Phala经济白皮书

Marvin Tong, Hang Yin

1. 项目简介

Phala Network采用了**TEE-区块链融合架构**（TEE-Blockchain Hybrid Architecture）实现了**保密智能合约**。

保密智能合约运行在CPU内的特殊安全区（Enclave），合约的执行与外界完全隔离，保证了数据的保密性。同时，结合区块链解决了TEE的功能性、安全性与易用性问题，让TEE变得真正可用。具体而言：

- 引入分层与事件溯源（Layered Design and Event Sourcing），让合约与其他合约、甚至是外部区块链之间得以互操作
- 分层设计保证了安全性，矿工停机对网络不会造成影响
- 任何人只要拥有符合标准搭载TEE的CPU都可以成为矿工，区块链负责验证矿工的每次执行，用户无需特殊硬件就可以安全地使用保密合约

此外，Phala Network基于Substrate开发，可以提供跨链保密合约支持。最终各链可以共享Phala基础设施，使整个区块链社区获利。

1.1 经济设计目标

> 基于团队对web3.0未来渗透率的信仰，我们坚定地认为区块链落地必须做到「不依赖强大信任中介也能保护商业机密」。因此，可信计算作为几年内解决此类需求的唯一可行的技术方案，市场上限难以预估。
>
> 传统TEE解决方案具有无法互操作的先天劣势。因为智能合约需要可组合性才能产生规模效应的价值，因此TEE网络提供的计算和数据交换服务就是我们团队长期构建的服务价值。

愿景：成为世界级的可信计算协议

2. PHA经济模型

PHA的初始总量为10亿，代币分配将在 Phala Network 主网启动后完成分发。主网启动前，将通过ERC20和测试网活动完成PHA的分发。

2.1 代币功能

- **获取可信计算资源**：所有 Phala 可信计算的算力购买、链上资源、链下数据存储，均使用PHA结算
- **数据交易协议费用**：Phala 以合约的形式提供了一个标准化的数据收集、分析、交易协议，作为数据交易基础设施。协议实现了买、卖各方保密且资产可信的生态。PHA是数据交易的法定结算货币，并参与市场调节

- **安全性保障**：Phala 网络需要 Gatekeeper 作为安全保障节点时刻在线，而竞选 Gatekeeper 需要抵押PHA作为保证金。若 Gatekeeper 作恶，将被罚没保障金
- **社区治理**：超过一定阈值的PHA代币持有者有权参与Phala DAO的治理和投票
- **支付其他服务**：Phala 还将被用于其生态下的其他应用或服务结算，如：Web3 Analytics、为其他公链提供保密智能合约的跨链转接桥等。

2.2 Phala Network 捕获的价值

PHA 捕获了网络中的资源以及数据交易价值。

其中 Phala 主网上每一个交易都需要消耗资源，资源的类型主要为以下三大类：

- 可信计算资源
- 链上计算、存储资源
- 链下存储资源

数据交易是 Phala Network 的核心能力，PHA 通过一系列标准化合约捕获数据价值。

2.2.1 可信计算资源

保密智能合约在TEE中执行，消耗隐私计算算力资源，占用矿工的设备运转时间。与传统区块链不同，Phala 保密合约的执行不依赖共识算法。因此每一个合约仅运行在一个TEE中，合约得以并行地在网络中执行。另一方面，合约的执行速度与共识算法无关，可以实现接近原生的执行速度，其实际性能取决于*合约所在机器的CPU性能*。使用完毕后隐私计算算力资源又可恢复到闲置状态。

在我们的设计中，获得隐私计算算力的方式有两种：

- 每笔使用到隐私计算算力的交易通过支付单笔计算费用的方式结算
- 有长期使用隐私计算算力资源需求的用户，可以购买资源包。资源包包括使用时间+资源配置，购买资源包后期间内将无需再支付单笔计算手续费

2.2.2 链上计算、存储资源

一笔交易被区块 Gatekeeper 打包并同步到全网将占用Phala的链上数据空间，这一过程需要消耗链上计算资源，且操作产生的数据量越大，需要消耗的链上计算资源越多。我们参考了EOS、以太坊等网络的资源设计，我们认为对费率市场是必不可少的，因此Phala协议将采用Gas费模型。如果用户需要调高交易的优先级，可以使用小费来提高交易优先级

2.2.3 存储资源

Phala网络的目标即是针对于大规模、长尾的数据加密状态下的联合计算设计的，因此Phala将尽可能的鼓励上传、调用他方数据在Phala协议下进行加密和TEE内解密计算，因此Phala协议的经济设计将使用PHA资金池-外部协议资金池的方式对链外资源进行长期供给.

2.2.4 数据交易价值

Phala 的标准化数据交易合约中定义了如下角色，并准备了对应的激励设计：

- 数据所有者：100%的所有权保障，可删除、转移、隐藏、售卖自己的数据，也可以通过 Phala 合约体系管理使用授权，获得数据利益

- 数据消费者：在合规的前提下放心购买他人数据，并通过分析获得价值。其中，对于数据源的可信度追踪是目前市场缺失的痛点
- 开发者：从金融分析到审计报告，数据开发者会利用自己对数据的洞察开发出好的数据产品供数据使用者使用，他们需要合理的收费制度才能够保障良性的市场生态
- 平台：去中心化的数据平台，需要在不同的市场状态下提供不同的运营策略、产品功能支持，才能让以上角色完整表达需求

因此，构建一个良好的市场是需要顶层设计和长期运营支持的，Phala协议会将数据交易基础模型的角色、契约工具等基础设施设计为标准化协议，因此这个良好运转的数据市场是Phala协议所提供的最重要资源之一——在提供系统级应用的同时，也可以作为重要的商业收入手段。

2.3 角色说明

在Phala网络中，维护共识的核心角色为Gatekeeper、提名人、TEE矿工和Phala DAO。

2.3.1 Gatekeeper

在保密合约中所有数据都加密保存，为了保证矿工随时可以使用数据我们需要 Gatekeeper 这一角色时刻在线并安全持有密钥。

Gatekeeper 在 Phala 网络里打包新区块、并管理系统中的密钥分配，因此需要时刻在线。Gatekeeper 需要抵押足够多的PHA，因为我们允许其他有资金的提名人推举一个或多个可以代表他们的 Gatekeeper ，所以 Gatekeeper 一部分的抵押并不是他们自己所拥有的，而是属于提名人的。

一个 Gatekeeper 必须在高可用、高带宽的可信设备上运行 Gatekeeper 客户端。每个区块上，节点都必须准备接收一个已提交的平行链上的新区块。这个过程涉及接受、验证、再发布候选区块。

