Quicksilver Protocol, The Cosmos Liquid Staking Zone

Joe Bowman
CEO - Ingenuity

Vish Modali
CPO - Ingenuity

Roea Mortaki
COO - Ingenuity

28th February 2022

Abstract

Quicksilver Protocol is a permissionless, sovereign Cosmos SDK blockchain that allows delegators to stake assets against any validator running on any IBC-enabled chain and receive in turn a voucher representing a claim against that staked position. Existing liquid staking solutions often limit users to small validator sets, are governed by external entities, require the sacrifice of governance rights, and only support a single chain. Quicksilver Protocol provides Interchain Liquid Staking that is scalable to all validators on all IBC-connected chains while preserving users' governance rights. It maximizes liquidity and capital efficiency, while simultaneously improving network security and decentralization.

Introduction

In a proof-of-stake blockchain, asset holders wishing to stake their tokens in order to earn staking rewards are required to lock their capital. This locked capital, known as a delegation, acts as a slashable security deposit in the event that their chosen validator should misbehave.

Staking within the Cosmos ecosystem (and indeed most proof-of-stake protocols), comprises two parties: a validator and a delegator. The validator runs hardware and a Cosmos-SDK based blockchain application to propose and validate blocks on the chain, in consensus with others. In order to prevent misbehavior by validator operators, delegators put up capital in the form of the chain's native staking token by way of security deposit. In the event of misbehavior—accidental or malicious—some portion of the staked deposit, in the order of magnitude of 0.1% for persistent downtime and 5% for a double-signing violation (whereby the validator signs more than once for a given block height), is burned or "slashed" as punishment.

As recompense for providing this security deposit, delegators earn staking rewards proportional to the value of their staked assets for each block validated. Validators in turn charge a commission upon these rewards for providing the validator service.

In order to protect against certain classes of attack, whereby validators can commit offenses and either they themselves, or their delegators, are able to unbond their deposit before the misbehavior is reported, an unbonding period—usually of three weeks—is instituted.

As validators earn commission on block rewards proportional to the stake delegated to them, it is therefore in the validators' best interest to ensure they behave appropriately and efficiently in validating the chain.

At time of writing, the maximum amount that a user may be slashed for any infringement on most, if not all, Cosmos-SDK networks is five percent, leaving **95 percent of capital illiquid and unutilized**.

Effects of Illiquidity

Staking assets in this way is capital inefficient. At most, five percent of a delegator's assets are at work, protecting the network. However, 100% of their capital is locked up and illiquid. Asset holders are unable to simultaneously secure the network in which they have invested and participate in opportunities to leverage their assets to make a return in, for example, Osmosis Liquidity Pools, collateral in a Kava CDP, or other such DeFi products.

In cases where the return of such products is significantly greater than the return from staking and exceeds the penalty incurred by unstaking one's assets, it becomes a trivial decision for an asset holder to unbond their security deposit to better utilize their capital. In this case, we see delegators unbonding assets from securing the network in order to migrate them to other zones to seek better returns, thus having a net negative effect on network security.

This was evident in the change in the bonded supply of ATOM tokens delegated on the Cosmos Hub in June 2021, when the Osmosis zone, an IBC-connected AMM, was launched. Over 2.5% percent of the bonded stake, valued at $61.7m at the time, unbonded in the days following the Osmosis launch, causing a significant outflow of previously bonded capital from the Cosmos Hub, reducing the security by a material amount.

