



Dipartimento di Impresa e Management

Cattedra di Matematica Finanziaria

ARBITRAGGI FINANZIARI NEL MONDO BLOCKCHAIN

Prof. Valeria D'Amato

RELATORE

Massimo Muscarà matr.271651

CANDIDATO

ANNO ACCADEMICO 2023-2024

SOMMARIO.....	2
INTRODUZIONE.....	3-4
CAPITOLO 1 “L’ARBITRAGGIO”	5-16
1.1 “L’arbitraggio come strumento finanziario”	5-6
1.2 “Strategie per l’arbitraggio”	7-13
1.3 “Il principio di non arbitraggio”	13-15
1.4 “Complessità e limiti”	15-16
CAPITOLO 2 “L’ARBITRAGGIO NEL MONDO BLOCKCHAIN”	17-29
2.1 “Il Mondo Blockchain”.....	17-19
2.2 “AMM – Automated Markets Maker”.....	19-21
2.3 “Attacco a Sandwich”.....	21-23
2.4 “Evidenze Empiriche nel caso di Arbitraggio a Sandwich”.....	24-29
CONCLUSIONI.....	29-30
BIBLIOGRAFIA E SITIOGRAFIA.....	31-32

INTRODUZIONE

La matematica finanziaria è una materia interdisciplinare che unisce principi matematici al mondo della finanza, esplorandone ed analizzandone temi legati agli investimenti, alla gestione del rischio, alla valutazione dei vari asset e all'ottimizzazione delle strategie. Questa disciplina studia e analizza principi che trovano applicazione in settori finanziari, come, ad esempio, settori bancari, settori assicurativi o società d'investimento. La matematica finanziaria offre supporto per prendere le migliori decisioni possibili, permettendo una comprensione più accurata possibile delle potenziali conseguenze di una scelta in ambito finanziario, il quale oggi diventa sempre più variegato e complesso.

In questa tesi si affronterà il tema dell'arbitraggio. L'arbitraggio è un'operazione che consente di ottenere un profitto certo azzerandone il rischio. Nel corso degli anni, il processo di arbitraggio si è evoluto e continuerà a farlo fin quando il mercato continuerà ad offrire nuovi orizzonti. Tuttavia, si possono collocare le prime operazioni codificate di strategia d'arbitraggio negli anni '70 negli Stati Uniti e, più precisamente, si possono attribuire all'azienda Salomon Brothers. L'attività di Salomon Brothers riguardava la sottoscrizione e la negoziazione di obbligazioni municipali, titoli di governo e obbligazioni societarie. L'azienda divenne pionieristica nel settore e ottenne la posizione di leader di mercato anche grazie al loro costante sviluppo di nuovi strumenti finanziari, tra cui nuove tecniche di arbitraggio.

La capacità di generare opportunità di profitto immediato per gli investitori e di individuare asimmetrie di mercato fecero sì che l'arbitraggio attirò a sé molti professionisti del settore, diventando un argomento di studio e ricerca sempre più approfondito e stimolante.

Come accennato in precedenza, l'arbitraggio stimolerà nuovi studi e ricerche soprattutto nel momento in cui il mercato offrirà nuovi orizzonti e, negli ultimi anni, il mondo finanziario è stato influenzato dall'avvento della tecnologia blockchain, introducendo nuove opportunità e metodologie di profitto. Anche in questo contesto l'arbitraggio ha trovato un suo ruolo, offrendo possibilità di guadagno sfruttando le discrepanze di prezzo tra i vari asset. Il mondo blockchain appare, tuttavia, anch'esso molto complesso; oltre alle differenze di prezzo, infatti, richiede di valutare e analizzare molteplici altre variabili finanziarie, informatiche e non solo.

Dunque, in questa tesi, non solo si offrirà una panoramica sull'arbitraggio nell'ambito finanziario più comune, ma ci si concentrerà anche sull'arbitraggio applicato nel mondo blockchain. Si analizzeranno le fondamenta teoriche di questa tecnologia, i suoi principi di funzionamento e le sfide che si dovranno affrontare qual ora ci si volesse far parte. In fine, attraverso questa ricerca, si vogliono offrire nuovi spunti di riflessioni sul tema dell'arbitraggio e sul tema della finanza decentralizzata che, ancora oggi, divide in più correnti di pensiero i professionisti del settore.

Volendo ricostruire una storia dell'arbitraggio, per individuarne un'evoluzione negli anni fino ai giorni d'oggi, si può risalire al XIX secolo. In quel periodo, infatti, gli operatori finanziari iniziarono ad utilizzare strumenti finanziari al fine di ottenere un profitto certo, senza assumersi rischi, sfruttando le discrepanze di prezzo tra i vari mercati e, questo, fu il primo concetto di arbitraggio definito come *arbitraggio classico*. Più avanti, nel XX secolo, vennero implementati modelli matematici e dati storici accostati ad una più moderna teoria finanziaria; da questo contesto emerse *l'arbitraggio statistico*, chiamato così perché basato su informazioni e dati. In questo contesto gli operatori iniziarono ad implementare le loro strategie con l'uso di modelli statistici per identificare inefficienze e discrepanze di asset; ad esempio, se si fosse previsto che il prezzo di uno stock sarebbe aumentato in visione dei suoi dati storici, un trader avrebbe potuto acquistare tale stock ed attendere prima di rivenderlo. Inoltre, sempre nel XX secolo, coincide anche la globalizzazione, grazie alla quale gli operatori iniziarono ad estendere le loro strategie per asset tra diverse borse mondiali e regioni del mondo. Infine, ai giorni odierni, l'avvento delle criptovalute, della tecnologia blockchain e della finanza decentralizzata hanno aperto a nuove opportunità di arbitraggio, *l'arbitraggio tramite blockchain*. Questo nuovo orizzonte permette di sfruttare anche le discrepanze di prezzo tra le monete virtuali su diverse piattaforme di scambio e tra diversi asset di scambio digitale.

CAPITOLO 1 - L'ARBITRAGGIO

1.1 L'ARBITRAGGIO COME STRUMENTO FINANZIARIO

Definizione 1 L'arbitraggio *consiste nell'esecuzione di due o più transazioni, di norma di elevato ammontare, contemporaneamente su due o più mercati al fine di conseguire un profitto privo di rischio.*¹

Come da definizione, si intuisce come l'arbitraggio sia una delle strategie finanziarie più veloci e sicure per creare un profitto senza assunzioni di rischio. Solitamente consiste nell'acquisto/vendita di un'attività finanziaria e in una contemporanea operazione di segno opposto su un mercato diverso dal precedente. Permette di sfruttare le imperfezioni dei mercati finanziari esistenti, combattendo il meccanismo di spontaneo allineamento dei prezzi che non permetterebbe il guadagno. Si può sinteticamente affermare che l'arbitraggio opera nei pochi istanti in cui i vari asset non sono in allineamento, così da sfruttarne le discrepanze e trarne profitto.

La strategia finanziaria che include l'arbitraggio è chiamata “*Opportunità di Arbitraggio*”. Volendo definire in maniera estesa “opportunità di arbitraggio”, si potrebbe includere in essa una qualsiasi strategia che, in almeno uno degli istanti di investimento, implichi un profitto positivo certo, pur ritrovandosi di fronte bilanci nulli nelle altre possibili date di intervento nel mercato.

Gli investitori che si dedicano all'arbitraggio sono chiamati *arbitraggisti* e si distinguono sia dagli *speculatori* e sia dagli *hedger*. Infatti, i primi prediligono l'investimento remunerativo sotto forma di capital gain, assumendosene i rischi del mercato e sperando che l'andamento del mercato sia in linea con le loro aspettative. I secondi tentano di costruire strategie di investimento minimizzando il rischio, scegliendo accuratamente il titolo a cui dedicarsi e il *timing* in cui investire. Gli arbitraggisti, invece, sono definiti come coloro che cercano aree di profitto nei disallineamenti dei prezzi sul mercato azzerando il rischio complessivo dell'operazione.

