Zloupotreba brzih zajmova za napade na DeFi ekosustav

Bubalo, Ivana

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:182923

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-07-24**

Repository / Repozitorij:

Repository of School of Applied Mathematics and Computer Science

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike; smjer: Financijska matematika i statistika

Ivana Bubalo

Zloupotreba brzih zajmova za napade na DeFi ekosustav

Diplomski rad

Osijek, 2022.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike; smjer: Financijska matematika i statistika

Ivana Bubalo

Zloupotreba brzih zajmova za napade na DeFi ekosustav

Diplomski rad

Mentor: izv. prof. dr. sc. Nenad Šuvak

Osijek, 2022.

Sadržaj

Uvod **1**

1 Osnovni pojmovi **2**

1.1 Cijene i povrati 2

1.2 Izvedenice 3

1.3 Varijanca 5

2 Uvod u decentrlizirane burze **7**

2.1 Decentralizirane u odnosu na centralizirane burze 7

2.2 Vrste decentraliziranih burzi 8

2.2.1 DEX temeljen na knjizi ograničenih naloga 8

2.2.2 Automatizirani Market Maker DEX 8

2.3 Trgovanje maržom 10

2.4 Ethereum Virtual Machine i prijelazi stanja 11

2.5 Brzi zajam 12

3 Razlika u dobiti kod atomske i neatomske arbitraže **13**

4 Parametarski optimizacijski model **15**

5 DeFi modeli **17**

5.1 Brzi zajam 17

5.2 Trgovanje po fiksnoj cijeni 18
5.3 Konstantni produkt AMM 18
5.4 Automatizirana rezerva cijena 20
5.5 Kolateralizirano pozajmljivanje i posuđivanje 21
5.6 Trgovanje maržom 22

6 Klasificiranje slučajeva zloupotrebe brzih zajmova 23
6.1 Arbitraža 23
6.2 Wash Trading 25
6.3 Zamjena kolaterala 26
6.4 Flash Minting 27

7 Analiza PA&A napada 28
7.1 Pump Attack i arbitraža 28
7.1.1 Brzi zajam 29
7.1.2 Otkup zajma 30
7.1.3 Identificiranje i kvantificiranje žrtve 30
7.2 Teorijsko optimiziranje Pump Attacka 31

8 Manipuliranje cjenovnim oracleom 34
8.1 Oracle problem 34
8.2 Analiza napada 35
8.2.1 Intuicija napada 35
8.2.2 Identificiranje i kvantificiranje žrtve 36
8.3 Teorijsko optimiziranje manipulacijskog napada na oracle 37

Literatura 40

Sažetak 43

Ključne riječi **43**

Summary **44**

Key Words **44**

Životopis **45**

Uvod

Središnja komponenta našeg gospodarstva je kredit. Ako kredit stvara novu i održivu vrijednost može se shvatiti kao pozitivna ekonomska snaga. Zlouporaba kredita, međutim, nužno povlači za sobom negativne buduće posljedice. Prekomjerno zaduživanje može dovesti do rizika neplaćanja duga, tj. dužnik više nije u stanju otplaćivati zajam uvećan za plaćanje kamata. To nas dovodi do sljedećeg pitanja: Što kada bi bilo moguće ponuditi kredit bez rizika da zajmoprimac ne vrati dug? Takav se koncept čini nepraktičnim u tradicionalnom financijskom svijetu. Bez obzira na to koliko je mali posuđeni iznos i koliko je kratak rok otplate kredita, postoji rizik od neplaćanja kredita. U ovom radu razmotrit ćemo neke primjere tehnologije koja omogućuje da tržište bude bliže ideji posuđivanja sredstava osobama čiji nam je identitet nevažan uz to što se osigurava mali rizik od neplaćanja kredita. Također, pokazat ćemo kako su opisani koncepti iskorišteni u zlonamjerne svrhe. Takozvani brzi zajmovi pojavili su se kao rezultat posebnosti pametnih ugovora i upravo su oni glavna tema ovog rada.
Klasificirat ćemo slučajeve zloupotrebe brzih zajmova te obraditi dva napada koja su se dogodila uzastopno na bZx-u (15. i 18. veljače 2020.), protokolu za posuđivanje temeljenom na Ethereumu od kojeg korisnici mogu posuđivati i trgovati maržom. To su prvi DeFi napadi golemog opsega, a u njima je bZx oštećen za približno $1 milijun. Prvi se napad dogodio zbog greške u pametnom ugovoru, a drugi zbog korištenja centraliziranog oraclea. bZx je mogao pretrpjeti i puno veće gubitke obzirom da trgovci nisu optimalno podesili parametre napada.

Poglavlje 1

Osnovni pojmovi

U ovom poglavlju uvodimo matematičku podlogu iz [28]. Prvo ćemo definirati cijene i povrate, a zatim izvedenice i volatilnost koje objašnjavaju [4] i [3].

1.1 Cijene i povrati

Neka S_t^i označava cijenu i-tog financijskog instrumenta u trenutku t, $i \in \{0, 1 \ldots, d\}, t \in \{0, 1 \ldots, T\}$, $T \in \mathbb{N}$, a $V_t(\phi)$ označava cijenu portfelja $\phi_t = (\phi_t^0, \phi_t^1, \ldots, \phi_t^d)$ u trenutku t.

Definicija 1.1. ***Povrat*** *je relativna promjena vrijednosti financijskog instrumenta u određenom vremenskom trenutku.*

Definicija 1.2. ***Relativni ili aritmetički povrat*** *i-tog financijskog instrumenta je postotna promjena njegove cijene u trenutku t s obzirom na trenutak* $(t-1)$ *:*

$$R_t^i = \frac{S_t^i - S_{t-1}^i}{S_{t-1}^i}, \ i \in \{0, 1 \ldots, d\}, \ t \in \{0, 1 \ldots, T\}.$$

Alternativni zapis

$$1 + R_t^i = \frac{S_t^i}{S_{t-1}^i}$$

označava bruto povrat.
Generalno, n-periodni relativni povrat i-tog financijskog intrumenta računa se kao

$$R_t^i(n) = (1 + R_t^i)(1 + R_{t-1}^i) \times \cdots \times (1 + R_{t-(n-1)}^i) - 1$$

$$= \frac{S_t^i}{S_{t-1}^i} \times \frac{S_{t-1}^i}{S_{t-2}^i} \times \cdots \times \frac{S_{t-(n-1)}^i}{S_{tn}^i} - 1 = \frac{S_t^i}{S_{t-n}^i} - 1$$

Umjesto relativnih povrata u financijama se češće koriste log-povrati obzirom da je n-periodni log-povrat jednak sumi jednoperiodnih log-povrata i time su lakše primjenjivi u analizama.

Definicija 1.3. ***Log-povrat*** *je prirodni logaritam bruto povrata* $(1 + R_t^i)$ *u trenutku* t

$$r_t^i = \ln(1 + R_t^i) = \ln \frac{S_t^i}{S_{t-1}^i} = \ln S_t^i - \ln S_{t-1}^i.$$

1.2 Izvedenice

Informacije o cijenama financijskih instrumenata na financijskom tržištu u diskretnom vremenu modeliramo σ-algebrom $\mathcal{F}_t \subseteq \mathcal{P}(\Omega)$ $, t \in \{0, 1, \ldots, T\})$. To znači da imamo rastući slijed informacija o financijskom instrumentu kojeg modeliramo filtracijom $\mathbb{F} = (\mathcal{F}_t : t \in \{0, 1, \ldots, T\})$. $\mathcal{F}_t$ sadrži sve informacije o cijenama financijskih instrumenata koje promatramo zaključno s trenutkom t.
$\{\varnothing, \Omega\} = \mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \mathcal{F}_2 \cdots \subseteq \mathcal{F}_T = \mathcal{P}(\Omega)$

Definicija 1.4. *Slučajni proces* $\phi = (\phi_t, t \in \{0, 1, \ldots, T\}) = ((\phi_t^0, \phi_t^1, \ldots, \phi_t^d), t \in \{0, 1, \ldots, T\}$ *s vrijednostima u* $\mathbb{R}^{d+1}$ *koji je predvidiv u odnosu na filtraciju* $\mathbb{F} = (\mathcal{F}_t, t \in \{0, 1, \ldots, T\})$ *zove se* ***dinamički portfelj*** *ili* ***strategija trgovanja****.*

Definicija 1.5. *Strategija trgovanja ili dinamički portfelj* ϕ *je* ***samofinancirajući*** *ako* $\forall t \in \{0, 1, \ldots, T\}$ *vrijedi* $\langle \phi_t, S_t \rangle = \langle \phi_{t+1}, S_t \rangle$ *.*

Definicija 1.6. *Dinamički portfelj* ϕ *je* ***dopustiv*** *ako je*

1) ϕ *samofinancirajući*

2) $V_t(\phi) \geqslant 0 \quad \forall t \in \{0, 1, \ldots, T\}$*, tj. vrijednost portfelja (dopustive strategije) u svakom trenutku* t *mora biti nenegativna.*

Dopustiv dinamički portfelj ϕ *je* ***arbitraža*** *ako, dodatno, vrijedi*

3) $V_0(\phi) = 0$

4) $P(V_t(\phi) \geqslant 0) \geqslant 0$*, tj. u trenutku dospijeća donosi zaradu s vjerojatnošću većom od nula.*

Definicija 1.7. ***Slučajni zahtjev*** *s dospijećem u trenutku* T *je* $\mathcal{F}_t$*-izmjeriva slučajna varijabla* C_T *na vjerojatnosnom prostoru* $(\Omega, \mathcal{F}, P)$ *kojim je opskrbljen model financijskog tržiša u diskretnom vremenu, gdje je* $0 \leqslant C_T \leqslant \infty$ *gotovo sigurno.*

Slučajni zahtjev zove se ***izvedenica*** *ili* ***derivativ*** *primarnih financijskih instrumenata $S_t^0, S_t^1, \dots S_t^d$ ako je C_T transformacija slučajnog vektora $(S_1, S_2, \dots, S_T)$, gdje je $S_t = (S_t^0, S_t^1, \dots S_t^d), t \in \{0, 1, \dots, T\}$.*

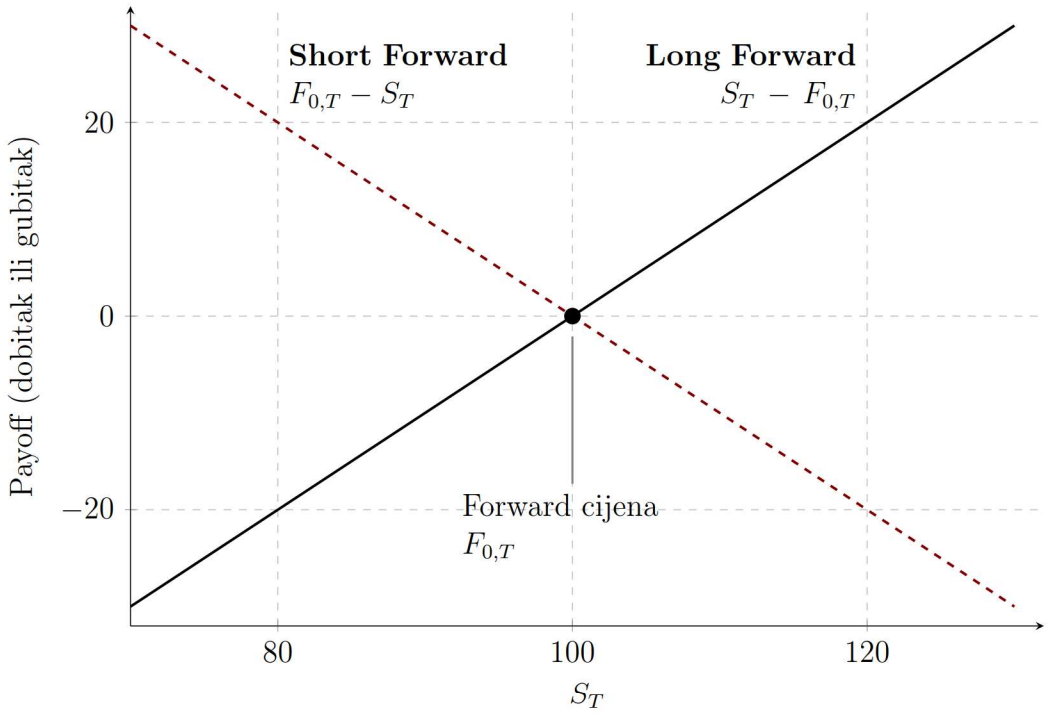
Izvedenice *(eng. derivatives)* su financijski instrumenti čija je vrijednost određena vrijednošću nekog drugog financijskog instrumenta. Pri tome taj drugi financijski instrument može biti neki vrijednosni papir, sirovina, valuta, indeks i slično. U ovom ćemo se radu ograničiti na izvedenice koje se odnose na financijske instrumente kojima se trguje na organiziranim financijskim tržištima. Osnovni motiv za upotrebu izvedenica je ograničavanje rizika, tzv. hedging. Da bi netko smanjio rizik mora postojati netko drugi tko će ga preuzeti, a pojedinci i institucije kupuju rizike i očekuju da će za preuzimanje istih biti kompenzirani pozitivnim povratom. Prema [4] izvedenice se prema strukturi dijele na unaprijedne ugovore (forwardi i futuresi), opcije, i zamjene *(eng. swaps).*

Definicija 1.8. ***Opcija*** *je ugovor koji vlasniku daje pravo, ali ne i obavezu kupiti ili prodati neku imovinu do određenog datuma (ili na određeni datum) po unaprijed dogovorenoj cijeni.*

Definicija 1.9. ***Forward*** *je ugovor koji daje pravo i obavezu da se određeni vrijednosni papir kupi po unaprijed određenoj cijeni u unaprijed određenom trenutku dospijeća T u budućnosti. Strana koja se obavezala kupiti vrijednosni papir u budućnosti nalazi se u dugoj poziciji (eng. long), a strana koja se obavezala isporučiti vrijednosni papir u budućnosti je u kratkoj poziciji (eng. short).* ***Cijena izvršenja*** *ili* ***forward cijena*** *je cijena definirana forward ugovorom.*

Donji graf je tvz. *payoff* dijagram i prikazuje odnos dobitka i gubitka za kratku i dugu poziciju u forward ugovoru s obzirom na cijenu referentnog vrijednosnog papira na datum dospijeća forwarda T. Sa $F_{0,T}$ označimo cijenu izvršenja forwarda u trenutku T, a sa S_T cijenu referetnog vrijednosnog papira u trenutku T koje se još naziva i *spot price*. Razmotrit ćemo dva slučaja: kada je dogovorena cijena izvršenja forward ugovora $F_{0,T}$ manja, odnosno veća od vrijednosti referentnog vrijednosnog papira u trenutku izvršenja.

