WHITE PAPER

Maya

A future inspired in our past

Introduction. Maya 1.0 & Maya 2.0 **1**

Part 1. Fair Launch **10**

Part 2. $MAYA Token **22**

Part 3. Liquidity Nodes **32**

Part 4. Security Nodes **45**

Part 5. Aztec Chain & $AZTEC token **63**

Part 6. Stable Pools & Route Optimization **98**

Maya 1.0
How we started

INTRODUCTION

How we started

The impressive feat of first designing and building a technically viable, completely decentralized, permissionless exchange is credited to THORChain and its relentless team of developers. Maya Protocol was meant to be nothing more than an effort to create a backup system, an alternative to $RUNE and to THORChain, for several fundamental reasons outlined below.

Maya Protocol's team believes there have been four technological breakthroughs that will soon change how our current economic systems work, they are:

- Bitcoin's Proof of Work
- Ethereum's Smart Contracts
- Tendermint's simple BFT Proof of Stake - easily programmable with Cosmos SDK
- THORChain sovereign blockchain - open-source and cross-chain

Like THORChain, Maya Protocol is a CosmosSDK-powered, replicated state machine to overwatch and coordinate the movement of digital assets, swaps or stakes without the need to wrap or peg any of them. In our own way, we are validating THORChain's lead and paying tribute to it. The idea to create Maya Protocol was born when a developer of THORChain publicly mentioned that he expected the market to be filled with at least 3 to 5 similar protocols in the future.

Maya will be the second to market.

Maya Protocol has its own native token called $CACAO. Why this name? We all know cacao is the main ingredient used for making chocolate nowadays but, in antiquity, this seed was also used as a medium of exchange and commerce by the Maya civilization in what today is the Yucatán Peninsula and Central America.

Here is an overview of why we think THORChain cannot and should not be the only cross-chain DEX out there:

- They need backup as a universal backend provider.
- THORChain cannot grow fast enough to capture all the addressable market.
- THORChain will eventually hit its TPS limit.
- The technology needs validation.
- Collaboration instead of competition.
- Focus on different target markets.
- Compatibility.
- They should not be dancing alone!
- Version Stability.
- Two minds are better than one.

Let's go through each one of them:

Backup as a universal backend provider.

01

We believe that Cross-Chain Decentralized Liquidity Protocols will serve as the backend to most of the volume moving across wallets, central exchanges, protocols and crypto businesses. It is very important to have a backup to any such system in case any problem could affect it and to prevent critical failure across the market. Think of somebody carrying a Visa and a Mastercard, both networks generate loads of transaction volume when people use their debit or credit cards to pay for goods and services but, if for any reason the Visa network stopped working, then all those users could still use their Mastercard instead. If THORChain was Visa, then Maya would be MasterCard.

THORChain cannot grow fast enough to capture all the market.

02

This is not a lack of trust in THORChain's ability to grow, rather a statement that stems from the understanding of the protocol. THORChain (and Maya) have some sort of a virtuous cycle that cannot be artificially accelerated: the growth of their security and the growth of their liquidity. One cannot grow without the other and this creates a constant "chicken and egg" problem. Security scales as more nodes join, bonding bigger amounts of $RUNE —$CACAO, in our case — but if the bonds grow too much then the protocol becomes very capital inefficient. On the other side, if too much liquidity is provided relative to the bonded capital, then the system becomes riskier. This process is continuously being optimized by specialized economic incentives, but it takes time to do so. We believe there is more demand for liquidity in the market and people willing to provide the underlying necessary bonds than the speed at which THORChain can currently capture it.

THORChain will eventually hit its TPS limit.

03

Even when THORChain continuously increases the liquidity in the protocol, eventually they will hit the Transactions Per Second limit, which sits around 100 - 500 t/s. At that point, swappers will either start clogging the network or will need to rely on another protocol, this is where Maya comes in.

Providing validation to the technology.

04

There are still naysayers of what THORChain has created. Once more protocols, like Maya, enter the picture and continue with the mission that THORChain set out to do, we will provide validation to the market and increase the confidence in this product. Our mission is clear: for Decentralized Exchanges to manage more liquidity than Centralized ones. Former smart contract DEXes do not have what it takes, we need a new generation of cross-chain Layer Zero DEXes that actually and definitively handle the majority of the market's transaction volume in an efficient, simple, quick and instantly-final fashion.

Collaboration instead of competition.

05

Some people might think we are competing with THORChain and some THORChain supporters might feel threatened by Maya, but this is completely unfounded: our real competition comes from CEXs and traditional DEXs. Any user that we bring from those alleys is a net positive for both THORChain and Maya. In other words, this is a game of adoption, and Maya will help drive this adoption forward!.

Any user that comes from a CEX to Maya and then switches to THORChain for any given reason will still make us very happy. We also believe that increases in THORChain's market share will help Maya Protocol, and that the reverse will also hold true!

Focus on different target markets.

06

The Market is huge and although there might be commonality with some of THORChain's users —especially hardcore yield seekers— Maya will be focused in the LATAM market and into much less technically oriented audiences.

Maya's emphasis is geared towards DeFi education, even using marketing channels like Tiktok and Instagram, to inform a segment of crypto users that has not been addressed by THORChain or anybody else - yet.

Compatibility.

07

We believe big institutional liquidity investors and swappers will take advantage of the compatibility between both protocols and that the same will be true for wallets, exchanges, and other platforms. Having code compatibility —due to the forked nature of Maya— will lead to easy implementation for bigger players that cannot rely on only one option. We believe most end users will eventually use THORChain and Maya interchangeably and unknowingly, kind of how we can use VISA and MasterCard with the same user experience. Every E-Commerce handles both since coded solutions support both.

Becoming price leaders together.

08

Simply put, today THORChain is dancing in an empty room. The arbitrage opportunities are constantly big since they have to be carried out against centralized exchanges and order books. This in turn creates more impermanent loss on THORChain's books, which although insured through Impermanent Loss Protection, still have a negative effect on the protocol's economy.

Having a second identical twin with whom to dance will create tighter arbitrage, distributed amongst both protocols and creating a smaller percentage of economic capture. We believe eventually an ecosystem of *Thorlikes* will exist that will dictate the actual prices of assets in a decentralized fashion. This would further drive down arbitrage value capture as a percentage of Total Value Locked in the protocols, protecting the liquidity capital of both Maya and THORChain. The objective is to create a network of L0's like Maya, THORChain and others who together become price leaders over CEXes. At that point, impermanent losses would be negligible.

Version Stability.

09

Some users look for new features and opportunities, others look for reliability and dependability. The first group will probably not choose Maya over THORChain since we will always lag behind them in updates and versions, making sure the implemented upgrades have been battle-tested first. These users will be using THORChain to take advantage of its exciting opportunities and rapid pace, but there will always be room for both groups.

Two minds are better than one.

10

Our community will grow in parallel to THORChain's and in turn bring more developers to both networks. Our teams and driving forces can help increase the rate of improvement of the THORChain ecosystem through both cooperation and competition. Additionally, we have come up with ways to further improve the protocol with an innovative multi-chain approach. Although we will be followers of the THORChain technology, we want to have a proactive approach as well, creating some cool first-mover advantages with new technologies and ideas we have developed like Stable Pools and Liquidity Nodes — more on this later.

Maya 2.0
Where we are going

INTRODUCTION

Where we are going

THORChain paved the way with their cleverly designed Proof of Bond protocol using Tendermint's powerful consensus algorithm along with excellent economic incentives for an ultra-secure Layer-0 protocol. Maya seeks to go even further by increasing the implied capital efficiency, by having more uses for its native currency, $CACAO, and by using the high security of Maya's node infrastructure for other valuable functionalities. It is important to mention that Maya will be backwards compatible with THORChain, which essentially means that Maya will inherit ThorFi - into MayaFi. We have been very selective with the changes that we do to our protocol, taking care of this compatibility with any future upgrades to the protocols we are emulating. This is very powerful, since Maya will be able to enjoy its own improvements plus the improvements of the other protocols included in its network.

Maya takes security very seriously, which is why the most sensitive aspects of the THORChain protocol, such as Bifröst, were left untouched. Additionally, audits will be conducted both before and after our launch —periodically— to ensure the security of all funds. The safer a protocol is, the more funds it attracts, especially from institutional entities.

Maya is not only committed to security, it is also committed to decentralization and censorship resistance, especially by governmental bodies, that are ever more involved in how we use cryptocurrencies. Because of this, our team will remain pseudonymous and our nodes will always be encouraged to remain anonymous.

It is our belief that delegation in protocols does not enhance security but rather harms it. Delegation creates artificially bonded nodes which have a higher incentive to become bad actors and an incentive for the node operators to reveal and promote their identities, decreasing overall censorship resistance. For these reasons, Maya Protocol and its multiple components will always work without delegation.

Besides, $CACAO holders will have other better uses for their tokens, like generating yield through liquidity providing or lending.

So what are we bringing to the table to achieve this mission? First, we will make the fairest launch possible by holding a Liquidity Auction, where all $CACAO ever to exist is shared in one event at the same discovered price by everyone, from the smallest investor to the largest whale. The team, investors and key strategic individuals will earn through their share of tokenized fees, which essentially means we only earn if we create value for $CACAO holders, liquidity providers and nodes. The Maya team then designed a whole different economic model for Nodes to increase Capital Efficiency without compromising Security, called Liquidity Nodes. This Security will be used to secure other algorithms, through our Security Node design. This feature will secure a popular Burn & Mint algorithm for truly decentralized and safe Stablecoins and Smart Contract compatibility. Some of these stablecoins can be made eligible as a trading pair in Maya for a more stable investment and to create deeper pools with decreased slippage.

We hope that the crypto community throughout the world will understand the huge implications of what we have designed and that they understand the importance and necessity of a decentralized, wide base and permissionless network of cross-chain alternatives. Centralized services in the cryptocurrency world will remain the cheapest option until a critical mass of adoption is reached, Maya Protocol is our team's shot at making this future more likely. Join us in the mission to topple Centralize Exchanges for good.

Read along each of the chapters of this whitepaper to see what we bring to the table. They cover our six unique features in detail and they all include sections such as an Introduction, Explain me like I'm five (ELI5), Philosophical perspective, Economic overview, Technical overview and Code.

Part 1. Fair Launch

No complex IDO, Maya will launch $CACAO
with our own Liquidity Auction design!

Maya has aimed to maintain its motto from the beginning: a **multi-chain liquidity protocol** in the hands of the community, protected by code and open to exchange. Initially we felt that the most successful way to achieve this goal was through an Airdrop allocation, but **it's time to upgrade to something that will boost liquidity** in the system even further: a Liquidity Auction.

ELI5

1. Different strategies are used to raise funds everytime a new crypto/DeFi project is born. Some models might be better than others but that really depends on the team's needs and creativity. There are many different ways in which DeFi projects can distribute their tokens to their users or community, some examples include holding public sales — 2017 ICOs are the classic example — Airdrops, farm rewards and more.

2. Maya Protocol's token distribution will work using a Liquidity Auction with the following cool pros:

- Lots of transparency – everybody knows when everything is happening and how.
- Permissionless – anybody can participate, there are no prohibitive minimum amounts or whitelists.
- Reduced volatility – there is symmetry of information, no one is excluded or earns less because they participated later.

3. "Liquidity Auction" sounds sophisticated but it is actually very simple:

- Anybody can contribute supported assets, such as $BTC, $BNB, $ETH, and even $RUNE, to the auction during a 21-day timeframe by sending them to a specified address. No KYC orregistration of any kind is required, except creating a Maya wallet beforehand (User Interfaces can do this for you). Also, no swaps and no withdrawals will be allowed during this period, only adding and withdrawing liquidity!

After the auction finishes, all the $CACAO tokens to ever exist —100M— are distributed to the participants proportional to their liquidity contributions. For example: if $BTC is 40% of the liquidity raised, that pool receives 40% of the $CACAO allocation.

That's it! Participants end up being Liquidity Providers by having their contributed assets + their new $CACAO tokens deposited inside Maya's pools, facilitating swaps to other users and earning a share of the fees generated.

Philosophical perspective

We truly believe that our Fair Launch process is one to be proud of. Learning from the experience of other protocols and DAOs, we came across what we think is something really open to anybody in the DeFi space to participate in. Compared to an IDO where investors with large amounts of tokens can manipulate the price and cause disadvantages for the rest, in Maya there is no minimum entry ticket, there is no previous whitelist, no special allocation for larger investors and the time range is wide and pre-announced.

In the end, we are pushing towards the objective of having one more protocol in a network of decentralized, Layer Zero cross-chain facilitators that dictate prices over the market. We want to concentrate the markets' liquidity there, instead of how it currently concentrates around centralized venues, and that is why we are looking to attract a diverse and wide user base that will become part of a community from the moment they get their first tokens.

The process also takes advantage of the built-in Asymmetrical Liquidity functionality from the THORChain codebase. We aim to:

A. Reduce Founding Team risks.
B. Make a decentralized protocol that is completely owned by its community.
C. Create incentives for the Founding Team to continue developing over the long-term.
D. Bootstrap the largest amount of external asset liquidity possible to secure the sustainable future of our protocol.

How does the Liquidity Auction tackle these issues? Let's look at its advantages:

The community ends up owning the token.

01

So the system governance is decentralized and permissionless. No founding person or investor can pump & dump, rugpull, etc. The team gets only a percentage of the fees, which means we only earn money if the community does. The team simply cannot create sell pressures for the token.

Symmetry of information.

02

Everyone has the same chances to participate during the 21 days duration of the auction. There are no discounts, no privileged information, front running or unfair allocations. Everyone essentially gets a 2x ROI during the launch, regardless of how much money is raised and what kind of assets they contributed with. There are no disincentives to share the liquidity auction details with other people, since everyone gets the same terms regardless of participation size and depth.

No inflation.

03

Which would lead to better and more attractive price action. Because we can have users and investors earn fees through the L1 codebase, it is no longer necessary to have an inflationary asset to incentivize staking. People can earn nice APY's or simply hold to keep a valuable non-inflationary asset. This will generate a more liquidity demand-sensitive system.

Large incentives to participate.

04

Remember there will not be any other $CACAO issuances, so anybody that wants to own the token will have to acquire it from somebody that got it during this mint. It is very likely that $CACAO's price will be the cheapest ever (in $BTC terms) right after the auction. This makes it more attractive for people to invest heavily during the liquidity auction - which is of course what we want, as it leads to deeper pools, reduced slippage and slip fees, attractive arbing opportunities, and overall liquidity depth. Deep liquidity attracts swap volume.

Simplicity.

05

Only one open permissionless cross-chain liquidity event to rule them all. The rules are clear: there are no KYC processes, people will have to understand and use Maya to participate - the Liquidity Auction will serve as a live Demo to our target participants - , the whole thing happens during an extended period of time and everyone participates under the same conditions. Everything is also managed directly in the Maya Blockchain, so it becomes very secure and everyone ends up being a liquidity provider!

A Liquidity Auction simply makes sense to secure the long-term future of Maya. It keeps us honest as a team, it gives everyone a fair set of rules to participate in and it will surely raise significant resources to start up a virtuous cycle for our liquidity blackhole. By having only one event, we are making sure it will be simple, interesting, and even urgent for anyone to participate, while helping Maya jump into the big leagues!

Economic overview

FAIR LAUNCH

Under normal operational conditions (after the Liquidity Auction finishes), all of Maya's AMM pools will have a 1:1 ratio between native assets and $CACAO, which means that anybody wanting to participate in the protocol would ideally have to match their native asset contributions with the same amount denominated in $CACAO tokens; this is called "symmetric liquidity".

If for some reason we would want to add only one of the two assets - "asymmetric liquidity" - a slip fee would be charged because imbalances would be generated within the liquidity pool.

During the liquidity auction, all the external liquidity provided will be asymmetric because nobody has had the possibility of buying $CACAO yet - it virtually does not exist yet! Particularly interesting is that users can participate in the auction by contributing $RUNE into our $RUNE / $CACAO pool and the effects that this pool will have for the Maya <> THORChain interconnection, presenting many arbitrage opportunities and inviting traders and bots to bridge between the two protocols continuously to take advantage of them (the first step in our vision of a network of L0's becoming price leaders in the crypto market!).

It is important to mention that, because $CACAO is a native coin to a CosmosSDK blockchain, it would be very easy to integrate into any wallet or exchange that can already handle $RUNE, $LUNA, $ATOM, $OSMO and many others. $CACAO enjoys the rest of the ecosystem's advantages as well, such as cheap transaction costs, fast settlement times (<10s), ease of use and secure wallet/transaction systems. Any exchange that wished to list our coin would be able to do so quickly and easily.

Technical overview

I. Liquidity Auction

To make the Liquidity Auction work, we will use already existing attributes of Ixmu - our equivalent for Mimir, in THORChain — plus some of our own. These attributes will control the actions that all liquidity providers can take on a specified time frame in order to successfully execute our Fair Launch.

Using Ixmu Key terms, we want to accomplish the following:

1. Users should only add/withdraw liquidity.
2. Users should not be able to swap or send.
3. Users should not be able to get $CACAO until the end of the Liquidity Auction.

The process we will follow starts by enabling the new “LiquidityAuction” Ixmu attribute which stops users from being able to swap between any assets, because all swaps between native assets without $CACAO would be discarded. This behavior will work for 21 days, after which the $CACAO is distributed and “LiquidityAuction” is disabled.

Here are the already existing transactions, along with the new ones and the specific actions that they disable:

ATTRIBUTE	SEND	SWAP	ADD	WHITDRAW
HaltChainGlobal	✓	✗	✗	✗
PauseLP	✓	✓	✗	✗
HaltTrading	✓	✗	✗	✓
LiquidityAuction	✓	✗	✓	✓

Maya

Distributing $CACAO tokens after the Auction process is simple and will require the use of the “Donate” message to dispense them into our pools, proportionally to their depth in USD terms, using an End-of-Auction over-all market price

Any user that contributed their native assets ends up having their original assets plus their newly earned $CACAO. Any and all UI’s supporting the Maya Stagenet —and therefore our Mainnet— can host the Liquidity Auction. Code Savvy individuals may also use the API/Transaction Memos directly.

1. As a user I should only be able to provide asymmetric liquidity throughout the Fair Launch, so that I can get $CACAO in the Liquidity Auction.

Acceptance criteria:

1.1 Users should only add/withdraw liquidity.
1.2 Users should not be able to swap or send.
1.3 Users should not be able to get $CACAO until the end of the Liquidity Auction.

2. As a Liquidity Provider I should be able to withdraw my liquidity at any point in time, so that I can recover my money if I no longer want to participate in the Auction.

II. Genesis Nodes

Our first nodes will be called "Genesis Nodes", and there will be six of them. Because they will start running the protocol with no $CACAO bonds — remember there will still be no $CACAO tokens until after the Liquidity Auction is finished — we will need them to already have some dependable reputation, which is why they will need to be pseudo-doxxed nodes, run by decentralized organizations close to Maya.
Once our chain and systems have been started, these initial nodes will exit over time as other nodes enter the network.

Genesis nodes will be approved using a specific custom-made token for this purpose, they will not be entitled to any fees, special allocations or pre-mines of any kind. For more details on our Genesis Nodes please refer to Part 4: Security Nodes of this document.

