JOIN Protocol White Paper

提供高可靠数据服务的预言机协议

2020-07

1.引言

智能合约（Smart Contract）这个术语至少可以追溯到 1995 年，是由多产的跨领域法律学者尼克·萨博（Nick Szabo）提出来的：“一个智能合约是一套以数字形式定义的承诺（Promises），包括合约参与方可以在上面执行这些承诺的协议。” 但当萨博提出智能合约的理论后，在很长一段时间里没有清晰的实践路径，直到以太坊的诞生。

随着在智能合约领域不断的尝试，去中心化金融（DeFi）已经开创了一个充满挑战和令人激动的领域：未来智能经济范式。未来智能经济将会具有去中心化、智能化、平等化、自由化等特性。正是依托于这些特性，可以确保任何人都可以无障碍的使用其提供的服务，不需要被审核，只要满足清晰明确的智能合约要求即可。

智能合约只有在去中心化基础设施（如：以太坊）上执行，才能保证已实现的执行准则不会受到某一方的干扰行为而改变。基于这种去中心化的可靠模式，才让世界上不同个体之间可以忽略地理、语言、文化的差异，而达成某种合作或者交易，这是对整个人类文明的进一步解放。但事物的两面性也给智能合约的发展带来了桎梏，智能合约需要使用更多人类活动产生的数据来构建更丰富的智能经济范式，这就需要通过一种高可靠的方式将链外数据传递给智能合约，此种方式被称之为“预言机”。

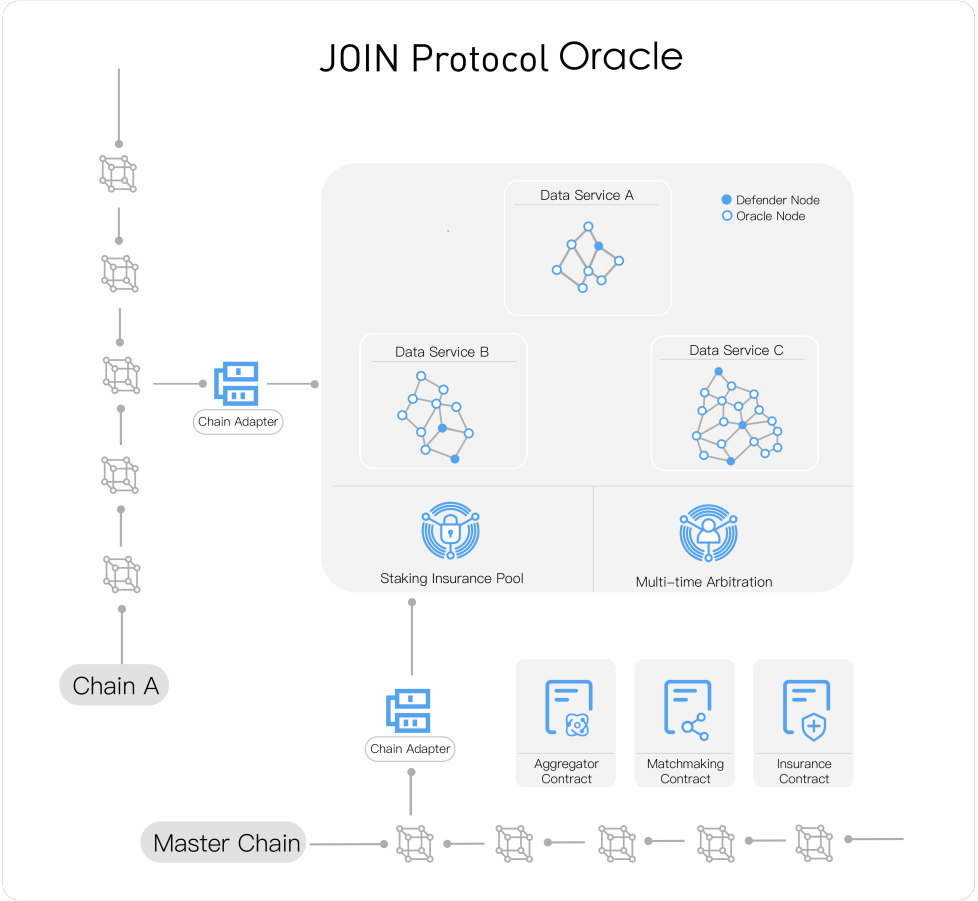
JOIN Protocol 正是为解决这一问题而提出，并致力于为未来智能经济范式打造一个提供高可靠的预言机协议。JOIN Protocol 具有四大特点，分别是：随机透明的节点出块策略，博弈完备的防作弊设计，原生去中心化经济模型以及多种数据提供方案。这些特点也是新一代高可靠预言机的基础。