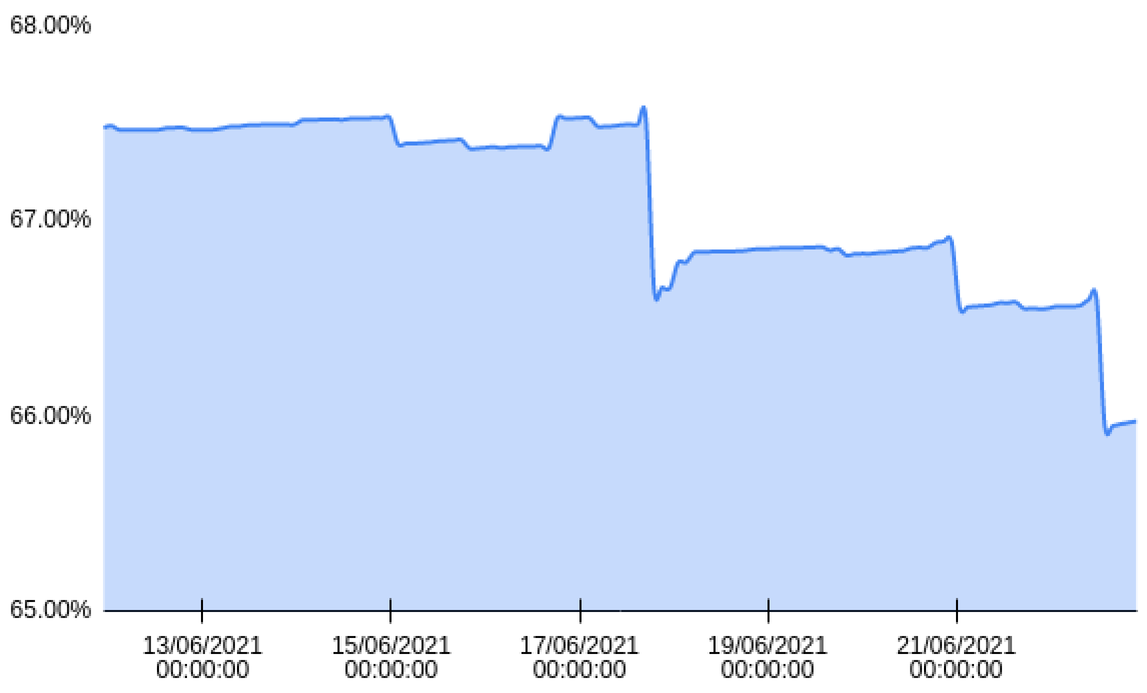

Figure 1. Cosmos Hub staked supply on and around Osmosis launch

Liquid Staking

Liquid staking, as a concept, is a mechanism in which these delegations are made liquid and can be transferred, traded, or otherwise utilized. Often this is implemented as a set of smart contracts, whereby the user deposits tokens in the smart contract and then some validators acting on behalf of the protocol are then delegated to by the smart contracts themselves.

A deeper insight into liquid staking can be gained by reading Chorus One's Liquid Staking Research Report, written in June 2020[1].

The goal of liquid staking is to allow delegators to maintain their staked position while simultaneously permitting them to seek out the best returns for their capital. This is achieved by minting an asset representative of the native bonded token at the point of delegation, which can then in turn be used by DeFi protocols.

The expectation with widespread adoption of liquid staking is that the bonded stake of a chain should converge upon some value near 100%, as the liquid version of the underlying token can be traded on markets in lieu of the native asset. As such, the security of the underlying zone reaches its theoretical maximum while maintaining a liquid supply.

However, the implementation of a protocol as a set of smart contracts is not without risk. A liquid staking protocol implemented this way is beholden to constraints placed upon it by the parent chain and its governance. The core developers and underlying chain will more often make decisions based upon its own requirements and benefits than that of protocols built on top of it.

Liquid Staking Module

The Liquid Staking Module (LSM) is implemented by Iqlusion[2], and will become a core Cosmos-SDK module. It enables delegators to tokenize their staked position without the need for unbonding. The tokenized positions, or 'shares', are non-fungible between validators and are limited in functionality to facilitate the transfer of bonded positions.

Protocols can utilize LSM in order to onboard existing delegators of a network onto the protocol without the need to unbond, and by extension, without the delegator losing rewards *nor* diminishing the security of the network. Shares are deposited with the protocol and the corresponding representative token is then minted.

Inter-Blockchain Communication

IBC is described by Goes (2020)[3], as "an end-to-end, connection-oriented, stateful protocol for reliable, ordered, and authenticated communication between modules on separate distributed ledgers".

It consists of two layers: the transport layer, whose role is to establish and manage connections and handle authentication of data packets flowing between endpoints, and the application layer, which defines how these packets should be interpreted and handled by the receiving end.

