Ares Protocol - WEB3.0

时代下的去中心化跨链预言机

project supported by
web3 foundation
grants program

Ares Protocol

为何需要预言机

Ares Protocol

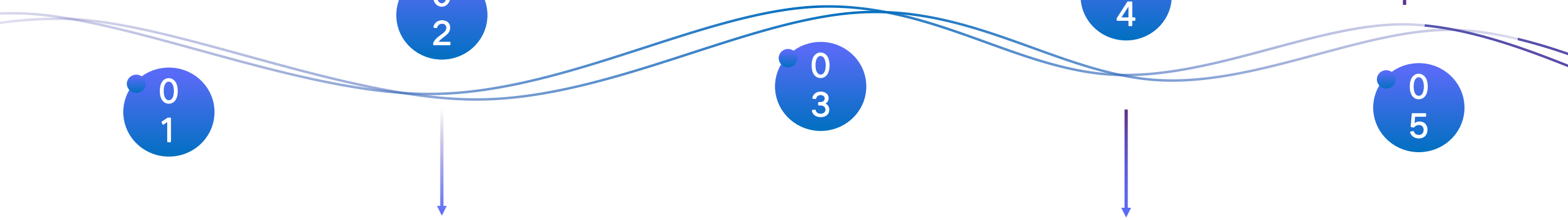
01 区块链是状态机
由交易触发

02 节点数据同步验证

03 无法访问网络
数据在不同时刻存在差异

04 连接智能合约与区块链
外部世界的中间件

05 offchain worker
是访问网络的工具



背景：传统Oracle

Ares Protocol

- 以太坊平台：ChainLink
- POS Validator：DOS，Band
- 与DeFi深度绑定

ALL | LENDING | DEXES | DERIVATIVES | PAYMENTS | ASSETS

DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
🏆 1.	Maker	Ethereum	Lending	$4.18B	-1.69%
🥈 2.	Aave	Ethereum	Lending	$3.06B	-0.82%
🥉 3.	Uniswap	Ethereum	DEXes	$2.75B	-0.84%
4.	Compound	Ethereum	Lending	$2.74B	1.02%
5.	Curve Finance	Ethereum	DEXes	$1.93B	-2.10%
6.	SushiSwap	Ethereum	DEXes	$1.74B	2.89%
7.	Synthetix	Ethereum	Derivatives	$1.69B	-27.94%
8.	Balancer	Ethereum	DEXes	$771.9M	-1.84%
9.	Badger DAO	Ethereum	Assets	$694.1M	-1.21%
10.	RenVM	Ethereum	Assets	$575.6M	-2.81%

