Threat modeling, Defi Derivatives : Option Model

2023. 07. 03
Presented by @ChainHunters

ChainHunters | Theori X DREAMPLUS ACADEMY

Table of Contents

S0: Introduction

S1: Related Work

S2: Our Approach

S3: Security Analysis

S4: Limitation & Future Work

Introduction

- About US
- Motivation
- Summary of project
- Final Vulnerability Analysis Results
- Defi Option Audit Matching Table

About US

Theori

setuid0 Mentor

Jungwon, Lim

Theori

wooz3k Mentor

Woosung Jung

ChainHunters

Zer0Luck PM

Yeoungun Kim

ChainHunters

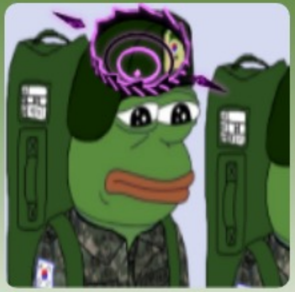
Junan Member

Junwon Seo

ChainHunters

hyeon Member

Yeonghyeon Choi



ChainHunters

Nugurii0 Member

Seonghwi Lee

Motivation

Interest in DeFi Option?

On-chain Pricing Implementation?

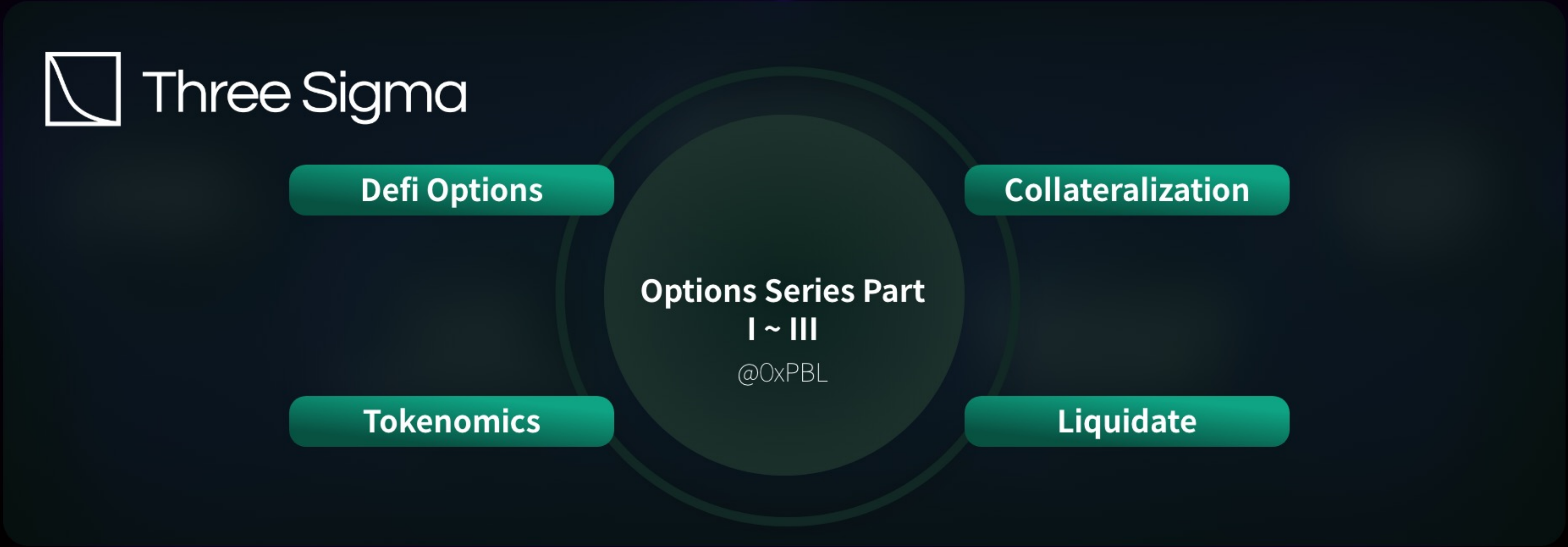
Not conducting audits after a new service launch?

Applications level implementation of the option?

On-chain Derivatives System?

This research is conducted to identify and address vulnerabilities caused by the lack of standardization in DeFi option models. **This will allow threats to the DeFi ecosystem to be blocked in advance.**

Motivation



Three Sigma

Defi Options

Collateralization

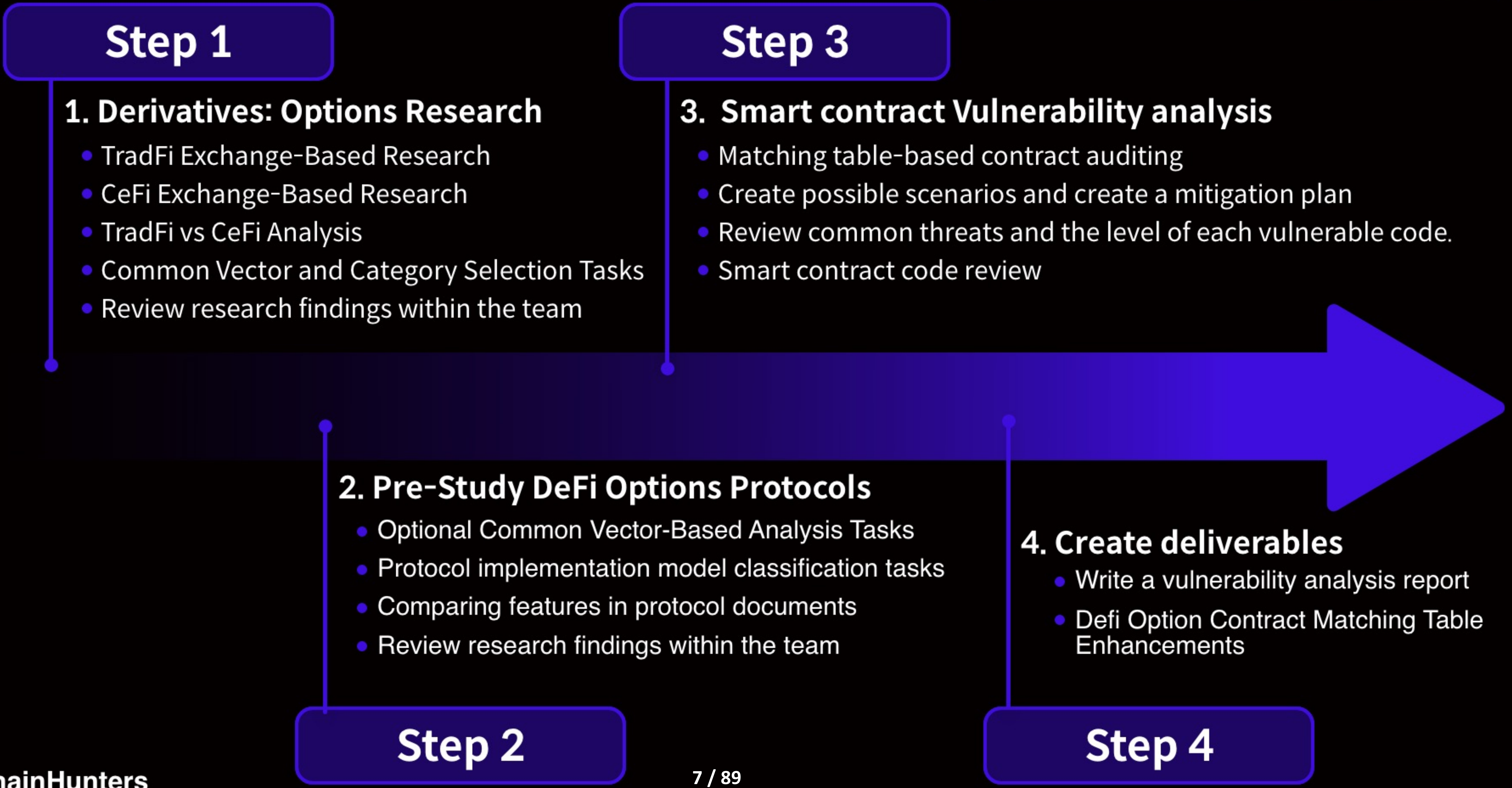
Options Series Part
I ~ III
@0xPBL

Tokenomics

Liquidate

Based on Three Sigma research and analysis of defi options,
implementing the intricate option structures of traditional finance on the blockchain
could introduce severe risks and potential financial problems.

Summary of project



Step 1

1. Derivatives: Options Research

- TradFi Exchange-Based Research
- CeFi Exchange-Based Research
- TradFi vs CeFi Analysis
- Common Vector and Category Selection Tasks
- Review research findings within the team

Step 2

2. Pre-Study DeFi Options Protocols

- Optional Common Vector-Based Analysis Tasks
- Protocol implementation model classification tasks
- Comparing features in protocol documents
- Review research findings within the team

Step 3

3. Smart contract Vulnerability analysis

- Matching table-based contract auditing
- Create possible scenarios and create a mitigation plan
- Review common threats and the level of each vulnerable code.
- Smart contract code review

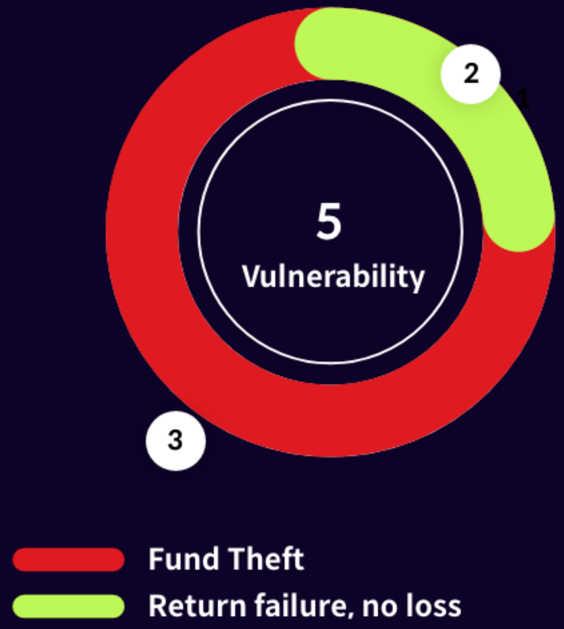
Step 4

4. Create deliverables

- Write a vulnerability analysis report
- Defi Option Contract Matching Table Enhancements

Final Vulnerability Analysis Results

Classification by vulnerability type



Immunefi

Defi Option Protocol

Opyn
Reported 1

Lyra
Reporting 1

Dopex
Reported 2

Ribbon
Reporting 1

Defi Option Audit Matching Table

❗ Vulnerable

⚠️ Centralized

✅ OK

Category	Opyn	Ribbon	Dopex	Lyra
On-Off Chain	⚠️	⚠️	❗	⚠️
Market Maker	✅	✅	✅	✅
Risk Managing	✅	✅	✅	✅
Margin	✅	✅	✅	✅
Oracle	✅	✅	⚠️	✅
Liquidate	✅	✅	✅	⚠️
Option Pricing	✅	✅	⚠️	❗
Role	⚠️	✅	✅	✅
Proof of Position	✅	✅	✅	✅
Option Write/Buy	❗	✅	✅	❗
Expire/Strike	✅	❗	❗	✅

Related Work

- Derivatives: Options ELI5
- Preliminary Findings: TradFI Structured Flowchart

Related Work

- Derivatives: Options ELI5

Options: Basic

Options?

- The right to buy or sell an underlying asset at an strike price on a future expiration date.

CALL/PUT

- **CALL,** The right to buy asset at a specific price
- **PUT,** The right to sell asset at a specific price

Buyer/Writer

- **Buyer (Long Position),** a person who buys the right to strike a call/put option.
- **Writer (Short Position),** a person who sells an option after it is issued for the purpose of earning an option premium.

Options: Type of strike price

Type

- **European option,** right on expiration date
- **American option,** right can be exercised at any time within the expiration date

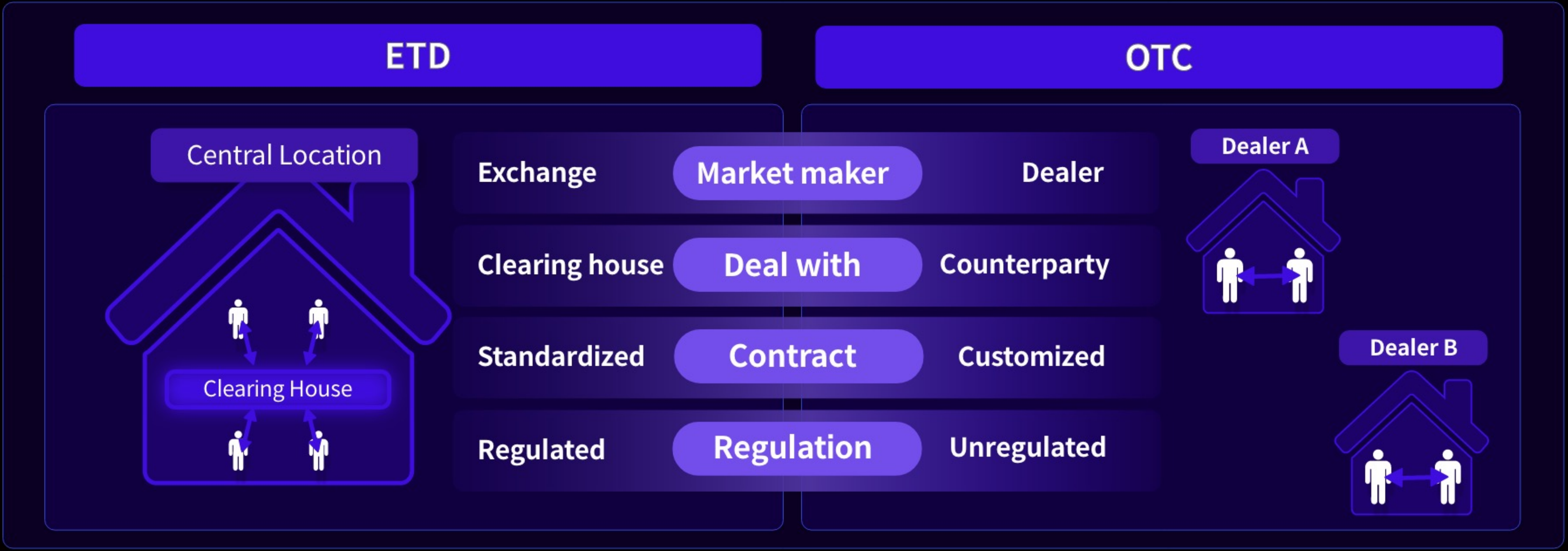
* Strike Price = Sp, Underlying Asset Price = Up

Type	Call Options	Put Options
ITM (In The Money)	Sp < Up	Sp > Up
ATM (At The Money)	Sp == Up	Sp == Up
OTM (Out Of The Money)	Sp > Up	Sp < Up

Options: Trade Type

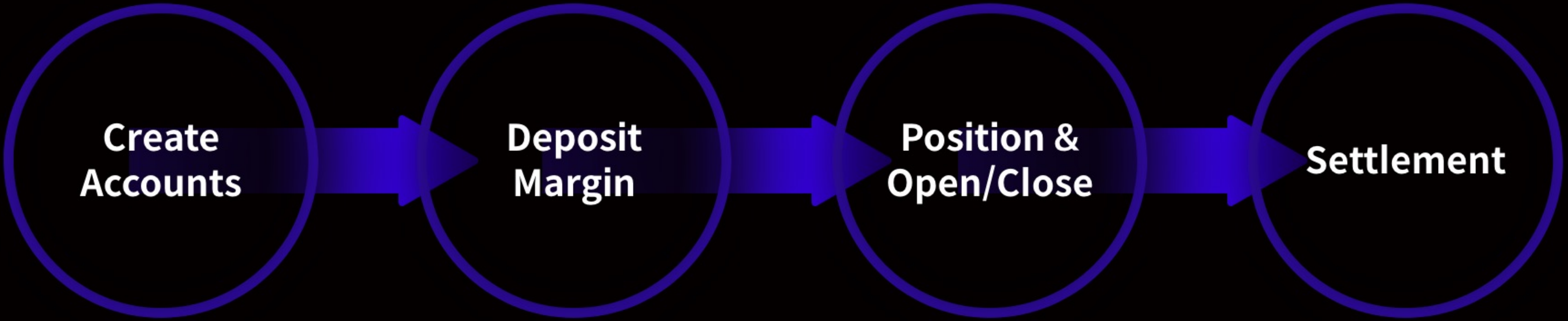
Type

- **OTC,** based on over-the-counter trading, where both parties trade directly.
- **ETD,** trades that are listed on an exchange and guaranteed to default through a clearinghouse



ETD		OTC
Exchange	Market maker	Dealer
Clearing house	Deal with	Counterparty
Standardized	Contract	Customized
Regulated	Regulation	Unregulated

