Ares Protocol

light paper

简介
Project Brief

Ares protocol 是波卡生态第一个去中心化跨链预言机服务协议，也是第一个实现数据链上验证的新一代预言机服务协议，并且首创为数据使用者因使用预言机数据遭受业务损失时开辟补偿通道。

作为连接现实世界和区块链网络的基础设施建设者，面向 WEB3.0 时代的宏大愿景，为万链互联和数字经济发展提供安全可信的数据服务。

特点
Project Features

◆ 开放性

只需质押少量 ARES 即可成为 ARES 网络的聚合者节点，以此来保证数据源的广泛性和分布式特性。

◆ 公平性

1.ARES 网络通过 VRF 的方式随机选择聚合者节点提供数据，有效的保证了节点之间的公平和去中心化的特点。任何节点都可能被随机选中为数据提供者。ARES 网络会为每一个节点累计信誉值，信誉值可作为申请治理委员会成员的重要参考指标。

2.ARES 网络首创补偿方案。当数据需求者使用 ARES 网络经过多层安全机制验证提供的数据而遭受业务损失时，可以向 ARES 国库发起提案申请一定的补偿，提案在治理委员会投票审议通过后，将补偿拨付给数据需求者。这给数据需求者又多加了一道服务保障。

特点
Project Features

◆ 安全性

1. 聚合多个数据源，有利于去除异常的数据，加权平均其他数据，当聚合链将价格提交到链上后会进行链上聚合来防止个别聚合者作恶，来切实保障数据的真实有效性。最明显的例子就是黑客通过人为蓄意影响 DEX 上资产价格，来影响预言机提供此价格给到 DEFI 借贷协议来达到套利目的时，ARES 网络早就在最开始聚合多个分布式数据源时将此异常价格去除，从而规避掉了这种攻击的可能性。

2. 当被选中的聚合者节点在提供数据后，任何节点都可以通过支付一定 GAS 来发起挑战，质疑其数据的真实有效性，仲裁委员会将会及时处理挑战者质疑。发起挑战成功将接受奖励，反之则接受惩罚损失 GAS。有效的规避掉了节点作恶的可能，也规避掉了挑战者节点作恶的可能，而且 ARES 网络的链上聚合功能，给数据源又多加了一层保障。这样在所有节点和网络的监督下，充分保证节点提供的数据是真实有效的。

◆ 实时性

ARES 通过数据链上验证和共享波卡网络的安全共识来保证数据需求方在发起请求后，能实时快速的接收到反馈结果。

优势
Project Advantages

ARES 网络如何做到数据的安全有效，
规避节点作恶和被攻击的问题?

1. 质押成本，质押一定的 ARES 代币数量（变量）方可成为 ARES 网络的候选节点

2. 候选节点需要完成 3 次（变量）测试任务且没有出现异常的情况下，方可申请成为正式节点

3. 当新增正式节点数在短时间内（比如 5 分钟，是个变量）超过已有正式节点总数的 1/3 时，所有新增正式节点将不会被信任，全部退回到候选节点队列，需要重新完成 3 次（变量）任务后方可再次申请成为正式节点

4. 当正式节点在提供第一次服务时就被判定为作恶或数据不被采纳时，我们会认为其作恶者的可能性非常大或者其服务资格不合格。其质押的 ARES 代币将会被罚没，并进入黑名单永不录用。

5. 每个节点在提供服务时都会积累相应的信誉值，信誉值越高，被选中的概率会越大。

优势
Project Advantages

6 成为正式节点后，如若被选中，其所提供的价格，其他任一节点都可以成为挑战者对其发起挑战，仲裁委员会来做最终的裁定。单一节点会从多个分布式数据源获取价格进行链下聚合后提交到链上