¹ “Glossario finanziario – arbitraggio”. <https://www.borsaitaliana.it/borsa/glossario/arbitraggio.html>

Nel contesto dell'analisi dell'arbitraggio finanziario è meglio stabilire un insieme di ipotesi che serviranno da fondamenta per i successivi approfondimenti. Con queste ipotesi si stabiliscono le condizioni per l'esamina ed efficacia delle strategie di arbitraggio.

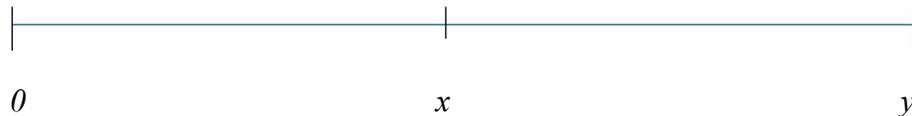
Ipotesi:

- Esistenza di opportunità d'arbitraggio; assunzione che i mercati finanziari presentino inefficienze sfruttabili dagli operatori al fine di arbitraggio. Tuttavia, illustreremo più avanti nella tesi anche il principio di non arbitraggio (par. 1.3).
- Assenza di costi di transazione; si presume che i costi di transazione per le operazioni di acquisto/vendita siano pari a zero.
- Liquidità abbondante; si suppone che i mercati presentino abbastanza liquidità da permettere agli operatori finanziari di eseguire le loro strategie senza trovare ostacoli nella compravendita degli asset e inoltre si assume che sia pari a zero il rischio di assenza di liquidità.
- Tassi di interesse risk-free; si assume sia possibile investire ad un tasso privo di rischio
- Massimizzazione del profitto; gli operatori di mercato, nella scelta tra due quantità monetarie, preferiscono sempre il profitto più alto.
- Tassazione pari a zero; non vi sono imposizioni fiscali.
- Esistenza di strumenti derivati; vi è la disponibilità di strumenti derivati che consentono agli operatori di implementare strategie di arbitraggio in maniera efficiente.
- Termini unitari; Si precisa che la maggior parte degli esempi si svolgeranno ragionando in termini unitari.

1.2 STRATEGIE PER L'ARBITAGGIO

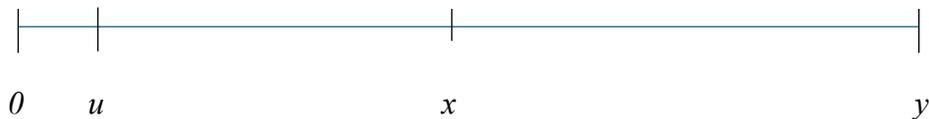
Per spiegare al meglio l'arbitraggio e le strategie connesse è importante stabilire inizialmente cosa siano il *prezzo a pronti* ed il *prezzo a termine*.

Prezzo a pronti:



Definizione 2 Il *prezzo a pronti* è quel prezzo definito come $v(x,y)$ e interpretato come il prezzo da dover pagare per comprare un titolo di valore unitario, se si tratta di un mercato secondario oppure come il prezzo incassato da chi emette il titolo. Dunque, rappresenta il prezzo che si paga per un'operazione che inizia all'epoca x e scade all'epoca y .²

Prezzo a termine:



Definizione 3 Il *prezzo a termine* è quel prezzo definito come $v(u,x,y)$ e interpretato come il prezzo del titolo fissato in u , che si paga in x per avere 1 euro all'epoca y .³

Queste due definizioni sono da fondamentali per due operazioni che si ritrovano nei mercati finanziari; una in cui il prezzo si forma e viene immediatamente pagato e l'altra in cui il prezzo si forma e viene pagato in un istante successivo. Le due operazioni sono rispettivamente:

- Operazioni *a pronti* il cui prezzo si indica con $v(x,y)$.

² Crenca, Fersini, Melisi, Olivieri, Pelle, (2018) "Elementi di matematica finanziaria"; editore: Pearson

³ Crenca, Fersini, Melisi, Olivieri, Pelle, (2018) "Elementi di matematica finanziaria"; editore: Pearson

- Operazioni *a termine* il cui prezzo si indica con $v(u,x,y)$.

Nella prima operazione la data di contrattazione coincide con la data di pagamento del prezzo stabilito. Invece, l'operazione *a termine* presenta:

- Il prezzo $v(u,x,y) > 0$ sempre.
- $v(u,y,y) = 1$.
- *Contratti forward*, ovvero contratti in cui il prezzo a termine viene fissato dagli operatori
- *Contratti futures*, ovvero contratti standardizzati e quindi scambiabili da un mercato (la Borsa) che offre sia contratti in acquisto sia in vendita fissando i prezzi in base alla domanda e all'offerta.

Dopo questa breve introduzione riguardante le *operazioni a termine* e le *operazioni a pronti*, si procede presentando due esempi pratici per illustrare come queste basi teoriche si applichino in situazioni di mercato reali. Oltre a ciò, gli esempi serviranno anche per capire come si muovono gli arbitraggisti in contesti di opportunità di profitto di derivanti da inefficienze nei prezzi dei titoli. Le disuguaglianze fondamentali, che spiegano in termini matematici il verificarsi di un'inefficienza di mercato, sono:

$$v(u,y) < v(u,x) \times v(u,x,y) \quad .1$$

e

$$v(u,y) > v(u,x) \times v(u,x,y) \quad .2$$

Nel primo caso ci si trova davanti ad una situazione in cui il prezzo attuale di un titolo con scadenza y è inferiore al prodotto di un prezzo a scadenza x per un prezzo a termine che copre l'intervallo da x a y (qui si indica una sottostima del titolo con scadenza a y che l'arbitraggista può sfruttare facendo acquisto di tale titolo).

Nel secondo caso, invece, si indica che il prezzo attuale del titolo a scadenza y è maggiore del prodotto del prezzo a scadenza x per il prezzo a termine che copre l'intervallo da x a y (qui si indica una sovrastima del titolo con scadenza a y che l'arbitraggista può sfruttare facendo vendita di tale titolo).

Inoltre, ai fini dell'esempio, è utile introdurre anche la formula teorica che descrive come il valore del denaro è influenzato dal passare del tempo:

Utilizzando il tasso precedente $\delta(0,3)$, e sapendo che $v(t) = e^{-\delta \times t}$ (formula .3, par. 1.2), si può ricavare il prezzo per acquistare un titolo che permette di ottenere 1 euro dopo 3 mesi. Quindi:

$$v(t) = e^{-\delta \times t} = e^{-0,04 \times 3/12} = 0,990 = v(0,3)$$

Adesso, premettendo che vi sia possibilità di scegliere se essere acquirente o venditore, si procede a confrontare $v(0,12)$ con $v(0,3) \times v(0,3,12)$ per scoprire se vi è un'opportunità di guadagno. Sapendo che:

$$v(0,12) = 0,804$$

$$v(0,3) = 0,990$$

$$v(0,3,12) = 0,929$$

E facendo il confronto di $v(0,12)$ con $v(0,3) \times v(0,3,12)$, si ottiene:

$$0,804 < 0,990 \times 0,929$$

$$0,804 < 0,919$$

Conclusioni: per un operatore di mercato è conveniente comprare l'operazione a pronti al prezzo di $v(0,12)$ e vendere le due operazioni (emettendo due titoli, uno a pronti e uno a termine), incassando così la somma di $v(0,3) \times v(0,3,12)$ e ottenere profitto.

Il procedimento è spiegato graficamente con tabella di seguito:

	0	3 mesi	12 mesi
Acquisto titolo a pronti	-0,804		+1
Emissione titolo a termine		+0,929	-1
Emissione titolo a pronti	+0,990	-0,929	
Tot. profitto	+0,186	0	0

Si può concludere affermando che: il profitto certo, immediato e senza rischi, è rappresentato dal valore unitario di +0,186 all'epoca zero.

