XY预言机网络：
基于来源证明的加密位置网络

Arie Trouw*，Markus Levin†，Scott Scheper‡

2018年1月

摘要

随着基于位置的互连技术快速发展，我们的隐私和安全高度依赖于位置信息的准确性和有效性。为了消除利用中心化实体来控制位置数据流的需要，人们做出了各种尝试，但是每一次尝试都依赖于在物理世界中收集这些数据的设备的“真实完整性”。我们提出了一种去信任的加密位置网络，该网络使用一个基于零知识证明链的新型公式，以确定位置信息的高度确定性。**XYO网络（XYO预言机网络）**是一种虚拟网络，可跨许多设备类别和协议执行分层的位置验证。该网络的核心是一套新颖的加密机制，被称为**来源证明**（Proof of Origin）和**绑定见证**（Bound Witness），可将区块链技术和现实世界数据收集方法整合成为一个系统，直接与当今的应用程序进行交互。

1 简介

目前，大多数智能合约的实施都依靠一个或一组权威性的预言机来解决合同纠纷。如果双方能够就特定预言机的权威性和真实性达成一致，也就没什么问题了。但是，在许多情况下，由于存在错误或损坏的可能性，根本不存在适当的预言机，或者预言机的权威性有待商榷。

位置预言机便属于这一类型。要预言物理世界中物体的位置，就要依赖于给定预言

*XYO Network, **arie.trouw@xyo.network**

†XYO Network, **markus.levin@xyo.network**

‡XYO Network, **scott.scheper@xyo.network**

机的报告、传递、存储和处理组件，而所有这些组件往往都会引入错误，并且可能会被破坏。由此导致的风险包括数据操纵、数据污染、数据丢失和共谋串通。

因此存在以下问题：由于缺乏去信任、去中心化的位置预言机，位置的确定性和准确性会受到严重影响。像以太坊和EOS这样的平台已经被人们广泛采用，因为这些平台能够以安全在线的方式调解交互，主要用例包括以初始令牌销售（ICO）形式筹集代管费用的托管交易。然而，到目前为止，由于当前信息渠道十分嘈杂，数据完整性可能会发生损坏，每个平台都只应用于网络世界，而不是现实世界。

XYO网络一直致力于让开发人员（例如为区块链平台编写智能合约的开发人员），通过类似于API的方式与物理世界进行交互。XYO网络是世界上第一个预言机协议，可支持两个实体在没有中心化第三方的情况下，在现实世界中进行交易。我们的虚拟网络可让开发人员通过去信任的方式执行位置验证，创造出了一种新的协议，未来应用前景十分广阔。

XYO网络将建立在现有基础架构之上，其中涵盖在全球流通的超过1,000,000台设备，这些设备遍布我们面向消费者的泛联业务渠道。XY的蓝牙和GPS设备允许日常消费者将物理跟踪信标放置在他们想要跟踪的事物上（如钥匙、行李、自行车甚至宠物）。如果他们错放或丢失了此类物品，他们可以通过智能手机应用程序查看其确切的位置。在短短的六年时间里，XYO网络创造了全球最大的消费者蓝牙和GPS网络。

---

2 历史背景与传统方法

2.1 位置证明

可证明位置的概念早在20世纪60年代就已存在，甚至可以追溯到20世纪40年代的陆基无线电导航系统，例如LORAN[2]。今天，一些位置服务可以将多种验证介质叠加在一起，通过三角方法和GPS服务创建位置证明。然而，这些方法仍无法解决我们今天在位置技术领域面临的最关键问题：设计一个能够检测欺骗性信号并阻止篡改位置数据的系统。有鉴于此，我们提出了具有.重大意义、聚焦于证明物理位置信号来源的加密定位平台。

令人惊讶的是，早在2016年9月，在以太坊的第二届开发者大会（DevCon2）上，来自柏林的以太坊开发人员Lefteris Karapetsas便提出了将区块链技术应用位置验证的概念。Karapetsas的项目“Sikorka”通过使用他所称的“存在证明”，能够将智能合约部署于现实世

界当中。他用于连接位置与区块链世界的应用程序主要聚焦增强现实用例，并且他还引入了新的概念，如关于位置证明的挑战问题 [3]。

2016年9月17日，“位置证明”一词正式出现在以太坊的社区中 [4]。之后，以太坊基金会的开发人员Matt Di Ferrante对此做出了进一步阐述：

> *“毋庸置疑，位置证明实际上是最难实现的事情之一。即使有许多参与者可以证明对方的位置，但不能保证这些参与者将来不会简单地串通了事，并且由于始终只能依赖多数人的“证言”，这会造成严重的缺陷。如果可以使用某种类型的专用硬件设备，这些设备具有防篡改技术，即便有人试图破解毁坏私钥或更改其上的固件，也可以实现较高的安全性，但同时，GPS信号也有可能会被篡改。要想正确实施这种方法，就需要大量支持资源和许多不同的数据源，才能保证准确性，而这种项目需要大量的资金。”[4]*
>
> *—Matt Di Ferrante，以太坊基金会开发人员*

2.2 位置证明的缺陷

总之，位置证明可以理解为利用区块链的强大特性，如时间戳和去中心化，并将它们与具有防欺骗功能的、位于区块链之外的位置感知设备相结合。我们将加密定位技术领域称为“加密定位”（crypto-location）。此外，类似于智能合约，加密定位系统也具有致命缺陷，具体来说，智能合约严重依赖于利用单一事实来源（因此也存在单一故障来源）的预言机，而当今的加密定位技术需要利用能够报告对象位置的离链设备。在智能合约中，离链数据源是预言机。而在XYO网络中，离链数据源是一种在现实世界中四处移动的特殊预言机，我们称之为“哨兵”。XYO网络的核心创新之处在于无标记、基于位置的证明，这是我们系统组件的基石，能够创建去信任的加密定位协议。

