XYO网络：
安全风险与管控预防

Arie Trouw*（阿里·特罗），Andrew Rangel（安德鲁·兰格），Jack Cable（杰克·凯布尔）

2018年2月

---

1 简介

XYO网络是一种去信任化、去中心化的加密位置网络，该网络应用零知识证明以保证位置验证的准确性。与其他去信任化、去中心化的的实体一样，XYO网络最致命的缺陷便是其系统的安全程度，这些缺陷包括设计缺陷、结构缺陷、错误代码、经济动机错误、社交工程等等。本文件主要适用于设计缺陷、结构缺陷和经济动机问题。

---

2 技术考虑

2.1 总结

本文件强调了有关XYO网络潜在安全风险的高级概念。由于去信任化系统的应用，该网络中涉及到的所有部分都可以被认定为缺陷所在（例如哨兵节点、桥接节点等）。本章节列举了一些已知的协议级攻击，并给出了相对应的行业标准保护措施，而在其他攻击中，系统内所使用的设备则极易受到攻击。

---

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

2.2 蓝牙

大多数蓝牙设备都是通过“长期密钥”建立PIN（个人识别码），从而进行加密保护。一旦密钥在配对过程中被人窃取，之后的所有传输内容便会轻易被人破解，而且，如今市面上还存有许多帮助人们破解个人识别码的工具，甚至一些设计周密、在协议外部设置密码的程序也会被此破译，从而失去保护，这也使得一些恶意攻击有机可乘。不仅如此，由于蓝牙设备极易购买，盗窃者也可以利用这些设备加速其破译过程。

要防止设备受到恶意攻击，第一种方法是借助白名单中的MAC 地址（介质访问控制地址），它能够阻止未授权设备访问哨兵节点和桥接节点，从而将恶意攻击扼杀于萌芽之中。第二种方法则需要用户在配对前“重置”设备，由此规避那些无法直接接触设备的人的窃取行为。

2.3 OTA（无线传输）

哨兵节点拥有无线推送升级信息的能力，而这一能力也使得设备能够快速更新补丁、修补漏洞，从而提高其稳定性和安全性。但是，这一特征也给攻击提供了机会，人们很有可能利用更新附加恶意代码。

2.4 硬件

使用XYO网络的设备遍布全球，这就意味着人们有可能将硬件组装成设备，而这也是XYO网络去信任化的原因之一。该网络的整个系统都依赖于一系列复杂算法，这些算法会细致的检测输入系统的各类数据，一旦有非高分、长链数据出现，其所对应的攻击设备便会受到处罚。

---

3 Poison the Well Attacks（病毒攻击）

3.1 总结

病毒攻击，即通过非正常操作或蓄意攻击，向系统内输入破损数据，从而降低系统输出结果的整体准确性和/或确定性。

3.2 动机

在病毒攻击中，攻击者的目的就是破坏或干扰已经传输至具体哨兵节点或桥接节点的数据，一旦操作完成，攻击者便可以引起短期和长期的经济混乱。XYO网络的去信任化系统对待这种恶意数据实行零容忍政策，绝不允许它们进入网络系统。

虽然攻击行为本身无法给攻击者带来直接利益，但他们却可以通过破解和/或干扰其他人的数据获利。假设警方利用XYO网络定位假释人员，并会在其违反假释条例时获知地理位置。如果他们利用该网络监视有酒驾前科的人在酒吧停留的时间，那么假释人员便可以通过病毒攻击向酒吧的桥接节点输入破损数据，直至网络中断，之后，他们便可以在不违反假释条例的基础上在酒吧一醉方休。即使数据显示他们的地理位置是酒吧，他们也可以篡改数据，保证系统内显示的停留时间不超过限制。

3.3 技术分析

GPS干扰器或非法射频干扰器可以阻碍已授权的无线电通信，从而干扰哨兵节点中的数据。GPS欺骗设备[1]可以向GPS接收器传输错误数据，从而使其获得错误的位置信息。

