Ares Protocol

首个链上验证的去中心化跨链预言机服务协议
为万链互联和数字经济提供安全可信的数据服务

https://aresprotocol.com/

白皮书 V1.0
Ares protocol 中文社区译
2020 年 11 月

介 绍

背景

人类经历了农业革命、工业革命，正在经历信息革命。随着新一轮科技革命中人工智能、区块链、云计算、大数据等数字经济基础设施的发展创新，让数字化的信息成为数字经济的关键生产要素，赋能数字经济强大发展动力。

数据作为关键生产要素，要解决数据的安全存储、确权定价、可信传输才能进入生产流通中。Web 3.0 的构想就是通过区块链技术，在基于信任和价值交换的去中心化网络中，让身份、资产和数据回归个人；并通过跨链技术，使得信任在不同的去中心化网络上可以流动起来，让资产、数据更好的流转、融合，倍增数据生产力。

区块链外信息写入区块链内的机制，被称为预言机。预言机是区块链和现实世界之间的纽带。现实世界的信息安全、可信、高效的传输到链上，让异构链、合约、DAPP 等可以去信任的获取链外数据，是构建数字经济的基础。Ares 的愿景是希望成为 Web 3.0 生态中的去中心化跨链预言机服务协议，为万链互联和数字经济提供安全可信的数据服务。

介 绍

现有方案

预言机作为链上和链下的桥梁，保证去中心化和数据安全可信是核心。目前市场上的预言机有预言机安全，公链安全，跨链安全。chainlink 之前使用的 21 个节点来提供数据可以称为预言机安全，而 Band 和 Dos 通过共识算法来达成预言机数据安全可信可被称为公链安全。

Ares 通过引入挑战者和声誉委员会对预言机数据进行了链上验证，实现了对数据的最终敲定，其原理和波卡中 Babe 出块，Grandpa 敲定原理类似，通过数据的链上验证来达到最高安全性。

