LUISS

Dipartimento di Economia e Finanza

Corso di laurea in Banche ed intermediari finanziari

Cattedra: Teoria e Politica Monetaria

DeFi: la Rivoluzione Decentralizzata del Sistema Finanziario

Prof. Giorgio Di Giorgio
RELATORE

Prof. Federico Carlini
CORRELATORE

Lorenzo Stagi
Matr. 754711
CANDIDATO

Anno Accademico 2022/2023

Che questo sia l'inizio di
qualcosa di ancora più grande.
Alla mia famiglia
e a chi mi vuole bene.

Grazie.

Indice

INTRODUZIONE

Nel corso degli ultimi anni la rivoluzione tecnologica ha sancito l'avvento di una nuova era per il sistema finanziario mondiale: quella della finanza decentralizzata, comunemente nota come DeFi (*Decentralized Finance*). Questa innovazione rappresenta una significativa evoluzione dalla finanza tradizionale (TradFi), offrendo un ecosistema in cui i servizi finanziari vengono erogati su piattaforme decentralizzate, eliminando intermediari e creando un sistema più efficiente, trasparente e accessibile.

Il presente lavoro si propone di esplorare in profondità questo nuovo settore, delineando le sue radici, i suoi meccanismi e le differenze e similitudini con la TradFi.

Inizieremo trattando il mondo della finanza tradizionale, tracciando una breve evoluzione storica e analizzando i suoi punti di forza e le sue inefficienze: indagine necessaria per comprendere le motivazioni alla base del crescente interesse per la DeFi.

Il secondo capitolo si concentrerà sull'infrastruttura della DeFi, fornendo una solida comprensione degli elementi fondamentali che la sostengono. Nello specifico esamineremo i presupposti tecnologici, con particolare attenzione alla blockchain, esplorando protocolli di consenso, smart contract e oracoli.

Nel terzo capitolo ci addentreremo nel cuore della DeFi, esplorando i diversi servizi e prodotti finanziari offerti da questo sistema: dalle più importanti piattaforme di prestito come MakerDAO, Compound e Aave, agli scambi come Uniswap, fino ai corrispondenti titoli obbligazionari e derivati. Metteremo in luce i parallelismi e le differenze con la finanza tradizionale, offendo una panoramica delle sfide affrontate, dei rischi associati e delle potenzialità di miglioramento del settore.

Infine ci concentreremo su un’analisi quantitativa del mondo DeFi, esaminando la fiducia degli utenti, il sentiment del mercato, la sua valutazione nel tempo e fornendo un'indagine comparativa tra i tassi d'interesse offerti dalle piattaforme decentralizzate e le banche tradizionali.

La rivoluzione decentralizzata è appena iniziata e questa tesi si pone l'obiettivo di fornire un quadro chiaro e approfondito della DeFi, comprendendone le ragioni della popolarità, la basi teoriche, il funzionamento pratico e le sue implicazioni future per un sistema finanziario più equo, aperto e innovativo.

CAPITOLO 1 - LA FINANZA TRADIZIONALE

1.1 Evoluzione storica

Dal baratto alla DeFi: questo è l'iter che il sistema economico ha compiuto per arrivare ad oggi.

È difficile immaginare un mondo senza denaro, ma questa era la realtà più di ottomila anni fa in cui l'unico sistema di negoziazione conosciuto era il baratto: operazione di scambio diretta di beni e servizi senza l'uso della moneta per soddisfare un bisogno di entrambi le parti. Questo metodo presentava vari limiti, come la cosiddetta "coincidenza dei bisogni" e la difficoltà nel valutare quando una transazione fosse equa. Dapprima si affermò così la moneta merce, cioè oggetti che avevano un certo valore intrinseco e venivano utilizzati come merce di scambio, come ad esempio bestiame, conchiglie rare, metalli. Si pensi allo "shekel" dei Babilonesi e al "pecus" dell'antica Roma, da cui il termine pecunia utilizzato tutt'ora.

Nel 600 a.C. nacque in Lidia (la moderna Turchia), diffusasi poi anche nell'impero greco e romano, la moneta coniata, formata da grumi di argento[1]. Solo stato aveva il diritto di stampare moneta, garantendone così il valore e obbligando i cittadini a riconoscerla come mezzo universalmente accettato[2].

La moneta, perché sia tale, deve essere disponibile, accessibile, durevole, fungibile, portatile e affidabile.[3] In accordo con John Hicks queste caratteristiche possono essere riassunte definendo la moneta come "la moneta è ciò che la moneta fa" e quindi individuare nella famosa "prima triade" le tre funzioni di una moneta[4]:

- Mezzo di pagamento: la moneta è utilizzata per facilitare li scambi, in quanto come abbiamo visto senza di essa dovremmo ricorrere al baratto.
- Unità di conto: il fatto di essere utilizzata negli scambi presuppone che la moneta sia unità di misura del valore di un bene o un servizio.

---

[1] Focus.it. (2022). "Quando è stata inventata la moneta?" https://www.focus.it/cultura/storia/quando-e-stata-inventata-la-moneta.

[2] Raiffeisen.it. "Quando e dove è stato inventato il denaro?" Consultato il 1 luglio 2023. https://www.raiffeisen.it/it/sapere-finanziario/dettaglio/quando-e-dove-e-stato-inventato-il-denaro.html.

[3] CONSOB. Dal baratto alla finanza. Consultato il 1 luglio 2023. https://www.consob.it/web/investor-education/dal-baratto-alla-finanza.

[4] Hicks, J. (1950). *A Contribution to the Theory of the Trade Cycle*. Oxford: Clarendon Press

- Riserva di valore: infine la moneta è un modo per conservare il valore nel tempo. Se una persona riceve moneta in cambio di beni o servizi, può conservare quella moneta e utilizzarla in futuro per acquistare beni o servizi.

Circa nel 700 d.C., probabilmente a causa di una carenza di metalli e per facilitarne il trasporto di grandi quantità, in Cina si iniziò ad usare al posto delle monete dei pezzi di carta: le cosiddette banconote. Per la prima volta veniva utilizzato come mezzo di pagamento un qualcosa che, a differenza delle monete, aveva valore intrinseco nullo e che quindi rappresentava esclusivamente una "promessa di pagamento". Si passò così ad un sistema basato sul credito. Quando nel 1271 Marco Polo visitò la Cina rimase colpito dall'idea e la introdusse agli europei, che nel 1661 in Svezia stamparono le prime banconote europee. Gli europei stavano ormai colonizzando il mondo e le banconote si diffusero in tutto il globo.

La storia degli istituti bancari come enti di finanziamento e deposito si può far risalire nelle antiche civiltà dei Greci e Babilonesi, dove i sacerdoti prestavano il ricavato delle offerte dei fedeli e custodivano ingenti quantità di oro e argento[5]. Con la nascita della moneta nacque in Grecia l'attività di cambiavalute, svolta dai trapeziti (dal nome del tavolo dietro cui sedevano), che lavoravano in prossimità dei porti concedendo anche prestiti. Durante il periodo romano tra il terzo e il secondo secolo a.C., si verificarono importanti sviluppi nel settore bancario. Le città più significative videro la nascita di "banchi", istituzioni autorizzate e controllate dalle autorità pubbliche, che esercitavano attività di prestito e di cambio nel commercio del grano, ma la loro funzione monetaria autonoma era notevolmente ridotta.

Il concetto di banca come lo conosciamo oggi ha avuto origine nel Medioevo in Italia, precisamente a Firenze, Genova e Venezia, dove le famiglie benestanti iniziavano a offrire prestiti ad altri. La famiglia Medici, con il loro Banco dei Medici a Firenze, è forse la più famosa di queste prime banche. Aprì numerose "filiali" in tutta Europa prestando soldi per botteghe, costruzioni o guerre, tanto che il fiorino era diventata una delle monete più usate in tutto il continente.

Con il passare del tempo, le banche si sono evolute da semplici prestatori a complesse istituzioni finanziarie che offrono una vasta gamma di servizi, tra cui depositi di risparmio, prestiti, investimenti e servizi finanziari. Il Banco di San Giorgio, fondato a

[5] Treccani. "banca". http://www.treccani.it/enciclopedia/banca

Genova nel 1407[6], è considerato da molti storici come una delle prime banche moderne. Nel XVII secolo, la Svezia ha fondato quello che è considerato il primo banco centrale, la Riksbank, nel 1668[7]. Ciò ha stabilito un nuovo standard per le banche, portando alla creazione di istituzioni simili in tutto il mondo, che svolgono funzioni chiave nel monitoraggio e nella regolazione dell'economia di una nazione.

Da qui, il sistema di transazioni finanziarie è stato tradizionalmente sovrinteso da banche centrali e altre istituzioni finanziarie che fungono da intermediari fiduciari per facilitare e regolare le transazioni.

Per attribuire un valore reale alla moneta cartacea, nel XIX secolo molti Stati introdussero un regime aureo della moneta nel quale il valore nominale della moneta era pari alle riserve auree dello stato: il cosiddetto *gold standard*. Questo modello permetteva alle banche centrali, Banca d'Inghilterra prima (1884) e negli Stati Uniti poi, di stampare moneta e garantirla con metalli preziosi. Questo regime cessò nel 1971, da quando la maggior parte delle monete del mondo divenne moneta fiat, cioè moneta che non ha valore intrinseco e il cui valore dipende dalla fiducia nei confronti dell'autorità emittente.

Dagli anni '90, con l'avvento del *world wide web* e di tutta la rivoluzione tecnologica connessa, si palesò l'esigenza di creare un sistema che permettesse di effettuare transazioni senza passaggio fisico di denaro: il cosiddetto *e-cash*. Questa forma di moneta rappresenta la digitalizzazione della moneta fisica, che tramite i progressi della tecnologia dell'informazione, viene trasferita da un ambiente tangibile a uno intangibile. L'avvento della fintech ha svolto un ruolo cruciale nell'evoluzione dei sistemi di pagamento, permettendo transazioni più veloci, più sicure e più efficienti. L'*e-money* ha gettato le basi per i successivi sistemi di pagamento digitali, come PayPal, lanciato nel 1999, che utilizzava internet per effettuare pagamenti e trasferimenti di denaro online in maniera semplice ed accessibile. Allo stesso tempo, l'evoluzione della tecnologia mobile ha permesso l'emergere di portafogli digitali e applicazioni di pagamento mobile, come Apple Pay e Google Wallet. Queste soluzioni hanno ulteriormente aumentato la velocità e la convenienza dei pagamenti digitali, rendendo possibile effettuare transazioni con un semplice tocco o scorrimento sullo schermo del telefono.

[6] Treccani. "SAN GIORGIO, banco di." https://www.treccani.it/enciclopedia/san-giorgio-banco-di_%28Enciclopedia-Italiana%29/ .

[7] Sveriges Riksbank. "History". https://www.riksbank.se/en-gb/about-the-riksbank/history/.

Lo scenario cambia nel 2008, con il white paper di "*Bitcoin: a peer-to-peer electronic cash system*", scritto da un individuo o gruppo anonimo, noto come Satoshi Nakamoto, che ha proposto un sistema di "denaro elettronico *peer-to-peer*[8] che usando il concetto di blockchain, che approfondiremo nel prossimo capitolo, eliminava la necessità di un intermediario fiduciario. Con la proposta di Nakamoto è nato un nuovo strumento di pagamento: le criptovalute, che hanno introdotto una nuova era nelle transazioni finanziarie.

1.2 Punti di forza

Prima di trattare l'oggetto specifico del presente lavoro e capire come la decentralizzazione possa aiutare la finanza tradizionale, è importante introdurre il sistema finanziario attuale, al fine di metterne in luce il funzionamento, i pregi e i difetti, e comprendere se un sistema decentralizzato potrebbe integrarsi o persino sostituirlo in determinati aspetti.

La finanza tradizionale (TradFi) è un sistema basato su istituzioni finanziarie come banche commerciali, banche d'investimento, società d'intermediazione e compagnie assicurative che, in cambio dei loro servizi, addebitano una commissione. Queste istituzioni sono società per azioni che fungono da intermediari tra risparmiatori e investitori, e svolgono un ruolo chiave nel facilitare le transazioni, la gestione dei rischi e l'allocazione efficace delle risorse (Figura 1.1).

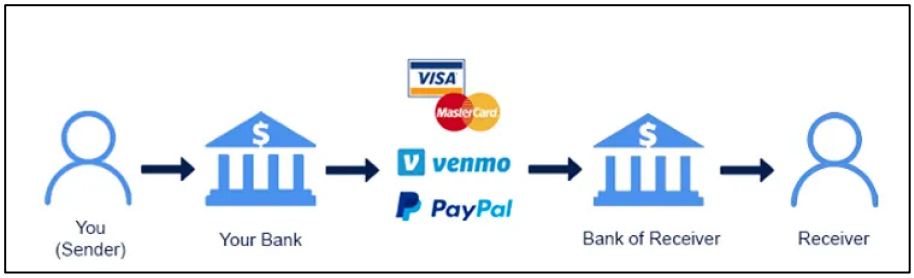


Figura 1.1: Finanza Tradizionale. Fonte: *Medium* (2019).

[8] Il *Peer to Peer Lending* (P2P) è un prestito tra privati, un prestito personale erogato da privati ad altri privati attraverso siti di imprese o enti di social lending, senza passare attraverso i canali tradizionali rappresentati dagli intermediari finanziari autorizzati ai sensi dell'art. 106 del Testo Unico Bancario, il Decreto Legislativo n° 385 del 1993 (banche, società finanziarie, ecc.). (Fonte: borsaitaliana.it)

Questo tipo di sistema finanziario si fonda sulla fiducia che riponiamo, per esempio, in una banca; essa custodisce il nostro denaro con la promessa che ci verrà dato ogni qualvolta dobbiamo effettuare una transazione. Gli intermediari finanziari mettono in collegamento tutti i soggetti economici, tra cui famiglie, aziende e lo Stato, avendo così un ruolo fondamentale nel tessuto economico. La loro efficacia nell'allocare le risorse verso investimenti fruttuosi è un fattore determinante per la crescita economica globale.
Dopo queste brevi considerazioni di carattere generale e storico, passiamo ora ad analizzare i punti di forza del sistema finanziario attuale in modo da cogliere le differenze fondamentali rispetto ad un modello decentralizzato.
Le istituzioni finanziarie tradizionali sono sottoposte a normative rigide e supervisione da parte di enti governativi, il che offre una maggiore sicurezza ai clienti. Cause come la crescente integrazione tra mercati finanziari dei diversi stati, lo sviluppo di nuovi prodotti finanziari e il verificarsi di crisi hanno determinato il cambiamento nella regolamentazione, rendendola più stringente e ponendo una maggiore tutela per il consumatore. Le banche svolgono attività che generano diversi rischi, tra cui il rischio di credito, il rischio di liquidità e il rischio operativo e questi rischi possono mettere a repentaglio la capacità della banca di rimborsare i depositanti e i suoi creditori e la stabilità del sistema finanziario. Pertanto, dal momento che le banche svolgono attività particolarmente rischiose, esse devono essere soggette a regolamentazione e vigilanza.
Fondamentale a questo riguardo è il grado di omogeneità con cui le norme vengono implementate e poi fatte rispettare, come dimostrato da Stati Uniti ed Eurozona. Nei paesi UE, per esempio, il coordinamento e la cooperazione tendono sempre più verso un assetto accentrato di scelte e decisioni comuni, basate su nuove regole e nuove istituzioni. La svolta c'è stata dopo la grande crisi del 2009, che ha messo in evidenza le debolezze delle banche dell'Eurozona e ha messo in luce l'esigenza di armonizzare le regole a livello UE per evitare arbitraggi regolatori ed aumentare la trasparenza. L'unione bancaria, ovvero il trasferimento delle competenze nel campo della vigilanza sulle banche dalle autorità nazionali ad autorità europee ha portato ad un corpus unico di norme prudenziali

armonizzate, il *single rulebook*, che si pone a garanzia di applicazione uniforme delle Regole[9].

Decenni di evoluzione normativa hanno portato quindi ad una infrastruttura giuridica che mette al centro la tutela del soggetto risparmiatore e consumatore in genere in quanto soggetto debole meritevole di tutela. La finanza tradizionale opera in un quadro giuridico consolidato, che protegge gli investitori e i consumatori, mantenendo un ottimo grado di fiducia nel sistema.

A tale riguardo non si può non citare la direttiva MiFID[10], che impone agli intermediari e ai consulenti finanziari di valutare le caratteristiche del cliente cui sono destinati i prodotti fin dal momento dell'ideazione del prodotto stesso.

Un'altra misura che ha come obiettivo quello di salvaguardare l'integrità del sistema nel suo complesso è l'assicurazione sui depositi che protegge in maniera significativa i risparmi dei clienti in caso di insolvenza della banca. Questa tutela è fornita da istituzioni governative che fungono da assicuratori di ultima istanza: negli Stati Uniti, per esempio, la Federal Deposit Insurance Corporation (FDIC) garantisce i depositi dei clienti fino a $250,000 per depositante per banca[11]. Diverso è il discorso in Europa, dove il sistema di garanzia dei depositi sono ancora organizzati a livello nazionale, in attesa dell'ultima componente dell'Unione Bancaria, con il limite di assicurazione sui depositi pari a 100,000 euro per depositante, imposto dalle direttive dell'Unione Europea[12].

La protezione dei depositi serve a mantenere la fiducia dei clienti nel sistema bancario. Questo è particolarmente importante in tempi di crisi finanziaria, quando la paura di un fallimento bancario potrebbe spingere le persone a ritirare i loro depositi, innescando così una corsa agli sportelli che potrebbe destabilizzare l'intero sistema.

Le banche e le istituzioni finanziarie tradizionali svolgono un ruolo cruciale nel fornire accesso a una ampia gamma di servizi finanziari. Questi servizi vanno dai più abitudinari, come prestiti e investimenti, a quelli la cui erogazione risulta più complicata, come per esempio assicurazioni, mutui ipotecari e consulenza finanziaria.

---

[9] Banca d'Italia. (n.d.). "L'Unione Bancaria". https://www.bancaditalia.it/compiti/vigilanza/unione-europea/index.html

[10] Capriglione, F., & Semeraro, G. (2019). *Manuale di diritto bancario e finanziario*. Giuffrè.

[11] Federal Deposit Insurance Corporation. (n.d.). Deposit insurance at a glance [PDF]. https://www.fdic.gov/resources/deposit-insurance/brochures/documents/deposit-insurance-at-a-glance-english.pdf.

[12] Direttiva Ue 49/2014

- Prestiti ed Ipoteche: tipi di prestito come ipoteche o prestiti per l'istruzione devono necessariamente essere erogati da istituzioni che hanno la capacità di valutare il merito creditizio dei clienti e recuperare i fondi in caso di inadempimento.
- Assicurazioni: il settore assicurativo tradizionale è altamente regolamentato e richiede un livello di competenza e infrastruttura che è difficile replicare in un contesto decentralizzato.
- Consulenza finanziaria personalizzata: Per alcune tipologie di clienti, pensiamo per esempio a quelli più anziani, avere davanti una persona fisica cui poter esprimere le proprie necessità può essere fondamentale.
- Accesso ai mercati dei capitali: le banche e le istituzioni tradizionali giocano un ruolo fondamentale nell'aiutare e permettere alle aziende di accedere al mercato dei capitali: per esempio facilitando le offerte pubbliche iniziali (IPO) e le emissioni di obbligazioni.

La finanza tradizionale esiste da decenni ed ha ormai un'infrastruttura ben radicata, composta da istituzioni finanziarie, organismi di regolamentazione e sistemi di pagamento, che si poggiano sulle abitudini e usanze dei cittadini e difficilmente cambieranno nel prossimo futuro. Anche le valute più importanti, come il dollaro americano, l'euro, la sterlina britannica e lo yen giapponese sono alla base del sistema finanziario. Queste valute sono emesse e regolamentate da banche centrali, che stabiliscono le politiche monetarie per controllare l'offerta di denaro e influenzare l'economia. L'ampia accettazione e riconoscimento di queste valute per le transazioni sia a livello nazionale che internazionale, supportate da un solido quadro legale, danno al sistema finanziario sicurezza e fiducia.

Pertanto, il sistema finanziario attuale gode di un enorme punto di forza che racchiude tutti i precedenti: la fiducia da parte del pubblico. Questa fiducia è alimentata da una percezione di sicurezza e stabilità, derivante principalmente da anni ed anni di lunga evoluzione normativa che riesce, o quantomeno tenta, di tutelare un'infrastruttura ormai affermata nella vita delle persone in grado di soddisfare ogni bisogno finanziario di cui il soggetto potrebbe necessitare.

1.3 Inefficienze

Nel corso della sua storia, il sistema finanziario tradizionale ha svolto un ruolo fondamentale nel sostegno dell'economia globale, facilitando la circolazione del denaro, stimolando la generazione di ricchezza e gestendo il rischio in modo efficace.
Nonostante i suoi indiscutibili vantaggi questo sistema presenta però molteplici aspetti negativi derivanti dalle complesse dinamiche interne, dalle sue connessioni con altri settori dell'economia e dalla sua scarsa reattività alle mutevoli condizioni economiche e tecnologiche globali. Queste sfide possono avere un impatto non solo sul funzionamento efficiente del sistema finanziario stesso, ma anche sulla salute generale dell'economia e sul benessere delle persone.
Nelle pagine successive affronteremo una serie di problemi significativi che affliggono il sistema finanziario tradizionale con lo scopo di chiarirne i difetti e stimolare una discussione costruttiva su come la Finanza Decentralizzata potrebbe aiutare la risoluzione di questi difetti.

1.3.1 Costi transazionali e tassi d'interesse

Nel contesto della finanza tradizionale una delle questioni più discusse riguarda le inefficienze connesse ai costi di transazione e ai tassi d'interesse. Questi ultimi rappresentano un aspetto fondamentale che influisce non solo sulla velocità e sull'efficacia delle operazioni finanziarie, ma anche sul livello di accessibilità e inclusione finanziaria per gli utenti. In questo paragrafo si esamina in dettaglio la natura di tali costi, come influenzano le operazioni giornaliere e come rappresentano una sfida per la finanza attuale.

Interchange rate

Nel 1950 venne emessa da Diners Club la prima carta di credito che permetteva ai possessori di pagare il conto alla fine del mese in 27 ristoranti di New York soltanto mostrando tale carta firmata. Successivamente altre società americane quali American

Express, Mastercard e Bank AmeriCard (oggi conosciuta come Visa) iniziarono ad emettere le proprie carte, riuscendo ad imporsi come circuiti di pagamento leader[13].
Oggi, quando viene effettuata una transazione con carta, le banche addebitano una percentuale dell'importo totale, chiamate tassi di interscambio o *interchange rate*[14].
Alle fine del 2021 i pagamenti con carta rappresentano il 49% del numero totale delle transazioni nell'area euro. Come la Figura 1.2 ci suggerisce, questa percentuale è destinata a salire; infatti, nel 2021 il numero di transazioni con carta è aumentato del 17,3% raggiungendo 56,3 miliardi e il volume totale è in aumento del 14,4% arrivando a 2,3 trilioni di euro, con un corrispondente valore medio di circa 40 € per transazione con carta[15].

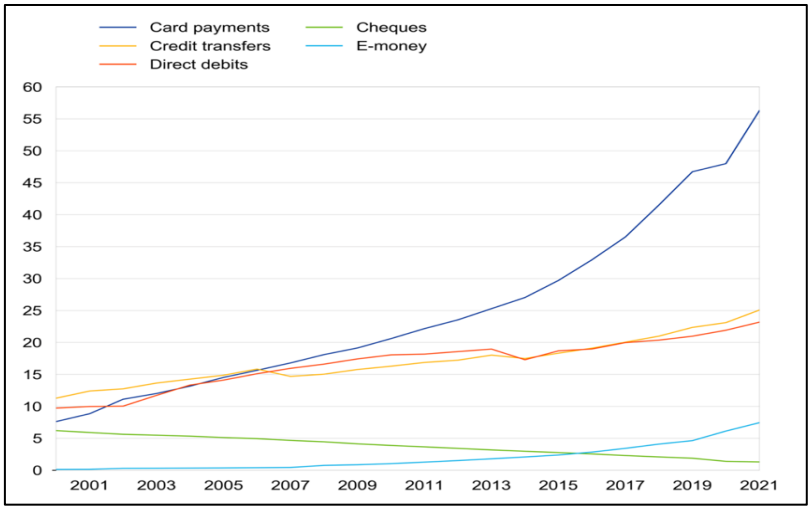


Figura 1.2: Utilizzo dei principali servizi di pagamento nell'area euro (numero di transazioni all'anno in miliardi). Fonte: *BCE* (2021)

Alla luce di questi dati è naturale chiedersi quanto sia la perdita che questo oligopolio di sistemi di pagamento affligge ai consumatori e piccoli business. Il costo che una transazione con carta comporta è composto da più componenti e dipende da una serie di variabili. Qui ci limitiamo a evidenziare che i costi di elaborazione della carta di credito,

[13] UBS. (2019). "The history of the credit card". https://www.ubs.com/ch/it/private/accounts-and-cards/information/magazine/2019/the-history-of-the-credit-card.html.
[14] Forbes Advisor. (2022). "Interchange fees: How they work and affect credit card rewards". Consultato il 5 luglio 2023. https://www.forbes.com/advisor/business/interchange-fees/.
[15] BCE (2021). "Payments statistics: 2021". https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2021~956efe1ee6.en.html.

comprese le commissioni per transazione e le spese di gestione del conto, ammontano al 3-4% del volume processato da un commerciante[16]. Quindi gli esercenti hanno dovuto sopportare un costo di interscambio pari a 80 miliardi, che mediamente equivale a 1,2 € per transazione effettuata con carta, che soprattutto per piccoli imprenditori è una cifra rilevante in termini di mancato guadagno.

Remittance fees

Il cosiddetto costo di rimessa, o *remittance fees*, è un costo che grava sui lavoratori migranti e le loro famiglie quando trasferiscono denaro nel paese d'origine. Circa un miliardo di persone in tutto il mondo dipende dalle rimesse: ogni anno 200 milioni di lavoratori migranti inviano fondi ai familiari e 800 milioni di persone ne beneficiano. Negli ultimi venti anni i flussi globali di rimesse sono cresciuti di cinque volte in valore, raggiungendo nel 2022 i 647 miliardi di dollari e con la previsione che, secondo World Bank Group (2023), essi raggiungeranno gli 840 miliardi a fine 2023[17] (Fig. 1.3).

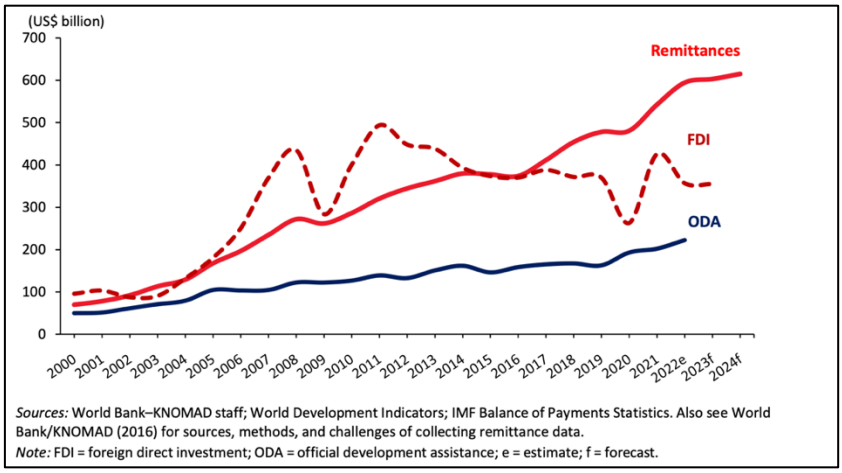
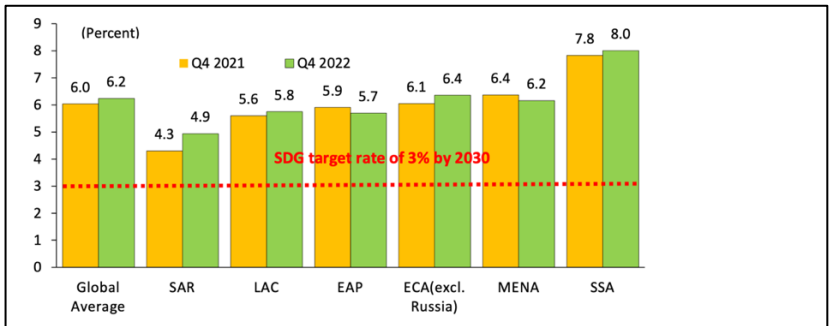


Figura 1.3: Rimesse, Investimenti Diretti Esteri e Flussi di Aiuti allo Sviluppo Ufficiale verso Paesi a Reddito Basso e Medio, escludendo la Cina, 2000-2024f

[16] Kehl F. (2023). "Credit card processing fees: how much will they cost your business & how can you lower them?" https://www.merchantmaverick.com/the-complete-guide-to-credit-card-processing-rates-and-fees/.