---

3 XY预言机网络

> *“众所周知，多年来，我们一直亟需一个难以攻克、坚若磐石的系统来补充全球定位系统（GPS）。GPS非常准确和可靠，但干扰、欺骗、网络攻击和其他形式的人为干涉似乎越来越频繁，严重性也日益攀升。这可能会对我们的生活和经济活动造成毁灭性的影响。”[5]*
>
> *—Dana Goward，RNT基金会主席*

3.1 简介

XYO网络致力于构建一个去信任、去中心化的位置预测系统，该系统能够抵抗攻击，并在查询可用数据时提供最高的确定性。我们利用一系列抽象技术构建了这个网络，通过零知识证明链大大降低了系统组件中出现位置欺骗的风险。

3.2 网络概述

我们的系统为互连设备提供了一个协议入口，通过一个加密证明链提供高度确定的位置数据。用户可以发起交易，称为"查询"，以便在任何拥有智能合约功能的区块链平台上检索一段位置数据。[1] 然后，XYO网络的聚合器会监听到发布到合约中的这些查询，并通过一组分散的设备（这些设备会将加密证明转发给聚合器）获取准确度最高的答案。然后，这些聚合器在就分数最高的答案达成共识后，会将这些答案反馈给智能合约。这些网络组件可以确定一个物体是否在给定时间处于特定的XY坐标上，并且具有最可证明的、去信任的确定性。

XYO网络包含四个主要组件：**哨兵节点**（数据收集器）、**桥接节点**（数据中继器）、**归档节点**（数据存储器）和**预言节点**（答案聚合器）。哨兵节点通过传感器、无线电和其他手段收集位置信息。桥接节点负责从哨兵节点处获取这些数据并将其提供给归档节点。归档节点负责存储这些信息，以供预言节点分析。预言节点负责分析归档节点提供的启发式位置数据，以便生成查询答案并为其分配准确性分数。然后，预言节点会将这些答案反馈给智能合约（因此，预言节点充当着预言机的角色）。准确性分数，即**来源链分数**，是通过被称为**来源证明链**的一系列零知识证明确定的。该链可保证两条或多条数据来自同一来源，而不显示任何底层信息。查询路径中的每个组件都会生成自己的来源证明，然后将证明链接到数据所抵达的每个组件。来源证明是一种新颖的公式，它会沿着网络中的中继器路径建立一个加密证明链，以提供高度可信的真实世界数据。这个**来源证明链**将我们对一段位置数据的信心封装到了收集数据的第一批设备中。我们将在下面的章节中探讨来源证明的工作原理。

为了在预言节点之间建立一个去中心化的共识机制，XYO网络将依赖一个公共的、不可变的区块链 —

XYOMainChain，该区块链会存储查询交易以及从预言节点收集的数据及其相关的来源分数。在我们深入了解整个系统的功能细节之前，我们将明确定义网络中每个组件的职责。

---

[1] 以太坊、Bitcoin+RSK、Stellar, Cardano、IOTA、EOS、NEO、Dragonchain、Lisk、RChain、Counter-party、Monax及其他。

3.2.1 哨兵节点

哨兵节点是位置见证人。它们负责观察数据启发式算法，通过生成带有时间戳的分类帐来确保启发式数据的确定性和准确性。哨兵的最重要作用是可以生成分类账，这样其他组件可以确定数据来自同一来源，其中的原因在于哨兵会将来源证明添加到一个加密证明中继链。鉴于XYO网络是一个去信任的系统，哨兵节点必须获得相应的奖励，以便提供可靠真实的位置信息。这可以通过将声誉组件与支付组件组合在一起而完成。当哨兵提供的信息用于回答查询时，哨兵将获得XYO网络令牌（XYO）奖励。为了增加获得奖励的可能性，哨兵必须创建与其他同类节点一致的分类帐，并提供来源证明来证明自己是位置信息来源的身份。

3.2.2 桥接节点

桥接节点是位置数据传输器。它们可以安全地将位置数据分类账从哨兵节点传输至预言节点。桥接节点的第一大重要作用是帮助预言节点确定从桥接节点接收到的启发式分类账没有经过任何更改。桥接节点的第二个重要作用是增添了一个额外的来源证明。鉴于XYO网络是一个去信任的系统，桥接节点必须获得相应的奖励，以便忠实可靠地提供启发式信息。这可以通过将声誉组件与支付组件组合在一起而实现。当桥接节点提供的信息用于回答查询时，便会获得XYO网络令牌（XYO）奖励。为了增加获得奖励的可能性，桥接节点必须创建与其他同类节点一致的分类帐，并提供来源证明来证明自己忠实地传输了启发式信息。

3.2.3 归档节点

归档节点负责存储以去中心化的方式从桥接节点接收到的数据，以便存储所有历史分类账。即使一些数据丢失或暂时不可用，系统仍然可以正常工作，只是准确性会降低。归档节点还会对分类账编写索引，以便在需要时能够返回一串分类帐数据。归档节点只存储原始数据，并针对数据检索及其后续使用而收取XYO令牌，数据存储始终免费。

归档节点彼此连接形成网络，当人们向一个归档节点提问问题时，该归档节点会向其他归档节点索要自己没有的数据。归档节点可以有选择性地存储返回给它的任何分类账信息。这很可能会导致两种类型的归档节点：处于“云端”数据生产边缘的节点和处于“云端”数据使用边缘的节点。处于中间位置的归档节点属于混合类型。数据存储选择不是强制性操作，但可以通过IPFS或其他去中心化的存储解决方案轻松完成。每次将数据从一个归档节点转移到另一个归档节点时，都会追加来源证明以跟踪付款，由此所有归档节点都