Volendo rappresentare la tabella con i prezzi non unitari dell'esempio, si ottiene:

(Prezzo non unitario del titolo a pronti che dà diritto a 52.000 euro tra 3 mesi:
 $52.000 \times 0,990 = 51.482,59$)

	0	3 mesi	12 mesi
Acquisto titolo a pronti	-45.000		+56.000
Emissione titolo a termine		+52.000	-56.000
Emissione titolo a pronti	+51.482,59	-52.000	
Tot. profitto	+6.482,59	0	0

Il guadagno senza rischi è di 6.482,59 euro.

Con il precedente esempio è stato illustrato come sia conveniente per un operatore acquistare un titolo a pronti ed emettere un titolo a termine ed uno a pronti. Il caso precedente è caratterizzato dall'informazione $v(u,y) < v(u,x) \times v(u,x,y)$. Adesso, sinteticamente, si analizzerà cosa accadrebbe nel caso in cui: $v(u,y) > v(u,x) \times v(u,x,y)$.

Il successivo esempio sarà strutturato con prezzi in termini unitari di un BOT.

Esempio 2: Si supponga sia disponibile un BOT con scadenza a 135 giorni e che è stato quotato 0,99647 all'epoca 0. Rappresentando graficamente ciò appena detto, si avrà:



Si consideri ora un altro titolo con data di scadenza a 302 giorni dall'epoca 0 che viene quotato 0,98738 (in epoca 0). Questo titolo, quindi, dà diritto a 1 a distanza di 302 giorni.

Rappresentazione:



Dunque, il prezzo delle due operazioni sarà:

$$v(0,135) = 0,99647$$

$$v(0,302) = 0,98738$$

Si immagini che, in un certo istante, i prezzi siano:

$$v(0,135) = 0,997$$

$$v(0,302) = 0,990$$

Inoltre, sempre nello stesso istante, si supponga si sia creato un prezzo a termine pari a:

$$v(0,135,302) = 0,989$$

Da questi dati, dunque, si confermerebbe il caso di $v(u,y) > v(u,x) \times v(u,x,y)$. Verificando:

$$v(0,302) > v(0,135,302) \times v(0,135)$$

$$0,990 > 0,989 \times 0,99738$$

$$0,990 > 0,986$$

Da questa situazione è possibile applicare una strategia di arbitraggio nella quale si emette un titolo a pronti e si acquistano un titolo a pronti ed uno a termine; il procedimento è spiegato anche con la seguente tabella:

	0	135 giorni	302 giorni
Emissione titolo a pronti	+0,990		-1
Acquisto titolo a termine		-0,989	+1
Acquisto titolo a pronti	-0,98641	+0,989	
Tot. profitto	+0,00359	0	0

In conclusione, si può dire che il profitto certo e senza assunzioni di rischio è rappresentato da +0,00359 all'epoca 0.

Come visto nell'esempio 2, ai fini dell'arbitraggio è necessario che il prezzo delle due operazioni cambi in un determinato istante e che si crei un nuovo prezzo a termine

È essenziale una simile situazione sul mercato poiché gli arbitraggisti sperano che, almeno in un istante della giornata, vi siano differenze di prezzo; altrimenti, senza quest'ultime, non potrebbero trarre nessun guadagno. Le discrepanze di prezzo nel corso della giornata, anche se per pochi istanti, sono vitali per permettere l'arbitraggio e l'operatore deve sfruttarle prima del loro riallineamento. Infatti, se non si verificassero mai tali disallineamenti, si avrebbe sempre la situazione $v(u,y) = v(u,x,y) \times v(u,x)$ e non ci sarebbe, in nessun momento, occasione di arbitraggio e si verificherebbe, in ogni istante, il principio di non arbitraggio.

1.3 IL PRINCIPIO DI NON ARBITRAGGIO

Un mercato, per essere definito come *mercato perfetto*, deve presentare queste caratteristiche:

- Mercato *non frizionale*: assenza di costi di transizione e di gravami fiscali; infinita divisibilità dei titoli; sono consentite le vendite allo scoperto.
- Mercato *competitivo*: gli agenti seguono il principio della "non sazietà", cioè massimizzano sempre il profitto.
- Assenza del *rischio di insolvenza*: si ipotizza che, in un mercato perfetto, tutti gli importi sono esigibili con certezza nelle date stabilite.
- *Principio di non arbitraggio*: i prezzi dei contratti finanziari scambiati nel mercato rispettano il *principio di assenza di arbitraggi privi di rischio* ed è esclusa la possibilità di realizzare profitto senza rischio.

Poiché in questa tesi si tratta l'argomento dell'arbitraggio, si farà un focus solo sull'ultimo punto di queste caratteristiche di un mercato perfetto, ovvero sul *principio di non arbitraggio*. È importante comprendere come questo principio sia una delle fondamenta delle dinamiche di un mercato. Infatti, dal *principio di non arbitraggio* nei mercati *perfetti*, deriva la *legge del prezzo unico*.

La *Legge del prezzo unico* afferma che due titoli o, più generalmente, due contratti che producono lo stesso pay-off in ogni situazione possibile, devono avere lo stesso prezzo.

Per comprendere meglio la differenza tra un *mercato perfetto* e un *mercato imperfetto* ai fini di una strategia di arbitraggio, verrà illustrato di seguito un esempio avente oggetto uno ZBC sia in un mercato che nell'altro:

Esempio 3: E' indicato con $v(u,x,y)$ il prezzo a termine, o prezzo *forward*, dello ZBC unitario che pagherà 1 euro in data y . Il *teorema dei prezzi impliciti* afferma che il prezzo a termine di un asset finanziario dovrebbe essere coerente con i prezzi a pronti corrispondenti a scadenze future; quindi, per il teorema dei prezzi impliciti, il prezzo dello ZBC a termine è coerente con i prezzi a pronti con stesse scadenze future.

Il teorema si può esprimere con la formula:

$$v(u,x,y) = v(u,y) \quad .4$$

e dunque si assume che non vi sia occasione d'arbitraggio e non vi siano modalità per guadagnare senza rischio.

Tuttavia, se si verificasse una situazione di arbitraggio vorrebbe dire che il prezzo a termine $v(u,x,y)$ sarà maggiore o inferiore del prezzo a pronti futuro $v(u,y)$ (riferimento a formule .1 e .2 par. 1.2).

In tale situazione, un operatore finanziario potrebbe vendere il titolo a termine ad un prezzo più alto per poi acquistare il titolo a pronti ad un prezzo più basso. Così da guadagnare la differenza tra i due prezzi poiché la condizione $v(u,x,y) = v(u,y)$ non sarà più soddisfatta.

Domanda: perché il mercato non presenta sempre le caratteristiche di un *mercato perfetto*?

Risposta: perché il mercato *perfetto*, di cui sono state descritte le caratteristiche all'incipit del par. 1.3, è solo un mercato teorico. Infatti, nel mercato reale, esistono molte variabili che lo rendono *imperfetto* e che permettono quindi l'arbitraggio; tra queste variabili si possono evidenziare:

- *Informazioni asimmetriche e/o incomplete*; se non vi sono continui scambi di informazioni tra diversi mercati o asset, sarà più facile creare situazioni di arbitraggio.
- *Assenza di costi di transazione*; l'assenza o il poco prezzo dei costi di transazione possono permettere l'esistenza di ampi i margini di guadagno al verificarsi di una situazione di arbitraggio.
- *Assenza di normative*; più un mercato è opensource e più gli arbitraggisti possono utilizzare strumenti e fonti per fare guadagno.
- *Mancata risposta immediata ai disallineamenti*; gli arbitraggisti sfruttano proprio questo momento per trarre guadagno; quindi, più è ampio il lasso di tempo per l'equilibrio tra gli asset e più vi sono occasioni d'arbitraggio.
- *Concetto di finanza comportamentale*; ovvero che le inefficienze del mercato possono essere causate dall'eccessiva fiducia, dai pregiudizi cognitivi e, più in generale, dalla mentalità e ottimismo degli operatori.
- *Concorrenza tra investitori*; se ci sono un gran numero di investitori che analizzano il mercato vi è rischio di sovraperformare il mercato. Invece, se vi sono meno investitori, potrebbero esserci maggiori opportunità d'arbitraggio.

