Gravity

与区块链无关的跨链通信和数据预言协议

Aleksei Pupyshev, Dmitry Gubanov, Elshan Dzhafarov, llya Sapranidi, Inal Kardanov, Vladimir Zhuravlev, Shamil Khalilov, Marc Jansen, Igor Pavlov, Sasha Ivanov

oracle @gravity. Tech

www. gravity. tech

摘要

本文旨在提出一种与区块链无关的协议的体系结构,该协议旨在用于区块链之间(即跨链）之间的通信以及与外界之间的区块链（即数据预言）的通信。

区块链行业中尖端技术的迅猛发展概述了以“技术和经济”高效且面向未来的方式解决语言机共识的需求和机遇。如果提出一种技术解决方案需要增加一层架构层，那么不可知论的区块链将受到固有的限制。因此，Gravity 协议被设计为真正的与区块链无关的协议。通过直接集成来确保奇偶性，并利用各个互连生态系统的稳定性和安全性，Gravity 避免了对专用，公共区块链和本机代币的需求。最终，Gravity 协议旨在通过提供用于创建网关，跨链应用程序和侧链的可靠基础架构来解决可伸缩性挑战。本文档介绍并定义了预言机共识的概念及其在名为 Pulse 共识算法的 Gravity 协议中的实现。拟议的共识体系结构使 Gravity 可以被视为与区块链无关的奇异分散式预言机。

版本：1.3.2

创建于：2020 年 4 月 17 日

最近更新：2020 年 6 月 10 日

介绍

区块链技术提出了一种固有的根本方法，即通过分散化来实现不变性和效率，从而解决了与集中式系统相关的技术挑战。这种核心意识形态进行了如此大刀阔斧的创新，因此整个行业正在迅速改变通信协议和开源生态系统等相关方面。通过加密货币，智能合约和跨链通信基础设施，出现了尖端的金融框架和工具，它们位于经济学，法律，社会学，数学和计算机科学的交汇处，通常被称为去中心化金融（DeFi）或 Web 3.0。

为了获得和 WWW 一样大的初始影响力，它必须拥有通过灵活和可扩展的通信网络即时可靠地交换信息的需求。 互联网的发展伴随着网络去中心化，自治和自动化水平的不断提高，这是通过试验和开发各种协议在网络集线器之间进行数据传输而实现的。如今，在区块链生态系统中依旧存在着对实验和创新的需求，尤其是在跨链通信方面，为了实现最终的共同目标：创建一个全球性的，相互连接的，分散的架构，每个人都可以使用，并且能够推动采用新的革命性构想，而 Web 2.0 则无能为力。

最终所需的技术解决方案之一是能够将数据从现实世界的信息源传输到区块链网络，并在这些独立网络之间建立通信的能力。为此，必须依靠所谓的神谕。然而，自相矛盾的是，可以得出这样的结论：在这样一种不信任的系统中，仍然需要信任各个元素。对于整个行业来说，研究和开发新框架以解决不信任的通信至关重要。

在现有解决方案与从意识形态上看，有效解决方案和现存方案具有明显区别。当前提出的架构的常见设计是通过将附加层插入协议，从而增加复杂性，从而解决与区块链无关的通信。不能不承认区块链对技术和金融进行了革命性的改进，但是，这似乎与大多数（即使不是全部）区块链相关的创新都需要专有链和代币的想法相关。本文介绍了一种解决方案，可解决预言机共识问题，该解决方案从专有的区块链和/或代币中剥离出来，旨在提高效率，安全性和包容性。从本质上讲，Gravity 是提出一种真正的与区块链无关的协议的提议。

消除了形成新区块链以解决跨链交互的需求，这显着影响了所提议协议的技术和经济成果。在 Gravity 环境中，跨链通信是指网络 A 直接与网络 C 进行通信，而不会插入新的专有网络 B。这通过消除复杂性层而获得了更有效的解决方案。但是，更重要的是,拥有与区块链无关的协议的专有代币会干扰内部生态系统的激励一致性。如果提出的解决方案允许与它连接的一个链（如果不是全部）的潜在竞争对手发生

潜在冲突，那么从理论上讲，就不可能实现区块链不可知论。消除这种部落设计限制的任何协议都可以使原本可以竞争的生态系统之间实现协同增效。此外，Gravity 的内部经济利用了它所连接的链条的本土经济。与在合并的金融结构中承保内在的经济安全相比，Gravity 通过所有 Gravity 连接的链的累积分散来分散稳定性以承保其经济安全。

