# Phala Network Token Economy Whitepaper

Marvin Tong, Hang Yin

## I. Introduction

Phala Network is a confidential smart contract network enabled by a TEE-Blockchain Hybrid Architecture.

It ensures confidentiality by running smart contracts inside the TEE Enclaves in the CPU. Also, such structure ensures TEE technology with more utility, stablity, security and scalability. To be specific, Phala Network is:

- Enabled with interoperability between contracts and even chains by introduing Layered Design and Event Sourcing;
- Miner-friendly as everyone can mine PHA with his own computer and the blockchain itself will verify the execution of the extrinsics.

Also, Phala Network supports cross-chain integration as a native blockchain built on Substarte, which empowers Phala to be the infrastructure of confidentiality for any blockchain across the world.

### 1.1 Vision of Phala's Token Economy

> Firmly believing in the penetration rate of Web3.0 tools, we think blockchain shoule be confidential without any third-party intermediary. Trusted computing, as the one and only technical solution to such needs, would be invaluable with unmeasurable market capitalization.
>
> Different from traditional TEE solutions, the value that Phala Network provids stands with smart-contract-enabled, scalable and interoperatable data exchange and privacy computing.

**Our vision: Build a global-scale trusted computing protocol**.

## II. Token Economy

**PHA** is Phala's native token with a 1-billion total supply, and its distribution would be completed via ERC20 and testnet before the mainnet launches.

### 2.1 Utilities of Phala Token

- Buy trusted computing resources: computing resources, on-chain storage, off-chain storage, etc.

- Data exchange fee: Phala provides a contract-based data exhcange infrastructure for standardized data collection, analysis, and trading protocols. With Phala's potocol, a confidential but trustful exchange ecosystem is built for both buyers and sellers.
- Security guarantee: To be a Gatekeeper one must stake a certain amount of PHA. The stake would be fined and took if he betrayed Gatekeeper rules.
- Governance: Stakeholders who owns a certain amount of PHA would be able to join Phala DAO to further participate in community governance.
- Other payments: Settlements for other services or products such as Web3 Analytics, cross-chain bridges for permissionless chains.

## 2.2 Value Captured by Phala Network

The value captured by PHA is the resources in the network and data exchanges.

Each extrinsic happened on the mainnet costs resources which are defined as the three types below:

- Computing Power : Trusted Computing Processing Unit
- On-chain Computing & Storage Resources
- Off-chain Storage Resources

Also, Phala captures the value of data exchange through a set of standardized contracts with data trading as its core ability.

### 2.2.1 Trusted Computing Resources

Smart contracts would occupy Privacy Computing Power and require the uptime of TEE miners. Unlike the one in traditional blockchains, Phala's contracts could run parallelly on each TEE node instead of relying on an expensive consensus algorithm. Performance of the execution can be close to native execution, as the computation is irrelevant to consensus algorithms. The network throughput is determined by total CPUs. The Privacy computing power could return to an idle state once it finishes its computing tasks.

In our design, there are two ways to buy Privacy Computing Power:

- Short term: Pay for Privacy Computing Power on an exchange-based one-off payment;
- Long term: purchase a predefined Privacy Computing Power resource package including PCP time and related resources in a limited time. With the resource package, one would not need to pay other fees for computation.

### 2.2.2 On-chain Computing & Storage Resources

The extrinsics included in blocks consume on-chain storage and computing resources. The larger the data is, the more the computing resource is consumed. After researching Ethereum and EOS, we concluded the fee market is essential. So Phala implements a Gas Fee Model which allows users to prioritize their tasks by tipping.

### 2.2.3 Off-chain Storage Resources

Phala is designed for large-scale and long-tail multiparty computation, thus encourages users to upload their own data or call third-party data and process cryptographic computations using Phala confidential contracts, as Phala token economy will establish a long-term supply of off-chain storage via “Phala-Assets-Pool — External-Assets-Pool” pattern.

### 2.2.4 Value of Data Trading

Phala’s standardized data trading contract defines the following roles and has the corresponding incentives:

- Data owner: take the 100% ownership over his data. Guarantee the right of deleting, transfering, and selling the data. Data Owner can also profit from the data if the data is authorized to be used by some 3rd parties.
- Data consumer: may purchase data under the premise of compliance, and gain value through analysis. Among them, the tracking of data sources credibility is a pait point that nobody solved.
- Developer: develop high quality data analysis products for data consumers. They should be reasonably funded to maintain a healthy market.
- Platform developer: operations and supports are necessary to allow the roles mentioned to be fully satisfied and expressed.

To build a healthy and sustainable market, it requires top-level design and long-term operational support. Phala will integrate the fundamental infrastructure of data trading into a standardized protocol. Such a well-functioning data market will be one of the most important resources provided as a profitable commercial revenue segment while also functioning as a system-level application.

## 2.3 Roles

In Phala Network, Gatekeeper, Nominator, TEE Miner, and Phala DAO are the core roles maintaining stability of the consensus.

### 2.3.1 Gatekeeper

A Gatekeeper must be 24-7 online to manage the keys for miners, as a key manager is required to run the confidential contracts.

A Gatekeeper produces new blocks in Phala Network and manages key distribution in the system. He needs to stake enough PHA to be elected or to be nominated by one or more nominators who would stake enough PHA for him. In such circumstances, part of the staking belongs to nominators instead of Gatekeepers.

A Gatekeeper must run the Gatekeeper client on a highly-available, high-bandwidth trusted device. Each Gatekeeper node should always be ready to receive new parachain blocks and add them into mainnet blocks, which involves receiving, verifying, and re-producing block candidates.

In the early stage, we expect to have 50 Gatekeepers who all stake enough PHA to be elected . The staking must reach a certain amount though, we didn’t set a minimum or maximum of the Gatekeeper staking. Gatekeepers will be re-elected based on the staking amount for each Era (about 24 hours), and receive rewards or get slashes for honest behavior or malicious behavior (such as going offline or endorsing invalid blocks).

The NPoS consensus algorithm will punish a Gatekeeper for his failures. Unintentional errors at the beginning will only lead to reward deductions though, repeatedly intentional error will lead to stake burning. Demonstrable malicious behaviors such as double-signing will lead the system to confiscate all the guarantee (a small part of it to be burned, with the rest given as rewards information providers and honest Gatekeepers).

### 2.3.2 Nominator

Nominators are entitled to nominate a Gatekeeper and delegate them to maintain the network on behalf of themselves.

Nominators will also receive rewards or be punished if the Gatekeeper he or she nominated were rewarded or proved to be evil.

