Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Informatica

ANALISI DEI MODELLI DI MERCATO NELLA FINANZA DECENTRALIZZATA

Relatore:
Chiar.mo Prof.
Cosimo Laneve

Presentata da:
Stefano Sgarzi

Sessione III
Anno Accademico 2020 - 2021

Abstract

In questo elaborato si analizzano le principali soluzioni di servizi di cambio decentralizzati, con particolare interesse al modello di mercato utilizzato. Per ogni modello si presenta il funzionamento, l'illustrazione delle possibili varianti e si discutono vantaggi e svantaggi.
Inizialmente viene presentata la finanza decentralizzata, accompagnata da una classificazione dei protocolli che la compongono e delle principali problematiche da affrontare. In seguito sono presentati brevemente i servizi di cambio tradizionali per poter introdurre il modello di mercato a libro di ordini. Si prosegue con l'analisi di EtherDelta, primo protocollo ad implementare il modello di mercato a libro di ordini nella finanza decentralizzata e si discutono le principali problematiche che hanno portato al suo fallimento. In seguito viene analizzato Uniswap, protocollo che ha per primo proposto il modello ad automated market maker, attualmente standard per l'implementazione di servizi di cambio decentralizzati. Infine viene discusso un ulteriore modello poco utilizzato nella finanza decentralizzata che risulta essere particolarmente vantaggioso in situazioni di mercato a bassa liquidità, in occasione dell'emissione di nuova criptovaluta.

Indice

Capitolo 1

Introduzione

La tecnologia blockchain, nata nel 2009 per realizzare Bitcoin, una valuta digitale decentralizzata, venne presto impiegata per altre applicazioni. Nel 2015 viene lanciata Ethereum che permette oltre allo scambio di valore anche l'esecuzione di programmi turing completi, gli smart contracts.
Potendo quindi decentralizzare l'esecuzione di un programma in grado di valorizzare gli oggetti trattati, le possibilità risultarono enormi.

Se i tentativi di applicazione sono stati innumerevoli, i principali settori[1] in cui la blockchain è risultata efficace sono stati il gaming, l'utilizzo di NFT per la vendita di arte digitale, le terre virtuali, le stablecoin decentralizzate ed ovviamente la finanza decentralizzata. Quest'ultima è stata la prima a nascere ed è attualmente il settore in cui la tecnologia blockchain è più utilizzata.

1.1 La finanza decentralizzata

La finanza decentralizzata, anche chiamata DeFi[2], è l'insieme di protocolli e applicazioni che offrono servizi bancari ed assicurativi tramite l'utilizzo di criptovalute. Si può quindi pensare alla finanza decentralizzata come ad una vera e propria infrastruttura finanziaria che vuole diventare un'alternativa alla finanza tradizionale.

1.1.1 Nascita della finanza decentralizzata

Non c'è una data condivisa da cui si considera nata la finanza decentralizzata ma ci sono una serie di elementi molto importanti che ne hanno creato le basi e permesso lo

[1] non sono considerate applicazioni della blockchain in ambito business to business ma solo quelle che impattano direttamente sull'utente finale

[2] da Decentralized finance

sviluppo.
La blockchain Ethereum viene lanciata nel 2015 e nel primo anno di sviluppo vide solamente alcuni progetti pionieristici tra cui Maker, concettualizzato già prima del lancio di Ethereum, ed EtherDelta, che approfondisco nel capitolo 3.
Nel 2017, con il mercato rialzista ci fu il folle periodo delle ICO[3] ed il principale utilizzo di Ethereum in questo periodo fu appunto la raccolta di capitale. Più del 95% dei progetti fallì, molti si rivelarono delle truffe ma i pochi che sopravvissero sono oggi parte dei pilastri della finanza decentralizzata. Si tratta di Aave (servizio di prestito e finanziamento) [1], Bancor (servizio di cambio) [2], Syntetix (servizio di trading su derivati) [3], per citarne alcuni.
Tra il 2018 ed il 2019 questi protocolli ed Uniswap, approfondito nel capitolo 4, lanciarono su Ethereum. Questa prima fase, dal lancio di Ethereum fino ad inizio 2020 può essere considerata il periodo di fondazione della finanza decentralizzata.

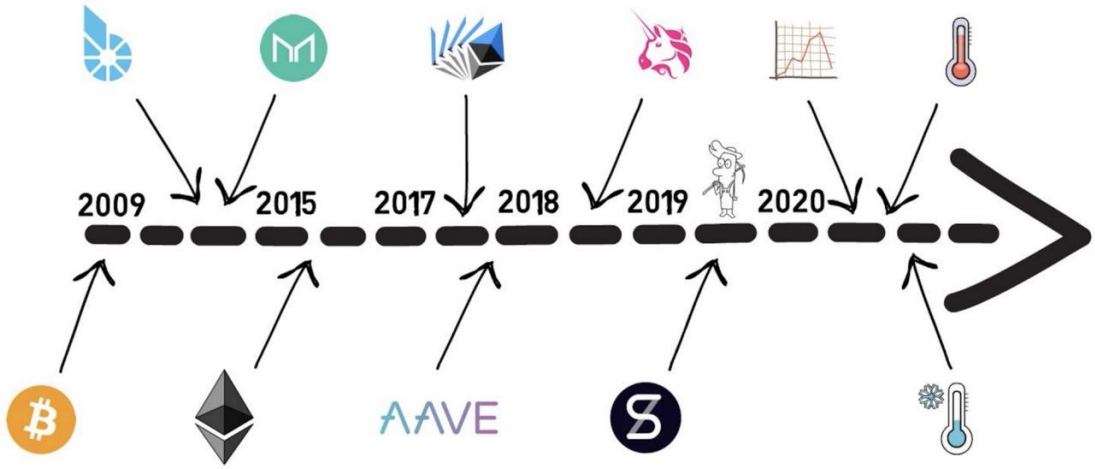

Figura 1.1: Preistoria della DeFi (Fonte: finematics.com)

La prima vera crescita avvenne nell'estate del 2020, ribattezzata "DeFi Summer", nella quale il protocollo Compound (servizio di prestito e finanziamento) [4] approfondito nella sezione 1.2 attivo' il programma di "liquidity mining". Ciò consisteva nell'incentivare l'utilizzo del protocollo tramite un premio in criptovaluta del protocollo stesso, COMP. Questo programma ebbe un enorme successo e venne replicato da innumerevoli protocolli a seguire.

[3]Initial Coin Offering. Nuovi progetti anziché finanziarsi in modo tradizionale tramite fondi d'investimento raccoglievano Ether in cambio della criptovaluta del progetto, promettendo alti ritorni

L'ultimo tassello fondamentale per lo sviluppo della finanza decentralizzata fu Yearn Finance, approfondito nella sezione 1.2, che lanciò ad inizio 2020 e distribuì la propria criptovaluta YFI a Luglio 2020, con un modello simile a Compound.
Con i protocolli citati si può considerare conclusa la storia della Defi. Gli anni successivi infatti furono principalmente concentrati sul lancio di nuovi protocolli decentralizzati, leggermente differenti da quelli esistenti oppure sviluppati su blockchain alternative ad Ethereum che permettevano minori commissioni di rete e maggiore velocità.
Si può quindi dire che la preistoria della DeFi termina nel 2019 e che l'inizio dell'utilizzo e gli ultimi sviluppi tecnici avvennero nel corso del 2020, anno in cui si può dire che sia "nata" la finanza decentralizzata.

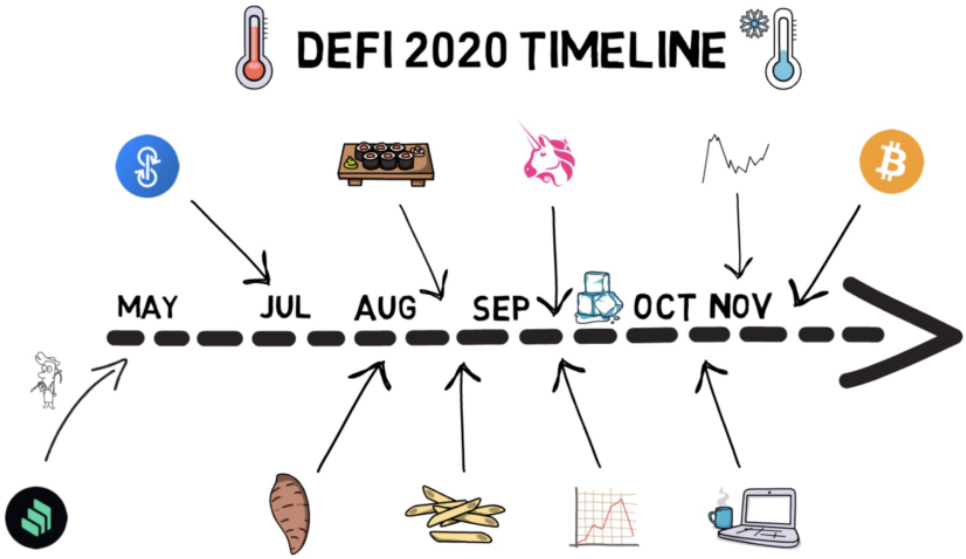

Figura 1.2: DeFi Summer (Fonte: finematics.com)

1.1.2 I motivi della crescita

La finanza decentralizzata ha avuto un'enorme crescita, specialmente negli ultimi anni. Il parametro comunemente utilizzato per analizzare il "valore" della finanza decentralizzata è il TVL (total value locked); esso rappresenta la somma del controvalore di tutte le criptovalute depositare su tutti i protocolli di finanza decentralizzata. Per poter utilizzare un protocollo è infatti necessario, nella maggior parte dei casi, depositare le criptovalute dal proprio portafoglio all'indirizzo del contratto.

Se il TVL sale significa che vengono depositate più criptovalute e che quindi l'utilizzo della finanza decentralizzata sta crescendo.
Dalla figura 1.3 si può osservare la crescita del TVL della finanza decentralizzata da Maggio 2020 fino ad oggi.

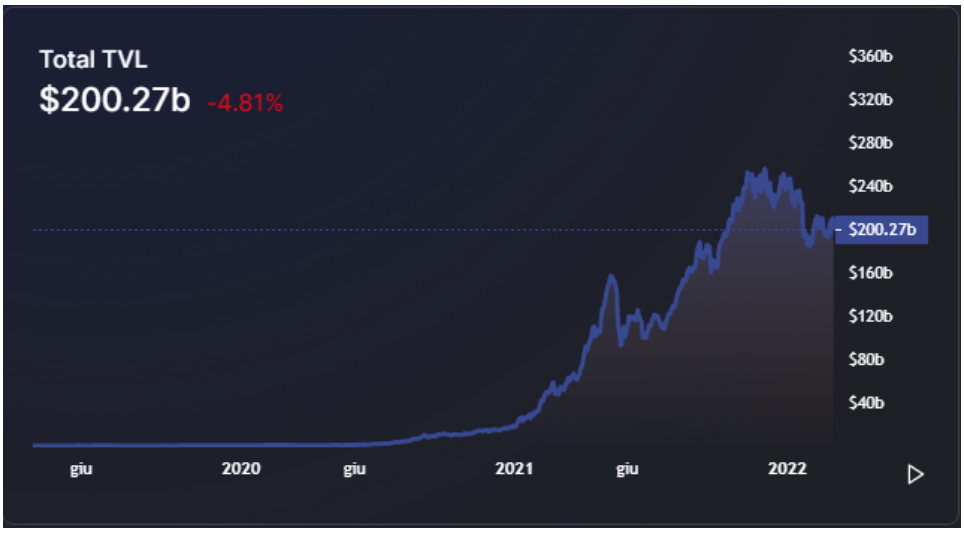

Figura 1.3: DeFi TVL (Fonte: Defi Llama)

Sebbene la finanza decentralizzata sia ancora un ambiente estremamente innovativo ed immaturo, lontano anni luce dalla finanza tradizionale ed utilizzato da una piccolissima percentuale di chi detieni criptovalute, presenta alcuni vantaggi strutturali che ne hanno determinato il successo in questa fase embrionale.

Il principale vantaggio deriva dal fatto che decentralizzando i servizi finanziari si va a sostituire l'intermediario con un software che agisce in modo autonomo. Questo permette di eliminare tutte le commissioni applicate da banche ed intermediari finanziari per l'utilizzo dei servizi. Gli utenti devono comunque pagare le commissioni di rete per poter eseguire la transazione, tuttavia si tratta di costi non paragonabili a quelli degli istituti finanziari e generalmente dipendenti dallo stato di utilizzo della blockchain su cui è implementato il servizio. Costi che saranno destinati a ridursi con lo sviluppo delle tecnologie blockchain.

Un secondo vantaggio è derivante dall'utilizzo di criptovalute: non ci si deve affidare ad una banca per detenere i propri fondi e per accedere ai servizi finanziari. Ognuno è responsabile del proprio denaro. Se questo viene perso per errore non c'è alcun modo di recuperarlo. Questo comporta più responsabilità ma anche più libertà, non dovendosi fidare di alcuna azienda ed essendo gli unici a poter agire sui propri averi.

Inoltre, a seconda della blockchain su cui il servizio è sviluppato è possibile eseguire transazioni ed inviare denaro in secondi o minuti. Garantendo una maggiore velocità ed elasticità rispetto alla finanza tradizionale dove spesso un bonifico richiede giorni per essere accreditato. Questi vincoli temporali non sono di carattere tecnico ma dipendono da politiche aziendali consolidate nella finanza tradizionale che però sono considerate assurdità nella finanza decentralizzata.

Un ulteriore vantaggio molto importante è dato dal fatto che la finanza decentralizzata è permissionless, non è infatti necessaria alcuna approvazione per utilizzare i servizi offerti. Chiunque, senza distinzioni di alcun tipo può accedere ai servizi offerti.
Questo non accade con la finanza tradizionale, facilmente accessibile solo nelle economie più sviluppate come quella americana ed europea. In regioni meno sviluppate o politicamente instabili non sono presenti banche e servizi finanziari. Gli abitanti di queste zone sono detti unbanked e nel 2020 erano 2 Miliardi [5] in tutto il mondo.
Per accedere alla finanza decentralizzata è sufficiente avere un dispositivo mobile ed una connessione internet.

1.2 Principali tipologie di applicazioni

In questa sezione riporto una possibile classificazione dei protocolli che compongono la finanza decentralizzata in base alla tipologia di servizio offerto. Descriverò le principali categorie tramite un'analisi dell'applicazione che ritengo essere meglio rappresentativa.
La classificazione proposta non è esaustiva, tratterò solamente le principali tipologie di servizi, ormai consolidati e con una forte base di utenti. Inoltre le distinzioni non sono esclusive, infatti alcuni protocolli offrono più servizi andando quindi a ricadere in più di una delle categorie indicate.

- **Compound - prestiti e finanziamenti**

  Il protocollo Compound, già citato nella sezione 1.1.1 per il primo programma di liquity mining, principale catalizzatore della crescita della finanza decentralizzata nell'estate del 2020, viene lanciato nel Settembre del 2018 [6] sulla blockchain Ethereum.
  Esso mette in comunicazione gli utenti che desiderano prendere in prestito criptovalute con gli utenti che desiderano depositare criptovalute per ottenere interessi. Questa categoria di protocolli viene chiamata "money market", mercato monetario. Infatti, in base a domanda ed offerta, su questi protocolli vengono determinati i tassi di interesse per il deposito e per il prestito delle diverse criptovalute.

Su compound sono presenti circa 20 criptovalute [4]; per ciascuna di queste è mostrato un interesse sul deposito (supply APY[5]) ed un tasso d'interesse per il prestito (borrow APY).
Un utente che detiene USDC può decidere di depositarli su Compound per ottenere un interesse del 2,10%, come mostrato nell'immagine 1.4.

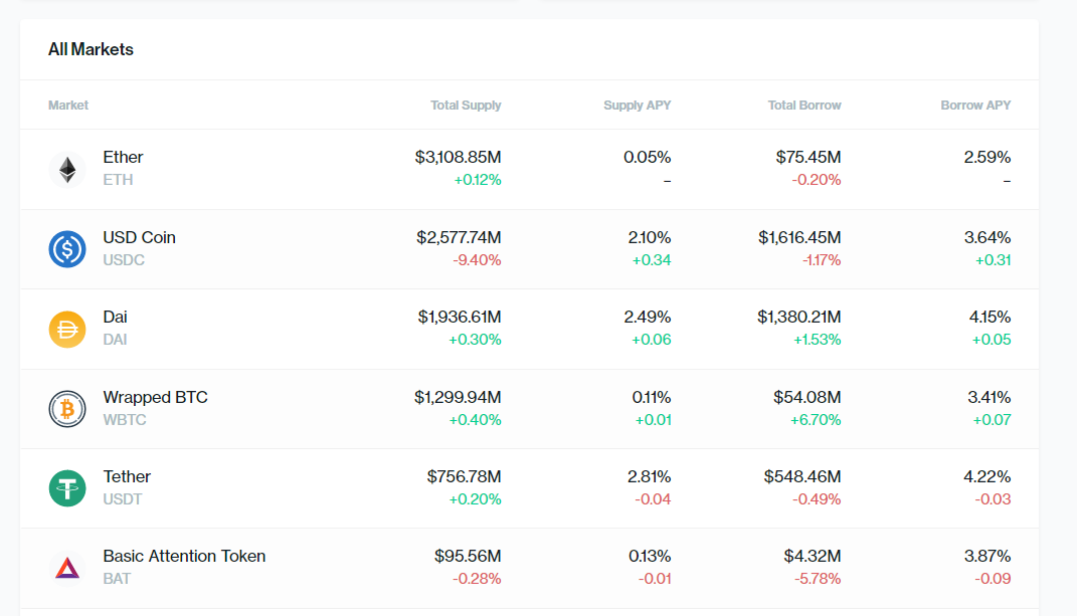

Figura 1.4: Interfaccia Compound

Un aspetto implementativo interessante di compound è che la registrazione dei depositi e dei prestiti non viene eseguite tramite un dizionario, su cui sono riportate le attività o passività di ciascun indirizzo (rappresentativo di un portafoglio utilizzato dall'utente) ma tramite token. Se infatti l'utente M deposita 1000 USDT riceverà una certa quantità X di cUSDC (USDC depositati su Compound). Il token cUSDC non è quotato sul mercato ma si apprezza nei confronti di USDC del 2,10% annuo. Di conseguenza se dopo un anno M desidera prelevare i propri USDC potrà depositare i suoi X cUSDC ed otterrà dal protocollo 1021 USDC: il deposito iniziale più gli interessi. Questa scelta implementativa è molto snella ed efficiente ed è adottata da tutti i protocolli della finanza decentralizzata.

