Automated Market Maker for Digital Options

Lianne Li
lianne.li@divergence-protocol.com

December, 2023

Abstract

Divergence v1 is a novel noncustodial automated market maker for options with a predetermined payoff structure. It enables access to an extensive selection of options pools, each with a distinct underlying asset, strike price, maturity, and collateral token. The decentralized protocol facilitates on-chain peer-to-pool swaps of options tokens, with minimal friction, enhanced capital efficiency, and low transaction costs. Its model-free pricing approach empowers individual users to flexibly price and tailor options exposure.

Introduction

Existing DeFi protocols have auctioned and settled tokenized options on-chain. Yet, there is a notable absence of a liquid and low-friction decentralized options market, where users can trade from self-custodied wallets at their chosen times and prices, with control over specifications including underlying assets, strike prices, maturities, and quote assets.

Divergence v1 proposes a permissionless, noncustodial automated market maker (AMM) for options with a predetermined payoff structure. Its fundamental idea is to facilitate real-time price discovery of options in DeFi.

In market transactions, the protocol eliminates the mandate for smart contracts or external agents to price options through traditional theoretical models, such as the Black–Scholes model. This model-free approach removes the need for gas-consuming computations and trust-based set-ups. It ensures reliable execution under extreme market conditions, without the constraints of preconceived model assumptions and ensuing adjustments. Crucially, it empowers buyers and sellers to price options at their own discretion, potentially setting the stage for higher-order volatility derivatives [3].

Tokenized Options

An option gives its holder the right, not the obligation, to engage in a financial transaction involving an asset or a basket of assets. A standard European call or put option, respectively, provides the right to buy or sell an asset for its strike price at maturity. The European style settlement permits the exercise of options at maturity.

Unlike standard options, digital options, also called binary or bet options, represent the right to receive a fixed amount of payout. These options offer the advantage of having a predetermined risk and reward prior to a transaction. Digital options can serve as building blocks of standard options [1] and replicate the payoff structure of any financial asset [2]. They are versatile instruments for trading DeFi asset volatility, and provide a suitable hedge against sudden price moves of illiquid underlying assets. They are also useful in other areas, including but not limited to prediction markets.

At maturity T, a European digital call on an asset worth S_T with strike K pays:

$$\begin{cases} 1, & S_T \geq K \\ 0, & S_T < K \end{cases} \tag{1}$$

A European digital put with the same specification pays:

$$\begin{cases} 0, & S_T \geq K \\ 1, & S_T < K \end{cases} \tag{2}$$

The payout of a portfolio holding a digital call and a digital put is therefore:

$$\begin{cases} 1, & S_T \geq K \\ 1, & S_T < K \end{cases} \tag{3}$$

Let a pool (`Battle`) contract facilitate minting, swapping and settling of digital calls as token 0 (`Spear`), and digital puts as token 1 (`Shield`) for a chosen underlying asset, strike, maturity, and an ERC-20 token collateral used as a quote asset.

To swap for a digital call (put) amount ΔV_0 (ΔV_1), a trader sends a collateral amount ΔC_0 (ΔC_1) to the pool contract, which gives us the effective price of options:

$$P_c^0 = \frac{\Delta C_0}{\Delta V_0} \tag{4}$$

$$P_c^1 = \frac{\Delta C_1}{\Delta V_1} \tag{5}$$

At time $t < T$, digital calls and puts are valued at a discount to their probable payout of one collateral at maturity. i.e., P_c^0, $P_c^1 \in (0, 1)$ but practically set within [0.01, 0.99].

At maturity T, the holder of a digital call (or put) option is entitled to receive one collateral token, provided that the price of the underlying asset meets or exceeds (or falls below) the specified strike price.

The options are considered *Cash-or-Nothing* if stable coins are paid out, or *Asset-or-Nothing* if (wrapped) underlying assets are paid out. If a token other than stable coins or (wrapped) underlying assets is used as collateral, the options payout may exhibit varying correlation or no correlation at all with the underlying price.

