Analiza različnih modelov trgovanja na decentraliziranih borzah

Poročilo za projekt pri predmetu Matematika z računalnikom

Špela Bernardič in Nika Pavlič

Maj 2024

1 Uvod

Najin projekt je zahteval osvojitev programskega jezika solidity in okolja hardhat, za razvoj pametnih pogodb. V projektu sva se osredotočili na Uniswap-V2 in Uniswap-V3. Cilj projekta je bil predvsem predstaviti razlike med verzijama ter prikazati zakaj je V3 boljši. Za Uniswap-V2 sva pripravili lastno kopijo, ter žetone in skripto, ki simulira izmenjavo žetonov. Za predstavitev razlik sva Uniswap V3 analizirali teoretično.

2 Nekaj pojmov in pojasnil

2.1 Pametne pogodbe

Pametne pogodbe so digitalne pogodbe, shranjene na blockchainu, ki se samodejno izvedejo, ko so izpolnjeni vnaprej določeni pogoji. Običajno se uporabljajo za avtomatizacijo izvajanja dogovora, tako da so lahko vsi udeleženci takoj prepričani o izidu, brez vpletenosti posrednika ali izgube časa. Prav tako lahko avtomatizirajo potek dela in sprožijo sledeče dejanje, ko so izpolnjeni vnaprej določeni pogoji.

2.2 ERC-20

ERC-20 je standard za *fungible* žetone (t.j. žetoni so si med seboj popolnoma enaki (po vrsti in vrednosti)). ERC-20 žeton na primer deluje enako kot ETH, kar pomeni, da 1 žeton je in bo vedno enak vsem drugim žetonom.

3 Uniswap

Uniswap največja decentralizirana borza, ki je začela delovati leta 2018. Uvedla je avtomatizirane vzdrževalce trga (ang.) *automated market maker*)(AMM) namesto tradicionalnih knjig naročil (ang. *order books*), ki jih uporabljajo borze. Deluje na Ethereum blockchainu in uporablja vrsto pametnih pogodb (ang. *smart contracts*) za varno zamenjavo ERC-20 žetonov med uporabniki brez posrednika.

Decentraliziran vidik protokola pomeni, da borze ne vodi nobena centraizirana avtoriteta. Namesto tega so zamenjave opravljene 'ena na ena ' (ang. *peer to peer*). Uniswap se trudi rešiti problem likvidnosti, s katerim se srečujejo na drugih borzah. Z vsako novo verzijo Uniswap poskuša zagotoviti bolj varno, efektivno in uporabno platformo.

3.1 Uniswap v2

Uniswap V2 je izšla maja 2020. V2 je uporabnikom omogočila neposredno trgovanje s katerima koli ERC-20 žetonoma, namesto preko ETH (kot v Uniswap-V1). S tem se je zmanjšalo število transakcij in prihranilo na t.i *gas fees*. Verzija je uvedla decentraliziran cenovni orakelj, ki je ponujal zanesljive podatke o cenah v realnem času. S tem je protokol postal bolj odporen proti manipulaciji s cenami. Uvedli so tudi t.i *flash swaps*, ki so omogočile, da si uporabniki izposodijo poljubno količino žetonov iz likvidnostega sklada, z njimi izvedejo želeno dejanje in v okviru iste transakcije vrnejo izposojene žetone.

3.1.1 Likvidnost

V Uniswap v2 je likvidnost enakomerno porazdeljena po cenovni krivulji $x \cdot y = k$, kjer sta x in y količina žetonov X in Y v likvidnostnem skladu, k pa je konstanta. Ideja je bila ohraniti konstantno razmerje znotraj likvidnostnega sklada, tako da bi bila skupna vrednost enega žetona vedno enaka skupni vrednosti drugega žetona v skladu, ne glede na trenutno medsebojno ceno. Likvidnost se torej zagotavlja za celotno cenovno območje $(0, \infty)$. V večini likvidnostnih skladov, ta likvidnost ni nikoli uporabljena.

Ponudniki likvidnosti Uniswapa V2 zaslužijo provizije le za majhen del svojega kapitala, kar lahko pomeni, da ne morejo ustrezno kriti cenovnega tveganja (IL), ki ga prevzemajo z velikimi zalogami obeh žetonov. Poleg tega so uporabniki pogosto izpostavljeni visokim stopnjam zdrsov (ang. *slippage*), saj je likvidnost porazdeljena po vseh cenovnih območjih.

