MIP-1
MinSwap: exchange descentralizado de múltiples pools en Cardano

Long Nguyen
long@minswap.org

Traducido al español por Alexander Vega y Adrian Elsässer Briones

Abril 2021

Abstracto

Este documento elabora los conceptos y motivaciones de MinSwap - un exchange descentralizado (en inglés: Decentralized Exchange o DEX) y creador de mercado automatizado (en inglés: Automated Market Maker o AMM) en Cardano el cual admite múltiples funciones de precio para un determinado grupo o pool de liquidez (en inglés: Liquidity Pool o LP). El documento también desarrolla ideas como el "trade routing", oráculo de precios en cadena (on chain) y redención automática de comisiones de Babel para los operadores de stakepools de Cardano (por sus siglas en Ingles: SPO).

1 Introducción

Tradicionalmente, los exchanges centralizados que siguen el modelo order-book han sido respaldados por creadores de mercado (market makers). Los creadores de mercado suelen ser grandes empresas de trading o agencias de bolsa con capital masivo, amplio conocimiento financiero y sujetos a un estricto cumplimiento normativo. Facilitan alta liquidez en exchanges centralizados (Centralized Exchange o CEX) y obtienen beneficios a través de los márgenes o spreads (diferencias entre los precios de compra y venta). Sin embargo, el surgimiento de los exchanges descentralizados y las DeFi (finanzas descentralizadas o por sus siglas en inglés, Decentralized Finance) ha popularizado el concepto de los creadores de mercado automatizados (AMM) que permiten a participantes de

mercado minoristas convertirse fácilmente en creadores de mercado y así obtener beneficios de las comisiones generadas mediante los spreads.

En un mercado automatizado (AMM), los creadores de mercado individuales, ahora llamados proveedores de liquidez (Liquidity Providers o LP) agrupan sus fondos para convertirse en un único gran creador de mercado. Los traders pueden intercambiar tokens en estos pools de liquidez en base a funciones de un algoritmo determinista. Aunque es conveniente y adecuado para contratos inteligentes on-chain, un AMM presenta su propia clase de problemas, como la pérdida impermanente, baja eficiencia de capital e inversión ventajista (frontrunning). Distintos proyectos en la blockchain de Ethereum ya han tratado de confrontar estos problemas, aunque cada uno de ellos tiene sus concesiones particulares. Sin embargo, actualmente no se dispone de ningún DEX en el ecosistema de Cardano y mucho menos de un AMM automatizado. Además, la existencia de AMMs diferentes para diferentes casos de uso también confunde a los usuarios no expertos, lo cual ha dado pie a agregadores de DEXs como 1inch [1] o Matcha [6], pero por cuyo servico cobran comisiones adicionales.

2 Pool de liquidez multifunción

Aprovechando múltiples funciones de fijación de precios para un solo pool de liquidez, los proveedores de liquidez (LP) tienen la opción de elegir el pool más óptimo para un par específico, es decir, aquel que producirá los beneficios más altos / la mayor eficiencia de capital. A primera vista, esto podría conducir a una fragmentación de la liquidez. Sin embargo, los LPs naturalmente harán fluir su capital hacia el pool más eficiente para un par específico, porque ese pool será aquel que más trades tenga en su contra. Por otra parte, estrategias como el cultivo de rendimientos (Yield Farming) tales como Yearn Finance [8] también ayudarán a los LPs a reequilibrar su capital dirigiéndolo hacia los pools más eficientes. Esto no es diferente de tener varios protocolos AMM con diferentes funciones de precios, pero mover la liquidez entre los distintos pools hará que el trading sea más rápido y barato ya que todos los pools estarán en una única plataforma. Otra ventaja de construir un AMM con la anticipación de poder acomodar múltiples pools con distintas funciones de precios es que esto conducirá a una integración armoniosa de las mejores ideas de la comunidad sin tener que hacer un hard fork o migraciones importantes.

Veamos qué tipo de pool de liquidez se puede construir en MinSwap.

2.1 Pool de producto constante (Constant-product pool)

UniSwap [2] populariza el concepto de creador de mercado de producto constante. La curva de precios del producto constante funciona bien para la mayoría de los pares, pero incurre en una pérdida impermanente [1] para pares correlacionados inversamente (es decir, pares que tienen precios que se mueven en sentido opuesto). La función de precio en un pool de producto constantes es realmente simple:

$$xy = const$$

2.2 Pool estable (Stable pool)

Curve [3] ha descubierto que existe una mejor función para los llamados pares estables (es decir, un par que tiene un precio similar, en su mayoría vinculado a un activo externo como BTC o USD). Es la combinación de funciones de producto constante y suma constante con un "coeficiente de amplificación" dinámico.

$$An^n \sum x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$$

Esto ayuda a reducir el deslizamiento (slippage [2]) en los pools de baja liquidez y, al mismo tiempo, garantiza la liquidez para las grandes operaciones.

2.3 Pool de múltiples activos (Multi-asset pool)

Balancer [5] generaliza el concepto de función de producto constante a más de dos activos mediante la fórmula.

$$\prod x_i^{w_i} = const$$

Permite crear un pool con cualquier cantidad de cualquier número de activos, en lugar de limitar a los LPs a proporcionar una cantidad igual de dos activos, el

[1] Impermanent loss o pérdida impermanente ocurre cuando un LP ha proporcionado liquidez a un pool y el precio de sus activos depositados baja en comparación con cuando los depositó.