Put-call Parity

Consider a portfolio holding a digital call and a digital put. According to the principle of put-call parity, it is valued at a forward contract delivering one collateral. A riskless profit can be made if a digital call and a digital put can be simultaneously bought for less than one collateral, given that either option pays out one collateral at maturity. The same holds true if a digital call and a digital put can be simultaneously sold for more than one collateral. To remain free of arbitrage, effective prices for digital calls and puts must add up to one:

$$\frac{\Delta \mathrm{C}_0}{\Delta \mathrm{V}_0} + \frac{\Delta \mathrm{C}_1}{\Delta \mathrm{V}_1} = 1 \tag{6}$$

When $\Delta \mathrm{V}_0$ and $\Delta \mathrm{V}_1$ are held equal, the expected return for holding $\Delta \mathrm{V}_0$ is the same as the collateral value of $\Delta \mathrm{V}_1$, i.e. $\Delta \mathrm{C}_1$, and vice versa:

$$\Delta \mathrm{V}_0 = \Delta \mathrm{C}_1 + \Delta \mathrm{C}_0 \tag{7}$$

$$\Delta \mathrm{V}_1 = \Delta \mathrm{C}_1 + \Delta \mathrm{C}_0 \tag{8}$$

When $\Delta \mathrm{V}_0 = \Delta \mathrm{V}_1 = 1$, $\Delta \mathrm{C}_0$ and $\Delta \mathrm{C}_1$ represent the value of token 0 and 1, respectively. The price of token 1 quoted by token 0 is conveniently:

$$\mathrm{P}_0^1 = \frac{\Delta \mathrm{C}_1}{\Delta \mathrm{C}_0} \tag{9}$$

which is bounded within [1/99, 99]. P_0^1 can be converted to the price of token 0 and 1 per collateral:

$$\mathrm{P}_\mathrm{c}^0 = \frac{1}{1 + \mathrm{P}_0^1} \tag{10}$$

$$\mathrm{P}_\mathrm{c}^1 = \frac{\mathrm{P}_0^1}{1 + \mathrm{P}_0^1} \tag{11}$$

Virtual Curve

Let us establish the relationship between collateral amounts C_0 and C_1, using the constant product function [4]:

$$\left(C_0 + \frac{L}{\sqrt{P_H}}\right)\left(C_1 + L\sqrt{P_L}\right) = L^2 \tag{12}$$

For $[P_L, P_H]$ inside [1/99, 99], liquidity is active when P_0^1 is in range. When P_0^1 exits this range, liquidity is deactivated. Per (10), (11), liquidity provided to the range $[P_L, P_H]$ is available at $[\frac{P_L}{1+P_L}, \frac{P_H}{1+P_H}]$ for token 1, and $[\frac{1}{1+P_H}, \frac{1}{1+P_L}]$ for token 0.

The pool tracks the current `sqrtPrice` $\sqrt{P_0^1}$, with $\Delta\sqrt{P_0^1}$ reflecting collateral deltas:

$$\Delta C_0 = \Delta\frac{1}{\sqrt{P_0^1}} \cdot L \tag{13}$$

$$\Delta C_1 = \Delta\sqrt{P_0^1} \cdot L \tag{14}$$

Triangular Swaps

Traders can swap collateral for either digital calls or puts. These swaps are long-only, comparable to market buying options in a traditional order book.

The virtual curve enables swaps via an arbitrage-free triangulation of exchange rates P_c^0, P_c^1 and P_0^1. Specifically, for an infinitesimal liquidity interval, no profit should be made from triangular swaps that theoretically proceed from ΔC_0 to ΔC_1 to ΔV_1 to ΔV_0, and finally back to ΔC_0, and similarly when executed in reverse.

To demonstrate that this triangulation is arbitrage-free, consider an amount of $\Delta C_0'$, which is to be triangulated for a digital call amount ΔV_0, and is converted back to ΔC_0. This calls for:

$$\frac{\Delta C_0'}{\Delta C_1'}\frac{\Delta C_1'}{\Delta V_1'}\frac{\Delta V_1'}{\Delta V_0} = \frac{\Delta C_0}{\Delta V_0} \tag{15}$$

First, $\Delta C_0'$ is swapped via the virtual curve to $\Delta C_1'$, which is exchangeable to a digital put amount $\Delta V_1'$ per equation (8):

$$\Delta V_1' = \Delta C_1' + \Delta C_0' \tag{16}$$

where $\Delta C_0'$ is paid out *if and only if* $\Delta V_1'$ settles in-the-money. Per equation (7), when exchanged for ΔC_0, the digital call amount ΔV_0 also expects a return of $\Delta C_1'$, claimable at expiry *if and only if* ΔV_0 settles in-the-money.:

$$\Delta V_0 = \Delta C_1' + \Delta C_0 \tag{17}$$

As we require $\Delta V_0 = \Delta {V_1}'$ for the same liquidity interval, $\Delta C_0'$ must equal ΔC_0. Our proof, therefore, confirms that this triangular swap mechanism is free from arbitrage under the given conditions.

