Phala Network：6年老项目，转型人工智能路由开新花？

### 引言

Phala Network成立于2018年，项目成立之初Phala Network将自身定位于隐私计算赛道，将智能合约执行环境与 TEE相结合，实现了安全可靠的智能合约执行。同时Phala Network还提供了完整的隐私保护机制，确保用户的数据掌控在用户自己的手中。在2023年的时候，因为美股带动了市场上以AI为主的风口，所以Phala Network当时紧跟AI风口，又做起了人工智能代理，并且又紧跟模块化的理念，将自身打造成为了人工智能的执行层。

### 项目基本信息

#### 基础信息

网站：https://phala.network/

推特：https://twitter.com/PhalaNetwork，粉丝12.2万

TG：https://t.me/phalanetwork

Discord：https://discord.com/invite/phala-network

白皮书:https://docs.phala.network/

上线时间：代币于2020年上线

#### 项目团队

核心团队

Marvin Tong：创始人&CEO。毕业于中国传媒大学，获得了硕士学位，毕业之后一直在腾讯、滴滴等公司做产品经理的工作。

Hang Yin: 联合创始人&首席技术开发。毕业于中国复旦大学。之前是 Google 搜索 ML 相关领域的专家，中国波卡大使之一，Bitcoin Gold 的创始人。

Zhe Wang: 联合创始人&首席运营官。毕业于中国华科大学，获得了硕士学位，是华科计算机硬件实验室的专家，Bitcoin Gold，小嘿科技和哈哈零售的CTO&CEO。

Jun jiang: 联合创始人&CTO。曾经是RubyChina的站长。前KnewOne的CTO，前大疆软件架构师。

顾问团队

Shun Fan Zhou: Phala Network 白皮书作者之一复日大学系统软件与安全实验室博士，曾在国际顶级安全会议USENIX Security 上发表对于以大坊生态中攻击交易与防御手段的研究，并协作发表多篇国际顶级安全会议论文。

Sandro Gorduladze：HASH CIB的天使投资人和合伙人。Sandro在HASH设立了研究部门，该部门因其深入的报告而声名大噪。加入HASH之前，Sandro曾在俄罗斯普华永道工作，为TMT行业的公司提供税务咨询。

Konstantin Shamruk：法国图卢兹大学经济学博士。主导了Phala Network经济设计的博奔论分析工作。

Jonas Gehrlein：Web3 基金会研究科学家。他在Web3基金会负责研究 Polkadot生态系统的经济问题。加入W3F之前，Jonas获得了伯尔尼大学的行为和实验经济学博士学位，在那里他研究了市场和组织中的人类行为。在此之前，他在康斯坦茨大学获得了定量经济学的硕士学位。

Zo Meckbach: Polkadot高级大使，研究者和Web3 和网络安全的倡导者。她目前是MH-IT& Service GmbH的COO，在加入MH-IT之前曾担任谷歌的应用分析职位。

### 融资情况：

Phala Network已通过一轮融资筹集约1000万美元。

种子轮

2020年7月，Candaq Group、IOSG Ventures、SNZ、Incuba Alpha Group、nfiChain、Exoplanet Capital 和Blue Mountain Labs投资此轮，金额为1000万美元。

### 开发实力

2018年Phala Network立项，由创始人Marvin Tong创立。项目发展的关键事件如表所示：



从Phala Network的项目发展路线图来看，Phala Network团队在项目的各个关键时间点都能够做到准时的完成项目预定计划，可以看出以Marvin Tong和Hang Yin领衔的技术开发团队的实力是非常强的，虽然Phala Network在进军了AI赛道之后有了更广阔的发展前景，但是其面临的技术挑战会变得更大，对技术开发团队的要求会变得更高。

### 技术特点

Phala Network是一个基于波卡生态的隐私计算基础设施，旨在通过可信执行环境（TEE）技术、云计算服务和跨链数据保密层，来实现数据的机密性和隐私保护。同时Phala Network采用人工智能协处理器，为在应用层集成加密和人工智能提供了安全、可验证的计算解决方案。

可以简单的理解为Phala Network在以原先隐私计算基础设施之上增加了一个人工智能协处理器，从而可以在Phala Network上部署人工智能代理合约，Phala Network成为了Web3人工智能的执行层。Phala Network通过TEE技术对其进行了隐私保护，现通过Phala Network的人工智能代理合约可以访问顶级 LLMs，并且控制权源自链上编写的智能合约。