User story:

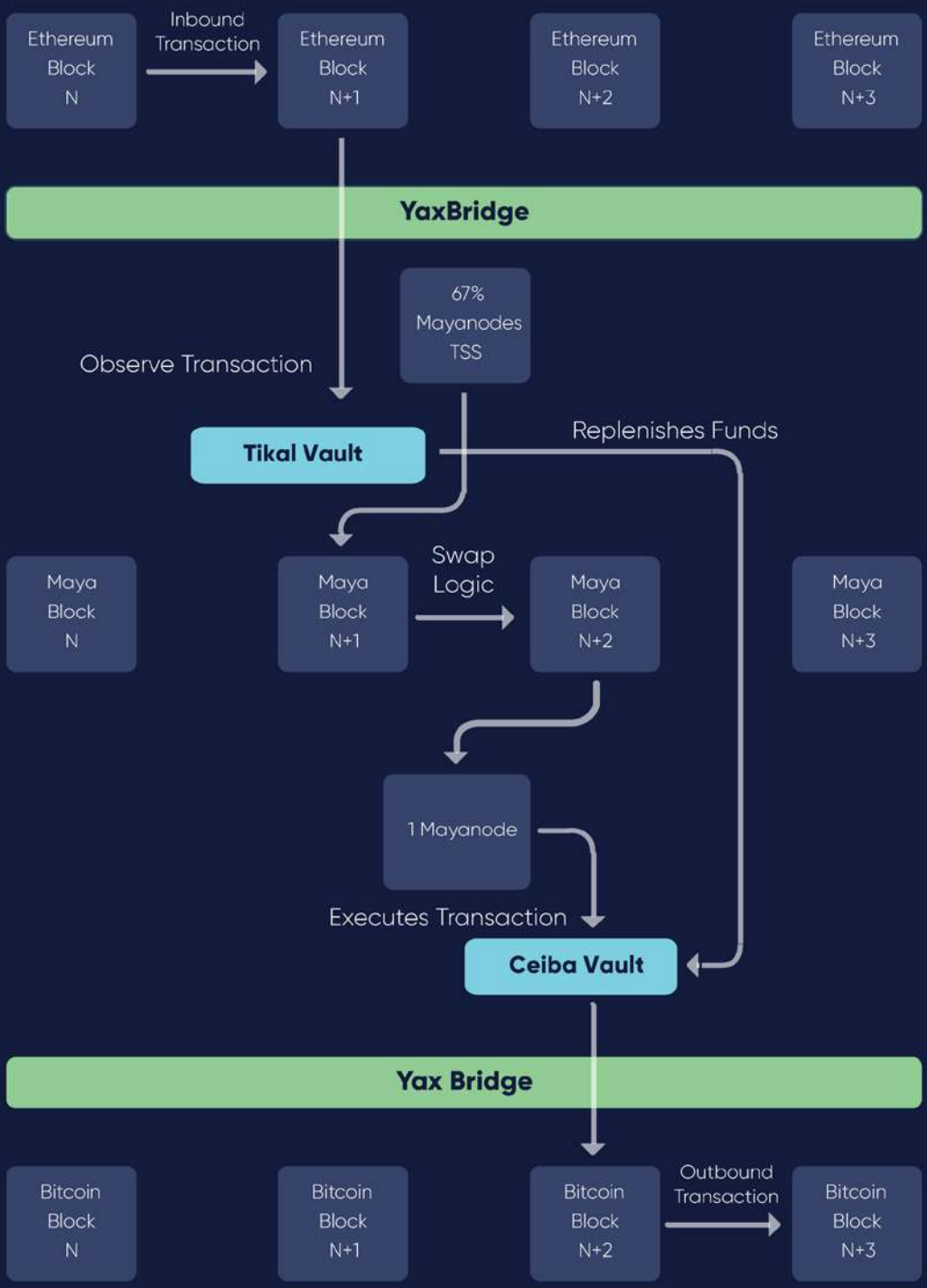
1. As a genesis node, I should be able to be a validator in the chain without contributing economically and without affecting the $CACAO supply. Also, I should not get any sort of pre-mine or reward during this period.

III. $RUNE

THORChain uses Bifröst, a module that makes it possible to generate a native asset exchange network. The Maya equivalent is Yax bridge. We are fully capable of receiving $RUNE transactions and have this token incorporated into our pool offering by adding our own THORChain client to the Yax bridge.

User story:

1. As a user, I should be able to add and withdraw $RUNE liquidity on Maya during and after the Liquidity Auction.
2. As a user, I should be able to swap $RUNE for any other asset in Maya after the end of the Liquidity Auction.



CODE

1. Liquidity Auction

https://gitlab.com/mayachain/thornode/-/issues/32
https://gitlab.com/mayachain/thornode/-/issues/34

2. Genesis Nodes

https://gitlab.com/mayachain/thornode/-/issues/33

3. $RUNE - Yax Bridge

https://gitlab.com/mayachain/thornode/-/issues/37

Part 2. $MAYA Token

Best way to benefit in Maya, passively.

We want to have an **additional option** to participate in our project, and that's why **$MAYA tokens** exist. With their profit-sharing model, **anybody can participate** from the fees generated by the protocol.

ELI5

1. Maya Protocol has been designed to be optimally fair and open. To accomplish this, two different tokens are contemplated: $MAYA and $CACAO. Both tokens can be freely traded and have different and important use cases.

2. $CACAO is our flagship token, and we will have 100M of them. They will all be minted at once and then distributed to the people participating in our Liquidity Auction. Aside from being required to run a node, they can be paired against other assets inside our liquidity pools to earn a percentage of the transaction fees generated by swaps.

3. $MAYA coins can be used to participate in our protocol's total revenues and there are exactly 1M of them. They served as our initial stages' funding mechanism and, by design, keep incentives for our developer team to continue their hard work in the short term and long term.

Philosophical perspective

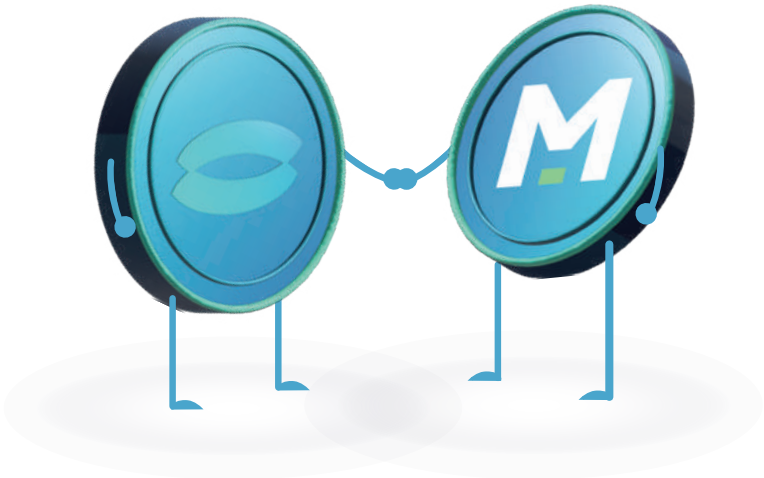
Having two tokens is directly related to our decision to launch using a Liquidity Auction and to how we want our community to be as equitable, as big and as widespread as possible.

$MAYA's design has been carefully planned to prevent incentives' misalignments for the insiders holding them and they allowed us to financially bootstrap our project in its earliest stages without having to recur to any pre-sales of $CACAO, which we really wanted to avoid.

Both tokens can be freely traded and they both offer their respective holders the right to earn a percentage of the fees generated inside our protocol although with different approaches, as described below.

> **On Governance.** To achieve a high level of decentralization Maya has minimal governance, in a similar way to THORChain. This aspect is directly related to the security of the protocol so that the nodes are the ones who carry out the governance and ensure that all incentives are granted through code. In the specific case of $MAYA tokens, they don't give any governance rights to their holders, or any other right whatsoever.

You can see more about this topic here:
https://docs.mayaprotocol.org/how-it-works/governance



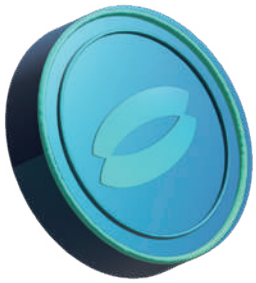
Economic overview

We will highlight the differences between $CACAO and $MAYA.

$CACAO

$CACAO tokens power the Maya Protocol ecosystem and provide the economic incentives to secure the network because they are required to run Maya nodes. Also, all of our liquidity pools consist of a native token paired against $CACAO, for example, $BTC / $CACAO or $ETH / $CACAO.

Because $CACAO is needed to become a liquidity provider but their supply is limited to 100M, the more people that would want to participate in our ecosystem, the higher the value of $CACAO tokens has to be. Their economic value would also grow if $CACAO tokens could be used natively and productively in other chains or projects - which we intend to do.



$CACAO

The bridge between blockchains. It is required to be paired as a settlement asset in continuous liquidity pools.

$MAYA Token

The native fee accrual token of Maya which earns a portion of the fees generated by the protocol.

$MAYA

$MAYA tokens perpetually capture 10% of all the fees generated by the users swapping inside our protocol. They are essentially a tokenization of our present and future cash flows which means, firstly, that the more active our exchange is, the better price they should have and, secondly, that $MAYA's token holders are heavily incentivized to see our protocol grow with time. Lastly, and most importantly, $MAYA holders only earn value if Maya's ecosystem earns 9x as much (and real value, since Maya does not have inflation or other artificial methods to boost APY).

These tokens will be initially held by participants of all levels inside of Maya: our private investors, our development team, our advisors and our founders. There is also a surprise for early Node Operators, for Thorstarter supporters and $RUNE owners.

P/E Ratios

Because of its economic design, $MAYA tokens can be treated as some sort of stock or economic participation in our project and are easy to value using traditional P/E and EPS ratios since $MAYA price, our current daily Fee Revenue and $MAYA's fixed supply are public in real time.

P/E = $MAYA last public price / 10% * Annualized Protocol Fee Revenue

EPS = 10% * Annualized Protocol Fee Revenue / 1,000,000

This also means there usually should not be many irrational fluctuations in its price and that $MAYA tokens will also reflect the market's perceived value of our future cash flows. It is important to mention that $MAYA has no governance rights over Maya Protocol or any other privilege or use aside from collecting 10% of fee revenue.

It is important to note that $MAYA will not be available in Pools on Maya Chain. This means there will be no recursive nature to $MAYA being priced into $CACAO creating artificially high values for $MAYA back. Additionally, this completely cuts off $MAYA of having any influence on the price of $CACAO. Finally, it makes it less liquid and harder to trade, making its owners more likely to simply hold them to collect fees passively.

Technical overview

Who will own the $MAYA tokens?

First of all, $RUNE owners!

We are a friendly fork of THORChain and have no interest in vampiring away any of their capital or any of their users. We even plan on sharing 10% of the total $MAYA token supply with them as an acknowledgement of their support for THORChain, which in turn makes Maya Protocol possible.

$RUNE owners will get $MAYA tokens freely, simply by:

A. Holding $RUNE in their wallets,
B. Having $RUNE locked in their LP positions and/or
C. Having $RUNE bonded in a Node.

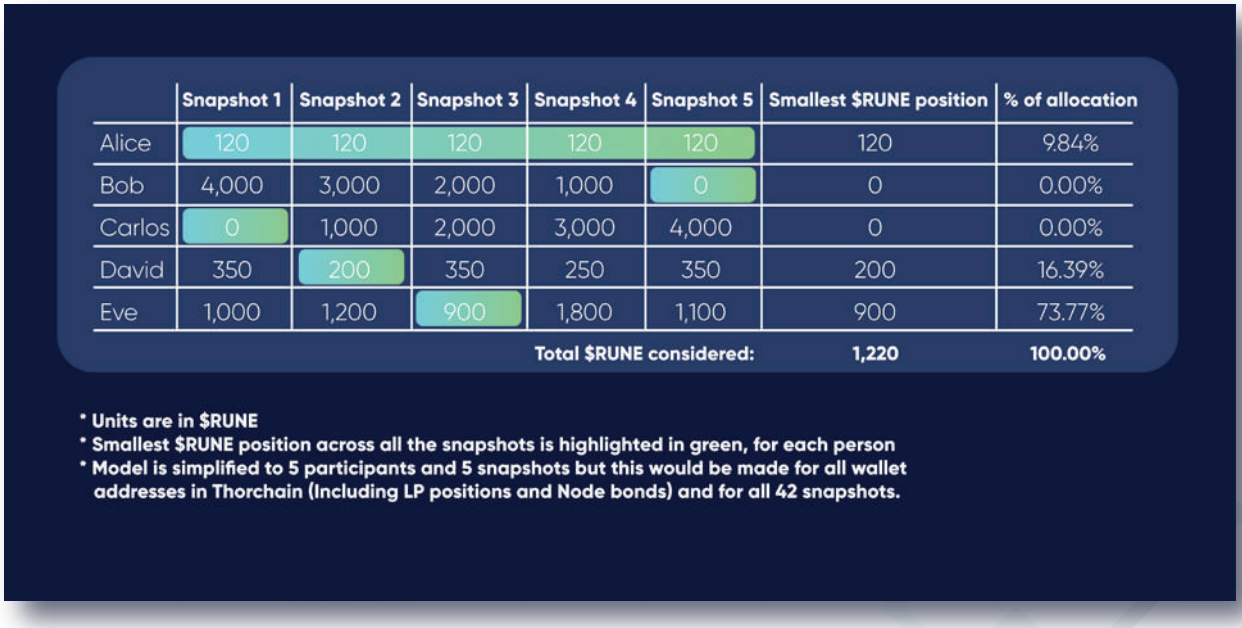
To make sure that only "fresh" capital is attracted during our launch (ie. there is no capital leaving THORChain) we designed the following rule set:

1. Daily snapshots of $RUNE distribution on Thorchain will be taken every day at random for 42 days, starting right before the Liquidity Auction and running through 21 days after the end of the Liquidity Auction.
2. $MAYA tokens will be distributed considering the smallest $RUNE position that the $RUNE owners held in any of these 42 snapshots.

This way, if, for example, whomever $RUNE holder sells half of his position to add it to our Liquidity Auction looking to get some $CACAO tokens, that holder would only get half of his $MAYA tokens at distribution.

Ultimately, if you want a bigger share of the $MAYA tokens as an OG THORChain supporter, you are encouraged to hold your $RUNE positions or even increase them, and if you simultaneously want a bigger share of $CACAO allocation, you are encouraged to participate in the Liquidity Auction with capital brought from other, different sources.

The process' details to create a Maya wallet that receives the corresponding $MAYA allocation as a $RUNE holder will be announced separately, but it will simply require you creating a Maya Address and sending at least 1 $RUNE as Add Liquidity asymmetrically or symmetrically (which can be withdrawn during the snapshot period, we only need this transaction to relate your Maya Wallet to your Thorchain Wallet).



	Snapshot 1	Snapshot 2	Snapshot 3	Snapshot 4	Snapshot 5	Smallest $RUNE position	% of allocation
Alice	120	120	120	120	120	120	9.84%
Bob	4,000	3,000	2,000	1,000	0	0	0.00%
Carlos	0	1,000	2,000	3,000	4,000	0	0.00%
David	350	200	350	250	350	200	16.39%
Eve	1,000	1,200	900	1,800	1,100	900	73.77%
				Total $RUNE considered:		1,220	100.00%

* Units are in $RUNE
* Smallest $RUNE position across all the snapshots is highlighted in green, for each person
* Model is simplified to 5 participants and 5 snapshots but this would be made for all wallet addresses in Thorchain (Including LP positions and Node bonds) and for all 42 snapshots.

Second, Early Nodes!

An additional 10% of the $MAYA total supply will be used to reward our early node operators like so:

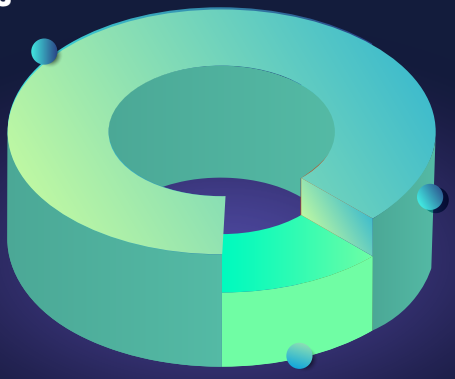
1. 3.33% of all the $MAYA tokens will be shared to the active Validator Nodes securing our network **one month after** the end of the Liquidity Auction.
2. An additional 3.33% of all the $MAYA tokens will be shared to the active Validator Nodes securing the network **four months** after the end of the Liquidity Auction.
3. An additional 3.33% of all the $MAYA tokens will be shared to the active Validator Nodes securing the network **twelve months** after the end of the Liquidity Auction.

This token incentive rewards our early heroes and supporters and potentially catalyzes our first bond wars since only churned-in nodes become eligible. While bond wars are great for THORChain, they will be even more beneficial to Maya's, for reasons that will be covered on Part 3 of this Whitepaper.

Last but not least, the Dev Fund

Finally, the remaining 80% of the tokens will be initially awarded to the Maya team, at all levels of the organization, including our developers, our advisors, our investors and other strategic individuals and institutions that have readily supported us.

90%
LPs & Nodes

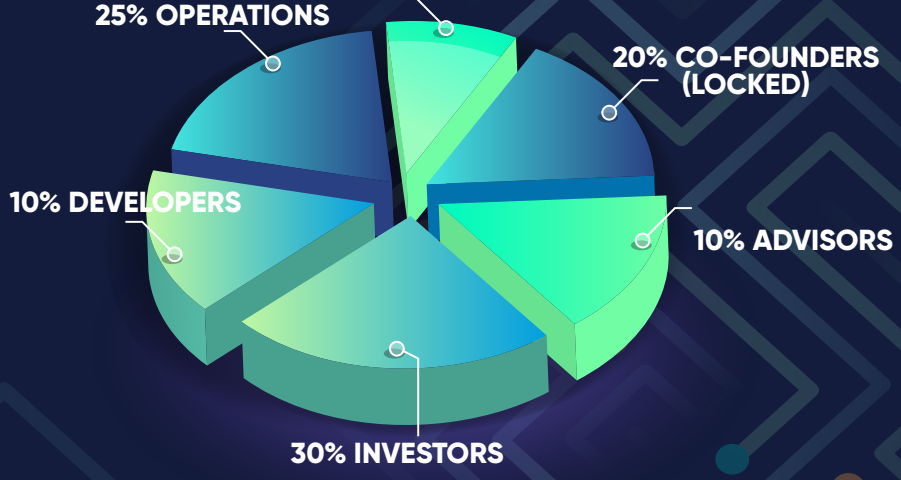


10%
Maya Fund

MAYA FUND

- 10% RUNE OWNERS
- 10% EARLY NODES
- 80% DEV FUND

DEV FUND



Remember none of them own any $CACAO yet, nor will they do at any point before or after our Liquidity Auction unless they participate in it with their own funds, under the same terms as any other participant. This is very positive for the Maya community, since there is no counterparty risk of these participants dumping or rugpulling $CACAO since they got it at the same price basis as anyone else during the Auction. Likewise, dumping $MAYA has no direct effect on the price of $CACAO. Therefore, $CACAO will have very little sell pressure from its origins, a liability that most protocols often have. $MAYA tokens are the only way to repay them for their big time commitment and sterling efforts, in a fair way that is aligned with the community.

As a final display of the Maya founders' commitment for the long run, their own share of $MAYA tokens will not be transferable and will be permanently locked in perpetuity. These tokens will only accrue $CACAO fees over time, which will be transferable.

Thorstarter's share of $MAYA tokens will be shared with Forge Stakers. Thorstarter will announce separately how their supporters can benefit from our launch.

User Stories:

1. Maya Fund

- As a Maya user, I want the Maya Fund to be funded with 10% of the gas and swap fees that are generated in the chain to distribute those funds among the Maya users that hold $MAYA Token, denominated in $CACAO.
- As a Maya user holding $MAYA, I want to receive $CACAO distributions from the Maya Fund proportional to the amount of $MAYA Tokens I own every 14,400 blocks (approximately every 24 hours).

