

Bancor 协议

通过智能合约为数字货币提供持续流动性

Eyal Hertzog, Guy Benartzi, Galia Benartzi

由 Omri Ross 编辑和数学公式

2018.3.18

摘要

Bancor 协议使智能合约区块链上的自动价格发现和自主流动机制成为可能。这些智能代币拥有一个或者多个连接器，连接到持有其他代币的网络，允许用户直接通过智能代币的合约，按照一个持续计算以保持买入卖出交易量平衡的价格，立即为已连接的代币购买或清算智能代币。

关于 Bancor 协议白皮书中文版

至今我们都无法准确地描述第一次看到 Bancor 白皮书的那个不眠之夜。我们的创始人响马在团队内部群里说：“混乱无序的通证市场，鱼龙混杂的中心化交易所，都会因为 Bancor 而改变！”。与此同时，我们团队一直

Bancor 协议的命名是为了纪念凯恩斯的提议，该提议通过引入一种叫做 Bancor 的超国家储备货币，使国际货币转换成制度化（布雷顿森林会议，1944 年）。

为之奋斗的“快速建立区块链落地应用平台”的目标，也因为融入了 Bancor 而进展神速。

在接下来的日子中，我们团队成为 Bancor 协议的坚定拥护者，全员深入学习 Bancor。但是随着学习的不断深入，短短 14 页的白皮书给我们带来的感觉，是越来越多意犹未尽，甚至是隔靴挠痒。

当我们把很多疑问带给响马大叔的时候，他很诧异，因为很多的答案都在英文版的白皮书里。至此我们才发现，现在业内广泛传阅的 Bancor 中文白皮书，是一年多以前的 0.97 版，最新的白皮书并没有被翻译。

这就是这篇译文的起源。我们希望为 Bancor 协议在中国区块链的业内的推广贡献我们的力量。同时也邀请任何对 Bancor 感兴趣的同仁一起加入下方的微信讨论组。

Bancor 协议白皮书翻译小组

编译: 刘昕玮, 校对: 罗远航

出品: FIBOS 团队

2018.7.18



Bancor 学习群

目录

1	前言	5
1.1	背景	5
1.2	价值互联网与流动性	5
1.3	长尾现象	6
1.4	Bancor 流动性网络	6
2	智能代币	7
2.1	非盈利的自动化市商	7
2.2	连接器权重 (CW)	8
2.3	代币网络	9
3	价格算法	9
3.1	价格公式	9
3.2	不同 CW 下的供求关系	10
3.3	处理价格变动	12
3.4	定价的例子	13
3.5	异步流动性	14
3.6	套利均衡价格	14
4	智能代币的优势	15
5	智能代币用例和含义	16
5.1	更可扩展和可靠的代币市场	16
5.2	小规模代币的长尾	17
5.3	启用新的代币应用程序	17
6	智能代币的配置	18
7	Bancor 生态系统	19
8	Bancor 网络代币	19
8.1	网络代币	19
8.2	BNT 代币发行活动	20
8.3	捐赠分配	20

目录	4
9 总结	22
10 致谢	23

FIBOS.10

1 前言

1.1 背景

我们生活在一个任何人都可以发表一篇文章，建立一个讨论小组，或者经营一个网上商店的世界里。低准入门槛使用户生成内容和平等参与得以出现，成为互联网时代的关键特征。我们正在见证用户生成的数字资产的出现。几个世纪以来，人类以纸币、债券、股票、礼品卡、积分、社区货币等多种形式发行和流通了各种各样的代币。2009 年，比特币 [1] 引入了一种基于加密共识的去中心化数字货币的概念，随后出现了一大波新的数字资产，即加密货币，俗称代币。

代币可用于管理服务的访问权限、作为众筹项目的出资证明、去中心化应用程序的激励、借据、本币、真实资产的所有权证明等等。它们通常是通过智能合约的“代币发行活动” (*Token Generation Events, TGEs*) 众筹发行的。智能合约是一个简单的软件程序，一旦提交到区块链，只要下层的区块链仍在运行，它就可以保证不可篡改。智能合约具有许多与常规区块链相同的能力，例如：它们可以调用其他智能合约，和持有被第三方保管的代币。一个明确的智能合约可以被视为可靠、廉洁、完全自动化的中间商。这使得智能合约特别适合发行和管理代币这一机械而又敏感的任务。

1.2 价值互联网与流动性

尽管不同代币的用途和特征不同，但是它们都可以抽象地表示某种经济价值。世界各地的代币所有者将交换代币作为他们日常业务的一部分，由此产生了价值互联网。目前，连接这个互联网的链接是互相买卖的交易者，不管是直接交易还是通过交易所之类的第三方服务进行交易。

不像互联网交换机之间始终接通、随时可以传输任何数据的电缆，代币交易之间的联系是短暂的，意味着为了让代币通过这个互联网，必须有一个买家和一个卖家（数字化地）同时存在于同一地点。这种在买家和卖家之间持续寻找匹配的挑战，在经济学上被称为“双向需求巧合 [2]”。为了使代币能够有效地参与全球代币经济（即价值互联网），它的交易量必须跨越一个关键的障碍，即买家和卖家之间的匹配必须频繁到足够可靠。这种交易的可靠性被称为流动性。如果一种代币易于实现买卖而不会持续影响其价格，我们就称这种代币为流动的。对那些最广泛使用的代币而言，流动性不是问题，但对于那些小额交易的代币（比如用于利基 DApp 的代币，或用于小