### 2.3.3 TEE Miners

The confidentiality of Phala's confidential smart contract is powered by TEE , which, similar to PoW chains, requires miners to run it on TEE enabled CPUs to execute confidential contracts. TEE miners will: access and profit from mining client which provides computing power for the network.

To guarantee rich computing power in the early stage, Phala will use preserved funds to attract miners through bounties and subsidies. The base and amount of bounties will be adjusted by Phala DAO Finance Committee. If the growth of trusted computing tasks could sustain miners' activity, the bounty will be reduced accordingly.

### 2.3.4 Phala DAO

Phala's governance is jointly participated by developers, Gatekeepers, investors, miners, and common users; as a DAO, they will be responsible for decisions making of community governance, development, finance, and the growth of the entire Phala Network.

Referring to the power distribution, Gatekeeper election, and proposal referendum of Polkadot though, Phala made its own innovations on voting algorithm and decision of committee:

- Adopt an on-chain secret voting mechanism to ensure the anonymity of voting through confidential contracts;
- Governance with Liquid Democracy – a fully free representative democratic system where anyone can delegate another voter with arbitrary random numbers of his votes which can be withdrawn at any time;
- Design our "Committee" as "DAO" which is open enough to let any eligible account address participate.

## 2.4 Consensus

Similar to Polkadot, Phala applies NPoS (Nominated Proof of Stake) Inflation Model on PHA issuance to reward Gatekeeper and nominators. The volume and rate of PHA inflation are flexible through sophisticated algorithms to appropriately guide token staking and achieve shared security and token liquidity.

### 2.4.1 NPoS Consensus Algorithm

NPoS is a consensus algorithm designed by Polkadot based on PoS algorithm. Validators run nodes to participate in the production and confirmation validation of blocks. Nominators can stake their own tokens for votes to obtain nomination rights to nominate validators they trust to get rewards.

The reward of NPoS mainly comes from the additional token issuance, which is the source of inflation as well.

### 2.4.2 PHA Economic Inflation

We expect 40% of tokens to be staked in the NPoS consensus system, and 60% to be used for resource expenditure and market circulation. Phala expects an annual inflation rate of 5% and the average annualized return on staking to be 12.5% at a 40% staking rate.

To achieve the expectation above, Phala prefers to guide the market through the following 3 rules :

- If the staking rate < 40%, the average annualized staking return > 12.5%, encouraging more stakings;
- If the staking rate = 40%, the average annualized rate of staking return = 12.5%;
- If the staking rate is> 40%, the average annualized staking return < 12.5%, encouraging redemption instead of staking.

A product with a 12.5% return rate, as we considered, is competitive enough compared with traditional financial products.

### 2.4.3 Formulas of Inflation Rate and Earning Rate

**Definition**

- staking rate \(X = PHA_ {Total staking} / PHA_ {Supply Amount}\)
- Annual inflation rate \(R = (PHA_ {end of year supply}-PHA_ {beginning supply}) / PHA_ {beginning supply}\)

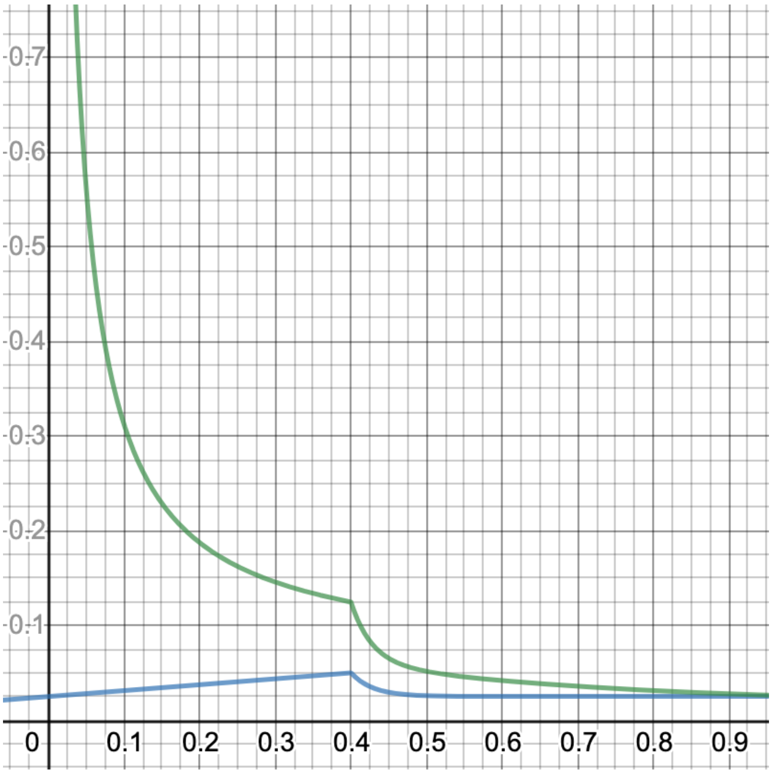
**Quantitative Parameter**

- Expected staking rate \(X_ {ideal} = 0.4\)
- Expected annualized return \(I_ {ideal} = 0.125\)
- Inflation rate when staking rate is 0 \(R_0 = 0.025\)
- Decay rate \(D = 0.02\)

**Formula**

- Inflation rate \(R_1 = R_0 + X * (I_ {ideal}-R_0 / X_ {ideal})\)
- Inflation rate \(R_2 = R_0 + (I_ {ideal} * X_ {ideal}-R_0) * 2 ^ {(X_ {ideal}-X) / D)}\)
- Inflation rate \(R = min (R_1, R_2)\)
- Annualized return \(i = I / x\)

Inflation Model Available for PHA:



From the figure above, the abscissa refers to the staking rate, the blue line refers to the annual inflation rate, and the green line refers to the annualized return.

### 2.4.4 Block Reward

Each time a block is generated on the mainnet, Phala system will issue a certain amount of PHA as block rewards. which The reward is flexible according to inflation rate related to the staking rate of the entire network. Block rewards are allocated according to the following rules:

- 80%: for the Gatekeeper that generated the block;
- 20%: going into a decentralized treasury which provides financial support for community contributors and developers, determined regularly by Phala DAO.

Among them, 80% is distributed to Gatekeepers who generated the block. Regardless of staking amount, all Gatekeepers have an equal chance to generate blocks.

Of the rewards distributed to Gatekeepers, part of the reward will be used to pay the commission set by Gatekeepers, with the rest paid to the nominators and Gatekeepers on a proportional basis (that is, proportional to the staking). Note that Gatekeepers will eventually receive two returns: first is the commission, second is the reward for their direct staking.