我们预期在初期，Phala 会招募 50 个 Gatekeeper，这些节点中的每一个都必须抵押PHA。抵押的数量没有最大或最小限制，但为了保持 Gatekeeper 身份，抵押量必须超过一定阈值。每一个 Era（约24小时），Gatekeeper 都会根据抵押金额重新选举。他们因诚实行为受到奖励，并因离线或提出无效区块而受到惩罚。

NPos共识算法会惩罚没有履行职责的 Gatekeeper。最开始非有意的错误，只会导致奖励扣除，但如果重复产生了错误，则会导致保证金销毁。而多次签名（double-signing）等可被证明的恶意行为，会导致他们损失全部的押金（小部分销毁，而大部分奖励给信息提供方和诚实的 Gatekeeper）。

2.3.2 提名人

提名人是一个拥有权益的群体，他们把PHA押金委托给 Gatekeeper。他们信任某些 Gatekeeper，委托他们代表自己维护网络。

在Gatekeeper获得奖励或惩罚时，提名人也会按照投票比例同时受到奖励或惩罚。

2.3.3 TEE矿工

Phala的核心能力是保密智能合约，其机密性是由TEE实现的。我们需要搭载TEE、可以执行保密合约的CPU来完成计算，这就需要类似PoW链中的矿工：接入“挖矿客户端”，为网络提供算力，并获得收益。

为保障网络启动初期算力充沛，我们将使用预留的一部分挖矿资金对可信矿工进行补贴。此类补贴的基数可由Phala DAO的财政委员会决策调整，当Phala网络的可信计算任务足够丰富、足以支撑矿工参与时，补贴将会减少。

2.3.4 Phala DAO

Phala的治理由开发者、Gatekeeper、投资者、矿工、普通民众共同参与，作为DAO负责社区治理、开发和财政决策，为Phala网络的价值增长负责。

Phala的治理将在权力分配、Gatekeeper选举、提案公投等机制上参考Polkadot，但在投票算法、决策委员会上，采用了独特创新：

- Phala将采用链上不记名投票机制，即通过保密合约保证投票的隐私性
- Phala将采用“流民主”设计，即充分自由的民主代理制度，任何人可以将任何票数委托给任何人决策投票，并可以随时撤回
- Phala的“委员会”将设计成充分开放的“DAO”，任何符合条件的地址均可参与DAO中

2.4 共识设计

参考Polkadot，Phala采用NPos通胀模型对Gatekeeper和提名人发行PHA代币用于奖励。Phala的通胀数量和通胀率不是固定的，而是通过精妙的算法设计，合理引导代币抵押数量，实现共识安全性和代币流动性。

2.4.1 NPoS共识算法

NPoS（Nominated Proof of Stake，提名权益证明）是Polkadot基于PoS算法设计的共识算法，验证人（Validator）运行节点参与生产和确认区块，提名人（Nominator）可以抵押自己的代币获得提名权，并提名自己信任的验证人，获得奖励。

NPoS的奖励主要来源于代币增发，这也是通胀的来源。

2.4.2 PHA的通胀经济

Phala希望有40%的代币被抵押到NPoS共识系统，60%的代币用于资源支出与市场流通。Phala预期年通胀率为5%。在40%的抵押率中，抵押代币的平均年化收益为12.5%。

以上参数并不是通过硬性规定、官方公告、社区喊单来达到，Phala的代币模型是通过实现以下3点达到引导市场的目的：

- 当抵押率 $< 40\%$，抵押平均年化收益率 $> 12.5\%$，鼓励更多代币抵押；
- 当抵押率 $= 40\%$，抵押平均年化收益率 $= 12.5\%$；
- 当抵押率 $> 40\%$，抵押平均年化收益率 $< 12.5\%$，鼓励赎回而不鼓励抵押。

我们认为，12.5%的年化收益率相比传统金融产品具有很大的优势。

2.4.3 通胀率和收益率公式

概念定义

- 抵押率 $X = PHA_{\text{抵押总数}}/PHA_{\text{供应量}}$
- 年通胀率 $R = (PHA_{\text{年末供应量}} - PHA_{\text{年初供应量}})/PHA_{\text{年初供应量}}$

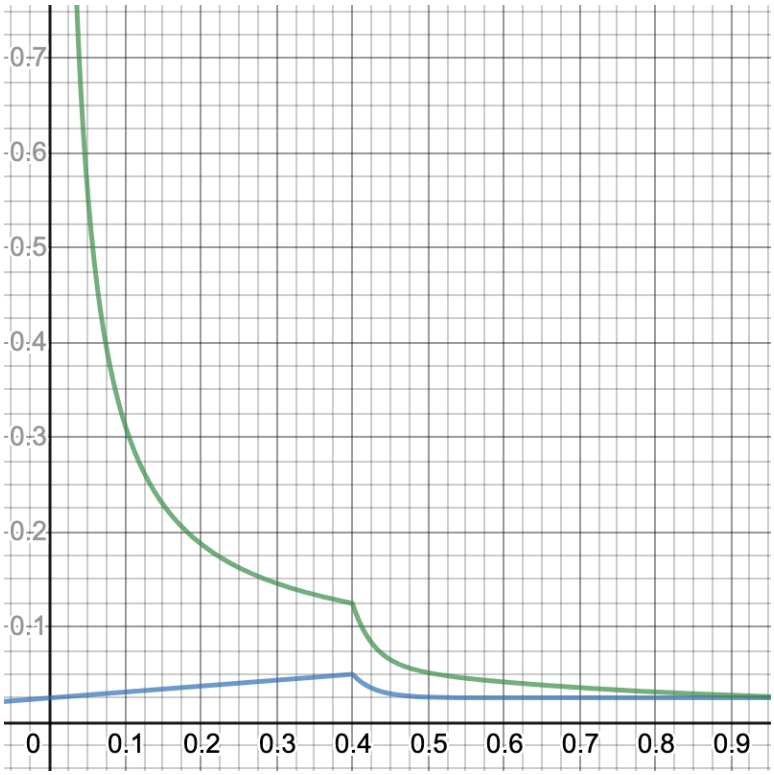
定量参数

- 预期抵押率 $X_{ideal} = 0.4$
- 预期年化收益率$I_{ideal} = 0.125$
- 抵押率为0时的通胀率 $R_0 = 0.025$
- 衰减率 $D = 0.02$

计算公式

- 通胀率 $R_1 = R_0 + X * (I_{ideal} - R_0/X_{ideal})$
- 通胀率 $R_2 = R_0 + (I_{ideal} * X_{ideal} - R_0) * 2^{(X_{ideal} - X)/D)}$
- 通胀率 $R = min(R_1, R_2)$
- 年化收益率 $i = I/x$