可以获得付款。对于检索，可以设置最低来源证明级别来提高有效性。哨兵、桥梁和归档三类节点的利益必须保持协调，以防止数据膨胀。

3.2.4 预言节点

预言节点是XYO网络中最复杂的部分。整体而言，预言节点的职责是从XYO网络获取最准确数据来响应查询，并将数据转发给查询的发布者。预言节点会轮询适用的区块链平台（即Ethereum、Stellar、Cardano、IOTA等）以回答发布至XYO智能合约的查询。然后，它们通过直接与归档节点网络交互，提取准确性/置信性分数最高的回答，从而针对查询做出回复。在这个过程中，它们会将证据与最佳来源证明链进行对比。在最短时间内获得分数最高的答案的预言节点将能够通过工作量证明（Proof of Work）在主XYO区块链（XYOMainChain）上创建区块。查询按照奖励规模和复杂性排列优先级，所以XYO提供的答案越多，查询的优先级就越高。

其他预言节点就区块的有效性达成共识并对区块进行数字签名。那个在该区块中充当在线钱包（coinbase）地址的预言节点将向智能合约发送一个包含答案以及其准确性分数的交易。它还发送其他预言节点的签名的列表，以防止攻击者发布虚假信息，通过冒充预言节点来进入区块链。然后，智能合约可以通过检查有效载荷的签名列表来验证此信息的真实完整性。

3.3 端到端功能

我们在上边章节已经详细介绍了每个节点的职责，接下来将通过端到端的功能来介绍整个系统的工作原理：

1. 哨兵节点收集数据

- 哨兵节点收集真实世界物体位置启发式数据，并准备来源证明，以供之后的节点使用。

2. 桥接节点从哨兵节点收集数据

- 桥接节点从在线哨兵节点收集必要的数据，并在其链条上附加来源证明，然后，将数据和证明传输给网络中的归档节点。

3. 归档节点对来自桥接节点的数据编写索引/进行汇集

- 桥接节点将数据传输给归档节点，然后归档节点以去中心化的方式存储数据以及启发式位置索引。

4. 预言节点提取用户查询

- 预言节点执行轮询以回答发送至以太坊智能合约的查询，然后开始执行答案制定流程。

5. 预言节点从归档节点收集数据

- 预言节点通过从归档节点网络提取适当的所需信息，然后针对查询做出回答。

6. 预言节点制定答案

- 预言节点针对查询从归档节点网络中选择来源链分数最高的回答。

7. 预言节点构建区块

- 预言节点在XYOMainChain上构建区块，其中包含答案内容、查询以及根据工作量证明支付的XYO令牌（XYO）。网络上的其他预言节点也会在该区块上的内容进行数字签名，然后在就有效区块达成共识后，在线钱包预言节点的账户明细会发生更新，以展示系统中工作量证明。

8. 预言节点将结果返回至查询发起者

- 预言节点会对答案、来源链分数以及一系列数字签名执行打包处理，然后将其发送至与XYO智能合约安全连接的适配器组件。适配器负责确保预言节点的真实完整性没有发生损坏，并将一组经过数字签名的答案发送至智能合约。这一切都发生于区块链构建流程完成之后。之后，在线钱包预言节点会根据工作量获得报酬。

9. XYO网络组件按照工作量获得奖励

- 来源证明链上的组件会根据其在查询答案提取过程中所做的贡献而获得奖励。哨兵节点、桥接节点、归档节点和预言节点都会因其工作量而获得相应的奖励。

在同一查询被多次询问的情况下，可能会产生不止一个答案，因为在给定时刻产生的答案是基于当时系统可提供的可用启发式信息得出的。将答案提交至区块链需要两个步骤。首先，必须进行分析以确定查询的最佳答案。如果系统生成多个答案，则节点将比较答案并始终选择更好的答案。举一个简单的查询示例：“在过去的某个特定时间，网络中的一个节点位于何处？”。

3.4 区块链即单一事实来源

从本质上讲，预言节点负责将相关数据转换为绝对数据。它们能够探索整个归档节点网络，以便在XYO网络上查询绝对答案。预言节点还负责构建区块并将区块添加到XYOMainChain上，并根据其工作量证明而获得奖励。由于归档节点网络存储的是未经处理的数据，而区块链存储的是经过处理的绝对数据，因此网络最终可以使用XYOMainChain上的最新信息来回答未来的查询，而不是依靠归档节点网络进行昂贵的计算。

由于XYOMainChain上的区块存储有用于回答查询的组件的来源证明链和图表，未来的预言节点可以探索这些绝对数据，从而以较低的带宽使用量获得准确的结果。因此，XYOMainChain将逐渐成为系统最重要的事实来源。不过，仍然需要归档节点网络，才能确保始终获取到由哨兵节点收集的最新的位置相关启发式信息。

3.5 XYO网络的最佳候选答案选择框架

我们将最佳答案定义为候选答案列表中的单一答案，该答案拥有最高有效性分数，并拥有高于最低准确性要求的准确性分数。有效性分数基于来源链分数。系统了解最高记录来源分数是多少，这个分数就是100％，直到出现更高的分数，然后更高的分数会变成新的100％。XYO网络允许使用最佳答案算法来确定最佳答案。这就为未来替代算法研究提供了扩展空间。

当数据由于被认为质量欠佳或不正确而被排除在答案之外时，它将会被分发给归档节点，然后归档节点会将这些数据从去中心化的存储器中清除出去。

3.6 与公共区块链的初步集成

XYO网络是一种虚拟网络，可以与任何支持智能合约的公共区块链（例如以太坊、Bitcoin+SK、EOS、NEO、Stellar、Cardano等）进行交互。举例而言，要与XYO网络进行互动，以太坊的用户可以向我们的XYO智能合约发布查询，并支付 XYO令牌（ERC20）。我们的XYO区块链中的预言节点将不断针对这些查询轮询以太坊，并以我们自己的XYO区块链货币（也称为XYO令牌）获得奖励。未来，我们将从ERC20令牌的持有者与