介 绍

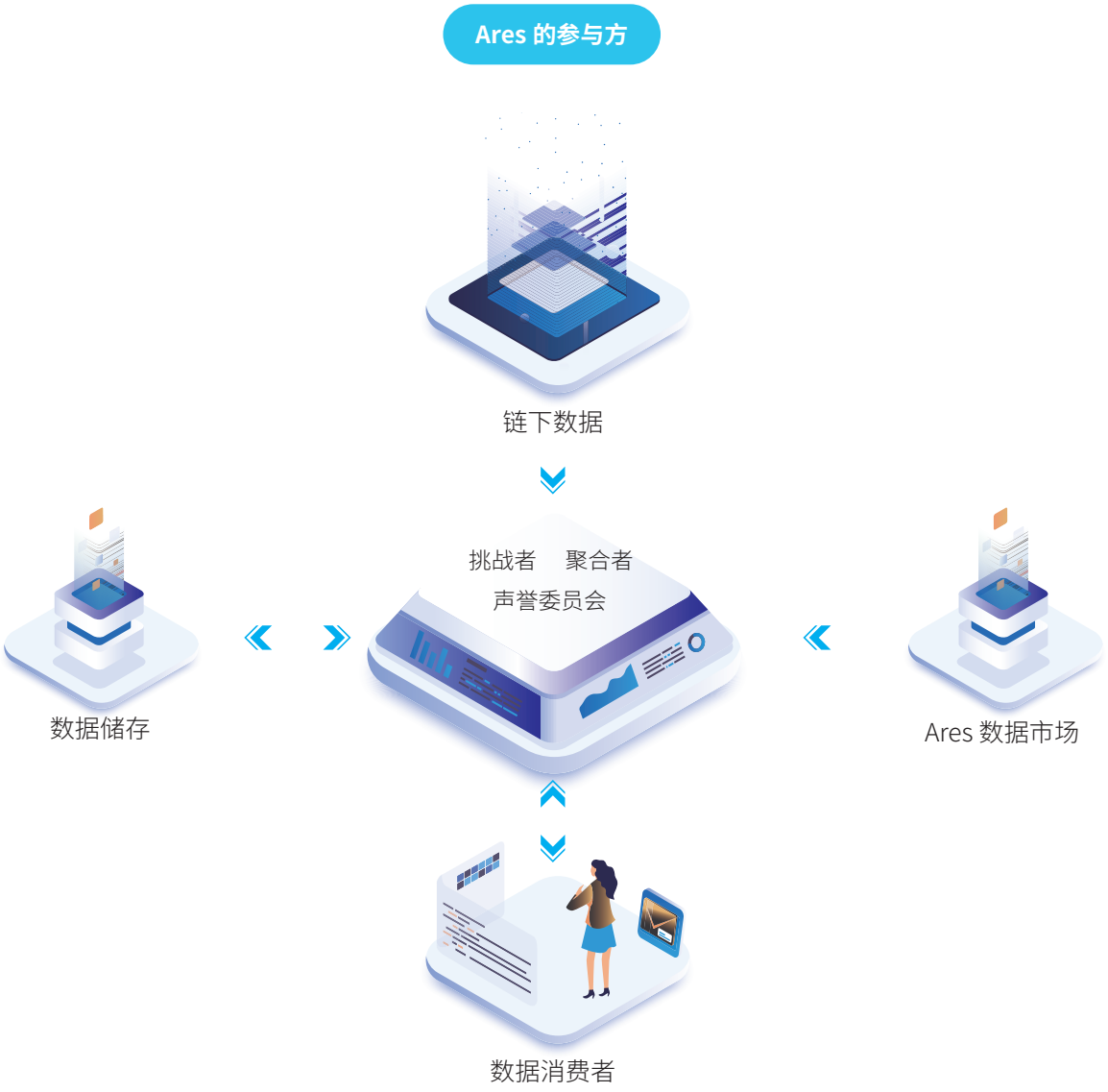
Ares Protocol 介绍

Ares 是一个去中心化混合式预言机，完全实现了预言机数据的上链和链上验证。通过引入 VRF 实现聚合者的随机选择，解决了数据的中心化问题，并保证了极低的参与门槛。然而聚合者的随机选择不能保证数据的准确性，为了解决数据的可用性问题，Ares 创新的采用了一种挑战者模式。当网络中的验证节点验证数据的过程中发现聚合者的数据存在问题，只需支付一定 Gas 即可发起挑战，这些数据会被传递给仲裁机构，仲裁机构由诚实的聚合者和 Token 持有人组成。正常情况下不工作，只有当网络中存在挑战时才解决冲突，每一个仲裁成员将会对挑战发起 BFT 投票，如果校验通过将会处罚聚合者，奖励挑战者。

Ares 作为一个开源的去中心化跨链预言机服务协议，通过引入通证模型和社区治理，构建去中心化的数据交易生态系统，让数据需求方安全有效的获取链下数据、并让优质的数据提供商通过链上治理和数据交易获利。

Ares 是建立在 Polkadot 生态下，Ares 通过 Substrate 构建，作为平行链链接到波卡生态，共享波卡的安全共识；其次，Ares 是一个可扩展的二层预言机网络，为波卡的其他平行链和主流区块链网络提供去中心化的数据预言机服务。

技术架构



去中心化金融　去中心化身份　物联网　• • • • • •　预测市场　博彩游戏

技术架构

聚合者

聚合者通过 Scanner 获取外界的请求数据，将请求发送到 processor 处理所有的 Oracle 请求。聚合者是通过 VRF 算法随机选择一个聚合者，调用 processor 聚合多个数据源的数据提交到区块里面，通过区块传播协议广播到 Ares 网络上。

