Paradigm DeFi Integration Specification

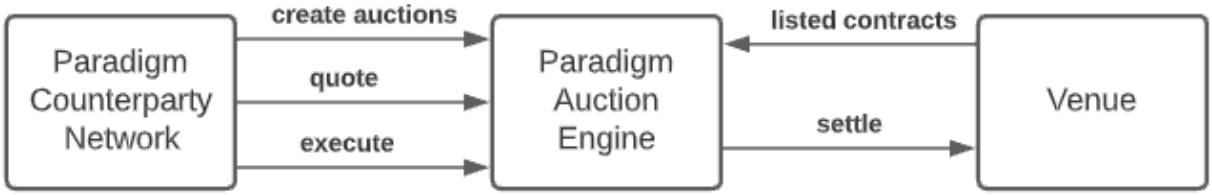
Purpose

This document is designed to provide readers with an overview of the Paradigm DeFi integration process.

Paradigm Overview

Paradigm provides supplemental liquidity to CeFi Exchanges and DeFi protocols – collectively referred to as "venues." Paradigm's liquidity comes from a combination of advanced auction technology (high performance Complex Order Books and RFQs with configurable auction microstructure) and a dedicated counterparty network of 700+ institutional traders.

When a venue is integrated with Paradigm, the venue's contracts are listed within Paradigm's platform, traders can create and participate in auctions, and on execution Paradigm sends the transaction to the venue to settle. See the statistics page for recent volumes.

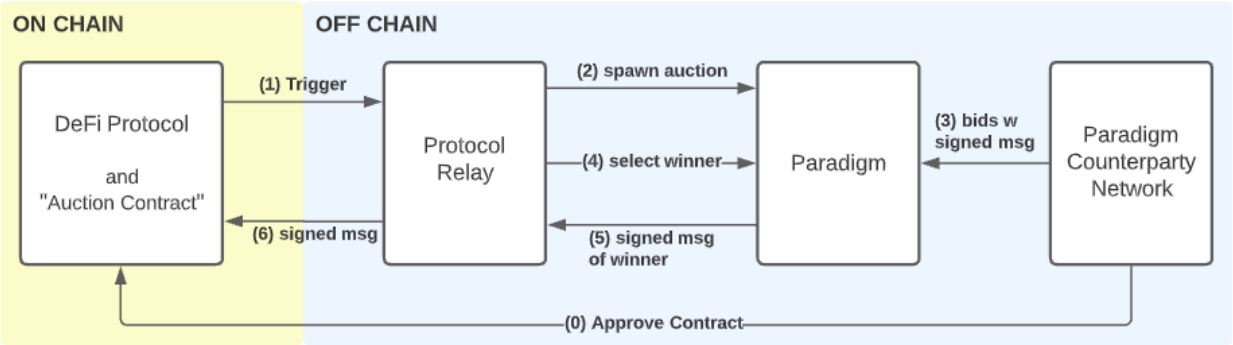


Paradigm's counterparty network trades $400-$800mm daily in complex multi-leg derivatives.

DeFi Integration Strategy

Paradigm provides liquidity to DeFi protocols through an off-chain relay. The DeFi protocol spawns an auction via relay when it requires liquidity for a transaction, and Paradigm's counterparty network competes with signed bids to provide the best price for this transaction. The winner conducts the transaction directly on-chain with the DeFi protocol, thereby maintaining all blockchain guarantees. This approach is commonly referred to as a State Channel, since all steps of the offchain process are signed, and all signatures are presented back to the protocol for the final settlement step.

This flow is shown in detail on the next page.



0) Traders on our platform who want to participate in these auctions will need to approve the relevant protocol contracts by providing a wallet signature. This ensures auction winners can execute the transaction later, on chain.

1) The DeFi protocol triggers an auction. This is typically done by creating a new smart contract "Auction Contract" (owned by the DeFi protocol). This Auction Contract has two purposes: (a) trigger auctions, the core protocol calls this contract to start the off-chain flow; (b) settle auctions, the winning bid (and associated signed message) is sent to the contract to trigger settlement. This Auction Contract is what is approved by the traders in step 0.

2) The Protocol Relay (owned by the DeFi protocol) monitors the Auction Contract and calls Paradigm APIs to create an auction when appropriate. The call includes an expiry time at which the auction will be canceled without executing.

3) Once the auction is triggered, Paradigm traders who are eligible to participate (have previously authorized the Auction Contract at the DeFi venue) can provide quotes. These quotes will contain signed messages that are used in step 6.

4) The Protocol Relay will interact with the Paradigm APIs to monitor the auction and select a winner (or cancel the auction).

5) The signed message of the winner will be returned to the Protocol Relay.

6) The Protocol Relay will send the signed message back to the on-chain protocol which will conduct the transaction (typically swapping premium from the winner for either a tokenized option or claim on an option payout directly from the DeFi protocol).

Auction Mechanics

The current supported auctions are traditional RFQs. This is a winner take all auction (quotes and execution is at full size), the makers quotes are anonymized and hidden from each other.