I rischi di deposito su Compound sono determinati da eventuali errori nel codice del protocollo ma non dipendono dalla possibilità del prestatario di ripagare il de-

[4]la rimozione di cryptovalute o l'aggiunta di nuove viene decisa dalla governance. Solo i detentori del token COMP possono effettuare proposte e votarne l'attuazione
[5]APY è l'acronimo di Annual Percentage Yield, il ritorno percentuale annuo sull'investimento

bito. Questo perché i prestiti sono sovracollateralizzati. Ciò significa che per poter prendere in prestito 1000 USDC è necessario aver depositato sul protocollo almeno 1250 USDC. Nel caso in cui il prestito non venga ripagato nei tempi previsti il protocollo si approprierà automaticamente del collaterale depositato. La quantità di criptovaluta che può essere presa in prestito rispetto a quella depositata è definita "Collateral factor", nel caso di USDC è l'80%.
Chiaramente risulta poco sensato depositare USDC per prendere in prestito meno USDC; generalmente si depositano criptovalute che non si ha intenzione di vendere per prendere in prestito altre criptovalute. Ad esempio un utente M che detiene 1 Ether può decidere di depositarlo su Compound come collaterale per prendere un prestito in stablecoin, da utilizzare per operazioni di trading. Fino a che il prestito non viene estinto non è possibile prelevare il collaterale.
Tuttavia, è importante riportare che se il prezzo di Ether scende e si avvicina pericolosamente al valore preso in prestito avviene un evento di liquidazione, con la conseguente perdita dell'Ether depositato.

Un altro servizio che gestire prestiti e finanziamenti degno di nota è Aave [1], presente anch'esso sulla blockchain Ethereum.

- **Yearn Finance - ottimizzatori di rendimento**

  Una categoria che racchiude un grande numero di protocolli è quella degli ottimizzatori di rendimento, comunemente chiamati "Yield Optimizer". Si tratta di applicazioni che, appoggiandosi ad altri servizi permettono di ottenere un aumento dei rendimenti. Il principale esponente, oltre che primo esempio di questa categoria è Yearn Finance, lanciato il 17 Luglio del 2020 da Andre Cronje.

  Il primo servizio offerto da Yearn Finance fu l'ottimizzazione dei ritorni su stablecoin. Era quindi possibile depositare le principali stablecoin ed il protocollo si occupava autonomamente di scegliere se depositare la liquidità su Compound o su Aave, a seconda dell'offerta migliore.
  In seguito, con il crescere delle opportunità di ritorno nella finanza decentralizzata, furono aggiunte nuove criptovalute e nuove strategie. La liquidità non veniva più depositata sull'indirizzo del protocollo ma furono create diverse piscine di liquidità, una per ogni strategia e con un proprio indirizzo, i cosiddetti "vaults".
  Attualmente su Yearn sono disponibili svariati vaults, ciascuno di questi ha una criptovaluta di riferimento, un ritorno annuo stimato e una sezione di testo che descrive la strategia applicata. Depositando nel vault si può così delegare l'esecuzione della strategia al protocollo ed attendere il momento di prelevare il proprio capitale arricchito dagli interessi.

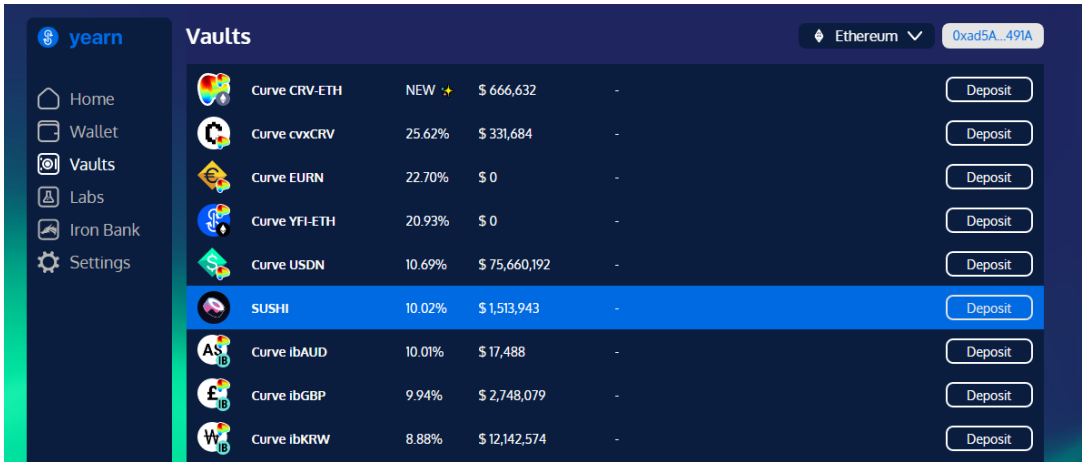

Figura 1.5: Interfaccia Yearn Finance

Grazie al vault è quindi possibile ottenere dei rendimenti superiori a quelli offerti dai money market o da altre tipologie di protocolli decentralizzati. In più, un importante vantaggio è dato dal fatto che quest'ultimo raccoglie la liquidità da tutti i partecipanti ma agisce come un unico indirizzo, di conseguenza viene pagata una sola transazione ad ogni trasferimento. Questo garantisce un abbattimento delle commissioni che spesso impattano in modo importante sui ritorni; specialmente per strategie che richiedono frequenti spostamenti, e di conseguenza un numero importante di transazioni.

Appartengono a questa categoria anche i cosiddetti "autocompounder", servizi che a differenza di Yearn Finance offrono vaults che implementano una specifica strategia.
I fondi presenti nei vaults vengono depositati in precise piscine di altri protocolli. In seguito, l'interesse ottenuto viene giornalmente convertito nella criptovaluta di base e ridepositato, per incrementare il valore totale ed aumentando così i ritorni futuri.
Gli autocompounder permettono quindi di sfruttare l'interesse composto, determinando un aumento considerevole del ritorno annuo[6].
I più conoscuiti sono Beefy finance ed Autofarm. Un altro yield optimizer degno di nota è Alpha Homora, specializzato in strategie che utilizzano la leva finanziaria.

[6]quando si fa riferimento al ritorno annuo composto si utilizza la sigla APY; quando si fa riferimento al ritorno annuo senza reinvestimento degli interessi si utilizza la sigla APR

- **Synthetix - trading su derivati**

  Synthetix è il primo protocollo decentralizzato che permette l'emissione di asset sintetici analoghi a quelli presenti nella finanza tradizionale. In più è presente un servizio di cambio decentralizzato dedicato a questi asset chiamato Kwenta.
  L'utilizzo di asset sintetici consente di acquistare o vendere svariati asset senza doverli detenere. Su Kwenta è possibile trovare asset sintetici che replicano il prezzo di valute fiat (euro, dollaro, yen, sterlina, ecc) criptovalute, azioni, materie prime (come oro, argento, petrolio, grano, soia, ecc) e indici di borsa o indici composti da altri asset.
  Gli asset sintetici sono molto diffusi nella finanza tradizionale ma Synthetix porta questi servizi anche nella finanza decentralizzata, mettendo a disposizione un'unica piattaforma per poter investire o fare trading su tutte le tipologie di asset esistenti. Questo tipo di servizi permettono inoltre l'accesso alla finanza tradizionale per gli unbanked.
  Un ulteriore servizio conosciuto che permette lo scambio di asset sintetici è Mirror protocol [7].

- **Uniswap - servizi di cambio**

  L'ultima categoria che riporto in questa classificazione sono i servizi di cambio, che permettono acquisto e vendita di criptovalute in modo decentralizzato, anche detti "decentralized exchange" o più brevemente "DEX".
  L'esempio più importante è Uniswap che verrà approfondito nel capitolo 4.

  Un altro servizio di cambio molto conosciuto è Sushi [8], emerso con un "vampire attack" ad Uniswap, dinamica che non approfondirò in questo lavoro. E' importante citare anche Curve [9], servizio di cambio specializzato in stablecoin e coppie di asset simili. Esso è il protocollo con maggior TVL[7] in assoluto. Infine altri due servizi di cambio piuttosto utilizzati che presentano importanti differenze rispetto ad Uniswap sono Bancor [2] e 1inch [10].

1.3 Problemi da risolvere per la finanza decentralizzata

Dopo aver analizzato, nella sezione precedente, le principali tipologie di applicazioni di successo presenti nella finanza decentralizzata, descrivo di seguito i principali problemi da affrontare ed i risultati che si potrebbero ottenere nello sviluppo del settore.

[7] Total Value Locked

Un primo problema da affrontare riguarda il rischio di exploit. I numerosi attacchi effettuati a danno di protocolli decentralizzati hanno causato perdite per un valore stimato di 1,3 Miliardi nel 2021, come dichiarato dal report di Certik [11], una delle principali aziende che si occupa verifiche e analisi formali su smart contracts, detti "audits".
Per quanto riguarda la finanza decentralizzata sviluppata sulla blockchain Ethereum e sulle altre blockchain EVM compatibili, gli utenti difficilmente utilizzano servizi privi di audits. Inoltre il TVL e la longevità del protocollo sono i principali parametri considerati dagli utenti nella scelta del protocollo; indicano infatti una minore probabilità di trovare gravi vulnerabilità nel codice.
Altre blockchain propongono linguaggi di programmazione formali, più facilmente analizzabili o adottano politiche closed source.

La problematica forse più sentita in questa fase riguarda le tecniche a disposizione dei protocolli per attrarre liquidità.
Dalla nascita della DeFi la strategia utilizzata dai protocolli per attrarre la liquidità consiste nel "liquidity mining". Ovvero incentivare il deposito di liquidità sul proprio protocollo con token di governance della piattaforma. Questo permette di aumentare i ritorni ed invoglia più utenti ad utilizzare il proprio protocollo.
Tuttavia, questo meccanismo ha sollevato una serie di problematiche. In primo luogo, quasi la totalità degli utenti che ottengono il token di governance non sono intenzionati a detenerlo e lo vendono alla prima occasione. Questo comporta una forte pressione ribassista sulla criptovaluta ed è piuttosto problematico per il protocollo stesso e per gli investitori. In più, con il passare del tempo, la riduzione del prezzo del token di governance va ad annullare l'incentivo.
In secondo luogo, una volta terminato o ridotto questo incentivo la liquidità si riduce velocemente. Infatti gli utenti sono alla ricerca di opportunità di rendita e difficilmente trattengono la liquidità sul protocollo per altri motivi.
Per queste motivazioni il principale interesse di ricerca in ambito DeFi è rivolto ad individuare nuove metodologie per distribuire la liquidità in modo efficace tra i protocolli.
Alcuna applicazioni che si propongono di risolvere questo problema sono Tokemak [12], lanciato su Ethereum nell'estate del 2021 e Solidly [13] lanciato di recente sulla blockchain Fantom il 24 Febbraio 2022.

Un ulteriore ambito di ricerca, di interesse soprattutto per gli utenti, è lo sviluppo di protocolli che offrono servizi assicurativi on-chain.
Come analizzato nella sezione 1.2, la tecnica utilizzata da Compound per registrare il deposito di criptovalute da parte di un utente si è velocemente imposta come standard. Quindi a seguito del deposito di X USDC sul protocollo Z si otterranno in cambio Y zUSDC (token rappresentativi del deposito). In alcuni casi i token zUSDC non sono disponibili sul mercato, in altri casi hanno un valore di mercato e possono essere depositati su altri protocolli, ad esempio in Yield optimizer per incrementare ulteriormente

il ritorno ottenuto dal protocollo Z. In più è anche possibile utilizzare gli zUSDC come collaterale per prendere un prestito ed utilizzare la liquidità ottenuta per aumentare nuovamente l'interesse complessivo. Questa procedura può essere ripetuta varie volte andando ad aumentare il ritorno finale ma aumentando anche i rischi di liquidazione.
A causa di queste possibilità e della complessità nel valutarne il rischio è sempre più forte l'esigenza di servizi assicurativi decentralizzati efficienti che siano in grado di coprire gli assicurati da liquidazioni a catena.
Un esempio di servizio assicurativo decentralizzato è Nexus Mutual [14], lanciato nel Maggio 2019. Questo protocollo è funzionante, tuttavia per poter ottenere il risarcimento è necessario richiedere l'approvazione ai detentori del token di governance. Essi dovranno pronunciarsi tramite una votazione sull'effettivo avvenimento dell'evento incriminato.
Questo intervento umano è visto da molti come uno svantaggio; con servizi assicurativi on-chain si intende un protocollo decentralizzato che verifichi tramite oracolo se l'evento è avvenuto e risarcisca automaticamente l'utente danneggiato.

1.4 Argomenti affrontati

Tra le varie tipologie di protocolli di successo della finanza decentralizzata analizzati nella sezione 1.2, considero, in questo lavoro, solamente i servizi di cambio. Esempio di servizi di cambio già citati sono Uniswap, EtherDelta e Bancor.
Questa tipologia di protocolli rappresenta un elemento fondamentale della finanza decentralizzata perché permette l'acquisto di criptovalute tramite la coin principale della blockchain di riferimento. Nel caso della blockchain Ethereum sarà presente su un servizio di cambio decentralizzato il cambio YFI/ETH che permetterà di scambiare criptovaluta di Yearn Finance con Ether e viceversa, quindi di effettuare un acquisto o una vendita nei confronti di Ethereum. Per molte cryptovalute questo è l'unico veicolo di acquisto in quanto, specialmente per quelle poco conosciute, l'ottenimento di un cambio su un servizio centralizzato risulta estremamente costoso.

Nell'analizzare le principali tipologie di servizi di cambio mi concentro sul modello di mercato utilizzato e sui vantaggi e svantaggi derivanti. Esso è un modello matematico (che non analizzo in modo formale) che descrive in che modo avvengono gli scambi di un bene tra gli operatori di mercato.
Più il modello di mercato è vicino alla realtà, più è preciso ed efficiente ma richiede anche molta liquidità ed ha dei "costi" di mantenimento[8]. Più il modello è semplice, minori saranno i costi generali, ma si discosterà di più da ciò che accade nella realtà. Potranno quindi presentarsi anomalie tra il prezzo del bene ottenuto dal modello ed il suo valore

[8]la natura di questi costi sarà approfondita nei capitoli successivi

reale. Tutte queste anomalie dovranno essere gestite opportunamente.

In questo lavoro approfondisco nel dettaglio i modelli di mercato utilizzati per implementare servizi di cambio decentralizzati, ne analizzo l'intuizione iniziale e le possibili varianti, ed infine riporto vantaggi e svantaggi di ciascun modello. Inoltre analizzo un ulteriore modello, poco utilizzato, che risulta particolarmente vantaggioso in situazioni di mercato a bassa liquidità.

1.5 Struttura della tesi

La tesi è strutturata come segue:
Il primo capitolo introduce la finanza decentralizzata e descrive gli argomenti affrontati in questo lavoro.
Il secondo capitolo tratta i servizi di cambio, iniziando con un'analisi di quelli tradizionali, volta a mostrarne l'utilità. In seguito viene analizzato il modello di mercato a libro di ordini, presentando la struttura ed il funzionamento con una serie di esempi ed illustrando quali sono le opzioni di acquisto o vendita. Infine viene mostrata l'utilità dei servizi di cambio decentralizzati.
Nel terzo capitolo si analizza EtherDelta, primo esempio di servizio decentralizzato, che utilizzava un modello a libro di ordini. Viene mostrata l'interfaccia, come utilizzarlo e si analizzano vantaggi e svantaggi. Nell'analisi degli svantaggi vengono approfonditi i market makers, elemento fondamentale per i mercati che è assente nella finanza decentralizzata.
Nel quarto capitolo si descrive l'interfaccia di Uniswap e la semplicità di utilizzo dopodiché si prosegue con l'analisi dell'automated market maker, il modello di mercato che si è imposto come standard nella finanza decentralizzata. In seguito viene illustrato il funzionamento del modello di mercato e le varianti di quest'ultimo. Infine sono riportati i vantaggi e gli svantaggi del modello.
Nel quinto capitolo viene presentato un terzo modello di mercato, poco utilizzato nella finanza decentralizzata che ha alcuni importanti vantaggi in situazioni di bassa liquidità. Viene illustrato il funzionamento del modello e la situazione in cui risulta essere più efficace. Dopo aver analizzato le possibili varianti del modello si discutono vantaggi e svantaggi.
Infine, nell'ultimo capitolo vengono raccolte le considerazioni finali e sono riportati possibili argomenti per ulteriori approfondimenti.

Capitolo 2

Servizi di cambio

In questo capitolo introdurrò i servizi di cambio, elemento importante per poter comprendere i capitoli successivi.
Un servizio di cambio fisico, comunemente noto come "cambiavalute", permette di scambiare la propria valuta con le altre disponibili. E' spesso presente negli aeroporti ed è anche offerto dalle banche.
Questo servizio risulta particolarmente utile per chi si deve recare in un paese extraeuropeo ed ha necessità di una moneta accettata nel paese di destinazione.
Sarà quindi possibile consegnare Euro, Dollaro o altre valute internazionali al cambiavalute ed ottenere la stessa quantità di valore economico nella valuta desiderata, differente da quella iniziale.
Il tasso di cambio tra valute è definito dai mercati valutari, anche detti "forex". Il servizio è offerto in cambio di una commissione, spesso applicata con una piccola modifica al tasso di cambio corrente, in questo modo la commissione non è fissa ma in percentuale al valore scambiato.