Options: Trading Process



Create Accounts

Deposit Margin

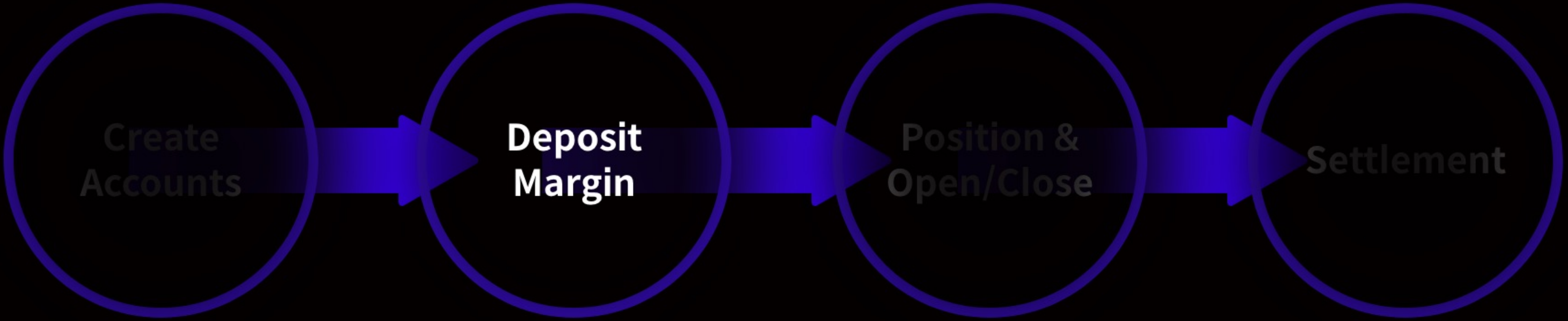
Position & Open/Close

Settlement

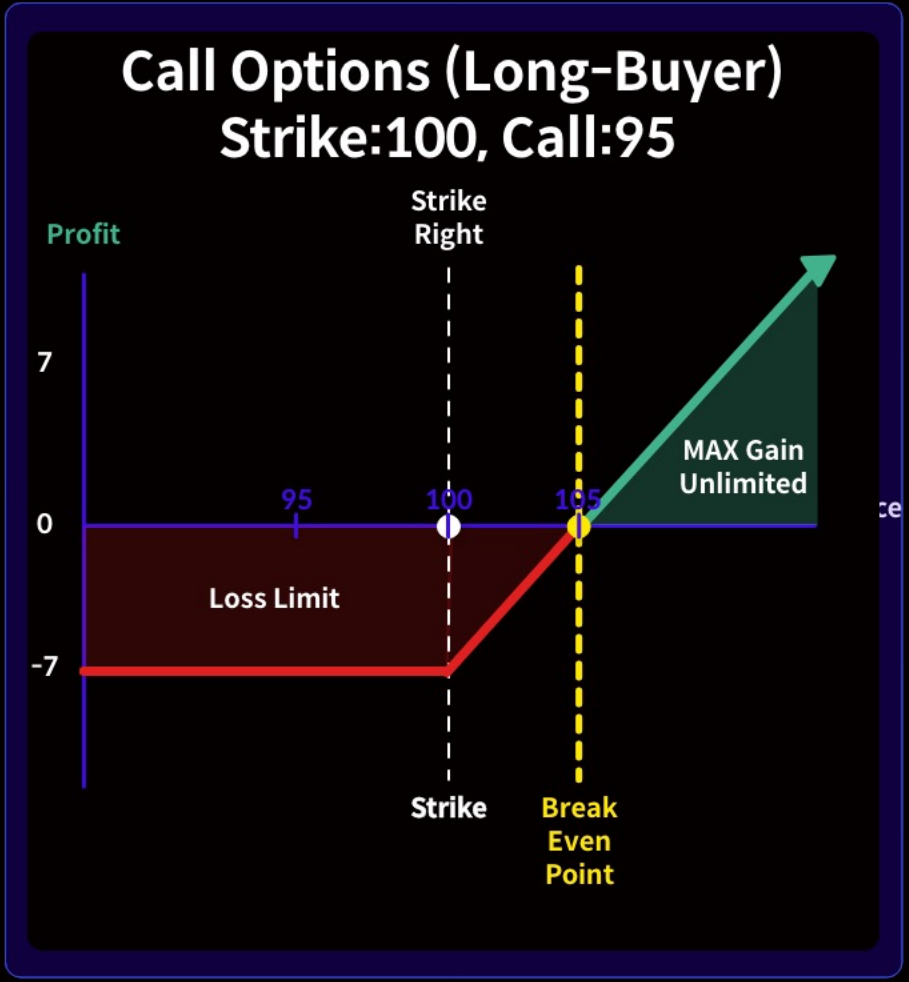
Options: Margin

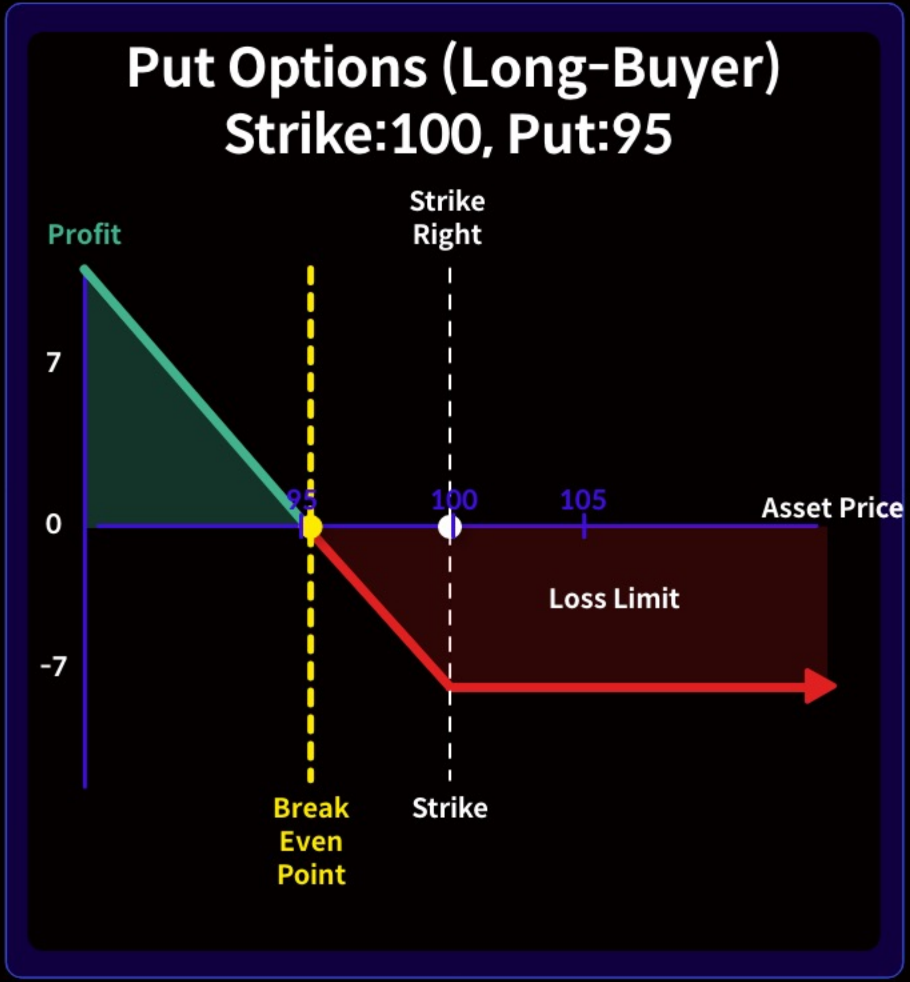
Margin

- **Initial Margin,** Deposit to open a trade
- **Maintenance Margin,** Maintain Margin Balance
- **Margin Call,** Notification to deposit additional margin if Maintenance Margin > margin balance



Options: Payoff (Call/Put)

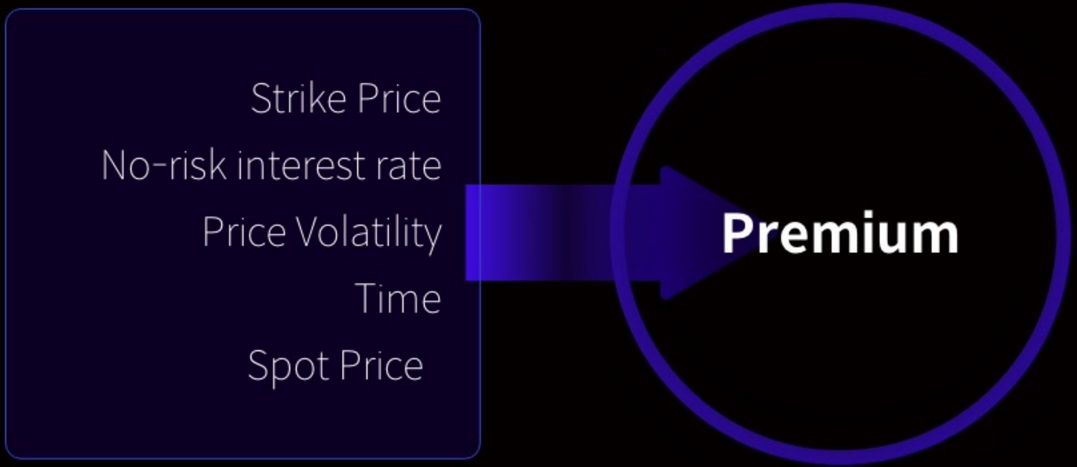


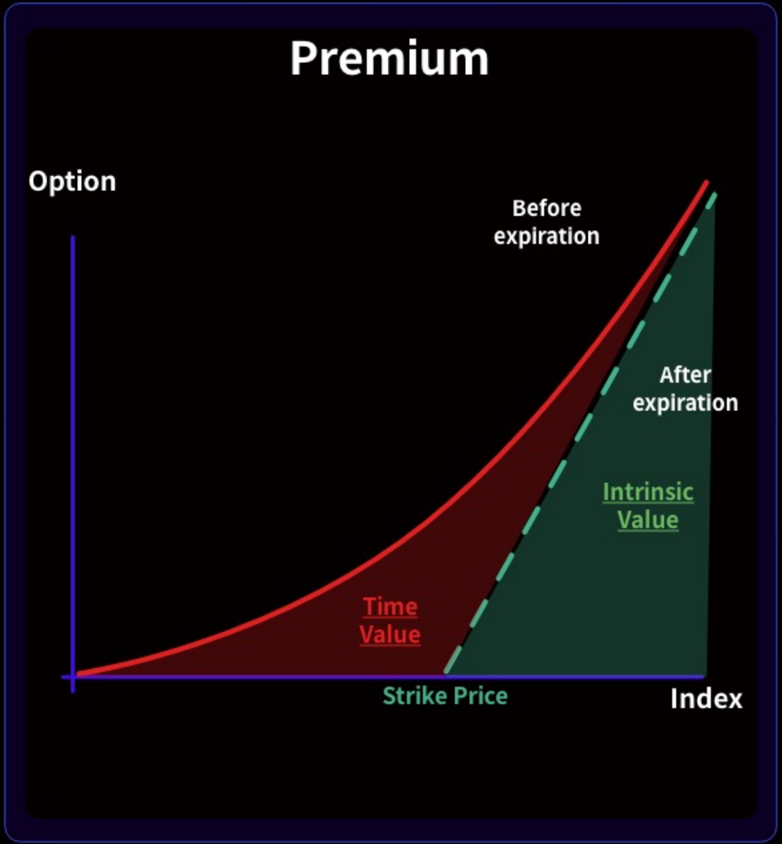


Options: Premium

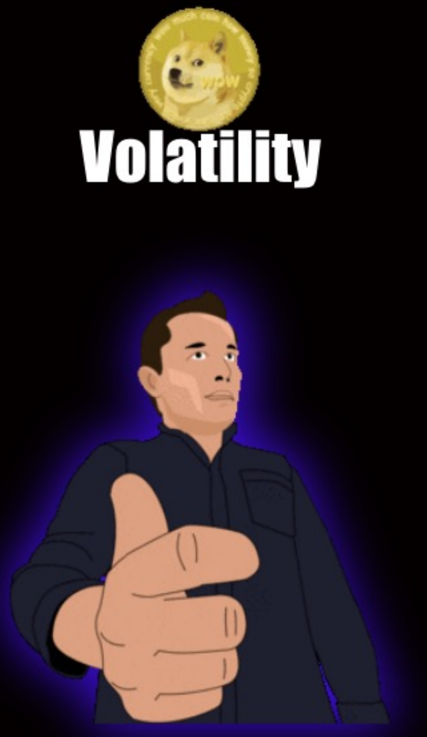
Premium

- **Intrinsic Value,** The realized value of exercising an option immediately
- **Time Value,** the probability value that the market price of the underlying asset will change in the option buyer's favor by the expiration date.





Options: Volatility



- **Market Volatility,** Realized Price fluctuation of an asset
- **Implied Volatility,** Market's future price movement expectations
- **Historical Volatility,** Market's past price movement

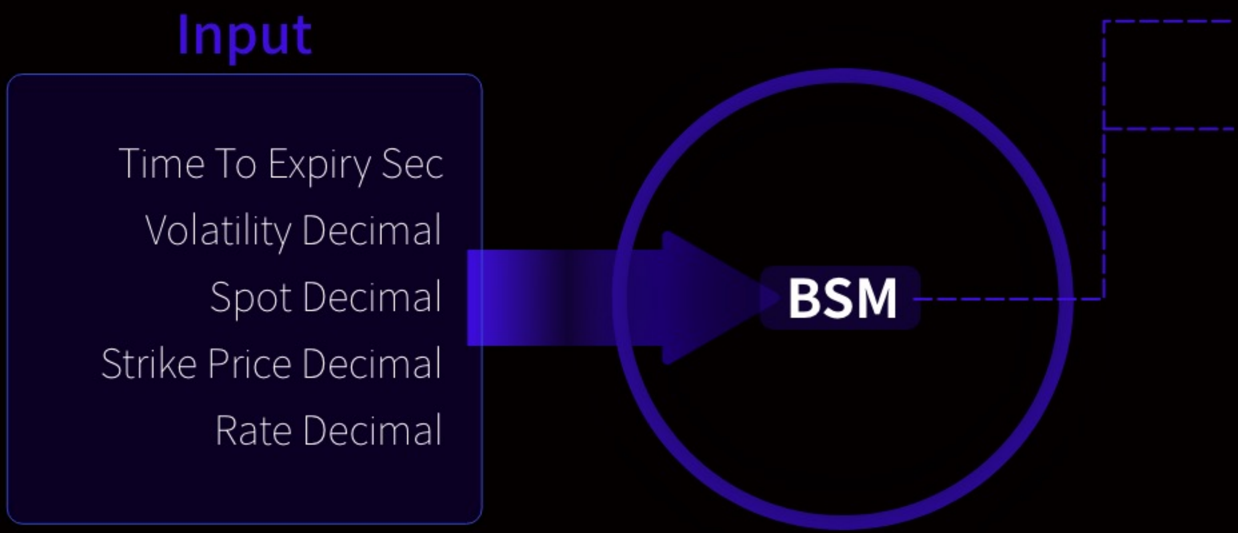
Historical Volatility

Implied Volatility

Options: Black-Scholes Model & Greeks

Black-Scholes Model

- Indeed used to calculate the price of call&put options
- The financial markets are efficient, and the price of the underlying asset follows a geometric Brownian motion with constant volatility



$$Call = S_t * N(d1) - N(d2) * Ke^{-rT}$$

$$Put = Ke^{-rT} * N(-d2) - S_t * N(d1)$$

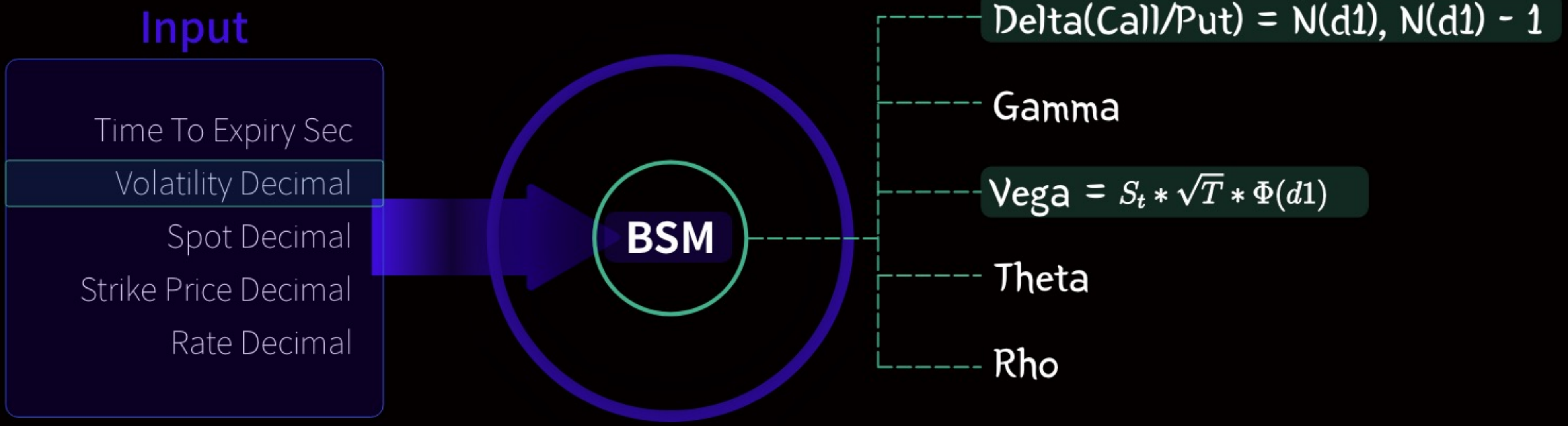
***Notation**

N	=	CDF of the normal distribution
St	=	spot price of asset
K	=	strike price
r	=	risk-free interest rate
t	=	time to maturity
σ	=	volatility of the asset

Options: Black-Scholes Model & Greeks

Greeks

- **Delta,** Change in option premium in response to a change in the underlying asset price
- **Gamma,** Change in delta for a change in the price of an underlying asset
- **Vega,** Change in option premium for an implied volatility of 1%
- **Theta,** Change in option price over time to expiration



Options: Risk

Complicated Market

- Macro market risk management options that affect asset prices are affected by all elements of risk.

Price Volatility

- The premium paid for an option depends on several factors, in addition to the price of the underlying token.

Selling Risks

- The option buyer can only lose the premium paid, but there are many additional risks.
  holder exercises the right => may include early exercise or margin calls on leveraged positions.

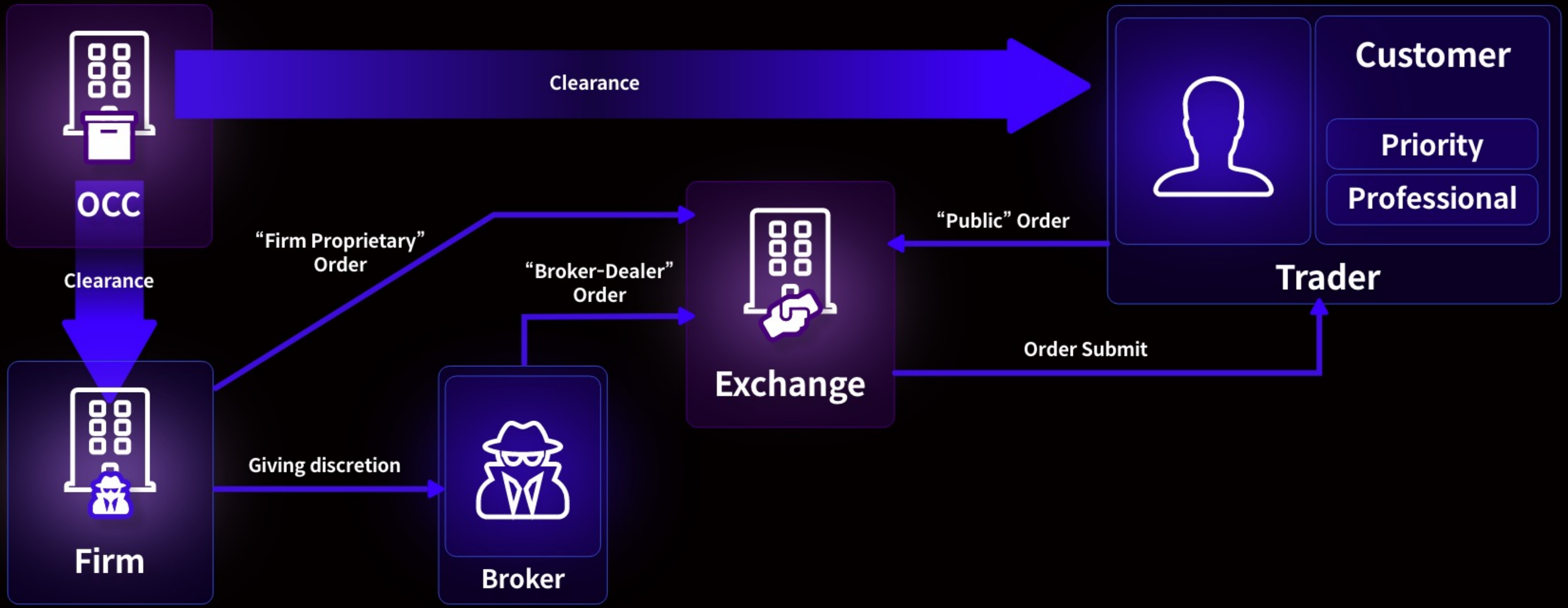
Time Decay

- Highly volatile value over time, as it decreases as it approaches expiration

Related Work

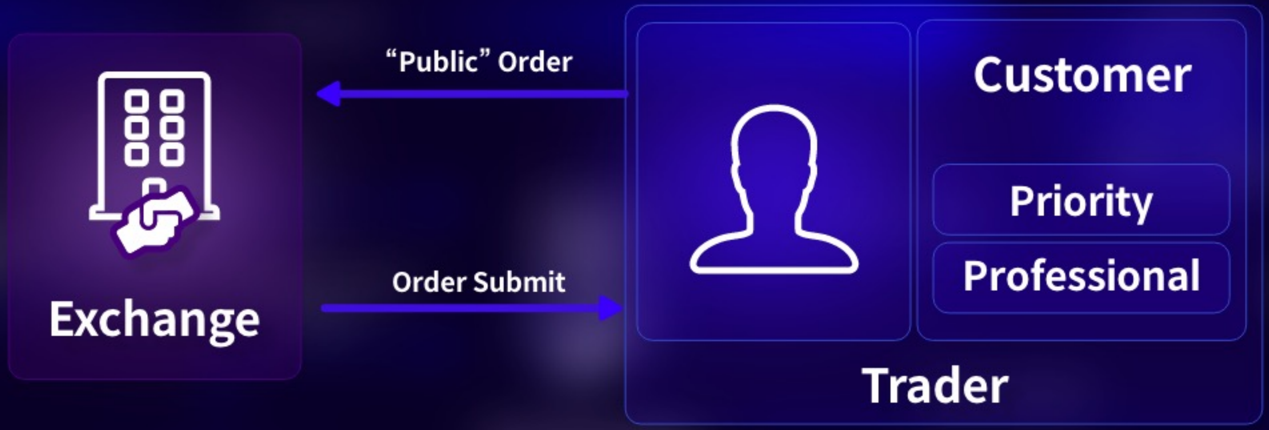
- Preliminary Findings: TradFI Structured Flowchart