出于说明目的，表 1 列出了 Gravity 与目前最流行的预言机解决方案和互操作性之间的显着差异。

	Gravity	ChainLink	Polka
激励机制	集成链代币	专用代币	专用代币
建筑	内部指示灯	专用代币	专用区块链和代币
网络管理	去中心化	集中	去中心化
网络治理	去中心化	集中	去中心化
节点间的专用共识	是（pulse）	否	是（Grandpa/Babe）
新节点的网络条目	开启	关闭	开启
与区块链无关*	是	否	否
区块链互操作性解决方案	是	否	是
预言机数据解决方案	是	是	否
侧链解决方案	是	否	是

*根据原则声明

原则声明

1.为了推进去中心化和开放金融行业，我们需要针对预言机和链间通信的真正的，与区块链无关的解决方案。

2.如果解决方案使用具有自己的本机代币的专用区块链，则不能完全与区块链无关。

3.专用代币使预言机之间的交互复杂化，不需要为预言机服务付费。

4. 预言机共识是真正的去中心化创新，而任何其他解决方案本质上都是中心化预言机的组合。

5.区块链行业需要一个统一的，可信任的，去中心化的，与区块链无关的预言机，

这是一个开放式网络，而不是单个独立预言机的市场。
6.统一区块链不可知的预言机的经济应得到其所连接的本机代币经济的支持，因此，可能会对其增长产生积极影响。
7.创建统一的分散式预言系统是所有公共区块链生态系统要确保其共生和繁荣的共同全球挑战。

当前面临的挑战

在本节中，我们描述了一个与当前的跨链通信和数据预言系统特别相关的问题的暂定清单，旨在回顾广泛的障碍，而这些障碍不一定能通过 Gravity 协议整体解决。 本节提供了有用的上下文背景，以方便对本文提出的概念进行解释。
挑战一：在没有可信的预言机或验证器的情况下，跨链通信是无法实现的。
由于挑战一的重要性，本文的重点主要在于将数据从外部源传输到目标区块链的协议的详细说明。在这种情况下，一个区块链可以充当另一个区块链的外部数据源。
挑战二：需要使用几个剩余的主数据源来提高聚合数据的可靠性和准确性。一个孤立的外部数据源可能会（偶然或恶意）以举报错误信息或由于受到检查，阻止或过滤数据或任何其他外部干扰的方式危害系统安全的行为。数据源的多样化可以帮助提高系统对所描述威胁的弹性。
挑战三：单个预言机的信任度不如几个独立预言机，后者中每个预言机对系统的信任级别相同。这个问题可以通过计算概率来证明，但是从直观上也可以看出，独立组织的几张票比信任程度相同的人的票更可靠。可以通过集成签名（或多重签名）来解决此问题，其中多个参与者同时验证数据，这降低了攻击成功的可能性。
挑战四：预言机系统需要信任。
信任是一个基本概念，代表对系统单个用户的风险级别，信任程度越高，在不可抗力或攻击的情况下对潜在损害程度的风险评估就越低。对系统的信任本质上是对各个预言机的信任总和，这取决于系统内部和外部的操作历史以及对预言机的信誉度进行监视和评估的内部机制。
为了保持预言机网络的可依赖性，有必要结合内置的安全系统和自治策略，这些系统应能够自动工作并可以进行人工干预。例如，已经被恶意感染并能够影响整个系统的预言机应自动从签署数据并将其交付给目标区块链的活动预言机的共识中排除。
挑战五：在基于信任的系统中，数据提供者需要一定程度的承诺，因为预言机的作

用至关重要。在相对较长的时间内存放代币可以作为对“善意”的确认，并且是新预言机的可信度的第一个指标。

挑战六：预言机的不当性能或恶意活动可能会对数据提供的结果产生负面影响，除非通过对其所有者造成财务后果来阻止它。至少有两种方法可以对突然变得恶意的预言机实施制裁：“大刀阔斧”（在某些情况下会受到处罚），或冻结已存放的资金较长时间。在本文中，我们仅考虑后者。

挑战七：分布式系统更容易受到攻击，如果这样做的代价比预期的收益要低，并且不会花费太多时间。在预言机自愿离开系统后，将存款锁定延迟一段较长的时间是一项安全措施，旨在为 Sybil 攻击等攻击引入复杂性，该攻击包括注册和重新注册大量节点。