Phala Network在添加了人工智能代理合约之前，Phala Network的主要技术特点就是通过多种技术手段实现数据的机密性和隐私保护。首先，Phala Network采用硬件隐私计算技术，特别是可信执行环境（TEE），来确保数据在计算过程中的机密性和完整性。在TEE中运行的所有计算都保证了程序执行的正确性以及数据的安全性，同时Phala Network还结合了零知识证明技术，这种技术可以实现隐私交易，使得智能合约的数据不必公开，从而保护用户的隐私。通过这种方式，Phala Network能够提供通用且易于使用的保密智能合约，支持零信任云服务。

其中重点的就是可信执行环境（TEE）和多层密钥轮换制度。

可信执行环境（TEE）：信任执行环境（TEE）是一种关注隐私的技术，它将节点的代码执行和操作与计算机处理器的主操作系统隔离开。Phala Network使用英特尔的软件防护扩展（SGX）进行TEE处理。这种系统确保即使是有物理访问权限的个人，比如Phala Network的操作员或恶意第三方，也无法查看节点的状态或操纵节点处理的数据。通常，信任执行环境被用来代替零知识证明（ZKPs）。在Phala Network中，TEE不仅用于保护数据的机密性和完整性，还支持复杂的计算任务。比如通过将智能合约的执行转移到由TEE支持的链下安全工作者身上，Phala Network能够充分利用单个工作者的计算能力，同时无需担心数据泄露或被篡改的风险。

多层密钥轮换制度：Phala Network拥有一组名为"守门员"的特殊工作节点，其主要任务是确保计算的安全性。在Phala Network中，Worker节点没有权限随时退出网络，因此任务需要部署到具有相同密钥的冗余Worker节点上，以确保可以访问加密的输入、输出和程序状态。守门员节点负责管理加密密钥，并将机密动态分配给工作节点，从而确保数据的安全性和完整性。同时Phala Network采用了全面的密钥轮换机制，以确保其合约的私密性和系统的整体安全性。这个过程根据选举规则定期更新主密钥。在新的周期新守门员经选举得出，并通过安全密钥交换协议生成新的主密钥。新密钥用于重新加密守门员状态，然后在新守门员之间分发和确认。在此过渡期间，矿工与守门员之间的通信会暂时中断，以保持一致性和安全性。只有在密钥轮换完成后，通信才会恢复，延迟时间为两次链上确认。除了轮换主密钥外，Phala Network还定期更新集群密钥和合约密钥以增强安全性。

Phala Network在添加了人工智能代理合约之后，Phala Network的主要业务就由原先的隐私计算基础设施转变为了Web3人工智能的执行层，其原先的隐私计算基础设施变为了现在Web3人工智能的执行层的基础，现有的人工智能代理合约就运营在原先的隐私计算基础之上。

人工智能代理合约：人工智能代理合约是一项用户用于构建智能合约的工具，用户可以使用它来控制能够在区块链上或链下运行的人工智能代理。这些人工智能代理的代码由TypeScript/JavaScript编写，并在Phala Network的节点中执行，并且它们能够从外部API中汇总数据，并插入自定义的人工智能代理。人工智能代理利用Phala Network的无信任云计算基础设施进行链外保密程序。在技术层面上，人工智能代理合约在工作节点内的TEE上运行，这些工作节点由Phala Network负责。守门员工作节点子集负责管理密钥，以确保网络安全。这些合约为开发者提供了强大的工具，使他们能够利用人工智能代理来执行各种任务，并且由于其运行环境的安全性和隐私性，在处理敏感数据时也能够得到保障。人工智能代理合约的发展为区块链技术的应用提供了新的可能性，同时也为开发者们带来了更多的创新空间。

pRuntime：工作节点通过将人工智能代理合约托管在节点的TEE中，在TEE保护工作负载的代码完整性和隐私，确保合约在执行过程中不受到恶意攻击和篡改的同时，为网络提供了强大的计算能力。而pRuntime（Phala Runtime）是一个运行在TEE内部的程序，他是Phala Network的工作节点的核心组件，pRuntime 负责接收并运行来自区块链的计算任务，确保计算的防篡改性和安全性。

综上所述，Phala Network通过引入人工智能代理合约，将人工智能代理变的像智能合约一样简单的运行，并且使得人工智能代理由智能合约管理，让人工智能代理能够随时的接受管理和访问控制。并且各个人工智能代理之间可以自由地相互调用，形成复杂的应用程序，并且这一切的操作都在TEE中运行，保证了代码的完整性和隐私。使得Phala Network在转变成为Web3人工智能的执行层也充分的利用了之前隐私计算基础设施的优势。

