

Bancor 协议 研究报告

——2018 年 10 月——



TokenClub
— 研究院 —

目录

- 1. 行业综述..... 4
 - 1.1 通证经济.....4
 - 1.2 首次代币发行 ICO..... 6
- 2. Bancor 协议概述..... 10
 - 2.1 Bancor 协议的由来.....10
 - 2.1.1 布雷顿森林会议.....10
 - 2.1.2 怀念凯恩斯.....12
 - 2.2 Bancor 协议的定义.....13
 - 2.2.1 Bancor 协议.....13
 - 2.2.2 Bancor 算法.....14
 - 2.3 Bancor 协议的特点.....14
 - 2.4 Bancor 协议的产生的意义.....15
 - 2.4.1 数字货币交易存在的痛点.....15
 - 2.4.1.1 流动性.....15
 - 2.4.1.2 长尾效应.....16
 - 2.4.2 解决方案.....17
- 3. Bancor 协议原理..... 18
 - 3.1 智能代币.....19
 - 3.1.1 非盈利的自动化市商.....19
 - 3.1.2 连接器权重 (CW) 20
 - 3.1.3 代币网络.....21
 - 3.2 价格算法.....22
 - 3.2.1 价格公式.....22

- 3.2.2 不同 CW 下的供求关系..... 23
 - 3.2.3 处理价格变动..... 25
 - 3.2.4 定价的例子..... 27
 - 3.2.5 异步流动性..... 28
 - 3.2.6 套利均衡价格..... 28
- 3.3 范例..... 29
 - 3.3.1 买入代币的过程..... 30
 - 3.3.2 卖出代币的过程..... 31
- 4. Bancor 协议的应用项目..... 33**
 - 4.1 EOS 的资源体系..... 33
 - 4.2 EOS 中的 RAM 概述..... 35
 - 4.3 EOS 中 RAM 的原理..... 36
 - 4.3.1 交易机制..... 36
 - 4.3.2 EOS 与 RAM 兑换机制..... 37
 - 4.3.3 RAM 的 Bancor 算法..... 37
 - 4.3.4 EOS 与 RAM 兑换流程图..... 39
- 5. Bancor 协议的优劣..... 40**
 - 5.1 智能代币的优势..... 40
 - 5.2 Bancor 生态系统的优势..... 42
 - 5.3 Bancor 协议存在的问题..... 43
 - 5.3.1 Bancor 交易平台损失的案例..... 43
 - 5.3.2 Bancor 协议的具体问题..... 43
- 6. Bancor 协议的应用场景..... 47**
 - 6.1 促成“用户生成货币”的长尾..... 47
 - 6.2 众筹一个项目..... 47
 - 6.3 代币兑换者..... 48

6.4 去中心化的代币篮子.....48

7. 未来展望.....50

参考文献.....51

风险提示.....52



1. 行业综述

凯文·凯利在《失控》一书中提出“未来是去中心化的”，并提出了一个全新的社会形态：“一种依赖于大众智慧、云计算与物联网、虚拟现实与敏捷开发共同协作，从而共赢共生进化的社会经济形态”。大家在探讨“去中心化”问题时正是沉浸在这一思想框架之下。无论是从电话电报到互联网，再到 P2P 通信，还是从银行、信托、保险到 P2P 网络借贷或众筹金融，再到比特币，大家对于自由信息交换环境，去中心化价值传递的追求始终没有改变，也正是基于这一初衷，最终形成了如今的区块链技术。

区块链时代充分验证了“去中心化”和“机械信任”的可能性，使得它在加密数字货币、金融、医疗等领域得到一定的应用。其中，加密数字货币是最重要的应用场景。数字货币是指对流通货币进行数字化，但在加密货币市场中，数字货币指代基于区块链网络而衍生出来的一种通证/令牌（代币），并无物理资产与之相对应。

1.1 通证经济

严格来讲，“代币”只是金融科技界和 IT 专家们为了区分区块链以及为区块链支撑的技术而抽离出来的概念，并且在今天还将两个意义相差巨大的词语——Cryptocurrency 和代币混为一谈。确切地讲，前者称之为“加密数字货币”，源于比特币网络，目的是作为互联网支付的货币；后者被广泛译为“代币”，但实际上在网络通信中，代币的原意是指“令牌、信令”。在以太网成为局域网的普遍协议之前，IBM 曾经推过一个局域网协议，叫做代币 Ring Network，“令牌环网”。网络中的每一个节点轮流传递一个令牌，只有拿到令牌的节点才能通信，这个令牌，逐渐被称之为“通证”，其实就是权益证明。

通证可以代表各种权益证明，从身份证到学历文凭，从货币到票据，从钥匙、门票到积分、卡券，从股票到债券，人类社会全部权益证明，都可以用通证来代表。同时“通证”并不是区块链的专属：游戏币、用户积分、打折卡、会员卡等都是通证的原型，都是数字权益证明，但由于缺乏密码学的应用，信用建设相对比较困难，流通也受限制。因此通证并不一定要跑在区块链上，甚至可以说通证是区块链最具特色、最具魅力和威力的应用。



通证是基于固有和内在的价值（Intrinsic value），通证立足于实体经济、为实体经济服务。首先，从供给侧来看通证的供给充分市场化，高度自由，任何人、任何组织、任何机构都可以基于自己的资源和服务能力发行权益证明，而且随时可验证、可追溯、可交换，其安全性、可信性、可靠性是前所未有的。其次区块链用流转和交易变得极其可靠。再则，通证的价格将由市场确定，是完全自由的市场经济，它将把“有效市场”渗透到微观领域的每一个角落。

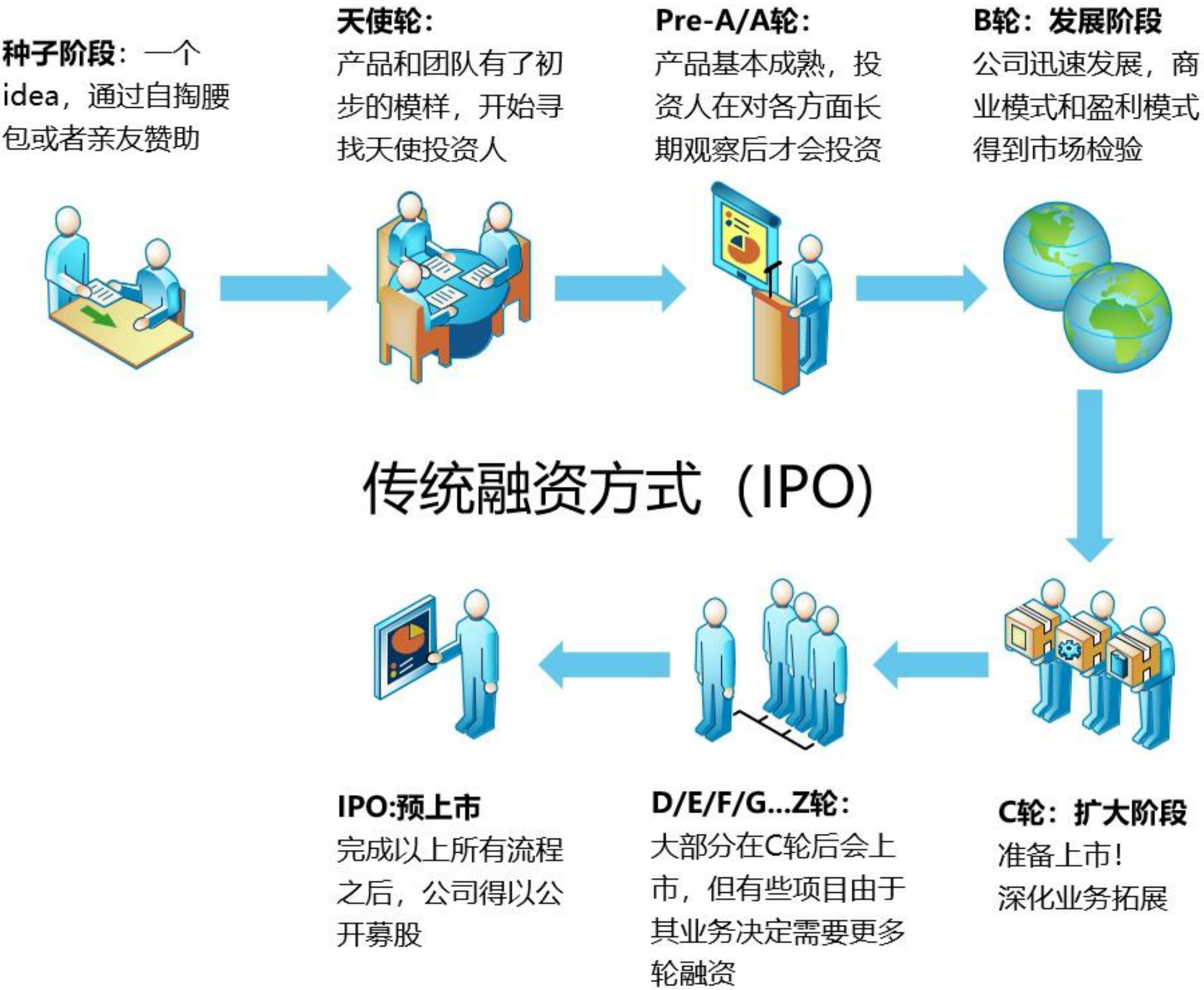
通证启发和鼓励人们把各种权益证明，比如门票、积分、合同、证书、点卡、证券、权限、资质等全部拿出来通证化，放到区块链上流转，放到市场上交易，让市场自动发现其价格，同时在现实经济生活中可以消费、可以验证，是可以用的

东西，这是紧贴实体经济的。“通证+区块链”彻底颠覆传统经济中组织、激励与分配结构，改变市场经济的生产、流通、分配与消费关系，并最终促使人类资产由资产到证券、再到数据、最终权益化。通证经济重新定义了交易和分配问题，同时通过用代币来进行 ICO（首次公开发行业代币融资）不失为一种创新的融资模式，ICO 将一级市场（发行市场）和二级市场（交易市场）混合，将股份制权益替换为“通证”。

1.2 首次代币发行 ICO

数百年来，不同类型的价值储备（以下称“货币”）一直以钞票、债券、股票、礼品卡、商家积分和社区货币 9 等形式发行和流通。接下来，出现了第一个去中心化的数字货币，比特币。各种新型数字加密货币的发行浪潮紧随其后。在通证经济的基础上，世界见证了又一新兴的、使用智能合约技术的、通过众筹 (ICO) 发行的资产类别，“代币”的崛起。

