BAND PROTOCOL

Band Protocol - 去中心化数据治理协议

May 1, 2019 Public Draft Version 3.0.1

原作者：

Soravis Srinawakoon(soravis@bandprotocol.com)

Sorawit Suriyakarn(swit@bandprotocol.com)

2019-9-8, Band Protocol 中文社区翻译版 v0.3

译者：Chen Hao, Ivy

摘要

去中心化应用程式具有巨大潜力是因为其自动化执行、无须信任的智能合约取代中心化的中间人将会对传统商业产生颠覆性的创新。在Web 2.0的时代，中心化的企业是数据储存及散布中获利最多的角色。而在Web 3.0中，去中心化网路可造成一个典范转移，可让使用者恢复自身数据所有权，并把互联网归还给使用者的手中。

然而，去中心化应用程式在一个无须信任的方式运行下仍然需要依靠数据，且智能合约目前没有一个简单的方法来访问可靠的现实世界数据之手段，这使其应用场景相当有限。当前去中心化应用程式仍然依赖于中心化数据中心，这代表单点故障的可能且在一开始就丧失了去中心化的意义。

Band是一种开源协议，有助于管理去中心化区块链系统中使用的数据，且作为数据处理和管理的开源标准。本白皮书概述了Band Protocol如何以完全去中化的方式解决数据可访问性和可靠性问题。这包括Band如何提供数据端点，以便任何智能合约都可以轻松访问现实世界数据与数据治理机制来确保数据完整性。

虽然Band最初是建立在以太坊之上，但协议本身是跨区块链平台的，最终将能够支援所有主要的智能合约平台，包括Cosmos Network和EOS。Band的愿景是成为去中心化的世界数据库，任何去中心化应用都可以依赖这些数据库来获取可信数据。

目录

1 介绍

在所有区块链平台操作和执行无须信任的智能合约代码时，都遇到需要使用外部中心化数据终端的问题。许多去中心化系统执行基本任务和计算时依赖于外部数据回传的，如资产价格、链间通信、现实事件和外部 Web API交互。

1.1 数据可用性问题

智能合约无法自行存取数据 - 对于去中心化的应用程式，没有简单且内建的查询介面来接收现实世界数据。在去中心化应用程式可以将实际外部数据输入连接到简单的函式呼叫之前，在采用该技术和实现开发人员想要开发的应用之间将会有很大的阻碍。

目前区块链智能合约的数据可用性解决方案要不高度依赖于中心数据库而可能导致单点故障或受限于非同步交互，从而导致延迟并使智能合约逻辑复杂化。

1.2 对可信和可靠数据的需求

在无需许可的去中心化系统环境中，维持避免他人破坏和攻击关键数据来源的经济激机和诱因是非常重要的。在通过建立强且有力的激励机制以确保高品质、可靠的数据提供之前，去中心化应用将有很大的风险并持续遭受这些安全性的问题。

例如，如果预言机提供的外部数据源控制了智能合约的数据输入，那么它就有能力决定该智能合约的反馈和行为。如果预言机受到损害，那么智能合约和所有依赖于智能合约的系统都一样发生了危害，从而区块链中的安全性和抗审查等特征中产生了明显的弱点。

为了使去中心化应用变得日益茁壮且更有效用，去中心化的对应设备中必须能够同样使用与中心化设置中相等的工具。最终，这将使得开发人员能够构建未来的去中心化应用程式，从而改善人们的生活。

1.3 智能合约元件层解决方案

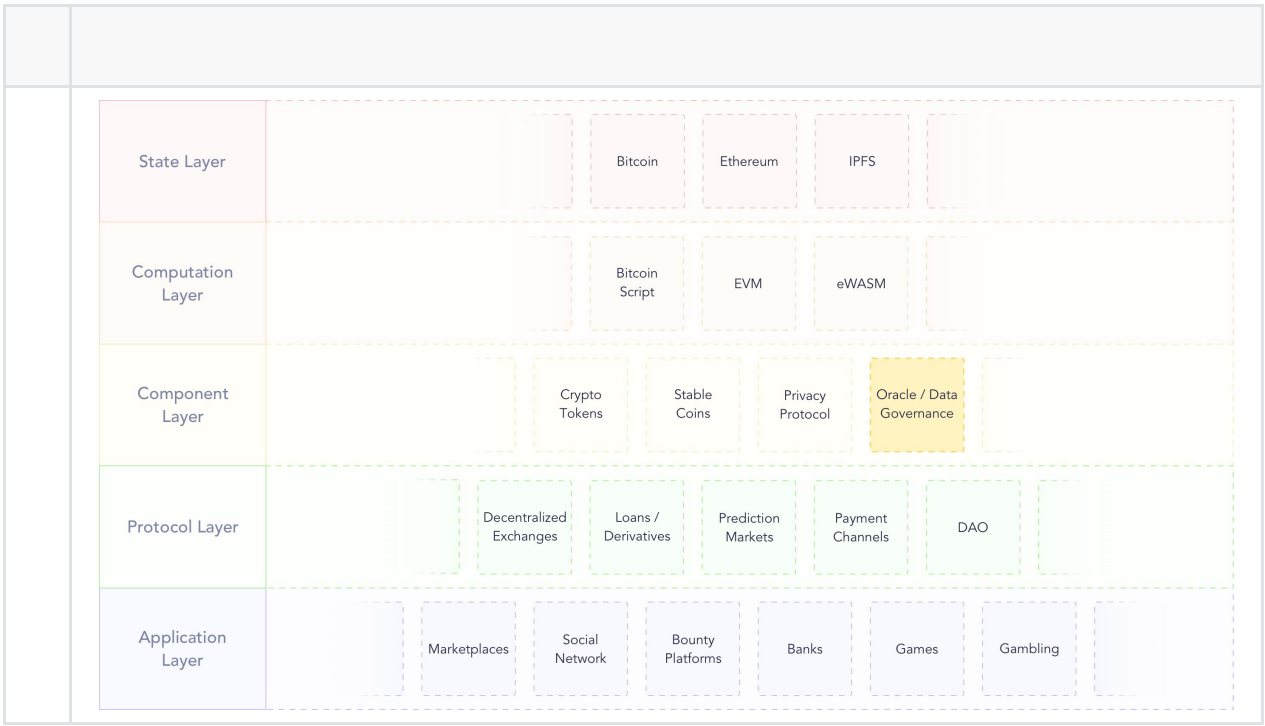

图1：Web 3.0技术栈概述。Band Protocol适合元件层，为其他去中心化协议提供可靠且可信的数据。

如图1所示，Band Protocol是一个Web3.0 元件层解决方案，用于管理数据，解决Web3 中区块链的数据可用性和可靠性问题的技术栈使用Band Protocol的Dapps通过Band的公用智能合约数据端存取数据，而不是通过区块链外部的预言机存取数据。**Band的数据是社区优化的数据来源**，为 dApp 使用者和开发者提供一个可以自行操作、优化和管理的数据来源框架，以达成可以被信任且可靠的目的。

通过创建社区治理型数据的标准框架，Band可以创建一种社区可扩展型的方法，以让所有的dApp可以广泛采用和集成可信数据。

Band数据介面与应用程式为可跨平台的，这意味着它们可用于优化和管理任何社区认为合适的数据目的。因此，数据来源可以使用平均值、中位数或多数进行聚合，并且可以从多个来源（如中心化外部数据来源或链上数据聚合器）进行聚合。范例包括：

资产价格数据来源包括加密货币对加密货币、加密货币对法币、传统证券和大宗商品价格。去中心化金融应用依靠这些外部价格数据来构建去中心化借贷、演算稳定币、衍生品交易等。

现实世界事件来源包括体育赛事、IoT 数据输出、现实付款交易结算等。许多智能合约需要依赖以上这些数据以达成交易。例如，预测市场可以非常简单的利用我们的运动事件来源建构，而不必须依靠代币持有人解决每个合约的输入输出。