### 2.4.5 Sanction of Slashing

If a Gatekeeper betrays the rules (being offline, acting against consensus protocols, etc.), he will be punished, the same as his nominator – they will lose their PHA staking according to their staking ratio.

Once the slashing occurs, the more a Gatekeeper stakes, the more PHA he and his nominators will lose. It is designed to encourage nominators to nominate less-voted Gatekeepers to reduce the potential loss.

# III. PHA Token Distribution

## Objects

- To Enhance product-market fit;
- To Encourage encourage fully participation in community's early stage so to realize enough decentralization;
- To ensure stable procession of fundamental development.

Based on those above, questions below may occur:

## 3.1 Who Do We Serve?

Phala Network is aimed to serve the usage scenarios of the users of confidential smart contracts. According to the Web3.0 concept of Web3s, we made a "Separation of Powers" on roles using data on Phala Network:

- Data owner
- Data computation executor
- Data consumer

### 3.1.1 Data Owner

They are the base of Phala Network who store and manage their encrypted data. No one can integrate and use their data in an unauthorized way. We expect the "data custodian" model pervading nowadays in Internet companies could be overthrown, as "privacy protection" and "dto generate value from data monetization" coexist on Phala Network.

### 3.1.2 Data Computation Executor

- Providing environmental support for computing the development of infrastructure, such as Phala network developers
- Providing calculation computation execution, such as TEE miners

### 3.1.3 Data Comsumer

- The first type: developers. Influenced by the value of Web3 values, privacy protection bills, and consumer demands, developers will gradually be aware of data protection and respect user's rights more on their products . They are regarded as our potential users of Web3 Analytics or similar products and the majority in users of trusted computing power as well.
- The second type: Platforms such as eEnterprises and data analysis companies, etc. These clients form the consuming demand yet frequently meet problems such as fake data or illegal sources when they make payment in data markets. Using Phala will free them from such troubles: all data are traceable and verifiable.

## 3.2 How to Ensure Fully Community Participation?

- Fair-enough Token token distribution. Taking a look at PoW and EOS PoS ecosystem, you will find that a key to community prosperity is: the fairer the token distribution, the stabler and longer the community attraction is (a bad example: allow the foundation to hold over 80% of tokens).
- Reasonable participation costs. Participation costs shouldn't be too high nor too low. For example, it's unreasonable to force users to sacrifice their data or attend impossible tasks. Another example is EOS: too much airdrop in the early stage would cause loss in quality users and token value.
- Legality. The US Supreme Court established the "Howey Test" in the SEC v. W. J. Howey Co case to determine whether an exchange constitutes an "investment contract" and thus a "security." The Howey test contains four elements:
  - capital investment;
  - investing for a shared business purpose;
  - expecting to obtain profits without being personally involved but counting on the initiator or a third party.

    To avoid being recognized as a security and arrested for violation of relevant laws, Phala will not participate public sale such as ICO where users could earn returns by shares.

## 3.3 How to Sustain the Infrastructure Development?

At the beginning of the project, there must be a core team with sufficient passion and ability to build the network. At this stage we will do our best to build the ideal Phala Network without seeking profit.

But because of team costs, we need to set a budget to support the development.our vision. A small proportion of PHA token will be used for fundraising financing (less than 15%), and various types of sponsorship will be considered and pursued.

After the project is launched, we have to guarantee fundamental or even more development. At this stage, we will complete the basic development and code iteration will be supported with 5% of tokens and funding from the treasury. Our PHA will be unlocked stage by stage as we accomplish works of each milestone.

When the community is large and mature enough, the community will be 100% autonomous. Grants will be distributed through the treasury a reasonable budget committee system to support daily development, function iteration, and ecosystem development.

## 3.4 Fair Distribution Mechanism

Only with a fair enough distribution mechanism can the protocol find its own target market. Phala will adopt a strategy to distribute tokens "according to community contribution" as much as possible to those people who make actual efforts for Phala protocol.

The framework of Phala Network's token distribution rules is as follows:

| Module | Ratio | Description |
|---|---|---|
| TEE Mining | 70% | Fixed amount of token for TEE miners; isolated from the inflation |
| Stakedrop and IPO ( Initial Parachain Offering) | 9% | Obtainable though Polkadot ecosystem tokens such as KSM, DOT, etc.; |
| Testnet Incentive | 1% | For testnet incentive programs |
| Private Sale | 15% | Supporting Phala team to develop the project and build the community in the early stage. 60% of this section will be unlocked after the mainnet launch or token transfer enabled, with 20% unlocked every 6 months. |
| Developer Incentive | 5% | Incentives for the core buliders, among which 20% (10,000,000) will be unlocked after mainnet launches or token transfer enabled, with 5% unlocked every month |

## 3.5 TEE Mining

When most of the people are sinking in a dream of data monopoly, a few of them awaken. But how to awake everybody else other than geeks? How to persuade others to take the red pill of awakening?

We will use 70% of PHA to encourage the growing of a trusted world by inviting TEE miners, data contributors, and users into this war of privacy. We call it "TEE mining". Its rewards are designed as below:

- Predictable: there is a clear release curve that determines the amount of release over any period of time;
- Sustainable: release speed of rewards is controllable and sustainable for long-run ecosystem development;
- Fair-distribution: the distribution rules are fair enough against violation from attackers;
- High-performance: reasonable on-chain computation load.

To this end, we designed an Exponential Decreasing Release Model (similar to Bitcoin halving): reward release rate will gradually decrease over time. All roles of in our ecosystem have to compete for rewards, at a certain percentage to adjust tThe release speed of rewards is dynamically adjusted through the difficulty factor.