2.1 Servizi di cambio classici

Sebbene esistano servizi di cambio fisici la maggior parte degli scambi tra valute avviene sui mercati finanziari. Gli utenti privati (non istituzionali) possono accedere a questi mercati tramite servizi di cambio online. Si tratta di servizi web offerti da intermediari finanziari, che a seguito di un deposito di euro (con bonifico bancario o carta di credito) permettono lo scambio con altre valute.
Questo tipo di servizi, non permettono il prelievo di contanti, di conseguenza non sono utilizzati per ottenere effettivamente un'altra valuta ma sono utilizzati per investimenti ed attività di trading.

Come esistono servizi di cambio di valute esistono anche servizi di cambio di criptovalute. Questi non hanno alcuna differenza di funzionamento sostanziale, l'unica differenza rilevante è la natura dello strumento finanziario trattato. In questo lavoro mi concentrerò solamente su servizi di cambio di criptovalute.

2.1.1 Utilità dei servizi di cambio di criptovalute

Questi servizi, anche detti "Exchange" permettono di scambiare cryptovalute. E' quindi possibile depositare euro, dollari o cryptovalute ed effettuare gli scambi desiderati.
I servizi di cambio non vengono utilizzati solamente per operazioni di trading o investimento, ma non essendoci un corrispettivo fisico per le cryptovalute sono utilizzati in larga parte per poter acquistare cryptovalute con valute tradizionali.

E' importante sottolineare che questi servizi sono offerti da Aziende, di conseguenza una volta effettuato un deposito di cryptovalute non si ha il possesso di queste ma un credito nei confronti dell'azienda.

Stablecoin Per poter dare una corretta panoramica del mondo delle cryptovalute è importante citare le cosiddette "stablecoin", valute stabili. Esistono infatti cryptovalute che hanno come scopo la replicazione, il più possibile esatta, delle valute tradizionali. Alcuni esempi sono USDT, USDC, DAI, UST ed altre. Ne esistono svariate che si differenziano per livello di sicurezza e per meccanismo di replicazione utilizzato, oltre che per la valuta tradizionale replicata. Queste svolgono un ruolo fondamentale perché permettono di proteggersi dalla forte volatilità che caratterizza questi strumenti. Nel caso in cui si reputi che ci sarà un crollo del valore è possibile scambiare le proprie cryptovalute con stablecoin e preservare il valore del proprio investimento.

Figura 2.1: Stablecoin più diffuse (Fonte: blog)

2.1.2 Modello di mercato a Libro di Ordini

Nel realizzare un servizio di cambio devono essere affrontate una serie di scelte tecniche. Una di queste è il modello di mercato da utilizzare.

Il modello di mercato diffusosi come standard tra i servizi di cambio è il modello a "Libro di Ordini", anche detto modello ad order book.
Questo modello si è imposto ed ha avuto successo perché è perfettamente rappresentativo del mercato reale.

Mercato Il Mercato può essere definito come il luogo, non necessariamente fisico, in cui avvengono gli scambi di un bene. Per poter parlare di mercato è necessario avere una serie di elementi:

- due o più attori
- il bene o asset scambiato
- un registro dove riportare le offerte

Buon esempio di mercato sono le prime borse valori, luoghi fisici in cui venivano scambiate azioni. In genere questi luoghi erano le piazze di una grande città; da cui deriva il termine "piazza affari".
In questo luogo sono presenti 22 **attori**, persone interessate ad acquistare o vendere.
Il **bene scambiato** sono i titoli azionari di un'azienda che produce acciaio.
Il registro non è presente perché si comunica in modo **verbale**, essendo una piazza.
Ogni attore possiede un certo numero di titoli, che vuole vendere, oppure ha dollari per acquistare titoli. Ogni attore dichiara verbalmente se vuole acquistare o vendere titoli, la quantità, ed il prezzo di queste. Dopo un certo numero di tentativi l'attore che vuole vendere N titoli al prezzo X troverà un altro attore che vuole acquistare N o più titoli al prezzo X. In questo modo avverrà lo scambio (di N titoli). Si può quindi immaginare una piazza con queste 22 persone che parlano l'uno con l'altro cercando di trovare la controparte ed arrivare ad un accordo.

Prezzo di mercato In questa situazione qual è il prezzo di mercato? Come si stabilisce?

Poiché il prezzo di mercato varia al passare del tempo consideriamo lo stato del mercato al tempo T. Ad ogni istante di tempo avviene almeno un'azione. Un'azione può essere uno scambio di N titoli tra acquirente e venditore (al prezzo X), oppure la modifica dell'offerta dell'attore B (acquirente o venditore). B può cambiare il numero N di titoli o il prezzo X a cui vuole acquistare o vendere.
Poiché alcune azioni possono essere contemporanee, al tempo T possono avvenire M azioni, con M maggiore di zero. Tra queste M azioni possono essere presenti scambi di

titoli, modifiche dell'offerta o entrambi.

Fatta questa premessa, per rispondere alla domanda è utile immaginare di ordinare gli attori nel seguente modo:

- gli attori sono disposti in due file opposte, rivolte verso il centro della piazza. Una parte da Nord e parte da Sud
- tutti gli attori che vogliono comprare titoli sono nella fila a Sud
- tutti gli attori che vogliono vendere titoli sono nella fila a Nord
- l'acquirente che offre il prezzo più alto è in testa alla fila, l'acquirente che offre il prezzo basso è in coda
- il venditore che offre il prezzo più basso è in testa alla fila, il venditore che offre il prezzo più alto è in coda
- Ogni attore riporta bene in vista un biglietto con scritto il numero di titoli ed il prezzo

Una volta disposti gli attori indichiamo con A l'acquirente in testa alla fila Sud, e con V il venditore in testa alla fila Nord. Supponiamo per semplicità che A e V vogliano scambiare la stessa quantità N di titoli.
Se il prezzo di acquisto per A, indicato con X, corrisponde al prezzo di vendita per V, al tempo T+1 avverrà lo scambio ed i due attori usciranno dal mercato perchè soddisfatti (quindi verranno rimossi dalle due file).
Il prezzo di mercato al tempo T sarà X. Possiamo quindi concludere che il prezzo di mercato al tempo T è uguale al prezzo dello scambio avvenuto a T-1. Poiché al tempo T-1 potrebbe non essere avvenuto uno scambio, ma semplicemente una modifica di offerte è più corretto dire che il prezzo di mercato al tempo T è uguale al prezzo dell'ultimo scambio avvenuto al tempo T-Y, con Y maggiore di zero.

Slippage E' interessante osservare come non sia necessario che il prezzo di A e V coincida per il funzionamento del mercato. Se ad esempio il prezzo di A è 5.3 euro per titolo ed il prezzo di V è 5.5 euro per titolo non è possibile eseguire lo scambio. In questo caso non avviene alcuno scambio e la differenza tra acquirenti e compratori è 0.2 euro.
Questa differenza è detta Slippage ed è un parametro molto importante per un mercato. Un alto slippage può essere causato da un inefficienza del mercato, in altre parole sono presenti troppi pochi attori sul mercato ed è difficile trovare una controparte per i propri scambi.

Nella maggior parte dei casi, nei servizi di cambio, lo slippage è voluto e calcolato e viene utilizzato per applicare commissioni non percepibili per l'utente. Gran parte dei servizi di compravendita di titoli che si dichiarano "senza commissioni" applicano la loro vera commissione aumentando lo slippage.
Quindi se, ad esempio, il prezzo di mercato di Apple è 165 dollari, sarà possibile acquistare Apple a 163 dollari oppure venderla a 167, la differenza viene trattenuta dal

servizio di cambio.

Abbiamo visto che se A e V non concordano sul prezzo sarà presente slippage e non sarà possibile effettuare lo scambio. Per risolvere questa situazione è necessario che uno degli attori modifichi il prezzo dell'offerta per raggiungere il prezzo di A o V. Nel caso in cui l'attore sia diverso da A o V sostituirà A o V posizionandosi in testa alla rispettiva coda.
Altrimenti è necessario attendere che arrivi un 23esimo attore che voglia acquistare o vendere titoli senza avere pretese sul prezzo e che quindi faccia da controparte per A o V.
Quest'ultimo attore svolge un ruolo differente da tutti gli altri. Egli non stabilisce il prezzo a cui vendere o acquistare ma si adegua al prezzo che offre il mercato.

Egli è detto "market taker", ovvero colui che "fa uso del mercato". Tutti gli altri attori visti fino ad ora sono detti "market makers" ovvero coloro che "fanno il mercato" perché decidono il prezzo a cui vendere o comprare.

Seguendo l'esempio delle prime borse valori ed utilizzando l'ordinamento degli attori proposto, abbiamo dedotto che tutte le azioni possibili al tempo T sono uno scambio o una modifica dell'offerta.
Lo scambio sarà tra A e V; la modifica dell'offerta di un attore comporterà un suo riposizionamento nella fila in base al nuovo prezzo offerto oppure riguarderà semplicemente una modifica del numero dei titoli. Quest'ultima potrà riguardare più di un attore contemporaneamente.
Altre azioni possono derivare dall'aggiunta di un attore che può essere un market maker o un market taker.
Nel primo caso si posizionerà nella fila corrispondente. Nel secondo caso andrà ad effettuare uno scambio con A o con V.

Price(USDT)	Amount(ETH)	Total
2630	5.6776	14,930.719
2629	5.3044	13,943.101
2628	23.6761	62,208.648
2627	19.2979	50,687.646
2626	39.8525	104,633.847
2625	41.9429	110,078.504
2624	85.1136	223,298.930
2623	78.2563	205,219.127
2622	54.3433	142,459.848
2621	108.2543	283,675.308
2620	259.6174	680,095.624
2619	32.4883	85,076.785
2,618.22↓ $2,618.22		More
2618	2.0684	5,415.442
2617	107.4549	281,233.226
2616	190.0717	497,337.179
2615	160.2595	419,129.925
2614	66.4412	173,711.406
2613	56.6834	148,137.209
2612	26.2959	68,696.121
2611	82.2587	214,811.696
2610	69.0666	180,279.959
2609	8.5970	22,435.208
2608	117.5020	306,454.055
2607	95.1909	248,196.482

Figura 2.2: Esempio di libro di ordini

Tutte queste azioni riassumono quello che può avvenire al tempo T sul mercato. La successione di queste fasi è perfettamente rappresentativa dell'evoluzione di un mercato e del prezzo del bene nel tempo.
Possiamo ora abbandonare l'esempio degli attori nella piazza ed immaginare che:

- gli attori siano sostituiti da operatori del mercato
- i titoli azionari siano sostituiti da unità di cryptovaluta
- la comunicazione non è più verbale o rappresentata da cartelli per ogni attore che indicano prezzo e numero di titoli, ma è presente un registro su cui sono riportate le offerte, esso viene chiamato "libro degli ordini".

Il libro degli ordini è una rappresentazione grafica che ordina tutte le offerte dall'alto verso il basso. In alto sono presenti tutte le offerte di vendita (fila Nord), accompagnate dalle unità di criptovaluta ed ordinate dal prezzo più alto al prezzo più basso. Segue una sezione per riportare il prezzo di mercato. Infine vengono riportate tutte le offerte di acquisto (fila Sud) dal prezzo più alto al prezzo più basso. Si può osservare un esempio di libro di ordini in figura 2.2. Una modifica dell'offerta comporta un aggiornamento dei valori riportati e l'eventuale riposizionamento dell'offerta.
Ogni scambio, acquisto o vendita, verrà effettuato utilizzando come controparte l'offerta di acquisto più alta (A) o l'offerta di vendita più bassa (V), perchè più convenienti. Infine l'aggiunta di un'offerta comporterà il suo posizionamento nella colonna.

2.1.3 Come acquistare o vendere

Dopo aver presentato il modello di mercato a libro d'ordini ed il suo funzionamento, indico come si può acquistare o vendere concretamente nei servizi di cambio.
Per poter effettuare un acquisto o una vendita è necessario utilizzare un "ordine".
Gli ordini si distinguono in ordini di acquisto ed ordini di vendita. Un'altra importante classificazione riguarda le tre modalità con cui è possibile acquistare o vendere.

- **Ordine a mercato**

  Un ordine a mercato permette di eseguire l'acquisto o la vendita senza specificare un prezzo.
  L'ordine sarà eseguito istantaneamente a prezzo di mercato, quindi utilizzando come controparte le offerte sul libro degli ordini.

  Consideriamo ad esempio il mercato Ethereum/dollaro. Quindi l'evoluzione del prezzo di 1 Ether (criptovaluta della rete Ethereum) in dollari, sinteticamente rappresentato con ETH/USD. Ipotizziamo che:
  il prezzo di mercato di Ether è 1210 dollari (1210 ETH/USD); la prima offerta di acquisto è a 1205 dollari, per 3 ETH; la prima offerta di vendita è a 1220 dollari,

per 2 ETH.
Inserendo un ordine a mercato di acquisto per 1 Ether, si otterrà 1 ETH per 1220 dollari e la prima offerta di vendita diverrà un'offerta di vendita a 1220 dollari per 1 ETH.
Nel caso in cui l'offerta di vendita fosse stata per 1 ETH l'offerta sarebbe stata rimossa (perché soddisfatta) lasciando posto alla successiva, ad esempio un'offerta di vendita a 1225 dollari, per 2 ETH).

In questo esempio ho voluto considerare lo slippage (la differenza tra la prima offerta di acquisto e la prima offerta di vendita) per completezza. In genere, nei migliori servizi di cambio, lo slippage è trascurabile. Per questo, nei prossimi esempi, ipotizzerò che lo slippage sia nullo e farò riferimento direttamente al prezzo di mercato (il prezzo dell'ultimo scambio avvenuto) invece di considerare la prima offerta di vendita e la prima offerta di acquisto disponibili. Esse saranno infatti ad un prezzo molto vicino al prezzo di mercato.

- **Ordine limite**

  Un ordine limite permette di eseguire l'acquisto o la vendita indicando il prezzo. Ciò significa che, perchè l'ordine sia eseguito, sarà necessario attendere che il mercato raggiunga il prezzo indicato.

  Ad esempio, se il prezzo di mercato di ethereum in dollari (ETH/USD) è 1200 e si inserisce un ordine limite di acquisto a 1100 per 2 ETH, quest'ultimo verrà eseguito solo nel caso in cui il prezzo di ethereum raggiunga i 1100 dollari. Fino a quel momento l'ordine rimarrà attivo ed ineseguito.

  Il libro degli ordini è costituito da ordini limite ineseguiti. Le varie offerte di acquisto e di vendita non sono altro che ordini limite di acquisto e di vendita ineseguiti. Quindi, al momento di inserimento di un ordine limite di acquisto a 1100 per 2 ETH (con prezzo di mercato 1200 ETH/USD) questo verrà inserito nel libro degli ordini accompagnato dalla quantità (probabilmente tra ordini di acquisto a 1101 e ordini di acquisto a 1099).

- **Ordini condizionati**

  L'ultima modalità di acquisto rappresenta gli ordini condizionati. Si tratta di ordini più complessi, generalmente utilizzati per attività di trading.
  Questi ordini permettono di eseguire ordini a mercato o ordini limite nel caso in cui avvenga una determinata condizione. Generalmente questa condizione è il raggiungimento da parte del mercato di un certo prezzo.
  Questa tipologia di ordini viene spesso utilizzata per semi-automatizzare l'attività di trading (quindi non è necessario essere presenti nel momento esatto in cui il

prezzo raggiunge un livello per eseguire operazioni) oppure per avere la garanzia di una perdita massima su un'operazione di acquisto (se il mercato scende più del 10% la cryptovaluta viene venduta automaticamente).

2.1.4 Alcuni servizi di cambio

Il modello a libro di ordini è utilizzato da tutti i servizi di cambio più importanti, sia che trattino valute tradizionali sia criptovalute.
Riporto di seguito alcuni dei servizi di cambio di cryptovalute più importanti: Binance, Coinbase, Huobi, Crypto.com, FTX, Gemini [15]. I servizi tra i più longevi sono The Rock Trading (italiano), Bitstamp, Bitfinex, Kraken.

2.2 Servizi di cambio decentralizzati

Grazie alla blockchain Ethereum ed all'emergere della finanza decentralizzata (dall'anno 2022) una diversa tipologia di servizi di cambio si è presentata sul mercato.
I servizi di cambio decentralizzati sono piattaforme che offrono il servizio di scambio di criptovalute, analogamente ai servizi classici, ma senza la presenza di una struttura aziendale alle spalle. Sono anche chiamati "Exchange decentralizzati" ed abbreviati con la sigla DEX (Decentralized Exchange).

Decentralizzazione Il concetto di Decentralizzazione è un elemento chiave nella comprensione della differenza tra servizi di cambio tradizionali e decentralizzati.
In tutte le situazioni umane in cui è necessaria un'interazione tra più soggetti, di diversa natura, e con interessi contrapposti sorge il problema di come trasmettere le informazioni. La soluzione attualmente utilizzata è quella di un intermediario umano, in genere un'azienda o un'organizzazione terza, che si pone come garante della comunicazione.
I soggetti partecipanti si fidano dell'intermediario, spesso lo pagano per il lavoro che svolge, ed in questo modo l'interazione ha successo.
Con la nascita della tecnologia blockchain emerge la possibilità di certificare e rendere immutabile l'informazione. Di conseguenza si propone di sostituire l'intermediario umano (che può sbagliare, può essere corrotto, ed è in una posizione di potere) con un software che segue determinate regole, concordate da tutti i soggetti, e registra le comunicazioni in modo immutabile sulla blockchain.
Questo software verrà eseguito su una blockchain che, per definizione, esegue operazioni in modo decentralizzato; di conseguenza le scelte non sono prese da un singolo server ma dalla moltitudine di nodi che partecipano alla rete.
In questo caso si parla di sistema decentralizzato, quando la gestione non dipende da un intermediario ma da un sistema in cui partecipano una moltitudine di soggetti distinti.