挑战者

挑战者对聚合者提交的数据进行完整性和有效性验证，将存在欺诈的聚合者交易和正确数据提交给声誉委员会以获得奖励。

声誉委员会

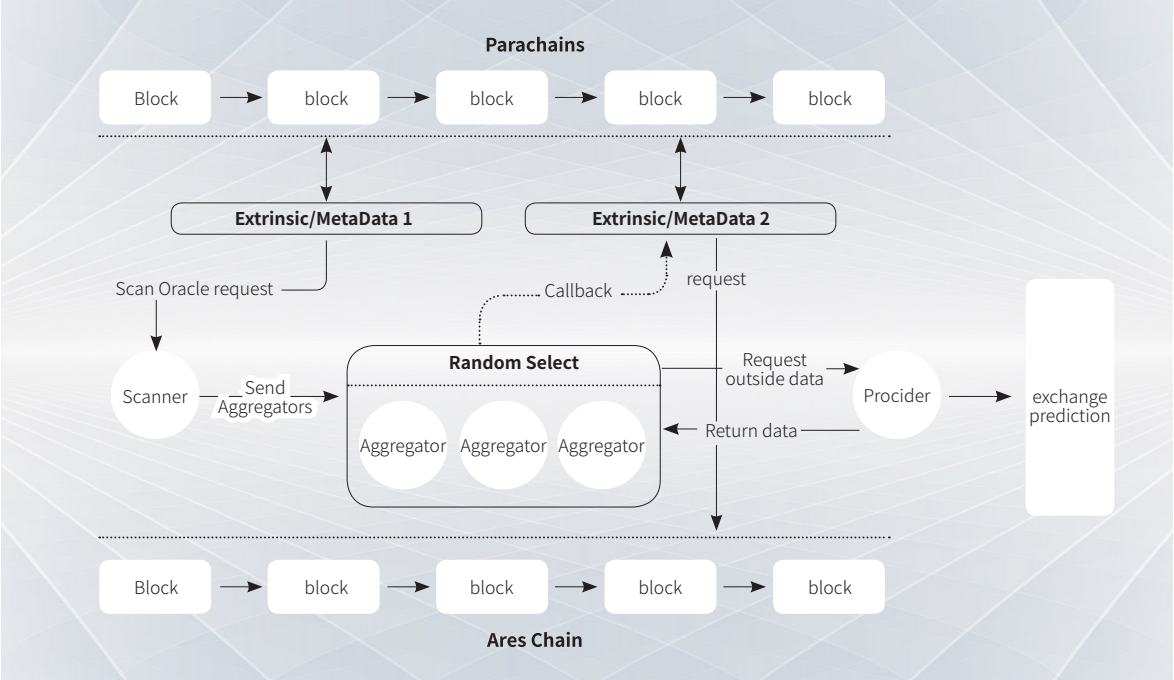
通过激励挑战者、惩罚作恶的聚合者，保证 Area 网络的安全。声誉委员会完全社区自治，通过通证抵押和信誉加权来竞选声誉委员会。声誉委员会内部仲裁需要通过 FSP 欺诈安全协议进行投票，仅在链上存在纠纷时运行。

数据消费者

数据消费者可以是智能合约、平行链、DAPP 中需要获取外界数据的对象，可以为 DEFI，预测市场，博彩提供各种可信有效数据，由于 Ares 的链上数据有一定的数据挑战期，数据消费者根据一定的安全规范获取链上数据。

节点运营商

节点运营商，作为 Ares 网络的全节点，通过和本地存储的数据市场对比来校验数据，保证 Ares 网络的安全并提供预言机 RPC 服务。



设计细节

Ares Protocol 是基于 Substrate 2.0 构建的，作为平行链 / 平行线程的方式接入波卡生态。具体的流程如下：

1. 波卡生态的平行链，通过集成 ares oracle pallet，提交数据请求；
2. Scanner 获取外界的请求数据，提交给聚合者；
3. Ares Chain 通过 VRF 算法随机选择一个聚合者；
4. 聚合者调用 processor 聚合多个数据源的数据提交到 Ares 区块链中；
5. 验证节点会验证聚合者的数据并提出挑战；
6. 声誉委员会校验挑战者提交的数据并进行仲裁。

设计细节

如何解决去中心化问题?

Ares 提出了两种方案来尽量避免问题节点的出现，即分布式的数据源以及分布式预言机。

分布式数据源

每个节点运营商，从多个不同的数据源来获得数据，以减轻异常数据源对于结果的影响。聚合函数可以将多个返回结果聚合成单一的答案。有很多方案可以完成数据聚合，比如去掉异常数据后的加权平均。