Preliminary Findings: TradFI Structured Flowchart



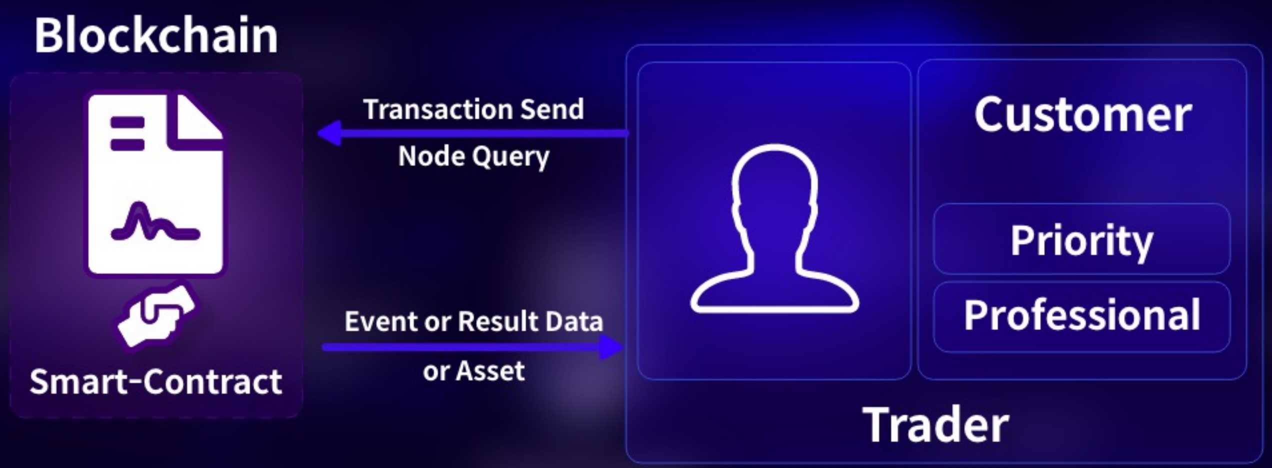
Preliminary Findings: CeFi Structured Flowchart

- Liquidation
- Risk management
- Role
- Trading Hour
- Regulation



Preliminary Findings: DeFi Structured Flowchart

- Liquidation
- Risk management
- Role
- Trading Hour
- Regulation
- Order Processing



Our Approach

- Approach for Option Target Selection
- Findings from Protocol Analysis
- Contract Design Pattern based on Audit Matching Table

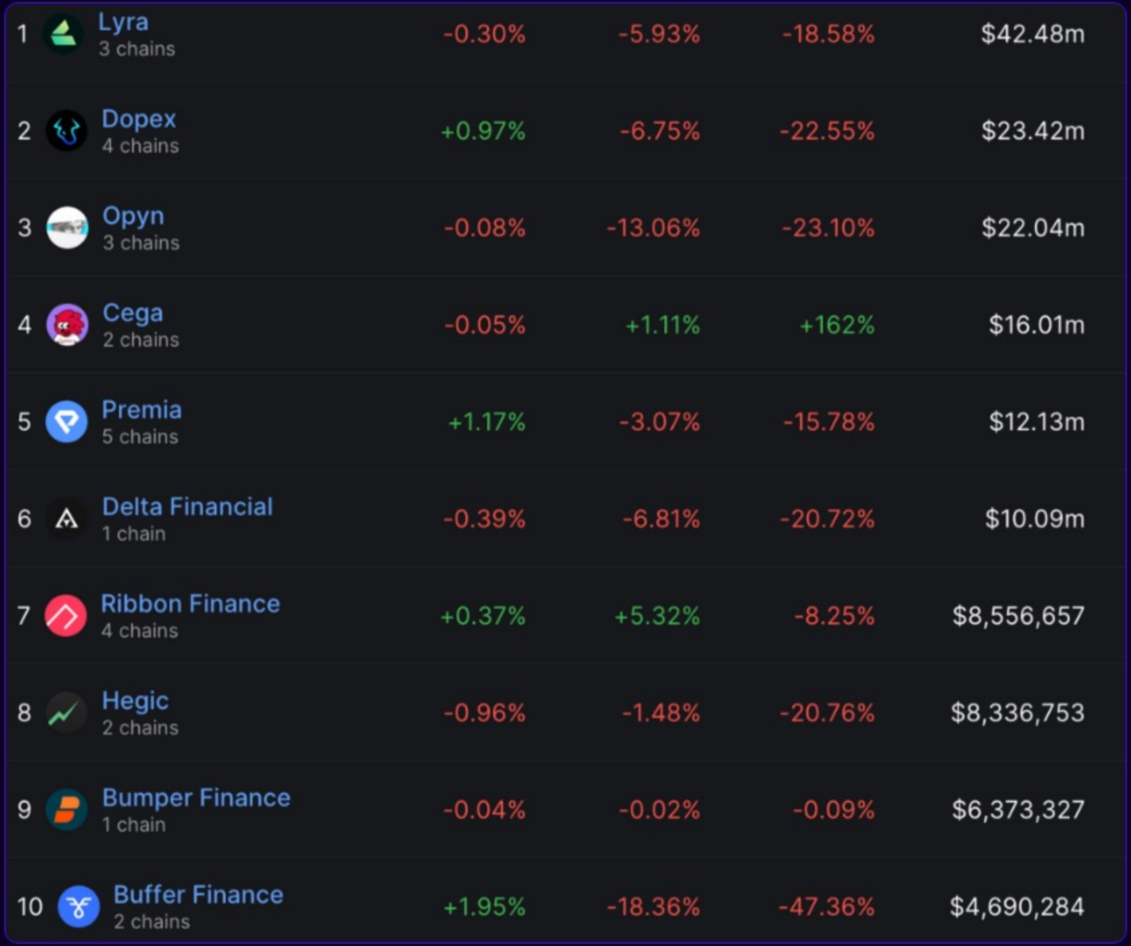
Our Approach

- Approach for Option Target Selection

Findings from Protocol Analysis

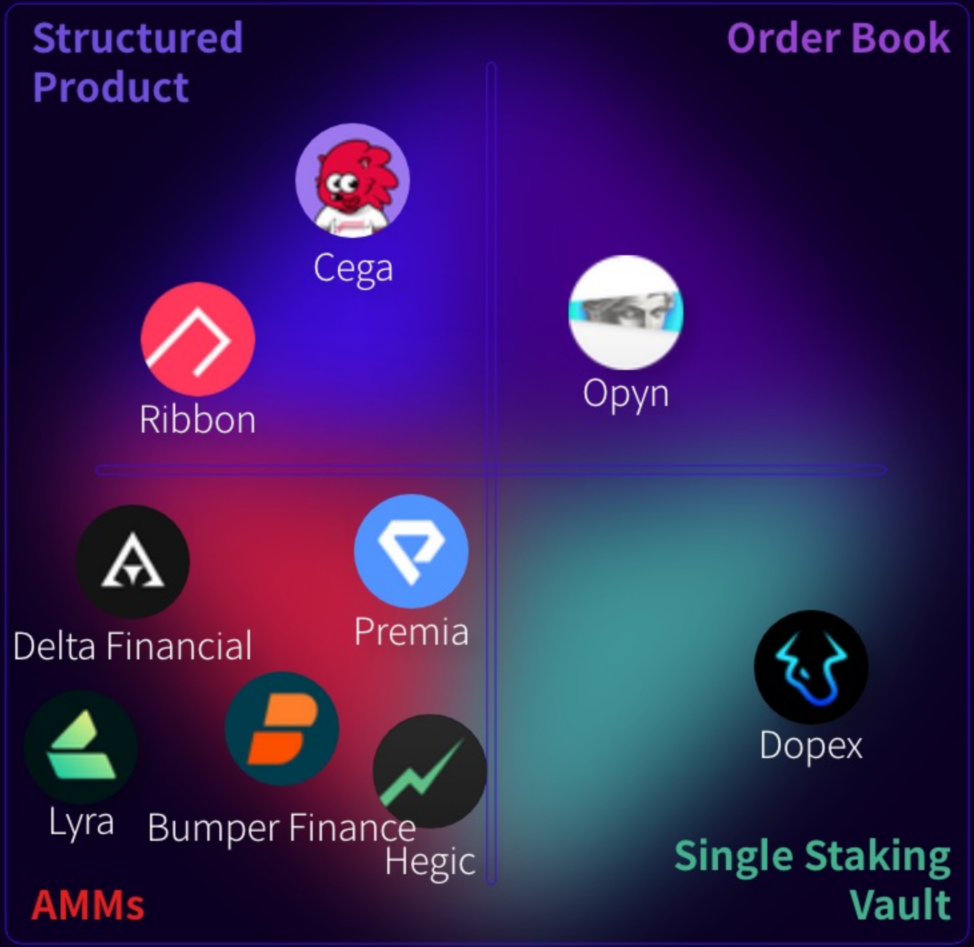
TVL-based Top 10 DeFi Option Protocol & Implementation Level Classification

TVL Rankings



1	Lyra 3 chains	-0.30%	-5.93%	-18.58%	$42.48m
2	Dopex 4 chains	+0.97%	-6.75%	-22.55%	$23.42m
3	Opyn 3 chains	-0.08%	-13.06%	-23.10%	$22.04m
4	Cega 2 chains	-0.05%	+1.11%	+162%	$16.01m
5	Premia 5 chains	+1.17%	-3.07%	-15.78%	$12.13m
6	Delta Financial 1 chain	-0.39%	-6.81%	-20.72%	$10.09m
7	Ribbon Finance 4 chains	+0.37%	+5.32%	-8.25%	$8,556,657
8	Hegic 2 chains	-0.96%	-1.48%	-20.76%	$8,336,753
9	Bumper Finance 1 chain	-0.04%	-0.02%	-0.09%	$6,373,327
10	Buffer Finance 2 chains	+1.95%	-18.36%	-47.36%	$4,690,284

Options Implementation Model



Findings from Protocol Analysis

TVL-based Top 10 DeFi Option Protocol & Implementation Level Classification

Opyn

- Gamma Protocol
- Squeeth

Ribbon

- Theta Vault
- Treasury Vault
- Earn Vault

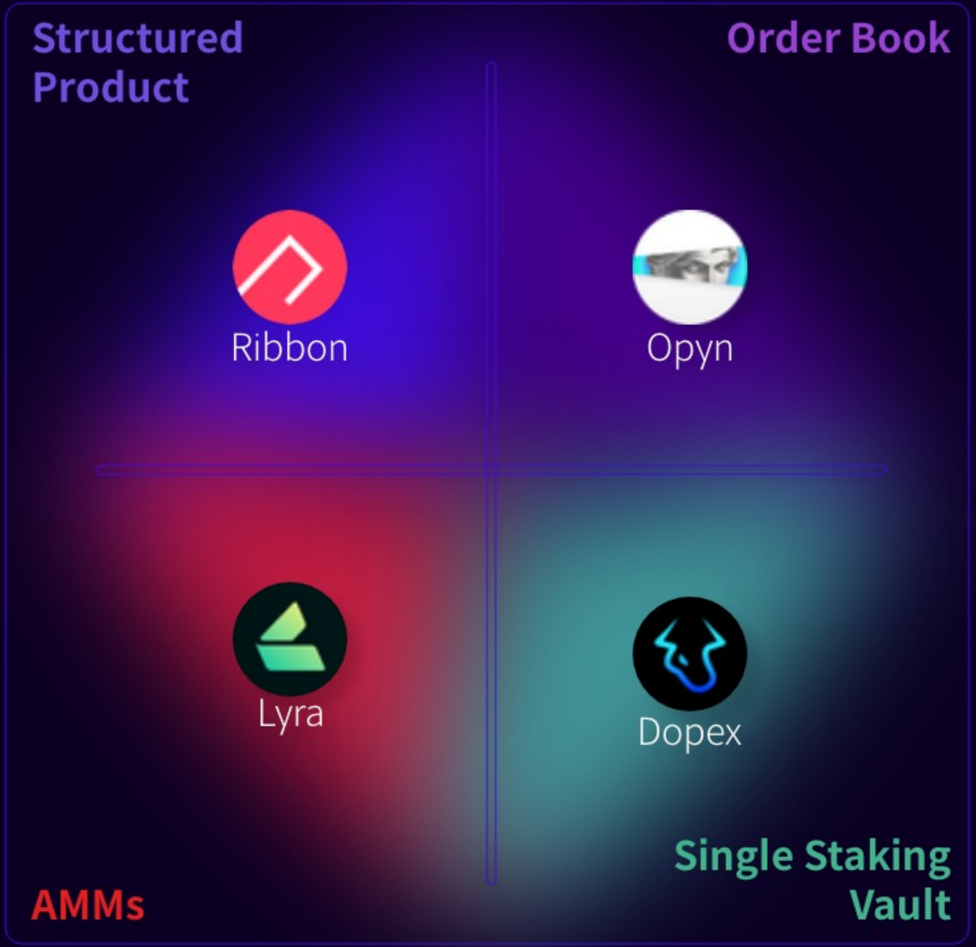
Dopex

- ssov
- 0dte
- Atlantic Straddle

Lyra

- Trade
- Earn
- Airdrop

Options Implementation Model



Structured Product

Order Book

Ribbon

Opyn

Lyra

Dopex

AMMs

Single Staking Vault

Our Approach

- **Findings from Protocol Analysis**

  Option: Order Bool Model (Opyn Protocol)

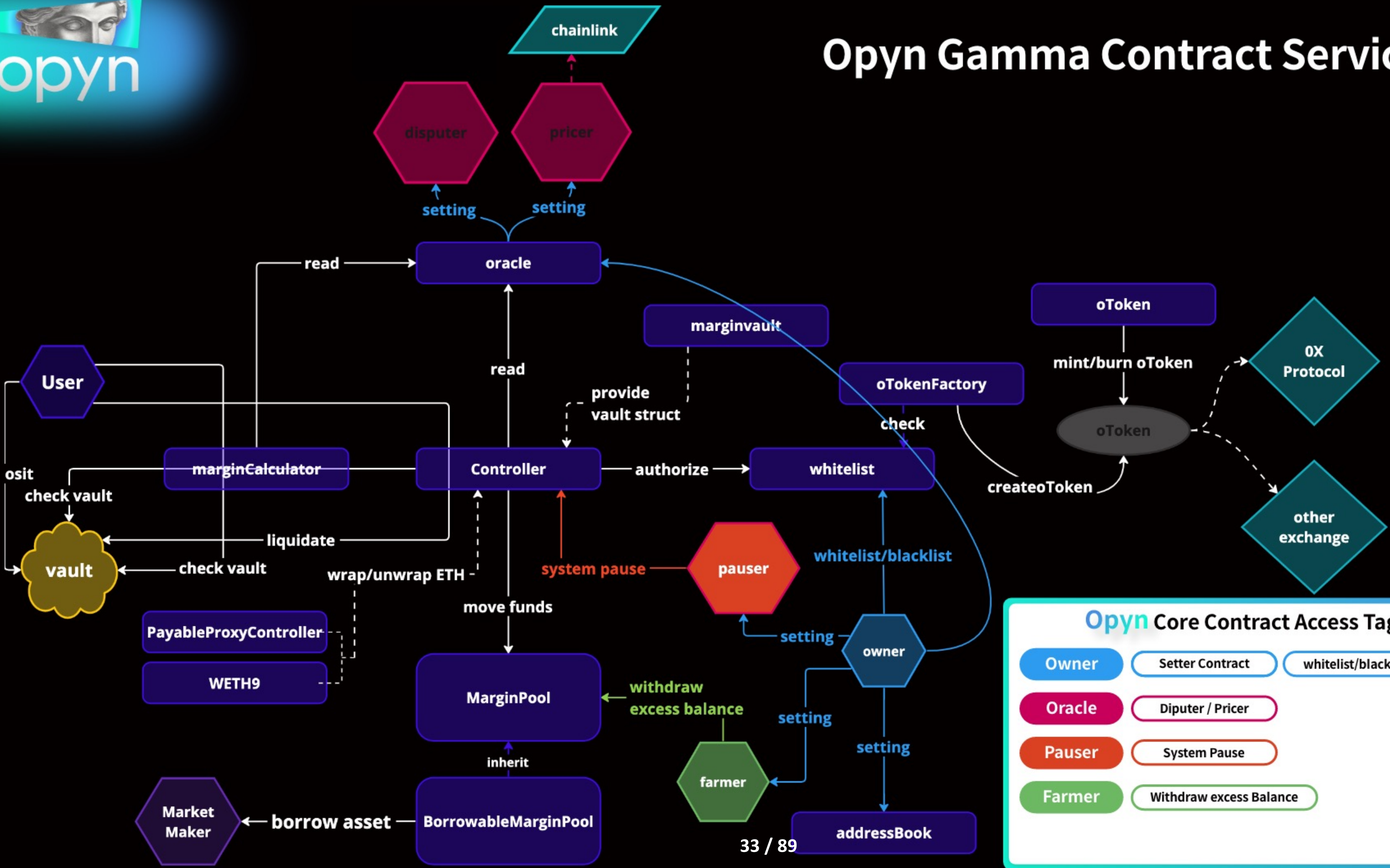
Opyn: Gamma Protocol

Opyn (Order Book Model) Specific issue

Opyn

Category	
Market Creation	Strategies should be implemented to maintain their liquidity without relying on other projects.
Whitelist	The whitelist should be updated appropriately and determined accurately whether it corresponds to when used.
Centralized Authority	Counterplan should be implemented against a decrease in confidence in asset prices and malicious price fluctuations.
Counterparty	A solution should be implemented when the trading is delayed due to the inability to find a counterparty-in the event of a lack of liquidity.
Vault Temaplate	When providing a DOV structure to users, it should be designed with an efficient and secure framework.

Opyn Gamma Contract Service Flow

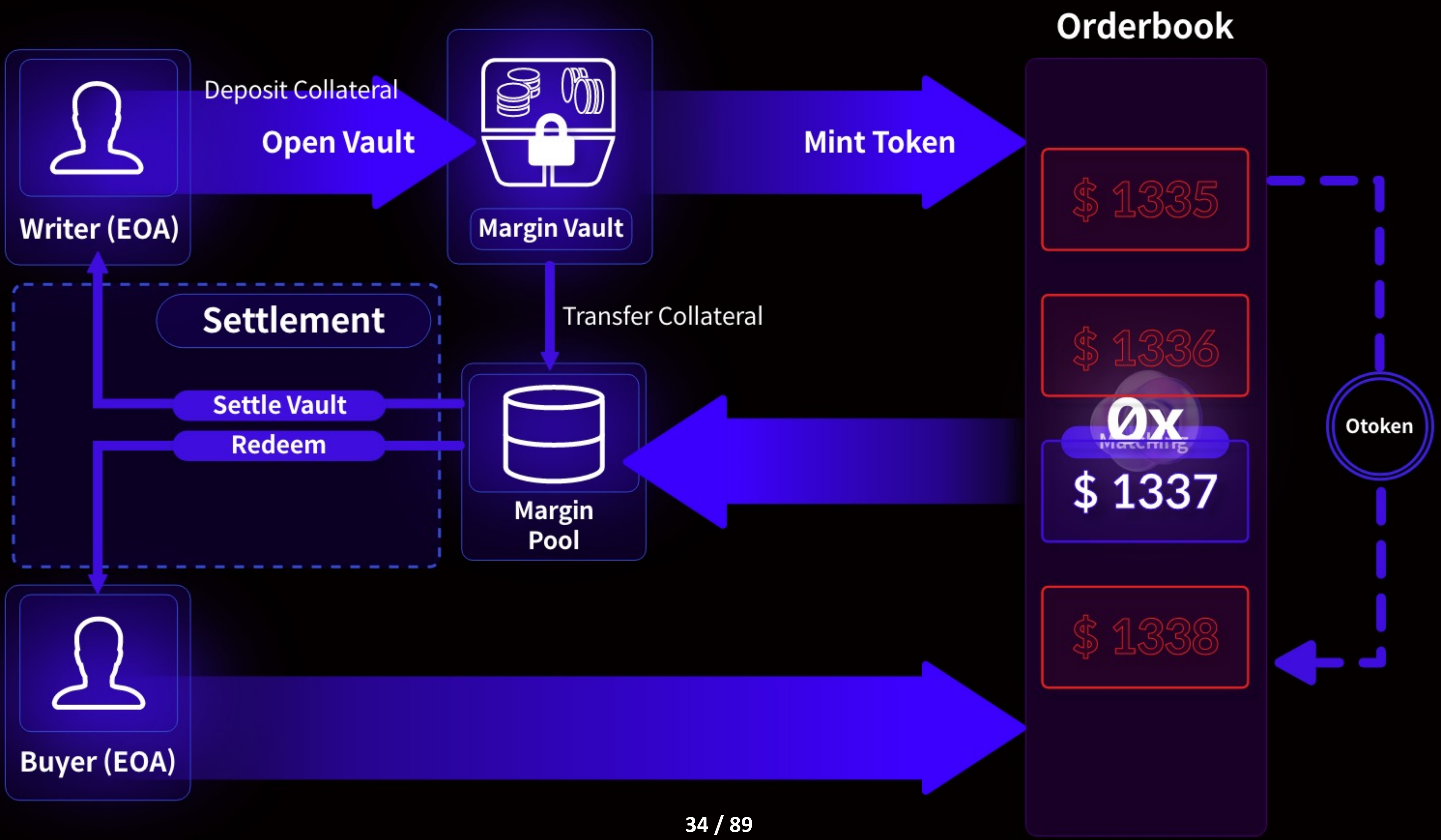


Opyn Core Contract Access Tag

Owner	Setter Contract	whitelist/blacklist
Oracle	Diputer / Pricer	
Pauser	System Pause	
Farmer	Withdraw excess Balance	

