Supernova: Ultimate Platform for staked assets (version Gamma 1)

Carina Labs

eric@a41.io
lucidpark@a41.io

Abstract. Cosmos is a pioneering ecosystem with foundations native to the multichain era. As their slogan 'The internet of blockchains' suggests, Cosmos is a decentralized network of independent yet interoperable app-chains that are connected through the Inter-Blockchain Communication (IBC) protocol. Due to its consensus algorithm, Tendermint, Cosmos requires token holders to stake a certain amount of their tokens to safeguard the chain's security. A chain's optimal outcome is acquiring more than a certain amount of staked tokens. So in order to incentivize the token holders to stake their tokens, app-chains provide economic incentives in the form of staking yield along with voting powers to the on-chain governance that provides the stakers the sovereignty to govern the ecosystem that they have an interest in. However, even with all the staking incentives, the most optimal behavior of token holders is not staking but DeFi activities.

The primary solution to this problem is liquid staking. Liquid staking enables token holders to earn staking yields on Proof-of-Stake blockchains and provides liquidity for the stakers as well. In other words, it can provide additional liquidity for the ecosystem while preserving the chain's security.

Supernova is the Ultimate Platform for staked assets. We provide three components for achieving the goal: First, provide liquid staking for all app-chain's native tokens and provide solid utility to the shadow tokens such as auto-compounding and using them as collaterals for CDP stablecoin. Second, develop and provide fair staked swap for staked assets. Finally, be a governance bribe protocol as we deploy a single validator on each app-chains.

We will provide all components that will serve as money lego within liquid staking and ultimately establish the infrastructure of the staking pools' ecosystem.

Keywords: Liquid Staking · Fairness · Staked Swap · Robustness

Table of Contents

1 Introduction

1.1 Staking Pools

Staking pool is the protocol that allows agents interested in transaction verification to open a pool and let other token holders delegate their shares to them. Staking pool blockchain is attractive because verifiers can get block rewards, and participants can receive incentives through delegation. However, it is also a problem because malicious agents can have a significant stake by operating a staking pool.

Security of Staking Pools The protocol is secure if $H > M$, where H stands for the total amount of assets delegated to honest verifiers and M stands for the amount delegated to malicious agents. Malicious agents are participants who harm the overall ecosystem to maximize their interests. Honest agents are participants who run verification or delegate their stake as the protocol requires. However, even honest agents also choose ways to maximize their returns while not violating the underlying intentions of the system.

The Trade-off between Security and Yields Staking is an element directly related to the security of the chain. Assigning assets to honest validators can be seen as contributing to the stability of the protocol because it eventually helps to satisfy $H > M$. However, participants often choose to use the asset in DeFi because it provides a higher yield compared to staking. Since assets cannot be used elsewhere during delegation, there is a trade-off between blockchain security-delegation- and income-maximization-.

Manually Re-stake Compound Interest Staking rewards can be re-staked to obtain compound interest. However, there is an inconvenience of periodically having to go online and perform the re-staking manually which incurs transaction fees.

Liquid staking Service The liquid staking service can solve the above two problems. It tokenizes delegated shares and allows them to use them in DeFi. In addition, the service integrates and cost-effectively manages delegations. The liquid staking service is attractive because it allows users to earn profits from the delegation and benefit from using DeFi through shadow tokens. In addition, the service may provide auto-compounding of the interests so that the stakers don't have to manually take care of the process.

1.2 Challenges on Liquidated Staking Pools

However, incumbent liquid staking services have several limitations such as:

The Oracle Problem Compared to a liquid staking service that runs on a single chain, a service that operates on multiple chains has the risk of not being able to acknowledge how many tokens are staked and how much should be liquidated. Therefore, an oracle feeder that delivers information to each other chains, is necessary here. However, several problems can arise with the timing of oracle updates. For example, an abnormal amount of assets may be withdrawn if a validator gets its staked tokens slashed but is not recognized by other chains. Therefore, it is necessary to design a stable protocol so that the protocol and participants do not lose their assets by managing the cycles of the oracle well.

Limitation of Withdraw Requests In Cosmos, there is a limit to the maximum number of requests for undelegation that one account can have for one verifier. Therefore, if the service has one account representing all delegators, it is important to address this maximum number limit. If the platform does not consider the maximum number limit, a bank-run may occur that cannot process the user's request in time.