[2] El slippage es la diferencia de precio que puede ocurrir entre el momento en que se coloca una orden de trading y su ejecución real en el mercado.

cual es el caso en los dos modelos presentados anteriormente. Básicamente, esto significa que un LP puede proporcionar todo su portfolio tal y como es y éste se equilibrará automáticamente mediante las comisiones que gana al depositar su capital en el pool.

2.4 Pool dinámico (Dynamic pool)

Kyber extiende el "factor de amplificación" de Curve de pares estables a otros pares en general. El concepto se denomina creación de mercado dinámico (Dynamic Market Making o por sus siglas DMM) [7]. Con DMM, el "factor de amplificación" se programa en función de la volatilidad inherente de un par. También introduce un mejor mecanismo de comisiones donde la comisión (trading fee) se ajusta dinámicamente en función del volumen de negociación y la volatilidad de los precios.

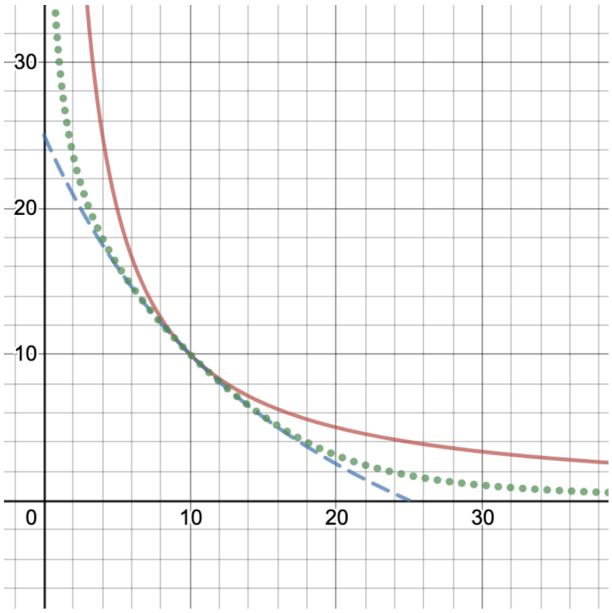

Figure 1: Curvas de inventario de Uniswap (rojo), Curve (verde) y curva de precios dinámica (azul)

Estos cuatro modelos de pools son solo ejemplos de lo que sería capaz de hacer MinSwap. El efervescente espacio de los AMM da luz cada día a nuevas y mejores ideas. En MinSwap, será la comunidad la que votará las mejores ideas para integrarlas en el protocolo.

3 Enrutamiento de múltiples pools

Con un par que esté presente en múltiples pools, el método de intercambiar el token A por token B no puede consistir simplemente en ejecutar la función constante en el grupo (A, B). Una solución simplista para este problema en cuestión, el enrutamiento de varios pools, es encontrar el pool que produce los rendimientos más altos para un par específico. Pero una mejor solución sería dividir el tamaño de la operación en partes más pequeñas y permutarlas en diferentes pools para encontrar los mejores retornos. El algoritmo de enrutamiento multipool se puede ejecutar completamente dentro o fuera de la blockchain, ya que Plutus admite ambos.

4 Oráculo de precios on-chain

Otro uso común de un AMM es actuar como oráculo de precios on-chain, proporcionando el precio on-chain de un par sin tener que consultarlo en una entidad fuera de la blockchain. Esto es posible porque los bots arbitrajistas siempre harán converger el precio del par en el AMM hacia el precio del mercado, siguiendo la ley del precio único. Con la presencia de múltiples pools para un solo par, el precio de un par será la media ponderada de todos los grupos para ese par:

$$price(A, B) = \frac{\sum_{i=1}^{n} w_i P_i}{\sum_{i=1}^{n} w_i}$$

donde w_i y P_i son el tamaño y el precio del pool i, respectivamente.

5 Redención automática de comisiones de Babel

Los activos nativos de Cardano permiten a los usuarios pagar una comisión de transacción de token en ese mismo token en lugar de en ADA. Este concepto se denomina comisiones de babel [4]. Aporta una mejor experiencia al usuario, ya que éste ya no tiene que tener una pequeña cantidad de ADA solo para facilitar las transacciones de tokens. Sin embargo, la tarifa en el token nativo se paga directamente a los operadores del de stakepools (SPOs) y podría causar una transacción lenta si el token es impopular y muy pocos SPOs quieren que se les pague en ese token. MinSwap ayudará al permitir que los SPOs intercambien rápidamente dicho token en ADA, incentivando así a los SPOs a procesar transacciones de con tokens nativos que no sean ADA.

Referencias

[1] *1inch*. URL: https://1inch.io/.

[2] Hayden Adams, Noah Zinsmeister, and Dan Robinson. *Uniswap v2 Core*. 2020. URL: https://uniswap.org/whitepaper.pdf.

[3] Michael Egorov. *StableSwap - efficient mechanism for Stablecoin liquidity*. 2019. URL: https://curve.fi/files/stableswap-paper.pdf.

[4] Prof. Aggelos Kiayias. *Babel fees - denominating transaction costs in native tokens*. URL: https://iohk.io/en/blog/posts/2021/02/25/babel-fees/.

[5] Fernando Martinelli and Nikolai Mushegian. *A non-custodial portfolio manager, liquidity provider, and price sensor*. 2019. URL: https://balancer.finance/whitepaper/.

[6] *Matcha*. URL: https://matcha.xyz/.

[7] Andrew Nguyen, Loi Luu, and Ming Ng. *Dynamic Automated Market Making*. 2021. URL: https://files.kyber.network/DMM-Feb21.pdf.

[8] *Yearn Finance*. URL: https://yearn.finance/.

Advertencia