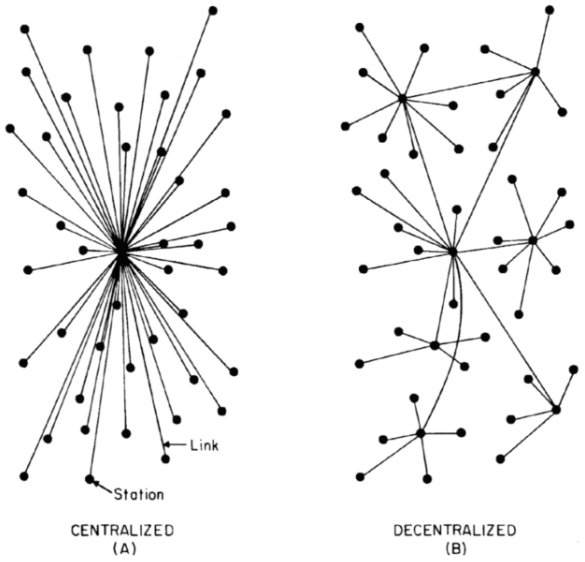

Figura 2.3: Sistema centralizzato vs sistema decentralizzato (Fonte: Dzone)

Quindi per ottenere un servizio di cambio decentralizzato è necessario individuare una rete blockchain da utilizzare, ad esempio Ethereum, e produrre il software necessario ad effettuare gli scambi richiesti.
Questo software verrà caricato sulla blockchain ed eseguito ad ogni utilizzo del servizio di scambio, in più ogni operazione dovrà essere registrata sulla blockchain.
La ricerca sui servizi di cambio decentralizzati si concentra sulla produzione di smart contracts che siano il più possibile efficienti e funzionali allo scambio di criptovalute.

Capitolo 3

EtherDelta

Già dai primi anni di crescita della blockchain Ethereum, nata a Luglio del 2015, iniziarono ad essere sviluppate le prime applicazioni decentralizzate.
Nel Giugno 2016 viene pubblicata theDAO [16], un fondo d'investimento decentralizzato. Questa applicazione ebbe un enorme successo, raccolse infatti 150 milioni di dollari in Ether[1]. Tuttavia, il mese successivo il protocollo venne hackerato e l'entusiasmo iniziale si arrestò.
L'interesse e l'entusiasmo per Ethereum ripresero nel 2017, l'anno del folle aumento di prezzi che fece conoscere la tecnologia blockchain ad un ampio numero di persone. A fine anno la bolla scoppiò e ci fu una lunga e profonda correzione di mercato che terminò solo all'inizio del 2019.
Tuttavia, già dal 2017 nacquero nuovi team intenzionati ad applicare la tecnologia blockchain in diversi ambiti. Nello specifico, le applicazioni più promettenti erano le stablecoin, gli NFT, e la finanza decentralizzata.

La ricerca sulla finanza decentralizzata si concentrava principalmente nella realizzazione di servizi di prestito e finanziamento e su servizi di cambio. Già nel 2017 erano presenti diversi servizi di cambio decentralizzati [17]. Il più utilizzato di questi era EtherDelta [18]. Esso fu lanciato il 12 Luglio 2016 [19] sulla blockchain Ethereum.

3.1 Utilizzo

EtherDelta cercava di replicare i servizi di cambio centralizzati ed implementava il modello di mercato a libro di ordini, standard utilizzato nei servizi tradizionali.
Era particolarmente noto per essere difficile da usare e poco piacevole alla vista, tuttavia fu uno dei primi servizi di cambio decentralizzati degno di nota.

[1] In quel periodo un Ether valeva circa 10 dollari

Per poterlo utilizzare era necessario importare il proprio wallet (inserendo chiave pubblica e chiave privata), connettersi con un wallet esterno oppure crearne uno nuovo e depositare degli Ether. Una volta importato il wallet era necessario depositare il capitale necessario sullo smart contract di EtherDelta tramite il bottone "deposit".
Dopo il deposito era possibile selezionare il token ERC-20 per ottenere il cambio desiderato. I cambi disponibili erano tutti del tipo T/ETH, con T il token ERC-20 selezionato.
Non erano presenti ordini a mercato ma si potevano inserire solamente ordini limite, era quindi necessario specificare la quantità, il prezzo e se l'ordine fosse di acquisto o vendita. In più era necessario specificare il numero di blocchi per i quali l'ordine sarebbe rimasto valido; conoscendo la durata media di chiusura di un blocco si poteva calcolare il numero di blocchi da inserire per ottenere il tempo richiesto. Al termine di questo periodo l'ordine sarebbe stato annullato.
Non era possibile annullare l'ordine una volta inserito ma era necessario attendere la scadenza.

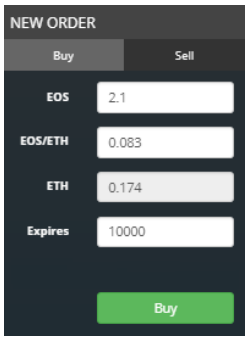

Figura 3.1: ordine limite su EtherDelta (Fonte: Chainbits)

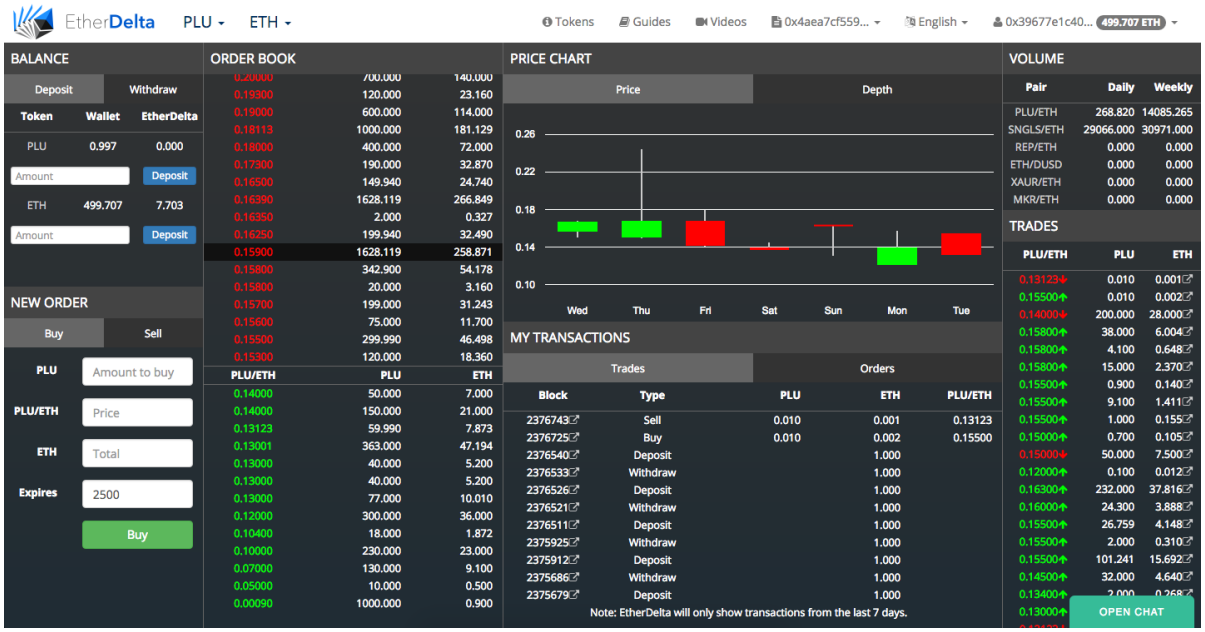

Figura 3.2: Interfaccia di EtherDelta (Fonte: Ethereum Reddit)

3.2 Vantaggi

EtherDelta, anche se poco utilizzato, divenne famoso in pochi mesi grazie alla struttura decentralizzata che lo contraddistingueva. Nonostante lo scarso interesse da parte degli sviluppatori nel realizzare un servizio semplice da usare, EtherDelta fu la dimostrazione che era possibile realizzare un servizio di cambio completamente decentralizzato (quindi indipendente da qualsiasi intermediario), con funzionalità molto simili ai servizi tradizionali.

Un altro vantaggio consisteva nel fatto che, come molti servizi decentralizzati, era permissionless; quindi non era necessaria alcuna autorizzazione all'utilizzo ed in generale non era presente alcun filtro umano. Ciò significa che era possibile, per chiunque possedesse la criptovaluta X, aggiungere un nuovo cambio X/ETH ed inserire ordini sul mercato in attesa della controparte.
Per questo EtherDelta era spesso l'unico servizio di cambio che permetteva di acquistare o vendere criptovalute minori. Esse infatti, erano raramente supportate da servizi di cambio centralizzati perché troppo poco note e non avrebbero generato sufficienti volumi per coprire le spese di aggiunta della criptovaluta.

3.3 Svantaggi

EtherDelta presenta una serie di svantaggi. Oltre alla già citata complessità di utilizzo dell'interfaccia, elenco di seguito alcuni svantaggi strutturali molto importanti:

3.3.1 Commissioni ad ogni azione

Essendo un protocollo completamente decentralizzato ogni azione effettuata deve essere registrata su blockchain; questa operazione ha un costo che dipende dal livello di utilizzo della rete. In generale si tratta di costi fissi non trascurabili.
Questi costi vanno registrati ad ogni azione: deposito dei fondi sullo smart contract di EtherDelta, approvazione di quest'ultimo ed inserimento dell'ordine. Nel caso in cui l'ordine non venga eseguito e si desideri reinserirlo si dovrà pagare un'ulteriore commissione per ogni reinserimento.
Ciò non avviene nei servizi di cambio centralizzati dove è presente una commissione fissa per i depositi ed i prelievi, ed una commissione percentuale sugli scambi effettuati, spesso trascurabile. infine l'inserimento o cancellazione degli ordini è gratuita.

3.3.2 Bassa liquidità

Quando un trader o un investitore, dopo aver scelto la valuta da acquistare, si appresta ad effettuare la scelta del servizio di cambio da utilizzare considera i seguenti fattori:

- commissioni
- slippage (commissioni implicite)
- liquidità

La liquidità è un parametro fondamentale nella valutazione di un mercato. Un mercato si dice "liquido" se gli scambi giornalieri sono alti, al contrario si dice "illiquido" o "poco liquido" se gli scambi giornalieri sono bassi.
Il parametro comunemente utilizzato è il volume: numero razionale che rappresenta la somma di tutti gli scambi per unità di tempo. Se, ad esempio il giorno G, sul servizio di cambio A, nel cambio ETH/USD, si registrano:

- una vendita di 2 ETH a 1300 USD
- un acquisto di 1 ETH a 1250 USD
- un acquisto di 3 ETH a 1300 USD

Il volume giornaliero del cambio ETH/USD (sul servizio di cambio A, il giorno G) sarà di 3850 dollari (oppure di 5 Ether).

Un investitore che ha la necessità di acquistare 20 Ether difficilmente utilizzerà questo cambio. Probabilmente cercherà un cambio con volumi giornalieri che siano almeno il doppio della quantità di Ether che desidera acquistare. Maggiore è il rapporto tra il volume giornaliero e l'importo che si vuole scambiare minore sarà l'impatto dello scambio stesso sul prezzo di mercato. Se il rapporto è troppo alto si rischia di allontanarsi troppo dal prezzo di mercato a causa del proprio stesso acquisto (o vendita), ottenendo così un prezzo sfavorevole.
La scelta di utilizzare il volume di mercato per valutare la liquidità di un cambio è in realtà un'approssimazione. Il parametro che incide direttamente sull'operatore di mercato è il numero di Ether presenti nel libro degli ordini ed il prezzo a cui gli ordini sono impostati.
Ipotizziamo che il prezzo di mercato di ETH/USD sia 1200 e che il libro degli ordini sia popolato nel seguente modo:

offerte di vendita

20 ETH	a	2000
3 ETH	a	1900
1 ETH	a	1300
2 ETH	a	1250

prezzo di mercato: 1200

offerte di acquisto

2 ETH	a	1150
8 ETH	a	1100
20 ETH	a	1000

Un operatore A che desidera acquistare 20 ETH non trova di fronte a sé un cambio sufficientemente liquido. Inserendo un ordine a mercato di acquisto per 20 ETH utilizzerà come controparte le offerte di vendite presenti. Quindi acquisterà 2 Eth a 1250 dollari, 1 Eth a 1300, 3 Eth a 1900 ed i rimanenti 14 Eth a 2000. Il prezzo di mercato si aggiornerà da 1200, 1250, 1300, 1900 fino a 2000 e rimarrà presente sul libro degli ordini un'offerta di vendita di 6 ETH a 2000 dollari.
A avrà così acquistato 20 ETH ma ad un prezzo di 1875 dollari. Infatti
$2 * 1250 + 1 * 1300 + 3 * 1900 + 14 * 2000/20 = 1875$.
Sul cambio attuale il prezzo di mercato è 2000 dollari ma su tutti gli altri cambi ETH/USD (in altri servizi di cambio) sarà rimasto a 1200. Ciò significa che A ha acquistato 20 Ether a 1875 dollari sebbene il prezzo di mercato globale sia 1200 dollari. Possiamo quindi dire che il costo di utilizzo di un cambio poco liquido per A è stato di (1875-1200)*20= 13500 dollari, su un acquisto complessivo di 37500 dollari, parliamo quindi del 36Su un cambio molto più liquido A avrebbe potuto acquistare 31 ETH con lo stesso capitale (37500/1200=31,25).

A avrebbe anche potuto decidere di utilizzare un ordine limite ed attendere che venisse eseguito. Avrebbe quindi inserito un ordine di acquisto a 1199 per 20 ETH.
Possiamo ipotizzare, in base al libro di ordini presentato, che il volume giornaliero sia di 5 Ether.
Con un volume giornaliero di questo tipo, ipotizzando che il 50% dei volumi giornalieri derivino da acquisti ed il restante 50% da vendite, A avrebbe dovuto attendere 8 giorni per poter vedere completato l'ordine. Ciò è vero solo ed esclusivamente nel caso in cui il prezzo di Ethereum non fosse salito nel frattempo.
Questo dimostra come un cambio con poca liquidità rende estremamente costoso o difficoltoso lo scambio ed è un forte disincentivo all'utilizzo.

EtherDelta sia per la complessità di utilizzo, sia perché è nato in una fase prematura per la finanza decentralizzata ha sempre presentato cambi poco liquidi. Questo ha comportato un forte disincentivo, specialmente per gli operatori di mercato con più capitali.

3.3.3 Assenza di market makers

Market makers

Ho già utilizzato il termine "market makers" per identificare gli attori di mercato che operano tramite ordini di tipo limite, in contrapposizione ai "market takers", coloro che utilizzano ordini a mercato. Questa classificazione ha finalità teoriche, infatti la distinzione tra gli operatori di mercato non è netta ma la maggior parte di questi agisce sia da market maker sia da market taker a seconda delle esigenze, utilizza quindi entrambe le tipologie di ordini.

In questa sezione e nelle prossime, con il termine "market makers" farò riferimento ad un altro concetto, che ha comunque alcune relazioni con il concetto precedente. Purtroppo nel linguaggio comune viene utilizzato lo stesso termine, ritengo corretto riprenderlo, anche per semplificare eventuali approfondimenti del lettore.
Sebbene ritengo sia corretto distinguere i due concetti, la polisemia del termine market makers è da ricondurre ad una contestualizzazione teorica e pratica. La prima accezione, illustrata in precedenza deriva da una distinzione teorica. La seconda accezione è di carattere pratico. Questo perché nei servizi di cambio tradizionali, oltre ad acquirenti e venditori sono presenti anche entità terze che si occupano di "portare la liquidità" rendendo di conseguenza efficiente il cambio in questione. Esse impersonano acquirenti e venditori, inserendo, cancellando e modificando ordini limite, ed eseguendo ordini a mercato in modo da generare scambi fittizi.

Queste entità sono i market makers: fondi d'investimento o aziende finanziarie che dispongono di grandi liquidità. Con l'esecuzione di scambi fittizi riescono a garantire agli utilizzatori del cambio un prezzo vantaggioso.
In questa accezione pratica gli utenti sono i market takers, coloro che "fanno uso del mercato" mentre i market makers si occupano di "fare i prezzi", in altre parole portano la liquidità. Tuttavia il termine "market takers" è raramente utilizzato in questo senso ed è principalmente utilizzato in riferimento all'accezione teorica.
Grazie ai market makers gli utenti meno esperti e gli attori di mercato che operano con capitali non ingenti possono effettuare scambi senza doversi preoccupare della liquidità del cambio. Saranno infatti i market makers a fare da controparte per gli scambi nel caso in cui questa non sia naturalmente presente sul mercato.
Esistono una serie di market makers [20], il più famoso (anche se non è il leader di mercato) è Alameda Research [21]. Fondata da Sam Bankman Fried, fondatore di FTX, servizio di cambio di criptovalute (centralizzato) emergente degli ultimi anni.

I market makers sono pagati dal servizio di cambio per il lavoro svolto. Dovendo fare da controparte agli utenti, acquistano e vendono la valuta regolarmente

e sono quindi esposti alle oscillazioni di mercato, potendo riportare delle perdite. Per poter rimanere in attivo mantengono uno slippage (differenza di prezzo tra il primo ordine di acquisto ed il primo ordine di vendita) concordato con il servizio di cambio. In questo modo, se sul cambio ETH/USD il prezzo è 1300, il primo ordine di acquisto sarà a 1290 ed il primo ordine di vendita sarà a 1310. Poiché il prezzo di mercato è 1300 il market maker tratterrà 10 dollari per ogni Ether acquistato o venduto.
In più, i market makers effettuano spesso attività di arbitraggio. Effettuare attività di arbitraggio significa sfruttare le inefficienze di mercato per equilibrare i prezzi. Se, ad esempio, su un servizio di cambio americano 1 Ether quota 1200 dollari, ed allo stesso istante, in un servizio di cambio giapponese il prezzo di Ether è 1300 dollari è possibile acquistare 10 ETH a 1200 dollari sul primo cambio e vendere 10 ETH a 1300 dollari sul secondo cambio. Il profitto totale sarà di 1000 dollari ($10 * 1300 - 10 * 1200 = 1000$).
Con l'attività di arbitraggio, l'applicazione dello slippage e la remunerazione ricevuta dal servizio di cambio i market makers coprono le eventuali perdite dovute all'attività di fornitura di liquidità e sono remunerati per il loro servizio.