首次代币发行（英语：Initial Coin Offering，简称 ICO）也称首次代币发售、区块链众筹，是用区块链把使用权和加密货币合二为一，来为开发、维护、交换相关产品或者服务的项目进行融资的方式。从证券界的 IPO（Initial Public Offering），即首次公开募股一词演变而来。



ICO融资方式



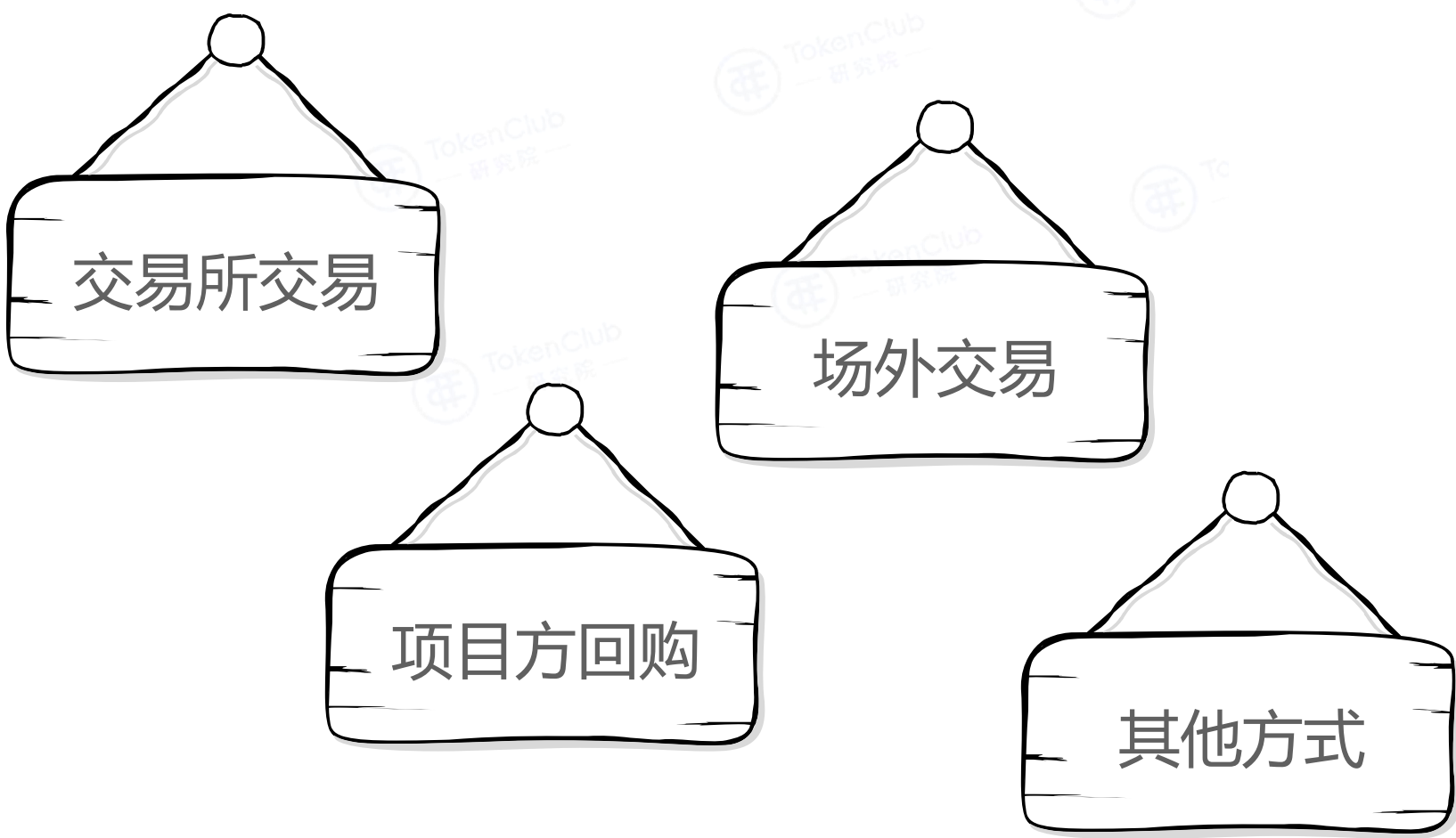
早期的 ICO 被解读为初始数字货币发行 (Initial Coin Offering)，考虑到私人发行数字货币的敏感性，“Coin” 本身是否是货币也有争议，该词一度被替换成了

“代币” (代币), 并加上了 “Crypto” (加密) 的修饰。因此, 将 ICO 解读为 Initial Crypto Offering 更为准确, 即通过发行加密代币的方式进行融资。所谓 “代币”, 在现实中通常是指在一定范围内使用的替代货币的某种凭证。这种代币同时也可视为一种在区块链上发行和流通的加密股权 (Crypto-Equity)。

通常情况下, 发起 ICO 的项目方筹集的虚拟币是比特币、以太坊。ICO 所得代币的常见用途:

- 代币可以在项目中直接使用;
- 代币相当于分红权益;
- 持有代币相当于持有项目股份;
- 项目方承诺以一定的资金 (比如一定比例的毛利润或净利润) 回购并销毁代币。

随着项目的发展, 代币价格与项目价值正相关。和所有的其他数字货币一样, ICO 所得的代币交易方式如下:



当前的代币交换模式有一个严重的障碍, 即需要一定的交易量来实现市场流动性。这使得小规模代币, 几乎不可能通过市场发现合理兑换价格并与主流数字货

币进行交换。没有足够的交易量，新加密货币不能加入多个交易所，因此它们对持有人来说是无法流通的。虽然很多加密货币可能对用户或投资者来说是有真实价值的，不过他们也不愿意支持不能最终兑换为比特币、以太坊或法币的加密货币。

Bancor 协议应运而生，旨在为区块链加密货币解决这些问题。



2. Bancor 协议概述

2.1 Bancor 协议的由来

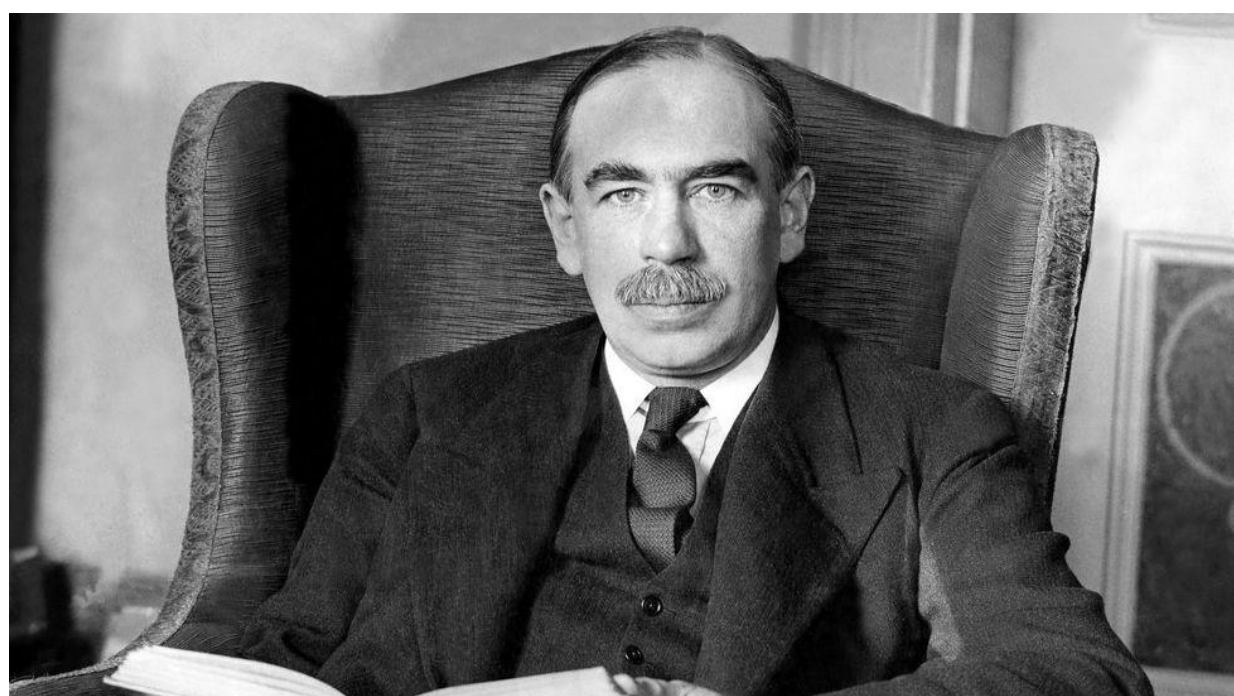
Bancor 算法之所以取名为 Bancor 是为了致敬凯恩斯计划。这个计划致力于引入一种名叫“Bancor”的超主权准备金货币，以此来推动形成二战后国际货币汇总体系。把 Bancor 算法的历史说清楚，这就不得不从一个重要的历史事件说起。

2.1.1 布雷顿森林会议

从 1944 年 7 月 1 日到 22 日，来自二战同盟国 44 个国家的代表在美国新罕布什尔州的布雷顿森林召开了“联合国货币和金融会议”，讨论战后如何对二战后世界的货币和金融秩序进行监管。

当时会议分成两派，争论的焦点放在两位经济学家的身上：英国的谈判代表凯恩斯和美国的谈判代表怀特。凯恩斯提出了非常激进的方法来管理世界各国的通货：成立世界中央银行和国际清算联盟（International Clearing Union，简称为 ICU）来平衡世界贸易盈余和赤字的建议。凯恩斯认为，如果一个国家的贸易赤字过大，会损害对一个国家和全球的长期经济增长。因为贸易赤字过大，或导致该国向债权国要支付大量利息，从而导致更大的赤字，使得债务国长久陷于不利的境地。

凯恩斯的国际清算联盟实际上是一个超越主权的国际大银行，发行自己的货币，该货币与世界各国的货币保持一个固定的汇率。他甚至给这个货币取了一个名字“班科（Bancor）”。



在凯恩斯「国际清算同盟计划」中，提出了建立全球中央银行，并发行超主权货币「Bancor」，根据二战前三年各国进出口贸易额的 75% 在各国政府间分配「Bancor」份额。

无论是凯恩斯计划，还是怀特计划，所解决的问题都是在各国主权分别发行货币与全球经济流通面临的不平衡问题。凯恩斯计划是在美国经济体占全球经济体很高程度下创建超主权「Bancor」，但是只要美国美元不参与，该计划必然无法阻挡具有强势购买力的美元经济强势入侵。后来，布雷顿森林体系锚定黄金价值，1971 年崩溃后世界完全进入美元信用时代，至此美元基本发挥了全球统一货币的作用。

