HaloDAO

Litepaper

Building a Global Stablecoin Market

Abstract

This paper describes an incentivisation system, embodied in a Decentralised Autonomous Organisation called HaloDAO, a stablecoin marketplace Protocol that connects traditional finance and decentralised finance (DeFi) by enabling deep liquidity networks for local stablecoins and money market fund products with foundational DeFi primitives.

We aim to create a foundational layer for the digital economy by;

1. Building a stablecoin optimized Automated Market Maker (AMM) that efficiently facilitates swaps and minimizes slippage between differently priced stablecoins (whereas Curve is only optimised for similarly priced tokens)
2. Bootstrapping a lending market, similar to Compound and Aave but focused on stablecoins that enables a foundational money lego to generate local currency derived yield off of permissionless lending and borrowing denominated in local currencies

HaloDAO is driving liquidity to regional, asset backed stablecoins by building a stablecoin optimized AMM and stablecoin focused Lending Market and linkages with existing wallets and exchanges around the world. With a greater supply of region specific stablecoins, users will be able to access the permissionless Decentralised Finance (DeFi) economy, thereby lowering the barrier to individual financial participation in a region of the world with a high potential of growth and impact.

Concepts

RNBW

RNBW is the ERC20 governance token, limited to 100,000,000 supply to be distributed over 5 years that enables holders to participate in governance and acts as a claim against local stablecoin earnings of the Protocol.

Asset Backed Stablecoin

An ERC20 stablecoin issued by a licensed financial institution in a relevant jurisdiction (such as one licensed by the Monetary Authority of Singapore in Singapore) that functions as a claim against fiat (physical notes issued by the relevant central bank or licensed e-money issuer) held as collateral on a 1 to 1 basis. An example would be 1 xSGD backed by 1 SGD in the bank account of the licensed issuer. This is similar to how USDC is issued and backed by US Dollars held in a traditional reserve account.

Stablecoin Earnings Pool

The repository of Protocol Earnings taken from;

1. Exchange fees from traders on the AMM
2. Commissions from interest gained through lending and borrowing local currency pegged asset-backed stables

This earnings pool will be used to fund long term DAO operations and also buyback and/or burn/redistribute RNBW from the market.

RNBW Rewards Pool

The repository of the RNBW governance tokens reserved as a reward to liquidity providers (across the stablecoin optimised AMM and lending market) and users of the protocol.

On/Off Ramp

The licensed cryptocurrency exchange or financial service entity that allows users to exchange local stablecoins for fiat or vice-versa.

Liquidity Provider

The entity, individual or smart contract that either;

1. Provides liquidity into an AMM pool supporting trades between other cryptocurrencies and asset backed stablecoins
2. Or lends collateral to borrowers for a fee in our Lending Market.

Tokenomics

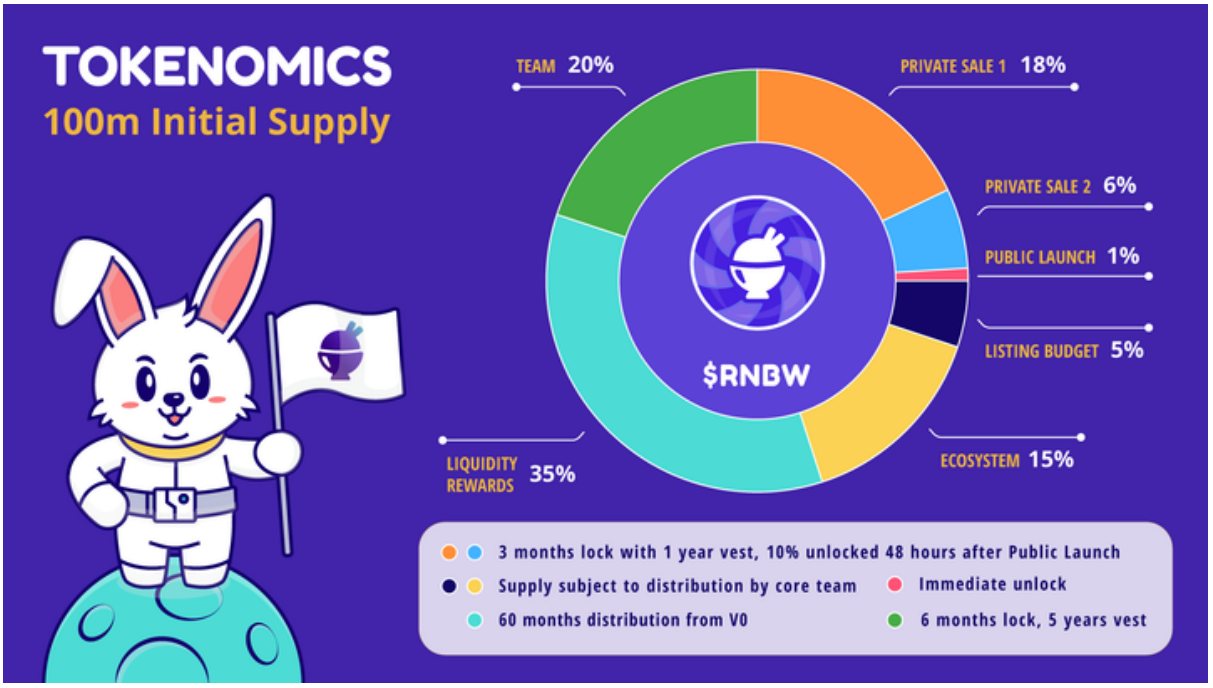


Figure 1: Token Distribution

The above diagram illustrates the breakdown of the initial 100 million supply of RNBW governance tokens. 24% of HaloDAO tokens has been sold in our Private Sale and 1% will be sold in the Public Launch. 5% will be reserved as Listing Budget for liquidity and market making to get the token into popular centralised exchanges. Another 15% will be kept for ecosystem support, such as grants, hackathons and other activities. 35%, the largest allocation, will be used to incentivise liquidity providers who will create and seed markets with region-specific stablecoin liquidity. 20% will be used to incentivise the team for long term participation in the project.