我们自己的区块链货币之间进行一对一转换，以便我们的平台能够获取交易费用，支持可扩展物联网用例所需的小额支付需求。在这些情况下，我们将允许用户直接向我们的区块链发出查询，而不是通过公共智能合约进行交互。

---

4 来源证明

借助由不受信任的节点组成的物理网络，就可以确定由边缘节点提供的数据的确定性，具体来说，就是根据基于零知识证明，验证两条或多条数据源自同一来源。使用这些数据集，结合大量类似的数据集和至少一个节点的绝对位置信息，就可以确定另一个节点的绝对位置。

4.1 来源证明简介

传统的去信任系统依赖于私钥来签署系统中的交易或合同。这种机制与以下假设非常匹配：网络上对讨论中的数据进行签名的节点从物理和虚拟角度而言都是安全的。但是，如果私钥遭到泄露，那么来源证明能力就会下降。

将去信任概念应用于物联网时，必须假定网络上的边缘节点并非在物理上或虚拟上都安全的。这就需要在不使用唯一ID的情况下验证边缘节点，同时不需要从网络外部获取任何知识的情况下，判断这些节点所产生的数据是真实有效的。

4.2 来源证明的核心：绑定见证

来源证明依赖于绑定见证概念。鉴于利用不可信的数据源来解析数字合同（预言机）无法产生理想效果，我们可以通过首先确定存在双向位置证明来大幅提高数据的确定性。主要的双向位置启发式算法是邻近原则，因为双方都可以共同签署交互来验证交互的发生和范围。这就产生了零知识验证方法来证明两个节点彼此邻近。

然后，我们需要判定去信任系统中的预言见证节点所收集的共享数据的确定性。在一个去信任的系统中，见证人节点可能会（由于缺陷或损坏）而产生错误数据。如果无效数据超出启发式算法允许的范围，那便会被轻易检测出来并删除。有效但不正确的数据（即错误数据）的检测难度更大。

4.3 单向与双向位置启发式数据

与物理世界相关的大多数数据（启发式）都是单向的。这意味着被测元素无法实现回溯，导致单向启发式数据非常难以验证。双向启发式方法是指被测元素可以将自己的测量结果报告给另一方，这使得验证成为可能。位置数据是一种罕见的启发式数据，因为它可以是双向的，由两个边缘节点相互报告。**举例来说，在现实世界中，两个彼此靠近的人自拍了一张照片，制作了两个照片副本，并各自都在照片上签了名。这个过程会给双方提供邻近证明（Proof of Proximity）。这两个人获得这些"数据"的唯一方法就是他们同处一个地方**。

接下来，我们探讨一下网络效应：设想在一个系统里，每个边缘节点在四处移动时都会不断产生这些"自拍"，并将它们存储在活页夹中。它们还能按时间顺序保留活页夹，并且绝不允许删除活页夹。这为每个边缘节点建立一个邻近记录器，可以与其他边缘节点的记录器交叉参考。

4.4 非边缘节点

所有节点都被认为是"证人"，包括桥接节点、中继节点、存储节点和分析节点。这允许任何数据从一个节点传输到下一个即将被绑定的节点。这是绑定见证概念。

4.5 交叉参考

分析由每个边缘节点产生并链接在一起的每组"自拍"，允许系统根据网络中所有节点的相对邻近度产生最佳答案。如果每个节点都真实而准确地报告数据，则边缘节点的所有相对位置映射将可能达到最高的确定性和准确性：100％。相反，如果每个节点都不真实或有缺陷，则确定性和准确性都可能会接近最小值0％。