可惜，英国经济和国际地位在二战末期已经大不如前，凯恩斯和他的代表团的建议，被以怀特委代表的美国代表团否决了。在部分吸收了凯恩斯的建议的基础上，怀特提出了比较温和建议：成立世界银行，国际货币基金和国际贸易组织（ITO）。这个建议被世界各国接受了。

凯恩斯在 1946 年死去。第二年，ITO 的建议很快被各国否决了，从一个多边协定变成了双边的关税贸易总协定（GATT）。

2.1.2 怀念凯恩斯

65 年过去了，作为布雷顿森林会议的成果，世界上最大的两大政府间经济组织——世界银行和国际货币基金组织（IMF），他们在成立之初，各自的角色是非常清晰的。国际货币基金主要任务是平衡各国的支付，监督成员国的经济政策；所以他的主要实施的是一些短期的融资和进行政策研究。世界银行的主要任务是对为成员国的长远发展进行融资。可是，自从 1973 年固定汇率体制崩溃之后，IMF 也开始进行长期的融资业务。世界银行在长期贷款之外，也开始提供预算支持。这样双方的业务开始不断的交叉。从 1980 年代，成员国可以同时向世界银行和 IMF 申请贷款。

世界银行和国际货币基金组织的变化，有些是好的，比如他们提供了非常齐全的世界各国经济社会发展的数据库，为世界各地的经济社会发展提供非常重要的决策依据。有些却是变坏了，比如他们变得越来越官僚和霸道。逼迫很多需要援助的国家接受一些不适合他们国家经济发展的经济政策。这已经完全违背了他们成立之初的设想，已经不能胜任稳定世界经济的任务了。正如凯恩斯当初预言：现在的这些机构的使命只停留在“口头上了”。

所以，很多国家和组织在思考着凯恩斯的 Bancor 方案，比如中国曾经提出的超主权货币的概念就是 Bancor 方案的延续。虽然不知道现实世界的 Bancor 货币能否成为现实，但是来自于硅谷和以色列的项目方，以 Bancor 方案为启发，找到了解决数字货币交易中问题的思路。该团队是凯恩斯经济学的追随者，他们通过设计一个协议，试图以代码的方式优化数字货币交易流程，该团队将这个协议命名为“Bancor 协议”也是对凯恩斯的致敬。

数字货币，本质上是货币问题解决方案的延伸，在全球金融危机后又一次引发了商品货币、商业货币等古老问题的回潮。Bancor 协议，其创立方向在于解决这种商品货币或商业货币流通长尾问题，即在不考虑商品货币或商业货币价值多少条件下，利用技术手段为其赋予一定的流通可能性。所以虽然与历史上的 Bancor 并不是一个东西，但不失致敬的意义。

2.2 Bancor 协议的定义

首选区分两个概念：Bancor 协议和 Bancor 算法。

2.2.1 Bancor 协议

Bancor 协议是一种协议而非一个公链，理论上讲，任何支持智能合约功能的公链都可以通过智能合约实现这种算法，并发行相应的代币。

在经济学中的资产交易方面有一个经典问题叫做“双重需求巧合”，Bancor 协议就是用来解决这类问题而设计的技术方案。Bancor 协议通过使用以区块链为基础的智能合约和储备货币来解决“双重需求巧合”。Bancor 协议可以让所有人创建代币，这种代币以预先设置的比率来持有一种或几种其它代币作为自己的储备金。这些储备代币可以是法币、数字化资产（如黄金）或其它加密货币（如比特币、以太币或其它）。通过使用这些储备金，新创建的代币直接获得价值，不管交易量怎样。它还直接获得了它本身和储备代币之间的汇率，因此不管什么时候它都能兑换回它的储备代币，不管有没有买家。

采用 Bancor 协议的代币可以直接获得跨币种交易的功能，是实现去中心化交易所的可行解决方案。Bancor 协议相当于加密数字资产世界的做市商，通过做市制度和储备金来维持整个市场的流动性，使普通投资者的交易需求在无需对手盘时便得到快速满足。

2.2.2 Bancor 算法

Bancor 协议中使用的算法规则称为 Bancor 算法。

Bancor 算法是一种能够根据买卖行为动态调节价格的算法。Bancor 算法通过数学公式，计算出每一次交易的实时价格。简单说来，每当有一个买单或卖单出现，算法会把买卖量拆分成很多微小的价格单，计算出整个交易量对整体动态价格的影响，得出一个有效价格。也就是说通过 Bancor 算法解决了代币交易中流动性不足问题等，提高了代币的流通性。

2.3 Bancor 协议的特点

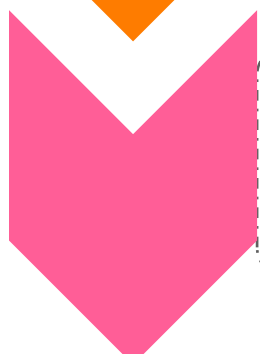
主要有三个特点：



不同于中心化交易所的撮合定价，Bancor 协议的定价是根据真实供需公式定价公开透明可预测。



没有竞价这个环节，不依赖流动性。刷单，刷交易量，刷净流入，净流出等操作都是无意义的。



没有对手风险，所有交易都是人机交易。买家不需要去找卖家，卖家不需要去找买家，交易信息公开透明。



2.4 Bancor 协议产生的意义

最近几年，全世界见证了大量新加密货币的出现和发展，不过它们大部分在获得区块链社区认可前都面临着许多的挑战。

2.4.1 数字货币交易存在的痛点

2.4.1.1 流动性

以太坊的出现，尤其是 ERC20 Token 标准的普及，让“资产通证化”变得非常容易（就是前面提到的 ICO），但是资产通证化面临着如同资产证券化一样的问题，即小股票的流动性很差，大量的交易发生在蓝筹股之间，而非全部市场。大资金由于流动性的顾虑，会更偏向流动性较好的证券或通证，而流动性较差的证券或通证，而且其价格发现机制较差。这就是流动性问题的现实反映。

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。

在区块链上，当买卖双方需求的代币价格刚好匹配时，即完成一个撮合交易。如果可以在不影响价格的前提下轻松的进行买卖，就可以说这个代币是具有一定流动性的，那么他的流动性风险较低。

现有的金融机构针对流动性低的问题的解决办法是，囤积大量资产，在交易市场中同时作为买方和卖方，他们向买方和卖方提供不同的价格，从中赚取差价。在新兴的区块链市场里，也是用交易所进行解决，但是如果仍然采用这种方案，违背了区块链去掉中间机构的理念，同时也使得代币的持有中心化。

2.4.1.2 长尾效应

长尾效应，英文名称 Long Tail Effect。“头”（head）和“尾”（tail）是两个统计学名词。正态曲线中间的突起部分叫“头”；两边相对平缓的部分叫“尾”。从人们需求的角度来看，大多数的需求会集中在头部，而这部分我们可以称之为流行，而分布在尾部的需求是个性化的，零散的小量的需求。而这部分差异化的、少量的需求会在需求曲线上面形成一条长长的“尾巴”，而所谓长尾效应就在于它的数量上，将所有非流行的市场累加起来就会形成一个比流行市场还大的市场。

如今，排名前 10% 的代币占整个代币市场市值的 95%，占有所有代币交易量的 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，这种现象就是前面提到的长尾效应。比如，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%。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。

目前这些小规模货币的痛点还包括：

- 为了保证其代币市场流通性，成本较高。
- 新代币在交易所上市是需要一笔不小的启动费用的。
- 中心化数字货币交易所权利过大，存在暗箱操作风险。

2.4.2 解决方案

举一个简单的例子：

比如以一个假想的 ABC 小众币，使用 Bancor 算法将 ABC 和 ETH 连接。买方小明购买时需要做的，不是向某个 ABC 币的持有者购买，而是向智能合约里转账。小明往智能合约转入 ETH 后，智能合约则发行新的 ABC 币并向小明转账 ABC，ABC/ETH 的兑换比例由智能合约自动计算。小明转入的 ETH 是由一个铁面无私的机器人掌控，它不会挪用任何人的押金，这也正是去中心化应用的优点。

从这个例子可以看出，Bancor 协议的功能很简单但意义深远：Bancor 协议是为了解决小众币流动性低的问题而创造的解决方案，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。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。

3. Bancor 协议原理

要理解 Bancor 协议的原理，先概略了解名词解释，而后进行详细的介绍：

连接器（connector）：可以认为连接不同代币的兑换桥梁。

连接器代币（connector token）：可以理解成抵押物，也可以理解为储备金。比如在 Bancor 网络中代币发行的最初阶段，就是通过锁定 ETH 作为抵押物来发行智能代币的。在“抵押 ETH 发行代币”这个过程中，ETH 就是连接器代币（储备金）。

智能代币（smart token）：简单理解成你想要发行的代币。还是用“抵押 ETH 发行代币”这个过程为例，智能代币就是那个想要发行的代币。

连接器权重（CW：connector weight）：理解成调节价格敏感系数的参数，也相当于恒定储备比例 CRR（Constant Reserve Ratio）。买入智能代币时价格上升，卖出智能代币时价格下降，但是涨跌幅度不是一个固定的值，都可以用 CW 进行调节。

3.1 智能代币

3.1.1 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上使用的 ERC20 代币标准，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来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。

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。

3.1.2 连接器权重 (CW)

如上所述，连接器的权重 (CW: connector weight) 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 3.2 节会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。

3.1.3 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。

拿 2.4.2 的例子来说明：假设一个智能代币 ABC 有一个连接器，该连接器持有一定数量的 XYZ 币。此外，假设另一个智能代币 NEW 币，其连接器也持有 XYZ 币。那么先将 ABC 币转换为 XYZ 币，然后将 XYZ 币转换为 NEW 币，用户就可以把 ABC 币转换为 NEW 币。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，NEW 币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。

3.2 价格算法

3.2.1 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 × 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。