通过蓝牙通信的哨兵节点则会通过另一种方式受到此类攻击，现实中攻击者也有许多可以欺骗蓝牙设备，并向其传输错误信息[2]的方法。即使人们将XYO网络创建的私人密钥即刻删除，也很有可能会存在第三方设备监视哨兵节点和桥接节点之间的通信，并将其复制保存，之后，攻击者便会仿造哨兵节点向设备传输破损数据，并同时干扰桥接节点向归档节点发送的信息。

3.4 协议风险管控策略

由于GPS干扰器工作时会在其目标所在的普通数据区产生大量数据垃圾，所以人们可以轻易的检测到它的存在。举例来说，当手机用户进入到GPS干扰器的目标区域时，其使用的很多手机应用都会突然失效，而只要时间允许，操作人员便可以找到问题所在，并确定是干扰器所为。FCC（美国联邦通信委员会）已明确规定，使用GPS干扰器属于违法行为[5]，所以这类高风险的攻击方式极易被检测到，现在的发生率也并不高。不过即便如此，人们也在不断开发复杂的GPS反欺骗软硬件科技，以提高设备的安全程度[1]。

除了这些安全措施外，现如今也有一些技术和策略可以帮助人们避免蓝牙欺骗和数据破解，比如安全验证连接。[3]

3.5 XY预言机网络风险管控策略

归档节点网络是一种在预言节点验证后将已验证数据返回发出方的网络。在归档节点接收到数据的同时（具体信息参考黄皮书），归档节点网络便会开始删除破损信息，这些信息会储存在链接中发回来源，并可供人们查询最近添加的破损信息，包括附着于长链接上的欺骗信息。每个归档节点都会对其他节点上的数据进行二次验证，从而保证网络的安全可靠。不过，由于归档节点 、桥接节点和哨兵节点需付费使用，所以固有的加密经济学只会拦截低级干扰因素。

3.6 总结

鉴于归档节点需从广泛的地理区域内获取数据，且攻击设备必须真实位于某地才能干扰该地数据，所以该类攻击的下场往往以失败告终。这也就是攻击XYO网络会使得攻击者经济受损的原因。

---

4 Assassination Attacks（暗杀攻击）

4.1 总结

暗杀攻击，起源自一位恶毒的攻击者，指试图破坏节点（人格诽谤）或使节点失效（技术偷袭）的行为。

4.2 动机

在暗杀攻击中，为了使自己控制的节点的可信性不断上升，攻击者往往会逐渐削弱合法节点的受信任度。而由于哨兵节点的受信任度是整个XYO网络运行的基础，节点的受信任度绝不能被轻易篡改。

试想一下这种情况：攻击者尝试在XYO网络中传播错误的位置信息（具体信息参考Force Field Attack（力场攻击）），在这种情况下，攻击者必须首先确定攻击目标，并逐渐削弱个人节点的受信任度。有一种方法能够完成这项工作，那便是选择性的向合法哨兵

节点提供错误信息（使节点数据显示异常），从而削弱XYO网络中节点的一致性。如此，便会削弱目标哨兵节点的可靠性。

不仅如此，攻击者还可能会使用破坏实体设备等技术偷袭方式。这些攻击方式同样也是为了篡改位置信息并使设备失效。

4.3 技术分析

想要攻击哨兵节点，攻击者必须配备至少一台设备，从而与目标哨兵节点进行选择性通信，而由于网络中的其他设备并不会产生带有恶意节点的数字签名，故这一恶意节点只会在目标节点上显示。

桥接节点位于网络外部，目标节点传送至此处的信息与其他桥接节点接收到的信息不一致，这也就导致了该目标节点可靠性的降低，而与此同时，其他哨兵节点则不会发现恶意节点的存在。

4.4 协议风险管控策略

若想阻止暗杀攻击，最基本的便是在发现节点选择性的参与认证时降低对其的受信任度。在这种情况下，恶意节点会选择性地参与认证，从而保证自己不被其他哨兵节点发现。

根据每个哨兵节点与其他哨兵节点表现的一致性建立受信任度，可以有效打击选择性参与认证的节点。受信任度高的节点可以对受信任度低的节点进行验证，若低受信任度节点是合法节点，它便会积极配合验证，使其全网可见，从而提高自己的受信任度。反之，如果某一结点选择性进行验证，那么受信任度高的节点便会通知全网有恶意节点拒绝验证。如果低受信任度节点进行了全部验证，那么合法节点便可以证明该选择性验证指控不实。