### 3.5.1 TEE Mining Reward Release

70% of PHA – 700,000,000 PHA – will be released by TEE Mining. The total amount of reward is fixed, and there would be no extra issuance. The ideal reward release decreases over time and fits the exponential decline function:

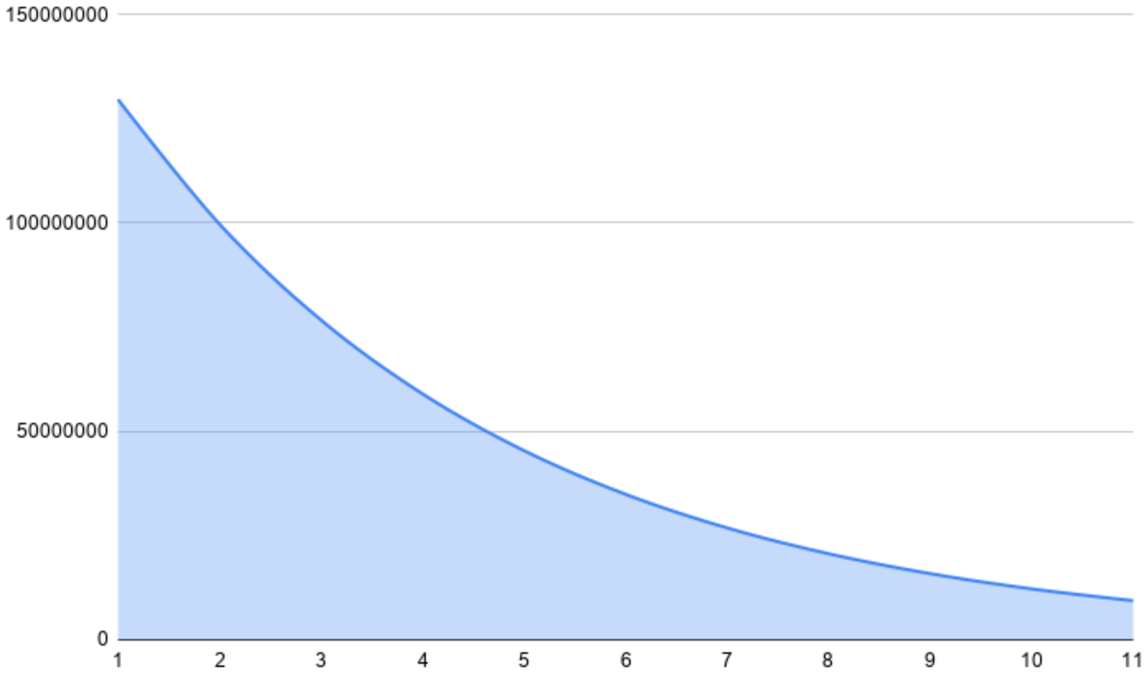
\\[ I_R(t) = I_{R0} \\cdot k^{t} \\]

Where \\(t\\) is the block time in Epoch, \\(I_ {R0}\\) is the initial release amount, and \\(k\\) is the attenuation decay coefficient factor of each Epoch, which satisfies:

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

The parameters used by Phala Network are:

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



From the figure above, it shows PHA reward attenuation is non-aggressive. We hope the initial miners can enjoy a high reward ratio while continuously supporting future computing power and data on the Network.

### 3.5.2 TEE Mining Reward Distribution

We want each type of our roles to be rewarded with a fixed percentage, as the total reward fits the release curve. However, it is unreasonable to strictly perform equal distribution proportionally in each Epoch, because reward events are prone to fluctuate a lot to generate large fluctuations (such as user data contribution), which is unfair and even negative for participants joining at different times . and even cause negative incentives.

Here by we introduced a difficulty adjustment mechanism based on an self-adaptive algorithm. The reward \(R_T(t)\) and the total reward \(R(t)\) for the role \(T\) are:

\[\begin{eqnarray} R_T(t) &=& n_T(t) \cdot k_T(t) \\ R(t) &=& \sum{R_T(t)} \end{eqnarray}\]

Where:

- \(n_T(t)\) is the number of reward actions in Epoch
- \(k_T(t)\) is the difficulty adjustment coefficient for the \(t\) period

By adjusting the difficulty factor, the expectation of \(T\)'s reward ratio could be adjust to meet the **ideal ratio** \(I_{PT}\), while controlling the sensitivity to fluctuations:

\[\begin{eqnarray} \mathbb{E}\big[\frac{R_T(t)}{R(t)}\big] &=& I_{PT} \\ \mathbb{E}\big[R(t)\big] &=& I_R(t) \end{eqnarray}\]

The incentivized roles and their ideal rewardshare ratio in Phala Network are shown in the following table:

| **\(T\)** | **\(I_{PT}\)** |
|---|---|
| TEE Miners | 30% |
| Privacy Computing Task Processing | 50% |
| Ecosystem Development (Treasury) | 20% |

The reward of each Epoch will be distributed through two queues:

| **Queue A** | **Queue B** |
|---|---|
| TEE Miners | Privacy Computing Task Processing |
| Ecosystem Development (Treasury) | |

- **How PHA reward is processed during each epoch:**
  - Queue A: for general rewards which will be automatically computed after each epoch ends
  - Queue B: for computing Task rewards
    - Miners who claimed and completed the computing tasks will share the PHA consisting rewards from all former non-computed epochs;
    - If there's no miner claiming computing tasks suring the current epoch, rewards will be automatically added to the prize pool of next epoch.

- **How often does Phala Network distributed the mining rewards**: 1 batch / 2 epochs

### 3.5.3 TEE Mining Difficulty Design

The difficulty coefficient factor of TEE mining is determined by weighted historical difficulty coefficient factor and adjustment target. The target difficulty coefficient factor is the value that satisfies the ideal proportion and ideal reward release:

\[ k_T^*(t) = \frac{I_R(t) \cdot I_PT}{n_T(t)} \]

The adjustment factor is weighted exponentially:

\[ k_T(t) = \left\{ \begin{array}{lcl} k_T^*(0) && {t = 0}\\ (1 - \lambda) \cdot k_T(t-1) + \lambda \cdot k_T^*(t) && {t > 0} \end{array} \right. \]

where for the weighting factor \(\lambda \in [0,1]\), the higher the value is, the more sensitive it is to the fluctuations. A reasonable \(\lambda\) can effectively adjust the difficulty of mining and achieve the expectation of the total reward and reward ratio in line with the ideal value.

Phala Network adopts \(\lambda = 0.2\).

### 3.5.4 Reward Details of TEE Miners

The previous approach only discussed the case where all rewards within each role are shared equally to simplify the formula. Yet in actual cases, the amount of rewards should be determined by the attributes of the participants. For example, the unit reward of high-performance TEE miners should be proportionally higher than that of normal TEE miners.

We thus introduced a weight \(w_ {Ti}\) for each role \(T\), which represents the weight of the \(i\)-th type reward behavior. The previous formula can be rewritten as:

\[\begin{eqnarray} R_T(t) &=& k_T(t) \sum_i{n_{Ti}(t) \cdot w_{Ti}} \\ k_T^*(t) &=& \frac{I_R(t) \cdot I_PT}{\sum_i{n_{Ti}(t) \cdot w_{Ti}}} \end{eqnarray}\]

Which means, the actual reward obtained for each behavior is the product of the reward factor and the difficulty factor. The scoring of different roles and their reward behavior is determined by specific attributes.