可得PHA的通胀模型：



上图中，横坐标为抵押率，蓝色线纵坐标为年通胀率，绿色线纵坐标为年化收益率。

2.4.4 区块奖励

Phala主网的每产生一个区块，系统都会发行一定数量的PHA，称为区块奖励。由于通胀率并不是一个固定的数值，与整个网络的实际抵押率相关，因此区块奖励浮动的。区块奖励按如下规则分配：

- 80％分配给产生该区块Gatekeeper；
- 20％进入去中心化财政系统，为社区贡献者、开发者提供财政支持。将由Phala DAO定期决策奖励分配。

其中，80%的区块奖励分发给产生该区块的 Gatekeeper。所有 Gatekeeper 有均等的机会产生区块，即与抵押比例无关。

在分发给 Gatekeeper 的奖励中，部分奖励用于支付该 Gatekeeper 设置的佣金，其余则按比例（即与抵押成比例）支付给提名人和 Gatekeeper。需特别注意，Gatekeeper 获得两种奖励：一是 Gatekeeper 设置的佣金，二是自己直接抵押的奖励。

2.4.5 Slash惩罚

如果 Gatekeeper 在网络上行为不当（例如离线、不遵守共识协议等），将会被惩罚。他的提名人也会损失百份比绑定/抵押中的PHA。

一旦惩罚发生，较多抵押的 Gatekeeper，会比较少抵押的 Gatekeeper 惩罚更多，所以我们鼓励提名人把他们的提名转移到得票较少的 Gatekeeper 从而降低潜在的损失额。

3.PHA的代币分发

Phala Network的Token分发目标

- 增强产品 / 市场契合度（Product-Market Fit）；
- 鼓励社区早期充分参与，使社区足够的去中心化
- 保证基础开发稳定进行

基于目标，我们可以提出以下问题：

3.1 产品的目标用户是谁?

Phala Network的市场目标是服务于保密智能合约的使用场景，根据Web3.0的理念，我们将使用Phala Network的数据角色进行了“三权分立”的角色划分：

- 数据所有者
- 数据计算执行者
- 数据消费者

3.1.1 数据所有者

即Phala网络所服务的最底层用户，他们通过Phala将自己的数据加密后保存、管理，在未经授权的背景下任何人都无法访问和使用。我们希望目前互联网公司“代为托管”的模式，在可信计算技术的推广下可以有所改变——“隐私保护”和“利用数据产生价值”可以在Phala Network共存

3.1.2 数据计算执行者

- 包括提供计算的环境支持，比如Phala网络建设
- 提供计算的执行，比如TEE矿工

3.1.3 数据消费者

- 开发者，此类开发者在web3价值观、隐私保护法案、消费者诉求的多重影响下，会越来越多的需要将原有产品朝更注重隐私保护、更注重用户权利的方向发展，因此他们是Web3 Analytics或此类产品的潜在用户，此类用户也是可信算力的主要使用者。
- 企业、数据分析公司等。这些客户是需要使用可信数据的消费端，在目前的市场中进行数据购买，会遇到数据不可信、所有者法律风险等问题，而在Phala中他们可以追溯到数据的产生，也可以通过验证等手段确信数据的可信度

3.2 如何才能吸引社区充分参与?

- 代币分配足够公平。我们参考POW社区和POS社区的生态就会发现，越公平的分发规则（比如基金会实际占有80%的代币就是不公平的）越能持续、稳定的吸引社区参与
- 合理的参与成本。此处参与成本既要足够低，有不可毫无门槛和成本。比如让参与者献祭自己的隐私，或参与极度复杂的任务，都是不可取的。早期POS社区的完全免费空投，将会导致Token价值毫无底线，最终导致社区流失。
- 合规性。参考“豪威测试”：美国联邦最高法院在 SEC v. W. J. Howey Co 一案中确立了「Howey 检验」，以确定一项交易是否构成「投资合同」进而构成「证券」。 Howey 检验包含四要素：资本投入; 投资于一个共同事业；期待获取利润;不直接参与经营，仅仅凭借发起人或第三方的努力。Phala代币不希望因违反证券交易法规而被绞杀，因此我们将会避免消费者通过投资Phala获取到Phala业务产生的分红，或设置ICO。

3.3 如何保证基础开发稳定运行?

在项目初期，必须要有一个对构建网络有着充分热情和能力的领袖团队。在这个阶段我们将竭尽所能的构建出理想中的Phala Network，并且不求盈利。

但因为团队成本需要，我们需要找到预算来支持事业。团队将通过少量的PHA代币融资（不超过15%）、获取各类赞助等方式支持Phala开发。

在项目启动后，基础开发将需要继续孤独前行，甚至投入的开发成本会更多。在此阶段，我们将以5%的代币+预算委员会拨款完成基础开发迭代。此阶段团队的PHA代币将会分阶段解锁，直至下一阶段完成。

在社区足够壮大和成熟后，社区将完成100%自治。通过合理的预算委员会制度分发Grant完成基础开发、功能迭代、生态建设。

3.4 公平分发机制

足够公平的分发机制才能够帮助协议找到自己的目标市场，因此Phala将采用“根据贡献公平分发”的策略，将Token尽可能的分配到对协议产生价值的人群手中。

Phala Network的代币分发规则框架如下:

分配模块	分配比例	分发方法
TEE挖矿	70%	由TEE矿工等角色挖出。数量固定，不参与通胀分配。
波卡社区建设和平行链拍卖	9%	贡献KSM、DOT等生态代币获取PHA
测试网奖励	1%	用于激励测试网的广泛参与
私募融资	15%	用于Phala开发经费、运营推广，我们不进行任何面向公众的融资。这部分PHA将在主网上线或代币流通后解锁60%。初次解锁后每6个月解锁20%
团队奖励	5%	用于开发团队的激励。主网上线或代币流通后释放20%，后每个月解锁5%

如上所述：Phala采用了非常激进的Token分发策略，我们将把80%的PHA Token分配给目标用户，团队只保留5%的奖励，并使用15%的PHA用以融资。

3.5 TEE挖矿

大部分人类还生活在数据被巨头垄断的世界中，少部分的觉醒者已经在暗流涌动。如果让大部分人民像极客们一样能够觉醒？如何鼓励人们吃下觉醒的红药丸？

我们需要让TEE算力矿工参与到红药丸的觉醒战争中来，为此我们将70%的PHA用于鼓励可信数据世界的增长！我们将其称为TEE挖矿，而挖矿奖励的设计遵循如下原则：

- 可预期：有一条释放曲线，可明确的确定任何时间段内的释放量
- 可持续：奖励释放速度可控，可以长期支持生态发展
- 分发公平：分发规则公平，无法被攻击者利用
- 高性能：链上计算量较小