型本地社区贸易的代币)，或者认购量很低的新代币而言，流动性是个明显的障碍。

就像大部分人不能访问互联网，是因为他们生活在偏远地区，连通对“链接”提供者而言还不够经济，大量的人不能参与到价值互联网，是因为他们拥有非流动性代币但缺乏“链接”，即通向大规模代币经济的、被视为流动和可靠的“链接”。在传统金融市场中，做市商解决流动性问题的方法是始终买进或卖出金融资产，即便市场对这些金融资产缺乏兴趣。这些是典型的大型金融机构，他们以市场流动性不足、和能承受流动性不足引发的巨大风险为基础，通过可观的资本储备来创造利润。他们利用向买方和卖方提供不同报价，长期赚取其中的价差。

在区块链领域，效仿传统做市商的方法来解决流动性问题，不但将违背剔除中间商的精神，而且将从新代币经济的重要资本持有人当中，形成明显中心化的金融权力。

1.3 长尾现象

如今，排名前 10% 的代币占整个代币市场市值的 95%，占有代币交易量的 99%（基于对 [CoinMarketCap](#) 上列出的 1000 多个代币的分析）。尾部的（即剩下的 90%）代币几乎无足轻重。这与许多其他在线生态系统形成了鲜明对比，在那些生态中，尾部累积在总量中占据明显比例，这种现象被称为长尾现象 [3]。如，销量小到无法在传统书店销售的书籍，估计占了亚马逊销量的 30%-40% [4]。一旦消除了形成长尾的障碍，长尾立刻开始出现。YouTube 使视频易于上传和观看，博客平台也让人们容易发布他们的内容。一个能够用于创造流动性代币的简单途径，就是阻止用户发行的货币形成长尾的障碍。

1.4 Bancor 流动性网络

在本白皮书中，针对去中心化的流动性，我们提出了基于 Bancor 协议的 Bancor Network，该协议能利用智能合约在代币中直接创建流动性。这种代币，我们称之为“智能代币”，它们始终可以通过它们的智能合约直接进行买卖。换句话说，代币的合约会一直向买家出售或向卖家收购代币。每个智能代币都有一个或多个连接器将智能代币与网络中的其他代币连接起来。这些连接器持有一定数量的其它代币，从而在智能代币和连接器持有的代币（或者说它的连接器代币）之间建立关系。智能代币连接器使用一个公

式（下文将详细阐述）在智能代币及其连接器代币之间建立价格关系。连接器的余额按照计算出的价格，为智能代币和它的任意连接器代币提供流动性。

所有的智能代币都是与 ERC20 兼容的代币，这意味着它们与任何支持以太坊代币的系统和服务都兼容。智能代币标准的结果是一个始终连接的价值互联网，因为每个代币都能自动维持连接器代币世界的流动性链接。通过提供一个现代的、高效的、全自动的流动性解决方案，我们相信 Bancor 协议能成为用户发行代币实现长尾的技术，从而为数百万小规模、用户发行货币的多元化经济铺平道路。这种多元货币的模式是可扩展的和去中心化的。

2 智能代币

2.1 非盈利的自动化市商

智能代币是 Bancor 协议的核心。智能代币的操作和常规代币无异，它遵循以太坊区块链 [6] 上使用的 ERC20 代币标准 [5]，但是其中也包含额外的逻辑，这使得用户总是能够通过自己的智能合约直接购买和销售这些智能代币，价格根据供求关系以算法进行调整。引人注目的是，智能代币具有内置的流动性机制，确保它们可以持续地与其他代币进行兑换。

为了实现这一点，每个智能代币都配置了连接器模块，这些连接器模块持有它们连接的另一个代币（例如，BNT 智能代币有连接到 ETH 的单独的连接器，它持有一定数量的 ETH）。通过把智能代币发送到它们的合约中，购买者可以使用任何连接器代币来购买智能代币，之后将发行对应数量的新的智能代币，这些新的代币将自动转账至买方。换句话说，任何人都可以通过将连接器代币存入智能合约来购买智能代币。在这种情况下，一旦新的代币被发行，智能代币的连接器余额和智能代币的供应量都增加了。类似地，卖方可以向其智能合约发送任何数量的智能代币，然后将这些智能代币从流通中移除，并从连接器余额中提取相应数量的连接器代币，并将它们发送给卖方。在这种情况下，连接器余额和智能代币的供应量都减少了。为了知道买方需要代币以及卖方需要提取多少代币，智能代币不断根据供给和需求重新计算它相对于它的每个连接器代币的价格。Bancor 公式（下文将详细阐述）通过在智能代币的值和它的连接器余额之间维持一个固定比率（称为权重，下文将对此进行讨论）来实现这一点。智能代币的适应性供应

(回想一下,它是在购买时新发行的,在出售时从流通中被移除)是一种独特的功能,使供应能够根据需求调整(不影响单位价格),并使智能代币能够持续被购买。在未来,Bancor 协议还将使用传统的固定供应量的方式使智能代币配置标准化。

虽然允许代币对自己进行发行和清算(增加和减少自己的供应量)可能听起来不太可靠,但这个逻辑是运行在不可篡改的区块链上的透明的(可公开查看的)智能合约中。此外,只有当连接的代币余额在其任何连接器中增加(通过购买)时,智能代币才会以算法计算的方式增加,如此确保了智能代币始终与链接到的另一个代币之间维持着某个比率值,从而防止意外发生。

目前,智能代币可以通过它的智能合约持有任何 ERC20 标准的代币,来连接到任何符合 ERC20 标准的代币。这使得 Bancor 协议与目前的大部分代币向后兼容。将来,Bancor 计划支持智能代币跨越多个区块链连接各种代币。