Lock-up Period on Undelegation For the stability and predictability of the protocol, it is common to restrict frequent delegation and undelegation from the protocol. In other words, they usually have a lock-up period during the undelegation process. Accordingly, liquidated assets are also used to bypass the lock-up. If someone swaps the liquidated asset with the original one, It has the same effect as getting an instant undelegation. However, since the value of a shadow token is deeply related to the original asset but cannot be traded 1:1, a more sophisticated swap mechanism design is required. The value of the shadow token continues to rise due to auto-compounding and because of this, the liquidity providers of the swap pool are exposed to continuous impermanent losses. Also, the users are exposed to slippages during the swap.

Carina Labs designed and implemented Supernova, a novel liquid staking service that addresses and solves the challenges illustrated above. Supernova is the first project to solve all of the above issues.

2 Terminology

2.1 Cosmos

Inter-Blockchain Communication IBC is a protocol for communicating arbitrary data between cosmos blockchains. IBC allows different chains to communicate with each other in a trustless manner and interoperate by exchanging arbitrary values. Data is transferred through a channel run by a relayer in a trustless setting and can be verified when the message reaches the target chain. The IBC specification includes special packets for tracking the status of the target chain, such as acknowledgment and timeout. The ACK indicates that the target chain has correctly performed the required state transition.

Interchain Account Interchain Accounts, ICA for short, allows users to create, control and manage accounts of other chains connected through IBC. Since the ICA uses the IBC specification, the ACK is used to validate the correct reception and performance of the target chain. The general account uses a private keys to sign transactions, but ICA is controlled only by the controller chain through IBC transactions.

Authz The Authz module allows participants to grant arbitrary authority from one account to another. Users can only allow delegation of certain types of transactions without being exposed to the risk of other unauthorized transactions being performed.

2.2 Supernova

Assets There are many kinds of assets between Supernova and other blockchains. It can be classified into Asset, wAsset, and snAsset.

Asset The Asset with no prefix is a fundamental asset given as a block reward or used as a transaction fee for blockchain. It is also referred to as Native Asset. ATOM is an asset of Cosmos Hub Gaia, for example.

wAsset The wrapped asset is an asset that has been transferred from another blockchain through IBC, bridge, et cetera. The native asset or the wAsset comes in from outside and becomes a wAsset, such as wATOMs on Supernova.

snAsset The *sn* prefix is an asset liquidated through a Supernova. For example, wATOMs can be liquidated into snATOMs. See Section 3 for a detailed lifecycle of the snAsset and Section 4 for the application of the snAsset.

Keeper For the security and maintenance of the protocol, a privileged user may be required sometimes. To avoid compromising the degree of decentralization, authorized users are often designed to be distributed through multisig or Decentralized Autonomous Organization (DAO). In this paper, such addresses, contracts, organizations, or implementations are referred to as keepers.

3 Features of Supernova

3.1 Lazy Minting

Fairness Incumbent liquid staking platforms often include an auto-compounding feature. Unfortunately, because of this feature, stakers may be exposed to loss depending on the timing of auto-compounding and the frequency of oracle. Let's look at the below example:

1. A malicious attacker gains stakes by staking in the block just before the oracle update.

2. Oracle is updated on the platform.
3. The attackers who gained shares just before the oracle update also get the same rate of value increase as existing stakers who staked between the oracle update or before.

In short, the person who obtained the stakes just before the oracle update takes unfair advantage. The attacker may continue to perform such actions to gain an unfair amount of returns. In addition, if there is a problem with the oracle bot and the synchronization between Gaia and Supernova is delayed, an attacker who has just deposited can take the whole interest of staked ATOMs for a delayed synchronization period.

Definition of Fairness The user can receive benefits of increasing or decreasing the value per share from the oracle update at time t *if and only if* he has staked from time $t-1$, the previous oracle update, to t.

Lack of Fairness Protocols that do not meet the criteria of fairness illustrated above are not fair. There may be malicious users who unfairly acquire an increase of shares.

Currently, no liquid staking protocol provides such a fair environment. Supernova is the only protocol that meets fairness.

Lazy Mint The user is not allowed to issue shares, the shadow tokens, immediately to mitigate the lack of fairness. The shares can only be issued after the oracle update of a given cycle is complete, and we defined this as 'Lazy Mint'.

Lazy Mint Suppose each oracle update has a unique oracle version t. If the asset is staked at t, the liquidated share can be received by requesting the minting at $t+1$ or higher.