### 3.5.5 Online TEE Miner

An “Online TEE Miner” refers to a TEE device online in an epoch. Each TEE device can be identified as one miner. As long as a miner participates in the network, they are already contributing to the supply whether they execute computing or not. And mining rewards will be obtained.

Phala will score TEE miners according to the following variables:

- Confidential Points (CP): the score measuring a miner from several aspects, including CPU threads, baseline performance, memory size, etc. The performance test will be open-sourced together with Phala codes.
- Totla Online Time: the longer the time a miner runs, the higher his score is.
- Number of successful executions: the number of extrinsics processed.
- Slash Rate:
  - Slash rate = number of slashed times / total number of processed extrinsics (the lower the better)

Weights of parameters:

| Behavior | Weight |
|---|---|
| Running Online | High |
| CP | Medium |
| Sum of Historical Online Time | Low |
| Number of Historicla Processed Extrinsics | Low |
| Historical Slah Rate | Negative |

To filer trusted and qualified TEE devices and better protect Phala Network, it is required that a miner has to stake a certain amount of PHA as bail for him to start mining.

- The staking requirement is fixed as 1,620 PHA per CPU core in the early stage.
  - if you are using 4-core devices, you have to stake 6,480 PHA for 1 device, 12,960 PHA for 2 devices, etc.
- The staking amount can be adjusted through referendum after 6 months of mainnet launches.
- Once staked, it will need 7 days to unbond.
- Phala will integrate a system-level protocal for miners to “borrow” staking PHA from “mining nominators”. The latter can share PHA return of the miner just as he stakes to validators of Gatekeepers. **With help from PHA lenders, a miner could start mining without costing too much on PHA trading**.

### 3.5.6 Privacy Computing Tasks

Three types of roles will be involved in this section:

- Online TEE Miners
- Computing TEE Miniers

### A. Task Distribution and Rewards Computation

Tasks will be delivered to TEE miners according to:

- Security Priority: miners who staked more PHA would be considered as more trustful and securer devices.
- Comtuing Performance Priority: Devices with higher Confidential Points would be considered as more reliable miners to process the tasks.

### B. Computing TEE Miners

Computing TEE Miners refers to miners who be responsible for computing power processing. They will gain rich returns for their work.

The Confidential Points would be the main reason for a miner to be chosen or not chosen. CP Indicates the number of tasks a miners can process and the user experience a miner can offer.

In real situations, Computing TEE Miners would shoulder important value to maintain security for the whole network. Thus Phala does not set any limitation on the PHA staking amount. We believe that the higher a miner stakes, the higher his cost is to do evil, which means the less security risk he shall cause.

The design of Computing TEE Miner is as follows:

| **Behavior** | **Weight** |
|---|---|
| Staked PHA | High |
| CP | Medium |
| Sum of Historical Online Time | Low |
| Number of Historicla Processed Extrinsics | Low |
| Historical Slah Rate | Negative |

## 3.6 Community

We hope our token distribution to be as fair as possible while, through opportunity cost, filtering target users who recognize and value Phala's vision. After researching relevant cases (Edgeware's LockDrop, NuCypher's WorkLock, and Rocco's Warlock), we consider LockDrop as a feasible good idea.

Combining the purpose of Phala's design, we improved WorkLock model and decided to hold two waves of PHA LockDrops:

- KSM Stakedrop: to receive PHA and KSM return through KSM staking;
- DOT Lockdrop: to support Phala and receive PHA by participating in the first parachain slot auction (IPO);

Among them, DOT Lockdrop will be launched for the first parachain slot auction, possibly based on the auction contract of Polkadot mainnet. In return, participants will receive PHA equivalent to their staking;

### 3.6.1 KSM Stakedrop

Stakedrop is a brand-new type of airdrop which requires participants to stake KSM to **"whitelisted validators"** for a certain period to receive **stakedrop points**.

To free the value of airdrop from mainnet launching time, airdrop PHA will be distributed to ETH addresses as erc20 tokens. An open-source script will be applied to monitor the staking statistics 24/7. If a participant met the requirements, he or she would be able to claim PHA on Ethereum.

#### 1) Brief

- Total amount: 27,000,000 PHA (estimated as 2.7% of the total supply and might occupy the amount of wave 3 Lockdrop if it were over-distributed)
- Who can participate: KSM holders (members from Kusama and Polkadot community)
- How-to: Stake KSM to Phala's whitelisted validators for 30-90 days.

Stakedrop is featured for:

1. 0 opportunity cost: one can receive both KSM returns and PHA rewards during the event
2. 0 threshold: one can easily claim his or her PHA after staking and waiting.
3. 0 influence on governance: all Kusama validators who have set their on-chain identity would enter **the whitelist** and help their nominators to win PHA. Nominators have enough choices instead of nominating only a few of them, erasing the democracy of Kusama governance.

#### 2) Model of Stakedrop

Formulas

1. Ideal Prize Supply: \[Q_{ideal} = 27,000,000\ \text{PHA}\]

2. Stakedrop points: \[P = Rank(Days) \cdot Lock_{KSM}\]

3. \(Rank(d)\): Score of staking period
   \[Rank(d) = \frac{1}{30} d \cdot 1.01^{(d-30)}\]

4. \(Q_{ideal}\) will be shared proportionally according to \(P\). If the usm of \(P\) exceeded the upper limit \(P_{max}\), participants would claim by a fixed exchange rate.