身份认证数据包括如认证身份、信用评分、学历和工作经验等相关资讯。去中心化的交换市场及市集是一些需要依赖此类型数据的潜在应用程式。

位置数据包括 GPS 位置。 任何需要利用地图的去中心化应用程式都可以依赖此类数据。

最重要的是，**Band并不定义数据该怎么处理，而是提供社区集体地决定该数据将如何被使用或是优化**。 Band不去假设数据该怎么处理或是优化，这种权力完全掌握在希望使用这些数据进行去中心化应用的社区手中。创建最佳的被激励参与者，可使其为他自己与其他使用者的去中心化应用创建一个可靠的数据来源。

除了推进真正去中心化世界的目标外，Band Protocol还在建立一个私营企业之间可共用隐私数据的生态系统。许多数据是敏感的，由许多私营企业托管，而这些数据是无法轻松、安全地在正确的利益相关者之间共用数据。Band Protocol扩展了我们对Web3.0的支援，以涵盖此类隐私资讯共用，以便创建包括身份和信任等关键和有用资讯的世界数据库。

2 Band Protocol 概述

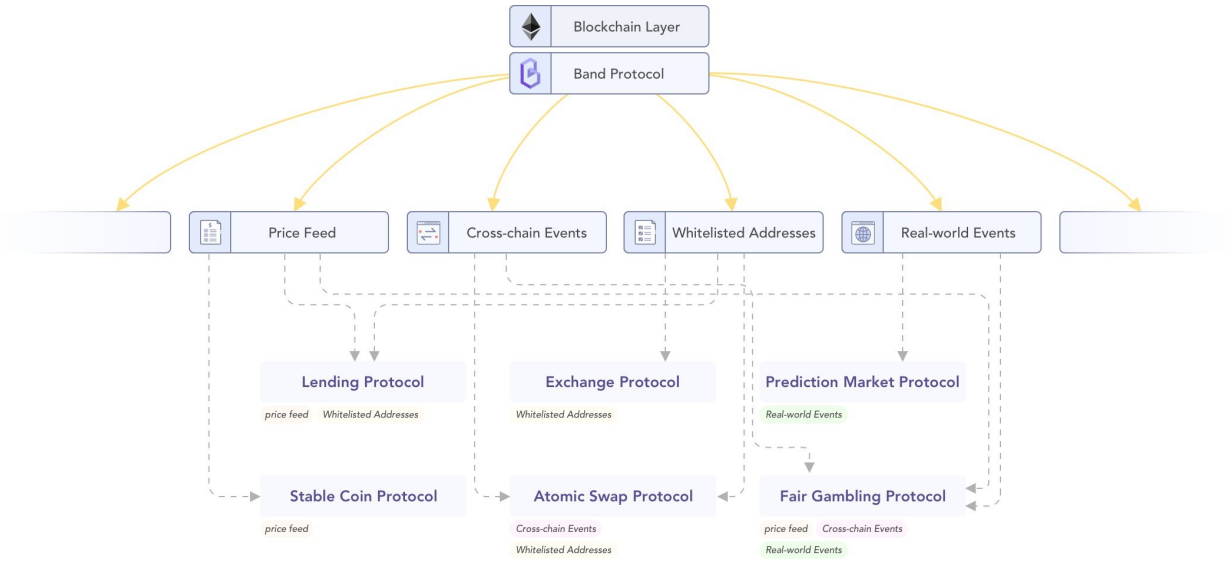

图 2：Band Protocol概述。区块链上共存多个社区化数据集，取决于其用途，不同的去中心化应用程式可对其进行组合运用。

Band Protocol的主要功能是弥合去中心化应用和现实世界数据之间的差距，利用经济激励模型同时可确保数据是准确和值得信赖的。Band Protocol最初将会是建立在以太坊网路上，但协议本身并不限于以太坊基础设施。随着该协议得到更广泛的采用，它将支援所有主流的智能合约平台，为新一代去中心化应用程式提供动力。

2.1 Dapps 的简单数据层

现有的数据提供者网路（如ChainLink或Oraclize ）需要智能合约和数据层之间的同步交互。这种方法不仅使实现智能合约复杂化，且因为两个区块链交易要按循序确认和执行故导致了重大延迟。

要获取数据，智能合约遵循图中所示的流程。

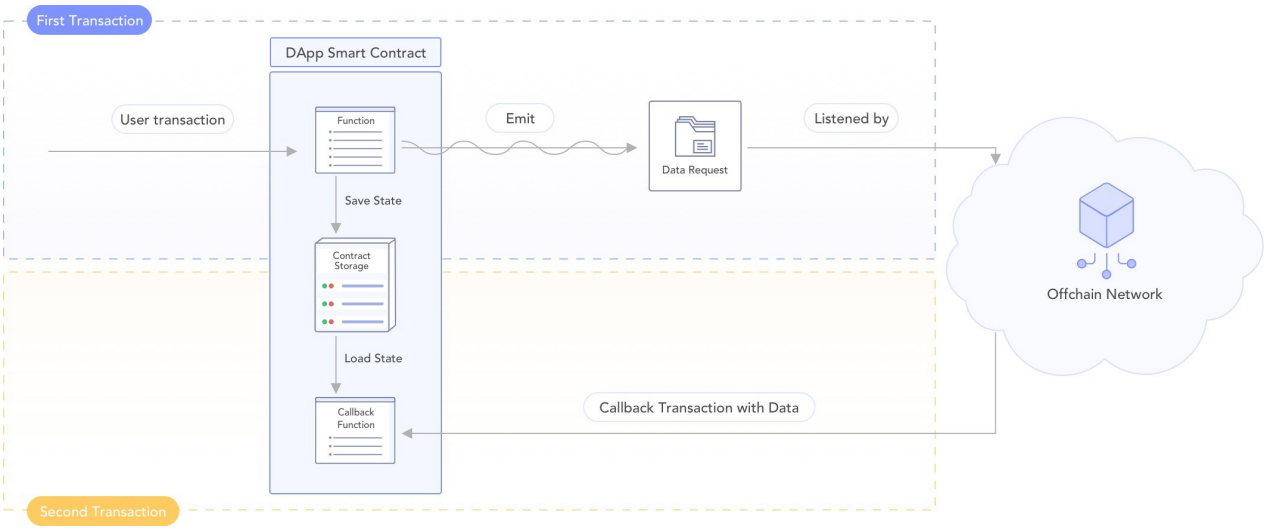

图 3：智能合约与现有预言机网路之间的交互。实现资讯交互需要两个分别的跨平台操作。

1. 合约将当前交易状态保存到合约的储存系统中。
2. 合约发出事件以请求数据，并停止当前交易。
3. 链下网路等待足够的交易确认数。
4. 链下网络利用提供的查询结果调用回调交易。
5. 合约验证交易，恢复状态，并继续执行。

Band Protocol改变了这个模式，除此之外还提供了去中心化应用程式一个直观的查询介面，只要对一个智能合约做简单函数调用，便能接收真实世界的数据。数据提供者负责将数据输入、整理到区块链，使其准备能在Dapps 同步时使用。