1.4 LIMITI E COMPLESSITA' DELL'ARBITRAGGIO

Nei paragrafi precedenti è stato mostrato l'arbitraggio come una strategia finanziaria che promette guadagni sicuri ed immediati. Tuttavia, se l'arbitraggio fosse come appena descritto sarebbe utilizzato dalla maggior parte degli operatori, i quali si arricchirebbero in pochissimo tempo e senza assumersi il minimo rischio. Purtroppo, o per fortuna, una strategia di arbitraggio non è così semplice come sembra.

I limiti e la complessità dell'arbitraggio derivano da alcuni vincoli da affrontare che ne limitano la capacità, diminuendo lo sfruttamento appieno delle inefficienze presentate dal mercato. Questi vincoli possono essere strutturali, come costi di transazione e liquidità, o comportamentali, come la percezione del rischio. Ciò significa che anche in presenza di

un'opportunità di arbitraggio, quest'ultima potrebbe non essere sfruttata dagli operatori di mercato per trarne profitto.

Entrando più nel dettaglio del concetto di limiti dell'arbitraggio, si forniscono di seguito alcuni punti chiave:

- Ruolo dei *costi di transizione*: i costi di transizione includono le commissioni all'acquisto e alla vendita dei titoli nei vari asset. Queste spese possono rappresentare una cifra che offusca i profitti dell'arbitraggio. Ad esempio, se un operatore individuasse una strategia di arbitraggio tra due titoli e facesse una doppia operazione tra acquisto e vendita, i costi di transizione si applicherebbero ad entrambe le operazioni e questi costi potrebbero ridurre, o nel peggiore dei casi annullare, il profitto derivante dalla strategia in atto.
- *L'impatto della liquidità*: la liquidità è la facilità con cui una posizione può essere acquistata o venduta senza alterarne il prezzo. Gli arbitraggisti possono trovare difficile entrare ed uscire rapidamente nei mercati con bassa liquidità, nei quali potrebbero anche cambiare le circostanze di mercato, perdendo di conseguenza l'opportunità di guadagno. Ad esempio, se un operatore individua un titolo sottovalutato, ma ci sono pochi acquirenti sul mercato e quindi poca liquidità, potrebbe riscontrare difficoltà nel vendere per trarne un profitto certo.
- *L'influenza comportamentale degli operatori*: la mentalità, i pregiudizi e le intuizioni possono impedire agli arbitraggisti di sfruttare pienamente tutte le inefficienze del mercato. Se ad esempio uno stock è sempre andato male, un operatore potrebbe vedere un'opportunità di arbitraggio ma allo stesso tempo potrebbe essere frenato dalla paura che il titolo crolli ulteriormente. Questi comportamenti con indole precauzionale possono prolungare le inefficienze presenti sul mercato, rendendole più durature.

CAPITOLO 2 - L'ARBITRAGGIO NEL MONDO BLOCKCHAIN

2.1 IL MONDO BLOCKCHAIN

Cosa è la tecnologia blockchain?

Definizione 4 La *Blockchain* (letteralmente "*catena di blocchi*") sfrutta le caratteristiche di una *rete informatica di nodi* e consente di gestire e aggiornare, in modo univoco e sicuro, un *registro contenente dati e informazioni* in maniera aperta, condivisa e distribuita senza la necessità di un'entità centrale di controllo e verifica.⁴

Oggi, è un momento storico in cui quest'innovazione sta attirando a sé moltissime attenzioni. Questa tecnologia blockchain può essere sfruttata in vari modi; può essere introdotta per disintermediare interazioni di varia natura, potenzialmente facendo a meno di banche, notai, ecc., oppure per creare processi sicuri per l'introduzione di nuovi modelli di interazione.

La blockchain fa parte della più ampia famiglia della tecnologia *Distributed Ledger*, ovvero sistemi basati su un registro distribuito, che si può leggere e modificare da più nodi di una rete.

Volendo descrivere brevemente la storia della blockchain fino ad oggi:

- 2009: nascita della blockchain con l'invenzione di Bitcoin. Tutto nasce come risposta alla crisi finanziaria del 2008, la quale era caratterizzata da un sistema finanziario opaco e controllato da pochi attori.
- 2016: hype mediatico con conseguente esplosione dei progetti blockchain; tuttavia, esaurito l'hype, si avrà una *bard season* (momento in cui il prezzo delle crypto decresce molto) nello stesso anno.
- 2020: iniziative da parte di banche centrali e governi. Si accelerano le sperimentazioni per emettere delle Central Banks Digital Currencies e la

⁴ Osservatori.net, (2023). "La Blockchain spiegata in maniera semplice: cos'è e applicazioni". https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni

commissione EU lavora nel Finance Digital Package per un regolamento dei crypto asset.

- 2021: cresce il mondo della finanza decentralizzata (DeFi); in contemporanea, i crypto asset guadagnano rilevanza.
- 2022: progressiva crescita delle applicazioni costruite su piattaforme pubbliche

Questi step, appena illustrati, servono a comprendere la continua evoluzione di questa tecnologia. Spostando l'attenzione sulla sua struttura, il mondo blockchain è formato da più piattaforme, ed ognuna di esse ha le sue particolarità, vantaggi e svantaggi. Tuttavia, è possibile identificare delle caratteristiche comuni; la prima fra tutte è, ovviamente, la digitalizzazione e la trasformazione dei dati in formato digitale. Di seguito, le altre che meritano attenzione:

- *Decentralizzazione*: al fine di garantire la sicurezza informatica e la resilienza dei sistemi, le informazioni vengono registrate e distribuite tra più nodi.
- *Disintermediazione*: l'assenza di intermediari per gestire le transazioni, di fatto, elimina la necessità di affidarsi ad un terzo soggetto.
- *Trasparenza e verificabilità*: il registro è trasparente, accessibile e può essere consultato e verificato da tutti.
- *Programmabilità dei trasferimenti*: le azioni possono essere programmate in vari modi (ad esempio, eseguire certe azioni solo al verificarsi di certi eventi).
- *Immutabilità del registro*: i dati non possono essere modificati senza un consenso della rete.

Queste caratteristiche dimostrano la sicurezza e l'affidabilità che offrono le varie piattaforme basate sulla tecnologia blockchain ai vari utenti e investitori.

La possibilità di creare piattaforme decentralizzate è offerta da *Web3*, una nuova forma di Web che permette agli sviluppatori di creare soluzioni personalizzate ed innovative. Infatti, è proprio grazie a Web3 che è possibile la creazione di componenti della tecnologia blockchain come i *token*, gli *smart contract* e i *wallet*.

L'applicazione, offerta da Web3 e blockchain, più funzionale allo scopo di questa tesi è quella dell'*Internet of Value*, ovvero lo scambio di valore sulle varie piattaforme. In questo

ambito si trovano sia le criptovalute sia le *stablecoin*, queste ultime, oggi non ancora sul mercato, sono monete digitali che offrono stabilità e sono proposte dalle banche centrali.

Definizione 5 Quando ci si riferisce all'*Internet of Value*, si fa riferimento ad applicazioni incentrate sullo *scambio del valore*, che spesso si concretizza attraverso *criptovalute*, *stablecoin* e *valute virtuali* supportate dalle banche centrali, note come CBDC. Queste applicazioni introducono un nuovo paradigma nell'amministrazione degli scambi di beni di valore, eliminando la necessità di intermediari.⁵

Dopo aver affrontato il tema dell'*Internet of Value* e della tecnologia blockchain, è necessario e importante dare rilevanza anche agli *Automated Market Makers* (AMM). Gli AMM, infatti, sono alcuni dei sistemi chiave che funzionano grazie ai principi di tali tecnologie, facilitando gli scambi di criptovalute e altre forme di valore digitale senza la necessità di intermediari tradizionali.