IBC is a trustless bridge protocol that utilizes light clients, and cryptographic proofs to ensure that the bridge has the same trust assumptions as the zones it bridges. This differs significantly from oracle- or witness-based bridges, which rely on a small number of trusted parties to verify that an event has taken place.

The protocol also describes the role of relayers, whose responsibility it is to listen to events emitted by one side of the connection and pass these as transactions to the receiving blockchain.

Interchain Accounts

The application-level IBC protocol known as Interchain Accounts (ICS27) allows for accounts on network A to be controlled by network B.

It consists of the concepts of Controller chain and Host chain. The Controller chain is able to register an account on the Host chain by way of opening a dedicated IBC channel between the two chains.

The Controller chain is able to compose transactions for execution on the Host chain on behalf of the Interchain account, encapsulate them in an IBC packet, and send them over the dedicated channel. The transaction is relayed to the Host chain, unencapsulated, and executed as if it were a local transaction.

Interchain Security

Interchain Security is an IBC protocol that allows the leasing of security from an established validator set. It enables a new zone without a mature validator set of it's own to have the same security parameters as the zone from which it has leased security.

Rennekamp (2021)[4] describes how the Cosmos Hub as a 'provider chain' would share it's validator set with a 'consumer chain', and produce blocks on its behalf. Provider chain validators run both the provider and consumer chain binaries, and the validator set updates that are traditionally emitted by the Cosmos-SDK to Tendermint every block, come from the provider chain over IBC instead. The consumer chain pays the provider chain's validators in its native, token as compensation for the security provided.

The benefit of such a system is that early stage zones, or those providing an ecosystem-wide good, are able to benefit from the security provided by the nearly $9bn ATOM market cap or other zones of substantial value. In the context of Quicksilver, it means that the Cosmos Hub validator set's staked supply is able to maintain a higher value than the assets controlled by the Quicksilver zone, something that would be otherwise difficult to ensure in the early days post-genesis.

Interchain Security v3 will allow consumer chains to supplement the provider chain validator set with their own validators, allowing the consumer chain to become less reliant on the Cosmos Hub over time as its own market cap grows, and enables the use of the consumer chain's native token for staking, rather than simply payment for security.

Quicksilver Protocol

The Quicksilver Protocol is able to increase capital efficiency by delegating tokens on behalf of users, and in turn minting a tokenized representation of the user's delegation, herein referred to as a `qAsset`. The `qAsset` takes the form of the onboarded zone's native asset prefixed with `q`, for example `qAtom` or `qOsmo`. `qAssets` are themselves liquid, fungible, and may be freely transferred away from the Quicksilver zone to be utilized in some other protocol (as collateral, liquidity, or traded on a decentralized exchange). The value of the `qAsset` is that of the original bonded asset, plus any staking rewards earned since minting, minus perceived slashing and protocol risk. As such, the pricing of the `qAsset` can be expected to increase in value over time relative to the original bonded asset, as risk remains largely constant and rewards increase over time.

Architecture

The Quicksilver protocol is implemented as a sovereign Cosmos-SDK chain. Quicksilver specific functionality is added by way of custom modules.

The primary functionality of Quicksilver is to enable delegators to move their delegations on a remote chain X, such that it is controlled by the Quicksilver Protocol, and in return, issue `qAsset` tokens that represent that position. The `qAsset` tokens constitute the user's claim to their original native assets, and must be burned at the point of redemption.

The `interchainstaking` module, for each onboarded chain, will generate and control a deposit account, as well as a number of delegation buckets by way of the Interchain Accounts IBC module.

The purpose of the deposit account is to receive the transfer of tokenized delegation shares (delegated positions that have been tokenized using the liquid staking module). Upon receipt of a transfer into the deposit account, the corresponding address on the Quicksilver chain will be credited with the appropriate `qAsset` to the value of the transferred delegation shares.

The delegation shares are then transferred to one or more delegation buckets and redeemed back into a native delegated position so that the Quicksilver protocol becomes the recipient of the rewards pertaining to said delegation.