挑战八：由预言机验证的数据需要可集体验证的链上签名（阈值签名），以便安全地传递到目标区块链。否则，无论在预言机内部共识中获得了什么结果，在目标区块链中签署数据的实体都将受到攻击。

挑战九：需要证明每个预言机独立于其他预言机以原始方式获取数据，才能使预言机货币化。

为了防范挑战九所代表的问题，预言机需要独立地从外部来源请求信息，而不是相互借用传输的数据值。此类问题通过提交公开方案解决，该方案在开始时仅显示从数据生成的哈希，其值随后披露。如果所公开的散列不对应于所公开的数据，则可被视为已经识别的欺诈行为。

挑战十：为了从预言机的工作中获利，必须分开验证获得的数据和将其交付给用户智能合约，并且仅在交付给客户时才公开（解密）数据本身。

验证数据而不在目标区块链中披露数据的过程允许将数据保密，并且仅在交付给接收者时才公开，接收者有权确定其对区块链中其他智能合约的可用性。该解决方案通过保护获取数据提供奖励的方式，增加了预言机传递数据的动力。

关键概念

预言机共识是预言机网络中的一个协议，该协议关于在某些条件下应认为有效的数据馈送值。在 Gravity 内，通过对目标区块链中预言机系统所做决定的链上验证，可以达成预言机共识。与块生成共识机制不同，预言机共识处理的是更复杂的系统，该系统由不同的数据流和利用它们的应用程序组成。

Pulse 共识是 Gravity 协议中预言机共识的实现。它包括两个阶段：提交发布和数据聚合以及多重签名链上验证。选择预言子集参加数据验证的机制取决于每个节点的信誉。

节点是 Gravity 网络的"构建块"元素。它是一种中间件，它在所有受支持的目标区块链和内部分布式账本中拥有并运营账户。每个节点都由基础架构组件组成，例如数据提取器，任务调度程序以及连接到目标区块链和内部分类帐的连接器。

数据馈送是规范定义的数据源。数据提要的一个案例是每天在世界上新注册的 COVID-19 案例数。

原始数据是来自主要来源（外部数据 API）的未处理数据。

数据是由节点的提取器处理的输出数据。提取器允许对从不同来源收集的数据点进行某些操作，并将其数字转换为适合特定目的和特定目标区块链的格式。例如，提取器可以将十进制数据值转换为整数。

Agg 数据是来自数据传递中涉及的所有节点的聚合数据，并对其应用了一定的数值转换（例如，平均值，中位数或最频繁的值）。

目标区块链是受支持的区块链网络，其中数据由节点写入。它包含智能合约，用于验证为数据交付付费的用户的签名和智能合约。

预言机是目标区块链中的一个帐户，用于签名和提供数据。

证明是一种加密签名，它采用消息和种子进行生成。它在智能合约中进行了验证，并且与预言机的相应公钥进行了匹配和比较。

USER-SC 是目标区块链中的用户应用程序（智能合约），它通过订阅模型从 Gravity 系统接收数据。

NEBULA-SC 是目标区块链中的智能合约，由许多预言家使用，它们在特定条件下（交付价格，信誉度阈值，最小预言家数）提供数据提要。该合同验证阈值签名参数，累积来自用户的付款并控制奖励在 nebula 的预兆提供商之间的分配。

SYSTEM-SC 是有关活动 Gravity 节点及其信誉得分的主要信息寄存器。每个目标链都有其自己的系统智能合约实例。它既管理新节点的注册，又管理已选择相应目标链进行其操作的节点的存款交易。它还充当相应目标链中所有受支持的数据馈送和星云的寄存器。

内部分布式分类帐（IDL）是一种"软件消息总线"，它支持 Gravity 节点之间的通信，并为存储提供快速的最终共识（例如 BFT）。

领事是网络中信誉得分最高的节点，这些节点在系统中获得特殊功能。他们被授权更新/迁移系统智能合约，星云智能合约，并在内部分类账中充当共识验证器。
Pulse 是产生脉冲的连续数据传送过程。每个 pulse 都始于将数据提要传递到目标区块链的任务，并导致成功验证和将数据传递给订户（USER—SC）。
领导者是选择在当前 pulse 内启动目标链中的数据传输事务的节点。它调用目标链中的两种类型的事务：pulseTx（用于验证通过多重签名从 Gravity 系统内聚合的数据生成的哈希值）和 sendDataTx（用于将已验证的数据传递给 USER—SC）。此外，领导者还从提供数据提要的所有节点收集哈希和汇总数据的证明。领导者选择基于 NEBULA—SC 中描述的规则（例如，节点可以根据目标链的高度交替作为领导者）。
订阅是用户对用户合同和应用于接收经过验证的汇总数据的公共方法的指示。
信誉是从对等节点放入 Gravity 节点的置信度的数字表示，是根据对所有节点的定期相互评估得出的。