Deposit and Claim on Supernova Figure 1 shows the process of depositing wATOMs and receiving token shares, snATOMs. User, Supernova, and Cosmos communicate with each other in this process which is as follows:

1. Deposit wATOMs.
   (a) Deposited wATOMs are transferred to Cosmos through IBC.
   (b) Related ACK is returned.
2. Bot makes the ICA call to delegate ATOMs.
   (a) Delegate ATOMs.
   (b) Related ACK is returned.
3. Bot updates oracle.
4. The user claims snATOMs.
   (a) Supernova mints snATOMs for the user.

Because communication between different chains is required, a constraint checking two ACKs is required apart from the oracle version check to mint snAssets safely.

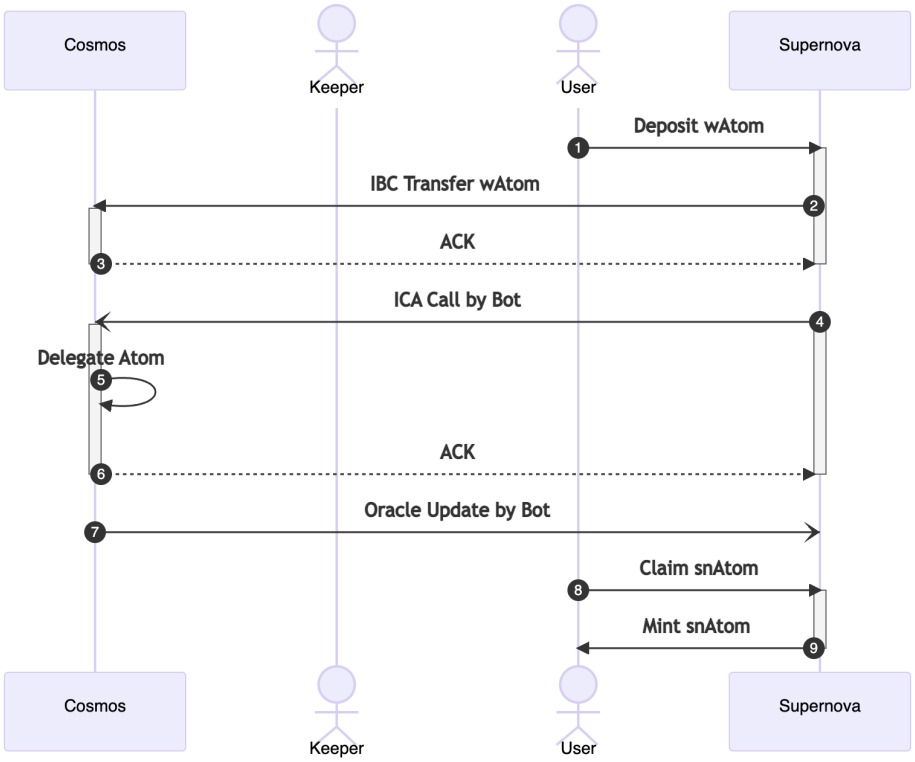

Fig. 1. The process of claiming snATOMs after depositing wATOMs through the lazy mint

3.2 Batch Withdraw

Batch Period Cosmos limits the number of undelegation requests that a single account can make at the same time to prevent overloading on the blockchain and remove the possibility of DoS attacks. The restriction size can vary from protocol to protocol, ranging from 7 to 10.

Supernova uses one ICA account to delegate ATOMs to Gaia. There may be more than 10 undelegation requests from users; therefore, the requests must be grouped into batches.

Lower Bound of Batch Period In an environment where only one account can send withdrawal requests, all requests can be processed without delay only if the following condition is met:

$$U \leq BM \tag{1}$$

consists of batch period B, undelegation period U, and the maximum number of undelegation requests M.

The above inequation can be used to calculate the minimum batch period $B' = \lceil U/M \rceil$ per diem. In other words, the protocol must use a longer batch period than B'. For example, all requests can be processed by grouping with a 3-or-more-day batch since Gaia's undelegation period is 21 days.

Bank-run A bank-run refers to large-scale withdrawals of money from banks in situations where many clients are worried about bankruptcy. The payment may be delayed, or all individual assets may not be returned in the case of a bank-run.

If there is a possibility that users' undelegation and withdrawal requests will not be processed at the time promised by the protocol, the protocol can be said to be in a state of a bank-run.

