Acala: The Decentralized Financial Network for Stablecoin and Staking Liquidity

Version 0.9 | January 2020

By the Acala Foundation
https://acala.network/

Abstract
This paper will introduce and elaborate on two decentralized protocols that enable cross-chain financial stability and liquidity on the Polkadot network - the Honzon Stablecoin Protocol and the Homa Tokenized Staking Liquidity Protocol, and briefly on the plan for participating in Polkadot parachain auctions.

See an introduction of the Acala Foundation, the vision of the project, and a high-level introduction of the Acala Network here

- 1. Introduction
- 2. Honzon - The Stablecoin Protocol
  - 2.1. Multi-Collateral-Type CDP
  - 2.2. ACA Token Utility & Governance
  - 2.3. The CDP Process
  - 2.4. Price Stability Mechanisms
    - 2.4.1. Risk Management
    - 2.4.2. Adjusting Liquidation Auction Parameters
    - 2.4.3. Adding New CDP Collateral Asset Type
    - 2.4.4. Removing Existing CDP Collateral Asset Type**
    - 2.4.5. Adjusting Oracles
    - 2.4.6. Making Network Upgrade Decision
    - 2.4.7. Triggering Emergency Shutdown
  - 2.5. Automatic Liquidations of risky CDPs
  - 2.6. Emergency Shutdown Procedure
    - 2.6.1. Single Asset Liquidation
    - 2.6.2. Global Liquidation
  - 2.7. Key Actors
- 3. HOMA - The Tokenized Staking Liquidity Protocol
  - 3.1 The Homa Protocol
  - 3.2 Staking
  - 3.3 Redeeming
  - 3.4 Tokenized Staked DOT: L-DOT
  - 3.5 Staking Strategy
  - 3.5 Governance
- 4. Initial Parachain Offering (IPO)
- 5. Summary
- Reference

CRYP2NOVA

Archived copy · cryp2nova.com

1. Introduction

Despite the promises and hopes that cryptocurrencies have brought to our future - a future of open-source, decentralization, redistribution of power, fairer, more truth and less trust, they remain extremely volatile with prices fluctuating rapidly and unpredictably, and can hardly be usable as a medium of exchange. **Stablecoin** since its inception to now widespread popularity (at least in the crypto world), **has proven its utility beyond speculation**: they have been used in alleviating economic and political hardship, and as a hedging mechanism for traders.

The existing USD stablecoins are most prevalent on the Ethereum platform, just to name a couple of USDC (centralized stablecoin) and DAI (decentralized stablecoin). In the decentralized stablecoin realm (using an over-collateral mechanism for securing the stablecoin), **single network assets are fundamentally limited by its underlying ledger** and the assets available on that platform as collaterals, hence **limiting their usage and adoption**.

The significance of cross-chain communication to the blockchain is like that of the internet to the intranet. Polkadot empowers a network of public, consortium and private blockchains, and enables true interoperability, economic and transactional scalability. **Acala is a first-of-its-kind decentralized finance consortium** delivering a set of protocols e.g. a stablecoin protocol to serve as Polkadot's DeFi building block. Acala's cross-blockchain stablecoin network will:

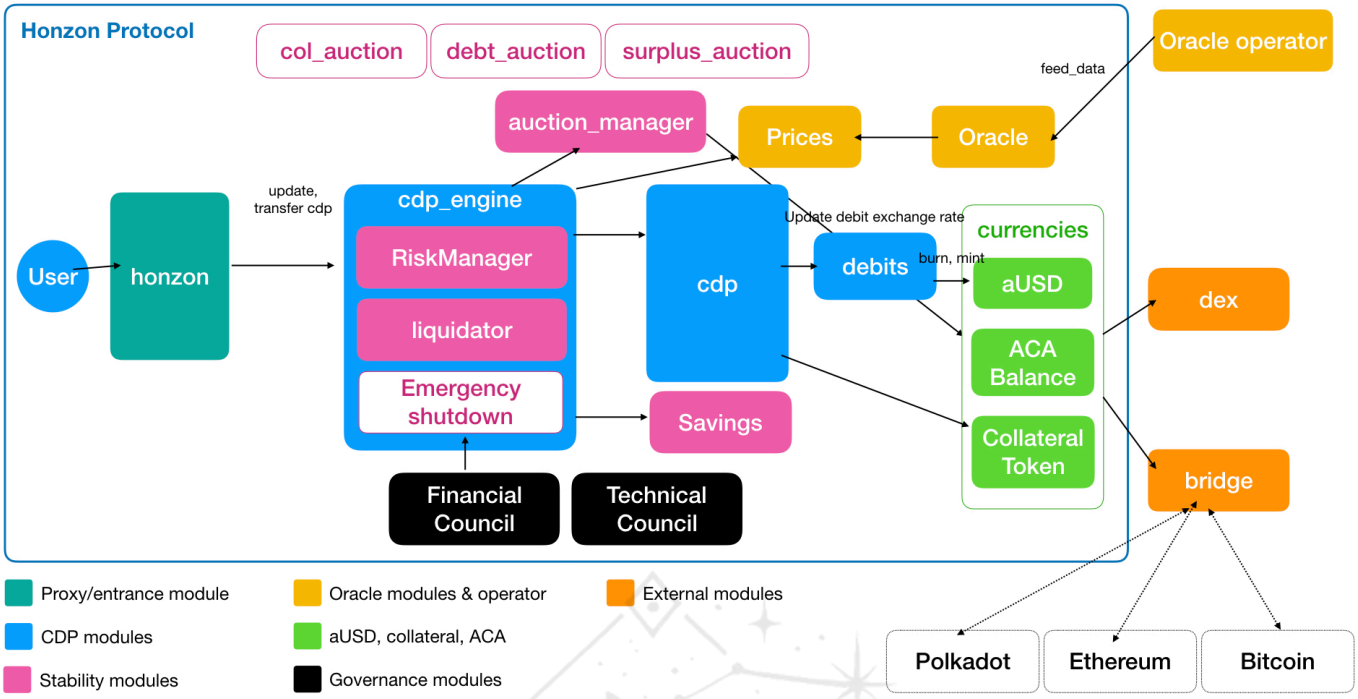
- create **a sound, stable currency** for low cost, borderless value transfer for all blockchains that are connected in a network
- collaterals can be from both Polkadot network and any other connected networks to achieve higher supply ceiling
- leverage Polkadot's **shared security** mechanism, to have the highest security on day one
- achieve true decentralization and censorship resistance through its consortium setup and token release model
- be a **specialized stablecoin network** that can have customized fee schedule while maintaining the security
- be **future proof with forkless and non-disruptive upgrade** with an on-chain governance
- serve as a building block for more open finance services

The Acala Dollar stablecoin (ticker: aUSD) is a multi-collateral-backed cryptocurrency, with value stable relative to the US Dollar (1 aUSD ≈ 1 $US). It is completely **decentralized**, that it can be created using assets from blockchains connected to the Polkadot network including **Bitcoin (BTC) and Ether (ETH) as collaterals**. It can be **used by any blockchains (or digital jurisdictions) on the Polkadot network** as well as applications on those chains.

Anyone who owns the type of crypto assets supported by the ACALA network can leverage them to generate aUSD tokens by creating a Collateralized Debt Position (CDP) through the Honzon protocol. Anyone may also choose to acquire the aUSD tokens by buying them from brokers or exchanges.

2. Honzon - The Stablecoin Protocol

Archived copy · cryp2nova.com



token: while the balance module handles the native token on the Acala Network, the `token` module supports additional multiple assets on the chain, to manage balance and transfer tokens.

currencies: makes the Acala Network a multi-currency chain by aggregating the `srml-balances` and `orml-tokens`

oracle: is an implementation of `DataProvider`, and a common price feeding module, storing incoming price in a key/value map.

prices: provides the price for an asset in chosen base currency; it uses asset prices in USD from `DataProvider`

auction: is a common auction interface for bidding on an item. How a particular auction is performed and settled is managed by individual implementation of `AuctionHandler`

The above modules are generic common good utilities that can be used for any projects. They reside in the Open Runtime Library.

honzon: is the proxy module that users will interact with for stablecoin functionalities such as create, update and transfer CDPs

cdp_engine: manages auctions, risks (to enforce stability fees, collateral ratio, debt ceiling, debt to asset ratio etc.), and liquidation

auction_manager: implements `AuctionHandler` and handles collateral, surplus and deficit auctions, manages auction parameters such as increment size, and duration etc.

cdp: manages maps of debt positions for accounts and collaterals, updates debt positions by updates aUSD balance via the `debit` module, and updates collateral balances