数据提供工作流程：pulsation
通常在预言机系统中，使用一种通用的工作流程模式，该模式包含三个全局实体：1．带有数据源的外部世界； 2．预言机系统；以及 3．应安全记录数据的目标区块链。图 1 显示了 Gravity 系统中的数据提供工作流程方案，称为 pulsation。 在某个时间点（块或块间隔）开始的数据传输应始终以脉冲事务验证结束。 如果由于某种原因验证失败，则不会执行当前时间点的数据传递。 有关从外部世界到目标链的数据传递阶段的详细说明，请参阅“提交—披露和数据聚合流”和“阈值签名和数据验证流”一章。

图 1

图 1：数据提供工作流程（pulse）：

1）用户选择要订阅的数据源和 nebula 合同；

2）节点的核心监视数据传递的状态并向数据提取器请求数据；

3）提取器以异步方式访问外部数据源，而与目标区块链无关；

4）将请求的原始数据馈送到提取器中；

5）提取器处理数据，执行所有必要的汇总和过滤；

6）每个 Gravity 节点的核心启动并执行提交-发布过程，包括对等体之间的数据聚合以及从对等体收集多重签名；

7）将由预言机（领导者）汇总的数据计算出的哈希值传递到目标链中的 nebula 合约，在此验证签名和其他必要条件（pulse tx）；

8）验证后的数据作为订阅服务交付给 USER-SC。

成为数据提供工作流程的一部分,用户没有义务选择特定的预言机或其子集来信任。取而代之的是，Gravity 网络的整个数据提供服务在其内部提供了所有必要的检查，以最终独立于最终用户的需求，使其对最终用户信任。此外，用户不需要应用自己的数据聚合方法，因为它可以在系统内自动执行，从而可以将最终数据和现成的数字或字符串值从数据源提供给用户应用程序（USER-SC）。

所传输数据的安全性验证是在目标区块链中部署的 NEBULA-SC 内进行的。NEBULA-SC 包含用于验证参与数据提供者签名的参数和说明，例如：活动提供者的公钥，阈值签名设置，节点接纳的信誉阈值和领导者选择规则。 Pulse 领导者是一个节点，该节点从对等方收集所有签名和汇总数据，然后通过调用 pulseTx 方法将其发送给 NEBULA-SC 合同进行验证。

Gravity 网络中潜在的 NEBULA-SC 合同数量是不限的。每个用户或节点操作员都可以通过以主机链的本机代币支付费用来创建具有自定义属性的合同。

建筑

节点结构

Gravity 网络的关键元素是 Gravity 节点。总体而言，节点是非同构的，这意味着提供程序可以自由地选择在一个或几个目标链中工作，或者不为所有可能的数据提要而是仅为相关子集实现提取器。Gravity 节点的主要组件是核心，负责实现协议的所有业务逻辑，以及所谓的数据提要提取器。 在图 2 中，描述了节点的整体结构。

图二

图二：节点结构

1）每个节点在每个受支持的目标区块链和内部分类账中都有一个公共密钥；

2）通信模块用于与支持的目标区块链之一和内部分类帐建立通信；

3）在核心模块中实现了 Gravity 节点用于信誉计算，提交发布操作，其余组件的聚合和协调的关键逻辑；

4）计划程序管理依赖于时间和任务状态的过程。例如，它可以根据预定的时间条件

开始计划的数据传输到目标链，并从外部源中提取数据；

5）提取程序的过程是请求和处理来自外部源的数据提要的服务。一个提取器对应于节点支持的一个数据馈送，但可以使用并组合多个数据源。

Gravity 节点支持的数据馈送可以描述为样板源代码，也可以描述为数据提取器形式的实现。每个提取器根据所需数据的规范收集数据。规范定义：

- 从何处获取数据（推荐来源或强制来源）
- 如何处理从不同来源收到的数据点（例如汇总它们为特定时间段内的中位数，平均值或众数）
- 在目标区块链中将数据传递给客户的格式