3.2.2 不同 CW 下的供求关系

下面 4 张图显示了在不同的 CW 值下智能代币的价格如何对需求变化作出反应。大致讨论一下所举的例子：

图 1 的例子是 $CW=100\%$ ，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。

图 2 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。

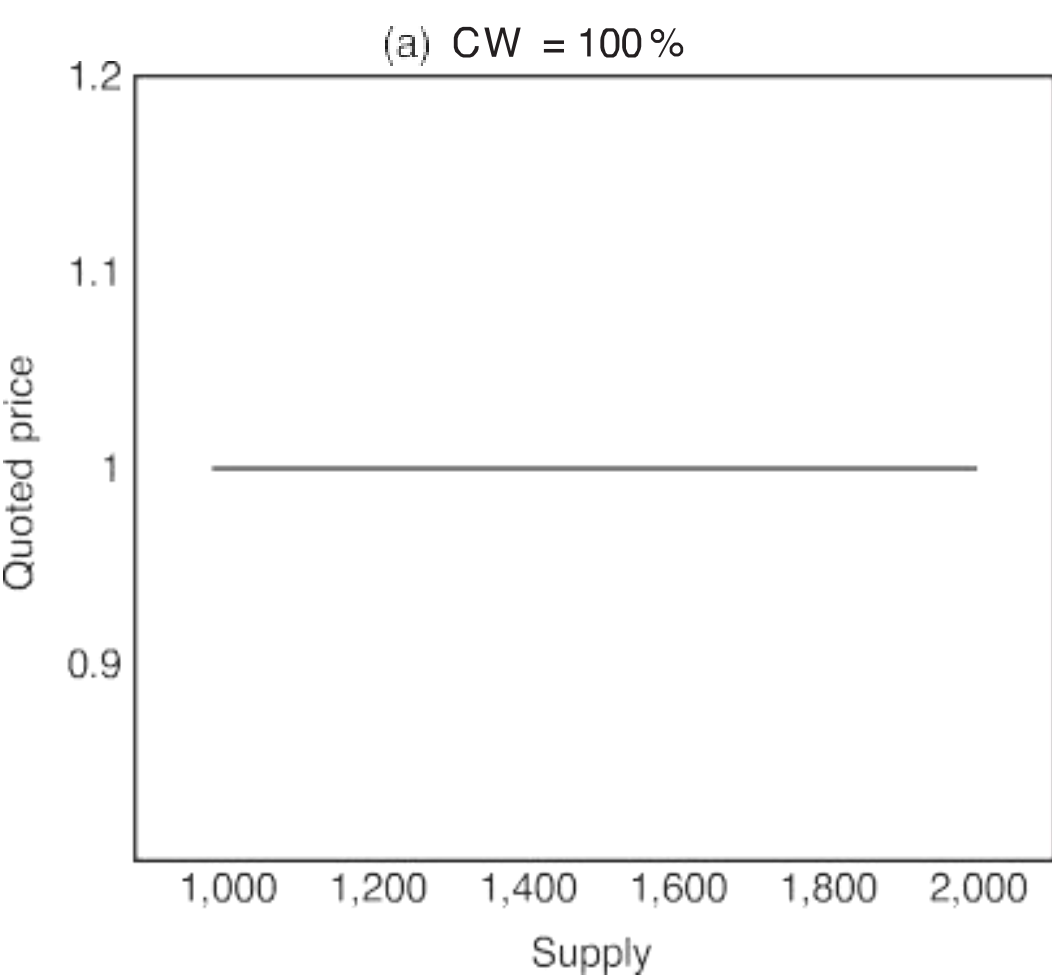


图 1

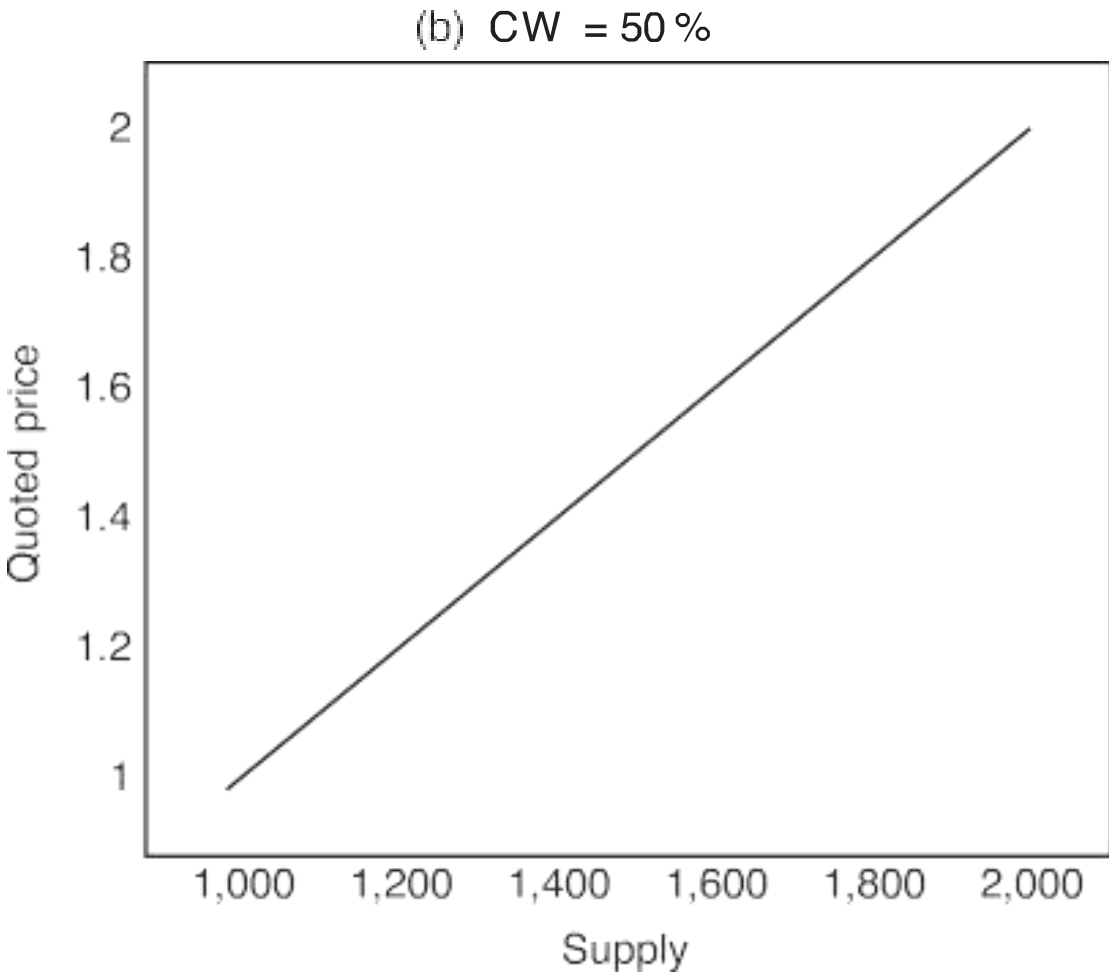


图 2

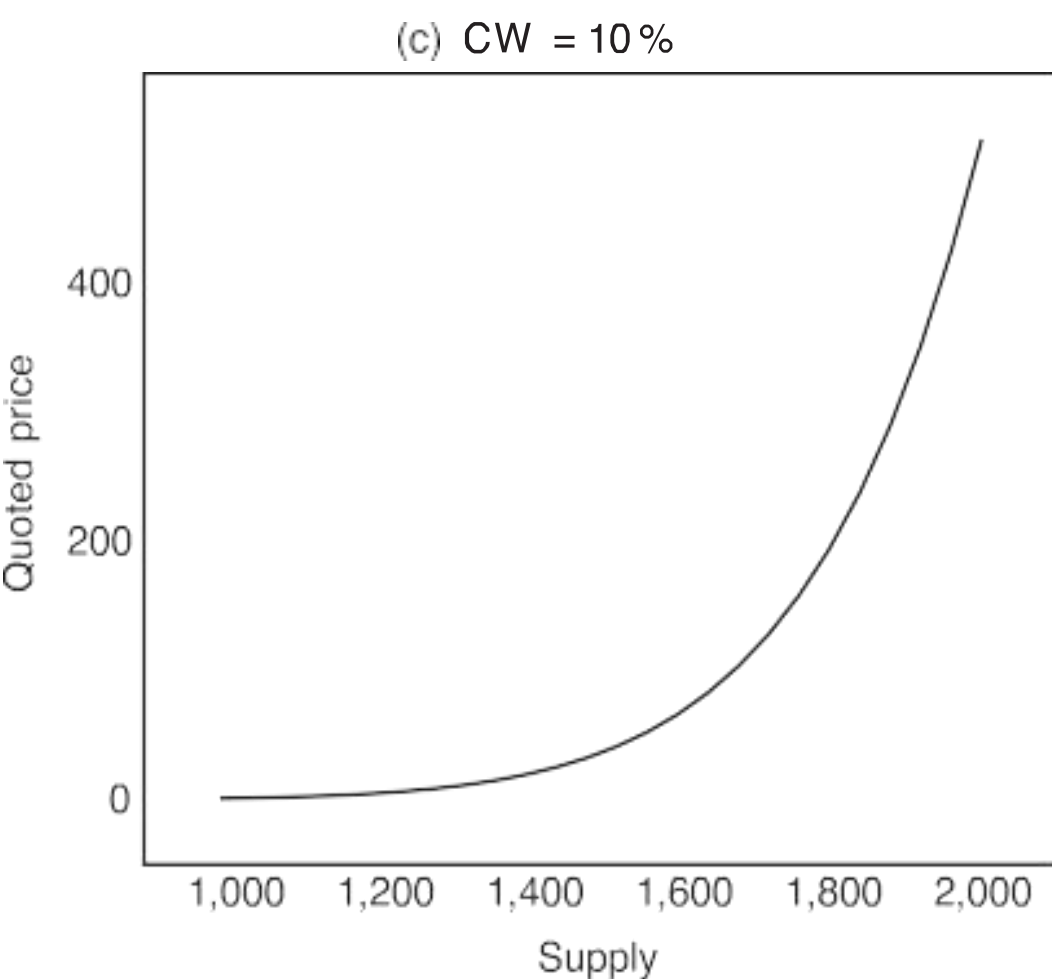


图 3

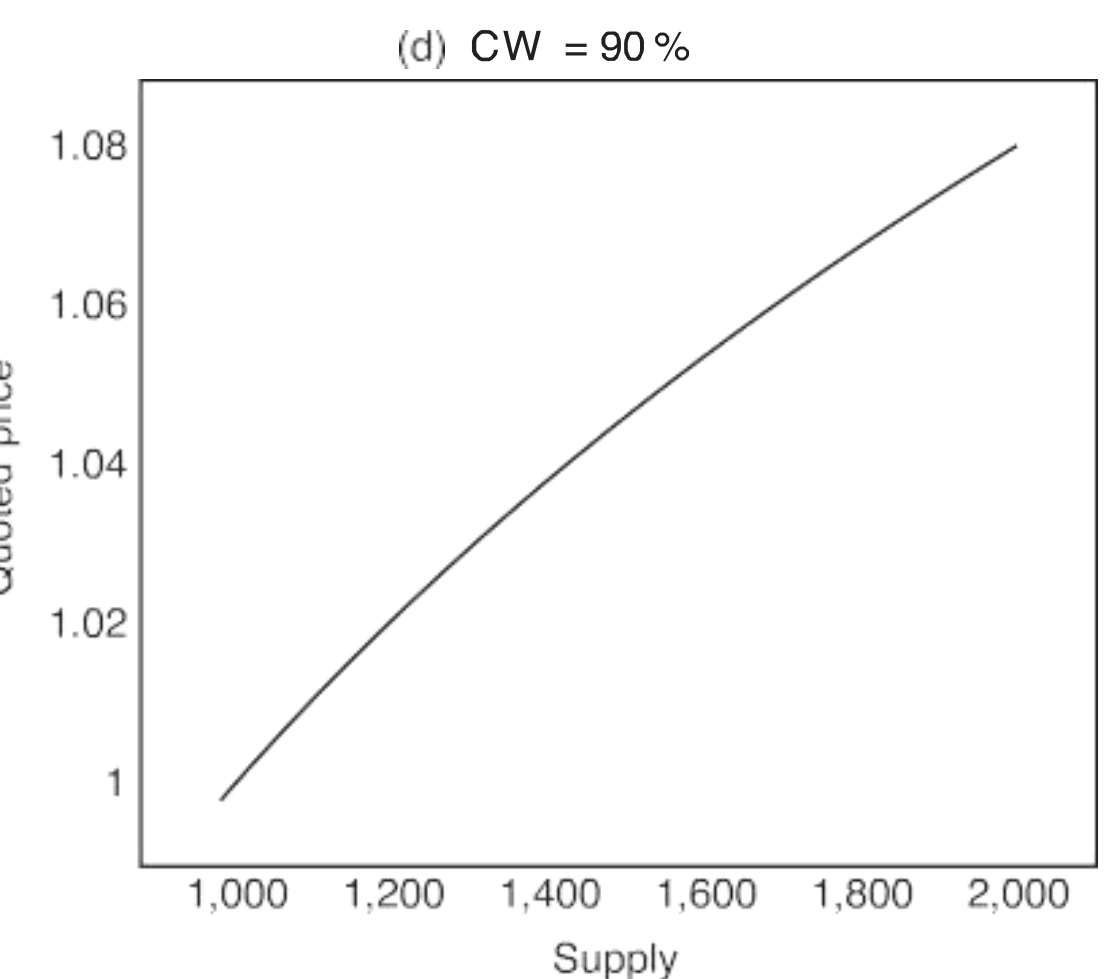


图 4

(这四张图显示了不同 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)

图 3 的非线性例子是 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 2）。

图 4 的非线性的例子是 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 2 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 1 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。

3.2.3 处理价格变动

上文中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）。

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