2.架构综述

在未来多链并存的情况下，JOIN Protocol 将采用资产和业务逻辑分离的方式来构建；资产将会由智能合约在不同公链上面进行管理，数据采集以及共识逻辑将由一系列组件构建的预言机网络集群来实现。代币将会在以太坊上发行，并通过可靠的跨链技术在其他公链上面流通。

JOIN Protocol 具有两种节点角色：预言机节点和卫士节点。预言机节点和卫士节点二者网络协议相同，前者用于提供预言机数据服务后者用于监督预言机节点行为。卫士节点竞选完全开放，满足抵押条件既可以加入，当选的预言机节点可以同时运行卫士节点，两种节点共同组成一个健康、博弈的预言机网络。

此外，从结构上面来看，JOIN Protocol 可以分为链上合约以及预言机网络协议。链上交互合约包含：排名合约、结果合约、撮合合约、风控合约、仲裁合约等；预言机网络协议包含：高效的 P2P 通讯网络、门限签名、数据源采集器、公链适配器等组件。



图一 JOIN Protocol 架构图

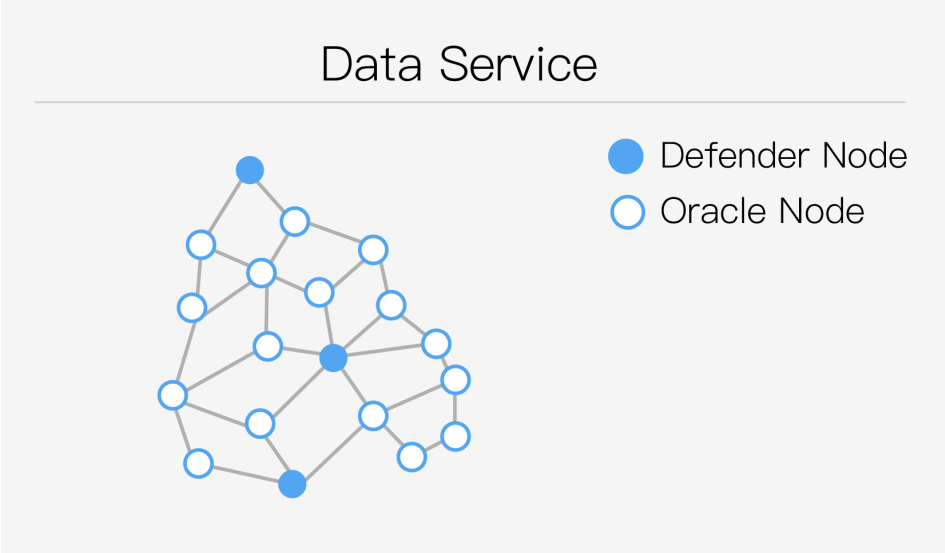
3.高可靠的预言机协议

采用预言机服务的智能合约以 DeFi 应用为代表，DeFi 对数据的需求不仅要数据准确，还需要保证数据的真实性，同时可以根据不同场景采用不同的可靠方式获取数据。JOIN Protocol 正是为此类场景设计。

3.1 随机透明的节点出块策略

“可信”是现实世界中交易的最基本条件，如果我们无法达成信任那么也就无法完成交易。信任对我们来说是如此的重要，然而很多时候难以达成信任，往往只能依赖于交易双方的信誉或者依托于某个可信的第三方。在复杂的场景中，这使得我们承担了更多的风险，耗费了更多的精力和资源。有些预言机服务的设计是基于可信数据源或者权威数据源这一假设，这样的假设从理论上来说有很大风险，无法保证这种数据源提供数据的真实性。

依托于一个开放的算力证明共识机制，比特币成为了一个可信的去中心化经济体的范例。伴随着其他共识机制的尝试与验证，PoS 成为了一个实现相对高效且兼顾去中心化的共识机制；但为了避免“巨鲸”成为整个系统的潜在风险，不同公链又结合自身的情况作了一些改进。