Ako je $S_T \geqslant F_{0,T}$ investitor koji ima dugu poziciju u forwardu zarađuje razliku $S_T - F_{0,T}$ jer prema uvjetima forwarda može kupiti vrijednosni papir po cijeni $F_{0,T}$, a na tržištu ga može prodati po većoj cijeni S_T. Investitor u kratkoj poziciji gubi isti iznos $S_T - F_{0,T}$. U slučaju $S_T < F_{0,T}$ vrijedi obratna situacija: investitor u kratkoj poziciji zarađuje $F_{0,T} - S_T$ dok investitor u dugoj poziciji gubi $F_{0,T} - S_T$.



Slika 1.1: *Graf profitabilnosti forward ugovora*

1.3 Varijanca

Definicija 1.10. *Neka je $(\Omega, \mathcal{P}(\Omega), P)$ diskretan vjerojatnosni prostor i X slučajna varijabla na njemu. Ako red $\Sigma_{\omega\in\Omega}|X(\omega)|P\{\omega\}$ konvergira, onda kažemo da slučajna varijabla X ima matematičko očekivanje i broj*

$$EX = \sum_{\omega\in\Omega} X(\omega)P\{\omega\}$$

zovemo matematičko očekivanje slučajne varijable X.

Definicija 1.11. *Neka je X neprekidna slučajna varijabla s funkcijom gustoće f. Ako je konačan integral*

$$\int_{-\infty}^{\infty} |x| f(x)\, dx$$

onda kažemo da slučajna varijabla X ima očekivanje i broj

$$E[X] = \mu = \int_{-\infty}^{\infty} x f(x)\, dx$$

zovemo matematičko očekivanje neprekidne slučajne varijable X.

Sada prema [3] možemo definirati varijancu slučajne varijable X kao očekivano kvadratno odstupanje slučajne varijable od njezinog očekivanja.

Definicija 1.12. *Ako postoji* $E(X - EX)^2$*, onda taj broj zovemo varijanca slučajne varijable* X *i označavamo s Var(X) ili* σ^2*.*

U slučaju da μ nije poznato, njegova procjena je uzoračko očekivanje

$$\hat{\mu} = \overline{x}_n = \frac{1}{n}\sum_{i=1}^{n} x_i.$$

Tada se nepristrana procjena varijance računa kao

$$\hat{\sigma}^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \hat{\mu})^2.$$

Za kvadratni korijen varijance, odnosno standardnu devijaciju σ, u financijama se često koristi naziv volatilnost. Kao što i sam naziv kaže ona se mjeri kao korijen očekivanog kvadratnog odstupanja realizacija slučajne varijable od njezinog očekivanja. Stoga niska volatilnost ukazuje na manju varijabilnost među podacima.

Poglavlje 2

Uvod u decentrlizirane burze

2.1 Decentralizirane u odnosu na centralizirane burze

Centralizirana burza (CEX) koja se ponekad naziva i skrbničkom burzom čuva imovinu korisnika u kolektivnim računima burze *(eng. pooled account)*. Neki primjeri centraliziranih burzi su *Coinbase, Kraken, Gemini* i *Robinhood*. Prednosti ovakve burze uglavnom počivaju u praktičnosti i korisničkom iskustvu. Zbog toga se oko 99% sve kriptoimovine trguje na centraliziranim burzama. Posljedica toga je da su centralizirane burze mete napada visoke vrijednosti što dokazuju brojna hakiranja. Primjerice, samo je u 2018. godini ukradena imovina vrijedna preko milijardu dolara. Kako bi trgovali na CEX-u korisnici šalju svoju imovinu u depozitni novčanik u vlasništvu burze koji je posebno kreiran za određenog korisnika. Ovaj novčanik zatim prosljeđuje sredstva u njihov glavni objedinjeni račun i registrira primljena sredstva koja se koriste za trgovanje.
Nasuprot tome, decentralizirana burza (DEX) obično se implementira kao pametni ugovor koji omogućuje trgovanje kriptoimovinom bez skrbništva. Korisnici šalju svoju imovinu u pametni ugovor, mogu komunicirati s njim radi trgovanja i ponovno se povući. Proteklih godina predloženo je više vrsta DEX-a, od kojih se neke aktivno koriste.

2.2 Vrste decentraliziranih burzi

Dvije glavne DEX varijante temelje se na knjigama ograničenih naloga *(eng. limited order book, LOB)* ili automatiziranim market makerima (AMM).

2.2.1 DEX temeljen na knjizi ograničenih naloga

Ograničeni nalog vrsta je naloga za kupnju ili prodaju vrijednosnog papira po određenoj cijeni: *ograničeni nalog za kupnju* je nalog za kupnju po unaprijed određenoj cijeni ili nižoj, dok je ograničeni nalog za prodaju nalog za prodaju vrijednosnog papira po unaprijed određenoj cijeni ili višoj. Međutim, nema jamstva da će ograničeni nalog biti izvršen. Drugim riječima, nalog se može ispuniti samo ako se dosegne određena razina cijena. Ograničeni nalozi korisni su ulagačima jer osiguravaju da ne plaćaju više za vrijednosni papir od unaprijed postavljene cijene koja je inicijalno određena nalogom. Knjigama naloga može se upravljati u lancu ili izvan lanca, ali stvarna namira trgovanja obično se događa u lancu. Dva primjera takvog DEX-a temeljenog na LOB-u su *EtherDelta* i *IDEX* koji rade na Ethereum blockchainu. Oba upravljaju svojim knjigama naloga izvan lanca što zahtijeva vanjsku uslugu s kojom korisnici komuniciraju. Unatoč tome mogu povući svoju imovinu u bilo kojem trenutku izravnom interakcijom s pametnim ugovorom. U slučaju *EtherDelta* korisnici šalju trgovinske instrukcije samom pametnom ugovoru, dok *IDEX* koristi zasebni račun za pokretanje trgovinskih instrukcija u pametnom ugovoru.

2.2.2 Automatizirani Market Maker DEX

AMM DEX-ovi kao što su *Uniswap* i *Kyber* značajno se razlikuju od LOB DEX-a. Korisnici ne trguju *peer-to-peer* već naspram fonda likvidnosti ili rezerve. Trgovanje se provodi pomoću pametnih ugovora.

Skup ili **fond likvidnosti** *(eng. liquidity pool)* je skup kriptovaluta ili tokena zaključanih u pametnom ugovoru koji se koristi za olakšavanje trgovanja sredstvima na decentraliziranoj burzi. Prije nego što su automatizirani market makeri ušli u igru, likvidnost kripto tržišta bila je izazov za DEX na Ethereumu. U to su vrijeme DEX-ovi bili nova tehnologija s kompliciranim sučeljem, a broj kupaca i prodavača bio je mali pa je bilo teško pronaći dovoljno ljudi voljnih redovito trgovati. AMM-ovi rješavaju ovaj problem ograničene likvidnosti stvaranjem fondova likvidnosti i nudeći pružateljima likvidnosti poticaj da opskrbe te fondove imovinom, a sve to bez potrebe za posrednicima treće strane. Što je više sredstava u skupu i što skup ima veću likvidnost, to

je lakše trgovanje na decentraliziranim burzama. Skupovi likvidnosti igraju ključnu ulogu u ekosustavu decentraliziranih financija (DeFi) obzirom da ne zahtjevaju podudaranje kupca i prodavača što znači da korisnici mogu jednostavno razmijeniti svoju imovinu koristeći likvidnost spomenutog skupa. Na *Uniswapu* svaka rezerva ili ugovor sadrži sredstva u obliku tokena i ETH. *Uniswap* ima mehanizam određivanja cijena koji se naziva formula *"konstantnog produkta AMM-a" (eng. constant product automated market maker, CPAMM).* Cijene su određene udjelom tokena i ETH sredstava u rezervi u odnosu na invarijantu ukupne likvidnosti koja ostaje stabilna tijekom trgovanja. Pružatelji likvidnosti popunjavaju skupove likvidnosti i uvijek moraju dati jednake količine tokena i ETH. Stanje (ili dubina) AMM tržišta X/Y definira se kao par (x, y), gdje x predstavlja iznos imovine X, a y iznos imovine Y u fondu likvidnosti. U trenutku pisanja ovog rada odnos BTC/USD je (22000, 1). Pružatelji likvidnosti mogu položiti ili povući sredstva X i Y kako bi povećali ili smanjili likvidnost.

Prilikom trgovanja na AMM burzi može postojati razlika između očekivane cijene i izvršene cijene, a ta se razlika naziva **klizanje** *(eng. slippage).* Klizanje na AMM-u najčešće je u razdobljima veće volatilnosti, a može biti uzrokovano nedovoljnom likvidnošću i drugim poslovima koji se vode unaprijed. Ono se pojavljuje kao rezultat nagle promjene raspona ponude i potražnje *(eng. bid-ask spread).* Računanje klizanja izuzetno je važan korak prije svake trgovine zbog ograničavanja potencijalnih gubitaka, posebice ako se bavimo izuzetno volatilnim vrstama imovine poput kriptovaluta. Formula klizanja je sljedeća:

$$\frac{ponuđena\ \ cijena - tražena\ \ cijena}{količina} \cdot 100\%.$$

Sudionici na tržištu mogu se zaštititi od klizanja postavljanjem limitiranih naloga. Dva su glavna razloga zašto dolazi do klizanja pri trgovanju kriptovalutama: likvidnost i volatilnost.

Volatilnost. Klizanje se događa u situaciji velike volatilnosti jer se cijena mijenja tako brzo da se cijena po kojoj se nalog izvršava dramatično promijenila od cijene po kojoj je nalog unesen. Trgovac očekuje da će dobiti cijenu po kojoj je unio nalog, ali zbog divljih oscilacija njegov nalog se izvršava po potpuno drugačijoj cijeni. Kriptovalute su još uvijek vrlo spekulativni instrumenti i kao rezultat toga dovoljan je samo jedan zvučan medijski naslov kako bi se izazvao značajan porast ili pad cijene.

Likvidnost. Drugi razlog za proklizavanje cijena kriptovaluta je nedostatak likvidnosti. Nekim se kriptovalutama ne trguje često zbog nedostatka popularnosti ili novosti u

usporedbi s drugim kriptovalutama. Kao rezultat toga, razlika između najniže tražene i najviše ponuđene cijene može biti velika, uzrokujući iznenadne dramatične promjene u cijeni — prije nego što se nalog koji je unesen može izvršiti. Kada imovina ima nisku likvidnost to znači da se ne može lako pretvoriti u gotovinu. Manje popularne kriptovalute su donekle nelikvidne jer za njih možda neće uvijek biti kupaca, što znači da se ne mogu pretvoriti u gotovinu. Niska likvidnost može uzrokovati značajno odstupanje jer s tako malo kupaca bit će i mali broj traženih cijena. Na primjer, likvidna imovina poput blue-chip dionica[1] će navesti investitore da navedu svoje ponude (iznos koji su spremni platiti) u širokom rasponu iznosa blizu trenutne tržišne cijene. Međutim, relativno malo ulagača želi kupiti nelikvidnu imovinu poput kriptovaluta kojima se manje trguje.

Recimo da je prodavač unio tržišni nalog za prodaju svoje kriptovalute za $1.50 što mu omogućuje da je proda čim se pojavi kupac. Prodavač na kupca može čekati dva dana, ali je kupac za to spreman platiti samo $0.50. Budući da se radi o tržišnom nalogu on će se izvršiti po bilo kojoj trenutnoj tržišnoj cijeni. Obzirom da samo jedan kupac nudi $0.50, tržišna cijena te kriptovalute će pasti s $1.50 na $0.50. Nedostatak kupaca znači da može dolaći do naglog pada tržišne cijene kroz jednu ili nekog manjeg broja transakcija.