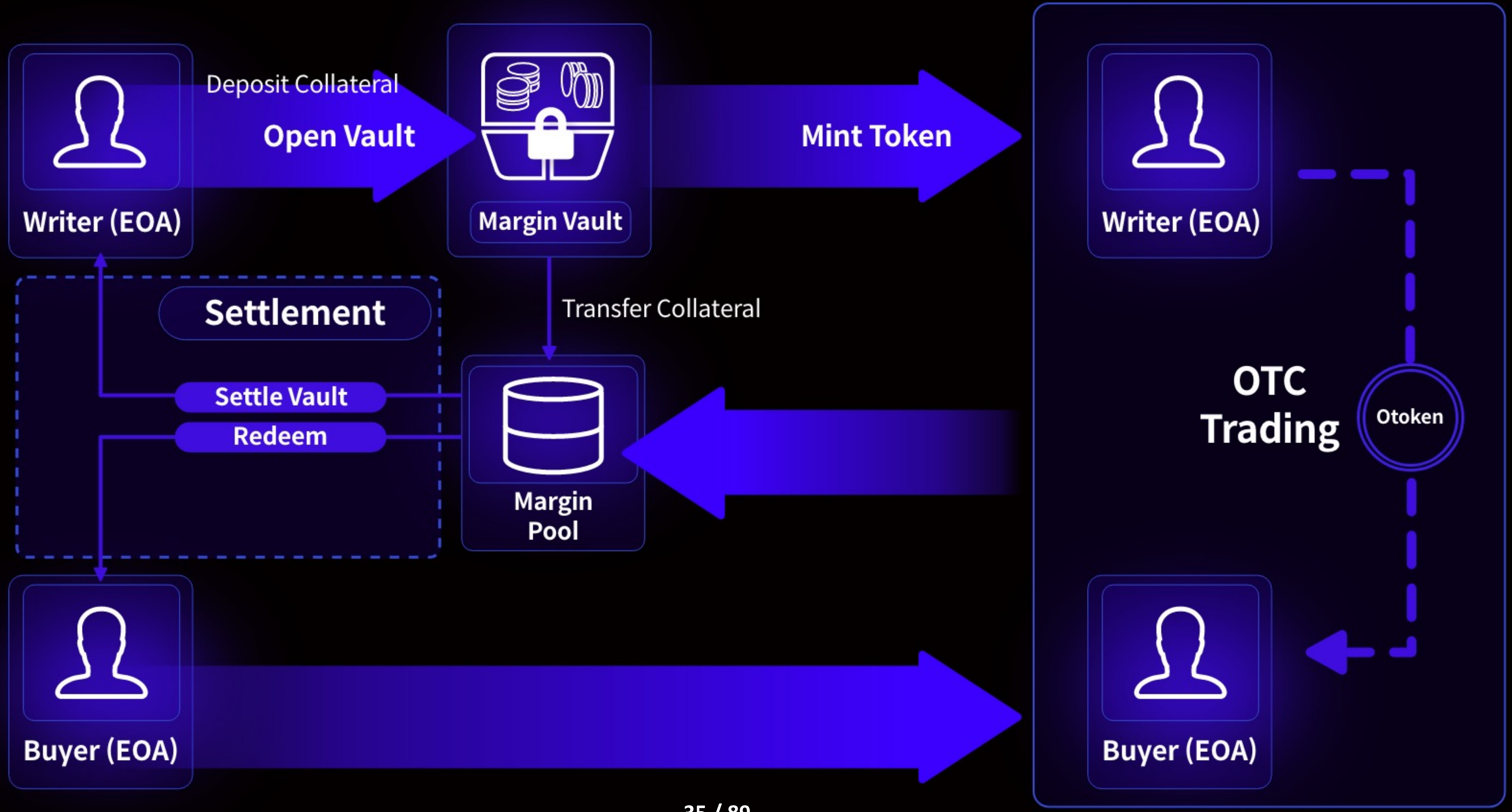
Opyn: Gamma Protocol

Trading Process



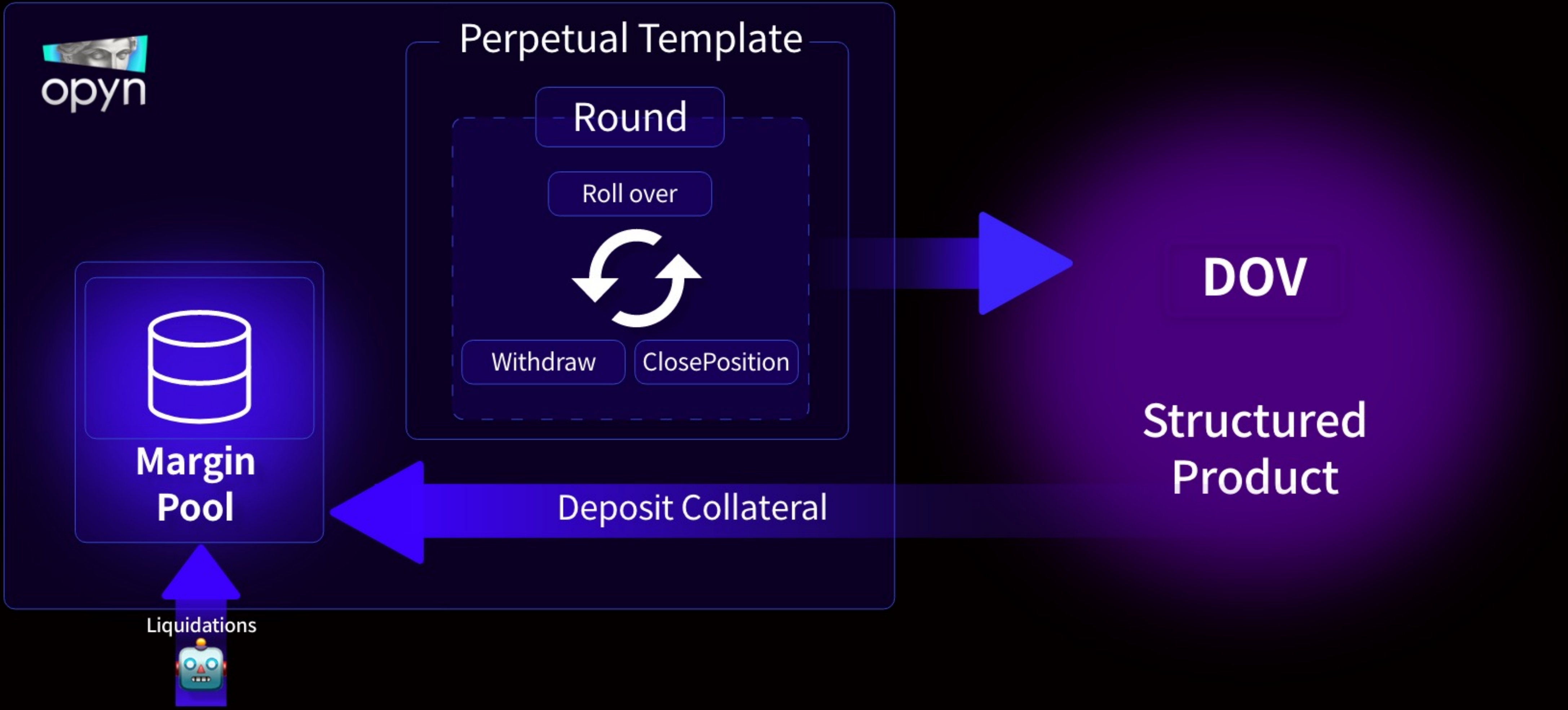
Opyn: Gamma Protocol

Trading Process



Opyn: Gamma Protocol

Operations Method



Opyn: Pros and Cons

PROS

1. Since it is an ERC-20 token, it can be traded in various markets

2. Buyers can quickly settle accounts without opening the vault or doing anything else

3. Strike Price can be set as seller's likes without interval restrictions

4. Since it provides a template, individuals or users can easily operate DOVs

CONS

1. Certain users have price adjustment rights, which violates decentralization

2. Centralization problems arise because the order book goes back from off-chain

3. The width of assets handled is narrow because Whitelist is designated

Our Approach

- **Findings from Protocol Analysis**

  Option: Struct Producted Model (Ribbon Protocol)

Ribbon: Treasury Vault

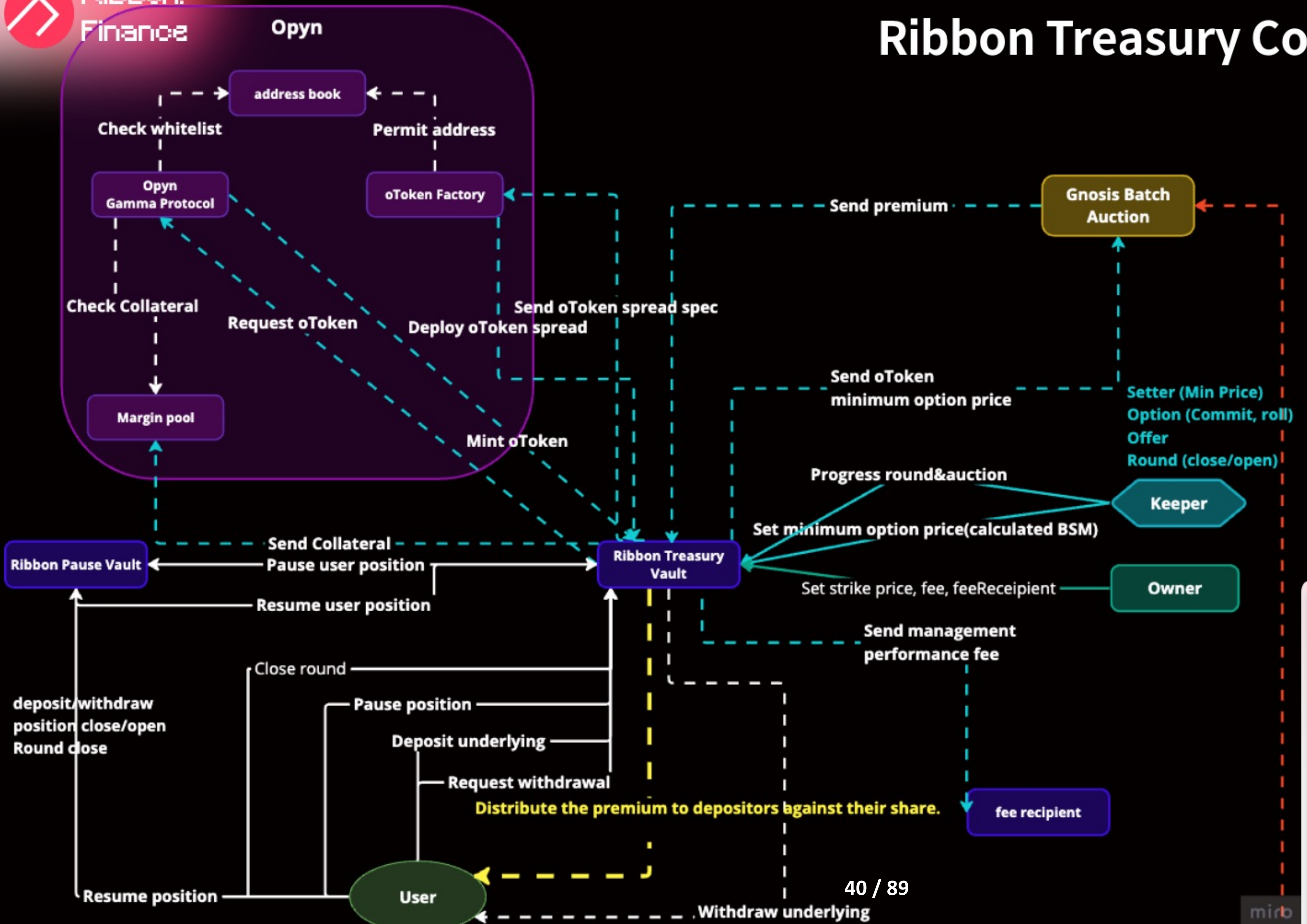
Opyn (Order Book Model) Specific issue

Ribbon

Category	
Custom Investment Strategies	Users with appropriate permissions should choose safe products to manage their assets.
Automated Strategies	It should be chosen as a haven for market changes.
Market Fluctuations Response	While the market is changing rapidly, there must be a way for users to react to it.
Option Selling Price Determination	Calculate option prices appropriately and be transparent about how they are calculated.
Staking Reward	An attractive compensation scheme must exist to maintain liquidity for option sellers.

Ribbon Finance

Ribbon Treasury Contract Service Flow



Ribbon Core Contract Access Tag

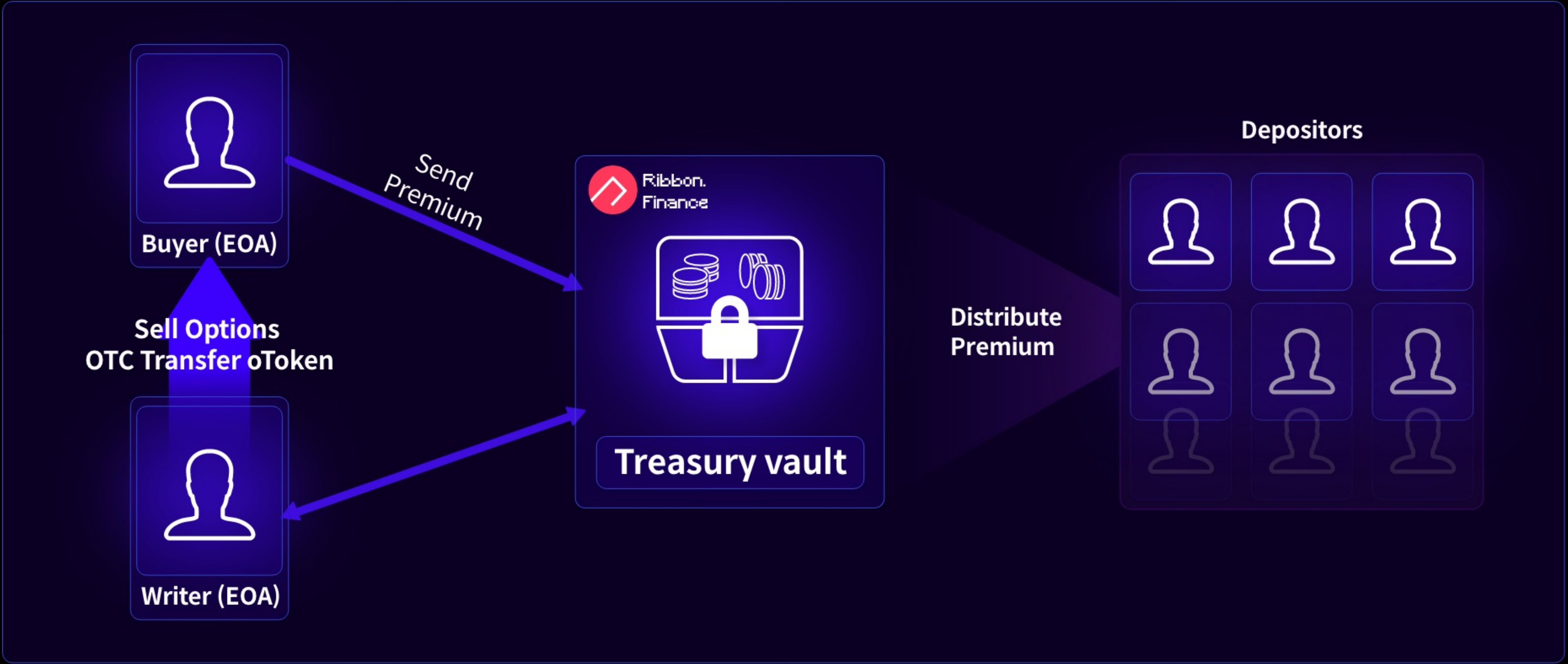
Keeper
Setter (*Price,*Fee)
Offer
Round (Close/Open)
Option Price

User
Deposit / Withdraw
Round Close
Position Close / Open
Set Price willing to pay

Owner
Setter(Price, Fee)

Ribbon: Treasury Vault

Trading Process



Ribbon: Treasury Vault

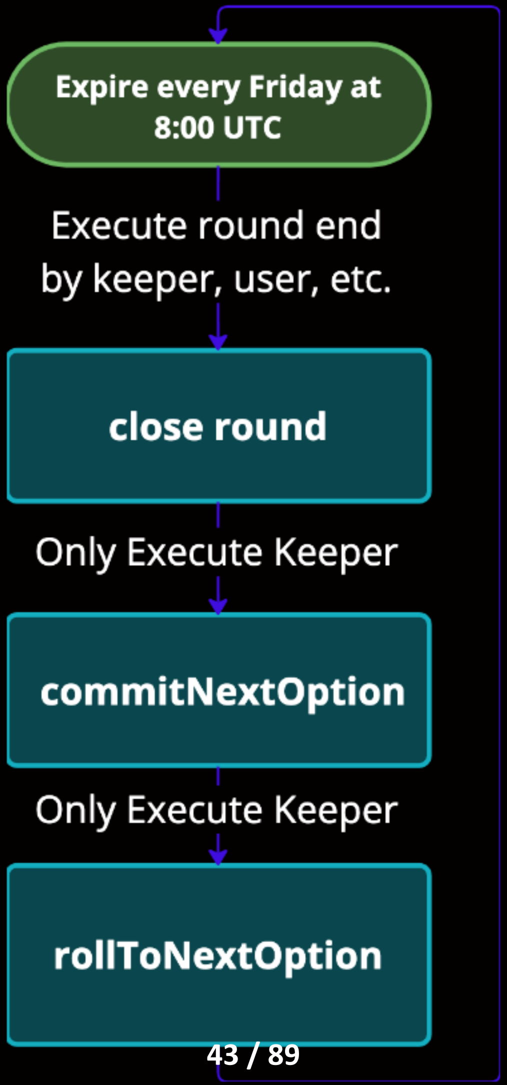
Operations Method

- Concept => rounds based on weekly expiry options
- At the end of the round, the next week will be counted as the next round
- Trade Only with vault deposit, as vault does the execution for you
- Yield farming using the governance token, the Vault Stake Token (RBN)
- Conduct auctions based on Gnosis Auction for option buyers

Ribbon: Treasury Vault

Operations Method: Round

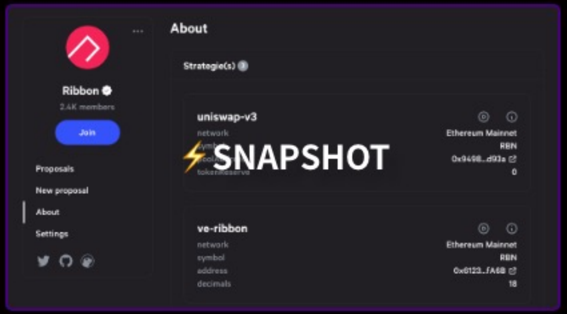
End Vault Round



Ribbon: Structured Product Model

Token & Governance Structure

- RBN, veRBN(vote-escrowed RBN) Token
- Re-distribute protocol fees based on stake
- Lock -> RBN Token, Earn <- veRBN (Reward distribution over time)
- Following Bravo's standard of one vote per token
- Voting is done through governance tokens and snapshots