At the end of each Epoch (3 days), each delegation bucket will redeem the rewards it has accrued and restake them. As such, at each epoch, the redemption rate for the `Asset:qAsset` pair will be adjusted to include the new rewards.

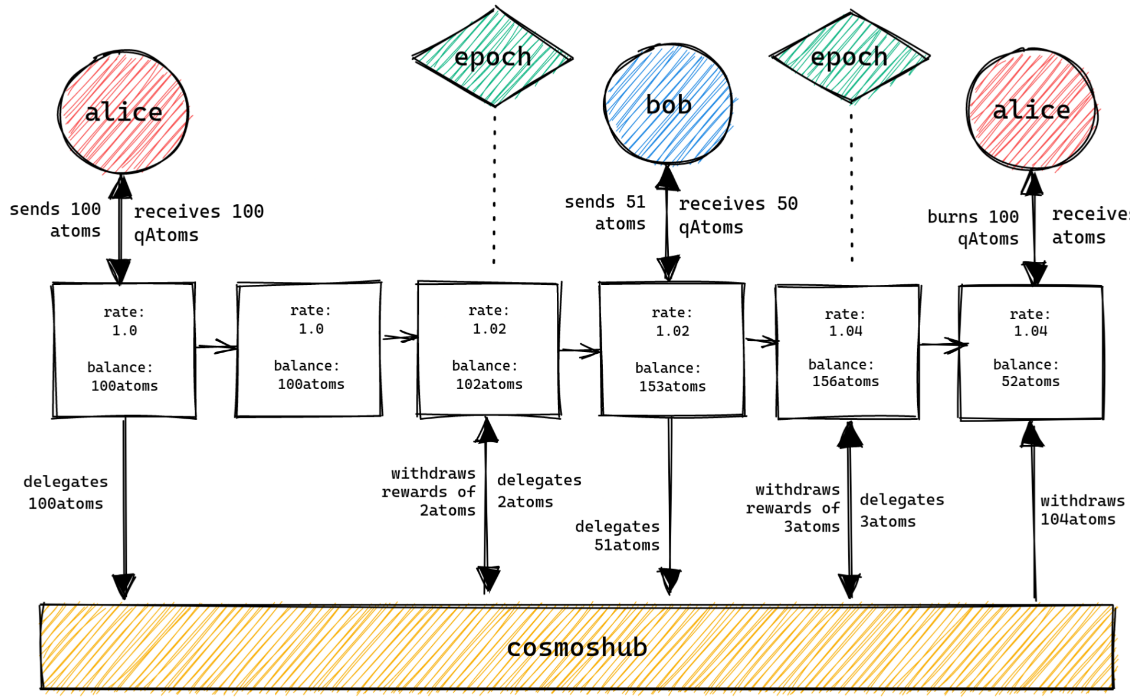

Figure 2. Simplified example of Delegation/Undelegation/Epoch lifecycle in Quicksilver

Additionally, each epoch will trigger a rebalance of funds among delegation buckets to ensure that a) delegators' wishes are appropriately represented on chain (see 'Signalling Intent' below) and b) the value of each delegation bucket is similar (to within some threshold) to facilitate proxy governance.

When a request for redemption is made by the user sending a `MsgRequestRedemption` transaction on-chain, a request is sent to the appropriate delegation bucket accounts to tokenize the corresponding number of shares (calculated as `qAsset` tokens / `Asset:qAsset` rate) and transfer these to the delegator's account on the remote chain.

The individual user workflows are covered in more detail below.

Reward Socialization

Given that validators are free to choose their own commission rates, a delegation to validator A does not provide the same rewards over period T as an equal delegation to validator B. In order to ensure fungibility between validators, we must be able to treat all delegations as equal. In order to achieve this, we must socialize rewards such that all `qAsset` holders will receive the same `Asset` rewards (that is, the collective `Asset/qAsset` redemption rate will increase) as one other, regardless of the validators with whom they choose to delegate.