给定一组报告的数据和一个针对边缘节点相对位置的查询，可以确定该位置的近似值以及确定性和准确性系数。

给定一组相同的数据和相同的分析算法，每个计算应该得到相同的位置近似值以及确定性和准确性系数。

4.6 图解

S'和S"（图2）都是收集启发式数据的哨兵（边缘节点）。当彼此接触时，它们会交换启发式数据和公钥。两者都构建了交互的完整记录并签署了最终交互。这条签名记录将

成为各自局部分类账中的下一个条目（S’为第16条，S”为第3条）。这一行动将这两个见证人绑定在一起，使他们彼此邻近。

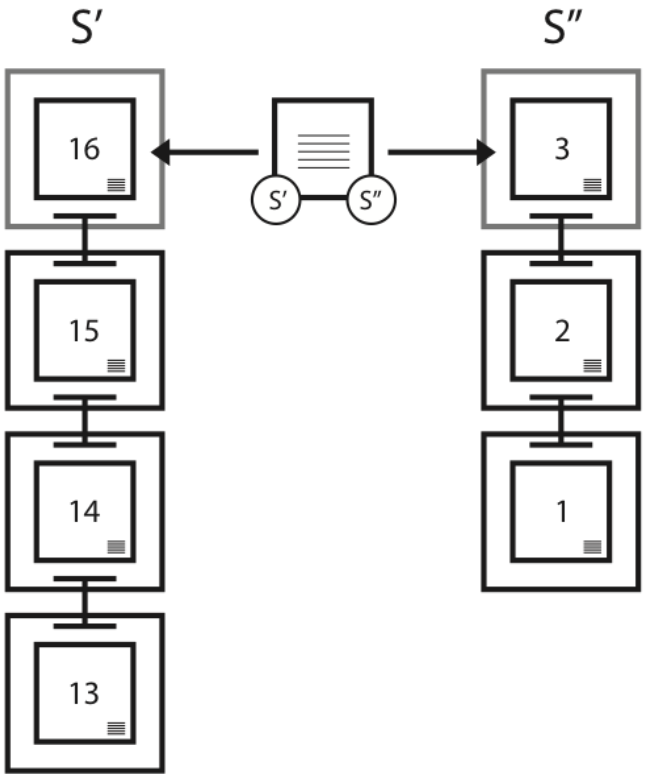

图2. 两个哨兵节点之间的绑定见证示例

4.7 来源链

每个来源都有自己的分类账，并对其签名以制作来源证明链。一旦来源证明上的信息被分享出去，它实际上就会成为一条永久性的信息。这是因为在共享结束之后发生的分叉会终止该链条，并将来自该见证人的所有未来数据视为来自新见证人。为了在来源证明链中生成一个链接，来源会生成公钥/私钥对。然后，在前一个和后一个区块中填入公钥之后，它会在两个区块上签字。在签名结束后，私钥会立即被删除。随着私钥的立即删除，密钥被盗或重复使用的风险大大降低。

在验证流入XYO网络的分类账是否有效方面，来源证明链具有关键作用。数据源没有唯一ID，因为它可以被篡改。私钥签名根本无法实现，原因在于XYO网络的大部分难以或不可能在物理角度实现绝对安全，所以动机不良的分子可以轻易窃取到私钥。为解决

这个难题，XYO网络采用了瞬态密钥链，这样一来，数据来源链条便无法被篡改。然而，一旦链条被打破，它就会永远被打破，无法继续，成为一个孤岛。

启发式分类帐每次在XYO网络中传递时，接收方都会附加他们自己的来源证明，这样来源证明链就会变得越来越长，并生成一个来源证明交点（Proof of Origin Intersection）。来源证明链和来源证明交点是预言节点用于验证分类帐有效性的主要指标。分类账信誉度（Ledger Reputation）实际上是XYO网络在制作与其相关的来源证明球（Proof of Origin Ball）方面的参与度百分比。理论上，如果100％的XYO网络记录都与来源证明相关联，并且经过全面分析，则其有效性就是100％。如果0％的XYO网络记录可用于分析，则有效性降至0％。

为了提升安全性，在第二个条目生成之前，都不会公开链条链接的公钥。这也就在条目之间留出了时间间隔，或者说允许其他数据存储在前一个或下一个链接中。

4.8 来源链分数

来源链分数计算方法如下（默认算法）：

- PcL = 来源证明链长度
- PcL = 来源证明链难度
- Pc’ Pc” O = Pc’和Pc”之间的来源证明链重叠率

$$Score = \prod_{i=0}^{i=n} \frac{PcL * PcD}{Pc' Pc'' O}$$

4.9 来源链分数

来源树（Origin Tree）用于计算答案的有效性近似值。它使用收集的数据生成理想树（Ideal Tree），该树体现了最适合于给定断言答案的数据。如果节点N位于坐标为X、Y、Z、T的位置，则集合中所有数据的误差必须保持为一个特定的值。为了计算这个误差，我们将计算最小值、最大值、平均值、中值以及与平均值的平均偏差值。

给定一组所有分数（s）的 S、来源证明链难度 PcD 和误差因数error，则最佳答案计算如下：

$$BestAnswerScore = \max_{\forall s \in S_j} [PcD * (1 - error)]$$

换句话说，具有最高最佳答案分数的断言答案是最佳答案。使用来源证明树，我们可以识别和修剪不可能的分支（异常值）。

4.10 瞬时密钥链

通过使用临时私钥来签署两个连续的数据包，可以将一系列数据包链接在一起。当数据包中包含与私钥配对的公钥时，接收者可以验证这两个数据包经由相同的私钥签名。在不破坏签名的情况下，数据包中的数据不能被更改，从而确保经签名的数据包不会被第三方（例如桥接节点或存储节点）更改。

4.11 链接深度

节点至少会为来源证明链中的每个链接生成一个链接深度为1的新公钥/私钥对。对于给定的分类帐条目，链接表中可能有N个条目，每个条目会指定将来添加链接第二部分时的时间间隔。任何两个链接都不会拥有相同的数量级（基础比例为2）。例如，条目[1,3,7,12,39]符合规定，但[1,3,7,12,15]就不符合规定。

在上一个区块被发布时，就创建、使用和删除深度为1的链接。但是，深度大于1的链接会在前一个区块被签名时生成它们的对，并且第二个签名不会在N个块之后发生，之后私钥将会被删除。由于这个原因，人们认为，深度大于1的链接不如深度为1的链接安全，但是它们可以用于提高性能和减少数据丢失情况。

4.12 固定顺序

确定分类账顺序的关键因素是分类账的报告顺序。鉴于设备无法更改任何来源证明签署分类账的顺序，可以通过集中查看所有分类账来建立绝对顺序。

4.13 倒数第二发布

构建来源证明的主要方法是基于以下事实：哨兵节点始终报告其倒数第二个块，而不报告最后一个块。这允许最后一个块将指向前一个块的签名链接作为链接的证据。

4.14 空链接

为了提高来源证明链的安全性，链条更新间隔不得小于十秒，且不得超过六十分钟。如果没有新数据可用，则向链条中添加一个空块。

4.15 图解

随着时间的流逝，正在构建的来源证明链会变得越来越长，如图3中从左到右的发展趋势所示。在任何给定时间，链条的生成者只会向调用者提供以黑色边框标识的条目，等待条目的第二次签名结束之后再予以提供。例如，在第3列中，只有条目2和1将作为链条的一部分返回。