2.3 Trgovanje maržom

Trgovanje maržom *(eng.maring trading)* pojam je koji znači da investitori posuđuju novac za kupnju financijskih instrumenata. To je rizična strategija trgovanja koja zahtijeva polaganje novca na brokerski račun kao kolateral za zajam. Trgovanje uz maržu omogućuje korištenje poluge za povećanje kupovne moći i veća ulaganja nego što bi mogli s vlastitim resursima. Treba imati na umu da kupovinom dionica posuđenim sredstvima riskiramo nagomilavanje većih gubitaka. To je vrsta osiguranog kreditiranja. Kada bi uzeli zajam od svog brokera ili platforme za kupnju uz maržu, zajam je osiguran ulaganjima koja kupimo.

Glavna prednost trgovanja maržom je veća kupovna moć: uz mali početni kapital moguće je dobiti pomoć za ulaganje u vidu dodatnog kapitala što otvara prostora za mogućnost visoke zarade. Negativna strana trgovanja maržom su potencijalno neograničeni gubici. On-chain platforme za trgovanje maržom zadržavaju kontrolu nad

[1]Blue-chip dionice su dionice kompanija s izvrsnom reputacijom koje su financijski stabilne i obično imaju tržišnu kapitalizaciju u milijardama američkih dolara. Među ulagačima postoji percepcija da takve dionice mogu nadvladati različite tržišne izazove. Neki primjeri blue chip dionica su Apple, IBM Corp., Coca-Cola Co. i Boeing Co..

posuđenom imovinom i stoga mogu izvršiti likvidaciju kada vrijednost kolaterala trgovca padne prenisko.

2.4 Ethereum Virtual Machine i prijelazi stanja

Ethereum Virtual Machine (EVM) okruženje je za implementaciju i izvođenje pametnih ugovora na Ethereum mreži. U fizičkom smislu, EVM postoji kao jedna cjelina koju održava tisuće povezanih računala koja pokreću Ethereum klijenta. Sam Ethereum protokol postoji isključivo sa svrhom održavanja kontinuiranog i nepromjenjivog rada stroja stanja. To je okruženje u kojem žive svi Ethereum računi i pametni ugovori. U bilo kojem bloku u lancu Ethereum ima jedno i samo jedno *kanonsko* stanje, a EVM je ono što definira pravila za izračunavanje novog valjanog stanja od bloka do bloka.

Analogija distribuirane knjige često se koristi za opisivanje blockchaina poput Bitcoina koji omogućuju postojanje decentralizirane valute koristeći temeljne alate kriptografije. Glavna knjiga odražava evidenciju aktivnosti gdje je obavezno pridržavanje skupa pravila koja određuju što netko može, a što ne može učiniti kako bi unio promjene u glavnu knjigu. Osim toga što ima vlastitu izvornu kriptovalutu ether (ETH) koja također slijedi određena pravila, Ethereum blockchain omogućuje vrlo moćnu funkciju: pametne ugovore. Za ovu složeniju značajku potrebna je sofisticiranija analogija. Umjesto distribuirane knjige Ethereum blockchain je distribuirani stroj stanja.

Stanje Ethereuma velika je struktura podataka koja sadrži sve račune i balanse (stanja računa), ali i stanje stroja koje se može mijenjati od bloka do bloka u skladu s unaprijed definiranim skupom pravila. EVM definira posebna pravila promjene stanja iz bloka u blok. Ponaša se kao matematička funkcija: s obzirom na ulaz proizvodi deterministički izlaz. Stoga ćemo formalno opisati Ethereum kao funkciju prijelaza stanja. S obzirom na staro važeće stanje S i novi skup valjanih transakcija T, Ethereumova funkcija prijelaza stanja $Y(S, T)$ proizvodi novo važeće izlazno stanje S'. U kontekstu Ethereuma stanje je struktura podataka nazvana modificirano Merkle Patricia stablo koje drži sve račune povezanima hashevima i može se svesti na jedan root hash pohranjen na blockchainu.

Pametni ugovori vrsta su Ethereum računa. To znači da imaju balans i mogu biti meta transakcija. Međutim, njima ne upravlja korisnik već se postavljaju na mrežu i rade onako kako su programirani. Korisnički računi mogu komunicirati s pametnim ugovorom podnošenjem transakcija koje izvršavaju funkciju definiranu pametnim ugovorom. Pametni ugovor prvi je opisao Szabo [27] kao računalni transakcijski protokol

koji izvršava uvjete ugovora. Opći ciljevi dizajna pametnog ugovora su zadovoljiti uobičajene ugovorne uvjete (kao što su uvjeti plaćanja, založna prava, povjerljivost i izvršenje), minimizirati iznimke bile one zlonamjerne ili slučajne te minimizirati potrebu za pouzdanim posrednicima. Povezani ekonomski ciljevi uključuju smanjenje gubitaka zbog prijevare, troškova arbitraže i provedbe te ostalih transakcijskih troškova.

Pametni ugovor može se programirati logikom poništavanja transakcije ako određeni uvjet nije ispunjen tijekom izvršenja. EVM stanje se mijenja samo ako se transakcija uspješno izvrši, inače se EVM stanje vraća na prethodno, neizmijenjeno stanje.
Neke od najpoznatijih ranjivosti pametnih ugovora proizlaze iz redoslijeda potvrđivanja transakcija, ovisnosti o vremenskoj oznaci bloka, pogrešno obrađenim iznimkama te ponovnim pozivanjem. Zainteresirani čitatelj u [22] i [21] može detaljnije proučiti ranjivosti pametnih ugovora.

2.5 Brzi zajam

Brzi zajam *(eng. flash loan)* je zajam koji vrijedi samo unutar jedne atomske blockchain transakcije. Brzi zajmovi podbacuju ako zajmoprimac ne otplati svoj dug prije završetka transakcije posuđivanja zajma. To je zato što se blockchain transakcija može poništiti tijekom izvršenja ako uvjet otplate nije zadovoljen, tj. EVM omogućuje poništavanje promjena stanja.
Brzi zajmovi donose tri svojstva kojih nema u tradicionalnom financiranju:

1. Nerizično posuđivanje *(eng. risk-free lending)*: Ukoliko zanemarimo ranjivosti pametnog ugovora i blockchaina, zajmodavac nije izložen rizicima neplaćanja duga. Budući da se transakcija i njezine instrukcije moraju izvršiti atomski, brzi zajam se ne odobrava ako transakcija ne uspije zbog neplaćanja duga.

2. Nema potrebe za kolateralom: Budući da se zajmodavcu garantira vraćanje duga, on zbog toga može izdati kredit bez kolaterala unaprijed od strane zajmoprimca. Brzi zajam nije kolateraliziran.

3. Veličina kredita: Brzi zajmovi mogu se uzeti iz javnih fondova likvidnosti kojima upravljaju pametni ugovori. Svaki zajmoprimac može posuditi cijeli fond u bilo kojem trenutku.

Poglavlje 3

Razlika u dobiti kod atomske i neatomske arbitraže

U ovom poglavlju objašnjavamo utjecaj atomičnosti transakcije na rizike arbitraže. U atomskoj blockchain transakciji radnje se mogu izvršiti kolektivno u nizu ili kolektivno ne uspjeti. Drugim riječima, ako jedan dio transakcije ne uspije tada cijela transakcija ne uspijeva, a stanje ostaje nepromijenjeno. Tehnički gledano, upravljanje DeFi radnjama u atomskoj transakciji jednako je:

- stjecanju zaključavanja na svim uključenim financijskim tržištima kako bi se osiguralo da nijedan drugi tržišni agent ne može u međuvremenu mijenjati tržišna stanja te
- otpuštanju zaključavanja nakon izvršenja svih radnji u njihovom nizu.

Kako bismo objektivno kvantificirali utjecaj atomičnosti transakcije na arbitražni profit, nastavljamo sa sljedećom metodologijom. Razmatramo arbitraže koje uključuju dvije razmjene *(eng. trades)* T_A i T_B kako bismo empirijski usporedili atomske i neatomske arbitraže (usp. slika 3.1). Definirajmo dobit od atomske i neatomske arbitraže:

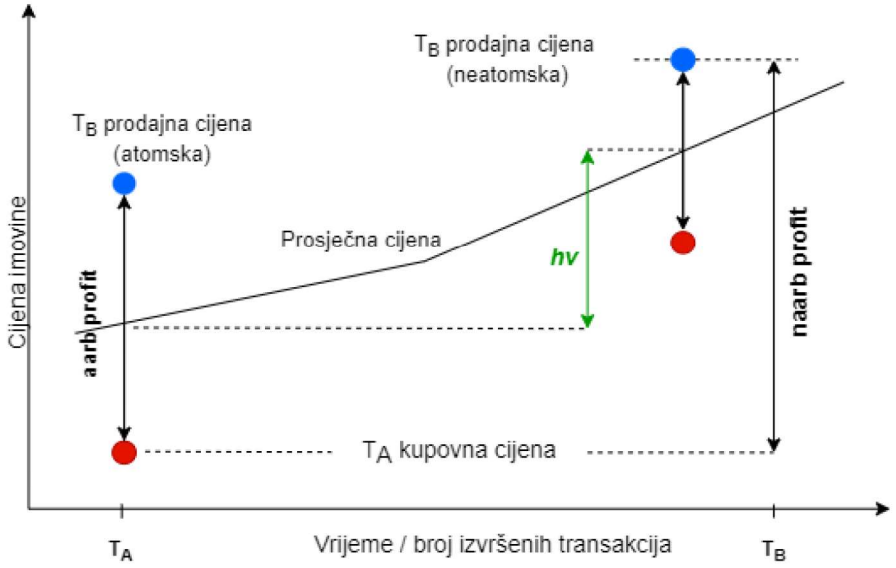
- **Dobit od atomske arbitraže *(aarb)*** definira se kao dobit od dvije atomski izvršene arbitražne razmjene T_A i T_B na burzama A i B.
- **Dobit od neatomske arbitraže *(naarb)*** definira se kao dobitak od arbitraže ako se prvo izvrši T_A, a izvršenje T_B slijedi nakon nekoliko posredničkih transakcija.

Neatomska arbitraža zahtijeva od arbitra zaključavanje imovine na kratko vrijeme (reda sekunda/minuta). Ta je imovina zbog vremenskog jaza izložena nestabilnosti cijena. Arbitar ponekad može ostvariti dobit ako imovina poraste u vrijednosti, ali jednako

tako ima rizik od gubitka vrijednosti.

Vrijednost držanja *hv (eng. holding value)* definira se kao promjena u prosječnoj cijeni zadanog para imovina na dvije burze, što predstavlja promjenu vrijednosti imovine tijekom neatomarnog razdoblja izvršenja. Uvodimo vrijednost držanja kako bismo neutralizirali volatilnost cijena i stoga možemo objektivno kvantificirati financijsku prednost atomske arbitraže. S obzirom na ove varijable definiramo razliku dobiti.

$$razlika\ dobiti = aarb - (naarb - hv)$$



Slika 3.1: *Utjecaj atomičnosti transakcije na arbitražu*

Slika 3.1 objašnjava utjecaj atomičnosti transakcije na arbitražu. Arbitar podnosi prvu razmjenu T_A koja ima za cilj kupnju imovine po nižim cijenama (crveno) i prodaju imovine na drugoj burzi po višoj cijeni (plavo). U neatomskom okruženju T_B se ne izvršava odmah nakon T_A. Vrijednost držanja je porast ili smanjenje cijene kada se imovina drži između T_A i T_B.

Poglavlje 4

Parametarski optimizacijski model

Atomičnost blockchain transakcija jamči kontinuitet izvršenja radnji. Kada je početno stanje deterministički poznato ova značajka omogućuje trgovcu da točno predvidi međurezultate nakon svakog izvršenja akcije i zatim optimizira ishod napada podešavanjem parametara akcije. Počinjemo modeliranjem različitih komponenti koje bi mogle sudjelovati u DeFi napadu.

Kvantitativno formaliziramo svaku krajnju točku koju pružaju DeFi platforme kao funkciju prijelaza stanja

$$S_0 = T(S; p)$$

$$s\ ograničenjima\ C(S; p),$$

gdje je S dano stanje, p su parametri koje je odabrao trgovac, a S_0 je izlazno stanje. Stanje može predstavljati nečiji balans ili bilo koji interni status DeFi platforme, dok su ograničenja postavljena zahtjevima izvršenja EVM-a (npr. ether bilanca entiteta nikada ne smije biti negativan broj) ili su to pravila definirana odgovarajućom DeFi platformom (npr. brzi zajam uvećan za naknade mora se otplatiti prije završetka transakcije). Kada kvantificiramo dobit zanemarujemo plaćanja kamata odnosno naknada za kredit i naknade za transakcije koje su zanemarive veličine u DeFi napadima koje obrađujemo u ovom radu.