However, we do look to delegators to signal the validator with whom their portion of the managed `Assets` should be delegated. Quicksilver should not determine which validators receive what percentage of delegations via the Quicksilver protocol; this should be directed by users as if they were delegating directly.

Signalling Intent

When a delegator first transfers their delegation to Quicksilver, the makeup of the transferred delegation will form their 'signal'. This signal can be changed at any point to reflect the user's desire to redelegate by submitting a MsgSignalIntent transaction on chain.

Epochly, the aggregate intent of all qAsset holders for a given chain will be calculated and used to determine how the delegations controlled by Quicksilver should be rebalanced. Given limitations in concurrent redelegations, this action is *eventually consistent*, meaning that over some period of time (up to 21 days), delegations will be moved to converge upon the aggregate intent.

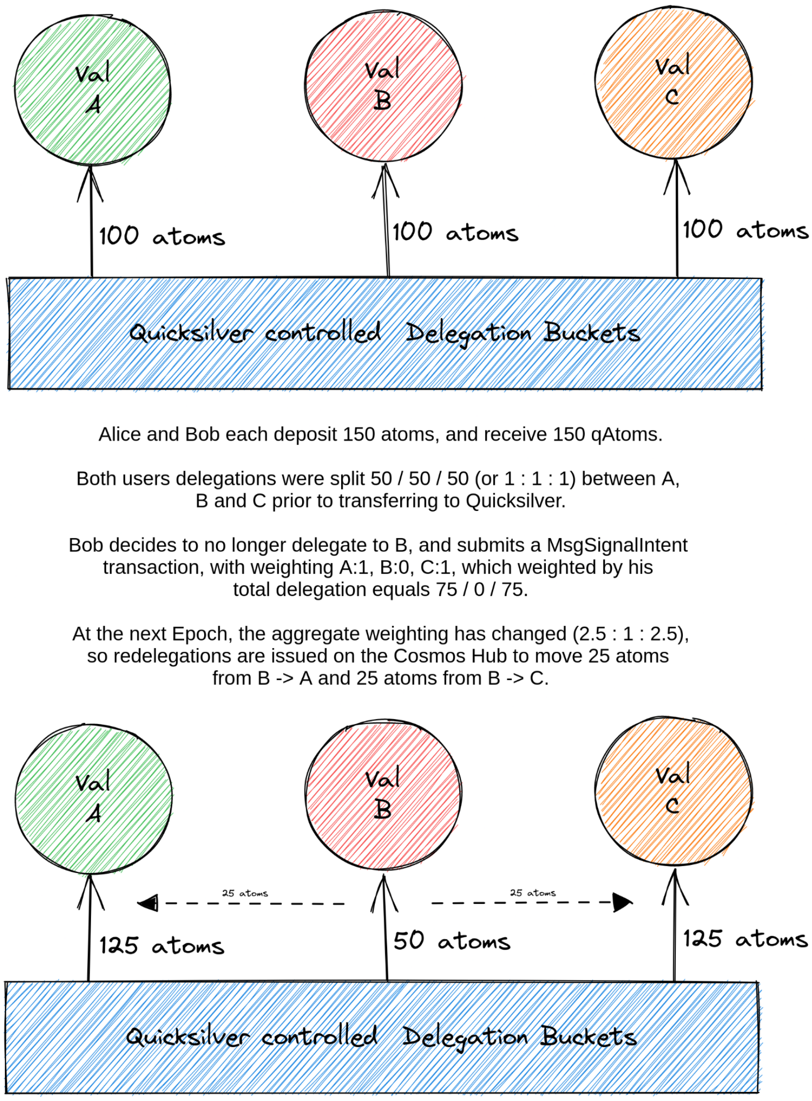

Figure 3. Simplified example of intent signalling in Quicksilver

Participation Rewards

Each epoch (based upon the signal submitted), a `qAsset` holder will receive a portion of the `QCK` inflation emissions as an incentive for making 'positive' delegation choices—that is signalling intent for performant (based upon rewards earned by the validator) and decentralized validators and those participating in governance.