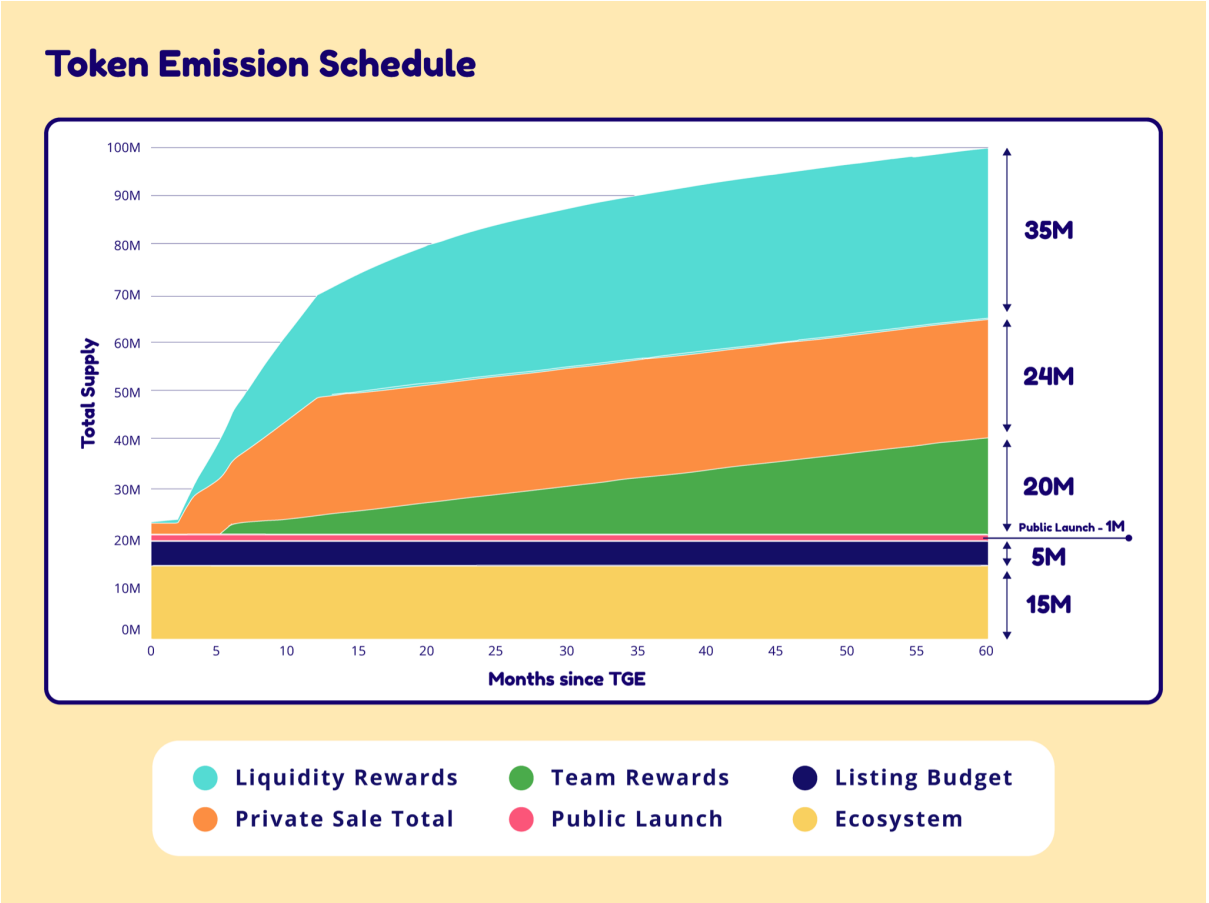


Figure 2: 5 Year Token Emission Schedule

Liquidity Rewards

A total of 35M RNBW tokens will be rewarded to liquidity providers for a target duration of 5 years. The distribution schedule will follow a decaying growth function in order to reward early adopters and then approach a zero limit towards the 60th month from launch as the RNBW market cap grows. The exact proportion of RNBW rewards between AMM LPs and Lending Market LPs will be determined on a rolling basis as the community provides liquidity and identifies important trading/lending pairs. These 35M RNBW tokens also include liquidity rewards that will be allocated for farming on other chains and Layer 2s. The disbursement rate of liquidity rewards may be revisited by the Foundation every few months as the Protocol grows and may be increased or decreased to match the incentivisation alignment needs of present and future liquidity providers. For the moment, however, the calculation is pegged to a 5 year emission schedule.

At current network parameters, RNBW is rewarded on every second linearly within a month's epoch;

$$RNBW_{\text{reward\_per\_second\_user}} = \frac{LP_{staked}}{TotalCollateral_{staked}} \times RewardsRatio \times RNBW_{\text{reward\_per\_second}}$$

Where;

- LP_{staked} is the liquidity provider's total collateral provided
- $TotalCollateral_{staked}$ is the total collateral provided by all liquidity providers
- RewardsRatio is the total rewards allocated for a particular pool (AMM/Lending Market). In total, all farming pools are allocated 80% of monthly liquidity rewards
- $RNBW_{\text{reward\_per\_second}}$ is the linear reward per second for that specific epoch (each epoch equalling one month and each subsequent month following a decaying rewards function)

At current network parameters, it will take ~5 years for the RNBW Rewards Pool to empty. Before that happens, however, the Foundation (or any other RNBW token holder) may propose a buyback vote which will replenish the RNBW Rewards Pool for Liquidity Providers. Of course, at any time RNBW holders may propose a vote to enact any miscellaneous action, such as burning RNBW upon buyback or to alter the minute network parameters to react to market changes. It is also important to note that the protocol supports the buyback and redistribution of network profits into the liquidity rewards allocation on every swap or borrow payment.

Team Rewards

20 million RNBW tokens are allocated to the team to incentivise good work to advance Protocol objectives. Roughly 325,000 RNBW per month will be paid to the core team for the same 5 year schedule.

Ecosystem

15 million RNBW tokens will be reserved as ecosystem support for wallet builders, payment processors or any other financial institutions that want to make use of HaloDAO's stablecoin liquidity. HaloDAO will provide any SDKs or tooling that might make it easier for these entities to onboard into the permissionless and borderless commerce inherent to Decentralised Finance (DeFi). Additionally, the Ecosystem fund could also provide grants and any other assistance to potential adopters of regional stablecoins.