Definiramo funkciju stanja ravnoteže $\mathcal{B}(\mathbb{E}; X; S)$ kako bi označili ravnotežu valute X koju drži entitet $\mathbb{E}$ u danom stanju S i zahtijevamo da vrijedi

$$\forall(\mathbb{E}; X; S) \quad \mathcal{B}(\mathbb{E}; X; S) \geqslant 0.$$

Vektor napada specificira redoslijed izvršenja različitih krajnjih točaka na različitim DeFi platformama i ovisno o tome formaliziramo jednosmjerni lanac prijelaznih funkcija

$$S_i = T_i(S_{i-1}; p_i). \tag{4.1}$$

Ugnježđivanjem prijelaznih funkcija dobivamo kumulativne funkcije prijelaza stanja $\mathcal{ACC}_i(S_0; p^{1:i})$ koje zadovoljavaju relaciju (4.2), gdje je $p^{1:i} = (p_1, ..., p_i)$:

$$S_i = T_i(S_{i-1}; p_i) = T_i(T_{i-1}(S_{i-2}; p_{i-1}); p_i)$$

$$= T_i(T_{i-1}(...T_1(S_0, p_1)...; p_{i-1}); p_i) = \mathcal{ACC}_i(S_0; p^{1:i}). \tag{4.2}$$

Stoga se ograničenja generirana u svakom koraku mogu izraziti kao relacija (4.3):

$$C_i(\mathcal{ACC}_i(S_0; p^{1:i}); p_i). \tag{4.3}$$

Pretpostavljamo da je vektor napada sastavljen od N prijelaznih funkcija. Funkcija cilja $\mathcal{O}$ može se izračunati iz početnog stanja S_0 i konačnog stanja S_N:

$$\mathcal{O}(S_0; \mathcal{ACC}(S_0; p^{1:N})). \tag{4.4}$$

S obzirom na početno stanje S_0 formuliramo vektor napada u problem ograničene optimizacije s obzirom na sve parametre $p^{1:N}$ (usp. jednadžbe (4.5)).

$$max\ \mathcal{O}(S_0; \mathcal{ACC}(S_0; p^{1:N}))$$

$$t.d. \quad C_i(\mathcal{ACC}_i(S_0; p^{1:i}); p_i) \quad \forall i \in \{1, \ldots, N\} \tag{4.5}$$

Poglavlje 5

DeFi modeli

U nastavku detaljno opisujemo kvantitativne DeFi modele primijenjene u ovom radu. Imajte na umu da ne uključujemo sva stanja uključena u DeFi napade već samo ona relevantna za ograničenu optimizaciju.

5.1 Brzi zajam

Pretpostavljamo platformu za brzi zajam $\mathbb{F}$ sa z_X iznosom imovine X koju trgovac $\mathbb{A}$ može posuditi. Potrebna kamata za posudbu b od X označena je s *b'*.

`Stanje:` U brzom zajmu stanje je predstavljeno saldom od $\mathbb{A}$: $\mathcal{B}(\mathbb{A}; X; S)$.

`Prijelazi:` Definiramo prijelazne funkcije `Loan` u relaciji (5.1) i `Repay` u relaciji (5.2), gdje parametar b_X označava posuđeni iznos.

$$\mathcal{B}(\mathbb{A}; X; S') = \mathcal{B}(\mathbb{A}; X; S) + b_X, \quad t.d. \;\; z_X - b_X \geqslant 0, \tag{5.1}$$

$$\mathcal{B}(\mathbb{A}; X; S') = \mathcal{B}(\mathbb{A}; X; S) - b_X - b', \quad t.d. \;\; \mathcal{B}(\mathbb{A}; X; S) - b_X - b' \geqslant 0. \tag{5.2}$$

5.2 Trgovanje po fiksnoj cijeni

Definiramo krajnju točku `SellXforY` koja dopušta trgovcu $\mathbb{A}$ da trguje količinom q_X od X za Y po fiksnoj cijeni p_m u trenutku m. $maxY$ označava najveći iznos od Y dostupan za trgovanje.

`Stanje:` Razmatramo sljedeće varijable stanja:
- stanje imovine X koju drži $\mathbb{A}$: $\mathcal{B}(\mathbb{A}; X; S)$
- stanje imovine Y koju drži $\mathbb{A}$: $\mathcal{B}(\mathbb{A}; Y; S)$.

`Prijelazi:` Funkcije prijelaza od `SellXforY` dane su relacijama (5.3):

$$\begin{aligned} \mathcal{B}(\mathbb{A}; X; S') &= \mathcal{B}(\mathbb{A}; X; S) - q_X \\ \mathcal{B}(\mathbb{A}; Y; S') &= \mathcal{B}(\mathbb{A}; Y; S) + \frac{q_X}{p_m} \\ t.d.\ \ \mathcal{B}(\mathbb{A}; X; S) - q_X \geqslant 0, &\quad maxY - \frac{q_X}{p_m} \geqslant 0. \end{aligned} \tag{5.3}$$

5.3 Konstantni produkt AMM

Konstantni produkt AMM (CPAMM) ima tržišni udio od 77% među AMM DEX proizvodima i najzastupljeniji je AMM model u trenutnom DeFi ekosustavu. S $\mathbb{M}$ označavamo instancu AMM s trgovačkim parom X/Y i tečajem f.

`Stanje:` Razmatramo sljedeće varijable stanja koje se mogu mijenjati u AMM prijelazu stanja:
- iznos X u skupu likvidnosti AMM: $u_X(S)$, što je jednako $\mathcal{B}(\mathbb{M}; X; S)$
- iznos Y u skupu likvidnosti AMM: $u_Y(S)$, što je jednako $\mathcal{B}(\mathbb{M}; Y; S)$
- saldo imovine X koji drži $\mathbb{A}$: $\mathcal{B}(\mathbb{A}; X; S)$
- saldo imovine Y koji drži $\mathbb{A}$: $\mathcal{B}(\mathbb{A}; Y; S)$.

`Prijelazi:` Među krajnjim točkama $\mathbb{M}$-a usredotočeni smo na `SwapXforY` i `SwapYforX` koje su relevantne krajnje točke za DeFi napade o kojima se govori u ovom radu. Parametar p_X predstavlja iznos imovine X kojim trgovac namjerava trgovati. $\mathbb{A}$ unosi p_X iznos od X u skup likvidnosti AMM i prima o_Y iznos od Y kao izlaz. Pravilo konstantnog produkta zahtijeva da vrijedi (5.4):

$$u_X(S) \times u_Y(S) = (u_X(S) + (1-f)p_X) \times (u_Y(S) - o_Y) \tag{5.4}$$

Skup likvidnosti imovine X uvećat će se za iznos imovine X kojom je trgovac trgovao i umanjiti za naknadu za trgovanje parom X/Y, dok će se skup likvidnosti za imovinu Y umanjiti za vrijednost koju je trgovac kupio. Relacijom (5.5) definiramo funkcije prijelaza `SwapXforY` i ograničenja (analogno za `SwapYforX`):

$$\begin{aligned}
\mathcal{B}(\mathbb{A}; X; S') &= \mathcal{B}(\mathbb{A}; X; S) - p_X \\
\mathcal{B}(\mathbb{A}; Y; S') &= \mathcal{B}(\mathbb{A}; Y; S) + o_Y \\
u_X(S') &= u_X(S) + p_X \\
u_Y(S') &= u_Y(S) - o_Y \\
gdje\ je\ \ o_Y &= \frac{p_X \times (1-f) \times u_Y(S)}{u_X(S) + p_X \times (1-f)} \\
t.d.\ \ \mathcal{B}(\mathbb{M}; X; S) - p_X &\geqslant 0.
\end{aligned} \tag{5.5}$$

Budući da AMM DEX $\mathbb{M}$ transparentno izlaže sve cjenovne prijelaze na lancu, druge DeFi platforme mogu ga koristiti kao cjenovni oracle[1]. Cijena Y u odnosu na X koju daje $\mathbb{M}$ u stanju S dana je izrazom (5.6):

$$p_Y(\mathbb{M}; S) = \frac{u_X(S)}{u_Y(S)}. \tag{5.6}$$

Primjer 5.1. *Pretpostavimo da neki CPAMM skup likvidnosti u stanju S sadrži 30,000 DAI i 10 ETH. Pravilo CPAMM-a je*

$$u_X(S) \times u_Y(S) = 10 \cdot 30,000 = 300,000$$

Trgovac će za prodaju 1 ETH dobiti $2,727.2727272727275$ DAI:

$$o_Y = \frac{p_X \times (1-f) \times u_Y(S)}{u_X(S) + p_X \times (1-f)} = \frac{1 \times 30000}{10+1} = 2,727.2727272727275 DAI.$$

Potvrdimo da formula 5.4 vrijedi:

$$u_X(S') \times u_Y(S') = 11 \cdot 2,727.2727272727275 = 300,000.$$

Napomena 5.1. *DAI i ETH imaju 18 decimala. Najmanja jedinica DAI-a je $1 attoDAI = 10^{-18} DAI$, a najmanja jedinica ETH je $1 wei = 10^{-18} ETH$. Jedinica $1 gwei = 10^{-19} wei$ često se koristi u prikazivanju cijena plina ili drugih naknada u kriptovaluti ETH.*

[1]Cjenovni oracle je sustav koji daje tečajeve ili cijene pametnim ugovorima DeFi protokola, a detaljnije je obrađen u poglavlju 8.

5.4 Automatizirana rezerva cijena

Automatizirana rezerva cijena još je jedna vrsta AMM-a koja automatski izračunava cijenu razmjene ovisno o imovini koja se nalazi u zalihama. Rezervu koja drži par imovine X/Y označavamo s $\mathbb{Z}$. Minimalna cijena $minP$ i maksimalna cijena $maxP$ postavljaju se prilikom pokretanja $\mathbb{Z}$. $\mathbb{Z}$ se oslanja na parametar omjera likvidnosti lr za izračun cijene imovine. Pretpostavljamo da $\mathbb{Z}$ sadrži $k_X(S)$ količinu od X u stanju S. Cijena Y dana je izrazom (5.7) .

$$P_Y(\mathbb{Z}; S) = minP \times e^{lr \times k_X(S)}. \tag{5.7}$$

Krajnja točka `ConvertXtoY` koju pruža $\mathbb{Z}$ omogućuje trgovcu $\mathbb{A}$ da zamijeni X za Y.

`Stanje:` Razmatramo sljedeće varijable stanja:
- inventar X u rezervi: $k_X(S)$ što je jednako $\mathcal{B}(\mathbb{Z}; X; S)$
- stanje imovine X koju drži $\mathbb{A}$: $\mathcal{B}(\mathbb{A}; X; S)$
- stanje imovine Y koju drži $\mathbb{A}$: $\mathcal{B}(\mathbb{A}; Y; S)$.

`Prijelazi:` S h_X označimo iznos imovine X koji $\mathbb{A}$ unosi u razmjenu za trgovanje u odnosu na Y. Iznos razmjene Y izračunava se sljedećom formulom:

$$j_Y = \frac{e^{-lr \times h_X} - 1}{lr \times P_Y(\mathbb{Z}; S)}. \tag{5.8}$$

Relacijama (5.9) definiramo funkcije prijelaza:

$$\begin{gathered}
k_X(S') = k_X(S) + h_X \\
\mathcal{B}(\mathbb{A}; X; S') = B(\mathbb{A}; X; S) - h_X \\
\mathcal{B}(\mathbb{A}; Y; S') = B(\mathbb{A}; Y; S) + j_Y \\
\\
gdje\ je\ \ j_Y = \frac{e^{-lr \times h_X} - 1}{lr \times P_Y(\mathbb{Z}; S)} \\
t.d.\ \ \mathcal{B}(\mathbb{A}; X; S)) - h_x \geqslant 0, \\
P_Y(\mathbb{Z}; S') - minP \geqslant 0, \\
maxP - P_Y(\mathbb{Z}; S') \geqslant 0.
\end{gathered} \tag{5.9}$$

5.5 Kolateralizirano pozajmljivanje i posuđivanje

Razmatramo platformu za pozajmljivanje *(eng. lending)* $\mathbb{L}$ s kolateralom koja pruža krajnju točku `CollateralizedBorrow` kojom zahtijeva od korisnika da kolateralizira imovinu X faktorom kolaterala cf t.d. $0 < cf < 1$ i posuđuje drugu imovinu Y po tečaju er. Faktor kolaterala određuje gornju granicu iznosa kojeg korisnik može posuditi. Npr., ako je faktor kolaterala 0.75 korisnik može posuditi do 75% vrijednosti kolaterala. Tečaj je, na primjer, određen vanjskim cjenovnim orcaleom. Maksimalni iznos imovine Y dostupan za posuđivanje označavamo z_Y.

`Stanje:` Razmatramo sljedeće varijable stanja i radi jednostavnosti zanemarujemo promjene ravnoteže $\mathbb{L}$ (platforme za kolateralizirani lending):
- saldo imovine X koji drži $\mathbb{A}$: $\mathcal{B}(\mathbb{A}; X; S)$
- saldo imovine Y koji drži $\mathbb{A}$: $\mathcal{B}(\mathbb{A}; Y; S)$.