为此，我们设计了一种指数递减释放模型（类似比特币减半），奖励释放速度随时间逐步降低。生态的多种角色按一定比例竞争奖励，并通过难度系数调整奖励的释放速度。

3.5.1 挖矿奖励释放

初始代币分配的PHA将有70%由TEE挖矿方式释放，总量为700000000枚PHA，奖励固定总额，没有增发。理想的奖励释放随着时间降低，符合指数下降函数：

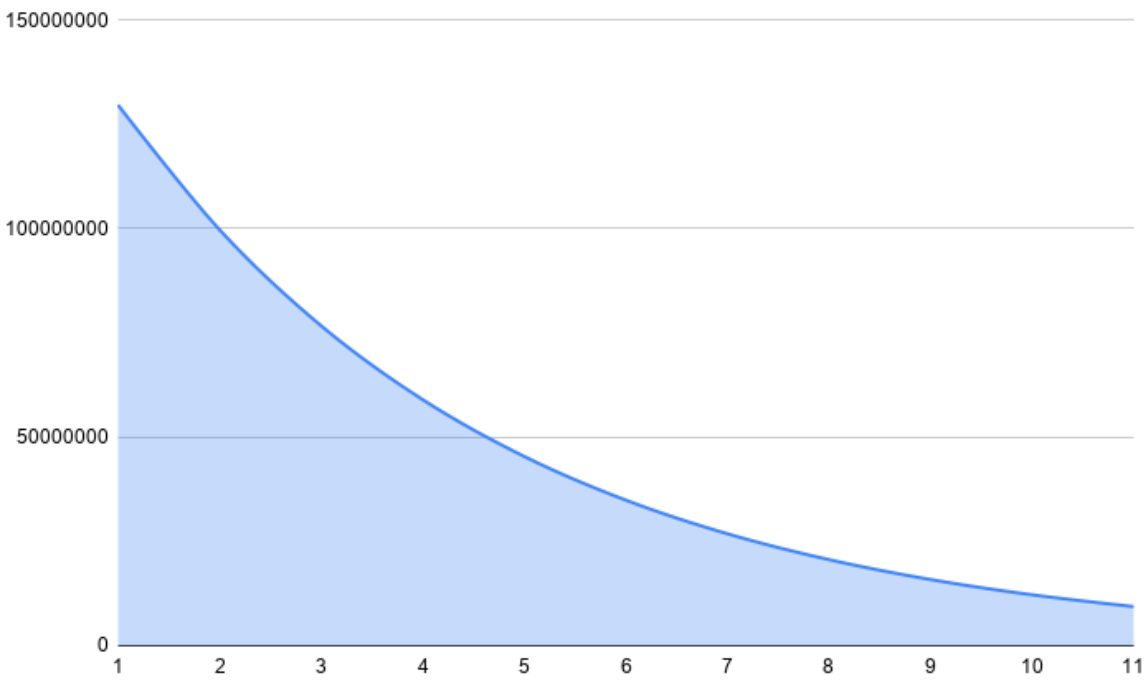
$$I_R(t) = I_{R0} \cdot k^t$$

其中 t 为区块时间，以 Epoch 为单位，I_{R0} 为初始释放量，k 为每个 Epoch 的衰减系数，满足

$$\sum_{t=0}^{\infty} I_R(t) = 7 \times 10^8$$

Phala Network 采用的参数为：

- $I_{R0} = 3 \times 10^4$
- $k = 0.9572$



根据上图可以看出，PHA的奖励衰减是非激进设计的，我们希望尽可能让初期矿工享有绝对的贡献投入产出比、且同时能够为协议的未来算力、数据支持做长久打算

3.5.2 挖矿奖励分配

我们希望每一类角色奖励符合固定的比例，且总奖励符合释放曲线。然而严格地在每个 Epoch 中进行等比均分并不合理，因为奖励事件容易产生大幅波动（例如用户贡献数据），在波动峰值与低谷处对参与者不公平，甚至造成负激励。

为此，我们引入了基于自适应算法的难度调整机制，角色 T 的奖励 $R_T(t)$ 以及奖励总 $R(t)$ 和为：

$$R_T(t) = n_T(t) \cdot k_T(t)$$
$$R(t) = \sum R_T(t)$$

其中：

- $n_T(t)$ 为 Epoch 中的奖励行为数量
- $k_T(t)$：t时段的难度调整系

通过调节难度系数，可以控制角色 T 的奖励占比期望符合**理想占比** I_{PT}，但又可以控制对波动的敏感度，即：

$$\mathbb{E}\big[\frac{R_T(t)}{R(t)}\big] = I_{PT}$$
$$\mathbb{E}\big[R(t)\big] = I_R(t)$$

Phala Network 中的激励角色与理想占比如下表所示：

T	I_{PT}
在线TEE矿工	30%
隐私计算任务奖励	50%
生态开发(财政库)	20%

每个Epoch的奖励将分为两个队列：

队列A	**队列B**
在线TEE矿工	隐私计算任务奖励
生态开发(财政库)	

每一个Epoch：

- 队列A的奖励均会在每个Epoch统计计算奖励
- 队列B会先统计是否有链上隐私计算任务被执行
  - 如果没有隐私计算任务(如机密智能合约交易)，则该部分奖励累积到下一个Epoch奖池
  - 如果有隐私计算任务在某Epoch被执行，则所有参与该Epoch隐私计算交易的矿工瓜分累计的隐私计算任务奖池

奖励发放：每2个ERA执行一次奖励发放

3.5.3 TEE挖矿难度

TEE挖矿难度系数由历史难度系数与调整目标的进行指数加权确定。目标难度系数即为满足理想占比与理想奖励释放情况下的数值：

$$k_T^*(t) = \frac{I_R(t) \cdot I_P T}{n_T(t)}$$

则调整系数由指数加权确定：

$$k_T(t) = \begin{cases} k_T^*(0) & t = 0 \\ (1-\lambda) \cdot k_T(t-1) + \lambda \cdot k_T^*(t) & t > 0 \end{cases}$$

其中加权系数 $\lambda \in [0,1]$ ，取值越高则对流量波动越敏感。一个合理的 λ 可以有效调节挖矿难度，实现总奖励与奖励占比的期望符合理想值。

Phala Network 采用 $\lambda = 0.2$。

3.5.4 矿工角色奖励细分

为了简化公式，前文仅讨论了每一种角色内部所有奖励都均分的情况。而实际情况通常需要根据参与者的属性决定奖励的大小。例如在单位时间内，高性能TEE矿工的奖励应该成比例的高于普通TEE矿工。