实际上,智能代币扮演着完全自动化和去中心化的市商的角色,通过在区块链上的网络体系结构中进行操作,它可以作为有效的和自主的兑换渠道,而不依赖于现有的基于手动的贸易方式以及不依赖于附带的牟利动机。

2.2 连接器权重 (CW)

如上所述,连接器的权重 (CW) 表示智能代币的总价值(其供应量 \times 单价)和对应连接器的余额价值之间的固定比率。智能代币的创建者为每个连接器指定所需的比率。由于连接器的余额和智能代币的总价值(有时称为“市值”)都会随代币的买卖而波动,因此会通过 Bancor 公式保持该比率不变。因为每次购买或出售智能代币都会触发连接器代币和智能代币数量的增加或减少,因此智能代币相对于其连接器代币的价格将不断地重新计算以保持恒定的连接器权重 (CW),即代币发行者指定的比率。这个比率决定了一个智能代币的价格需要调整多少,才能在每笔交易中保持稳定,换句话说,这一数值表示了价格的敏感性。连接器余额和智能代币数量之间的比率越高,价格敏感度就越低,这意味着每一次买卖都会对智能代币的价格走势产生相对柔和的影响。连接器余额和智能代币之间的比率越低,价格敏感性就越高,这意味着每一次买卖都会对智能代币的价格走势产生相对强烈的影响。可以说,更高的连接器权重会导致智能代币与其连接器代币之间的相对价格比较稳定,而较低的权重会导致智能代币与其连接器代币之间的

相对价格的波动性更强。第 3 节进一步阐述了代币定价算法，并根据智能代币的品质来对连接器的权重进行选择。

智能代币连接器可以被视为去中心化的、自主的、透明的和可预测的市商，而不是交易所。智能代币通过算法调整它们的价格以保持它们与智能代币的总代币值之间的恒定比率，来保持连接器的余额。由于它们的逻辑是透明的，而且是不可篡改的，所以总能预测一个智能代币的购买或销售将如何影响其价格，这最终将导致更稳定的代币价格。这种公式化的机制使得智能代币成为供求关系中的可靠中介。

2.3 代币网络

智能代币允许在它们自己和它们的任何连接器代币之间进行即时转换。这个功能能让一个智能代币立即转换为任意数量的以类似方式连接到同一网络的其他代币。换句话说，通过网络，智能代币可以立即转换到它的任何一个连接器代币，也可以转换到它的任何一个连接器代币的连接器代币，等等。

假设一个智能代币 ABCCoin 有一个连接器，该连接器持有一定数量的 XYZCoin。此外，假设另一个智能代币 NEWCoin，其连接器也持有 XYZCoin。那么先将 ABCCoin 转换为 XYZCoin，然后将 XYZCoin 转换为 NEWCoin，用户就可以把 ABCCoin 转换为 NEWCoin。用户只需要进行一个操作，以上过程将在后台无缝完成。

此外，NEWCoin 本身可能会连接到其他代币，从而扩展了连接范围。通过这种方式，智能代币可以传递地连接到无限数量的代币，从而创建一个去中心化的流动性网络，该网络能够连接由数百万个代币组成的价值互联网，所有代币都能够以持续计算的比率进行相互间的自动转换。

3 价格算法

3.1 价格公式

Bancor 算法定价公式是系统设计和潜力的核心，因为它使得智能代币始终能够确定自身可靠的、可预测的价格，这对大规模采用代币而言至关重要。该公式建立在一个概念上，即前一节中介绍过的：每个智能代币都会在智能代币的总价值（其供应量 \times 单价）和对应连接器的余额之间维持一个

比率。我们称这个比率为连接器权重，简称 CW 。

$$CW = \frac{\text{连接器代币余额}}{\text{智能代币总价值}}$$

智能代币的总价值，即它的市值，表示的是以当前价格出售所有代币（全部智能代币供应量）所能获得的金额。智能代币的价格按照连接器的代币计价（例如，BNT 的价格以 ETH 计价，ETH 是其连接器的代币）。

$$\text{智能代币总价值} = \text{代币单价} \times \text{智能代币总供应量}$$

这些关系是 Bancor 定价算法的关键，因为它们允许系统使用代数方法解决智能代币的定价，其价格由 CW 、连接器代币余额、以及智能代币结余供应量所决定。

$$\text{代币单价} = \frac{\text{连接器代币余额}}{\text{智能代币结余供应量} \times CW}$$

在任何给定的时间，每个连接器总是精准地记录着它的连接器代币余额以及当前的智能代币的供应量，所以它只需要知道 CW 就可以在连接器余额变化时以及其代币供应量变化时持续计算出正确的智能代币价格。 CW 表达为介于 0% 与 100% 之间一个百分数，如前文所述， CW 的初始值是在配置智能代币之初由代币创建者指定的。 CW 的值明显影响代币的定价，且可以修改，取决于智能代币的设定。

3.2 不同 CW 下的供求关系

图 1 显示了在不同的 CW 值下智能代币的价格如何对需求变化作出反应。让我们大致讨论一下所举的例子：

- a) 第一种例子是 $CW = 100\%$ ，在这种情况下，不管需求如何变化，智能代币的价格永远不会因其连接器代币余额或供应而改变。价格有效地与它的连接器代币余额挂钩，智能代币成为了该值的代理。这可以被比作金本位的货币制度，在该制度下，发行机构承诺货币价值与特定数量的黄金挂钩。例如，1971 年之前，美元与黄金挂钩的汇率是每盎司 35 美元。
- b) 第二种线性的例子是 $CW = 50\%$ ，其中智能代币价格随供应量线性变动（随连接器余额的增加或减少而变动）。当需求较低时（当销售量大