About

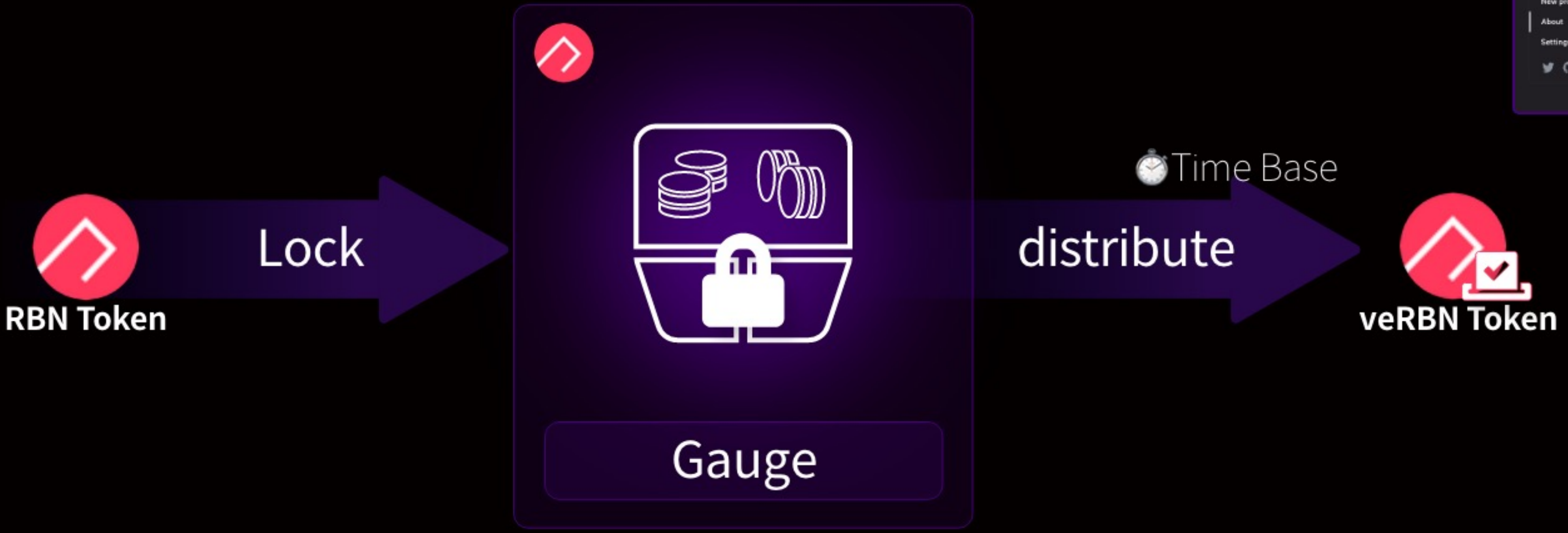
Strategie(s)

uniswap-v3

network	Ethereum Mainnet
symbol	RBN
poolAddress	0x9498...d93a
tokenReserve	0

ve-ribbon

network	Ethereum Mainnet
symbol	RBN
address	0x0123...fA68
decimals	18



Gnosis Auction

Ribbon: Pros and Cons

PROS

1. Save on gas by having a keeper process users' combined funds at once when selling options.

2. The keeper automatically trades the option for you, so you don't have to take any action.

3. The vault is configured to allow you to select different underlying assets and strategies.

4. Does not charge protocol fees in case of option losses

5. Earn additional income by staking share tokens

CONS

1. Centralized option pricing with keepers

2. It is impossible to hedge against rapid market movements within a round.

3. 1-week delay in processing deposits and withdrawals, so you cannot immediately access assets

4. Protocol fees are high due to centralized processing by keepers

Our Approach

- **Findings from Protocol Analysis**

  Option: AMM Model (Lyra Protocol)

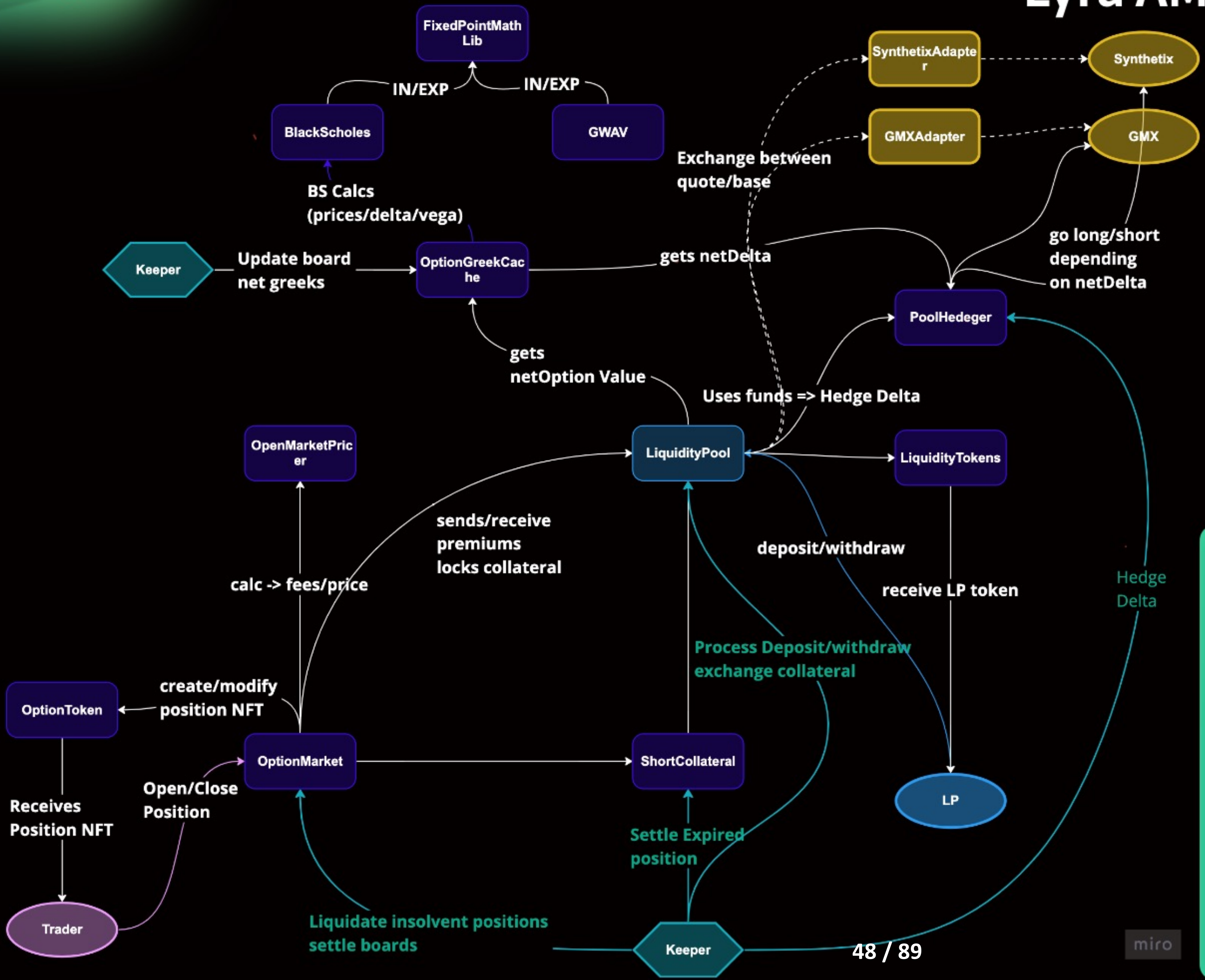
Lyra: Amms

Lyra Specific issue

Lyra

Category	
Internal AMMs	AMM liquidation should be standardized based on the collateral options.
AMM Liquidity Provide	The profit structure based on liquidity provision should account for the losses incurred due to sustained trader win rates.
AMM Settlement	Option expiration settlements should be conducted by immediately reflecting the Chainlink price feed after maturity through the Keeper bot.
withdrawal Delay	Liquidity providers should be unable to withdraw funds from the pool during the cooldown period for stability.
AMM Insurance Fund	An insurance system should be in place to mitigate the volatility of option prices based on liquidity demand and supply.
AMM Price Calculation	The algorithmic price adjustment should be conducted based on the inherent volatility of option prices, considering the demand and supply dynamics at different price levels.
GMX / Synthetix Delta Neutrality	Based on AMM price management, price protection should be implemented through a Delta-list hedging pool.

Lyra AMMs Contract Service Flow



FixedPointMath Lib

IN/EXP

IN/EXP

BlackScholes

GWAV

BS Calcs (prices/delta/vega)

SynthetixAdapter

Synthetix

GMXAdapter

GMX

Exchange between quote/base

Keeper

Update board net greeks

OptionGreekCache

gets netDelta

go long/short depending on netDelta

PoolHedeger

gets netOption Value

Uses funds => Hedge Delta

OpenMarketPricer

LiquidityPool

LiquidityTokens

sends/receive premiums locks collateral

deposit/withdraw

receive LP token

Hedge Delta

calc -> fees/price

Process Deposit/withdraw exchange collateral

OptionToken

create/modify position NFT

OptionMarket

ShortCollateral

LP

Receives Position NFT

Open/Close Position

Settle Expired position

Trader

Liquidate insolvent positions settle boards

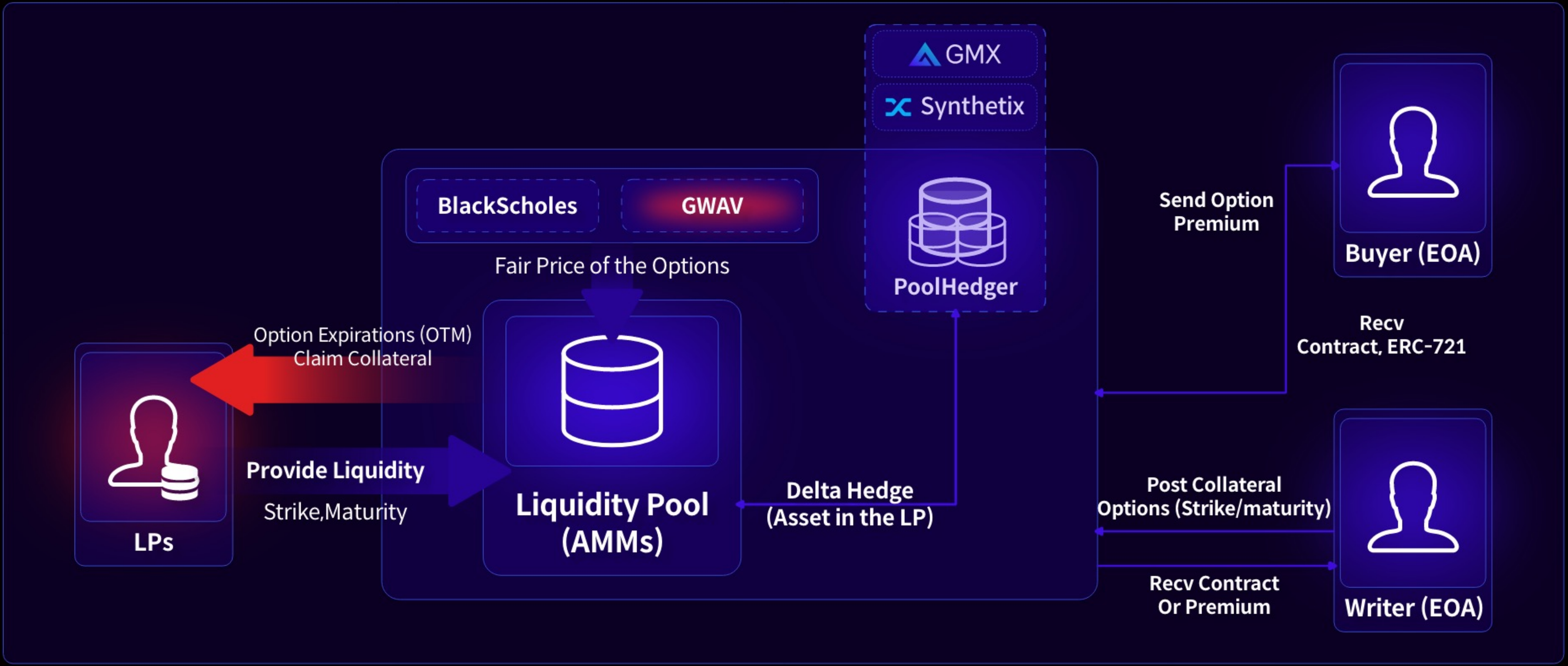
Keeper

Lyra Core Contract Access Tag

Keeper	Settle Expired Board	Liquidate Position		
	Process Withdraw queue	Process deposit queue	Update Board/Greeks	
	Delta Hedge			
Trader	Position Open / Close	Collateral add		
Owner	Market Pause	Update	Init	Setter
Guardian	Circuit Breaker			

Lyra: AMMs Model

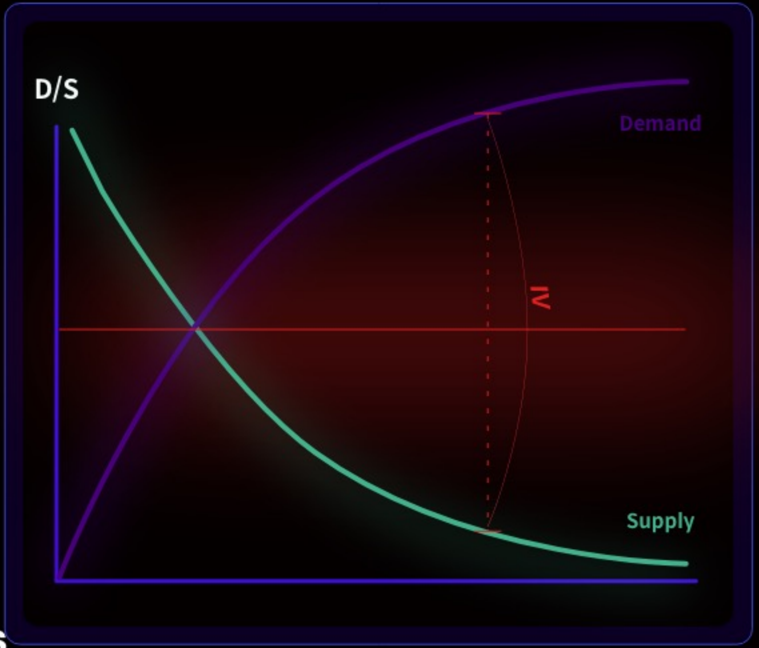
Trading Process

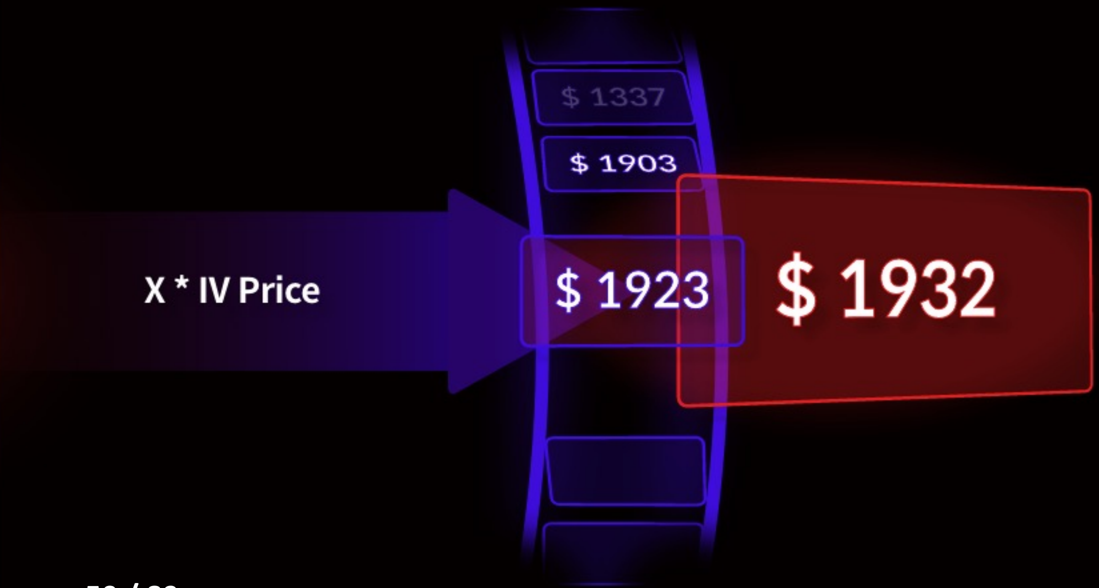


Lyra: AMMs Model

How trading works?: AMM Option Pricing

- Market Composition determines the Market Value of IV, which is the time-based expected volatility.
- Change in the cost of the same option based on the rate of change in IV.
- AMM IV management core mechanism, IV price adjustment based on supply and demand **(Demand ⬆ IV ⬇ | Supply ⬆ IV ⬇)**

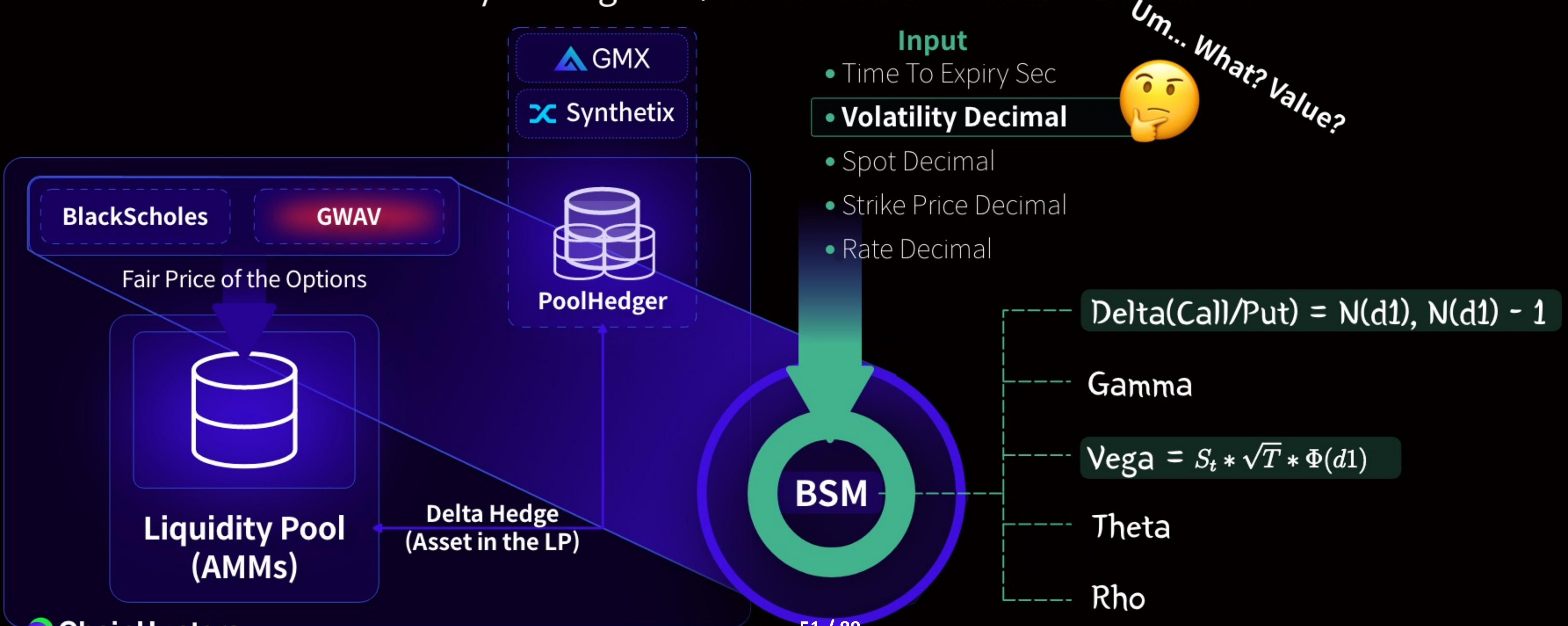




Lyra: AMMs Model

How trading works?: Black Scholes Model

- Since MM knows the other variables except IV, but not the actual IV data, the trader is essentially trading on IV, but the actual IV data is unknown.



Um... What? Value?