Archived copy · cryp2nova.com

debits: accounts for debt balance for given collateral when a loan or cdp is created/updated/closed, based on collateral to aUSD exchange rate; it also takes into account of stability fee (or interest rate) and updates the debit exchange ratio every period (e.g. every block)

other modules: `primitives` module defines constants such as collateral currencies supported, `support` module for defining types

Find more details here

2.1. Multi-Collateral-Type CDP

Every aUSD is backed in excess by a crypto asset and is stabilized against the US Dollar, through the Honzon Protocol - a dynamic system of Collateralized Debt Positions (CDPs), on-chain governance and incentivized key actors. The CDP mechanism design is inspired by the first decentralized stablecoin project MakerDAO, which has become the DeFi building block in the Ethereum ecosystem. Together with a set of incentives, supply & demand balancing, and risk management mechanisms, as the core components of the Honzon stablecoin protocol on the Acala Network, the value of an aUSD token is pegged to the value of a US Dollar, with relative stability.

Collaterals can be either native Polkadot assets like DOT, or beyond. For instance, popular assets like BTC and ETH can be bridged into the Polkadot network and used as collateral to achieve a higher supply ceiling. Stablecoins powered by the Acala Network can be transferred to all chains in the Polkadot network, which will boost its liquidity and adoption to a degree that a single-chain asset would not be able to achieve.

Every CDP holds the collateral assets deposited by the user who opened the CDP that created the aUSD tokens, together with its associated aUSD debt position. The deposited collateral assets inside the CDP is locked and cannot be withdrawn by the user until the associated aUSD debt is paid back. Active CDPs are always over collateralized with the collateral with value that exceeds the value of the debt.

Unlike Ethereum, where an external liquidator is required to monitor and close dangerous positions, which is by and large due to the limitation of Ethereum, the Honzon Protocol is able to use Off-chain Worker - an automatic scheduler service unique to Substrate - to automate this process and inherently increase security and stability of the stablecoin.

2.2. ACA Token Utility & Governance

ACA is the native token of ACALA Network. The total supply of the ACA Tokens will be minted at the launch of the mainnet and stored in the ACA Reserve Pool to be distributed to ACALA Foundation, Seed Investment Partners, IPO Participants as Reward, and the rest sold to the public.

ACAs serve three key functions in ACALA Network:

- **Network Utility Token**
  ACA tokens are used for paying network transaction fees, stability fees (interest rate of the aUSD loan), and penalty fees in case of liquidation.

  To close any CDP that has been created to generate aUSDs in the ACALA Network, some ACA tokens are required to be paid as the Stability Fee. Unique to the ACALA Network, an equivalent amount of aUSDs or other supported assets can be accepted as payment of fees, which can be automatically exchanged to ACA via the built-in exchange. When ACA is received, it is burned and removed from the supply permanently. As market demand for aUSDs and CDPs increases, demand for ACA increases as

Archived copy · cryp2nova.com

users needs them to pay the Stability Fee.

All active CDPs are constantly monitored by the system, and for each type of collateral, ACA holders would vote for a liquidation ratio - the mininum collateral-to-debt ratio required to avoid liquidation of an open CDP. Once the collateral-to-debt ratio has fallen below the liquidation ratio, then the CDP becomes risky. The CDP will then be automatically liquidated by the system in a Collateral Auction mechanism where a liquidation penalty paid in aUSD will be deducted from the collateral sales. The liquidation penalty will be automatically used to purchase ACA tokens in an exchange by the system, which will be burnt and permanently removed from the ACA supply.

- **Governance of the Network**
  As a governance token, ACA token holders have rights to propose network upgrades, and risk parameter adjustments (such as Stability fee, Debt Ceiling, Liquidation Ratio, and Liquidation Penalty), which will be approved or declined by the elected on-chain General Council. Note that, merely holding the ACA token does not entitle holders to any rights to returns generated by the Acala Network.
- **Contingency Solution**
  In situations such as a sudden price collapse of a collateral asset resulting in under-collateralized CDPs, ACA tokens will be automatically diluted and sold on the market for system recapitalization.