Risk Socialization and Slashing

Similar to Reward Socialization above, given that validators are independent, run different hardware and software configurations and are run by different teams with different experience and priorities, the risk profile of each validator is different. In order to maintain fungibility, this risk must also be socialized. A slashing event for one `Asset` validator is therefore borne by all `qAsset` holders through a negative movement in the `Asset:qAsset` redemption rate. Given sufficient decentralization across validators, slashing events are hedged against. The outcome of such a double-sign slash (5%) for an average (1% of managed supply) validator, will lead to a 0.05% reduction in the redemption rate; similarly, the same validator being jailed for downtime (0.1%) will lead to a 0.001% reduction in the rate.

When a validator is tombstoned for a double-sign infraction, the protocol will, insofar as redelegation limitations permit, move the delegation to the validator that replaces it in the active validator set.

Governance by Proxy

Another important feature of Quicksilver is the ability for `qAsset` holders to continue to exercise their governance rights as if they were delegating natively. The Quicksilver protocol will monitor governance proposals submitted on connected chains and mirror the vote on the Quicksilver zone to permit `qAsset` holders to submit their vote. Voting on Quicksilver ends some period prior to the completion of the voting period on the target zone, and Quicksilver will submit transactions to mirror the intent of the qAsset holders on behalf of the delegation buckets. This allows the protocol to confer governance rights to users to within a small percentage of the cast vote. Users that do not vote will approximately inherit the vote of their signalled validators.

Unrestricted Validator Sets

The default position of the Quicksilver protocol will be to enable delegators to delegate to any of the validators in their target chain as if they were doing so natively. This is a departure from the norm within existing liquid staking protocols, but we believe that the liquid staking protocols should not determine which validators are able to inherit an unnatural proportion of voting power in a given zone. We hope this will lead to better distribution of voting power across all validators of a chain.

However, `QCK` token holders are able, by means of a governance proposal, to deny specific validators a place on the list; for example, if they choose to remove validators run by centralized exchanges or those demonstrating behavior considered harmful to the network, they are able to do so.

Quicksilver (`QCK`) Token

Roles

The Quicksilver native token, with the ticker `QCK`, has three specific roles:

Governance

Governance is a critical component of the Quicksilver network. Onboarding of new zones and corresponding incentivisation, spending of community controlled funds, changing of network parameters and control of the upgrade process are all events handled by the governance process. `QCK` token holders are able to use their assets to vote on behalf of the protocol.

Security

Initially, it is intended that Quicksilver utilizes Interchain Security, an IBC module that facilitates the 'leasing' of security from a well established validator set. In this instance, the `QCK` token will be used as payment to that validator set for the provision of security. As soon as Interchain Security development permits, it is the intention of the Quicksilver protocol to supplement this with our own validator set. At this point, the `QCK` token will become the staking token of the Quicksilver protocol, and be used to secure the network.

Fee Payment

Additionally, the QCK token is used to pay fees for transactions submitted to the network. These fees are paid to block producers on the network as compensation for ensuring a transaction is included in a block.

Network Onboarding and Airdrops

Network onboarding is controlled by governance of the Quicksilver zone. `QCK` token holders may submit a transaction in order to trigger a governance vote to onboard a zone—the governance proposal transaction contains all information required to connect to the new zone.

In order to facilitate onboarding the users of a new zone, the Quicksilver protocol will conduct on-chain airdrops for onboarded zones. Over 50% of the genesis supply of `QCK` and 30% of inflation (at genesis) will be directed to an Incentivization pool. A new mechanism is being designed such that through the same governance process, a snapshot of accounts can be provided for a new onboarded zone and those accounts will then be able to claim some portion of that pool.

Users will be required to use the protocol to unlock their full rewards, and rewards not claimed within some time period will be reclaimed by the protocol and credited back to the Incentives pool for future use. The Incentives pool may also be used, at the behest of the zone governance, to provide liquidity incentives for qAsset pairs on DEXs.

Inflation schedule

The `QCK` token will experience yearly inflation until it reaches a maximum supply of 1 billion. The token will be highly inflationary in the beginning to incentivize early usage and reward early adopters of the protocol. Inflation in the first year will be 100% (200 million tokens emitted), and then the inflation rate drops by 25% every year. As such, 95% of all QCK will be in supply by year 7, and 99% will have been emitted by year 15.