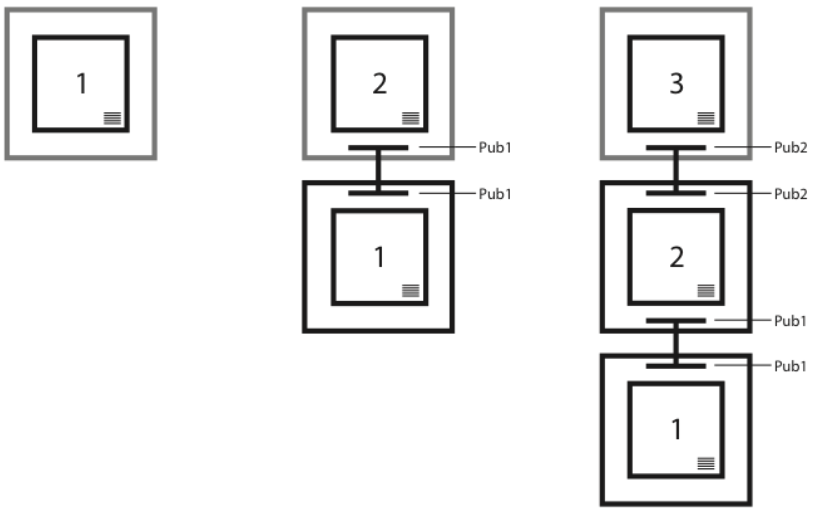

图3. 来源证明链中的链接内容示例

4.16 总结

如果一系列数据包使用临时私钥按顺序对进行了签名，并且包含配对的公钥，那么可以绝对确定数据包来自同一个来源。

---

5 安全注意事项

5.1 虚假预言节点攻击

一组数字签名被发送到了XYO智能合约，因为合约需要验证发送答案的预言节点的真实完整性。然后，合约可以在一个高置信度区间内验证签署此签名列表的其他预言节点。如果没有识别到其他节点，中继预言节点将会成为系统内单一的故障和风险来源。

5.2 哨兵节点DDoS攻击

需要考虑的另一个攻击是发生在特定区域中哨兵节点之间的分布式拒绝服务（DDoS）攻击。攻击者可能试图建立大量指向哨兵节点的连接，以阻止这些节点向桥接节点传输正确信息或任何信息。我们可以通过要求任何试图连接到哨兵节点的人员回答一个小型加密拼图来规避这个问题。由于查询不会涉及大量指向Sentinels的连接，因此这不会对XYO中继系统造成严重影响，并且攻击者需要花费大量资源才能对我们网络执行一次DDoS攻击。由于来源证明存储在XYOMainChain上，因此任何人在任何时间都可以验证这些证明。这可以确保在链条中的单个实体受到感染时，查询答案的准确性（来源链接分数）将降至为0。

---

6 XYO令牌经济

在去中心化应用程序的权力和基础架构需求方面，预言机占有很大比重，主要围绕权威性预言机的连接和聚合方面。我们认为，去中心化应用程序需要一个完全去中心化且去信任的预言机系统，才能发挥最大潜力。

6.1 XYO网络加密经济效益

我们使用XYO令牌来激励提供准确可靠的启发式位置数据的理想行为。为了验证指定对象的XY坐标，XYO令牌可以被认为是与真实世界进行交互所需的“媒介”。

整个过程如下：令牌持有者向XYO网络发布了一个查询（例如，“我有一个电子商务包裹，XYO地址为0x123456789，请问目前这个包裹位于哪里？”）。然后，查询被发送到一个队列中，等待系统处理和回答。用户可以在创建查询时设置他们所需的置信度和XYO媒介价格。查询的成本（以XYO令牌计算）由提供查询答案以及市场动态所需的数据量决定。所需数据越多，查询费用越高，并且XYO媒介价格也越高。对XYO网络的查询有可能规模非常大且费用十分昂贵。例如，一家货运和物流公司可以询问XYO网络，“我们车队中每辆车位于什么位置？”

一旦XYO令牌持有者向XYO网络发起了查询并支付所需的媒介费用，所有参与这项任务的预言节点都会调用相关的归档节点，以检索回答查询所需的相关数据。返回的数据来自桥接节点，而桥接节点最初是从哨兵节点收集了这些数据。哨兵节点本质上是验证物体位置的装置或信号，比如蓝牙追踪器、GPS追踪器，内置于物联网设备中的地理位置追踪器、卫星追踪技术、二维码扫描器、RFID扫描器等实体。XY Findables率先推出了消费类蓝牙和GPS业务产品，能够测试和处理真实世界的启发式位置数据。在XY Findables消费类业务产品方面的所有努力都极大地推动了XYO网络区块链协议设计进程。

如果在回答查询的过程中使用了哨兵设备（例如蓝牙信标）提供的数据，则参与交易的所有四个组件都会收到令牌持有者支付的XYO媒介费用的一部分，这四个组件分别为：预言节点（搜索答案）、归档节点（存储数据）、桥接节点（传输数据）和哨兵节点（记录位置数据）。在XYO网络的四个组件，有三个部件会获得相同比例的奖励，剩余的一个组件，也就是预言节点，与之不同，因为它们在提供答案的过程中参与范围更为广泛。在每个组件内部，所获得的奖励都平均分配。

6.2 独立性优势

位置数据采集设备是网络的原子块，单个设备可以充当系统四个组件中的一个或多个。但是，设备充当两个以上组件角色的情况十分少见，尤其是在大型的XYO网络中。此外，具有更多独立来源证明的区块链分类帐将受到人们越来越多的关注，因此对于充当多个组件的设备来说，存在一种加密经济损失。

6.3 恒稳真实完整性优势

XYO网络中的哨兵节点被分配一个恒稳性系数，用于衡量哨兵节点在整个生命周期中的移动距离。哨兵节点在一段时间内移动距离越短，所提供数据的可信度越高。当考虑使用哪些哨兵节点来处理查询时，归档节点会跟踪和分析哨兵节点的恒稳性系数。

6.4 激励令牌使用行为

如果一个系统不鼓励令牌持有使用令牌进行交易，长此以往，则会面临基础的经济问题。因为这种系统无法提升令牌使用率和流动性，而是会带来一个价值储备非常稀缺的生态系统，并导致系统用户形成不爱使用令牌的习惯。