Gravity 节点的每个运算符都可以根据描述的规范开发和使用自定义实现。 Gravity 开发人员将规范的开发,文档或提取器的实现作为开源开发流程的一部分进行管理。提取程序服务在 Gravity 节点运营商的服务器上进行管理和独立运行。对于运营商而言，以插件的形式集成提取器，实现提取器的自定义版本或支持某些类型的提取器的可能性是可选的并且是可选的。

Gravity 节点通过在内部分布式分类帐中发送交易，通过帐户通信器模块相互通信。内部分类帐还用于从其他节点读取消息日志。

智能合约和账户结构

除了节点网络之外，该协议还包含部署在目标区块链中的基础架构，数据馈送中的信息将传输到这些基础架构中。图 3 显示了实现 Gravity 协议的区块链架构的组件。

图三

图 3：智能合约和结构：

1）Gravity 系统代表节点社区，其中每个节点都是特定目标链的预言；

2）每个节点在每个受支持的目标链和内部分类帐中都有帐户；

3）具有快速共识确定性的内部分布式账本（例如：pBFT）使 Gravity 节点之间的通信，提交显示，汇总，记账和 p2p 分数计算成为可能；

4）给定目标链中的系统智能合约充当所有 Gravity 节点及其分数的寄存器，以及受支持数据馈送的寄存器。它还存储和管理节点存款；

5）Nebula 智能合约，用于验证和访问预言机中的数据，是用户订阅的注册以及收集付款并在预言机中分配付款的帐户；

6）用户智能合约包含从 Gravity 交付数据的订阅；单个用户合同可以接收来自不同数据源的数据；

7）领事是网络中得分最高的几个预言机的选择。他们被授权权利进行更新/迁移 SYSTEM-SC，并在内部分类账中充当共识验证者；

所描述的系统足够灵活以管理多个连接的数据馈送和订阅。这种多合同方法可简化实施，提高安全性并简化代码审核，包括对各个组件进行正式验证。

声誉管理

Gravity 将其绑定在一起并使其完整性（作为系统或可信任的分散式服务）的关键特征是参与者的声誉管理协议。正是由于这种分散的信誉系统，才能实现诸如重力网络中的自我管理之类的属性，以及实现断开恶意节点的安全机制以及通过产生可能突然占多数的恶意节点来防范网络攻击的安全机制。此外，Gravity 信誉管理的灵活性也是一个重要的优势，它可以吸引和保留在行业中享有很高声誉的新参与者，从而可以扩展正在运行的 Gravity 网络的用户群。

内部分类帐是节点用来相互通信的软件总线，它处理节点对对等方的信任等级和汇总的信誉值。 Gravity 节点评估彼此的性能，并发送他们自己对 Gravity 的所有其他节点的置信度分数，然后通过 EigenTrust 算法将其转换为特定节点的 Gravity 分数[6]。图 4 显示了四个节点的成对估计的示例。

图四

图四：基于 p2p 分数的信誉管理：

1）所有操作节点以事件和异步的方式评估它们对 Gravity 其他节点的信任级别；

2）形成配对信任估计矩阵；

3）使用 EigenTrust 算法，将估计矩阵转换为重力得分的矢量；

4）所获得的得分值允许对所有 Gravity 节点按从 0 到 100 归一化的得分进行排序。

所有对等估计都是基于 Gravity 网络中被评估节点的活动历史记录以及来自外界的任何相关信息独立形成的。

对等评分基于：

1）自动评分：

a）发送自动关机信号：

i）如果来自 oracle 的数据与合计值相差很大，

ii）如果节点停止接收和处理来自其对等方的数据提要，

iii）如果节点停止响应 Gravity 服务的任何请求。

在这种情况下，对等方可以将其等级设置为零，以确保快速关闭节点以保护 Gravity 网络免受恶意节点的攻击。

b）基于在预定时间段内的操作稳定性，为新节点定期建立渐进式重力评分。

2）由节点操作员手动评分。手动计分程序是构成 Gravity 网络治理机制的关键要素。通过手动计分，对因自动关闭而断开的节点（如事件 1.1 中所述）进行评分修改的过程，或者在需要手动对已建立节点的运营商节点进行“得分提升”时在行业中的声誉（例如，大型交易所或流行的数据聚合器）。一旦进行了手动评估，已收到评分的节点就会停止从发起手动评估程序的对等方收集自动分数。例如，当怀疑节点 B 有某种恶意行为的节点 A 的所有者手动将节点 B 降级以降低其得分时，节点 A 停止发送有关节点 B 的评估，而单独的节点 C 仍将继续对节点 B 进行评估。