实施这项针对节点选择性验证的操作，等于是在接收信息不一致时，赋予了每个哨兵节点一套防御机制，可以有效阻止XYO网络节点受到恶意破坏。

4.5 XY预言机网络风险管控策略

为每个哨兵节点建立受信任度能够有效打击进行选择性认证的节点，这一操作通过赋予所有哨兵节点以惩处能力，能够缓解攻击者对节点的破坏。虽然物理上的破坏（比如损坏设备）很难在网络层面加以预防，但是XYO网络的弹性很大，仅仅毁坏一台设备并不会影响整个网络的运行。

4.6 总结

信任机制的建立不仅迫使每个哨兵节点必须表现良好，还能够有效的剔除恶意节点。这就是XYO网络对待暗杀攻击的策略。

---

5 Deception Attacks（欺诈攻击）

5.1 总结

欺诈攻击指攻击者尝试终止系统中错误但有效的数据，并从中获取个人利益的行为。

欺诈攻击的其中一种由Multi-Chain Forging（伪造多链）造成，攻击者会创造多个不同链接，使其在多地同时存在。

5.2 动机

攻击者会创建多个假位置链接，由此伪造信息。在创建新区块的过程中，攻击者会通过密钥将其中一条假链接发送给一个或多个位于不同区域的目标设备，之后，他们便可以不断地从同一地址创建新的位置连接了。

攻击者可以在传播错误的位置信息的过程中获利，当然，在这一过程中，位置的准确性是非常重要的。就拿制造不在场证明来说，攻击者需要用地理位置来证明自己在某一时间段内在某地出现过，而拥有多链接便可以让攻击者选择对其最为有利的位置信息进行发送。

5.3 技术分析

随着链接变得越来越长，欺诈攻击也比之前更加难以实行了。随着时间的变化，某一特定节点的信息会通过XYO网络进行传播，这就意味着在过去的任何时间点都有可能会有人对链接进行更改，从而使系统受到攻击。

虽然这一过程并不会降低攻击的可能性，但是在通过桥接节点时，恶意哨兵节点需与其分享其中一条假链接，而由于连接均为有效连接，桥接节点及其上级设备并不能马上

判定链接作假。反而，哨兵节点需将其通信记录与其他节点的记录做比对，二次验证该节点是否同时在不同地方出现过。

5.4 协议风险管控策略

本质上说，因为任何伪造的长链接都会与网络中的标准链接不符，XYO网络是可以检测到多链攻击的。由于位置数据的及其重要性，为了防止链接中存在微小改动，用户可能需要等待归档节点的再次确认，比如验证分布式节点的签名等。随着时间的增加，任何假链接都会浮出水面。

5.5 XY预言机网络风险规避策略

数据分散在归档节点各处，而归档节点中包含了已验证的哨兵节点通信单。在实际操作中，即使链接（虽仍然有效）中只发生了一点点改变，XYO网络也是可以检测到的。如果某一哨兵节点想要发动多链攻击，其他受过攻击的节点便会将攻击信息传送全网，最终，该哨兵节点的受信任度便会降到最低，其包含的所有链接也会被一并删除。

因此，XYO网络可以对通信内容进行二次验证，从而阻止网络受到该类攻击。

5.6 总结

XYO网络中的大量数据不仅可以阻止攻击者通过降低恶意哨兵节点的受信任度传播错误数据的行为，还会将该恶意节点从网络中删除。

---

6 Same-Machine Sybil Attack（同一设备女巫攻击）

6.1 总结

同一设备女巫攻击，指恶意攻击方使用同一设备创建多个节点的攻击行为。XYO网络内的设备并没有各自单独的身份认证，这就使得攻击者能够轻易获得该项身份认证。之后，通过验证模拟节点中的数据包，攻击者便能增强其节点的受信任度，从而使得这些节

点代替合法节点工作。代替合法节点后，攻击者便会让这些节点与其附近不同的节点进行通信，从而将不同信息收集在初始验证链接中。这一操作的最终结果会导致所有模拟节点获取到丰富的初始链接评分，这也就使得攻击者可以廉价、大量的创建节点，对某一区域甚至全球的网络进行女巫攻击。