大多数加密经济激励措施所存在通病是，过于关注令牌挖掘者（例如哨兵、桥接、归档和预言节点），而忽略了令牌用户。XYO令牌充分考虑了这两个问题。

根据XYO令牌模型激励机制，如果挖掘者提供了准确的数据，或者了解何时不能提供数据，那么这类挖掘者便会获得奖励。当与网络流动性较高时相比，网络流动性较低时，系统会鼓励最终用户执行更多交易并为其提供奖励。因此，XYO令牌的生态系统能够保持良好的平衡性、流畅性和稳健性。

6.5 XYO令牌规格

通用令牌销售采用分层定价结构，起始价格为1 ETH：100,000 XYO，最高价格为1 ETH：33,333 XYO。有关基于发行数量和时间的定价结构的详细信息将稍后公布。

- 智能合约平台：以太坊
- 合约类型：ERC-20
- 令牌：XYO
- 令牌名称：XYO网络公用令牌

- 令牌地址：0x55296f69f40ea6d20e478533c15a6b08b654e758
- 总发行量：限定在令牌正式销售活动结束后达到的最高数量
- 预计 XYO 币上限：4800万美元
- 未售出和未分配的令牌：令牌销售活动结束后予以烧毁。正式销售阶段结束后不再生成XYO令牌。

---

7 XYO网络用例

XYO网络的应用范围十分广泛，覆盖多个行业。以一家电子商务公司为例，该公司可以为其高级客户提供货到付款服务。为了能够提供这项服务，电子商务公司将利用XYO网络（使用XYO令牌）（在以太坊平台上）编写智能合约。然后，XYO网络可以在每一个履行步骤中跟踪发送给消费者的包裹的位置，覆盖从仓库货架到运输快递，再到消费者住宅期间经历的每个位置。这可以使电子商务零售商和网站以去信任的方式验证包装不仅出现在顾客的家门口，而且还安全地放在家中。一旦包裹到达客户家中（通过特定的XY坐标定义和验证），货物运输即视为已完成，并向供应商付款。XYO网络在电子商务领域的应用能够保护商家免受欺诈，并确保消费者只需支付到达家中的商品。

另外，XYO网络正在与一家酒店评论网站进行合作，该网站面临的问题是人们常常不相信网站上的评论。自然，酒店业主会不惜一切代价改善网站评论的可信度。如果有人能非常肯定地说，有人从圣地亚哥飞往巴厘岛的一家旅馆并在那里住了两周，然后返回了圣地亚哥，在此之后写了一篇关于酒店住宿体验的评论，那会怎样？这篇评论肯定会广受人们的欢迎和信任，如果评论的作者是一位发表过多篇文章的撰稿人，并且其位置数据经过了验证，那么可信度更会大大提高。

---

8 XYO网络扩展

我们很幸运能够成功利用涵盖全球超过100万个蓝牙和GPS设备的真实世界网络，建立起一个高效的消费者业务渠道。大多数位置网络没能走到这个阶段，也没有获取建立广

泛网络所需的大量关键资源。我们创建的哨兵网络只是一个起点。XYO网络是一个开放的系统，任何定位设备运营商都可以参与并开始赚取XYO令牌。

一般来说，XYO网络中的哨兵基数越大，就越可靠。为了进一步扩大网络规模，XYO网络正在与其他企业合作，将其哨兵网络扩展到自己的XY Findables信标网络之外，以期实现更大的发展。

---

9 鸣谢

这份白皮书是一个团队努力的硕果，正是由于以下人士对我们企业愿景的信任与支持，才使这份出版物得以与读者见面：Raul Jordan（哈佛学院，泰尔学员，XYO网络顾问），感谢他帮助我们润色语言，帮助我们将技术类信息清楚明了地传达给全世界。我们感谢Christine Sako秉承职业道德，对我们的工作给予详细认真的评价，同时帮助我们调整文章结构，如实地反映最佳实践的详细信息。我们感谢Johnny Kolasinski在适用用例研究和汇编方面的贡献。最后，我们感谢John Arana对我们的文章做出仔细检查并提出了建设性建议。

参考文献

[1] 康卡斯特。《调查：近三分之一的美国人遇到过包裹在家门口被人偷走的情况》。美国商业资讯，宾夕法尼亚州费城，2017年12月14日。

[2] Blanchard, Walter。《双曲线机载无线电导航设备》。Journal of Navigation期刊，第44（3）期，1991年9月。

[3] Karapetsas, Lefteris。Sikorka.io。http://sikorka.io/files/devcon2.pdf。上海，2016年9月29日。

[4] Di Ferrante, Matt。《位置证明》。https://www.reddit.com/r/ethereum/comments/539o9c/proof of location/。2016年9月17日。

[5] Goward, Dana。《RNT基金会前往国会作证》。美国众议院听证会："引领前行：美国导航设备的未来"，华盛顿哥伦比亚特区，2014年2月4日。

[6] Freeman, Scott。《菲亚特货币充当交换媒介》。国际经济评论，第30（1）期，新泽西州霍博肯，1989年2月。

词汇表

准确性

一种置信度衡量标准，用于判定数据点或启发式数据是否处于特定误差范围之内。

归档节点

归档节点会将启发式数据作为去中心化数据集进行存储，以便存储所有历史分类帐，但并不需要存储所有分类账。即使一些数据丢失或暂时不可用，系统仍然可以正常工作，只是准确性会降低。归档节点还会对分类账编写索引，以便在需要时能够返回一串分类帐数据。归档节点仅存储原始数据，并仅针对数据检索收取费用，而数据存储始终免费。