[17] Ratha D., Plaza S., Kim E.J., Chandra V., Kurasha N., e Pradhan B (2023). *Migration and Development Brief 38: Remittances Remain Resilient But Are Slowing*. KNOMAD–World Bank, Washington, DC. https://www.knomad.org/sites/default/files/publication-doc/migration_and_development_brief_38_june_2023_0.pdf.

Come illustrato in Figura 1.4, il quadro dei costi di rimessa mondiale è abbastanza frastagliato, ma in media possiamo dire che le *remittance fees*, inclusive delle conversioni in valuta, ammontano circa al 6-6.5%: il doppio dell'obiettivo fissato dall'ONU come obiettivo di sviluppo sostenibile da raggiungere entro il 2030. Quindi, nel 2022 circa 40 miliardi di dollari (200 dollari a immigrato all'anno) sono stati assorbiti da intermediari quali Western Union, MoneyGram e pochi altri per gestire le spese di conversione e trasferimento del denaro. Queste istituzioni sono limitate e dato che la competizione è scarsa creano un monopolio di mercato, potendosi permettere di addebitare alte fees.



Source: World Bank's Remittance Prices Worldwide database.
Note: Red dotted line represents the SDG 10 target of 3 percent. EAP = East Asia and Pacific; ECA = Europe and Central Asia; LAC = Latin America and the Caribbean; MENA = Middle East and North Africa; SAR = South Asia; SDG = Sustainable Development Goal; SSA = Sub-Saharan Africa.

Figura 1.4: Quanto costa spedire 200$? Costi per le rimesse regionali 2021-22

Le Figure 1.5a e 1.5b evidenziano i paesi il cui PIL dipende in larga misura dalle rimesse, arrivando addirittura a costituire in 60 nazioni almeno il 4% del loro PIL[18].

[18] The World bank. (2022). "Personal remittances received (% of GDP)". https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS.

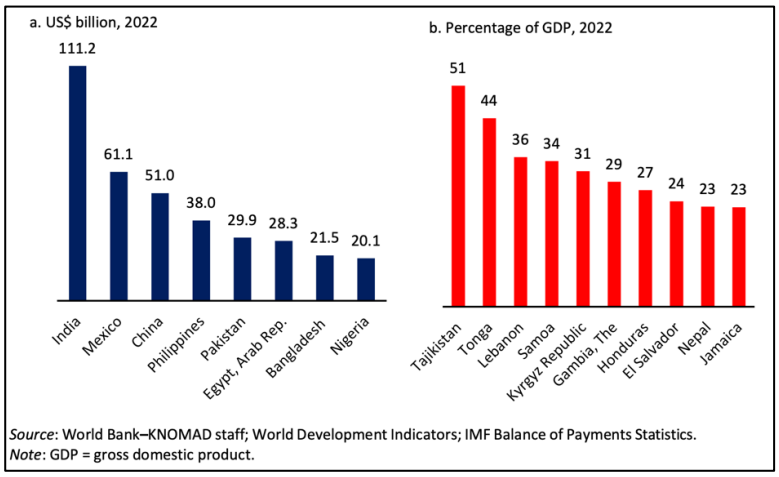


Figura 1.5a e 1.5b: Principali destinatari di rimesse tra i Paesi a basso e medio reddito, 2022

I soldi delle *remittance fees* potrebbero essere investiti per promuovere lo sviluppo economico nei paesi che ricevono rimesse. Infatti il 75% delle rimesse viene utilizzato per mettere cibo sul tavolo, coprire le spese mediche, le tasse scolastiche o le spese di alloggio. Il restante 25%, pari a 125 mld di dollari all'anno, può essere risparmiato o reinvestito in vari settori, come l'istruzione, la sanità, le infrastrutture o le piccole e medie imprese, creando ulteriori posti di lavoro e sostenendo l'economia locale.

Interest rates

Il principale canale di generazione di profitto per le banche si basa sul margine di interesse, cioè la differenza tra il tasso di interesse che una banca paga ai depositanti e quello che incassa dai debitori. Queste banche tengono bassi i tassi sui depositi e alti i tassi attivi sui prestiti in modo da coprire i loro *brick-and-mortar costs*[19]: questi costi operativi comprendono costi di utilità, costi del personale, costi di sicurezza, costi di gestione del denaro e molti altri. Riducendo, o addirittura eliminando, questi costi sarebbe possibile contrarre il margine d'interesse che le banche guadagnano dalla gestione.
L'innovazione tecnologica e l'avanzamento del settore fintech hanno aperto la strada ad un nuovo modello di business che può ridurre o eliminare molti di questi costi operativi.

[19] I *brick-and-mortar costs* sono le spese associate all'operatività di un business fisico, cioè un negozio che offre prodotti o servizi ai propri clienti faccia a faccia.

L’online banking non richiede strutture fisiche e può essere gestito con una forza lavoro ridotta, comportando costi notevolmente inferiori rispetto alle banche tradizionali[20].
Sebbene l'online banking rappresenti un passo importante verso la riduzione dei costi operativi non elimina completamente la necessità di un ente centrale e i costi ad esso associati. Oltre a quelli legati alla gestione e al mantenimento di un'entità centrale, responsabile di numerose funzioni cruciali, come il controllo delle transazioni, la gestione del rischio, la sicurezza dei dati e l'assistenza clienti, si devono considerare anche i costi associati alla creazione e al mantenimento dell'infrastruttura tecnologica sicura e aggiornata.

1.3.2 Accessibilità e inclusione finanziaria

Secondo un recente studio del World Bank Group, oggi 1.7 miliardi di persone sono *unbanked* (Figura 1.6), cioè che più di un quarto della popolazione mondiale (un terzo degli adulti) non ha accesso a servizi bancari convenzionali quali conti correnti, carte di credito, prestiti o assicurazioni[21]. Questo è un problema importante perché limita la capacità di queste persone di risparmiare denaro, investire per il futuro, ottenere prestiti o semplicemente coprire eventuali spese d’emergenza giornaliere che possono presentarsi in una piccola attività imprenditoriale.

[20] Forbes. (2023). “Best Online Banks Of 2023”. https://www.forbes.com/advisor/banking/best-online-banks/.
[21] Abdulhakeem, S. A., & Hu, Q. L. (2021). “Powered by Block- chain Technology, DeFi (Decentralized Finance) Strives to Increase Financial Inclusion of the Unbanked by Reshaping the World Financial System”. *Modern Economy,* 12, 1-16.

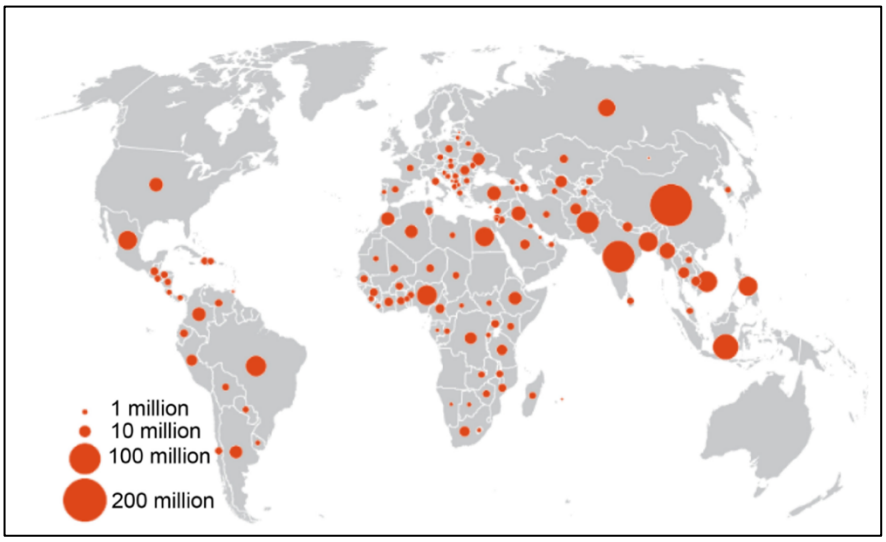


Figura 1.6: 1,7 miliardi di persone unbanked. Fonte: *The Global Findex Database 2017*[22]

Come abbiamo già evidenziato, le banche sono soggette a regolamenti e alti costi associati alla gestione del denaro, il che rende i loro servizi sempre più inaccessibili; 26 milioni di lavoratori migranti nel GCC[23] non riescono ad aprire un conto bancario a causa di vari motivi, tra cui le elevate commissioni bancarie, la necessità di documenti specifici per aprire un conto e la mancanza di filiali bancarie nelle vicinanze[24].

L'attuale sistema bancario esclude molte famiglie a basso reddito e invece attira solo il segmento a medio-alto reddito, soprattutto nei paesi più poveri. Esiste una forte correlazione fra persone povere e "non bancarizzate", il che rende la diseguaglianza un problema del nostro sistema finanziario. Il 75% della popolazione che non riesce a usufruire dei servizi bancari è povera e non riesce ad accedere ai servizi di sostegno sociali essenziali, in quanto molte forme di assistenza richiedono un conto bancario per depositare i fondi[25].

---

[22] Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). "The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution". Washington DC, World Bank.

[23] GCC è l'acronimo di Gulf Cooperation Council (Consiglio di Cooperazione del Golfo in italiano). È un'organizzazione regionale intergovernativa fondata 1981 che comprende tutti gli Stati Arabi del Golfo Persico, tranne l'Iraq. I membri del GCC sono: Bahrain, Kuwait, Oman, Qatar, Arabia Saudita e Emirati Arabi Uniti.

[24] King, N. (2017). "The App Connecting the GCC's Low Paid Workers with Bank Accounts". https://gulfbusiness.com/the-app-connecting-the-gccs-low-paid-workers-with-bank-ac counts/.

[25] Felsenthal, M., & Hahn, R. (2018). "Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows".

Inoltre, la maggior parte delle persone in tutto il mondo non ha accesso alle piattaforme di shopping online in quanto, a causa delle complesse richieste stabilite dagli emittenti e dalle banche, non possiede carte Visa e Mastercard, che sono i circuiti di pagamento più popolari[26].

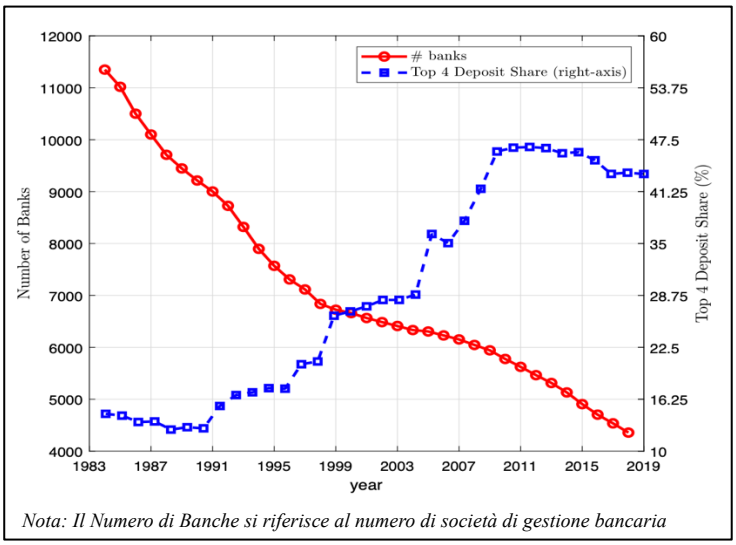
In questo contesto l'accesso ai servizi finanziari tradizionali comporterebbe spese aggiuntive: costi di viaggio, tempo impiegato e dipendenza da altri intermediari e emittenti di prestiti che addebitano prezzi ancor più elevati per i servizi. Tutto ciò condurrebbe gli individui *unbanked* ancor di più nella povertà.

1.3.3 Concentrazione di ricchezza e potere

Un altro svantaggio dell'attuale ecosistema finanziario è la centralizzazione. La maggior parte dei consumatori e imprese fanno accordi con una singola istituzione bancaria per beneficiare dei loro servizi finanziari. Queste banche commerciali, pur essendo soggette alla regolamentazione e alla politica monetaria delle banche centrali, sono in grado di imporre le proprie commissioni e condizioni sui prestiti e sui conti correnti.

Per esempio, come mostra la Figura 1.7, il sistema americano è altamente concentrato, basti pensare che le quattro maggiori banche hanno il 44% dei depositi assicurati, rispetto al 15% nel 1984, con il trend che ha fermato la sua crescita dopo la crisi del 2008. Il numero di banche negli Stati Uniti, conseguentemente, ha un andamento inverso, ed è diminuito da più di 11mila nel 1984 a meno di 5mila oggi[27].

[26] Abdulhakeem e Hu, "Powered by Blockchain Technology," 1-16.
[27] Corbae D., D'Erasmo P. (2020). "Rising bank concentration", *National Bureau of Economic Research*. https://www.nber.org/system/files/working_papers/w26838/w26838.pdf.



Nota: Il Numero di Banche si riferisce al numero di società di gestione bancaria

Figura 1.7: Numero di banche e concentrazione bancaria negli Stati Uniti (quota di deposito delle prime 4 banche). Fonte: *Call Reports*.

Questa concentrazione è un modo per le banche di accrescere il proprio potere di mercato, accedere a nuovi mercati e beneficiare di economie di scala, che le rendono più efficienti e competitive. Allo stesso tempo, però, questo porta a una diminuzione della concorrenza nel settore, con conseguenze negative per i consumatori in termini di costi e qualità dei servizi. La centralizzazione ha ostacolato la crescita delle imprese di tutto il mondo, consentendo alle banche di imporre regole e costi per i pagamenti con carta e rimesse, che ha portato alla perdita di ulteriori potenziali clienti e reso le persone ancora più povere.

1.3.4 Limitata interoperabilità

I consumatori e le attività imprenditoriali devono fronteggiarsi con le istituzioni finanziarie in un ambiente che blocca l'interoperabilità. Per interoperabilità s'intende la capacità di due o più sistemi, reti, mezzi, applicazioni o componenti, di scambiare informazioni tra loro e di essere poi in grado di utilizzarle.[28] Nel contesto finanziario possiamo individuare due aree in cui il sistema finanziario attuale mostra carenze di interoperabilità:

[28] Health Governance Initiative. 2012. "Discussion Paper on Semantic and Technical Interoperability." https://health.ec.europa.eu/system/files/2016-11/ev_20121107_wd02_en_0.pdf.

- Interoperabilità tecnica: Questo è il livello più basilare di interoperabilità e riguarda la capacità di due o più sistemi o componenti tecnologici di scambiare informazioni e di utilizzarle. Questo tipo di interoperabilità è limitata dall'infrastruttura legacy[29] esistente che può limitare l'implementazione di nuovi sistemi a causa dell'incompatibilità con le nuove tecnologie. Nel contesto del settore bancario e finanziario, l'infrastruttura legacy include sistemi informatici obsoleti che gestiscono operazioni critiche come il trattamento delle transazioni, la gestione dei conti clienti o l'analisi dei dati finanziari. Inoltre, molte aziende potrebbero essere riluttanti a condividere i loro innovativi strumenti di pagamento attraverso una piattaforma per paura di perdere il loro vantaggio competitivo[30]. Questa mancanza di integrazione tecnica, quindi, facilita l'esclusione finanziaria e ostacola l'innovazione e può portare a inefficienze come maggiori costi, tempi più lunghi o barriere all'entrata per start-up fintech. Un tentativo per mitigare questo problema fu fatto da Visa, che nel 2019 provò ad acquistare Plaid, una società fintech che fornisce una piattaforma che permette alle applicazioni di connettersi con i conti bancari degli utenti, ma l'antitrust americano ha messo il veto sull'affare[31].
- Interoperabilità semantica[32]: La semantica ha un ruolo chiave nella interoperabilità, essa deve assicurare che lo scambio di informazioni tra controparti sia effettuata in maniera efficace. Questo livello riguarda il significato delle informazioni scambiate tra i diversi enti finanziari e la capacità di interpretare queste informazioni in modo uniforme. Su questo aspetto la disciplina regolamentativa ha fatto notevoli passi avanti al fine di omogeneizzare i protocolli di comunicazione e le ontologie dei dati, ma in un mercato altamente competitivo

[29] Techopedia. (n.d.). Legacy system definition. https://www.techopedia.com/definition/6815/legacy-system.
[30] Dargahwala, Tasneem, and Elisabeth Riedl. 2021. "Powered by Blockchain Technology, DeFi (Decentralized Finance) Strives to Increase Financial Inclusion of the Unbanked by Reshaping the World Financial System." *Modern Economy* 12:1-16. https://doi.org/10.4236/me.2021.121001.
[31] Rooney K. (2021). "Plaid valuation tops $13 billion in first funding after a scrapped $5.3 billion merger with Visa", CNBC. https://www.cnbc.com/2021/04/07/plaid-hits-13point4-billion-valuation-in-the-wake-of-scrapped-visa-deal.html.
[32] Di Orio, G., Brito, G., Maló, P. (2022). Semantic Interoperability Framework for Digital Finance Applications. In: Soldatos, J., Kyriazis, D. (eds) *Big Data and Artificial Intelligence in Digital Finance*. Springer, Cham. https://doi.org/10.1007/978-3-030-94590-9_4.

come quello bancario molte aziende sono molto protettive dei loro segmenti di target e della privacy dei dati. Pensiamo per esempio alle diverse metodologie utilizzate dalle banche per la valutazione del merito creditizio dei clienti: ognuna di queste ha un proprio sistema che limita l'interpretazione dei dati.

1.4 Il passaggio alla DeFi

L'attuale infrastruttura finanziaria, nonostante i momenti di crisi, ha funzionato per decenni e ha portato il mondo ad una crescita economica e tecnologica senza precedenti. Ha reso possibile un'era di globalizzazione e integrazione economica che ha cambiato la storia del pianeta, elevato il livello di vita di miliardi di persone e spianato la strada a innovazioni rivoluzionarie in molti settori.

Tuttavia, come evidenziato in precedenza, il sistema finanziario attuale mostra segnali di cedimento. Da un lato le inefficienze e i costi che abbiamo esaminato ostacolano l'innovazione e la crescita economica, dall'altro conducono ad aumentare la non inclusività e quindi ad aggravare l'ineguaglianza. Dovrebbero esserci uguali opportunità per tutti e un progetto dovrebbe essere finanziato sulla base della qualità dell'idea e del piano di esecuzione, non rispetto ad altri fattori. Basti pensare che gli Stati Uniti, la "terra delle opportunità", hanno uno dei più bassi tassi di migrazione del reddito dal quartile peggiore a quello migliore[33].

Nel 2008, mentre il mondo era sul precipizio di una crisi finanziaria globale, i sostenitori di Bitcoin intravedevano un'opportunità: quella di creare un nuovo sistema economico, completamente svincolato da quello tradizionale, basato su una forma di denaro elettronico completamente indipendente[34]. Essi credevano che Bitcoin, impattando sulle idee consolidate di dati, accessibilità e governance, avrebbe cambiato il funzionamento del sistema finanziario, rendendolo migliore.

[33] Chetty, R., Hendren, N., Kline, P., e Saez, E. (2014). Where is the Land of Opportunity? The Geography of Intergenerational Mobility in the United States [PDF]. National Bureau of Economic Research. https://www.nber.org/system/files/working_papers/w19843/w19843.pdf

[34]PricewaterhouseCoopers. (n.d.). DeFi: Defining the future of finance. PwC Switzerland. Retrieved July 24, 2023, from https://www.pwc.ch/en/insights/digital/defi-defining-the-future-of-finance.html

Nonostante i tentativi di adattarsi e riformarsi, la TradFi ha faticato ad adeguarsi all'era digitale nella quale stiamo vivendo, fallendo in parte le aspettative di inclusione, costi più bassi e interoperabilità che i consumatori e le aziende si aspettano.
È in questo contesto che emerge la finanza decentralizzata, o DeFi. La DeFi rappresenta un nuovo approccio alla finanza, che cerca di sfruttare le potenzialità delle tecnologie blockchain e delle criptovalute per creare un sistema finanziario più aperto, accessibile e trasparente. La tecnologia alla base è ancora in continuo sviluppo e ci sono molti ostacoli da superare, ma il potenziale di questa nuova forma di finanza è enorme.
Nel prossimo capitolo esploreremo più in dettaglio le origini della DeFi e la sua infrastruttura. Analizzeremo come questa nuova forma di finanza cerca di affrontare le debolezze dell'attuale sistema finanziario e quali soluzioni offre. Esploreremo inoltre le sfide che la DeFi deve ancora affrontare e come potrebbe evolversi nel futuro.

CAPITOLO 2 - L'INFRASTRUTTURA DELLA DE.FI.

Prima di analizzare nel dettaglio l'infrastruttura e il funzionamento dei servizi finanziari della finanza decentralizzata, riteniamo opportuno soffermarci sui presupposti che hanno reso possibile questa innovazione rivoluzionaria.

2.1 Presupposti tecnologici

Secondo Zetzsche, Arner e Buckley la nascita della DeFi è il risultato diretto di un insieme di sviluppi tecnologici chiave[35]. La legge di Moore, che più che una legge si tratta di un'osservazione empirica, enunciata per la prima volta nel 1965, sosteneva che il numero di transistor (i componenti elettronici che amplificano o commutano i segnali elettrici) che poteva essere inserito su un microchip raddoppiava circa ogni 18-24 mesi[36]. Ciò, significava che la potenza di elaborazione dei computer stava crescendo esponenzialmente, con un miglioramento sostanziale nella velocità e nelle capacità di calcolo ogni due anni circa. Analogamente, la capacità di archiviazione dei dati è cresciuta in un modo simile, come illustrato dalla legge di Kryder. Queste leggi hanno sottolineato come la potenza di calcolo e la capacità di immagazzinare dati sono diventate sempre più abbondanti e accessibili, alimentando la crescita e lo sviluppo della tecnologia blockchain. Parallelamente, l'enorme crescita della larghezza della banda larga a partire dagli anni Novanta ha permesso la trasmissione rapida e affidabile di enormi quantità di dati, un elemento essenziale per il corretto funzionamento delle reti.

Questi fattori insieme hanno portato alla virtualizzazione dell'hardware, un passaggio cruciale che ha reso possibile un modello di servizi software molto più efficiente. La virtualizzazione dell'hardware ha permesso l'adozione di modelli orientati ai servizi come il *Software as a Service* (SaaS), che tra i vantaggi principali ha la gestione immediata delle risorse e la maggior flessibilità nella distribuzione e protezione delle applicazioni.

Il SaaS a sua volta ha permesso lo sviluppo del *Blockchain as a Service* (BaaS) che, facendo leva sulla tecnologia cloud, ha permesso di superare molte delle complessità

[35] Dirk Andreas Zetzsche, Douglas W. Arner, & Ross P. Buckley, "Decentralized Finance (DeFi)," *Journal of Financial Regulation* 6 (2020): 172–203, https://ssrn.com/abstract=3539194.
[36] Treccani, "Legge di Moore," *Enciclopedia della Scienza e della Tecnica*, 2008, https://www.treccani.it/enciclopedia/legge-di-moore_(enciclopedia-della-scienza-e-della-tecnica)/.

tecniche precedentemente associate alla blockchain, eliminando in tal modo importanti barriere all'ingresso, agevolando la diffusione e l'uso della blockchain e ponendo le basi alla DeFi.

Le radici su cui si fonda la DeFi sono state ribattezzate con l'acronimo ABCD: Artificial intelligence (AI), Blockchain, Cloud e Data.

L'intelligenza artificiale è quella di un software che imita le funzioni cognitive umane, come l'apprendimento e il problem solving. L'IA sta cambiando il modo in cui le organizzazioni operano all'interno del settore finanziario, permettendo l'automazione di compiti complessi, l'analisi dei dati a un livello senza precedenti e la personalizzazione dei servizi finanziari. Può essere utilizzata per il rilevamento delle frodi, la gestione del rischio, l'assistenza clienti automatizzata e molto altro ancora.

Il machine learning è un sottoinsieme dell'Intelligenza Artificiale che si occupa di creare sistemi che, tramite metodi statistici, hanno l'obiettivo di permettere ai sistemi informatici di perfezionare autonomamente le loro abilità in una specifica funzione, senza la necessità di intervento umano. Questo miglioramento si concretizza attraverso un processo intensivo di "addestramento" durante il quale la macchina si sottopone a numerosi cicli di backtesting. In ogni ciclo la macchina è valutata sulla base del suo successo o insuccesso nel completare un'operazione, affinandosi gradualmente nelle sue competenze.

Nel contesto della finanza decentralizzata, il *cloud computing* rappresenta un elemento chiave per la decentralizzazione della gestione dei dati e della potenza di elaborazione. Invece di affidarsi a un unico server centralizzato (data center) la DeFi utilizza il cloud computing per distribuire i dati su una rete di tanti centri server, rendendoli accessibili via Internet a utenti in diverse parti del mondo. Questa decentralizzazione è il cuore della filosofia alla base della DeFi, poiché consente l'accesso su richiesta a risorse di archiviazione ed elaborazione senza che gli utenti debbano possedere o controllare direttamente i server.

Secondo il National Institute of Standards and Technology (NIST) un modello cloud deve avere 5 caratteristiche essenziali[37]:

[37] Peter Mell & Timothy Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology*, 2011, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.

- *On-demand self-service*: un consumatore può autonomamente fornire e ottenere archiviazione e capacità di elaborazione, secondo le necessità, automaticamente, senza interagire con un fornitore di servizi umano.
- *Broad network access*: le funzionalità sono disponibili attraverso la rete e accessibili mediante meccanismi standard che ne promuovono l'utilizzo tramite diverse piattaforme (ad esempio telefoni cellulari, tablet o laptop).
- *Resource pooling*: le risorse informatiche del fornitore sono raggruppate per servire più consumatori utilizzando un modello *multi-tenant*, con diverse risorse fisiche e virtuali assegnate dinamicamente e riassegnate in base alla domanda dei consumatori.
- *Rapid elasticity*: le capacità possono essere fornite e rilasciate elasticamente, in alcuni casi automaticamente, per scalare rapidamente verso l'esterno e verso l'interno in modo proporzionato alla domanda. Per il consumatore, le capacità disponibili per il provisioning appaiono spesso illimitate e possono essere adeguate in qualsiasi quantità in qualsiasi momento.
- *Measured service*: i sistemi cloud controllano e ottimizzano automaticamente l'utilizzo delle risorse sfruttando una capacità di misurazione a un certo livello di astrazione appropriato al tipo di servizio (ad esempio archiviazione, elaborazione, larghezza di banda e account utente attivi). L'utilizzo delle risorse può essere monitorato, controllato e segnalato, fornendo trasparenza sia al fornitore che per il consumatore del servizio utilizzato.

Con l'aumento esponenziale dei dati disponibili è nata la necessità di ricorrere a metodologie e strumenti più avanzati, cioè le tecniche dei Big Data. Questi approcci sono stati sviluppati proprio per rispondere alla sfida di raccogliere ed elaborare in pochissimo tempo volumi di dati che superano la capacità delle metodologie tradizionali.

2.2 Blockchain

L'elemento più distintivo dell'ABCD è indubbiamente la blockchain, pilastro fondamentale senza il quale la DeFi non avrebbe vita. Il concetto di blockchain fu introdotto per la prima volta dallo pseudonimo Satoshi Nakamoto nel suo famoso *white paper*. La blockchain non è un concetto semplice da comprendere ed esistono, infatti,

diverse definizioni basate su aspetti differenti, come la sua struttura tecnica, le tecnologie correlate o le sue implicazioni nel mondo degli affari e nella società. La blockchain è un libro mastro (*ledger*) digitale, decentralizzato e distribuito su un network, strutturando una catena di registri ("blocchi") responsabili dell'archiviazione dei dati, dalle transazioni di valore a intere applicazioni digitali[38]. Essa rientra in un insieme più ampio di tecnologie che è quello della *Distributed Ledger Tecnhology* (DLT), in cui, dal punto di vista strutturale alla base c'è un ledger digitale. Con la DLT ci riferiamo a tutti i database che funzionano a un registro distribuito, in cui i dati o le risorse sono distribuiti su più server (o nodi) e possono essere accessibili e modificabili da più punti (Figura 2.1).