Figura 3.3: Cambio senza market makers (Fonte:Dexalot)

Cambio senza market makers

In assenza del market maker gli utenti non troveranno sempre una controparte ma dovranno attendere che questa sia presente naturalmente sul mercato. Nei cambi più noti come ETH/USD e BTC/USD, se il servizio di cambio scelto è molto utilizzato potrebbe non essere facile notare la differenza.
In tutte le altre situazioni risulterà difficile trovare la controparte per il proprio

Figura 3.4: Cambio con market makers (Fonte: Kucoin)

ordine ad un prezzo ragionevole, anche se l'ordine è di piccola entità.
Quello che si può fare in pratica è evitare di utilizzare ordini a mercato ed inserire un ordine limite sperando che questo venga eseguito in un tempo ragionevole.

Nelle immagini 3.3 e 3.4 è riportato il grafico a candele del cambio AVAX/USDT in due servizi di cambio diversi: il primo è un servizio di cambio senza market makers, il secondo presenta market makers. I due grafici fanno riferimento allo stesso periodo temporale. Si può ben vedere come nel secondo caso sono sempre presenti scambi ad ogni istante, mentre nella prima immagine sono riportati solo gli scambi effettivi. E' quindi molto improbabile trovare una controparte in breve tempo in un mercato senza market maker.
Il grafico a candele è un tipo di grafico più informativo rispetto a quello lineare. Quest'ultimo riporta, per ogni unità di tempo (nell'esempio per ogni ora) il prezzo al termine dell'unità di tempo. Il grafico a candele riporta invece quattro informazioni per unità di tempo: il prezzo iniziale, quello finale ed il minimo ed il massimo; dà quindi più indicazioni sul movimento fatto dal mercato.

Motivi dell'assenza di market makers

E' importante sottolineare che l'assenza di market makers su EtherDelta dipende da diversi fattori. In primo luogo dalla presenza di commissioni ad ogni inserimento e cancellazione di ordine ed in secondo luogo dal fatto che i cambi con poca liquidità e pochi volumi portano a poche opportunità di arbitraggio e minori profitti dallo slippage, determinando un bassissimo incentivo per i market makers.

Questo incentivo non poteva essere colmato da EtherDelta in quanto non era presente un budget dedicato. In ogni caso è importante evidenziare che questi costi sarebbero stati comunque difficilmente sostenibili da parte di un protocollo di questo tipo.

3.4 Conclusioni

EtherDelta è stata la prima dimostrazione che è possibile realizzare un servizio di cambio completamente decentralizzato. Tuttavia, con l'arrivo della competizione, le difficoltà di utilizzo divennero determinanti.
In più gli svantaggi indicati quali: costi ad ogni azione, bassa liquidità (quindi impossibilità soddisfare ordini importanti), oltre che assenza di market makers, assolutamente necessari in un servizio di cambio a libro di ordini, lo resero un servizio molto costoso e poco efficiente. Di conseguenza non vide mai un forte incremento di utenti o di volumi. In più, in seguito ad alcune complicanze legali del founder, multato per gestione di un servizio di cambio privo di licenze [22]; il progetto è stato abbandonato a fine 2018, e non ha potuto godere della crescita della Finanza Decentralizzata, iniziata nel 2020.

Capitolo 4

Uniswap

In concomitanza con il "fallimento" di EtherDelta, a Novembre 2018 [23] viene lanciato un nuovo servizio di cambio decentralizzato: Uniswap [24].
Uniswap propone un modello di mercato completamente diverso dal precedente, il modello ad "automated market maker", spesso abbreviato con AMM. Esso, a differenza del modello a libro di ordini, non è perfettamente rappresentativo di un mercato reale ma apporta alcune semplificazioni. E' quindi in un certo senso limitante perché gli attori hanno meno azioni a disposizione, tuttavia queste semplificazioni permettono di risolvere in gran parte il problema della liquidità. Per questo motivo il nuovo modello di mercato si rivelò il compromesso ideale per lo sviluppo della finanza decentralizzata. Uniswap fu infatti uno degli elementi che ne permise la crescita a partire dall'estate del 2020.

Attualmente il modello ad automated market maker ideato dal team di Uniswap è lo standard per la finanza decentralizzata. La sua diffusione è stata facilitata dal fatto che il codice è open source; con lo sviluppo del settore e l'emergere delle blockchain alternative ad ethereum sono nati innumerevoli servizi di cambio che riutilizzavano il codice e personalizzavano la parte grafica, i cosiddetti "fork".
Attualmente su Uniswap avvengono circa il 60% degli scambi presenti su Ethereum [25] e più del 35% degli scambi sull'intera finanza decentralizzata [26]; i fork sono più di 220 [27].

4.1 Utilizzo

L'interfaccia di Uniswap è molto semplice ed intuitiva. Raggiunto il sito ci si ritrova sulla pagina "scambia" e come si può vedere dall'immagine 4.1, è presente una semplice interfaccia con quattro elementi. I due bottoni a destra riportano le criptovalute coinvolte nello scambio mentre le due caselle di testo sulla sinistra conterranno la quantità di criptovaluta coinvolta nello scambio.

Dopo aver selezionato il secondo token (il primo token preselezionato è Ether) è possibile impostare la quantità che si desidera scambiare e verrà mostrato, in base al prezzo di mercato, il numero di token che si otterranno. Lo scambio avverrà dalla valuta in alto verso la valuta in basso. Quindi, seguendo l'esempio dell'immagine 4.2, stanno per essere scambiati 0,03 Ether per 81,34 usdt (stablecoin legata al dollaro). Cliccando sul bottone "Scambia" viene inviata la transazione al proprio wallet e dopo una semplice azione di conferma, la transazione viene effettuata. In questo caso ci sarà una vendita di Ethereum per usdt. Per effettuare un acquisto è sufficiente cliccare sulla freccia centrale che invertirà le due valute e permetterà di scambiare 81,34 usdt per 0,03 Ether.

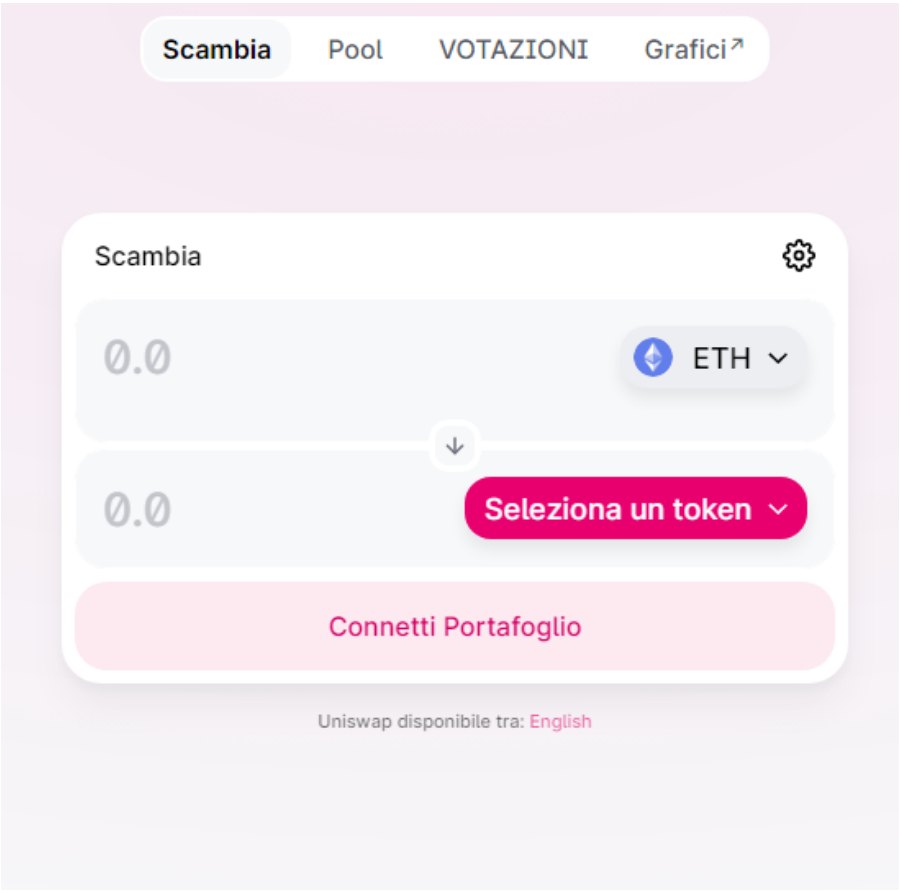

Figura 4.1: Interfaccia Uniswap iniziale

L'operazione di scambio è quindi molto semplice, e l'interfaccia è intuitiva e facile da utilizzare. E' interessante notare che per selezionare il cambio di mercato è sufficiente scegliere la coppia di criptovalute desiderate e che per specificare se l'ordine è di acquisto o vendita è sufficiente scambiare la posizione delle due criptovalute.

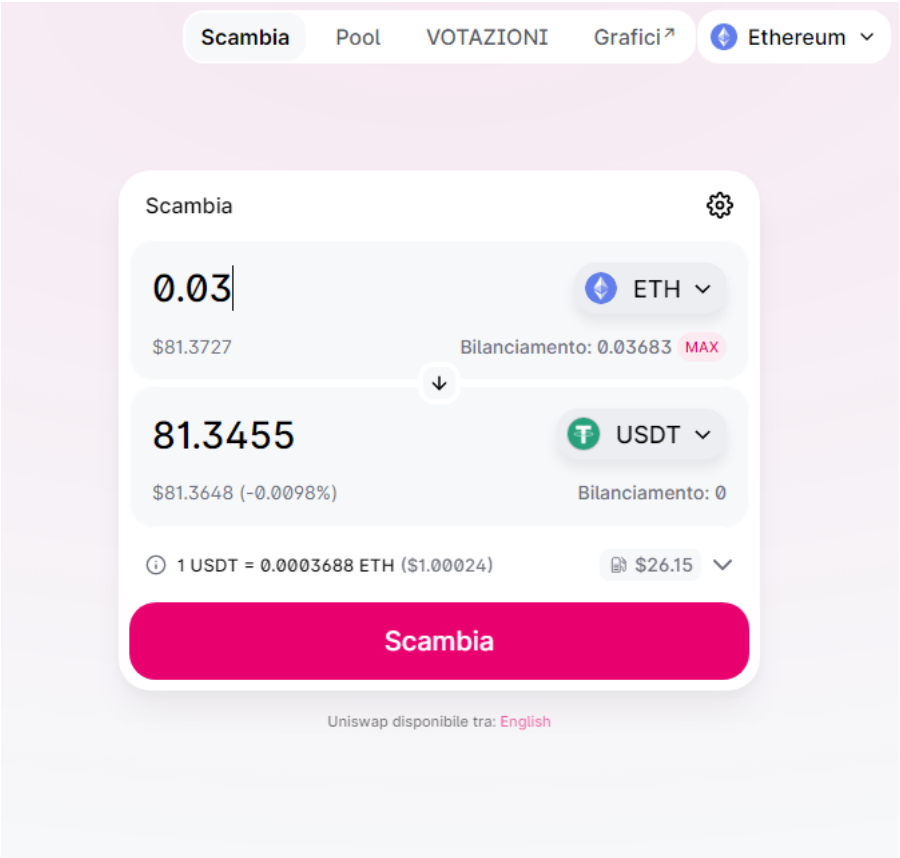

Figura 4.2: Interfaccia Uniswap pre scambio

Un altro aspetto importante è che non sono presenti ordini di tipo limite, non è infatti in alcun modo possibile indicare il prezzo a cui si desidera acquistare o vendere, è possibile specificare solo la quantità che si desidera scambiare. Questo perché il modello di mercato ad AMM permette solamente ordini a mercato.

4.2 Automated Market Makers (AMM)

4.2.1 Intuizione

Come analizzato nel capitolo X, le criticità che impedirono lo sviluppo di EtherDelta derivavano sia dalla complessità di utilizzo della piattaforma (quindi erano in buona parte migliorabili) che da caratteristiche intrinseche della blockchain e della situazione di mercato. In particolare, svantaggi come la necessità di dover pagare una commissione per ogni inserimento o modifica di un ordine di tipo limite e l'altissimo costo di impiego di market makers (con la conseguente impossibilità di disporne) sembravano essere vincoli

insormontabili. Dipendevano infatti dalla struttura della blockchain (ogni interazione ha un costo) e dal fatto che i volumi di scambio erano ridotti (perché la finanza decentralizzata doveva ancora vedere la prima crescita sostanziale).

Di fronte a questi limiti apparentemente insuperabili, l'intuizione fu agire sul modello di mercato. Passando ad un modello più semplice che permettesse di risolvere le due criticità prima citate.
Poiché queste ultime (commissioni ad ogni modifica di ordine limite ed assenza di market makers) si traducono nella difficoltà di fornire una controparte agli utenti del servizio di cambio, si pensò ad un nuovo modello di mercato in cui la controparte fosse creata artificialmente, la cosiddetta "piscina di liquidità". Nello specifico, siccome non era possibile disporre di market makers professionisti, in quanto troppo costosi in questa situazione, si decise di permettere a chiunque di fare da market maker mettendo a disposizione la propria liquidità in cambio di un incentivo. Quest'ultima sarebbe stata utilizzata per riempire la piscina di liquidità che agisce da controparte per gli utenti. In questo modo i due attori di mercato non sono più market takers e market makers ma utenti e fornitori di liquidità.

4.2.2 Modello di mercato

Presento di seguito la struttura del modello di mercato analizzando quali sono gli attori, come cambia lo stato del modello durante uno scambio ed in che modo viene calcolato il prezzo di mercato.

- **Attori di mercato**

  In questo nuovo modello si distinguono gli utenti ed i fornitori di liquidità.

  Gli utenti sono operatori di mercato che utilizzano Uniswap per acquistare o vendere criptovalute.

  I fornitori di liquidità sono operatori di mercato che forniscono liquidità al protocollo. Per ogni cambio presente su Uniswap (ETH/USD, BTC/USD, ETH/BTC, ecc) ci sarà una corrispondente piscina di liquidità che conterrà entrambe le valute. Il fornitore di liquidità depositerà una o entrambe le criptovalute nella piscina corrispondente ed in cambio otterrà il 100% delle commissioni generate dal cambio in questione. In genere le commissioni sono una percentuale del volume scambiato (ad ogni scambio degli utenti viene trattenuta una piccola percentuale).
  Se più fornitori di liquidità contribuiscono a riempire una piscina le commissioni generate dal cambio verranno divise in proporzione alla liquidità fornita da ciascuno.

- **Funzionamento**

  In questo paragrafo andrò a descrivere esattamente come avviene uno scambio. Ricordo che in questo modello di mercato è possibile eseguire solamente ordini a mercato.

  Ipotizziamo che A voglia acquistare 2 Ether con dollari. Nella piscina di liquidità sono presenti 20 Ether e 10000 dollari. Una volta selezionato il cambio ETH/USD, ed inserito 2 Ether potrà sempre concludere lo scambio a meno che non abbia dollari a sufficienza.
  Supponiamo che il prezzo ETH/USD sia 1000, A otterrà 2 Eth in cambio di 2000 dollari. La piscina, a seguito dello scambio, conterrà 18 Ether e 12000 dollari.
  Questo è il funzionamento di un modello ad automated market makers. Viene utilizzata la piscina di liquidità come controparte in modo da poter eseguire gli scambi in modo istantaneo.

- **Determinazione del prezzo di mercato**

  Per definizione il prezzo di mercato del cambio A/B è il prezzo dell'ultimo scambio avvenuto sul cambio A/B.
  In questo modello la determinazione del prezzo di uno scambio avviene in modo algoritmico. Questa è un'ulteriore semplificazione derivante dall'assenza di ordini di tipo limite.

  Nel modello a libro di ordini il prezzo dello scambio viene deciso dal "market maker" quindi colui che ha inserito l'ordine limite che è stato utilizzato come controparte dal "market taker" per effettuare lo scambio. Nel modello ad automated market maker il prezzo di scambio è determinato algoritmicamente e dipende dal numero di token restituiti dal protocollo.

  Se, ad esempio, il prezzo ETH/USD è 2000 ed A desidera vendere 3 Ether, il numero X di dollari necessari allo scambio sono determinati dal protocollo e non dal fatto che un attore di mercato sia disposto ad acquistare 3 Ether ad X dollari. Ipotizziamo che X sia uguale a 5850. Avremo quindi che il prezzo di scambio è stato 5850/3=1950, quindi il prezzo di mercato del cambio ETH/USD è 1950.
  Il numero X di dollari da restituire all'utente in cambio di 3 Ether viene determinato in base ad una proprietà Z. Questa proprietà asserisce che il numero di token A ed il numero di token B presenti nella piscina di liquidità, sia sempre uguale ad una costante K, detta invariante.
  Al variare della proprietà Z si ottengono diverse tipologie di automated market maker, con diverse caratteristiche, che analizzerò nela sezione seguente.

4.3 Tipologie di automated market makers

Dopo aver introdotto Uniswap ed il modello di mercato ad automated market maker, analizzo le principali soluzioni utilizzate nella finanza decentralizzata andando a definire la proprietà Z.
Oltre alle soluzioni presentate in questo lavoro sono state analizzate in letteratura diverse varianti raccolte nel documento [28].

Nelle sezioni successive andrò a considerare un generico cambio A/B (con A e B due criptovalute) di un servizio di cambio decentralizzato che utilizza AMM.
nA è il numero di criptovalute A nella piscina di liquidità, nB è il numero di criptovalute B nella piscina di liquidità e K è l'invariante, il termine che deve rimanere costante ad ogni scambio di token A e B.

Descriverò la proprietà, mostrando in che relazione si trovano le due variabili nA ed nB, in seguito mostrerò la curva della funzione, utile a comprendere il comportamento. Proseguirò analizzando con un esempio cosa accade ad uno scambio e terminerò analizzando vantaggi e svantaggi della proprietà considerata e della tipologia di AMM risultante.