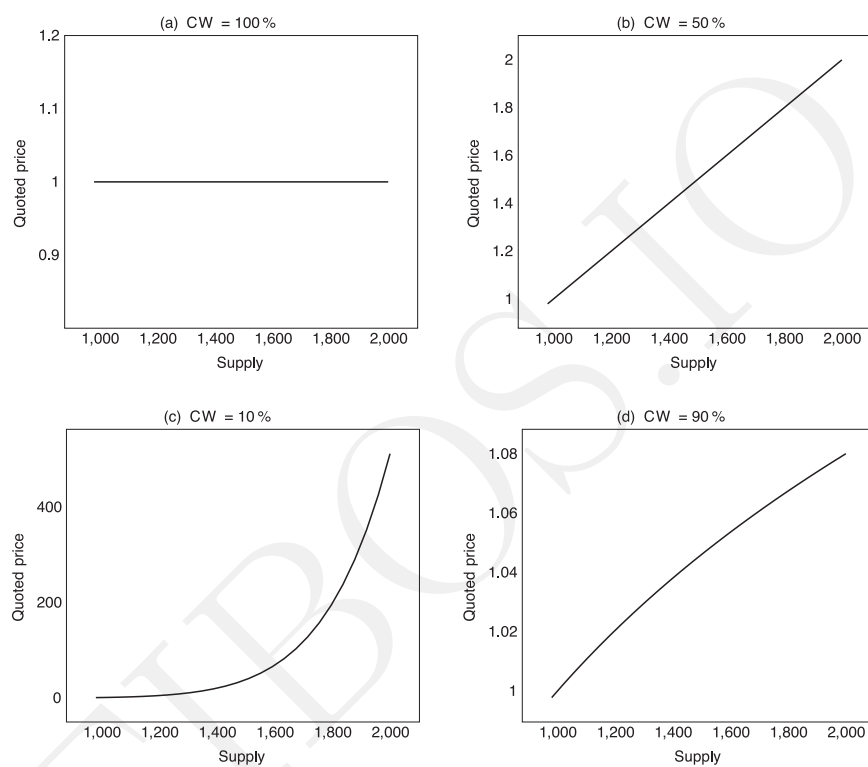


图 1: 显示了不同 CW 下智能代币的价格与其供应量的关系。表中初始价格为 1, 智能代币的初始供应量为 1000, 但是, 由于只有 CW 定义价格的弹性, 对于不同的初始价格和供应量, 曲线的走向是大致相同的, 尽管坐标轴上具体的值会不同。

于购买量时)，智能代币的价格会下跌；当需求量较大时（当购买量大于售出量时），智能代币的价格会上涨。这种关系是供求关系的典型运作方式，唯一的不同是，一个智能货币的供应量不是固定的，而是由需求决定的，而且供应量上涨也不会稀释单价。

- c) 第三种非线性例子是 CW 介于 0% - 50% 之间，显示了价格和供给之间的增长关系类似，但随着供给的增加，价格曲线增长更为迅猛。该图表显示了 CW = 10% 的特定价格曲线。低于 10% 的 CW 值会比这个反应更强烈（更尖锐的指数曲线），而高于 10% 的 CW 会在接近 50% 的时候相对趋于线性（如图 b）。
- d) 最后一种同样非线性的例子是 CW 介于 50% - 100% 之间，价格和供给之间增长关系的曲线看上去不如图（b）那么迅猛，这意味着智能代币的价格对供应量的变化越来越不敏感，直到 CW 达到 100%，曲线就和图（a）一样了。该图表显示的是 CW = 90% 时的价格曲线。

理论上，一个智能代币的 CW 值也有可能大于 100%，但是，这是一个特例，当需求增加时代币会变得更便宜，这一特例超出了本文讨论的范围。

3.3 处理价格变动

上文中，我们给出了在任何指定时间确定智能代币价格的公式。但正如图表所示，当购买或出售智能代币（从而增加或减少其供应量）时，它们的价格会变化！事实上，即使最微小的交易也将使智能代币价格变化到一个新水准，这意味着如果买家将订单拆分成许多小的交易，将得到一个不同的价格。为了解决这个问题，在我们需要计算换算价格时，我们查看智能代币必须返还多少代币给买家（在新发行的智能代币中），或者卖家（在连接器余额中取出的连接器代币中）会收到多少代币（不管是来自买家的连接器代币，还是来自卖家的智能代币）。

$$\text{代币新发行量} = \text{代币当前总供应量} \times \left(\left(1 + \frac{\text{支付的连接器代币数量}}{\text{连接器代币余额}} \right)^{CW} - 1 \right)$$

这个公式的推导过程是将一笔交易视为很多笔无穷小的交易，每笔无穷小的交易都影响智能代币的供应和连接器余额，由此每次后续增量都将导致新价格。一笔特定数量交易的实际价格，是这笔交易包含的每个无穷小

增量对价格造成影响之后得到的最终价格。[这里有一个正式的数学证明](#)。这个等式对于买单和卖单来说是很类似的，对于智能代币合约收到特定数量的代币，我们知道需要发行多少智能代币（给买家）或者从连接器余额中取出多少连接器代币（给卖家）。

$$\text{取出的连接器代币} = \text{连接器代币余额} \times \left(\sqrt[{\text{CW}}]{1 + \frac{\text{被销毁的智能代币数量}}{\text{代币当前总供应量}}} - 1 \right)$$