`Prijelazi:` Parametar c_X predstavlja iznos imovine tipa X koju $\mathbb{A}$ želi osigurati kolateralom. Iako bi $\mathbb{A}$ mogao posuditi manje nego što bi njegov kolateral dopuštao, pretpostavljamo da $\mathbb{A}$ koristi cijeli svoj kolateral. Izrazima (5.10) prikazujemo funkcije prijelaza `CollateralizedBorrow`.

$$\begin{aligned} \mathcal{B}(\mathbb{A}; X; S') &= \mathcal{B}(\mathbb{A}; X; S) - c_X \\ \mathcal{B}(\mathbb{A}; Y; S') &= \mathcal{B}(\mathbb{A}; Y; S) + b_Y \\ gdje\ je\ \ b_Y &= \frac{c_X \times cf}{er} \\ t.d.\ \ \mathcal{B}(\mathbb{A}; X; S) - c_x \geqslant 0;&\quad z_Y - b_Y \geqslant 0. \end{aligned} \tag{5.10}$$

Trgovac može povratiti svoj kolateral otplatom posuđenih sredstava putem krajnje točke `CollateralizedRepay`. Izrazima (5.11) dane su funkcije prijelaza i zbog jednostavnosti zanemarujemo naknadu za kamatu na kredit:

$$\begin{aligned} \mathcal{B}(\mathbb{A}; X; S') &= B(\mathbb{A}; X; S) + c_X \\ \mathcal{B}(\mathbb{A}; Y; S') &= B(\mathbb{A}; Y; S) - b_Y \\ t.d.\ \ \mathcal{B}(\mathbb{A}; Y; S) - b_Y &\geqslant 0. \end{aligned} \tag{5.11}$$

5.6 Trgovanje maržom

Platforma za trgovinu maržom $\mathbb{T}$ omogućuje trgovcu $\mathbb{A}$ da otvori long ili short poziciju za imovinu Y davanjem sredstva X kao kolateral uz financijsku polugu l *(eng. leverage)*, gdje je $l \geqslant 1$. Usredotočit ćemo se na krajnju točku `MarginShort` koja je relevantna za napade na DeFi platforme koji se razmatraju u ovom radu.
Pretpostavljamo da $\mathbb{A}$ otvara short poziciju za Y u odnosu na X na $\mathbb{F}$. Parametar d_X označava iznos od X koji $\mathbb{A}$ daje kao kolateral unaprijed kako bi otvorio marginu. w_X predstavlja iznos of X koji drži $\mathbb{F}$ a koji je dostupan za short marginu. $\mathbb{A}$ je u trgovanju maržom dužan prekomjerno kolateralizirati po stopi od *ocr*. U našem modelu, kada se otvori kratka margina (kratka Y u odnosu na X), $\mathbb{F}$ obavlja trgovinu na vanjskim X/Y tržištima (npr. *Uniswap*) kako bi pretvorio X s polugom u Y. Trgovana imovina Y je zaključana sve dok je margina zatvorena ili likvidirana.

`Stanje:` U short poziciji trgovanja maržom *(eng: short margin trading)* uzimamo u obzir sljedeće varijable stanja:
- saldo imovine X koji drži $\mathbb{A}$: $\mathcal{B}(\mathbb{A}; X; S)$
- zaključani iznos Y : $\mathcal{L}(\mathbb{A}; Y; S)$.

`Prijelazi:` Pretpostavljamo da $\mathbb{F}$ obavlja transakcije s vanjskog tržišta po cijeni od *emp (eng. external market price)*. Prijelazne funkcije i ograničenja dani su izrazima (5.12).

$$\begin{aligned} \mathcal{B}(\mathbb{A}; X; S') &= B(\mathbb{A}; X; S) - c_X \\ \mathcal{L}(\mathbb{A}; Y; S') &= \mathcal{L}(\mathbb{A}; Y; S) + l_Y \\ gdje\ je\ \ l_Y &= \frac{d_X \times l}{ocr \times emp} \end{aligned} \tag{5.12}$$

$$t.d.\ \ \mathcal{B}(\mathbb{A}; X; S)) - c_x \geqslant 0; \quad w_X + d_X - \frac{d_X \times l}{ocr} \geqslant 0.$$

Poglavlje 6

Klasificiranje slučajeva zloupotrebe brzih zajmova

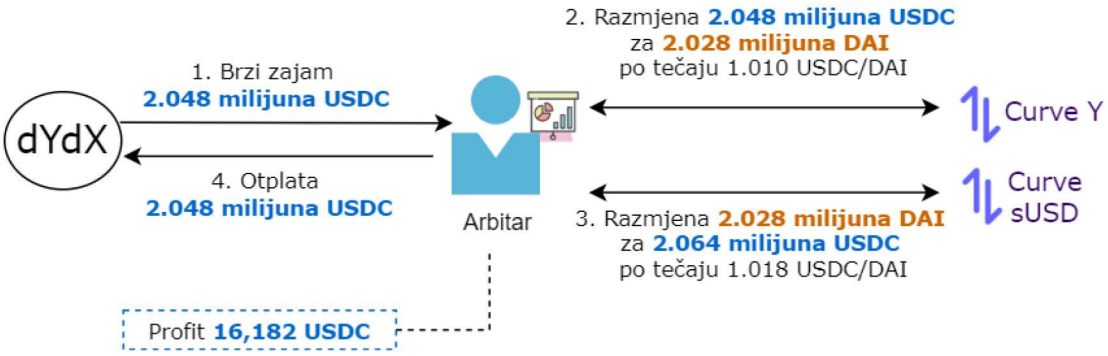
Među DeFi platformama *Aave* se među prvima istaknula omogućavanjem brzih zajmova. U vrijeme pisanja ovog rada *Aave* naplaćuje konstantnu kamatu od 0.09% za brze zajmove i prikupila je ukupnu likvidnost veću od 12 milijardi USD.
Dominantan slučaj upotrebe brzih zajmova je arbitraža, a osim arbitraže još neki slučajevi upotrebe brzih zajmova su:

1. **wash trading**: lažna inflacija obujma trgovanja,
2. **loan collateral swapping**: trenutačna zamjena s jednog kolaterala za drugi,
3. **flash minting**: trenutno uvođenje tokena i smanjenje imovine.

6.1 Arbitraža

Vrijednost imovine obično je određena ponudom i potražnjom na tržištu, na različitim burzama. Zbog nedostatka trenutne sinkronizacije među burzama istim se sredstvom može trgovati po različitim cijenama na različitim burzama. Arbitraža je proces iskorištavanja razlika u cijenama među burzama za financijsku dobit.

Primjer 6.1. Arbitraža
Na slici 6.1 predstavljamo primjer procesa izvršenja arbitražne transakcije temeljene na brzom zajmu. Arbitar je posudio brzi zajam od 2.048 milijuna USDC, izvršio dvije razmjene i ostvario dobit od približno 16,182 USDC (što je ekvivalentno $16,182), vidi transakciju.



Slika 6.1: *Izvršenje arbitražne transakcije temeljene na brzom zajmu*

Tijek transakcije:
(1) brzi zajam: na *dYdX*-u posuđeno je 2.048 milijuna USDC
(2) razmjena USDC za DAI[1] u *CurveY* skupu likvidnosti
(3) razmjena DAI za USDC u *Curve sUSD* skupu likvidnosti
(4) otplata.

Arbitar je uočio razliku u tečaju u različitim skupovima likvidnosti. Na *Curve Y* je tečaj za USDC/DAI iznosio 1.01 dok je na *Curve sUSD* tečaj iznosio 1.018 što znači da je USDC jeftiniji (a DAI skuplji) na *CurveY* nego na *Curve sUSD*. Stoga ga trgovac namjerava jeftinije kupiti i skuplje prodati. Na početku procesa trgovac uzima brzi zajam u iznosu od 2.048 milijuna USDC-a. Spomenuti iznos od 2.048 milijuna USDC mijenja za DAI u *CurveY* po tečaju USDC/DAI = 1.01, a zatim ga mijenja po tečaju USDC/DAI = 1.018 u *Curve sUSD*. Razlika u tečaju iznosi 0.008 što znači da bi trgovac trebao zaraditi 16,384 USDC no zbog raznih naknada za obavljanje transakcija on zarađuje 16,182 USDC.

[1]Dai je stabilna kriptovaluta *(eng. stablecoin)* na Ethereum blockchainu čiji je cilj održati svoju vrijednost što je moguće bliže jednom američkom dolaru putem sustava pametnih ugovora i decentraliziranih sudionika koje ti ugovori potiču na obavljanje funkcija održavanja i upravljanja. DAI je denominacija za Dai kada se trguje na burzi, kao što je to BTC za bitcoin ili ETH za ether.

6.2 Wash Trading

Wash trading je oblik tržišne manipulacije u kojem investitor istovremeno prodaje i kupuje iste financijske instrumente kako bi stvorio obmanjujuću, umjetnu aktivnost na tržištu. Investitor će prvo postaviti prodajni nalog, a zatim dati kupovni nalog za kupnju od samoga sebe. Razlozi takvom ponašanju na tržištu su sljedeći:
1) umjetno povećavanje obujma trgovanja ostavlja dojam da je instrument traženiji nego što zapravo jest,
2) generiranje provizija brokerima kako bi im se nadoknadilo nešto što se ne može otvoreno platiti. Učinili su to neki od sudionika afere Libor [18], [10].

Neke burze sada imaju ugrađene zaštite, ponekad obvezne za sudionike, kao što je STPF (funkcija sprječavanja vlastite trgovine) na Interkontinentalnoj burzi (ICE) [26]. Praksa je uobičajena na tržištima nezamjenjivih tokena *(eng. non-fungible token)* koja ne podliježu oštroj državnoj regulativi [30], [19]. Wash trading na DEX-u zahtijeva da trgovci drže i koriste stvarnu imovinu zato što neku imovinu treba staviti u nalog za prodaju ili s nekom stvarnom imovinom kupuju tu imovinu. Brzi zajmovi mogu ukloniti ovu prepreku, a troškovi wash tradinga tada se smanjuju na kamate za brzi zajam, naknade za trgovanje i blockchain transakcijske naknade, npr. plin *(eng. gas)*.

Primjer 6.2. Wash trading
2. ožujka 2020. brzi zajam od 0.01 ETH posuđen od $dYdX$-a izvršio je dvije povratne trgovine na *uniswapu*. Prvo je 0.01 ETH pretvoreno u 122.1898 LOOM, a zatim je 122.1898 LOOM pretvoreno natrag u 0.0099 ETH. 24-satni obujam trgovanja na tržištu ETH/LOOM porastao je za 25.8% (sa 17.71 USD na 22.28 USD) kao rezultat dvaju trgovanja (usp. vidi transakciju).

6.3 Zamjena kolaterala

Na sljedeći način klasificiramo DeFi platforme koje se oslanjaju na korisnike koji obavljaju poslove korištenjem kriptovaluta:
(i) DeFi sustav u kojem se nova imovina iskuje *(eng. mint)* i podupire kolateralom kojeg daje korisnik (npr. *MakerDAO*-ov DAI ili SAI) i
(ii) DeFi sustav u kojem se nude dugoročni zajmovi, a imovina se agregira unutar fondova likvidnosti.

Nakon što se otvori kolateralna pozicija DeFi platforme pohranjuju, odnosno zaključavaju kolateralnu imovinu u trezor dok se nova imovina ne uništi ili posuđena imovina ne vrati. Budući da cijene kriptovaluta fluktuiraju ovo zaključavanje imovine nosi valutni rizik. Kod brzih zajmova moguće je kolateralno sredstvo zamijeniti drugim sredstvom čak i ako korisnik nema dovoljno sredstava da uništi *(eng. burn)*, odnosno vrati novo ili posuđeno sredstvo. Korisnik može zatvoriti postojeću poziciju kolaterala s posuđenim sredstvima, a zatim odmah otvoriti novu kolateraliziranu poziciju koristeći drugu imovinu.

Primjer 6.3. Zamjena kolaterala *(eng. Collateral Swapping)*
Korisnik 20.2.2020. na *MakerDAO* uzima brzi zajam od 20 DAI-a stavljajući 0.175 wETH[2] u kolateral. Zatim je od *Aavea* posudio 0.175 wETH s kojima kupuje 178.08 BAT-a na *Uniswapu*. Tih 178.08 BAT-a stavlja u kolateral na *MakerDAO* umjesto 0.175 wETH koje izvlači van iz kolaterala te s tim iznosom otplaćuje zajam *Aaveu*, vidi transakciju.
Poanta procesa je zamijeniti temljeni kolateral zajma koristeći nula kapitala. Osim zamjene temeljnog kolaterala korisnik je zbog postojanja valutnog rizika ostvario arbitražnu dobit od približno $4.

[2]Wrapped ether (wETH) je ERC-20 kompatibilna verzija ETH-a kojom se može trgovati i može se koristiti za interakciju s drugim ERC-20 sredstvima. Mnoge decentralizirane aplikacije (DApps), kripto-novčanici i mjenjačnice izvorno podržavaju ERC-20 tokene. Međutim, ether i ERC-20 ne slijede potpuno ista pravila budući da je ether stvoren mnogo prije nego što je ERC-20 implementiran kao tehnički standard. ERC-20 tokenima može se trgovati samo za druge ERC-20 tokene, ne i ether. Kako bi se premostio ovaj jaz Ethereum mreža uvela je wETH kako bi se omogućila razmjena ethera za ERC-20 tokene (i obratno). Jedan se wETH trguje za jedan ETH, wETH/ETH = 1.