评级是在事件驱动的基础上重新计算的，但 1.1 除外，因为重新计算是定期的。

收集到的对等点的评估共同构成了一个 NxN 表数据结构，其中 N 是 Gravity 节点的总数。根据 EigenTrust 算法进行的此类矩阵的某些转换，可以计算每个节点的最终分数。节点不断更新内部分布式分类帐中相邻节点的估计值，当写入目标区块链时，领事将其用作重力得分估计值的来源。因此，实现了所有使用的目标链之间的估计的一致性。

EigenTrust 算法伪代码

算法图

其中C是 $[c_{ij}]$归一化本地信任值的矩阵，$c_{ij} = \frac{max(sij, 0)}{\sum max(sij, 0)}$; t为全局信任向量

Sepandar Kamvar和Mario Schlosser [6]在论文中描述了更多细节。

网络设置

得分最高的几个节点将成为领事。领事形成内部分类账的共识核心，例如 pBFT 共识最终确定区块和交易。领事委员会的组成并不固定，取决于参与者的分数。
SYSTEM—SC 部署在每个受支持的区块链网络中，该系统负责系统交互和存款锁定，节点注册以及有关彼此的 Gravity 节点得分的收集。数据提供商可以通过在选定区块链的本机代币中的任何受支持的公共主机链中锁定一年的存款来加入网络。
加入网络时，会自动为每个新成员分配默认的对等得分值（从其他 Gravity 节点进行评估）为 0。尽管 Gravity 节点在注册后便可立即激活，但它仍能够参与提取器的数据传递，仅在其信誉评分达到一定水平时才被选择为区块链。
Gravity 网络的退出是免费的。要离开系统，节点操作员需要在进行注册的同一区块链的 SYSTEM—SC 中使用 deactivate 方法。如果退出时信誉级别为零，则存款将被锁定，并且可以在退出一年后释放，否则在注册后一年释放。
将存款锁定在阈值之上不会对节点的初始特性产生直接影响。但是，大量的存款可以证明运营商为整个网络的利益工作的意图，节点社区可以将其视为手动提高其节点信誉等级的信号。

Pulse 共识算法

Pulse 算法是一个分为两步的过程，涵盖了 Gravity 作为数据服务的核心内部机制，以及在支持的目标区块链之一中进行链上数据验证和交付的外部部分。 Pulse 是一个过程，从请求将数据传送到目标区块链开始，到成功验证并将数据传送给订户（USER—SC）为止。
提交发布和数据聚合流程
图五依次显示了特定数据馈送的数据交换，验证和聚合的主要阶段。

图五

图五：Pulse：提交披露和数据聚合流程

1）Gravity 节点从外部来源收集信息。几种可靠的数据源可用于一个数据馈送。

2）节点提取器模块可以从单个源（节点 1）收集数据，也可以从多个源（节点 2 或者 3）收集原始数据；

3）在提交阶段，每个节点都会根据数据生成哈希并将其写入内部分类帐；

4）在揭示阶段，节点将数据和盐泄漏出来，以便对照散列进行检查，并验证数据是从正确的外部来源获取的事实。揭露阶段从至少

收集到 K 个提交开始，其中 K 由足够数量的签名规则定义（例如 BFT 规则，在 11 个提交中有 8 个可用）；

5）所有来自预言机的经过验证的数据都可在内部分类帐中使用，以供同行按需读取；

6）每个节点汇总其邻居的数据（例如：计算中位数）。

7）每个节点对聚合值进行哈希处理并为其形成加密签名。所有的哈希值和签名都是由作为首领的预言家收集的；

8）领导者在目标链中执行了几笔交易：用于阈值签名验证 pulse tx 和用于将数据传输到用户智能合约的 sendData tx。

门限签名和数据验证流程

图六依次显示了生成散列，从每个节点传输的数据的加密证明以及验证阈值签名条件的主要阶段。

图六

图六：pulse：阈值签名和数据验证流程

1）每个节点汇总其他节点的数据（例如：计算中位数），对汇总值进行哈希处理，并使用当前时间戳和数据 Feed ID 为哈希生成加密签名；

2）Pulse Leader 从对等方收集所有哈希及其签名，并从内部分类帐中读取它们。 Pulse Leader 通过将散列和签名传递到相应的 nebula 协定来在目标链中执行脉冲事务；