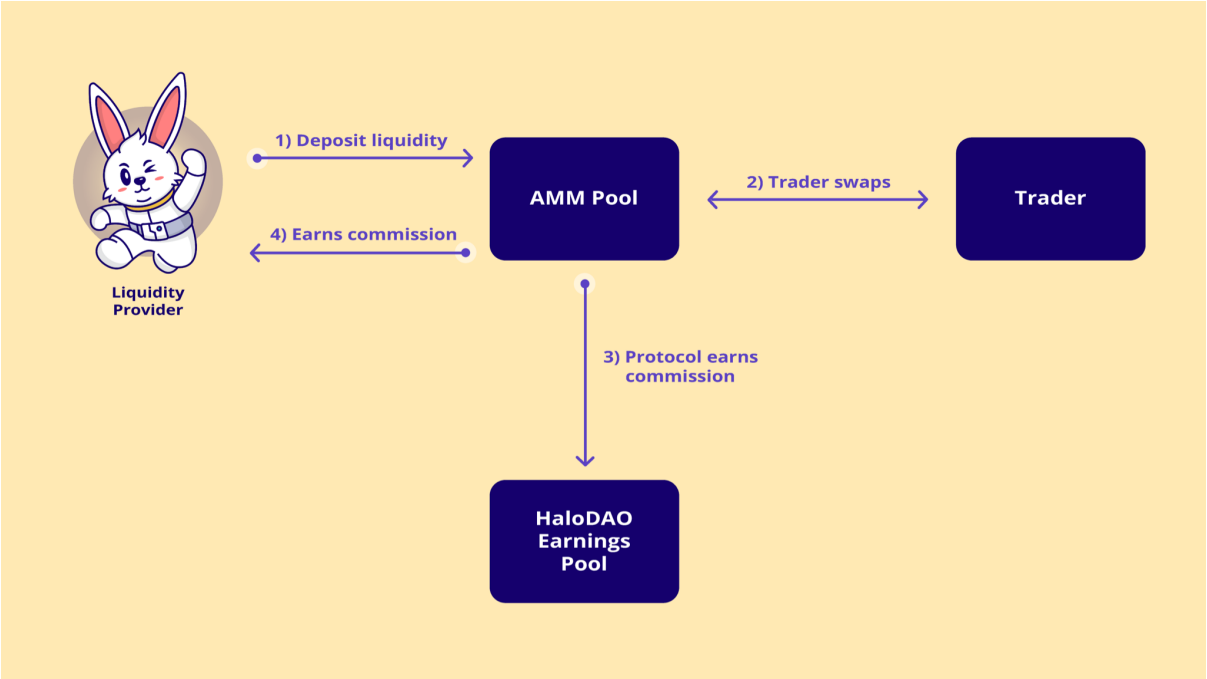
Private Sale

Last but not least, institutional money is necessary to get the initial team and product off the ground. For this reason, the team has allocated a total of 24M tokens to sell for the current private and public rounds to fund initial development, liquidity, launch and future development.

Profit Drivers

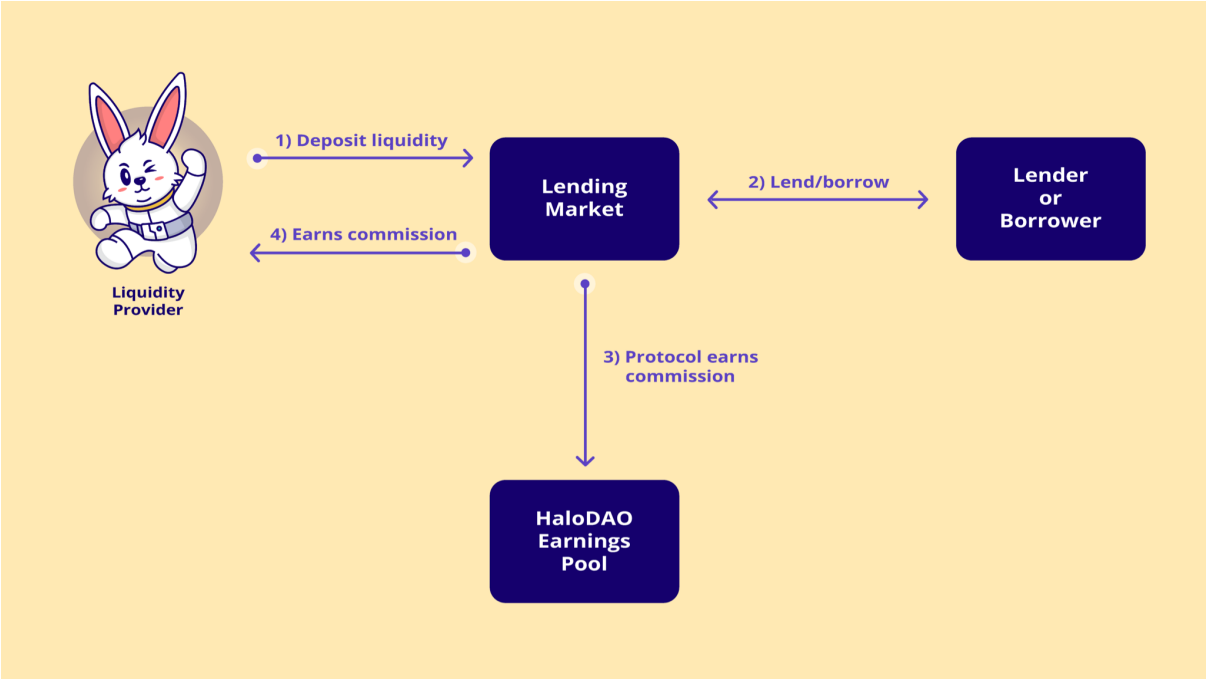
The main profit drivers of the RNBW network are;

1. Exchange fees from the AMM



The protocol will start by implementing a 0.3 % liquidity provider fee and 0.05% protocol fee. This protocol fee will go into the RNBW Earnings Pool. xRNBW token holders will receive a portion of this revenue. Additionally, these parameters are changeable by governance votes by token holders.

2. Interest commissions from the Lending Market



The protocol will take a commission from borrowers who pay fees to lenders. xRNBW token holders will receive a portion of this revenue. Additionally, any relevant parameters will be changeable by governance votes by token holders.