GMX

Synthetix

BlackScholes

GWAV

Fair Price of the Options

PoolHedger

Liquidity Pool (AMMs)

Delta Hedge (Asset in the LP)

Input

- Time To Expiry Sec
- **Volatility Decimal**
- Spot Decimal
- Strike Price Decimal
- Rate Decimal

BSM

Delta(Call/Put) = N(d1), N(d1) - 1

Gamma

Vega = $S_t * \sqrt{T} * \Phi(d1)$

Theta

Rho

Lyra: AMMs Model

How trading works?: Dynamic Fees used to VEGA

- Dynamically change the value based on Vega sensitivity, determined by differences in the Following variables

Fees 💵

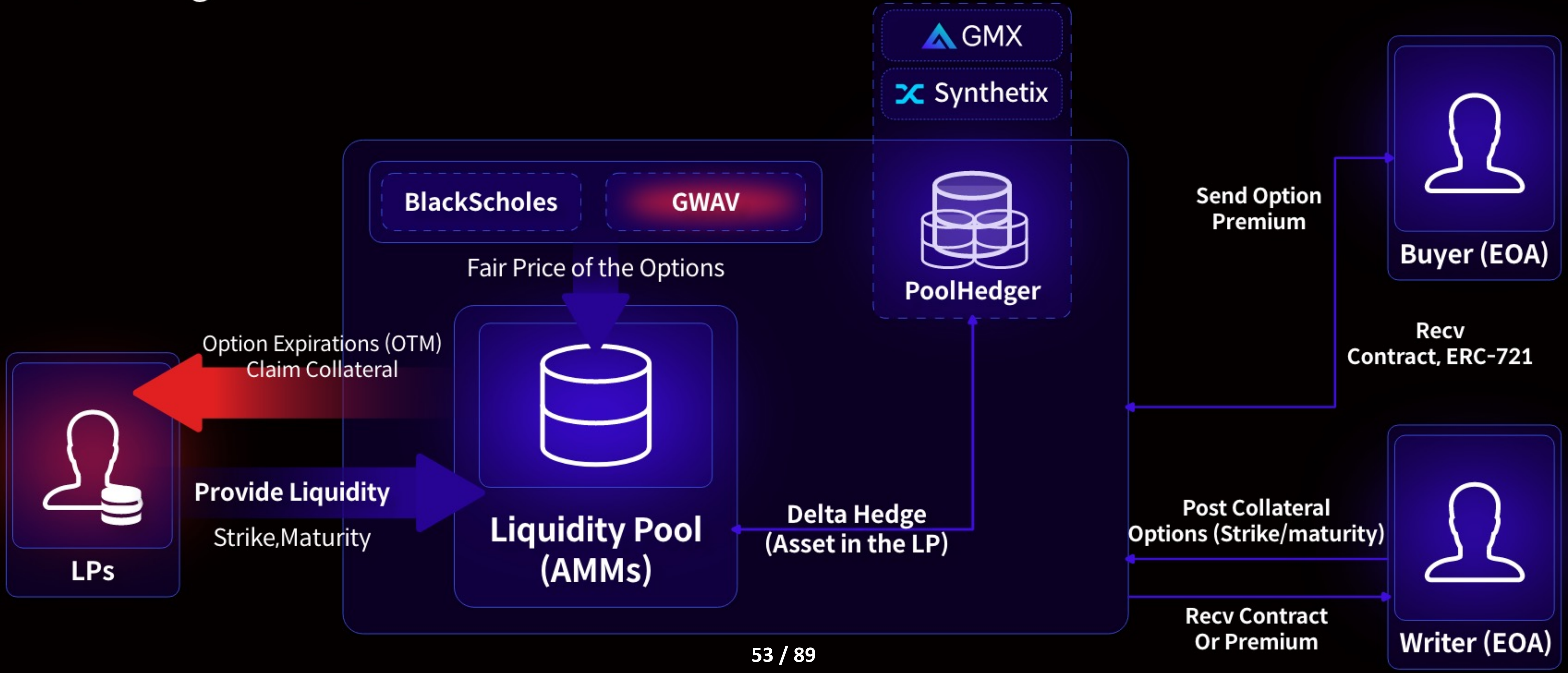
- Fixed Fee (Option Price)
- Fixed Fee (Exchange Price)
- **Dynamic Fee (Liquidity Pool Vega Risk)**

baseIV * GWAV * Trade Strike Skew ratio * vega

Lyra: AMMs Model

Operations Method: Unlimited deposit/withdrawal type for options products

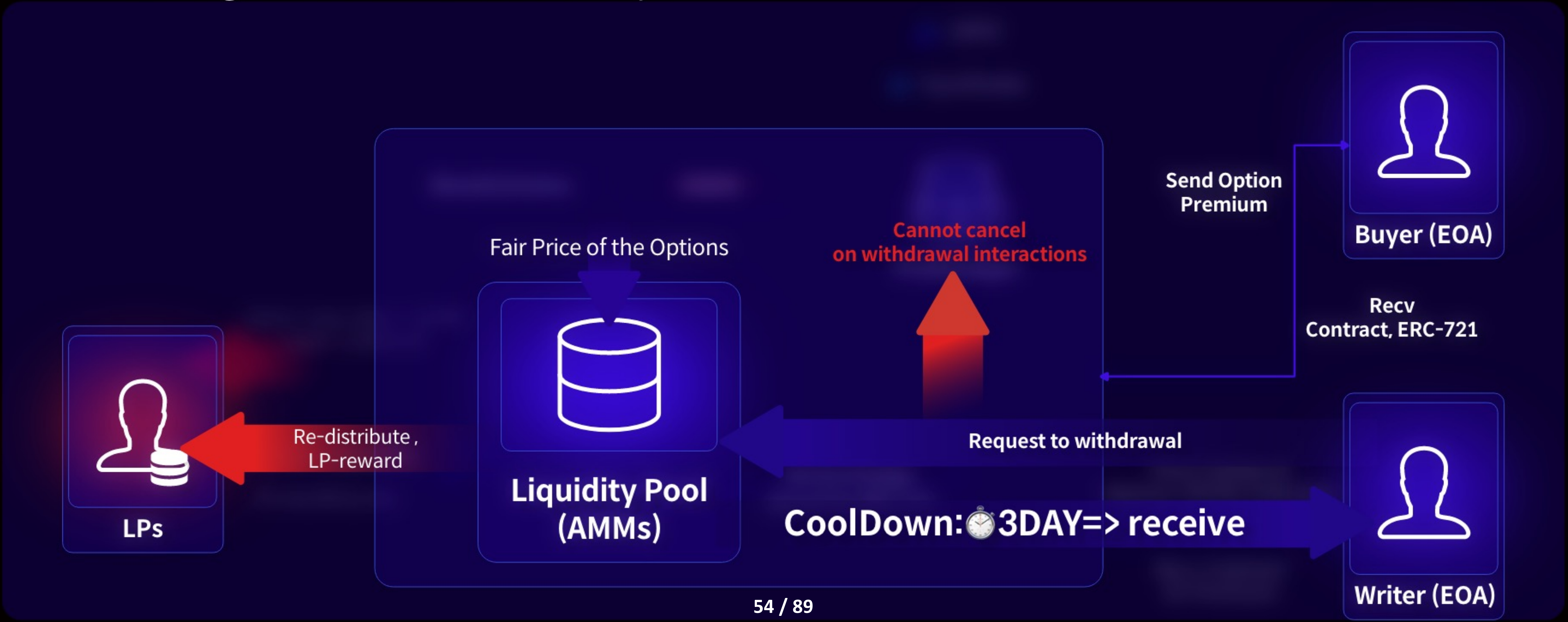
- Dynamically change the value based on Vega sensitivity, determined by differences in the Following variables



Lyra: AMMs Model

Operations Method: Unlimited deposit/withdrawal type for options products

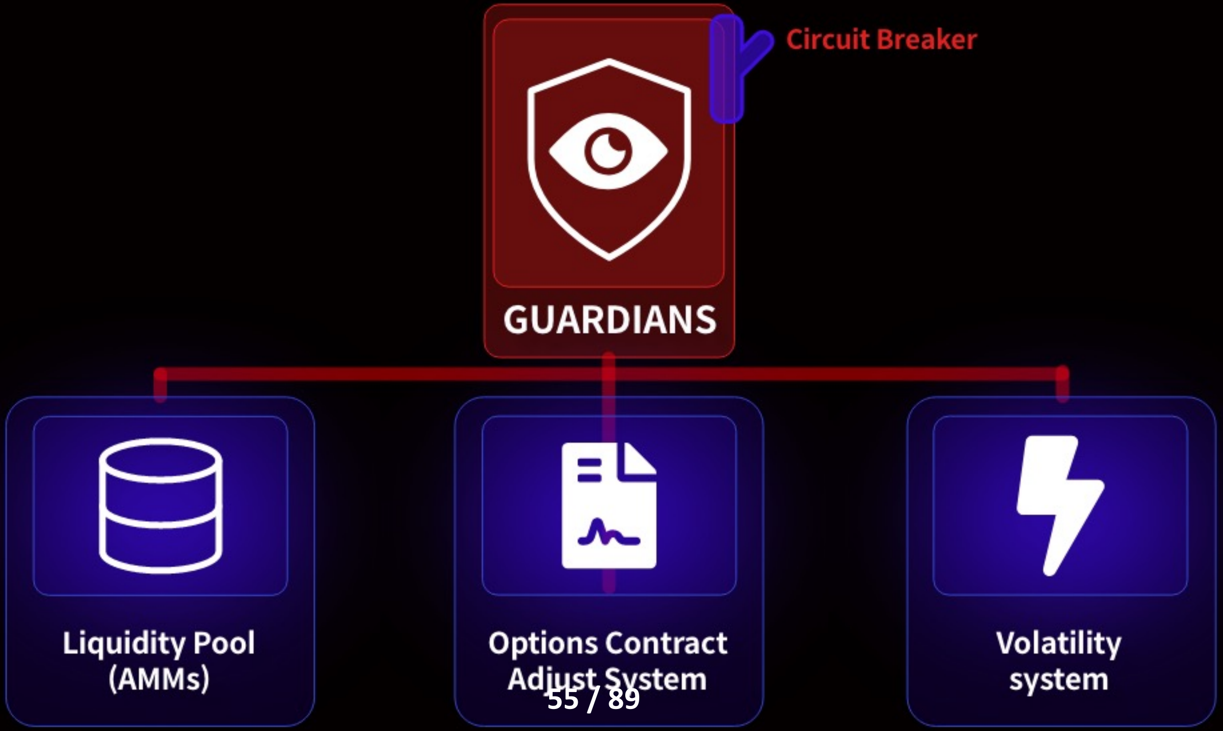
- Implement a structure for deposit/withdraw funds to and from AMMs at any time without incurring withdrawal fees and delays



Lyra: AMMs Model

Operations Method: AMM Pool Protected use Circuit Breaker System

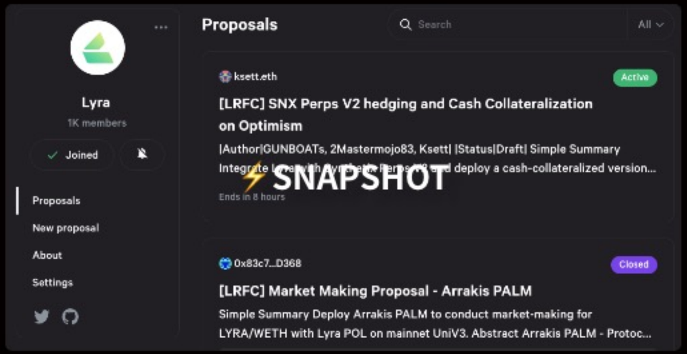
- Protect existing LPs, it’s build with circuit breakers
- If any of the circuit breakers are triggered, all deposits/withdrawals are blocked until The condition is resolved.
- CoolDown Timer will start, during which deposits/withdrawals will continue be blocked



Lyra: AMMs Model

Token & Governance Structure

- Naive Token:LYRA (L2)
- Governance => Protocol System
- Lyra Council representation centered on a committee of five LYRA token holders, elected by the public.
- LEAP Framework
- Elect a new Council after 4 months of activity



⚡SNAPSHOT

ksett.eth — Active

[LRFC] SNX Perps V2 hedging and Cash Collateralization on Optimism

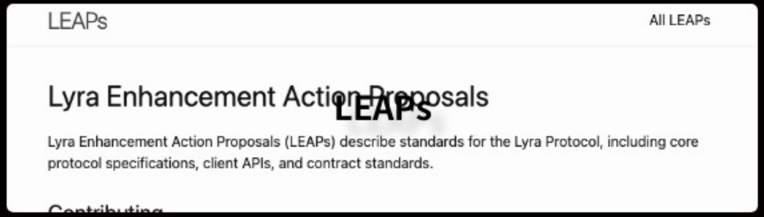
|Author|GUNBOATs, 2Mastermojo83, Ksett| |Status|Draft| Simple Summary Integrate Lyra with Synthetix Perps V2 and deploy a cash-collateralized version...

Ends in 8 hours

0x83c7...D368 — Closed

[LRFC] Market Making Proposal - Arrakis PALM

Simple Summary Deploy Arrakis PALM to conduct market-making for LYRA/WETH with Lyra POL on mainnet UniV3. Abstract Arrakis PALM - Protoc...



LEAPs

Lyra Enhancement Action Proposals

Lyra Enhancement Action Proposals (LEAPs) describe standards for the Lyra Protocol, including core protocol specifications, client APIs, and contract standards.

Contributing

Lyra: Pros and Cons

PROS

1. Based on the AMM model, it is possible to manage liquidity pools using ERC-20 tokens in a market-based approach, utilizing the skew adjusted pricing model.

2. Hedge the risks generated by liquidity providers using Synthetix/GMX to maintain more liquidity in the protocol.

3. Apply the Black-Scholes option pricing model to handle non-permanent losses and the pricing of unbuyable options.

4. Hedge LP delta lists by leveraging the underlying assets through the AMM model.

5. Quantify the vega risk and integrate it into a dynamic fee structure to support risk reduction in order to facilitate advantageous trades.

CONS

1. If there is insufficient liquidity for delta-neutral positions in Synthetix/GMX, position management may be restricted.

2. Incorrect price estimation, delayed liquidation, and settlement errors can occur due to flaws in third-party protocols, resulting in losses for the AMM.

3. Centralized processing through the Keeper bot, including critical operations such as Black-Scholes coefficients and major settlement processing, can lead to system limitations in case of malfunctions.

4. During periods of high pool utilization, liquidity providers may face restrictions on withdrawing funds from the pool after the cooldown period.

Our Approach

- **Findings from Protocol Analysis**

  Option: SSOV Model (Dopex Protocol)

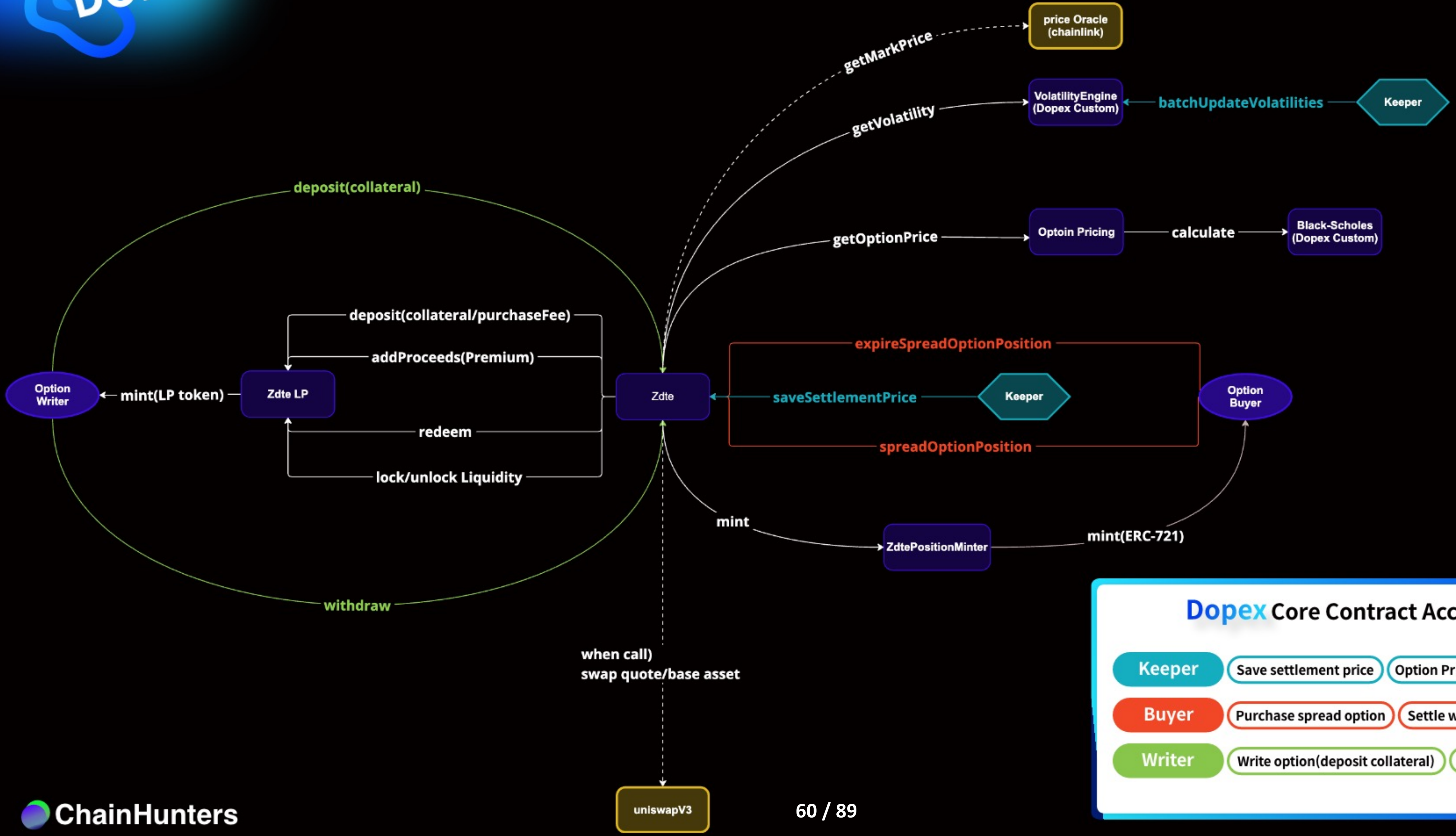
Dopex: 0dte

Dopex (Single Staking Option Vault) Specific issue

Dopex

Category	
Option writer constraints	If the option seller’s collateral has not been utilized, it should be possible to withdraw.
Option writer constraints	The option seller must be able to specify a minimum option price.
Limitations on Strike Scope	There should be a range of strike prices that the option seller and buyer can specify.
Staking Reward	If the value of the staking reward decreases, it should be changed to an attractive one.
Strategy Product	When constructing strategy instruments, consider the minimum amount of swaps.

Dopex 0dte Contract Service Flow

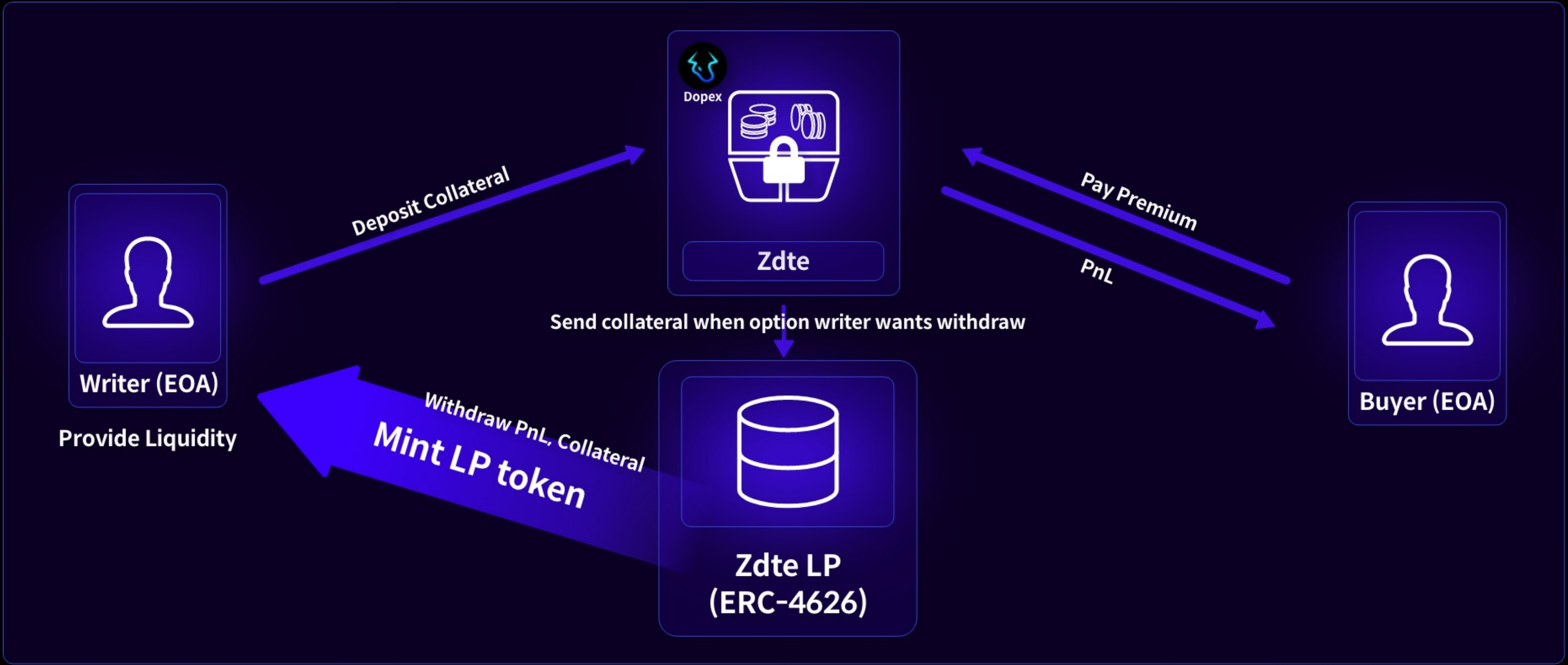


Dopex Core Contract Access Tag

Keeper	Save settlement price	Option Pricing Volatility Update
Buyer	Purchase spread option	Settle with NFT receipt
Writer	Write option(deposit collateral)	Withdraw using LP token

Dopex: 0dte

Trading Process

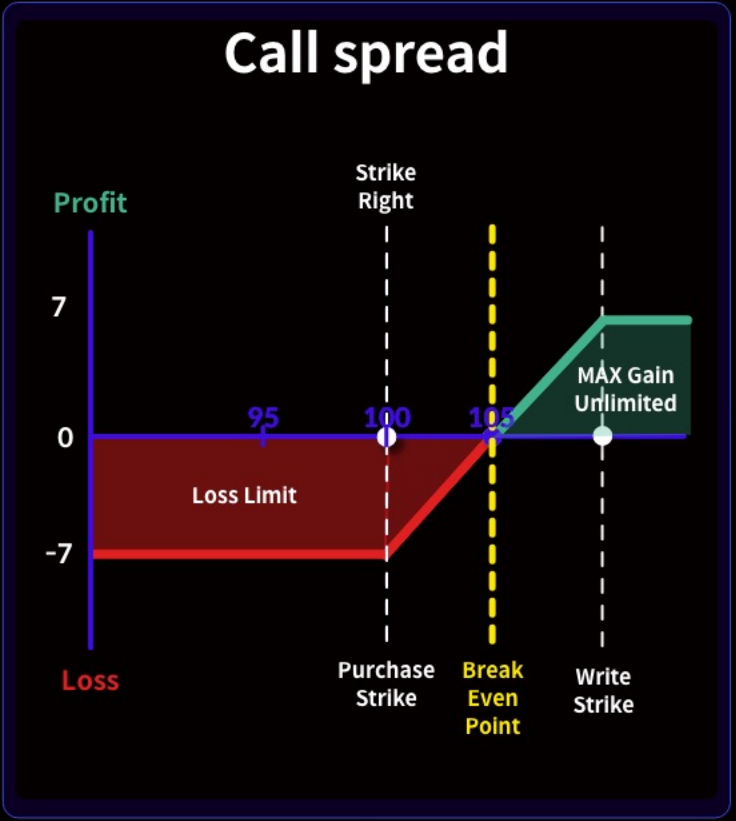


Dopex: 0dte

Operations Method

- Concept => rounds-based 1-day expiry spread strategy options.
- Option writers can't select which strike price they want to sell the option. The short option's strike price must be deep OTM than the long option.
- Option buyer selects call or puts option spread.
- At the end of the round, Option Buyer settled pnl.
- The option writer's collateral will automatically roll over.
- Fully-funded margin is possible since 0dte is a spread strategy option.