Swap Equations

In practice, a trader needs not triangulate prices for a pool. At the start of a swap $\Delta\sqrt{P_0^1}$ is derived from collateral input deltas using equations (13), (14). Subsequently, options token outputs can be conveniently computed from $\Delta\sqrt{P_0^1}$ and the liquidity invariant, by combining equations (7), (8) and (13), (14):

$$\Delta V_0 = \Delta\sqrt{P_0^1} \cdot L + \Delta\frac{1}{\sqrt{P_0^1}} \cdot L \tag{18}$$

$$\Delta V_1 = \Delta\sqrt{P_0^1} \cdot L + \Delta\frac{1}{\sqrt{P_0^1}} \cdot L \tag{19}$$

The direction of a swap determines whether the output is ΔV_0 or ΔV_1. When a trader swaps in options premiums ΔC_0 (or ΔC_1), the current `sqrtPrice` $\sqrt{P_0^1}$ moves lower (higher). The pool reserves ΔC_0 and ΔC_1 for contingent payout at settlement. A ΔV_0 (or ΔV_1) output amount is minted, as the `sqrtPrice` moves within an active liquidity range.

Essentially, the collateral premiums ΔC_0 for call options (or ΔC_1 for put options) can meet the contingent claims of any new puts ΔV_1 (or calls ΔV_0) to be minted for the same liquidity interval. To enable a swap, the expected return ΔC_1 for call options (or ΔC_0 for put options) is provided by seed liquidity.

Convertible Liquidity

Divergence v1 liquidity providers (LPs) are passive sellers of digital options. In a chosen price range, LPs can convert collateral to digital options exposures, or vice versa. They collect fees while taking on or off defined risks.

A liquidity position is minted as a non-fungible token (NFT), using collateral or prior purchased options tokens. LPs can opt for one of the three liquidity types: `seedCollateral`, `seedSpear`, or `seedShield`.

Initiating a liquidity position does not increase the circulation of options tokens. Options tokens are not minted until a buy transaction occurs within range. Once used as `seedSpear` or `seedShield` liquidity, options tokens are burnt and taken out of circulation. Unsold amounts, if any, can be reminted and reclaimed upon liquidity withdrawal.

For swap execution, the pool contract uses the aggregated liquidity invariant and does not track liquidity amounts for individual positions. Instead, the specific liquidity invariant of each LP is recorded at the individual position level, and is calculated using different methods when the position is initiated.

When an amount of `seedCollateral` is provided, it is considered as ΔC_0 and/or ΔC_1, based on the current `sqrtPrice` relative to the selected price range:

$$\Delta C_0 = \begin{cases} \Delta L \left(\frac{1}{\sqrt{P_L}} - \frac{1}{\sqrt{P_H}}\right), & \sqrt{P_0^1} < \sqrt{P_L} \\ \Delta L \left(\frac{1}{\sqrt{P_0^1}} - \frac{1}{\sqrt{P_H}}\right), & \sqrt{P_L} \le \sqrt{P_0^1} < \sqrt{P_H} \\ 0, & \sqrt{P_0^1} \ge \sqrt{P_H} \end{cases} \tag{20}$$

$$\Delta C_1 = \begin{cases} 0, & \sqrt{P_0^1} < \sqrt{P_L} \\ \Delta L \left(\sqrt{P_0^1} - \sqrt{P_L}\right), & \sqrt{P_L} \le \sqrt{P_0^1} < \sqrt{P_H} \\ \Delta L \left(\sqrt{P_H} - \sqrt{P_L}\right), & \sqrt{P_0^1} \ge \sqrt{P_H} \end{cases} \tag{21}$$

As equations (20), (21) suggest, Initiating an in-range liquidity position for a given collateral amount is similar to combining two out-of-range positions with a shared boundary of $\sqrt{P_0^1}$.