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

#### 3) Supply of Stakedrop

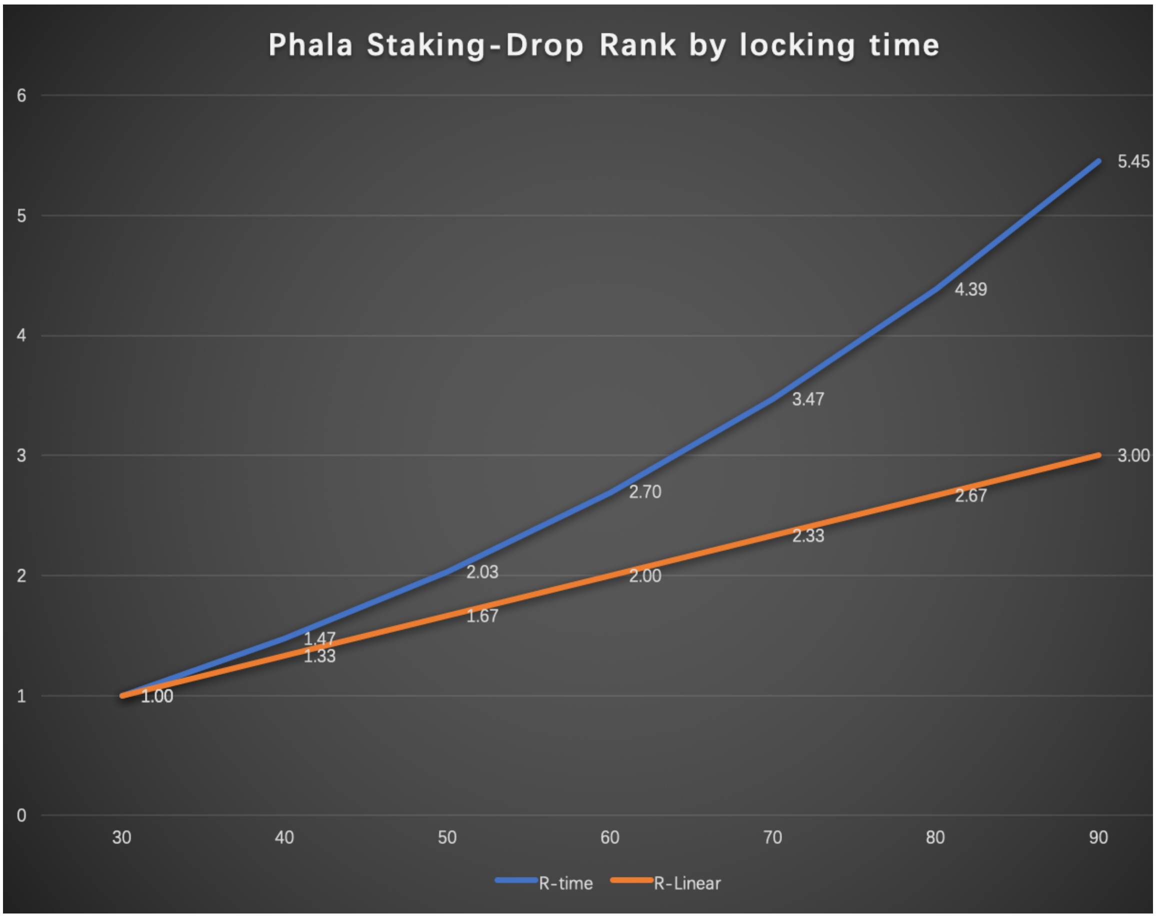
The baseline of stakedrop reward exchange rate is 1 KSM = 1 PHA.

- If the total amount of stakedrop KSM $\leqslant$ 2,700,000 KSM:
  - Participants will share the 27,000,000 PHA proportionally.

- Else:
  - Participants will claim PHA by the baseline exchange rate. This means the total supply of airdrop will exceed 27,000,000 PHA, squeezing the reward amount of wave III airdrop.

### 4) Weight of Prize

In general situations, the locking reward is linearly relevant to the locking period parameter \(Days\) (the orange line below). But in Stakedrop, as it's almost costless for participants to receive rewards, we deigned the parameter \(Days\) to be exponentially relevant to staking reward.



# IV. Governance of Phala

## 4.1 Mechanism

It is quite professional for Polkadot to introduce modern democratic system into their community governance. There are 3 highlights in Polkadot's system that can't be ignored:

- All the on-chain changes are decided by governance, instead of a few parameters;
- Set a council to interact with the referendum mechanism;
- introduce the concept of staking time for voting weight.

Phala, then, absorbing and adopting those advantages of Polkadot, proposes our own innovations:

- Anonymous voting: using confidential contracts to complete voting to guarantee democratic anonymity;
- Liquid Democratic Voting Mechanism and relevant algorithm: to fully increase the voting participation rate;
- Introduced DAO instead of Committee: to increase openness and align the interests of decision makers and the community by staking.

## 4.2 Introduction

### 4.2.1 Vision

- Highly-democratic and open: PHA will be the only token representing public opinion
- Highly-participated: we will lower comprehension costs and barriers to participation
- Expert-combined: Decision-making teams should be capable of giving expert suggestions

### 4.2.2 Governance Model

- Everyone can draft his proposal which will only be valid after passing the referendum.
- To introduce DAO working as parliament in a representative system for professional proposals which can balance the blindness of referendum through professionalism.
- Each wave of referendum and DAO election will be completed through anonymous voting and Liquid Democracy

### 4.1.3 Participants

- PHA holders: The core of Phala governance is the PHA token, which enables direct and efficient participation in community proposals. PHA holders may initiate proposals, change the order of proposals, vote on all valid proposals, elect Phala DAO members, and apply for a Phala DAO member.
- Phala DAO: It is elected through democratic election. To align the interests of participants and Phala protocol, we set the rules similar to Monoch DAO that one must stake his PHA to exchange shares in DAO and get back the tokens through his quitting with specific requirements. Phala DAO will be responsible for initiating or nullifying proposals (professional and highly-participated).

We can tell from above that any PHA holder may submit a proposal; all proposals require a referendum to pass; The elected Phala DAO has certain veto power over the rationality of the proposal, yet balanced by the democracy of the whole people.

## 4.3 Proposal and Referendum

### 4.3.1 Proposal Contents

All amendments to Phala protocol require a referendum to be validated, including but not limited to:

- Code upgrade
- System parameter adjustment
- Changes in governance rules
- Treasury allocation
- Elections and recalls

### 4.3.2 Proposal Procedure

Each member is entitled to submit a proposal with a small amount of PHA staked though, proposals will only be validated after the referendum.

Phala DAO will vote to filter proposals first to nullify garbage ones. High-weight proposals will be prioritized and entered into the referendum stage; while the ones which do not receive a majority of DAO votes may not enter the referendum stage.

Proposals approved by DAO require a majority of referendum votes before they can be implemented.

Each approved proposal has to wait for a certain period of time before it is actually applied on the chain. This allows participants who disagree with the proposal to leave (such as selling tokens in their hands), and tokens of supporters will be locked until the proposal is executed.