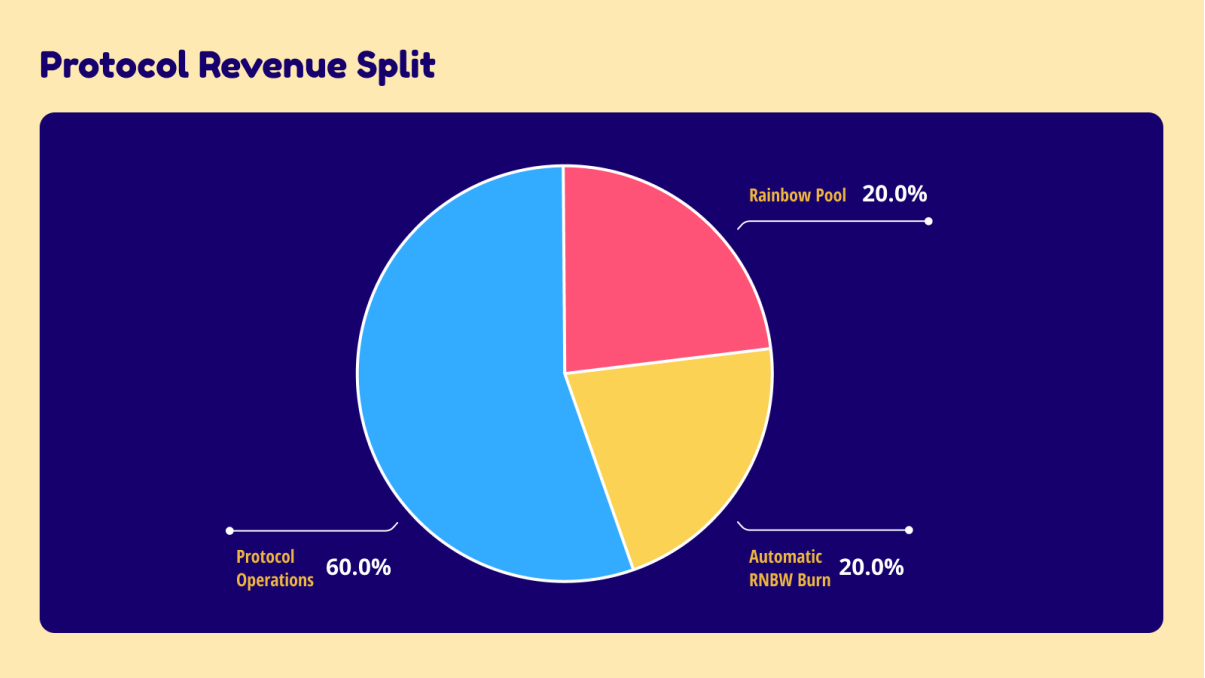


Figure 3: Protocol Revenue Split

On every AMM swap or Lending Market borrow repayment, the stablecoin fees will be used to buy RNBW off the market. That RNBW will then be divided between;

Rainbow Pool LPs (xRNBW holders)

LPs that are actively staked in the Rainbow Pool will automatically receive 20% of all stablecoin revenues every block. Take note that this vesting reward is different from the liquidity rewards given to Liquidity Providers. It is the protocol's mechanic to reward longer term token holders with network profits.

Automatic RNBW Token Burn

20% of all stablecoin revenue earned by the Protocol will automatically be used to buy RNBW from our AMM and burn it, decreasing the total supply of RNBW.

Protocol Operations

Allocation on the remaining 60% of Protocol revenue will be done via RNBW Token Holder vote. Examples of allocations could be, but not limited to, buybacks and redistribution to the RNBW Rewards Pool for Liquidity Providers, additional RNBW token burns, reinvestment into the Protocol, reinvestment into additional liquidity, grants to builders, etc.

Do note that the percentages in the figure above are adjustable via successful governance vote at any time.

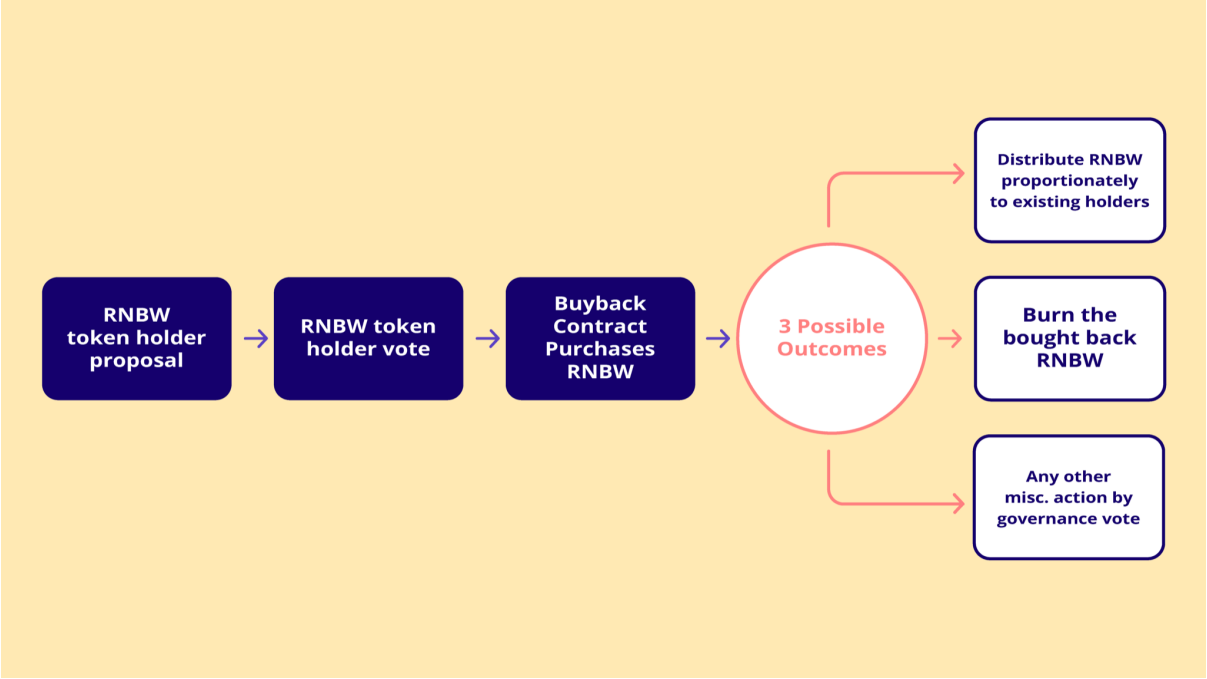


Figure 4: RNBW Buyback Mechanism

Aside from the regular Protocol Revenue Split, an RNBW token holder may propose a manual buyback in a specific epoch. If a buyback proposal receives a majority vote, then the BuyBack Controller on chain will immediately use the available balance of a specific token in the Earnings Pool to buy RNBW from our AMM (or even others) at market price. The proposal may detail an automated action after buyback, such as:

1. Redistribution to Rainbow Pool (xRNBW holders)

   The bought back RNBW would be used to replenish the RNBW Rewards Pool where only liquidity providers can earn it for supporting the Protocol.