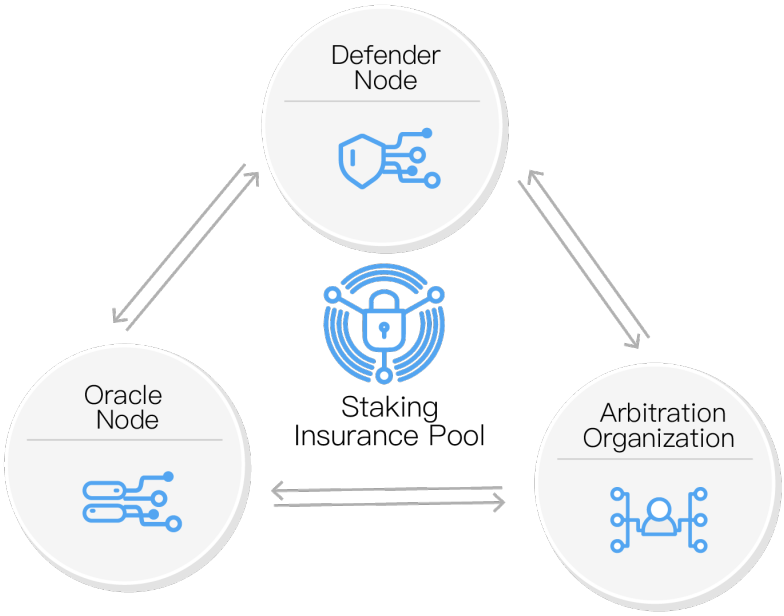
图二 JOIN Protocol 数据服务拓扑图

JOIN Protocol 将会采用可验证随机函数的 PoS 共识机制来达成预言机数据的可信共识。对于一个预言机数据服务来讲，将会由抵押数量最高的不少于 15 个数据提供商来组建预言机服务网络，满足不少于 3/2n+1 的节点签名的结果作为此次数据服务的结果。

3.2 博弈完备的防作弊设计

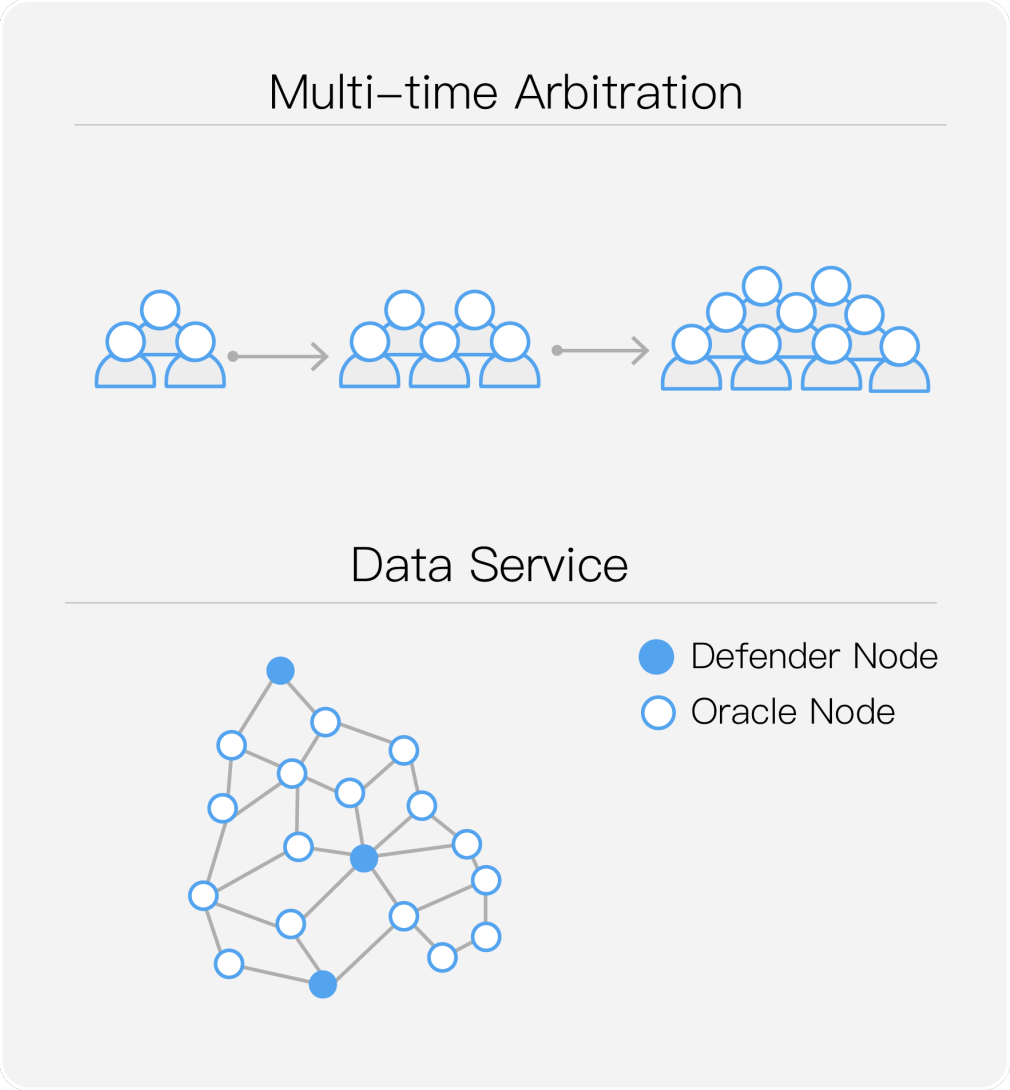
预言机是图灵机模型引入的概念，由于停机问题以及数学不完备性的原因，引入该概念后会得到一些标准图灵机所不能得到结果。在图灵机里它是确定性的，但在区块链中引入的预言机却很难得到理论上定义的特点，究其原因是因为区块链本身就是建立在容错逻辑之上，其本身并不要求输入的确定性，甚至允许存在欺骗行为，这