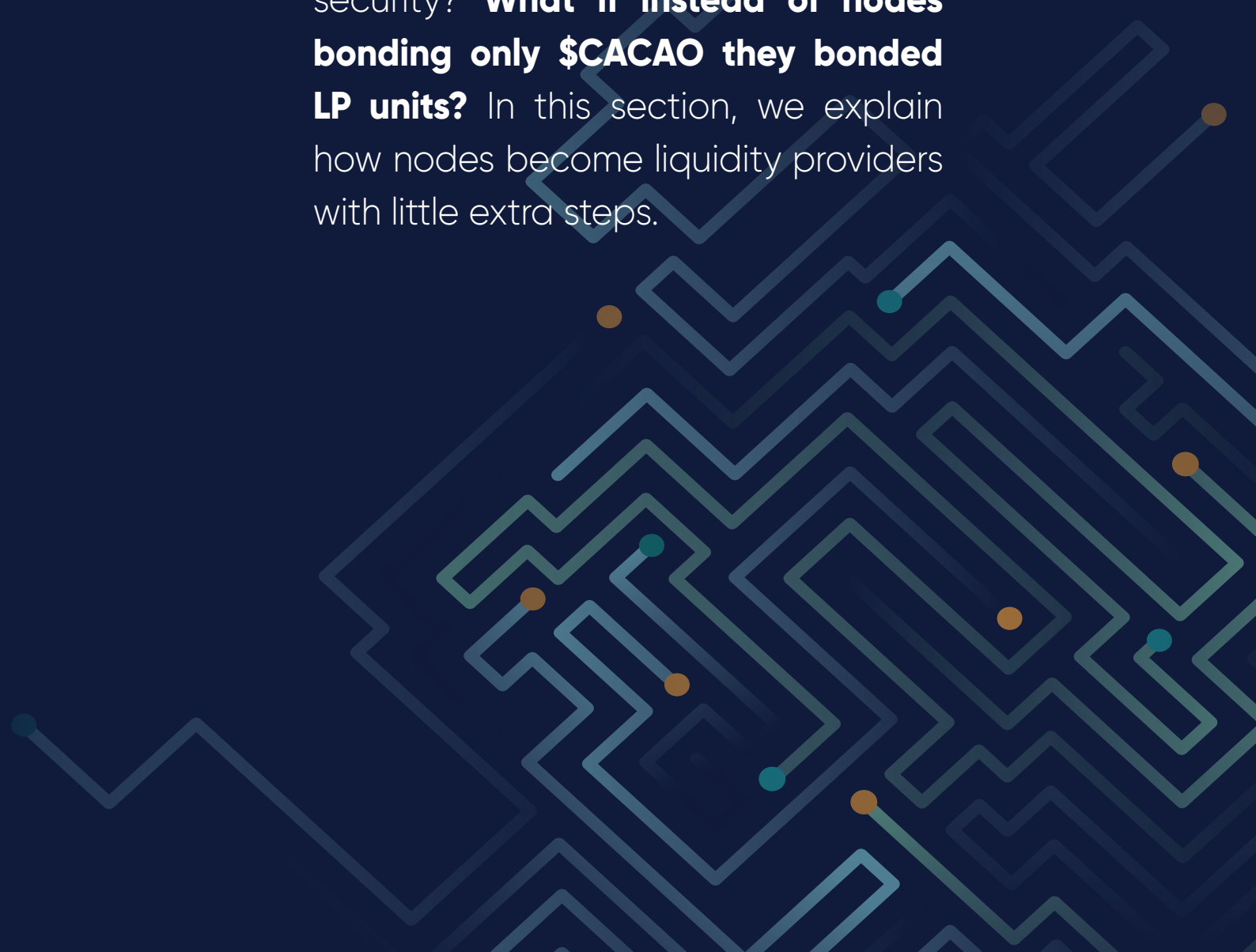
Code

https://gitlab.com/mayachain/thornode/-/issues/39

Part 3. Liquidity Nodes

How MAYA obtains superpowered capital efficiency

How do we accomplish more capital efficiency without compromising security? **What if instead of nodes bonding only $CACAO they bonded LP units?** In this section, we explain how nodes become liquidity providers with little extra steps.



ELI5

1. Traditionally, to secure a place in the Pure Bond Model, you need to buy and stake a big amount of native asstes. It isn't called staking, it's called bonding, but the principle is similar: you entrust your assets to a system that will hold them for you temporarily. This is all ingrained into the Pure Bond Model architecture as a security feature since all of these bonded assets are susceptible to being seized if the node misbehaves or breaks the rules in any serious way. This keeps nodes honest, since bonds are higher than the assets they secure.

2. In Maya Protocol, nodes still need to buy and bond a big amount of $CACAO for the exact same security reasons but we store them in a totally different place. Whereas in the the other model bonded native tokens are locked up unproductively inside a specific address, bonded $CACAO in Maya is deposited inside our Liquidity Pools, paired with other native assets and generating yield! Any capital bonded by our node operators participates in the fees generated by the pools in which they are deposited, making our use of capital much more efficient!

3. This feature is great because it means that Maya node operators can supercharge their invested capital efficiency by earning both Liquidity Provider rewards plus their regular Validator Rewards. Capital efficiency is no longer inversely proportional to Security!

Philosophical perspective

Node operators becoming Liquidity Providers simultaneously have several economic and tokenomic implications:

The efficiency of the capital employed (ie. bonded) to obtain a place in the nodes' list is enhanced considerably when compared to the Pure Bond Model —where the native token is being used solely as an economic guarantee and is not generating any type of yield on its own.

Not all assets will be bondable either. Only, relatively, lower volatile external assets such as stablecoins, BTC or ETH will be; other Bond Pools could be added with a 67% nodes' consensus. For security reasons, it is suggested that no more than 2 assets per chain are bondable (ie. BUSD and BNB on Binance Chain, but not any other BEP2 coins).

This innovative alternative to traditional bonding model simply follows the economic principles of efficient use of capital and resources. Any investor that can generate better risk-adjusted capital returns will tend to do so and so we want to offer our operators this efficient and interesting model.

We should also mention here that whereas the traditional economic design and bonding requirements result in a theoretical deterministic value for $RUNE's market cap of 3X its Total Value Locked (TVL), in Maya $CACAO's deterministic price will be 1X TVL. This might look lower at first glance but is actually the reflection of the higher capital efficiency within our protocol and the tighter relationship of $CACAO price to liquidity and fee generation.

Finally, we designed a model that creates a liquidity flywheel effect while permitting for similar security parameters than the legacy pendulum and brings other advantages that we can test —audits and Maya Stagenet first of course— for THORChain to implement if we all find them practical and successful.

Economic overview

Liquidity Nodes result in adjustments to the Pure Bond Model security policies, which we tailored to accomplish three important things:

1. More than 67% of capital should be bonded by our nodes, to keep them honest, in fact, closer to 85% is preferred. A sybil attack at 67% nets a loss of at least 12% of the attacker's funds, and at 85% nets at least a 20% loss*
2. This capital balance must be found by rational market forces (ie. supply and demand).
3. We must incentivize decentralization (ie. a high node count).

*The magnitude of these losses assumes the $CACAO price did not rise as the attacker accumulated $CACAO, added it as LP in different addresses in one block and churned-in 67% of the Nodes on the same block. This is an unreasonable assumption, since the buy pressure of the accumulation would bring $CACAO's price higher, making the cost basis of the attacker higher relative to incumbent Nodes and LPs; making his/her loss higher. Additionally, adding more LP positions increased TVL which again increased $CACAO price to the attacker at a profit to incumbents. Finally, churning in is limited and successfully doing so with many Nodes while competing against other Nodes is difficult, given the attack so far has made optics for Maya bullish and become a Node more attractive. If there are 40 Nodes, attacker needs to churn-in 27, winning the Liquidity Bond war at least 27 times (and as more of Attacker's nodes are churned-in, it is more likely at churn-out that one of its nodes are churned-out). This all amounts for a significantly higher loss to Attacker than the aforementioned 12% and 20%.

We call our resulting model "The Incentive Curve" and it works by algorithmically balancing the nodes' and markets' incentives to either provide more liquidity or bigger bonds by increasing or decreasing the participants' rewards on each of these sides, periodically.

“The Incentive Curve”: For every new block...

System income is divided as follows:

$$Yield = 0.9\ System\ Income$$
$$Maya\ Fund\ Allocation = 0.1\ System\ Income$$

Yield:

$$Yield(x) = NER(x) + LR(x)$$

Where NER = Node Exclusive Rewards and LR = Liquidity Rewards, where clearly

$$LR(x) = Yield - NER(x)$$

Our incentive curve uses the following equation for NER(X)

$$NER(x) = \begin{cases} 1, & x < 0.6667 \\ 3(1-x), & x \geq 0.6667 \end{cases}$$

$$W\ ere, x = \frac{Bonded\ LP}{Total\ LP}$$

Thus, Nodes’ Average Earnings (NAE)

$$NAE = LR(x)\frac{x}{Node\ Count} + \frac{NER(x)}{Node\ Count}$$

Liquidity Providers’ Average Earnings (LPAE):

$$LPAE = \frac{LR(x)(1-x)}{LP\ Count}$$

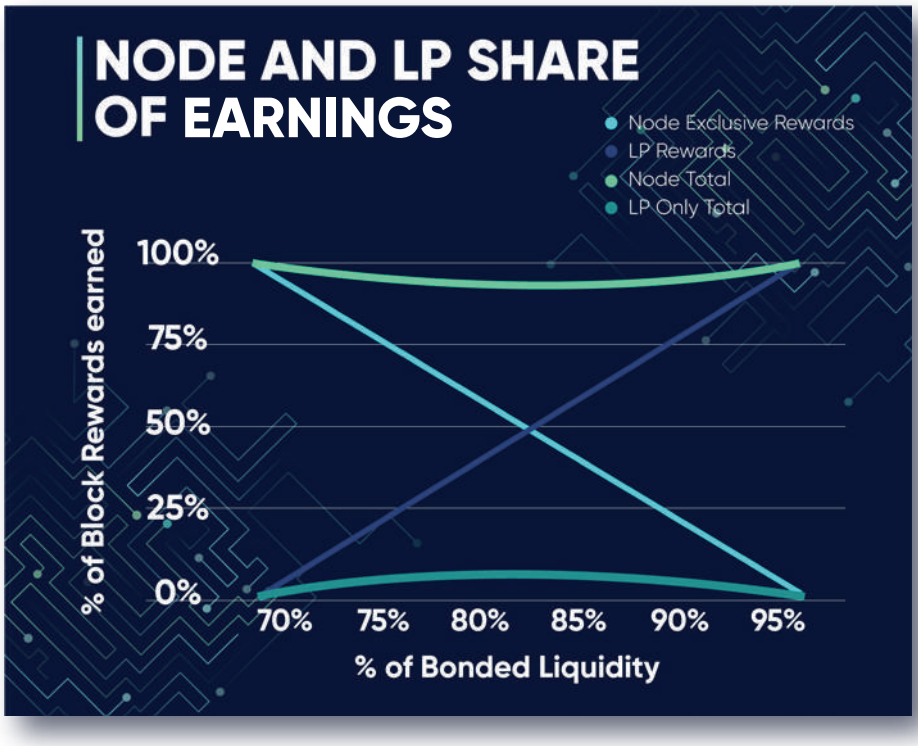
For any individual LP, Earnings is equal to the increase in value of their own LP Units due to the Yield that was kept in pools that LP participates in.

For any individual Node, Earnings is equal to the increase in value of their own LP Units due to the Yield that was kept in pools that LP participates in, plus the Node Exclusive Reward divided by the amount of Nodes.

Please note:

- Nodes earn both Node Exclusive Rewards (NER) and Liquidity Rewards.
- LP's earn only Liquidity Rewards (LR).
- Node Exclusive Rewards (NER) is distributed evenly among all nodes whereas Liquidity Provider Rewards (LR) is paid out relative to their bonded liquidity.

All the calibration of the economics and incentives that manage the system are algorithmic and code driven, whenever the total network's liquidity is tilted too much into either side of the spectrum (too much bonded liquidity vs. too much provided liquidity) the incentive mechanism reacts by balancing out the rewards conversely. Visually, the curve looks like so:

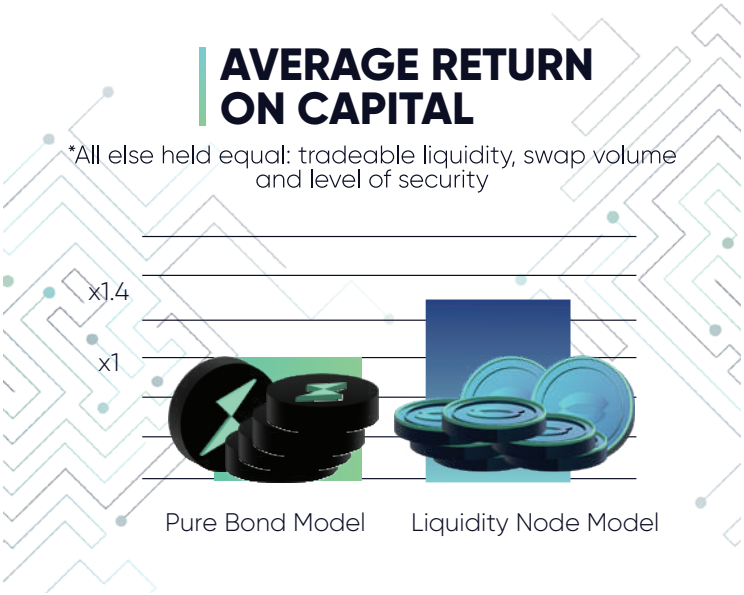


And it basically creates a liquidity flywheel, where:

- At a moderately highly bonded state, there is an incentive for new capital to be added via LP'ing. Liquidity can be added this way much more rapidly than nodes' can churn in or out.
- If too much liquidity is provided by LP's then the network would tip into an unsafe state, which would incentivize the nodes to bond more capital, benefiting our depth and volume in the process again.
- Liquidity is bonded by the nodes that brought the most liquidity on the next churn, and the system comes back to or above balance.

- Notice that TVL is increased when the incentive mechanism pulls in either direction, whereas on Thorchain the pull increases TVL in only one direction. This means assets are pulled into the protocol regardless of whether it's moving from unsafe towards overbonded or it's moving back.
- This process can go on and on, attracting new liquidity every time, as long as cross-chain swaps remain plentiful, in a bright multichain future.

We can compare the behavior of this model with respect to the traditional one by normalizing through "Node Premium" where Node Premium is a measurement of how much more a node earns with respect to LP's per unit of capital invested, in average. On both Thorchain and Maya the designed equilibrium is at Node Premium = 2, where nodes earn on average twice as much as LPs. This point sits at 66% bonded native tokens in the Pure Bond Model and at 85% bonded liquidity in Maya.



The following table shows this comparison, ie. how much more a Node earns compared to LP´s for the same investment in those conditions, assuming the same fees and tradeable liquidity. "Node M/T" refers to the increase in earnings for equivalent swap volume conditions between our Liquidity Node's model and the Pure Bond Model. Same for "LP M/T" for Liquidity Providers. It is important to mention that the Maya figures in this comparative analysis already take into account the 10% $MAYA Token deduction, we are comparing apples to apples here. Finally, M/T comparisons were done by multiplying a one day ROI by 365, APY would be compounded and show a greater difference.

Shared Criteria	**Pure Bond Model**		
Node Premium	**Bonded RUNE**	**Pooled RUNE**	**ASSETS/TVL**
0.33	80.00%	20.00%	17%
1	71.90%	28.10%	22%
2	66.67%	33.33%	25%
3	63.75%	36.25%	27%
5	59.90%	40.10%	29%
320	50.30%	49.70%	33%
Infinity	33.00%	67.00%	40%

Shared Criteria	Maya		
Node Premium	Bonded Liquidity	Unbonded Liquidity	ASSETS/TVL
0.33	N/A	N/A	N/A
1	100.00%	0.00%	50%
2	84.70%	15.30%	50%
3	79.75%	20.25%	50%
5	75.00%	25.00%	50%
320	66.77%	33.23%	50%
Infinity	50.00%	50.00%	50%

Shared Criteria	Pure Bond Model	MAYA		
Node Premium	ASSETS/TVL	ASSETS/TVL	Node LN/PB	LP LN/PB
0.33	17%	N/A	N/A	N/A
1	22%	50%	104.86%	105.46%
2	25%	50%	46.22%	46.03%
3	27%	50%	25.98%	28.44%
5	29%	50%	4.76%	13.63%
320	33%	50%	-31.45%	-53.50%
Infinity	40%	50%	-55.67%	N/A

Shared Criteria	Comments
Node Premium	
0.33	This situation is not possible in Maya
1	
2	Designed equilibrium for both
3	
5	Slow Capture attack profitable in both Maya & PB
320	Slightly above where Node coordination attack is profitable on PB
Infinity	Fast Sybil attack profitable in both Maya & PB. To note that in both models, LPs have gotten 0% APY on their Liquidity since the step above.

Notice a few things from the table above. The first is we are conserving the Pure Bond Model security boundaries at the same Node Premium's, making security relatively equivalent. A small caveat here is that losses are steeper with the Pure Bond Model than they are on Maya due to the attacking node losing all its native tokens while on Maya, $CACAO is only half of losses at stake to Attacker. So although breakeven for attacks are at the same Node Premiums, losses rise more quickly from above that point on the traditional model.

This consideration is important since although a rational actor would not consider attacking at a 20%+ loss*, an irrational/externally motivated bad actor could accept the loss. This is why it is important to have a diversity of chains with deep liquidity, making it more difficult and expensive for irrational actors to take down the entirety of cross chain DEX infrastructure. The bigger the TVL, the bigger this loss is in absolute terms and the harder it is for irrational actors to risk enough funds for an attack.

Second thing to notice from the table above is that the increased yield relative to the legacy incentive pendulum model is higher at higher bonded states. This means that Maya operates much better at high bonded states when compared to the old model. This is good, since we generally prefer to err towards the side of overbonding. As the tip scales towards the underbonded state, the system stops becoming noticeable better than the old model.

Finally, notice Nodes never risk earning less returns per dollar invested than LPs do. By the time earning parity is marginally reached (Node Premium = 1.01), although LPs earn great returns on the investment and it is very attractive to become an LP, Nodes still earn more than LPs and then the same at the limit. This means that it is much more likely that more LPs join when reaching these overbonding levels than Nodes leaving, given they are still getting an attractive return on their investment.

On slashing...

Slashing mechanisms needed a little revamp too, since whenever we slash a node we are still interested in keeping their liquidity available in our pools. Additionally, sometimes slashing is a mistake, so we need to account for these slash points but only execute them once a Node withdraws its liquidity. We are thus introducing "anti LP units" which are assigned to nodes that showed potential malicious behavior or downtime in proportion to their merited slash. These Anti LP units specify the value accrual of a slash point's liquidity that no longer belongs to the penalized nodes and how much of their assets will be redirected to the Protocol Owned Liquidity whenever these nodes decide to withdraw their bond.

When any node's Anti LP tokens become 20% of their provided liquidity, it becomes dangerous that they protect any funds since they no longer own a significant part of their original bond. These nodes are therefore subject to being banished, which means they are unbonded and their assets are completely redirected to paying back all owed liquidity to the protocol through the slash fees generated.

Nodes can avoid being banished —also losing ILP seniority and their node spot— by adding more liquidity to offset this Anti LP tokens percentage and then wait to be churned-out to settle any pending accounts while they are unbonded.

Manual and automatic forgiving of slashing work using these Anti LP units too, with mechanisms designed to remove them in special situations like whenever all the nodes accrue them simultaneously or because of any critical consensus failures.

Liquidity Nodes in a Nutshell

1. Capital Efficiency is no longer inversely proportional to Network Security.
2. All of TVL is in pools and is actively traded, making Maya significantly more productive with capital.
3. Increased Capital Efficiency means increased average yield for all ecosystem players.
4. On average, Nodes with lower bonds get higher return per dollar invested than Nodes with higher bonds, making churn-in competitions fiercer and contributing to decentralization and bond homogenization.
5. As more Nodes compete to churn-in, they add more liquidity. This increased liquidity turns Incentive Curve further down making it even more attractive to become the winner Node.
6. As Bond Wars compete on Liquidity Provider Units, Pool Depth increases.
7. As the incentive curve system pulls in any direction, Pool Depth increases.
8. Increased Yield and increased Pool Depth make affordable swaps more likely.
9. Node to LP and LP to Node latency is reduced and very easy to do for Operators, without incurring slip fees.
10. Standby Nodes earn yield while they wait to win the Bond War and churn-in, making it less risky to compete.
11. Nodes no longer need 100% exposure to $CACAO, making it more likely for Institutional Investors to opt-in as Nodes.
12. Node misbehavior causes slashing of a Node's LP units that are converted into Protocol Owned LP Units that count towards unbonded liquidity. These Protocol Owned LP units will never exit, staying as a buyer of last resort.
13. Liquidity Auction makes a lot of sense in Maya due to all capital already being locked in Pools as LP ahead of Liquidity Node churn-in competition.
14. Liquidity Auction is the cheapest time for a Node to acquire enough LP units to compete for churn, making it very attractive for aspiring Nodes to participate in the Auction with as much liquidity as they feel comfortable with, setting Maya up for deep pools from the very beginning.

Technical overview

User stories:

1. LP bonding

- As a node operator I want to be able to use added liquidity as a bond by providing a node address in the bond message and signing the message with the liquidity provider address, so that the network can take advantage of the bond to be part of the liquidity. The Node address and LP address are one to one.
- As a liquidity node I want withdrawals to be disabled for the liquidity that was bonded, so that any node operating has stake on the network.

2. AntiLP slashing

- As a Node Operator, I want other nodes slashed when they don't vote, have downtime or misbehave. This slash is in the form of LP slash points, or Anti-LP Units, that will later be settled by the slashed node at withdrawal.
- As a node operator I want to forgive LP Slash points with the following format FORGIVE:[Asset]:[Amount]:[Address (optional)] with 67% consensus, so that systemic network problems don't affect node funds and security.
- As a node operator I want LP Slash points owed by the 1st quartile Node automatically forgiven every 120 blocks, so that most slash points given by network errors are negligible, and Slash is mostly for considerable down time and misbehavior.
- As a node operator I want other Node Operators forcefully removed from the validator set if their AntiLPT tokens become 20% of their bonded liquidity, so that they do not represent a security risk for the network.