This also has the effect of lessening both the freely circulating and total staked RNBW supply, thereby increasing returns for investors + liquidity providers, and thus increasing intrinsic demand for free market RNBW. Of course, a governance vote may also decide to burn the bought back RNBW tokens or even reinvest it in the Protocol in whatever form.

2. RNBW token burn

   The bought-back RNBW would then be burned, thus lessening the total RNBW supply and benefiting all RNBW holders.

3. Miscellaneous action by Governance Vote

   Manual, miscellaneous action by the Foundation, such as reinvesting into Protocol development or anything else that may be proposed by governance. Governance may also vote for the Foundation to manually allocate the bought back RNBW for any purpose the RNBW token holders deem necessary.

Technical Overview

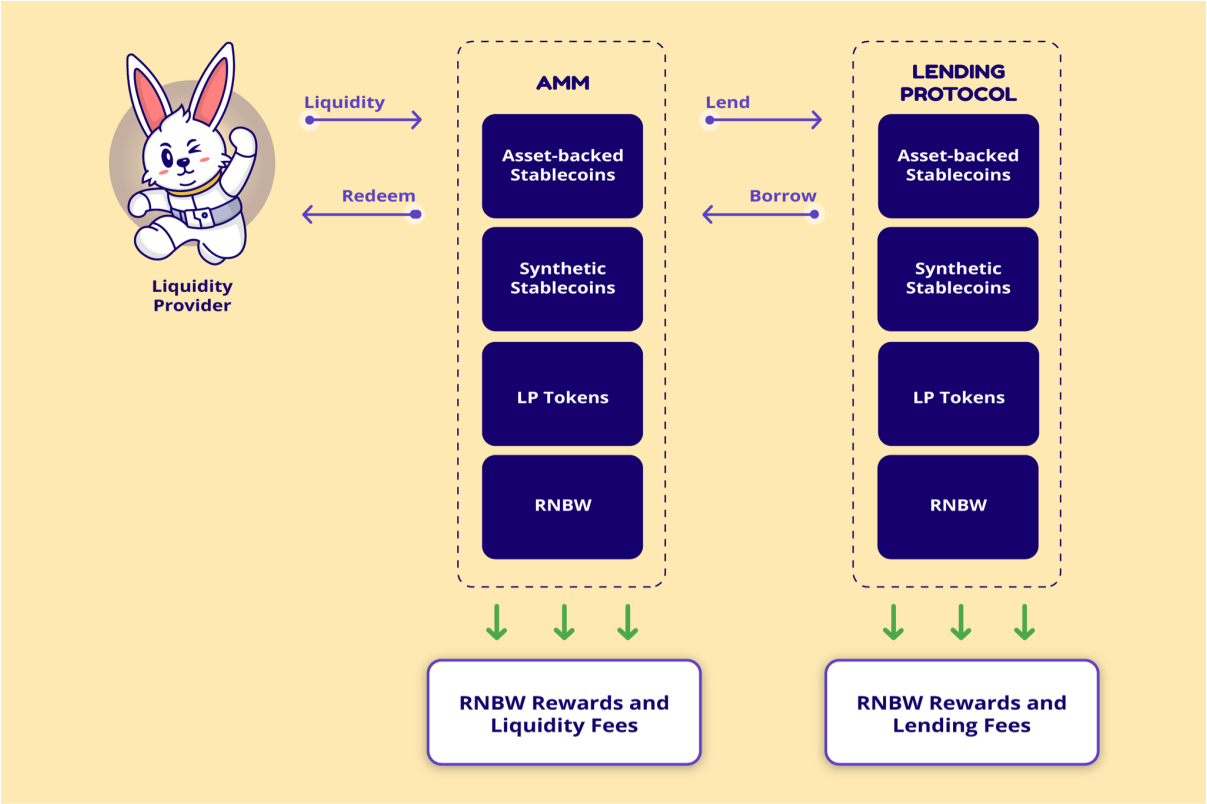


Figure 5: HaloDAO Value Chain

Automated Market Maker (AMM)

HaloDAO will incentivise liquidity provision and trading between asset backed stablecoins and important pairings between those stablecoins and popular currencies, such as ETH, WBTC, USDC, USDT, etc.

Lending Protocol

It is not enough to simply be able to trade between stablecoins and build something like an on-chain forex market. The goal of HaloDAO is to build up a regional lending and borrowing market for stablecoins so that end users will be able to get a regional currency-denominated interest rate on their holdings - essentially “local currency farming”.