3）在合同内部，在执行 pulse tx 期间，将验证签名与签名者的对应关系，并带有实际时间戳，星云和领导者。至少 K 个散列应该有效，其中 K 由足够数量的签名规则定义（此参数在 NEBULA-SC 中设置，例如 11 个中的 8 个）；

4）将 pulse 状态（用于数据哈希，时间戳和其他可验证参数）写入 nebula 协定的存储区；

5）Pulse Leader 代表 NEBULA-SC 进行交易，该交易将数据提供给 USER-SC；

6）作为发送交易验证的一部分，验证 pulse 验证状态，来自汇总数据和发送给用户合同的数据以及接收者本身的哈希值的有效性；

7）在一个验证数据 pulse 内，领导者调用接受验证数据的用户方法。

*nebula ID 是合同的说明者，即数据提要的接收端口。验证用于特定星云合约的签名是必需的。为了简单起见，在图示中省略了一些阶段。

pulse 共识的伪代码

Begin

Each node： Check if O i is a provider selected from {O i} N Each node： Send request to scheduler for params (t) Each node： Send request to extractor with params (t) Each node： Process raw data

Each node： Broadcast commits to peers {O i} N.

commit = hash(reveal)；reveal = message+proof

IDL ：Wait until at least K (threshold signature rule) commit messages from distinct O i are received，where K< = N

Each node： Broadcast reveal messages to the peers {Oi } K

IDL ：Verify all received commits and reveals，check the threshold signature rule (i.e. 8 out of 11)

Each node： Compute agg. data from reveals of the peers {Oi } K

Each node： Execute hash (agg_data) and generate proof from hash，timestamp & seed

Leader ：Call pulse—tx invocation with peer's hashes & proofs in nebula contract

Nebula ：Verify hashes，timestamp，proofs，threshold signature rule，and leader Leader ：

For all subscribers s j from {s j} S，

call sendDataTx with agg. data verified by nebula contract

End

经济

分散金库

Gravity 协议被设计为与开源区块链无关的协议，而没有其自己的实用程序代币。用于支持长期财务可持续性以及由不同团队赞助开发和研究以及吸引感兴趣的赞助者的可用选项在此类系统中受到限制，需要一种创新的方法。为了解决此难题，我们提出了一种针对每笔交易的征税/收费模型，以在 Gravity 服务处注册或为 USER—SC 的数据提供付款。在这种模式下收集的所有资金都将进入一个分散的跨链金库基金，在这里可以由一个特殊的分散的自治组织（DAO）管理。

DAO 的活动将致力于实现协议开发的长期财务可持续性。任何对开发和推广协议感

兴趣的外部项目发起人都可以补充金库资金。 DAO 功能的体系结构和机制的描述超出了本文的范围，并将在专门针对该模型的新文档中概述。

网络货币化

Gravity 用户可以选择使用以下两种方式之一来支付 Gravity 服务的费用：将存款存入指定的区块链账户并将其保持在一定阈值以上，或支付定期订阅费。

在第一种情况下，用户可以通过调用 NEBULA-SC 中的存放方法来存放代币。只要它们的余额足够，USER-SC 就会从 Gravity 预言机中接收带有数据的消息。

在第二种情况下，付款与用户合同方法（USER-SC）的每次执行同时进行，并被发送到 NEBULA-SC 帐户。如果在此操作过程中未收到付款，则该订阅被视为已暂停，需要用户重新激活。

所有未分配的利润都通过 Gravity 智能合约累积并每周分配。重力智能合约（SYSTEM-SC 和 NEBULA-SC）在所有主机区块链中保留每个预言机的活动日志。在利润分配时，将计算每个 Gravity 节点可以索取的资金百分比，其中单个预言机所获得的报酬份额是其活动和信誉得分乘以资金总额的乘积。