Possibility of Bank-Run Protocols that do not meet the inequation 1 are likely to be exposed to bank-run.

Impossibility of Bank-run on Supernova There is no possibility of the bank-run on Supernova, since it meets the lower bound of batch period lower limit. For example, Supernova has a three-day batch for Cosmos' undelegation that meets the condition $21 \leq 3 * 10$.

Parallelization If more frequent undelegation requests are needed, the protocol can have more than one ICA account in the relative chain of the Supernova. If three ICA accounts run on Gaia, they can handle the undelegation requests in a 1-day batch.

Undelegation and Withdrawal on Supernova Figure 2 shows the process of withdrawing the deposited ATOMs which functions as follows:

1. Send snATOMs to request undelegation of the corresponding value.
   (a) Burn snATOMs.
2. During the three-day batch period, the undelegation requests are gathered into one, and the bot sends an aggregated request through ICA call.
   (a) Request to undelegate ATOMs.
   (b) Related ACK is returned.
3. After the undelegation period, the bot sends ATOMs withdrawal request.
   (a) Undelegate ATOMs.
   (b) wATOMs are transferred to Supernova through IBC.
   (c) Related ACK is returned.
4. The user withdraws wATOMs.
   (a) Supernova transfers wATOMs to the user.

The maximum waiting time of the user is the sum of the batch period and undelegation period. For Cosmos, it is $3 + 21 = 24$ days. It can be calculated as $\min(B + U) = \min(B) + U = B' + U = \lceil U/M \rceil + U$.

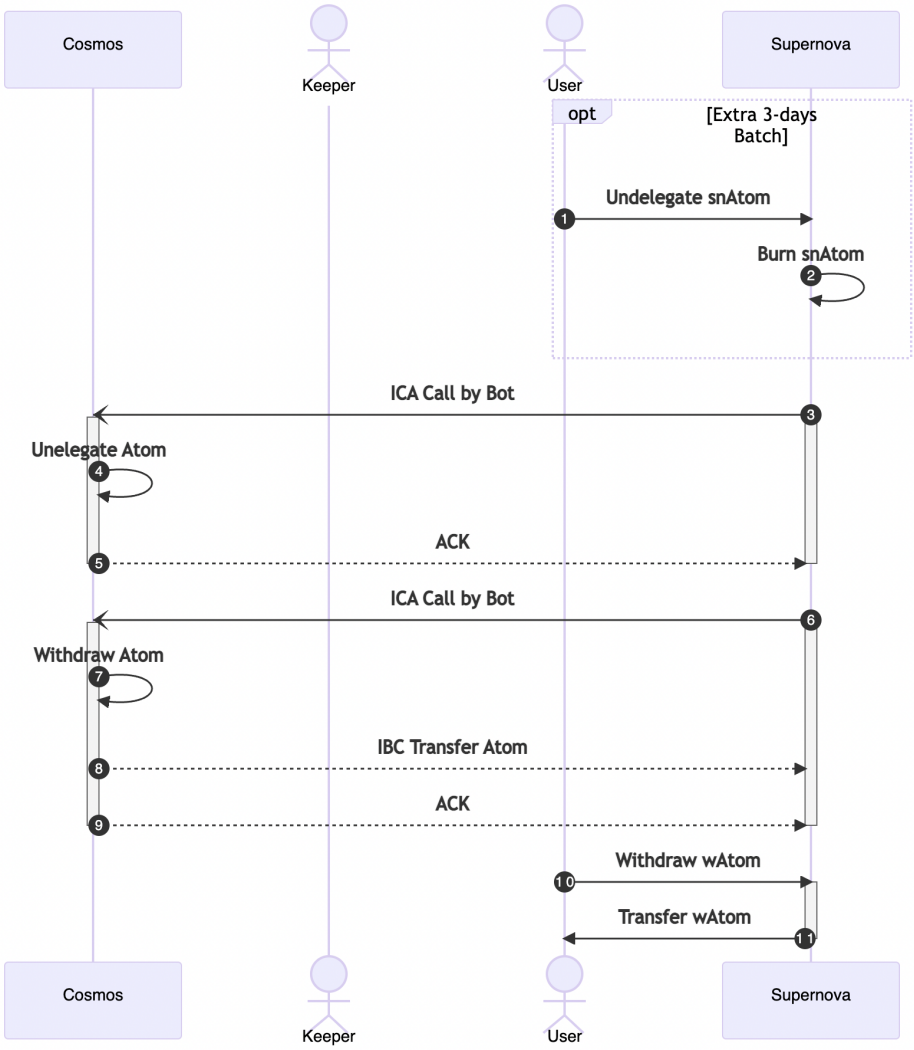

Fig. 2. Burning of snATOMs to undelegate and withdraw wATOMs after the undelegation period.