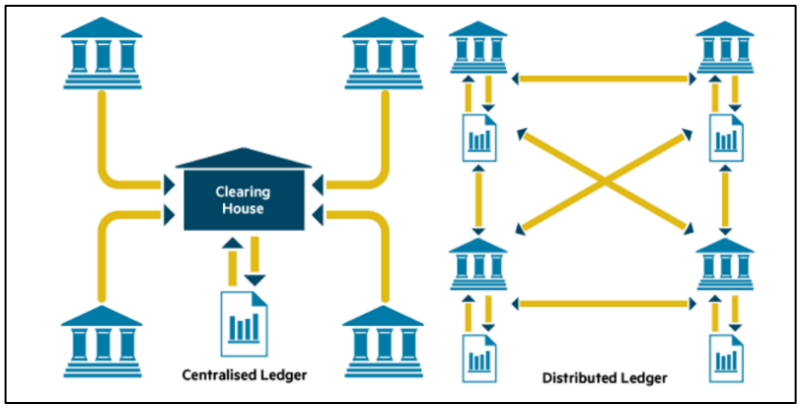


Figura 2.1. Ledger centralizzato vs ledger distribuito. Fonte: *Medium*

I ledgers distribuiti eliminano la necessità di un centro di controllo e diversamente dai database tradizionali, consentono l'uso da parte di utenti non fidati senza supervisione. Questa caratteristica rende la blockchain particolarmente utile nel settore finanziario, dove fiducia, sicurezza e trasparenza sono cruciali. La specificità della blockchain, a differenza delle altre DLT, risiede nell'organizzazione dei dati in blocchi crittograficamente collegati, garantendo che i dati, una volta inseriti, siano immutabili: è possibile aggiungere nuovi blocchi di informazioni al ledger, ma non è invece possibile la modifica o la rimozione di blocchi preesistenti nella catena.

Fondamentalmente le blockchains sono protocolli software che permettono a molteplici parti di operare sotto presupposti e dati condivisi senza la necessità di fidarsi l'uno

[38] G. Chiap, J. Ranalli, & R. Bianchi, *Blockchain: Tecnologia e applicazioni per il business* (Hoepli, 2019).

dell'altro. In questo sistema la crittografia e i protocolli di consenso garantiscono sicurezza e immutabilità. Il risultato è un sistema aperto, neutrale, affidabile e sicuro, in cui le possibilità di utilizzo e la fiducia nel sistema non dipendono da alcun individuo, intermediario e istituzione.

Una critica che viene spesso mossa a questo tipo di tecnologie è che la mancanza di autorità porti ad un'assenza di controllo tale da incentivare attività illegali o illecite[39]. È chiaro che una maggiore regolamentazione è essenziale per tutelare gli utenti dalle frodi e per evitare che l'anonimato che permette la blockchain possa favorire pratiche proibite. Tuttavia è fondamentale sottolineare che, mentre altri sistemi e tecnologie affrontano una moltitudine di sfide esterne e interne, il mondo della DeFi si trova in una posizione unica: la sua principale sfida è la tecnologia su cui si basa, ovvero la blockchain stessa.

Introdotta la blockchain, passiamo ora agli altri strumenti che le permettono di esistere, funzionare e porsi come tecnologia fondamentale alla base della DeFi. Esploreremo i protocolli del consenso, che garantiscono affidabilità e sicurezza da parte degli utenti, e i meccanismi che le permettono di operare in maniera autonoma e di connettersi con il mondo esterno.

2.2.1 Sicurezza: i protocolli del consenso

È già stato precedentemente illustrato che la blockchain è un sistema a tecnologia DLT che opera attraverso un insieme di nodi concatenati, dai quali sono osservabili e si diramano le informazioni sulle operazioni effettuate. Quando gli utenti effettuano transazioni su una rete blockchain, queste transazioni vengono inizialmente verificate dai nodi e poi accumulate in un pool. Da questo pool, un minatore o validatore[40] approva un insieme di transazioni e crea un blocco proposto, che però non viene immediatamente aggiunto alla blockchain. In primis, deve passare attraverso un protocollo di consenso, come il *proof-of-work* o il *proof-of-stake* (vedremo in seguito di cosa si tratta), per garantirne la validità. Dopo che la rete raggiunge un consenso sull'autenticità e sulla

[39] Bruce Scheneir, "There's no good reason to trust blockchain technology," *Wired*, 2019, https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/.

[40] I minatori sono utenti di una blockchain che utilizzano hardware specializzati per verificare e registrare transazioni sulla rete. Sono responsabili della creazione di nuovi blocchi e della loro aggiunta alla blockchain. Come ricompensa per i loro sforzi ricevono una certa quantità di criptovaluta che stanno estraendo. Fonte: *CoinMarketCap.*

correttezza del blocco, questo viene definitivamente aggiunto alla blockchain. La connessione tra blocchi viene generata mediante una funzione crittografica (nello specifico la funzione crittografica di *hash*[41]), la quale crea un collegamento matematico indissolubile tra essi. Una volta avvenuto ciò, le transazioni all'interno di quel blocco sono considerate confermate e diventano parte del registro immutabile della blockchain (Figura 2.2).

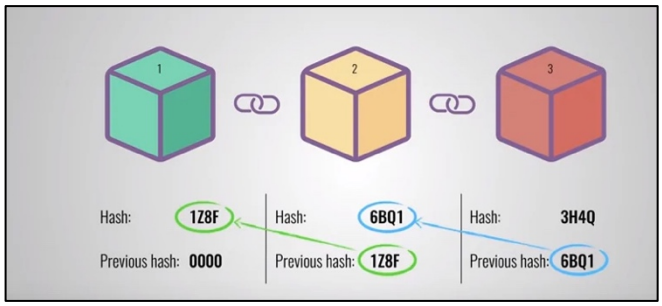


Figura 2.2. Funziona crittografica di hash. Fonte: *Simply Explained*

Grazie alle proprietà delle funzioni hash, una volta che un blocco viene aggiunto alla blockchain, l'inclusione dell'hash del blocco precedente e il proprio hash rendono estremamente difficile (quasi impossibile) modificare le informazioni all'interno di quel blocco senza modificare anche tutti i blocchi successivi. Ciò implica che se un attacco hacker manipolasse le informazioni di una transazione si modificherebbe anche l'hash della transazione e quindi dell'intero blocco (Figura 2.3).

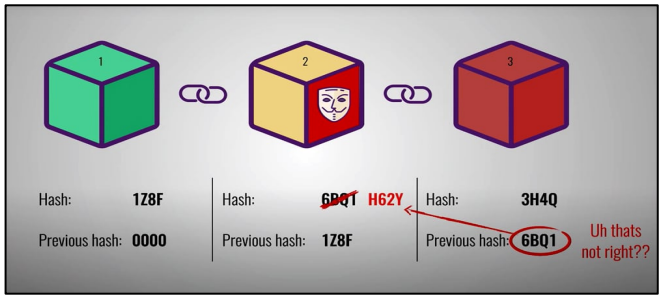


Figura 2.3. Funzione hash contro attacchi. Fonte: *Simply Explained*

[41] Un *hash*, o funzione *hash*, è un algoritmo crittografico che trasforma un dato di dimensione arbitraria in stringhe alfanumeriche di dimensioni fisse. La lunghezza dipende dalla funzione di hash che si vuole utilizzare. Fonte: *Blockchain tecnologia e applicazioni per il business*.

Se ciò avvenisse il tutto sarebbe osservabile dato che ogni variazione, per quanto minima, all'interno di un blocco porta alla generazione di un hash completamente diverso. Oltre a ciò, ogni hash è accompagnato da una marca temporale, detta *timestamp*. Pertanto, se un blocco, che avrebbe dovuto essere chiuso e immutabile, mostra un cambio nel suo hash in una data successiva, è immediatamente riconoscibile come segno di potenziale manipolazione. Infine, poiché ogni nodo della rete blockchain ha una copia completa del registro, qualsiasi discrepanza in un blocco rispetto alle altre copie verrebbe rapidamente identificata da altri nodi. Questa struttura interconnessa, insieme all'utilizzo di funzioni hash crittografiche, garantisce un alto livello di sicurezza, trasparenza e immodificabilità nella blockchain, rendendo le transazioni e i dati al suo interno altamente resistenti a manipolazioni e attacchi esterni.

Come anticipato prima, le blockchains sono possibili grazie ai protocolli del consenso che rispondono alla domanda "come fa un nodo a decidere di accettare o meno un blocco?". Questi meccanismi sono stati progettati per resistere a pratiche di sabotaggio, frodi e attacchi malware, garantendo la sicurezza, l'integrità e la fiducia tra i partecipanti della rete.

Esistono diversi tipi di protocolli per raggiungere il consenso distribuito, tra cui i più popolari sono il *Proof-of-Work* (PoW) e il *Proof-of-Stake* (PoS). I nodi che partecipano attivamente al processo di consenso, aggiungendo nuovi blocchi e validando transazioni, sono chiamati minatori (*miner*) e svolgono un processo chiamato *mining*.

Il *Proof-of-Work*, utilizzato nelle blockchain di cui si tratta in questo lavoro, richiede che i miner risolvano sfide matematiche particolarmente complesse per guadagnarsi il diritto di validare e registrare transazioni. Nonostante il processo sia criticato per il suo notevole dispendio energetico, esso dota la blockchain di un'eccezionale sicurezza e robustezza contro possibili attacchi, assicurando l'integrità e l'immutabilità dei dati registrati.

Ma come funziona esattamente questa protezione? Se un attaccante volesse alterare una transazione in un blocco già confermato, si troverebbe di fronte alla necessità di eseguire nuovamente il Proof-of-Work per quel blocco e, a causa della catena di hash interconnessi, anche per tutti i successivi. Inoltre, mentre l'attaccante è impegnato in questo tentativo di ricalcolo, i minatori onesti continuano il loro lavoro, aggiungendo costantemente nuovi blocchi alla catena e quindi incrementando l'*hashrate* totale della

rete. Quando parliamo di hashrate ci riferiamo alla potenza di calcolo e rappresenta quindi la velocità con cui un miner può completare un'operazione nel codice Bitcoin. Per avere successo nell'alterazione, l'attaccante dovrebbe controllare un hashrate superiore al 50% dell'intera rete, in modo da poter aggiungere blocchi alla propria versione fraudolenta della blockchain più velocemente di quanto facciano tutti gli altri minatori messi insieme. Questo scenario, conosciuto come "attacco del 51%", dimostra quanto sia cruciale l'hashrate nella protezione e nella sicurezza di una rete basata su Proof-of-Work. Un attacco del 51% è realizzabile ed è già stato effettuato diverse volte; tuttavia risulta praticamente impossibile raggiungere un hashrate del 51% su blockchain importanti come Bitcoin. Per incentivare i miner a generare nuovi blocchi e mantenere il network sicuro, sono previste delle ricompense. I miner che creano un nuovo blocco sono ricompensati con tutte le commissioni delle transazioni incluse nel blocco, più eventualmente le nuove monete (criptovalute).

Il Proof-of-Work è stato fondamentale nello stabilire la blockchain come una tecnologia sicura e affidabile. Tuttavia, a causa delle preoccupazioni legate al consumo energetico, molte nuove criptovalute e progetti blockchain stanno esplorando o adottando alternative come il *Proof-of-Stake* (PoS). Il PoS è un meccanismo in cui i nodi, o validatori (l'equivalente del miner nel PoW), vengono alternati e scelti in anticipo basandosi sulla quantità di token in loro possesso per la relativa blockchain e sulla durata per cui hanno mantenuto tali token.

È considerato più efficiente in termini energetici rispetto al PoW, ed è per questo che la blockchain Ethereum nella sua transizione ecologica ha scelto di adottare questo protocollo[42]. Anche questo meccanismo del consenso è considerato sicuro, sebbene vulnerabile a un attacco del 51%; un attaccante, in questo caso, non avrà bisogno del 51% di hashrate totale ma del 51% dei token totali. Tuttavia, se un hacker cercasse di acquisire il 51% dei token si avrebbe un duplice effetto che scongiurerebbe l'attacco.

Innanzitutto il mercato reagirebbe con un rapido aumento del prezzo dei token che segnalerebbe l'anomalia e inoltre un attacco avrebbe la controproducente conseguenza di rovinare la fiducia in quella blockchain e quindi nel valore del token.

[42] C. Cervi, "Ethereum passa al proof-of-stake: dopo lo stop al mining, cosa cambia?", *Money.it*, 2023, https://www.money.it/ethereum-passa-al-proof-of-stake-dopo-stop-al-mining-cosa-cambia.

La resistenza agli attacchi è fondamentale per le blockchain: senza protocolli di consenso affidabili, gli aggressori potrebbero facilmente manipolare o alterare i dati, compromettendo la fiducia nell'intero sistema. Grazie a questi protocolli, le blockchain possono funzionare come registri decentralizzati immutabili che sono praticamente immuni da interferenze esterne non autorizzate.

2.2.2 Automazione: gli smart contract

Il concetto di *smart contract* esiste dal 1994 quando Nick Szabo lo definì "un protocollo di transazione digitale che esegue i termini di un contratto", ma è nella blockchain che ha trovato un approdo ideale, che ne esalta le qualità: automatismi, trasparenza e sicurezza[43].
In questo contesto quindi quando parliamo di smart contract ci riferiamo ad un programma generico, salvato ed eseguito all'interno di una blockchain, in grado di avere tutte le caratteristiche di un contratto del mondo reale, in cui sono definite le regole e che automaticamente impone alle parti coinvolte di rispettarle.
Essi consentono di eseguire automaticamente determinate azioni quando certi parametri o condizioni predefinite vengono soddisfatti, eliminando la necessità di intermediari e garantendo l'adempimento degli accordi minimizzando la possibilità di azioni malevoli. L'accordo non è vincolato dalla legge, ma dal contratto stesso attraverso il consenso del network. A livello tecnico uno smart contract può essere visto come una funzione "if/then" incorporata in software informatici.
Il loro campo di applicazione è vasto e spazia dai servizi finanziari, in particolare nel settore assicurativo, ai registri di proprietà, alla gestione della supply chain, e ovunque vi sia la necessità di automatizzare processi basati sul raggiungimento di specifici parametri.
La blockchain Ethereum addebita una *gas fee* per ogni operazione effettuata sulla sua rete, come l'invio di Ether (ETH) o l'esecuzione di uno smart contract, che serve a remunerare i minatori o i validatori per l'esecuzione e la registrazione della operazione sulla blockchain. Il gas necessario per effettuare una transazione viene spesso paragonato al carburante usato da un'automobile per compiere un tragitto. Infatti nel nostro contesto il

[43] D. Aquaro, "Smart Contract: Cosa sono e come funzionano le clausole blockchain," *Il Sole 24 Ore*, 2019, https://www.ilsole24ore.com/art/smart-contract-cosa-sono-e-come-funzionano-clausole-blockchain-ACsDo2P?refresh_ce.

gas viene utilizzato per allocare le risorse della macchina virtuale di Ethereum[44] (EVM) in modo che le applicazioni decentralizzate come gli smart contract possano auto-eseguirsi in modo sicuro ma decentralizzato. L'unità di misura delle gas fee si calcola in piccole frazioni della criptovaluta Ether (ETH), comunemente indicato come wei (1 ETH = 10^18 wei = 10^9 gwei) e in pratica rappresentano il "prezzo" che gli utenti pagano per il potere computazionale necessario per processare e validare le transazioni sulla blockchain di Ethereum.

I pagamenti delle commissioni di gas su Ethereum sono stati rivoluzionati con l'introduzione dell'EIP-1559, che ha reso le tariffe più prevedibili e stabili. "EIP" sta per "Ethereum Improvement Proposal" (Proposta di Miglioramento di Ethereum) ed è stata una delle modifiche più significative del protocollo, introdotta nel 2019 ed implementata ad agosto 2021[45]. Oggi quando viene processata una transazione su Ethereum ci sono tre parametri da considerare: le unità di gas usate, la commissione di base e la commissione prioritaria. Il primo è il numero di wei da pagare per unità di gas e viene determinato in base alla domanda e all'offerta di transazioni. La componente dinamica del prezzo del gas (ovvero la "commissione di base") è stata riprogettata per essere più prevedibile. Prima dell'EIP-1559, gli utenti offrivano prezzi più alti per le loro transazioni in un'asta per garantire che venissero processate rapidamente, il che portava a fluttuazioni significative nelle tariffe. Con l'introduzione della commissione di base, che viene "bruciata"[46] (*burn*) per ridurre l'offerta di ETH, una parte della tariffa è stabilita in base all'attuale congestione della rete, rendendola più prevedibile. Infine, gli utenti possono ancora offrire una "mancia" o una commissione prioritaria ai minatori per accelerare il processamento delle loro transazioni, e questa parte può variare in base alla domanda e offerta.

Il costo totale di una transazione è quindi dato dalla formula:

[44] La *Ethereum Virtual Machine* o EVM è una macchina virtuale che ha la funzione di consentire l'esecuzione di programmi o smart contract al fine di distribuire una serie di funzionalità aggiuntive sulla blockchain in modo che gli utenti possano usufruirne. Fonte: *bit2meAcademy.*

[45] Ethereum.org, "Gas e commissioni," ultima modifica 10 luglio 2023, https://ethereum.org/it/developers/docs/gas/.

[46] Nel contesto delle criptovalute, il termine 'distruggere' un token o una moneta viene spesso descritto con il termine inglese '*burn*'. Esso si riferisce al processo di eliminazione permanente di una criptovaluta dal circolante, rendendola irrecuperabile.

Costo transazione = Unità di gas usate × (commissione di base + commissione prioritaria)

Oltre a remunerare il miner, il costo delle transazioni nella blockchain di Ethereum è necessario per bloccare eventuali attacchi o errori di programmazione nei contratti che potrebbero generare loop infiniti e sovraccaricare la blockchain. In questo senso il gas agisce da fattore limitante, che assicura Ethereum da attacchi eccessivamente costosi.

2.2.3 Interfaccia: gli oracoli

Gli smart contract sono eseguiti in un ambiente controllato e isolato (Ethereum Virtual Machine) e non possono interagire con il mondo al di fuori della blockchain. Come fare quindi nel caso di uno smart contract che abbia bisogno di alcuni dati dal mondo esterno per effettuare un calcolo? La risposta a questa domanda sono gli oracoli.
Gli oracoli sono servizi che prendono dati raccolti da fonti esterne alla blockchain (*off-chain*) e li mettono sulla blockchain stessa (*on-chain*) per renderli utilizzabili ai contratti intelligenti. Oltre a estrarre i dati off-chain e trasmetterli su Ethereum, gli oracoli possono anche immettere le informazioni prese dalla blockchain in sistemi esterni.[47]

2.3 Elementi fondamentali

Dopo aver presentato la blockchain e le sue caratteristiche essenziali, questo paragrafo si propone di esplorare tre aspetti che costituiscono i meccanismi fondamentali della DeFi. In primo luogo ci addentreremo nel mondo delle criptovalute e dei token, presentandone funzionalità e differenze. Successivamente ci focalizzeremo sulla regolazione della fornitura: un meccanismo essenziale per mantenere l'equilibrio e la stabilità del valore in un ambiente spesso volatile. Infine, affronteremo il concetto di *swap*, una procedura cruciale che permette scambi diretti tra asset digitali senza intermediari. Attraverso questa

[47] Ethereum.org, "Oracles," ultima modifica 17 luglio 2023, https://ethereum.org/it/developers/docs/oracles/.

analisi, si avrà una visione chiara e dettagliata di come questi elementi interagiscono e contribuiscono al funzionamento complessivo della DeFi.

2.3.1 Criptovalute e token

La più popolare applicazione per le tecnologie blockchains sono le criptovalute, tokens (solitamente di un numero limitato) crittograficamente sicuri e trasferibili. È importante però fare una distinzione tra criptovaluta e token[48].

Una criptovaluta è una valuta virtuale che, secondo la definizione di Banca d'Italia, costituisce una rappresentazione digitale di valore ed è utilizzata come mezzo di scambio o detenuta a scopo di investimento[49]. Ora sorge una questione: moneta e criptovaluta hanno le stesse funzioni?[50] Sappiamo che alle monete a corso legale vengono solitamente riconosciute le funzioni di unità di conto, riserva di valore e di mezzo di pagamento comunemente accettato. L'elevata volatilità delle cripto non consente sicuramente la funzione di misurare il valore di mercato di beni o servizi. Questo tipo di valute fluttuano molto anche all'interno di un singolo giorno, ciò rende impossibile il loro utilizzo di unità di conto. Per quanto riguarda la seconda funzione le criptovalute sono state progettate in modo che il loro numero totale sia limitato, il che potrebbe, in teoria, preservare il loro valore nel tempo, poiché non possono essere inflazionate. Infine esse hanno il potenziale per essere utilizzate come mezzo di scambio in futuro, specialmente poiché la tecnologia diventerà sempre più diffusa e accettata.

Per risolvere il problema dell'elevata volatilità è emersa una nuova classe di criptovalute: le *stablecoin*. Esse sono progettate per mantenere un valore stabile nel tempo, ancorato a valute fiat, metalli preziosi o panieri di beni, rendendole particolarmente adatte per essere utilizzate in transazioni e contratti. In questo modo le stablecoin riescono a coniugare i vantaggi della tecnologia blockchain, come efficienza e velocità delle transazioni, con la stabilità tipica delle valute tradizionali, risultando una forma di moneta digitale che può fungere effettivamente da unità di conto, mezzo di scambio e riserva di valore.

In base all'asset con il quale sono ancorate e garantite si possono distinguere principalmente tre categorie di stablecoin: le *fiat-collateralized*, le *cripto-collateralized* e

[48] C.R. Harvey, A. Ramachandran e J. Santoro, *DeFi and the Future of Finance* (Wiley, 2021).
[49] Banca d'Italia, "Avvertenza sulle valute virtuali," 2015, https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/index.html.
[50] CONSOB, "Criptovalute," https://www.consob.it/web/investor-education/criptovalute.

le *non-collateralized.* La maggior parte di stablecoin sono del primo tipo, in quanto il loro valore è ancorato ad una riserva di asset target reali off-chain, solitamente controllati da entità esterne. Questo è il caso di Tether (USDT) e USDC, che insieme raggiungono circa i 108 miliardi di dollari di capitalizzazione di mercato, l'87% del mercato complessivo delle stablecoin[51]. Le stablecoin cripto-collateralized sono invece garantite da altre criptovalute, piuttosto che da asset tradizionali come valute fiat o metalli preziosi. A causa della volatilità intrinseca delle criptovalute, queste stablecoin spesso richiedono un surplus di cripto-asset come collaterale, sono cioè sovracollateralizzate. Questo tipo di stablecoin è più decentralizzato rispetto alle stablecoin fiat-collateralized perché non dipende da istituzioni finanziarie per la custodia degli asset garanti. DAI, la stablecoin creata dal protocollo MakerDAO, garantita da ETH e altre cripto, è l'esempio più noto di questa categoria. Le non-collateralized, d'altro canto, non sono garantite da nessun tipo di asset e per mantenere il loro valore utilizzano meccanismi come algoritmi di controllo della domanda e dell'offerta. Queste stablecoin sono completamente decentralizzate e non dipendono da entità esterne per mantenere il loro valore, ma sono anche le più complesse da progettare e implementare efficacemente e potrebbero essere più vulnerabili a volatilità e ad attacchi di mercato.

Una criptovaluta, intesa come moneta (*coin*), può essere vista come un oggetto digitale il cui unico scopo è quello di trasferire valore. Quando si parla di BTC (Bitcoin), BNB (Binance) o USDT (Tether) solitamente si usa il termine moneta per sottolineare la loro funzione di mezzo di scambio di valore[52]. Se aggiungiamo le potenzialità di uno smart contract a una criptovaluta possiamo creare delle criptovalute con funzionalità che vanno oltre il semplice trasferimento di valore: in questo caso si parla di token. L'Osservatorio Digital Innovation del Politecnico di Milano ha definito il token come "un'informazione digitale, registrata su un registro distribuito, univocamente associata a uno e un solo specifico utente del sistema e rappresentativa di una qualche forma di diritto: la proprietà di un asset, l'accesso a un servizio, la ricezione di un pagamento, e così via".

La prima distinzione che è necessario fare è tra token fungibili e non fungibili.

I token si definiscono fungibili se rappresentano beni che sono interscambiabili l'uno con l'altro, cioè ogni unità del token ha lo stesso valore e le stesse caratteristiche delle altre

[51] DeFiLlama, Stablecoin Market Cap. https://defillama.com/stablecoins. Consultato il 20 luglio 2023.
[52] Chiap et al., *Blockchain*, 110.

unità. Pensiamo ad esempio alla moneta da 1€, essa vale esattamente quanto ogni altra moneta da 1€.

L'interfaccia più comune di questi token su Ethereum è ERC-20, intendendo per interfaccia un set minimo di funzionalità richiesto. Grazie a questo standard numerosi token fungibili possono essere facilmente utilizzati su piattaforme decentralizzate, come forma di scambio, collaterale o ricompensa.

L'interfaccia ERC-20 definisce la seguente funzionalità di base:

- totalSupply() - dice quante unità di un determinato token esistono in totale;
- balanceOf(account) - legge il saldo del token per un determinato account;
- transfer(indirizzo destinatario, quantità) - invia una certa "quantità" di token dal mittente della transazione all'indirizzo del destinatario;
- transferFrom(indirizzo mittente, indirizzo destinatario, quantità) - permette a una terza parte (come uno smart contract) di trasferire token per conto di un utente, a condizione che tale utente abbia precedentemente concesso l'autorizzazione attraverso la funzione approve();
- approve(spender, quantità) - un utente può autorizzare un altro indirizzo, spesso uno smart contract, a prelevare un certo numero di token dal proprio saldo;
- allowance(indirizzo proprietario, indirizzo spender) - indica il saldo "approvato" che uno spender può ancora prelevare.

Il contratto rifiuterà trasferimenti che coinvolgono saldi insufficienti o spese non autorizzate.

A seconda delle modalità di utilizzo i token ERC-20 si dividono in tre categorie:

- *Utility token*: sono dei token che forniscono esclusivamente un diritto di accesso a un servizio. Il suo valore è correlato alla domanda effettiva per tale token e non è pensato come strumento di investimento.
- *Security token*: un security token rappresenta un investimento digitale e può rappresentare la proprietà di un asset, come azioni di una società, obbligazioni, partecipazioni in fondi di investimento o altri diritti di proprietà o reddito.
- *Governance token*: sia i token di governance che gli equity token (un sottotipo dei security token) rappresentano una quota della società, ma i primi si riferiscono ai diritti di voto. Questi token danno ai detentori il diritto di influenzare le decisioni

all'interno di un sistema o una piattaforma, come votare su proposte di modifiche o sugli aggiornamenti del protocollo.

I token non fungibili (NFT) hanno la caratteristica di essere unici, non sostituibili, non ripetibili e non divisibili[53]. Su Ethereum lo standard che definisce la non fungibilità è ERC-721. È simile all'ERC-20, ma invece di memorizzare tutti gli ID come un saldo unico, ogni unità ha un proprio ID unico che può essere collegato a metadati aggiuntivi, che lo differenziano da altri token derivanti dallo stesso contratto. Il valore distintivo degli NFT consiste nella loro capacità di collegare il mondo finanziario e quello non finanziario tramite oggetti da collezione (ad esempio un token potrebbe rappresentare la proprietà di un'opera d'arte, un video, musica, o anche un tweet).