2.3. The CDP Process

- **Depositing Collateral**
  To create a CDP, the user firstly sends a request to Honzon protocol and deposits the crypto asset that will be locked as collateral to become a CDP holder. While multiple types of crypto assets are supported by the Honzon protocol, only one single type of asset is collateralized in the creation of a particular CDP.
- **Borrowing aUSD and Opening CDP**
  The user would send a request to borrow the desired amount of aUSD tokens, capped by the quotient of the value of the crypto assets deposited and the collateral-to-debt ratio. The Honzon protocol would lock the asset deposited, then mint the aUSD tokens accordingly, and mark the same amount as a debt in the CDP. The locked collateral will not be released until the outstanding debt in aUSD is paid.
- **Paying back aUSD and Stability Fee**
  If the CDP holder wants to close an active CDP that is not at risk, he needs to deposit enough aUSD tokens to pay back the outstanding debt in the CDP, as well as to pay a stability fee, the accumulated cost of borrowing the aUSD. The stability fee can be paid in ACA tokens, or in aUSD that will be exchanged to ACA tokens automatically by the system.
- **Closing the CDP**
  After receiving the outstanding aUSD in debt and the stability fee, the CDP becomes debt-free, that the CDP holder is able to retrieve his collateral back and the CDP is then closed by the Honzon protocol.

2.4. Price Stability Mechanisms

1:1 Peg to US Dollar

The aUSD is designed to peg to US Dollar at 1:1 ratio that the ACALA Network aims to maintain the value of one aUSD token approximate to one US Dollar at all times. Our unique strong peg to US Dollar is achieved through an automatic risk management algorithm within the Honzon Protocol together with community governance. More details on them in the following sections.

Archived copy · cryp2nova.com

2.4.1. Risk Management

ACA token holders have governance rights and responsibilities for managing risks of the ACALA Network, including authorizing manual or automatic (algorithmic) adjustments of risk parameters.

Since multiple types of crypto assets with different risk profiles are accepted as collaterals of CDPs, all risk parameters of CDPs and liquidation auction parameters are set up separately across collateral types and are to be adjusted by the Honzon Protocol automatically or by voting of ACA token holders.

Adjusting Risk Parameters of CDPs

- **Stability Fee**
  Adjusting stability fee or interest rate is one way to influence the supply and demand for aUSD loans consequently stability of its price. To close any active CDP, some ACA tokens are required to be paid as the Stability Fee, charged in the percentage of the outstanding debt of the CDP, presenting interest payable of the debt position. An equivalent amount of aUSDs at the current market price is also accepted by the official portal and will be exchanged to ACA automatically. When ACA tokens are received, they are burnt and removed from the supply permanently.
- **Liquidation Ratio**
  The price fluctuation of underlying collateral assets affects the risk profile of the borrowed aUSD, hence adjusting the liquidation ratio to a degree creates a stability shell of the stablecoin. The collateral-to-debt ratio of all active CDPs is monitored constantly by the system, by dividing the current market value (in aUSD) of the collateral locked in the CDP by the outstanding debt balance. Once the current collateral-to-debt ratio of an active CDP becomes lower enough that it reaches a certain threshold, the Liquidation Ratio, the system will automatically trigger a liquidation of the CDP. A more risky collateral asset type is usually associated with a higher Liquidation Ratio, and vice versa.
- **Liquidation Penalty**
  The liquidation penalty is a disincentive for users to leave a position in danger, hence provides additional safeguard and stability of the stablecoin. All active CDPs are constantly monitored by the system, once the value of the CDP collateral has fallen below the liquidation ratio, the CDP is regarded to be risky and is automatically liquidated by the system that a liquidation penalty in aUSD will be charged to the CDP holder and sourced from the collateral sale auction. The liquidation penalty will be automatically used to purchase ACA tokens in external exchange by the system, which will be burnt and permanently removed from the ACA supply.

- **Debt Ceiling**
  For each type of asset that can be used as collateral for CDPs, a maximum amount of total outstanding debts in aUSD, the Debt Ceiling, is preset to cap the total collateral of such assets in the ACALA network, which ensure both diversification and risk management of the collateral portfolio. Once the Debt Ceiling for an asset is reached, no new CDP can be generated until some existing CDPs are closed.