7 ARES 网络会链上聚合所有节点提供的价格，去掉最高和最低后加权平均来作为比对值，在允许偏差范围内方可被采纳。

8 ARES 网络会启用备用数据源来作为比对值参考。会通过链下工作机聚合前十交易所的资产价格数据，将最高和最低的价格定性为异常数据，一旦被选中节点提供的价格与异常数据相同，则该价格首先就不会被采纳，网络会重新选择节点去提供价格服务

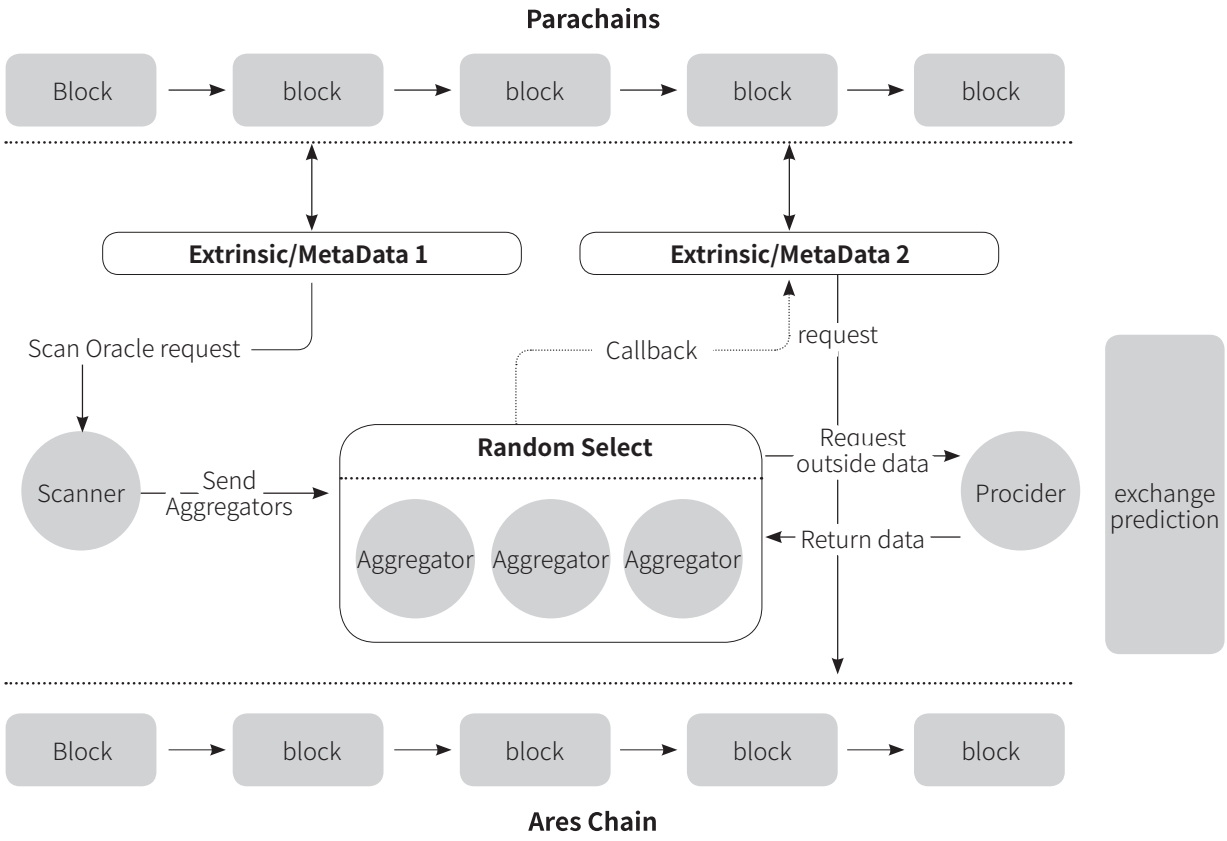
9 ARES 网络会截取某一历史时段的数据作为比对值参考，一旦提供的价格与历史价格出入很大，也不会被采纳。