### 与同赛道项目相比的创新

Phala Network在引入了人工智能协处理器之后，虽然Phala Network的项目底层运行逻辑并没有发生改变，但是项目的主要叙事已经由原先的隐私计算基础设施赛道转变为了AI赛道中的细分赛道：算法赛道，其竞争对手也变为了Morpheus、QnA3.AI、Fetch.AI、SingularityNet、ChainGPT等项目。



超强的隐私性：得益于Phala Network在转型AI赛道之前是从事隐私计算业务，从而其具备了先天的隐私优势。Phala Network采用了硬件隐私计算技术，特别TEE，来确保数据在计算过程中的机密性和完整性。TEE中的所有计算都保证了程序执行的正确性和数据的安全性。同时还结合了零知识证明技术，实现隐私交易，保护智能合约数据不必公开，从而维护用户隐私。通过这种方式，Phala Network为用户提供安全可靠的隐私计算解决方案，为区块链应用的隐私保护提供坚实的技术支持。

强大的功能：Phala Network引入了人工智能代理合约使其在人工智能代理赛道中占有了绝对的优势，人工智能代理合约，将人工智能代理变的像智能合约一样简单的运行，并且使得人工智能代理由智能合约管理，让人工智能代理能够随时的接受管理和访问控制，同时使EVM智能合约能够在链外扩展其功能，使得人工智能代理的部署和工作效率得到了极大的提升。从而做到了以智能合约为中心的人工智能代理。

丰富的集成：Phala Network通过对人工智能代理合约的使用，使得其能够汇总来自外部 API 的数据，并插入自定义AI Agent。同时消除了访问去中心化应用程序的学习困难。从而可以大规模轻松的接入外部的优秀AI工具和项目，比如：OpenAI、LangChain、GPT4等。

更广泛的应用：因为人工智能代理合约的使用，使得Phala Network的人工智能代理的部署非常简单并且部署的领域也非常广泛，用户可以根据自己的喜好和需求将自己制作的人工智能代理链接至Social、Defi或者Dao，来提高自己工作、生活中的效率。

综上所述，Phala Network凭借其优越的性能，将人工智能代理的部署使用变为了一件非常简单的事情，在替用户解决了操作和部署简易性的同时也解决了部分用户对隐私性的顾虑，使得Phala Network在AI赛道的竞争中获得了非常大的优势。

### 项目模型

#### 业务模型

由于Phala Network现在的基本叙事已经由隐私计算转变为了AI赛道，所以Phala Network经济模型由四者角色组成：矿工，质押用户，使用人工智能代理合约的用户，使用隐私计算的用户。

矿工：Phala Network的矿工是网络算力的提供者，矿工将自身能够控制的电脑CPU算力提供给Phala Network，是Phala Network中唯一负责实际计算的人，他们是整个网络存在的基础，其提供的算力越多，就可以获得越丰厚的报酬。

质押用户：因为Phala Network的挖矿设计中需要矿工不仅仅提供算力，为了防止矿工作恶从而必须要质押一定数量的PHA代币作为保证金，但是有的矿工只愿意提供算力不想提供额外的代币质押，从而质押用户就可以分为两种：Stakepool和Vault。其中Stakepool只是属于提供算力并且愿意提供质押代币的矿工或者将自身所持有的PHA代币直接提供给Stakepool，而持币用户如果不想将代币直接质押给某个Stakepool，还可以将代币放入Vault，由Vault根据每个Stakepool的业绩而进行质押。

使用人工智能代理合约的用户：使用人工智能代理合约的用户现在是Phala Network项目中的主要使用者，他们在 Phala Network上运行工智能代理合约的同时需要向Phala Network支付用费用，费用是通过PHA代币的形式支付，也是Phala Network的主要收入来源之一。

使用隐私计算的用户：Phala Network凭借其优秀的隐私计算业务仍然会吸引一些对隐私计算有真实需求的用户。使用隐私计算的用户支付的费用也是矿工和Phala Network主要收入来源之一。