Spread buyer Pepe



Dopex: Pros and Cons

PROS

1. Reduce liquidation risk with fully-funded margins

2. Enable option selling through the Vault method to provide liquidity in the Fully-Funded method

3. Provide liquidity for selling options by offering to stake rewards to cover impermanent and infinite losses on the seller's side.

4. Reward distribution is proportional to the time deposited and utilization is on a FIFO basis, allowing option sellers to quickly deposit collateral to enable option purchases.

CONS

1. No MM concept makes it impossible to sell/buy options at the time wanted

2. Exposure to collateral risk when constructing a strategy with a fully-funded margin structure

3. Unable to set desired option price because options are sold by depositing into a vault.

Our Approach

- Contract Design Pattern based on Audit Matching Table

Contract Design Pattern based on Audit Matching Table

Common matching category: margin

Category

- **Margin**
- Liquidate
- Oracle
- Option Pricing
- Managerment to Risk
- Role
- Strike Style
- Proof of Position
- Market Maker
- Option Writer / Buyer
- On-Off Chain

- Hold the initial margin sufficiently to cover the option buyer's max pnl in Fully-Funded.

- Prevent bad debt by continuously evaluating the collateral value and appropriately notifying margin calls.

- Ensure that the necessary margin is properly calculated to prevent damage to the protocol.

Contract Design Pattern based on Audit Matching Table

Common matching category: Liquidate

Opyn

Category

Margin

Liquidate

Oracle

Option Pricing

Managerment to Risk

Role

Strike Style

Proof of Position

Market Maker

Option Writer / Buyer

On-Off Chain

- Evaluate the value of collateral with liquidation robots to keep its position safe.

- Make liquidation more active by paying users rewards for liquidation.

- The price interval should be appropriately selected, If an auction is held for each block to proceed with liquidation

Contract Design Pattern based on Audit Matching Table

Common matching category: Oracle

Category

- Margin
- Liquidate
- **Oracle**
- Option Pricing
- Management to Risk
- Role
- Strike Style
- Proof of Position
- Market Maker
- Option Writer / Buyer
- On-Off Chain

- Bring a reliable Oracle price to protect the reliability of the protocol.

- Derive accurate computational results by taking recent data safe from manipulation accurately.

- Determine Values used as self-updates, such as IV by voting like governance notes

- users should not have permission to set prices.

Contract Design Pattern based on Audit Matching Table

Common matching category: Option Pricing

Lyra

Category

- Margin
- Liquidate
- Oracle
- **Option Pricing**
- Managerment to Risk
- Role
- Strike Style
- Proof of Position
- Market Maker
- Option Writer / Buyer
- On-Off Chain

- Use the correct formula and avoid making a mistake in calculation.

- Update Indicators in an appropriate cycle to reflect the flow of the market, If implemented on-chain

- Manage the implementation formula transparently if implemented off-chain.

- Assign weights and values of uniform frequency to the intrinsic rate of change, determining the price of black Scholes.

Contract Design Pattern based on Audit Matching Table

Common matching category: Managerment Risk

Category

- Margin
- Liquidate
- Oracle
- Option Pricing
- **Managerment to Risk**
- Role
- Strike Style
- Proof of Position
- Market Maker
- Option Writer / Buyer
- On-Off Chain

- The ability to stop the system in an emergency must be present to prevent protocol disruption

- Asset Prices should not be manipulated by external factors.

- Countermeasures must be taken to prevent damage caused by abnormal asset prices in the case a market event occurs

- Insurance fund or other countermeasures should be prepared in case of liquidation failure or lack of liquidity

Contract Design Pattern based on Audit Matching Table

Common matching category: Role

Category

- Margin
- Liquidate
- Oracle
- Option Pricing
- Managerment to Risk
- **Role**
- Strike Style
- Proof of Position
- Market Maker
- Option Writer / Buyer
- On-Off Chain

- A governance vote shall determine the keeper who sets the round, updates the volatility, and sets the expiry date.

- Dangerous tasks when set by ordinary users should be properly identified and approved by guaranteed users.

- The qualification requirements should be properly evaluated When granting centralization rights to users

Contract Design Pattern based on Audit Matching Table

Common matching category: Strike Style

Dopex

Ribbon

Category

- Margin
- Liquidate
- Oracle
- Option Pricing
- Managerment to Risk
- Role
- **Strike Style**
- Proof of Position
- Market Maker
- Option Writer / Buyer
- On-Off Chain

- Prices should be standardized through Strike intervals to increase market efficiency.

- Calculate Premiums, rewards, pnl, etc., through appropriate calculation formulas minimizing errors or errors.

- The setting of the settlement price should be limited to one time so that the settlement price cannot be overwritten.

- Tokens for position verification should be incinerated when settlement is completed to prevent duplicate settlement.

- verify that the settlement price has been set at the time of settlement.

Contract Design Pattern based on Audit Matching Table

Common matching category: Proof of Position

Category

- Margin
- Liquidate
- Oracle
- Option Pricing
- Managerment to Risk
- Role
- Strike Style
- **Proof of Position**
- Market Maker
- Option Writer / Buyer
- On-Off Chain

- To prevent ERC4626 vault share token inflation, each share token minting implementation must ensure that it operates within a specified range.

- When handling ERC721 receives proper validation should be added to avoid accessing internal state variables and giving them excessive scope.

- If the token value is used in practical services, token allocation, and retrieval should be carried out appropriately.

- Manage status data to ensure accurate matching of information about options in the token and have it verified by internal reviewers and validators.

- If the user's position information is stored as a local variable, it should be updated promptly to ensure that there are no problems with the settlement process.

Contract Design Pattern based on Audit Matching Table

Common matching category: Market Maker

Category

- Margin
- Liquidate
- Oracle
- Option Pricing
- Managerment to Risk
- Role
- Strike Style
- Proof of Position
- **Market Maker**
- Option Writer / Buyer
- On-Off Chain

- Ensure that underlying and collateral assets that the maker provided liquidity are validated within the protocol.

- A dynamic algorithm should be applied to set the price range so that the compensation of makers complies with the allowed value.

Contract Design Pattern based on Audit Matching Table

Common matching category: Option Writer / Buyer

Opyn Lyra

Category

- Margin
- Liquidate
- Oracle
- Option Pricing
- Managerment to Risk
- Role
- Strike Style
- Proof of Position
- Market Maker
- **Option Writer / Buyer**
- On-Off Chain

- Make sure that the strike price is the strike price used in the round to prevent abnormal PNLs and utilize collateral.

- Bad debits should be prevented by ensuring that only as many options can be purchased as the vault's liquidity allows.

- Make sure that the deposit of collateral and the purchase of options are in the corresponding rounds, so that it is not possible to deposit collateral in a round that has already taken place, or to purchase options in a round that has not yet taken place.

- Prevent option sellers from settling for more than the collateral they have deposited.

Contract Design Pattern based on Audit Matching Table

Common matching category: On-Off Chain

Dopex

Category

- Margin
- Liquidate
- Oracle
- Option Pricing
- Managerment to Risk
- Role
- Strike Style
- Proof of Position
- Market Maker
- Option Writer / Buyer
- **On-Off Chain**

- Ensure that the Maker’s liquidity supply is healthy and that the underlying and collateral assets are validated assets within the protocol.

- To prevent liquidity supply inflation, weights, verification levels, and access from unauthorized accounts should be considered.

- Dynamic algorithms should be applied to set price ranges to ensure that Makers’ reward issuance adheres to the allowed values.

- When implementing on-chain options, it is important to be aware of the situations where MEVs are possible and have a plan in place to deal with them.

- On-chain, it is important to recognize that the expiration of an option does not mean that the option’s settlement price is set, and ensures that the the settlement price is set at settlement.

Contract Design Pattern based on Audit Matching Table

Threat modeling: Options Model implementation-unique issues

Order Book

- Market Creation
- OTC Transactions
- Centralized Authority
- Counterparty
- Expiration Date Liquidty
- Liquidation System

AMMs

- Internal AMMs
- AMM Liquidity Provide
- AMM Settlement
- Withdrawal Delay
- AMM Insurance Fund
- AMM Price Calculation
- GMX/Synthetix Delta-Neutrality

Structured Products

- Custom Investment Strategies
- Automated Strategies
- Market Fluctuations Response
- Option Selling Price Determination
- Staking Reward

Single Staking Vault

- Option Writer Constraints
- Limitations on option trading-range
- Staking Reward
- Strategy product

Security Analysis

- Dopex: Lack of check on settlemtPrice

Lack of check on settlemtPrice

Critical

Fixed

On-Chain<->Off-chain Network

Strike Style

DOPEX

Inspection Checklist for Defi Option Matching Table.

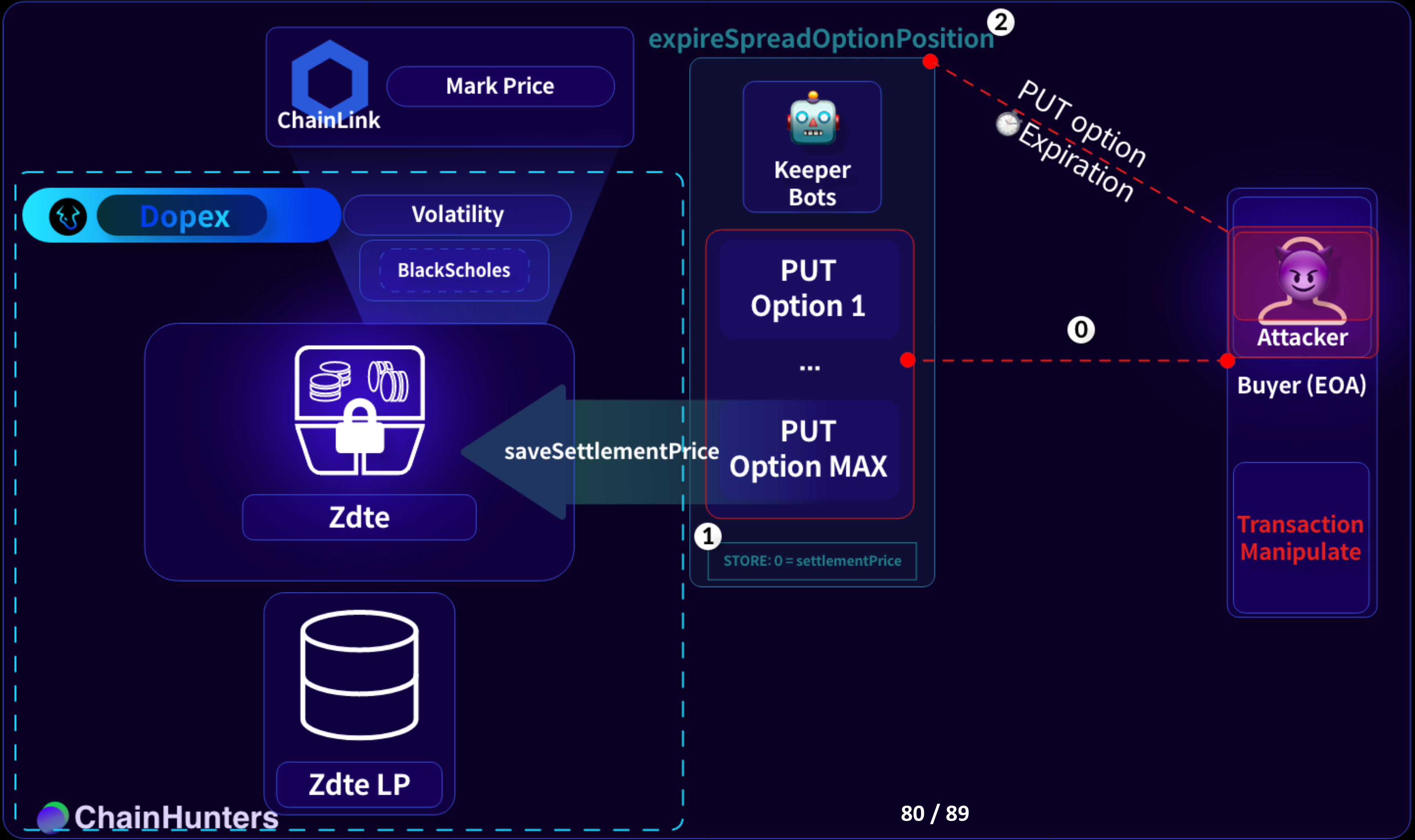
Common Category Table

Dopex

Category !	
On-Chain<->Off-chain Network	Must recognize that the On-chain expiration of an option does not mean that a settlement price has been set.
Strike Style	When creating an option protocol, make sure that the settlement price is set, not just the time of settlement.

Dopex: vulnerability flow

Lack of check on settlemtPrice Critical



Audit Matching Tag

On-Chain<->Off-chain Network

Strike Style

Vulnerability Flow Tree

0 The attacker purchase 0dte put option as much as possible

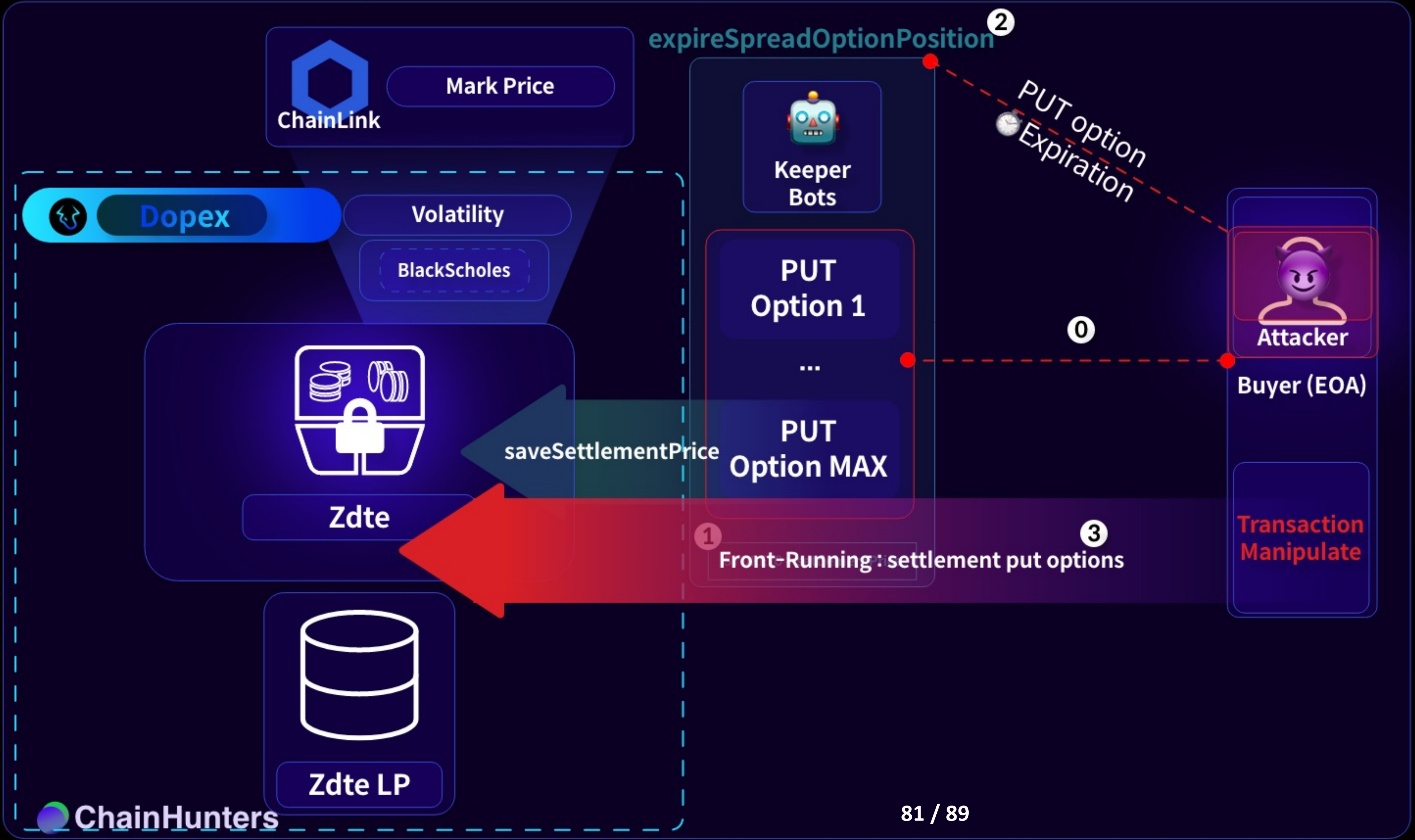
1 The settlementPrice of the put option purchased by the attacker is written to storage as 0 until it is set by the keeper after expiration.

2 The attacker calls the settlement function when the purchased The 0DTE option expires.

ChainHunters

Dopex: vulnerability flow

Lack of check on settlemtPrice Critical



Audit Matching Tag

- On-Chain<->Off-chain Network
- Strike Style

Vulnerability Flow Tree

0 The attacker purchase 0dte put option as much as possible

1 The settlementPrice of the put option purchased by the attacker is written to storage as 0 until it is set by the keeper after expiration.

2 The attacker calls the settlement function when the purchased The 0DTE option expires.

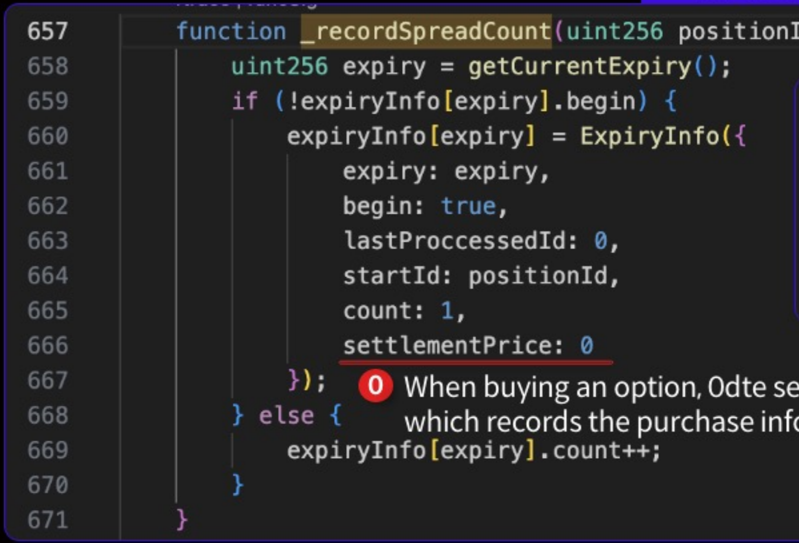
3 If the attacker can settle before the settlementPrice is set, the attacker will be able to settle a put spread option that was purchased with a settlementPrice of zero.