为此，我们为每一种角色 T 引入权值 w_{Ti}，表示第 i 类奖励行为的权值。则前文公式可改写为：

$$R_T(t) = k_T(t) \sum_i n_{Ti}(t) \cdot w_{Ti}$$

$$k_T^*(t) = \frac{I_R(t) \cdot I_P T}{\sum_i n_{Ti}(t) \cdot w_{Ti}}$$

即每种行为所获得的实际奖励为奖励系数与难度系数的乘积。不同角色及其奖励行为的打分由具体属性分别确定。

3.5.5 在线TEE矿工

在线TEE矿工是指 Epoch 期间在线的TEE设备，一个设备我们认为是一个矿工。只要矿工将TEE设备接入了Phala协议并保持在线，不管是否有计算行为，都为供给端体验做了贡献，因此我们都将提供一部分挖矿奖励。

Phala网络对TEE矿工得分的计算取决于以下变量：

- CP值 (Confidential Points)。包括CPU线程数、基准性能评价分数、内存大小等，性能测试逻辑将随着Phala开源
- 个体总在线时长。总在线时长越长的矿工得分越高
- 个体成功执行数。即已经处理的交易数
- 个体惩罚率。惩罚率=被惩罚的次数/总交易数，惩罚率越低矿工得分越低

我们对TEE矿工的奖励计算系统设计如下：

奖励行为	权重
在线	高
CP值	中
历史在线时长	低
历史成功执行数	低
历史惩罚率	负

为保障网络安全性，TEE矿工必须抵押定量PHA才可以参与挖矿：

- 初期抵押额为固定值，每个CPU核心需要抵押1620个PHA
- 抵押值每6个月可以通过公投修改一次
- 抵押后的解锁周期为7天
- Phala协议会提供系统级协议，帮助矿工和持币者撮合抵押市场。这种情况下，有机器的矿工无需购买PHA也可以参与挖矿。

3.5.6 隐私计算任务奖励

隐私计算任务奖励将由执行隐私计算交易的TEE矿工获得。

A. 派单算法和奖励周期

隐私计算任务的派单算法将主要参考以下特征：

- 安全性：算法随机性选择在线TEE矿工、优先考虑高抵押额的TEE矿工
- 计算体验：优先高CP值的TEE设备、优先网络延迟低的TEE地址

B. 运算TEE矿工

运算TEE矿工是指为在一个Epoch间真正参与了运算订单的TEE矿工，我们将为这类矿工提供较为丰厚的奖励。

在线TEE算力(CP值)代表着Phala Network可以承接的计算量，且代表着提交隐私计算任务的用户的体验。而实际参与运算的TEE矿工承担着更多安全性职责，因此Phala协议允许希望执行任务的TEE矿工进行更多的PHA抵押申请。抵押越多PHA的TEE矿工，作恶成本越高，安全性风险越低。

我们对运算TEE矿工的奖励计算系统设计如下：

奖励行为	权重
抵押量	高
CP值	中
历史在线时长	低
历史成功执行数	低
历史惩罚率	负

3.6 社区建设和平行链拍卖

我们希望尽可能公平的发放Token到目标用户手中，同时希望能够通过机会成本的筛选，筛选出认可Phala价值的用户。在参考了Edgeware的LockDrop、NuCypher的WorkLock、Rocco的WarLock机制之后，我们觉得Lockdrop是个好主意。

结合Phala网络的设计目标，我们将WorkLock进行了模型改进。PHA的锁仓空投共有两期，分别是：

- 抵押KSM到Phala的节点即可获得KSM利息奖励和PHA的空投
- 通过首次平行链拍卖（IPO）空投，持有DOT的用户均可以参与

其中，DOT锁仓将用于首次平行链槽位拍卖，可能会使用波卡主网的拍卖合约进行。作为回报，参与者得到与抵押物等值的PHA。

3.6.1 KSM Stakedrop

Stakedrop是Phala团队设计的一种新空投方式。参与者抵押手中的KSM，提名给**白名单**中的**验证人**，以获得**空投点数**。最终会根据空投点数兑换PHA。

我们不希望社区空投的价值被主网时间限制住，因此Stakedrop的PHA在Phala主网上线前以ERC20代币的形式分发。我们将通过开源脚本持续监视记录Kusama链上抵押情况。若参与者的抵押符合我们的要求，则抵押期满之后，参与者可以在以太坊上领取释放的PHA。

1）概要

- 分发代币数量：预期值为Phala初始总量的2.7%，即2700万枚PHA。
- 目标对象：KSM持币人 (Polkadot社区，Kusama网络参与者)
- 参与方式：在Kusama网络参与提名，抵押至白名单内的验证人，持续30-90天，即可获得PHA

这个方式有几个好处：

- 无机会成本损失：在NPoS中继续享有KSM的Staking收益
- 极容易获得空投糖果：无需特地参加活动，只要为白名单内的验证人抵押了KSM达30天以上，就可以获得PHA空投
- 有利于提高Kusama网络安全性：通过StakeDrop的吸引，人们更愿意抵押KSM至网络中，达到Kusama的抵押目标
- 不影响治理：验证人白名单足够大，所有在Kusama做过身份验证的验证人都将进入“白名单”，而只要提名了白名单内的验证人就可以得到空投——这样做的唯一目的是尽可能少的影响Kusama的公平性