2.4.2. Adjusting Liquidation Auction Parameters

The auction process is an essential mechanism to balance profit and debt accumulated in the system - it's the pedestal that upholds the stability of the entire system. The global debt (issuing and burning aUSD) is managed by CDP Treasury. The stability fee is calculated in each block and is accounted for as system profit. For risky CDPs, the system will take over the debt as system debt, it will then auction off part or all of its collateral to repay outstanding positions. Periodically, the system will balance its books, that if system profit exceeds a certain limit, it will be used to purchase (via exchange or auction) ACA tokens from the market,

Archived copy · cryp2nova.com

which will be burnt immediately. If system debt exceeds a certain limit, system will issue more ACA tokens, and sell them off (via exchange or auction) to pay back aUSD debts.

- **Auction Length**
  Duration of the auction once liquidation of an active CDP is automatically triggered by the system.
- **Auto Extension Period**
  To discourage sniping, the length of all auctions is automatically extended for a short period if a last-minute bid is placed, shortly before the preset auction close time. An auction will be continuously extended for another auto extension period if another new bid is placed during the current extension period, and the auction will be only closed when no further bid is placed in the latest extension period.
- **Bid Increment**
  A bid increment is a minimum amount by which a bid must be raised for the next bid. Increments are determined by the market value of the auctioned collateral and the current bid price to promote efficient bidding.
- **Lot Size**
  To liquidate a CDP backed with a high valuation of collateral that associated with a large amount of outstanding aUSD debt, the total collateral will be broken into smaller lots to be auctioned separately.

2.4.3. Adding New CDP Collateral Asset Type

ACA Token holders may vote to add a new type of crypto asset as collateral to generate CDPs and set its risk parameters and liquidation auction parameters.

2.4.4. Removing Existing CDP Collateral Asset Type**

ACA Token holders may vote to remove an existing type of crypto asset to be accepted as collateral to generate future CDPs, e.g. considering such assets becoming too risky.

2.4.5. Adjusting Oracles

Oracles are essential for normal operation of the ACALA network that ACA Token holders may vote to add new Oracle or remove existing ones.

2.4.6. Making Network Upgrade Decision

ACA Token holders may vote to make a strategical decision on network upgrade as the whole network grow, such as whether to upgrade the existing network from a Polkadot Parachain to an independent chain bridging to Polkadot.

2.4.7. Triggering Emergency Shutdown

ACA Token holders may vote to trigger the Emergency Shutdown procedure immediately in emergency situations.

2.5. Automatic Liquidations of risky CDPs

Archived copy · cryp2nova.com

The value of collateral in every active CDP is constantly monitored by the Honzon Protocol to ensure that the associated outstanding debt in aUSD can be recovered anytime by selling the collateral. The Honzon Protocol triggers a liquidation of an active CDP if it is considered to be too risky, i.e. when the current collateral-to-debt ratio of the CDP reaches the liquidation ratio of the asset type that the collateral belongs to.

After a liquidation is triggered, the Honzon Protocol will run a special auction mechanism in order to cover the outstanding debt by selling the minimum proportion of the collateral as possible.

- Firstly, the entire collateral of the CDP will be **auctioned in an ascending auction** automatically to any potential buyers on the market until the leading bid in aUSD reaches preset aUSD goal, the sum of the outstanding debt and the liquidation penalty.
- Then, once such a bid has been reached, the auction **switches to a descending reserve auction** that allow any potential buyers to **bid the minimum amount** of the collateralized asset they are willing to accept by paying the amount of the preset aUSD goal. Auction ends when no lower bid is placed within the auto extension period.
- Lastly, the part of collateral sold in the auction mechanism is transferred to the auction winner, and any remaining collateral is returned to the original CDP holder. The amount of the aUSD that is equal to the outstanding debt of the CDP is burnt, and the remaining amount of the aUSD paid as the liquidation penalty is converted to ACA tokens automatically and burnt permanently from the ACA supply. And the Honzon Protocol closes the CDP.

In rare situations when the auction mechanism fails to reach the preset aUSD goal, another auction will be run to raise enough aUSD to cover the uncovered difference in outstanding debt in the CDP, by running a descending auction to sell the minimum amount of ACA tokens possible to gain enough amount of aUSD to close the CDP.

Since we support CDP to be collateralized with multiple types of crypto assets, risks associated with different types of assets are considered by setting different liquidation ratios for CDPs collateralized with a different type of assets, which is adjustable in real-time by the Honzon Protocol.