在预言机参与的每个合同中，预言机都有能力提取与其影响份额成正比的资金。

从由在相应主机区块链上创建的 NEBULA-SC 填充的池中补充 SYSTEM-SC。

NEBULA-SC 合同在每次向 USER-SC 传送数据时都会收到付款。

案例

处理“ COVID-19 个病例”数据馈送的 NEBULA-SC 在一周内已从订户中收集了 100 个代币。节点 V 已提供了所有已验证数据哈希的 10%。在计算时，该节点的重力分数为 85gr。因此，对 nebula 性能影响的非归一化值为 0.1 * 0.85 = 0.085。让我们假设其余六个节点具有影响值[0.2 * 0.7、0.2 * 0.7、0.2 * 0.7、0.1 * 0.6、0.0 * 0.9]。所有影响的总和等于 0.705。这意味着在运行的最后一周，节点 V 产生了约 12%的标准化影响。结果，节点 V 可以从 NEBULA-SC 的每周未分配利润中收集 12 个代币。

应用领域

资料提供

该协议的数据提供功能已在本文档的主要部分中进行了详尽介绍，但尤其重要的是要注意，数据提供方案是下文所述的高级和专用协议应用程序的基础。

trigger

尽管本文中描述的协议专注于将网络同意的预言机数据传递给目标区块链，但从实际角度来看，另一项有价值的功能是定期调用用户智能合约的指定方法而不向其传输任何数据。例如，智能合约功能的调用可以与区块链或公共门户网站上事件的真假结果联系在一起。在这种情况下，Gravity 系统将能够报告事件发生的时间。这些应用程序称为触发器，可以在 Gravity 协议上实现，而对 NEBULA—SC 和 USER—SC 的修改和自定义最少。

可以对所谓的 pacemaker 预言机实现类似的流程，这些 pacemaker 预言机用作那些智能合约系统的外部事件触发器，在这些智能合约系统中，合约只是验证程序脚本，没有循环和递归，并且可能不是完整体[7]。

跨链传输网关

Gravity 协议的另一个有用应用是数字资产（代币）的跨链转移。两个区块链网络之间的数据提供是此类应用程序的关键链接，主要原理是将代币锁定在一个区块链（起源）中，并将此事件报告给另一个区块链（目的地），后者将发布完全相同数量的代币。在未发生代币发行的紧急情况下，将启动争端解决程序，该争端解决程序将发出信号以解锁原始区块链上的代币。这种通往网关的方法要求在两个目标区块链中的 Gravity 网络的预言机之间进行协调操作。如果有密码学支持，则存在多种方式来实现此类应用程序，例如，Merkle。

实现网关的另一种方法是根据特定资产的价格，根据专门的数据馈送创建信号提供者。构建网关协议归结为在 Gravity 协议上设计应用程序层协议。值得注意的是，这些协议本身可以完全分散，并基于智能，无参与者的合同，以避免将集中的故障点引入系统。

跨链委托网关

与跨链传输类似，相同的方法也适用于其他实际数据解决方案。通过跨链委托网关，一个区块链（来源）中的帐户持有人能够在另一个区块链（目的地）中创建事件，这意味着部署在区块链 A 中的应用程序的用户可以直接从区块链 B 中进行管理而无

需账户实现此类应用程序需要相当复杂的跨链信令逻辑和稳定的基础架构组件，例如触发器和跨链传输。我们相信 Gravity 协议可以为创建和推广这种类型的尖端跨链去中心化应用程序提供坚实的基础。

侧链

跨链通信的一种特殊情况称为侧链技术，它可以实现已经部署的公共网络的可伸缩性。通常，为了将经济价值赋予侧链代币，跨链提供商应确保将一定数量的本机代币锁定在源区块链上，并将其相应的总供应量锁定在侧链上。为了管理这些过程并验证侧链中的系统更改或对原始区块链中的更改做出正确反应，需要一个去中心化的预言机，该预言机通过结构上相关的数据馈送从一个区块链到另一个区块链提供的信号。 Gravity 网络就是这种预言机的一个例子，它与原始和侧链区块链中的智能合约形式的其他模块结合使用，因为它跨越了两个不同的区块链，但是仅利用了一个公用事业代币，从而提高了原始区块链的计算和交易性能。

总结

本文所述的 Gravity 概念允许实施一个复杂的预言机交叉网络，支持区块链网络与外界的通信，跨链通信和转移以及将侧链集成在一个整体且自治的环境中系统。由于提出了共识设计，因此 Gravity 可以被视为与区块链无关的单个分散式预言机。