我们现在可以通过连接器代币与智能代币之间的汇率来计算一笔交易的有效价格，即智能代币相对于连接器代币的价格。交易的规模不同，实际价格也不同，并且对于具有多个连接器的代币来说，不同的交易规模，所有的连接器代币相对于智能代币的有效价格也不同。

$$\text{有效价格} = \frac{\text{参与兑换的连接器代币的数量}}{\text{参与兑换的智能代币的数量}}$$

有效价格有一个特性，累计金额相同的十笔小交易和一笔大交易将导致完全相同的费用。

3.4 定价的例子

我们来看一个例子，一个当前总供应量为 1000 的智能代币，它的连接器拥有 250 数量的连接器代币，CW 值为 50%，此智能代币可按以下价格转换为其连接器代币：

$$\text{价格} = \frac{250}{1000 \times 50\%} = 0.5$$

假设买家想要将 10 个连接器代币转换为智能代币。她会收到多少智能代币呢？

$$\text{代币新发行量} = 1000 \times \left(\left(1 + \frac{10}{250} \right)^{50\%} - 1 \right) \approx 19.8$$

根据新发行的智能代币的数量，我们现在可以得出 10 个单位的连接器代币转换为智能代币时的有效价格：

$$\text{有效价格} = \frac{10}{19.8} \approx 0.5051$$

请注意，有效价格与挂牌价格是不同的，在这个例子中，有效价格会稍微高一些。这种差异是由于前一节中所解释的这个特定交易规模引起的价格变动。换句话说，通过增加到连接器余额和智能代币的供应量中，10 个代币交易中的每个无穷小增量单位都导致了价格上行压力。实际上买方已经为自己的交易导致的价格变动付出了代价。在将代币发送给智能合同之前，买方能够进行这些计算，这使她能够准确地判断代币价格将如何随着她的兑换而变化。价格变化的可预测性和一致性是 Bancor 公式的一个关键益处。

3.5 异步流动性

在智能代币的转换过程中，价格将趋向于买卖量之间的均衡。在传统的交易模式中，买卖双方为了互相匹配，必须具备有效的流动性保证两个订单随时可靠地匹配。这在 Bancor 协议中不是必须的，因为智能代币总是立即处理购买和销售（通过其连接器余额转换它们），因此会不断地计算价格。传统上单独计算每笔交易的价格（当买卖双方匹配时），而每笔智能代币的兑换都会逐渐地、直接地影响其价格。这使得 Bancor 的价格决定机制是真异步的。

3.6 套利均衡价格

智能代币也可以在不同的交易所进行交易，它们的市场价格可能会与智能代币的挂牌价格相背离。由于智能代币不具备观察外部世界价格的功能，似乎存在智能代币价格碎片化的风险。然而，这种情况不太可能持续太久，因为它形成了一个明显的套利机会。例如，如果市场价格高于智能代币的报价，任何人都可以从智能代币购买并在市场上出售，直至价格持平。套利能力能够激励市场参与者在智能代币和外部价格之间达成价格共识。

同样值得注意的是，智能代币发行新代币以及增加总供应量（当连接器代币被添加至连接器余额时）的功能，只有在与智能代币直接交互时才有效。在外部交易所上市、买卖的智能代币，或直接在人与人之间转账，不会触发这种功能，而是流通已供应的代币。尽管如此，通过前文所述的套利机制，现有供应量下的价格将对智能代币的价格产生影响。

4 智能代币的优势

智能代币是代币市场上的一种新模式，因为它们将自动化的和去中心化的代理结合在一起，这些代理按照精确反应市场供需关系的价格，持续完成交易，并且根据兑换规模实时调整。与传统的基于交易所的交易相比，这带来了多种优势：

连续流动性 用户总能通过智能合约在网络中直接购买或出售代币，即便市场中只有很少或者没有其他买家或卖家。因为价格会根据兑换规模进行调整，所以总可以使用特定价格来兑换代币。Bancor 协议有效地使得流动性与交易量脱钩。

没有内置手续费 默认情况下，智能代币不会对它们执行的兑换收取费用。用户承担的唯一费用是处理下层区块链交易所需的费用（例如，以太坊的 gas）。虽然智能代币的发行者可能为通过他们的特定智能代币进行的兑换设定可选的使用费（称为捐赠）。Bancor 协议不会为了获取运营利润而收取兑换费用，而是从代币网络的扩展以及用户数量的增长中获利。

可调整的价格敏感度 大量连接器余额和高权重的带来的影响，是使得智能代币价格对大宗交易导致的短期投机和价格波动更不敏感。例如，一个 CW 为 10% 的智能代币，相当于交易所里一个占代币市值 10% 的订单。这种灵敏度可以通过 CW 和连接器余额进行调整，以实现特定智能代币的预期配置。

没有价差 Bancor 公式在处理买单和卖单时使用同样的价格计算方法。这与传统交易所不同，传统交易所的买入价格总是低于卖出价格。买卖价差，即所谓的价差，是传统的做市商赚取利润的原因。如上所述，Bancor 协议不会为了运营而获得这种利润，另外为了鼓励采用该网络，可能会引入去中心化的价差，从而使所有参与者受益。

价格可预测 智能代币的价格算法是完全透明的，允许用户在执行兑换之前预先计算他们想要兑换的有效价格。这与传统的以订单为基础的交易所形成了鲜明对比，在传统交易所，大量订单可能导致价格不可预测地下滑至明显不同的水平。

