MIP-1
MinSwap - Multi-pool decentrale exchange op Cardano

Long Nguyen
long@minswap.org

April 2021

Samenvatting

Dit document legt de motivaties en het beeld van Minswap uit - een geautomatiseerde market-maker (AMM) decentrale exchange/beurs (DEX) op Cardano, waarbij meerdere prijsdata ondersteund worden voor één liquiditeitspool. Het legt ook de begrippen trade-routing, on-chain prijs oracle en automatische babel fees redemption/transactiekosten inning die door Cardano stake pool operators (SPOs) gekozen worden.

1 Introductie

Traditioneel werden centrale order-book beurzen ondersteund door market makers. Market makers zijn meestal grote handelsbedrijven of brokers met heel veel kapitaal, financieel begrip en regulatie gehoorzaamheid. Ze verschaffen veel liquiditeit op centrale beurzen en verdienen geld via handel spread (het verschil tussen koop- en verkoopprijzen). Echter heeft de opkomst van decentrale beurzen/exchanges en DeFi het concept van Automatische Market-Making (AMM) populair gemaakt. AMMs maken het worden van market maker door individuele beleggers makkelijk, waarbij ze geld kunnen verdienen aan transactiekosten.

Op een AMM beurs, poolen/verzamelen individuele market makers - genaamd liquiditeit aanbieders/ liquidity providers (LPs) - hun kapitaal/ funds bij elkaar om zo één grote automatische market maker te worden. Handelaars kunnen tokens verhandelen op deze liquiditeitspools, gebaseerd op een deterministisch algoritme. Hoewel AMMs makkelijk en geschikt zijn voor on-chain smart contracts, bevatten ze hun eigen set aan problemen, zoals impermanent

loss, lage kapitaal efficiëntie en front-running. Er wordt op de Ethereum blockchain op verschillende manieren gewerkt aan deze problemen door verschillende projecten, met verschillende trade-offs/ bijwerkingen. Maar aan zo'n soort DEX wordt (nog) niet gewerkt op het Cardano ecosysteem en al helemaal niet aan een geoptimaliseerde AMM. Het hebben van verschillende AMMs voor verschillende doelen zorgt voor verwarring bij beginnende gebruikers en bovendien resulteert dit in DEX aggregators, zoals 1inch [1] of Matcha [6] die extra servicekosten eisen.

2 Multi-functionele liquiditeitspool

Door het gebruiken van meerdere prijsfuncties voor een enkele liquiditeitspool, hebben liquiditeit aanbieders (LPs) de mogelijkheid om een pool te kiezen die voor een specifieke paar het meest geschikt is, waarbij het meest verdiend kan worden/ dat het meest kapitaal efficiënt is. Initieel kan dit leiden tot de gedachte dat dit zorgt voor liquiditeit fragmentatie, echter gebruiken LPs natuurlijk hun kapitaal voor een specifieke paar met de meest kapitaal efficiënte pool, dat het meest verhandeld wordt. Een automatische yield farming strategie (die gecreeërd is door een gemeenschap, zoals Yearn Finance [8]) helpt LPs om hun kapitaal te herbalanceren in de meest efficiënte pools. Dit is niet anders dan het hebben van meerdere AMM protocols met verschillende prijsfuncties, maar het verplaatsen van liquiditeit tussen pools en het handelen/ traden is sneller en goedkoper aangezien alle pools op één platform zijn. Het bouwen van een AMM met de gedachte aan meerdere poolfuncties zorgt ook voor de makkelijke integratie van de beste ideeën van de gemeenschap, zonder dat een hard fork of grote veranderingen nodig is/zijn.

Laten we eens bekijken wat voor soort liquiditeitspool op MinSwap gebouwd kan worden .

2.1 Constant-product pool

UniSwap [2] heeft het concept van een constant-product market maker populair gemaakt. Constant-product prijskromme werkt goed voor de meeste paren, maar het zorgt voor wat impermanent loss voor invers-gecorreleerde paren (bijv. een paar waarbij de ene prijs omhoog gaat en de andere prijs omlaag gaat). De prijsfunctie van een constant-product pool is best simpel:

$$xy = const$$

2.2 Stabiele pool

Curve [3] is erachter gekomen dat er een betere functie is voor stabiele paren (bijv. een paar dat similair in prijs is, meestal gepaard aan een externe asset zoals BTC of USD). Het is de combinatie van constant-product en constant-sum functies met een dynamische 'amplification coefficient'.

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

Dit zorgt voor minder spreiding/slippage bij pools met weinig liquiditeit, terwijl er altijd genoeg liquiditeit is voor grote transacties.