3. Incentive Curve

- As a liquidity node I want to receive both node-exclusive rewards AND liquidity awards according to the Incentive Curve model, so that I can cover operating expenses of running a node.
- As a liquidity provider I want to receive liquidity awards according to the Incentive Curve model, so that the network always remains safe.

4. Fair Launch Consideration

- As a genesis node, I want to set an Ixmu Key that overrides the Bonded Liquidity / Total Liquidity parameter to 85% such that LPs do get rewards right after the Liquidity Auction despite there being 0 bonded liquidity at that time.
- As a genesis node, once more than 12 Nodes have churned in, I want to keep overriding Ixmu Keys slowly lower over an extended period of time until the real parameter equals the overwritten parameter, ensuring the network is in a safe state before genesis nodes churn out.

CODE:

LP Bonding
https://gitlab.com/mayachain/thornode/-/issues/43
Slashing
https://gitlab.com/mayachain/thornode/-/issues/44
Fair Launch Considerations:
https://gitlab.com/mayachain/thornode/-/issues/33
Incentive Curve:
https://gitlab.com/mayachain/thornode/-/issues/45

Part 4. Security Nodes

Exporting security to other Application-Specific-Blockchains and creating a Maya Economy.

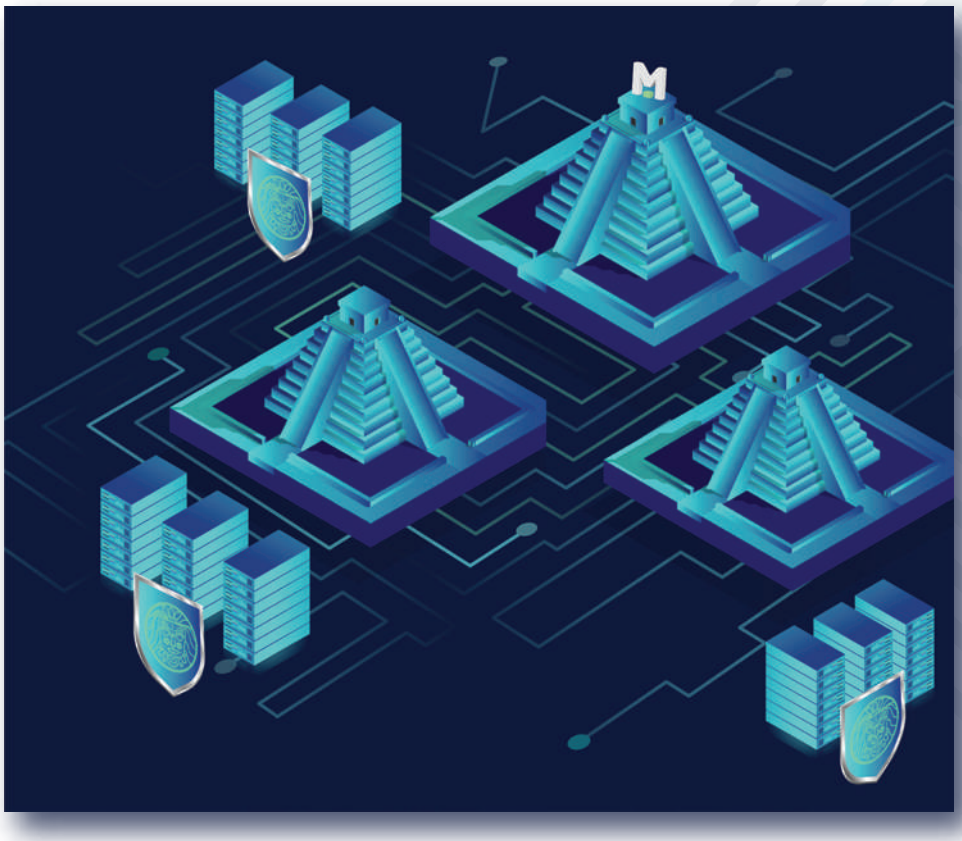
Maya Protocol is designed to be **safe, useful** and **solvent** in order to attract Liquidity Providers and facilitate cross-chain exchanges. Due to its economic design and incentives, it has the ability **to export this Security and Solvency** to other, affiliated chains while sharing $CACAO tokens. Maya can remain a conservative space even though $CACAO can be used in other, more flexible or fast growing environments, which would create **new use cases** and demand for it while bringing back **more economic activity** to the Maya Economy.

ELI5

1. Maya is by design a very solvent, very secure and very censorship resistant network. It also has the tradeoff of not supporting some interesting capabilities like smart contracts, DeFi, derivative products, NFTs, etc.

2. Maya could export its security and solvency architecture to other side chains, by sharing the same nodes and the same native token - $CACAO. This can be accomplished with triple redundancy, by having an IBC bridge, a Yax Bridge - our Bifröst equivalent - and what we call a “Security Nodes” model. In exchange for securing alternative chains, Maya Protocol can earn fees or taxes in different ways.

3. Alternative chains could have a plethora of functionalities and economic activity that benefit $CACAO and the whole Maya ecosystem. As long as it is done within certain limits and parameters, there is little to no downside in having more chains.



Philosophical perspective

To help bring the decentralization revolution to the masses, a network of financial, contractual, entertainment and utility products must exist, but it is very difficult to compound many of these functionalities into only one chain since trade-offs between security and network clogging are faced constantly; this is why we believe in a multi-chain approach.

Some Application-Specific Blockchains (ASBC's) are powerful and useful, but then lack the security and solvency to operate securely. We believe that this is the case for most of the CosmosSDK-based chains except for THORChain.

Whereas most of the Cosmos-based chains rely on weakly-bonded, doxxed nodes with delegated funds, Thorchain requires nodes that bond huge amounts of their own capital, running an often over-bonded chain that remains completely anonymous.

Enter Security Nodes

By sharing Maya nodes' capacities with other projects and chains, we can export our security and solvency and allow for more specific applications - think trading, NFT's, stablecoins, metaverse, etc. - to integrate with us and generate additional demand for $CACAO in the process.

In other words, the nodes' set of any Application-Specific Blockchains (ASBC's) that would want to connect to our ecosystem would always belong to the set of Maya nodes too, which means that these side chains would be secured by nodes with huge stakes in $CACAO and that all of the involved participants would have aligned incentives to care for the stability and growth of the token. This would mean that to capture a Maya sidechain, you would have to capture Maya itself first, which is economically unfeasible for a rational actor.

New chains would need to bring utility and growth to the ecosystem of course, since running them and exporting $CACAO to them would have economic costs. In this regard, they can be thought of as economic ventures, which may or may not succeed.

There is a max limit of $CACAO token withdrawals for each one of these side chains that we call “Max Debt” and which can be modulated by the Maya nodes’ consensus. Should one of these chains be called risky / faulty / failed then the Max Debt variable could be reduced by our nodes slowly, to repatriate the previously exported $CACAO, until all $CACAO has been recalled.

During growth cycles, if $CACAO’s price rises too much, the Max Debt variable could be reduced as well, to repatriate the tokens in preparation for any potential ensuing contraction cycle. Conversely, after economic headwinds, Max Debt could be slowly increased to leverage the sidechain through lower prices, to boost its economic activity and to prepare for potential future growth.

Economic overview

Let's see an example of how one of these Application-Specific Blockchains (ASBC's) could connect into Maya and what the economic implications would look like. What we describe here also holds for other, consequent, chains, although an effort has to be made as to not have too many of them just doing the same things and being redundant.

For the sake of this exercise we will call Maya's chain "Chain A" and a new, arbitrary, cosmos-based utility chain, "Chain B".

Both Chain A and Chain B have their own treasury. This treasury is meant to accumulate $CACAO and other assets with time, holding them during economic expansion times and spending them during economic contraction times. They would also generally behave programmatically, according to various parameters set by and modifiable by each chain's set of nodes' consensus.

Chain A looks like so:

All of its native token - $CACAO - was minted and distributed at launch to early liquidity providers who brought external assets with them. Its liquidity is useful and productive, constantly being exchanged and generating yield for its bearers.

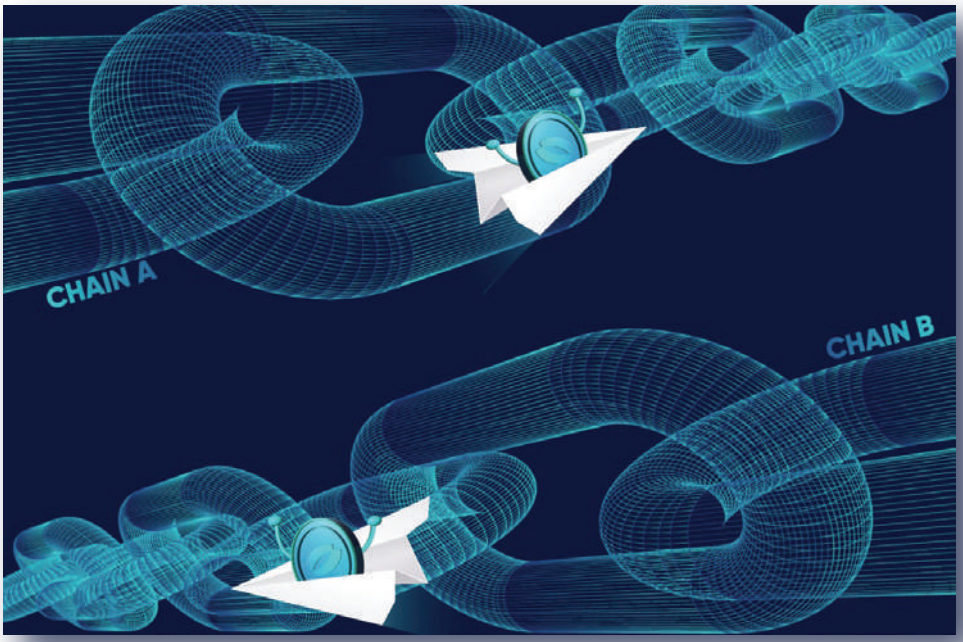
Liquidity Providers can seek higher yield if they upgrade into Liquidity Nodes by bonding their Liquidity Provider Units and if they are the highest bond holder during the next node churn round.

Liquidity Bond Wars emerge where participants try to acquire enough $CACAO to pair with other native external assets in order to beat their peers and become an active node. Nodes have big stakes in Maya, half of which are made up of $CACAO.

$CACAO liquidity is very sticky since the unbonding process takes time.

Chain B comes to the stage...

Chain B needs $CACAO to work and it needs to import it from Chain A since they cannot mint it themselves. The easiest to acquire it should be via the Liquidity Pools inside Chain A, "paying" for it with other native assets, such as BTC or ETH. This process increases Chain A's TVL, generates some nice swap fees (ie. protocol revenue) and decreases $CACAO supply inside Chain A. After their acquisition, the tokens can be routed through the IBC into Chain B, which was always programmed to recognize it as its native token.



Sharing nodes, limits on $CACAO withdrawals...

Nodes in Chain A can choose if they want to become nodes for Chain B or not, mainly based on their interest in the $CACAO fees being generated by the economic activity happening there (via Smart Contracts, NFTs or any other functionality attainable in the CosmosSDK framework). Becoming a node in Chain B would require them to post a second bond, denominated in $CACAO and, since we do not support delegation, this bond would be their own skin in the game.

We require that all nodes in Chain B already be active validators in Chain A; if you are kicked out of the node count in Chain A, you are also kicked out of Chain B's. Without this, Chain A could maliciously choose to cut off Chain B and remove all its liabilities from its balance sheet, harming the ecosystem of Chain B and whoever holds assets there.

It is important to have aligned interests between both chains because a massive return of $CACAO from Chain B to Chain A could have very negative, volatile or inflation-like effects, like the price decreases too much or it is swapped back to external native assets that then leave Chain A's balance sheet. In fact, we start perceiving any $CACAO outside of Chain A to be somewhat of a liability.

If we think of it as a liability then, why permit it? For the same reason any bank or business issues debt, to set itself up for growth. If used productively it can create synergy for the whole system too.

We also believe that we can design a system that handles these debts / productive liabilities and keeps a healthy balance sheet through economic expansions and contractions by balancing out how much $CACAO is allowed to be withdrawn, how the system's treasury takes profits during economic expansions (in the form of fees or taxes) and how it uses them during economic contractions.

These parameters would be taken care of via the "Degrees of Freedom" of the system, modifiable by nodes in Chain A and Chain B.

Degrees of Freedom:

1. Max Debt to Chain B.
2. Dynamic Inflation parameters on Chain A.
    a. Participation Rate for minimum inflation.
    b. Participation Rate for maximum inflation.
    c. Minimum Inflation.
    d. Maximum Inflation.
    e. Treasury Cut.
3. Percentage of fees from Liquidity Pools in Chain A that connect to Chain B assets through Yax Bridge.
4. Virtual Depth for slip fees when exchanging between $CACAO in Chain A and $CACAO in Chain B.
5. Percentage of transaction fees in Chain B.
6. Exclusivity on positive arbitrage between Chain B and Chain A when the limit reached and $CACAO in Chain B reaches a higher price than $CACAO in Chain B (we call this "Marginal Wealth tax").

Nodes must carefully balance out these parameters for the system treasury to extract value from the side chain economy in a reasonable manner. Too little value extraction would mean the Maya Economy would not be prepared for economic downturns, too much value extraction would suffocate the sidechain's economy.

Nodes can tweak these parameters on the fly to set things up for any developing economic situation and they do this with the typical 67% majority consensus model. Nodes hold around 80% to 90% of liquidity in Maya, half of which is in $CACAO, so it is in their best interest to do the best job possible at adjusting these values.

Example Degrees of Freedom

1. Max Debt = 10%

Means only 10,000,000 $CACAO can leave Chain A into Chain B.

2. Dynamic Inflation

a. Min = 0%
b. Max = 35%
c. Min Participation = 90%
d. Max Participation = 50%
e. Treasury Cut = 20%

Means there will be 0% of inflation at 90% participation rate, ie. when more than 90% of the Total Supply of $CACAO is in liquidity pools in Maya - provided by both, nodes and LP's.

Inflation would appear and increase linearly, up to 35%, at less than 50% participation rate.

20% of any newly minted $CACAO would go to Chain A's treasury, the rest into Pools.

3. Pool Tax = 10%

Means the Maya treasury would collect 10% of all yield generated by any $CACAO_Chain_A / $CACAO_Chain_B or $CACAO_Chain_A / $TOKEN_Chain_B pools.

4. Virtual Depth Tax = 1,000,000 CACAO on either side (could be asymmetrical)

Means the treasuries would collect slip fees whenever $CACAO is sent from Chain A into Chain B or vice versa, as if there was a liquidity pool with 1,000,000 $CACAO on either side. Since there are no LPs involved in this process, all the proceeds go to the correspondent treasury, ie. They go to Chain A's Treasury when $CACAO goes from Chain A to Chain B and to Chain B's treasury when $CACAO goes from Chain B to Chain A.

5. Sidechain Fee Tax = 10%

Means how much of the fees generated in Chain B will be redirected to its own treasury. These fees can include gas fees, transaction fees, swap fees and all others.

6. Marginal Wealth Tax = 1 (this parameter is on or off).

Whenever the Max Debt threshold is reached, arbitraging between Chain A and Chain B becomes impossible, which would lead to a fragmented market. Marginal Wealth Tax gives Chain A's treasury exclusivity over this arbitrage trade by allowing it to surpass the Max Debt Limit.

When the price of $CACAO inside Chain B normalizes these tokens are then exchanged for external assets inside Chain A and the treasury nets positive returns.

Chain B's treasury can use the newly input $CACAO to buy assets, such as Maya Synths and sends them back to the Chain A's treasury, which then proceeds to sell the Synths for Chain A $CACAO, closing the loop. Chain A's profits some external assets - which it no longer owes to any synth minters - and in $CACAO.

This can happen for as long as $CACAO's price is higher in Chain B than in Chain A.

If for any significant reason, consensuated nodes decide that it is necessary, they can also dramatically decrease the fees charged when sending $CACAO from Chain B to Chain A while leaving the opposite path untouched - this would repatriate $CACAO slowly over time - or even inflate Chain A's $CACAO supply to make Chain B's $CACAO represent a smaller percentage of total supply.

The mechanism requires the following simple set of rules:

1. Wallets in Chain B can always send $CACAO back to Chain A.
2. Wallets can only send $CACAO from Chain A into Chain B if the transaction does not contravene the Max Debt limit.
3. Whenever Marginal Wealth Tax is 1, Chain A's treasury can send $CACAO to Chain B above the Max Debt limit, whenever it is 0, no one can.

Some simulated scenarios
Let's analyze four possible market conditions:

1. Chain A grows relative to Chain B.
2. Chain B grows relative to Chain A.
3. Chain A contracts relative to Chain B.
4. Chain B contracts relative to Chain A.

Chain A grows relative to Chain B.

01

a. This can happen if the overall crypto market cap or TVL increases, for example, or if demand for cross-chain swaps surges suddenly.
b. $CACAO would repatriate organically to Chain A given that its price would be higher there. These repatriated tokens could be either used as a trading pair or to extract external assets and, because in this regard repatriated $CACAO would be slowing Chain A's growth down, the lesser of these tokens that come back, the better for both chains.
c. $CACAO in Chain B becomes more scarce gradually which in turn protects Chain B's economy and the security budget held by its Nodes. The dual chain system allocates capital naturally and assures both chains grow as much as they are warranted to grow.
d. Chain A should seek to reduce Chain B taxing proportionally.

Chain B grows relative to Chain A.

02

a. This can happen if Chain B's economy booms, isolated to the rest of the market or to the demand for cross-chain swaps.
b. $CACAO would expatriate from Chain A into Chain B given that the price there would be higher. Expatriated $CACAO would catalyze growth inside Chain B while diminished supply in Chain A would increase its security budget.
c. Chain B would attract Chain A derivatives (Synths), all of the expatriated $CACAO would have been acquired via swaps from external assets inside Chain A.
d. Both treasuries would be collecting taxes actively out of Chain B's growth. $CACAO supply increases in Chain B until reaching Max Debt, after which Marginal Wealth Taxation is triggered.

Chain A shrinks relative to Chain B.

03

a. This can happen if the overall crypto market cap plunges or if the demand for cross-chain swap falls while Chain B's activities thrive.
b. Chain B's $CACAO inflow quickly reaches Max Debt while Chain A's supply is reduced.
c. Chain A's treasury can start arbing $CACAO with exclusivity into Chain B which would pocket it some profits. This would keep reducing $CACAO's supply in Chain A which would create incentives for new external capital inflows.
d. More fee volume in Chain B would ensure that more nodes try and compete to make it into this chain's node roster but, since being a node in Chain B requires a node in Chain A, both chains' node liquidity and healthy competition are enhanced.
e. All of the most representative assets of Chain B would be available to trade inside Chain A's liquidity pools which would bring external capital and swap volume to Chain A.
f. Both Chain A's and Chain B's treasuries could use any of their capital resources to stimulate Chain A; they could buy synthetic assets, add LP positions, donate $CACAO into any pools they find convenient or execute any other strategies that the nodes may adopt by supermajority vote.
g. Chain A would be strengthened and better prepared to weather any potential economic downturn while the markets recover, sufficient demand comes back or the Maya team adjusts or delivers any required code or strategy upgrades.

Chain B shrinks relative to Chain A.

04

a. This can happen if Chain B's economics dwindle or if the utility or demand for its services wane off, while Chain A's thrive.
b. Chain B $CACAO would repatriate into Chain A organically, making some slip fees for the latter's treasury.
c. $CACAO supply in Chain A would increase, overall price and purchasing power would decrease. This could prompt participants to swap back into external assets and exit the Maya ecosystem.
d. Depending on the total fees collected and economic activity generated by Chain B, the chain could have still done more good than harm.
e. At some point - and if Chain B's economics still make sense - $CACAO would stop leaking out because there would be so little of it that its purchasing power would increase considerably.
f. Both Chain A's and Chain B's treasuries could use any of their capital resources to stimulate Chain B and provide any assistance it could use until its markets recover, demand for its services come back or the developing team adjusts or delivers any required code or strategy upgrades.

All in all, we believe that this model of interconnected chains provides a lot of potential upside for the ecosystem with little to negligible downside, as proved by the described four scenarios before, and as long as it's done securely and within certain limits; code for these interconnections would be carefully audited before activating in all cases.

Third-Party Chains

At Maya we are thrilled with our current roadmap, which already includes a few of these chains planned for development and launch ;-) , and yet, any external team can decide to build a chain that is secured by the Maya Protocol architecture.

We recommend that they create a $MAYA-like token and a Maya fund-like vehicle that benefit their teams via a protocol fee revenue model since no new $CACAO will be minted with any new chain additions.