2）Stakedrop模型

用户参数：

- 锁仓KSM数额 $Lock_{KSM} \in [10, +\infty)$
- 锁定时间 $Days \in [30, 90]$

分发规则：

1. 理想供给

$$Q_{ideal} = 27,000,000 \text{ PHA}$$

2. PHA 最终按照空投点数 P 分发

$$P = Rank(Days) \cdot Lock_{KSM}$$

3. 其中 $Rank(d)$ 为抵押 d 天的奖励权重，呈指数增长

$$Rank(d) = \frac{1}{30}d \cdot 1.01^{(d-30)}$$

4. 所有参与者按照各自的 P 均分 Q_{ideal}，除非点数之和超过临界值 P_{max} 时，则按照固定比例兑换PHA

$$Drop = \frac{P_i}{min(P_{max}, \sum P_i)} \cdot Q_{ideal}$$

5. 其中临界指 P_{max} 为2700万KMS抵押满90天的点数

$$P_{max} = Rank(90) \cdot 2.7 \times 10^6$$

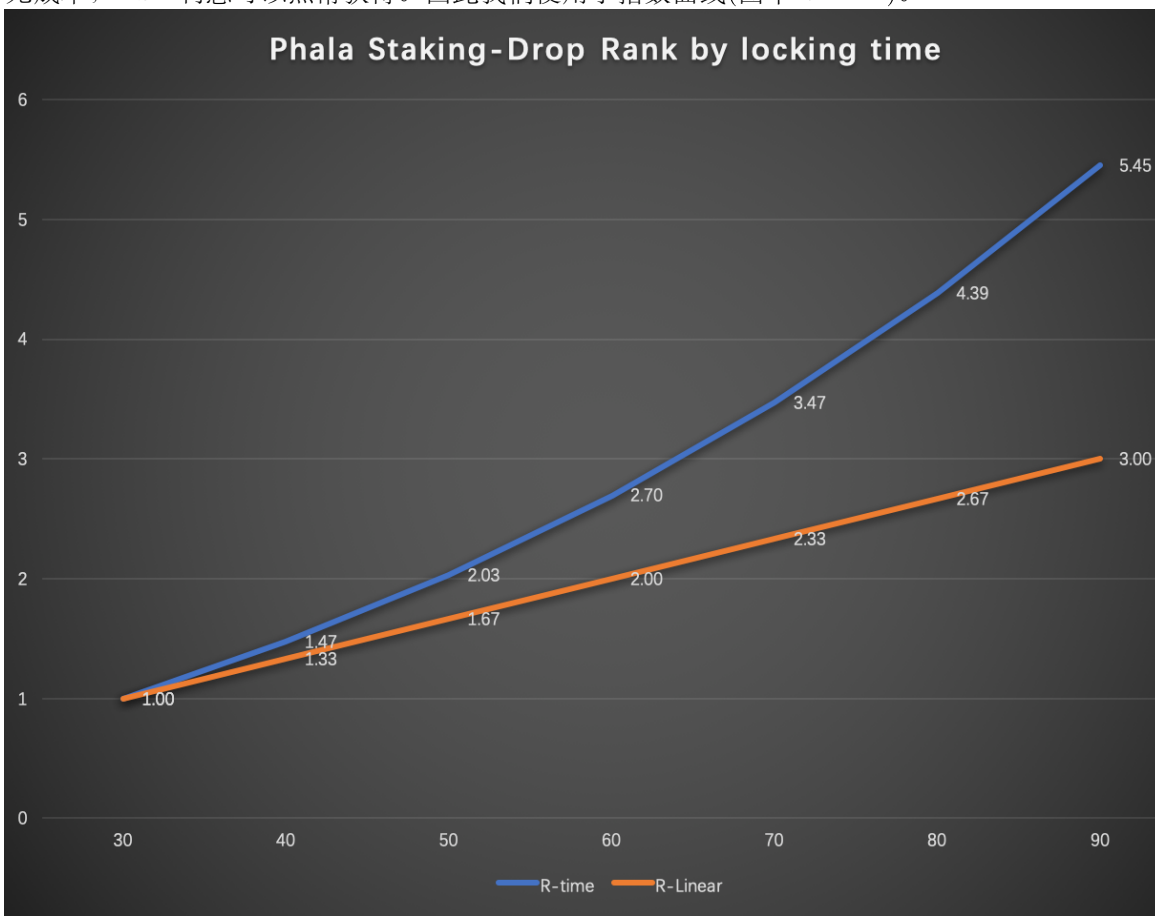
3）空投供应量

Stakedrop中，所有参与者按照空投点数均分所有的PHA。为了给参与者一个基准奖励预期，我们设定了奖励的最低值，即 $1\,\text{PHA/KSM}$ 。

- 当抵押产生的空投点数不足临界值（2700万KMS抵押满90天）时，参与者按点数比例瓜分2700万PHA
- 当抵押产生的空投点数超出临界值，锁定最低奖励兑换率，这种情况下空投量将超出 Q_{ideal}

4）奖励权重

通常意义上锁仓奖励与锁仓时长 $Days$ 是线性相关(图中R-Linear)的。但是在Stakedrop中，参与者几乎无成本，KSM利息可以照常获得。因此我们使用了指数曲线(图中R-Time)。



4.Phala社区治理

4.1 治理机制

Polkadot对社区治理的设计十分专业，引入了现行民主制度的某些优点，我们认为有三点尤为特殊：

- 所有链的更改通过治理决定，而非仅局限于部分参数
- 设置了理事会，并能够对公投的机制互相作用
- 投票权重引入抵押时间的概念

Phala将会吸收和采用Polkadot的治理优点，并提出了自己的创新：

- 匿名投票，我们将使用保密合约完成投票，因此民主的匿名性可以保障
- 流民主投票机制和算法，充分提高投票参与率
- 将委员会改制为DAO，提高开放程度，并通过抵押制度保证决策层的利益与社区绑定

4.2 治理机制概述

4.2.1 治理目标

- 足够民主和开放，意味着PHA将作为唯一代表民意的Token
- 高参与度，意味着理解成本和参与门槛要降低
- 决策团需要具有专业性，即有给出专业决策建议的能力

4.2.2 治理模型

- 所有的提案可被任何人发起，需要通过公投才能生效
- 引入代议制，即通过DAO作为议会来负责提出专业性提案，并可通过专业性来制衡盲目性公投
- 公投、DAO的选举，均通过匿名性投票与流民主投票完成

4.2.3 参与者

- PHA持有者：Phala 治理的核心是 PHA 代币，它让参与社区提案变得非常直接和高效。PHA持有者可以发起提案、改变提案顺序、给所有生效的提案投票、选举Phala DAO成员、申请成为Phala DAO成员
- Phala DAO：通过民主选举产生，为保证核心参与者与Phala协议利益绑定，我们将参考Moloch DAO的设计，参选者必须用抵押的PHA来换取DAO的内部票数，并只有通过特定条件才能退出并解锁代币。Phala DAO负责：发起提案（专业性和高参与度）、使提案不生效

由上可见，任何PHA持有者都可以提出提案，且所有提案都需要公投才能通过，选举产生的Phala DAO对提案合理性拥有一定否决权，但仍被全民民主所制衡

4.3 提案与公投机制

4.3.1 提案内容

Phala协议的所有修改都需要公投来完成，包括但不限于：

- 代码升级
- 系统参数调整
- 治理规则的变动
- 财政拨款
- 选举与罢免

4.3.2 提案流程

任何 PHA 持有者都可以提交提案，提交提案需抵押极少数PHA。

为了避免大量无效提案，Phala DAO会先对提案进行投票，权重高的提案会被优先处理进入公投阶段，而没有获得DAO多数同意的提案，不能进入到公投阶段。

获得理事会多数同意的提案，需要在公投中获得多数同意，才能执行。

每一个批准的提案需要等待一段时间才可以真正部署到链上。这样可以让那些不同意提案的参与者离开（比如卖掉手中的代币），而投票支持这个提案的 PHA 持有者的代币会被锁定，直到提案被执行。