2.2 AMM - AUTOMATED MARKET MAKERS

Definizione 6 Gli *Automated Market Makers* (AMM) sono i protocolli sottostanti che alimentano uno scambio decentralizzato. Consentono di scambiare asset utilizzando pool di liquidità crypto come controparti. Gli AMM utilizzano algoritmi per abbinare acquirenti e venditori in modo sicuro ed evitare situazioni rischiose o controproducenti.

(D. Xu; 2022)

Entrando nello specifico, gli AMM usano formule criptate, aritmetiche ed economiche conosciute anche come smart contract, per consentire lo scambio di coppie di token, di cui ne è un esempio la coppia Bitcoin-USDollar. Una componente essenziale di questo sistema è la *memory pool* (o, abbreviando, *mempool*), la quale può essere immaginata

⁵ Osservatori.net, (2023). "La Blockchain spiegata in maniera semplice: cos'è e applicazioni". https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni

come una sala di attesa per le transazioni prima che vengano confermate in blockchain. Sono proprio in questi istanti di attesa che vi è il rischio di dar luogo a pratiche speculative come il *front-running* o il *back-running*. Più in particolare:

Il *front-running* si verifica quando un malintenzionato decide di inserire una transazione anticipando le altre, pagando una *fee* più alta e ottenendo la priorità di conferma dell'ordine (infatti, le transazioni con commissioni e *fee* più alte hanno la priorità sulle altre). Questa speculazione può ovviamente influenzare il prezzo di un asset, poiché permettere al malintenzionato di acquistare o vendere un asset ad un prezzo vantaggioso che sarà diverso da quello della transazione originale.

Il *back-running* differisce dal front-running poiché la transazione viene inserita subito dopo la transazione originale, la quale ci si aspetta che influenzerà positivamente il prezzo di un asset per sfruttarne, in questo modo, l'aumento di valore.

Queste due pratiche, rischiose e speculative, trovano applicazione nell'ambito degli *attacchi a Sandwich* sui Dex, dove anche gli AMM ricoprono un ruolo di cruciale importanza.

Prima di approfondire il tema dell'*attacco sandwich*, bisogna spiegare, anche sinteticamente, una caratteristica fondamentale dei meccanismi di pricing negli AMM, ovvero la cosiddetta regola del *Constant Product Market Maker* (CPMM); cioè, quella regola che permette al mercato di rimanere liquido e funzionante nonostante le fluttuazioni dei pool dovute a domanda ed offerta per ciascun asset. In particolare, un market maker di prodotto costante (CPMM), soddisfa l'equazione:

$$(R_\alpha - \Delta\alpha) * (R_\beta + \gamma\Delta\beta) = K \quad .5$$

Dove R_α e R_β sono le riserve di ciascun asset e γ è la commissione di transazione. Negoziare qualsiasi importo di una delle due attività deve modificare le riserve in modo tale che, quando la commissione è pari a zero, il prodotto $R_\alpha \times R_\beta$ rimane uguale alla costante K . Questo è spesso semplificato nella forma $x * y = K$, dove x e y sono le riserve di ciascuna attività. Senza questa regola, il pool potrebbe diventare altamente instabile;

infatti, il mantenimento del prodotto costante, è un principio fondamentale per garantire il corretto ed efficiente funzionamento dei sistemi AMM, allontanando la possibilità che si presentino eccessive manipolazioni degli asset.

2.3 ATTACCO A SANDWICH

L'attacco a Sandwich, noto anche come *attacco di inserimento*, è una forma avanzata e specifica di arbitraggio nel contesto degli AMM nell'ambito degli scambi decentralizzati. Tradizionalmente, l'arbitraggio, come già precedentemente spiegato, è visto come un contributo all'efficienza del mercato poiché individua e aiuta i mercati a raggiungere l'uniformità dei prezzi nei vari asset. Al contrario, l'attacco sandwich è visto come una strategia di manipolazione del mercato e delle transazioni in essere, con lo scopo di ottenere profitto dalla variazione dei prezzi manipolati. Si può intuire come l'attacco a sandwich sfrutti una dinamica simile al tradizionale arbitraggio, ma con etica e intenti totalmente diversi. Questa strategia di manipolazione si avvale della visibilità, come anticipato nel par. 2.1, delle transazioni nella mempool prima che esse vengano definitivamente confermate; è proprio in quest'intervallo di tempo, tra l'invio della transazione e la sua conferma, che l'aggressore avvia la sua speculativa strategia d'attacco, posizionando un ordine prima e uno dopo rispetto alla transazione originale dell'altro utente ignaro.

Volendo descrivere un ipotetico scenario di un tipico attacco a sandwich, si può immaginare un pool di liquidità che contenga 1000 token A e 100 ETH, con un valore di prodotto costante (CPMM, formula .5, par. 2.2) di 100.000, stabilendo, inoltre, che il prezzo di A sia 0.1 ETH. In questa ipotesi si assuma poi che ci siano due protagonisti: Tizio e Caio; il primo è l'aggressore che ha ottenuto informazioni dalla mempool sulla transazione originale, il secondo è l'utente ignaro dell'attacco e autore della transazione originale.

Il processo che permette a Tizio di compiere un attacco di inserimento inizia con una transazione da parte di Caio che viene iscritta sulla mempool in attesa di conferma. A questo punto Tizio agisce con *front-running*, investendo 5 ETH per acquistare i token A prima di Caio. La formula del prodotto costante (CPMM, formula .5, par. 2.2) dell'AMM necessita che:

$$(1000 - X) * (100 + 5) = 100000$$

Dunque, risolvendo l'equazione, si trova che:

$$X = 47,62$$

Si può affermare che Tizio acquista 42,62 token A per 5 ETH. La manipolazione del mercato inizia da questa transazione; poiché, con l'acquisto di Tizio, viene influenzato il prezzo per le transazioni successive, compresa quella di Caio.

Successivamente Caio, ignaro delle azioni di Tizio, riceve conferma per il suo acquisto. Questo, però, avviene con uno stato del pool di liquidità diverso da quando Caio inviò il suo ordine; infatti, il nuovo pool di liquidità, sarà di 952,38 token A e 105 ETH.

Ipotizzando che Caio abbia speso 10 ETH, con il nuovo stato del pool di liquidità e risolvendo sempre l'equazione della regola del prodotto costante, si nota che:

$$(952,38 - X) * (105 + 10) = 100000$$

$$X = 82,81$$

Caio acquista 82,81 token A al prezzo di 10 ETH; il prezzo d'acquisto si può notare come sia più alto e questo, proprio a causa dell'azione precedente di Tizio, farà acquistare a Caio meno token del previsto.

Dopo la transazione di Caio, il pool di liquidità è stato nuovamente modificato, in questo momento è di 869,57 token A e 115 ETH.

A questo punto Tizio effettua immediatamente un'azione di *back-running* e vende subito i suoi 47,62 token A precedentemente acquistati e riesce ad ottenere:

$$(869,57 + 47,62) * (115 - Y) = 100000$$

$$Y = 5,97$$

Tizio ottiene 5,97 ETH dalla vendita dei suoi token A.

Mettendo a confronto la prima transazione di Tizio con l'ultima, si può notare come:

$$5 \text{ ETH} < 5,97 \text{ ETH}$$

Dunque, Tizio realizza un profitto di 0,97 ETH proveniente dalla differenza tra l'operazione d'acquisto (con *front-running*) e vendita (con *back-running*).

Questo scenario immaginario ha dato la possibilità di notare come l'accesso a informazioni riguardanti transazioni nella mempool possa permettere a malintenzionati di manipolare il prezzo di un asset per trarne guadagno a discapito di altri utenti. Questa specifica forma di arbitraggio, *l'attacco a sandwich*, sfrutta le strutture e le regole del CPMM e degli AMM, le quali hanno però un fine legittimo di adattare gli asset ad ogni variazione delle proporzioni di riserva nei pool di liquidità.