3.3 Swap

Swap allows snAssets to be swapped with wAssets immediately without going through the lockup period. Also, liquidity providers can earn fees from swaps—one of the use cases of snAssets.

Stable Swap Supernova has a stable swap with the variable 'A' initially set to 1 to operate like CPMM but adjustable.

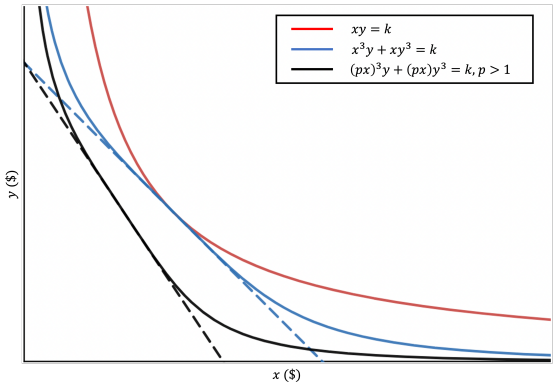

Fig. 3. Uniswap ($xy = k$), simple stable swap ($x^3y + xy^3 = k$), and example of staked swap ($(px)^3y + (px)y^3 = k$, $p > 1$). The dotted line indicates the slope the curve pursues.

However, shadow tokens do not have the same value as original tokens because:

- Being able to skip undelegation period via swap
- Related DeFi (collateral et al.)
- Supernova's credibility

Therefore, using a stable swap curve that follows $x+y = k$ between staked Assets and original ones is not suitable. The pool will leverage the CPMM method for the time being, but it will be updated to use the Staked Swap method that is currently under development.

Staked Swap snAssets generate interest and increase in value due to the auto-compounding feature. This means that the value of snAsset will continue to rise. Therefore, an appropriate AMM that reflects the characteristics of snAsset is needed. The stable swap is unsuitable when the value of a variable in a given pair continues to rise.

Although the value of snAsset may decrease due to events such as slashing, it is not something that happens if not in an extreme situation. Therefore, we shall only discuss cases where the value of snAssets increases throughout this paper.

Mispricing from Appreciation To take a concrete example, we consider the most stable case of a swap situation, $x + y = k$ where $(x, y > 0)$, that the curves of the stable swap aspire to follow. If the ratio of $x : y$ is $1 : 1$ as $x = 5000000$, $y = 5000000$, and $k = 10000000$; you can receive $100y$s with $100x$s.

If $x : y$ changes into $1.1 : 1$, you will expect to receive $110y$s but will actually receive $100y$s since the equation is $x + y = k$. Even if the pool ratio changes

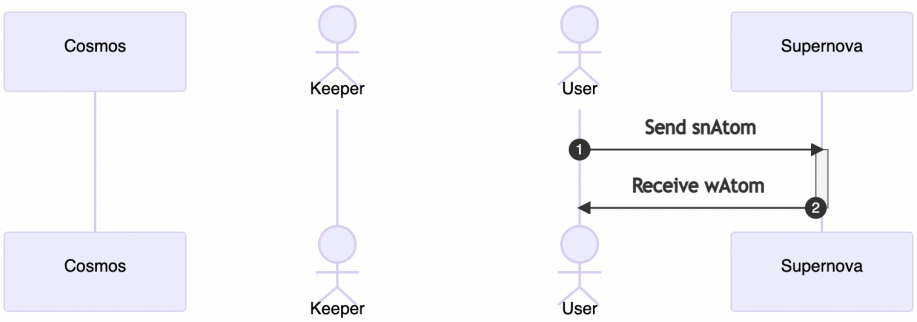

Fig. 4. Send snATOMs and receive wATOMs via swap.

to meet $1.1:1$ at the same $k = 10000000$, approximately $x = 4761904.762$ and $y = 5238095.238$; you can still receive $100y$s with $100x$s, not $110y$s.

We defined this loss as 'Mispricing from Appreciation'. In this example, Mispricing from Appreciation is $10y$s.