最佳答案

我们将最佳答案定义为候选答案列表中的单一答案，该答案拥有最高有效性分数，并拥有高于最低准确性要求的准确性分数。

最佳答案算法

一种用于在预言节点选择答案时生成最佳答案分数的算法。XYO网络允许添加专门的算法，并允许客户指定使用哪种算法。当给定相同数据集时，该算法在任何预言节点上运行时都会得出相同的分数。

绑定见证

绑定见证是一种通过确定存在双向启发式位置数据而实现的概念。鉴于利用不可信的数据源来解析数字合同（预言机）无法产生理想效果，通过这种启发式方法可以大大提升数据确定性。主要的双向位置启发式方法是邻近原则，因为双方都可以共同签署交互来验证交互的发生和范围。这就产生了零知识验证方法来证明两个节点彼此邻近。

桥接节点

桥接节点是一种启发式转录器。它可以安全地将启发式分类账从哨兵节点传递给预言节点。桥接节点的第一大重要作用是帮助预言节点确定从桥接节点接收到的启发式分类账没有经过任何更改。桥接节点的第二个重要作用是增添了一个额外的来源证明。

确定性

一种置信度衡量标准，用于判定数据点或启发式数据是否发生了损坏或篡改。

加密定位

加密定位技术的领域。

加密经济学

一门独立学科，研究管理去中心化的数字经济中产品和服务的生产、分配和消费的协议。加密经济学是一门专注于研究这些协议的设计和特征的实用科学。

预言节点

预言节点可以通过分析由XYO网络存储的历史数据，回答给定问题。存储在XYO网络中的启发式数据必须具有较高水平的来源证明，以确定启发式数据的有效性和准确性。预言节点通过根据来源证明来判断证据的真伪，获得并提供答案。鉴于XYO网络是一个去信任的系统，预言节点必须获得相应的奖励，以便提供可靠真实的启发式数据分析结果。与哨兵节点和桥接节点不同，预言节点使用工作量证明来将答案添加到区块链中。

启发式数据

一个关于现实世界相对于哨兵位置（邻近情况、温度、光线、运动等等）的数据点。

预言机

作为DApp（去中心化应用）系统的一部分，预言机负责通过提供准确且确定的答案来解析数字合同。术语“预言机”源于密码学，表示一个真正的随机源（例如一个随机数）。这提供了从密码方程通向世界的必要之门。预言机可从区块链以外（真实世界或离链环境）提取智能合约信息。预言机是从数字世界进入现实世界的接口。举一个令人毛骨悚然的例子，假设有一份针对临终遗嘱的合约。遗嘱的条款会在确认遗嘱人已故的情况下执行。通过汇编和汇总来自官方来源的相关数据，可以构建一个预言机服务来触发遗嘱。然后，预言机可以用作智能合同能够调用的信息源或端点，以便检查遗嘱人是否已故。

来源链分数

分配给来源链的分数以确定其置信度。这项评估考虑了长度、混乱、重叠和冗余因素。

来源树

一个从各种来源链中获取的分类账条目数据集，用于确定启发式分类帐条目的来源具有特定水平的确定性。

来源证明

在验证流入XYO网络的分类账是否有效方面，来源证明具有关键作用。数据源没有唯一ID，因为它可以被篡改。私钥签名根本无法实现，原因在于XYO网络的大部分难以或不可能在物理角度实现绝对安全，所以动机不良的分子可以轻易窃取到私钥。为解决这个难题，XYO网络采用了瞬态密钥链，这样一来，数据来源链条便无法被篡改。然而，一旦链条被打破，它就会永远被打破，无法继续，成为一个孤岛。

来源证明链

将一系列绑定见证启发式分类帐条目连接在一起的瞬时密钥链。

工作量证明

工作量证明是一条满足特定要求的数据，很难生成（即昂贵、耗时），但易于其他人进行验证。工作量证明生成流程可以是发生概率较低的随机过程，因此在创建有效的工作证明前，需要进行严格的试验和错误检查。

哨兵节点

哨兵节点是一种启发式见证人。它负责观测启发式数据，通过生成带有时间戳的分类帐来确保启发式数据的确定性和准确性。哨兵的最重要的作用是可以生成分类账，这样通过向预言器添加来源证明，确保它们来自同一来源。

智能合约 Nick Szabo

在比特币出现之前发明的一种协议，据称是在1994年（这就是为什么有些人认为他是比特币背后的神秘发明者Satoshi Nakamoto）。智能合约背后的原理是将法律协议写入程序，并让分散式计算机执行其条款，而不用人类解释并执行合同。智能合约将资金（例如Ether）和合约合二为一。由于智能合约具有确定性特征（如计算机程序），并且完全透明且可读，成为了取代中介机构和经纪公司的有效方式。

瞬时密钥链

瞬时密钥链使用瞬时密钥加密技术连接一系列数据包。

去信任

一种系统特征，在这种环境中，所有各方可以就标准事实达成共识。权力和信任分布于网络中的利益相关者（例如开发方、挖掘方和消费者）之间（或由其共享），而不是集中于单个个人或实体（例如银行、政府和金融机构）手中。这是一个很容易被误解的术

语。区块链实际上并没有消除信任，而是尽可能减少系统中任何单个参与者所需的信任量。具体来说，就是经济游戏在系统中的不同参与者之间分配信任来实现这一点，该经济游戏会激励参与者按照协议所定义的规则进行合作。

XY预言机网络

XYO网络。

XYO网络

XYO网络代表“XY预言机网络”。它由包含哨兵节点、桥接节点、归档节点和预言节点的整个XYO组件/节点系统组成。XYO网络的主要功能是作为一个门户网站，用于通过真实世界的地理位置确认执行数字智能合约。

XYOMainChain

XYO网络中一个不可变的区块链，用于存储查询交易以及从预言节点收集的数据及其相关的来源分数。