兼容 ERC20 智能代币是与 ERC20 兼容的代币（尽管具备额外的功能），它们与现有的代币应用程序（如钱包或 DApp）无缝集成，因为它们符合流行的 ERC20 代币标准。此外，任何现有的 ERC20 标准代币都可以通过带有连接器的智能代币连接到 Bancor 网络，这使得 Bancor 协议向后兼容现有的 ERC20 代币。我们在下面的第 6 节详细阐述了多种智能代币配置。

5 智能代币用例和含义

我们认为 Bancor 协议的独特属性使它适合各种用例，从为现有代币提供更可靠的交易基础设施，到促进小型代币长尾的出现，再到促成全新形式的创新代币市场行为。在下面的部分中，我们将对一些用例进行深入探讨。

5.1 更可扩展和可靠的代币市场

用于去中心化流动性的 Bancor 网络可以作为中心化交易所的替代，用于连接到网络中的任何代币，并带来诸多积极意义。例如，一个带有两个连接器的智能代币，其 CW 值为 100%，其功能类似于去中心化代币交易对。我们将这种智能代币称为中继代币。（我们会在后续章节中详细阐述这种智能代币和其他特殊智能代币。）中继代币允许用户通过一个即时的两步过程在两个连接的代币之间进行转换，即使用其中一个连接器代币购买中继代币，然后立即将其出售给另一个连接的代币。由于定价算法，这将导致中继代币相对于连接器代币的价格上升（由于购买），和中继代币相对于连接器代币的价格下降（由于出售），这与预期完全一致。如前所述，中继代币的挂牌价格不太可能长久地与外部交易所中任何一个连接器代币的价格明显抵触，因为套利机会鼓励套利者在中继代币相对于连接器代币的价格与其在其他市场上的价格趋于相同。这种特殊的智能代币配置允许不符合 Bancor 协议的现有标准代币（没有连接器）也可以向后兼容（换句话说，通过中继代币与网络中的每个代币进行转换），从而增强了可行性并接触到流动性网络。

此外，当用户通过智能代币转换代币时，用户不需要直接与交易对手方进行交易，也不需要将代币存放在交易所中，从而降低黑客劫持代币或者交易所业务结构性挑战带来的风险。这与 MtGox 和 Bitfinex 的痛苦经历形成鲜明对比，即黑客从用户帐户中窃取了价值数百万美元的加密货币，或者可能在代币可用性上忍受长时间的延迟。通过在一个去中心化的、自治的、低

成本的网络中聚合流动性，用户可以从更大的、持续的流动性和相对的价格稳定中获益，而不是在如今支离破碎的、面向交易的市场格局中获益。

5.2 小规模代币的长尾

智能代币提供了一个解决流动性问题的创新方案，这个问题阻碍了小规模代币或新发行的代币形成长尾现象（见第一节）。试想，缺少足够数量的买家和卖家意味着现有的绝大多数代币实际上没有任何交易，尽管小规模代币也有许多有效的用例，比如众筹、本地商业、社区协作等。

例如，一个想要募集资金录制专辑的音乐家可以创建一种新的代币，并承诺出售专辑只用这种代币。然后，她可以发起一场众筹活动，按照支持者的捐赠比例来向他们发行代币。竞选期间捐赠 1% 的支持者可得到所有代币的 1%。如果专辑获得成功，对这一代币的需求将会增加。

到专辑发行时，这个代币的活跃度可能已下降到鲜有最初的支持者愿意卖掉他们的代币。在目前缺乏流动性的小规模代币市场，对专辑感兴趣的人可能买不到所需的代币。由于 Bancor 智能代币总能对自己进行买卖，潜在的唱片购买者可以用根据当前的买卖量数学计算出的价格、及时得到他们需要的代币。尽管买家可以通过合约购买智能代币，而不仅仅通过卖家购买，现有代币持有者也不会错过，以后价格诱人时他们可以把智能代币卖回合约。这突出了 Bancor 协议流动性的真异步特征。

还有许多通过用户发行代币获益的小项目例子，包括鼓励人们参与本地社区的小区代币、用于优先访问有限资源（如计算能力）等的平台代币。毫无疑问，随着智能代币的应用促成成千上万种不同代币的长尾，我们肯定会看到许多用户发行代币的新颖应用，不论大小。如今，所有这些潜在的创新都受制于自主和异步流动性的不足，这给代币创造者带来了“鸡生蛋蛋生鸡”问题，为了提供最初支持所需的流动性，他们需要先确保交易活动有规模。

5.3 启用新的代币应用程序

智能代币不仅可以解决保证代币转换安全、初始化、连续代币缺乏流动性等现有问题，而且还可以在新兴的区块链世界中启用全新的应用程序。

考虑一下智能代币作为去中心化的代币数组的例子，由于它们有许多连接器。一个拥有大量连接器且 CW 为 100% 的智能代币，可以作为一个去中心化的代币，来跟踪给定的（和由用户配置的）一组其他代币的价值。

套利者可以通过它确保智能代币的价格与外部市场同步，这意味着智能代币的价值永远是最新的。这些智能代币允许用户直接持有这种类型的代币，而不需要任何金融服务商作为中介。

另一个例子可能是一个去中心化的应用程序，其智能合约需要代币汇率信息。常规做法是依赖可信任的第三方将信息转发到区块链上，但是使用 Bancor 协议，这些智能合约可以简单地通过任何智能代币直接查询当前价格。智能代币充当链上价格观察者的角色，免除了外部输入的必要。

