Quasar: A Protocol for Interchain Asset Management

March 2023

Abstract

The Quasar protocol is an application-specific proof-of-stake blockchain for decentralized asset management combining expert and community-led decision-making and designed to interoperate with a broad network of independent blockchains. Quasar uses efficient architecture to provide templates for multi-party smart contracts capable of aggregating assets from multiple discrete blockchains. We call these vaults. Vaults can adaptively employ what we simply call "strategies" — composable financial strategies designating how capital is deployed. By joining a vault, users 1) subscribe to the vault's active strategy to deploy their assets in a non-custodial and automated manner, and 2) can participate in vault-specific governance to select strategies.

Vaults and strategies use the Inter-Blockchain Communication Protocol (IBC) to interact with independent blockchains, enabling interchain asset transfers and strategy execution. Quasar's infrastructure allows integration with exchanges, automated market makers, lending/borrowing platforms, and other asset management protocols. Some applications for Quasar may include social trading, generating exchange-traded funds (ETFs) or custom indexes, and digital hedge funds.

Introduction

Decentralized finance (DeFi) has introduced a paradigm shift in financial markets. Traditional financial instruments are being emulated and augmented using blockchain technology, and, though still relatively young, the decentralized exchange (DEX) sector has seen tremendous growth. Total value locked (TVL) in decentralized exchanges has grown from $600 million USD in 2020 to roughly $40 billion USD at the start of 2023[1].

With a multitude of crypto assets emerging in the DeFi economy alongside newly efficient means of investment and trade, the importance of decentralized asset management is rapidly growing. Notably, asset management protocols have demonstrated business models with the potential for high revenue quality and strong pricing power[2]. However, many who could be benefitting from these new opportunities are not.

Quasar is addressing the need for accessible, decentralized, and equitable asset management for the emerging multi-blockchain economy. Current decentralized applications in this domain lack a dedicated

cross-chain infrastructure for managing baskets of assets across multiple blockchains. Further, existing decentralized asset management applications have been constrained by the policies of their governing Layer 1 protocol. Examples such as Set Protocol (allows amalgamations of tokenized assets to be converted into ERC-20 tokens, transforming them into tradable derivatives), STFX (a marketplace for custom and shareable trading ideas), dHedge (a platform for discovering strategies and investment managers), and Yearn (automatically switches deposited assets across multiple DeFi projects to optimize yield generation) are all confined within a single Layer 1 protocol.

Quasar is built as an application-specific blockchain for decentralized asset management with vaults. By making use of infrastructure solutions that are inherently dynamic, Quasar's infrastructure can provide value in a wide variety of contexts now and into the future. Quasar has also broken new ground by contributing significantly to the development of key components of the shared interchain infrastructure of IBC that enables our services across a constellation of diverse blockchains.

Challenges for Asset Management in Multi-Chain DeFi

Quasar focuses on solving two key challenges for decentralized asset management in the current and evolving DeFi landscape:

1) Crowdsourcing assets: creating a vehicle to crowdsource capital and connect liquidity providers with expert financial strategies, all while accommodating both community-led and professional management in a non-custodial, transparent, and permissionless way
2) Borderless asset deployment: activating infrastructure to deploy capital strategically across numerous, heterogenous, independent blockchains in a secure and trustless way

Connecting Crowdsourced Capital with Expert Strategies

Asset management in traditional finance is hindered by slow transactions and layers of permission needed for execution. While DeFi largely solves this, the availability of expert asset management in DeFi is still insufficient. Experts lack approachable tools to craft and carry out strategies, and non-technical users lack the proficiency needed to develop complex strategies. Both require a better UX to capitalize on the power of DeFi while saving time and money.

By connecting tools for strategy creation with vehicles for crowdsourcing capital, users can access financial strategies that might otherwise be unavailable to them, while experts can access the global capital made available by DeFi. The infrastructure that makes this possible needs to be highly

customizable, so that experts have the power to craft tailored strategies and non-experts have access to a variety of options to meet their asset management goals.

This infrastructure must also be secure, designed to avoid unnecessary risk, and employ mechanisms that cannot be maliciously exploited. It must also be transparent, giving users and strategists full access to available information needed to make informed financial decisions. It must be permissionless, allowing anyone with capital to provide liquidity and anyone with competency to lead strategies.

Lastly, our decentralized asset management infrastructure should be designed to maximize end-user self-custody. This constraint is practical and philosophical. Pragmatically, allowing users to move assets at will with minimal friction improves the velocity of assets and thus the efficiency of the market. Philosophically, Quasar aligns with core tenets of decentralized finance, aiming to minimize the risk of single points of failures induced by bad actors and emphasizing financial sovereignty.

Connecting Strategic Asset Management to Multi-Chain DeFi

Even with the tools and expertise for the execution of complex financial strategies, a lack of pathways for reliable and secure cross-chain communication means limited access to liquidity and limited access to diverse assets. Crypto assets exist as functions of their underlying blockchains. Without a good method of exchanging information across chains, dApps and protocols must be built on the same blockchain where the applications and assets they wish to engage with reside. This is the model of Ethereum, where a single blockchain hosts a wide array of assets and applications.

Increasingly, DeFi projects (and their assets) are establishing independent blockchains and moving to multi-chain ecosystems, such as Polkadot and Cosmos, that exist in contrast (but not necessarily in opposition) to the single-chain model of Ethereum. dYdX, a popular DEX emphasizing derivatives, recently moved in this direction[3] to take advantage of greater customizability and performance. Building independent blockchains is becoming easier and the benefits of app-specific blockchains are becoming clearer. For these reasons, we are bullish on a multi-chain (or if you prefer, interchain) future.

In this context, the importance of finding solutions for securely communicating across blockchains is magnified. Decentralized asset management infrastructure needs to be able to securely access a breadth of assets distributed across multiple blockchains, and existing cross-chain solutions are inadequate. Cross-chain bridge hacks[4] account for more than $2 billion USD of stolen cryptocurrency, with more than

$600 million USD stolen[5] at once from the Poly cross-chain network. Solutions that involve trusting a third party for communication should be treated with extreme caution.

Composability & Interoperability on an App-Specific Blockchain

Why does it make sense for Quasar to be a blockchain? A blockchain is a state machine capable of recording transactions and accumulating an immutable database of information. As such, it is well-suited for the fundamental operations of an asset management platform. But why should Quasar be an appchain, rather than a dApp atop an existing chain like Ethereum?

Appchains: Decentralization, Sovereignty, and Verifiability

A decentralized blockchain is executed and reproduced on multiple distributed computers via trustless consensus. It is not operated by a single entity and thus has no one point of failure or control. This helps make it secure and censorship-resistant; no single entity can alter the database to suit its own ends. Because all transactions remain recorded on an append-only ledger, information is also traceable. These properties are ideal for verifiable and transparent asset management. Accuracy of information is ensured, and all individuals — whether they are contributing security, liquidity, or strategies — can be vetted and held accountable.

A public (i.e. permissionless) blockchain is ideal for an equitable asset management platform, allowing access to an innovatively broad scope of liquidity providers and asset managers. Access to sophisticated asset management solutions should not be limited by net worth or geographical location.

Using trustless smart contracts to create blockchain applications enables asset management strategies to be implemented without the need for trusted third parties. This reduces costs, improves speed, and opens up new possibilities when compared to traditional financial solutions.

The model of a single general-purpose blockchain has its limits. Applications with their own dedicated blockchain typically enjoy faster transaction speeds and lower transaction costs, as there is no need to compete with a wide array of dApps for block space. A protocol with sovereignty over its own blockchain is freer and can be more dynamic in its design and decision-making — developers get access to the full stack of technology and can optimize it to the protocol's needs. As a result, appchains can be uniquely built to unlock specific features that would be difficult or impossible on a general-purpose blockchain. Importantly, chain-level governance decisions can focus entirely on the protocol's use cases rather than considering a myriad of dApps with varying demands.

Composable, Flexible, and Dynamic Infrastructure

Composability means components can be replicated, altered, and combined while retaining the capacity to interoperate with essential software components. Composable infrastructure can be used to create new outputs and use cases, an essential feature for the infrastructure of Quasar's vaults and strategies. Vaults and strategies are designed to be hyper-customizable and dynamic to enable unique and sophisticated decentralized asset management applications.

The appchain model involves a decoupling of the consensus/network layer from the application/execution layer, allowing for the modularization of chain functionality. With the Cosmos SDK, multiple interoperable modules handle binary-level processing while smart contracts handle virtual machine execution.

The Cosmos SDK is a generalized framework of specifications for a suite of modules used as components for building an appchain's application layer. The SDK emphasizes modularity and composability; components are designed to be interchangeable and customizable for various purposes. In alignment with this theme is Cosmos WebAssembly (CosmWasm), a library for building composable smart contracts that interoperate with the Cosmos SDK (CosmWasm can be implemented with the SDK's *wasm* module) to execute logic on or atop the blockchain.

Security is embedded into the application layer. The languages used by Cosmos SDK and CosmWasm — Golang and Rust, respectively — are general-purpose, type-safe, and widely audited. CosmWasm's design precludes reentrancy attacks, a major class of exploits to which Solidity smart contracts are vulnerable. The SDK utilizes an object-capability model which confines code implementations to their intended use cases by preventing unnecessary rights from being included with shared objects by default.

Secure and Efficient Consensus: Tendermint BFT

Tendermint is a proof-of-stake (PoS) consensus algorithm designed with Byzantine Fault Tolerance (BFT), meaning that it is able to operate reliably even if ⅓ of its nodes fail or act maliciously. Tendermint, as an out-of-the-box consensus engine, dramatically decreases the activation energy needed to launch a new blockchain. With this backbone in place, developers can spend more resources on developing the application layer.

Further, PoS offers greater flexibility in designing governance schemes and lower transaction fees compared to PoW. In the case of Quasar, this facilitates governance and incentive mechanisms at both the blockchain and application layers.

Scalability and Secure Interoperability: IBC

In an ecosystem of appchains, fragmentation across multiple chains is a feature, not a bug. The Inter-Blockchain Communication Protocol (IBC) is an interoperability protocol that provides specifications for establishing a secure connection for general-purpose message exchange between blockchains. Generally, when we describe something as "interchain" we mean that it is connected to the broad network of IBC-enabled blockchains. IBC can be understood as a universally implementable cross-chain infrastructure for a multi-chain ecosystem. The Cosmos SDK includes a module that simplifies IBC implementation for appchains.

IBC does not use third-party entities or intermediary blockchains to link blockchains. Instead, it utilizes off-chain processes with multiple layers of verification. Like TCP/IP or TSL protocols, IBC functions primarily by sending packets and receiving acknowledgments. IBC implementation is specified in the form of Interchain Standards (ICS) which offer definitions for IBC components and their use. Any chain implementing IBC with these standards is able to exchange with any other IBC-enabled chain, as long as they are both using the same updated version of IBC.

Key to the functions of Quasar vaults and strategies are the Fungible Token Transfer, Interchain Accounts, and Interchain Queries standards. The Fungible Token Transfer (ICS-20) standard enables interchain token transfers that enable Quasar vaults to securely operate with a variety of assets.The Interchain Accounts (ICS-27) standard unlocks the ability for users on one chain to execute actions on other chains, such as sending and receiving funds or accessing data streams. The Interchain Queries (ICS-31) standard unlocks the capacity to read values and balances across an IBC connection. Strategies and vaults depend on the ability to know the price of assets on other blockchains. Quasar, along with Polymer Labs and Strangelove Ventures, has contributed significantly to the development of Interchain Queries.

Vaults and Strategies

We leveraged the Cosmos SDK and CosmWasm to create "vaults" and "strategies." A vault is a composable multi-party smart contract for crypto asset pools. A strategy is a composable smart contract template for algorithms implementing financial strategies. Strategies allow financial strategists to interface with interchain DeFi. Vaults are customizable vehicles for crowdsourcing and deploying capital,

allowing liquidity providers (depositors) and experts (strategists and portfolio managers) to effectively connect to each other in a permissionless way. With in-vault governance, liquidity providers and administrators curate the strategies incorporated by their vault, together.

Vaults and strategies provide a unified UX to equip users (whether they are liquidity providers, portfolio managers, or strategy developers) with the appropriate tools to interface with interchain DeFi from a single point of access. Both technical and non-technical users can benefit from bypassing the need to actively manage multiple wallets or log into multiple platforms.

Vaults: Composable Smart Contracts for Crypto Asset Pools

Vaults track assets aggregated from the self-custody wallets of multiple individuals for deployment via strategies. They are Quasar's bookkeeping mechanism, tracking who is a vault member, their assets, returns, and share of governance.

Vaults implement the CW-4626 standard (based on ERC-4626), which specifies parameters and functions for yield-bearing vaults. It is our minimal interaction base for asset-bearing vehicles accommodating multiple parties. CW-4626 extends the CW-20 token standard, with additional features for multi-party membership and governance. These standards apply specifically to yield-bearing tokens and make use of the concept of shares to represent fractional ownership of vault assets.

A vault must first be created by an individual designated as a Vault Creator. Administration rights can be linked to a single wallet or groups of individuals with a multi-signature wallet. Creators and administrators have the power to define initial vault settings and select an initial strategy. Vaults can customize their governance schemes to implement processes such as quorum or weighted voting. Some vault settings may require community input before full initialization.

Once a vault is created, it is open for liquidity providers to join. Users will ultimately be able to select from multiple vaults, each with different goals and strategies to meet those goals. Vault history will be transparent so that potential members can make informed decisions.

A simple user flow for vaults is as follows:

1. To launch a new vault, a creator must delegate a specified minimum amount of $QSR to network validators.

2. Liquidity providers initiate transactions to deposit CW-20 assets into the vault. A percentage of funds is allocated to a reserve pool to cover transaction fees.
3. Decisions about how to deploy aggregated assets based on specified goals are expressed at the vault level. The vault dynamically incorporates strategies to meet its goals.
4. After a specified interval (reward epoch), yield from deployed assets appears as vault shares (vault-specific tokens) and is distributed accordingly to liquidity providers, the strategist(s), the vault creator, and any administrators.
5. Each deposit transaction will store a separate object to facilitate the calculation of future rewards based on the duration and percentage of assets locked. If one of two deposits of the same size is active for a longer period of time, it will receive a bigger reward for the time it overlaps in reward epochs.

Each vault mints vault-specific tokens that track fractional shares of vault assets across its members. Vault creators, strategists, and administrators receive a specified fraction of vault tokens based on vault parameters. Liquidity providers receive tokens based on the amount of capital they've contributed to the vault as a deposit. Vault shares are fungible and tradable, and can be redeemed via the vault smart contract itself. As the returns generated by a vault increase, so does the value of its shares.

Though liquidity providers allow the vault to deploy their assets via strategies, they can unbond their assets from the vault and its active strategy at any time. Still, transferring assets back into one's self-custody wallet requires a specified unbonding period (i.e. an exit timer). Note that vaults and strategies are decoupled such that multiple vaults employing the same strategy will see unique results depending on their particular implementation and handling of their strategy instance.

Strategies: Composable Smart Contracts for Financial Strategies

Strategies are composable smart contracts with execution logic to carry out financial strategies. Strategies are integrated as sub-components of vault smart contracts to execute financial strategies, within constraints set by the vault. Strategies are developed independently of vaults. Once a strategy is developed, it is available to be called from and integrated into any number of vaults.

A strategy template can serve like a chassis thats strategists can expand upon to construct customized asset management algorithms. The primary function of a strategy template is to equip a strategy with the minimal infrastructure needed to deploy a contract capable of gathering data via IBC, transporting funds

between IBC-enabled chains, and executing more complex yield-bearing transactions on other chains, such as joining AMM pools.

The lifecycle of a strategy is as follows:

Creation: An individual or team builds atop a strategy template. The developed smart contract is reviewed and audited and can be backtested on the Quasar testnet.

Voting: The strategy becomes available to vaults. Strategy developers can propose their strategy to one or more vaults for integration. Vault governance will allow vault participants to enter a voting period to decide whether or not a strategy will benefit their community's goals. Once a strategy has passed governance, it can enter its final review before integration.

Integration, Execution, and Termination: Integration of strategies involves simply upgrading the vault smart contract to point to the proposed strategy smart contract on-chain. Any actively managed components in the strategy that an individual or team must monitor should be assigned prior to the execution of the smart contract. Termination of the strategy is the reverse of integration, requiring a vault smart contract upgrade that removes the called strategy.

Vaults allow for dynamic, goal-oriented management of strategies. An advanced strategy might operate as a metastrategy, deploying assets across multiple strategies. This level of customization sets Quasar strategies apart from existing asset management solutions. For example, unlike other single-chain asset management protocols, vaults and their strategies could be configured to remain agnostic to the type of token received as yield, returning whatever crypto asset makes sense at the time of execution.

Quasar will make template code for community-audited vaults and strategies publicly available. Having smart contracts with minimal deviations from these templates would receive lower risk assessment scoring. This is just one example of the features that may be implemented to ensure a secure and dynamic environment for asset management.

Tokenomics & Governance: Aligning Incentives for Decentralized Asset Management

The various purposes of the $QSR token ensure it is tied to inherent utility. $QSR is used to provide proof-of-stake security, facilitate sustainable scaling of vaults, incentivize high-quality vaults, and support on-chain governance for chain upgrades. The primary functionality of the $QSR token is outlined below:

1. Support of Quasar's PoS consensus
2. Payment for transaction fees on the Quasar chain (rewarded to validators)
3. Vault creation (by staking to network validators)
4. Chain-level governance (e.g. voting on protocol upgrades and adjustments to base transaction fees)
5. Q-Treasury governance (e.g. setting swap fees and voting on which vaults should receive incentives)

Proof-of-Stake Consensus

Quasar's PoS blockchain, built with Tendermint, uses $QSR to provide security to the chain. Validators can participate in committing blocks to the blockchain by staking a required minimum sum of $QSR.

Tendermint consensus works by offering the opportunity to commit a block to a randomly selected validator at regular intervals. Validators can increase their chances of being selected by staking more $QSR. Upon successfully generating a new block, the validator receives a portion of transaction fees from the network as a reward. If a selected validator is unavailable or acts maliciously, they are penalized (referred to as slashing) and lose a portion of their staked $QSR.

Non-validator $QSR holders can delegate their $QSR to validators and receive a share in a portion of rewards for successful block generation (and slashing penalties when a selected node fails). These incentives promote security by encouraging greater decentralization of the liquidity powering the consensus layer, making it significantly more difficult for a validator or group of colluding validators to disrupt the network.

Transaction Fees

All transaction fees on the Quasar chain are paid in $QSR, and each vault has a reserve pool of $QSR to cover fees involved in asset deployment. Collected fees are provided as rewards to validators securing the network.

Vault Creation

In addition to the $QSR token's basic utility for PoS and transaction fees, $QSR regulates vault creation for sustainable scaling. To create a new vault, creators are required to delegate a minimum amount of $QSR to a network validator. This acts as a barrier to indiscriminate vault creation, alleviating the threat

of spamming fraudulent or non-productive vaults which could clog the chain's resources. Importantly, having vault creators stake $QSR aligns their objectives with that of validators and the Quasar chain more broadly. This prevents coordinated attacks to devalue $QSR and compromise consensus-level security.

If the market value of the $QSR token drops suddenly and dramatically, consensus-level security may be compromised by validators quickly buying up enough stake in $QSR to overcome Byzantine fault tolerance and manipulate on-chain transactions. This effect could be exacerbated by vaults running strategies that generate returns from $QSR depreciation. Vault creators should thus be aligned with the health of the Quasar protocol and its security. By requiring vault creators to stake $QSR as delegators, all Quasar vaults will have a vested interest in the sustainable growth of Quasar at the application level.

The Q-Treasury

New projects with their own cryptocurrency naturally have to generate liquidity to grow. The common method of liquidity mining programs, providing fleeting rewards to mercenary liquidity providers, is prone to becoming unsustainable. Instead, Quasar uses Q-Treasury — a unique vault, governed by $QSR holders, for protocol-owned liquidity. Its objective is to support the sustainable growth of the $QSR token's value. To do this, Q-Treasury coordinates strategic issuance, absorption, and containment of the $QSR token.

With Q-Treasury, Quasar is taking inspiration from the model of protocol-owned liquidity[6] pioneered by Olympus DAO.[7] The Q-Treasury holds a reserve of $QSR which is made available to Quasar users via a bonding mechanism. Buyers will be able to purchase $QSR with other assets (as long as the Q-Treasury supports it) at a discounted rate. Purchased $QSR will be available to the buyer after a short bonding period of several days. This mechanism allows Quasar to regulate the supply of $QSR while also gathering liquidity from a variety of sources, allowing $QSR to be backed by a diverse set of assets.

The Q-Treasury also functions as a community pool. All $QSR holders are intrinsically participants of Q-Treasury and can take part in Q-Treasury governance decisions such as choosing how to deploy assets, setting swap fees, and voting on which vaults should receive incentives. Liquidity gathered in Q-Treasury can be allocated through governance to fund and provide incentives for endeavors contributing to the Quasar ecosystem. For example, Q-Treasury can potentially be governed to deploy gathered liquidity into other Quasar vaults to jumpstart those that show promise.

By supporting the value of $QSR, Q-Treasury protects against aforementioned chain-level attacks; a strong $QSR token prevents malicious actors from buying up enough of a share to coordinate an attack. It also ensures that validator rewards and penalties have meaningful value and risks.

Vault Governance

The same vault-specific token used for tracking fractional shares in a vault is used for vault-level governance. Within vaults, participants can engage in collective decision-making to change certain vault settings and select from or modify available Strategies. This encourages members of a vault to share information amongst themselves to best contribute to effective decision-making, with considerations such as risk management and changing market conditions.

Through governance, decision-making in vaults goes beyond being the exclusive domain of the vault creator and/or administrators. Vault governance schemes can be customized and tuned toward more collective or more authoritative decision-making depending on the goals of the vault and the composition of its members. One vault might emphasize a model that emulates a fully democratic referendum with long voting periods. Others might choose to weigh governance power based on the share of deposited funds, similar to PoS validation. Still others may decide to give full power to the vault administrator(s).

Successful vault governance will likely involve a balance between allowing administrators the freedom they need to actively manage and respond to changing market conditions while giving vault participants the power to influence decisions that may have a significant impact on them. Additional specifications about the particulars of vault-level governance mechanics are still being developed and will continue to evolve as the community develops.

Blockchain Governance

The $QSR token importantly functions as a governance token for decentralized decision-making for the evolution of the Quasar chain. $QSR holders will decide the future of the protocol by proposing, vetting, and passing upgrades and changes to the protocol. Changes to Quasar cannot be imposed by Quasar's development team without input from the community of users.

Quasar's on-chain governance scheme is largely typical of PoS blockchains. All stakers of $QSR can participate in governance decisions regarding the blockchain to make changes to key parameters defining how the Quasar chain functions (e.g. adjustments to transaction fees or migrations). The weighting of voting power is measured 1:1 with an account's $QSR holding.

Validators are expected to have a greater stake in terms of $QSR and as security providers, so are expected to have more governance power. Simply, the more you participate and the more you are invested, the more voting power you will have.

References

1. https://defillama.com/
2. https://newsletter.banklesshq.com/p/the-best-defi-business-models
3. https://www.exodus.com/news/dydx-moves-to-cosmos/
4. https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/
5. https://research.kudelskisecurity.com/2021/08/12/the-poly-network-hack-explained/
6. https://medium.com/coinmonks/what-is-protocol-owned-liquidity-a-primer-on-the-model-developed-by-olympus-dao-55368f200d66
7. https://docs.olympusdao.finance/main/overview/intros.