Ares Protocol 是什么

Ares Protocol

开放性

- 无需KYC即可质押成为报价节点

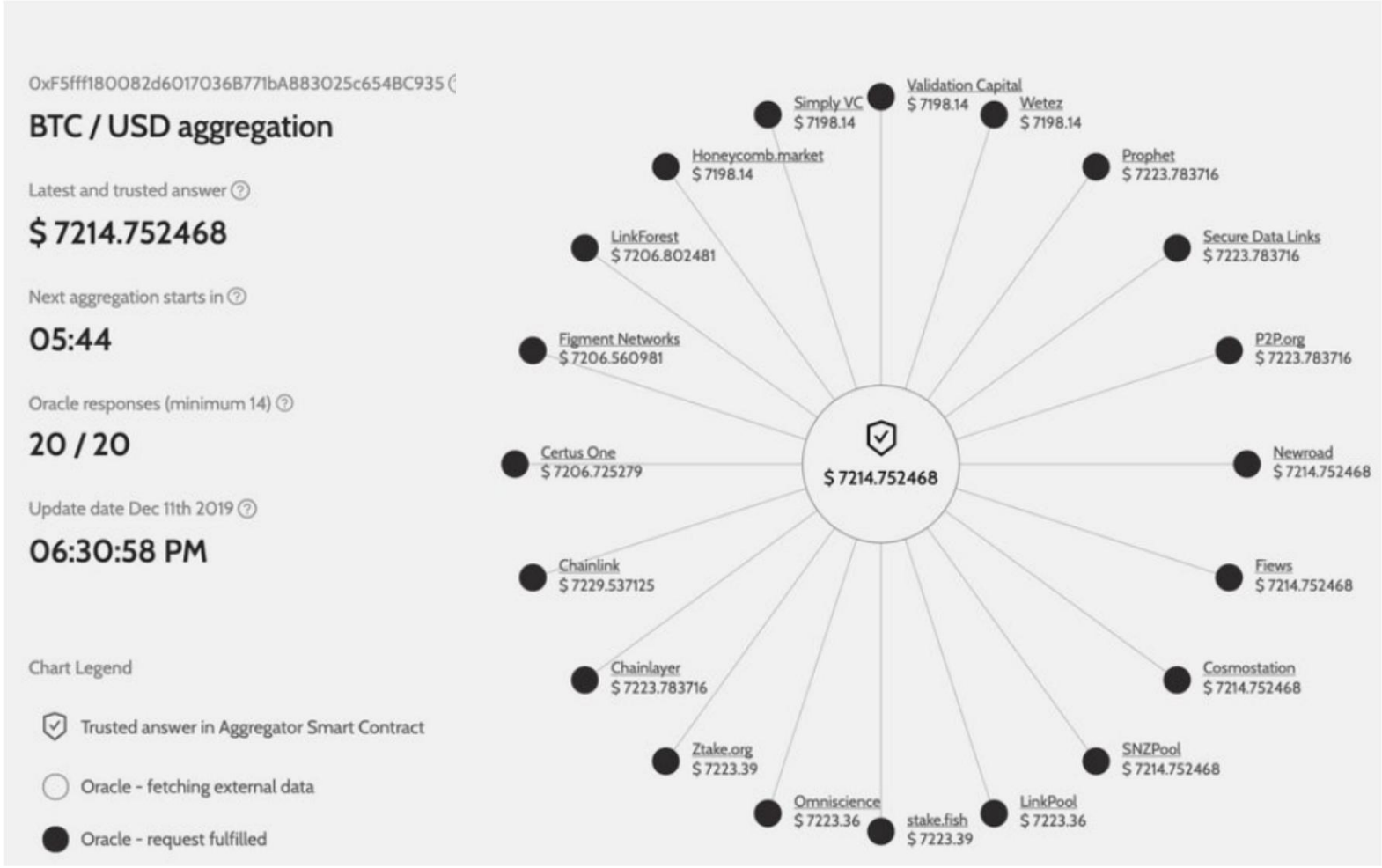
安全性

- 分布式数据源

  Compound清算事件中，单一Coinbase pro喂价
- 随机选择聚合者 -BABE真随机
- 链上聚合和数据模型
- 链上验证

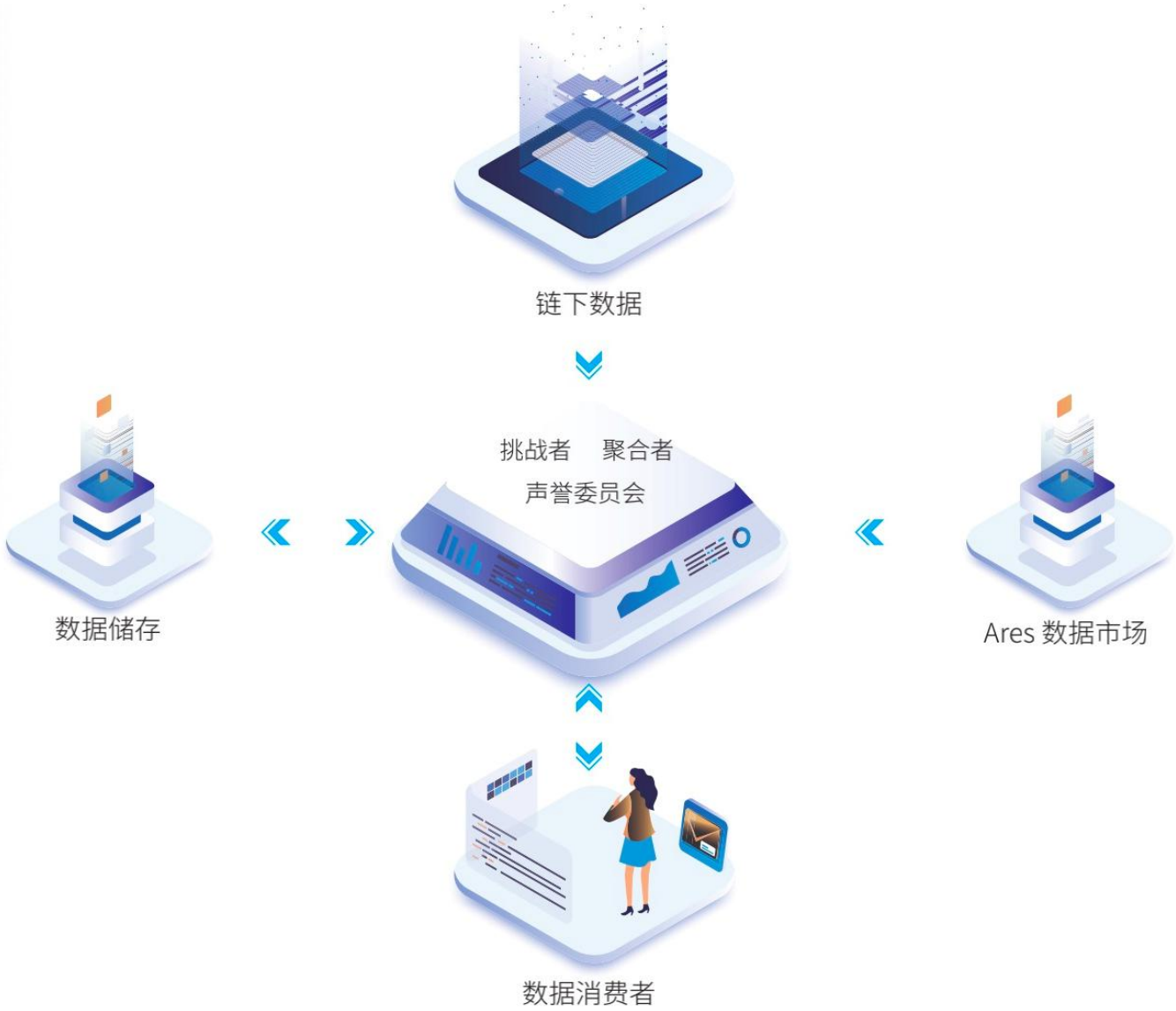
实时性

- POS共识 6s出块 20区块链上聚合只需2分钟



Ares Protocol 协议架构

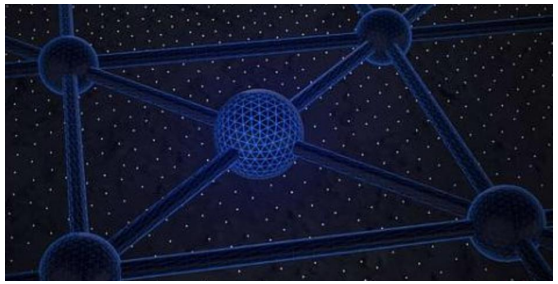
Ares Protocol



什么是链上验证

Ares Protocol