Curve with an Adjustable Slope Mispricing from Appreciation occurs because the slope of the Stable Swap curve is fixed at 1. Changing the slope of the stable swap is necessary to deal with mispricing.

Fortunately, depending on the interest rate and frequency of compounding, the increase in snAsset value p can be roughly calculated as $p = (1 + r/n)^n t$.

Table 1. The notations used to calculate the curve of the staked swap

Notation	Description
p	slope of the curve
r	interest rate (inflation rate)
n	number of times interest applied per time period
t	number of time periods elapsed

Therefore we can use px instead of x in the stable swap, and p can be adjusted to solve the Mispricing from Appreciation. Figure 3 shows the difference between the curves of Uniswap, Stable Swap, and Staked Swap. The slope of Staked Swap can be adjusted through p.

Swap on Supernova Figure 4 shows the process of swapping snATOM to ATOM. Staked assets can be immediately unwrapped without waiting throughout the lock-up period.

1. Send snATOMs to swap.
2. Receive a calculated amount of wATOMs according to the curve.

The swap was implemented through CosmWasm smart contract on Supernova. Therefore, the swap can actively communicate with other user-developed contracts, such as a router, aggregator, etc.

3.4 Auto Compounding

Robustness Some protocol functionality should stay persistent to provide security and user convenience, even in abnormal situations such as Supernova updates, bot malfunctions, or IBC/ICA disconnection. For example, periodic compounding from the relative chain is recommended to maximize profit, regardless of the status of Supernova.

Definition of Robustness In a service where two or more chains are interconnected, the protocol is defined as not robust if the entire protocol is stopped due to the malfunctions of one chain. Conversely, the protocol is defined as robust if the entire protocol is not stopped and provides some functionality even when one or more chains are exposed to issues and halts.

Robustness of Supernova Auto Compounding Compensation for ATOM in Supernova can be performed in two ways: The first one is to request compounding via ICA Call from Supernova. The second method is to request compounding directly from Gaia's account, which is authorized through Authz. The latter can perform compounding regardless of the operation of Supernova, even if the chain stops. Therefore, we can say auto-compounding of Supernova is robust.

Request from Supernova Figure 5 shows the compounding and oracle update process that starts from Supernova:

1. Bot makes the ICA call to trigger compounding.
   (a) Withdraw and immediately delegate rewards.
   (b) Related ACK is returned.
2. Bot updates oracle.

Request from Cosmos Figure 6 shows the compounding and oracle update process that starts from Gaia:

1. Keeper, which is a multisig or DAO account, requests compounding.
   (a) Withdraw and immediately delegate rewards.
2. Bot updates oracle.

The two compounding-related processes are much alike, but they do have differences. In Figure 6, Gaia is the starting point of the compounding and where withdrawal and re-deposit rewards are made. Therefore, Supernova's compounding feature is robust because it is an independent operation that is unaffected by other blockchains.

Because compounding changes the amount of staking assets, it is recommended to update Oracle to accurately reflect the snAsset value of Supernova.

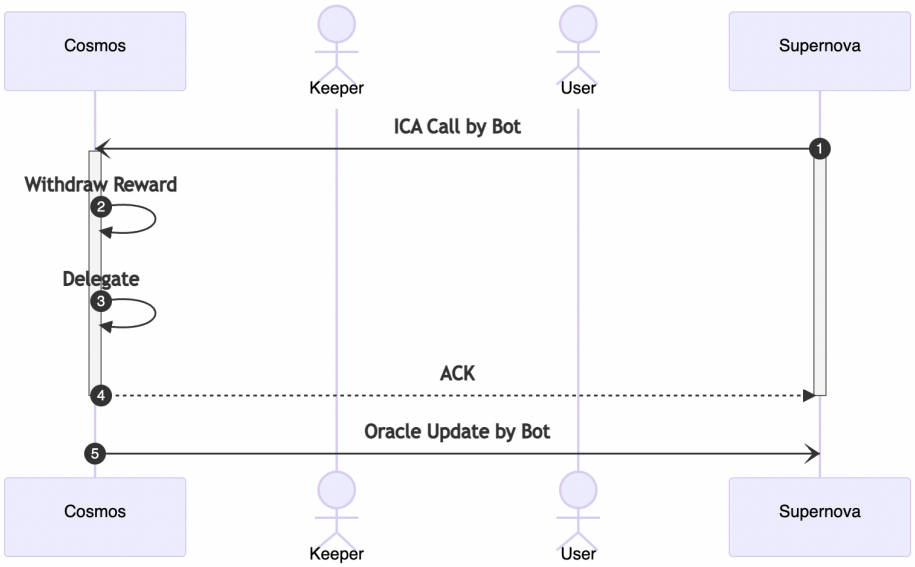

Fig. 5. Request compounding through ICA from Supernova.