4.3.1 AMM a somma costante

Un automated market maker con la seguente proprietà determina un AMM a somma costante:

$$nA + nB = K \tag{4.1}$$

E' possibile realizzare una curva sul piano cartesiano ponendo nA=x ed nB=y ed ottenendo

$$x + y = K$$

$$y = K - x$$

Ciò che accade, riscontrabile anche dalla curva ottenuta, è che la somma delle unità di criptovaluta presenti nel pool di liquidità deve rimanere costante. Quindi nA+nB=K. Ciò significa che vendendo x A si otterranno esattamente x B.
Ipotizziamo che nA = 10, nB = 10, avremo che K = 20.
Un operatore M desidera vendere 3 A per B. Per fare in modo di mantenere l'invariante è necessario restituire la stessa quantità di B ad M.
Formalmente:

$$(nA + 3) + (nB + X) = K$$

$$(10 + 3) + (10 + X) = 20$$

$$13 + 10 + X = 20$$

$$X = 20 - 23 = -3$$

Il nuovo nB sarà $10 + (-3) = 7$. Nella piscina saranno presenti 13 A e 7 B ed M venderà 3 A per ottenere 3 B.
Possiamo quindi concludere che il prezzo del cambio A/B sarà sempre 1. Infatti, per come abbiamo definito il prezzo di mercato su AMM e per poter mantenere la proprietà è necessario, in ogni situazione, restituire lo stesso numero di criptovalute depositate.

Questa tipologia di AMM presenta quindi la forte limitazione di non poter rappresentare prezzi diversi da 1, di conseguenza è difficilmente utilizzabile se non per coppie di stablecoin.
Un altro svantaggio molto importante è la possibilità di svuotare la piscina di liquidità e rendere in seguito impossibile eseguire lo scambio in quanto non sono presenti più criptovalute A o B.
Se, seguendo l'esempio precedente, M desidera vendere 13 A invece di 3 A la situazione finale è la seguente: M ottiene 10 B in cambio di 10 A e non riesce a completare l'ordine; in più nella piscina sono presenti 20 A e 0 B. Non è quindi più garantita la possibilità di vendere A per B (ma è ancora possibile acquistare A con B).
Per quanto riguarda i fornitori di liquidità è possibile depositare in ogni momento criptovaluta A, B o entrambe, evitando così lo svuotamento della piscina. Tuttavia non c'è alcuna garanzia che operatori terzi forniscano liquidità ed il rischio di avere un cambio non utilizzabile da un istante all'altro non è accettabile. Questo svantaggio è estremamente grave ed è il principale motivo per cui questa tipologia di AMM non è utilizzata nella finanza decentralizzata.

4.3.2 AMM a prodotto costante

Un'altra tipologia è l'automated market maker a prodotto costante. Esso è definito dalla seguente proprietà:

$$nA * nB = K \tag{4.2}$$

E' possibile realizzare una curva sul piano cartesiano ponendo $nA = x$ ed $nB = y$ ed ottenendo

$$x * y = K$$

$$y = K * 1/x$$

La curva ottenuta è la parte positiva di un'iperbole equilatera. La presenza di asintoti è una proprietà importante che approfondirò in questa sottosezione.

Osservando cosa accade a seguito di uno scambio consideriamo $nA = 10$ e $nB = 10$, ed avremo che $K = 100$.

Ipotizzando che l'operatore M desideri vendere 2 A per B il numero di criptovaluta B ottenuto è X definito come:

$$(nA + 2) * (nB + X) = K$$

$$(10 + 2) * (10 + X) = 100$$

$$12 * (10 + X) = 100$$

$$120 + 12X = 100$$

$$12X = -20$$

$$X = -1,67$$

Avremo quindi che M otterrà 1,67 B a seguito di una vendita di 2 A.
Il prezzo del cambio A/B è 1,67/2=0,83.
A seguito dello scambio nella piscina ci saranno 12 A e 8,33 B.

In caso di acquisto, quindi l'operatore M desidera acquistare A depositando 2 B otterrà Y A.

$$(nA + Y) * (nB + 2) = K$$

$$(10 + Y) * (10 + 2) = 100$$

$$(10 + Y) * 12 = 100$$

$$120 + 12Y = 100$$

$$12Y = -20$$

$$Y = -1,67$$

M otterrà quindi 1,67 A con un pagamento di 2 B. Avremo quindi che il prezzo del cambio A/B è 2/1,67=1,19.
Quindi nella piscina ci saranno 8,33 A e 12 B.

Possiamo quindi osservare che ad ogni acquisto avviene un aumento del prezzo del cambio A/B ed in modo speculare, ad ogni vendita, avviene una discesa del prezzo del cambio A/B.
Allo stesso modo si può osservare come al crescere dell'importo scambiato l'impatto sul prezzo è maggiore. In più, la suddivisione di un ordine in N ordini minori non modifica in alcun modo l'impatto sul prezzo dello scambio. Una vendita di 5 A e 5 vendite di un A hanno lo stesso impatto sui prezzi e sull'operatore.
Inoltre, un altro aspetto molto importante è osservabile dalla presenza dei due asintoti della curva in figura n.X. Questi ci mostrano come non sia possibile rimuovere completamente una delle due criptovalute dalla piscina.

La curva può essere interpretata nel seguente modo: ogni punto rappresenta uno stato del cambio e della piscina dove la coordinata x riporta il numero di criptovaluta A e la coordinata y il numero di B.
Ipotizzando di partire dal punto (10,10), come nell'esempio, a seguito di una vendita (consideriamo 2 A per riprendere i valori del primo esempio) arriveremo ad uno stato in cui saranno entrati 2 A nella piscina e fuoriusciti 1,67 B. Saremo quindi al punto (12,8.33). Con una vendita si percorre la curva verso destra, perché il numero di A nella piscina aumenta ed il numero di B diminuisce. Con un acquisto ci si sposta verso sinistra perché avviene il contrario.
Si può quindi osservare che non si potrà mai arrivare ad una situazione in cui i token A o B terminano. Questo perché il prezzo crescerà o si ridurrà infinitamente impedendo lo svuotamento della piscina e garantendo che il cambio rimarrà sempre disponibile agli utenti.

Uno svantaggio di questa tipologia di AMM deriva dal fatto che al crescere del numero di criptovaluta che si desidera scambiare, ed in particolare al crescere del valore dell'ordine lo slippage aumenta.
Nel modello a libro di ordini abbiamo definito slippage la differenza tra la prima offerta di acquisto e la prima offerta di vendita. In questo modello, lo slippage coincide con la variazione di prezzo che avviene ad ogni scambio. Come abbiamo visto ad ogni scambio avviene un cambiamento di prezzo, questo cambiamento è maggiore al crescere dell'importo. Di conseguenza lo slippage è crescente. Da questa inefficienza nasce anche il problema del "front running" che non approfondirò in questo lavoro.

Per quanto riguarda i fornitori di liquidità, rispetto alla soluzione a somma costante in questo caso è necessario rispettare alcuni vincoli. Il primo fornitore di liquidità andrà a creare la piscina e potrà scegliere in che rapporto inserire i due token. In questo modo stabilità il prezzo di partenza del cambio.
Inserendo ad esempio 5 A e 10 B imporrà un prezzo di partenza del cambio A/B di 2. Da questo momento potranno iniziare gli scambi da parte degli utenti, che andranno ad influenzare l'equilibrio della piscina e di conseguenza il prezzo del cambio. I successivi fornitori di liquidità, nell'aggiungere le criptovalute A e B dovranno rispettare il cambio corrente. Se ad esempio, nella piscina le criptovalute sono diventate 7 A e 8 B, il prezzo sarà 1,14 A/B e tutti i fornitori di liquidità dovranno inserire A e B in modo da mantenere il rapporto, evitando così di agire sul prezzo del cambio.

4.3.3 StableSwap

l'AMM a prodotto costante è il più utilizzato sul mercato mentre il modello a somma costante non è utilizzato. Tuttavia il secondo modello di AMM più diffuso è il cosiddetto "stableswap" [29], ovvero "cambio per stablecoin". Esso è l'unione del modello a somma

costante e del modello a prodotto costante.

Questo modello, introdotto da Curve, un servizio di cambio molto importante, trova la sua applicazione in tutti i cambi di mercato in cui le criptovalute A e B hanno lo stesso prezzo o replicano lo stesso bene. Più nello specifico vengono utilizzati per cambi di mercato in cui A e B sono due differenti stablecoin che replicano il valore della stessa valuta. Questo tipo di cambio viene utilizzato dagli utenti per passare da una stablecoin all'altra. Contrariamente a quanto ci si può aspettare questo tipo di servizio è molto richiesto nella finanza decentralizzata [9].

La proprietà che deve essere rispettata in uno stableswap è la seguente:

$$x * (nA + nB) + (nA * nB) = x * K + (K/n)^n \tag{4.3}$$

Analizzando la formula di può vedere una componente dell'AMM a somma costante $nA + nB = K$ moltiplicata per un fattore x e la componente del'AMM a prodotto costante $nA * nB = C$, con $C = (K/n)^n$.
Il grafico nell'immagine riporta la proprietà dello stableswap in blu, la proprietà a somma costante in giallo e la proprietà a prodotto costante in viola.

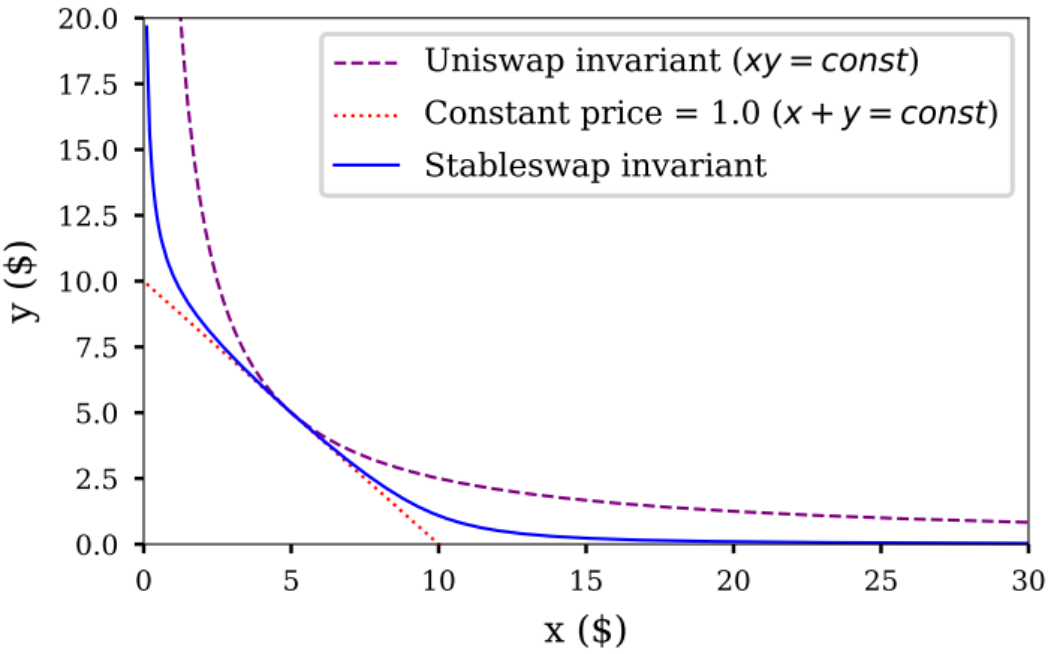

Figura 4.3: Curva di uno stableswap (Fonte: Curve)

L'obiettivo dello stableswap è quello di ottenere un AMM a somma costante nel momento in cui i prezzi sono equilibrati per poi passare ad un AMM a prodotto costante nel caso in cui il prezzo di sbilanci eccessivamente.
In questo modo si può sfruttare il basso slippage di un AMM a somma costante fino a che i prezzi sono corretti. Nel momento in cui avviene una forte vendita o acquisto che porta a sbilanciare molto i rapporti nella piscina di liquidità, entra in gioco la parte di AMM a prodotto costante che rende impossibile l'esaurimento di una delle due criptovalute.
Nel caso in cui il fattore x è zero si ottiene un AMM a prodotto costante. al crescere del fattore x aumenta l'importanza della componente di somma rispetto alla componente di prodotto andando a ridurre lo slippage.
L'opportuna parametrizzazione del fattore x permette di ottenere l'effetto descritto nelle righe precedenti e mostrato nell'immagine 4.3.

4.4 Caratteristiche AMM

In questa sezione andrò a concludere il capitolo sul modello di mercato ad automated maker makers analizzando vantaggi e svantaggi dello stesso. Questa analisi sarà effettuata sulla variante a prodotto costante: soluzione utilizzata da Uniswap e più diffusa sul mercato.

4.4.1 Vantaggi

Il vantaggio principale è senza dubbio la semplicità di utilizzo derivante sia dal modello di mercato semplificato sia dall'interfaccia estremamente intuitiva, contenente pochi e chiari elementi.

Altro vantaggio importante è la risoluzione delle problematiche riscontrate da EtherDelta e dipendenti dal modello di mercato utilizzato: commissione ad ogni azione e assenza di market makers.
Non essendo presenti ordini di tipo limite, le azioni possibili sono ridotte all'acquisto e alla vendita. Queste azioni hanno sempre avuto un costo e comportano un beneficio diretto: lo scambio. Per questi motivi l'utente non ha più la sensazione di pagare troppe commissioni.
L'assenza di market makers viene risolta dalla piscina di liquidità. Saranno quindi i fornitori di liquidità a rendere liquido il cambio permettendo scambi agevoli per gli utenti.

Poiché chiunque può diventare fornitore di liquidità, il servizio di cambio offre una duplice funzionalità: permettere lo scambio di criptovalute e permettere il deposito di criptovalute in cambio di una rendita. Questa rendita deriva dalle commissioni generate

dal cambio corrispondente alla piscina di liquidità in cui sono stati depositati i fondi. Su Uniswap le commissioni sono lo 0,3% di ogni scambio.

4.4.2 Svantaggi

I vantaggi illustrati nella sezione precedente hanno permesso la crescita di Uniswap e lo sviluppo della finanza decentralizzata. Tuttavia, apportando una semplificazione al modello di mercato classico, si presentano anche una serie di svantaggi.

Come più volte riportato non è possibile eseguire ordini di tipo limite. È solamente possibile acquistare o vendere a prezzo di mercato.

La determinazione dei prezzi in modo algoritmico risulta essere una forte limitazione in alcune situazioni. Nel modello ad AMM il cambiamento di prezzo dipende dalla quantità di criptovaluta acquistata e venduta e non da una libera scelta del mercato.
Nel modello di mercato a libro di ordini il cambiamento di prezzo non dipende solamente dagli scambi che avvengono sul mercato ma anche dalla modifica degli ordini limite. Ricorro ad un esempio per analizzare questa fattispecie. Ipotizziamo che il cambio ETH/USD al tempo T riporti il seguente libro degli ordini:

offerte di vendita

2 ETH	a	1650
3 ETH	a	1600
1 ETH	a	1550

prezzo di mercato: 1500

offerte di acquisto

2 ETH	a	1450
4 ETH	a	1400

Al tempo T+1 non è avvenuto alcuno scambio ma gli ordini sono stati modificati, alcuni sono stati cancellati ed altri sono stati aggiunti. Il libro degli ordini è nel seguente stato:

offerte di vendita

5 ETH	a	2200
1 ETH	a	2100
2 ETH	a	2050

prezzo di mercato: 1500

offerte di acquisto

2 ETH	a	1850
6 ETH	a	1800
4 ETH	a	1750

Il passaggio illustrato dagli esempi è perfettamente legittimo in quanto dal tempo T al tempo T+1 possono avvenire N modifiche degli ordini.
Il prezzo di mercato è ancora 1500 perché rappresenta il prezzo dell'ultimo scambio. Tuttavia possiamo dedurre che il prossimo scambio avverrà a 2050 dollari o a 1850. In più, tale scambio non deve necessariamente nascere da un operatore reale ma potrebbe essere semplicemente un'operazione fittizia svolta dal market maker per riequilibrare i prezzi. In questo caso verrà effettuato un ordine a mercato con la minima quantità di Ether disponibile.
Ho quindi mostrato come è possibile modificare il prezzo di mercato senza effettuare scambi.
In genere gli scambi sono sempre presenti, grazie ai market makers, tuttavia può accadere che a seguito di notizie importanti o per semplici dinamiche di mercato il numero di persone disposte a vendere cala drasticamente. Riprendendo l'esempio, nessuno vuole vendere Ether a 1500 dollari. Di conseguenza la maggior parte dei venditori decide che venderà solo a 2000/2100 dollari. In questo modo la variazione del prezzo di mercato non dipende solo da scambi ma principalmente dai "market makers", intesi come coloro che inseriscono ordini di tipo limite.

Analogamente a quanto anticipato nella sottosezione 4.3.2, un altro svantaggio derivante dalla scelta algoritmica dei prezzi riguarda lo slippage, che è crescente al crescere dell'importo scambiato.
Maggiore è la quantità di criptovaluta scambiata, maggiore è il divario tra nA e nB, e maggiore sarà lo spostamento lungo la curva (immagine n.X) determinando un aumento del prezzo pagato dell'utente.
In un modello a libro di ordini, la dimensione dell'ordine non determina sempre un alto slippage. Infatti, se il mercato è sufficientemente liquido, quindi sono presenti sufficienti ordini limite che agiscono da controparte (vicino al prezzo di mercato) l'ordine potrà essere eseguito con uno slippage estremamente basso.

Sono presenti svantaggi anche per i fornitori di liquidità. Nel caso dell'AMM a somma costante il prezzo dei token A e B è sempre costante, ciò non accade per i fornitori di liquidità di un AMM a prodotto costante. Vediamolo con un esempio:
Il fornitore di liquidità A deposita 2 Ether e 2000 dollari in un cambio ETH/USD con prezzo di mercato 1000. Il valore depositato è 4000 dollari.
Nel caso in cui il prezzo di Ether diventi 4000 dollari, nella piscina saranno presenti 1 Ether e 4000 dollari. Se A decide di ritirare la liquidità otterrà 1 Ether e 4000 dollari

che equivalgono a 5000 dollari di controvalore.
Ma, nel caso in cui non avesse depositato la liquidità, avrebbe ancora 2 Ether e 2000 dollari per un controvalore attuale di 10000 dollari. Questo mancato profitto è chiamato "impermanent loss" ed è un rischio per il fornitore di liquidità. Esso dipende dal fatto che la liquidità viene utilizzata come controparte dal mercato, quindi in situazioni di forte rialzo o forte discesa una delle due valute verrà ridotta progressivamente in favore dell'altra ed il controvalore complessivo della liquidità si ridurrà. Lo stesso fenomeno avviene anche nel caso in cui Ether scenda perché nella piscina caleranno i dollari ed aumenteranno gli Ether che però valgono meno.