也是区块链建立拜占庭容错结构之上的原因。因此区块链的预言机与传统意义上的预言机有着本质的区别。



图三 JOIN Protocol 博弈模型角色关系

面对非可信数据提供者问题，简单的确定性计算模型显然已经无能为力，为此我们引入博弈的系统模型来解决这些问题。概括的讲，不单纯的将预言机看作是系统的信息提供点，而是将其看作博弈的参与方与信息使用者共同构建博弈模型。并通过引入惩罚机制以及多回合博弈机制来建立可信承诺，通过多信息提供点的信息选取机制达到谢林点，从而提高信息的可信性；此外通过引入卫士节点并加入奖惩机制，构建对数据服务提供者的囚徒困境，进一步保证可信性。



图四 JOIN Protocol 博弈模型

下面针对在该博弈模型下的作弊情况进行一些讨论。

假设，数据提供方集合为 **[dp1,dp2,...,dpi,....，dpn]** ，其中：

- 该集合共包含 **n** 个元素
- 其中 **dpi** 为编号为 **i** 的数据提供方
- 对于任意的数据提供方假设其已经提供服务次数为 **Ki**

- 每次提供数据的收入均为 **X，**抵押系数为 **dr**，基础抵押金额为 **db**

对于任何数据提供方 **dpi** 其在本次提供服务时，所抵押的总金额为：

$$Ki*X*dr + db$$

整个该类型数据集中总的抵押金额为:

$$Z = X*dr*\sum Ki+n*db$$

在某次预言数据关系到 **Y** 金额的资产分配，那么当 **Y=Z** 时，刚好可以做到即使在资产分配的利益方与所有的数据提供方串通作弊，也能在仲裁胜利后得到损失的 **100%** 赔付。

统计意义上的从应用数据到发现数据错误的平均时间我们称之为“反应期”。对于低密度数据因为有较长的反应期，因此 **Y=Z** 是平衡点；但对于高密度应用时，由于反应期内可以进行多次分配，因此其不能只考虑单次情形。下面假设在反应期内可以进行 **T** 次分配，那么其单次所能承受的风险值为：

$$(X*dr*\sum Ki+n*db)/T$$

假设此次资产分配涉及到的总金额为 **Y**，对于 **n** 个数据提供方其本次作弊所得收入为 **Y/n** ，在不考虑数据使用者发现问题的情形下，只有当 **Y/n>Z-X*dr*Ki+d** 时其作弊才有意义，否则诚实的检举会是最优策略。进一步假设每个人抵押相同，那么有 **Y/n=Z*(n-1)/n => Y=Z*(n-1)**，也就是说从这个意义上看平衡点上升到了 **Z*(n-**