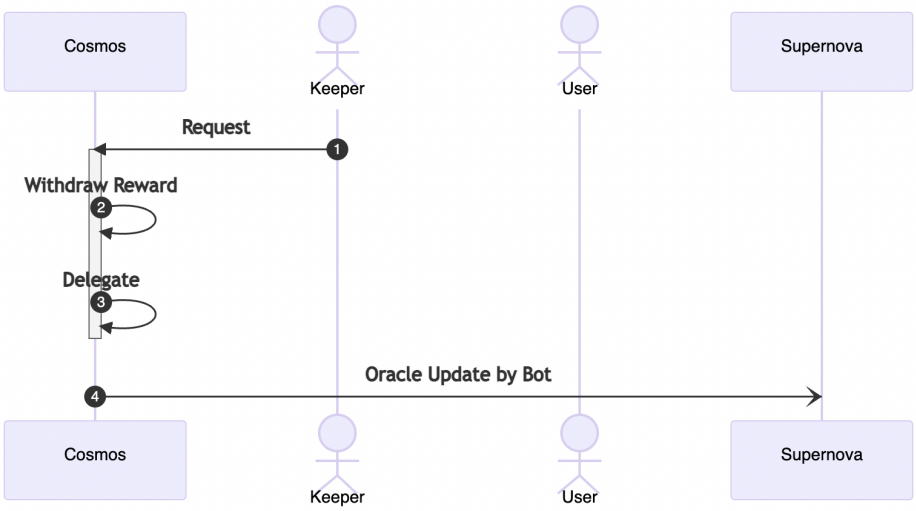

Fig. 6. Request compounding from Gaia, the Cosmos hub.

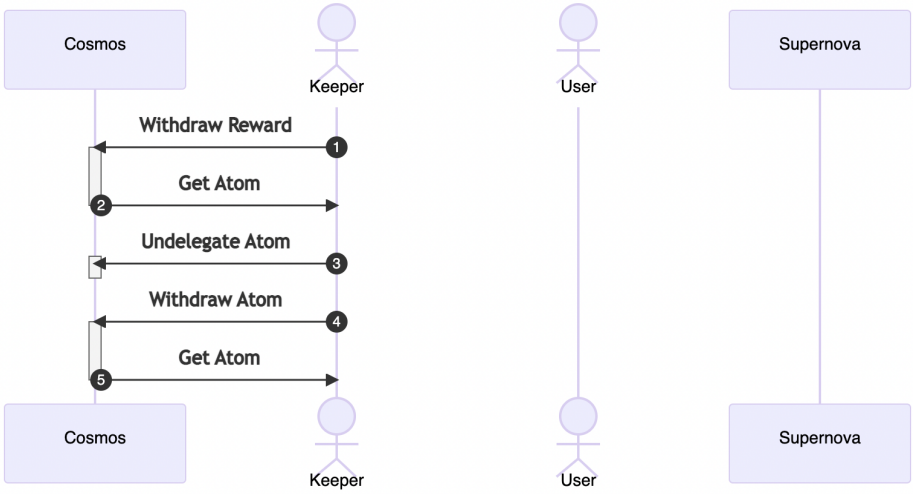

Fig. 7. The keeper can withdraw staked assets and rewards in case of emergencies.

3.5 Emergency Withdraw

Robustness of Supernova Staked Assets Just as compounding is robust because it has independence from Supernova, each staked asset minted as snAsset is robust because it can be withdrawn even if Supernova is disrupted. Users who delegate and liquidate assets through Supernova are guaranteed a safe withdrawal of their original assets regardless of Supernova's status.

In case of an emergency, rewards and assets can be withdrawn from the Gaia account authorized through Authz.

Emergency Withdraw on Supernova Figure 7 shows the process of emergency withdrawal. In this example, the keeper withdraws both the staked Atoms and the yield that is generated which functions as follows:

1. The keeper requests the withdrawal of all assets.
   (a) Withdraw rewards.
   (b) Request to undelegate staked ATOMs.
2. After the undelegation period, the keeper sends a transaction to withdraw ATOMs.