- **链上验证：对链上数据做最终敲定**
- 聚合者只能把数据提交到链上，不能保证数据的真实可信



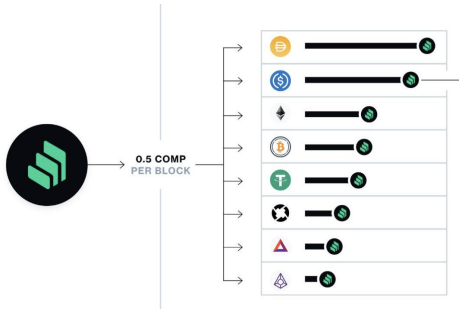
挑战者/提案人

实时处理/异步投票

仲裁委员会最终确认

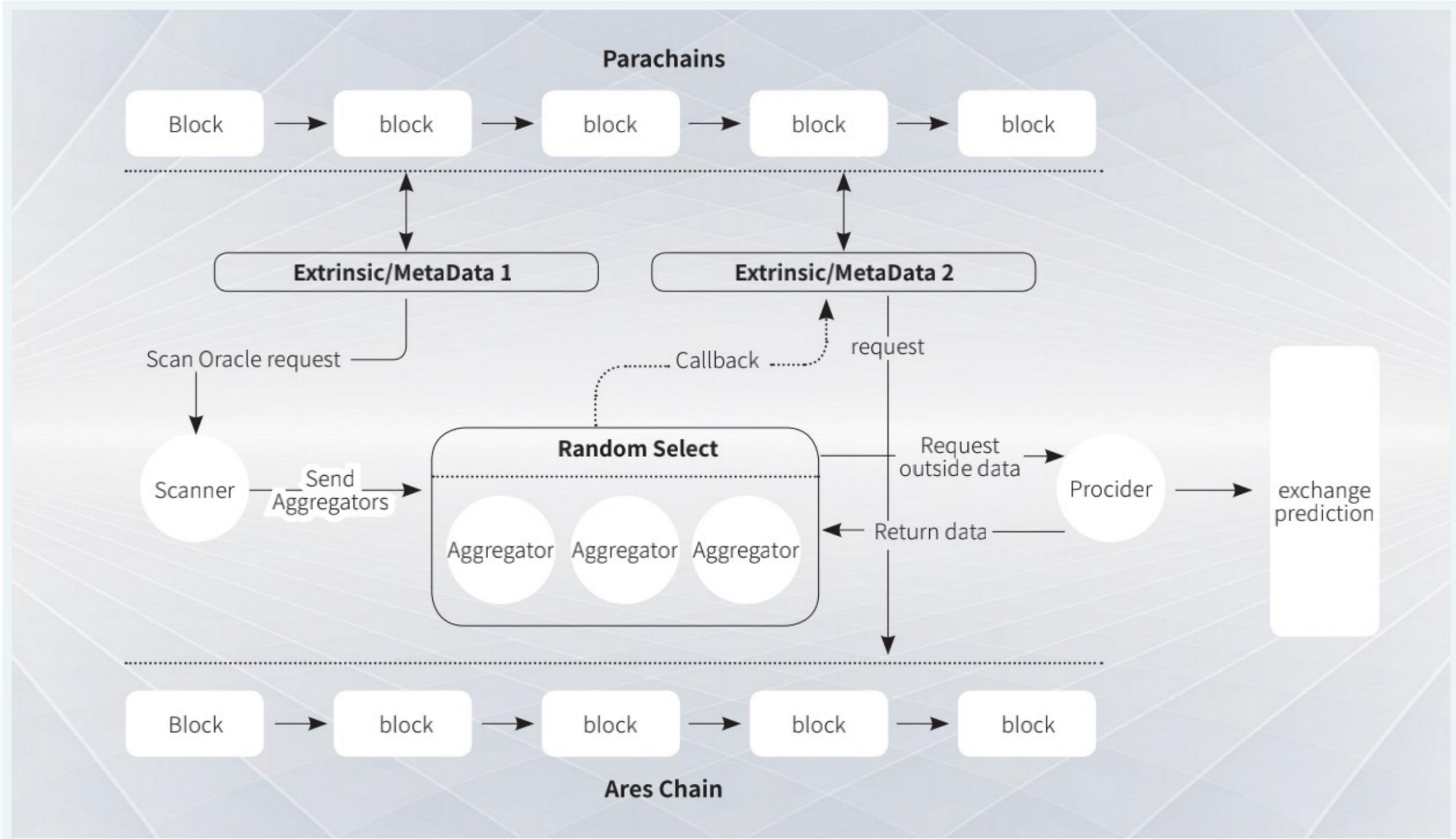
Ares Protocol 使用场景

Ares Protocol

			Nexus Mutual
DeFi	稳定币	合成资产	保险和预测市场
• 获取价格 • 资产清算 • 流动性收益	• 超额抵押	• 股票 • 债券 • 传统资产	• 航班信息 • 索赔

Ares Protocol 平行链交互

Ares Protocol



Ares Protocol 基本流程