6.2 动机

攻击者可能会利用同一设备女巫攻击扩大其在某一特定区域的影响力。通过使用同一设备，攻击者会创建出多个假节点，从而降低网络对女巫攻击的拦截力度。相比于创建多个攻击设备，使用同一设备创建多个假节点则会容易很多。

6.3 技术分析

想要骗过蓝牙设备，使其不能辨别信息真假其实并不难[4]。攻击者可以利用一个计算机创建多个节点，并让每个节点在外人看来是在不同地点进行运作。

一旦创建出大量的虚拟哨兵节点，攻击者便可以操作这些哨兵节点，并使其对外表现出多个不同实体节点的特征。这些哨兵节点表现统一，会验证其临近哨兵节点的相关信息。不仅如此，攻击者还会创建一幅虚拟地图，使其在虚拟哨兵节点验证时显示出来。

6.4 协议风险管控策略

由于同一电脑运行的虚拟哨兵节点会表现出相同的RSSI（接收信号强度），所以对抗同一设备女巫攻击的关键就在于分析讯号强度，判断重复数据。经过检测，外部哨兵节点会发现，源自同一电脑的虚拟哨兵节点的表现会极为相似（即讯号强度相同）。若要阻止此类攻击，合法哨兵节点必须能够检测出捆绑设备，并将其发出的信息作为单一节点对待。

6.5 XY预言机网络风险规避策略

XYO网络检测同一设备女巫攻击的首要方式便是检测蓝牙设备的讯号强度（接收信号强度），这一方式拥有双层度量标准，需经两个节点共同许可。经过检测，想要进行同一设备女巫攻击的虚拟节点便会表现出相同讯号强度，而重复数据也会被归档节点剔除，

使得所有虚拟节点只能作为单一节点运行。这一方式能够有效打击同一设备女巫攻击，使得单一计算机创建的多个节点失效。

6.6 总结

XYO网络能够检测蓝牙设备的讯号强度，删除重复数据，抵抗女巫攻击，并将单一计算机创建的多个节点作为单一节点对待。

---

7 力场攻击

7.1 总结

力场攻击，指将暗杀攻击和传统女巫攻击结合在一起，在网络中混入错误数据的攻击行为。这种攻击拥有两层特征：第一，攻击者会向合法节点输送错误信息；第二，在外者看来，攻击者的节点网络与其他节点网络表现一致。

7.2 动机

力场攻击和女巫攻击一样，其攻击者的目的也是完全控制某一区域内的网络，但是，若想要对XYO网络发动单纯的女巫攻击，攻击者必须拥有数量超过合法节点的设备。为了消除这一阻碍，力场攻击应运而生，它作为暗杀攻击和女巫攻击的结合物，能够通过暗杀攻击降低目标节点的受信任度，从而达到合法节点之间信息不一致的目的。

设想这样一种情况：攻击者想要完全控制某一地区内的网络，通过力场攻击，他可以首先干扰合法节点之间信息的一致性，降低节点的受信任度，从而减少节点对攻击的拦截力度。如此，攻击者便可以利用其数量超过受信任度低的合法节点的设备，完全控制目标区域。

7.3 技术分析

攻击者会选择性地进行验证，以达成干扰合法节点，降低合法节点间的一致性的目的。他们会将恶意节点安插进地区网络内，让每个节点只与特定设备进行通信，虽然合法节点会传播与之通信的恶意节点的位置信息，但其他合法节点却不会检测到该恶意节点的存在。宏观来说，这会导致网络内的每个节点出现较大的差异性，而对桥接节点等外部来源来说，该地区内所有节点的受信任度都会降低。

一但这项工作完成，攻击者便可以利用降低的受信任度，将自己的哨兵节点安插进整个系统。当然，有可能攻击者的设备早就已经存在于网络之中，而受信任度降低则会让这些假节点发挥更大的作用。

这种攻击方法会因地区内节点数量的不同产生变化，也就是说，节点数量越大，操作难度就会越大。

7.4 协议风险管控策略

对抗力场攻击和对抗暗杀攻击一样，也是通过惩处选择性验证的节点进行的，因为力场攻击也是通过恶意节点的选择性验证，使得XYO网络中的目标合法节点与其他节点出现不一致性。