数据源之间可能会存在互相获取数据的情况，这也可能导致聚合结果的错误。我们会持续关注这类问题，并对数据源的独立性进行报告。

分布式聚合者

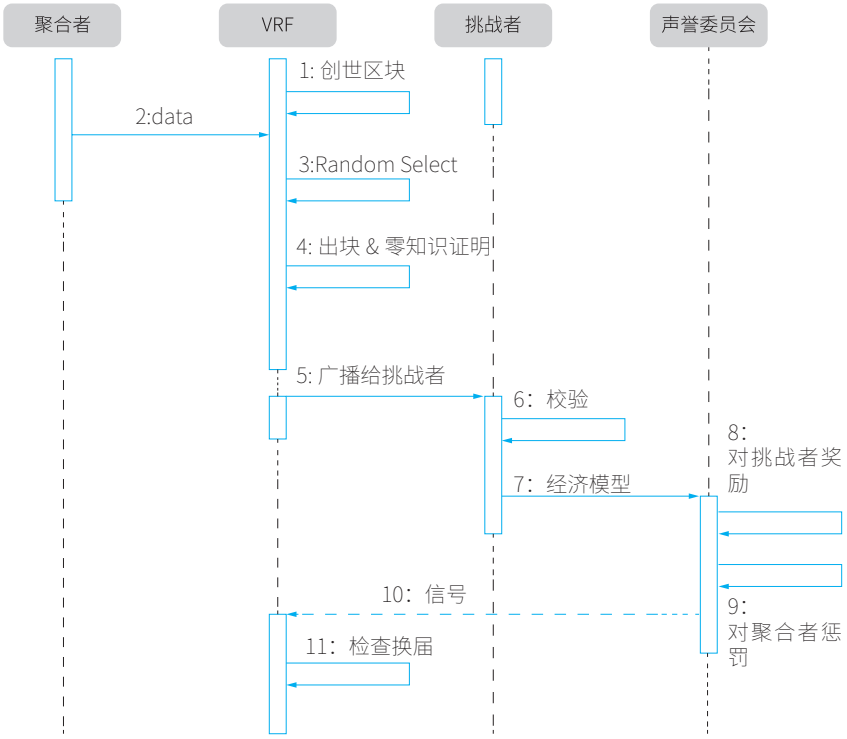
聚合者（即矿工）主要负责提供各种类型的数据，挑战者（即验证人）验证并质疑数据提供者提供的各种数据并发送给议会（仲裁机构）。声誉委员会对数据验证者提出的挑战进行仲裁，如果校验通过奖励挑战者，惩罚聚合者。

在提供数据报价的所有聚合者矿工节点中，Ares Network 通过可验证随机函数（VRF）来随机选择一组聚合者节点，以竞争提供最准确的市场数据。通过将 VRF 引入系统，可以大大提高系统的分散程度。

通过 VRF 随机选择聚合者节点提供外部数据上链在提供数据报价的所有聚合者矿工节点中，Ares Network 通过可验证随机函数（VRF）来随机选择一组聚合者节点，以竞争提供最准确的市场数据。通过将 VRF 引入系统，可以大大提高系统的分散程度。

通过 VRF 随机选择聚合者节点提供外部数据上链

设计细节



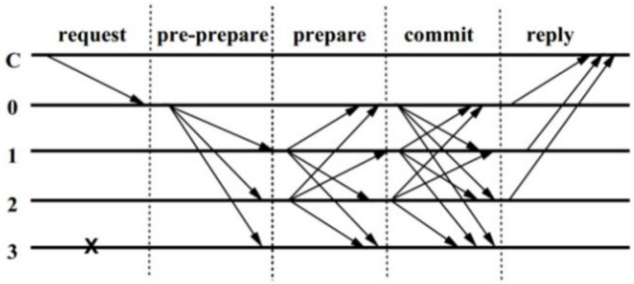
Ares 经过 VRF 的运算可选定聚合者，最终确定某个聚合者在当前高度出块，通过零知识证明以验证聚合者，这部分将在出块同时广播出去普通验证节点收到区块后验证在允许偏差范围内则校验通过。

设计细节

声誉委员会治理

BFT（Byzantine Fault-Tolerant）算法于 20 世纪 80 年代开始被研究，旨在解决所谓拜占庭将军问题。BFT 类算法中最著名的是 PBFT，该算法是基于消息传递的一致性算法，在弱同步网络下，算法经过三个阶段可以达成一致性，复杂度为 O(n2)。在无法达成一致时，这些阶段会重复进行，直到超时。