In comparison, `seedSpear` (`seedShield`) liquidity must be added to a price range below (above) the current `sqrtPrice` level by adapting equations (18), (19):

$$\Delta V_0 = \begin{cases} 0, & \sqrt{P_0^1} \le \sqrt{P_L} \\ \Delta L \cdot \left(\sqrt{P_H} - \sqrt{P_L}\right)\left(1 + \dfrac{1}{\sqrt{P_H \cdot P_L}}\right), & \sqrt{P_0^1} \ge \sqrt{P_H} \end{cases} \tag{22}$$

$$\Delta V_1 = \begin{cases} \Delta L \cdot \left(\sqrt{P_H} - \sqrt{P_L}\right)\left(1 + \dfrac{1}{\sqrt{P_H \cdot P_L}}\right), & \sqrt{P_0^1} \le \sqrt{P_L} \\ 0, & \sqrt{P_0^1} \ge \sqrt{P_H} \end{cases} \tag{23}$$

A liquidity position can accumulate unlimited gross shorts in both digital calls and puts, achieving auto risk-reduction through offsetting short call and put exposures. Its net shorts in calls or puts define its open exposure. The amount of net shorts are capped by the position's price boundaries, per equations (22), (23). As detailed in the **Seller Obligations** section, these net shorts are backed by the seed liquidity provided by the LPs to ensure their solvency.

The open options exposures of a position is impermanent until liquidity is removed from the pool. If the price crosses back a liquidity interval before liquidity is removed, options exposures are reversed. There are important distinctions from traditional limit orders for each liquidity type:

- A `seedCollateral` liquidity position is similar to a limit order to naked short either digital calls or puts. It works as an alternative to long-only swaps, as a short digital call (put) has the same expected return as a long digital put (call). As the price crosses back, the net short exposures in digital options are effectively reduced.

- A `seedSpear` (or `seedShield`) liquidity position acts like a limit close order for an existing long position. It is treated similarly as one with `seedCollateral` as the price crosses back. The options sale proceeds are effectively used as liquidity, which reverses the close order.

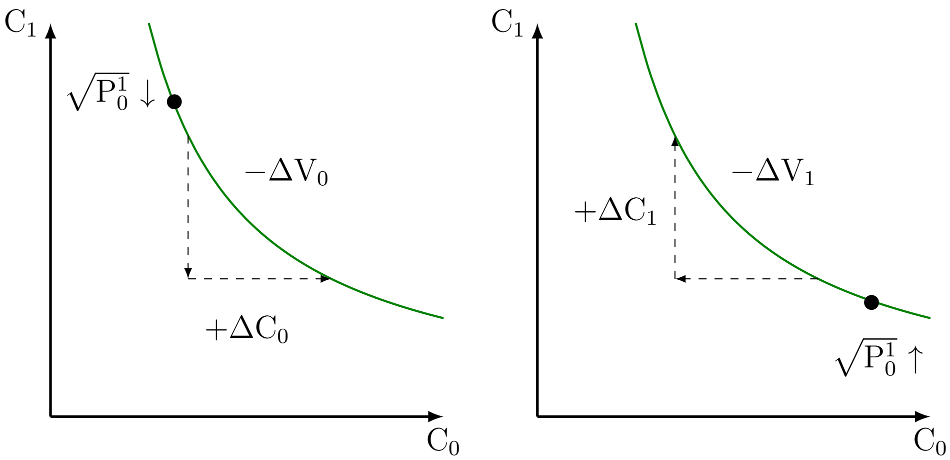

Figure 1: Swapping Collateral for Digital Call (left) or Put (right)