4 Applications

4.1 Stable Coin

Since most tokens are volatile, stablecoin, whose value is pegged with fiat USD, is required for various financial positions and risk management. Generally, a stablecoin is recognized as a financial infrastructure of the blockchain ecosystem.

Stablecoins are largely divided into two categories by the minting process, collateralized and algorithmic. The former is recognized as more secure and safe. What is pointed out as a shortcoming of overcollateralized stablecoin is that the capital efficiency is relatively low. However, issuing stablecoins based on shadow tokens can partly solve the capital efficiency problem because shadow tokens themselves unlock the liquidity of the staked tokens which would have been locked-up otherwise.

4.2 Governance Aggregating Platform

Since Supernova has a single validator on each app-chains, the Supernova validator itself has voting power. Supernova will act as a governance aggregating and bribe platform on Cosmos to decentralize the governance and reflect the will of the community.

We will deploy a bot that subscribes to all the proposals submitted to each app-chains and submit the proposals on the Supernova governance, a customized governance module that will handle the process.

Holders of the NOVAs will have the power to vote on the proposals until 24 hours before the vote on the original chain closes. This rule was made since the voting period varies depending on the platform. For instance, Gaia has a 14-day voting period, while Osmosis has a 5-day.

5 Discussion

5.1 Risks and Mitigations

Price of snAsset If the price depeg between snAssets and wAssets increases, it will inevitably be traded with slippage that users cannot afford. It can be solved with sufficient liquidity or arbitrage, but it can be mitigated fundamentally through the Staked Swap.

Bots Many bots run on Supernova, such as oracle feeders and compounding bots; however, it has no risk even if the bot unexpectedly stops. Thanks to features like Lazy Minting, auto-compounding, and emergency withdrawal through Authz, users will not be exposed to losses even if the bot stops working.

5.2 Future Work

IBC Query The IBC query allows sending queries to the other chain to receive a response with proofs. Through this, required information such as the quantity of staked assets by a specific verifier can be collected without harming the degree of decentralization. Research on IBC queries is also underway, and once the module is developed, it will replace Supernova's oracle bot and distribute its role to relayers.

Liquid Staking Module Liquid Staking Module is a module that issues vouchers for staked assets and allows utilizing them. Through Liquid Staking Module, users can easily mint shadow tokens of staked assets, such as those delegated to different verifiers. Integrating this module is expected to massively expand the ecosystem of Supernova, which is aimed to become the ultimate platform for staked assets.

6 Conclusion

We developed a novel platform for staked assets called Supernova. Supernova provides the liquid staking service that provides shadow tokens with strong utility from the get-go. Through this, it can contribute to the security of the Cosmos ecosystem and become a powerful instrument in Cosmos DeFi.

To provide a fair and robust liquidity solution, Supernova proposed several features. We propose Lazy Minting to address the vulnerabilities from unfairness due to asynchronous oracle feeding that incumbent liquid services have. To resolve the limit of withdrawals, we proposed Batch Withdraw so that withdrawals from the protocol are not delayed. To solve the withdrawal limit, we proposed a Batch Withdraw feature that prevents any delays in protocol withdrawal. In addition, we are developing solutions to mitigate possible mispricing problems in the swap. The compounding and emergency withdrawal functions will be provided to add robustness to Supernova through Authz.

Several attractive DeFi solutions are possible using yield-bearing liquidated assets through Supernova. It is possible to provide a stablecoin with snAssets as collateral. It also functions as a bribe platform for governance of other connected blockchains through NOVA, a native asset of Supernova.

With the emergence of IBC query and Liquid Staking Modules, Supernova is expected to become more decentralized and robust by integrating them.

References

1. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.
2. Kwon, Jae, and Ethan Buchman. "Cosmos whitepaper." A Netw. Distrib. Ledgers (2019).
3. Cosmwasm Homepage, https://cosmwasm.com. Last accessed November 18, 2022
4. Zhang, Yi, Xiaohong Chen, and Daejun Park. "Formal specification of constant product (xy= k) market maker model and implementation." White paper (2018).
5. Egorov, Michael. "StableSwap-efficient mechanism for Stablecoin liquidity." Retrieved Feb 24 (2019): 2021.
6. Lido Homepage, https://lido.fi. Last accessed November 18, 2022