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。

3.2.4 定价的例子

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 个数量的连接器代币，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。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。

3.2.5 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。

3.2.6 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。

3.3 范例

为了便于理解 Bancor 协议的原理，下面举例说明。

继续使用 3.2.4 节中提到的例子：假设一个当前总供应量为 1000 的智能代币 ABC；它的连接器拥有 250 个数量的连接器代币余额（储备金），连接器代币这里定为 ETH；CW 值为 50%，此智能代币 ABC 可按以下公式进行转换：

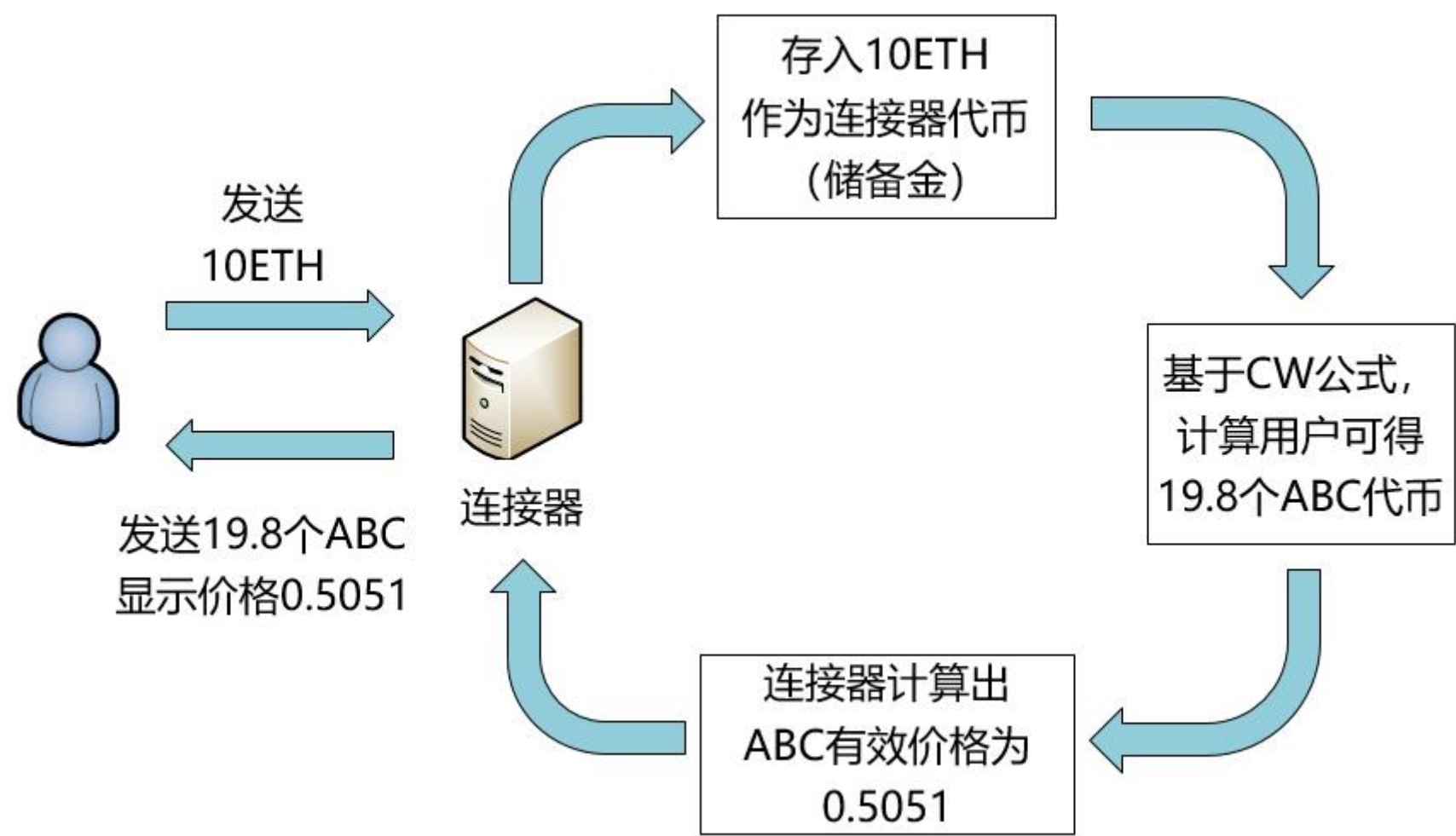
$$\text{价格} = \frac{250}{1000 \times 50\%} = 0.5$$

通过计算，智能代币 ABC 定价为 0.5。



3.3.1 买入代币的过程

当用户打算花 10 个 ETH 来兑换一定量的智能代币 ABC 时，Bancor 协议的执行步骤是：



- 1.将 10 个 ETH 发送给连接器；
- 2.连接器将 10 个 ETH 存入，作为连接器代币（储备金），连接器代币余额增加；
- 3.连接器基于 CW 公式，计算出用户可以分得 19.8 个 ABC 代币；