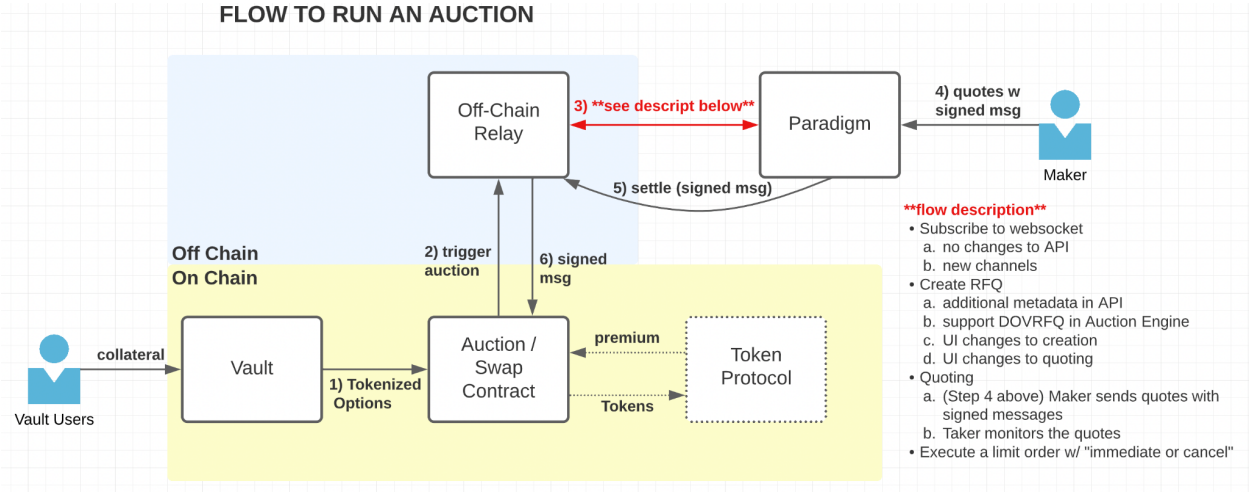
Auctions will stay open after execution incase of settlement failure (margin or authorization issues) so that additional quotes can be executed.

Other types of auction mechanics like sweeping, partial fills, or lit order books will be added in the future. These types of auctions are already supported on our platform for CeFi venues and will be rolled out to DeFi protocols as demand arises.

Integration Details

Paradigm integrates over a standard interface for all DeFi Protocols. This interface abstraction allows Paradigm's auction technology to be agnostic to the protocol, blockchain, wallet and signature scheme. This interface consists of four key components

1. **Protocol Relay** - used to call Paradigm APIs to conduct the auction
2. **Wallet Approval Workflow** - used by traders to enable their wallet on the DOV protocol
3. **Settlement Contract** - receives the executed signed quotes and settles the trade
4. **Protocol SDK** - used by traders and Paradigm to interact with the protocol



1. Protocol Relay

The protocol relay is responsible for spawning the auction, reviewing the active quote, and executing the best quote when ready. The Protocol Relay is playing the role of the Taker in the Paradigm workflow. Below is a list of relevant endpoints, full documentation can be found at ***https://api.stage.paradigm.co/v1/docs***

Note: the API endpoints are not finalized and may change slightly from what is listed here

Endpoint	Description
POST `/v1/vrfq/rfqs/`	Create a Vault Auction.
POST `/v1/vrfq/orders/{id}/`	Choose the winning auction quote.

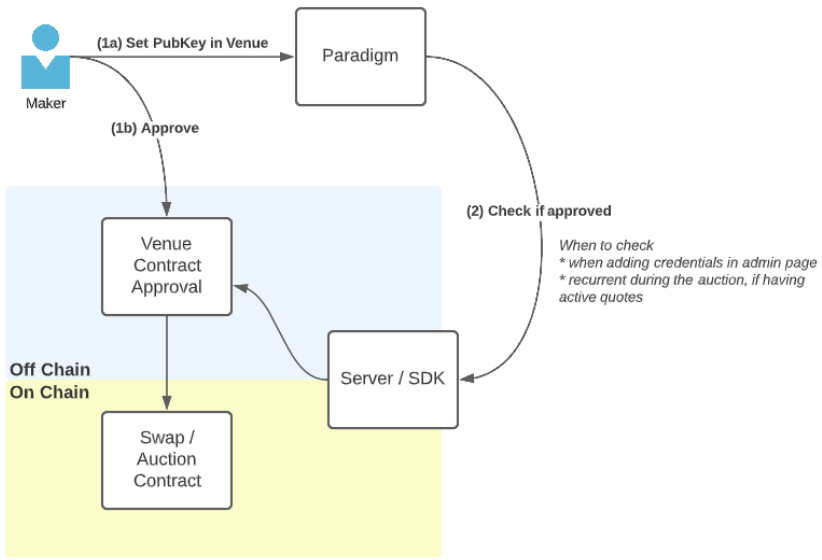
PUT /v1/vrfq/trades/{trade_id}/	Notify Paradigm of the transaction status.
DELETE /v1/vrfq/rfqs/{id}/	Cancel a vault auction.
GET /v1/vrfq/quotes/{id}/	Return the quote details a specific quote at {id}.
GET /v1/vrfq/rfqs/{id}/quotes/	Return all active quotes for the RFQ.