受信任度高的节点可以对受信任度低的节点进行验证，并会将拒绝验证的节点上报系统，以将其进行选择性验证的可能性降到最低。

系统一旦发现有节点在进行选择性验证，都会将其快速删除，这也就让力场攻击变得更加难以进行了。

7.5 XY预言机网络风险规避策略

对于选择性验证的节点，XYO网络会对其采取惩罚措施，这就促进了节点积极进行认证，并向XYO网络不断输送数据的行为。若某些节点仍然拒绝验证，系统便会降低其受信任度，这一手段就使得力场攻击中的暗杀攻击部分几乎不可能成功。如此，攻击者若便只能将力场攻击转变为传统的女巫攻击，而传统的女巫攻击却需要多个设备和计算机才能完成。

7.6 总结

就哨兵节点的受信任度来说，想要在XYO网络中进行力场攻击，攻击者的成本巨大，几乎不切实际。

---

8 Teleportation Attack（传送式攻击）

8.1 总结

传送式攻击，指攻击者通过“传送”其他位置信息掩盖其真实所在的行为。如果某一哨兵节点是一部智能手机或一个蓝牙信标，当该哨兵节点向系统发送位置信息时，攻击者便会篡改数据，向系统发送别让的位置信息。如果攻击者要利用网络制造不在场证明，那么他便可以覆盖原始数据，向系统发送错误信息。

8.2 动机

此类攻击也可以通过软件进行，攻击者仅需将其密钥分享给一人或多人即可。如果有人通过该网络查看酒店评价，而网页上只会显示可信任度高、历史记录良好的评价，攻击者便会与酒店中的一人分享密钥，如此一来，其位置信息便会显示为酒店，就好像攻击者真实在那里一样。

8.3 技术分析

如果攻击者将密钥提供给用户，攻击者便能创建一个类似用户设备的假设备，而只要用户设备与密钥相连，Software Defined Radio（软件无线电）的应用就能使假设备呈现出用户具体设备的特征。这将使得系统判断不出设备位置信息的真假。同时，该攻击也会影响区块链中的数据，使其很难判别合法设备是否遭到传送式攻击。

8.4 协议风险管控策略

由于数据自然间断的特征，这种攻击所对应的检测方法也较为复杂，举例来说，如果某部手机是一个哨兵节点，一旦它被关机，那么它在下次开机前都将与网络失去联系。因此，我们便需要复杂算法来区分收到的信息间断到底是自然间断，还是设备受到攻击后的行为。

8.5 XY预言机网络风险规避策略

如果归档节点互相之间能够分享信息、验证数据，那我们便有可能打击传送式攻击。由于网络中合法设备的数量会大幅减少，服务器比较大范围内的数据也就成为了可能，而由此，语言节点便可以发现重复位置信息和传送式攻击中的恶意数据，从而利用算法对其进行筛检和惩罚。

8.6 总结

虽然我们很难在协议级别对抗传送式攻击，但是归档节点等XYO网络更高级别的服务器却可以检测并惩处这些恶意数据。而且，这些服务器也会相互分享信息，不断增加可信信息，剔除恶意数据。

---

9 Stealth Attack（隐秘攻击）

9.1 总结

隐秘攻击指设备通过伪装自己在网络进行攻击的行为。XYO网络中的很多使用案例都要求设备拥有良好的历史记录。

9.2 动机

促使攻击者使用这种方式对XYO网络进行攻击的原因并不多，因为XYO网络的目的在于确定某人或某物位于某地，而不是证明其所经过的所有地方。这两者之前存在巨大差别，就好像协议级别的数据可以不准确，但是节点的受信任度却不能很低。

尽管如此，恶意用户也可以故意开启和关闭手机或蓝牙设备的定位服务，造成数据链破损无效，因为通过这样的行为，网络收集不到他们不想公布的行踪，故而只记录对其有利的位置信息。