1)。考虑到卫士节点以及每个数据提供者都可以提起申诉的情况，这将演化为典型的多人博弈的囚徒困境，诚实的检举将会变成最优策略。

上述模型中只考虑了一次博弈的情形，由于系统本质上是重复多次博弈的模型，长期来看对于有着稳定收入的预言机数据提供者，在公示了部分身份数据信息后其背叛成本将远高于上述讨论的理论值，而提供者在多轮博弈中其对立的属性并未改变。

系统的规则对于理性的参与者来说是静态的可预见的，因而诚实公正地进行参与才是其优势策略，对于非理性的参与者系统也能够以极大概率予以惩罚，从而使得整个预言机服务将会正向、健康、高效的运行。

3.3 原生去中心化经济模型

从群体行为角度来看，预言机可以看成是部分成员执行，但需要广泛人员监督的群体协作行为模式。需要制定一套激励机制，才能让不同的角色各司其职。

JOIN Protocol 将具备“抵押保险池（SIP, Staking Insurance Pool）”机制，抵押保险池的作用在于激励社区参与并为 JOIN 预言机提供的数据服务承担概率极小的数据事故风险赔偿。

抵押保险池奖励来源：

- 数据使用者支付费用的 20% 将会进入保险池
- JOIN 代币总量的 38% 将会逐步释放到保险池

抵押保险池规则：

- 无门槛，任何人都可以将自己的 JOIN 代币进行抵押并获取收益
- 奖励的分配按照所抵押的 JOIN 数量进行比例分配
- 如果出现事故，保险池将会补偿数据提供者抵押额的 1/3 对使用者进行赔偿
- 取消抵押需要等待 3 天的收回期

抵押保险池本身就是一种去中心化的智能经济模式，可以不断的促进 JOIN 生态发展壮大。

3.4 多种数据提供方案

JOIN Protocol 提供多种方式来实现数据的分发，可以保证在复杂的调用场景中预言机服务一直可用。

3.4.1 数据直接上链

数据提供者先行写入数据到链上，使用者读取。可以通过这种方式来提供一些免费的外部数据，这种场景数据公开，没有访问门槛，可以促进 JOIN Protocol 基础生态的多样性。

3.4.2 监听回调

数据提供者监听调用事件，链上主动推送数据到使用者。这种场景将是在公链资源比较充足情况下的主要形式。

3.4.3 链下回调

数据提供者监听调用事件，链下主动推送数据到使用者。相比 3.4.2 形式，这种形式可以不再链上暴露任何数据，安全隐私。

3.4.4 全链下交互

链下完成数据交互，签名保证数据可靠。这种形式依托于采用私钥签名的数据确权方案，可以避免公链资源紧张导致的服务不可用。

4. 数据市场

由于不同团队的技术方案、资金投入的差异，在经过一段时期的市场竞争以后，更优秀的预言机服务提供商将会更受市场青睐。JOIN Protocol 的数据市场不仅是一个预言机服务的开放卖场，更是一个和使用者进行交流的内容沉淀平台。数据市场可以按照不同维度，根据链上统计数据进行智能分析、归类、排名；用户也可以方便的针对 JOIN Protocol 的预言机服务进行对比，可以快速找到符合要求的数据服务。用户也可以发布定制的数据需求，然后悬赏社区中有对应数据资源的组织来提供该类服务。

5.长期技术战略

5.1 多金融场景延伸

金融服务的发展是循序渐进、环环相扣的。金融产品可分为基础证券（如股票、债券等）和衍生证券（如期货、期权等）两大类；其次，根据所有权属性，金融产品又可分为产权产品（如股票、期权、认股证）和债权产品（如国库券、银行信贷产品等）两大类。

目前在区块链世界，DeFi 仍处于发展的早期，相比人类生活中的金融服务，仍然需要更丰富的基础设施来进行构建，这就需要预言机服务不断深化行业场景的抽象，提供针对性的数据服务产品。

5.2 基于零知识证明的可信数据提供

随着加密技术的发展，可信的隐私数据也必将成为区块链预言机服务的一种重要形式；为此，JOIN Protocol 将基于零知识证明来构建一套可验证的保密数据预言机服务。该服务主要针对数据保密性要求高，数据有效性可以快速验证的场景，这使得区块链隐私类数据市场成为可能。