### 4.3.3 Referendum

Given the voting rate data of mainstream blockchains, we believe it is necessary to lower the participating cost of referendum while managing well the democracy where a low voting rate exists. The rules of Phala's Liquid Democratic Secret Voting will be as follow:

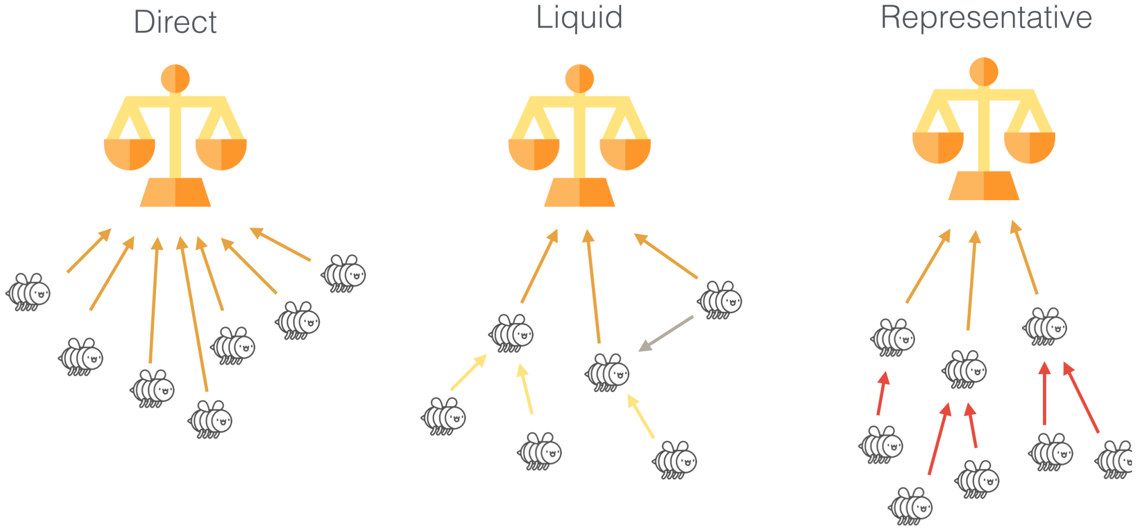
- Each member may delegate a representative with a arbitrary number of votes he or she holds; the delegated person may delegate others to split his or her votes as well;
- Each member may delegate a representative with a arbitrary number of votes he or she holds; the delegated person may delegate others to split his or her votes as well;
- The amount and time of PHA staking will determine the voting weight. Staking time shall not be shorter than 4 weeks;
- We apply majority rule and there is no requirement of minimum voting rate.

### 4.3.4 Algorithm of Liquid Democray

Direct democracy, a mechanism where proposals are decided through each single vote from each person, reflects the populist attitude of the voters, yet with obvious shortcomings such as low voting rate and voters' unknown intelligence. Indirect democracy, a mechanism where voters vote out representatives first and delegate them to make decisions on behalf of themselves, is the most commonly implemented political system in real society. It's rather achievable, more professional, and more rational, yet easily-corrupted and mobility-freezing.

Liquid democracy originates from Bryan Ford's paper "Delegative Democracy" published in 1884 – for a certain issue, one can vote directly, or to delegate the right to a representative. We referred to the paper published by ASrearch on arXiv – *Implement Liquid Democracy on*

*Ethereum: A Fast Algorithm for Realtime Self-tally Voting System* – to research its application on the blockchain community.

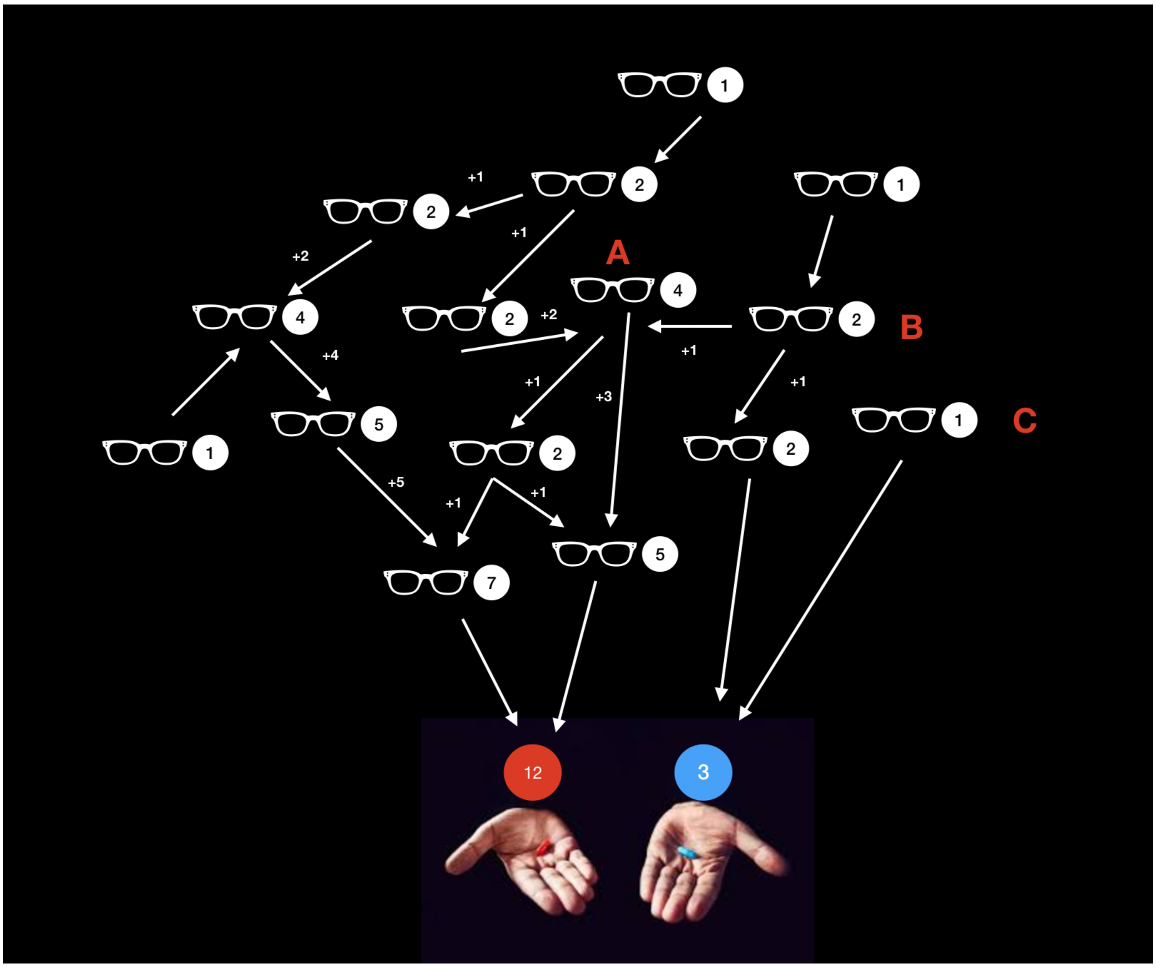


From Liquid Democracy, Ethereum, and the slow path to revolution.