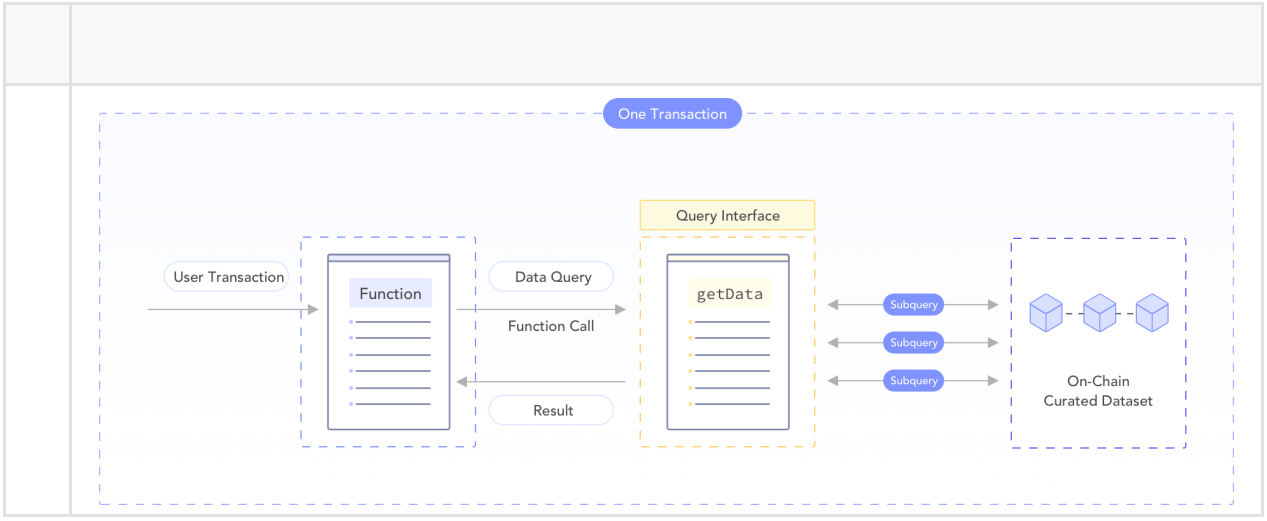

图 4：智能合约和Band Protocol之间的交互，请求参数仅发生在一个交易中

如图4所示，因此，对Band Protocol进行查询数据将非常简单，只会产生少许手续费(GAS)成本。此方法还可让更多应用程式同时使用一个数据集，因为数据随时可供多方使用，然而现有的解决方案需要每个应用程式执行冗余数据查询。

2.2 数据治理组联盟

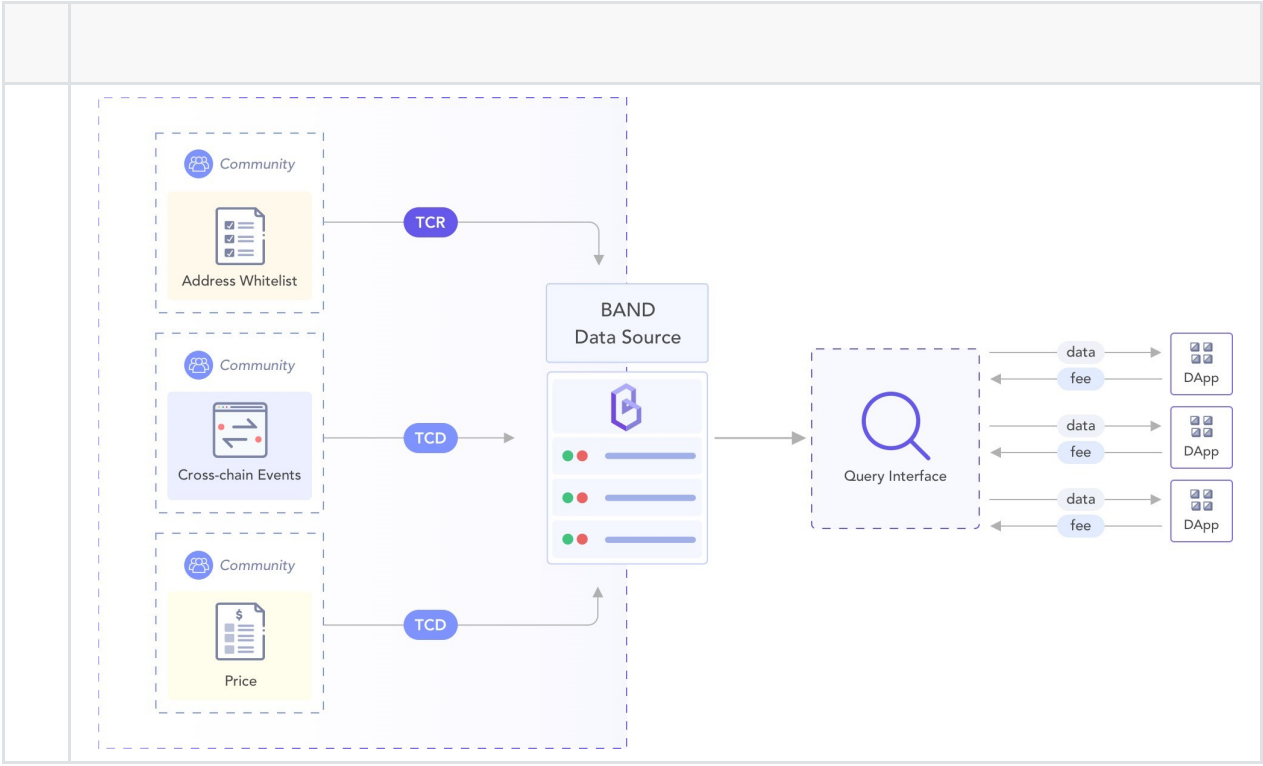

图 5：Band Protocol体系结构概述，多个独立社区一起为 dapps 提供数据。

Band Protocol 内部的数据集被拆分为多个数据治理组，每个治理组利用其自己独特的“数据集”代币，通过像**优化代币注册表**或**优化代币数据来源**这样的机制来控制、优化和管理其数据集。 虽然数据治理组是独立的，并且不共享相同的代币，但它们都通过与Band Protocol原生代币的绑定来保护。这与其他数据管理协议（如DIRT协议）有根本上的不同，其对所有的数据优化使用同一个代币。

而每组数据治理组都有一个代币有两个优点。

• **代币持有者有直接的动机来优化真实的数据。**当代币的价值直接与该组中管辖的特定数据集绑定，那整理真实数据这件事将完全带给代币持有者本身好处。相反来说，如果全网只有一个代币，则导致无法得知任何特定数据集的贡献是否会有显著的价值。因此，数据的安全性和可靠性模型较弱。这很容易导致**公地悲剧**(*Tragedy of the Commons*)和数据分歧。

• **贿赂代币持有者变得更加困难。**反面来说，如果全网仅有一个代币，一个错误的数据集可能不会导致代币的价值显著下降。因此，贿赂代币持有者来操作一个数据集的可能性比一个数据集有一个代币的情况更可能发生。因此在个别数据集个别代币这种情况下，代币持有者的损失将大于数据集的品质下降，更可防范贿赂的情况发生。

有关数据治理组（包括代币分发和治理模型）的详细资讯，请参阅第3节以了解更多详细讯。

2.3 Band Protocol 原生代币

Band Protocol是围绕自身的原生代币，Band Token(BAND)构建的。BAND 最初以ERC-20代币在以太坊区块链上发行。而随着我们部署到更多的区块链，BAND将支持在更多的区块链间转换。代币为协议生态提供了四个主要功用。

• **为数据治理组提供流动性并保证代币价值。**当发行数据集代币时，需要使用BAND代币来进行抵押。任何人都可以借由将 BAND 发送到数据治理组的连结曲线函数智能合约来购买数据集代币。相反，数据集代币可以被出售给连结曲线函数以接收回BAND。类似于ERC-20代币的利基，而较少流动的数据集代币亦会有一个利基。BAND当作全网代币，在它们之间提供全球流动性，因此任何人都可以随时在任何数据集代币之间购买、出售或切换。

• **保持所有数据集的价值。**当要铸造任何新的数据集代币时，都需要有BAND代币来当抵押。因此，随着数据集代币需求的增加，BAND的需求也会增加。这有双重效果。首先，BAND价格和代币的价值将会增加，使其有效地反映在所有数据治理组的价值上。其次，由于数据集代币按BAND价值进行估价，因此，BAND价格的上涨会提高所有数据治理组的安全性。