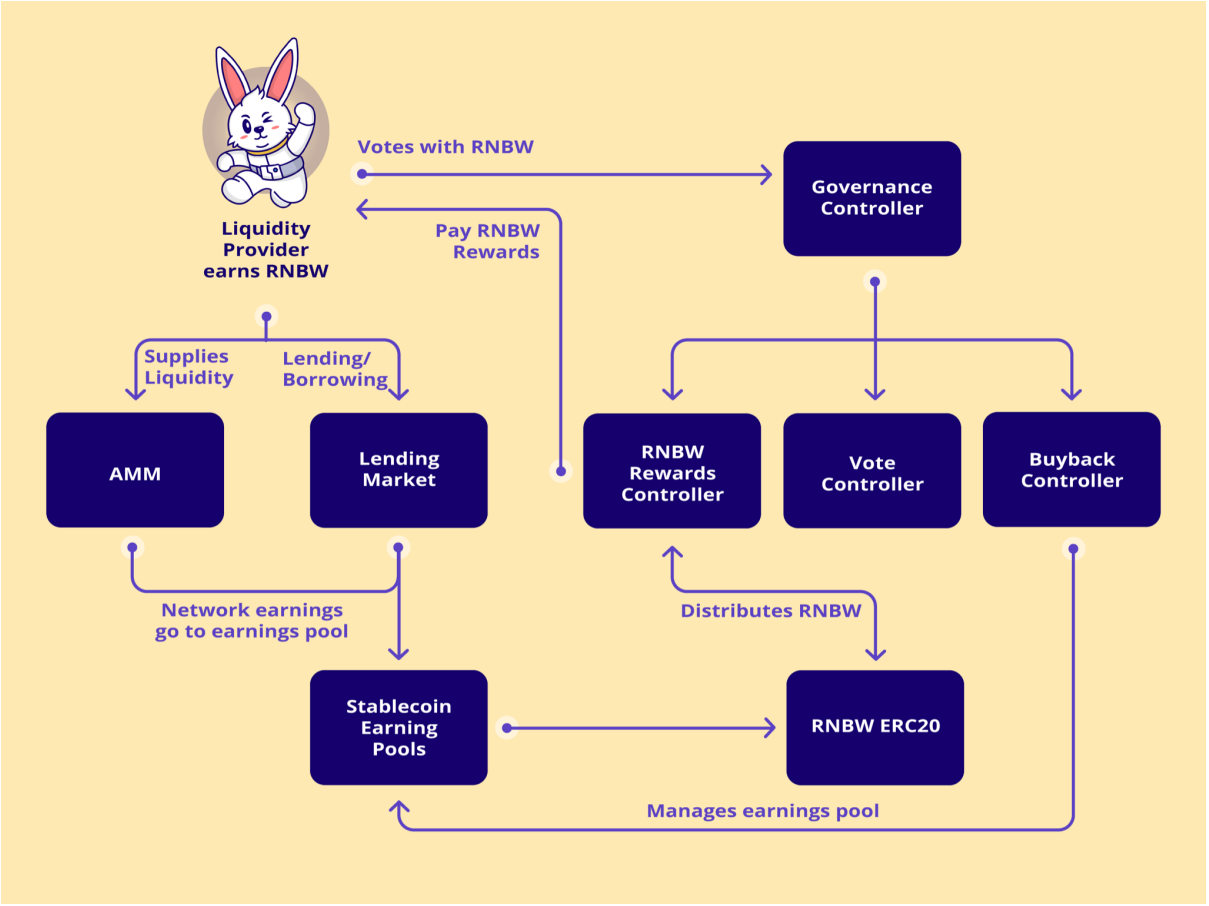


Figure 6: HaloDAO High Level Components

The core modules enable the:

1. Swapping of region specific asset backed stablecoins
2. Lending and borrowing of these region specific stablecoins
3. The earning and vesting of RNBW rewards for actions along the profit drivers of the above
4. Governance of the HaloDAO Protocol by token holders who propose and vote on protocol parameters

   Potential governance proposal types and methodology are further described in the Governance section below.

Governance

Informal Discussion

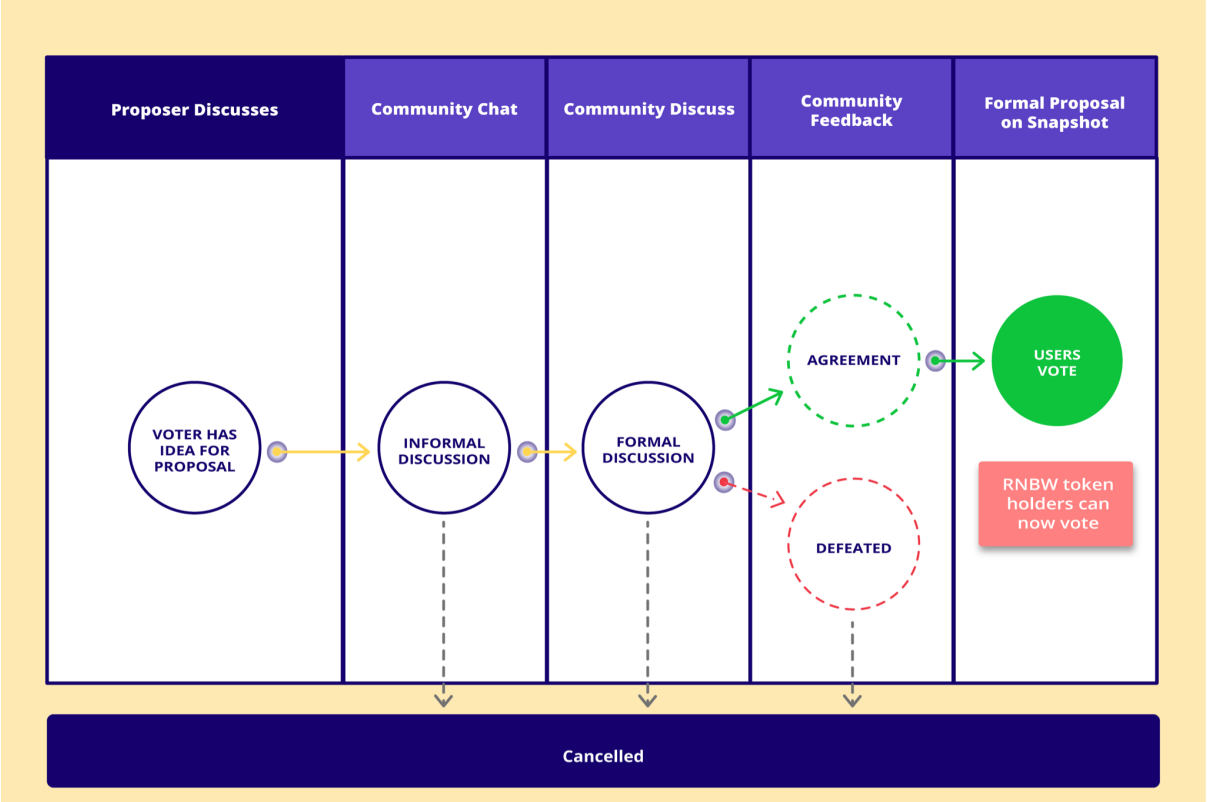


Figure 7: Informal Discussion Flow Chart

The proposal and voting process begins with informal and high level proposals on Discord and other channels the community chooses. That would be followed by intermediate proposals with some level of detail on Discourse, which could also be linked to proposed changes outlined in a Pull Request or Issue to the HaloDAO Github.