类似地，现在可以创建能够交换服务（通过代币）的去中心化应用程序。例如，可以通过 Bancor 的链上兑换机制，来集成两个需要使用不同代币进行支付的服务。

由于降低了流动性障碍和其他障碍，代币长尾出现时我们能找到更多例子，就像创建代币的技术便利。

6 智能代币的配置

虽然智能代币的新配置会不断涌现，但是目前智能代币的配置分为如下几类：具有一个、两个或多个连接器的智能代币；CW 为 100% 或 100% 以下的智能代币；以及具有单一未激活连接器的智能代币。虽然所有的智能代币共享某些属性，但是每个配置组合都有一些不同的属性。

CW 低于 100%（通常低于 20%）的智能代币被称为流动代币。它们可能有一个或多个连接器。例如，BNT 是一个具有单个 10% ETH 连接器的流动代币。流动代币可以购买和出售任何连接器代币（使用 Bancor 公式来确定其相对于连接器代币的价格），并根据购买或出售调整总供应量。

CW 为 100% 的智能代币也可以有一个、两个或多个连接器。使用一个连接器、CW 为 100% 智能代币被称为代理代币。使用两个连接器、CW 为 100% 的智能代币称为中继代币。使用三个或多个连接器、CW 为 100% 的智能代币称为数组代币。代理代币、中继代币和数组代币可以购买和出售任何连接器代币（使用 Bancor 公式来确定其相对于连接器代币的价格），并根据购买或出售调整总供应量。任何代理代币、中继代币或数组代币中的连接器代币，可以是其他智能代币，或任何符合 ERC20 标准且总供应量不变的代币，从而允许现有的 ERC20 代币与 Bancor 网络向后兼容。

具有单一未激活连接器（也就是连接器余额为 0）的智能代币被称为奖金代币，它适合向早期持有者（比如社区支持者）分发未来将要发行的代币。

当往奖金代币中存入连接器代币时，奖金代币将会成为流动代币，可以跟新的连接器代币兑换。

被其他智能代币的连接器作为连接器代币的智能代币，被称为网络代币。（第 8 节有更多说明）。例如，由于许多智能代币在其连接器中持有 BNT，以便与 Bancor 网络集成，因此 BNT 可以称为网络代币。BNT 也是一个流动代币。

7 Bancor 生态系统

Bancor 去中心化流动性网络的成功取决于不同用户的参与程度。我们将简要介绍参与者可在 Bancor 生态系统中扮演的关键角色。

交易者 持有、兑换和转账智能代币的终端用户。

智能代币发行方 发行新的智能代币的个人、公司、社区、组织或基金会，他们限定了智能代币的初始供应量、价格、CW，并管理代币的初始发行。这也包括中继代币的创建者，它可以将任何现有的 ERC20 代币连接到网络。

资产代币化发起者 代理代币或者数组代币的发行者镜像其他区块链上的真实资产或代币。这可以让智能代币连接到更广泛的资产组合，如比特币、货币、黄金或其他新兴的区块链代币。

套利交易者 监控流动性网络中与外部交易所或其他智能货币价格不一致的交易者，然后通过套利恢复价格的一致性。套利交易者天然地激励价格保持一致，因此是 Bancor 生态系统的重要参与者。有关 Bancor 协议中套利机制的进一步解释，请参见第 3.6 节。

8 Bancor 网络代币

8.1 网络代币

在第 2.3 节中，我们描述了带有两个连接器的中继代币是如何通过其中一种连接器代币转换为另一种连接器代币，这一过程分为两步，先为一种连接器代币购买中继代币，然后为另一种连接器代币出售中继代币。如前所

述，这两步过程可以实现网络中的任何代币对任何其他代币之间的兑换，前提是它们至少有一个共有的连接器代币，不管多分离。我们称这种共有的连接器代币为网络代币，因为它将许多不同的智能代币连接到一个代币网络中。

根据本文描述的 Bancor 公式自动定价机制，网络代币通过将其网络中的所有智能代币相互转换来充当“代币的代币”。在这样的网络中增加购买任何代币也将增加网络代币的供应（因为通过将网络代币存入连接器余额中增加了其子代币的供应）。这种对网络代币供应的上行压力反过来又会影响其网络中的其他每个代币，因为它们的连接器代币余额增加了。

网络代币模型创建了成员智能代币之间的协同关系，就像是每一个成功的以太坊服务都可以提升以太币的价值、促进整个以太坊平台和生态系统。对于这样的网络模型，有许多用例存在，包括社区货币的区域网络、视频游戏工作室发行的所有游戏共享的积分、一组独立商家支持的联合会员项目等等。网络代币也可以是其他网络的一部分，通过实现它自己的连接器。

8.2 BNT 代币发行活动

第一个发行的智能代币是 Bancor 网络代币 (BNT)，它用作网络代币的枢纽，连接 Bancor 网络中的所有代币。BNT 目前只有一个 ETH 连接器 (CW 为 10%)，并且由瑞士非营利组织 Bprotocol 基金会进行管理，该组织的核心目标是将 Bancor 协议推广为智能代币的全球标准，通过 Bancor 网络实现自主、去中心化的流动性网络。

BNT 的代币发行活动（于 2017 年 6 月 12 日举行）的捐赠用于培养一个健康的基于 Bancor 代币和应用程序的生态系统。使用 BNT 作为其连接器代币的新智能代币将有资格获得 Bprotocol 基金会的支持，以鼓励大家发行新的智能代币，同时通过上面讨论的网络效应加强现有的 BNT 社区。