9.3 技术分析

简单的隐秘攻击可以通过关闭设备进行，而复杂的则可以通过应用法拉第笼进行。如果不想使用实体设备，人们也可以利用拒绝服务攻击进行攻击。

9.4 协议风险管控策略

由于蓝牙等其他设备可以轻易断开网络连接，对抗这种攻击的方法便会复杂一些。其中，弥补该缺陷最主要的方式就是采用强效软件，对传输破损数据链的哨兵节点和桥接节点进行处罚。而随着算法日渐成熟，其对有效数据和无效数据之间微妙差别的理解也日渐深入，系统的检测能力也会随之增加。

9.5 XY预言机网络风险规避策略

若节点中的历史记录出现间断，系统便会立刻怀疑该设备，并要求其向XYO网络提供连续的位置信息证明。一旦数据到达，归档节点便会对其进行严格的筛查程序，验证间断信息，并对其中不一致的信息作出处罚。XYO网络最主要的特征就是能够从混乱的数据中提取出最准确的位置信息。

9.6 总结

鉴于XYO网络以往的使用案例，隐秘攻击在经济层面是很难达成的。

10 拒绝服务攻击

10.1 总结

拒绝服务攻击（DoS），指恶意或不正常设备引起的当地、地区或整个系统运行中断的的行为。

10.2 动机

破坏者意图通过破坏XYO网络，阻止其验证位置信息证据。

10.3 技术分析

因蓝牙协议限制，蓝牙信标只能一次连接一个设备，这就意味着任何接收未验证命令的设备都能被轻易检测到，并剔除网络。但是，通过手机应用传送蓝牙命令便会容易得多，例如，攻击者可以向设备发送“播放声音”等16进制的参数信息与其建立连接。链接一旦建立，该设备与其他设备的通信便会被完全屏蔽掉，不仅如此，通过使用软件无线电，攻击者还能继续运行脚本，发送16进制的参数信息，连接更多设备。

10.4 协议风险管控策略

XYO网络中的蓝牙设备应该只能接收已验证命令，或使用介质访问控制地址白名单。因此，减少已配对设备的数量能够尽可能的避免拒绝服务攻击。

10.5 XY预言机网络风险规避策略

XYO网络由运行归档节点和语言节点的服务器构成，这两者都会与同类节点分享已验证信息，所以，若想检索数据，就必须通过节点验证。虽然攻击者可以破坏掉协议级网络服务的一小部分，但整个网络系统极其庞大，想要攻击整体是几乎不可能的。

10.6 总结

鉴于XYO网络分散式的特征，即使遭受拒绝服务攻击，该网络也能正常运行。而由于拒绝服务攻击需要大量的计算能力和物理接入，即使破坏XYO网络的一小部分也需要花费大量的人力物力。

---

11 鸣谢

此红皮书是在白皮书和绿皮书的基础上，对XYO网络安全性做出的进一步推论。感谢Christine Sako（克里斯汀 · 塞克）作出的详细评述以及应用的最佳方法。

参考文献

[1] Jafarnia-Jahromi, Ali. Ali Broumandan, John Nielsen, and Gerard Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. https://www.hindawi.com/journals/ijno/2012/127072/cta/ International Journal of Navigation and Observation, Alberta, Canada, May 2012.

[2] Padgette, John, John Bahr, Mayank Batra, Marcel Holtmann, Rhonda Smithbey, Lily Chen, and Karen Scarfone. Guide to Bluetooth Security. http://nvlpubs.nist.gov/nistpubs /SpecialPublications/NIST.SP.800-121r2.pdf U.S. Department of Commerce, National Institute of Standards and Technology, May 2017.

[3] Dunning, JP. Breaking Bluetooth by being bored. https://www.defcon.org/images /defcon-18/dc-18-presentations-/Dunning/DEFCON-18-Dunning-Breaking-Bluetooth.pdf DefCon, August 2010.

[4] haxf4rall. Spoofing a Bluetooth device. http://haxf4rall.com/2016/05/11/spoofing-a-bluetooth-device/ May 11, 2016.

[5] Chief, Enforcement Bureau. FCC Enforcement Advisory. https://apps.fcc.gov/edocs public/ attachmatch/DA-14-1785A1.pdf FCC.gov, December 8, 2014.

词汇表

准确性

一种置信度衡量方法，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。

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。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。

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。

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。

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。

XYO网络

XYO网络代表“XY预言机网络”。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。