2.3.2 Regolazione della fornitura

La regolazione della fornitura si applica specificamente ai token fungibili e alla capacità di creare (coniare) e ridurre (bruciare) la fornitura tramite un contratto intelligente. Bruciare un token significa rimuoverlo dalla circolazione e può essere fatto in due modi: inviarlo manualmente a un indirizzo Ethereum non posseduto o, più efficientemente, creare un contratto che non è in grado di spenderlo. I motivi per distruggere (*burn*) riserve di token possono essere molteplici e dipendono dalla piattaforma e dal fine che si vuole ottenere. Alcuni esempi d'uso sono: rappresentare l'uscita da una pool e il riscatto del sottostante (comune nei token di equity come cTokens per Compound), aumentare la scarsità per far salire il prezzo e penalizzare comportamenti scorretti.

Aumentare (*mint*) la fornitura è un processo che si esegue, tra gli altri, nei casi opposti a quelli sopracitati: per rappresentare l'ingresso in una pool e acquisire una quota di proprietà corrispondente, aumentare le riserve per abbassare il prezzo, ricompensare comportamenti degli utenti.

La fornitura di token è regolata in base ad una "curva di legame" (*bonding curve*), che permette di determinare il prezzo di un token in base alla sua fornitura corrente[54]. Immaginiamo una bonding curve molto semplice, dove *TKN* è il prezzo del token e *S*

[53] Borsa Italiana. "Differenza tra token fungibili e token non fungibili." https://www.borsaitaliana.it/notizie/sotto-la-lente/differenza-tra-token-fungibili-e-token-non-fungibili.htm.

[54] Harvey, Ramachandran e Santoro, DeFi and the Future of Finance, 42-46.

indica la fornitura. Questa banale relazione è rappresentata dall'equazione $TKN = c$, significa che ogni token (*TKN*) ha sempre un prezzo fisso di *c* ETH, indipendentemente da quanti token sono in circolazione. Per esempio *se* $c = 1$, ETH e *TKN* sono sempre scambiati in un rapporto 1:1 (Figura 2.4)

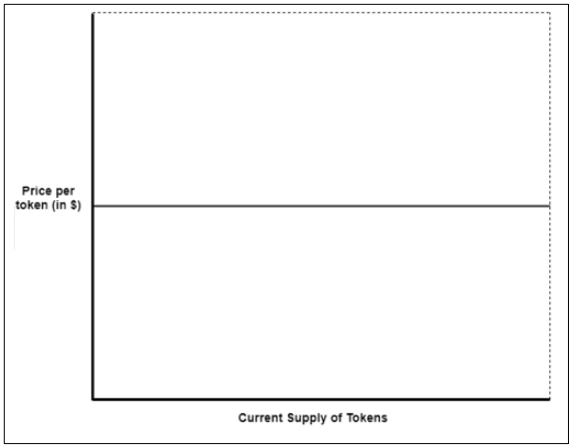


Figura 2.4: Curva di legame costante. Fonte: *phemex*

Se consideriamo una curva di legame lineare, rappresentata dalla formula $TKN = m \cdot S + c$, dove *m* è la pendenza e *c* l'intercetta della curva, allora il prezzo del token cambierà linearmente con la fornitura. Se $m = 1$ e $c = 0$, il prezzo sarebbe perfettamente correlato con le riserve del token: quando compri il primo token, ti costerà 1 ETH, se vuoi comprare un altro token, il prezzo per il secondo token sarà di 2 ETH, il terzo costerà 3 ETH, e così via (Figura 2.5).

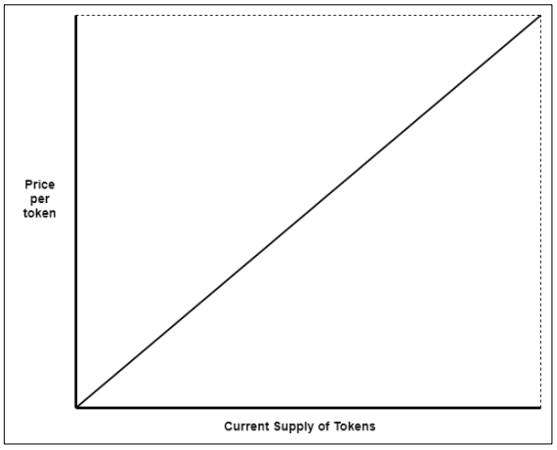


Figura 2.5. Curva di legame lineare. Fonte: *phemex*

Con una curva di legame del genere, monotona crescente, gli investitori che acquistano i token nelle fasi iniziali possono trarre beneficio man mano che la fornitura aumenta. Ogni token acquistato o emesso ne fa crescere il valore e ciò permette agli investitori precoci di detenere un qualcosa che avevano pagato molto meno. Ovviamente vale anche il contrario: se la domanda diminuisse il valore del token diminuirebbe.

La curva può essere rappresentata come un singolo smart contract con opzioni per l'acquisto e la vendita del token sottostante. Il token da vendere può avere una fornitura illimitata, con la curva di legame che funge da emittente autorizzato, oppure una fornitura massima predeterminata che viene accantonata nel contratto della curva. Quando gli utenti acquistano i token, la curva di legame mette in garanzia i fondi ricevuti per un momento futuro in cui tali utenti potrebbero volerli rivendere contro la curva.

Il tasso di crescita, *m*, è importante per determinare le prestazioni degli utenti. Rispetto al caso presentato prima, un ritorno ancora più estremo potrebbe derivare da un tasso di crescita superlineare, come $TKN = S^2$ (Figura 2.6). Il primo token costerebbe 1 ETH e il centesimo costerebbe 10.000 ETH.

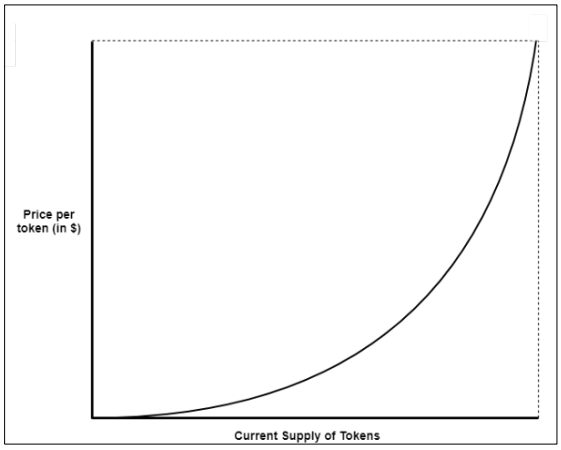


Figura 2.6. Curva di legame superlineare. Fonte: *phemex*

Nella realtà, la maggior parte dei progetti adotta un tasso di crescita sublineare. Questo comporta che, mentre l'aumento dell'offerta di token, l'incremento del prezzo del token rallenta progressivamente, seguendo spesso una dinamica logistica. Quest'ultima, come mostrato in Figura 2.7, ha una forma ad "S", cioè inizia con una crescita lenta, poi accelera

in una fase di crescita rapida e infine rallenta di nuovo, convergendo verso un prezzo massimo predeterminato. Questo approccio riduce la volatilità ed evita prezzi eccessivamente elevati e potenziali bolle speculative.

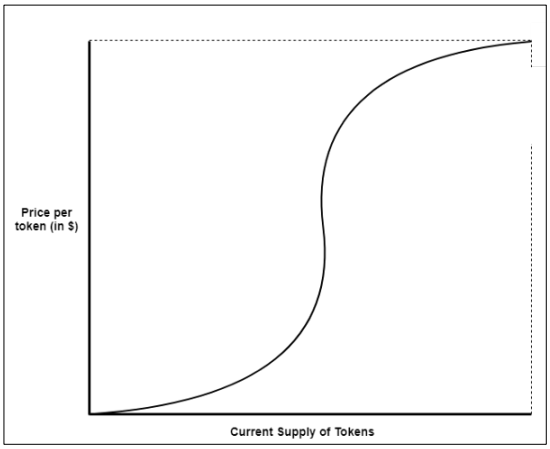


Figura 2.7. Curva di legame logistica. Fonte: *phemex*

Molti protocolli utilizzano una curva di legame con una relazione di prezzo diversa per gli acquirenti e per i venditori, in cui la curva di vendita ha un tasso di crescita o un'intercetta inferiore rispetto alla curva di acquisto. Questa differenza tra le due curve è il valore accumulato dallo smart contract e potrebbe rappresentare una commissione per l'uso o essere utilizzata per finanziare funzionalità più complesse all'interno del sistema.

2.3.3 Funzionamento degli scambi

Uno swap è semplicemente l'interscambio di un tipo di token con un altro. I fondi sono custoditi in uno smart contract e possono essere prelevati prima che lo scambio sia completato. La transazione avviene solo se tutte le condizioni sono rispettate, se invece non lo sono la transazione è annullata e i fondi restano al sicuro.
Gli operatori di criptovalute hanno due opzioni per gli scambi: utilizzare un exchange centralizzato (CEX) gestito da un intermediario, oppure un exchange decentralizzato (DEX) dove le transazioni sono facilitate da algoritmi.
Un CEX (*Centralized Exchange*) è una piattaforma di scambio di criptovalute che funziona come intermediario tra gli acquirenti e i venditori. Sono gestiti da organizzazioni centralizzate che detengono la custodia delle criptovalute dell'utente e facilitano le

transazioni. Gli utenti di un CEX depositano i loro fondi direttamente sulla piattaforma e realizzano transazioni attraverso ordini che l'exchange abbinerà. Esempi noti di CEX includono Binance, Coinbase e Kraken, e sebbene offrano una maggiore liquidità e facilità d'uso rispetto ai DEX, i CEX possono essere obiettivi di attacchi hacker, dato che conservano grandi quantità di criptovalute in un unico luogo essendo centralizzati.

Per quanto riguarda i DEX (*Decentralized Exchange*) esistono due meccanismi principali[55]: l'abbinamento tradizionale degli ordini (*Order-book Matching*) o un sistema automatizzato chiamato AMM (*Automated Market Makers*).

Un Order-book Matching richiede che in un DEX le parti concordino su un tasso di scambio. I fornitori di mercato stabiliscono offerte e chiedono prezzi e le transazioni avvengono quando un altro utente accetta quel prezzo. Questo sistema può essere lento e costoso poiché gli aggiornamenti necessitano di transazioni sulla blockchain. Un grande svantaggio è che entrambe le parti devono essere pronte a scambiare al tasso concordato, limitando la flessibilità.

Un Market Maker Automatico (AMM) è un tipo di smart contract che detiene risorse in coppie di trading e stabilisce un prezzo basato sull'equilibrio tra queste risorse. Invece di avere un rapporto di prezzo fisso, un AMM adeguato modifica il suo prezzo in base alle condizioni correnti del mercato, cercando di evitare squilibri e sfruttamenti arbitrari. Questo meccanismo fa sì che acquistare una risorsa diventi progressivamente più costoso man mano che la sua disponibilità all'interno dell'AMM diminuisce. Un vantaggio fondamentale degli AMM è la loro costante disponibilità: sono sempre pronti ad eseguire transazioni, eliminando la necessità di una controparte tradizionale. Ciò riduce notevolmente i rischi associati alle transazioni poiché gli utenti mantengono la custodia dei loro fondi fino al completamento dello scambio. Un altro vantaggio è la "liquidità componibile". In sostanza, un AMM può sfruttare la liquidità e i tassi di cambio da un altro, rendendolo estremamente adattabile e interconnesso nel ecosistema DeFi. Questa interconnettività viene spesso paragonata ai "DeFi Legos", alludendo alla capacità di costruire soluzioni complesse combinando semplici "mattoncini" finanziari.

Lo svantaggio principale di un AMM è la "perdita impermanente". Si tratta della dinamica del costo opportunità tra offrire attività per lo scambio e il mantenere tali attività per potenzialmente beneficiare delle variazioni dei prezzi. Questa perdita è definita

[55] Ibid., 50-54

"impermanente" perché può essere recuperata se il prezzo torna al suo valore originale[56]. Per capire meglio si consideri 100 unità di due assets A e B, che vengono scambiati in un rapporto di 1:1 nell'AMM, indicando che hanno lo stesso valore all'interno di quel contratto. Con il passare del tempo, i prezzi nel mercato esterno cambiano (per esempio su Coinbase). L'asset B diventa particolarmente prezioso, raggiungendo un valore di 4 ETH, mentre l'asset A si apprezza solo a 2 ETH. Dal momento che l'AMM mantiene erroneamente un rapporto di cambio fisso di 1:1 tra A e B, gli arbitraggisti vedono un'opportunità. Scambiano tutto il loro asset A per l'asset B all'interno dell'AMM, perché all'interno dell'AMM possono ottenere l'asset B (che nel mercato esterno vale 4 ETH) in cambio di A che vale solo 2 ETH nel mercato esterno. Dopo aver ottenuto l'asset B dal contratto AMM a un tasso favorevole, gli arbitraggisti lo vendono nel mercato esterno ricavando 800 ETH (4 ETH * 200 unità). Dopo che gli arbitraggisti hanno sfruttato questa opportunità, l'AMM si ritrova senza alcuna unità di B e con 200 unità di A. Valutando queste 200 unità di A al prezzo esterno di 2 ETH/unità, l'AMM ha ora un totale di 400 ETH di valore. Se l'AMM avesse potuto aggiornare i suoi prezzi in tempo reale o se avesse potuto vendere l'asset B prima che gli arbitraggisti ne approfittassero, avrebbe avuto un valore totale di 600 ETH. Invece, ha solo 400 ETH. La differenza di 200 ETH rappresenta la perdita impermanente. Questa perdita è "impermanente" perché, se in futuro i prezzi degli asset tornassero ai valori originali e l'AMM avesse quantità uguali di entrambi gli asset, allora non ci sarebbe più alcuna perdita.

2.4 dApp

Nell'ambito della trasformazione digitale, il concetto di Web3 rappresenta una nuova era dell'internet. A differenza del Web2, che ha visto il dominio di piattaforme centralizzate high tech come Facebook, Google e Amazon, il Web3 mira ad un'architettura internet più decentralizzata. Si basa sulla tecnologia blockchain, che consente transazioni e interazioni

[56] Binance Academy. "Impermanent Loss Explained." https://academy.binance.com/it/articles/impermanent-loss-explained.

peer-to-peer (P2P) senza la necessità di intermediari[57]. In questo contesto, Ethereum e le altre blockchain hanno dato origine alle applicazioni decentralizzate, o dApp.

Quindi le dApp sono software open source che funzionano su una rete peer-to-peer basata sulla tecnologia blockchain e che a differenza delle applicazioni tradizionali, queste applicazioni eliminano la necessità di intermediari centralizzati, permettendo interazioni dirette e trasparenti tra gli utenti all'interno dell'ecosistema. La loro caratteristica decentralizzata implica che, una volta che uno sviluppatore ha pubblicato il codice sorgente di una dApp, altri hanno la possibilità di svilupparla ulteriormente (*permissionlessness*)[58]. Un altro aspetto fondamentale è la loro "resistenza alla censura" (*censorship resistance*). Questa caratteristica, grazie alla natura decentralizzata, evidenzia la capacità di un'applicazione di sottrarsi a tentativi esterni di alterare, bloccare o censurare informazioni. In altre parole chiunque può usare le dApp, ma nessun singolo individuo può controllarle.

Un concetto diverso ma strettamente collegato è la DAO (*Decentralized Autonomous Organization*). Questo nuovo tipo di struttura organizzativa, che il Sole24Ore definisce "azienda decentralizzata"[59], costruita con la tecnologia blockchain, ha la sua natura autonoma nelle sue regole di funzionamento incorporate negli smart contract[60]. In questi protocolli la governance è delegata agli shareholder, i quali, attraverso l'utilizzo di un token di governance, possono esercitare i loro diritti decisionali partecipando a votazioni. Attraverso questo meccanismo si assicura un sistema decisionale decentralizzato, in cui coloro che hanno un interesse diretto nel protocollo hanno anche voce nelle sue evoluzioni e direzioni future.

---

[57] Valeria Portale e Jacopo Fracassi. "Dentro la rivoluzione: la finanza DeFi e i nuovi business model." Il Sole 24 Ore. 10 dicembre 2021. https://www.ilsole24ore.com/art/dentro-rivoluzione-finanza-defi-e-nuovi-business-model-AEb27ZUB

[58] Alexander S. Gillis e Corinne Bernsteiun. "Blockchain dApp (decentralized application)." TechTarget. 2022. https://www.techtarget.com/iotagenda/definition/blockchain-dApp.

[59] Marco Trabucchi. "Con la prima DAO riconosciuta in Italia si sperimenta l'azienda decentralizzata." Il Sole 24 Ore. 11 ottobre 2022. URL: https://www.ilsole24ore.com/art/con-prima-dao-riconosciuta-italia-si-sperimenta-l-azienda-decentralizzata-AEXVnU7B.

[60] Kevin Roose. "What Are DAOs?" The New York Times. 18 marzo 2022. URL: https://www.nytimes.com/interactive/2022/03/18/technology/what-are-daos.html.

2.5 Stratificazione

Alla luce di quanto esposto finora possiamo delineare una visione olistica della finanza decentralizzata. La DeFi si articola in una serie di strati (*layer*) interconnessi, disposti gerarchicamente, dove ciascun livello trae fondamento e funzionalità da quello sottostante. Questa strutturazione stratificata assicura che ogni segmento abbia un ruolo distintivo e cruciale nell'ecosistema complessivo, garantendo l'efficienza e l'innovazione dell'intera architettura finanziaria decentralizzata[61].

Come mostrato nella Figura 2.8 l'architettura si identifica in cinque livelli distinti:

i. *Settlement layer*: consiste nella blockchain e nel suo protocollo nativo (ad esempio BTC sulla blockchain di Bitcoin e ETH sulla blockchain di Ethereum). Funziona come un registro distribuito e garantisce che tutte le transazioni siano sicure, immutabili e decentralizzate.

ii. *Asset layer*: consiste in tutti gli asset che vengono emessi sopra il livello1. Include gli asset di protocollo nativi e qualsiasi asset aggiuntivo che viene emesso su questa blockchain (token).

iii. *Protocol layer*: comprende i protocolli fondamentali della DeFi, come gli scambi decentralizzati, i protocolli di prestito o i mercati dei derivati.

iv. *Application layer*: crea applicazioni orientate all'utente che si connettono ai singoli protocolli. L'interazione con gli smart contract è solitamente agevolata da un'interfaccia basata su browser web, rendendo i protocolli più facili da utilizzare.

v. *Aggregation layer*: è il layer "frontend" della DeFi. Gli aggregatori mettono insieme alcune applicazioni, creando piattaforme orientate all'utente. Di solito forniscono strumenti per confrontare e valutare i servizi e permettono agli utenti di semplificare l'esecuzione di compiti altrimenti complessi, connettendosi a diversi protocolli contemporaneamente e combinando informazioni rilevanti in modo chiaro e conciso.

[61] Schär, Fabian. "Decentralized Finance: On Blockchain and Smart Contract based Financial Markets." Center for Innovative Finance, University of Basel; scritto il 8 marzo 2020.

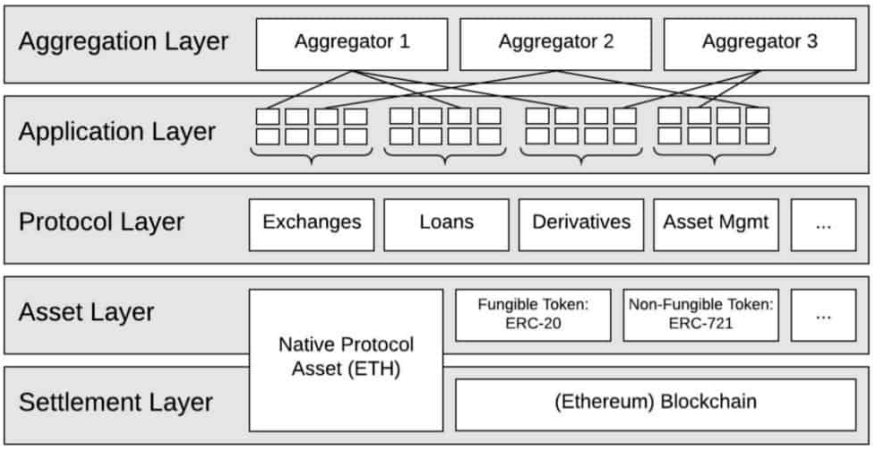


Figura 2.8. Stratificazione della DeFi. Fonte: *Schär, Fabian*. "Decentralized Finance: On Blockchain and Smart Contract based Financial Markets."

CAPITOLO 3 - SERVIZI FINANZIARI NELLA DEFI

Nel mondo in rapida evoluzione della finanza decentralizzata, le dApp stanno emergendo come pilastri innovativi che rivoluzionano il panorama finanziario tradizionale. Queste dApp, alimentate dalla tecnologia blockchain, promettono di affrontare e superare le sfide e le inefficienze della finanza convenzionale, molte delle quali sono state discusse nel primo capitolo. Qui esploreremo le dApp più influenti e innovative che operano in settori critici come il lending/credit, i DEXes (scambi decentralizzati) e i derivati, delineando il loro funzionamento e analizzando come ciascuna di esse si pone come soluzione ai problemi della finanza tradizionale. Attraverso un'analisi dettagliata, concentrata maggiormente sulla piattaforma più popolare Ethereum, sveleremo come questi protocolli decentralizzati stiano non solo reinventando i servizi finanziari, ma anche plasmando il futuro della finanza come non avremmo neanche immaginato.

3.1 Prestiti

Iniziamo con le applicazioni di lending quali MakerDAO, Compound e Aave, che offrono soluzioni di credito innovative, democratizzando l'accesso al capitale e ponendosi come validi competitor ai sistemi tradizionali.

3.1.1 MakerDAO

MakerDAO, nata dalla visione di Rune Christensen, attuale CEO della Maker Foundation, ha mosso i suoi primi passi nel marzo del 2015. Il cuore pulsante del progetto, il DAI, ha visto la sua prima menzione in un post di Christensen su Reddit intitolato "Presentazione di eDollar, la stablecoin definitiva costruita su Ethereum". In quel contesto emergeva l'ambizione di Christensen di fondare una DAO su Ethereum con l'obiettivo di lanciare una stablecoin ancorata al valore del dollaro e di creare un ecosistema comunitario, dove la governance del protocollo offrisse opportunità esclusive ai suoi partecipanti[62].

[62] BrightNode. "La storia del progetto MakerDAO." BrightNode, 2021. https://brightnode.io/it/la-storia-del-progetto-makerdao/.

MakerDAO è uno dei progetti più noti della finanza decentralizzata e funziona come una banca che svolge attività di prestito crittografico e offre altre funzionalità come diritti in termini di governance. Il protocollo Maker sfrutta gli smart contract di Ethereum per automatizzare la collateralizzazione e il prestito della sua stablecoin decentralizzata DAI ancorata al dollaro. Ciò significa che la stablecoin funziona in maniera autonoma senza che un'autorità esterna provveda a garantirla, custodirla e controllarla.

MakerDAO è un modello a due token, che aggiunge a DAI anche il governance token MKR. I detentori di MKR garantiscono la stabilità, la trasparenza e l'efficienza del DAI gestendo il protocollo Maker e i rischi finanziari attraverso un sistema di governance scientifica che include sondaggi e meccanismi di votazione esecutiva. Un token MKR fissato in un contratto di votazione[63] è pari a un voto[64].

Come si generano i DAI?

1. Creazione del *vault*: un utente crea un Maker Vault (o semplicemente vault) e vi deposita una certa quantità di criptovaluta come garanzia, ETH o qualsiasi altro asset supportato da ERC-20 come collaterale. Il vault è uno smart contract che prende in pegno il collaterale e monitora in tempo reale il valore, denominato in USD, del collaterale stesso.
2. Generazione di DAI: una volta depositato il collaterale, l'utente può generare (cioè prendere in prestito) DAI fino a un certo limite, determinato dal rapporto di indebitamento del collaterale specifico. Questo crea un debito in DAI che andrà restituito al vault. Nel frattempo l'utente può disporre dei DAI come crede, per esempio può venderli in cambio di valute fiat oppure scambiarli con altre cripto per iniziare un processo di leveraging.
3. Mantenimento del rapporto di indebitamento: gli utenti devono mantenere questo rapporto al di sopra di un certo livello minimo e se il valore del collaterale scende eccessivamente a causa delle fluttuazioni del mercato cripto, il vault può essere "liquidato", il che significa che parte del collaterale viene venduto per rimborsare il DAI prestato e per pagare una penale. A causa della volatilità di ETH o degli altri asset, infatti, il DAI generato è *over-collateralized* solitamente del 150-200%.

[63] Il contratto di votazione assicura ai detentori di MKR la possibilità di votare in base al peso degli MKR fissati.
[64] MakerDAO. "Il Protocollo Maker." Whitepaper, 2020. https://makerdao.com/it/whitepaper/#il-protocollo-maker.

4. Rimborso e recupero del collaterale: gli utenti possono restituire il DAI per recuperare il loro collaterale. Pagando una "stability fee" (tasso di interesse), l'utente può recuperare il proprio collaterale e chiudere il vault.

Una domanda che può sorgere spontanea è: perché si dovrebbe voler prendere in prestito DAI pur avendo già accesso a liquidità o altri tipi di asset? Ecco alcune delle motivazioni più comuni:

- Spese inattese: se un individuo detiene una significativa quantità di criptovaluta e si trova a dover fronteggiare una spesa inaspettata o urgente, potrebbe non voler vendere immediatamente la sua criptovaluta.
- Leverage: se un investitore è ottimista riguardo al futuro rialzo di un particolare asset (es. Ethereum), potrebbe decidere di depositare quel bene come collaterale e prendere in prestito DAI per acquistare ulteriori quantità dello stesso asset. Se l'asset apprezza come previsto, l'investitore può trarre profitto da entrambe le posizioni, pagare il debito in DAI e conservare la differenza come profitto.
- Implicazioni fiscali: la vendita di criptovalute, quando vi è necessità di contanti, potrebbe comportare l'incasso di una plusvalenza tassabile. Prendendo in prestito DAI garantendoli con criptovaluta, l'individuo può ottenere liquidità senza innescare un evento tassabile.
- Diversificazione del portafoglio: un investitore potrebbe desiderare di diversificare il proprio portafoglio senza vendere le proprie criptovalute.
- Opportunità di arbitraggio: ci potrebbero essere opportunità di arbitraggio sui tassi in diversi mercati o piattaforme. Gli utenti possono prendere in prestito criptovaluta per sfruttare queste differenze di prezzo in maniera immediata.

Consideriamo un esempio. Un possessore di ETH ha bisogno di liquidità, ma non vuole vendere i suoi ETH perché pensa che si apprezzeranno. L'investitore ha 5 ETH ad un prezzo di mercato di $200 (valore totale $1000). Se la collateralizzazione richiesta è del 150% allora egli può generare al massimo 667 DAI (= $1000/1.5). Se l'utente prende tutti i 667 DAI e il valore di ETH scendesse sotto $200 allora il prestito non sarebbe più collateralizzato e il vault liquidirebbe automaticamente una parte del collaterale, oltre ad una penalità di liquidazione che viene detratta per coprire i costi associati al processo di liquidazione. Questo processo è l'equivalente della *margin call* nella finanza tradizionale, ma nel nostro caso il processo di liquidazione avverrebbe in maniera automatizzata e

immediata. Solitamente gli utenti decidono di generare meno di 667 DAI, in modo da darsi un margine di tolleranza (*buffer*). Mettiamo il caso che l'investitore prenda in prestito 500 DAI, che equivale ad un collateralization ratio di 2.0 (= $1000/500) e immaginiamo due scenari.

Nel primo supponiamo che il prezzo di ETH cresce del 50%, così che il collaterale vale adesso $1500; in questo caso l'investitore può aumentare la dimensione del suo prestito di 250 DAI (750 DAI totali, mantenendo il rapporto di collateralizzazione a 2).

L'altro scenario, più interessante, è quello in cui il valore di ETH diminuisce del 25% da $200 a $150: in questo caso il valore del collaterale scende a $750 e il fattore di collateralizzazione diventa 1.5 (= $750/500).