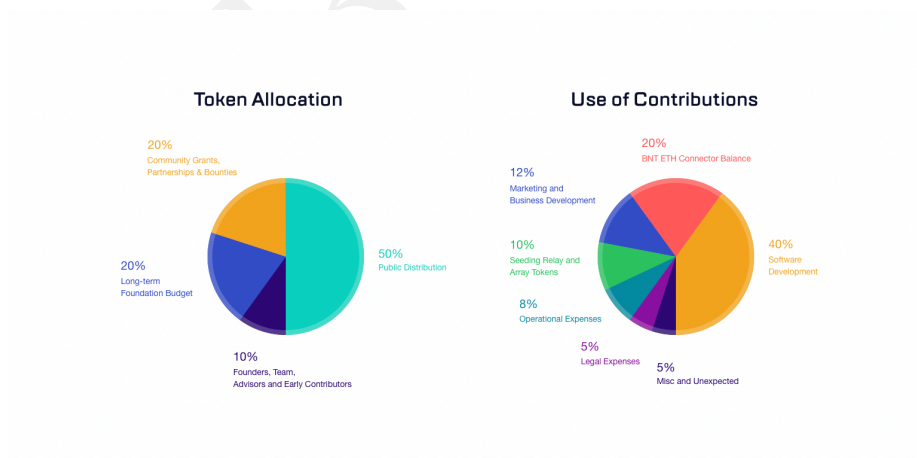
8.3 捐赠分配

为了提高透明度和充分披露各项信息，BNT 代币发行活动得到的以太币捐赠的具体分配如下图所示：

- 20% 由 BNT 智能代币的 ETH 连接器持有，建立一个强壮和充满活力的 10% CW 初始值。

- 40% 用于开发 Bancor 协议和相关技术。这包括：实现 Bancor 智能合约协议到当前以及未来的区块链；开发用户友好的应用程序以方便终端用户使用智能代币，如智能代币钱包、智能代币发行和管理的相关接口、智能代币市场、发现门户、中继代币的创建、智能代币治理以及报告等等。
- 12% 用于推广 Bancor 协议和发展 Bancor 生态系统，例如支持 Bancor 网络中的创新和战略性智能代币项目，并向全球相关受众增加对 Bancor 协议和 Bancor 网络的认识和理解。这些努力将确保围绕 Bancor 网络形成一个强大社区，同时加速用户发行代币长尾的开发。
- 10% 用于为流行的 ERC20 代币设置和推进中继代币和数组代币的示例，以及在以太坊平台上发行代理代币，用于将其他区块链的加密货币和各种真实资产整合到 Bancor 网络中。
- 18% 指定用于运营成本，包括法律支持和其他管理费用。

BNT 智能代币初始发行量的一半分发给各个捐赠者，而另一半是由 Bprotocol 基金会持有，用于它的长期预算（锁定两年）、现有的和未来的团队和顾问（既定 2 年）、伙伴关系（既定 2 年以上）以及用于帮助 Bancor 协议建立长尾的社区赠款，如下图所示：



9 总结

新的基于区块链的经济有可能创建一个价值互联网，它能吸引数以百万计的创新的、小规模、用户发行的代币。这一多样化和富有弹性的未来的关键障碍是，确保每一种商品都有一个流动性市场，而不管其数量如何。在这篇白皮书中，我们提出了去中心化流动性网络的 *Bancor* 协议，该协议基于一种称为智能代币（Smart token）的新型代币的标准。智能代币通过将自主的、低成本的市商功能直接纳入其智能合约，提供持续的流动性。智能代币利用连接器代币余额和智能的开源公式，永远可以通过计算以可预测的价格进行买卖，以换取与它们相关的其他代币。

在系统级别上，智能代币组成了一个相互连接的代币的自治全局网络。这种新颖的体系结构允许系统成员代币能够对所有其他系统成员代币进行转换，而不存在缺乏流动性的风险，并创造出让整个代币生态系统受益的网络效应。

Bancor 协议通过引入一种技术解决方案来解决双向需求巧合和小规模代币所面临的流动性问题，从而推进了资产兑换。这一解决方案成为一种可靠和全面的替代方法，可以替代目前在传统金融市场和交易所中所采用的专业做市商的手动模式。

10 致谢

我们要向许多支持我们写这篇论文的人表示感谢。特别感谢 Meni Rosenfeld, Yudi Levi, Amatzia Benartzi, Ron Gross, Assaf Bahat, Sefi Golan, Joshua Alliance, Brian Singerman, Adi Scope, Dory Asher, Tal Keinan, firmo.network, Wings.ai, TheFloor, Israel Monetary Change Movement 的 Arie Ben-David, Ithacash 的 Scott Morris, Benjamin Egelund-Müller 以及 Blockito 团队和 Blockchain Labs 以及来自 Bancor 团队的 Ilana, Asaf, Omry, Itay 和 Mati。你们的支持和反馈对我们改进本文是非常重要的。感谢你们!

参考文献

- [1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2009. URL <http://www.bitcoin.org/bitcoin.pdf>.
- [2] Wikipedia. Coincidence of Wants, . URL https://en.wikipedia.org/wiki/Coincidence_of_wants.
- [3] Wikipedia. Long Tail, . URL https://en.wikipedia.org/wiki/Long_tail.
- [4] Erik Brynjolfsson, Yu Jeffrey Hu, and Michael D. Smith. From Niches to Riches: Anatomy of the Long Tail. Sloan Management Review, 47(4):67–71, 2006. URL <http://sloanreview.mit.edu/article/from-niches-to-riches-anatomy-of-the-long-tail/>.
- [5] Fabian Vogelsteller and Vitalik Buterin. ERC-20 Token Standard, 2015. URL <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md>.
- [6] Vitalik Buterin. Ethereum White Paper, 2014. URL <https://github.com/ethereum/wiki/wiki/White-Paper>.