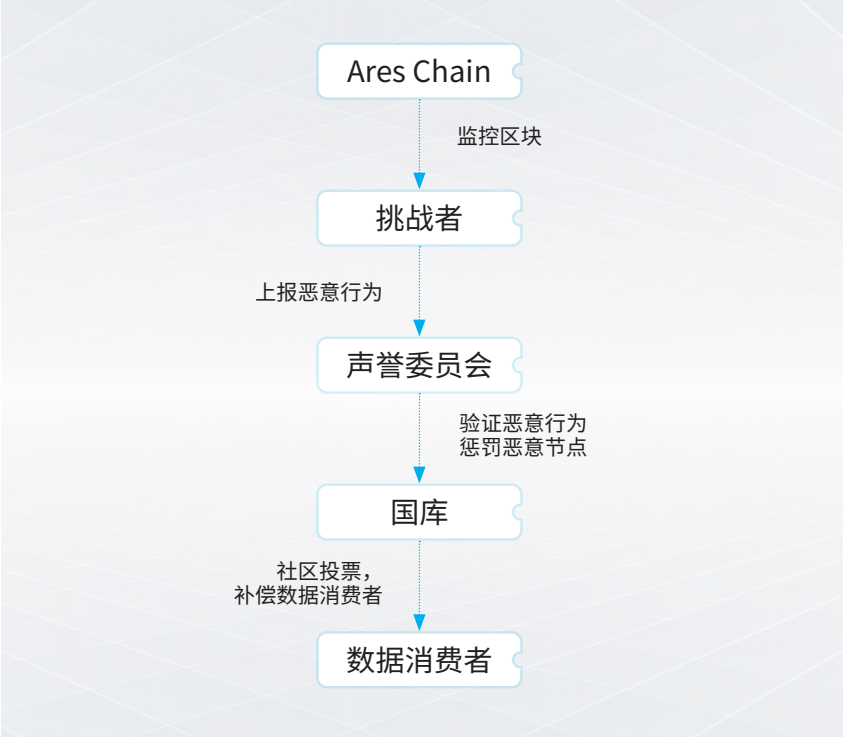
PBFT 的优点是收敛速度快、节省资源、具有理论上的安全界（理论上允许不超过 1/3 的恶意节点存在，即总节点数为 3k + 1，其中正常节点超过 2k + 1 个时，算法可以正常工作）。



议会成员是从聚合者或是持币人中进行选择的，里面有一个关于声誉值和持币量的映射比例。保证议会成员不会被持币人操纵。聚合者每提交一次正确的数据，其声誉价值就会增长，将会维护一个议会成员列表和等待队列，每一月会更新一次议会成员。议会只能批准或拒绝挑战者提交的欺诈证明。由于挑战是需要支付一定数量的 GAS 费，正常情况下议会是不需要工作的，只需要在验证者提出欺诈证明时处理争议，可以向理事会提交欺诈证据。如果委员会验证欺诈证明通过，它将奖励挑战者和惩罚聚合者，它的声誉将会下降。议会成员间处理挑战者争议时需要使用 BFT 算法来进行快速的确认，这里面会设置一个安全区间，如果聚合者把数据上链后，验证者在校验的时候发现了数据错误并在下一个块出块前广播了出去，此时挑战者获胜收到的奖励是最高的，后面依次递减，奖励会分配成议会成员，有一小部分分配成国库，当在数据错误时用来申请赔偿，这会只治理模块中讨论。

设计细节

如何解决争议?



Ares 网络的安全性由非常严格的带处罚的 POS 来保障，如果一个节点运营商被识别为攻击者的话，他所抵押的所有 Ares 通证将被分配成声誉委员会，挑战者，国库。

对应不同的数据市场，如 DEFI，为了防止恶意报价，Ares 设计了一个挑战机制，挑战者（任何 Ares 全节点）可以对报价提出异议。发起挑战需要支付少量的 ARES 通证，并广播到声誉委员会，如果声誉委员会 2/3 的节点审核为恶意行为，那么他将被标记为恶意节点，抵押的通证被冻结，节点抵押的通证被转移到声誉委员会，挑战者，国库。