4.3.3 公投机制

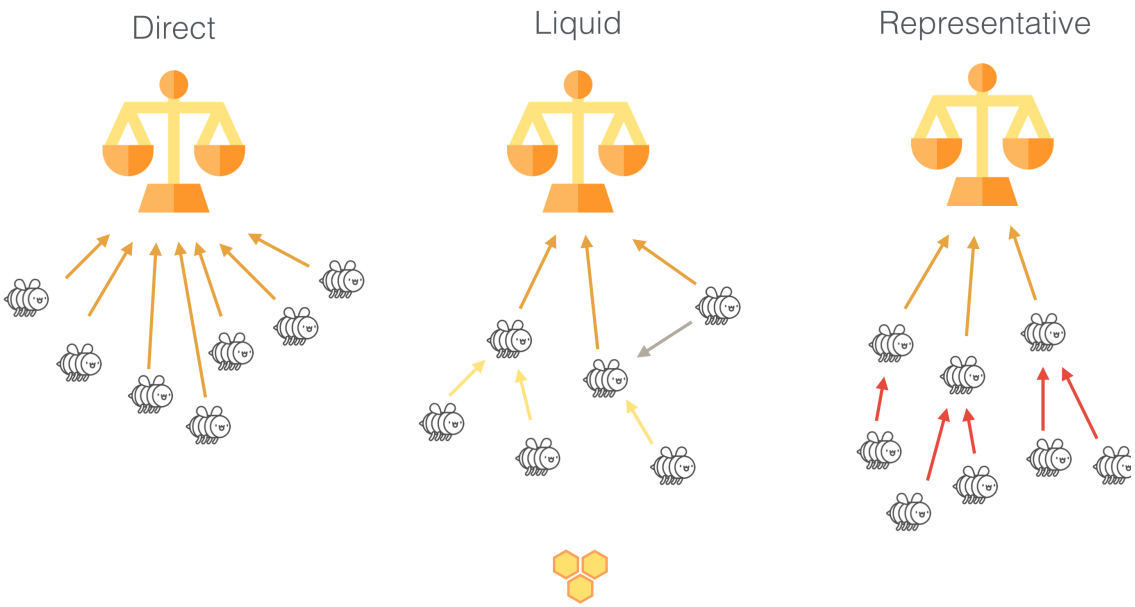
参考目前主流区块链的投票率，我们认为既需要降低投票参与成本，又需要准备好低投票率下的民主，因此流民主不记名公投的基础规则如下：

- 任何人都可以委托任何代表以任意自己持有的票数，被委托人也可以分票委托其他人
- 委托关系只有发起-接受端知晓，其他人无法获悉委托关系、投票数量，即通过保密合约实现匿名投票
- 抵押PHA的数量和时间将决定投票权重，最少锁仓时间为4周
- 无最低投票率设计，少数服从多数

4.3.4 流民主算法

直接民主，即一人一票决定议题，优点是反应了选民民粹态度，但是缺点是投票率低，以及受限于选民的知识水平和政治素养，容易导致民粹暴政。间接民主，即先投票选择代表，再由代表来处理政治议题，是现实社会最普遍实行的政治制度，其优点是可实现、更专业、更理性，但缺点是选举出来的代表可能作恶成本低，位置固化会导致民主的流动性差。

流民主起源于Bryan Ford在1884年发表的论文《Delegative Democracy》，即针对某个议题，可以直接投票，也可以把投票权委托给一个代表，再由这个代表投票决定这个议题。我们参考了AS-rearch发表于arXiv的论文——*Implement Liquid Democracy on Ethereum: A Fast Algorithm for Realtime Self-tally Voting System*对流民主在区块链的研究。

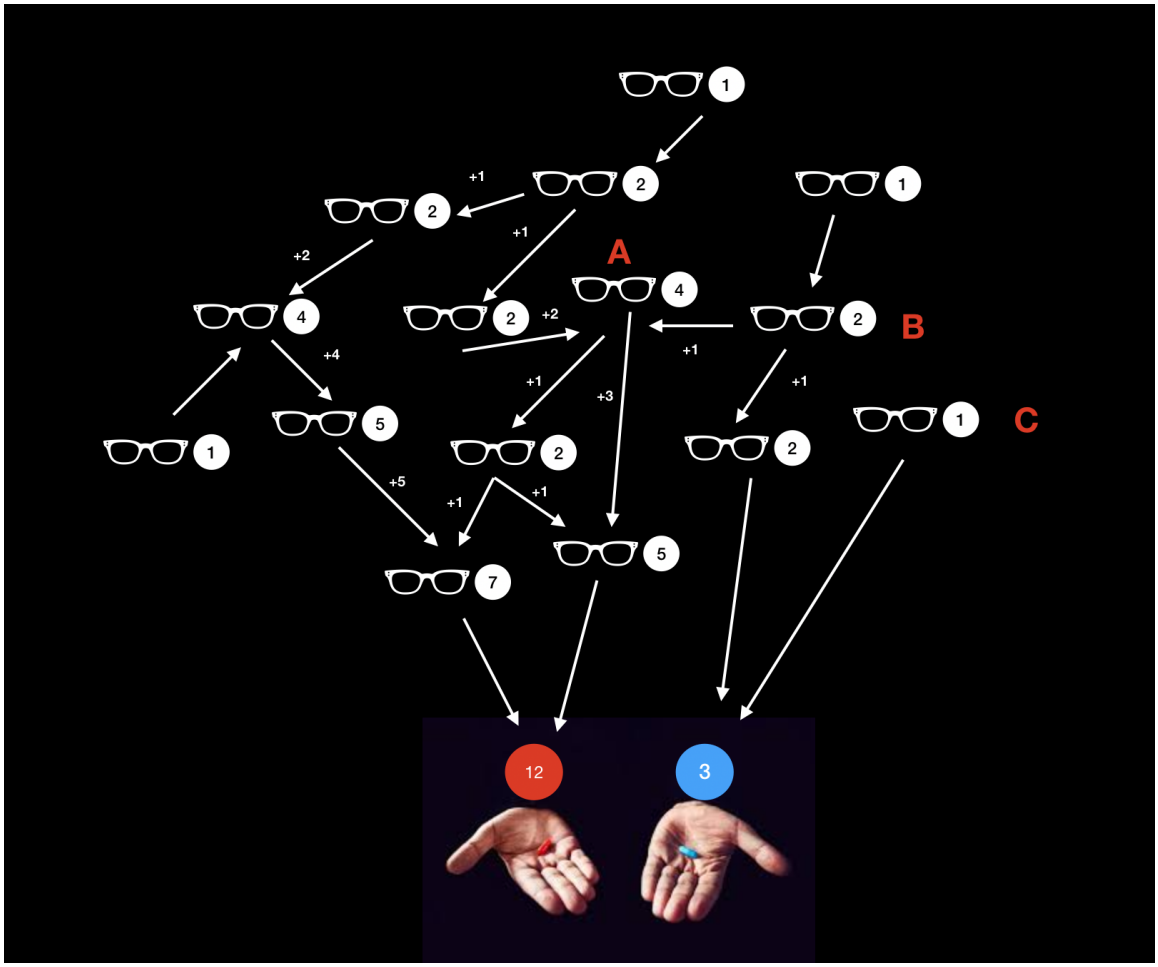


From Liquid Democracy, Ethereum, and the slow path to revolution.