The newly minted tokens would be allocated in the following areas, at genesis:

Figure 4. Split of inflation emissions in Quicksilver

- 30% emitted as Staking Rewards to reward validators and their delegators for securing the Quicksilver network.
- 30% to the Incentive Pool for ongoing incentives to new users and liquidity providers.
- 30% would be distributed as Participation Rewards to users on an epochly basis for using the Quicksilver Protocol.
- 10% to the community pool controlled by governance, to be spent on projects benefiting the Quicksilver community.

This allocation can be changed at the discretion of the `QCK` token holders through a governance proposal.

Genesis Token Allocation

The initial token allocation of the Quicksilver native token, `QCK`, will be 200 million. This will be allocated as follows:

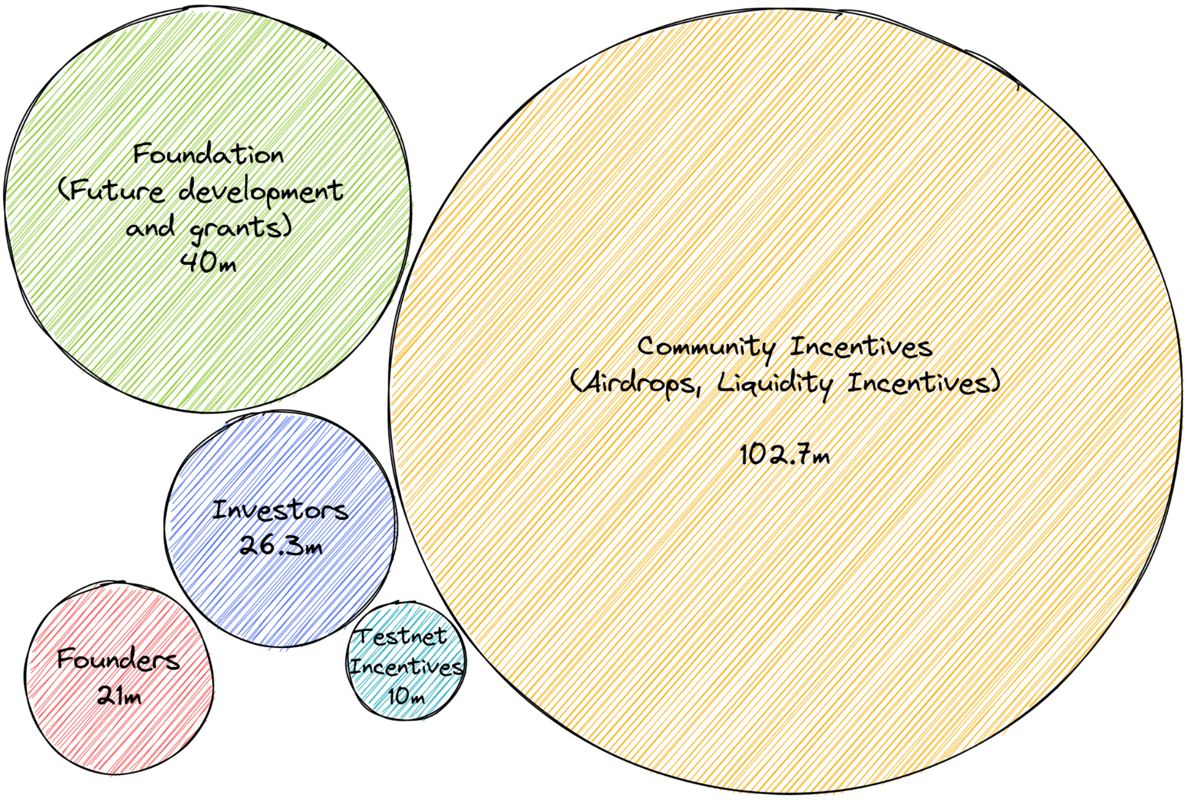

Figure 4. Genesis token allocation in Quicksilver

Allocation	Tokens	Percentage	Vesting
Founders and Core Developers	21m	10.5%	Schedule 1
Investors	26.3m	13.15%	Schedule 1
Testnet Incentives	10m	5%	Schedule 2
Community Pool - Grants and Future Development	40m	20%	No vesting - Governance controlled
Incentives Pool	102.7m	51.35%	No vesting - Governance controlled