2.6. Emergency Shutdown Procedure

2.6.1. Single Asset Liquidation

If a particular collateral asset has exceeded the acceptable risk threshold, liquidation of this asset can be triggered with the following process

- stop accepting this asset as collateral
- increase liquidation ratio to gradually close positions
- forced liquidation of residual positions after a certain time limit

2.6.2. Global Liquidation

For whatever reason the system is adversely affected and is on a seemingly irreversible worsening trend, the global shutdown can be triggered with the following process

- snapshot of latest oracle pricing
- stop accepting any assets as collateral, adjusting positions
- liquidate system debt and profit

Archived copy · cryp2nova.com

- aUSD holder can proportionally redeem collaterals

2.7. Key Actors

In addition to the core CDP runtime modules, Acala relies on the following network and system participants to maintain security and operation.

- **Collators**
  In Polkadot's shared security model, parachains such as the Acala Network will rely on **Collators** to provide recent state transitions to the validators on the Polkadot Relay Chain. The validators on the Relay Chain would operate under NPoS (Nominated Proof-of-Stake) mechanism to maximize chain security.

  Collators maintain a "full-node" for the Acala Network parachain, producing parachain blocks and proving bad behaviors, and in return are awarded ACA tokens.

  More details on the exact incentise scheme and Collator requirements would be released as we progress.
- **Oracle Operators**
  The Honzon Protocol require a real-time market price for the stablecoin, the collateral assets and the ACA token, in order to trigger liquidations or dynamically adjust certain risk parameters.

  Initially, during the bootstrap phase, there will be a whitelist of Oracle Operators participate in the price feeding operation, later this will be governed by ACA token holders. We are also watching closely the development of governance standards and operations in the oracle space, will gradually improve this, and open to collaboration to making it more resilient.

  Our oracle module has implemented certain safety mechanisms when combining price feed data into the system to minimize the impact of faulty or compromised feeders. For example, any compromised feeder is able to influence the price to a limited degree due to the price cap function built into the module. A K'th largest algorithm will be able to tolerate up to K compromised servers.
- **Liquidator**
  Liquidator monitors collateral levels of the CDPs, triggers a liquidation of collateral, debt and surplus auctions. The limitation of Ethereum requires such actors to be external to trigger liquidation, whereas Acala would have an automatic liquidator utilizing Off-Chain worker (aka automatic scheduler type mechanism implemented in runtime modules in Substrate). This will further increase the autonomy and responsiveness of the system.

  If collateral-to-debt ratio of a CDP reaches the liquidation ratio, the liquidator will trigger a collateral auction to sell proportional or the entire collateral to pay back the oustanding aUSD debt. The collateral auction may result in debt (if winning bid of the entire collateral was not enough to pay back all oustanding aUSD debt). In such situation, some sufficient amount of ACA tokens would be minted and auctioned for aUSDs to pay off the remaining debt. Dilution of the ACA tokens would create an incentive for the ACA holders to better govern the system.

3. HOMA - The Tokenized Staking Liquidity Protocol

Archived copy · cryp2nova.com

Unlike Bitcoin-like Proof-of-Work (PoW) chains, which uses computing power to secure the network while consuming large amounts of energy, Proof-of-Stake networks uses stake aka its network token and variations of the Byzantine Fault Tolerant (BFT) algorithm to secure the network. Polkadot uses NPoS (Nominated Proof-of-Stake) as its mechanism for selecting the validator set. It is designed with the roles of validators and nominators, to maximize chain security.

Polkadot network targets 50% active DOT staking with a 20% annual return. Effectively this creates an **opportunity cost for using DOT** in other applications versus staking. Ethereum as it currently stands as a PoW network has no such barrier, and in fact, has an incentive for ETH holder to participate in DeFi applications like MakerDAO or Compound. On the other hand, if DeFi lending applications provide a better yield than staking, it could motivate the collective movement of funds from staking to lending, **causing a 'bank run' and risking the security of the entire network**.