• **未来协议升级的治理。**类似于项目0x的ZRX代币，BAND可以被用来对于未来协议改进的提案和投票上。一但当Band Protocol部属后，其内部逻辑不能轻易更改，因为升级可能会影响系统的安全性和可用性。BAND代币将作为每个数据治理组中的利益相关者的治理代币，以投票的方式来解决未来的去中心化升级和治理问题，例如更改投票方案或添加新的优化数据方法。

• **通过已优化数据集注册表控制数据集品质。**最初第一组数据集将被严格精心挑选。但是，当Band Protocol逐渐朝向去中心化，创建或是优化数据集都将会变成是无需许可的。为了控制生态内部数据集的品质，BAND代币持有者将共同维护一个已认证的数据集注册表。BAND代币将为唯一表决的管道以保护注册表免受恶意参与者的侵

害。

2.4 协议经济

没有适当的经济激励，一个协议就无法继续生存。Band Protocol依靠查询费用来支付给数据提供者，并激励诚实的数据优化。**每当智能合约发出数据查询函式呼叫时，它必须附加区块链的本地货币（以太坊的情况下则为ETH）**。查询费用则根据数据集的提供者及代币持有者在治理参数设置的费用表来决定。

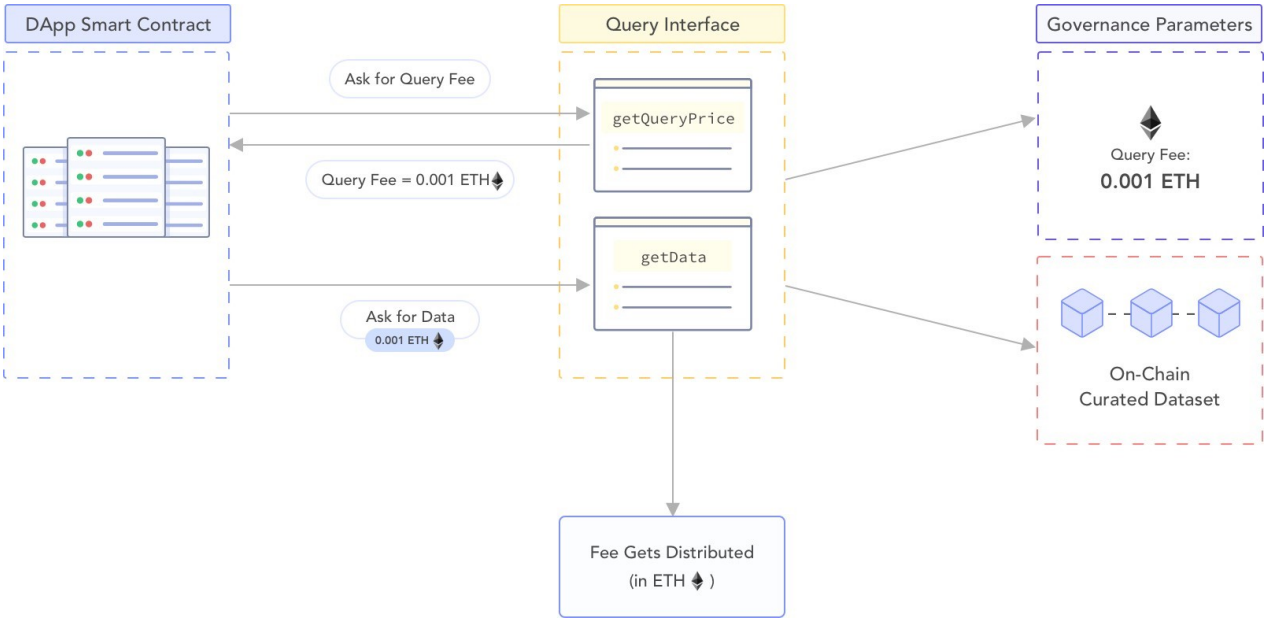

图 6：Dapps通过标准查询介面请求价格，该介面将会把结果转发到负责数据集治理参数的合约。

决定接受该区块链的原生货币主要是为了简化载入和集成的过程，因为要去假设每个程式都愿意去持有数据集代币或是BAND代币都是不太合理的。在实际运作中，Band Protocol利用去中心化交易协议，如Uniswap，即时将接受的货币转换成BAND代币，然后通过同一交易中的连结曲线函数转换为数据集代币。 因此，尽管Dapps 以原生货币支付，数据供应者和代币持有者仍会分得在数据集代币中的收入。此过程中，当越来越多的BAND被锁定到连结曲线函数中，数据集代币的供应量将会增加，从而导致这两种代币的价格升高。

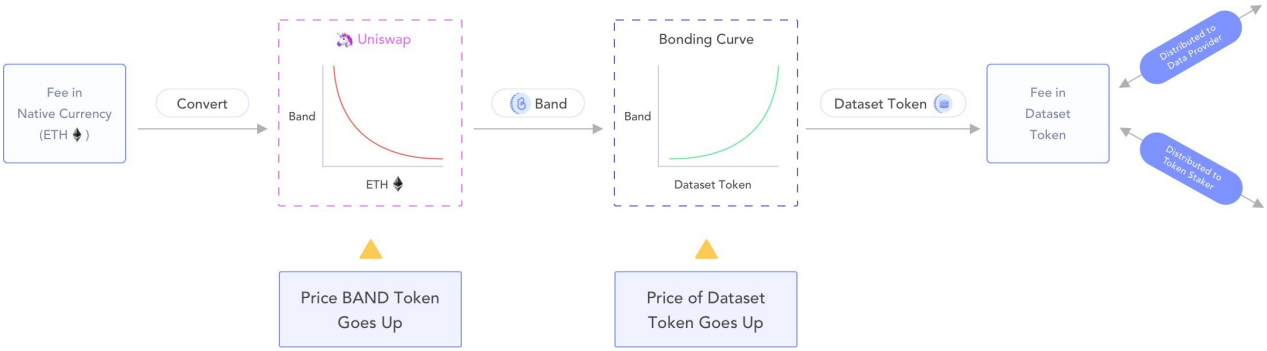

图 7：在查询价格时收到的原生货币手续费可透过Uniswap及连结曲线函数转换成数据集代币。

需要注意的是，在特定的数据管理办法中不一定需要收入才能给予参与者一定经济上的收入，像是优化代币注册表。在这种情况下，数据集社区可能集体决定将查询费用设置为零。

3 数据集治理组

数据集数据治理组是Band Protocol中最基本的单位。Band Protocol由多个数据组组成，每个数据组都有自己特别的代币。数据集代币持有者参与社区治理和数据库整理，作为回报，他们接受大众使用数据时所消耗的手续费，并从代币增值中获利。