L'attacco a sandwich, chiamato così poiché "mette in mezzo" un ignaro utente tra due transazioni manipolatrici, sfrutta l'equità e la trasparenza dei mercati decentralizzati, i quali ne fanno in realtà punto di forza e vanto, per ottenere un certo profitto.

Nonostante la possibilità di elevato guadagno, l'attacco a sandwich non è sempre redditizio. Infatti, chi esegue questo tipo di attacco deve possedere le capacità e le competenze avanzate per individuare i migliori AMM da attaccare, per selezionare le coppie di token corrette, per individuare i migliori istanti per dare luogo all'attacco. Ad esempio, se viene eseguito un attacco di inserimento quando i prezzi delle *fee* ("*fee*", si rimanda a par. 2.2) sono particolarmente alti, vi è il rischio, sommando anche altri costi di commissione, di andare in perdita o di avere un guadagno pressoché nullo.

Inoltre, per concludere, è doveroso evidenziare come, con il tempo, gli AMM hanno preso certamente delle contromisure per prevenire questi tipi di attacco. 1Inch, volendo citare un Dex, ad esempio, ha introdotto la funzione dei cosiddetti "*Flash bots*"; ovvero una funzione che impedisce la registrazione delle transazioni sulla mempool fino al completamento dell'ordine. In questo modo, per un ipotetico utente malevolo o bot, è impossibile individuare transazioni su cui effettuare l'attacco.

2.4 EVIDENZE EMPIRICHE NEL CASO DI ARBITRAGGIO A SANDWICH

Nel paragrafo precedente si è illustrato un semplice esempio di attacco a sandwich che si potrebbe verificare in un determinato Dex. Lo scenario presentava alcuni elementi indispensabili, come le varie transazioni e i due protagonisti (Tizio e Caio, rispettivamente l'aggressore e la vittima); tuttavia, per semplificazione e al fine di una più facilitata comprensione, venivano omesse altre variabili che avrebbero potuto incidere sul profitto finale derivante dall'attacco.

In un processo d'acquisto o vendita di criptovalute su un Dex, vi sono infatti molteplici variabili che possono incidere sulla conversione euro in criptovaluta e quindi sul guadagno effettivo. Tra queste si trovano le commissioni da pagare per ogni azione compiuta e, spesso, dipendenti soprattutto dalle politiche del Dex su cui si sta effettuando la transazione e dalla quantità d'acquisto. Tornando al caso di un attacco a sandwich, è fondamentale includere le commissioni nel calcolo del profitto, poiché potranno avere un'incidenza significativa sul risultato finale.

Successivamente, oltre le commissioni, è di primaria importanza il fattore tempo. Basti pensare che: se in un determinato istante con 1 euro si può acquistare 1 crypto, già dopo pochi secondi la situazione non sarà più la stessa. Questo è dovuto al fatto che le quotazioni sono in continuo aggiornamento e il rapporto euro – criptovaluta cambia di secondo in secondo. Tuttavia, il tempo non è pericoloso solo per un cambio di quotazione, ma anche per la possibilità che si inserisca una nuova transazione che modifichi il pool di liquidità su cui si sta eseguendo l'attacco; in quest'ultimo caso il guadagno potrebbe essere minimizzato (o trasformato in perdita) solo per colpa di una transazione effettuata da una terza persona che si inserisce, anche involontariamente, nel processo.

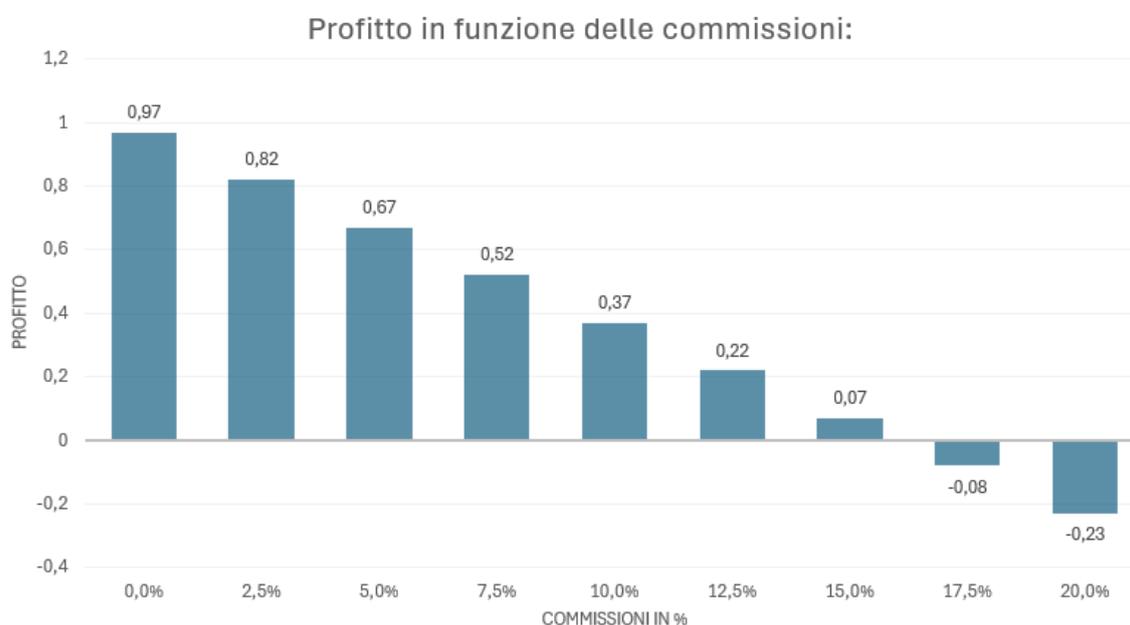
Se si riesce a comprendere il “potere” che queste variabili hanno su una singola transazione; si riuscirà senza dubbio a comprendere il potenziale di queste variabili nell'influenzare il profitto in un processo di attacco a sandwich, il quale, si ricorda, è composto da: due transazioni da parte dell'aggressore; da una *fee* (“*fee*”, si rimanda a par. 2.2), ovvero commissione, più alta per avere una prelazione sulla conferma dell'ordine, e dallo stretto arco di tempo in cui tutto deve essere eseguito.

Al fine di comprendere meglio l'influenza di queste variabili, successivamente, verranno illustrati i vari casi di un attacco a sandwich in cui si evidenzierà come le commissioni, il tempo e un nuovo stato del pool di liquidità impattino sul profitto effettivo in un attacco a sandwich. Come scenario di attacco a sandwich viene preso in esame l'esempio già riportato nel capitolo precedente, nel quale, senza le nuove variabili, si riportava un profitto di $0,97 \text{ ETH}$ per l'aggressore Tizio. Inoltre, i risultati che verranno esposti sono frutto dell'inserimento di ulteriori dati nelle formule e non saranno frutto di immaginazione.

COMMISSIONI:

Le commissioni, per semplificazione, sono comprensive di commissioni sulle transazioni e di commissioni sulla conversione euro – moneta digitale. Inoltre, le commissioni non sono calcolate per Caio, poiché inutili ai fini del profitto per l'aggressore.

Grafico 1:



Il grafico 1 mostra sull'asse verticale il profitto e sull'asse orizzontale le commissioni in % applicate alle due transazioni effettuate da Tizio, quella di acquisto e quella di vendita.

Si osserva come le commissioni impattino negativamente sul profitto di Tizio. Nella situazione originale, con 0% di commissioni, Tizio guadagna 0,97 ETH. Invece, con l'applicazione di % sempre più alte per le commissioni, il grafico mostra come il profitto dell'aggressore si riduca drasticamente, fino a diventare negativo quando le commissioni raggiungono o superano il 17,5%. Questo ribadisce l'impatto delle commissioni nel risultato di redditività per un aggressore in un attacco a sandwich.