3.1.2 Impermanent loss

Impermanent loss (IL) je izguba, ki jo ponudnik likvidnosti utrpi, ko zagotovi likvidnost skladu, potem pa se cene vloženih sredstev spremenijo. IL se pojavi zaradi stalnega uravnovešanja likvidnostnih skladov, kot odziv na gibanje tržnih cen. Izguba se ne realizira dokler ponudnik likvidnosti ne umakne svojih sredstev iz sklada. Če se cene žetonov vrnejo v prvotno razmerje IL izgine. Ponudniki likvidnosti za zagotavljanje likvidnosti prejemajo provizije od trgovanja, ki lahko izravnajo IL, vendar lahko na nestabilnih trgih ali med ektremnimi gibanji cen IL preseže zaslužene provizije.
Poglejmo si primer IL:

- Recimo, da smo ponudnik likvidnosti v 50/50 ETH/CRO sklad in da je trenutna cena ETH $P_0 = 1000$ CRO. V sklad damo enako vrednost ETH in CRO npr. 5 ETH in 5000 CRO.
- Po tem, ko dodamo likvidnost se cena ETH podvoji in se trguje po ceni $P_1 = 2000$ CRO. (Arbitražni trgovci bodo v sklad dodali CRO in odstranili ETH, da se cena ETH/CRO ujema z zunanjimi borzami).
- Po formuli konstantnega produkta $X \cdot Y = k$ izračunamo k:
$$5\ (ETH) \cdot 5000(CRO) = 25000.$$
- Izračunajmo imetje po arbitražnem trgovanju:
$$likvidnost_{ETH} = \sqrt{k/P_1} = \sqrt{25000/2000} = 3,5355$$
$$likvidnost_{CRO} = \sqrt{k \cdot P_1} = \sqrt{25000 \cdot 2000} = \ 7071,0678$$
- Če sedaj iz sklada umaknemo likvidnost prejmemo 14142,0678 CRO ($3,5355\ ETH\ \cdot\ 2000 CRO + 7071,0678\ CRO$).
- Če bi žetone držali namesto jih dali v sklad bi sedaj imeli 15000 CRO ($5\ ETH \cdot 2000\ CRO + 5000\ CRO$).
- V tem primeru je naš IL $15000\ CRO - 14142\ CRO = 858\ CRO$.

3.1.3 Provizije

V Uniswap V2 se za vsako zamenjavo žetonov zaračuna fiksna provizija v višini 0,3 %. Ta provizija se razdeli med ponudnike likvidnosti glede na njihov delež likvidnostnih rezerv. Ko uporabniki izvedejo zamenjavo, se provizije, ki jih plačajo, takoj dodajo k likvidnostnim rezervam. Ponudniki likvidnosti lahko svoj delež provizij poberejo tako, da uničijo (ang. *burn*) svoje likvidnostne žetone, s čimer se odstrani sorazmeren znesek osnovnih rezerv.

3.1.4 Vpliv cene (ang. *Price Impact*)

Kot je zgoraj omenjeno je cena žetonov določena s tem na kateri točki v cenovni krivulji smo v danem trenutku. Vsaka transakcija vpliva na sestavo likvidnostnega sklada (torej se premikamo po krvulji) in s tem se spreminja cena žetonov. Spremebo v ceni žetona definiramo kot *Price impact*, ki je razlika med tržno ceno (ang. *market price*) in tem kako uporabnikova menjava vpliva na ceno žetona v skladu.
Primer zamenjave z izračunom vpliva cene (manjši likvidnostni sklad):

1. Pred zamenjavo:
    - Naj bo X trenutna količina ETH v ETH/CRO likvidnostnem skladu: $X = 50$ ETH
    - Naj bo Y trenutna količina CRO v ETH/CRO likvidnostnem skladu: $Y = 50000$ CRO
    - Potem je konstantni produkt $k = 50 \cdot 50000 = 2500000$
    - Naj bo P_0 cena ETH žetona: $P_0 = 50000/50 = 1000$ CRO.
2. Zamenjava:
    - Želimo zamenjati 1 ETH za CRO.
    - V sklad dodamo 1 ETH žeton, dobimo pa $\Delta Y = Y - k/(X + \Delta X)$ $= 50000 - 2500000/51\text{ETH} = 980.39$ CRO.
    - vpliv cene $= (1000 - 980.39)/1000 = 1,9\%$
    - V skladu je sedaj 51 žetonov ETH in 49019,61 žetonov CRO.
    - Cena ETH je sedaj $49019,61/51 = 961,17$ CRO.

V zgornjem izračunu ni upoštevana provizija, če pa bi bila, bi v manjavi uporabnik dobil $977,45$ CRO.

Izračun primerjamo z razultatom, ki ga dobiva v najini kopiji uniswapa. Pripravili sva skripto kjer definirava likvidnostni sklad z 50 žetoni kovanca1 in 50000 žetoni kovanca2. Nato sva izvedli zamenjavo 1 kovanca1 in zanj sva dobili 977 kovanca2. To se ujema z izračunom, saj se upošteva tudi provizija, ki jo plačamo.