Formal Proposal and Voting

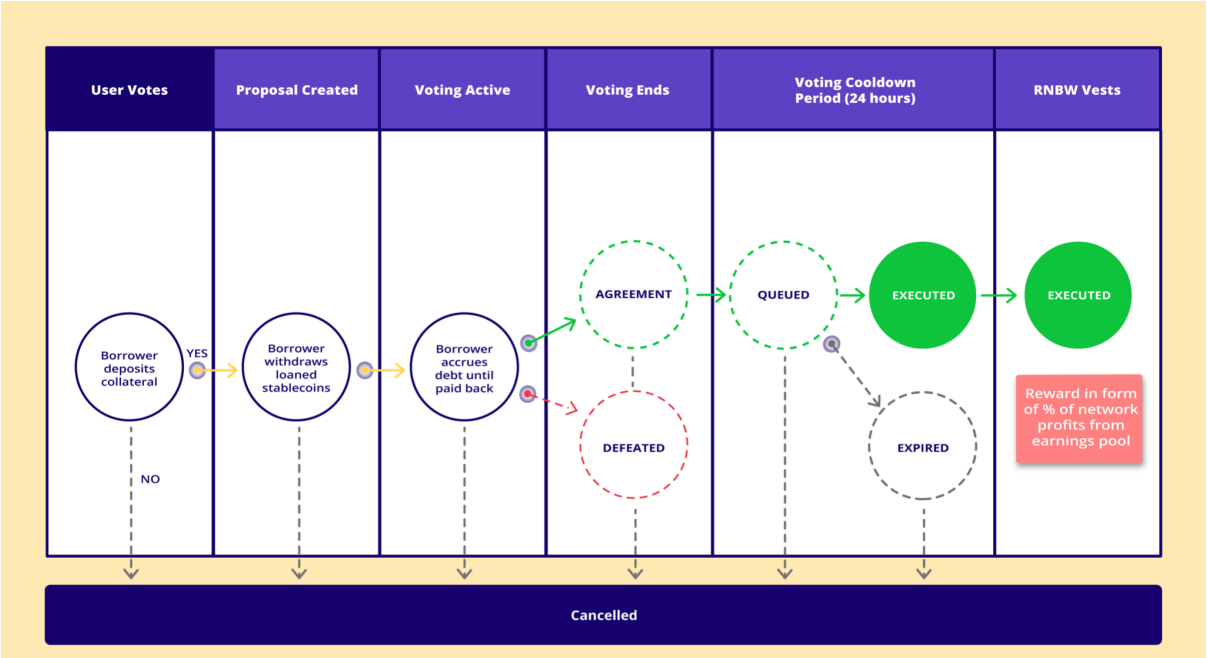


Figure 8: Formal Proposal and Voting Flowchart

Formal proposals and subsequent voting can be kicked off by any RNBW token holder who can create a new proposal on Snapshot consisting of a;

- description of the proposal (potentially with a link to the Github PR or Issue)
- and the proposal data itself: an array of multisend transaction payloads executable by the Gnosis Safe module.

Each proposal on Snapshot is linked to a Reality.eth question asking if

1. the linked Snapshot proposal passed
2. did the proposal include the payload, and
3. does the payload do what the proposal describes.

If the proposal passes on Snapshot, then Reality.eth should resolve to the same outcome, and after a 24 hour cooldown period, the proposal's transactions are executable by anyone. Reality will use the RNBW ERC20 governance token for the bond. The minimum bond can be set by way of a proposal to the DAO.

Optimistic Voting

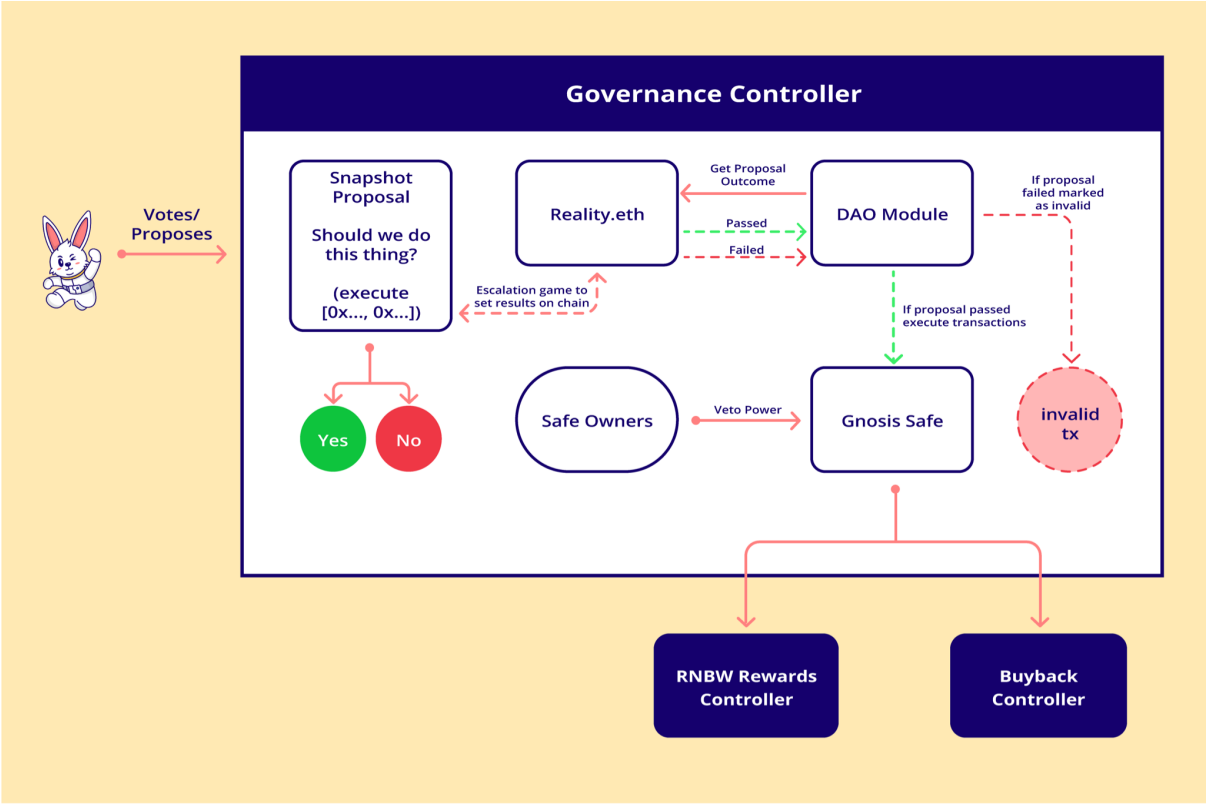


Figure 9: Optimistic Voting flowchart

The above diagram is partially taken from [Gnosis SafeSnap](), which HaloDAO (among other well established protocols) will leverage to enable off chain voting and on chain execution of proposals. While development is ongoing, the Safe Owners highlighted in the diagram will be a multisig as safeguard operated by HaloDAO and will hold veto power to proposals. This multisig, however, will be removed once the protocol reaches maturity in roughly a year after launch when most of the protocol components have been built out and battle tested.