Launching along this lines, by the way, has several benefits for any developer team, compared to launching a sovereign chain, including:

1. Bootstrapped liquidity! This is certainly vital and tremendously attractive.
2. Full compatibility and access to the Maya Protocol's economy. Derivative assets can be included within the Maya pools.
3. Sharing of $CACAO, a token with significant value and an established purchasing power.
4. Solid security, provided by a capable network of highly-invested, censorship-resistant nodes, from block #0.
5. Synergic professional relation with the Maya Protocol team:
  a. Friendly access to our network and community.
  b. Support from within our experienced technical team.
  c. We will support or pay for the necessary code audits that functional projects, successfully tested in our Maya Stagenet, might require.

External developers can focus on building with this platform instead of starting a chain from scratch, which requires many different skills beyond coding.

Long Tail Chains & Assets

If at any time the Yax Bridge connecting other chains into Maya is saturated with too many requests, we could launch a secondary Maya chain (a fork) and connect it using the Security Nodes model to support the long tail assets and chains, simultaneously increasing supported chain capacity, assets, $CACAO demand, network value and transactions per second.

Said fork would aggregate inbound transactions from “Maya 2” to “Maya 1” through the IBC to facilitate exits of outbound short tail assets. Likewise, inbound transactions from “Maya 1” could aggregate to “Maya 2”.

On Sovereignty and Independence.

A situation where Chain B becomes much more successful than Chain A can happen too... In this case, Maya could become a burden rather than a safety net and the community could try and vote to separate into an independent project.

This scenario would have the following consequences:

1. The IBC would be taken down. $CACAO can no longer be sent interchangeably.
2. Chain B’s $CACAO would be renamed to $BCACAO, or whatever other, different name.
3. Chain B’s assets would remain inside Maya Pools if they were there already. A new pool $CACAO / $BCACAO can be added if enough liquidity is behind it.
4. The requirement that a Chain B Node must be an Active Validator Node in Maya is deprecated. Chain B Nodes at that moment remain Nodes in Chain B.
5. Both chains could jointly decide to have a new IBC, where $CACAO sent from Maya to Chain B is no longer native there. Other Maya derivatives can also be sent through IBC to sovereign Chain B. Maya will not accept $BCACAO within Maya Chain.

Maya would end up erasing all the $CACAO liabilities from its balance sheet - since $BCACAO would no longer be directly redeemable for external assets that could then leave Maya - and would keep all the revenue raised from taxing Chain B throughout its history.

While possible, this scenario is highly unlikely because it works against network effects and network value, which are very important for blockchain ecosystems.

On Death and Taxes.

The opposite scenario could also occur, where Chain A’s nodes become disinterested in protecting Chain B, if they don’t find the right economic incentives; users could also simply not use Chain B or they would migrate to another better chain. Nodes could trigger a Chain Retirement in any of these cases.

An advance notice would be communicated for $CACAO to be recalled into Maya over a determined time period (ex. 10 days) and Chain B would be shut down by the nodes thereafter.

Finally, all revenues raised by taxes during this process would be kept by the Maya’s Treasury, which would end in no way worse off than it was before Chain B was introduced.

Technical overview

User Stories:

Node Whitelist

- As a Maya node operator, I should be able to register a Chain B validator address and set its public key as an attribute of my Maya node.
- As a node operator, I require that nodes of Chain B can only become validators if they have an active validator in Maya.
- As a node operator, I require that nodes of Chain B that have been churned out of Maya are also churned out from Chain B.
- As a node operator, I require that the Validator Node Set in Chain B be only 80% the size of the Maya Node Set, essentially a subset of Maya Nodes.
- As a node operator, I require that nodes compete on pure $CACAO bonds in Chain B to be part of the Chain B Node Set.

IBC

- As a user of Chain B, I want to be able to change tokens from one chain to another securely, so that I can use $CACAO as a native token in each of them.
- As a user of Chain B, I want to pay fees in $CACAO and have Chain B governance dependent on $CACAO.

Treasuries

- As a Maya node, I want a treasury to exist in Maya that can be made to do automatic coded actions as well as allocate capital by supermajority node vote at will.
- As a Chain B node, I want a treasury to exist in Chain B that can be made to do automatic coded actions as well as allocate capital by supermajority node vote at will.

Taxation

- As a Maya node, I want the treasury to collect fees from expatriation and repatriation of $CACAO.
- As a Maya node, I want to be able to tweak Max Debt as well as taxation constants for Chain B through validator node supermajority vote.

CODE:

Maya
https://gitlab.com/mayachain/thornode/-/issues/40
https://gitlab.com/mayachain/thornode/-/issues/41

Aztec
https://gitlab.com/mayachain/terra/-/issues/2
https://gitlab.com/mayachain/terra/-/issues/3
https://gitlab.com/mayachain/terra/-/issues/4

Aztec

Part 5. Aztec Chain & $AZTEC token

A new ecosystem for $CACAO

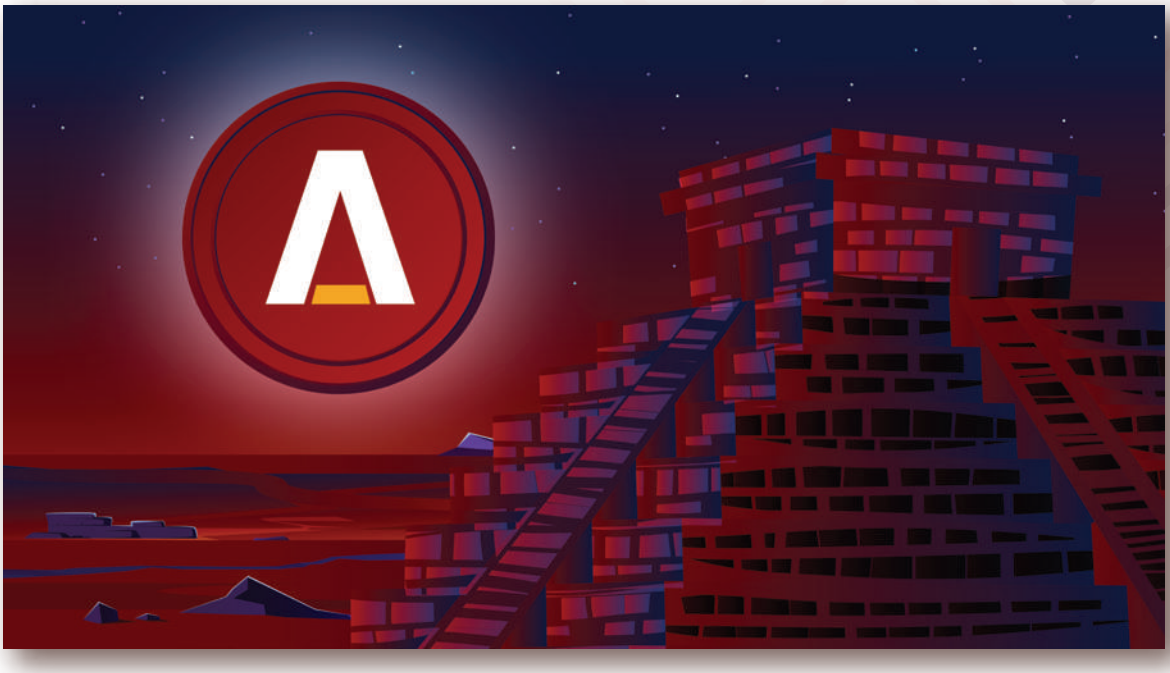
Aztec is a **powerful demonstration** of the high potential of the Maya Protocol's design and how it can **expand** horizontally to offer different complementary products. We are excited about the **endless possibilities** of combining Maya's liquidity blackhole properties with Aztec's Smart Contracts and economic capabilities!

ELI5

1. Smart Contracts are necessary to add complexity and dynamism to flourishing crypto economies because they provide builders and developers with flexibility to create and experiment. Smart Contracts will provide an avenue for Maya derivatives —i.e. Synths— to find use cases beyond arbitrage.

2. Aztec is a fork of the Terra blockchain. We decided to do this based on several factors like its compatibility with CosmWasm, its mature infrastructure, its extensive Smart Contract development, and its vibrant community, despite recent events. On the latter, we are happy to announce that $LUNA and $UST token holders pre-depeg will be allocated $AZTEC tokens!

3. Aztec **will** take a role in the algorithmic stablecoin quest, but it will not have a "one mechanism for all" approach, instead it will work with a full suite of different tokens that coexist, complement each other and offer different types of risks. Our algorithmic stablecoins will be turned off at launch, giving us time to finish with the economic design and to run the appropriate bounties' programs, etc. Maya and Aztec will **never subsidize yield** to inflate demand of any of its own stablecoins or derivatives.



Philosophical perspective

Aztec's mission is to complement and underpin the DeFi space. With this project, we express our strong belief in permissionless money and in truly open and transparent monetary platforms, controlled exclusively by open-sourced coded rules and policies.

Although we could try to achieve this with Linklikes, Osmolikes or Etherlikes side chains, we believe a Terralike chain is an excellent first step, especially given the high complementarity —and stark difference— with Maya, our existing Thorlike chain.

The Aztec protocol also comes in at a big and important moment for our industry, after the Terra / LUNA collapse. Yes, we will be seeking to contribute to the decentralized stablecoins experimentation and to continue the iteration progress, without losing any sight of the successes and mistakes of past protocols. Please refer to **Roadmap: Maya 3.0** section for more details on our upcoming stablecoins.

Finally, the more usefulness that we can give to our token, $CACAO, the stronger the Maya ecosystem becomes. We believe the Aztec Chain serves this purpose adequately.

Economic overview

The Aztec Chain means that $CACAO will be used for new and different things than it could have had if only Maya existed. As Chapter 4 explains, the usage of our tokens in a side chain is beneficial for the overall Maya Economy. Remember: because there are no new mintings, all $CACAO that comes into Aztec needs to be imported from Maya, paying slip fees to Maya's Treasury in the process.

Aztec soundly complements our economic model, attracting creators via excellent UX/UI compatibility and programmability; lending, Smart Contracts, NFTs, and a whole plethora of options become available for interaction with $CACAO and Maya derivatives.

If Maya works like a central bank + foreign trade, Aztec works like the vibrant merchant economy that develops in nearby territory, enriched with security and stability from Maya.

$AZTEC

Similar to $MAYA, $AZTEC tokens grant their holders the right to a proportional fraction of the "Aztec Fund", which captures 10% of all the fees generated by all swaps and transactions in the network.

$AZTEC tokens can thus be treated as some sort of stock or economic participation in the project and will most probably reflect the market's perceived value of the present and future growth of the network.

They will be initially held by participants of all levels inside our team, including our private investors, developers, advisors, and founders. There is also some $AZTEC set aside for our early Node Operators and Terra adopters.

Builders

As a smart contract friendly environment, anyone can jump in and participate, building the protocol's reach further. Whereas Maya is a very secure and conservative environment, Aztec is meant to be more progressive. Any builder is welcome to contribute, build and reach out; we will provide all the support they need to operate successfully.

Technical overview

Who will own the $AZTEC tokens?

First of all, $LUNA and $UST owners!

Although we really did not expect the Terra / LUNA situation to unfold as it did in May 2022, we had long planned on awarding $AZTEC tokens to $LUNA holders, in the same fashion we are doing with $RUNE holders.

The Terra community's situation is continuously evolving but our ethos has always been to collaborate and be a positive force in the DeFi community, that is why we have designed the following "registration" mechanism to redeem $AZTEC:

1. Create an Aztec Wallet.
2. Wait for us to provide a wallet address in the Terra Classic blockchain.
3. Send any transaction that includes your Aztec Wallet address in the memo to the provided Terra Classic address.

This process is only necessary for Aztec to relate your Maya Wallet with your Terra Wallet and thus the transaction amount can be as small as possible, the registration period will be open for a period of 60 days.

After we have this information, we will snapshot the registered addresses' $LUNA and $UST positions on Terra Pre-Depeg and distribute 10% of our $AZTEC tokens among them, proportional to their holdings on said date.

We are sorry about the Terra / LUNA outcome and hope that this airdrop helps ease the pain a bit for some people.

Second, Early Nodes!

An additional 10% of the $AZTEC total supply will be used to reward our early node operators like so:

1. 3.33% of all the $AZTEC tokens will be shared to the active Validator Nodes securing our network one month after the launch of Aztec Chain.
2. An additional 3.33% of all the $AZTEC tokens will be shared to the active Validator Nodes securing the network four months after the launch of Aztec Chain.
3. An additional 3.33% of all the $AZTEC tokens will be shared to the active Validator Nodes securing the network twelve months after the launch of Aztec Chain.

This token incentive rewards our early supporters and potentially catalyzes our first bond wars since only the nodes with the biggest $CACAO bonds in Aztec wil become validators.

Dev Fund

Finally, the remaining 80% of the $AZTEC tokens will be initially awarded to the Maya team, which includes our software developers, advisors, investors, and other strategic individuals and institutions that have readily supported us.

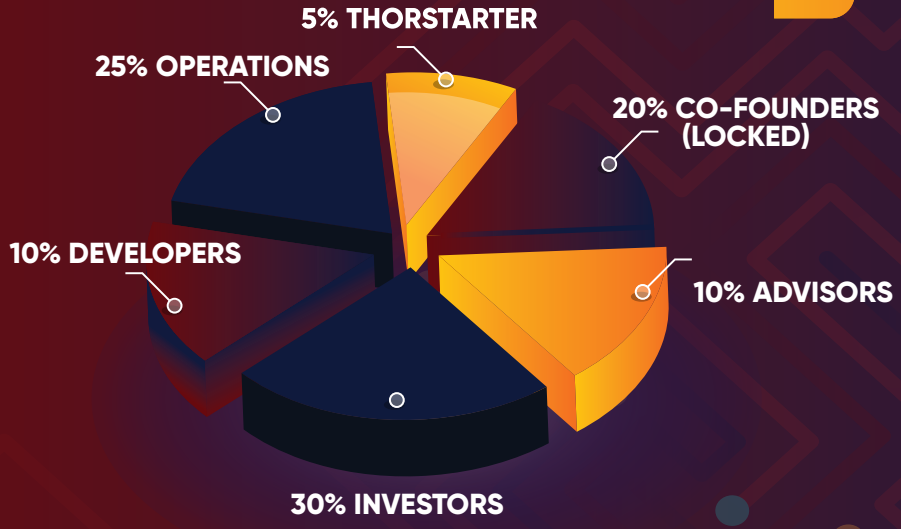
90%
LPs & Nodes

10%
Aztec Fund

AZTEC FUND

- 10% $LUNA AND $UST OWNERS
- 10% EARLY NODES
- 80% DEV FUND

DEV FUND



User Stories:

1. Remove Delegation Logic

- As an Aztec validator, I want to stake without delegation, so that I have a large enough stake to incentivize good behavior. I can only be a Validator in Aztec if I already am a validator in Maya.

2. Aztec Fund

- As an $AZTEC holder, I want the Aztec Fund to be funded with 10% of the gas and transaction fees that are generated in the chain to distribute those funds among the Aztecs users that own $AZTEC, denominated in $CACAO.
- As an $AZTEC holder, I want to receive funds from the Aztec Fund proportional to the amount of $AZTEC tokens I own, distributed every 24 hours.

3. Turn off mint/burn mechanism

- As an Aztec user, I want to use a safe protocol. Until many things are validated about the economic design, I want all stablecoin mechanisms turned off.

Code

Remove Delegation
https://gitlab.com/mayachain/terra/-/issues/2

Aztec Fund
https://gitlab.com/mayachain/terra/-/issues/1

Roadmap. Maya 3.0

Not all Stablecoins are created equal.

The search for a decentralized stablecoin has been a tough one and unfortunately, many attempts have failed to this date. In Maya, we believe that there is no such thing as an optimal universal model for stablecoins, one that rules them all... we believe that diversification of risks is key for stability and we are building with this idea in mind.

We have named this Roadmap: Maya 3.0 since everything in this Whitepaper after this section **will not** be available at launch, since it requires further work, design, code, economic audits, among other things. In other words, everything before Maya 3.0 will be available at launch, after the Liquidity Auction takes place. Turning Maya 3.0 on or leaving it off forever will be decided by community discourse and Nodes when the time comes, if the proposed design makes sense and has gone through the necessary audit and community review processes.

ELI5

1. Decentralized stablecoins have been called one of the “Holy Grails” of crypto and our industry has experimented with different approaches and models to work them out. Today, Algorithmic Stablecoins are still risky and Overcollateralized Stablecoins are still tough to scale and capital-inefficient.

2.By looking at previous experiments, we believe that stablecoin models have always assumed they would succeed. Instead, we believe in iterative design and have approached the issue with a “fail-safe” attitude, where the risks of depeg always exist and need to be balanced and offset in more than one way.

3. Maya will have 5 different stablecoins in its suite. Each one will be best suited for a specific type of user / investor since all of them have their own strengths and weaknesses, which will be clearly laid out at all times, to everybody.

Philosophical perspective

We believe in iterative learning and we have been following the Terra / LUNA ecosystem —and subsequent implosion— for months now. In pursuing an algorithmic stablecoin system that considers depegs, death-spirals, and bank runs as highly probable scenarios, we designed an innovative assortment of stablecoins plus a Treasury Bond mechanism.

These are the tenets that we looked for and applied to our design philosophy:

1. Decentralized Stablecoins are good for DeFi and necessary to the future of Crypto.
2. Decentralized Stablecoins' design hasn't reached maturity yet, we are still in the iteration phase.
3. These constant iterations mean that failure is always a possibility, but it should not grow into a big, uncontrollable systemic risk.
4. Single Points of Failure must be avoided.
5. Inflating our native token beyond its total supply should not be an option since it is the core of our economy and security budgets.
6. Demand for our stablecoins should be real, solid and deep rooted; instead of artificial and mercenary
7. Fairness should drive decision making

The Maya Economy will have 5 stablecoins in its suite, each one with a different economic design plus different strengths and weaknesses; they will all help share the market's needs and alleviate external pressures on the supply and demand. Failure of one design should not trickle into the others and systemic shocks should have orderly and reasonable responses.

	$USm	$USa	$USs	$USb	$USc
Name	Maya USD	Aztec USD	Synth USD	Bond USD	Colaterallized USD
Nickname	Milk Dollar	Almond Dollar	Sugar Dollar	Butter Dollar	Chocolate Dollar
What is it?	Algorithmic Stablecoin, minted through MayaFi	Algorithmic Stablecoin, based on an improved Terra-like design	Over-collateralized stablecoin, backed by Synths	Long term, low-interest stable debt	First completely decentralized, fully collateralized stablecoin, backed by a basket of all the previously mentioned stablecoins
Origin Chain	Maya Chain	Aztec Chain	Aztec Chain	Aztec Chain	Aztec Chain

Economic overview

As mentioned before, we believe in a multi-product design for our stablecoin solution, one that distributes the load and risk among different mechanisms to reduce systemic risk and increase antifragility. Above all, $CACAO supply and price must at all times be protected, let's look at the economics of each one of them:

We actually came about with one of our stablecoin's design by accident, while tweaking models and trying to answer some important questions... Can we design a fail safe system in the event any of our stablecoins fail? If one of our stablecoins is algorithmic, can we avoid $CACAO hyperinflation? As it's often the case, we looked for inspiration in TradFi, specifically in Government Treasury Bonds.

Treasury Bonds are a way for governments to fund themselves, they are used to raise capital for government expenditure, especially during tough times, and to relieve the pressure on taxes and inflation, as well as stimulate economic growth. In playing around with this idea, we were interested in a way to create a Treasury Bond mechanism for Maya and Aztec.

People would be able to convert a depegged stablecoin into a BOND object, which would represent the value owed to the owner (the full USD $1.00, not the depegged value) and allow him or her to be paid over time by System Income of both chains, accruing interest on unpaid principal.

In TradFi, bonds approximate the price of their "face value" or "par value" as they mature but can trade at a premium or at a discounted price around that price, depending on several things like their interest rate or the present value of their future cash flows. If designed correctly, BOND's can themselves be approximately worth what the original debt is worth... so our fail safe pressure relief valve is incidentally our new stablecoin: $USb.

Bond USD

Ticker: $USb
Nickname: Butter Dollar

$USb is designed to protect a stablecoin holder's value. Because it's supposed to accrue its full value over time, it will not be precisely valued at $1.00 USD all the time, but will instead derive its value from the market conditions and Maya's perceived creditworthiness.

A holder of one $USb owns a virtual $1 dollar iou at present value, guaranteed by the system's future income. As long as the Maya Economy and network value are active, that note is getting paid down. All of our other stablecoins can be converted into $USb, irreversibly, if their owner decides to do so.