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

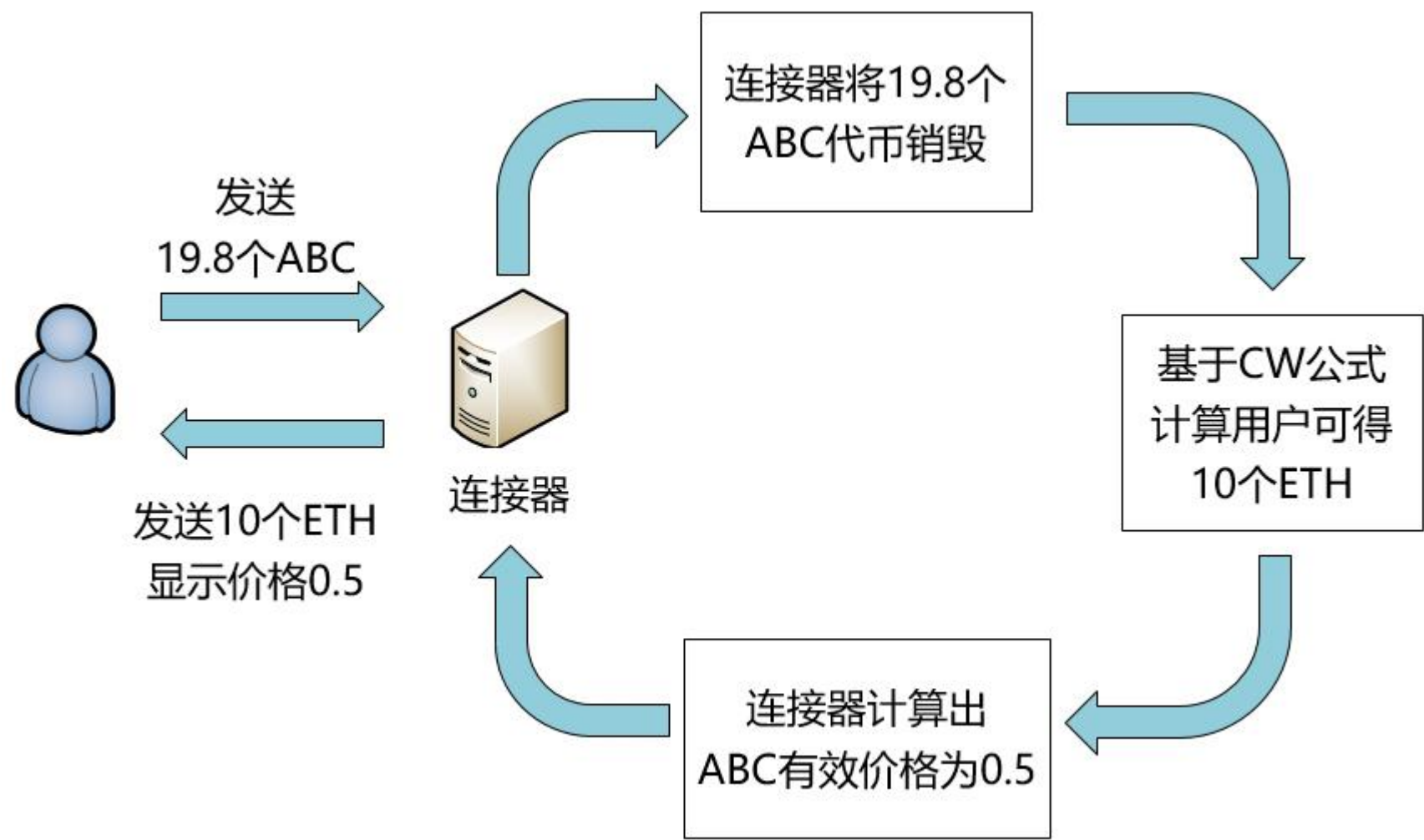
- 4.连接器计算出 ABC 代币有效价格上升为 0.5051；

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

- 5.连接器将 19.8 个 ABC 代币发送到用户地址，显示价格 0.5051。

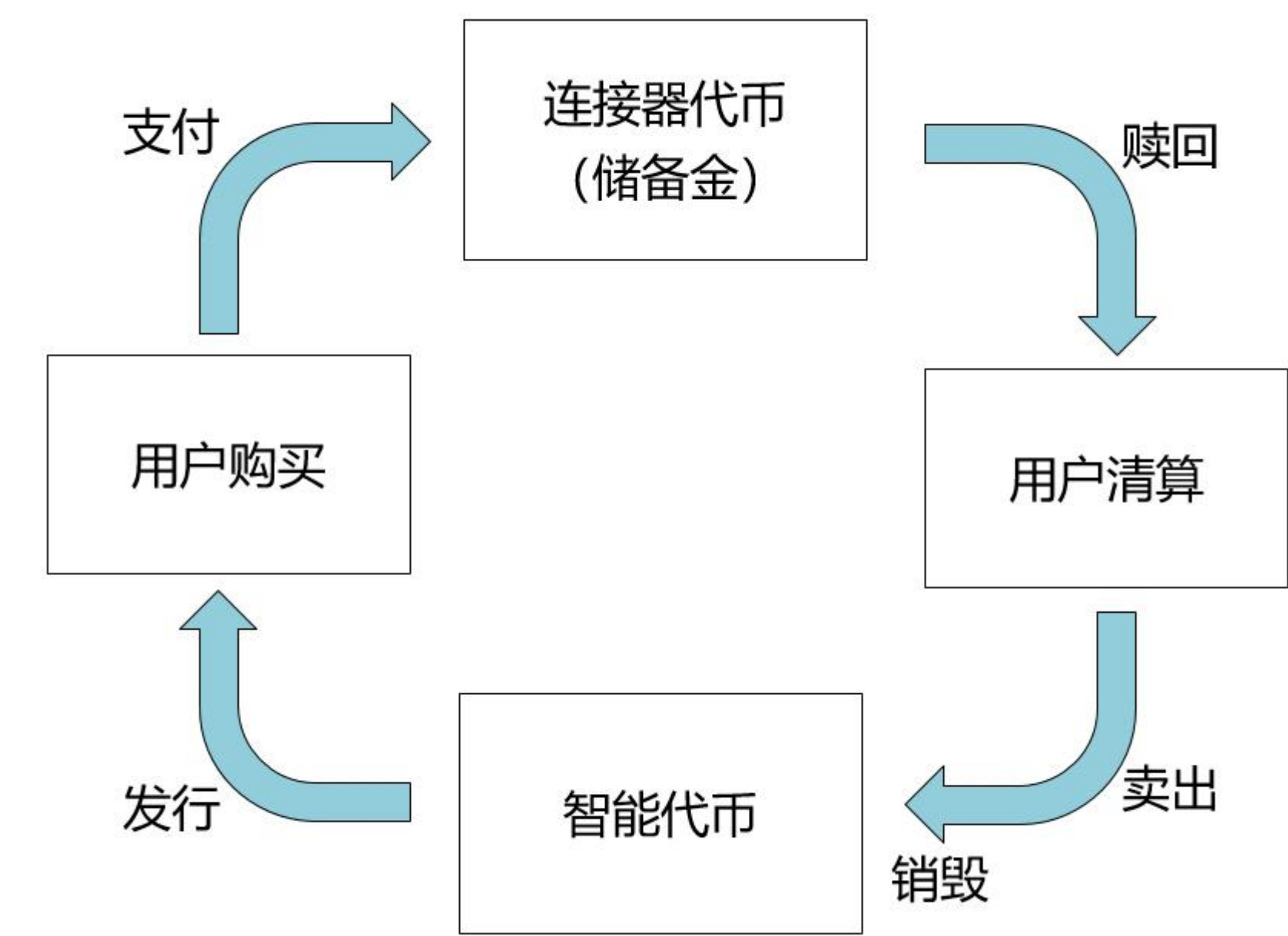
3.3.2 卖出代币的过程

当用户卖出打算卖出刚刚买入的 19.8 个 ABC 代币时，Bancor 协议的执行步骤是：



- 1.将 19.8 个 ABC 代币发送给连接器；
- 2.连接器将 19.8 个 ABC 代币进行销毁；
- 3.连接器基于 CW 公式，计算出用户可以从连接器代币（储备金）中拿回 10 个 ETH，连接器代币余额减少。
- 4.连接器计算出 ABC 代币有效价格下降为 0.5。
- 5.连接器将 10 个 ETH 发送回用户地址。

综合来看，将买入卖出步骤总结为下图



4. Bancor 协议的应用项目

2017 年有一个名为 Bancor 的区块链项目，它利用 Bancor 协议做了一个去中心化交易所，短短三个小时能通过 ICO 筹得 390000 个以太币，当时市值 1.5 亿美元，打破了当时的 ICO 世界记录。Bancor 协议已经具备了大量的拥簇者，它的落地案例将来有可能越来越多，遍地开花。这蕴含着一个巨大的商机。

本文列举 Bancor 协议现阶段落地案例中最火的项目：EOS 的 RAM。前段时间，EOS 主网中的内存资源（RAM）买卖成为了热点话题，每 kB 价格从最初的 0.017 一路飙升至最高点 0.9，最多涨了近 52 倍。

4.1 EOS 的资源体系

先介绍 EOS 的资源体系，目前网络上 EOS 的资源体系一共有两类：

第一类资源，以 CPU 为主、以周期为单位，需要锁定一定数量的 EOS。目前 CPU 是 3 天一个周期，在这个期间锁定的 EOS 不可交易或转移。而网络带宽大体和 CPU 资源的锁定机制类似，而且相对来说更廉价，需要锁定的 EOS 也更少。CPU 和网络带宽都是免费使用的，不过需要先用 EOS 抵押，可以赎回。

第二类资源，是目前的 EOS 内存，因为其 RAM 的稀缺性，RAM 的价格相比于其他资源更加抢手。目前消耗 RAM 最多的场景就是 EOS 钱包的开户，其次就是转账和一些应用内的操作，因为 EOS 账号不是免费的，需要消耗 RAM，每个账号会有 3.98K 的 RAM，抵押 0.1EOS 的 Net 和 0.1EOS 的 CPU。

含义	初始值
RAMCORE 的发行总量	100 亿 RAMCORE
EOS 池子里 EOS 的数量	100 万 EOS
RAM 池子里可用 RAM 的容量	79.07G

目前 RAM 的价格已经稳定在 0.1024 EOS/KB，因为 RAM 的价格是根据 BM 所创建的 Bancor 算法，算法会根据市场中 RAM 的占用率自行调节价格，当市场中剩余的 RAM 较少时，价格就会上升，反之亦然，RAM 较为充足的时候，价格会回调。



4.2 EOS 中的 RAM 概述

BM 对 EOS 的期望是成为区块链世界中的操作系统，因此可以把其中的一些概念对标到传统计算机来理解：EOS 中的 RAM 可以对标到计算机中的运行内存，而 EOS 区块链数据库可以对标到计算机中的硬盘。如何理解 EOS 的 RAM，这里概括为以下四个方面：

- 1. 由于 EOS 高吞吐量（TPS）的设计，链上数据膨胀速度会很快，所以 EOS 设计者采用账户模型而非 UTXO 模型。RAM 就是 EOS 主网中的内存，用于存储用户在 EOS 中的高调用频率的决策类数据量（账户余额、合约状态等）。
- 2. RAM 交易采用 Bancor 协议模式，不采用撮合式交易模式：即以系统账户（eosio.ram）作为 Bancor 协议的连接器，所有交易都发生在用户与指定系统账户（eosio.ram）之间，用户之间不能进行交易。
- 3. RAM 每 kB 平均价格由系统合约（eosio.system）控制并动态调整，影响因子为当前 eosio.ram 账户中的 EOS 余量以及系统 RAM 余量。除了在你决定出售 RAM 时社区愿意通过 eosio 系统合约向你购买之外，合约不设定 RAM 市场价格，市场价格由通过系统合约交互以进行买卖的人设定。定价算法简而言之：一句话：买入越多，价格越高！卖出越多，价格越低！
- 4. Bancor 算法是一种保证数字货币流通性、推动价格发现进程的手段。BM 在 EOS 中对 Bancor 进行了不小的改造，EOS 到 RAM 的兑换过程就涉及了两个公式，简单公式复杂化。

4.3 EOS 中 RAM 的原理

4.3.1 交易机制

EOS 系统合约 (eosio.system) 规定, RAM 交易不采用撮合式交易模式, 所有交易都发生在用户与指定系统账户 (eosio.ram) 之间, 用户之间不能进行交易, 且这个过程是需要手续费的。

- 1.EOS 系统合约 (eosio.system) 规定了每次交易的手续费为用于购买 RAM 的 EOS 数量的 0.5% 加上 199, 再除以 200。
- 2.EOS 系统合约 (eosio.system) 规定了所有交易都是与 eosio.ram 这个系统账户进行交易的, 交易的手续费会转移到 eosio.ramfee 账户中。
- 3.用户在进行 RAM 买卖时, 需要将 RAMCORE 作为中间兑换物, 具体原因在下文解释。
- 4.EOS 系统合约 (eosio.system) 表示, 每 kB 的 RAM 价格是由 exchange_state 文件中规定 covert 函数的 Bancor 算法确定的。