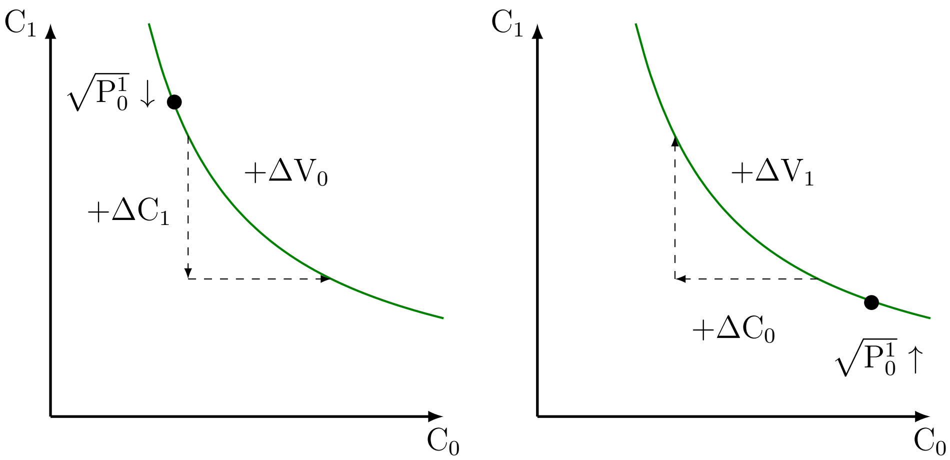

Figure 2: Adding Liquidity for Digital Call (left) or Put (right)

Ticks

`Ticks` form the discrete boundaries of active liquidity ranges. The pool contract identifies the virtual curve $\sqrt{P^0_1}$ by an integer index i:

$$\sqrt{P^0_1(i)} = \sqrt{1.0001}^i \quad (24)$$

The nearest tick below the last price is recorded as the current tick:

$$i_c = \left\lfloor \log_{\sqrt{1.0001}} \sqrt{P^0_1} \right\rfloor \quad (25)$$

Only ticks with indexes that are divisible by a default `tickSpacing` of 30 can be initialized as position boundaries.

Growth Variables

To account for fees and token deltas accrued at an individual liquidity position, `GrowthX128` info struct of fees, collateral inputs (`collateralIn`), and options token outputs (`spearOut`, `shieldOut`) are tracked per unit of liquidity at the pool (`global`), tick (`outside`) and position (`InsideLast`).

When a tick is initialized, `GrowthX128Outside` variables are treated as occurring below that tick. They are updated only when an initialized tick is crossed. As an example for all growth variables, `collateralIn` is used to record the cumulative collateral premiums from selling digital call and put options:

$$\mathrm{C_{inOutside}} := \mathrm{C_{inGlobal}} - \mathrm{C_{inOutside}(i)} \tag{26}$$

The `GrowthX128Below` and `GrowthX128Above` of `collateralIn` for a tick i are:

$$\mathrm{C_{inAbove}(i)} = \begin{cases} C_{inGlobal} - C_{inOutside}(i) & i_c \geq i \\ C_{inOutside}(i) & i_c < i \end{cases} \tag{27}$$

$$\mathrm{C_{inBelow}(i)} = \begin{cases} C_{inOutside}(i) & i_c \geq i \\ C_{inGlobal} - C_{inOutside}(i) & i_c < i \end{cases} \tag{28}$$

The `GrowthInside` of `collateralIn` between a lower tick i_l and an upper tick i_u is:

$$\mathrm{C_{inInside}} = \mathrm{C_{inGlobal}} - \mathrm{C_{inBelow}(i_l)} - \mathrm{C_{inAbove}(i_u)} \tag{29}$$

The pro rata share of `collateralIn` owed to an LP between time t_0 and t_1 is computed with the given liquidity invariant of a position:

$$\mathrm{C_{inOwed}} = \mathrm{L} \cdot (\mathrm{C_{inInside}(t_1)} - \mathrm{C_{inInside}(t_0)}) \tag{30}$$

Seller Obligations

For every option sold, an equivalent amount of collateral is set aside for settlement. The `seedCollateral` of a liquidity position first backs options sold in a single direction, with the `collateralIn` received then backing options sold in both directions subsequently.