The BOND Mechanism

$USb tokens record a stablecoin debt to their holder, paid out in $CACAO via an interest rate every x number of blocks. This interest rate is partially set by Nodes and can be modified by supermajority vote (we will cover why it is only partially set later).

Let's see how each part of the mechanism would work in a simulated scenario:

Suppose a 3.717% APY, payable every 14,400 blocks (roughly every day). $USb holders would be then getting a daily 0.01%, coming from the System Income, in $CACAO.

01

Minting.

Anybody, at any moment can mint $USb by burning one of our other stablecoins, the reverse process is never allowed.
The process is not liquidity sensitive and would not incur any slip fees.
Slightly different conversion rates can be used depending on the burnt stablecoin. Ex. Our overcollateralized stablecoins could be allowed to mint 1.0 $USb while our algorithmic stablecoins would be allowed to mint only 0.99 $USb.

02

Staking.

$USb must be staked to receive interest payments, we need to do this so that we can burn some of them later.
Unstaked $USb can be transacted as any other token would.
The tokens can be sent through the IBC to other Cosmos-based chains although they would stop accruing interest.

03

Funding.

Whenever there is staked $USb in the Bond Reserve Pool, a consensual percentage of the System Income —Maya's, Aztec's or both— is routed to the Bond Reserve, in $CACAO.

04

Proportions.

Every 14,440 blocks a snapshot of the staked and unstaked $USb is taken.

05

Payout.

The entirety of the $CACAO in the Bond Reserve is paid out directly to the addresses that staked their $USb, proportional to their percentage of the total stake.
This is liquid $CACAO that can be traded for any asset or otherwise used elsewhere, inside the Maya Economy.

06

Burning.

Paid for $USb is then burnt and removed from the Staking Pool.
$CACAO's price, denominated in USD, is fed from an oracle.

07

Paydown.

Staked $USb maintains the original proportions but the Staking Pool depth has decreased.
We use these percentages to keep accounting records for the next 14,399 blocks until the next paydown is due.

08

Interest.

Aztec Chain augments 0.01% of the total unstaked $USb circulating supply and distributes it to all unstaked $USb holders, proportionally to their positions, essentially acknowledging the interest owed on outstanding principal.

09

Repeat.

After 14,400 blocks - or approximately one day - the process starts again.

Exactly how should $USb be valued?

1. Market forces will dictate the market price of $USb, according to classic supply and demand (with some demand elasticity, as will be covered later). $USb's primary market will be a $USb / $CACAO pool available in Maya. Other secondary markets are bound to exist.
2. Staked $USb should be valued like a debt instrument to an investor, with a variable interest rate and maturity.
3. Unstaked $USb could be valued by any long-term holder and believer of Maya Protocol as a perpetual bond, which accumulates pending payments until it is staked.
4. Unstaked $USb could also be valued, by traders, as a Coupon Bond whose face value depends on how long it remains unpaid.

In TradFi, Perpetual Bonds, Coupon Bonds, and Fixed Payment Loans are valued using the following means:

Market price (Liquidity providers)

$$M_o = \frac{\text{Stable Supply}}{\text{CACAO Supply}} \times \frac{\text{CACAO Supply}}{\text{Bond Supply}}$$

Fixed Payment Loan (Lenders)

$$L_o = \sum_{i=o}^{n} \frac{PMTi}{(1 + dr)^n}$$

$$\text{Where } n = \frac{\text{Log}\left(\frac{PMT_o}{PMT_o - P_oC}\right)}{\text{Log}\,(1 + C)}$$

$$PMT = P \times \frac{c\,(1 + c)^n}{(1 + c)^n - 1}$$

Perpetual Bond (Holders)

$$P_o = \frac{C}{dr}$$

c = Coupon payment
dr = Discount rate

Coupon Bond (traders)

$$B_o = C\left[\frac{1 - \frac{1}{(1+dr)^n}}{dr}\right] + \frac{\text{Face Value}}{(1+dr)^n}$$

Face Value = Max [M, L]

Discount Rate (dr): It is the rate at which money is losing value over time due to inflation or costs of capital, an essential element to calculate the Net Present Value (NPV) of money.
Although different investors can use the above equations to set their own discount rates and the actual loss of value for money over shorter periods of time is difficult to obtain, we believe that two useful baselines are: the Risk-Free Rate, which usually means the U.S.' 3-month Treasury Bill rate of return, and the 12-month Secured Overnight Financing Rate (SOFR), which is updated every day by diverse global economic data providers.

Uncertainty Risk (U): There are inherent risks to any investment, including bonds. Debt issued by big sovereign countries, usually considered the safest investments in TradFi, are still somewhat risky since governments can be overthrown, they can lose wars, have a popular leader decide not to pay their lenders, and more. These risks, and any other black-swan events, become more probable with longer time horizons.
Maya's equivalent risks include hacks and code vulnerabilities, a decreased demand for our product —cross-chain swaps— for any reason like only one blockchain ends up dominating all the market, an overall implosion of the crypto industry, and more.
Although we consider that the risk of our nodes not honoring their payments is close to zero —since they know that also means killing the network's reputation— as long as the market considers any risks to be existent then the Uncertainty Risk should be non-zero.

Coupon Rate (C) & Interest Rate: Maya and Aztec should seek to pay an attractive Interest Rate, one that is above the Discount Rate, but one that is not too high to become a burden.
In the case of $USb, the Coupon Rate is the same number as the Interest Rate and we can use them interchangeably, for the sake of clarity or simplicity.

How Nodes set (C): Due to its daily updates, Maya would begin using the 12-month forward SOFR as the Discount Rate, which is obtained using a Node run oracle feed; the community can also propose a better reference rate. After nodes set the Uncertainty Risk (U) constant (ex. to 1%) the Coupon Rate would be set to U + Dr.
This is what was meant before with "nodes only partially set" the interest rate. If the market, during rational times, is starting to sell $USb for less than $0.99, our nodes can vote to increase U; if the market is selling $USb for more than $1.01, our nodes can vote to decrease U.
U cannot be negative and should not be higher than 2%, as it is not meant to be a speculative investment or attract mercenary capital. If U is already 2% and the market still sells $USb below $0.99 that means that either the market is behaving irrationally or that Maya is not deemed creditworthy anymore.
In such an event, Maya cannot make the market rational or increase its creditworthiness by increasing its debt obligations. Therefore, if Nodes already pulled all their available levers and $USb is off the peg, Nodes should allow $USb to continue trading downwards until the market corrects itself or Maya is deemed creditworthy again. In spite of the bond not trading on par, the bond owner is in fact receiving their pay downs to maintain an above $1.00 present value to the holder.
One of our nodes' tools to improve our Uncertainty Risks would be to continue paying down debt, reducing the Time dimension to uncertainty and bringing $USb closer to its original peg.
Let's now analyze each value method carefully.

M_o: The Market Price. which we can't directly influence.
Anything too far from $1.00 would mean that the real world discount rate is different than what Nodes are reporting, that uncertainty risk is greater than projected, that the markets are acting irrationally (typically fear), and that total $USb supply is very high or any combination of the above.
Nodes can indirectly influence Mo by manipulating the Coupon Rate (through changing U), as well as paying down debt more quickly, reducing time risk, default risk, and market uncertainty simultaneously.

P_o: The Perpetual Price. The value of the bond to a long-term and risk-averse investor that plans to hold it to virtual perpetuity.
This value would be always equal to $1.00 if the Coupon Rate was equal to the Discount Rate. The Coupon Rate will most often be higher than the Discount Rate, to account for the Uncertainty Risks that the market might perceive. Investors holding the bond in perpetuity thus hold more than $1.00, in present value.

L_o: The Loan Price. the present value of the bond when it is staked by an investor who seeks to get recurring paydowns on both principal and interest.
The real Loan Price is greater than $1.00 if the Coupon Rate > the Discount Rate. The faster the principal is paid, the more the Loan Price asymptotes to $1.00; the slower the principal is paid, the higher the Loan Price leans away from $1.00 (if the Coupon Rate > the Discount Rate it goes higher, if the Coupon Rate < the Discount Rate it goes lower).
Given C = Dr + U, and U >= 0, the fair Loan Price will go below $1.00 only if the data used to measure the Discount Rate is wrong. If the community is constantly valuing Loan Price below $1.00, it is a strong indicator that nodes should change how Dr is measured.

B_o: The Coupon Bond Price. the present value of the bond is most likely used by Bond Traders, who are constantly seeking to maximize value and have a shorter time horizon.
Traders don't ever get paid the bonds' Face Value by the treasury, rather, they will either resell, hold or stake them to benefit the most from them.
Traders set an expected value of L or M, which we can call Le and Me, at some point in the future, whenever they intend to realize their profit - or loss.
Whenever Lo is high, or Mo is low, traders will prefer to earn by staking the bonds.
Whenever Mo is high, or Lo is low, traders will look to unstake and sell them.
N is simply the number of days between the present and the chosen point in the future. Whenever these bond traders are expecting changes to Le or Me, they will hold unstaked positions for N days to realize their value.
Bo is by far the most subjective way to value the bond and will depend mainly on each trader's investment thesis and future outlook.

R_o: The return. we speak of Ro whenever we are talking about Lo, Bo and Po interchangeably- notice that Mo is left out. It is the all-encompassing term to call the present value of the Return on the bond in general.

Stability Requirement

if dr = inflation then

$$C = dr + u \quad \therefore \quad P_o \geq B_o \geq L_o \geq M_o \leq \frac{1USD}{\$USb}$$

dr = Discount rate
U = Time & risk

if U is 0, then $P_o = B_o = L_o$

Having gone through the above, we should notice there are 3 maxims that will always hold true for $USb:

1. If C > dr, the present value of Ro will always be worth more than $1.00 USD.

2. Price of Mo≤Minimum[Price of each Stablecoin], or more interestingly, the Minimum[Price of each stablecoin] ≥ Price of Mo, for 2 reasons:

a. If Mo goes above this value, demand for the bonds in the market dries up since it would be cheaper to mint $USb from another stablecoin which would make $USb demand decrease.
b. If a stablecoin drops starkly below its peg, such that the Mo price is greater than its price, arbitrageurs can acquire that stablecoin in the market, burn-in exchange for $USb, and sell them for $CACAO (or another asset in the market), which would make $USb supply increase.

3. Bond demand is very elastic to Mo. Bond demand is very elastic in relation to Mo. As the price of Mo decreases, and given that the present value of Lo, Bo and Po are unchanged by market movements, the ROI an investor gets from buying Mo increases countercyclically.
Essentially, the investor's ROI = Ro / Mo, and the further that Mo depegs from $1.00 the better the ROI that a $USb investor would get. For example, if Mo is $0.50 then the investor's ROI becomes 2x what the Ro was designed to be. We can generalize this behavior as Demand Elasticity for $USb in the market being greater than 1.

$$\varepsilon = \frac{\%\Delta Q}{\%\Delta P} = -\frac{\Delta Q/Q}{\Delta P/P} = -\frac{\Delta Q}{\Delta P}\frac{Q}{P}$$

Q = quantity of the demanded good
P = price of the demanded good

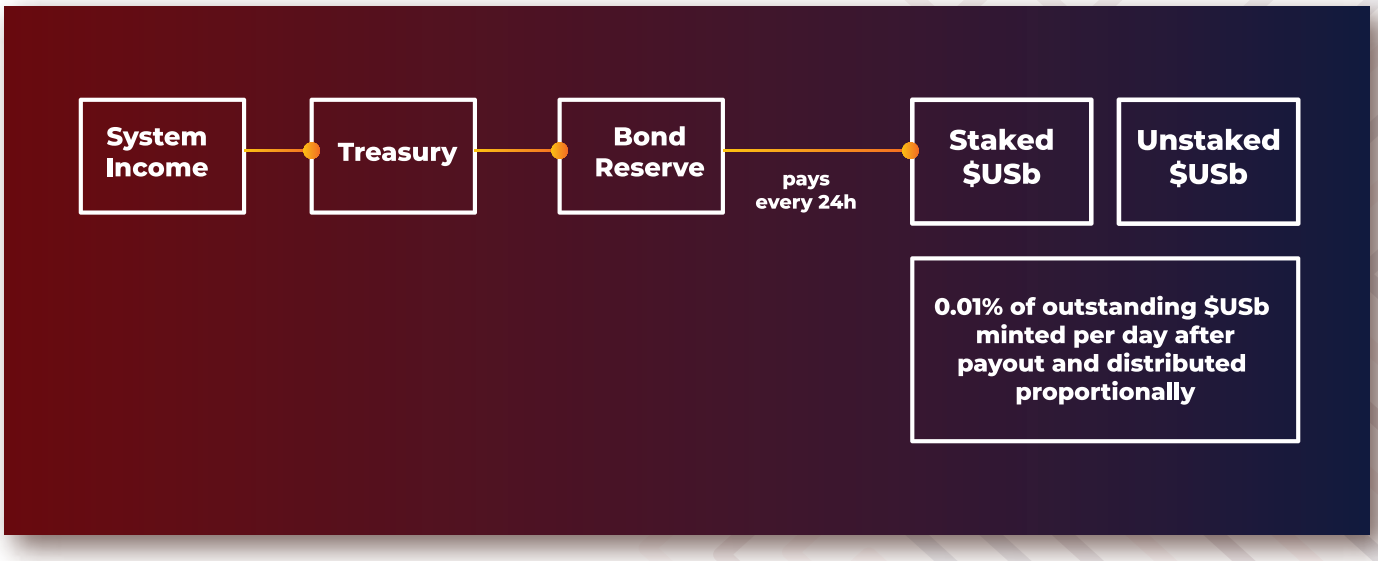
$USb as the peg sink.

$USb serves as an excellent tool of last resort in the case that anyone other of our stablecoin depegs from $1.00 because, with every lost cent, it becomes more and more desirable for rational actors to buy up the troubled stablecoin, burn it in exchange for $USb and then hold, stake, or sell their new tokens, which of course increases the strained stablecoins' demand and decreases their supply. Importantly, $USb achieves all this without ever-inflating $CACAO's supply and without using any funds in the Treasury.

In the case of asset-backed stablecoins (see our delicious assortment here), whenever they are burnt in exchange for $USb, they are leaving valuable assets behind in our networks... As long as those assets are more productive —or appreciate more— than the interest paid to the new $USb holders, then the network will generate profits. This means the Maya and Aztec chains are fundamentally long crypto and the multichain future!

There would likely be a lag between the re-pegging of the affected stablecoin and the re-pegging of Mo, which would be acceptable since keeping peg is not Maya and Aztec's top priority, rather, they are interested in paying back debt to all $USb stakers.

Also, notice how the Treasury never tries to maintain the affected stablecoin's peg artificially, it will only make sure Ro is above $1.00 and confidence in $USb is high. Instead of trying to pay off any panic sellers, the treasury only spends a small fraction of its reserves by paying $CACAO to all $USb stakers, at a reasonable pace and rate.



$USb makes the Maya Economy Antifragile, merely by existing it makes depegging events less likely because it provides a safety net that ultimately makes stablecoin holders less prone to panic selling.

Finally, we should note how the structure becomes safer the higher the system income gets and how the founding team —including investors and developers— are compensated only with this metric: we are incentivized to maximize system income instead of inflating any of our tokens' price. We know the first option makes $USb better, safer, and more attractive, whereas a baselessly inflated token price does exactly the opposite.

So now that we have an antifragile system with an excellent peg sink, a correctly incentivized team, and a safety net that prevents any systemic failures, let's see the rest of our stablecoins offering.

The stablecoins that will power the Maya Economy

Table 1

	$USm	$USa	$USb	$USs	$USc
Name	Maya USD	Aztec USD	Bond USD	Synth USD	Colaterallized USD
Nickname	Milk Dollar	Almond Dollar	Butter Dollar	Sugar Dollar	Chocolate Dollar
What is it?	Algorithmic Stablecoin, minted through MayaFi	Algorithmic Stablecoin, based on an improved Terra-like design	Long term, low-interest stable debt	Over-collateralized stablecoin, backed by Synths	First completely decentralized, fully collateralized stablecoin, backed by a basket of all the previously mentioned stablecoins
Origin Chain	Maya Chain	Aztec Chain	Aztec Chain	Aztec Chain	Aztec Chain
Best compared with	$TOR	$UST	TradFi Treasury Bonds	$DAI	$USDC
Differences with their counterparts	1. CR starts at 110% 2. Only double asset exposure allowed for lending (single asset exposure is covered by $USs and by future single asset liquidity in Thorchain). 3. $CACAO cannot be re-minted above total supply 4. Pool liquidity is more sitcky due to Liquidity Nodes.	1. No subsidized fixed rate to drive artificial demand. 2. More marginal demand for $CACAO. 3. $CACAO cannot be re-minted above imported supply.	1. Accrues interest daily 2. Gets paid down daily 3. Easy to issue 4. Faster to liquidate in Maya Pools 5. No KYC	1. Lower CR, 2. Shorter block time, 3. Instant finality, 4. Collateral is productive, 5. No governance token to burn with surplus (MKR), rather profits are kept in treasury 6. Stability fees will be lower. 7. No auctions & sell orders.	1. 100% transparent on-chain proof of reserve, anytime 2. Cheaper to issue 3. Faster to issue and redeem than centralized stablecoins 4. No KYC
Status	Development Paused	Ready	To be technically and economically audited	To be developed	To be developed
Best for	1. ASSET-CACAO exposure with low CR and 0% interest 2. Maya Arbers	1. Rapid exit from positions 2. Foreign Exchange	1. Risk Averse Investors 2. Panic sellers	1. Increasing Single Asset Exposure 2. Safest peg, but most expensive	1. Business Treasuries 2. Best of all worlds
Limit	Set by liquidity sensitivity	Set by $USA holder vote	No limit	Set by Synth mint limits in Maya	Set by portoflio allocation limit
How do the treasuries profit in normal operations ?	1. Slip fees from anchor pool when minting & redeeming go to treasury.	1. Slip fees from sending $CACAO between Maya and Aztec. 2. 5% of seigniorage.	1. Reducing short term obligations while keeping assets.	1. Small Stability/ Interest rate 2. Profit from liquidations	1. All mentioned earlier, since they are required to mint $USC. 2. Flat 0.01% issue and redeem fee.
What does the treasury do with its profits?	Re-mint $CACAO if under limit. Hold $USm if at limit.	Re-mint $CACAO if under limit. Hold $USa if at limit.	N/A	Keep them in $USs, inside the treasury. Can choose to convert to $USb or directly back to assets when a lot is accumulated.	Keep them in $USc, inside the treasury. Can choose to convert to $USb or directly back to assets when a lot is accumulated.
Can be burnt to mint $USB	Yes	Yes	N/A	Yes	Yes
Can be minted from $USB	No	No	N/A	No	No
Rate to mint $USB	1 $USm = 0.993 $USB	1 $USa = 0.990 $USB	N/A	1 $USs = 1 $USB	1 $USc = 0.996 $USB
Peg Stability in normal conditions	Excellent	Best	Not good	Good	Good
Risk	High	Highest	Lowest	Low	Medium

Maya USD

Ticker: $USm
Nickname: Milk Dollar

THORChain hit the ball off the park with their $TOR design, and $USm is our own version of it. $TOR offers a great option for arbitrageurs as the start and end of their operations and features an excellent mechanism to maintain its peg. Let's see how $USm works and how they are different:

1. How it works. $USm is always redeemable for $1 USD worth of $CACAO. The exchange rate is calculated using the median value of the Maya's $CACAO / exogenous stablecoin pools' prices and does not require any oracles nor does it have mint or burn soft caps.

Instead, there is a slip-based (liquidity-sensitive fee) virtual $CACAO / $USm Anchor Pool where larger transactions pay higher fees, to disincentivize panic selling.

Our virtual Anchor Pool will not be as deep as the combination of all the rest of the stablecoin pools, instead only as deep as the deepest stablecoin pool. This leads to a shallower pool that is more profitable for the treasury and the first difference with $TOR's design.

We believe that making the pool deeper than this would be an overkill since $USm is already superior for arbitrageurs, compared to other stablecoins in the ecosystem, given their shorter block time, instant finality, requiring less time to settlement on the Yax Bridge (Bifröst), cheap on-chain transaction fees, etc.

$USm main economic use is fast entry and fast exit, with a stable value between the two events. Velocity is more important than cost for most arbitrage opportunities. This small change would keep $USm supply lower and more manageable, and higher revenues from the virtual Anchor Pool would go to the treasury.

2. LP Loans. Anyone can borrow $USm using LP units from our bluechip pools as collateral. There will be no single side collateral in Maya to avoid a "Top-Heavy" design.