Proposal Types

One thing to note is that various governance proposal types can be categorized into either Self Executing or needing Manual Execution. Self-executing proposals are those detailed below that can simply go through the governance process described above and are generally programmable parameters in HaloDAO's smart contracts. Manual execution, however, would require action from human actors and would not be part of the governance process described above. There would be no "standard way" to handle manually executed proposal types, as it

would be something outside the scope of programmable parameters in the smart contracts.

Examples of Self Executing proposal types are the following, but not limited to;

Self Executing Proposals	Sample value	Comment
AMM LP swap fee	0.003	Equal to 0.3% of the swapped transaction amount
AMM LP swap fee	0.0005	Equal to 0.05% of the swapped transaction amount
Governance active voting period		
Voter reward per epoch	0.2	Equal to 20% of network profits per epoch
Owner property of various smart contracts	Ethereum address (0x...) of smart contract	This will be changed upon governance vote (for example from the current dev admin wallet to the Gnosis Safe for decentralised governance)
EpochRewardAmount	100,000	RNBW tokens set aside every epoch for liquidity rewards
VestingRewardRatio	0.2	% of EpochRewardAmount set aside for Vesting rewards

Table 1

Governance Roadmap

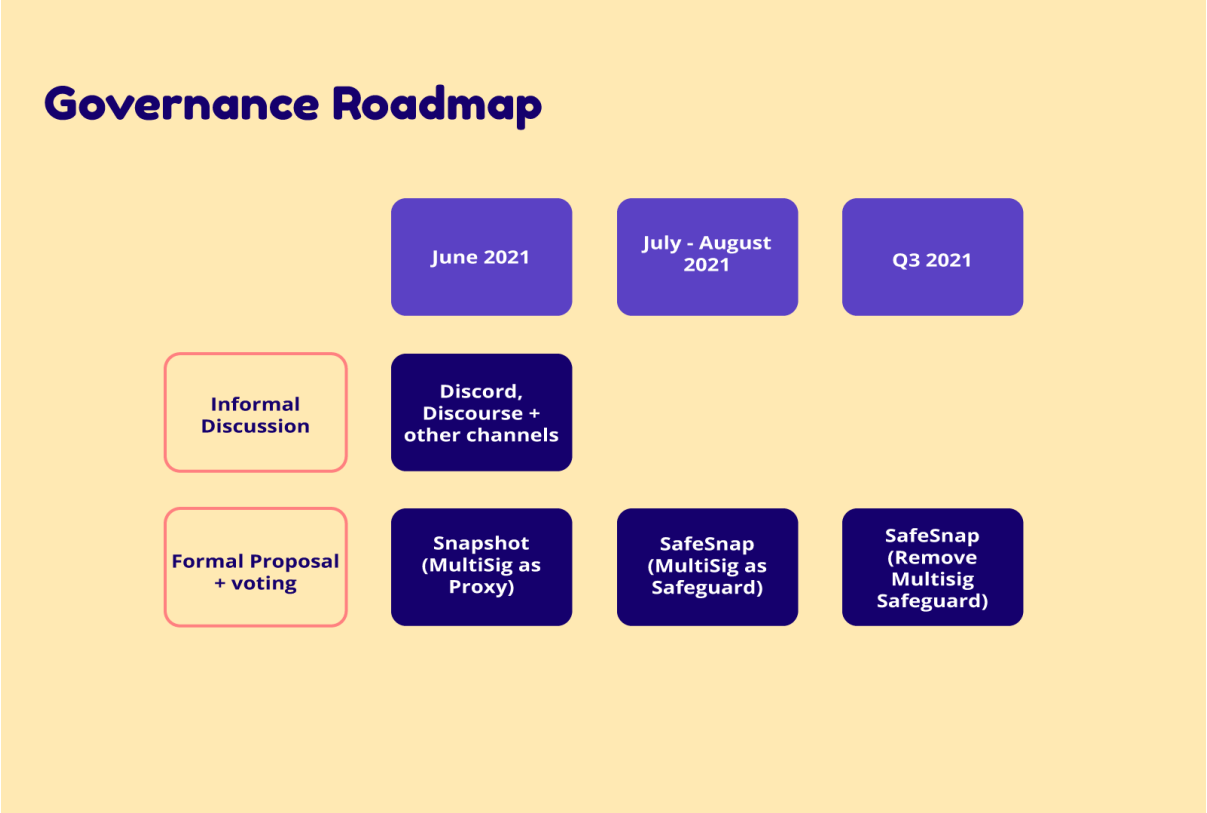


Figure 10: Governance Roadmap

The Foundation is actively building the governance module described in this section, which will enable community management of the Protocol with a strong emphasis on security and stability, with the constant guiding principle of increasing and maintaining complete decentralisation to avoid any central point of failure. At initial launch of the protocol, the Foundation will maintain a Snapshot voting portal with a MultiSig as Proxy to execute all successful proposals. The immediate next step roughly 2 or 3 months after initial launch and development of the relevant products (AMM & Lending Market), the Foundation will simply maintain the ability to suspend the now running Formal Proposal and Voting system via an emergency shutdown mechanism and veto power (MultiSig as Safeguard).

Once the Foundation is confident that the governance system is operating in a reliable, distributed manner (expected by roughly Q3 or Q4 2021), the team will recommend to the community via a proposal that the failsafe be removed (Remove MultiSig Safeguard). This would be accomplished by removing the Safe owners, thus removing the last guard rail, from the Gnosis Safe.