Questa sensibilità del profitto ai costi di transazione potrebbe indurre i vari Dex ad aumentare, anche leggermente, le commissioni al fine di disincentivare attacchi come quello a sandwich; d'altra parte, però, devono bilanciare questa strategia con la necessità di rimanere competitivi e attraenti per i clienti. Infatti, qual ora si alzassero troppo le commissioni, gli utenti si sposterebbero su Dex più convenienti se pronti ad esporsi ad un rischio maggiore di subire attacchi. Inoltre, come già affermato in precedenza, il grafico evidenzia il fatto che per gli aggressori è fondamentale considerare attentamente le commissioni nei loro calcoli iniziali; poiché, come da grafico, una commissione elevata può trasformare un attacco potenzialmente redditizio in una perdita.

FATTORE TEMPO:

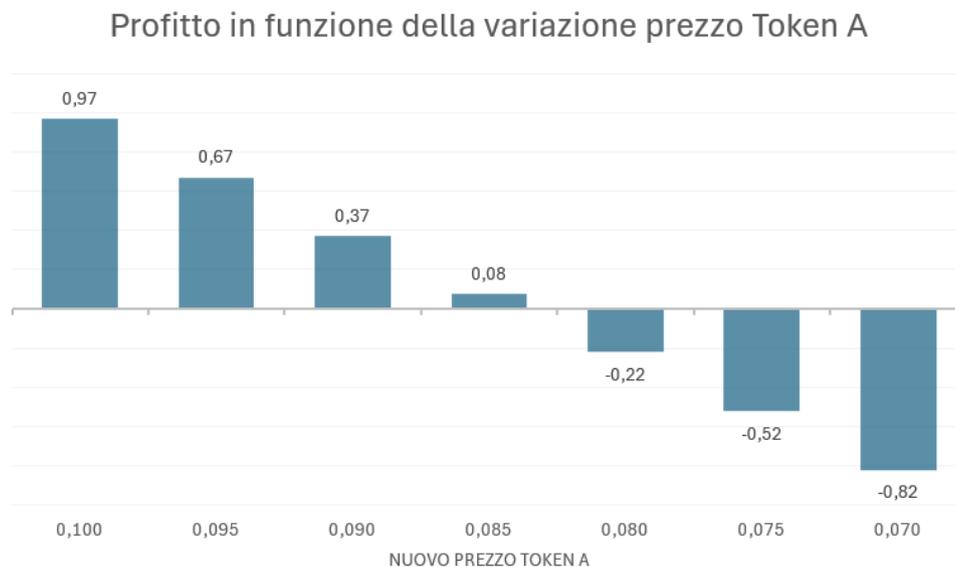
Il fattore tempo incide sia sul prezzo della moneta virtuale, sia sullo stato del pool di liquidità di un Dex. Entrambi possono essere influenzati anche da innumerevoli altre variabili; alcune di queste possono essere: fattore tempo, nuove transazioni poste in essere, fattori strutturali, ritardi software, latenza connessione, modus operandi di specifici Dex, altri rischi sistematici.

Di seguito si andrà ad analizzare come il fattore tempo incida sul profitto di un aggressore autore di attacco a sandwich, utilizzando l'esempio del par. 2.3, e analizzando l'ipotesi in cui a variare sia il prezzo del Token (1) o lo stato del pool di liquidità (2).

1) Variazione prezzo del Token A:

Si ipotizza un cambio del prezzo del Token A successivo alla conferma d'acquisto di Caio e precedente all'azione di back-running di Tizio. Dunque, solo la quantità di Token A ottenuti da Tizio con l'azione di back-running saranno influenzate dal nuovo prezzo.

Grafico 2:



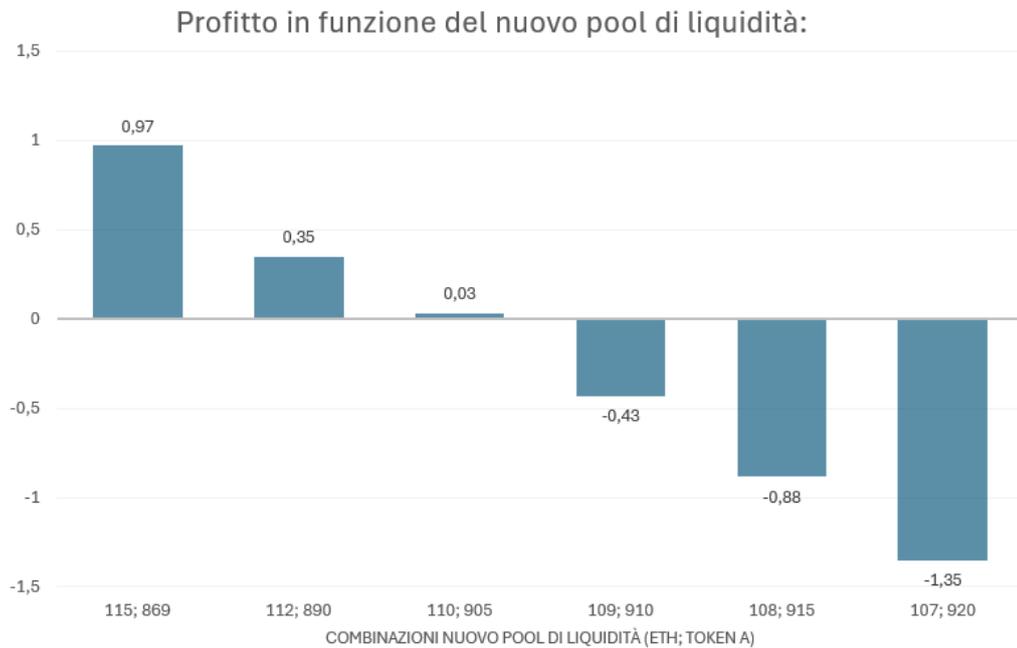
Si può notare dal grafico 2 che la diminuzione del prezzo per i Token A è direttamente proporzionale al profitto conseguito da Tizio per tutta la sua operazione di attacco a sandwich. Provando a spiegare ciò, si può affermare quanto segue:

Se il prezzo di 0.1 ETH rimane invariato dall'inizio del processo fino al suo termine, Tizio guadagna 0.97 ETH come da esempio par.2.3. Tuttavia, man mano che il prezzo scende (0.095, 0.090, 0.085, ...) il profitto diminuisce (rispettivamente 0.67, 0.37, 0.08, ...) fino a portare Tizio dal riscontrare un guadagno al subire una perdita. Infatti, da diminuzioni dal prezzo iniziale del 20% circa, Tizio inizierà ad essere in perdita e tutta l'operazione di attacco a sandwich porterà solo a risultati negativi.

Tutto ciò mette in evidenza come le strategie di front-running e back-running possano essere gravemente influenzate da una variazione più o meno improvvisa del prezzo di un Token. Nel nostro caso, la strategia di Tizio risulterà compromessa se il prezzo del Token A dovesse calare significativamente. Inoltre, a questo possibile rischio, bisogna aggiungere i costi di commissione prima citati, i quali influenzerebbero negativamente ancor di più la possibilità di guadagno in un momento di calo dei prezzi.

2) Nuovo stato del pool di liquidità

Grafico 3:



La tabella sopra mostra alcune ipotesi di volatilità dei pool di liquidità e le loro conseguenze sul profitto di Tizio. Come da esempio del par .2.3, la prima ipotesi riporta un guadagno di 0.97 ETH senza alcuna variazione inaspettata del pool di liquidità. Tuttavia, se il pool di liquidità dovesse variare portando il numero di ETH a 107 e il numero di Token A uguale a 920 (ipotesi più pessimistica presa in esame per l'aggressore), Tizio non otterrebbe più un guadagno, bensì subirebbe una perdita di -1.35 ETH.