For some additional context, here are the corresponding list of endpoints that will be used by Makers to quote in the auction, however we don't expect the Protocol Relay to use these.

Endpoint	Description
POST /v1/vrfq/rfqs/{id}/quotes/	Create a quote for the RFQ.
DELETE /v1/vrfq/quotes/{id}/	Cancel a single quote.
PATCH /v1/vrfq/rfqs/{id}/quotes/	Replace a quote for the RFQ.
GET /v1/vrfq/quotes/	Lists all quotes belonging to the trading desk.
GET /v1/vrfq/rfqs/	Returns list of RFQs the user is participating in.

2. Wallet Approval Workflow

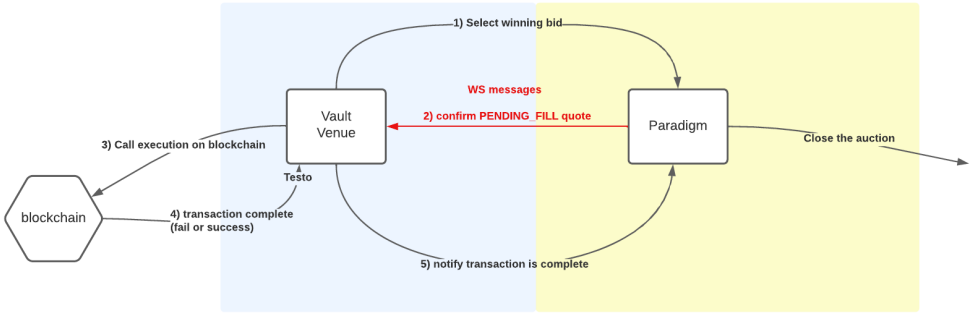
Paradigm's Market Makers will need a way to register their with the vault. This will enable the Protocol Settlement Contract to settle the trade when it receives the signed quotes. An example of this is [Ribbon's page for Wallet Approval.]



3. Settlement Contract

The Settlement Contract receives countersigned messages from Makers/Takers and can perform the on-chain settlement. This part of the integration doesn't interact with Paradigm directly; this contract instead talks to the Protocol Relay. However the message payload is defined by Paradigm.


```
{
    "buyAmount": 1000000000000000000,
    "nonce": 1,
    "referrer": "0xc3848824baEb9678847aF487CB02EAba792FECX6",
    "sellAmount": 6000000,
    "signerWallet": "0x58848824baEb9678847aF487CB02EAba782FECB5",
    "swapId": 1,
    "r": "0xd48860fab24673d45a03d58428f36bd7d62ac115972bd2a94e040503415a9478",
    "s": "0x32eed933d6532dc613e3167a5e839bce2c1d577b3c4b2c73eea7411fec1c9a53",
    "v": 27
}
```

EXECUTION DETAILS

4. SDK Development

The SDK provides a standard interface for Paradigm and Traders to interact with the protocol. The SDK will provide the following functions. Examples can be found at https://github.com/tradeparadigm/sdks

Functions to make available:

Function	Input	Output
Asset Parameters Used to lookup	Token address, or asset identifier	• collateralAsset • expiryTimestamp • Put/Call

information about the asset		• StrikeAsset • StrikePrice • Underlying Asset
Bid Signing Used to sign quotes	Domain • Name (vault name) • version • chainId (which blockchain) • verifyingContract (swap config address) Payload • swapId • nonce • signerWallet public address • sellAmount • buyAmount • referrer	• Success or Failure
Wallet validation check wallet balance and token, if applicable	• Swap config • Token Address	• Success or Failure
Validate bids	Payload • swapId • nonce • signerWallet public address • sellAmount • buyAmount • referrer	• Success or Failure
Test Auction Initiation		• ID of test contract for auction
Test Settlement	• ID of test contract for auction	• Success or Failure

Once the SDK is developed, we will be able to move forward with testing on Paradigm's Testnet.

Paradigm Product and Engineering staff are actively available throughout the entire integration process to help answer any questions and expedite the integration.

Launching

Testnet

Paradigm and the DeFi partner will work together to confirm the successful implementation of the integration across both Paradigm's *test* environment as well as the DeFi partner's *test* environment. Paradigm will also progressively load test the integration and actively share the results with the DeFi partner to ensure sufficient performance.

Auto Taker Example (on Paradigm Github)

Production

Paradigm and the DeFi partner will coordinate specific release dates and times to suit each party's respective organization, business development and marketing efforts.

First Auction

Paradigm and DeFi partner will coordinate on the first auction for the first vault. Our Client Service team will be on hand to provide makers any live assistance necessary to ensure there are no issues quoting or executing trades.

Scaling Auction

Once we've completed the first successful auction, the DeFi partner will be empowered to scale up to as many auctions across as many vaults they desire at their own discretion. In the future Paradigm will be adding features to our DeFi auction offerings in order to enable more complex auctions.