3.1 The Homa Protocol

In any case, the task at hand is to solve the **illiquidity challenge of staked assets**. We would introduce the Homa Protocol that establishes a staking pool tokenizing users' staked assets as L-Asset (e.g. L-DOT as locked DOT), which users can invest or use in other applications. For example, lend L-DOT to earn interest or use L-DOT as collateral for stablecoin aUSD. The Homa Protocol tokenizes staked DOT as L-DOT where

1. **L-DOT is tradable and liquid cross all chains** on the Polkadot network
2. **L-DOT is redeemable** for underlying DOTs at any time, with option to redeem **immediately or earlier** transferrable unbounded DOTs
3. decentralized on-chain **collective governance by L-DOT and ACA holders**
4. **algorithmically adjusted staking strategy** to optimize return and ensure liquidity
5. leverage Polkadot's shared security mechanism, to have **highest security on day one**
6. **fee schedule can be customized** to boost usability

The Homa Protocol resides on the Acala Network, establishes a **decentralized staking pool** where users would lock their DOTs to gain staking yield while receiving **L-DOTs as a receipt that are liquid and tradable**. The protocol manages issuance of L-DOTs and redemption of underlying assets. The protocol would managed the locked assets, participate in staking, execute staking strategies (e.g. validator selection based on uptime etc.), manage rewards and slashed penalties.

3.2 Staking

Unlike direct validating or nominating, where a user's asset are bonded directly for staking, the Homa Protocol would aggregate the supply of each user, and participate in staking collectively.

DOTs supplied to the staking pool are represented as L-DOT account balance, which entitles the owner to a likely increasing quantity of underlying assets. The DOTs being used to stake would earn block reward, and incur punishment (DOTs being slashed) in case of validator found to be misbehaving (e.g. not maintaining required uptime).

The balance of the two is the profit/loss that would increase/decrease the amount of the underlying asset of L-DOT. This means **earning staking reward is as simple as holding an L-DOT token**, while L-DOT is cross-chain capable and can be used to participate in other network activities such as lending or as collaterals in Honzon Stablecoin Protocol.

Archived copy · cryp2nova.com

3.3 Redeeming

When users redeem L-DOTs for the underlying DOTs, the protocol would unbound staked assets; generally one would have to wait for certain recovery time (28 days as this is written) for the DOTs to be transferrable. The redeem service fee is payable in ACA tokens.

The protocol may reserve a portion of the locked asset, so users can redeem and use the DOTs immediately or in a shorter period of time than normally required. Users would need to **pay a premium in DOTs to compensate for the lost yield and time value for immediate or earlier liquidity**.

At any point in time, the Homa Protocol

- may have a certain amount of reserved DOTs available immediately for redemption.
- may have varied amount of unbounded DOTs available at varying timeframes for redemption.

The amount of premium payable is algorithmically set relative to a number of factors including the amount withdrawn, transferrable timeframe required, potentially lost yield if any, etc. The premium would be retained in the staking pool and shared amongst L-DOT holders.

3.4 Tokenized Staked DOT: L-DOT

Through the Homa Protocol, staked DOTs become fungible and liquid L-DOTs that exploit the derivative value of the DOTs fueling and powering more applications without sacrificing the security of the whole network.

Users can essentially mint L-DOTs by supplying DOTs to the staking pool managed by the Homa Protocol, and redeem L-DOTs for the underlying DOTs. The exchange rate between L-DOTs and the underlying DOTs are likely to increase over time, as staking rewards are accrued by validating and nominating, and is equal to

$$R_{ExchangeRate} = (\frac{N_{sum} + N_{profit}}{N_{L-DOT}})$$

The effective profit/loss, however, is determined by various factors including but not limited to

- inflation rate of DOTs. more details
- the chosen staking strategy.
- the performance of chosen validator nodes.

3.5 Staking Strategy

The Homa Protocol will execute the staking strategy to deploy locked DOTs. The staking strategy and parameters are governed via the Homa council where L-DOT holders can submit change proposals and have voting rights

The staking strategy would be devised with but not limited to the following components

- voted preferred validators by the Homa Council
- divest strategy e.g. risk/reward with a number of validators, this may be dynamically adjusted to maximize return, in combination with the built-in optimization mechanism of Polkadot
- validator selection criteria e.g. security, validator commissions, reputation, uptime, optimization to

Archived copy · cryp2nova.com

mitigate slashing risk, reliability e.g. multi-infrastructure for multi-validators
- reinvest strategy: the protocol will periodically rebalance the reward received, new staking and redemption activities, and algorithmically decide whether to re-invest and earn compounded rewards.

There will be an economic whitepaper detailing further the algorithms, calculations and staking strategies.

3.5 Governance

The overall Acala network is governed by the General Council and specialized councils. Specialized councils would govern specific domains of the network e.g. the Financial Council would govern the financial and risk management of the network, and the Homa Council would govern the Homa protocol.