Loans will start at a very competitive 110% Collateralization Ratio, which will increase as further loans of the same asset are created, to prevent overleverage on only one asset.

These loans will carry a 0% interest rate given that the collateralized LP Units are productive for the ecosystem.

3. IBC. It will be possible to send $USm into the Aztec Chain although it will have to pay a second liquid sensitive fee when returning into the Maya Chain.

It won't be possible to send $USm into other chains, through IBC, since its main use is for arbitrage inside Maya and that demand driver should be good enough.

4. Maya Pool. $USm sent through IBC to the Aztec Chain could be LP'd into Maya through the Yax Bridge. This Maya Pool will serve to capture liquidations without using order books.

5. Liquidation Allocation. Whenever a loan goes below the collateralization ratio, a liquidation event is triggered.

Every pool has a Liquidation Allocation (LA) variable, set between 0% and 100%.
If LA.BTC is set to 70%, which means that a liquidation event on Bitcoin will make 70% of the LP Units to remain as Protocol Owned Liquidity —which serves as a liquidity provider of last resort— and 30% to be withdrawn asymmetrically into $CACAO that then buys $USm from the corresponding pool.

Acquired $USm is burnt (settling the protocol debt), unless burning all of it would burn more $USm than what was minted in the loan. In this second case, profits are kept as $CACAO in the treasury, and only enough $USm is burnt to settle protocol debt.

Theoretically, liquidations should always represent a profit for the system given that the Collateralization Ratio (CR) would always be 110% or more. The more volatile or risky a pool is, the closer to 0% the Liquidation Allocation should be, conversely, the less volatile or risky the pool (ex. BTC or Stablecoin pools), the closer to 100% the Liquidation Allocation can be. This parameter is set by the nodes' consensus.

6. Liquidity Stickiness. Most of the liquidity in Maya is bonded by the nodes thanks to our Liquidity Nodes functionality. This means our liquidity is sticky which makes $USm safer.

7. No $CACAO minted above total supply. Even after the security mechanisms for $USm, like a shallower pool, price penalization for panic sellers and a safe exit into $USb, there is still a risk of depeg if Maya burnt $CACAO Market Cap diminishes and comes close to $USm's market cap. Because $CACAO cannot be re-minted above the Total Supply, in this case a $USm holder can only:

1. Hold until the peg is recovered.
2. Sell $USm at a loss.
3. Convert to $USb.

Massive use of t third option could then cause a depegging of Mo with $USb, and then the user's could only:

1. Hold until the peg is recovered.
2. Sell $USb at a loss.
3. Stake their $USb to get interest payments over time.

Aztec USD

$USa is our version of $UST, an algorithmic, decentralized stablecoin pegged to the USD that could be used for permissionless foreign exchange trading, remittances and more. We all know what, unfortunately, happened to the Terra / LUNA project, where demand for $UST increased disproportionately, in unproductive and unfavorable ways for the protocol.

Let's see how $USa works and how it iterates over the lessons that $UST left us with:

1. Liquidity Sensitive Fees. $USa is minted with $CACAO, which is a productive asset, with real use cases outside of the Aztec chain. This is a stark difference with the Terra / LUNA model and is extremely important because it limits death spiral risks.

$CACAO is productive because moving it around between chains and using it to provide liquidity generates revenues for the system. The system's treasury can use these revenues in economically smart ways and can use them to pay down outstanding debt, held by $USb owners.

2. Most seigniorage burnt from the beginning. 90% of the seigniorage is burnt from the very beginning, giving more room for new $CACAO to be burnt into $USa; the remaining 10% is kept in its entirety by the treasury.

3. No Artificial Demand. Maya and Aztec will never provide funds, let alone treasury funds, to drive up demand artificially. It's better to grow slowly and sustainably, rather than aggressively but with a time bomb. There will be efforts by the team to find more uses and demand for $USa on-chain, especially for its main use as remittances and foreign exchange, but that is all.

4. IBC. It won't be possible to send $USa into other chains, through IBC; extra demand would only increase stress on the system plus this way it stays closer to its primary market and core functions.

5. No $CACAO minted above imported supply. Even after the security mechanisms for $USa, like liquidity sensitive fees, price penalization for panic sellers and a safe exit into $USb, there is still a risk of depeg if and when Aztec burnt $CACAO Market Cap diminishes and comes close to $USa's market cap. Because $CACAO cannot be re-minted above the Total Supply, in this case a $USa holder has the following options:

1. Hold until the peg is recovered.
2. Sell $USa at a loss.
3. Convert to $USb.

Massive use of the third option could then cause a depegging of Mo with $USb, and then the user has these options:

1. Hold until the peg is recovered.
2. Sell $USb at a loss.
3. Stake their $USb to get paid down over time.

$USa, our version of $UST.

Synth USD

Ticker: $USs
Nickname: Sugar Dollar

$USs is our own version of $DAI, which was a DeFi breakthrough. MakerDAO developed what is arguably the best decentralized stablecoin model to date, with many diverse use cases and billions in locked value.

$DAI does have some scalability problems, as will $USs but, let's see what makes them different:

1. Tendermint. Having instant finality, short block time, low transaction costs and no need to burn a governance token is in itself already a big leap forward.

2. Supported collateral. $USs will allow for $sBTC, $sETH and $CACAO collateral only. $USs will not use centralized stablecoins as collateral, another big leap.

3. Supply and demand levers. A Stability Fee of 1% to 3% will be implemented and charged to borrowers, this fee will be used to stimulate demand or cool down supply without subsidizing yields artificially, via the "Aztec Holding Rate" (AHR), which is paid to lenders / savers / stakers of $USs.
Because not all of the $USs holders will be staked, leftover fees would be kept by the Treasury, as profit.

4. Liquidations through Maya Pools. Given that both $CACAO and Synths are always tradeable inside Maya Pools, and that $USs itself will be available in a pool through the Aztec Yax Bridge, liquidations do not have to go through a complex auctioning process.
Simply, the Aztec treasury can send back liquidated synths / $CACAO through IBC to the Maya Treasury, which will use aggregated instructions to exchange $CACAO and synths to $USs inside Maya Pools.
The principal of the loan will be burnt, settling the debt. Leftover $USs - considered profit - can be accumulated to then buy back $CACAO and Synths such that the treasury holds 50% of its portfolio in $USs and 50% in the average weighted collateral basket.

5. Collateralization Ratios. Tendermint capabilities and liquidations happening inside Maya Pools mean that liquidation speed is increased greatly and liquidation risks are reduced greatly. This allows us to offer lower Collateralization Ratios than $DAI does - especially for $CACAO, that must only go through 1 pool to liquidate into $USs (Synth to $USs is essentially two swaps).
Also, given the nature of the Maya pools and their slip-based fees, it is way cheaper to liquidate smaller transactions than it is to liquidate bigger transactions.
In light of this, Collateralization Ratios can be as low as 120% for a small position in $CACAO and up to 150% for a big position in Synths.
Finally, collateralization ratios can be lowered by the nodes to incentivize more $USs minting or increased to achieve the opposite effect.

6. Limits. There is no need to implement further limits to the $USs system, given that $CACAO numbers are already limited by the Max Debt parameter in the Aztec Chain and that minting Synths is limited to 16.5% of Maya Pool depth.

7. Depegging downward. When $USs is below $0.99, the treasury can swap its Synth and $CACAO portfolio back to $USs while increasing the stability fees to decrease supply and the AHR to increase demand. If the treasury runs out of Synths and $CACAO, nodes would proceed to increase the collateralization ratios, for example, $CACAO at a maximum of 140% and Synths at a maximum of 150%.
If $USs keeps depegging, nodes can vote on a global settlement where $1 USD of collateral is shared to $USs holders proportional to its basket and the rest of the collateral is kept by the treasury, benefiting those who held $USs or bought $USs below the peg, and penalizing those who sold below the peg.
If $USs depegs even further, converting it into $USb becomes more appealing, which, as we have seen before, generates demand for it and decreases supply.

8. Depegging upwards. Whenever $USs trades above $1.01, the treasury can swap its $USs for Synths and $CACAO while lowering the stability fees to increase supply and the AHR to decrease demand. If the treasury runs out of $USs to swap, nodes can decrease collateralization ratios, for example, $CACAO to a minimum of 120% and Synths to a minimum of 130%.
If $USs keeps depegging upward, nodes can vote on a global settlement, where $1 USD of collateral is shared to $USs holders proportional to its basket and the rest of the collateral is kept by the treasury, benefiting those who bought at the peg and penalizing those who bought above the peg.

9 .Productive Collateral. During the whole depegging event, Synth collateral has been actively producing yield for Nodes and LP's in Maya, as well as the Maya Treasury if a non-zero amount of fees from yield is allocated to it. Collateral is never simply sitting in a vault, rather it is used to stimulate the Maya Economy.
Likewise, $CACAO collateral means a reduced $CACAO circulation inside Aztec, which also means less $CACAO is available to mint into $USa. If near or above the Max Debt Limit, $CACAO price in Aztec Chain increases and provides an arbitrage opportunity for the Maya Treasury.

10. IBC. It will be possible to send $USs into other Cosmos-based chains, via IBC. In fact, we will actively spread it into other ecosystems, centralized or decentralized. Where $USm and $USa can mostly have demand issues - too much of it - , $USs faces the opposite problem, so increasing demand with this means will help it get adoption and alleviate pressure on our other stablecoins, mainly $USm and $USa.

11. Governance. There is no complex governance structure for $USs. Nodes have skin in the game and they are involved deeply in the Maya and Aztec chains so they get to decide on these complex issues. $CACAO users can vote with their money by buying or not buying into $USs.
Nodes must be honest, fair and above all communicative to the Community in order to drive up $USs adoption, which is best in their interest.

Collateralized USD

Ticker: $USc
Nickname: Chocolate Dollar

$USc, and $UScc, our versions of $USDC.

Creating a 1:1 collateralized and decentralized stablecoin is very difficult... Collateralizing with fiat would eventually get you into trouble with Uncle Sam and collateralizing with other somehow centralized assets would only move the problem to another layer, which doesn't really solve anything.
People have tried with multisig solutions, DAOs and smart contract escrows but central planning keeps leaving its mark and creating vulnerable points of failure.
We believe that $USc and $UScc can creatively sidestep these issues, let's see how:

1. Collateral. Both $USc and $UScc work exactly the same way: by tracking the price of a basket of other stablepools.
$USc tracks a basket composed of our other stablecoins - $USm, $USa, $USs and $USb - while $UScc's tracks a basket that also allows for synthetic and external Cosmos-based stablecoins. Oh btw, did you notice how our Milk dollar + our Almond dollar + our Sugar dollar + our Butter dollar form our Chocolate dollar? Yes, we really are geeks too.
$USc does not need to rely on any third-party dependency or project while $UScc has a higher risk diversification.

2. Basket. $USc holders themselves are best suited to decide on this! We will implement an "always on" vote mechanism for each wallet address, where a simple transaction with four numbers is sent to indicate the preferred stablecoin allocation.
One of these transactions might look like this: "Portfolio:20:10:45:25", which would indicate the holder suggests his positions should be backed up by 20% of $USm, 10% of $USa, 45% of $USs and 25% of $USb. These preferences would reflect the market outlook and situation.
The vote is always on and can be overwritten at any time by doing a new Set Portfolio transaction. Every addresses' vote is multiplied by the number of full $USc that they hold, wallets holding less than 1 $USc get their votes nullified.
If the wallet has never set a Portfolio Split, its vote is nullified. All votes are tallied and the median value of each asset is chosen. Because the sum of all 4 medians will most likely not be equal to 100, they must be normalized to 100, simply by dividing by the sum of the medians.

3. Minting. There is a short 20 minute delay in minting and burning $USc because:

a. $USc is not a fast exit liquidity stablecoin. It is instead meant to steadily hold its value.
b. They are competing against "several business days" centralized stablecoin issuers.

During this delay, users can post more collateral in any proportion. After the delay, Aztec will issue as many $USc / $UScc as the collateral proportion allows, trying to pair any unbalanced collateral with other users using FIFO. Any stablecoins that the system was unable to pair during the delay will be readily refunded.

4. Redeeming. When redeeming $USc, the user will always get back the real portfolio ratios worth of Aztec stablecoins. Again, there is a 20 minute delay in redeeming.

5. Changing the basket. When the basket changes, simply the pairing for new $USc minting changes, whereas redeeming is always done with the real portfolio ratio, not the ideal set ratio. Therefore, real ratios change slowly, only as people continue to redeem and mint.

6. Limits. There are no limits to the minting of $USc itself, but since other stablecoins (except for $USb) have their own limits, it will be limited to how much collateral is available to mint $USc.

7. Global Settlement. Just like with $USs, a global settlement event can occur if $USc or $UScc market prices go significantly above or below the peg.

8. Profits and assets left. The small minting fee will be kept in $USc by the protocol, to accumulate it and hold it. Notice $USc helps stabilize the whole ecosystem also, since it is a source of demand for all stablecoins (with the load shared between all of them) and locks these stablecoins off from being sold off quickly in panic sales. $USc can also lose the peg while collateral remains healthy, creating buy and burn demand for $USc to create $USb. These transactions leave $USc and therefore collateral behind, which is now owned by Aztec Treasury.

9. Collateral drop. Since any stablecoin's drop likely causes a drop in $USb price as well, there is always a risk that 2 out of the 4 collateral types fall together (albeit a smaller fall than if $USb did not exist). This would cause the $USc price to fall also, albeit in a smaller magnitude given that it holds the other 2 stablecoins as well, causing one of three outcomes for every user: 1. Those who hold and wait until peg is regained by the underlying collateral and therefore $USc 2. Those who choose to redeem and realize their loss or 3. Those who choose to convert to $USb, leaving their collateral behind to the Aztec Treasury. If the depeg persist and $USc is therefore still significantly off the peg, $USc holders will most likely change their on-chain vote to reduce exposure of the depegged assets significantly, thus slowly changing the collateral portfolio composition to a better pegged combination as some users redeem and and others re-mint.

10. Opportunistic minting of $USc. When a stablecoin is severely depegged, and $USc has exposure to it, a situation can happen where a holder of a depegged stablecoin can attempt to mint $USc at a profit using only the depegged coin. To stop this, Nodes can vote to disable disproportional minting of $USc during crisis times, requiring users to post perfectly proportional split of the different stablecoins to mint $USc, according to the latest basket split. This behavior could be automated carefully so no Node vote is required.

11. IBC. $USc will be IBC-enabled and proliferated in other Cosmos Based chains and other centralized and decentralized ecosystems.
As our Chocolate USD, and first 1-to-1 backed decentralized stablecoin, it will be our flagship token for stability in off-chain uses. The team will actively seek to build bridges for $USc to other ecosystems like Ethereum and Solana. Importantly, $USc can have high demand given that it shares the load among different failure modes and its portfolio composition will most likely be voted to be inversely proportional to each stablecoin's risk. Finally, it will be the only Aztec stablecoin to not have a $CACAO/$USc Maya Pool, for reasons that will be outlined in Chapter 6.

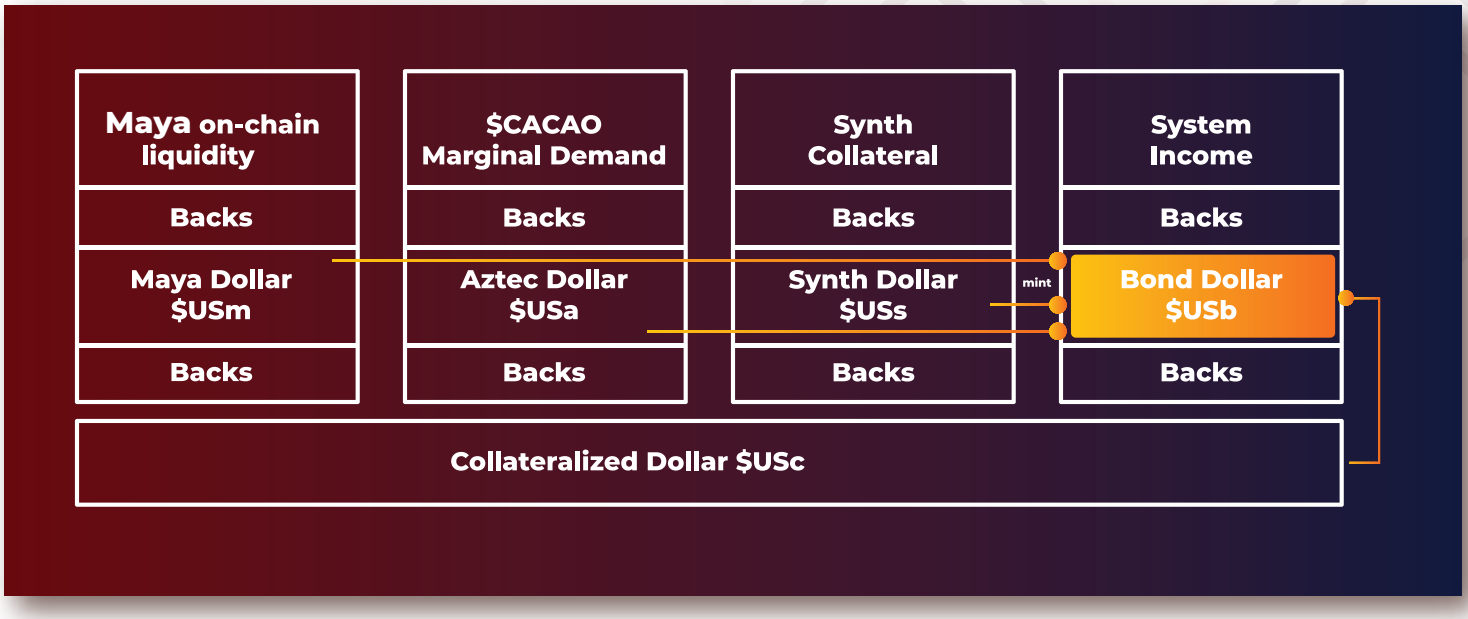
Final remarks.

We believe our stablecoins' designs have several advantages, in addition to the way it distributes the demand load between all of them:

$USc, which becomes our major stablecoin, re-balances continuously, sharing all of the other stablecoins' advantages and disadvantages. It also motivates disclosure, critical thinking and transparent discussion about the underlying strengths and weaknesses. This also helps our users ultimately decide on what tokens to use, based on their needs or investment thesis, and considering their desired risk / reward ratios.

All of our designs are also of course subject to iteration and failure, but are well covered for the latter with our Bond mechanism. Our stablecoins can and will grow as much as they are demanded.

Finally Maya Pools are a set of Continuous Liquidity Pools, run by the same nodes that keep Aztec secure, and that also have a huge vested interest in the well-being of $CACAO and the whole of the network.



Technical overview

$USa and $USb have been fully developed according to specs. They were developed directly on-chain for native functionality using Golang and the CosmosSDK. This means that they can be regularly updated, improved, patched, iterated upon and are under node governance.

Likewise, $USm, $USs and $USc will have all their functionality developed natively. This is in line with our ethos of iterating on designs, a possibility out of reach for Smart Contracts, which have to regularly migrate all their liquidity from one place to another, making iteration complicated and even undesirable.

Given this, a lot of how all 5 stablecoins work will likely change, with respect to descriptions in this document. For instance, taking advantage of on-chain always-on voting can lead to developing a Stop/Go voting mechanism for $USa, or caps might be implemented or lifted. Parameters can be tweaked and new ideas can be introduced.

The decentralized stablecoin field is still young, with plenty of space for improvement and development, these facts must be hard coded into their implementation, into our culture and our community.

Given that $USm, $USs and $USc are still to be developed, user stories and code herein apply exclusively to $USa and $USb.

Although $USa and $USb code will be audited before Maya's fair launch, economic audits might take longer and it will be the decision of our community to leave $USa and $USb in stand-by mode, until our stablecoin suite is more solid. $USb can also be turned on before $USa and others to make sure it works as intended, both technically and economically, before the rest of the suite comes online.

User Stories:

1. $USa

- As a user, I want a liquidity sensitive fee implemented for expatriating and repatriating $CACAO between Maya and Aztec so the Treasury has funds to keep my investment safe.
- As a user, I want 90% of seigniorage burnt to leave more room for $CACAO re-minting during $USa sell off events. I also want 10% to go to the treasury so it has funds to keep my investment safe.

2. $USb

- As a user, I want to be able to mint $USb by burning $USa or other stablecoins in a non-reversible way.
- As a $USb owner, I want to receive interest payments in $USb, regardless of whether I'm staking $USb or not.
- As a $USb owner, I want to be able to stake and unstake my $USb at will.
- As a $USb staker, I want to receive my share of $CACAO pay downs. I need the treasury to have a way to fund the Bond Reserve for these payments to take place.