6.4 Flash Minting

Kriptovalute su općenito ili deflacijska ili inflacijska imovina, odnosno broj jedinica imovine može biti konačan ili se može povećavati. Flash minting *(eng. mint = kovanje)* koncept je koji omogućuje trenutačnu izradu proizvoljne količine novih tokena pod uvjetom da uništi isti broj tokena prije završetka iste transakcije. **Flash-mintable tokeni** (FMT) nemaju pokriće vrijednosti, a mogu se potrošiti u punoj nominalnoj vrijednosti. Prije završetka transakcije iskovani će novčići bit uništeni (metodom *burn*). Ako je raspoloživa količina tokena koje treba uništiti do kraja transakcije manja od one koja je iskovana, transakcija se poništava. Na početak oznake ovakvog tokena obično se dodaje malo slovo *f* ili prefiks *fm*. Jedan se fwETH trguje za jedan ETH, fwETH/ETH = 1.

Primjer 6.4. Flash Minting
Pretpostavimo da na početku imamo 0 fwETH i 0 ETH unutar nekog ugovora, burza A ne posjeduje ETH ali ga prihvaća.
Kako se izvodi arbitraža pomoću flash minta: Prvo, flash-mintamo 10 fwETH (pomoću pametnog ugovora), a zatim tih 10 fwETH pošaljemo na burzu A gdje zauzvrat dobivamo 1200 DAI-a. Iako ova burza ima 0 ETH, ona prihvaća fwETH pa smo u mogućnosti razmijeniti fwETH za DAI.
DAI možemo prodati na burzi B gdje je on skuplji (odnosno ETH je jeftiniji) i za njega ćemo dobiti 12 ETH. Na kraju ove transakcije uništit će se 10 fwETH. Međutim, mi više ne posjedujemo fwETH jer smo ga prodali burzi A. Kako bismo uspješno završili ovu transakciju, mintat ćemo još 10 fwETH tako da dok transakcija završi tih 10 fwETH će biti uništeno i transakcija će biti uspješna.
Poslat ćemo 10 ETH nazad u ugovor s 10 fwETH čime će se stvoriti još 10 fwETH.
Sada fwETH ugovor sadrži 20 fwETH i 10 ETH, burza A ima 10 fwETH, a mi imamo 10 fwETH i profit od 2 ETH. Na kraju transakcije poništit će se 10 fwETH iz ugovora i naših 10 fwETH.
Konačno stanje: bilježimo profit od 2 ETH, a burza A ima 10 fwETH podržanih s 10 ETH iz fwETH ugovora.

Poglavlje 7

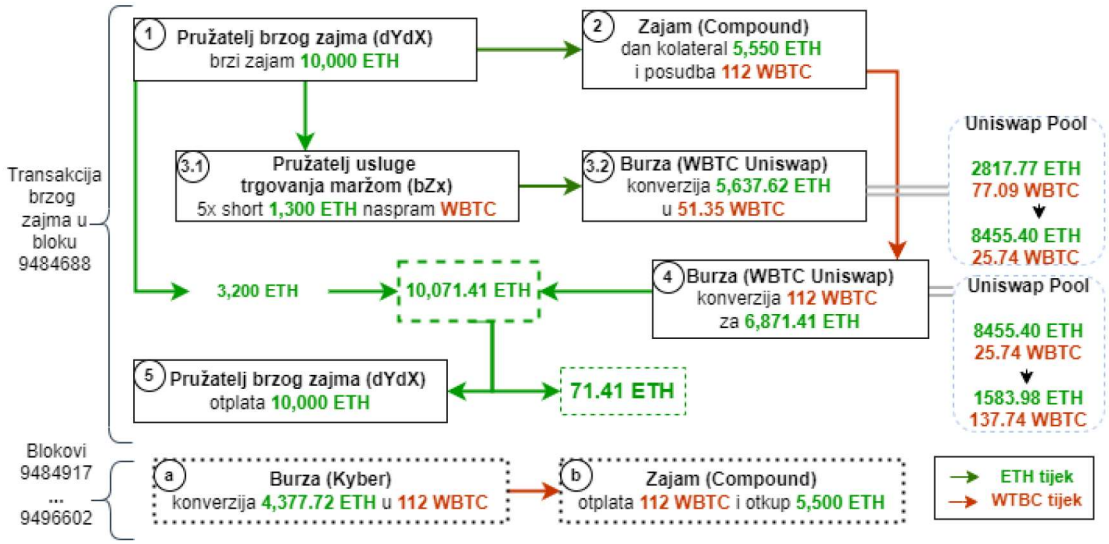
Analiza PA&A napada

Ovim ćemo poglavljem započeti detaljniju analizu prvog velikog napada na DeFi ekosustav koji se dogodio 15. veljače 2020. pružatelju usluge davanja zajmova bZx. U prvom ćemo odlomku pokazati stvarni tijek događaja te izračunati trgovčevu zaradu. Naime, trgovac u opisanom napadu nije optimalno podesio parametre i stoga je propustio priliku za kudikamo veću zaradu. Stoga se u drugom odlomku bavimo teorijskom optimizacijom. Isto vrijedi i za drugi napad opisan u poglavlju 8.

7.1 Pump Attack i arbitraža

Temeljna ideja PA&A je da napadač koristi ETH zarađen trgovanjem maržom kako bi povećao cijenu ETH/WBTC na CPAMM DEX-u (u ovom se konkretnom slučaju radi o *Uniswapu*). S WBTC-om kojeg je ranije posudio putem platforme za zajmove (*Compound*) trgovac kupuje ETH po nižoj cijeni na manipuliranom DEX-u (*Uniswap*).

Transakcija brzog zajma (usp.vidi transakciju, po ETH cijeni od 264.71 USD/ETH) donijela je dobit od 1,193.69 ETH što je tada vrijedilo oko $350,000 s obzirom na transakcijsku naknadu od $132.36. Kao što je prikazano na slici 7.1 *Pump attack i arbitraža* ovaj se napad uglavnom sastoji od dva dijela. Radi jednostavnosti izostavljamo konverziju između ETH i wETH.



Slika 7.1: *Pump attack i arbitraža*

7.1.1 Brzi zajam

Prvi dio napada sastoji se od 5 koraka unutar jedne transakcije.

1. `Loan`: Trgovac uzima brzi zajam u iznosu od 10,000 ETH od pružatelja brzih zajmova *dYdX*.

2. `CollateralizedBorrow`: Trgovac u platformu za posuđivanje *Compound* stavlja kolateral iznosa 5,500 ETH kako bi posudio 112 WBTC. Imajte na umu da trgovac ne vraća 112 WBTC unutar brzog zajma što znači da preuzima rizik od prisilne likvidacije naspram kolaterala od 5,500 ETH ako cijena fluktuira.

3. `MarginShort` & `SwapXforY`: Trgovac daje 1,300 ETH za otvaranje short pozicije za ETH u odnosu na WBTC (na *bZx*) s polugom 5×. Po primitku ovog zahtjeva *bZx* vrši transakcije (kupuje) 5,637.62 ETH na burzi *Uniswap* za 51.35 WBTC (po tečaju 109.79 ETH/WBTC). Trebamo imati na umu da na početku bloka 9484688 *Uniswap* ima ukupnu ponudu od 2,817.77 ETH i 77.09 WBTC (po tečaju 36.55 ETH/WBTC). Klizanje ove transakcije je značajno sa $\frac{109.79 - 36.55}{36.55} = 200.38\%$.

4. `SwapYforX`: Trgovac prodaje 112 WBTC (posuđenih od platforme za posuđivanje *Compound*) za 6,871.41 ETH na *uniswapu* (po tečaju 61.35 ETH/WBTC).

Napominjemo da je kapital trgovčevog maržnog računa negativan nakon maržnog trgovanja zbog značajnog kretanja cijene. Napad se mogao izbjeći da je *bZx* provjerio negativni kapital i poništio transakciju. U vrijeme napada ova je logika postojala u *bZx* ugovorima, ali se nije ispravno pozivala.

5. `Repay`: trgovac vraća brzi zajam uvećan za proviziju od 107 ETH.

Nakon transakcije brzog zajma trgovac bilježi dobit od 71.41 ETH ($\star$) i ima dug od 112 WBTC prekomjerno kolateraliziran s 5,500 ETH (49.10 ETH/WBTC). Ako je tržišna cijena ETH/WBTC ispod ovog tečaja trgovac može otkupiti kolateral zajma na sljedeći način.

7.1.2 Otkup zajma

Drugi dio trgovanja sastoji se od dva ponavljajuća koraka (korci *a* i *b* na slici 7.1) između Ethereum blokova 9484917 i 9496602. Te transakcije imaju za cilj otkupiti ETH otplatom WBTC-a koji je ranije posuđen na *Compoundu*. Kako bi se izbjeglo klizanje pri kupnji WBTC-a trgovac izvršava drugi dio u malim iznosima tijekom razdoblja od dva dana na DEX-ovima *Kyber* i *Uniswap*. Trgovac je ukupno razmijenio 4,377.72 ETH za 112 WBTC (po 39.08 ETH/WBTC) kako bi otkupio 5,500 ETH.

7.1.3 Identificiranje i kvantificiranje žrtve

U trećem koraku trgovac je otvorio short poziciju s 1,300 ETH naspram WBTC. Taj korak zahtjeva od pružatelja likvidnosti *bZx* kupovinu WBTC koju obavlja na *uniswapu* po tečaju od 109.79 ETH/WBTC. Ovaj tečaj ne odgovara tržišnoj cijeni koja je iznosila 36.55 ETH/WBTC prije napada, stoga pružatelj likvidnosti preplaćuje WBTC gotovo 3×.
bZx gubi 4,337.62 – 51.35 × 39.08 = 2,330.86 ETH.

↳ (ETH od davatelja zajma) - (protuvrijednost WBTC ostaje u short poziciji) ×(tržišni tečaj ETH/WBTC)

Trgovac zarađuje 5,500.00 - 4,377.72 + 71.41 = 1,193.69 ETH.

↳ (kolateral ETH zajma u *Compoundu*) - (ETH za kupnju 112 WBTC) + ($\star$)

7.2 Teorijsko optimiziranje Pump Attacka

U nastavku ćemo detaljno opisati proceduru izvođenja problema optimizacije PA&A napada. Tablica 7.1 sažima oznake i stanje na lancu kada je napad izvršen (tj. stanje S_0). X i Y označavaju ETH odnosno WBTC. Radi jednostavnosti zanemarujemo naknade za trgovanje u CPAMM-u (tj. f = 0 za $\mathbb{M}$). Krajnje točke koje se izvode u pump attacku i arbitraži navedene su u redoslijedu izvršenja kako slijedi:

1. `Loan` ($dYdX$)
2. `CollateralizedBorrow` ($Compound$)
3. `MarginShort`(bZx) & `SwapXforY` ($Uniswap$)
4. `SwapYforX` ($Uniswap$)
5. `Repay` ($dYdX$)
6. `SellXforY` & `CollateralizedRepay`($Compound$).

Opis	Varijabla	Vrijednost
Maksimalan dostupan iznos ETH za brzi zajam	v_x	$10,000.00$
Faktor kolaterala	cf	0.75
Devizni tečaj osiguranog (kolateraliziranog) zaduživanja	er	36.48
Maksimalni iznos WBTC-a za posuđivanje	z_Y	155.70
Rezerva ETH na Uniswapu	$u_X(S_0)$	$2,817.77$
Rezerva WBTC na Uniswapu	$u_Y(S_0)$	77.08
Omjer prekoračenja kolaterala	ocr	1.153
Poluga	l	5.00
Maksimalni iznos ETH za financijsku polugu	w_X	$4,858.74$
Tržišna cijena WBTC-a	p_m	39.08

Tablica 7.1: Početno stanje lanca

U vektoru PA&A napada namjeravamo podesiti sljedeća dva parametra:
(i) p_1, iznos imovine X kolateraliziran za posuđivanje Y u krajnjoj točki 2 (usp. koraci 2 i 3 na Slici 7.1) i
(ii) p_2, iznos imovine X kolateraliziran za otvaranje short pozicije Y u krajnjoj točki 3 (usp. korak 4 na Slici 7.1).
Slijedeći postupak iz poglavlja 4 nastavljamo s detaljima konstrukcije sustava ograničenja. $u_X(S_4)$ je nelinearna s obzirom na p_1 i p_2. Napominjemo da postoji pet linearnih rubnih uvjeta i samo jedno nelinearno što implicira da se optimizacija može učinkovito riješiti.