但极端情况下，当数据消费者由于恶意节点上报数据而导致损失时，可以向国库发起提案申请补偿，然后通过社区投票，通过后通过国库给数据消费者进行补偿。

应用场景

去中心化金融

Ares 为去中心化的稳定币、交易所、借贷、保险、金融衍生品等去中心化金融提供高精度、实时、安全可靠的链外资产数据，方便的为 DeFi 项目的开发提供开箱即用的稳定基础设施。

去中心化身份

去中心化身份解决方案，提供安全、可控和便携的数字身份，为钱包供应商、验证供应商、DAPP 开发商和基础设施供应商、提供一站式解决方案。

物联网

通过 Ares Protocol，将物联网设备可信上链，解决物联网终端身份确认与数据确权的问题，保证链上数据与应用场景深度绑定，重构供应链、食品安全、溯源、智能家居行业。

预测市场

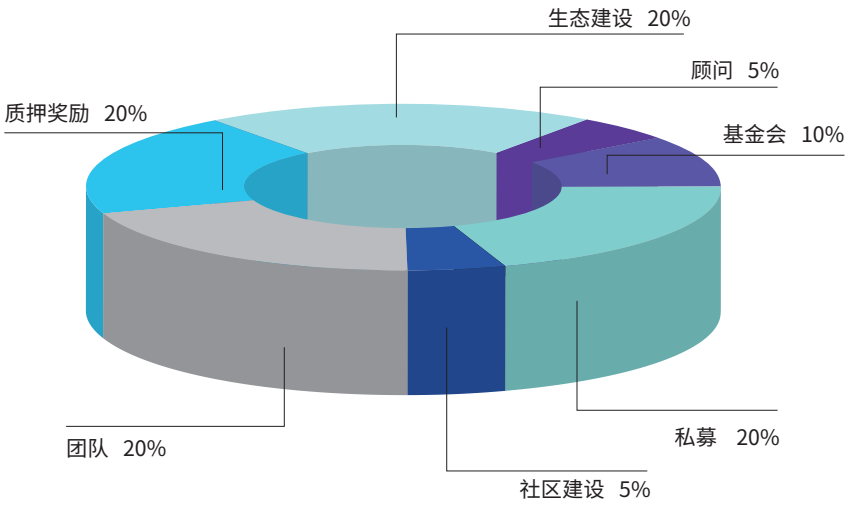
去中心化预测市场，如 Augur 和 Gnosis，利用人群的智慧来预测现实世界的结果，如总统选举和体育博彩结果。

博彩游戏

Ares Protocol 将提供链上可验证随机数，赋能区块链游戏和 NFTs 更多玩法。

经济模型

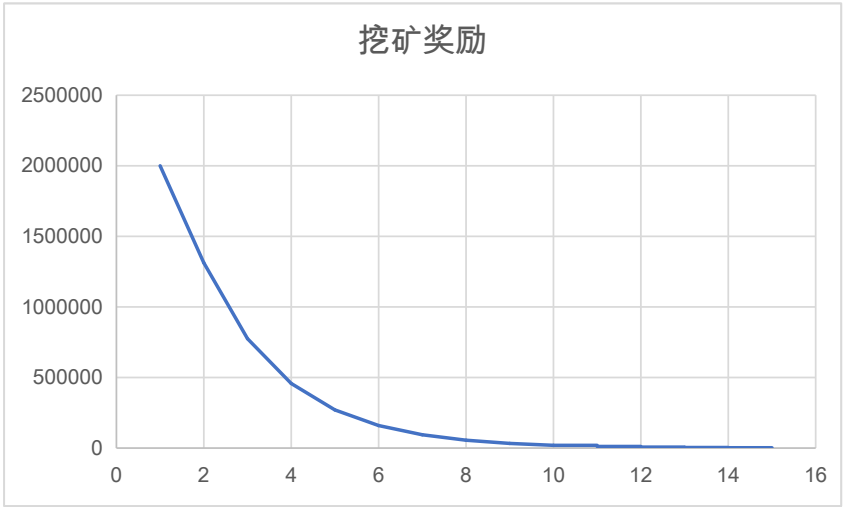
我们将发布 ARES 通证，用于激励系统中的各参与方，并通过社区治理，确保生态系统的增长和发展。原始发行量 10 亿枚。