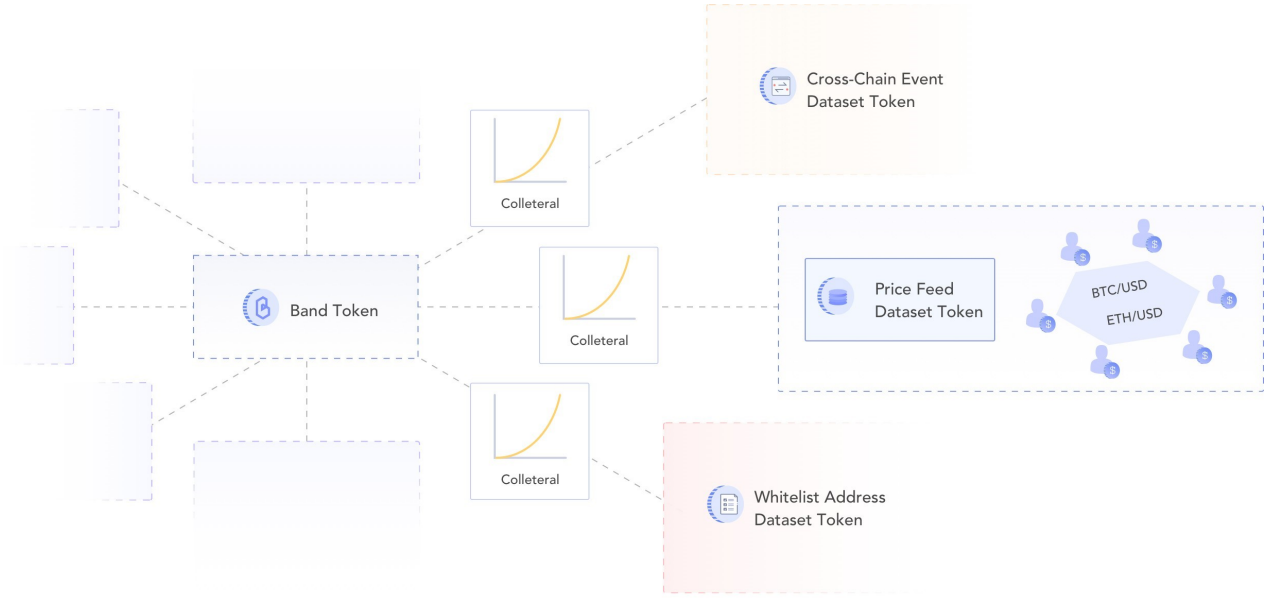

图8：Band Protocol中的每个数据集治理组都使用自己的代币进行数据治理。但是，每个代币都使用BAND代币绑定。以 BAND 作为抵押品可确保数据集代币始终具有有形的经济价值，并且不能无中生有。

3.1 数据集代币

数据集代币是 ERC-20类行的代币，在创建时与治理组一起部署。代币供应量由连结曲线函数合约控制，曲线函数合约具有铸造及销毁数据集代币的完全权限。数据集代币借由**激励代币的数据组织**管理和整理数据。Band Protocol为ERC-20 合约添加了三个额外的功能，以改善使用者体验。

• **ERC-223 的转接和调用**允许合约在单个交易中接收和处理代币。

• **最小余额快照**允许合约查询任何帐户的历史余额。这主要用于确定表决权和消除双重投票的可能。

• **转帐冻结**允许已授权的合约关闭代币转帐功能。这主要可用于实施权利证明机制，同时仍允许持有者保留其代币保管权。

3.2 担保代币发行

数据集代币发行权是以BAND代币为担保与数据治理组的连结曲线函数所结合。连结曲线函数概念最初由*Simon de la Rouviere*提出 。连结曲线函数确保（1）数据集权证的供应量上升时整体价值也会跟着上升，和（2）代币持有人总是可以选择借由出售其数据集代币以接收回等比例的BAND代币此退出机制。这可确保数据集代币在任何情况下都保持流动性和有效性，有一个好的激励保护机制是成功执行的关系。

3.2.1 价值-供给 功能

这种凸函数和单调递增函数可以说明数据集代币的总供给量与其所有抵押的BAND代币总价值之间的关系。 换句话说，假设现在供给S，V（s）产生在连结曲线函数合约中抵押的BAND的总数。 可以注意的是，通过定义此供应函数的值，任何人都可以轻松地借由给定总供应量P（s）的数据集代币的现货价格推导出该特定供应值处的价值。

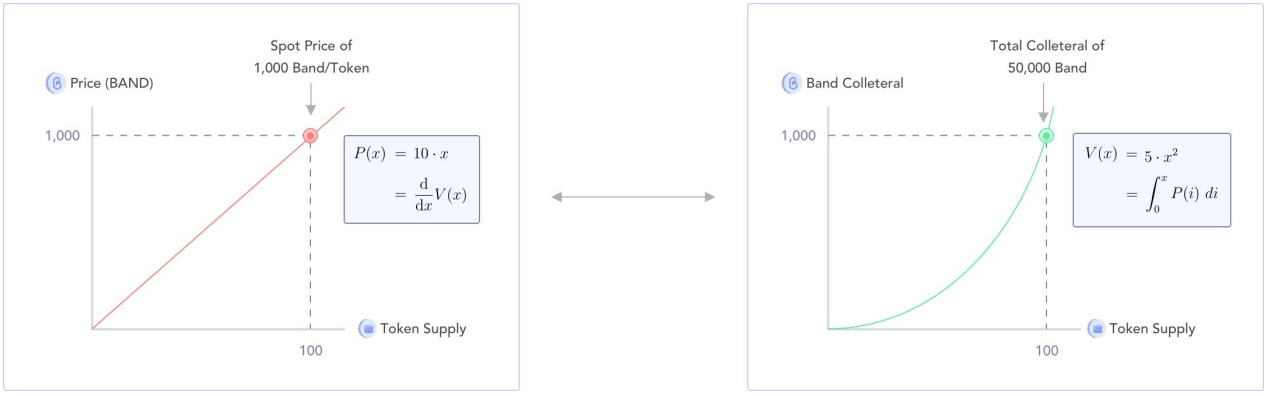

图 9：具有线性价格的代币和二次抵押品的连结曲线函数示例。这两个图形是相等的。

每当有人要购买数据集代币时，买家就会将 BAND 代币发送到连结曲线函数合约。合约计算调整后的数据集代币供应量，并将铸造完成额外供应量给买方。当有人决定使用卖出数据集代币时，就会发生相反的转换。

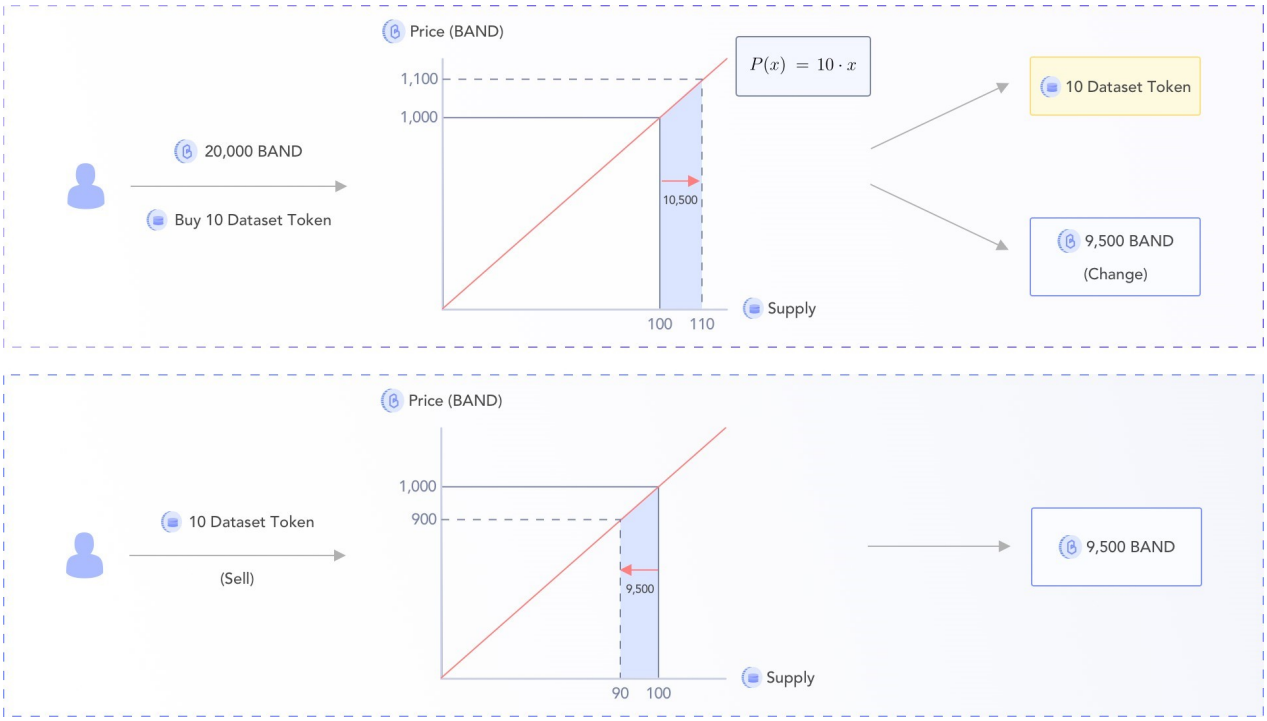

图10：当有人决定借由连结曲线函数合约购买或出售代币时的情况示例。

为了防止超前交易，连结曲线函数合约允许用户限定价格，模拟传统限价单。 如果交易未达到限制条件，则该交易将会重制，防止使用户执行错误的订单。

3.2.2 程式代码库

Band Protocol提供了一个通用的智能合约库，用于在 Solidity 中建构任意的程式码（有关更多详细资讯，请参阅视频说明）任何可以由二进制和三元运算来表述的递回应用及数字常数皆可被编码。