Il vault holder, ovvero l'utente che ha creato il vault, ha adesso tre alternative:

1. Può incrementare il valore del collaterale, per esempio aggiungendo 1 ETH. La garanzia andrebbe a valere $900 ($150 x 6) e il prestito tornerebbe ad essere notevolmente sovracollateralizzato, con un rapporto di 1.8 (= $900/500).
2. Può usare 500 DAI per ripagare il prestito e riottenere i 5 ETH, che ora valgono $250 meno, ma questa svalutazione si sarebbe verificata anche senza il loro utilizzo nel prestito.
3. L'ultima possibilità è che il prestito venga liquidato da un *keeper*, ovvero un partecipante del sistema che monitora costantemente la salute dei prestiti e l'adeguatezza del collaterale. Se il rapporto di collateralizzazione scende al di sotto di una soglia minima prestabilita, il keeper ha il diritto di liquidare una porzione del collaterale al fine di ripristinare un adeguato livello di sicurezza per il prestito. Questo processo generalmente comporta la vendita di una parte del collaterale ad un prezzo scontato, assicurando così che il sistema sia sempre sufficientemente collateralizzato. La differenza tra il valore di mercato del collaterale venduto e il prezzo scontato può essere considerata come una sorta di penale imposta al vault holder per non aver mantenuto il prestito adeguatamente collateralizzato. La situazione nel dettaglio è la seguente: per ripagare i 500 DAI il keeper vende 3.33 ETH (= 500/750 x 5), 1.47 ETH vengono restituiti al vault holder e 0.2 ETH sono la penalità di liquidazione che si intasca il keeper per monitorare i vault e vendere i collaterali in caso di sotto collateralizzazione.

L’intero ecosistema di MakerDAO dipende dall’ancoraggio 1:1 del DAI al dollaro americano. Questo è permesso da vari meccanismi in grado di stimolare la domanda o l’offerta consentendo così il mantenimento del rapporto.

Il primo è la cosiddetta *stability fee*, un tasso di interesse variabile che i vault holders pagano in DAI su ogni debito di DAI che hanno generato. Questa fee assicura la stabilità del valore del DAI rispetto al dollaro e ha diverse funzioni: serve come incentivo economico per incoraggiare gli utenti a restituire il DAI piuttosto che mantenerlo in prestito a lungo termine, aiuta nella gestione della domanda e dell'offerta di DAI regolandone la circolazione e fornisce un reddito al sistema, compensando i detentori di token MKR che partecipano alla sua governance.

Parallelamente il sistema MakerDAO ha introdotto il *DAI Savings Rate* (DSR), che offre un tasso di interesse ai detentori di DAI che bloccano le loro monete, incentivando la domanda e contribuendo ulteriormente alla stabilità del “peg” 1:1 con il dollaro. L’analoga situazione avviene nella finanza centralizzata, dove il tasso sui prestiti è maggiore del tasso sui depositi.

Infine vi è il limite di debito (*debt ceiling),* che riguarda la quantità massima di DAI che può essere emessa a fronte di un particolare tipo di collaterale. Questo limite viene stabilito per garantire che non vi sia un'eccessiva emissione di DAI basata su un singolo tipo di collaterale, mitigando così i rischi associati ad una eccessiva esposizione a un particolare asset.

Per completare il quadro di questo rivoluzionario protocollo decentralizzato passiamo ora all’analisi del token Maker (MKR) e del sistema di governance. Come ogni DAO, la governance è decentralizzata e appartiene agli shareholder. Il token MKR, il governance token del protocollo Maker, consente a chi lo detiene di votare sulle modifiche del protocollo. I possessori di MKR prenderanno decisioni per i migliori interessi finanziari per la piattaforma. I possessori di questo token sono di fatto i possessori dell’organizzazione (come lo sono gli azionisti di una società) e sono interessati al benessere della piattaforma per incrementare il valore dei loro token (quota). Votano e decidono su ogni tipo di questione, come se accettare nuovi collaterali, aggiungere nuove

funzionalità oppure addirittura distribuire “dividendi”, generati dalla differenza tra il tasso d’interesse incassato dai prestiti e il DAI savings rate (DSR). [65]

Se i detentori dei token MKR non gestiscono adeguatamente il protocollo, come ad esempio se scelgono tassi di interesse o parametri inappropriati, potrebbero destabilizzare il DAI e far emergere problematiche tali da mettere a rischio l'intero ecosistema. In questi casi può attivarsi un meccanismo di emergenza chiamato *global settlement*, una procedura di sicurezza progettata per proteggere gli utenti in scenari estremi, che, una volta avviata, sospende tutte le attività del sistema: non si può più generare DAI o creare nuovi vault. Contestualmente viene stabilito un prezzo fisso per i collaterali basato su un feed esterno di prezzo e chi possiede DAI ha la possibilità di convertirlo in una quantità proporzionale del collaterale al prezzo stabilito. I proprietari dei vault possono recuperare la parte in eccesso del loro collaterale, ma solo dopo aver saldato il loro debito in DAI al prezzo predeterminato[66].

MakerDAO è stato il pilastro fondamentale nella nascita della finanza decentralizzata. La sua criptovaluta, il DAI, non solo ha rivoluzionato il settore non solo grazie al suo ancoraggio stabile al dollaro, ma anche per il suo innovativo meccanismo di collateralizzazione basato su Ethereum. Questa combinazione ha reso DAI una delle principali stablecoin nel panorama delle criptovalute, garantendo affidabilità e trasparenza nel suo utilizzo.

Concludiamo l’analisi della piattaforma Maker spiegando perché questo protocollo decentralizzato ha creato un punto di rottura con la finanza tradizionale, offrendone una valida alternativa. Evidenziamone brevemente i principali punti di forza e le innovative soluzioni rispetto ad un sistema centralizzato.

Nella TradFi i tassi di interesse e le regole sui prestiti sono decisi da enti intermediari e regolamentativi, mentre in MakerDAO il governo della piattaforma è affidata completamente ai detentori dei token di governance, i quali hanno i migliori interessi per il bene finanziario dell’organizzazione. Qualunque tipo di prestito, eccetto un *flash loan* (vedremo in seguito di cosa si tratta), richiede una garanzia. Nella finanza tradizionale

[65] MakerDAO. "Governance del Protocollo Maker." Whitepaper, 2020. https://makerdao.com/it/whitepaper/#governance-del-protocollo-maker.
[66] MakerDAO. "Chiusura di Emergenza." Whitepaper, 2020. https://makerdao.com/it/whitepaper/#chiusura-di-emergenza.

questa garanzia è costituita dalla propria affidabilità creditizia e l'accesso ai servizi finanziari può essere per gran parte della popolazione lento e limitato da requisiti di credito, aree geografiche, capitale minimo. Il protocollo, invece, offre a tutti la possibilità di prestare o prendere liquidità velocemente con una posizione collateralizzata di un qualsiasi ERC-20 token a tassi d'interesse favorevoli. Inoltre propone un rendimento sui depositi (DSR) che essendo valutato in dollari (DAI è ancorata al dollaro statunitense) è facilmente confrontabile con altri investimenti tradizionali.

In un sistema centralizzato, le transazioni, quali trasferimenti di denaro o prestiti, possono comportare commissioni fisse, percentuali o entrambe, stabilite dalle istituzioni bancarie o finanziarie. In MakerDAO i tassi d'interesse sono *pooled*, cioè i fondi sono raggruppati in "pool", per essere poi prestati e generare rendimenti. Questa forma di aggregazione consente una gestione collettiva e automatizzata dei fondi attraverso smart contract. Inoltre favorisce una distribuzione equa degli interessi guadagnati e offre agli utenti un sistema più trasparente e efficiente rispetto ai modelli centralizzati.

Infine la mancanza di interoperabilità è uno dei problemi maggiori della finanza tradizionale, che impedisce la creazione di un sistema aperto e interconnesso. In questo contesto, infatti, non è possibile utilizzare in modo affidabile e senza intermediari il dollaro o token collateralizzati in dollaro all'interno di accordi basati su smart contract. Il protocollo Maker risolve la questione attraverso l'emissione di DAI, che essendo un token basato su blockchain può essere integrato e utilizzato in qualsiasi dApp senza la necessità di intermediari.

In pratica MakerDAO ha creato un ponte tra la finanza tradizionale e quella decentralizzata, consentendo l'interazione fluida tra monete tradizionali fiat e il mondo emergente blockchain. Così facendo non solo aumenta l'interoperabilità, ma rende anche l'intero sistema DeFi più inclusivo, trasparente ed efficiente.

3.1.2 Compound

Compound è una piattaforma di lending e borrowing di attività ERC-20 che lavora sulla blockchain Ethereum. Il protocollo stabilisce mercati monetari, ovvero pool di assets con tassi d'interesse derivanti da algoritmi, basati sulla domanda e sulla offerta dell'attività. I fornitori (e i mutuatari) di un bene interagiscono direttamente con il protocollo,

guadagnando (e pagando) un tasso di interesse variabile, senza dover negoziare con una controparte termini come la scadenza, il tasso o la garanzia. Ogni asset di Ethereum ha un mercato proprio e tutti i token di un mercato sono raggruppati insieme, in modo che ogni prestatore guadagni lo stesso tasso variabile che pagano i prestatari[67].

In maniera simile a MakerDAO anche Compound opera attraverso un meccanismo di aggregazione: il protocollo aggrega gli asset in una riserva comune, offrendo una grande liquidità, flessibilità e facilità d'uso. Gli utenti possono ritirare i loro beni in qualsiasi momento senza attendere la scadenza di un prestito specifico, a meno che ogni asset nel mercato non sia in prestito. Anche se il protocollo non garantisce la liquidità, utilizza un modello basato sui tassi di interesse per mantenerla: quando la liquidità scarseggia a causa di una forte domanda, i tassi di interesse salgono, spingendo le persone a offrire più asset e a ridurre i prestiti.

Nel protocollo Compound i prestiti sono garantiti da asset diversi da quello prestato che hanno un valore superiore all'importo del prestito, sono cioè "overcollateralized". Ogni tipo di mercato ha un coefficiente di garanzia (*collateral factor*) associato, che varia tra 0 e 1. Questo coefficiente indica quale percentuale del valore totale di un asset può essere effettivamente presa in prestito. Ad esempio, con un coefficiente di garanzia di 0.80 (o 80%), un utente che deposita 100 unità di valore potrebbe prendere in prestito fino a 80 unità di un altro asset.

Un altro parametro importante è il tasso di collateralizzazione, che rappresenta il rapporto tra il valore del prestito e il valore totale dell'asset dato come garanzia. Può essere pensato come un equivalente del concetto "Loan To Value" (LTV) nel mondo finanziario tradizionale ed è il rapporto tra 100 e il coefficiente di garanzia. Se il valore dell'asset in garanzia diminuisce troppo rispetto al valore del prestito, il rapporto di collateralizzazione dell'utente può superare il limite accettabile e, in questo caso, la sua posizione verrà automaticamente liquidata per proteggere l'interesse dei prestatori.

È possibile anche utilizzare più collaterali diversi allo stesso tempo. In questo caso il rapporto di collateralizzazione è la media pesata delle diverse garanzie per il loro peso nel portafoglio. Vediamo un esempio. Un investitore deposita 100 DAI con un fattore di garanzia di 90. Se 1 DAI = $1 l'utente può prendere in prestito qualsiasi altro asset fino al valore di $90. Ciò corrisponde ad un rapporto di collateralizzazione del 111%. Se egli

[67] Compound, Whitepaper. 2019. https://compound.finance/documents/Compound.Whitepaper.pdf.

aggiungesse anche 2 ETH dal valore di $200/ETH, con un fattore di garanzia di 60, la fornitura totale sarebbe di $500, il fattore di garanzia totale 66 (0.8 · 60 + 0.2 · 90) e il rapporto collateralizzazione 151% (100/66).

I tassi di interesse per l'offerta (*supply interest rate*) e per il prestito (*borrow interest rate)* sono determinati dal protocollo attraverso una combinazione di parametri, alcuni calcolati automaticamente in base ai dati disponibili, mentre altri stabiliti dalla governance:

a) Percentuale di utilizzo (*Utilization percentage*): indica quale frazione degli asset depositati nel protocollo viene effettivamente presa in prestito. Si calcola come rapporto tra il totale degli asset prestati e il totale degli asset.

$$U_n = \frac{Prestiti_n}{Cassa_n + Prestiti_n} \quad \text{per ogni mercato n.}$$

b) *Base rate*: rappresenta l'intercetta y della funzione del borrow rate, ed è il minimo tasso quando la domanda per i prestiti è nulla.

c) *Slope*: è l'incremento del tasso di interesse rispetto alla percentuale di utilizzo. Fondamentalmente, determina quanto rapidamente il tasso di interesse cresce man mano che la percentuale di utilizzo aumenta.

d) *Kink*: si riferisce al punto di flessione nella curva dei tassi di interesse. Dopo aver raggiunto la "kink", l'incremento dei tassi di interesse diventa più ripido. Questo significa che, al di sopra di una certa percentuale di utilizzo, l'aumento dei tassi diventa più aggressivo per incentivare maggiormente l'offerta e disincentivare ulteriori prestiti. Solo alcuni mercati utilizzano questo parametro.

e) *Reserve factor*: rappresenta una percentuale di interessi guadagnati sui prestiti che viene accantonata in una "riserva" invece di essere distribuita direttamente ai fornitori di liquidità. Queste riserve fungono da cuscinetto per coprire eventuali perdite inaspettate, come potrebbero essere quelle dovute a default sui prestiti o altre situazioni avverse.

Il tasso di interesse sui prestiti è il seguente:

$$Tasso\ di\ interesse\ sui\ prestiti_n = base\ rate + U_n * slope$$

Il tasso sui depositi è il tasso sui prestiti moltiplicato per la percentuale di utilizzo, in modo che all'aumentare della domanda di prestiti (e quindi della percentuale di utilizzo)

anche i fornitori di liquidità vengano incentivati con tassi di interesse più elevati sui loro depositi.

Illustriamo adesso un esempio numerico per capire meglio l'importanza del kink.

Supponiamo prima un mercato senza kink, per esempio il mercato DAI, dove 100 milioni di DAI sono depositati e 90 milioni di DAI sono presi in prestito, ciò equivale ad un tasso di utilizzo del 90%. Il base rate e la slope sono fissati rispettivamente al 1% e 10%.

Il borrow interest è pari a 0.01 + 0.90 * 0.10 = 0.1, cioè 10%, e il tasso massimo sui depositi equivale a 0.1 * 0.90 = 0.09, ovvero 9%. Se consideriamo anche il reserve factor, pari per esempio a 10, significa che il 10% del tasso sui prestiti è accantonato ad una riserva di DAI. I nuovi valori del tasso sui prestiti e sui depositi sono rispettivamente 9% (10% - 10% · 0.01) e 8.1% (9% · 0.90).

Adesso includiamo anche il parametro "kink", supposto essere 80%. Introducendo questo parametro nella formula dei tassi di interesse su Compound dovremmo tener conto di una curva a due segmenti per il calcolo del tasso di interesse sul prestito. Il kink rappresenta un punto di flesso nel modello di tassi di interesse, al di sopra del quale la pendenza del tasso aumenta significativamente: in questo caso, all'80% di utilizzo (che ricordiamo abbiamo supposto essere 90%). Fino a quel livello, la pendenza (slope) è del 10%; superando l'80%, invece, la pendenza aumenta, per esempio, al 40% (anche questo parametro è determinato dalla governance del protocollo).

La formula per il calcolo del borrow rate diventa:

$$Tasso\ d'interesse\ sui\ prestiti\ =\ base\ rate\ +\ (U_n^1 * slope^1)\ +\ (U_n^2 * slope^2)$$

Dove:

- U_n^1: percentuale di utilizzo fino al kink
- $slope^1$: slope sotto il kink
- U_n^2: percentuale di utilizzo oltre il kink (0.90 - 0.80 = 0.10)
- $slope^2$: slope oltre il kink

Con i dati dell'esempio si trova che il tasso d'interesse sui prestiti è pari a:

$$0.01\ +\ (0.80\ *\ 0.10) +\ (0.10\ *\ 0.40) = 13\%$$

Il protocollo Compound, come molte altre piattaforme finanziarie decentralizzate, funziona mettendo in garanzia (*escrow*) i token depositati dagli utenti. Questo significa che quando un utente deposita i suoi token sulla piattaforma, questi non sono direttamente

accessibili all'utente ma sono invece bloccati dal protocollo. Mettere in garanzia i token, oltre a garantire la liquidità, permette anche al protocollo di tenere traccia delle partecipazioni di ciascun utente. In sostanza ogni volta che un utente deposita token su Compound riceve in cambio un token di rappresentanza (*security token*), chiamato cToken (ad esempio cETH corrisponde al mercato Compound ETH), che indica la sua quota di proprietà nel mercato specifico. Questo meccanismo assicura che, in qualsiasi momento, un utente possa ritirare i suoi token originali (più eventuali interessi maturati) e che la piattaforma tenga traccia accurata di chi possiede cosa.

Inoltre i cTokens sono token ERC-20 standard, il che significa che possono essere trasferiti, scambiati o utilizzati in altri protocolli DeFi. Questa interoperabilità ha permesso l'interazione con altre piattaforme, per esempio i cTokens possono essere usati come collaterale in MakerDAO, rendendo il protocollo Compound ancora più versatile. Questi tokens hanno sempre un valore maggiore che l'asset sottostante, a causa degli interessi pagati continuamente ai depositanti.

Illustriamo questo meccanismo con un esempio. Immaginiamo una situazione iniziale in cui nel mercato Compound di DAI ci sono 5000 DAI, rappresentati da 1000 cDAI. Questo significa che ogni cDAI ha un valore di 5 DAI. Consideriamo due investitori principali: il primo possiede il 60% dei cDAI in circolazione, pari a 600 cDAI, mentre il secondo detiene il restante 40%, ovvero 400 cDAI. Quando un terzo investitore decide di partecipare al mercato, deposita una somma di 2500 DAI, portando il valore complessivo del mercato a 7500 DAI. Data la conversione attuale di 5 DAI per cDAI, il deposito del terzo investitore produce un ulteriore 500 cDAI, portando il totale dei cDAI in circolazione a 1500 (1000 + 2500/5). Vediamo ora cosa succede dopo un anno di interessi che assumiamo essere del 10%. Alla fine dell'anno ci saranno 8250 (= 7500 · 1,10) DAI e gli utenti vedranno aumentare il valore dei loro cDAI: dal valore di 1 a 5 si passa a 1 a 5,5 (= 8250/1500) valore al quale possono riscattare i cDAI ottenendo un ritorno maggiore rispetto al loro deposito iniziale.

I cDAI offrono una flessibilità significativa nel mondo della finanza decentralizzata. Un trader può depositare cDAI al posto dei DAI, in modo che i cDAI non rimangano inutilizzati ma generino interessi tramite il pool di Compound. Ad esempio, il trader potrebbe utilizzare i cDAI come collaterale necessario per aprire una posizione perpetua sui futures su dYdX o potrebbe operare come market maker su Uniswap utilizzando una

coppia di trading basata su cDAI (dYdX e Uniswap sono presentati più avanti nel capitolo).

Nelle prime fasi della crescita di Compound la governance era affidata agli amministratori. Uno degli obiettivi degli inventori però, come quasi in tutti i protocolli DeFi, era quello di lasciare la leadership agli utenti tramite un token di governance: COMP. Chiunque con almeno l'1% di partecipazione può proporre azioni da implementare, sotto forma di codice eseguibile (non suggerimenti o progetti da discutere). Tutte le proposte sono soggette a un periodo di votazione di tre giorni, e qualsiasi indirizzo che abbia almeno un COMP può votare a favore o contro. Se la maggioranza, con almeno 400.000 voti (il 4% dell'offerta totale dei COMP), vota per la proposta, viene messa in coda nel *Timelock*[68] e può essere implementata dopo due giorni[69] (Figura 3.1).

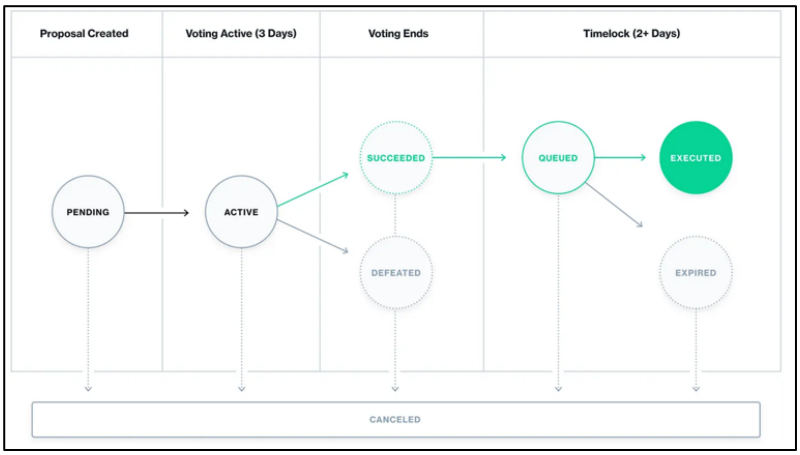


Figura 3.1. Diagramma di flusso dello stato delle proposte su Compound. Fonte: *Compound*

Il COMP è usato per votare su questioni riguardanti, tra le altre, i parametri relativi ai tassi d'interesse, l'aggiunta di nuovi mercati, i volumi di deposito e prestito oppure la scelta di un "amministratore delegato". È Importante evidenziare che la governance di Compound non ha il potere di distribuire fondi o di impedire agli utenti di effettuare prelievi.

[68] Il *Timelock* è un meccanismo che impone un ritardo nell'esecuzione di determinate azioni o trasferimenti al fine di garantire trasparenza e sicurezza. Fonte: Compound.finance
[69] Compound, Governance. https://docs.compound.finance/v2/governance/.

I token COMP di Compound possono essere ottenuti in vari modi. Principalmente, a seguito della proposta "Distribuite COMP to users[70]" del 15 Giugno 2020, vengono distribuiti come ricompense a coloro che forniscono o prendono in prestito fondi sulla piattaforma Compound. Inoltre è possibile acquistarli su diverse borse di criptovalute oppure guadagnarli partecipando attivamente alle decisioni di governance del protocollo e attraverso lo *yield farming*, cioè depositando token e fornendo liquidità in specifici pool. In sintesi il principale punto di forza di Compound è la sua capacità di ampliare l'orizzonte permettendo l'interazione con una gamma più ampia token ERC-20. I tassi di interesse, a differenza del protocollo Maker, sono determinati algoritmicamente in base all'offerta e alla domanda di un particolare asset e solo i parametri tramite i quali tali tassi si formano sono decisi dai possessori di COMP. Questa combo tra efficienza e flessibilità permette di offrire tassi d'interesse competitivi sia ai prestatori che prestatari. Allo stesso modo di MakerDAO e di tutte le principali dApp, anche Compound ha un modello di governance decentralizzato che incentiva i detentori di COMP a portare valore alla società.
Per concludere, una sfida significativa della finanza tradizionale è stata l'incapacità di monetizzare o utilizzare la garanzia in una posizione di prestito, limitando la liquidità e le opportunità di investimento per gli investitori. Il meccanismo dei cToken di Compound consente agli utenti di generare token dalle loro posizioni, trasformando asset statici in asset produttivi di rendimento. Così possono vedere in modo chiaro e continuo come i loro interessi vengono accumulati e, poiché i cToken sono ERC-20, possono essere trasferiti, scambiati o utilizzati in altre piattaforme DeFi promuovendo la creazione di strategia finanziarie ancora più complesse.

3.1.3 Aave

Aave è un protocollo di lending simile a Compound, ma rispetto a quest'ultimo offre ulteriori opzioni.
Innanzitutto Aave offre attualmente tredici tokens ERC-20 in più dei nove previsti da Compound. Inoltre il protocollo Aave, a differenza delle altre piattaforme DeFi, propone

[70] Compound, 15 Giugno 2020. "Distribute COMP to Users". https://compound.finance/governance/proposals/7.

la capacità di creare mercati completamente nuovi, ciascuno composto da una serie di pool di token con tassi di interesse specifici per deposito e prestito. Questa peculiarità rende ciascun mercato indipendente, il che significa che i token in un determinato mercato funzionano come garanzie solo all'interno di quel pool. Questa separazione è cruciale per mitigare il rischio di contagio: se un token in un mercato dovesse avere problemi, essi non si estenderebbero agli altri mercati. Ciò non solo protegge gli utenti da potenziali perdite, ma rende anche Aave estremamente flessibile. Se un gruppo di utenti desiderasse creare un mercato per un nuovo tipo di token o una specifica strategia di investimento, potrebbe farlo senza interferire con i mercati esistenti, garantendo così sia l'adattabilità alle esigenze emergenti nel settore DeFi sia una robusta protezione per gli utenti.

La caratteristica distintiva di Aave è senza dubbio i *flash loans* ("prestiti istantanei"). Solitamente il tasso d'interesse sui prestiti tradizionali è più alto quanto più lunga è la durata del credito, perché maggiore è la probabilità che il debitore vada in default. Questo significa che prestiti a breve termine dovrebbero essere meno rischiosi e richiedere meno compenso per il prestatore. Un flash loan è un prestito istantaneo che permette agli utenti di prendere a prestito senza garanzie, a condizione che questo sia rimborsato in una singola transazione (*one block borrows*)[71]. Il concetto è simile a quello dei depositi overnight effettuati tra banche, ma con la differenza che i flash loans sono automatizzati grazie agli smart contract. Se, per qualsiasi motivo, l'utente non riesce a rimborsare l'importo entro la fine della transazione, questa viene automaticamente annullata. Ciò significa che tutte le operazioni eseguite durante quella transazione vengono annullate e i fondi non vengono trasferiti. I flash loans, se non vengono rimborsati, è come se non fossero mai stati concessi; questo di fatto elimina il rischio di controparte e il rischio di duration. Aave applica una commissione di 9 punti base sull'importo totale del prestito. Questa commissione viene poi distribuita all'asset pool per ricompensare coloro che hanno depositato fondi, riconoscendo così il loro contributo al pool.

Uno degli impieghi più frequenti dei flash loans è fornire un accesso rapido al capitale, consentendo agli utenti di ristrutturare o rifinanziare le loro posizioni in maniera efficiente. Per vedere un'applicazione pratica si assuma che il prezzo di ETH sia 200 DAI e che un utente abbia depositato 100 ETH su Compound e ha poi deciso di prendere in prestito 10.000 DAI per aumentare la leva. Con questi DAI l'utente ha acquistato altri 50

[71] Aave, "Flash Loans". https://docs.aave.com/developers/guides/flash-loans.

ETH, che ha prontamente depositato su Compound (per un totale di 150 ETH). Adesso, però, si accorge che sta pagando un tasso d'interesse piuttosto alto: 15% annuo, mentre sulla piattaforma Aave, il tasso d'interesse per lo stesso prestito è solamente del 5%. L'obiettivo è rifinanziare il prestito per sfruttare il tasso più basso offerto da Aave, il che è analogo a rifinanziare un mutuo, un processo lungo e costoso nella finanza tradizionale. A questo punto, l'utente ha due opzioni. La prima, la più convenzionale, sarebbe chiudere direttamente il prestito su Compound (cioè restituire i 10.000 DAI), vendere parte degli ETH per ottenere nuovamente i DAI necessari e poi depositare gli ETH e prendere in prestito i DAI su Aave. Tuttavia, questo metodo è macchinoso e costoso a causa delle commissioni di cambio e delle *gas fee*. La seconda opzione, molto più efficiente, sfrutta i flash loans di Aave. L'utente può prendere in prestito istantaneamente 10.000 DAI da Aave, utilizzarli per chiudere il suo prestito su Compound e liberare tutti i suoi ETH. Contestualmente, deposita gli ETH su Aave e prende un normale prestito di 10.000 DAI (a un tasso molto più conveniente del 5%) e li utilizza per rimborsare il flash loan. Questo processo, pur sembrando complesso, avviene in una sola transazione, riducendo così costi e complessità. Quest'ultimo approccio evita efficacemente gli step di scambio di ETH per DAI per annullare e ricreare la leva, consentendo agli utenti di trasferire una posizione da una dApp all'altra con un semplice click.

Un'ulteriore innovazione di Aave rispetto agli altri protocolli DeFi riguarda la delega di credito, o *credit delegation*. La delega di credito permette ad un utente di depositare fondi nel protocollo per guadagnare interessi e delegare potere di prestito (cioè il loro credito) ad altri utenti. In pratica, il depositante offre la sua capacità di prendere a prestito ad un terzo, senza rinunciare al controllo dei propri fondi. La concessione del prestito e delle sue condizioni sono concordate tra il depositante e i mutuatari, che possono essere stipulate fuori dalla blockchain attraverso accordi legali oppure on-chain tramite smart contract[72]. A differenza della maggior parte dei prestiti in DeFi, che richiedono che l'utente metta una garanzia per prendere un prestito, con la credit delegation il mutuatario non deve fornire garanzie. Il rischio e la fiducia sono essenzialmente trasferiti al depositante, che in caso di mancato rimborso da parte del mutuatario è responsabile del debito.