从以上分析可以看出Phala Network的收入是：

使用人工智能代理合约的用户支付的使用费

使用隐私计算的用户支付的使用费

### 代币模型

根据白皮书显示：PHA总量为10亿枚，现在流通量为7.383亿枚，流通率为73.83%。总体的代币分配如下：



#### 代币的赋能：

根据白皮书显示，PHA在Phala Network中的用途如下：

矿工奖励：网络中的矿工获得用于挖掘新区块的PHA代币，要求他们提供算力。

使用费用：使用人工智能代理合约和使用隐私计算的用户用PHA代币缴纳费用。

参与治理：质押PHA代币后可以参与PhalaDAO的治理。

参与质押：Phala Network的挖矿设计中需要矿工不仅仅提供算力，为了防止矿工作恶从而必须要质押一定数量的PHA代币作为保证金。

#### PHA的价值判定

根据白皮书介绍，在Phala Network网络中，对PHA代币的赋能中规中矩，其中加入了质押机制，从而变相的增加了对PHA代币锁定来增加项目价值这一个关键点，现在PHA代币的流通率达到了73.83%，在流通率的角度来看，现在PHA的流通率稍高，但是仍处在接近三分之一的代币没有被开发的阶段，所以在今后项目发展的过程中对PHA代币更多的价值增加是来自Phala Network项目的本身价值，也就是市场用户对使用人工智能代理合约的使用程度，如果使用较高，那么随着代币价格的上升，使得矿工的收益也越来越高，从而导致更多的矿工进入挖矿锁定更多的代币来减少代币的流通率，以此来形成一个正向的飞轮。但是PHA代币不存在集中销毁或者定期销毁的场景，使其代币经济学中不足的一点。如果Phala Network的业务没有形成良好的发展，那么其代币价格也不会随之上涨。

### 代币价格表现



根据Coingecko统计数据，PHA自2023年7月近一年以来，价格已经上涨超过4倍（最低点0.0816美元，最高点0.3465美元），主要交易场所为Binance，OKX，HTX等一线交易所，今年的上涨主要是因为占了AI赛道发展的红利。

#### 市值

PHA现币价为0.126美元，现流通量为738,334,838枚，市值为：9343万美元。

#### FDV

PHA现币价为0.126美元，总流通量为10亿枚，市值为：1.2654亿美元。

#### 日均交易量：

PHA日均交易量大概在566万美元上下。



PHA的日交易量566万美元，其流通市值约为1.2654亿美元，虽然换手率只有4.47%，属于偏低水平，但是更多的是因为目前市场大的环境比较低迷，最近受Mtgox事件影响，导致用户们大多处于观望状态。

#### 前十名代币持有地址



由图可以看出，PHA持有地址前十名总共占有92.19%。

#### PHA持币人数



可以看出虽然近一年中持有PHA代币的人数一直在稳步增加。

#### 日活账户



可以看出Phala Network的日活账户一年来一直在持续增加。

#### 质押情况



从图中我们可以看出PHA的循环量应该是8.4727亿枚，但是实际流通量是7.3833亿枚，可以得出其实际的质押量应该是1.0894亿枚。

### 项目风险

虽然Phala Network在推出了人工智能代理合约之后将其项目的赛道改变到了AI赛道上，有利于其项目的发展和币价的增长，但是其面临的技术挑战也是成倍的增加，尤其是Phala Network在隐私计算的基础之上采用了比较复杂的人工智能代理合约，并且今后会不断的接入新的AI Agents，对其技术团队也是产生了不小的挑战，所以今后必定会产生一些系统问题，这就要看Phala Network团队的解决问题的能力以及Phala Network的人工智能代理合约是否像宣传的那样功能强大，从而现在来看不确定性因素较多。

### 总结

Phala Network通过引入人工智能代理合约，使人工智能代理变得与智能合约一样容易运行，并由智能合约进行管理，实现了对人工智能代理的实时管理和访问控制。不同的人工智能代理可以自由互相调用，构建复杂的应用程序，并且所有操作在可信执行环境（TEE）中进行，以确保代码的完整性和隐私性。这使得Phala Network可以充分利用之前的隐私计算基础设施优势，将其转变为Web3人工智能执行层。这一创新为人工智能应用程序的安全性和隐私保护提供了全新解决方案，并为智能合约与区块链技术的融合提供了有力支持。

Phala Network在推出人工智能代理合约后，将项目定位于AI赛道，这对项目发展和币价增长都有利。然而，随之而来的技术挑战也成倍增加。特别是Phala Network在隐私计算基础上采用了复杂的人工智能代理合约，未来还将不断接入新的AI Agents，对技术团队提出了巨大挑战。

总而言之，Phala Network项目本身通过对可信执行环境（TEE）的引入，使其在隐私计算基础设施赛道中占据了一定的优势。并且现在又有人工智能代理合约的加持，如果其能够按照项目之后的规划如期进行，那Phala Network在AI赛道中也会占有一定的优势。

### 参考资料

Understanding Phala Network: A Comprehensive Overview

Phala Network白皮书

波卡生态中的 DePin 项目，Phala Network 能杀出一片重围吗？