3.2.3 流动性价差

流动性价差控制数据集代币的买入和卖出价格之间的差异。可以通过在*bonding:liquidity_spread*下的治理参数设置。高流动性价差使得恶意参与者更难**预先交易攻击(Front-running attacks)**。然而，高价差会导致代币持有者在兑换数据集代币时收到较少的BAND。流动性价差收入将会发送到由*bonding:revenue beneficiary*参数指定的合约位址。预设是治理组的建立者地址。

3.3 治理参数

数据治理组内的治理参数决定了该组的其他智能合约的逻辑如何执行。也就是说，治理参数内会有一组 32 位元组金钥和 32 位元组的值配对。32 位元组值依其金钥可以为整数、百分比值、区块链地址或 IPFS 杂凑值。举例来说，*bonding:liquidity spread*的参数控制连结曲线函数买入和卖出现货价格之间的价差百分比的整数。数据集代币持有者可以通过以下过程对参数进行更改。

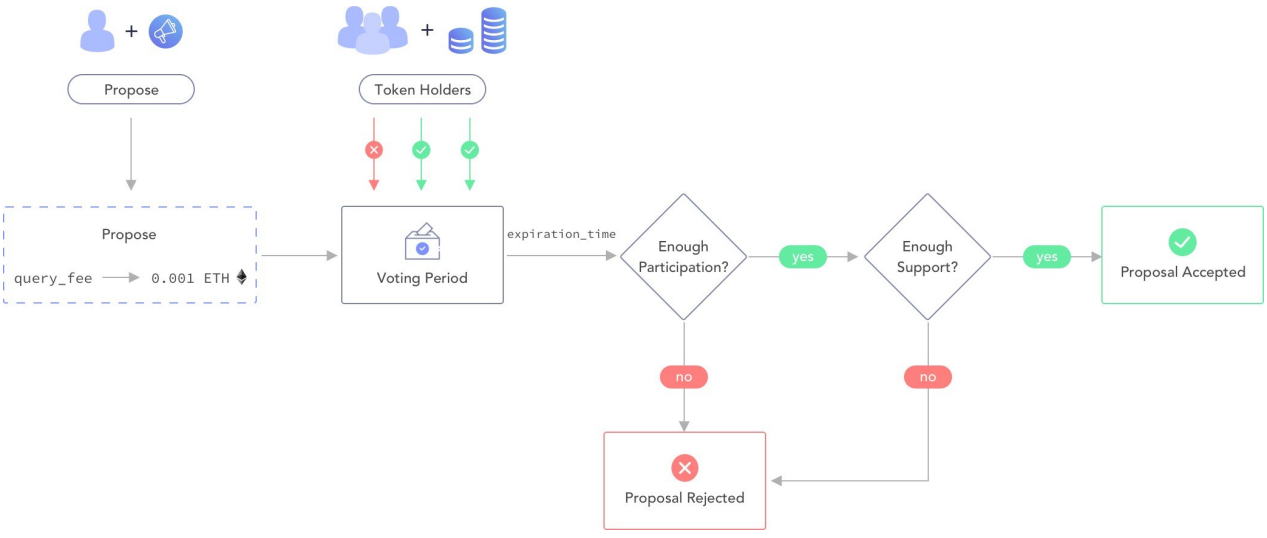

图 11：更改参数提案的周期。

1. 数据集代币持有者若想更改一个或多个参数，可以对治理合约发起一个”提案”交易，从而创建一个提案。一旦提案创建后，这个提案将在*params:expiration_time*的时间内保持开放。
2. 当提案开放时，代币持有者可以**投票赞成**或否决该提案。
3. 投票期结束后，如果（1）所有参与投票的比例超过*params:min particiation pct*的比例，和（2）超过 *params:support_required_pct*：支持投票批准的参与代币的百分比，提案获得批准并应用更改后的参数。
4. 此外，为了促进一致的参数更改，当所有同意票的代币大于*params:support_required_pct*比例，则可以在提案到期之前完成修改。

在创建数据治理组期间，将会需要同时设置连结曲线函数和治理合约的初始参数。需要注意的是，治理合约本身的三个参数也可以通过相同以上的提案投票过程进行更改。

4 激励代币的数据组织

在第一次主网启动期间，Band Protocol将为数据治理组提供两个主要模型，以利其之数据集代币得共同治理和梳理数据。我们目前还在积极研究更多的数据优化模式，并将在未来的协议升级中添加。另外数据治理组不一定只能使用一种优化模式，同一数据集代币可用于在同一数据治理组中的多个数据集。本节主要讨论技术代币机制。更具体将在*潜在应用场景*部分中解释。

4.1 优化代币数据来源

优化代币数据来源（TCD） 是一种用大吞吐量来管理数据的方法。TCD在许多面向类似于**委托持有量证明(DPoS)**。**代币持有人**以候选人的名义获取代币，从而共同选择数据提供者。**数据提供者**在特定的情况下有权向公众提供数据，并赚取从数据查询中收取的部分费用。

• **数据提供者**申请向数据集提供数据的许可权。拥有最多代币的提供者得到提供数据的权利。 他们收到大部分的查询费，从而愿意提供他们的服务。

• **代币持有者**将代币押用于他们信任的数据提供者。他们赚取一小部分的查询费用，以换取保护最可信数据供应商的名单。

4.1.1 TCD 优化如何工作？

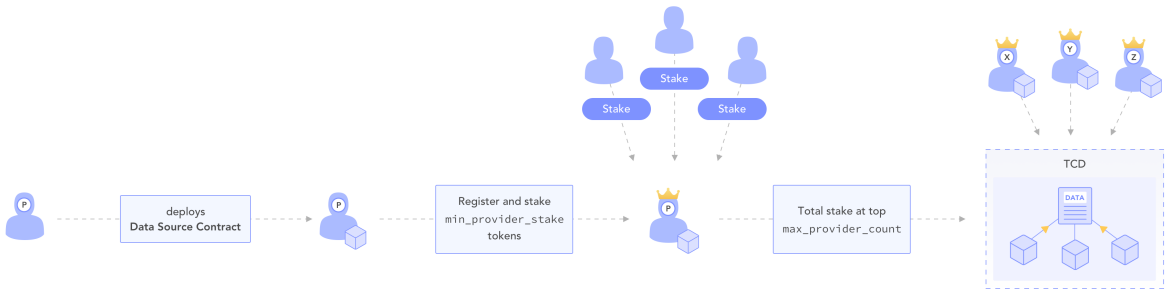

图12：TCD供应商促使自己能成为提供数据的一员之流程图。

• 希望成为数据提供者的代币持有者将部署**数据来源合约**，并借由持有*min_provider_stake*数量的代币后注册成为供应商候选人。

• 其他代币持有者可以为他们信任的供应商候选者提供代币当作权益证明。拥有最大函数max_provider _count代币持有量的数据提供者候选人将成为**有效数据提供商**。

• 每当出现数据查询时，TCD合约都会向每个有效数据提供者发出子查询。查询结果将**聚合**成为数据查询的最终结果。

• Dapps必须为每个查询支付*query_price*价格的ETH，该查询得到后会转换成社区代币有效数据提供者将得到*owner_revenue_pct*比例的收入。其余的归社区成员，与他们的代币持有量成正比。