[72] Aave, "Credit Delegation". https://docs.aave.com/developers/guides/credit-delegation.

Ad esempio, un produttore potrebbe avere un capitale di 40.000 DAI in Aave che genera interessi. Il produttore è interessato a massimizzare il suo rendimento e decide di delegare una parte del suo capitale a un partner commerciale di fiducia. Il partner, a sua volta, potrebbe utilizzare questo capitale per finanziare l'acquisto di una certa quantità di beni, impegnandosi a restituire il capitale al produttore con un interesse prestabilito. La particolarità di questa operazione è che non c'è una vera e propria garanzia formale che obblighi il partner a rispettare l'accordo; tutto si basa sulla reciproca fiducia e sulla storia condivisa tra le due parti.

Questa funzione potrebbe aprire le porte a nuove forme di prestiti e ad una maggiore inclusione finanziaria, permettendo a chi non ha garanzie di accedere comunque a prestiti, basandosi su relazioni di fiducia o altri meccanismi di valutazione simile a quelli per il merito creditizio nella finanza tradizionale. Questi sistemi non sono ancora attivi, ma nel futuro potremmo assistere all'introduzione di funzioni automatizzate di valutazione del merito creditizio basate su blockchain, che incorporeranno queste dinamiche di fiducia, rendendo il sistema ancora più robusto e accessibile.

In sintesi, rispetto ai protocolli di lending analizzati precedentemente, Aave introduce principalmente tre novità importanti. Oltre all'introduzione di tassi d'interesse fissi, che possono risultare particolarmente attrattivi in periodi di alta volatilità garantendo una maggiore sicurezza e stabilità, la principale innovazione di questo protocollo riguarda i flash loans. Questi prestiti istantanei democratizzano l'accesso alla liquidità per esigenze imprenditoriali imminenti e nuove strategie finanziarie, senza necessitare di asset da dare in garanzia. Inoltre Aave permette la credit delegation, un'altra soluzione (oltre a quella offerta da Compound) per rendere monetizzabile l'eccesso di collaterale in un posizione creditizia. Ciò si traduce in un sistema di prestito *peer-to-peer* potenziato, dove gli utenti con fondi improduttivi possono "prestare" la loro capacità di credito a chi necessita di liquidità, ma non possiede il collaterale necessario. Queste funzionalità promuovono ulteriormente l'idea di un sistema finanziario più flessibile, aperto e inclusivo.

3.2 Scambi: Uniswap

Una delle innovazioni più dirompenti della DeFi è la nascita degli scambi decentralizzati (DEX), che, al contrario delle tradizionali piattaforme, offrono un livello di trasparenza e accessibilità senza precedenti. In questo paragrafo ci concentreremo esclusivamente su Uniswap, che emerge come il protocollo più noto e influente di questo segmento della finanza decentralizzata. Esploreremo la sua architettura e il suo funzionamento seguendo le sue diverse versioni, cogliendo come questo protocollo abbia ridefinito il concetto di scambio di criptovalute, in un contesto sicuro ed efficiente senza la necessità di intermediari.

Dal suo lancio iniziale, nel novembre 2018, Uniswap ha percorso un lungo cammino. La sua introduzione nel mondo della finanza decentralizzata come Market Maker Automatizzato (AMM) su Ethereum ha ridefinito come gli individui scambiano token su piattaforme basate su blockchain. Con l'avvento di Uniswap v2, nel maggio 2020, il progetto ha apportato significative ottimizzazioni e nuove funzionalità, registrando un volume di oltre 135 miliardi di dollari di scambi[73]. Questa versione ha introdotto un concetto fondamentale nella determinazione del prezzo e nella gestione della liquidità basato sul principio di prodotto costante, rappresentato dalla formula $x \cdot y = k$, dove x e y sono le riserve dei due asset in un pool della piattaforma. k è il prodotto delle riserve di due token in un determinato pool di liquidità e l'invarianza di questa costante è ciò che permette a Uniswap di funzionare senza necessità di un order book tradizionale. Per acquistare una certa quantità di x, si deve vendere una certa quantità di y. Il rapporto di cambio è dato da x/y ed è il prezzo neutro al rischio, poiché il contratto è ugualmente disposto a comprare o vendere a questa tariffa fintanto che la costante k rimane invariata[74]. Immaginiamo una situazione nel mercato Uniswap USDC/DAI. Inizialmente, nel contratto ci sono 8 DAI e 4 USDC. Questo stabilisce un tasso di cambio iniziale di 2 DAI per 1 USDC, con una costante k di 32 (= 8 · 4). L'investitore decide di vendere 2 DAI. Per sapere quale sia la quantità di USDC che viene sottratta dal pool dobbiamo trovare quel valore che mantiene inalterata la costante k considerando il nuovo ammontare di DAI. Il valore è calcolabile dall'equazione $k = (DAIiniziali + DAIvenduti) *$

[73] Uniswap, "Introducing Uniswap v3", 2021. https://blog.uniswap.org/uniswap-v3.
[74] Harvey, Ramachandran e Santoro, *DeFi and the Future of Finance*.

(USDCiniziali – USDCacquistati). Quindi, depositando questi 2 DAI nel contratto, il saldo di DAI diventa 10 e l'utente ritira 0,8 (= 4 – 32/10) USDC, lasciando un saldo di 3,2 USDC nel contratto. Dopo questa operazione, la costante *k* rimane ancora 32, ma il tasso di cambio si modifica, diventando ora di 3,125 (= 10/3,2) DAI per 1 USDC.

Questa rilevante variazione nel tasso di cambio riflette l'effetto dello *slippage*, che si manifesta quando c'è una bassa liquidità nel mercato. In questo contesto lo slippage si riferisce alla differenza tra il tasso di cambio atteso per una certa transazione e il tasso di cambio effettivo a cui viene effettivamente eseguita. Se viene effettuato uno scambio di piccole dimensioni in un pool con molta liquidità, lo "scivolamento" sarà minimo perché la transazione ha un impatto trascurabile sulle riserve totali del pool. Viceversa, se si effettua uno scambio di grandi dimensioni in un pool con liquidità limitata, la transazione può spostare significativamente il rapporto tra i token.

Immaginiamo una situazione diversa, con una maggiore liquidità: ci sono 200 DAI e 100 USDC nel contratto, con una costante di 20.000. Se l'investitore decide di vendere 5 DAI, questa volta può prelevare all'incirca 0,99 USDC per mantenere la costante. Nonostante l'utente venda una quantità maggiore di DAI, come previsto, lo slippage è notevolmente ridotto per la maggiore liquidità del pool e il tasso effettivo dopo la transazione è molto vicino al tasso iniziale, risultando in 2,04 DAI per 1 USDC.

In Uniswap ogni transazione eseguita su una coppia di trading comporta una commissione dello 0,3% che viene reinvestita nel pool di liquidità. Il sistema di distribuzione delle commissioni in Uniswap è simile al modello cToken utilizzato da Compound. La partecipazione di un fornitore di liquidità in un pool specifico di Uniswap è rappresentata da token UNI. Queste commissioni vengono distribuite ai partecipanti al pool proporzionalmente alla loro quota e quando un fornitore di liquidità decide di ritirare la sua partecipazione dal pool può riscattare i suoi token UNI ottenendo non solo i fondi inizialmente depositati ma anche la sua quota delle commissioni accumulate durante il periodo in cui ha contribuito con la liquidità. Ad esempio, per coloro che forniscono liquidità alla coppia DAI/ETH, ricevono in cambio token UNI DAI/ETH, che rappresentano la loro quota nel pool.

Quando un utente decide di diventare un fornitore di liquidità, deposita una coppia di token in un pool di liquidità specifico su Uniswap. Questo deposito deve includere una quantità equivalente di entrambi i token della coppia di trading, basata sul tasso di cambio

corrente. A causa delle fluttuazioni del mercato, al momento del ritiro, la proporzione degli asset potrebbe non corrispondere a quella iniziale, portando a ciò che è noto come *impermanent loss*. Questa perdita, il cui rischio è bilanciato dalle commissioni guadagnate sulle transazioni, come abbiamo già avuto modo di vedere rappresenta un costo opportunità, poiché detenendo gli asset, si eviterebbe. I partecipanti ai pool guadagnano un reddito passivo proporzionale al volume del mercato che riforniscono, ma per ottenere un saldo positivo le commissioni devono superare le perdite impermanenti. Per questo molti utenti preferiscono fornire liquidità a pool di coppie di stablecoin, come ad esempio USDC/DAI. Questa stabilità nel valore relativo rende minore la probabilità di perdite impermanenti rispetto ad altre coppie di asset con volatilità più alta.

Uno dei problemi centrali di Uniswap è che esso tratta tutte le coppie di trading allo stesso modo, indipendentemente dalla natura degli asset sottostanti. Le stablecoin, ad esempio, che hanno uno slippage molto basso dato che il loro valore non dovrebbe fluttuare significativamente, sono trattate da Uniswap nello stesso modo di Ethereum (ETH) e un'altra criptovaluta, che potrebbero avere prezzi molto più volatili. Questo significa che gli arbitraggisti, che cercano di sfruttare le piccole differenze di prezzo tra le piattaforme, potrebbero approfittare di questa inefficienza nel modello di prezzi di Uniswap, ottenendo profitti che, in condizioni ideali, andrebbero ai fornitori di liquidità.

Un altro AMM, Curve[75], ha riconosciuto questo problema e ha creato un modello di prezzi specializzato per coppie di trading ad alta correlazione, come le stablecoin. Il suo approccio potrebbe quindi attirare più liquidità per tali coppie rispetto a Uniswap, dato che potrebbe offrire condizioni migliori ai fornitori di liquidità.

Un ulteriore inconveniente del modello AMM è la sua particolarmente suscettibilità al *front-running*, che non va confuso con il front-running[76] "illegale" che affligge la finanza centralizzata. Quando un utente invia una transazione su una blockchain come Ethereum, prima che essa venga confermata e inclusa in un blocco, passa attraverso una zona chiamata *memory pool*[77] o "mempool". Poiché le transazioni in questi nodi sono visibili

[75] Curve, https://dao.curve.fi.

[76] Nella finanza tradizionale per *front running* si intende "Pratica illegale messa in atto da un operatore finanziario che, ricevuto da un cliente un ordine di acquisto o di vendita in grado di influire sul prezzo del titolo, pone in essere un'operazione per conto proprio." Fonte: borsaitaliana.it

[77] Un *mempool* è il meccanismo di un nodo di criptovaluta per memorizzare informazioni sulle transazioni non confermate. Agisce come una sorta di sala d'attesa per le transazioni che non sono ancora state incluse in un blocco. Fonte: academy.binance.com

pubblicamente, gli attori malintenzionati (i front-runners) possono vedere in anticipo quale operazione un utente sta cercando di eseguire. Questi attori possono quindi decidere di effettuare una transazione simile, ma offrendo una gas fee più alta, assicurandosi che il loro scambio venga confermato prima di quello dell'utente originale. Dopo aver approfittato di questa posizione anticipata, possono effettuare una transazione opposta per vendere l'asset e incassare il profitto, a scapito dell'utente iniziale. Per esempio si immagini che un'utente stia per acquistare una grande quantità di ETH usando DAI in Uniswap, cosa che farà aumentare il prezzo dell'ETH. Un front-runner vede la transazione in sospeso nel mempool e, prima che la transazione venga confermata, il truffatore offrendo una gas fee più alta acquista rapidamente ETH. Subito dopo la transazione dell'utente viene confermata, facendo salire il prezzo dell'ETH come previsto. Il front runner può ora vendere immediatamente il suo ETH al prezzo più alto, realizzando un profitto a scapito del consumatore, il quale ha pagato di più per l'ETH a causa dell'azione malevola.

Le stime dei ricavi dal front-running, che avvengono direttamente a spese degli utenti, sono passate da centinaia di migliaia di dollari, quando il front-running è stato dimostrato pubblicamente per la prima volta nel 2017, a centinaia di milioni di dollari a metà del 2021. Questa pratica è favorita dalle grandi transazioni, soprattutto nei mercati illiquidi con alto slippage. Per questo motivo Uniswap permette agli utenti di impostare uno slippage massimo, che se viene superato la transazione non verrà eseguita. Questo limita il profitto che i front-runners possono fare, ma non elimina completamente il problema.

Per risolvere questo e altri problemi, nel maggio del 2021 è stata introdotta la nuova versione Uniswap. Le principali innovazioni di Uniswap v3 sono:

- Liquidità concentrata: i fornitori di liquidità (LP) possono scegliere un range di prezzi specifico in cui posizionare la loro liquidità. Ciò significa che possono ottimizzare la loro esposizione in base alle proprie aspettative sul prezzo e guadagnare più fee in proporzione alla quantità di liquidità che forniscono in quel range di prezzi.
- Più livelli di commissioni: ciò consente agli LP di essere adeguatamente compensati per l'assunzione di vari gradi di rischio.

L'idea fondamentale della liquidità concentrata è che sia possibile vincolare la liquidità entro un certo intervallo di prezzo. Nelle versioni precedenti la liquidità era distribuita uniformemente lungo l'intero intervallo di prezzo (0, ∞). Questo meccanismo è semplice da implementare e consente di aggregare in modo efficiente la liquidità, ma significa che gran parte degli asset detenuti in un pool non vengono utilizzati[78]. Uniswap v3 introduce un'idea rivoluzionaria: invece di distribuire la liquidità su un'ampia gamma di prezzi, gli LP possono "concentrare" i loro fondi in un intervallo di prezzo specifico (“posizione”). Una posizione deve mantenere riserve sufficienti solo per supportare le transazioni entro il suo intervallo e quindi può comportarsi come un pool a prodotto costante con riserve virtuali maggiori entro quell'intervallo. La Figura 3.2 rappresenta questa relazione per una posizione in un intervallo $[pa, pb]$ e un prezzo corrente $pc \in [pa, pb]$.Per essere più chiari: se il prezzo dell'asset X dovesse aumentare fino al limite massimo dell'intervallo, la posizione avrebbe bisogno di usare tutte le sue riserve di X per soddisfare le richieste di scambio. Al contrario, se il prezzo dovesse scendere fino al limite minimo, avrebbe bisogno di tutte le sue riserve dell'asset Y. Se il prezzo esce dall'intervallo di una posizione, la liquidità non è più attiva e non guadagna più commissioni. Ciò perché, a questo punto, avrà esaurito completamente una delle due riserve e la liquidità sarebbe composta interamente da un singolo asset. Tuttavia, se il prezzo rientra nell'intervallo, la liquidità diventa nuovamente attiva.

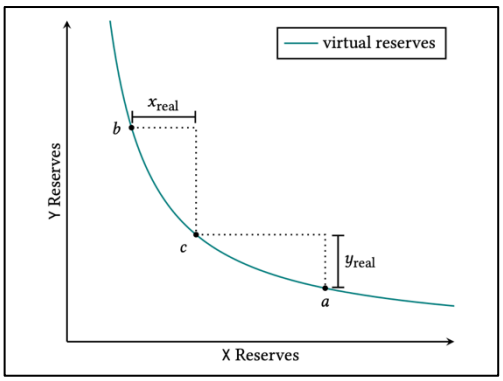


Figura 3.2. Gestione della liquidità. Fonte: *Uniswap v3 whitepaper*

[78] Uniswap. (2021). *Uniswap V3 Whitepaper*. https://uniswap.org/whitepaper-v3.pdf.

Ciò che rende Uniswap v3 ancora più interessante è che puoi creare più posizioni, ciascuna con un intervallo di prezzo diverso e con vari importi di liquidità. Ad esempio, si potrebbe avere una posizione con un alto importo di liquidità in un intervallo ristretto vicino al prezzo attuale e un'altra con meno liquidità in un intervallo più ampio, per coprire eventuali grandi movimenti di prezzo (Figura 3.3).

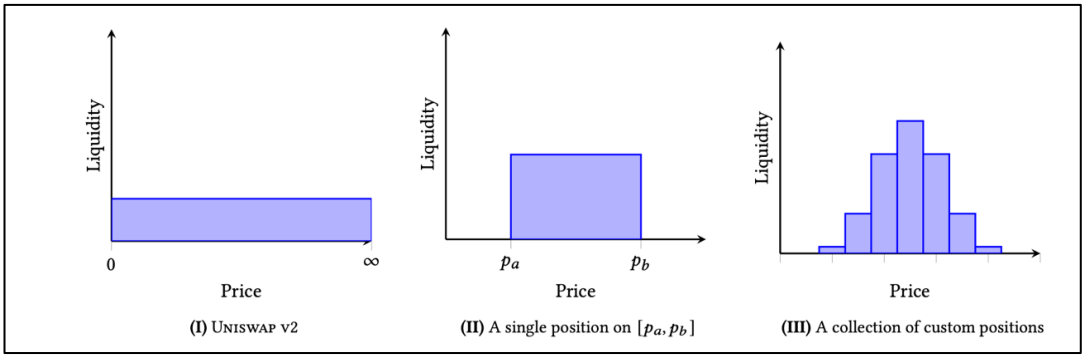


Figura 3.3. Liquidità distribuita su Uniswap v3. Fonte: *Uniswap v3 whitepaper*

Illustriamo meglio con un esempio le differenze tra Uniswap v2 e v3. Supponiamo che Mario e Alice vogliano entrambi fornire liquidità in un pool ETH/DAI su Uniswap v3. Ognuno di loro ha 500.000 DAI e il prezzo attuale di ETH è di 2.000 DAI. Mario decide di distribuire il suo capitale in tutta la fascia di prezzo (come avrebbe fatto in Uniswap v2). Deposita 250.000 DAI e 125 ETH (per un totale di 500.000 DAI). Alice invece sceglie una strategia diversa: decide di concentrare la sua liquidità solo nella fascia di prezzo da 1.500 a 2.500 DAI, depositando 36.500 DAI e 18,25 ETH, per un valore totale di 73.000 DAI, e conservando i restanti 427.000 DAI per altri investimenti o scopi. Alice, dato che ha concentrato la sua liquidità in un intervallo più stretto, anche se ha depositato molto meno capitale (73.000 DAI rispetto ai 500.000 DAI di Mario), guadagnerà la stessa quantità di commissioni di Mario ogni volta che il prezzo di ETH/DAI rimane entro la fascia di prezzo da 1.500 a 2.500 DAI. Se il prezzo di ETH dovesse crollare al di sotto di 1.500 DAI, la liquidità di Alice verrebbe convertita interamente in ETH, con una perdita potenziale di 73.000 DAI, mentre Mario avrebbe rischiato il suo intero deposito di 500.000 DAI. Inoltre Alice può usare i suoi ulteriori 427.000 dollari per proteggersi dall'esposizione al ribasso o per investire in qualsiasi altra strategia concepibile.

La seconda fondamentale innovazione di Uniswap V3 è l'introduzione dei livelli di commissione per i fornitori di liquiditá (LP): non piú soltanto un'unica tariffa per tutte le coppie di assets, come stabiliva V2, ma quattro livelli di commissioni diversi per ogni coppia: 0.01%, 0,05%, 0,30% e 1,00%.

Ciò fornisce flessibilità agli LP che possono adeguare le loro commissioni in base alla volatilità della coppia in questione e al profilo di rischio che ritengono più opportuno alle loro esigenze. Ad esempio, con coppie stabili come USDC/DAI gli LP possono essere disposti, dato il minor rischio, ad accettare una commissione bassa come lo 0,01% e 0,05%; con coppie più volatili come ETH/DAI potrebbe essere più appropriata una commissione dello 0,30%; coppie con alta volatilità ("esotiche") potrebbero richiedere, per compensare il rischio, la commissione più elevata dell'1,00%. Nonostante la possibilità di frammentazione della liquidità che si viene così a creare, si prevede che la maggior parte delle coppie converga verso un tasso di commissioni predominante.

Uniswap emerge come una valida alternativa alla finanza tradizionale. Nella TradFi le piattaforme di scambio hanno il potere decisionale su quali coppie di valute possono essere scambiate. Invece, in Uniswap, anche quando non esiste una coppia di trading, è permesso a chiunque creare una nuova coppia di scambio e il protocollo indirizza automaticamente le transazioni attraverso il percorso più efficiente garantendo così ai suoi utenti il miglior tasso possibile. Inoltre tradizionalmente le migliori opportunità d'investimento e tassi di rendimento per fornire liquidità sono limitate alle grandi istituzioni, lasciando il piccolo investitore ai margini. In questo protocollo invece ogni singolo individuo ha l'opportunità di diventare un fornitore di liquidità e, in cambio, guadagnare commissioni. Infine, c'è la questione dell'interoperabilità. Nel mondo tradizionale, quando si scambiano beni o titoli su una piattaforma, trasferire o estendere questa operazione ad un'altra può essere un processo complesso, se non impossibile. Uniswap consente ad ogni applicazione DeFi, che necessita di uno scambio di token, di integrare e sfruttare facilmente questa dApp, rendendo le transazioni tra piattaforme un processo fluido.

3.3 Obbligazioni: Yield protocol

Lo Yield Protocol propone un modello derivato per emulare nel mondo decentralizzato obbligazioni sicure senza cedola. L'elemento fondamentale risiede nei fyTokens, simili alle obbligazioni zero-coupon bond nel mondo finanziario tradizionale. Questi tokens sono garantiti e consentono effettivamente prestiti a tasso fisso, utilizzando il rendimento implicito sul prezzo scontato del token rispetto all'importo target: quando un investitore acquista fyTokens sta prestando denaro oggi in cambio di un importo superiore in futuro[79]. Supponiamo che un investitore spenda X DAI per acquistare fyTokens; questo importo X rappresenta il denaro che l'investitore ha "prestato" oggi. Al momento del regolamento, quando l'investitore riscatta i suoi fyTokens, riceverà *X+interesse*. Questo "interesse" non è esplicitamente menzionato o garantito, ma è implicito nella differenza tra il prezzo a cui l'investitore ha acquistato il fyToken e il valore dell'asset target. Questo è simile al modo in cui funzionano le obbligazioni a zero cedola: vengono acquistate a uno sconto rispetto al loro valore nominale e, alla scadenza, vengono riscattate al loro valore nominale, con la differenza che rappresenta l'interesse guadagnato. Dall'altra parte della transazione, qualcuno che emette (o "crea") e vende fyTokens sta prendendo in prestito denaro, anch'egli ad un tasso prestabilito.

Supponiamo che un utente voglia prendere in prestito DAI utilizzando ETH come garanzia e quindi decida di utilizzare fyDAI per farlo. Egli compra 1 fyDAI, con un asset target di 1 DAI garantito da ETH, con scadenza esatta tra un anno, al prezzo di 0,92 DAI e la differenza di 0,08 DAI rappresenta l'interesse fisso che guadagnerebbe. Dalla formula per il calcolo del prezzo di uno zero-coupon bond possiamo ricavare il tasso di rendimento dell'operazione: $0.92 = 1/(1+r)^t$, da cui r = 8,7%.

Quindi, conservando il suo fyToken fino alla scadenza, ha effettivamente bloccato un tasso di interesse dell'8,7%. Dato che l'ETH viene utilizzato come garanzia per il DAI preso in prestito, se il valore dell'ETH dovesse scendere drasticamente, ci sarebbe un meccanismo per garantire che il prestito sia ancora coperto, simile a quello dei protocolli già analizzati.

Un ulteriore utilizzo di questo strumento potrebbe essere la creazione di un portafoglio di diverse scadenze che reinveste i profitti a breve termine nei contratti fyTokens a lungo

[79] Yield Protocol, "Introduction". https://docs.yieldprotocol.com/#/.

termine per generare un prodotto perpetuo. Ad esempio, il portafoglio potrebbe includere fyTokens con scadenza a tre, sei, nove mesi, e ad un anno; una volta maturati i tokens di tre mesi, lo smart contract può reinvestire il saldo negli fyTokens con scadenza di un anno. In questo caso i detentori di tokens sperimenterebbero sostanzialmente un rendimento a tasso variabile con aggiornamenti del tasso ogni tre mesi, fornendo loro un mix di stabilità (data dalla natura a termine fisso dei fyTokens) e flessibilità (data dagli aggiornamenti trimestrali).

I rendimenti degli fyTokens su più scadenze permettono anche la costruzione di *yield curve* che possono fornire informazioni utili su come gli investitori valutano il rischio nel tempo. Questo fornisce informazioni preziose non solo sullo stato attuale del mercato, ma anche sulle aspettative future degli utenti.

Yield è un protocollo innovativo che propone prodotti a tasso fisso sulla piattaforma Ethereum. Questa caratteristica lo rende particolarmente attraente poiché può essere integrato con altri programmi che offrono tassi variabili, dando vita a un sistema di finanziamento robusto e flessibile, ideale per soddisfare le esigenze degli utenti della DeFi. Protocolli come Yield hanno il potenziale di giocare un ruolo cruciale nell'evoluzione e nell'espansione del mercato DeFi. Infatti, grazie ai tassi fissi, hanno il potere di aumentare la domanda per investitori istituzionali che cercano stabilità e prevedibilità dei loro investimenti.

3.4 Derivati

I mercati dei derivati hanno assunto una dimensione e una rilevanza impressionante nel panorama finanziario globale, tanto da eclissare spesso la dimensione complessiva di molti altri mercati tradizionali, come quelli azionari e obbligazionari. Il valore nominale di questi strumenti ha raggiunto nel 2022 i 620mila miliardi di dollari[80], evidenziando la loro importanza nella gestione del rischio, nell'ottimizzazione di portafoglio e nelle strategie speculative. Se la DeFi ambisce a replicare, migliorare e forse un giorno a sostituire i sistemi finanziari tradizionali, è essenziale che integri e adotti strumenti

[80] Gennai, Andrea. "Derivati, la montagna sale a 620mila miliardi (e supera il pre Lehman)." Il Sole 24 Ore, 18 dicembre 2022. https://www.ilsole24ore.com/art/derivati-montagna-sale-620mila-miliardi-e-supera-pre-lehman-AEL7eqPC

derivati adeguati per soddisfare le esigenze sempre più complesse degli investitori di oggi.

Dopo aver esplorato il mondo dei protocolli di lending e degli scambi criptovalutari in un contesto decentralizzato, concludiamo l'analisi delle dApp addentrandoci ora in un altro importante segmento della DeFi: i derivati. Analizzeremo ora Yield Protocol, dYdX e Synthetix che hanno contribuito, ognuno con le proprie innovazioni, alla creazione di strumenti finanziari decentralizzati molto avanzati.

3.4.1 dYdX

L'evoluzione e l'espansione delle tecnologie blockchain hanno rivoluzionato il mondo delle finanze, offrendo possibilità inedite di possesso e trasferimento di beni in un contesto decentralizzato, senza la necessità di fidarsi di intermediari. Tuttavia esiste un gap evidente quando si tratta di strumenti finanziari avanzati. Ecco dove entra in gioco dYdX, una piattaforma che ha l'obiettivo di portare la sofisticatezza dei prodotti finanziari derivati nel mondo decentralizzato, offrendo agli investitori gli strumenti per una gestione del rischio più avanzata, oltre a nuove opportunità di speculazione[81].

dYdX è un protocollo che presenta un DEX spot, permettendo agli investitori di effettuare scambi di asset basandosi sulle offerte attuali (*bid-ask*) visualizzate nel libro degli ordini. In pratica, dYdX registra ordini che sono già stati preapprovati ma non li invia immediatamente alla rete Ethereum; attraverso l'uso della crittografia, si garantisce che questi ordini siano utilizzati solo per effettuare scambi nell'ambito dei termini concordati. Dato che ci potrebbero essere tempi di inattività, in cui nessun ordine viene pubblicato o abbinato, il meccanismo di funzionamento di questo protocollo richiede un certo livello di fiducia da parte degli utenti. Tuttavia, questo sistema minimizza i rischi in quanto gli ordini, una volta firmati, sono vincolati dalle condizioni dello smart contract, il che significa che non possono essere manipolati in modo improprio o fraudolento. Dopo che gli ordini sono abbinati correttamente, vengono poi trasferiti alla blockchain Ethereum, dove avviene la fase finale di liquidazione attraverso lo smart contract.