L'impermanent loss è una problematica molto sentita dai fornitori di liquidità in quanto difficilmente viene colmata dalle commissioni derivanti dal cambio. Per questo i protocolli decentralizzati premiano i fornitori di liquidità con altre criptovalute, in modo da aumentare l'incentivo a depositare liquidità sui propri cambi. L'attività di depositare liquidità per ottenere questi incentivi è detta "farming".

Capitolo 5

Soluzione proposta

Dopo aver analizzato EtherDelta, la prima soluzione di servizio di cambio decentralizzato, che utilizzava un modello di mercato a libro di ordini; e la soluzione attualmente più diffusa, il modello di mercato ad AMM; analizzo un ulteriore modello di mercato che trova la sua ideale applicazione in situazioni in cui il cambio A/B è caratterizzato da un basso utilizzo.
Il basso utilizzo di un cambio può dipendere sia dal fatto che una delle due criptovalute presenti sia caduta in disuso e non c'è più alcun interesse ad effettuare scambi, sia dal fatto che una criptovaluta sia rivolta ad un numero contenuto di utenti. In questo caso, il basso utilizzo non dipende dal successo o dall'adozione della criptovaluta ma dal fatto che la criptovaluta è rivolta ad un target ristretto.
Questa situazione è tipica di alcuni utility token, criptovalute che non hanno finalità di investimento o speculazione ma che consentono l'accesso o migliorano l'utilizzo di un servizio. Se il servizio è rivolto ad una nicchia di mercato, il cambio A/B registrerà comunque pochi scambi rispetto ad un cambio tradizionale, anche se il servizio è di successo.
Questa tipologia di cambio può essere anche definita a bassi volumi o a bassa liquidità; per questo motivo utilizzerò il termine "cambio a bassa liquidità" riferendomi ai cambi illustrati in questo paragrafo. Quindi a tutti i cambi che presentano un basso utilizzo non perché fallimentari ma per via del ristretto numero di possibili utenti.

Tipicamente, nella situazione in cui il cambio è rivolto ad un numero ristretto di utenti il numero di detentori della criptovaluta sarà contenuto, si avrà un numero di scambi ridotto e le commissioni derivanti dagli scambi saranno molto basse. Di conseguenza ci sarà pochissimo incentivo ad essere fornitori di liquidità e la piscina conterrà poca liquidità. Minore è il numero di criptovalute nella piscina maggiore sarà lo slippage derivante da uno scambio perché ci saranno meno criptovalute A o B a disponibili per lo scambio e quindi un maggior rischio di svuotamento. Lo slippage è un disincentivo all'acquisto, di conseguenza ci saranno meno detentori della criptovaluta ed il circolo vizioso riparte

dal punto di partenza.
Si può quindi comprendere come sebbene il modello di mercato ad automated market maker sia un ottimo compromesso per la finanza decentralizzata, caratterizzata da liquidità e volumi inferiori rispetto alla finanza classica; in situazioni di mercato ancora più di nicchia, quindi per cryptovalute riservate a pochi utenti, il modello attualmente utilizzato risulta svantaggioso.
Per questi motivi, in questo capitolo analizzo un ulteriore modello di mercato che si adatta meglio a situazioni di mercato a bassa liquidità.

5.1 Intuizione

Analogamente a quanto evinto nell'analizzare le problematiche di EtherDelta, anche in questo caso risulta che gli svantaggi riscontrati dipendono dal modello di mercato utilizzato. Non è infatti possibile attuare aggiustamenti parziali, come l'aggiunta di vincoli o di parametri, per risolvere il problema mantenendo lo stesso modello di mercato. Per questo è necessario crearne uno nuovo, costruito su misura per le situazioni di mercato a bassa liquidità.

Inoltre, riprendendo l'analogia tra modello a libro di ordini ed il modello ad automated market maker, ci ritroviamo in una situazione in cui è conveniente rinunciare ad alcune efficienze di mercato per ridurre la complessità, che richiede risorse per essere gestita. In altre parole, un modello di mercato ad AMM non è adatto a situazioni di bassa liquidità perché troppo complesso e di conseguenza, troppo costoso da gestire. In assenza di questo "budget"[1] nascono le problematiche riscontrate. Per questo è necessario portare un'ulteriore semplificazione per ridurre la complessità del modello e renderlo funzionale al nuovo contesto individuato.

Osservando il circolo vizioso analizzato nel paragrafo precedente [paragrafo X](prima dell'introduzione) si può osservare come entrano in gioco tutti gli attori: utenti e fornitori di liquidità.
L'intuizione di questo nuovo modello di mercato, seguendo l'esigenza di un'ulteriore semplificazione, consiste nel rimuovere uno dei due attori: i fornitori di liquidità, ed automatizzare ulteriormente la gestione della liquidità e la scelta del prezzo.

Non avendo trovato in letteratura un nome condiviso in riferimento al modello presentato, nelle sezioni seguenti farò riferimento a questo modello di mercato con il termine "preset market maker" o PMM. Infatti in questo modello, l'attività di market making intesa come scelta dei prezzi è predefinita. Nel modello a libro di ordini l'attività di

[1] Con "budget" assente si fa riferimento a costi non sostenibili per il mercato. Un esempio può essere l'assenza di fornitori di liquidità disposti a riempire la piscina.

scelta dei prezzi viene eseguita dagli operatori di mercato che utilizzano ordini di tipo limite, quindi i market makers (nell'accezione teorica) sono gli utenti.
Nell'automated market maker i prezzi vengono scelti automaticamente dal protocollo in base agli scambi avvenuti.
Nel preset market maker la scelta dei prezzi rimane automatizzata ma è definita a priori in base al numero di criptovaluta in circolazione.

5.2 Preset market maker

Dopo aver descritto le problematiche del modello ad AMM in situazioni di bassa liquidità ed aver esposto i motivi per cui risulta necessario ideare un nuovo modello di mercato, entro nel merito della soluzione proposta, il preset market maker. Di seguito presento la struttura del modello, descrivo come si utilizza dal punto di vista dell'utente ed analizzo il suo funzionamento.

- **Attore**

  E' presente una sola tipologia di attore di mercato, l'utente. Esso può utilizzare il servizio di cambio per acquistare o vendere A per B. Non sono presenti fornitori di liquidità.

- **Utilizzo**

  Considero il cambio A/B che permette acquisto o vendita di criptovaluta A per criptovaluta B. Gli utenti possono interagire con il cambio A/B solo tramite ordini a mercato. E' quindi sufficiente inserire la quantità di criptovaluta A da scambiare e specificare se si desidera acquistare o vendere, dopodiché il cambio preleverà o consegnerà la quantità di criptovaluta B necessaria.
  L'utilizzo è molto semplice, come nel modello ad AMM.

- **Funzionamento**

  Sebbene l'utilizzo è analogo al modello precedente la struttura ed il funzionamento del cambio sono differenti.
  Non è più presente la classica piscina di liquidità, contenente i token A e B, ma sono presenti due piscine, una per ciascuna criptovaluta. Ci sarà quindi la piscina A, che contiene tutte le criptovalute A del cambio, ed una piscina B, che contiene tutte le criptovalute B del cambio. Se ad esempio esistono 1000 unità di A, 400 possono essere nel cambio A/B, 200 nel cambio A/C e le restanti 400 sono sul mercato, quindi non sono depositate nello smart contract del cambio ma sono nei

portafogli degli utenti.

Alla creazione del cambio A/B il gestore del servizio di cambio andrà a depositare criptovaluta A e B nelle rispettive piscine. Dopo la creazione sarà ancora possibile aggiungere A o B, oppure prelevarle, ma solo per il creatore del cambio.
In seguito, un utente che desidera utilizzare il cambio A/B per un acquisto di A, fornirà il numero di criptovalute B richiesto dal prezzo di mercato ed otterrà A. Le criptovalute A ottenute provengono dalla piscina A, le criptovalute B depositate andranno ad aggiungersi alla piscina B. In caso di vendita il funzionamento è speculare.
Per ogni scambio la controparte è svolta dalle due piscine.

Riporto un esempio:
L'operatore di mercato M desidera vendere 2 ETH utilizzando il cambio ETH/USD. Il prezzo di mercato è 1000, quindi 1 Ether vale 1000 dollari. La piscina ETH contiene 10 Ether, la piscina USD contiene 5000 dollari.
M inserirà un ordine di vendita a mercato per 2 Ether ed una volta eseguito l'ordine riceverà i 2 Ether, dopo aver depositato i dollari.
Il cambiamento di prezzo, quindi il numero di dollari che M deve depositare, dipende da una curva predefinita. Questa curva indica il prezzo in funzione del numero di criptovalute A emesse dal cambio. Approfondiremo questo aspetto nella sezione X.

Dal funzionamento illustrato si può facilmente capire che una delle due piscine può essere svuotata. Non c'è infatti alcun vincolo nella scelta della funzione che descrive il prezzo a disincentivare o rendere impossibile lo svuotamento di una delle due piscine, cosa che accade nell'AMM a prodotto costante.
Ipotizziamo, per semplicità e senza perdere in generalità, che la curva che descrive il prezzo sia una costante, quindi il prezzo di mercato del cambio ETH/USD è sempre 1000. Ed ipotizziamo che la piscina ETH contenga 10 ETH e che la piscina USD contenga 10000 dollari. Se un operatore di mercato M desidera acquistare 10 ETH la piscina ETH verrà svuotata. Mentre la piscina USD conterrà 20000 dollari. Non sarà quindi più possibile effettuare un ulteriore acquisto di ETH.

5.3 Emissione di nuova criptovaluta

La situazione in cui questo modello di mercato risulta essere vantaggioso è l'implementazione di un servizio di cambio che offra scambi di criptovalute destinate a mercati ristretti, quindi per situazioni di mercato a bassa liquidità.

Tuttavia, poiché è comunque necessario che il gestore del servizio di cambio depositi criptovaluta A e B nelle piscine, è importante specificare un'ulteriore premessa nella quale contestualizzare questo modello. La situazione di emissione di una nuova criptovaluta.
In assenza di questa premessa la soluzione proposta potrebbe non essere vantaggiosa, proprio perché la creazione del cambio ha un costo corrispondente al valore di criptovaluta A e B da depositare nelle piscine. Questa quantità deve essere in linea con i volumi di scambio attesi e può non essere indifferente.

Se una o più persone vogliono creare una nuova criptovaluta, generalmente necessaria ad accedere ad un servizio, sorge il problema di come creare il primo cambio di mercato. Questo permetterà l'acquisto della criptovaluta agli investitori ed agli utenti del servizio. Se il servizio in questione si rivolge ad un numero di utenti ristretto la soluzione migliore è utilizzare un servizio di cambio che implementi il modello di mercato a preset market maker.

Una volta che è stata creata la criptovaluta A sarà necessario scegliere la criptovaluta B con cui permettere lo scambio. Ipotizzando che la criptovaluta si chiami TOK, il cambio creato potrà essere TOK/USD, TOK/BTC, TOK/ETH ecc. Generalmente non c'è la necessità di creare più di un cambio, soprattutto per i progetti piccoli. Se infatti è disponibile solo il cambio TOK/ETH ma un utente desidera acquistare la criptovaluta con BTC potrà effettuare lo scambio BTC/ETH su un servizio di cambio centralizzato. In questo modo otterrà ETH e potrà effettuare l'acquisto tramite il cambio TOK/ETH sulla finanza decentralizzata.

Ipotizziamo che il creatore abbia scelto di creare il cambio TOK/ETH e che sono stati creati 10000 TOK in totale, quindi la fornitura totale di TOK è 10000 unità. Di questi, 2000 vengono trattenuti dal creatore ed i restanti 8000 sono destinati alla vendita sul mercato.
Il creatore, dopo essersi recato su un servizio di cambio che implementa PMM (preset market maker) potrà creare il cambio TOK/ETH e riempire le piscine. Depositerà quindi 8000 TOK nella piscina relativa ma dovrà lasciare la piscina ETH vuota. In questo modo un utente potrà utilizzare il cambio TOK/ETH solo ed esclusivamente per acquistare TOK. Se infatti la piscina ETH è vuota non ci sono ETH disponibili per lo scambio; in altre parole non è presente la controparte e per questo le vendite sono disabilitate.
Tuttavia, l'impossibilità di vendere non è un'anomalia ma è perfettamente in linea con le logiche di mercato. Infatti nessun utente detiene TOK perché sono tutti nella piscina e nel portafoglio del creatore.
Al primo scambio l'operatore M acquista un numero N di TOK. Gli Ether utilizzati per l'acquisto andranno nella piscina ETH ed gli N TOK ottenuti proverranno dalla piscina TOK. Con il susseguirsi degli acquisti la piscina ETH si riempirà e sarà quindi possibile utilizzare il cambio TOK/ETH in entrambe le direzioni: acquisto e vendita.

E' stata quindi effettuata l'emissione della nuova criptovaluta TOK.

Tutte le analisi e le considerazioni fatte di seguito saranno riferite alla situazione di immissione di nuova criptovaluta, e non a situazioni in cui la criptovaluta sia già presente sul mercato o sia già stata distribuita agli utenti tramite transazioni su blockchain.

5.4 Curva del prezzo

Come già anticipato, in un modello di mercato a preset market maker sarà presente una curva, più precisamente una funzione, che descrive l'andamento del prezzo in funzione al numero di criptovaluta A presente sul mercato. Il prezzo sarà quindi strettamente legato al numero di criptovalute A in circolazione e questo permette di avere un controllo importante sul futuro prezzo della criptovaluta.

La curva del prezzo è una funzione F che ha come dominio l'insieme $[0, T]$ e come codominio l'insieme reale $[0, +\infty]$, dove T è il numero massimo di criptovalute TOK presenti sulla piscina (nell'esempio precedente 8000).
$y_0 = F(x_0)$ sarà il prezzo in ETH di TOK con x_0 il numero di TOK in circolazione sul mercato, quindi il numero di TOK venduti dal momento del lancio.

Per quanto riguarda tipologia di funzione F utilizzabile non sono presenti particolari vincoli se non il fatto che questa funzione deve essere coerente con le dinamiche di mercato.
La legge della domanda e dell'offerta prevede che il prezzo di un bene limitato, nel caso in cui la domanda sia costante, cresce al diminuire dell'offerta e cala all'aumentare dell'offerta. Avrebbe quindi poco senso utilizzare una funzione non crescente (che quindi è strettamente decrescente in un intervallo del dominio), come quella illustrata in figura [X].

Come si può osservare dall'immagine, la funzione è strettamente decrescente nell'intervallo $X = [1000, 3000]$. Ciò significa che se sono presenti sul mercato da 1000 a 3000 TOK, il prezzo scende in continuazione ad ogni acquisto. Questo chiaramente è un controsenso in quanto la domanda di TOK è crescente ma il prezzo diminuisce.
Inoltre, andando ad osservare ciò che accade a livello granulare, quindi da un acquisto al successivo, accadrà che l'operatore di mercato M che desidera acquistare TOK, dopo aver effettuato l'acquisto vedrà un calo di prezzo invece di un aumento. Questo perché il prezzo di mercato mostrato al momento dell'acquisto si riferisce, per definizione, all'acquisto precedente. Quindi solo a seguito dell'acquisto si aggiorna il prezzo di mercato considerando lo scambio appena avvenuto.
Lo slippage, analogamente al modello AMM, sarà la differenza tra il prezzo di mercato al momento dell'acquisto ed il prezzo di mercato aggiornato, quindi quanti ETH M paga

per un TOK.
Per concludere, l'unico vincolo imponibile alla curva del prezzo è che sia crescente.
Non è necessario che sia strettamente crescente, infatti non è anomalo il fatto che il prezzo rimanga stabile a seguito di un acquisto. Questa situazione è percepita anche nei servizi di cambio a libro di ordini, più efficienti e meglio rappresentativi delle dinamiche di mercato. Infatti, nel caso in cui lo slippage è minimo ed il cambio è molto liquido l'utente non osserva un movimento di prezzo a seguito del proprio acquisto.

Dopo aver mostrato il vincolo della non decrescenza riporto le principali soluzioni di curva dei prezzi. Queste permettono un processo di market making[2] coerente con le logiche di mercato.

5.4.1 Funzione costante

Una curva dei prezzi caratterizzata da una funzione costante del tipo:

$$y = k, \text{ con } k > 0 \tag{5.1}$$

In questo caso il prezzo del cambio A/B sarà sempre k, indipendentemente dal numero di criptovaluta A in circolazione.
Questo tipo di curva è perfetta per un cambio di stablecoin, ad esempio USDT/USDC, due stablecoin che replicano il prezzo del dollaro [30][31].
In tutte le altre situazioni non risulta essere una scelta sensata tuttavia è un primo esempio utile a comprendere meglio il funzionamento della curva.

5.4.2 Retta

L'utilizzo di una retta risulta essere una soluzione semplice e ragionevole, la curva sarà del tipo:

$$ax - y + c = 0, \text{ con } a >= 0, \ c > 0 \tag{5.2}$$

o espressa come funzione:

$$y = ax + c, \text{ con } a >= 0, \ c > 0 \tag{5.3}$$

In questo modo si avrà una crescita lineare del prezzo al crescere del numero di criptovaluta presente sul mercato. Ciò è corretto perché rispetta le logiche di domanda e offerta.

Alcune considerazioni importanti sui parametri:
Un valore corretto di a è nell'intorno di 1, quindi poco maggiore o poco minore di 1. Una retta con pendenza molto alta ($a > 2$) risulterebbe difficilmente sostenibile ed il

[2] inteso come scelta dei prezzi

prezzo mostrato dal cambio PMM risulterebbe troppo distante dal valore reale della criptovaluta.
Un valore molto piccolo ($a < \frac{1}{4}$) potrebbe anche in questo caso non essere una soluzione coerente con il mercato. Tuttavia è importante specificare che queste considerazioni sono di carattere generale; la scelta del parametro a ideale è fortemente dipendente dal prezzo del cambio A/B. Se il prezzo è 10000 una valore di a corretto è 1; se il prezzo è 1 o minore una valore di a corretto potrebbe essere 1/100.
Il parametro c rappresenta il punto di intersezione della retta con l'asse delle y ed in questa situazione è il prezzo di partenza del cambio A/B. c quindi non potrà essere 0 altrimenti l'acquisto della prima criptovaluta A sarebbe gratuito e non avrebbe senso.
Oltre a ciò non sono presenti altri vincoli, se non quelli già imposti su a e c dalla definizione 5.3.