Dopex: Code Review

S3: Security Analysis

1. Lack of check on settlemtPrice

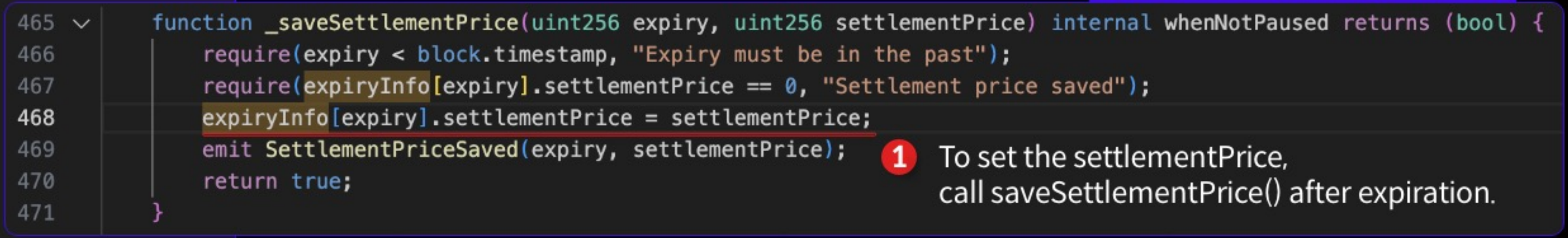
Zdte._recordSpreadCount()



```
function _recordSpreadCount(uint256 positionId) internal {
    uint256 expiry = getCurrentExpiry();
    if (!expiryInfo[expiry].begin) {
        expiryInfo[expiry] = ExpiryInfo({
            expiry: expiry,
            begin: true,
            lastProccessedId: 0,
            startId: positionId,
            count: 1,
            settlementPrice: 0
        });
    } else {
        expiryInfo[expiry].count++;
    }
}
```

0 When buying an option, 0dte sets the settlement price to zero and stores it in expiryInfo, which records the purchase information for the same expiration date.

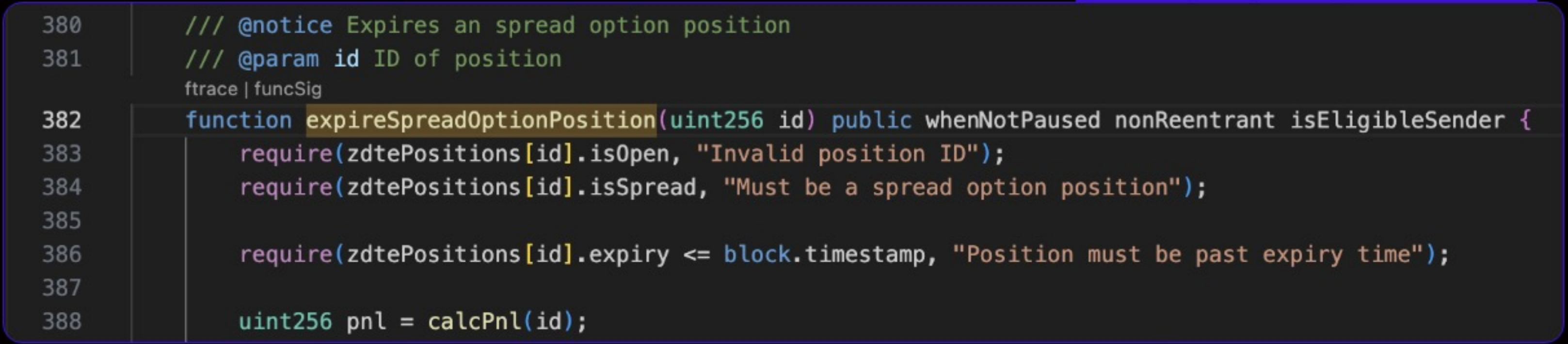
Zdte.saveSettlementPrice()



```
function _saveSettlementPrice(uint256 expiry, uint256 settlementPrice) internal whenNotPaused returns (bool) {
    require(expiry < block.timestamp, "Expiry must be in the past");
    require(expiryInfo[expiry].settlementPrice == 0, "Settlement price saved");
    expiryInfo[expiry].settlementPrice = settlementPrice;
    emit SettlementPriceSaved(expiry, settlementPrice);
    return true;
}
```

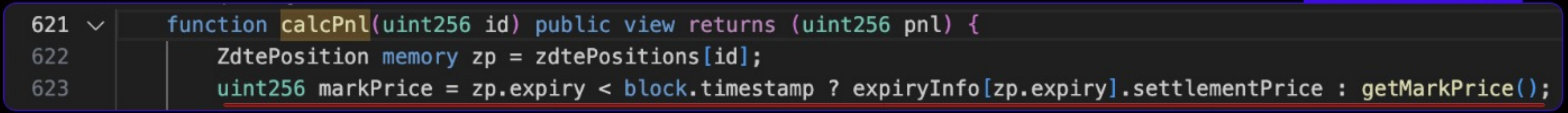
1 To set the settlementPrice, call saveSettlementPrice() after expiration.

Zdte.expireSpreadOptionPosition()



```
/// @notice Expires an spread option position
/// @param id ID of position
ftrace | funcSig
function expireSpreadOptionPosition(uint256 id) public whenNotPaused nonReentrant isEligibleSender {
    require(zdtePositions[id].isOpen, "Invalid position ID");
    require(zdtePositions[id].isSpread, "Must be a spread option position");

    require(zdtePositions[id].expiry <= block.timestamp, "Position must be past expiry time");

    uint256 pnl = calcPnl(id);
```

Zdte.calcPnl()



```
function calcPnl(uint256 id) public view returns (uint256 pnl) {
    ZdtePosition memory zp = zdtePositions[id];
    uint256 markPrice = zp.expiry < block.timestamp ? expiryInfo[zp.expiry].settlementPrice : getMarkPrice();
```

2 The settlement function only checks if the option has expired when settling after the expiry and uses the settlementPrice stored in expiryInfo as the settlement price.

Dopex: POC

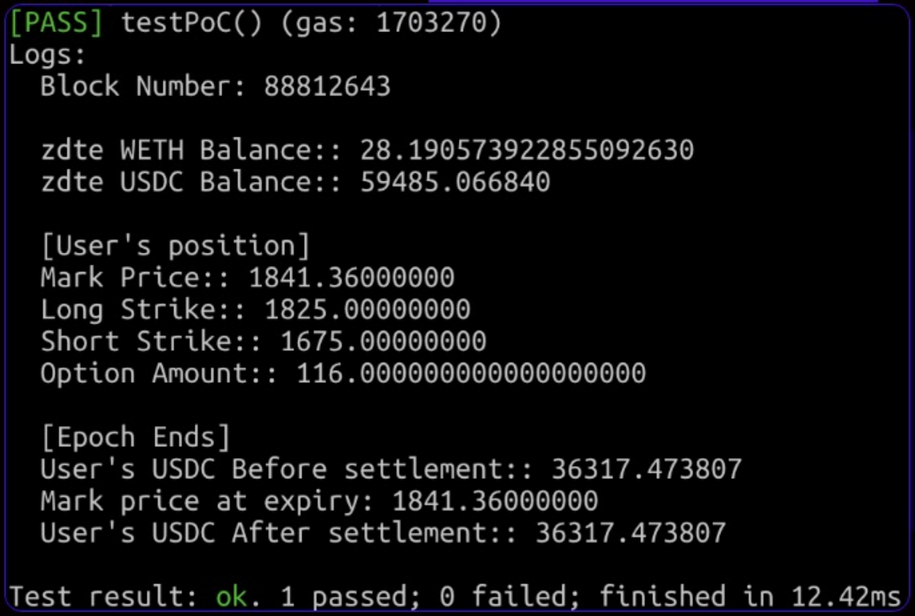
S3: Security Analysis

1. Lack of check on settlemtPrice

setup

Block Number: 88812643
strategy = put option spread

Normal Process

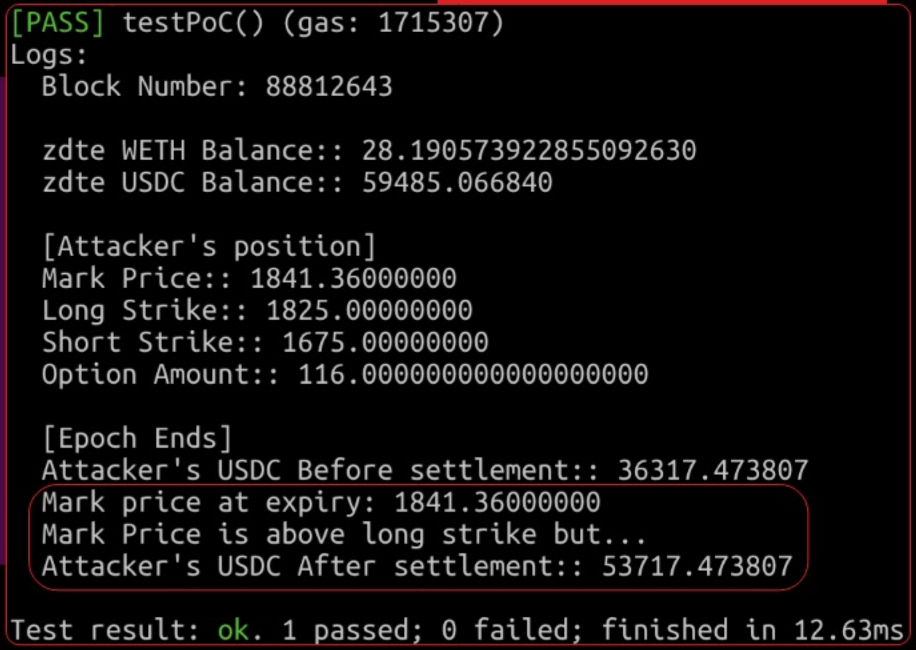


```
[PASS] testPoC() (gas: 1703270)
Logs:
  Block Number: 88812643

  zdte WETH Balance:: 28.190573922855092630
  zdte USDC Balance:: 59485.066840

  [User's position]
  Mark Price:: 1841.36000000
  Long Strike:: 1825.00000000
  Short Strike:: 1675.00000000
  Option Amount:: 116.000000000000000000

  [Epoch Ends]
  User's USDC Before settlement:: 36317.473807
  Mark price at expiry: 1841.36000000
  User's USDC After settlement:: 36317.473807

Test result: ok. 1 passed; 0 failed; finished in 12.42ms
```

Diff Resource

Settle before the keeper sets the settlementPrice

Exploit Process

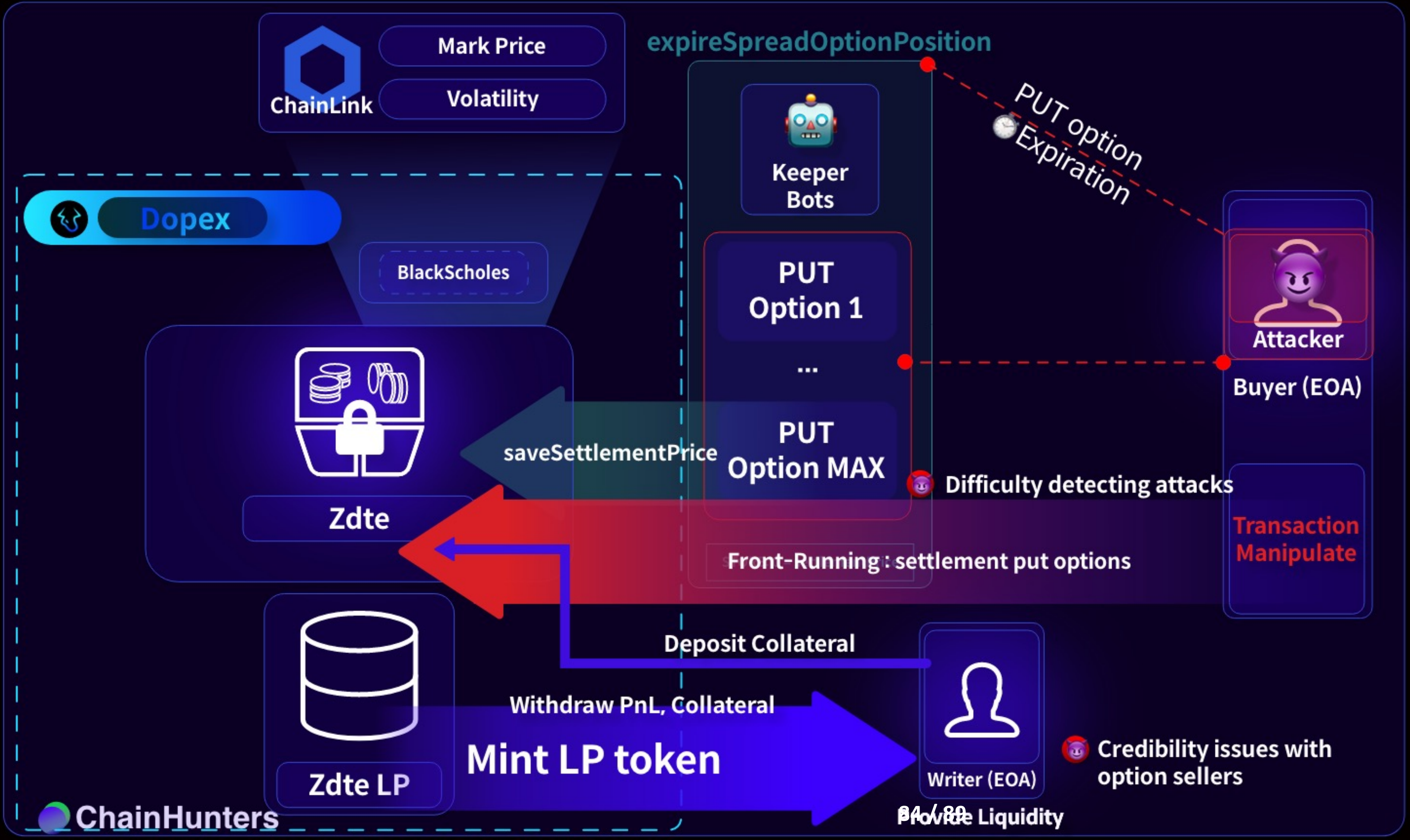


```
[PASS] testPoC() (gas: 1715307)
Logs:
  Block Number: 88812643

  zdte WETH Balance:: 28.190573922855092630
  zdte USDC Balance:: 59485.066840

  [Attacker's position]
  Mark Price:: 1841.36000000
  Long Strike:: 1825.00000000
  Short Strike:: 1675.00000000
  Option Amount:: 116.000000000000000000

  [Epoch Ends]
  Attacker's USDC Before settlement:: 36317.473807
  Mark price at expiry: 1841.36000000
  Mark Price is above long strike but...
  Attacker's USDC After settlement:: 53717.473807

Test result: ok. 1 passed; 0 failed; finished in 12.63ms
```

Dopex: Vulnerability Impact

S3: Security Analysis

1. Lack of check on settlemtPrice



Audit Matching Tag

On-Chain<->Off-chain Networ

Strike Style

Impact

Credibility issues with option sellers

Due to the nature of option vaults, using fully-funded margin, the option seller's collateral is directly exposed to the risk of the contract.

Due to the nature of Option vault, where there are no market makers, it is impossible to buy options if there are no option sellers.

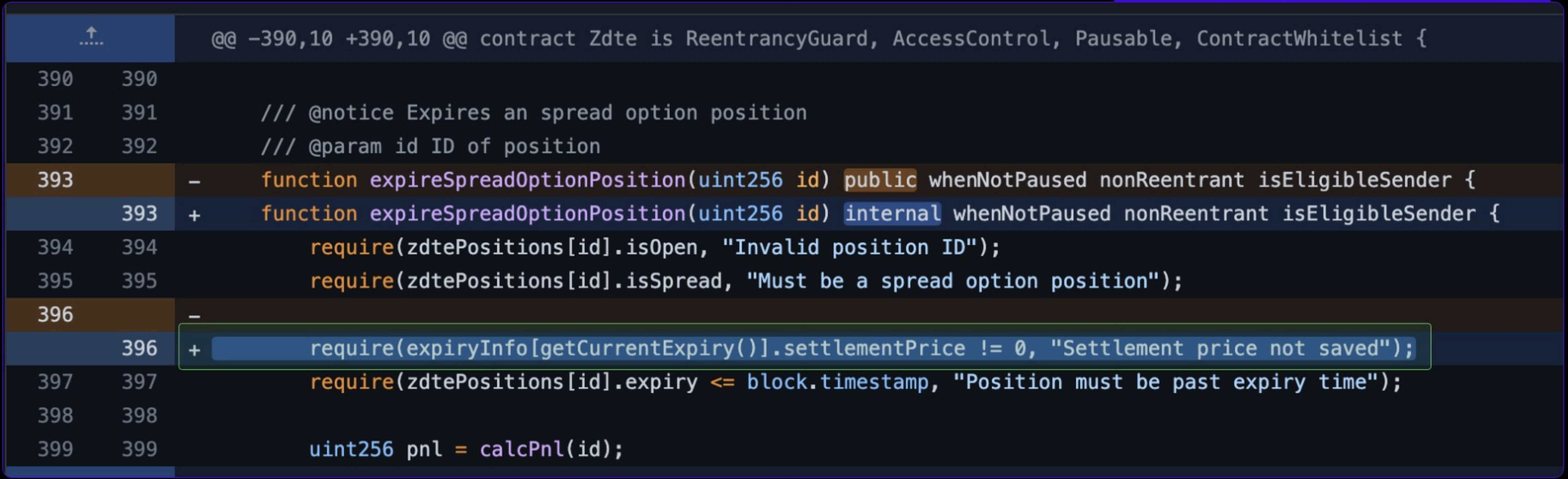
Difficulty detecting attacks

This attack only requires a settlement just before the keeper sets the settlementPrice, making the previous option purchase look like a normal option purchase.
This makes the attack unpredictable, making it easier for the attack to succeed.

Dopex: Vulnerability Mitigations

1. Lack of check on settlemtPrice

Zdte.expireSpreadOptionPosition()



```diff
@@ -390,10 +390,10 @@ contract Zdte is ReentrancyGuard, AccessControl, Pausable, ContractWhitelist {

     /// @notice Expires an spread option position
     /// @param id ID of position
-    function expireSpreadOptionPosition(uint256 id) public whenNotPaused nonReentrant isEligibleSender {
+    function expireSpreadOptionPosition(uint256 id) internal whenNotPaused nonReentrant isEligibleSender {
         require(zdtePositions[id].isOpen, "Invalid position ID");
         require(zdtePositions[id].isSpread, "Must be a spread option position");
-
+        require(expiryInfo[getCurrentExpiry()].settlementPrice != 0, "Settlement price not saved");
         require(zdtePositions[id].expiry <= block.timestamp, "Position must be past expiry time");

         uint256 pnl = calcPnl(id);
```

Validate if the settlement price is zero on expiration

Limitation & Future Work

Limitation & Future Work

Unfinished Tasks

- Complete multiple protocol validation and modeling tasks based on the DeFi Option Audit Matching Table.

Future Work

- Research to formalize and model the threats posed by implementing or operating trading strategy-structures outside the traditional options model structure at the code level.
- Conduct a global threat modeling study for DeFi option protocols implemented in multi-chain, non-EVM environments.
- Research the threats to chains that only apply DeFi services rather than scaling and rollups to solve problems caused by blockchain delays.

Conclusion

**The standards for DeFi options protocols have yet to mature,
and security still needs to be established.**

DeFi has introduced trading strategy structures and options systems from several existing off-chain-
environments. However, there are several threat levels due to vulnerabilities
in the intelligent contract code level for options systems and-
vulnerabilities for each implemented option model.

**If developers identify these model-specific vulnerabilities and share standardized
option model-specific audit matching tables, option protocols can be designed more safely.**

Thank You

ChainHunters | Theori X DREAMPLUS ACADEMY