Primer Price Impact-a pri večjem likvidnostnem skladu:

Naj bo sedaj v skladu 5000 ETH in 5 mio CRO. P_0 je torej enak kot prej. Ko sedaj zamenjamo 1 ETH za CRO, dobimo 999,8 CRO oz 996,8 CRO če upoštevamo provizijo. Price Impact pa je v tem primeru veliko manjši in sicer 0.02 %.

Skripto ponovno zaženeva še z večjim likvidnostnim skladom in dobiva razultat: za menjavo 1 kovanca1 dobimo 996 kovanca2.

3.1.5 Zdrs (ang. *Slippage*)

Ko uporabnik predloži transakcijo na Ethereum-u je hitrost izvedbe transakcije odvisna od cene izvedbe transakcije, ki jo je pripravljen plačati (ang. *gas price*). Več kot plača gas, hitreje se bo transakcija izvedla. Če transakcija oziroma zamenjava dolgo čaka na izvedbo, se lahko razmerje valut v likvidnostnem skladu v tem času spremeni, saj so se med čakanjem izvedle že druge zamenjave. To lahko pomeni, da bo uporabnik zaradi čakanja na izvedbo transakcije dobil manj željenih žetonov kot jih je pričakoval. Zdrs je razlika v cenah po kateri mislimo da bomo kupovali žeton in po kateri potem dejansko kupimo. Zdrs je ponavadi večji pri velikih transakcijah in v majhnih likvidnostnih skladih.

Da bi uporabnike zaščitili pred velikimi izgubami zaradi zdrsa je definirana toleranca za zdrs (ang. *Slippage tolerances*), ki pove za koliko se lahko razmerje žetonov spremeni, da se transakcija še vedno izvede. Torej, če se razmerje žetonov v likvidnostnem skladu med čakanjem transakcije na izvedbo spremeni za več kot to dovoljuje toleranca za zdrs, se transakcija ne izvede in Uniswap vrne napako `INSUFFICIENT_OUTPUT_AMOUNT`.

Definirana je tudi omejitev največ koliko časa lahko transakcija čaka preden se izvede (ang *deadline*). Če se transakcija ne izvede do roka, se jo prekliče in Uniswap vrne napako Expired. S tem se uporabnika zaščiti pred dolgim čakanjem na izvedbo zamenjave in velikimi spremembam cen.

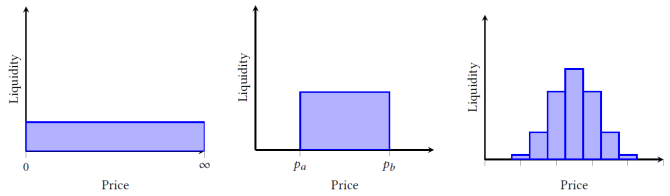
Vrnimo se k prejšnjem primeru. Denimo, da želimo narediti zamenjavo 1 ETH žetona, ko je v likvidnostnem skladu $X = 50$ ETH in $Y = 50000$ CRO. Nek drug uporabnik je bil za izvedbo transakcije pripravljen plačati več, zato on prvi izvede zamenjavo prav tako 1 ETH za CRO. Kot smo izračunali zgoraj, je po njegovi zamenjavi stanje v likvidnostnem skladu enako $X = 51$ ETH in $Y = 49019,61$ CRO. Cena ETH je sedaj $49019,61/51 = 961,17$ CRO. Potem pride na vrsto za izvedbo transakcije prvi uporabnik in zamenja 1 ETH za 942,68 CRO po novi ceni. Za 1 ETH dobi 37,71 CRO manj kot drug uporabnik. Zdrs je razlika v ceni po kateri pričakujemo, da bomo kupili žetone, in po kateri potem dejansko kupimo. V tem primeru je to $1000 - 961,17 = 38.83$. Če pa izvedemo isti scenarij v primeru z večjim likvidnostnim skladom je zdrs le $0,4$ in za enako menjavo dobi prvi uporabnik le 0,4 CRO manj od drugega drugega uporabnika.

3.2 Uniswap V3

Uniswap V3 je tretja verzija protokola, ki je izšla maja 2021 in prinesla veliko izboljšav. Med njimi je najpomebnejša koncentrirana likvidnost.

3.2.1 Koncentrirana likvidnost

V sistemu Uniswap V2 so uporabniki torej svojo likvidnost razpršili po celotnem cenovnem razponu, v sistemu Uniswap V3 pa se lahko ponudniki likvidnosti odločijo, da bodo svoj denar skoncentrirali na določen cenovni razpon. Tem cenovnim razponom pravimo pozicije. Pri tem lahko združijo poljubno število različnih koncentriranih pozicij znotraj enega sklada.