• 代币持有者可以随时**提取**其代币，并将其代币与部分收入一起收回。提款后，将重新计算有效提供者清单。

• 数据供应商也可以**提取**其代币。但是，他们必须通知TCD智能合约关于他们的倾向撤回的*withdraw_delay*持续时间。这允许普通代币持有者在数据者之前先撤回其代币，预防数据者恶意操作。

4.1.2 与查询介面串接

查询外部数据的使用者利用查询介面查询数据，该介面聚合当前有效数据提供者之间的数据。并且仅当超过2/3的有效数据提供者提供此类数据时，数据点才有效。 这可以保证系统可以容忍多达1/3的恶意数据提供者。 Band Protocol将会在一开始提供两种聚合数据的方式，例如：

• 给定在金钥里所有结果中的中位数。

• 给定在金钥里所有结果中的多数值，如果没有多数则宣告失败。

4.1.3 经济分析

本小节讨论优化代币数据来源的经济观点。

对于数据提供者是低成本的。更新数据点对数据提供者的成本非常小，举例来说数据提供者在Ethereum上更新键值，其GAS成本是约26000 GAS（5000用于存储字元更新，21000用于完成交易）。因此每小时更新一次此数据点的成本仅为(假设5Gwei的GAS价格)26000*24*5/109 =0.00312 Ether，或是每天$0.624美元(ETH定价200 USD/ETH)。对于重要数据点（如现实世界的价格反馈或其他区块链的哈希值），每天每个数据点的更新成本只要不到一美元是相当低的。 此外，在未来的Band Protocol更心中，数据提供者还可以通过提供数据集的*哈希树值(Merkle hash)*而不是每个单独的数据点来节省成本。有关详细信息，请参阅第7.1节。

对于数据消费者是低成本的。数据消费者在向网络广播交易时已经支付了GAS。 假设复杂的交易需要平200000 GAS，GAS价格为5 Gwei，则交易已经花费20美分（200 ETH/USD）。 因此，假使为确保数据安全而额外支付10美分不应该会破坏用户体验。请注意，可以根据数据的安全需求调整费用。

健康的利润率和名誉收益。结合前两点，我们可以看到数据提供商只需要少量的查询数即可达到盈亏平衡点。使用上面的数字，如果有10个数据提供者，则每天只需要10*0.624/0.1≈60个查询来支持数据提供者。超过这些外，数据提供商就是纯粹的经济利益。除了经济效益之外，数据提供商还通过采用该协议获得声誉。例如，加密货币交易所可以通过向网络提供有效和最新的价格信息来获得支持去中心化生态系统的声誉。

市场可扩充性。随着更多的去中心化应用程式加入Band Protocol，它们就可以开始消耗数据和支付费用，而不会给数据供应商带来任何边际成本。这直接导致了数据集市值的增加，使数据提供者和代币持有者受益。此外，数据治理组可以扩展以支持更多TCD，而无需发出不同的数据集代币。

4.1.4 安全分析和可能的攻击媒介

≤1/3的提供者商串通：少数数据提供商可能串通以篡改数据结果—恶意攻击者数量微不足道不会影响网路的整体数据完整性。我们下面显示案例分析。

> 2/3的有效数据提供者持续提供数据：在这个案例中，诚实的提供者提供了大于一半的数据（因为> 2/3提供有效数据，≤ 1/3提供恶意数据）。这归功于中位数级多数，得以抵抗小于一半的恶意数据点，我们的协议还是可以正常运作。

≤2/3的有效数据提供者持续提供数据：在这个案例中，我们的协议将会暂停提供数据给用户。也就是说我们宁愿暂停也不愿提供不安全的数据。当>2/3的数据继续被有效提供，数据供给才会继续，以确保数据的正确性。

> 1/3的提供者商串通：多数数据提供商可能串通篡改数据结果 — 如果超过三分之一的提供商提供不良数据，协议将不可避免地向dApp提供不良数据。 但是，如果发生此类攻击并且数据变得不那么有用，则代币的价值基本上被破坏，因为不再有任何dApp愿意为这些数据付费。 “撤销延迟”机制阻止数据提供者在普通代币持有者之前将数据集代币转换为BAND。这可确保数据提供商在治理组崩溃中遭受最大的损失。巨大的经济损失威胁应足以阻止全社区与数据提供者勾结。 不仅与此，一旦串通的话现实声誉损失也可以作为防止数据提供商恶意行为的动机。在未来，我们还会考虑强制使用代币削减作为惩罚条件来进一步消除不诚实行为。

富有的攻击者： *富有的对手可能使用大量资本购买代币并获得显著的攻击力，对TCD进行1/3攻击* –然而购买代币推翻现有的代币持有者是令人望而却步的昂贵。由于代币发行的连结曲线函数性质，新的代币越来越昂贵。作为一个具体的例子，要在20%的储备比率下实现1/3的连结曲线函数供应量，需要铸造目前供应量的50%。成本是1.5（100%/ 20%）≈当前抵押品的7.6倍，对于市值很高的治理组来说，成本极高。未来可能遇到的威慑还包括延迟成为数据提供者的资格，例如他们需要先购买并持有代币一段时间才能够享受持有权益。这样的延迟治理组可对突然上涨的价格做出反应

拒绝服务：由于数据提供者的身份可能为人所知，恶意攻击者可能会直接攻击提供者，使他们无法提供数据 - 数据提供者负责对于服务正确连结到区块链，但与直接提供给使用者数据的传统数据 API供应商不同，Band Protocol 利用区块链基础设施来达成数据分发。攻击者几乎不可能关闭 Band Protocol的数据服务，除非他们关闭整个区块链系统。

4.2 优化代币注册表

代币持有者可以使用**优化代币注册表（TCR）**共同构建公共数据集。TCR 是包含 32 位元组项次（包括字串、地址、数量或杂凑）的链上清单数据结构。 总共有三方参与构建 TCR，包括**应用程式候选人**、**代币持有者**和**数据消费者**。

• **应用程式候选**将数据集代币抵押于系统中的项次，实质上可作为数据提供者。如果它们的项次与TCR的准则不一致，则它们可能会丧失代币。

• **代币持有者**监视TCR上项次的品质。他们筛选低品质项次，并以投票的方式支援持续的筛选。而他们因执行管理工作而获得奖励。

• **数据消费者**读取和利用有关 TCR 项次的资讯。消费者不付费，他们为TCR项次的拥有者提供内在价值。

可能通过TCR进行众筹来源和优化的数据示例包括但不限于，已验证满足某些标准的加密货币项目清单、符合社区标准的新闻和研究清单，或由受信任的第三方提供的唯一身份认证清单。当涉及到透明度和庞大规模时，TCR提供潜在优势超过中心化数据整理方式。

4.2.1 TCR 优化如何工作？

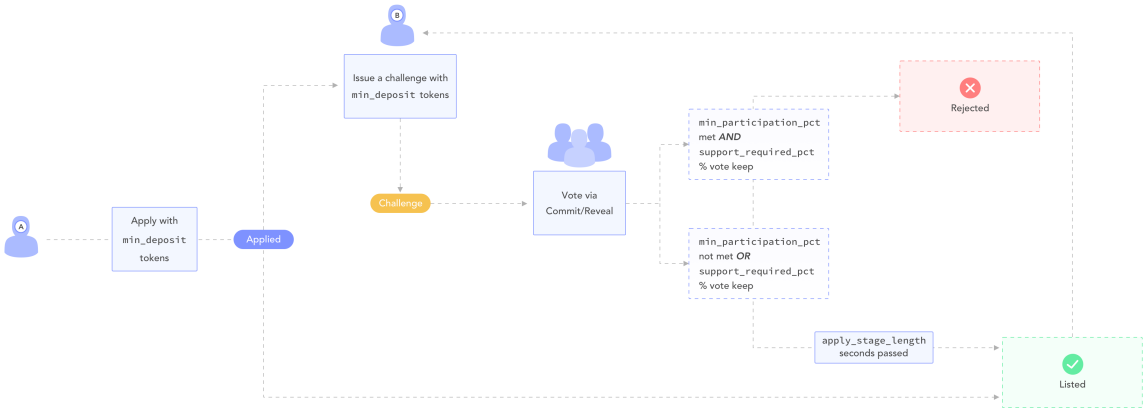

图13：TCR内项次的周期

1. 候选人通过透过持有min_deposit函数的数据集代币来申请在 TCR 上列出项次。如果该项次在*apply_stage_length*函数持续时间中没有被提出质疑，则会自动列出该项次。
2. 代币持有者可以通过持有匹配的存款来质疑项次。项次进入投票期间，使用***信息提交协议(commit-reveal)***，代币持有者投票保留或删除该项次。
3. 如果参与的代币参与率不到*min_participation_pct*函数，则认为该质疑没有成功。匹配的存款将返回给质疑者，并且项次保留在 TCR 上。
4. 如果有足够的代币参与，并且超过*support_required_pct*函数比例投票的项次将