在论文中，ASresearch发现流民主的一个应用例子是Google员工通过Google Votes决定今天吃什么，如果某人不知道今天要吃什么，他先把决定权委托给口味相近的同事，再由这个同事决定今天吃什么。流民主的优点在于对直接民主和间接民主的折衷，既保证了足够真实、纯粹的民主，也提高投票率、能够专业、理性去解决问题。但是流民主的执行过程非常复杂，需要频繁的、实时的统计投票权。

我们假设在《黑客帝国》中，墨菲斯并不是对Neo提出问题，而是对程序特工Smith提出问题：红色代表现实，蓝色代表虚拟，你选择哪个？

我们假设有15个Mr.Smith，每个Smith都有投票权，每人1票，这次决定需要15个Smith来参与，每个Smith可以把票委托给其他同胞。假设其投票数等于其序号，箭头方向代表委托方向。则在这次关键的投票决策中，很有可能发生如下情况：



- A号Smith先生是一个KOL，颇有威望且爱分享权力：他不仅拿到了委托人的3票，还将自己持有的4票分别以1票、3票委托给了其他人
- B号Smith先生拿不好是去往现实、还是去往虚拟世界的主义，所以他索性在两个党派分别押注
- C号先生意志坚定，且不相信其他人能贯彻他的民主意图，所以自己投了蓝药丸（现实世界）一票。

在流民主的DAO中，其委托关系是一个树，为了计算和更新每个节点的投票数，每次投票都需要对这个树进行先序遍历或后续遍历，其时间复杂度为O(n)。

这部分的实现技术在传统区块链中较为困难，因为流民主的计算数据庞大导致区块大小有限、gas手续费高昂。而在Phala协议中，我们将采用TEE计算方式来解决性能问题，同时保障流民主的隐私。

4.3.5 匿名投票

值得注意的是，如果委托关系可以被全网洞察，就存在通过数据计算、数据挖掘，找出贿选方法的可能性。因此民主制度的投票往往是不记名的。

Phala Nerwork实现了保密智能合约平台，因此在系统级设计中可以使用保密合约来保障委托关系和票型的匿名性，同时能够验证选举是真实可信的。

4.4 Phala DAO

Phala的治理将由去中心化的DAO形式完成，我们使用DAO来替代：代议制的委员会制度或上议院制度。我们将部分采用Moloch DAO的部分设计用于Phala DAO设计：MolochDAO 是一个去中心化的拨款协调系统，为以太坊开发项目分配资金。它的建立就是为了协调决策过程，实现快速按需分配资金。如果要加入 MolochDAO，需要由现有的 DAO 成员进行邀请。

DAO 成员通过审查背景、声誉和其他指标，考核潜在成员是否能够为整个团队提供足够的资源。一旦投票出资后，将获得 DAO 的股权。拥有这些股权，所有成员能够提议、投票，或通过销毁股权来离开 DAO。当一项融资提议通过后，它获得的 DAO 股权可立即转换为 PHA。从本质上讲，DAO 将一个组织分解成一个单一的决策过程，同时激励其成员高效地加入或离开。

4.4.1 成为Phala DAO一员

DAO内部的投票权定义为Share，Share不可转让且可以无限增发，但是总比例始终为100%，因此DAO的决策系统以少数服从多数为输入，输出为同意或不同意

创世团队会通过抵押手中的PHA来创立Phala DAO，因此Phala DAO的初始股权将被设定一个入金价格。之后任何人都可以通过提交DAO申请+公投选举获得入金对应的share。

从选民到加入DAO需要经过以下流程：

- 先设定好自己需要的Share数量，并选择奉献任意数量的PHA到合约中，这部分PHA会进入DAO的A资金池
- 系统会根据奉献的PHA与索取的Share判断是否高于目前的汇率，若抵押汇率，则需要经过“动议”流程才可进入公投
- 若等于或高于当前汇率，则无需动议即可由全民公投，**此类公投不得被DAO驳斥**
- 公投完成后，DAO成员被加入其中，其获取的share数量即DAO内部的票数

注意，因为DAO申请人在提出share申请时已经抵押了PHA到A池，而A池中的抵押物只能兑换share，不可参与公投或质押生息，因此降低了巨鲸同时操纵DAO和公民票数的可能性。

退出Phala DAO需要满足以下条件：

- 在一个动议通过后的“公投”期或48小时“冷静期”内
- 在该提案对应“动议”的DAO投票中，投了反对票且提案通过，或投了赞成票但提案未通过
- 满足以上两个条件即可发起退出指令，DAO合约将清算Share比例对应的A池资金给该退出成员

这样的设计参考了 Moloch 的怒退（Ragequit），该机制大幅降低了协调成本：它可以确保如果 Moloch 的成员实在不喜欢某个提案，可以在该提案通过之前带着自己的资金退出。这样一来，协调成本就可降至几乎为零。

4.4.2 Phala DAO的决策系统

Phala DAO将拥有对提案的筛选权，即“动议”。“动议”通过，被筛选后的提案才会进入公民投票环节

Phala DAO的投票系统

- Phala DAO内部投票由Share作为票数依据
- 无最少参与率限制，少数服从多数即可
- 每个提案被发起48小时后将进入“动议”环节，由Phala DAO进行投票，7天后将清算投票结果，如若通过则将会进入全民公投队列，链上一段时期内只能有一个在进行的公投
- 如果动议被迅速全体通过，则该动议无需等待7天结算，它可以在48小时后进入公投队列

Phala DAO的决策内容：

- 任何提案的“动议”。由DAO决策是否可被通过，通过的若干动议将根据DAO投票权重排序；未通过的动议将失效
- DAO成员的管理，即A池对应的share决议
- 去中心化财政（B池）提案，只能由DAO成员发起提案

4.4.3 财政决策

财政库的收入主要由两部分组成：

- TEE挖矿的20%生态贡献捐献
- NPos机制的20%税率

这部份收入的使用将分为两个类型：

- 长期拨款
- 拨款提案

长期拨款将由系统进行标准化设计，参数均由Phala DAO在提案中填写，例如：

- Phala DAO和社区决定将财政库的50%收入作为研发奖励的长期拨款
- 则提交该提案需要填写“长期拨款”提案的多个参数，并在链上提交申请
- 经过投票后，该“长期拨款”提案将自动执行：每一笔流入到财政库的收入，都将分配50%至研发团队地址
- “长期提案”的申请类型中包括“中止”类型，流程一致

普通拨款提案，流程与其他提案一致