[81] dYdX, "A Standard for decentralized Margin Trading and Derivatives", 2017. https://whitepaper.dydx.exchange.

dYdX offre prestiti e finanziamenti simili a Compound e Aave, con posizioni long o short con leva fino a dieci volte, utilizzando una garanzia marginale. Le posizioni possono essere isolate in modo che venga utilizzato un singolo deposito collaterale *oppure cross-margined*, che raggruppa i saldi degli investimenti di un utente per funzionare come garanzia.

Offre anche flash loans gratuiti (quelli di Aave non sono gratuiti), il che lo rende una scelta popolare per la liquidità flash DAI, ETH e USDC. Poiché i prestiti istantanei non richiedono alcun capitale iniziale, democratizzano l'accesso a fondi per vari casi d'uso. Presentando Aave abbiamo mostrato come questi prestiti possono essere utilizzati per rifinanziare un prestito. Illustreremo ora l'uso dei prestiti flash per sfruttare un'opportunità di arbitraggio in dYdX.

Supponiamo che il tasso di cambio effettivo per 1.000 DAI per ETH su Uniswap sia di 6 ETH/1.000 DAI (il tasso di cambio istantaneo sarebbe diverso a causa dello slippage.) Inoltre ipotizziamo che il DEX dYdX abbia un prezzo di vendita di 5 ETH per 1.000 DAI (gli ETH sono più costosi su dYdX che su Uniswap). Per sfruttare questa opportunità di arbitraggio, senza alcun capitale oltre alla gas fee, un investitore può eseguire un flash loan per prendere in prestito 1.000 DAI, scambiarlo su Uniswap per 6 ETH e utilizzare 5 di questi ETH per scambiare 1.000 DAI su dYdX. Infine, l'investitore può rimborsare il prestito flash con i 1.000 DAI e tenersi l'1 ETH di profitto. Tutto ciò, ricordiamo, avviene in una singola transazione.

I principali prodotti derivati che dYdX offre sono i futures perpetui ETH e BTC, oltre ad altri futures di criptovaluta. Il concetto di future perpetuo (o “perpetual swap”) è stato introdotto per la prima volta da Shiller (1993)[82], ma solo grazie al mondo blockchain questo mercato si è sviluppato. Un contratto future perpetuo è simile a un contratto future tradizionale ma senza una data di scadenza predefinita, permettendo quindi alle parti di mantenere aperta la posizione per un periodo di tempo indefinito. Un future long (short) consente all'investitore di comprare (vendere) in futuro l'asset ad un prezzo prestabilito. Se il prezzo di mercato sale (scende), l’investitore può comprare (vendere) l'asset ad un prezzo inferiore (superiore) al prezzo di mercato e il profitto sarà la differenza tra il prezzo di mercato e il prezzo del contratto.

[82] Shiller, Robert J. 1993. "Measuring Asset Values for Cash Settlement in Derivative Markets: Hedonic Repeated Measures Indices and Perpetual Futures." *The Journal of Finance* 48 (3). https://www.nber.org/system/files/working_papers/t0131/t0131.pdf.

Entrando in un contratto futures perpetuo, l'investitore sta semplicemente scommettendo sul futuro prezzo di un asset. Il contratto può essere long o short e con o senza leva; utilizza un prezzo indice basato sul prezzo medio dell'asset sottostante attraverso le principali borse. L'investitore deposita una garanzia marginale e sceglie una direzione e un importo di leva, poi, a seconda della domanda degli investitori, il contratto può essere scambiato con un premio o uno sconto rispetto al prezzo indice.

In un mercato ideale, il prezzo di un futures perpetuo dovrebbe coincidere o essere molto vicino al prezzo spot dell'asset sottostante. Se ci fosse una grande differenza tra i due prezzi, emergerebbero opportunità di arbitraggio e gli operatori potrebbero sfruttare la differenza di prezzo per ottenere profitti senza rischio. Tuttavia, a causa di vari fattori come la leva, la domanda e l'offerta e le aspettative future, il prezzo del future perpetuo può deviare dal prezzo spot.

Per evitare che il prezzo del contratto futures perpetuo si discosti troppo dal prezzo spot dell'asset sottostante, viene introdotto da dYdX un meccanismo che funziona tramite un *funding rate*[83]. Questo è un tasso di finanziamento che mantiene il prezzo del future vicino all'indice e la cui entità è determinata dalla differenza di prezzo rispetto all'indice pagato da una controparte all'altra. Se il contratto future viene scambiato ad un prezzo superiore all'indice significa che ci sono più persone con posizioni long (che hanno aspettative rialziste). In questo caso chi ha una posizione long pagherà chi ha una posizione short. Ciò rende meno attraente mantenere una posizione long, riducendo così la domanda e portando il prezzo del future più vicino al prezzo spot. Viceversa, se il contratto viene scambiato ad un prezzo inferiore, sono le posizioni short a pagare quelle long: questo tasso spinge gli investitori a prendere posizioni opposte alla maggioranza per mantenere il prezzo del contratto vicino all'indice.

Come un contratto futures tradizionale, anche il contratto futures perpetuo ha due tipi di margine: iniziale e di mantenimento. Finché rispetta il margine di mantenimento richiesto, l'investitore può sempre chiudere il contratto alla differenza del prezzo della posizione nozionale al netto di un'eventuale perdita che potrebbe aver ridotto il suo margine. Ad esempio, se l'investitore ha una posizione long con un margine del 10% e il prezzo di mercato del sottostante scende del 10%, la garanzia viene persa perché la differenza tra l'acquisto al prezzo del contratto e la vendita sul mercato, tenuto conto della perdita,

[83] C.R. Harvey et al. *DeFi and the Future of Finance*

annulla il valore della garanzia. A differenza delle borse tradizionali, dove c'è una margin call se il valore della garanzia raggiunge il margine di mantenimento, su dYdX se qualsiasi posizione scende al di sotto di questo margine i keepers avviano la liquidazione immediatamente (se rimane qualche garanzia, possono tenerla come ricompensa).

Immaginiamo che l'indice del prezzo BTC è valutato 10.000 USDC. Se il prezzo del Bitcoin aumenta del 5%, portando il suo valore a 10.500 USDC/BTC, un investitore che ha investito 1.000 USDC utilizzando una leva di 10x, vedrà amplificare il suo profitto di 10 volte. Ciò significa che ha guadagnato un profitto del 50% sul suo investimento iniziale di 1.000 USDC, ovvero un guadagno di 500 USDC. Tuttavia è cruciale notare che la leva finanziaria è una lama a doppio taglio: se il prezzo del Bitcoin avesse avuto una tendenza negativa, diminuendo del 5%, l'investitore avrebbe perso 500 USDC, ovvero la metà del suo deposito iniziale.

Per capire meglio il meccanismo di collateralizzazione possiamo considerare la situazione in un altro modo. Quando un investitore apre una posizione long a 10.000 USDC/BTC si impegna contrattualmente ad acquistare Bitcoin a quel prezzo, creando un "debito" di 10.000 USDC. Per sostenere questo impegno deposita 1.000 USDC come garanzia, lasciando un ammontare dovuto di 9.000 USDC. Nonostante l'obbligazione, l'investitore ha un saldo positivo equivalente al prezzo d'acquisto concordato di 10.000 USDC. Questa relazione tra l'importo garantito e l'importo dovuto dà un rapporto di collateralizzazione del 111,11%, (= 10.000/9.000) indicando un margine di sicurezza dell'11% prima di una potenziale liquidazione.

Ora vediamo la dinamica di una posizione short. Quando un investitore apre una posizione short, scommette che il prezzo dell'attivo sottostante, in questo caso il Bitcoin, diminuirà. Prendendo una posizione short a 10.000 USDC, l'investitore si impegna a venderlo a questo prezzo, anche se non lo possiede. In pratica, "prendendo in prestito" il Bitcoin per venderlo, l'investitore spera di poterlo ricomprare più tardi a un prezzo inferiore, incassando la differenza. Con il prezzo di vendita fissato a 10.000, l'investitore ha un saldo positivo di 10.000. Questo è amplificato dal margine che ha depositato, di 1.000 USDC, portando il saldo totale a 11.000. Tuttavia, poiché ha venduto qualcosa che non possedeva, ha un dovere di acquistare il Bitcoin, che è attualmente valutato a 10.000. Questo debito rappresenta il saldo negativo. Il rapporto di collateralizzazione ci dice

quanto saldo positivo l'investitore ha rispetto al suo debito: con 11.000 di saldo positivo e un debito di 10.000, il rapporto è 110%, con un margine del 10%.
Ma cosa succede se il mercato si muove contro l'investitore? Se il prezzo del Bitcoin aumenta del 5% a 10.500, il rapporto di collateralizzazione cambia, diventa 104,76% (= 11.000/10.500) ed equivale ad un margine del 4,76%. Se questo margine scende al di sotto di una certa soglia, la posizione dell'investitore potrebbe essere liquidata. Il saldo netto della posizione è ora di 500 USDC: ciò che il liquidatore (keeper) potrebbe incassare chiudendo la posizione dell'investitore.
Il contratto futures perpetuo BTC su dYdX permette agli investitori di accedere ai rendimenti del BTC anche sulla blockchain Ethereum, utilizzando qualsiasi asset ERC-20 come garanzia. I futures perpetui stanno guadagnando popolarità e questa funzionalità potrebbe continuare ad attrarre liquidità nel tempo.

3.4.2 Synthetix

Synthetix è una piattaforma specializzata nel fornire un'esposizione ad asset come valute, materie prime, azioni e indici, senza richiedere il possesso fisico dell'asset sottostante. L'azienda emette "Synth", token il cui valore è ancorato 1:1 a un feed di prezzo sottostante e sostenuto da una garanzia. Teoricamente i Synths possono seguire qualsiasi asset, in posizione lunga o corta, e persino posizioni leveraged[84].
Synthetix permette agli utenti di emettere Synths utilizzando il token nativo della piattaforma, l'SNX, come collaterale. Per esempio, un Synth che traccia il valore del dollaro statunitense viene chiamato sUSD, uno che segue il prezzo del Bitcoin è sBTC e uno ancorato al valore dell'oro viene chiamato sXAU (XAU è il codice che rappresenta una oncia troy d'oro).
Una caratteristica unica di Synthetix è la gestione del debito. Quando gli utenti emettono Synths, utilizzando come garanzia SNX, diventano responsabili di questo debito, nel senso che, per sbloccare la loro garanzia SNX, devono restituire il valore totale in dollari. Il debito globale di tutti i Synths è condiviso collettivamente dai detentori di Synth in base alla percentuale del debito in USD che possedevano quando hanno aperto le loro

[84] Synthetix, "Litepaper", 2023. https://docs.synthetix.io/synthetix-protocol/the-synthetix-protocol/synthetix-litepaper.

posizioni. Ciò che è fondamentale comprendere è che se un utente desidera recuperare i suoi token SNX, bloccati come collaterale per emettere Synths, deve bruciare quest'ultimi. Ciò serve per garantire che la quantità di Synths in circolazione sia sempre supportata da una quantità appropriata di collaterale SNX. Se il valore del Synth in possesso dell'utente aumenta rispetto al momento dell'emissione, dovrà restituire un valore superiore di Synths per riscattare il suo SNX, perché è come se avesse un "debito" maggiore a causa dell'aumento del valore del Synth. D'altra parte, se il valore del Synth scende, l'utente si trova in una posizione vantaggiosa: potrà "bruciare" una quantità inferiore di Synths rispetto a quanto originariamente emesso, beneficiando della differenza tra il valore depositato inizialmente e il valore finale del Synth.

Per capire meglio immaginiamo che tre trader hanno ciascuno investito $10.000 nel sistema, per un totale di $30.000, collateralizzando le loro posizioni con il token SNX. Il primo trader detiene un sBTC che rappresenta il valore di un Bitcoin, valutato $10.000, il secondo trader detiene sETH per un valore di 50 Ethereum, valutati $200 ciascuno, e il terzo trader 10.000 sUSD. Quindi in questo caso ogni trader ha una quota del 33,3% del debito totale del sistema. Se il valore del Bitcoin sale a $11.000 e quello dell'Ethereum sale a $300, il valore totale dei Synths e quindi del debito totale diventa $36.000 (= 1 BTC · $11.000 + 50 ETH · $300 + $10.000). Poiché ogni trader ha una proporzione del debito del 33,3%, il debito di ciascun trader è di $12.000. Confrontiamo ora il valore detenuto da ciascun trader con il loro debito:

1. Primo trader (sBTC): $11.000 - $12.000 = -$1000 (in perdita).
2. Secondo trader (sETH): $15.000 - $12.000= $3000 (in profitto).
3. Terzo trader (sUSD): $10.000 - $12.000 = -$2000 (in perdita)

Nonostante l'aumento del prezzo di Bitcoin, a causa dell'aumento proporzionalmente maggiore del prezzo dell'Ethereum solo il trader che detiene sETH è in profitto.

Un altro scenario si potrebbe verificare nel caso in cui il prezzo del Bitcoin e dell'Ethereum scendano rispettivamente a $8.000 e $150. In questo caso il valore totale del debito diventa $25.500 e il debito di ciascun trader è pari a $8500. La situazione è la seguente:

1. Primo trader (sBTC): $8,000 - $8,500 = -$500 (in perdita).
2. Secondo trader (sETH): $7,500 - $8,500 = -$1,000 (in perdita).
3. Terzo trader (sUSD): $10,000 - $8,500 = $1,500 (in profitto).

Grazie alla stabilità degli sUSD in un mercato ribassista, solo il trader che li detiene è in profitto.
È importante notare che tutto ciò avviene in un contesto in cui si sta utilizzando SNX come collaterale per emettere Synths. Se si fa semplicemente trading di Synths, le dinamiche del profitto e della perdita sono come per qualsiasi altro asset o criptovaluta: comprare basso e vendere alto.
La piattaforma Synthetix dispone anche di un exchange decentralizzato interno che consente agli utenti di scambiare tra loro vari Synths. Questi scambi avvengono al tasso attuale fornito dagli oracoli, in particolare Chainlink.
Il token SNX, oltre a servire come collaterale, permette agli utenti, detenendo e bloccando SNX, di partecipare alla governance della piattaforma e ricevere una quota delle commissioni generate dagli scambi sul DEX di Synthetix.
Synthetix offre un meccanismo robusto e flessibile per la creazione e lo scambio di asset sintetici, fornendo opportunità sia ai trader che agli investitori all'interno dell'ecosistema DeFi. In particolare la possibilità di non detenere fisicamente assets, come Bitcoin o oro, permette agli utenti di non pagare commissioni di entrata e uscita nei vari mercati e garantisce una elevata interoperabilità per il trading di categorie di assets molto diverse.

3.5 Rischi

Nei paragrafi precedenti abbiamo esaminato il vasto mondo della finanza decentralizzata e come esso permetta di accedere ad una ampia gamma di servizi finanziari. La DeFi ha eliminato il rischio di controparte, togliendo gli intermediari e permettendo agli utenti di interagire direttamente tra loro in maniera sicura, rapida e innovativa. Tuttavia il contesto decentralizzato in cui questi servizi si inseriscono non è certo privo di inefficienze e sfide, che gli utenti e gli sviluppatori devono affrontare e comprendere appieno. È fondamentale valutare questi rischi e le possibili soluzioni per garantire non solo la sicurezza dei fondi degli utenti, ma anche la stabilità e la sostenibilità del sistema DeFi nel suo complesso.

3.5.1 Smart contract risk

La maggior parte degli incidenti di sicurezza che avvengono nella DeFi sono causati dalle inefficienze degli smart contract, piuttosto che da capacità eccezionali degli hacker. Nonostante il loro nome, infatti, gli smart contract non sono privi di problemi e rischi. Il funzionamento di questi algoritmi tramite processi *self-executing* può sembrare molto efficiente, tuttavia questi codici sono scritti da persone umane e come tali suscettibili di errore. Inoltre una volta lanciati è difficile, se non impossibile, correggere queste imperfezioni, perché i protocolli di governance richiedono agli utenti di votare prima di modificare qualcosa. Ciò rende la risoluzione di problemi molto rigida e lunga.

Il più grande attacco di hacking è stato nel 2018, con l'exchange giapponese Coincheck che ha perso più di 500 milioni di dollari[85]. Solo nel 2020 sono stati rubati più di 100 milioni[86] e con la crescita esponenziale che la DeFi sta subendo questa cifra è destinata purtroppo a salire. Recente è il caso di Curve, una popolare piattaforma di scambio, che nel luglio 2023 è stata attaccata tramite una *reentrancy vulnerability*[87]. Questa situazione si verifica quando uno smart contract "chiama" un altro contratto esterno alla piattaforma e quest'ultimo poi "richiama" il contratto originale, causando potenzialmente un ciclo infinito. Un "attacco di rientro" è un metodo che consente ad un utente malintenzionato di effettuare una chiamata ricorsiva alla funzione originale prima che il saldo del suo contratto si sia aggiornato nel tentativo di svuotare i fondi[88].

Lo smart contract risk può assumere la forma, oltre che di un hack permesso da un errore nel codice, anche di un exploit economico, cioè una manipolazione del mercato che consente ad un attaccante di prelevare fondi dalla piattaforma oltre la funzionalità prevista per trarre profitto in modo ingiusto[89].

---

[85] Cheng, Evelyn. 2018. "Japanese cryptocurrency exchange loses more than $500 million to hackers." CNBC, 26 Gennaio. https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html.

[86] Sergeenkov, Andrey. 2021 "What Is Smart Contract Risk?" *Crypto Basics*; https://coinmarketcap.com/alexandria/article/what-is-smart-contract-risk.

[87] Pereira, Ana Paula. "Factory pool di Curve Finance exploitate per oltre 47 milioni di dollari a causa di una reentrancy vulnerability." *Cointelegraph Italia*, 31 luglio 2023. https://it.cointelegraph.com/news/curve-finance-pools-exploited-over-24-reentrancy-vulnerability.

[88] Geeksforgeeks, Reentrancy Attack in Smart Contracts. https://www.geeksforgeeks.org/reentrancy-attack-in-smart-contracts/

[89] C.R. Harvey et al. *DeFi and the Future of Finance*

Ad esempio, consideriamo due exchange. Il DEX Alpha è a bassa liquidità e quindi a causa della sua dimensione ridotta risulta essere particolarmente sensibile alle grandi operazioni di acquisto o vendita. Al contrario, il DEX Beta è un grande exchange con un elevato volume di trading e molte più risorse che, invece di determinare autonomamente il suo prezzo per un particolare token, utilizza l'Exchange Alpha come exchange oracolo, ovvero è come un fornitore di prezzi su cui altri si affidano. Un trader malevolo effettua un acquisto significativo di token sul DEX Alpha e dato il suo volume limitato questo acquisto fa salire il prezzo del token in modo considerevole. Poiché il DEX Beta si basa sul prezzo di DEX Alpha per il suo tasso di cambio, anche il prezzo da esso proposto aumenta. A questo punto il trader vende i token che ha appena acquistato sul DEX Alpha al prezzo più elevato sul DEX Beta, ottenendo un profitto. In sintesi, l'attaccante ha sfruttato la bassa liquidità presente nell'exchange Alpha e la dipendenza tra i due DEX, manipolando il mercato a suo favore. La situazione diventa ancora più complessa con l'introduzione dei prestiti flash, che danno la possibilità a chiunque nel network Ethereum di accedere temporaneamente a grandi somme di denaro, amplificando ulteriormente la capacità di un attaccante di sfruttare e manipolare il sistema a suo vantaggio.
Il modo migliore da parte degli sviluppatori per mitigare il problema è quello di condurre ampi audit sugli smart contract prima di lanciare i protocolli. Gli attacchi recenti dimostrano la fragilità della programmazione degli smart contract e aziende di audit come Quantstamp, Trail of Bits e Peckshield stanno emergendo per colmare questa lacuna. Questa soluzione è molto onerosa in termini di costo e tempo, ma è l'unico modo possibile per prevenire i rischi legati ai contratti intelligenti e garantire l'integrità del sistema.

3.5.2 Governance risk

Un aspetto unico della DeFi è la capacità dei possessori dei token di governance di influenzare il funzionamento delle piattaforme tramite il loro diritto di voto. Ad esempio, le proposte di governance possono alterare i pesi nei pool degli AMM o i rapporti di garanzia nei protocolli di prestito, modifiche che possono avere un impatto significativo sulla sicurezza, sulla liquidità e sul rendimento del protocollo.
Un aspetto preoccupante della governance DeFi è la crescente centralizzazione in molte dApp. Sebbene i token di governance di solito abbiano una fornitura fissa che aiuta a

resistere ai tentativi di chiunque di acquisire una maggioranza assoluta, rimane il rischio di un controllo significativo da parte di un attore malintenzionato.
Inoltre, a differenza delle società tradizionali, dove gli investitori attivisti sono vincolati da un "dovere di lealtà" giuridicamente vincolante nei confronti degli azionisti di minoranza (art. 2392 c.c.), nella DeFi questo non esiste.
Nel marzo 2021 True Seigniorage Dollar subì un'incursione legata alla governance. All'epoca, il team di sviluppatori deteneva solo il 9% e un individuo malintenzionato ha iniziato ad acquistare progressivamente $TSD fino a raggiungere una quota del 33% all'interno del DAO. Successivamente ha presentato una proposta di modifica al protocollo e ha votato per essa. Questa modifica gli ha permesso di emettere una quantità gigantesca di $TSD e dopo aver realizzato questa manovra, l'individuo ha successivamente venduto 11,8 miliardi di questi token sulla piattaforma Pancakeswap[90].
Imporre limiti di voto o adottare meccanismi di *lock-up* e *vesting* sono alcune possibili soluzioni che potrebbero agire da deterrente per pratiche di governance malevoli. Il lock up limita la trasferibilità dei token, per un periodo specificato, dopo l'offerta iniziale di monete (ICO) o altro evento di vendita di token, mentre il vesting si riferisce a un periodo durante il quale le azioni o i token assegnati a un individuo diventano progressivamente di sua proprietà[91]. Entrambe le pratiche sono progettate per allineare gli interessi degli stakeholder e garantire una stabilità a lungo termine.

3.5.3 Oracle risk

Gli oracles sono necessari per il corretto funzionamento della maggior parte dei protocolli DeFi. Senza questi strumenti le blockchain sarebbero completamente auto-contenute e non avrebbero conoscenza del mondo esterno oltre alle transazioni aggiunte alla blockchain nativa. Molti protocolli DeFi richiedono l'accesso a prezzi di asset sicuri e resistenti alle manomissioni per garantire che azioni di routine, come le liquidazioni e la

[90] Medium. 2021. "Exploiting a Smart Contract without Security Vulnerabilities: Analysis of True Seigniorage Dollar Attack Event." 17 Marzo. https://certik.medium.com/exploiting-a-smart-contract-without-security-vulnerabilities-analysis-of-true-seigniorage-dollar-c319dce45783.
[91] Bit2Me. 2022. "Cos'è il lock-up e il vesting?." https://support.bit2me.com/it/support/solutions/articles/35000194500-cos-è-il-lock-up-e-il-vesting-.

definizione dei mercati, funzionino correttamente. Il rischio oracoli consiste nella dipendenza del protocollo da questi flussi di dati.

Fino ad ora sono emerse tre principali soluzioni per gli oracle nel mondo della DeFi[92]. La prima è quella degli oracoli di tipo Schelling-point (o *focal point*), dove i detentori di un particolare token votano per determinare l'esito di un evento o per stabilire il valore di un bene. Questo tipo di oracoli si basano sulla teoria dei giochi, dove i detentori di un token specifico votano sul dato richiesto (ad esempio il prezzo di un asset) e la maggioranza viene premiata, incentivando la veridicità. Se si vota ciò che si ritiene che gli altri voteranno come vero, si viene ricompensati, altrimenti il sistema punisce chi fornisce dati scorretti[93]. Questo tipo di oracoli è rappresentato da piattaforme come Augur e UMA. Pur mantenendo un certo grado di decentralizzazione, la loro principale debolezza è la lentezza nel fornire una risposta definitiva.

La seconda è un oracolo API, un sistema che permette ai contratti intelligenti su una blockchain di ricevere dati dal mondo esterno tramite API (*Application Programming Interface*), un'entità centralizzata che risponde in modo asincrono alle richieste di dati o prezzi. Questo tipo di oracolo, quali Provable, Oraclize e Chainlink, agisce come un ponte tra la blockchain e le risorse esterne, come i database o altri servizi web. Tutti i sistemi che si affidano agli oracles basati su API devono fidarsi del fornitore di dati per rispondere con precisione a tutte le richieste.

Il terzo tipo di oracoli è un servizio oracle specifico per le applicazioni Maker e Compound e il suo design varia in base alle esigenze del protocollo per cui è stato sviluppato.

Gli oracoli, così come esistono oggi, rappresentano il rischio più elevato per i protocolli DeFi che ne dipendono. Tutti gli oracles on-chain sono vulnerabili al front-running, e milioni di dollari sono stati persi a causa degli arbitraggisti. Inoltre, servizi oracle come Chainlink e Maker hanno subito gravi interruzioni con effetti a valle catastrofici. Fino a quando gli oracles non saranno nativi della blockchain, rinforzati e dimostrati resilienti, rappresentano la minaccia sistemica più grande per la DeFi oggi.

---

[92] C.R. Harvey et al. *DeFi and the Future of Finance*

[93] Garay, Jose. 2018. "On Oracles and Schelling Points: Schelling schemes and seeking consensus in a Decentralized Oracle Network." Medium, 24 Settembre. https://medium.com/witnet/on-oracles-and-schelling-points-2a1807c29b73.

3.5.4 Scaling Risk

La scalabilità di un sistema si riferisce a quanto esso può crescere senza incontrare un degrado delle prestazioni. Come abbiamo visto, Ethereum e altre blockchain basate precedentemente sul *proof-of-work* avevano una dimensione di blocco fissa. Affinché un blocco diventi parte della catena ogni minatore di Ethereum doveva eseguire tutte le transazioni incluse sulla propria macchina. È irrealistico aspettarsi che ogni minatore elabori tutte le transazioni finanziarie per un mercato finanziario globale. Per esempio la versione precedente di Ethereum era limitata a un massimo di 30 transazioni al secondo (TPS), nonostante quasi tutta la DeFi risiedesse su questa blockchain. Rispetto a Visa, che può gestire oltre 65.000 TPS, Ethereum era capace di gestire meno dello 0,1 percento delle transazioni. La mancanza di scalabilità di Ethereum avrebbe messo a rischio la DeFi di non essere in grado di soddisfare la domanda necessaria[94].

Per superare questo problema, Ethereum si è aggiornato, lanciando a settembre 2022 Ethereum 2.0. Con questa nuova versione c'è stato il passaggio al meccanismo del consenso *proof-of-stake* che ha permesso di elaborare un numero molto maggiore di transazioni al secondo (100.000) e di ridurre il consumo energetico.

Staci Warden, CEO della Algorand Foundation, ha sottolineato come l'accesso a fonti di energia stabili a costi marginali bassi sia fondamentale per la scalabilità delle criptovalute[95]. La migrazione a Ethereum 2.0 è promettente in termini di riduzione dell'impronta di carbonio e miglioramento della sostenibilità, ma gli stakeholder dovrebbero rimanere attenti ai potenziali ostacoli legati alla scalabilità durante questa fase di transizione.

Lo *sharding* di Ethereum 2.0 è una delle principali innovazioni previste per migliorare la capacità e la velocità della rete. Ciò consiste nel "partizionamento dei database" e in pratica permette di dividere la blockchain in molteplici catene minori (*shard chains*) che funzionano in parallelo. Questo permette alla rete di processare molte più transazioni contemporaneamente, riducendo i tempi e aumentando la capacità di elaborazione[96].

---

[94] Chiap et al., *Blockchain*, 78-79.
[95] Duggan, Wayne. 2023. "Che cos'è Ethereum 2.0? Ecco spiegato il Merge." Forbes, 18 febbraio. https://www.forbes.com/advisor/it/investire/criptovalute/merge-ethereum/.
[96] Chiap et al., *Blockchain*, 120.