被删除，项次的存款成为质疑者的奖励。质疑者接收*dispensation_percentage*函数百分比的代币，而获胜投票者得到剩余的部分。

5. 另一方面，如果质疑失败，质疑者抵押的代币将被没收，并在项次所有人和投票保留人之间分配。项次所有者接收*dispensation_percentage*百分比，而获胜投票人得到剩余部分。

Band Protocol正在积极试验在项次存列中加入***降价抵押模型***，它允许项次在随着时间的推移而价值减少。

4.2.2 安全性与经济分析

自2017年以来，TCR的经济和安全一直在被积极研究。感兴趣的读者可以从*TCR Reading List*中了解更多关于机制的知识。 除了众所周知的观点之外，如2.2节所述，Band Protocol在每个治理组的基础上使用不同的数据集代币这一事实也有助于提高系统的内在激励和安全性。

5 潜在问题和限制

5.1 寄生数据来源

寄生智能合约将会消耗数据集中的数据，然后以更低的成本将其重新分发到其他 Dapps。在本质上，它充当原始事实的缓存层，导致原始优化数据集的收入损失。虽然传统公司可以以法律阻止转售企业数据，但自主数据治理组的智能合约却没有这种特权。不幸的是，Band Protocol作为开放式协议无法阻止这种存在。

但是，选择依赖寄生智能合约的Dapps是会冒着收到已失效或恶意数据的风险。 随着Dapps变得越来越大，由于他们的信任和声誉受到威胁，他们应该就会选择消费来自官方数据源的数据。

5.2 链上投票

基于代币的链上投票的可行性尚未得到充分证明，特别是在潜在的贿赂方面。 这个主题已经被几个团队积极研究。 然而，截至目前，基于代币的投票是最广泛采用的机制，是对抗**女巫攻击(Sybil Attack)**的最佳方式。 Band Protocol实现了以下额外的层来阻止攻击。

• 虽然数据集代币可以通过连接曲线函数自由买入或卖出，但合约在买入和卖出价格之间施加了小的流动性价差。这使得购买代币只是为了影响特定的投票必须付出高昂的代价。

• 声誉对于权益也是关键资源。数据提供者一般需要提交他们的身份，以获得社区的信任。因此，每个数据提供者是将货币价值和声誉都抵押于数据集 — 这也降低了他们采取恶意操作的动机。

• 每个在Band Protocol内部以投票为基准的决定都可以被社区重新考虑。如果前一个质疑者以不利的结果结束，则可以再次发起TCR质询。治理提案也是同样的道理，可以被重新提案。

Band Protocol将继续积极研究链上投票，如果更好的技术和实现方式，将会升级开发投票机制。

6 潜在应用场景

6.1 去中心化金融

大多数现有的去中心化金融（DeFi）应用共用一个关键的单点风险来源：**外部价格数据来源**，知名的项目，如MakerDAO、Compound、Dharma、dYdX、或是SET，仅仅依靠相对较少的受信任开发人员来向协定提供链外价格资讯。而Band Protocol可以填补提供此关键资讯，使项目能够于在专注于他们最擅长的方面的同时享受Band数据供应商带来的安全数据。这也延伸到未来的去中心化金融应用，例如现实世界资产的衍生品交易，这需要获取现实世界的数据，如利率，外汇汇率，股票，债券和大宗商品等证券的价格。

6.2 去中心化商业

许多去中心化应用程式使用代币作为付款条件，这意味着他们必须以代币为其产品和服务定价。但这很是困难的，因为这些应用通常会以稳定的法定价格定价，而这些代币的价格波动却很大。 因此，他们需要一个机制来不断将其商品的法币价值转换为代币价值，这需要一个可靠，持续的提供加密货币价格的来源。

6.3 身分识别层

许多去中心化应用程式难以处理假帐户和女巫攻击(Sybil attacks)的难题。如Vitalik所言，身份层是构建抗串通代币系统的关键部分之一 。Band Protocol可以作为不同平台间身份认证服务的协议，以共同管理身份资讯，通过简单的查询介面程式进行整合。

6.4 游戏、赌博和预测市场

游戏和赌博一直是区块链生态系统中最大的行业之一。通过使用Band Protocol，dApp 可以访问不受单一现实来源控制的可信现实世界资讯。与 DeFi 类似，这允许开发人员专注于其核心功能，同时利用Band Protocol的安全性。

6.5 供应链溯源

使用加密货币以完全无需信赖的方式购买和销售真实世界的产品，在当前技术下几乎是不可能的。Band Protocol允许供应链相关数据，如发货讯息或非区块链支付，智能合约可以在链上验证此类资讯，并有效地执行财务逻辑。

6.6 现实世界API连接

智能合约目前是有限的，因为它们无法在数位世界和物理世界之间架起桥梁。而Band Protocol可以支援现实世界API连接，所以智能合约完全意识到现实世界事件以及能够向 API提供输入到触发特定事件。举例来说，若连接银行API，智能合约可以确切知道有链下交易发生，或是当有链下交易发生可以自动触发合约。

7 未来技术目标

7.1 优化大量数据集

为了使Band Protocol成为数据查询的所在，就像是于传统的网路*维基百科*或*维基数据*，它必须能够支援大量数据集。在目前的 TCD 设计中，数据供应商必须将数据集中的每个数据都提交到区块链，由于成本高昂，这根本上不可行。Band Protocol的下一次版本将允许数据提供程式仅提交完整数据集的***哈希树(Merkle root)***。原始数据将通过链下网路分发，代币持有者将共同验证数据。链上智能合约可以通过同一查询介面检查数据有效性。

7.2 跨链通信

数据集数据治理组将可用于整理其他区块链的杂凑值。结合上述的哈希树压缩，以太坊智能合约将能够检查其他区块链上发生的情况，如Bitcoin或EOS。

我们将Band Protocol设定为跨区块链的协议，每个被支援的区块链（包括 Cosmos Network和EOS）都提供Band Protocol。为此，Band 代币将支援区块链之间的跨链原子交换，类似于 BancorX，尽管使用由 Band Protocol 本身提供的去中心化数据外部呼叫。启用此功能后，我们可以有效地将不同区块链间相连结，并增强更广泛的去中心化应用。

7.3 链上数据隐私

某些数据无法作为纯文字进行存储和发布。个人资讯（如姓名、年龄或信用评分）是隐私的。然而，这样的资讯对于解放去中心化应用的潜力至关重要。例如，非抵押贷款申请需要个人信用才能做出合理的贷款决定。在未来的Band Protocol升级中，我们计划采用尖端的加密技术，包括***可信执行环境 （TEE）***和***零知识证明***等等允许在不损害使用者隐私的情况下进行不须信任的数据决定。

白皮书细节以原文为主，相关翻译建议或是加入 Band 讨论群，请加 wechat id: ivyair1995。