2.3 Multi-asset pool

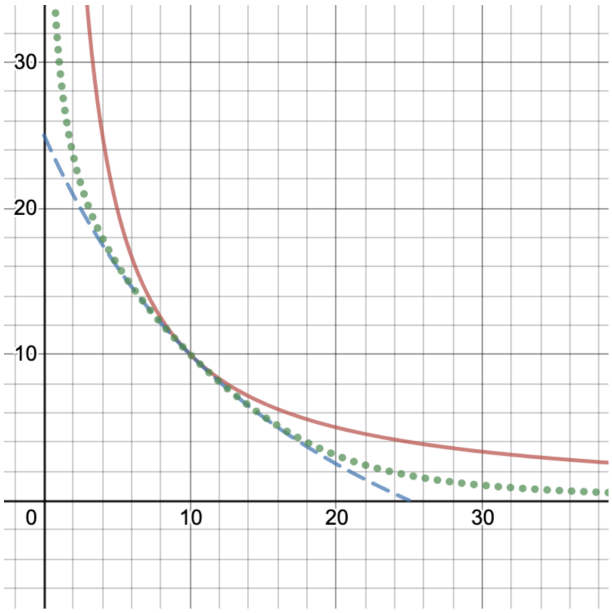
Balancer [5] is het bekendste voorbeeld van het concept van constant-product functies bij meer dan twee assets.

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

Het maakt het mogelijk om een pool the creëren met zo veel assets als gewenst is, dus geen limitatie waarbij LPs een zelfde waarde van twee assets moeten verschaffen. Dit betekent dat een LP de hele portfolio kan verschaffen, en automatisch wordt geherbalanceerd terwijl er transactiekosten verdiend worden.

2.4 Dynamische pool

Kyber breidt Curve's 'amplification factor' van stabiele paren meestal uit naar andere paren. Het concept heet Dynamic Market Making (DMM) [7]. Met DMM, is de 'amplification factor' geprogrammeerd gebaseerd op de volatiliteit van een paar. Het introduceert ook een beter mechanisme van transactiekosten, waarbij transactiekosten dynamisch aangepast worden op basis van handelsvolume en prijsvolatiliteit.



Figuur 1: Inventaris kromme van Uniswap (rood), Curve (groen) en dynamische prijskromme (blauw)

Deze vier pools zijn enkel voorbeelden van wat Minswap in staat zou kunnen zijn. De AMM omgeving krijgt elke dag steeds nieuwere en betere ideeën, en de beste ideeën zullen geïntegreerd worden in Minswap na stemming door de gemeenschap.

3 Multi-pool routing

Als een paar meerdere pools heeft, is het ruilen van token A naar token B niet zo gemakkelijk als het uitvoeren van de constant functie bij pool(A,B). Een makkelijke oplossing van multi-pool routing is het vinden van de pool (van een specifieke paar) met het hoogste rendement. Een betere oplossing zou kunnen zijn om het handelen op te splitsen in kleinere onderdelen, en op te splitsen in verschillende pools om het beste rendement te vinden. Het multi-pool routing algoritme kan volledig on-chain of off-chain uitgevoerd worden, aangezien Plutus beide mogelijkheden ondersteund.

4 On-chain prijs oracle

Een veelgebruikte toepassing van een AMM is de levering van een on-chain prijs, van een paar, zonder querying en het moeten gebruiken van een off-chain instantie. Dit is mogelijk doordat bots van arbitrageurs altijd komen om de AMM prijs te laten bewegen richting de marktprijs, zoals de wet van één prijs (the law of one price). Met de aanwezigheid van meerdere pools van één paar, zal de prijs van een paar gemiddeld gewogen worden door alle pools van dat paar:

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

waarbij respectievelijk w_i en P_i de grootte en prijs van pool i is.

5 Automatische babel fees ruil

Cardano native assets staan gebruikers (in de toekomst) toe om transactiekosten van een token te betalen in de desbetreffende token i.p.v. ADA. Dit concept heet babel fees [4]. Het zorgt voor een betere gebruikservaring, aangezien de gebruiker geen (kleine) hoeveelheid ADA in bezit moet hebben om de transactiekosten van de token te betalen. Maar de transactiekosten van de native token worden direct betaald aan stake pool operators (SPOs), waardoor langzame transacties kunnen ontstaan als de token onpopulair is en zeer weinig SPOs de token accepteren. Minswap helpt hierbij, doordat SPOs de mogelijkheid hebben om de desbetreffende token snel in te ruilen voor ADA. SPOs worden dus gestimuleerd om de native token transacties te behandelen.

Referenties

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

[2] Hayden Adams, Noah Zinsmeister en 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 en 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 en Ming Ng. *Dynamic Automated Market Making*. 2021. URL: `https://files.kyber.network/DMM-Feb21.pdf`.

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

Disclaimer

Dit document is enkel voor algemene informatie. Het bevat geen investeringsadvies of een aanbeveling of beroep om een investering aan te gaan of af te breken en zou niet gebruikt moeten worden bij een beslissing over een investering. Het hoort niet deel uit te maken tot boekhouding, legaal- of belastingadvies of investeringsaanbevelingen. Dit document reflecteert de huidige meningen van de auteurs en is niet gemaakt namens Minswap Labs of hun leden, en weerspiegelt niet per se de meningen van Minswap Labs, hun leden of elk ander individu verbonden aan Minswap Labs. De meningen die hier zijn weerspiegeld kunnen verandert worden zonder dat hier een update wordt gedaan.