Funkcija cilja	$\mathrm{u}_X(S_0) + \frac{p_2 \times l}{ocr} - u_X(S_4) - p_2 - \frac{p_1 \times cf \times p_m}{er}$
Rubni uvjeti	$\mathrm{p}_1 \geqslant 0, p_2 \geqslant 0$ $\mathrm{v}_X - p_0 - p_1 \geqslant 0$ $\mathrm{z}_Y - \frac{p_1 \times cf}{er} \geqslant 0$ $\mathrm{w}_Y + p_2 - \frac{p_2 \times l}{ocr} \geqslant 0$ $\mathrm{B}_0 + u_Y(S_0) + \frac{p_2 \times l}{ocr} - u_X(S_4) - p_1 - p_2 \geqslant 0$

Tablica 7.2: Funkcija cilja i rubni uvjeti

Pretpostavljamo da je početni saldo X u vlasništvu $\mathbb{A}$ iznosio B_0:

$$\mathcal{B}(\mathbb{A}; X; S_0) = B_0.$$

`1. Flash loan`: $\mathbb{A}$ dobiva brzi zajam u imovini X iznosa $p_1 + p_2$:

$$\mathcal{B}(\mathbb{A}; X; S_1) = B_0 + p_1 + p_2$$

$$uz\ uvjete \quad p_1 \geqslant 0, \quad p_2 \geqslant 0, \quad v_X - p_1 - p_2 \geqslant 0.$$

`2. CollateralizedBorrow`: $\mathbb{A}$ kolateralizira p_1 kako bi posudio Y od platforme za posuđivanje $\mathbb{L}$:

$$\mathcal{B}(\mathbb{A}; X; S_2) = \mathcal{B}(\mathbb{A}; X; S_1) - p_1 = B_0 + p_2$$

$$\mathcal{B}(\mathbb{A}; Y; S_2) = \frac{p_1 \times cf}{er}$$

$$uz\ uvjet \quad z_Y - \frac{p_1 \times cf}{er} \geqslant 0.$$

`3. MarginShort & SwapXforY`: $\mathbb{A}$ otvara kratku marginu s p_2 uz polugu l na platformi za trgovanje maržom $\mathbb{T}$; $\mathbb{T}$ zamjenjuje *(eng. swap)* X za Y na CPAMM $\mathbb{M}$:

$$\mathcal{B}(\mathbb{A}; X; S_3) = \mathcal{B}(\mathbb{A}; X; S_2) - p_2 = B_0$$

$$u_X(S_3) = u_X(S_0) + \frac{p_2 \times l}{ocr}$$

$$u_Y(S_3) = \frac{u_X(S_0) \times u_Y(S_0)}{u_X(S_3)}$$

$$\mathcal{L}(\mathbb{A}; Y; S_3) = u_Y(S_0) - u_Y(S_3)$$
$$uz\ uvjet \quad w_X + p_2 - \frac{p_2 \times l}{ocr} \geqslant 0.$$

4. `SwapYforX`: $\mathbb{A}$ prebacuje sav posuđeni Y na $\mathbb{M}$:

$$\mathcal{B}(\mathbb{A}; Y; S_4) = 0$$

$$u_Y(S_4) = u_Y(S_3) + \mathcal{B}(\mathbb{A}; Y; S_2)$$
$$u_X(S_4) = \frac{u_X(S_3) \times u_Y(S_3)}{u_Y(S_4)}$$
$$\mathcal{B}(\mathbb{A}; X; S_4) = B_0 + u_X(S_3) - u_X(S_4).$$

5. `Repay`: $\mathbb{A}$ otplaćuje brzi zajam:

$$\mathcal{B}(\mathbb{A}; X; S_5) = \mathcal{B}(\mathbb{A}; X; S_4) - p_1 - p_2$$

$$uz\ uvjet \quad \mathcal{B}(\mathbb{A}; X; S_4) - p_1 - p_2 \geqslant 0.$$

6. `SellXforY & CollateralizedRepay`: $\mathbb{A}$ kupuje Y s tržišta po tržišnoj cijeni p_m i preuzima kolateral od $\mathbb{L}$:

$$\mathcal{B}(\mathbb{A}; X; S_6) = \mathcal{B}(\mathbb{A}; X; S_5) + p_1 - \mathcal{B}(\mathbb{A}; X; S_2) \times p_m.$$

Funkcija cilja je trgovčev ETH prihod:

$$\begin{aligned}\mathcal{O}(S_0; p_1; p_2) &= \mathcal{B}(\mathbb{A}; X; S_6) - B_0 \\ &= u_X(S_0) + \frac{p_2 \times l}{ocr} - u_X(S_4) - p_2 - \frac{p_1 \times cf \times p_m}{er}.\end{aligned}$$

Poglavlje 8

Manipuliranje cjenovnim oracleom

8.1 Oracle problem

Decentralizirano financiranje (DeFi) pojam je koji se pojavio tijekom posljednjih nekoliko godina za opisivanje financijskih instrumenata koji se ne oslanjaju na centralizirane posrednike poput brokerskih kuća, burzi ili banaka. Kako bi implementirali te instrumente, DeFi protokoli koriste pametne ugovore smještene na blockchain sustavima. Ti su pametni ugovori programi koji implementiraju logiku klasičnih financijskih instrumenata.
Širok raspon aplikacija već je u produkciji, od štednih računa s kamatama, protokola za posuđivanje, do sintetičke imovine ili platformi za trgovanje. Ova industrija brzo dobiva na popularnosti u smislu broja korisnika i tržišne kapitalizacije. Jedna od popularnih DeFi primjena sastoji se u izdavanju određenog broja tokena korisniku u zamjenu za kolateral koji će biti zaključan u pametnom ugovoru sve dok korisnik ne vrati svoj dug. Očito, da bi proces bio pravedan potrebno je znati trenutni tečaj između izdanog tokena i tokena zaključanog kao kolateral. Ovdje na scenu stupa cjenovni oracle. Cjenovni oracle je sustav koji daje tečajeve ili cijene pametnim ugovorima DeFi protokola. Oni prikupljaju podatke iz izvora izvan lanca, kao što je API, i unose ih u pametni ugovor. Važnost oraclea temelji se na činjenici da pametni ugovori mogu pristupiti samo podacima koji se nalaze unutar njihove vlastite digitalne mreže pa su im oraclei potrebni kao komunikacijski instrumenti koji prevode događaje iz stvarnog svijeta (nedeterministički podaci) u digitalne vrijednosti kojima pametni ugovori znaju baratati (deterministički podaci). Podaci dobiveni putem oraclea postaju nepromjenjivi tek nakon što se evidentiraju u decentraliziranoj knjizi. To nas dovodi do pitanja: Tko provjerava autentičnost podataka dostavljenih lancu?
Sažeto, problem oraclea odnosi se na sukob između sigurnosti, autentičnosti i povjerenja u oracle treće strane za nepovjerljivo izvršavanje pametnih ugovora. Oracli zadržavaju

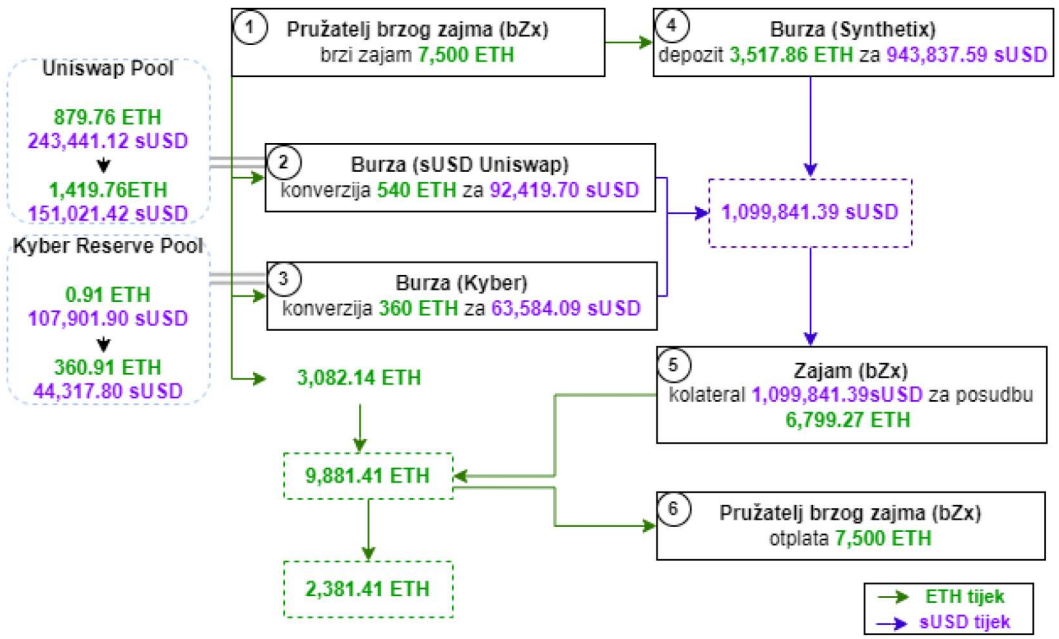
visok stupanj moći nad pametnim ugovorima u načinu na koji se izvršavaju jer podaci koje pružaju određuju kako se pametni ugovori izvršavaju. Stoga podaci iz izvora trećih strana imaju značajan utjecaj na izvršenje pametnog ugovora uklanjajući njegovu nepovjerljivu prirodu kao dijela decentralizirane mreže. Ova dilema između autentičnosti podataka iz oraclea i tradicionalnih pretpostavki o povjerenju u blockchain poznata je kao *Oracle problem*.

8.2 Analiza napada

Nastavljamo s detaljima drugog napada korištenjem brzog zajma koji donosi profit od 2,381.41 ETH (što je tada vrijedilo približno $634,900) unutar jedne transakcije (usp. vidi transakciju, 18. veljače 2020. po tečaju od 282.91 USD/ETH) uz naknadu za transakciju od $118.79.

8.2.1 Intuicija napada

Srž ovog napada je manipulacija cjenovnog oraclea korištenjem brzog zajma koji snižava cijenu sUSD/ETH. U drugom koraku trgovac ima korist od ove smanjene cijene sUSD/ETH posuđujući ETH uz sUSD kao kolateral.



Slika 8.1: *Napad manipulacijom oraclea*

Identificiramo ukupno 6 koraka unutar ove transakcije (usp. Slika 8.1).

1. `Loan`: U koraku 1 trgovac na *bZxu* posuđuje brzi zajam od 7,500 ETH.

2. `SwapXforY`, 3. `ConvertXtoY`, 4. `SellXforY`: U sljedeća tri koraka (2, 3, 4) trgovac pretvara ukupno 4,417.86 ETH u 1,099,841.39 sUSD (u prosjeku po tečaju 248.95 sUSD/ETH). Tečaj u koraku 2 i 3 iznosi 171.15 i 176.62 sUSD/ETH. Ova dva koraka smanjuju cijenu sUSD/ETH na 106.05 sUSD/ETH na *Uniswapu* i 108.44 sUSD/ETH na *Kyber Reserveu* koji se zajednički koriste kao cjenovni oraclei platforme za posuđivanje *bZx*. Imajte na umu da je *Uniswap* CPAMM, dok je *Kyber Reserve* AMM prema drugačijoj formuli. Tečaj na trećem tržištu *Synthetix* u koraku 4 još nije pod utjecajem prethodnih trgovina.

5. `CollateralizedBorrow`: Trgovac daje kolateral za sve kupljene sUSD (1,099,841.39) kako bi posudio 6,799.27 ETH (po $\frac{tečaj}{faktor\ kolaterala} = max(106.05, 108.44) \times 1.5 =$ 162.66 sUSD/ETH na *bZx*).

6. `Repay`: Trgovac posjeduje $6,799.27 + 3,082.14$ ETH i u posljednjem koraku otplaćuje brzi zajam u iznosu od 7,500.00 ETH i stoga ostvaruje prihod od 2,381.41 ETH dok plaća samo 0.42 ETH ($118.79) transakcijskih naknada.

8.2.2 Identificiranje i kvantificiranje žrtve

Zlonamjerni je trgovac iskrivio oracle cijene (*Uniswap* i *Kyber*) sa 268.30 sUSD/ETH na 108.44 sUSD/ETH, dok ostale DeFi platforme ostaju nepromijenjene na 268.30 sUSD/ETH. Slično PA&A napadu, zajmodavac *bZx* je žrtva koja gubi imovinu kao rezultat manipuliranog cjenovnog oraclea.
Zajmodavac *bZx* je izgubio 6,799.27 ETH - 1,099,841 sUSD što je približno na 2,699.97 ETH (po 268.30 sUSD/ETH).
Trgovac zarađuje 6,799.27 - 3,517.86 - 360 - 540 = 2,381.41 ETH.

↳ (ETH od posuđivanja, korak 5) - (ETH za kupnju sUSD, korak 4) - (ETH za kupnju sUSD, korak 3) - (ETH za kupnju sUSD, korak 2).

8.3 Teorijsko optimiziranje manipulacijskog napada na oracle

U napadu manipulacije oraclea X označava ETH, a Y označava sUSD. Zanemarujemo naknade za trgovanje u CPAMM (tj. f = 0 za $\mathbb{M}$). Varijable početnog stanja prikazane su tablicom 8.1. Navodimo krajnje točke uključene u vektor napada manipulacije oraclea u redoslijedu izvršenja kako slijedi:

1. `Loan` (*bZx*)
2. `SwapXforY` (*Uniswap*)
3. `ConvertXtoY` (*Kyber* reserve)
4. `SellXforY` (*Synthetix*)
5. `CollateralizedBorrow` (*bZx*)
6. `Repay` (*bZx*).