技术架构
Technical Framework

Ares 的参与方

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

设计细节
Design Details

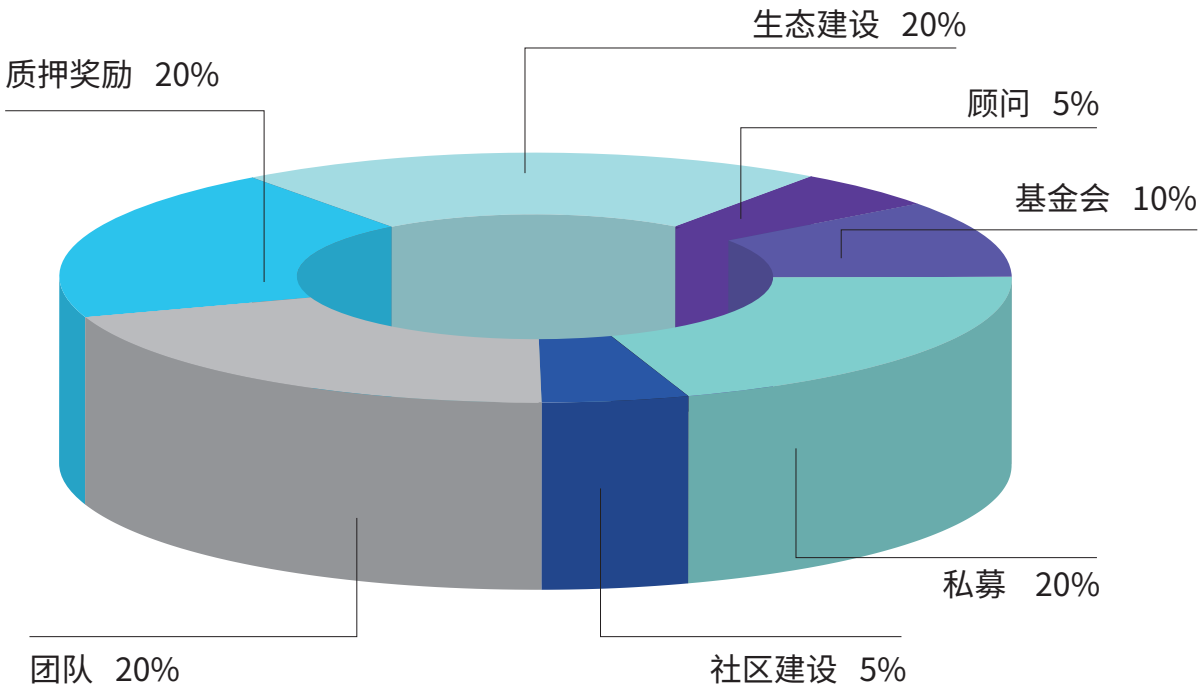


Ares Protocol 是基于 Substrate 构建的，作为平行链 / 平行线程的方式接入波卡生态。具体的流程如下：

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。

经济模型
Economic Model

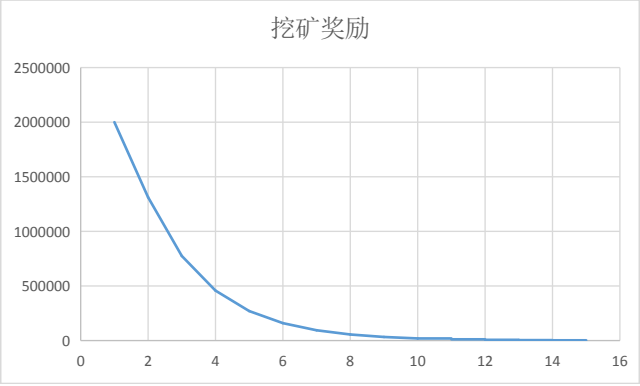
Ares Protocol 的代币名称是 ARES，发行总量 10 亿，代币分配如下：



◆ 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
Economic Model

◆ 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
Team

◆ 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
Team

◆ 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
Road Map

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

关注我们


info@aresprotocol.com


https://t.me/Aresprotocols


https://twitter.com/AresProtocol


https://medium.com/@aresprotocol


https://github.com/aresprotocols

Ares Protocol

https://aresprotocol.com/