5.3 IoT 数据交易智能通道

随着 5G 技术的加速落地，将催生出丰富的商业场景，大量的智能设备产生海量的数据，基于这些丰富的数据，数据交易场景以及需求将会变得更迫切，比如针对某一区域的气候检测系统数据交易，穿戴设备收集的无敏感信息年龄和身高抽样数据等场景。JOIN Protocol 将针对 IoT 行业推出数据交易智能通道，为物联网设备打造从数据产生到数据消费的完整技术方案和通路。

5.4 全链路风险控制方案

尽管依托于“抵押模型、多轮博弈”所引入的相关博弈方法可以最大限度的使整个系统良性的运行，然而系统所面对的却是最为复杂的特例和难以预料的情形（尽管这些情况必然是小概率的），因此还要对整个系统的安全性进行进一步的加强。为了最大限度的保证系统安全，设计上将考量多回合欺诈的最差情形下，数据和资金的安全问题。此时数据提供者们变为意志统一的单一个体来参与到系统中来，且可以在短时间内进行多次欺诈行为。这种情况下，简单的考量单回合博弈已不能满足要求，需要引入风险控制体系，采用限时冻结和延时发放相结合的策略来解决该问题，从而保证其在被发现作恶的前提下对其进行惩罚。

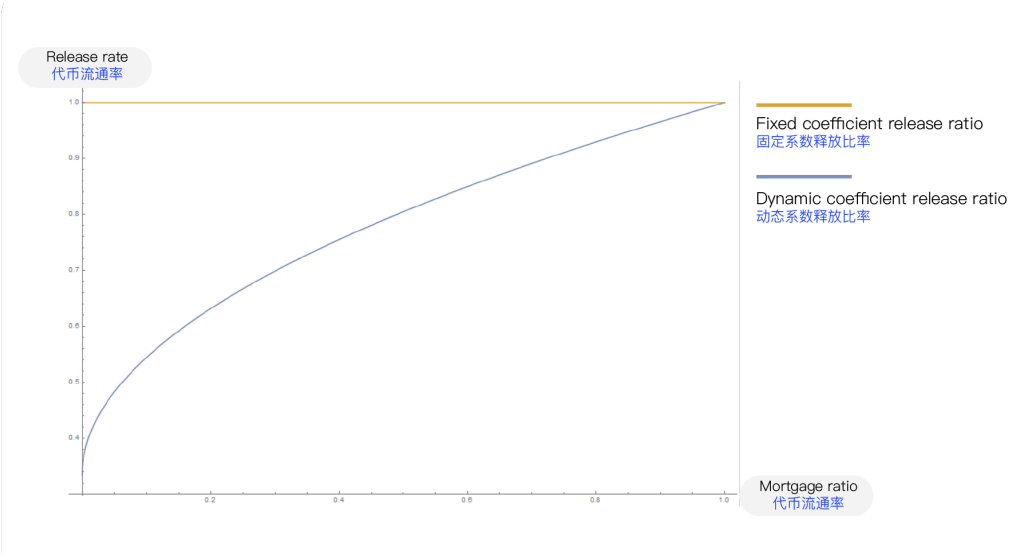
6.经济模型

良好的经济模型设计是整个生态稳定繁荣的基础，对于 JOIN 来说则更进一步，JOIN 的经济模型还承担了预言机服务安全性的构建和强化功能。由于整个预言机是构建在博弈理论基础之上，并且抵押机制作为惩罚的锚点又是博弈的前提，因此 JOIN 的经济模型将采用多币混合抵押与以抵押率作为分配参数相结合的分配模式来保障和促进惩罚锚点的稳定性，从而提高威慑力以及增强作恶触发灵敏度。