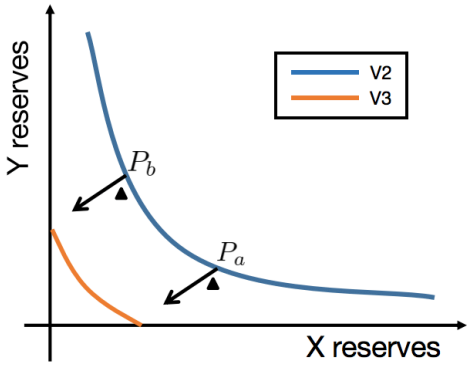


(I) Uniswap v2 **(II)** A single position on $[p_a, p_b]$ **(III)** A collection of custom positions

Koncentriranje likvidnosti ponudnikom likvidnosti povečuje kapitalsko učinkovitost, saj so sredstva razporejena tam, kjer je trgovanje najbolj verjetno. Ponudniki likvidnosti lahko v V3 zaslužijo enake provizije za manj kapitala, v primerjavi z V2. Po drugi strani pa lahko ponudnik v V3 z enakim kapitalom kot v V2, zagotovi več likvidnosti, za kar pa mora prevzeti več tveganja IL. Koncentrirana likvidnost ima prednost tudi za trgovce, saj ti zaradi večje likvidnosti v ozkih cenovnih razponih, dobijo boljše cene, kar zmanjšuje zdrs. Koncentriranje likvidnosti in boljše provizije pa imajo tudi svojo ceno, predvsem v IL.

V primeru, da se tržna cena premakne izven določenega območja, je likvidnost ponudnika izvzeta iz sklada in ponudnik ne prejema provizij, dokler se cena ne premakne nazaj v cenovno območje, ki ga je določil oz. dokler ne spremeni mej cenovnega območja. Na tej točki bo pozicija tega ponudnika sestavljen le iz enih žetonov.

Na primer, da smo tako kot prej v ETH/CRO likvidnostni sklad dodali enako vrednost ETH in CRO npr. 5 ETH in 5000 CRO pri ceni ETH $P_0 = 1000$ CRO. Odločimo se, da bomo ponujali likvidnost v območju cene ETH med 800 CRO in 1200 CRO, torej se bo naš kapital uporabljal le dokler se bo cena gibala v tem območju. Na začetku smo v likvidnostni sklad dodali enako vrednost obeh žetonovo, torej je razmerje žetonov ki nam pripada pri ceni ETH $P_0 = 1000$ CRO enako 50:50. Ko se tržna cena žetonov spremeni, bodo arbitražni trgovci uravnavali razmerje v skladu, da se bodo cene ujemale z zunanjim svetom. Ko cena ETH pade na $P_a = 800$ CRO ali nižje, se razmerje naših žetonov v skladu spremeni na 100:0, torej imamo le ETH žetone. Obratno se zgodi, če cena ETH zraste na $P_b = 1200$ CRO ali višje, takrat nam v skladu ostanejo le CRO žetoni.



Zaradi koncentrirane likvidnosti ponudnikove likvidnostne pozicije niso več zamenljive in v protokolu niso več predstavljene kot ETC-20 žeton. Namesto tega so predstavljene kot NFT-ji.

3.2.2 Prilagodiljive provizije

Uniswap V3 je uvedel prilagoljive provizije, kjer lahko ponudnik likvidnosti določi provizijo, glede na ugotovljeno tveganje para žetonov, za katerega zagotavlja likvidnost. Na podlagi volatilnosti para lahko izbira med provizijami v višini 0.05 %, 0.3 % in 1 %. To ponudnikom likvidnosti omogoča večjo fleksibilnost pri izbiri ravni provizij, ki je skladna z njihovimi preferencami in strategijami trgovanja.

4 Zaključek

Čeprav imata tako V2 kot V3 svoje prednosti, je temeljna razlika v kapitalski učinkovitosti in potencialnih donosih za ponudnike likvidnosti. Uvedba koncentrirane likvidnosti v različici V3 je spremenila način zagotavljanja likvidnosti v sistemu Uniswap in ponudila možnost veliko večjih donosov na naložbe. Medtem ko ima V2 enostaven pristop k zagotavljanju likvidnosti, je V3 kompleknejša in zahteva globlje razumevanje tržne dinamike in gibanja cen. Ponudniki likvidnosti V3 morajo bolj aktivno upravljati svoje pozicije in prilagajati cenovna območja za svojo likvidnost.