When liquidity is withdrawn, the pool reserves collateral matching the greater of `spearObligation` ($\mathrm{V_{0Obligation}}$) or `shieldObligation` ($\mathrm{V_{1Obligation}}$). In the case of liquidity positions with `seedSpear` or `seedShield`, the obligations for options sold up to those seeded amounts are met by their originating positions. Therefore after adjustments:

$$V_{0Obligation} = \begin{cases} V_{0outOwed} - V_{0seed} & V_{0outOwed} > V_{0seed} \\ 0 & V_{0outOwed} \leq V_{0seed} \end{cases} \tag{31}$$

$$V_{1Obligation} = \begin{cases} V_{1outOwed} - V_{1seed} & V_{1outOwed} > V_{1seed} \\ 0 & V_{1outOwed} \leq V_{1seed} \end{cases} \tag{32}$$

A liquidity range established above the initial `sqrtPrice` must be crossed from the lower toward the upper bound, before it can be crossed back. Its cumulative gross shorts in puts ($\mathrm{V_{1outOwed}}$) can exceed those in calls ($\mathrm{V_{0outOwed}}$). The difference is capped by the maximum amount of put output in a single trade across the range, as determined by equation (23) for `seedShield` computation:

$$V_{1outOwed} - V_{0outOwed} \leq V_{1seed} \tag{33}$$

Conversely, per equation (22), liquidity range set below the initial `sqrtPrice` have:

$$V_{0outOwed} - V_{1outOwed} \leq V_{0seed} \tag{34}$$

The net short exposure of a position is therefore capped by its `seedSpear` or `seedShield` liquidity, and fully backed by its `seedCollateral`:

$$V_{netObligation} = \begin{cases} V_{0Obligation} - V_{1Obligation} & V_{0Obligation} > V_{1Obligation},\ \mathrm{S_T} \geq \mathrm{K} \\ 0 & V_{0Obligation} > V_{1Obligation},\ \mathrm{S_T} < \mathrm{K} \\ 0 & V_{0Obligation} \leq V_{1Obligation},\ \mathrm{S_T} \geq \mathrm{K} \\ V_{1Obligation} - V_{0Obligation} & V_{0Obligation} \leq V_{1Obligation},\ \mathrm{S_T} < \mathrm{K} \end{cases} \tag{35}$$

When liquidity is withdrawn before expiry, a position's options exposures are finalized. It has to reserve for settlement:

$$C_{obligation} = \max(V_{0Obligation}, V_{1Obligation}) \tag{36}$$

Remaining collateral amount is returned:

$$\mathrm{C_{owed}} = \mathrm{C_{seed}} + \mathrm{C_{inOwed}} - \mathrm{C_{obligation}} \tag{37}$$

Unsold amounts of `seedSpear` or `seedShield` are also reclaimed:

$$\mathrm{V_{0owed}} = \begin{cases} V_{0seed} - V_{0outOwed} & V_{0seed} > V_{0outOwed} \\ 0 & V_{0seed} \leq V_{0outOwed} \end{cases} \tag{38}$$

$$\mathrm{V}_{\mathrm{1owed}} = \begin{cases} V_{1seed} - V_{1outOwed} & V_{1seed} > V_{1outOwed} \\ 0 & V_{1seed} \leq V_{1outOwed} \end{cases} \tag{39}$$

LPs can `redeemObligation` before settlement to fully close out net short exposures. This is comparable to the traditional short-covering process, where sellers buy back the asset to neutralize short exposure. After removing liquidity, LPs can send back to the pool a `Spear` or `Shield` amount matching their net obligation to reclaim an equal amount of collateral reserved for settlement.

Settlement

Once options expire, options pools are settled by public functions, which secure the underlying prices from an external oracle. Holders of in-the-money options can exercise options to collect payouts. For options that expire out-of-money, LPs can `withdrawObligation` to claim collateral amounts matching their net obligations.

Fees

Transaction fees are set at 0.3% on the notional value of options and paid in collateral tokens, ensuring an even distribution of fees across the entire price curve. An exercise fee of 0.15% is applied when option holders claim payoffs. The protocol retains 30% of the transaction fee, as well as the exercise fee. Alternative fee structures are electable via community governance.

References

[1] Reiner, E. and Rubinstein, M.: 'Unscrambling the Binary Code.' *Risk*, no.4 (1991): 75-83.

[2] Blyth, S.: *An Introduction to Quantitative Finance*, Oxford University Press, 2013.

[3] Carr P, Wu L.: 'A tale of two indices', *The Journal of Derivatives.* Vol 13, no. 3 (2006), 13-29.

[4] Hayden, A., Zinsmeister, N., Salem, M., Keefer, R., and Robinson, D.: Uniswap v3 core. Technical report, 2021. Retrieved Friday 15th December, 2023 from https://uniswap.org/whitepaper-v3.pdf