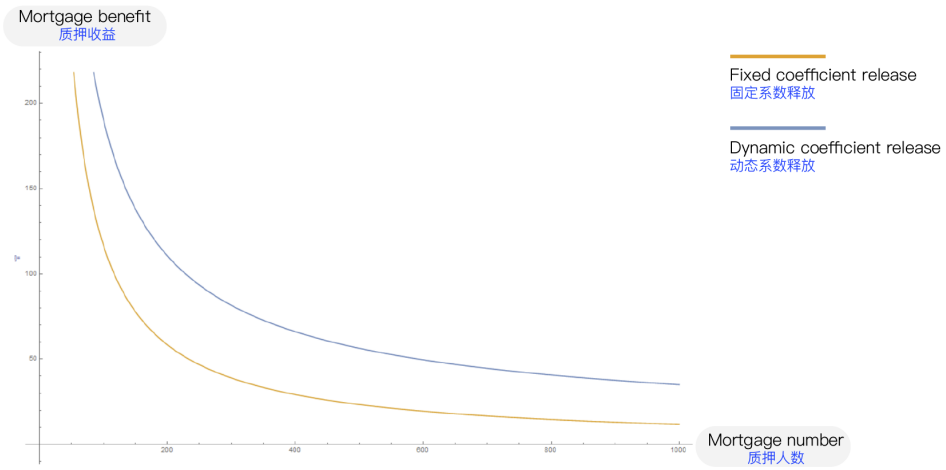
此外，JOIN 通过采用将分配策略与博弈角色进行结合的方案，不仅可以激励诚实的数据提供者，同时也促进卫士节点对数据数据提供者进行监督，系统提供数据的可靠性将得到提高。抵押保险池机制的引入会提高整个生态的抵押率，并为系统安全建设增加补偿机制，使得预言机的安全达到一个全新的高度。

在充分考虑了经济模型对预言机安全作用的同时，JOIN 的激励方案还将吸引更多的人参与到生态建设之中。实现增强预言机安全性的同时又将去中心化和公平公正的理念深化。使得人人可以成为预言机参与者，人人可以是预言机的安全贡献者，同时人人也会是预言机激励的受益者。无论对于 JOIN 的价值还是预言机本身的安全性来讲，这将无疑会形成一个良性的循环。

作为提供高可靠数据的预言机协议，公平与稳定是 JOIN Protocol 的核心理念。 JOIN 的释放策略会将抵押量以及预言机的使用频率考量在内，进而调节代币每天的释放量。代币的流通量与预言机的使用活跃度建立了相关性，使得流通中的代币与其使用规模以及获取难度达到了动态平衡，进一步维护系统的稳定以及 JOIN 价值的稳定。



图五 每日固定系数释放与动态系数释放比率对比图



图六 固定系数释放与动态系数释放收益率对比图

如图五、图六所示，调整后的每日释放率会随着抵押率以及调用频率的增加而增加。当更多的人参与到预言机系统中，将会有近 2/3 的调整空间，这使得挖矿收益的曲线变得更加的平缓，这有助于减小预言机参与者收益的波动性，并稳定 JOIN 价值预期。

通证激励方案如下：

- 名称：JOIN
- 总量：21,000,000
- 分配方式：
    - 38% 激励数据提供者
    - 38% 释放到质押保险池
    - 10% 激励数据使用者
    - 10% 社区空投
    - 4% 生态基金

其中，除生态基金以外，其余释放部分的 10% 将作为项目发展基金。

社区空投将采用 Uniswap 锁仓空投，其中 USDT-ETH、USDC-ETH、 DAI-ETH、SUSD-ETH 、JOIN-ETH（2 倍奖励）、USDT-JOIN（2 倍奖励）。

生态基金在将来的仲裁、生态激励中会按照规则释放。

日分配量 S 函数为：

$$S = (2/3 * (F1*q*F2 + (1-q)*F1) + 1/3) * S0$$

其中：

- S0 为第一个周期分配量，取值 7000
- q 为调节系数，取值 0.1
- 每释放一半的 JOIN，S0 将进行减半
- F1 = (s/t)^0.5； F2 = i/max_i
    - s：JOIN 抵押总额
    - t：JOIN 流通总量
    - i：当前服务被调用频率，5000 块为统计周期
    - max_i：截止当前最大调用频率
    - F2 取值范围 (0, 1)

结语

JOIN Protocol 将会成为未来智能经济范式所需要数据的基础平台，使得区块链技术的价值超越了其货币属性，延伸到了金融产品构建和规则的制定上。这种延伸将会解决或改进许多现实世界的信任问题，从而扩大区块链的应用边界。

参考文献

[1]: Prisoner's Dilemma: John Von Neumann, Game Theory and the Puzzle of the Bomb

[2]: Jurišić, Marko, D. Kermek and M. Konecki, 2012, "A Review of Iterated Prisoner's Dilemma Strategies," Proceedings of the 35th International Convention MIPRO, 1093–1097.

[3]: ——, 1994, Playing Fair: Game Theory and the Social Contract 1, Cambridge, MA: MIT Press.

[4]:——, 1997, "Rationality and Backward Induction," Journal of Economic Methodology, 4: 23–41.

[5]: Verifiable Random Functions

[6]: Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme