HyperQuant Oracles: A Decentralized Oracle Solution for the HyperLiquid Ecosystem

HyperQuant (HQ)

August 10, 2024

Abstract

HyperQuant Oracles is a decentralized oracle service designed to bring HyperLiquid (HL) spot prices on-chain, starting with Ethereum. By leveraging cutting-edge cryptographic techniques and a trustless architecture, HyperQuant Oracles aims to facilitate the creation of decentralized financial applications such as prediction markets, lending protocols, and stablecoins. This whitepaper details the architecture and security mechanisms of HyperQuant Oracles, as well as the roadmap for future developments, including the introduction of staking mechanisms and community-driven validator node operations.

1 Introduction

The advent of HyperLiquid (HL), a new alternative Layer 1 (alt-L1) blockchain, promises to revolutionize high-speed trading by incorporating an order book engine while maintaining the Ethereum EOA (Externally Owned Account) model. HyperLiquid's infrastructure eliminates the need for sign-ups or KYC processes, thus ensuring a seamless user experience.

HyperQuant (HQ) is dedicated to building services within the HyperLiquid ecosystem. Our flagship product, HyperQuant Oracles, is a decentralized oracle service that securely and trustlessly brings HyperLiquid spot prices on-chain. The availability of reliable on-chain price data will enable the construction of various "money legos," such as prediction markets, lending protocols, and stablecoin protocols.

2 Architecture of HyperQuant Oracles

2.1 Data Acquisition

The initial phase of the oracle's operation involves acquiring spot prices from the HyperLiquid WebSocket API. This process is straightforward and reliable, ensuring that accurate market data is obtained in real-time. However, the challenge lies in securely posting this data on-chain to prevent manipulation or hacks.

2.2 Trustless and Decentralized Data Posting

To achieve a trustless and decentralized architecture, HyperQuant Oracles will operate five validator nodes distributed across five distinct geographical regions. This distribution ensures resilience and minimizes the risk of centralized failure.

2.2.1 Shamir's Secret Sharing Scheme

Each validator node will hold a fragment of the private key used to sign transactions that post prices on-chain. To achieve this, we utilize Shamir's Secret Sharing scheme. Shamir's scheme allows a secret, S, to be divided into n shares, such that any k out of n shares can reconstruct the secret, but fewer than k shares reveal no information about the secret. Mathematically, the secret S is represented as the constant term in a polynomial of degree $k-1$:

$$S = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$$

The secret shares S_i are generated as:

$$S_i = f(x_i) \quad \text{for } i = 1, 2, \ldots, n$$

where $f(x)$ is the polynomial, and x_i are distinct non-zero values. The security of the system is guaranteed as no single node has access to the full private key.

2.2.2 Secure Multi-Party Computation (sMPC)

To post data on-chain, the nodes engage in a Secure Multi-Party Computation (sMPC) protocol. sMPC enables the nodes to collectively compute the signature required for a transaction without reconstructing the full private key on any single node. This ensures that even if one node experiences downtime, the oracle service remains functional. The sMPC protocol securely computes a function $f(x_1, x_2, \ldots, x_n)$ over inputs x_i held by each node, where:

$$f(x_1, x_2, \ldots, x_n) = \sigma(\text{price data})$$

The result, σ, is the signature that is then used to post the price data on-chain.

2.3 Transaction Execution

Transactions are signed and executed in a trustless manner. The prices will be posted on-chain regularly, in batches, twice an hour. To facilitate omnichain readiness, the transactions will be handled using a factory contract deployed via the CREATE3 opcode. This ensures that the oracle can be seamlessly integrated with other chains, leveraging the same address across multiple deployments.

3 Security Considerations

The HyperQuant Oracle system is designed with a strong emphasis on security. The combination of Shamir's Secret Sharing and sMPC ensures that no single point of failure exists within the system. Additionally, the decentralized nature of the validator nodes prevents any potential collusion or manipulation of price data.

4 Future Developments: Staking and Validator Participation (v2)

Version 1 of HyperQuant Oracles focuses on establishing a secure and trustless infrastructure for posting price data on-chain. In Version 2, we will introduce a staking mechanism that allows users to stake their HQ tokens and participate in the validator node operations. This will further decentralize the oracle service and incentivize community participation.

5 Conclusion

HyperQuant Oracles represents a significant advancement in bringing secure and trustless on-chain price data to the HyperLiquid ecosystem. By utilizing a combination of cryptographic techniques and decentralized infrastructure, HyperQuant Oracles is poised to become a foundational component in the creation of decentralized financial applications. The introduction of staking and community-driven validator nodes in future versions will further enhance the decentralization and security of the system.