3. Translate Terra Bifröst

- As a user, I want to be able to bridge my stablecoin liquidity to other external assets through an Aztec Yax Bridge to Maya.

Code

Add $USb logic
https://gitlab.com/mayachain/terra/-/issues/5

Add $USa logic
https://gitlab.com/mayachain/terra/-/issues/6

Add Aztec Yax Bridge Client
https://gitlab.com/mayachain/thornode/-/issues/46

Part 6. Stable Pools & Route Optimization

Optimizing can only be done when there's more than one option. What if we break transactions into smaller trades that always take the path of least resistance? Can we do this while increasing Maya's internal economic value and creating healthy demand for $USc?

ELI5

1. Liquidity Pools are piles of cryptocurrencies locked up inside smart contracts, usually in pairs, by people called “Liquidity Providers” (LP’s). DeFi users can buy from or sell to these smart contracts at all times and the price that they can give or ask is balanced out by the ratio between the assets inside them.

2. Assets usually have to be contributed into Liquidity Pools in equal USD denominations, for example in an typical ETH / $CACAO pool, LP’s would need to input $100 USD worth of $CACAO for every $100 USD worth of ETH. This requirement might not be ideal for many investors, who do not want exposure to the price fluctuation of $CACAO or who do not want to risk having Impermanent Loss.

3. In addition to our $CACAO pools, we have designed special Liquidity Pools that pair assets against our stablecoin $USc, that enjoy Impermanent Loss Protection and that are enhanced with slip-fees optimizers in order to attract more institutional and conservative investors. Internally, our systems will route all trades in the most efficient way using both our regular and our Stable Pools to give our users better prices and bigger notional depth. We hope that external DEx User Interfaces like this model of pools and connect to them, in combination with THORChain’s.

Philosophical perspective

If decentralized Cross-Chain technologies are going to replace CeFi, they will require serious liquidity depth and tremendous volume. And because volume follows depth, this should be our main focus and priority, only behind security. With enough depth, slip fees make swaps more affordable for larger trades too.

Our Stable Pools feature is one additional step to increase our liquidity and depth - should Maya 3.0 be enabled - plus, as we outlined in Chapter 5, the creation of $USc tokens and their subsequent lockup inside pools is a net positive for our ecosystem and for the economics of $CACAO.

Our offering of pools that imply less uncertainty is also obviously great news for institutional investors and more conservative players since they can get exposure to our LP opportunities and to our protocol success without having to worry too much about different sources of volatility.

Because of the way orders are routed using both regular and Stable Pools - see details in our Economic Overview - when trading assets across different blockchains, users experience a bigger notional depth, one that sums the depth of all the pools involved in their trade, with the corresponding slippage and slip fee benefits that this brings.

Outside of the Maya blockchain, as usual, only one transaction needs to be sent and only one transaction needs to be received, and so gas fees in the source and target chains are not increased.

Notice how this is all positive for the Maya Economy in many ways:

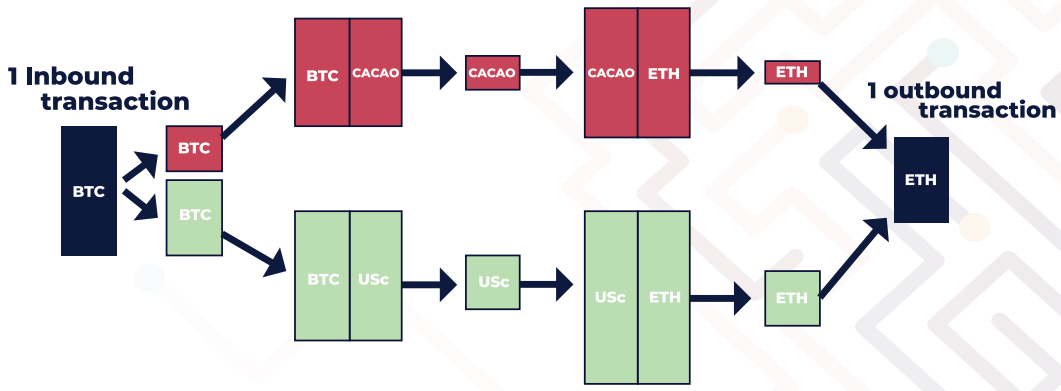
1. More perceived depth means lower slip fees, with the increased affordability comes increased swap demand and thus better yield for the system players.
2. To add $USc to Maya Stable Pools, an investor had to buy $USc (generating demand) and lock it all up in the LP position. Although impermanent loss is greatly reduced in Stable Pools, Impermanent Loss Protection is still attractive and serves as an additional incentive for the Stable LP Units to remain for at least 100 days.
3. For the investor to have acquired $USc, the investor had to buy it from someone who had to post $USa, $USm, $USs and $USb as collateral at the voted portfolio distribution. In the process, $CACAO expatriation fees were paid, $CACAO was burnt, Synths were minted (increasing pool depth in Maya) and short term debt was converted to long term debt.
4. $USc is brought to Maya and paired to its primary market and generates yield there, creating real and deep rooted demand.
5. Stable Pool's LP units won't count towards bondable liquidity for our nodes. This means that the system would tend towards the lower end of our Incentive Curve for Liquidity Nodes (see Chapter 3) and would increase yield for our nodes, making it more attractive for LP's to upgrade and compete in the churn rounds while generating $CACAO demand and increasing the security budget.

Finally, to any and all User Interfaces that already work with THORChain and that wish to connect into Maya to increase reliability and decentralization, we suggest that they use this method too, breaking big transactions into smaller ones, and routing them through both protocols, proportional to the best available pool depths. This would of course result in better trading fees while benefiting both LP's in both protocols. In the following Economic Overview section we explain why it is economically attractive for User Interfaces to operate in this way.

Economic overview

Inside Maya, all trades to or from $CACAO, as well as trades to or from $USc can clearly use only one pool, for example someone trading BTC for $CACAO will readily use the BTC / $CACAO pool.
However, for “longer” swaps, like BTC to ETH, the transaction can be completed using all four pools, as long as the partition is known for how to get lower slip-based fees. In the same example, these four pools are: BTC / $CACAO, BTC / $USc, $CACAO / ETH and $USc / ETH.

The optimal amounts and paths considering four pools is not trivial, given that they can all have different depths and that you need to commit to a proportion of the funds from the beginning.



To find the best proportion to transact into the pools we need to get the local maximum of a function that takes into account the differences in depths and the truncation of the routes. Note: for this derivation, it is advised to already understand the CLP derivation THORChain created in their design of the Slip Based Fees for AMM swaps:

$$\textbf{Eqn12a:}\quad y = \frac{x\,Y\,X}{(x + X)^2}$$

Where: X is the balance of the inbound asset, Y is the balance of the outbound asset, x is the inbound asset input and y is the outbound asset output, to the desired wallet. The difference between y and x*Y/X is the slip fee, which is retained in the pool.
This equation depends on knowing the balance of each asset before the transaction and we can further simplify it by using percentages instead of absolute numbers. If x is input as a percentage of X then both X and Y cancel out (as 100% = 1) and y becomes also a percentage output. The simplified equation looks as follows:

$$y = \frac{x}{(x + 1)^2}$$

Translating the equation into percentages also helps abstract away the underlying asset balances and, with this simplified version, we can truncate it into itself one more time to describe a single route (by substituting y with the equation above):

$$z = \frac{y}{(y+1)^2} \longrightarrow z = \frac{\frac{x}{(x+1)^2}}{\left(1 + \frac{x}{(x+1)^2}\right)^2}$$

The above represents the equation of one route through two consecutive pools that charge slip-based fees. This equation assumes both pools are equally deep so, to adjust for the depth difference, we introduce the first weighting factor Dn , which is the measure of how much deeper (or shallower) the second pool is relative the first pool along route n, calculated simply as the depth of the second pool divided by the depth of the first pool in terms of the common asset they share. Notice $D_n > 0$.

$$z_1 = \frac{\frac{x_1}{D_1(x_1+1)^2}}{\left(1 + \frac{x}{D_1(x+1)^2}\right)^2}$$

We have added the subscript “1” to z and x as well, to label the route as Route 1. Now that we have the generalized equation for one route, let’s sum two together, simply like so:

$$Z_t(x_1,x_2) = Z_1 + Z_2$$

Where: total z is the sum of both route’s assets. This sum assumes both routes are identical and is not breaking up the asset allocation x1 and x2 as a zero-sum game. To set these equations we need to have x1 depend on x2 and vice versa. To continue we will require a few significant adjustments:

First, we will stop using x1 and x2 as the percentages of the inbound asset. Instead, we will substitute them with new variables:

$$X_1 = \frac{A_{in} p\,(1 + R_1)}{R_1} \qquad X_2 = (1 - p)(1 + R_1)A_{in}$$

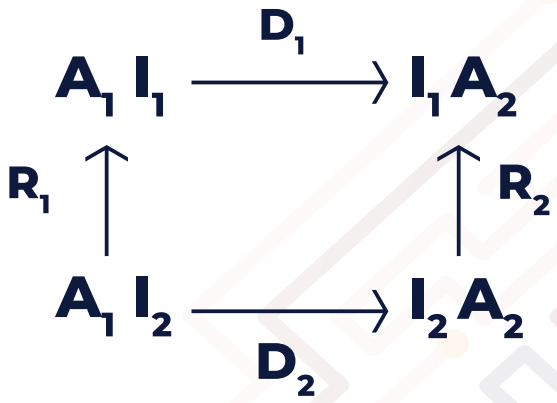
Where Ain is the inbound asset traded into Maya as a percentage of the sum of both inbound pools’ inbound assets, p is the proportion of the inbound asset to be swapped through Route 1 and (1-p) is the proportion of the inbound asset to be swapped through Route 2. R1 is the Relative Depth between the 1st Pools along each route, calculated simply as the depth of the first pool of Route 1 divided by the depth of the first pool of Route 2, in terms of the common asset they share. Finally, z1 and z2 must be weighted as well, so we similarly introduce R2 to weigh the Relative Depth between the 2nd Pools along each route.

$$Z_t(x_1,x_2) = \frac{Z_1 R_2 + Z_2}{1 + R_2}$$

Substituting everything and simplifying, we get:

$$A_{out} = \frac{A_{in}(1+R_1)}{1+\frac{R_1D_1}{D_2}} \cdot \left[\frac{\frac{p}{\frac{R_1D_1}{R_1}\left(1+\frac{A_{in}p(1+R_1)}{R_1}\right)^2}}{\left(1+\frac{A_{in}p(1+R_1)}{R_1D_1\left(1+\frac{A_{in}p(1+R_1)}{R_1}\right)^2}\right)} \cdot \frac{R_1D_1}{D_2} + \frac{\frac{(1-p)}{D_2(1+(1-p)(1+R_1)A_{in})^2}}{\left(1+\frac{(1-p)(1+R_1)A_{in}}{D_2(1+(1-p)(1+R_1)A_{in})^2}\right)^2} \right]$$

R_2 has been substituted to constrain it to its possible values along the determined line defined by the other weights. To avoid confusion, A_{out} has been introduced to substitute z_t, defined as the outbound asset traded out of Maya as a percentage of the sum of both outbound pools' outbound assets. Notice that by definition: $0 < A_{in}, A_{out}, p < 1$, as well as that all weights are greater than zero.



The diagram above shows each weight more clearly. All weights can be easily calculated given that they always share a common asset to compare depths - "apples to apples". "A" stands for Asset and "I" stands for intermediary.

Wherever the first order derivative of A_{out} with respect to p is equal to zero between $0 < p < 1$ maximizes A_{out}, essentially the optimal proportion p to break the inbound transaction through the first route and sending 1-p through the second route, minimizing slip fees for the transaction.

$$A_{out}\,(A_{out}'(p) = 0) = Max\,[\,A_{out}\,]$$

This is also the optimal strategy for incumbent and future User Interfaces, Wallets and Institutional Investors routing large transactions (where slip is most important). As long as the slip savings are larger than the double gas expense on inbound and outbound chains, it is in their best interest economically to break the transaction up routing volume to both Maya and THORChain. User Interfaces can implement the above optimizations using THORChain as Route #1 and Maya as Route #2. So, everytime the following condition is met, User Interfaces would be better breaking up the transaction:

$$(MOD + TOD) \cdot Max\,[A_{out}] - \text{double gas} > Max\,[\,MOD \cdot Z_1\,(1)\,,\, TOD \cdot Z_2\,(0)\,]$$

Where MOD stands for Maya Outbound Depth and TOD stands for Thorchain Outbound Depth. Assuming Thorchain is Route 1 and Maya is Route 2.

This is key, given that it is not only more convenient for User Interfaces to have more than one provider for reliability and redundancy matters, but there are also direct and economical incentives to integrate and use various Thorlikes simultaneously, for each transaction.

This in turn increases the likelihood of a multi-thorlike future of cross-chain technologies, where a network of L0's collaborate together, route liquidity to each other and mutually increase their resilience.

The optimization works for any arbitrary number of routes (by adding more terms, with their appropriate weights), so it would work for any number of interconnected cross-chain liquidity networks. Keep in mind that servicing inbound transactions is throttled down as transaction size grows bigger, so this strategy would also yield faster swaps given their smaller size relative to each protocol's depth when broken down.

Interestingly, our simulation results have been outstanding. Even if Thorchain pools are 3x deeper than Maya, users still get around 23.8% saved in transactions of 1% depth of the inbound pools when using the optimized double route. That is very significant for any user at those amounts, so User Interfaces should really take supporting Maya seriously. It is important to note that User Interfaces would still get the same affiliate fee in absolute amounts, their users would just pay less, making User Interfaces who support Maya more competitive than those who don't. To illustrate an example, BTC pool in Thorchain at the time of writing is $35M and ETH pool is $20M. If Thorchain is 3x deeper, it would mean Maya has $11.67M and $6.67M in its BTC and ETH pools respectively. A 1% transaction of the inbound asset would mean $233,000 being swapped from BTC to ETH, 24% saved by going optimized double route would mean $3,800 USD saved by the swapper, no loss for the User Interface and both Thorchain and Maya being more attractive overall, jointly increasing cross chain demand thanks to increased affordability. This is how we get to mass adoption.

For a 2% transaction of total inbound asset (Ain) with all else equal, the savings is "lower" as a percentage of total fees paid, but significantly higher in absolute terms. The swapper would save 22.7% on $16,000 in fees paid: $13,800 in savings going Double Route.

On the other end of the spectrum, for a 0.2% transaction of total inbound asset, 24.7% is saved on $675 in fees paid: $167 in savings going Double Route. At these levels, gas fees in the source and especially the target chain start playing a more significant role with current depths, but as TVL grows larger in both protocols, savings in absolute terms increase while gas fees remain the same, making it ever more attractive to go Double Route at lower slip transactions.

It is important to note that for Maya to have $11.67M and $6.67M depth in its BTC and ETH pools, it just needs to raise half of those amounts during the Liquidity Auction given that the CACAO side is being donated. $5.83M of BTC and $3.33M of ETH are very much attainable given the scope of Maya, its very attractive launch model and its battle-tested code.

Same goes for $USc pools in the future, if 25% of liquidity in Maya is in $USc paired pools, our users will perceive 24.7% savings in 0.02% inbound asset transactions that are routed to Maya, and this time gas fees don't play a role given that there is only 1 inbound transaction in the source chain and 1 outbound transaction in the target chain.

As a last economical remark, external assets in Stable Pools in Maya do not count directly towards the deterministic value of CACAO given that it is not paired with CACAO. Despite this, more funds in stable pools create lower slip fees and therefore larger swap volume without increasing bonded liquidity, therefore increasing yield for Nodes who need to buy CACAO using external assets to then add CACAO + ASSET liquidity, increasing TVL in the process.

This is because liquidity provided into our "Stable Pools" by any node will never count towards its bond. In other words, the LP tokens that help them churn-in can only come from bonding with $CACAO, to help it stay as our main trading token and as the super majority of our liquidity. Remember also that, as we covered in Chapter 5, $USc has a capped supply amount, which comes from the limits of the underlying stablecoins that comprise it, to prevent over-leverage in the system. Between these two phenomena, Stable Pool share of total liquidity will always remain below 33% but realistically will be as low as 10% to 15%. Above 33% Stable Pool share, Liquidity Rewards are 0 and all block rewards go to Nodes equally, providing no incentive for LPs or Nodes to add more $USc paired liquidity and even remove it, while incentivizing new Nodes to pair $CACAO in pools to churn-in. In other words, adding more liquidity to Stable Pools has quickly diminishing returns for all players adding Stable Pool Liquidity as its share gets closer to a 33% share, a behavior that is desired.

Technical overview

Compare our findings! To model the optimization yourself, you can use the following Desmos Link: https://www.desmos.com/calculator/uaxekehi4f

And follow these steps:

1. Desmos: Modify the weights (R1, D1 and D2) and Ain to simulate. Weights are set at 3x Route 1 vs. Route 2 depth and 1% total inbound asset transaction, but you can modify these values to simulate other cases.
2. Desmos: To refresh, R1 is how much deeper Route 1 Pool 1 is compared to Route 2 Pool 1. D1 and D2 is how much each route's second pool is bigger than the first. If Pool 2 along Route 2 is half as deep than Pool 1 of Route 2, then D2 = 0.5. Use Ain as the percentage of the overall inbound asset in pools (Route 1 + Route 2) that you wish to simulate a trade for.
3. Desmos: Look for the local maximum y point in the graph between $0 < x < 1$. You can find it by clicking the line, a small circle should appear at the maximum value. If you hover over the circle, coordinates for x and y at that point should appear right above the circle.
4. Desmos: The x-coordinate of that point in the graph is "p", the y-coordinate in the graph is "Aout".
5. Excel: Compare the simulation with this excel sheet: https://bit.ly/3y8UToo, which uses Thorchain's classic slip based fee formula to compare Single Route to Double Route. Double Route here means that a transaction passes through $RUNE in Thorchain and $CACAO in Maya, respectively. You can modify the values in the yellow cells to play around with the model, only make sure they are changed in Desmos as well. Thorchain is used as Route 1 and Maya as Route 2.
6. Excel: If you use any other "p" partition value between 0 and 1, the slip fees should always be greater than that of the optimized "p" value that was found using the Desmos simulation. You can compare this by making sure that the 2nd and 3rd simulation cases have values below and above the optimized "p" partition in the red box.
7. Excel: The final balance of the outbound asset should be equal between the classic calculation compared to calculating using Aout * (TOD + MOD) from the Desmos simulation. You can compare this at the bottom of the 1st simulation case. If the amounts are slightly different it is because of significant figures used by Desmos, running the simulation on Python yields exactly the same result for the Maya Route Optimization compared to Classic CLP derivation in steps.

Remember none of the above has been implemented in our code or on-chain since neither $USc or Maya 3.0 are implemented yet. No code has been developed for the use of User Interfaces either because their approaches and technologies vary a lot, nevertheless, we believe the optimizations discussed can easily be incorporated into their processes.

Their implementation can choose to do the derivative and find the relevant zero in y' between 0 < x < 1, and then use that value as the partition. Another option is to calculate the maximum value of y using a 0.01 step (or any other arbitrary step size) for x between 0 < x < 1 and use the value of x at the maximum as the partition proportion. The second implementation is simpler but can lead to more computational work.

Our recommendation is that User Interfaces set an "Auto" setting, where bigger transactions calculate and use this optimization and where smaller transactions are simply routed through the deeper route, taking into account inbound and outbound chain gas fees.

They can also implement an "Auto / Manual" toggle, where their users decide whether they want to use this optimization across THORChain and Maya or only one of them (or another future similar provider!). Recurrent checks can monitor both protocols' health too, if one of them is not working optimally, said User Interface can automatically route all their transactions through the other one, without optimizing.

Finally, liquidity provided into our "Stable Pools" by any node will never count towards its bond. In other words, the LP tokens that help them churn-in can only come from bonding with $CACAO, to help it stay as our main trading token and as the majority of our liquidity. Remember also that, as we covered in Chapter 5, $USc has a capped supply amount, which comes from the limits of the underlying stablecoins that comprise it, to prevent over-leverage in the system. Between these two phenomena, Stable Pool share of total liquidity will always remain below 33% but realistically will be as low as 10% to 15%. Above 33% Stable Pool share, Liquidity Rewards are 0 and all block rewards go to Nodes equally, providing no incentive for LPs or Nodes to add more $USc paired liquidity and even remove it, while incentivizing new Nodes to pair $CACAO in pools to churn-in.

CODE

To be developed.