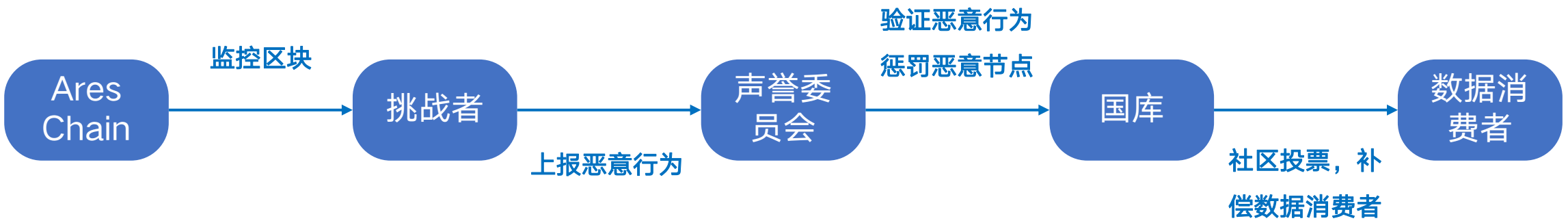
Ares Protocol

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

Ares Protocol 链上验证

Ares Protocol



Ares Protocol 技术规划

Ares Protocol

平行链Pallet

Ares链随机聚合

挑战模型

波卡生态外SDK

Grants milestone

M1： 基于Substrate创建Oracle模块（Pallet）

- 解析请求事件提交价格
- offchain-worker获取ares数据源获取价格
- 自持多资产和价格链上聚合
- 一个end-to-end的演示视频和教程，关于请求，解析，价格聚合