5.4.3 Funzione a tratti continua crescente

Un'ulteriore soluzione corretta e coerente con le logiche di mercato ma più complessa di una retta è una funzione a tratti crescente del tipo:

$$y = \begin{cases} k & \text{per } x \in [0, x_1[\\ x + c & \text{per } x \in [x_1, x_2[\\ \log_b x + d & \text{per } x \in [x_2, +\infty[\end{cases} \tag{5.4}$$

$$\text{con } k > 0,\ c \neq 0,\ b > 1,\ d > 0$$

$$\text{con } f(x_1)^- = f(x_1)^+,\ f(x_2)^- = f(x_2)^+$$

Quindi la funzione deve essere continua su tutto il dominio R_0^+.

Utilizzando una funzione a tratti si ha modo di gestire diversamente il cambiamento del prezzo in base alle fasi di utilizzo della criptovaluta. Nell'immagine n.[X] sono stati dati dei valori ai parametri k, c, b e d per poter avere un esempio concreto e comprendere come evolverà il prezzo nel tempo.
La funzione F[1.2 es - num con il label] è definita su tutto il dominio R_0^+ ma in modo distinto su tre intervalli $[0, x_1]$, $[x_2, x_2[$, $[x_2, +\infty[$. Nell'immagine anche $x1$ e $x2$ sono stati definiti.
Nel primo intervallo, da 0 a 2000 TOK, sul mercato il prezzo è costante, quindi per gli utenti che acquistano in questa fase non c'è alcun vantaggio tra chi acquista prima o chi acquista dopo, infatti il prezzo è sempre lo stesso. Terminati i 2000 TOK il prezzo inizia a salire linearmente fino a 5000 TOK in circolazione, quindi chi aveva acquistato nel tratto precedente può realizzare un profitto andando a vendere TOK. Nell'ultimo tratto c'è un aumento logaritmico del prezzo di TOK all'aumentare della domanda. In questo modo si tende ad evitare che il prezzo salga al di sopra di alcuni valori o comunque che

cresca rapidamente.

E' importante specificare che la funzione F[1.2 es - num con il label] non rappresenta tutte le possibili funzioni a tratti ma vuole essere un esempio per comprendere le potenzialità della curva dei prezzi a tratti. Essa potrebbe anche essere composta da due o più di tre intervalli e contenere solo tratti composti da rette, o in generale prima un tratto logaritmico e poi un tratto lineare, ecc. Non sono presenti vincoli in questo senso.
Un vincolo che però deve essere rispettato, come indicato nelle condizione della funzione F[1.2], è la continuità su tutto il dominio. Poiché i vari tratti sono composti da funzioni continue è necessario porre l'attenzione sull'unione tra un tratto e l'altro; questa deve avvenire allo stesso prezzo. In questo modo sono impediti salti improvvisi di prezzo a seguito di un piccolo acquisto, situazione estranea alle dinamiche di mercato.

Si può quindi osservare come, in un modello a PMM si può gestire l'attività di market making in modo previsionale e mirato. Questo permette di ridurre e disincentivare le speculazioni, facili da realizzare e particolarmente impattanti in situazioni di mercato a bassa liquidità. In più, agendo sull'aumento dei prezzi, è anche possibile modellare l'economia della propria criptovaluta nel tempo. Seguendo l'esempio in figura n.[X] è stata definita una fase embrionale, in cui il prezzo non aumenta, una fase di crescita ed una fase di stazionamento o maturità.

5.5 Vantaggi

Di seguito riporto i vantaggi nell'utilizzare un modello di mercato a preset market maker in caso di emissione di nuova criptovaluta per situazioni di mercato a bassa liquidità.

In primo luogo, la semplicità di questo modello porta a ridurre di gran lunga i costi di creazione e gestione del cambio. Inoltre, come già visto nelle sezioni precedenti, il modello ad AMM risulta essere inadatto a queste situazioni.
Tuttavia, un aspetto molto interessante è che a seguito di vendite successive il prezzo diminuisce (in accordo con le logiche di mercato) ma allo stesso tempo diminuisce l'offerta sul mercato. Infatti tutte le criptovalute vendute sono nella piscina del cambio e non sul mercato. In questo modo, nel momento in cui ci sarà un aumento della domanda il prezzo potrà tornare a salire senza particolari problemi.

Nelle situazioni di mercato a bassa liquidità risulta spesso più difficile la stima del numero di utenti che vorranno utilizzare il servizio. Il numero di utenti andrà ad impattare direttamente sulla domanda di mercato che dovrebbe essere coerente con il numero di criptovalute create ed il prezzo iniziale di vendita.
Ipotizziamo che la domanda per la criptovaluta A è 10000 dollari, suddivisa tra 2000

utenti, quindi l'intenzione media di acquisto dell'utente è di 5 dollari. La soluzione ideale sarebbe la creazione di 15000 unità di A e la vendita iniziale di 10000 A (tramite il cambio A/USD) al prezzo di 1 dollaro. Le rimanenti 5000 unità saranno destinate in parte al creatore, ad esempio 2000 e le rimanenti 3000 saranno inserite nella piscina A per ulteriori acquisti.
In questa situazione il creatore di A è riuscito a raccogliere 10000 dollari dalla vendita della propria criptovaluta.
Tuttavia, nella maggior parte dei casi risulta estremamente difficile effettuare una stima adeguata della domanda perché questa dipende da molti fattori. Se la stima è 10000 dollari ma al momento della vendita gli acquisti sono equivalenti a 1000 dollari, essendo presenti 10000 unità sul mercato (secondo la legge di domanda e offerta) il prezzo di A si adeguerà all'offerta raggiungendo valori vicini a 0,1 dollari. Di conseguenza i primi utenti che hanno acquistato A ad 1 dollaro avranno una perdita del 90Tramite il modello a PMM, per via del suo funzionamento, è possibile evitare questo rischio perché l'offerta sarà sempre uguale alla domanda. Se infatti la domanda cresce l'offerta cresce perché vengono vendute più unità; se la domanda diminuisce si arrestano gli acquisti e probabilmente ci saranno delle vendite di A portando ad una riduzione dell'offerta.
Quindi in base alla stima sulla domanda sarà sufficiente creare molte più unità di criptovaluta (10 o 100 volte il necessario) in modo da avere la garanzia che ne sia a sufficienza. Tutte le criptovaluta A invendute non saranno sul mercato ma rimarranno nella piscina A, quindi non contribuiranno ad aumentare l'offerta che impatterebbe negativamente sul prezzo di A.
Il modello di mercato a PMM si adegua alla domanda corrente permettendo una vendita il più possibile efficiente.

Un altro vantaggio molto importante, strettamente legato all'elasticità del modello a PMM nei confronti della domanda di mercato, è la garanzia che non si potrà scendere al di sotto del prezzo iniziale.
Per spiegare questo vantaggio utilizzo la curva dei prezzi a retta in figura n.[X].
Dall'immagine si può osservare come il prezzo di vendita di A è 3 dollari. Questo prezzo sarà accessibile solo per il primo acquisto, all'aumentare degli acquisti il prezzo cresce linearmente. Infatti dopo le prime 1000 unità di A vendute il prezzo sarà 5 dollari; quando le unità sul mercato saranno 5000 il prezzo sarà 13 dollari. Nel caso in cui vengano vendute 4000 A si ritornerà ad un prezzo di 5 dollari, perché le unità di A rimaste sul mercato sono 1000.
Nel caso altre 1000 unità vengano vendute il prezzo tornerà a 3 dollari. Poiché però non sono presenti altre criptovalute A sul mercato non sarà possibile effettuare nuove vendite, quindi il prezzo non potrà mai scendere sotto i 3 dollari.
Questa proprietà è molto interessante e garantisce, in ogni situazione, che il prezzo della criptovaluta A non scenderà mai al di sotto del prezzo di lancio. Questa proprietà vale per tutti i cambi a PMM che presentano una curva dei prezzi non decrescente.

Un ultimo vantaggio che riporto in questa sezione è il costo pressoché nullo della creazione di un nuovo cambio.
Ipotizziamo che una o più persone vogliano creare la criptovaluta TOK. Ne creano 1000 unità di cui 200 destinate al team (o al creatore) ed 800 da vendere sul mercato. Finora il costo è quasi zero, sarà infatti necessario pagare le commissioni di creazione dello smart contract relativo alla criptovaluta.
Per poter mettere sul mercato la criptovaluta TOK e permettere a tutti gli utenti l'acquisto il team potrà affidarsi ad un servizio di cambio a preset market maker. Creerà il cambio TOK/ETH (ad esempio), riempirà la piscina TOK e lascerà vuota la piscina ETH.
In questo caso il costo di lancio è quasi zero, infatti è necessario pagare le commissioni della blockchain per creare lo smart contract della criptovaluta e quello del cambio (poche centinaia di dollari).
Nel caso di un cambio ad automated market maker, sarebbe stato necessario creare il cambio e depositare TOK ed ETH in ugual misura per creare la piscina. Se il prezzo TOK/ETH è 0,1 e si depositano 800 TOK nella piscina è necessario depositare anche 80 Ether. Se un ETH vale 2000 dollari (attualmente 2500) si tratta di 160000 dollari di costi per la creazione del cambio.
Si può quindi ben capire quanto sia conveniente l'utilizzo di un PMM.

5.6 Svantaggi

Dopo aver analizzato i vantaggi nell'utilizzo di un modello a PMM per l'immissione di una nuova criptovaluta analizzo anche gli aspetti negativi.

Uno svantaggio consiste nel fatto di non poter creare un secondo cambio A/C oltre al cambio iniziale A/B. Sebbene non sono presenti vincoli tecnici che ne impediscono la creazione e bene non creare un secondo cambio perché potrebbero facilmente presentarsi anomalie di mercato.
Poiché il modello a PMM è un'importante semplificazione delle dinamiche di mercato funziona bene solo se è l'unico cambio che contiene A. Se infatti fosse presente anche un cambio A/C (o anche A/B), su un altro servizio di cambio che utilizza un modello di mercato a libro di ordini o ad automated market maker (con tutti i problemi di liquidità che questo comporta), potrebbero facilmente presentarsi divergenze importanti di prezzo tra i due cambi. Essendo infatti l'attività di market making del PMM predefinita, si priva il mercato di alcuni gradi di libertà. Nel secondo cambio non sarà presente questa costrizione ed i prezzi seguiranno logiche differenti.
In conclusione si avrebbero ampie divergenze tra i prezzi dei due cambi e la perdita di

alcune importanti proprietà del modello a PMM, rendendolo così poco efficace.

Un secondo svantaggio riguarda lo svuotamento delle piscine. Come già analizzato, seguendo l'esempio di un cambio A/B, la piscina B sarà inizialmente vuota e le vendite di A disabilitate. Tuttavia questo non è un problema perché nessuno, oltre al creatore della criptovaluta, detiene A.
Il vero problema è che la piscina A può essere svuotata nel caso in cui tutte le criptovalute A vengano acquistate ed immesse sul mercato. In quel momento saranno disponibili le vendite di A ma non saranno più disponibili acquisti ed il prezzo del cambio A/B non potrà più salire, anche se la domanda è crescente.
Questa condizione è purtroppo intrinseca al modello a PMM e non è superabile se non con una transizione ad un modello AMM o con un'importante modifica alla struttura della criptovaluta.

Capitolo 6

Conclusioni

La finanza decentralizzata rappresenta attualmente la maggiore applicazione della tecnologia blockchain ed è composta da una serie di applicazioni che offrono servizi finanziari. In questo lavoro è stata analizzata una tipologia di questi protocolli, i servizi di cambio, con particolare interesse al modello di mercato utilizzato.
Il più comune ed intuitivo è il modello a libro di ordini. Esso infatti, è perfettamente rappresentativo della realtà perché descrive ogni interazione che avviene in un mercato reale. Inoltre è il modello utilizzato per implementare tutti i servizi di cambio tradizionali, utilizzati per investire e speculare sui mercati classici.
Per questi motivi EtherDelta, il primo servizio di cambio decentralizzato, implementava il modello a libro di ordini. Questa scelta si rivelò però fallimentare in quanto la struttura della blockchain impone il pagamento di commissioni ad ogni azione. Questo, oltre a determinare un aumento del costi per l'utente rende anche impossibile l'attività dei market makers, fondamentali per portare liquidità e per aumentare l'efficienza dei cambi. In assenza di questi elementi EtherDelta fu destinato al fallimento.
Dopo alcuni anni arrivò Uniswap, un nuovo servizio di cambio che si diffuse raccogliendo enorme successo e contribuendo alla crescita della finanza decentralizzata. Esso si impose grazie ad un nuovo modello di mercato che diventò presto lo standard per i servizi di cambio, l'automated market maker. Questo modello introduce il concetto di piscina di liquidità, una riserva di criptovalute utilizzata come controparte per gli scambi. Grazie a questa intuizione ogni utente poteva effettuare lo scambio anche se non c'era una controparte reale. Questa semplificazione determina anche alcune anomalie di mercato che sono però inferiori ai benefici apportati.
In questo lavoro, dopo aver analizzato i due modelli prima citati, presento un terzo modello poco utilizzato nella finanza decentralizzata che però risulta particolarmente utile in mercati a bassa liquidità ed in particolare per l'emissione di nuova criptovaluta. In questo modello il prezzo è determinato dalla quantità di criptovaluta presente sul mercato. Tale modello permette di risolvere i problemi presentati da un automated market maker in situazioni di bassa liquidità. Inoltre presenta interessanti proprietà come l'impossibi-

lità del prezzo di scendere al di sotto del prezzo di lancio e l'adattamento dell'offerta di criptovaluta alla domanda presente sul mercato.

6.1 Possibili approfondimenti

Alla luce di quanto analizzato in questo lavoro sarebbe interessante approfondire le seguenti tematiche:

- **Impermanent loss:** da dove deriva questa inefficienza e come può essere mitigata, se c'è la possibilità.
- **Defi 2.0:** in che modo i protocolli di nuova generazione propongono di gestire la liquidità nella finanza decentralizzata. Analisi e comparazione delle soluzioni di Tokemak e Solidly

Riferimenti

[1] Aave. https://aave.com/.

[2] Bancor. https://www.bancor.network/.

[3] Syntetix. https://synthetix.io/.

[4] Compound. https://compound.finance/.

[5] acuant. The World's Unbanked Population. November 2020.

[6] Coinmarketcap. Compound. https://coinmarketcap.com/currencies/compound/. relevant information: compounds date of launch.

[7] Mirror. https://www.mirror.finance/.

[8] Sushi. https://www.sushi.com/.

[9] Curve. https://curve.fi/.

[10] 1inch. https://1inch.io/.

[11] Eliza Gkritsi. Funds Lost to DeFi Hacks More Than Doubled to $1.3B in 2021: Certik. January 2022.

[12] Tokemak. https://www.tokemak.xyz/.

[13] Solidly. https://solidly.exchange/swap.

[14] Nexus mutual. https://nexusmutual.io/.

[15] Major cryptocurrencies exchanges. https://coinmarketcap.com/rankings/exchanges/.

[16] Samuel Falkon. The Story of the DAO — Its History and Consequences. December 2017.

[17] TheLuWizz. Uniswap — User-friendly decentralized exchange. January 2021.

[18] Etherdelta. https://etherdelta.com/.

[19] Practical Law Corporate Securities. EtherDelta: SEC Issues First-Ever Enforcement Action Against Digital Asset Trading Platform. November 2018.

[20] Ledgerlink Labs. Top Crypto Market Makers 2021. October 2021.

[21] Alameda research. https://www.alameda-research.com/.

[22] Ana Berman. Multato il fondatore di EtherDelta, per la SEC si tratta di un exchange di security non registrato. November 2018.

[23] Uniswap blog. A short history of Uniswap. February 2019.

[24] Uniswap. https://uniswap.org/.

[25] Dex tracker - decentralized exchanges trading volume. https://defiprime.com/dex-volume. Last updade: 03/01/2022.

[26] Top exchange decentralizzati su coingecko per volume di trading. https://www.coingecko.com/it/dex. Last updade: 03/01/2022.

[27] Defilama.com. Uniswap forks. https://defillama.com/forks/Uniswap. Last updade: 03/01/2022.

[28] Yongge Wang. Automated market makers for decentralized finance (defi). *arXiv preprint arXiv:2009.01676*, 2020.

[29] Michael Egorov. Stableswap-efficient mechanism for stablecoin liquidity. *Retrieved Feb*, 24:2021, 2019.

[30] Tether stablecoin. https://tether.to/en/.

[31] Circle stablecoin. https://www.circle.com/en/usdc.

[32] Andrew Bloomenthal. Market Maker. August 2021.

[33] Miguel Mota. Understanding StableSwap (Curve). July 2021.

[34] Messari. Uniswap Decentralized Exchange - Overview History. February 2022.

[35] Jakub of Finematics.com. History Of DeFi – From Inception To 2021 And Beyond. April 2021.

[36] Anonimus Author. DeFi - All of The Problems, Some of The Solutions. April 2021.

[37] Ian Bezek. Decentralized Finance (DeFi). February 2022.

[38] Rakesh Sharma. Decentralized Finance (DeFi) Definition. February 2022.

[39] Yearn finance. https://yearn.finance/#/home.

[40] Alpha homora. https://homora.alphafinance.io/.

[41] Beefy. https://beefy.finance/.

[42] Autofarm. https://autofarm.network/.

[43] Laurel Tincher. Compound Finance (COMP), Explained. July 2021.

[44] Brady Dale. What Is Yearn? The DeFi Gateway Everyone Is Talking About. September 2020.

[45] Kain Warwick. What Is Synthetix and How Does It Work? December 2020.