In order to make any changes to the Homa Protocol, the idea is to compose active L-DOT and ACA holders, via the General Council and the Homa council together to administrate a Homa protocol-specific upgrade decision. A change proposal can be raised by the council or the public (L-DOT or ACA) holder, but the decision to approve or against it is made collectively. There is a pathway to decentralization from elected council referenda to public referenda.

Any network upgrade would be under the governance of the General Council. L-DOT holders are entitled to govern Homa protocol-specific proposals through the Homa Council. The General Council would have oversight of the Homa Council to ensure the overall welfare of the Acala network.

Special voting rights would be afforded to L-DOT holders to participate in voting for or against Homa protocol related proposals, which include but no limited to these areas

- update exchange rate model
- update fee structure
- update staking pool reserve
- update redeem premium rate model
- update and propose new staking strategy

4. Initial Parachain Offering (IPO)

There are multiple ways to participate in the Polkadot network from high usage to low usage, from high to limited customization:

1. deployed as **parachain** with permanent (for the auctioned slot period) on-going security for high usage and fully customised chain
2. deployed as **parathread** for fully customised chain with lower usage, pay-as-you-go security renting economic model
3. deployed as **smart contracts** on a parachain or parathread to leverage Polkadot security through their economic model

Becoming a Parachain by leasing a Parachain slot from Polkadot would be an ideal option to bootstrap the Acala Network, and maximize its benefits and reach to other chains and applications on the Polkadot network. Polkadot utilizes a specially designed Candle Auction to sell the leasing right of Parachain slots. It is a mechanism designed for fairness, e.g. to prevent early sniping and provide bidders with higher valuation higher chances of winning.

Cryp2Nova

Archived copy · cryp2nova.com

To secure a parachain slot, the Acala Network will require supportive DOT holders to lock their DOTs to bid for a slot collectively, that a Crowdfund IPO (Initial Parachain Offering) will be conducted, and ACA tokens will be distributed as rewards to DOT owners who participate in the IPO successfully, to compensate their opportunity costs of having their DOTs locked for the first round of 24 months.

We plan to lease the Parachain slot for three rounds of six years (24 months in each round), and switch to our independent blockchain bridging to Polkadot after six years. Detailed proposal is available in our Token Economy Whitepaper.

In case our first Parachain slot auction was not successful, we will continue to launch our mainnet on Parathreads instead. DOTs raised in IPO will be returned to their owners, and ACA tokens will still be minted at launch, but only distributed to ACALA Founders and Seed Investment Partner according to the original plan, with the rest reserved for future investment opportunities including IPO in the second Parachain auction.

Compared to Parachain, there are gas costs using Parathreads, depending on frequency of validation. The more frequent a validation is processed, the safer the network is, at a price of higher gas costs. ACA holders will vote to determine the frequency. A small amount of ACA tokens will be released from the reserve and sold to public for DOTs daily to cover the entire gas costs of the network daily validation. For say, if the total gas costs are estimated to be 5 ACA tokens worth of DOTs for the day, 5 ACA tokens will be released and sold by the system. Another IPO will be raised to lease a Parachain slot before the second Parachain auction.

5. Summary

The Acala Network is a first-of-its-kind DeFi infrastructure chain governed by a decentralized consortium and powering financial activities for all chains on the Polkadot network. Specifically it will solve the problem of stability and liquidity:

- stability of financial instrument via the Honzon Protocol - a sound and stable currency for low cost, borderless value transfer for all blockchains that are connected in a network
- liquidity for staked DOT - to extract all derivative values of DOTs, and power more financial activities without compromising overall network security

Reference

1. Polkadot Network https://polkadot.network/
2. MakerDAO https://makerdao.com/
3. Compound https://compound.finance/
4. Parachains https://wiki.polkadot.network/docs/en/learn-parachains
5. Parachain Allocation https://research.web3.foundation/en/latest/polkadot/Parachain-Allocation.html
6. NPoS Staking https://research.web3.foundation/en/latest/polkadot/NPoS/index.html
7. On-chain Governance https://wiki.polkadot.network/docs/en/learn-governance
8. Cross-chain Message Passing (XCMP) https://research.web3.foundation/en/latest/polkadot/XCMP.html

Archived copy · cryp2nova.com