M2： 基于Substrate创建Ares的runtime业务逻辑

- Ares在Polkadot生态中可用
- 平行链离线交易触发Ares chain提供数据和解析数据
- Babe模块添加offchain worker获取价格和价格聚合
- 创建一个教程平行链请求数据，通过跨链模块触发ares chain提供数据
- 一个演示视频，展示平行链和Ares链的跨链交互

M3： 实现Ares 的链上验证

- 实现挑战者模型设计
- 仲裁委员会链上审核投票
- 添加对应polkadot js模版，可查看挑战结果
- 一个演示视频，展示作恶者如何被仲裁委员会惩罚

Ares Protocol 插槽拍卖

Ares Protocol 插槽拍卖

Ares Protocol

Transaction 0x86f5946d01dd32f07943a8c68e4131977a2487a318eef4d8191cd6815943340f

Block	429427
Timestamp	Jan 18, 2021, 6:13:18 PM
Transaction Index	2
Transaction Hash	0x86f5946d01dd32f07943a8c68e4131977a2487a318eef4d8191cd6815943340f
Module	proposeparachain
Call	propose_parachain
Description	Propose a new parachain This requires: - `para_id`: The id of the parachain. - `name`: The name of the parachain. - `validation_function`: The wasm runti...
Address	5Et7jm5iTFd48MX5km3P3PtbPBNp1noPg9T9Eufcs4gEvQMs 5Et7jm5iTFd48MX5km3P3PtbPBNp1noPg9T9Eufcs4gEvQMs
Nonce	3
Signature	0x82750974778321cc90cfef866297ffd92e8f8fd6b9494ad177ee594f24b2d9179d1f2fe9d76d0c9278562511873bd0b89babe07b46217b8f2ce7dc25129ad382
Result	✔

Parameters

Para_id	8686
Name	ARES
Validation_code	Download binary
Genesis_head	0x0000000000000000000000000000000000000000000000000000000000000005f8d97ab14aa81558789b46a232030def9fab19549eab3ad7b32dddfa703f9c903170a2e7597b7b7e3d84
Validators	0: 0x7ca164245d48ed5035eb6fecd7557ec58ac8869c54855c6663b8a3439960d611 1: 0x5894738c512a8c4b38be5d7677749722f8df750961933412b0eccbe4c48f4c2e
Balance	1000000000000000

Ares Protocol 路线图

Ares Protocol

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

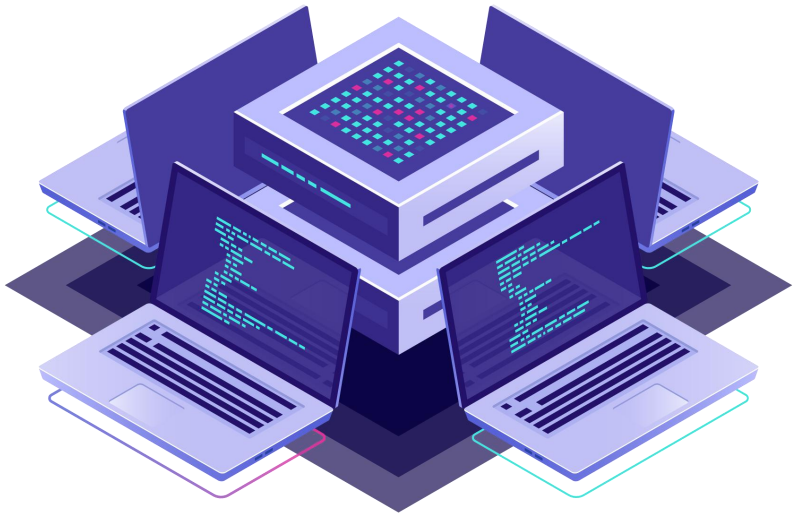
- 技术黄皮书发布
- 完善预言机用户的跨链交互
- 实现聚合者的随机选择和链上聚合
- 完善挑战者和仲裁议会模型
- Token上线二级市场

2020 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



Ares Protocol

Ares Protocol

在以下链接可以找到我们

官网： http://www.aresprotocol.com/

Github: https://github.com/aresprotocols

Telegram: https://t.me/Aresprotocols

Twitter: https://twitter.com/AresProtocol

期待未来

更多会面！