做市商）加入 KyberNetwork。网络支持的代币数量将会增加，因为我们可以在我们的平台上获得更多的储备。

KyberNetwork 还将与其他战略合作伙伴一起构建 API，以允许其平台中的用户以各自期望的代币的形式高效地赎回代币/共享费用。例如，许多平台、项目都在采用费用分摊模式。在这个模式中，代币持有者可以分享用户在平台上所花费的费用（这些费用可能会以多种代币的形式分发）。如果这些平台使用我们相关的 API，那么在这些平台中的代币持有人就可以通过 KyberNetwork 无缝地获得符合各自需求代币形式的共享费用，比如 ETH。

5.4.阶段 3: 支持高级金融工具交易

预计交付：2018 年第四季度（美东时间）

一旦我们的开发和运营稳定下来，我们将部署 KyberNetwork 的第三阶段。在这个阶段中，我们支持交易第 4 部分所述的高级金融工具。

我们计划与去中心化的对冲基金平台（比如，由 Melonport 提供的平台）进行合作。人们可以对符合无须信任特性的对冲基金进行投资，并从高效的基金管理中获得利润。我们的团队需要在相关平台之间进行讨论、交易和构建 API，以便能够以安全的方式去实现我们的目标。同样，与那些为项目的创始人、顾问提供归属计划的 ICO 项目合作也是我们的重要目标。

5.5.阶段 4: 支持跨链交易

预计交付：2018 年末/2019 年初（美东时间）

此阶段的部署将允许用户实现以太币/其他代币与比特币、ZCash 和 ETC 等代币之间的交易。我们有两种方法来实现此目标：使用链中继技术（例如 BTCRelay 和 ZecRelay）或使用跨链通信协议（例如 Cosmos，Polkadot）。我们将密切关注这些协议的发展，并继续密切配合，以决定在 KyberNetwork 中采用哪种解决方案。

6. 众筹和 KyberNetwork Crystal 代币

一定数量的 KyberNetwork Crystal 代币（KNC）将被用于众筹来换取 Ether 贡献。KNC 的具体数量，如何分配，众筹如何进行等问题细节将在我们官网和官方博客公布。

6.1 代币的使用

储备库需要 KyberNetwork Crystal（KNC）代币来参与网络，KNC 代币也用来奖励为平台带来更多交易活动的各方。KyberNetwork 将依靠各合作伙伴，包括软件和硬件钱包，区块链资源管理器和链上智能合约，以引导用户到 KyberNetwork 平台。每引入一笔交易，这些合作伙伴将得到 KNC 奖励。

在运营之前，KyberNetwork 储备需要预购并且存储 KNC 代币。在每笔交易中，交易量中的一小部分 KNC（具体数额待定）将由储备库支付给 KyberNetwork 平台。这是储备库支付给平台的费用，以换取对平台的运营权并从平台的交易活动中获取利润。从这些费用中收集的 KNC 代币，除去营开销及支付给合作伙伴以后，余下的将***被销毁***，也就是让其不再流通。销毁的代币可以潜在提升其余 KNC 的价值，因为流通的总量减少了。为了决定网络费用，运营者将根据各个交易所的交易，将 KNC 与 ETH 的兑换率频繁地更新到 Kyber 合约中。

例如，对于 10 ETH 的交易，收取 0.01％的费用，相应的价值 0.001 ETH 的 KNC 将由选定的储备库支付给 KyberNetwork，作为使用储备控制面板和访问网络用户的费用。假设交易时兑换率为 1 KNC 等于 0.1ETH，则储备库需要向 Kyber 平台支付 0.01 KNC。帮助用户发起交易的钱包/网站将可能得到 5％的费用，或 0.0005 KNC。其余的 95％，或 0.0095 的 KNC 将被销毁，并在整个生态系统中不复存在。

随着平台交易量的增加，这种方式可以增加人们对现存 KNC 代币的需求。同时，这种方式也正好回馈了所有帮助网络生态系统成长的参与者。KNC 代币持有人可以很容易的通过合约信息追踪代币的总供应量，而并不需要依赖任何链下会计公司。

7. 致谢

诚挚感谢我们的顾问，他们是 Wong Lee Hong，Vitalik Buterin，Leng Hoe Lon, Prateek Saxena 和 Pandia Jiang，以及我们的朋友 Tsun Ngai Lee，Stelian Balta 和 Reto Trinkler。他们对本文早期的版本提出了宝贵的建议。