Inoltre, si può anche notare come piccole variazioni possano incidere sul profitto. Se si prende in analisi la combinazione dei pool di liquidità (112; 890) e il relativo profitto di 0.35 ETH, ci si rende subito conto che vi è una differenza di -0.62 ETH rispetto al profitto originale di 0.97 ETH. Questo vale a dire che il 63.9% del profitto viene vanificato a causa della variazione, tra l'altro la meno pessimistica, presa in esame nella tabella di sopra.

L'efficienza di una strategia a sandwich dipende fortemente dalla stabilità del pool di liquidità. Se il pool è soggetto a variazioni inaspettate, il profitto atteso può calare significativamente o trasformarsi in perdita.

Tutto ciò scoraggia eventuali aggressori dall'effettuare attacchi di questo tipo, poiché, anche se eseguiti alla perfezione, il rischio di volatilità non è né controllabile né prevedibile dagli utenti; infatti, si tratta di un rischio amplificato da: fattori esterni, nuove transazioni poste in essere, fattori temporali e fattori strutturali dello specifico Dex utilizzato.

In sintesi, le evidenze empiriche appena mostrate dimostrano come un attacco a sandwich sia estremamente sensibile a variabili esterne. Anche se un aggressore, Tizio in questo caso, potesse progettare e pianificare il suo attacco nei minimi dettagli, ci sarà sempre un'intrinseca instabilità nel mercato che potrà trasformare potenziale profitto in pesante perdita. Inoltre, dalle riflessioni emerse dai paragrafi precedenti si suggerisce che i rischi connessi ad operazioni di trading, e non solo connesse ad attacchi a sandwich, rendono certe tattiche, all'apparenza da guadagno facile e veloce, meno affidabili del previsto.

CONCLUSIONI

In questa tesi si è esplorato il concetto di arbitraggio, partendo dalle sue origini come strategia finanziaria fino ai giorni di oggi, dove trova applicazione anche in contesti digitali come blockchain e Automated Market Makers (AMM).

Nel primo capitolo è stato esaminato l'arbitraggio tradizionale, ovvero come strumento finanziario di cui sono state illustrate le caratteristiche, le strategie e i principi fondamentali. Inizialmente era stato definito l'arbitraggio come opportunità di guadagno veloce e senza assunzione di rischio, attraverso transazioni simultanee su diversi mercati per sfruttarne le discrepanze di prezzo. Successivamente, ne sono stati discussi i limiti e le complessità, tra cui ricordiamo i costi di transazione e la liquidità stessa di un mercato, e come questi possano influenzare la capacità di trarre un profitto certo da questa strategia finanziaria.

Nel secondo capitolo si è spostata l'attenzione sul mondo digitale, in particolare sulla tecnologia blockchain, e su come l'arbitraggio si adatti a questo nuovo contesto. Di questo mondo è stato descritto il funzionamento con le sue principali caratteristiche, tra cui: la decentralizzazione, la trasparenza e la sicurezza. A seguito si è fatto un focus sugli AMM, i quali facilitano gli scambi di criptovalute senza la necessità di intermediari, basandosi anche sulla regola del Constant Product Market (CPMM) per mantenere stabile il mercato. In particolare, nel mondo AMM, si è approfondito il concetto degli attacchi a sandwich e di come queste pratiche sleali possano minare alla manipolazione del prezzo di un asset al fine di un profitto. Per spiegare come avviene questo tipo di attacco è stato presentato un esempio pratico, dove si spiega come un aggressore possa trarre guadagno sfruttando informazioni sulle transazioni nella mempool. Tuttavia, la successiva analisi empirica ha evidenziato come variabili esterne possano influenzare significativamente il risultato finale, trasformando un profitto atteso in perdita. Durante il capitolo sono emerse anche riflessioni scoraggianti per eventuali aggressori, sia in merito alla gestione del rischio e sia, anche se con brevi cenni, sull'impiego di misure di prevenzione adottate dai Dex ("Flash Bots"; par. 2.3).

Si può concludere questa tesi affermando che l'arbitraggio, sia nel contenuto tradizionale che in quello digitale, offre interessanti opportunità di profitto, ma richiede una profonda conoscenza e comprensione delle dinamiche di mercato in aggiunta ad un'avanzata capacità di gestione del rischio. Si possono riassumere le strategie di arbitraggio evidenziando come all'apparenza sembrino sicure e facile da eseguire, ma come poi, in realtà, risultino complesse e piene di insidie, specialmente senza aver piena conoscenza del mercato di riferimento.

BIBLIOGRAFIA E SITIOGRAFIA

- Crenca, Fersini, Melisi, Olivieri, Pelle, (2018) “Elementi di matematica finanziaria”; editore: Pearson.
- Xu, Park, Lin, (2022). “XDBS : On Mitigating Frontrunning attacks in Ethereum”; Massachusetts Institute of Technology.
- “Glossario finanziario – arbitraggio”.
<https://www.borsaitaliana.it/borsa/glossario/arbitraggio.html>
- Borsa Italiana, (2009). “Sfruttare le differenze di prezzo al fine di ottenere un profitto”. <https://www.borsaitaliana.it/notizie/sotto-la-lente/arbitraggio.htm>
- FasterCapital, (2024). “Inside Salomon Brothers svelare l’arte dell’arbitraggio”.
<https://fastercapital.com/it/contenuto/Inside-Salomon-Brothers--svelare-l-arte-dell-arbitraggio.html>
- FasterCapital. “Arbitraggio Statistico”.
<https://fastercapital.com/it/parola-chiave/4-arbitraggio-statistico.html>
- FasterCapital, (2024). “Finanza comportamentale Mind sui mercati”.
<https://fastercapital.com/it/contenuto/Finanza-comportamentale--Mind-sui-mercati--Finanza-comportamentale-per-Arbitrageurs.html#i-limiti-di-arbitraggio>
- FasterCapital, (2024). “Finanza comportamentale per Arbitrageurs”.
<https://fastercapital.com/it/contenuto/Finanza-comportamentale--Mind-sui-mercati--Finanza-comportamentale-per-Arbitrageurs.html#i-limiti-di-arbitraggio>
- Osservatori.net, (2023). “La Blockchain spiegata in maniera semplice: cos’è e applicazioni”. https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni
- Forbes, (2024). “What is Crypto Arbitrage? How Does It Work?”.
<https://www.forbes.com/advisor/in/investing/cryptocurrency/crypto-arbitrage/#:~:text=This%20arbitrage%20strategy%2C%20also%20known,higher%20price%20at%20another%20exchange>

- CoinDesk, (2023). “Crypto Arbitrage Trading: What Is It and How Does It Work?”. <https://www.coindesk.com/learn/crypto-arbitrage-trading-what-is-it-and-how-does-it-work/>
- Kraken. “Crypto arbitraggio”. <https://www.kraken.com/it-it/learn/trading/crypto-arbitrage>
- Bit2me, (2022). “Che cos'è un Market Maker automatizzato (AMM)?”. <https://academy.bit2me.com/it/que-es-automated-market-maker-amm/>
- Medium, (2020). “Constant Function Market Makers: DeFi’s “Zero to One” Innovation”. <https://medium.com/bollinger-investment-group/constant-function-market-makers-defis-zero-to-one-innovation-968f77022159>
- Techopedia, (2023). “Mempool”. https://www.techopedia.com/definition/mempool?roistat_visit=2440892
- Cointelegraph, (2022) “What is front-running in crypto and NFT trading?”. https://cointelegraph.com/explained/what-is-front-running-in-crypto-and-nft-trading?roistat_visit=2440892
- B2binpay, (2023). “Che cos'è un Attacco Sandwich DeFi?”. <https://b2binpay.com/it/what-is-a-defi-sandwich-attack/>
- Bitconio.net, (2024). “Attacchi a sandwich e aumento commissioni di Ethereum”. <https://www.bitconio.net/enormi-profitti-manipolando-le-transazioni/>