In the paper, Ford found a typical example of liquid democracy: Googlers' votes on lunch. To decide what to eat at lunch, one can ask a colleague to choose for him or her. The advantage of liquid democracy lies in the compromise between direct democracy and indirect democracy, which not only guarantees a real and pure democracy, but also increases the turnout rate and can solve problems professionally and rationally. However, the implementation could be quite complicated and requires frequent and real-time votes counting.

Here we may refer to another example. If we assume in "The Matrix", Morpheus was not asking Neo but Smith – which pill would you take: the red pill to reality, or the blue pill to virtuality?

If there were 15 Mr. Smiths, each Smith has the right to vote, 1 vote per person, this decision would require 15 votes to validate. Each Smith can delegate his vote to other Smiths. If we take their vote sequence as their serial number, it is likely that the following will happen:



- A Smith is a KOL with a lot of prestige and love to share power: he not only got 3 votes from others, but also delegated his 4 votes to 2 other Smiths as 1 vote and 3 votes;
- B Smith, can't make his decision, so he simply bet all his votes on both of the two parties;
- C Smith is determined and does not believe that others can carry out his democratic intentions, so he voted for Blue Pill (reality).

In a liquid democratic DAO, the delegation relationship is progressed as a dendrogram. To calculate and update the number of votes, it is necessary to process preorder traversal or postorder traversal when each vote occurs. The complexity of time cost would be O(n).

It is hard to achieve in traditional blockchains but achievable on Phala Network. Liquid democracy computation requires mass data processing which is infeasible in a blockchain. Yet with TEE technology, we can perform liquid democracy with efficiency and confidentiality.

### 4.3.5 Secret Vote

If the delegated relationship could be observed by the entire network, it would be worthless to hold a secret vote because finding a bribery method through data computation or data mining can be easy. This is the reason why democratic voting is anonymous at most of the time.

But, as a confidential smart contract platform, Phala Network is able to make each election verifiable and trusted in system design as trust relationships could be calculated confidentially.

## 4.4 PhalaDAO

Phala's governance will be managed through DAO instead of a representative committee system or the House of Lords system.

As a team with DAO experience (founder of memeDAO), Phala team will take Moloch DAO as a reference for Phala DAO design. MolochDAO is a decentralized funding coordination system that allocates funds for Ethereum development projects. It was established to coordinate the decision-making process and achieve rapid on-demand allocation of funds. To join MolochDAO, an invitation must be made by an existing DAO member.

DAO members will investigate background, reputation, and other indicators to assess whether potential members can provide sufficient resources for the entire team. Once staked, one will claim DAO shares. With these shares, all members can propose, vote, or leave the DAO by destroying the shares. When a financing proposal is approved, DAO shares could be immediately converted into PHA. In essence, DAO deconstructs an organization into decision-making processes, motivating its members to join or leave efficiently.

### 4.4.1 To Join Phala DAO

The voting right of DAO is defined as "Share". Share is non-transferable and can be issued indefinitely though, the total proportion is always fixed as 100%. DAO's decision-making system follows the majority rule and output results as "approve" or "disapprove".

Phala's core team will establish Phala DAO by staking PHA. The initial shares of Phala DAO will be set at a deposit price. After that, anyone can claim shares corresponding to the deposit by submitting a DAO application and passing the referendum election.
From a voter to a member, the following process is required:

- Set the number of Shares you need, and stake a number of PHA into protocol. These PHAs will enter Fund Pool A of DAO;
- System will automatically judge whether the exchange rate of wanted shares and staked PHA is higher than current rate; if it's lower, a candidate has to be approved in DAO's "motion" before he is voted in a referendum.
- If the exchange rate of a candidate is equal to or higher than the current one, his application will directly be voted in referendum, whose result shall not be denied by DAO.
- Candidate will become a member as the referendum passes his application and claim shares equivalent to his votes.

It is noted that, as candidates have staked their PHA to pool A for application, PHA in pool A can't be used for referendum or staking for profits. This will protect DAO from being manipulated by big holders.

To quit Phala DAO, the following conditions must be met:

- Within the 48-hours "cool-down period" after a motion has been passed or the "referendum" period or;
- In the "motion" of DAO, voted a "NO" for a passed proposal or a "YES" for a rejected proposal;
- Submitted an application to quit if the two above were met. DAO will refund the PHA equivalent to one's shares.

Such design takes Moloch's "Ragequit'' as a reference and can largely reduce communication costs. It ensures that members of Moloch who don't like some proposal may quit as they wish with their funds. Thus coordination costs can be reduced to almost zero.

### 4.4.2 Decision-making System of Phala DAO

Phala DAO has the right to filter proposals, which is called "motion". Only proposals filtered and passed in motion can enter a referendum.
Phala DAO's Voting System:

- Phala DAO internal voting is based on Share votes;
- rule of majority works with no minimum voting rate limit;
- "motion" will start 48 hours after each proposal is initiated. Results will be cleared and announced within 7 days. Approved proposals will be voted in referendum and only one proposal may be voted on chain within a certain period.
- If the motion is passed in a quite short time, it will be able to enter the referendum queue after 48 hours without waiting for another 7 days.

Contents of Phala DAO's Decision:

- "Motion" of any proposal: it is up to the DAO to decide whether or not a proposal can be passed. Approved ones will be ranked by weights and disapproved ones will be non-effective;
- Management of DAO members: shares resolution corresponding to pool A;
- Decentralized Treasury (Pool B) Proposal: can only be initiated by DAO members;

### 4.4 Treasury

The income of Treasury mainly comes from:

1. Ecological donation from TEE mining;
2. Taxes charded from the 20% tax rate of NPoS.

Funds will mainly be used in:

1. Long-tern grant
2. Allotment of proposals

Long-tern grants would be desigend as a standardized system in which parameters can be changed by Phala DAO members.

**Case: grant long-tern developers with 50% of Treasury revenue**

1. Submit a proposal and clarifying all the requirements
2. If passed, the proposal will be part of the automatically procedure and 50% of the income will be delivered to the development team everytime when there's income into Treasury.
3. It can also be suspended according the same procedure.

Procedures of proposal allotments would be the same with normal proposals.