Opis	Varijabla	Vrijednost
Maksimalni dostupan iznos ETH za brzi zajam	$v_X(S_0)$	7500.00
Rezerva ETH na Uniswapu	$u_X(S_0)$	879.757
Rezerva WBTC na Uniswapu	$u_Y(S_0)$	243441.12
Stopa likvidnosti	lr	0.00252
Najmanja sUSD cijena na Kyber Reserveu	$minP$	0.0037
Najveća sUSD cijena na Kyber Reserveu	$maxP$	0.0148
Inventar ETH-a u Kyber Reserveu	$k_X(S_0)$	0.90658
Tržišna cijena sUSD	p_m	0.00372719
Najveći iznos sUSD dostupan za kupovinu	$maxY$	943837.59
Faktor kolaterala	cf	0.667
Maksimalni iznos ETH za posuđivanje	z_Y	11086.29

Tablica 8.1: Početno stanje lanca

$\mathcal{B}(\mathbb{A}; Y; S_4)$ i $P_Y(\mathbb{M}; S_2)$ su nelinearne s obzirom na p_1, p_2 i p_3. Od 7 rubnih uvjeta, 5 je linearnih i dva se nelinearna što znači da se optimizacija može učinkovito riješiti.

Funkcija cilja	$\mathcal{B}(\mathbb{A}; Y; S_4)\ \times cf \times \mathrm{P}_Y(\mathbb{M}; S_2)$ - $p_1 - p_2 - p_3$
Rubni uvjeti	$p_1 \geqslant 0, p_2 \geqslant 0, p_3 \geqslant 0$ $v_X - p_1 - p_2 - p_3 \geqslant 0$ $maxP - minP \times e^{lr \times (k_X(S_0) + p_2)} \geqslant 0$ $maxY - \frac{p_3}{p_m} \geqslant 0$ $z_Y - \mathcal{B}(\mathbb{A}; Y; S_4) \times cf \times P_Y(\mathbb{M}; S_2) \geqslant 0$

Tablica 8.2: Funkcija cilja i rubni uvjeti

Problem uvjetne optimizacije konstruiramo na sljedeći način:

1. `Loan`: $\mathbb{A}$ uzima brzi zajam od X iznosa $p_1 + p_2 + p_3$:

$$\mathcal{B}(\mathbb{A}; X; S_1) = p_1 + p_2 + p_3$$

$$uz\ uvjete \quad p_1 \geqslant 0, \quad p_2 \geqslant 0, \quad p_3 \geqslant 0, \quad v_X - p_1 - p_2 - p_3 \geqslant 0.$$

2. `SwapXforY`: $\mathbb{A}$ mijenja p_1 količinu od X za Y iz CPAMM $\mathbb{M}$:

$$\mathcal{B}(\mathbb{A}; X; S_2) = \mathcal{B}(\mathbb{A}; X; S_1) - p_1 = p_2 + p_3$$

$$u_X(S_2) = u_X(S_0) + p_1$$
$$u_Y(S_2) = \frac{u_X(S_0) \times u_Y(S_0)}{u_X(S_2)}$$
$$\mathcal{B}(\mathbb{A}; Y; S_2) = u_Y(S_0) - u_Y(S_2).$$

3. `ConvertXtoY`: $\mathbb{A}$ pretvara p_2 iznos od X u Y iz automatizirane rezerve cijena $\mathbb{Z}$:

$$\mathcal{B}(\mathbb{A}; X; S_3) = \mathcal{B}(\mathbb{A}; X; S_2) - p_2 = p_1$$

$$k_X(S_3) = k_X(S_0) + p_2$$
$$P_Y(\mathbb{Z}; S_3) = \min(P) \times e^{lr \times k_X(S_3)}$$
$$\mathcal{B}(\mathbb{A}; Y; S_3) = \mathcal{B}(\mathbb{A}; Y; S_2) + \frac{e^{-lr \times p_2} - 1}{lr \times P_Y(\mathbb{Z}; S_0)}$$

$$t.d. \quad maxP - P_Y(\mathbb{Z}; S_3) \geqslant 0.$$

4. `SellXforY`: $\mathbb{A}$ prodaje p_3 količinu X za Y po cijeni od p_m:

$$\mathcal{B}(\mathbb{A}; X; S_4) = \mathcal{B}(\mathbb{A}; X; S_3) - p_3 = 0$$

$$\mathcal{B}(\mathbb{A}; Y; S_4) = \mathcal{B}(\mathbb{A}; Y; S_3) + \frac{p_3}{p_m}$$

$$uz\ uvjet\ \ maxY - \frac{p_3}{p_m} \geqslant 0.$$

5. `CollateralizedBorrow`: $\mathbb{A}$ kolateralizira sav Y kako bi posudio X prema cijeni koju daje CPAMM $\mathbb{M}$ (po tečaju $e_r = \frac{1}{P_Y(\mathbb{M}; S_2)}$):

$$\mathcal{B}(\mathbb{A}; X; S_5) = 0$$

$$\mathcal{B}(\mathbb{A}; X; S_5) = \mathcal{B}(\mathbb{A}; Y; S_4) \times cf \times P_Y(\mathbb{M}; S_2)$$
$$uz\ uvjet \quad z_Y - \mathcal{B}(\mathbb{A}; Y; S_4) \times cf \times P_Y(\mathbb{M}; S_2) \geqslant 0.$$

6. `Repay`: $\mathbb{A}$ otplaćuje brzi zajam:

$$\mathcal{B}(\mathbb{A}; X; S_6) = \mathcal{B}(\mathbb{A}; X; S_5) - p_1 - p_2 - p_3$$

$$uz\ uvjet \quad \mathcal{B}(\mathbb{A}; X; S_5) - p_1 - p_2 - p_3 \geqslant 0.$$

Funkcija cilja je preostali saldo od X nakon otplate brzog zajma:

$$\begin{aligned}\mathcal{O}(S_0; p_1; p_2; p_3) &= \mathcal{B}(\mathbb{A}; X; S_6) = \mathcal{B}(\mathbb{A}; X; S_5) - p_1 - p_2 - p_3 \\ &= \mathcal{B}(\mathbb{A}; Y; S_4) \times cf \times P_Y(\mathbb{M}; S_2) - p_1 - p_2 - p_3.\end{aligned}$$

Literatura

[1] Aave, *Aave Protocol https://github.com/aave/aave-protocol*

[2] *Aavewatch - live protocol stats! https://aavewatch.now.sh/*

[3] M. Benšić, N. Šuvak, *Uvod u vjerojatnost i statistiku*, Odjel za matematiku Osijek, 2013.

[4] D. Brborović, *Upravljanje financijskom imovinom (nastavni materijali)*, Prirodoslovno-matematički fakultet, Matematički odsjek, Zagreb, 2015.

[5] bZx, - *a protocol for tokenized margin trading and lending https://bzx.network/*

[6] Compound, *https://compound.finance/*

[7] dYdX, *https://dydx.exchange/*

[8] S. Eskandari, S. Moosavi, J. Clark, *Sok: Transparent dishonesty: front-running attacks on blockchain*, International Conference on Financial Cryptography and Data Security, Springer, 2019.

[9] Ethereum.org, *Ethereum Virtual Machine (EVM)*

[10] Europska komisija, *Antitrust: Commission fines banks € 1.49 billion for participating in cartels in the interest rate derivatives industry*, Priopćenje za javnost, 4.12.2013.

[11] N. Gandal, N. Hamrick, T. Moore, T. Oberman, *Price manipulation in the Bitcoin ecosystem*, Journal of Monetary Economics 95(4), pp. 86–96, 2018.

[12] J. Hamrick, F. Rouhi, A. Mukherjee, A. Feder, N Gandal, T. Moore, M. Vasek , *The economics of cryptocurrency pump and dump schemes*, 2018.

[13] E. Hildenbrandt, M. Saxena, X. Zhu, N. Rodrigues, P. Daian, D. Guth, M. Rosu, *Kevm: A complete semantics of the ethereum virtual machine*, 2017.

[14] Home, — *prevent flash loan attacks*

[15] Investopedia, *Slippage definition & example*

[16] B. Jiang, Y. Liu, W. Chan, *Contractfuzzer: Fuzzing smart contracts for vulnerability detection*, Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, pp. 259–269., 2018.

[17] J. Kamps, B. Kleinberg, *To the moon: defining and detecting cryptocurrency pump-and-dumps*, 2018.

[18] D.J. Keenan, *My thwarted attempt to tell of Libor shenanigans*, Financial Times, 26.6.2012.

[19] A. Khalid, *Traders are selling themselves their own NFTs to drive up prices*, Engadget, 4.2.2022.

[20] Kyber, *Kyber*

[21] C. Liu, G. Liu, Z. Cao, Z. Chen, B. Chen, B. Roscoe, *Reguard: finding reentrancy bugs in smart contracts*, 018 IEEE/ACM 40th International Conference on Software Engineering: Companion (ICSE-Companion). pp. 65–68. IEEE, 2018.

[22] L. Luu, D.H. Chu, H. Olickel, P. Saxena, A. Hobor, *Making Smart Contracts Smarter*, Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 254–269, 2016.

[23] Maker, *MakerDao*

[24] MakerDao, *Intro to the Oasisdex protocol*

[25] S. Nakamoto, *Bitcoin: A peer-to-peer Electronic Cash System*, 2008.

[26] *Self Trade Prevention Functionality, ICE Futures Europe, 2020.*

[27] N. Szabo, *Smart Contracts*, 2006.

[28] N. Šuvak, *Matematičke financije (nastavni materijali)*, Odjel za matematiku, Osijek, 2021.

[29] Uniswap, *https://uniswap.org/*

[30] V. von Wachter, J.R. Jensen, J. Rude, F. Regner, O. Ross, *NFT Wash Trading: Quantifying suspicious behaviour in NFT markets* , 2022.

[31] G. Wood, *Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper*, 2014.

Sažetak

Kredit omogućuje zajmodavcu da pozajmi višak kapitala zajmoprimcu. U tradicionalnom gospodarstvu kredit nosi rizik da zajmoprimac ne može platiti svoj dug, stoga zajmodavac od zajmoprimca zahtijeva kolateral unaprijed. Zbog atomičnosti blockchain transakcija zajmodavci mogu ponuditi brze zajmove (eng. flash loans), tj. zajmove koji vrijede samo unutar jedne transakcije i moraju se otplatiti do kraja te transakcije. Ovaj koncept doveo je do brojnih zanimljivih mogućnosti napada. Ovaj rad istražuje implikacije atomičnosti transakcija i brzih zajmova za ekosustav decentraliziranih financija (DeFi). Kvantitativno pokazujemo kako atomičnost transakcije povećava prihod od arbitraže. Brzi zajmovi omogućuju svakome trenutni pristup ogromnom kapitalu. Pokazujemo kako to može imati negativne učinke te objašnjavamo dva napada na bZx omogućena brzim zajmovima koji donose ROI iznad 500,000%.

Ključne riječi

brzi zajam, blokchain, EVM, Ethereum, prijelazi stanja, arbitraža, oracle, bZx

Misisue of flash loans for attacking the DeFi ecosystem

Abstract

Credit allows a lender to loan excess capital to the borrower. In the traditional economy, credit carries the risk that the borrower cannot pay his debt, so the lender requires collateral from the borrower in advance. Due to the atomicity of blockchain transactions, lenders can offer flash loans, i.e. loans that are valid only within a single transaction and must be repaid by the end of that transaction. This concept has led to a number of interesting attack possibilities. This paper explores the implications of transaction atomicity and quick loans for the decentralized finance (DeFi) ecosystem. We quantitatively show how transaction atomicity increases arbitrage revenue. Flash loans give anyone instant access to huge amounts of capital. We show how this can have negative effects and explain two attacks on bZx made possible by flash loans that bring ROI above 500,000%.

Key words

flash loan, blockchain, EVM, Ethereum, state transitions, arbitrage, oracle, bZx

Životopis

Rođena sam 16. kolovoza 1995. u Slavonskom Brodu gdje sam pohađala osnovnu školu, a zatim Prirodoslovno-matematičku gimnaziju Matija Mesić. Tijekom školovanja bila sam uspješna na natjecanjima iz matematike, fizike, kemije, biologije, povijesti i geografije. Preddiplomski studij matematike na Odjelu za matematiku u Osijeku završavam 2019. s temom završnog rada "Tehnologija Bitcoina i kriptovaluta" pod mentorstvom izv.prof.dr.sc. Domagoja Matijevića. Iste godine upisujem diplomski studij na smjeru Financijska matematika i statistika na Odjelu za matematiku u Osijeku. Tijekom studiranja bila sam član udruga IAESTE kao nacionalni koordinator za financije te AIESEC od koga sam dobila nagradu za najveći razvoj poslovanja u skupini AIESEC Balkan. Trenutno sam zaposlena kao konzultant za poslovnu analitiku i poslovnu inteligenciju u tvtki Koios Savjetovanje d.o.o. gdje radim na FinTech projektima vezanim za tržište kapitala i surađujem s jednom od najvećih Fund Managment korporacija na svijetu. Aktivan sam član udruge *Alice in Blockchains* čiji je cilj promicanje znanja među ženama o temama kao što su kriptovalute, blockhchain, Web3 i financijska pismenost.