8. 团队

8.1. 核心成员

1. **Loi Luu**

Loi Luu 是一名研究员，专注于加密货币、智能合约安全以及分布式共识算法的研究。有关他研究内容的出版物可以在线获得。此外，他还是比特币和以太坊研讨会（如 DevCon2，EdCon，Scaling Bitcoin）的演讲常客。

Loi 相信以太坊和区块链技术的力量，他大部分的工作都围绕着这个社区。他开发了 Oyente，这是第一个基于以太坊智能合约的开源安全分析器。此后，他联合创办了另一个开源项目 SmartPool，该项目包含对现有加密货币矿池去中心化的研究。他从社区获得灵感，并创建了 KyberNetwork 项目，希望持续为区块链的去中心化及其无须信任的特点发挥热量，从而为社区带来更大的价值。

2. **Yaron Velner**

   Yaron Velner 是 SmartPool 项目的研究员和联合创始人。他的研究重点是区块链协议中的博弈理论激励机制和智能合约的形式化验证。他拥有特拉维夫大学计算机科学博士学位。他的博士论文研究了博弈理论技术在计算机程序和系统的形式化验证中的应用。

   Yaron 还是一位经验丰富的软件开发人员，拥有超过 10 年的高级软件工程师和担任 EZchip semi-conductors（该公司最近被 Mellanox technologies 收购了）技术领导的经验。在 EZchip，他是数据结构和算法团队的成员，并参与开发了基于 IP 路由的新型数据结构。

3. **Victor Tran**

   Victor Tran 是一名高级后端工程师和 Linux 系统管理员。他曾为多个社会营销平台和广告网络开发和建设基础设施，在行业内有着丰富的经验。他对构建高性能的多平台应用十分感兴趣。

   Victor 共同创立并成为几家社会营销创业公司的首席技术官。他建立并维护数个每月数百万活跃用户的平台。 Victor 目前是 SmartPool 项目的首席工程师。

4. **Cuong Nguyen**

   Cuong 是一位资深的 Web 开发人员，多年来构建了不少有趣的 Web 应用。他最近大部分时间都在尝试在诸如比特币、以太坊和 IBM 的 Fabric 账本等多个区块链平台上进行实验。

8.2. 顾问

1. **Wong Lee Hong**

   Wong Lee Hong 在他超过 30 年的职业生涯里横跨多个行业。他在消费电子、多媒体、电脑游戏、互联网和银行领域拥有广泛的分销和业务发展经验。他下半部分的职业生涯主要从事一家大型金融机构的银行业务网络开发、初创公司的战略投资风险管理。他与亚洲银行监管机构在银行技术、运营事务等相关方面都有深入交流。目前他是区块链爱好者和投资者。

2. **Leng Hoe Lon**

   Leng Hoe Lon 与新加坡国立大学共同创立了 Shentilium，旨在利用最新的数据驱动技术来推动业务决策并获得竞争优势。他还共同创立了 TrackRecord Asia，其愿景是任何人都可以学习如何在遵循专业风险管理框架的前提下，在金融市场上盈利。在此之前，他在金融行业担任过多个职位，包括 Deustsche Bank（伦敦和新加坡），JPMorgan（新加坡），ABN Amro（新加坡）。他曾担任高盛集团香港亚洲宏观交易集团董事总经理，伦敦亚洲外汇交易员。他也是全球宏观对冲基金都铎资本新加坡的首席执行官。

3. **Prateek Saxena**

   Prateek Saxena 是新加坡国立大学计算机科学研究教授，从事区块链和计算机安全研究。他的研究影响了今天广泛使用的浏览器平台、网络标准和应用商店的设计。他多次荣获包括麻省理工学院 TR35 Asia 在内的多项首要奖项。

4. **Vitalik Buterin**

   Vitalik Buterin 是以太坊的创始人和首席研究者。他也是比特币杂志（Bitcoin Magazine）的创办者和撰稿人。他在 2011 年创办了该公司，由此开启了他在加密货币领域的职业生涯。他对于创建安全、高效、可靠的系统十分感兴趣，并为密码学领域中的多个项目提供**咨询。**

5. **Pandia Jiang**

   Pandia 是灵钛科技的创始人，也是中国和世界一些以太坊研讨会的组织者。在建设和管理中国社区，提供加密业务咨询方面堪称专家。