4.3.2 EOS 与 RAM 兑换机制

EOS 与 RAM 正是通过创建中继代币（relay token）的方式实现 EOS 和 RAM 币币兑换的。这里面有 3 个角色：

储备金 1（连接器代币）——EOS

EOS 的内存账户以 100 万个 EOS 作为初始储备金 1，占 50% 市值

储备金 2（连接器代币）——RAM

EOS 的内存账户以 64G 的初始空余内存作为初始储备金 2，占 50% 市值

中继代币——RAMCORE

RAMCORE 总量 100 万亿，以 EOS 和 RAM 作为准备金，为 EOS 和 RAM 提供兑换媒介。

4.3.3 RAM 的 Bancor 算法

RAM 的 Bancor 算法并不复杂，它仅仅是在本文第 3 章讲到的 Bancor 协议原理的基础上，进行了变化。其中，增加设置了 RAMCORE 这一中间环节，经过推导，RAM 每 KB 的价格公式如下图，即买入单价等于 eosio.ram 账户下交易结算后的 EOS 余额除去 RAM 余额，卖出单价等于 eosio.ram 账户下 EOS 余额除以交易结算后 RAM 余额，也就是单价等于总价值除以数量。

$$\text{Price} = \frac{\text{Balance}}{\text{Supply}}$$

可简写为

$$P = \frac{B}{S}$$

P 为购买 RAM 的平均单价（积分结果除以总花费）、在买入过程中，Balance 为 eosio.ram 账户对该笔交易结算后的 EOS 余量，等于 B（EOS 原余量）+B（EOS 买入量）、Supply 为系统的 RAM 原余量；在卖出过程中，Balance 为 eosio.ram 账户的 EOS 原余量，Supply 为对该笔交易结算后的系统 RAM 余量，等于 S（RAM 原余量）+S（RAM 卖出量）。公式如下图所示：

买入 RAM：

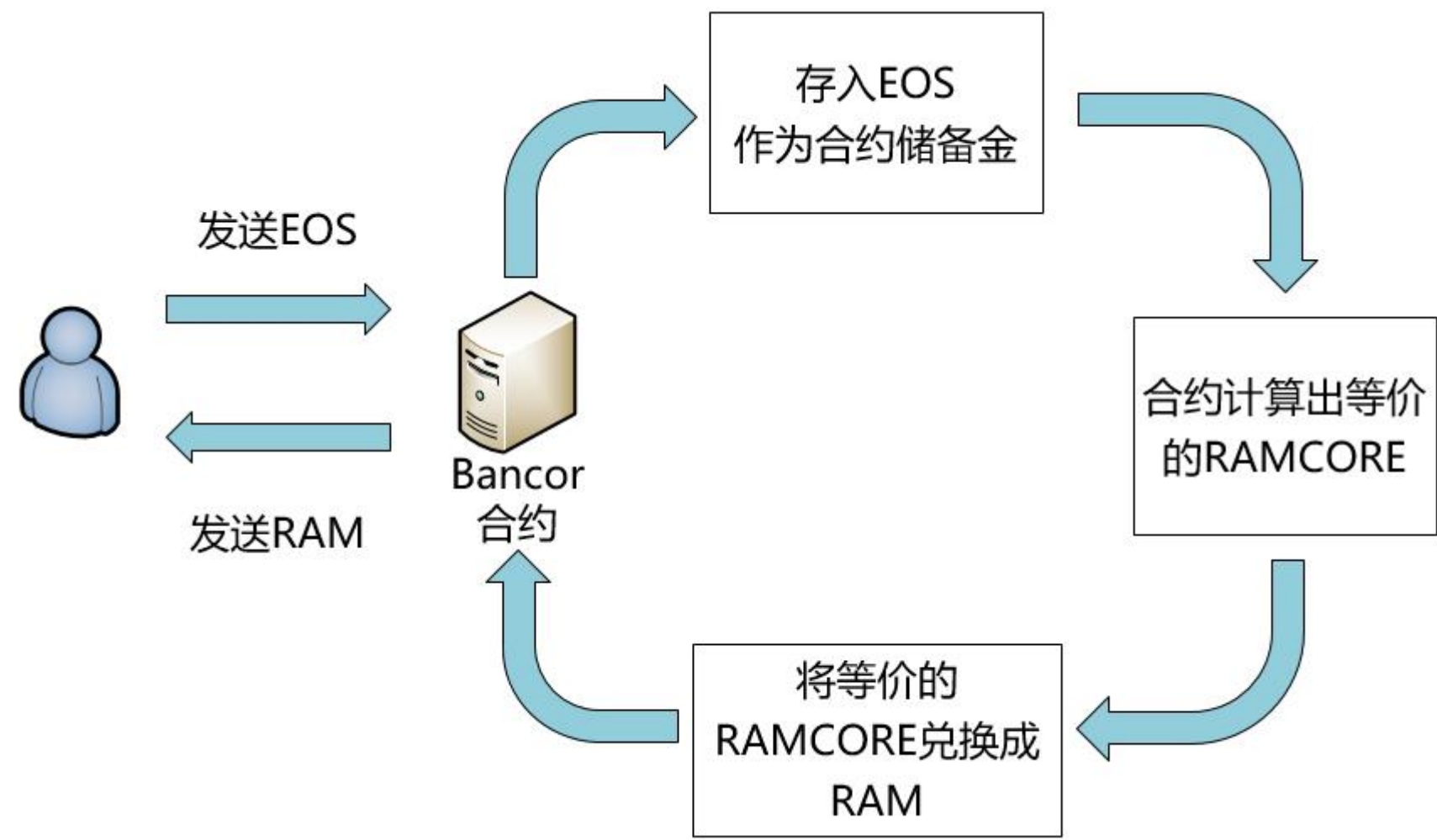
$$P = \frac{B_{\text{EOS原余量}} + B_{\text{EOS买入量}}}{S_{\text{RAM原余量}}}$$

卖出 RAM：

$$P = \frac{B_{\text{EOS原余量}}}{S_{\text{RAM原余量}} + S_{\text{RAM卖出量}}}$$



4.3.4 EOS 与 RAM 兑换流程图



上图为用户用 EOS 购买 RAM 的流程图，而用 RAM 兑换回 EOS 的流程与上图的方向相反。

5. Bancor 协议的优劣

5.1 智能代币的优势

Bancor 协议提出了智能代币这个概念，这是代币市场上的一种新模式，因为它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：

5.1.1 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。

5.1.2 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。

5.1.3 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。

5.1.4 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。

5.1.5 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。

5.1.6 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。

5.2 Bancor 生态系统的优势

5.2.1 轻松创建 Token

Bancor 使创建数字资产变得更容易，解放用户生成 Token 的巨大潜力。这些 token 还提供便宜的访问服务，这些服务之前都是很昂贵的，或者其他方式无法访问的。

5.2.2 模块化工具包

Bancor 协议建立了唯一的标准从而使多种应用场景变得可能。由于智能代币能够将其他智能代币作为储备，它们可以被用来作为新的金融，银行或其他货币解决方案的模块，这些模块能够向它们自己乃至整个生态系统传递价值。

5.2.3 嵌套估值

通过在储备中持有一个预先存在的代币，智能代币与相关资产有一个预先的估值。因此，由于与这些预先储备的代币的联系，智能代币的建立，或直接或间接的与更大的价值相连接（这些预先存在的代币所代表的价值）。生态系统的长期演变是开放的，对于 Bancor 协议来说，网络可能会设定它们对投机或波动性的偏好。

5.2.4 互联的框架

通过帮助一些非常小的实体和网络在无须牺牲个体独特性的前提下共享和交换资源，智能代币使它们连接成一个更大的网络。

5.3 Bancor 协议存在的问题

5.3.1 Bancor 交易平台损失的案例

加密货币交易平台 Bancor 于 7 月 10 日称遭到攻击, 丢失 24,984 个 ETH, 3,236,967 个 BNT, 229,356,645 个 NPXS, 折算法币金额为 1250 万美金的以太坊, 1000 万美金的 Bancor 代币和 100 万美金的 Pundix 代币。

初期不少媒体报道称 Bancor 智能合约存在安全漏洞。但实际上, Bancor 平台被盗事件与 BancorConverter 合约有关, 攻击者 (黑客/内鬼) 极有可能获取了账户的私钥。

5.3.2 Bancor 协议的具体问题

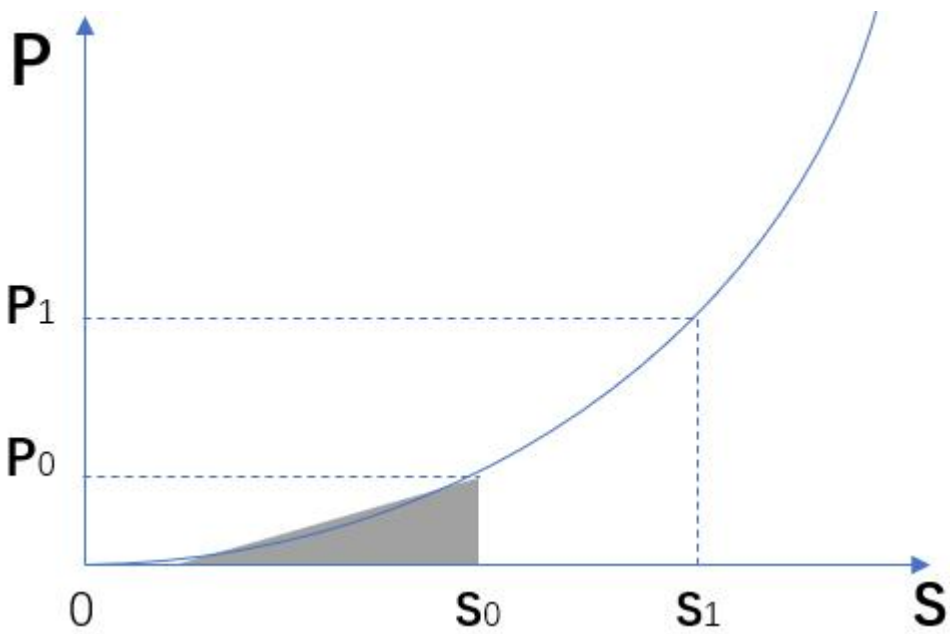
5.3.2.1 单点失效

对于 Bancor 协议建立的去中心化交易所, 都是用代币合约来处理交易。虽然说明面上是去中心化交易所, 但是需要在合约中设立超级管理员权限。当有账户存在超级管理员权限时, 整个代币生态极容易发生单点失效。超级管理员权限是把双刃剑。在 Bancor 事件中, 黑客利用了管理员权限盗取代币, 而项目方也正利用了管理员权限来降低损失。不过我们认为, 开发者依然可以通过良好的代码设计来降低代币和协议合约对管理员的依赖。