节点抵押

任何第三方都可以通过抵押少量的 ARES 通证成为节点接入 Ares 网络，提供预言机服务，并享有挖矿奖励。

矿池初始通证总量占比 20%，每年从剩余矿池挖 10% 分给节点，挖矿奖励逐年减少但永远挖不完。



经济模型

交易费

每次的 oracle 请求，需要向节点支付处理费（gas）。其中 80% 归聚合者，20% 纳入国库。

ARES 通证会作为首个支持的费用通证，通证持有者也有投票治理权来决定哪些其他的代币也可以作为 Ares 网络里支持的费用通证，比如稳定币等。

仲裁

通过挑战者的争议来处罚聚合者或是挑战者，一部分费用会奖励给声誉委员会。

国库

Ares 网络的财政局，国库资金来源于：部分交易手续费、恶意节点的惩罚、质押产生的通胀等。国库资金用于奖励挑战者、弥补数据需求者的损失和生态建设等。

国库资金可以通过发起提案来使用，任何 Ares 网络的通证持有人都可以参与公投，通过民主治理模式让 Ares 网络健康发展。

社区治理

持有 ARES 通证的任何人享有治理权，可以通过投票进行协议升级和声誉委员会选举等。声誉委员会通过激励挑战者、惩罚作恶的节点，保证 Area 网络的安全。

团队介绍

keric CTO

6 年区块链开发经验，精通公链和联盟链开发，曾参与多个区块链项目开发工作，精通 go 和 rust 语言。是波卡早期的技术追随者之一。

Fred 核心开发

在多个技术系统包括硬件网络、软件网络和服务器端应用程序拥有超过 13 年的嵌入式网络开发经验。

Eric 核心开发

拥有 20 年 IT 技术开发经验，多年协议栈制定与开发经验，对大数据、区块链、量化机器人等研究颇深。

Daniel 核心开发

11 年物联网软件研发和管理工作经验，熟悉合约和 DAPP 研发。

scott 核心开发

7 年软件开发经验，全栈专家，熟练使用 /Java/Golang/node 等编程语言。2018 年开始从事区块链研发工作，熟悉 eos/eth 等。

团队介绍

Andy Ray 研究员

波卡早期投资者，10 年互联网创业经历，5 年区块链从业经历，精通二级市场，擅长经济模型设计，对分布式商业做过大量的研究和分析。

Alex

面向对象的设计和开发，多线程编程，实时和高性能软件，通信系统和协议方面专家。

毕业于伊朗大学和谢里夫理工大学，通讯工程专业毕业，（硕士）电气工程。

Feng Guo

奥克兰 Blockchainlabs（技术团队）开发人员

软件开发 / 集成方面拥有超过 15 年的经验。

Cherry Liang

5 年软件开发经验，熟悉 polkadot js ，曾于 2019 年 9 月参加 Polkaworld Cup Hackathon

World’s First Substrate Blockchain Developing Contest 并取得第二名。

路线图

2020 Q4

白皮书 1.0 发布

核心协议设计

WEB3 基金会 Grant 申请

基于 pallet 和 offchain work 的原型开发

2021 Q1

技术黄皮书发布

完善预言机用户的跨链交互

实现聚合者的随机选择和链上聚合

完善挑战者和仲裁议会模型

Token 上线二级市场

2021 Q2

完善经济模型设计

上线测试网

接入生态合作伙伴测试

2021 Q3

上线主网

开展多渠道服务合作

正式对接企业合作

生态马拉松开发者活动

总结

我们提出了一种去中心化的预言机解决方案，实现了预言机数据的上链和链上验证，为 Web3.0 时代的万链互联和数字经济提供安全可信的数据服务。在这个协议下，各参与方为了自身利益共同维护整个系统的安全。我们给出了这个架构的大体轮廓，包括生态系统的各个参与方、他们的经济激励模型和他们需要做的操作。我们会在未来迭代并提供更详尽的黄皮书来描述设计细节，请持续关注。

Ares Protocol


info@aresprotocol.com


https://t.me/Aresprotocols


https://twitter.com/AresProtocol


https://medium.com/@aresprotocol


https://github.com/aresprotocols