Figure 5. Genesis token allocation and vesting information in Quicksilver

Vesting Schedules

Schedule 1: 20% liquid at genesis plus 10% every 6 months over 4 years

Schedule 2: 20% liquid at genesis plus 10% every 3 months over 2 years

User Flows

Delegation Flow

In order to delegate via Quicksilver protocol, the delegator must send either unbonded `Assets`, or in the case they are already bonded, delegation 'shares' as emitted by the Liquid Staking Module, to the Quicksilver deposit account. This address can be retrieved from the Quicksilver API at any time.

The Quicksilver zone witnesses the deposit event and immediately mints the corresponding number of `qAssets` and sends to the account represented by the same public key on the Quicksilver zone.

Asynchronously, the Quicksilver protocol will distribute the shares, or liquid atoms, from the deposit account to a number of 'delegation buckets', each an ICA-controlled account, managed by the Quicksilver chain. Any 'shares' are reconstituted into the native token delegation.

Undelegation Flow

In order to reverse the flow and exit the protocol, the user submits a `MsgRequestRedemption` transaction to the Quicksilver chain, specifying the number of `qAssets` they wish to redeem, and which account on the destination chain they wish to credit.

Quicksilver will burn the user's `qAssets` and determine which delegation buckets will Tokenize their delegations, sending the appropriate transactions via IBC to the target chain to do so, and to send those tokenized shares to the destination address. The user will receive native assets (delegated), to the value of the `qAssets` burned multiplied by the current redemption rate for that asset pair.

Long Term Vision

The initial product roadmap has support for all the items listed above, however the long-term plan looks beyond the Cosmos ecosystem. IBC is not a Cosmos-specific protocol, and there are already a number of non-Cosmos, and indeed non-Tendermint, projects looking at integrating IBC into their stack. Once chains are IBC-connected and implement the Interchain account (ICS27), they will be ripe for onboarding to Quicksilver.

In addition, the advent of `qAssets` on the Quicksilver chain opens up interesting avenues of research and experimentation for future development of on-chain DeFi protocols. It is envisioned that the base `qAssets` become a key part of DeFi in the Cosmos ecosystem, providing significant additional liquidity to these protocols that is currently locked in staking.

Summary

In conclusion, it is clear that liquid staking is critical for the health of the staking paradigm, in a world where better returns are available for an asset holder outside of delegation. In light of this, the Quicksilver protocol aims to become the liquid staking solution for the Cosmos ecosystem, and over time, the wider Interchain. Specific focus has been spent on ensuring the protocol incentivizes decentralization, and on developing a solution that allows users to maintain governance rights. The token allocation and inflation emission schedule has been designed such that the Quicksilver zone's native `QCK` token ends up in the hands of Cosmos ecosystem participants and protocol users, not VCs, funds, and entities based outside of the ecosystem; and as such, the protocol will be governed by those parties that have a vested interest in ensuring the Cosmos ecosystem grows stronger a result.

A new 'post-genesis' airdrop module is being developed to support future airdrops so that the protocol can continue to support new zones that launch and are subsequently onboarded, post-genesis.

References:

1. Liquid Staking Research Report. Chorus One, 2020: https://mirror.chorus.one/liquid-staking-report.pdf

2. Liquidity Stake Module. Iqlusion Inc., 2021: https://github.com/iqlusioninc/liquidity-staking-module

3. Interchain Security is coming to the Cosmos Hub. Rennekamp B, 2021: https://blog.cosmos.network/interchain-security-is-coming-to-the-cosmos-hub-f144c45fb035

4. The Interblockchain Communication Protocol: An Overview. Goes C, 2020: https://media.githubusercontent.com/media/cosmos/ibc/old/papers/2020-05/build/paper.pdf