5.3.2.2 牺牲交易深度

Bancor 协议的问题是价格曲线调节参数完全受项目方控制, 参与而且鼓励价格投机, 越早买入的人越容易获利。买盘能够推高价格, 同时买盘也会降低价格, 一旦曲线上升停滞容易发生「踩踏」造成较大的波动。所谓牺牲深度带来流动性。

5.3.2.3 估值失效问题



第一种估值失效是指项目的估值容易存在不合理性。结合上图，比如某个项目推出之始给自身估值 500 万 ABC 代币，那么这个估值是市场给的，还是投资机构给的？其实都不是，是项目方自身给的。而当该项目启动后只要有购买者推动 S_0 向右移动，在市场炒作并存在外部市场条件下，项目的估值容易存在不合理性。

第二种估值失效是指流动性特别差的代币估值是失效的。虽然通过 Bancor 协议，流动性差的代币始终存在对手盘，即在 Bancor 协议下 P_0 可以无限接近于 0；然而，这种情况特指某种代币流动性特别差，差到虽然存在市场有很大存量，但是价格低到无法弥补人们去兑换或交易的成本，这种流动性极差情况已经脱离市场。即类似于 Bancor 协议中，流通性差的代币虽然存在流通通道，但是并不存在流动性，从估值上来讲，就是虽然存在市值，但是这种市值其实是失效的。

5.3.2.4 价格承载力问题

价格承载力的问题，是指在 Bancor 协议模式下，每一个价格滑点对应的代币发行量是等密度的，通过曲线积分便是买方的付出或卖方的获得。在正常的交易市场下，虽然价格点可能不如 Bancor 模式连续，但是在每个价格点下代币发行的量却不是等密度的。在存在交易深度的前提下，交易方一定会优先选择外部交易市场。然而当外部市场不满足深度条件时，即外部市场买卖盘深度不足或价格不

连续过于严重，Bancor 模式下的内部市场是可能优于外部市场的。所以，「价」和「量」之间存在互相牺牲的关系。

在长期均衡条件下，内部市场和外部市场价格会因为「套利」机制保持相等，这里说的价格是成交均价，不是中间价。随着时间推移，外部市场的「量」逐渐加深，吸引投资者进行外部交易，这时 Bancor 系统的市场作为套利市场存在。当项目方发生巨大变化时，外部市场无法及时反应，比如项目方跑路，内部市场发挥主要作用；另一种情况是项目出现重大利好，外部市场惜售严重，内部市场发挥供给作用。

5.3.2.5 参数被操控问题

Bancor 算法根据参数 CW 的不同，以及构造关系不同，会产生不同的数学图形，或杠杆效果。比如常见的四类图形，如 3.2.2 节 4 张图所示。市场对价格变化的预期几乎完全基于 CW，因为它决定了价格曲线。那么如果项目中途改变 CW 参数呢？RAM 和 FIBOS 项目都发生过这一的情况，只不过一个是简单粗暴，一个是有其他参数配合的「合理解释」的。这类风险也是目前 Bancor 协议投资者面临的最大风险。

首先，为什么一个项目方有动力去中途改变 CW？以 RAM 举例，对于一个可以被炒作的稀缺资源，如果项目方在发行初期把 CW 定的非常小，比如 0.5%，那么一定会出现价格的指数型疯狂上涨，和韭菜的不断追高。但是到了某一个临界点，没有人接盘的时候，市场怎么涨上来的，就会怎么跌回去，按照指数曲线再往左移动。如果这时候，项目方突然把 CW 变为一个很大的数，比如 50%，则下跌的恐慌大大降低了，因为下跌是沿着线性平缓曲线，而不是倒着的指数。

此外，曲线改变了，曲线的积分就会改变。甚至有可能有极端情况，项目方通过中途改变 CW，将一个空气币从 0 炒到某点，再归零，但项目方反而赚了，因为积分面积的改变。

最后，调整 CW 是一个更复杂的动态问题。因为在项目获得融资后，Bancor 系统更多发挥交易流通功能，在估值规律条件下，人工调整其实不能改变市场规律。所以要么会存在没有意义的情况，要么会存在财富挤压的情况，要么会存在财富蒸发情况等等。



6. Bancor 协议的应用场景

6.1 促成“用户生成货币”的长尾

智能代币是非常独特的，它们可以单方面按照“计算出来的价格”自由购买或清算。这种模式不再必要双方的需求同时匹配。这意味着，通过使用 Bancor 协议，预期交易量较低的小规模货币将拥有提供持续的流动性的能力，从而消除与全球经济挂钩的屏障，形成小规模货币长尾。

6.2 众筹一个项目

众筹行业正在繁荣发展。智能代币能用于加密货币众筹项目。参与众筹者获得代币，这些代币具备流动性的而且有市场定价。

例如，音乐家可以筹集资金来录制一张专辑，音乐家获得资金，出资者获得代币。专辑完成后以代币定价销售。喜欢音乐的人购买专辑需要使用代币。他们可以从代币持有者手中获取代币用于支付专辑。一张成功的专辑将带来市场对该种代币的强烈需求，拉升该种代币的价格，由此奖励那些持有它们的人。这种小规模代币因为预期缺乏流动性而发行困难，有了 Bancor 协议的支持，问题就解决了。这种运用 Bancor 协议众筹的方式又被称为 IBO（Initial Bancor Offering）。

这里就众筹这方面的应用举了一个简单的例子，实际上，还有更多的可能性案例，比如众筹一个风险投资基金或为某社区货币筹集初始资金等。

6.3 代币兑换者

当用户将“恒定储备率”设定为 100% (意味着“储备金余额”等于“代币流通量”), 并在储备金中放入两种不同数字货币 X 和 Y 时, 该用户就具备了将这两个货币进行兑换的能力, 被称为“货币互换者”。例如, 该用户想把货币 X 兑换成货币 Y, 他只需要将货币 X 存入储备金中, 然后再销毁“智能代币”, 从储备金中提出货币 Y。值得一提的是, 改变 X 和 Y 的“储备金余额”和“代币流通量”将影响其价格, 而当 X 和 Y 在 Bancor 网络中的价格和其在外交易所市场的价格出现差价时就产生了无风险套利 (Arbitrage) 机会。货币互换者通过不断地发现套利机会, 在经济激励下有效地使得 Bancor 网络中各个货币价格和市场价格保持一致。

MtGox 和 Bitfinex 等主流中心化交易所曾遭入侵, 数百万美元的资产被盗走。而用“代币兑换者”将一个代币转换为另一个代币不需要在中心化交易所中存入资金, 从而消除了过程中的交易对手风险。

另一个重要的好处是, 由于“代币兑换者”天然的去中心化属性, 和其他即时交易解决方案(场外交易)的一样, 这种模式不需要应用任何交易限额。虽然其他“去中心化交易所”也提供这种好处, 但智能代币可以不依赖交易量来提供流动性。

6.4 去中心化的代币篮子

智能代币可以作为去中心化的代币篮子使用, 其功能类似于 ETF 或指数基金。实现这个功能只需持有总计 CW (CRR) 为 100% 的准备金代币组合即可。在这个模型里, 智能代币的价格随着准备金代币的价格涨跌而涨跌。

与“代币兑换者”类似, 这里也有套利者。他们被激励着反复比照“市场价格”去调整兑换率, 依据这些准备金在外部市场的价格来保证这些准备金代币之间的

配额比例恰当。通过这种模式，这些“智能代币”使用户能够越过金融服务提供商等中介，直接持有资产篮子。



7. 未来展望

Bancor 协议所建立的不仅仅是一类新的数字资产，它也在货币，银行，金融，交易领域为那些前所未有的创造和创新力开辟了无限的可能性。

虽然不可避免的会在市场和经济学中存在很多问题，但有了 Bancor 协议，世界就有了一个可以创造新的金融系统的工具箱，用于设计新的金融系统，这些新的金融系统也许能够对现有的系统所不重视的部分进行价值运作。可以说，这就像是大家回到了布雷顿森林会议，现在可以自由的选择想要执行的提议。

Bancor 协议未来的用途还有很多可能，比如外汇或通证兑换、构建一个智能代币包含一揽子通证（类似通证 ETF），都是非常有趣的构思和尝试。也就是各种代币的发行和流通，将会激活之前无法纳入经济系统的生产要素，进一步促进数字经济发展。

Bancor 协议甚至可以脱离区块链而存在，比如将这个协议稍加改善，结合 STO 的概念，甚至可以将 H 股和新三板的流动性问题大大缓解。

总的来说，Bancor 协议是一个很棒的去中心化货币解决方案，虽然在几十年前就被凯恩斯提出，但是因为中心化（政治）的原因被废弃。像 Bancor 这样曾经因为技术水平或者中心化组织出于自身利益被废弃却很棒的提议，是否都可以随着区块链的普及而复活，从而为整个世界带来更有效率地运行方式？所以要感谢区块链的兴起，又把 Bancor 带回了大众的视野，并在区块链的技术支持下，得到了完全实现。Bancor 协议无疑是在去中心化交易方面迈出了独特的一步，创造了一个自动化的做市商，无流动性风险的分层货币体系正在长尾数字货币交易市场蓬勃发展，有理由相信，Bancor 协议会有很好的发展。

参考文献

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2009. URL:<http://www.bitcoin.org/bitcoin.pdf>.

[2] Bancor Protocol Whitepaper, 2018.

URL :https://storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor_protocol_whitepaper_en.pdf.

[3] EOSIO RAM Market & Bancor Algorithm,2018.

URL:<https://medium.com/@bytemaster/eosio-ram-market-bancor-algorithm-b8e8d4e20c73>

[4] 超主权货币与 Bancor 算法,2018.

URL:<https://www.jianshu.com/p/9fa8299b5666>

[5] Bancor 算法及 IBO 的未来,2018.

URL:<https://wallstreetcn.com/articles/3412586>



风险提示

本报告所采用的数据均来自合规渠道，分析逻辑基于作者的职业理解，本报告清晰准确地反映了作者的研究观点，力求独立、客观和公正，结论不受任何第三方的授意或影响，特此声明。

本报告的信息来源于已公开的资料，代币 Club 研究院对该等信息的准确性、完整性或可靠性不作任何保证。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议。

本报告版权仅为代币 Club 研究院所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制、发表或引用。如征得代币 Club 研究院同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“代币 Club 研究院”，且不得对本报告进行任何有悖原意的引用、删节和修改。



TokenClub 是国内领先的数字货币投资社区，致力于构建一个自治、信任、高效的数字资产投资服务生态。

“TokenClub 研究院”是 TokenClub 旗下研究区块链的专业机构，专注于区块链行业研究、项目评级。



扫码关注
TokenClub 研究院



扫码下载
TokenClub APP