Parallelamente agli sforzi di migrazione verso Ethereum 2.0, che mira a introdurre profonde migliorie alla scalabilità e all'efficienza attraverso meccanismi come il Proof-of-Stake e lo sharding, sono state sviluppate diverse soluzioni a livello di Layer 2.
Queste soluzioni, come i Rollups ottimistici e gli ZK-Rollups, sono strategie progettate per aumentare la capacità e velocità delle transazioni sulle reti blockchains senza necessariamente effettuare modifiche al protocollo di base, chiamato Layer 1. Queste soluzioni funzionano agendo sul layer sopra la blockchain principale, permettendo ad una grande quantità di transazioni di avvenire off-chain e successivamente essere riportate in un insieme ridotto che viene registrato sulla blockchain principale[97].

3.5.5 Regulatory risk

Una delle aree DeFi in cui vi è minor certezza è sicuramente quella normativa.
L'espansione rapida del mondo decentralizzato ha attirato l'attenzione di organi normativi come l'Unione Europea e la SEC (Security Exchange Commission), con preoccupazioni particolari riguardanti l'identificazione dei clienti, la trasparenza delle operazioni e la natura dei token emessi da vari progetti. A seguito dell'annuncio di Libra, stablecoin di Facebook, vi fu un'ondata di interesse e preoccupazione riguardo alla regolamentazione della DeFi. Le azioni recenti, come la sanzione dell'Office of Foreign Assets Control (OFAC) americano al mixer di criptovalute Tornado Cash nell'agosto 2022[98] e l'iniziativa della Casa Bianca di valutare i rischi legati alla DeFi, mostrano un crescente interesse governativo nel settore. La senatrice Warren ha anche proposto norme riguardo alla tracciabilità delle transazioni e alla conformità delle cripto. Altre giurisdizioni come Abu Dhabi e Dubai stanno cercando di adattare le loro regolamentazioni per la DeFi, mentre altre, come Singapore, stanno adottando quadri rigorosi per attirare imprese e investitori istituzionali.
All'indomani del crollo di FTX a novembre 2022, la senatrice Warren ha presentato una proposta di legge che richiede al Segretario del Tesoro di creare una norma che impedisca

[97] Dexilon, 2022, "Problem of Scaling DeFi". https://dexilon.io/company-and-product/problems-of-scaling-defi/.
[98] Tornado cash è una dApp americana che permette mescolare diversi flussi di criptovalute potenzialmente identificabili. L'8 agosto 2022 il Tesoro degli Stati Uniti ha bloccato il servizio con l'accusa di aver contribuito al riciclaggio di criptovalute per un valore di oltre 7 miliardi di dollari in tre anni. *Fonte*: Wired. https://www.wired.it/article/tornado-cash-privacy-criptovalute/

alle istituzioni finanziarie di effettuare transazioni con i portafogli *self-custody*[99]. Un portafoglio self-custody è un tipo di portafoglio di criptovaluta in cui l'individuo detiene e controlla direttamente le proprie chiavi private, piuttosto che affidarle a una terza parte, come un exchange o una banca. La preoccupazione di alcuni regolatori e politici è che questi portafogli possano facilitare attività illecite, come il riciclaggio di denaro o la frode, poiché sono meno soggetti a regolamentazione e supervisione rispetto alle piattaforme centralizzate.

In Europa, il 20 aprile 2023, il Parlamento europeo ha approvato il regolamento relativo ai mercati dei cripto-asset, MiCAR (*Markets in Crypto-Assets Regulation*), che porterà nuove norme per l'intero settore in tutti i 27 Paesi dell'UE. Tuttavia, questo regolamento si applica principalmente alle persone fisiche e giuridiche e a "determinate altre imprese" e non è esplicitamente presa in considerazione la DeFi. Il regolamento potrebbe in futuro potenzialmente applicarsi ai protocolli decentralizzati e alle DAO, a seconda del livello di decentralizzazione coinvolto[100]. La conformità a livello di protocollo non sarà facile: molte questioni normative devono ancora trovare risposta, soprattutto quelle relative al KYC (*know your customer*), all'antiriciclaggio e altre ancora.

Esiste un trade-off ben visibile tra regolamentazione ed innovazione, che potrebbe anche limitare la libertà e l'innovazione nell'ecosistema delle criptovalute. Se l'ambiente normativo in un determinato paese è troppo severo, l'innovazione si sposterà all'estero; ma, se le regolamentazioni sono troppo permissive, molti consumatori sentiranno venire meno la loro fiducia. Questo settore è tecnicamente impegnativo e l'innovazione è molto veloce e ciò rende la regolamentazione difficile e facilmente obsoleta.

[99] Stadelmann, Kadan. 2023. "I legislatori puntano ora a una regolamentazione dedicata alla DeFi." Cryptonomist, 9 aprile. https://cryptonomist.ch/2023/04/09/i-legislatori-regolamentazione-dedicata-alla-defi/.

[100] Garavaglia, Roberto. 2023. "Cripto-asset: MiCAR approvato dal Parlamento europeo." PagamentiDigitali.it, 20 aprile. https://www.pagamentidigitali.it/esperti-e-analisti/cripto-asset-micar-approvato-dal-parlamento-europeo/#MiCA_e_DeFi.

CAPITOLO 4 - ANALISI QUANTITATIVA DEL MONDO DEFI: FIDUCIA, SENTIMENT DEL MERCATO E TASSI D'INTERESSE

La Finanza Decentralizzata nasce con l'ambizione di replicare prodotti e servizi finanziari tradizionali all'interno di un ecosistema completamente, o quasi, decentralizzato, eliminando intermediari come banche e organismi di controllo garantendo efficienza e sicurezza. La fiducia rappresenta la forza motrice di questo sistema, agendo come catalizzatore della sua impressionante ascesa in un arco di tempo così breve. In un mondo dove la credibilità verso le istituzioni finanziarie tradizionali viene minata frequentemente da crisi e fallimenti, la DeFi si propone come alternativa trasparente in grado di rafforzare e garantire la fiducia dell'utente. Questa non deriva da promesse verbali o da regolamentazioni esterne, ma dalla sicurezza criptografica e dalla decentralizzazione delle operazioni, che riducono il rischio di interferenze, manipolazioni o frodi.

Questo capitolo ha l'obiettivo di analizzare l'evoluzione nel tempo della fiducia e del sentiment generale delle persone verso i protocolli DeFi e come ne hanno influenzato l'uso. Cercheremo poi di capire come gli investitori percepiscono il valore delle criptovalute mentre cresce la reale fiducia nel sistema, offrendo anche una panoramica quantitativa della maturità della DeFi e della sostenibilità economica nel lungo termine. Infine quantificheremo i benefici tangibili dell'utilizzo di applicazioni decentralizzate in termini di rendimenti, evidenziando possibili opportunità e rischi.

Quindi nel primo paragrafo ripercorreremo innanzitutto l'andamento generale delle principali metriche di valutazione del settore: il *Total Value Locked* (TVL), la capitalizzazione di mercato (*Market Cap*) e il numero di utenti che utilizzano le piattaforme. Nel secondo paragrafo entreremo nel dettaglio analizzando la correlazione tra il valore totale bloccato e la percezione degli investitori sul valore delle criptovalute, mentre nel terzo svolgeremo un'indagine sulla valutazione del settore tramite un approfondimento sulla evoluzione del *MarketCap/TVL ratio*. Il quarto e ultimo paragrafo mostra una ricerca reale e attuale sui tassi d'interessi, mettendo a confronto quelli offerti dalle banche tradizionali e quelli che troviamo nelle dApp.

4.1 Panoramica generale

Iniziamo la nostra analisi globale con il parametro più indicativo del mondo DeFi: il *Total Value Locked* (TVL). Questo si riferisce all'importo totale delle attività, tipicamente denominate in criptovalute, bloccate all'interno delle dApp presenti su una blockchain, offrendo indicazioni cruciali sulla scala e sull'attività all'interno dell'ecosistema[101]. Il TVL è un parametro fondamentale per gli stakeholder, in quanto permette loro di valutare il successo e la crescita dei progetti, riflettendo il livello di fiducia e di allocazione del capitale in queste piattaforme.

Valori TVL elevati indicano un forte livello di coinvolgimento e fiducia da parte dei partecipanti, segnalando la popolarità e l'adozione di un particolare protocollo all'interno della comunità. Questo può a sua volta attirare nuovi utenti, investitori e sviluppatori verso un particolare progetto o blockchain, portando ad una maggiore liquidità, innovazione e sostenibilità. Grandi e improvvisi picchi possono significare l'introduzione di un nuovo protocollo, di un aggiornamento di uno preesistente o cambiamenti normativi favorevoli. Al contrario, un calo significativo può indicare una perdita di fiducia improvvisa, causata magari da eventi come una vulnerabilità scoperta nel protocollo, un attacco informatico o bug nei contratti intelligenti e può essere paragonata alle *bank run* tradizionali, in cui i soggetti per paura di perdere i loro soldi li ritirano dagli sportelli. In ogni caso, fluttuazioni improvvise del TVL, sono un segnale per gli operatori di mercato che permettono loro di identificare potenziali opportunità o rischi di investimento.

Prima di passare all'andamento del TVL del mondo DeFi è interessante cogliere un ultimo aspetto. A differenza della capitalizzazione di mercato, metrica ampiamente usata nella finanza tradizionale per valutare una società quotata, il Total Value Locked non rappresenta quegli investitori passivi che hanno interessi nel protocollo esclusivamente perché commerciano criptovaluta. Questi potrebbero non usare necessariamente l'applicazione attivamente, ma semplicemente detenere il token sperando che il progetto cresca e abbia successo[102].

[101] Porcelli, Andrea. "Il Total Value Locked (TVL) nel mondo delle crypto: una panoramica sul 2023." *Cryptonomist*, 24 Giu 2023, https://cryptonomist.ch/2023/06/24/tvl-mondo-crypto-panoramica-2023/.
[102] Portal Cripto. "Che cos'è l'indicatore TVL DeFi?". 28 settembre 2021. https://portalcripto.com.br/it/o-que-e-tvl-indicador-defi/.

L'andamento generale del Total Value Locked del mondo DeFi è rappresentato nella Figura 4.1 ed esso racchiude il TVL di tutte le piattaforme decentralizzate presenti fino ad oggi (settembre 2023).

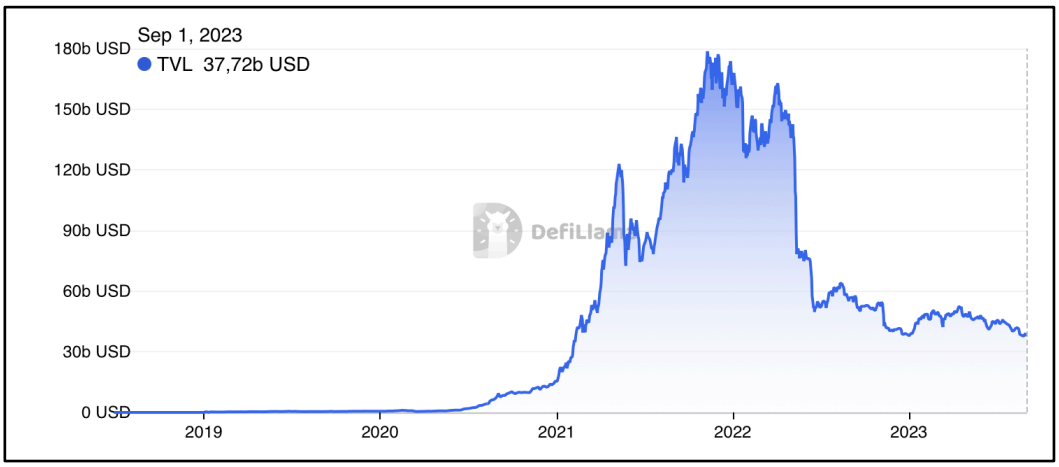


Figura 4.1: Andamento TVL globale DeFi. Fonte: *DeFiLlama*[103]

Il 2020, l'anno della pandemia mondiale da Covid-19, è stato l'anno di svolta per il mondo decentralizzato, che ha spinto il TVL della DeFi da milioni a miliardi. In particolare, fino a maggio 2020, il "capitale bloccato" non superava il miliardo di dollari, ma dopo la cosiddetta *DeFi Summer* (il periodo che va tra giugno e settembre 2020), ha raggiunto circa i 10 miliardi.

Durante questo periodo sono stati lanciati molti nuovi protocolli che offrivano una serie di servizi finanziari inclusivi e quelli già esistenti hanno visto un aumento significativo nel loro TVL. La prospettiva più attraente è stata sicuramente quella di guadagnare reddito passivo tramite lo *yield farming*, ma anche l'introduzione da parte di Compound, Aave e Curve dei token di governance, che permettono agli utenti di guadagnare premi e partecipare alle decisioni della piattaforma, ha incuriosito e attratto molti early adopters. Questi fattori, uniti ai tassi d'interesse tradizionali estremamente bassi a causa della pandemia, hanno favorito la nascita di una nuova era del mondo finanziario.

Tuttavia questo periodo è stato soltanto il primo slancio del mondo della finanza decentralizzata, che ha raggiunto l'apice il 9 novembre 2021, con un valore bloccato totale che ha superato i 178 miliardi di dollari. L'inizio del 2022 è stato molto turbolento con

[103] DeFi Llama, All protocols, https://defillama.com. Consultato il 3 settembre 2023.

una volatilità del TVL molto elevata: probabilmente il mercato DeFi ha iniziato a saturarsi, con molti "imprenditori crittografici" che lanciavano progetti clonando quelli già esistenti, senza un reale valore di fondamento, con l'unico scopo di speculare. Lo yield farming era diventato un gioco per le cosiddette *whales*, indirizzi che detengono grandi quantità di criptovalute e possono influenzare i mercati con le loro operazioni, e molti investitori, perdendo soldi, hanno ritirato i propri depositi. Questo crollo ha segnato la fine della prima fase per il settore DeFi, in quanto il TVL, influenzato dai crash di protocolli di rilevanza come Terra (Maggio 2022), Celsius (Giugno 2022) e del DEX FTX (novembre 2022), avrebbe continuato a scendere per tutto il 2022 perdendo più del 75% in un anno. Il primo semestre del 2023 è stato abbastanza stabile, con il TVL che si è stabilizzato oggi intorno ai 38 miliardi di dollari.

Il secondo aspetto che valutiamo è la capitalizzazione di mercato. Questa metrica, ampiamente usata nella finanza tradizionale per determinare il valore di una società, è utilizzata per indicare la dimensione relativa di una criptovaluta o token rispetto all'intero mercato cripto. Viene calcolata moltiplicando il prezzo corrente di una moneta o token per il suo numero totale in circolazione.

La capitalizzazione totale del mercato DeFi, mostrata in Figura 4.2, rappresenta il valore combinato di tutti i token e le monete associate alle piattaforme DeFi, cioè tutti i token, criptoasset e stablecoin.

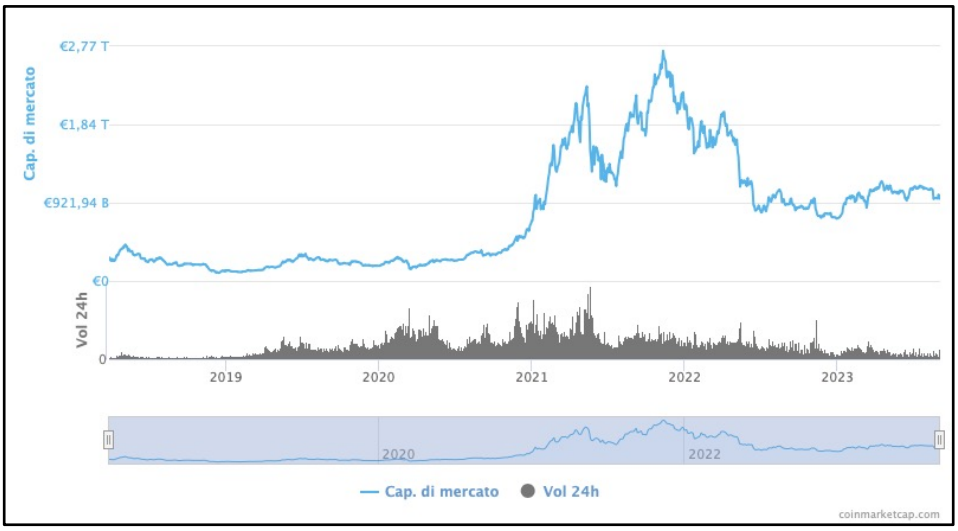


Figura 4.2: Andamento Market Cap globale DeFi. Fonte: CoinMarketCap[104]

[104] CoinMarketCap, Global Cryptocurrency Chart – Total Cryptocurrency Market Cap, https://coinmarketcap.com/charts/. Consultato il 5 settembre 2023.

Questo parametro fornisce un'indicazione dell'opinione pubblica nell'ecosistema DeFi e serve come indicatore della dimensione e dell'importanza del settore. È fondamentale notare che essa, mentre un TVL elevato mostra un ampio utilizzo e fiducia in una particolare piattaforma o criptovaluta, non è necessariamente una misura di successo o di stabilità, poiché fornisce esclusivamente una panoramica quantitativa del valore attribuito dai partecipanti al mercato a un token o dApp.

Già a prima vista si può notare una correlazione molto forte tra il Total Value Locked e il Market Cap cripto complessivo; infatti l'andamento generale della metrica è molto simile a quello del TVL precedentemente analizzato, con il suo picco a novembre 2021 (€2,7 bilioni) e un 2022 molto turbolento. Un approfondimento dell'argomento verrà svolta nel secondo paragrafo.

Un ultimo parametro da considerare riguarda quello degli utenti della DeFi.

Prima di analizzare questo dato occorre fare una precisazione: il concetto di "utente" nella DeFi può essere ambiguo, perché una singola persona potrebbe avere più indirizzi ed interagire con protocolli DeFi da ciascuno di essi, risultando come "multipli" nelle statistiche.

Nonostante che il TVL e il Market Cap siano stati molto volatili nel corso degli anni, con periodi di evidenti flessioni e crisi, gli utenti, dal 2021, sono cresciuti in maniera quasi lineare, superando i 40 milioni a giugno 2023 (Figura 4.3).

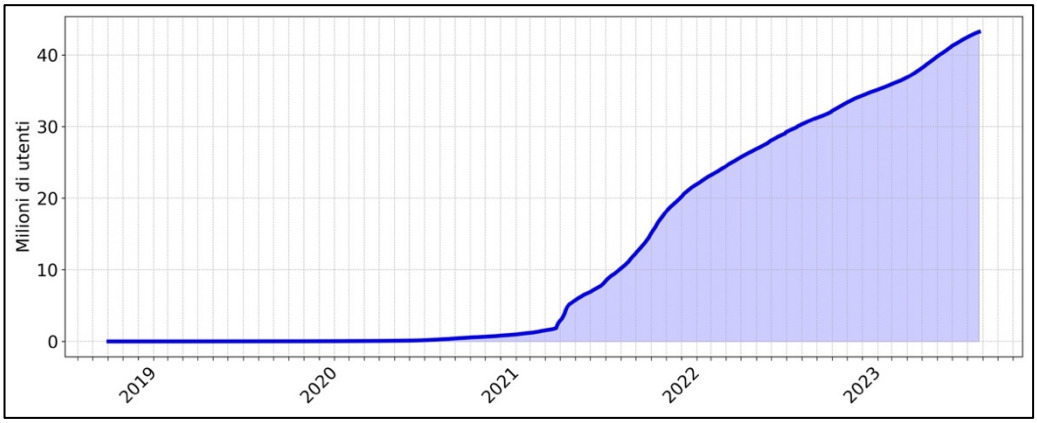


Figura 4.3: Utenti DeFi. Fonte: Dune[105]

[105] Dune, Defi users over time, https://dune.com/rchen8/defi-users-over-time.

Le cause di questa asincronia possono essere molteplici. Innanzitutto il 2020, come detto precedentemente, ha segnato l'inizio del fenomeno dello yield farming, ma, come suggerisce Google Trends, è stato nel 2021 che ha guadagnato un'attrazione mainstream[106]. Infatti man mano che nuovi protocolli nascevano e quelli esistenti lanciavano nuove versioni, con sempre maggiori funzionalità, si è venuto a creare il cosiddetto fenomeno *DeFi Legos*. Questi "blocchi lego", virtualmente rappresentati dalle funzionalità del mondo DeFi, possono essere integrati e considerati come un protocollo unico con più funzioni che soddisfano tutte le esigenze. Inoltre i miglioramenti relativi alle interfacce e all'esperienza dell'utente hanno reso le piattaforme più users friendly, contribuendo a rendere la DeFi più comprensibile e accessibile per la persona media[107]. Con il passare del tempo, nonostante qualche crash, gli investitori possono aver notato una certa resilienza agli attacchi e affidabilità dei protocolli. Questo fattore, insieme alla nascita di protoccoli di assicurazione come Nexus Mutual[108], dApp che mitiga lo smart contract risk offrendo assicurazioni sui depositi, può aver aumentato la fiducia degli utenti nel settore. Un ulteriore motivo che può aver spinto l'introduzione di nuovi utilizzatori sono le soluzioni legate all'interoperabilità. Come menzionato nel paragrafo riguardante lo scaling risk (*3.5.4*), l'evoluzione dell'infrastruttura tecnologica attraverso soluzioni di Layer 2 e aggiornamenti significativi, in particolare sull'Ethereum, ha offerto la promessa di transazioni più veloci e a costi ridotti, promuovendo una maggiore inclusività, efficienza e diversità nel settore. Tuttavia, nonostante Ethereum sia rimasta la principale piattaforma di riferimento per i protocolli DeFi, le sfide persistenti legate alle gas fees e alla scalabilità hanno spianato la strada alla nascita e all'ascesa di nuove blockchain come Binance e Polygon. Queste nuove catene, sfruttando l'interoperabilità e integrandosi con soluzioni di Layer 2, non solo hanno risolto alcune delle sfide esistenti, ma hanno anche introdotto e ospitato nuovi protocolli DeFi, ampliando in modo significativo l'offerta e la diversità dell'intero ecosistema.

---

[106] "Yield Farming," Google Trends, https://trends.google.it/trends/explore?date=today%205-y&q=yield%20farming&hl=it.
[107] Crabb, Jon. "DeFi Design Tips: Volume One." *Medium.* February 9, 2022. https://medium.com/@JonCrabb/defi-design-tips-volume-one-6507512f9c98.
[108] Nexus Mutual. https://nexusmutual.io.

4.2 Dall'importo bloccato al valore di mercato: Correlazione e Causalità

Abbiamo visto cosa sono e come si sono mossi nel tempo i due indicatori più osservati del mondo DeFi. Ma in che modo queste due metriche interagiscono tra loro? C'è una correlazione diretta tra l'ammontare dei fondi bloccati in tutti i protocolli e la loro valutazione di mercato? E se sì, oltre a correlazione c'è causalità? Cosa può dirci questo legame sulle dinamiche di mercato e sulle potenziali opportunità o rischi per gli investitori? Nel presente paragrafo risponderemo a questi quesiti.

Come evidenziato precedentemente, i grafici delle due metriche sono facilmente sovrapponibili e quindi già questa informazione ci fornisce una buona probabilità che ci sia una forte correlazione. Per esserne sicuri è stata svolta un'analisi più approfondita, che ha come obiettivo quello di scoprire il coefficiente di correlazione tra le due serie storiche.

Inizialmente, è stato svolto un *Augmented Dickey-Fuller* (ADF) test sulle singole serie storiche per testare l'ipotesi che esse non siano stazionarie. La stazionarietà è un presupposto fondamentale per l'analisi statistica delle serie storiche: implica che le proprietà statistiche di una serie, in particolare media e varianza, rimangano costanti nel tempo. Il test non ha rigettato l'ipotesi nulla di non stazionarietà, per cui prima di procedere è stato necessario trasformare le serie in forme stazionarie, ricorrendo alla differenziazione. Questo metodo, che implica la sottrazione di osservazioni correnti da quelle precedenti, ha l'obiettivo di eliminare eventuali tendenze temporali, rendendo le proprietà statistiche delle serie più affidabili.

Il coefficiente di correlazione tra le serie del TVL complessivo e della capitalizzazione di mercato totale su base settimanale, differenziate, è pari a 0.73. Lo scatter plot con retta di regressione è mostrato in Figura 4.4.

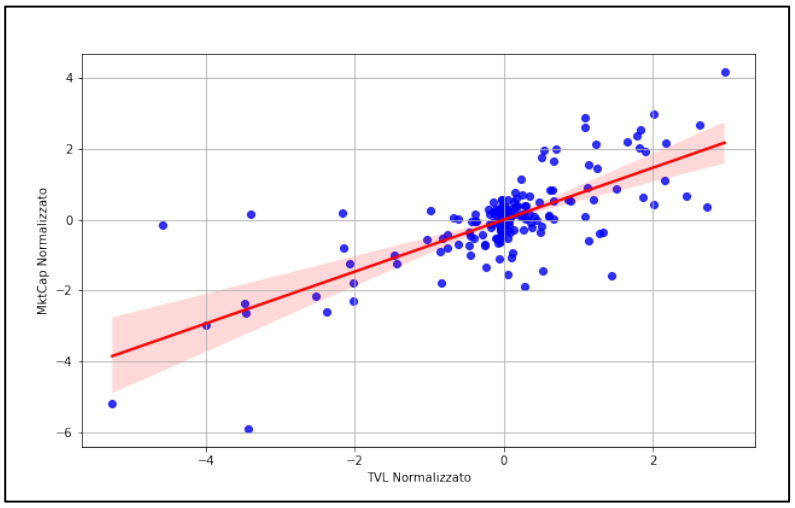


Figura 4.4: Correlazione tra TVL e Market Cap differenziati e normalizzati

Questo valore implica una forte relazione lineare positiva tra i fondi bloccati nei vari protocolli e il valore complessivo dei token. Se vediamo il TVL come un indicatore di fiducia da parte degli utenti, una crescita del Market Cap contestuale ne è la conferma: l'incremento del TVL delle piattaforme DeFi è supportato da una valutazione di mercato quasi corrispondente.

Tuttavia "correlazione" non implica necessariamente "causalità", cioè non possiamo essere certi che, nonostante questo coefficiente sia elevato, una variabile fornisca informazioni utili per prevedere l'altra. Per testare la causalità, quindi, è stato fatto il test di causalità di Granger, dove sono stati provati entrambi i casi: se il TVL causa (nel senso di Granger) il Market Cap e viceversa. Prima di procedere è necessario fare una precisazione statistica: in questo contesto per causalità non significa che ci sia una relazione causale diretta nel senso tradizionale, ma bensì che i valori passati di una serie hanno un effetto statisticamente significativo sui valori presenti dell'altra serie. È emerso che soltanto il Market Cap potrebbe fornire informazioni significativamente utili per prevedere il TVL e non il contrario: gli utenti potrebbero interpretare la capitalizzazione di mercato come un indicatore di affidabilità e fiducia, aumentando (o diminuendo) la quantità di fondi da loro depositati nei protocolli.

È prudente tenere in considerazione che potrebbero esserci altri fattori che influenzano entrambe le metriche, quali eventi esterni, condizioni generali dei mercati e introduzione

di nuovi protocolli; ciò nonostante i risultati trovati rimangono un'analisi affidabile del mercato DeFi nel suo complesso.

4.3 Valutazione della DeFi: il MarketCap/TVL ratio

Concludiamo l'indagine generale del settore utilizzando le due metriche con cui abbiamo finora lavorato per calcolare e studiare l'andamento di un'altra variabile: il *MarketCap/TVL ratio*. Questo indice è dato dal rapporto tra la capitalizzazione di mercato e il Total Value Locked e indica la valutazione di un protocollo rispetto alla sua domanda[109]. Può essere visto come il P/E ratio dei mercati tradizionali, nel senso che fornisce le stesse informazioni utili per gli investitori riguardo la valutazione e potenzialità del caso preso in esame, ma qui lo utilizziamo per determinare se l'intero settore DeFi è sopravvalutato o sottovalutato. Un ratio elevato potrebbe indicare che gli investitori hanno alte aspettative per il futuro della DeFi (o che il settore potrebbe essere in una bolla); al contrario un rapporto basso potrebbe indicare che il mercato vede la DeFi come sottovalutata rispetto al valore che sta effettivamente creando.
Plottando l'andamento del MarketCap/TVL ratio nel tempo è emersa una cosa molto interessante: il rapporto è drasticamente calato nel corso del tempo, avvicinandosi a valori "sostenibili" solo negli ultimi due anni (Figura 4.5).

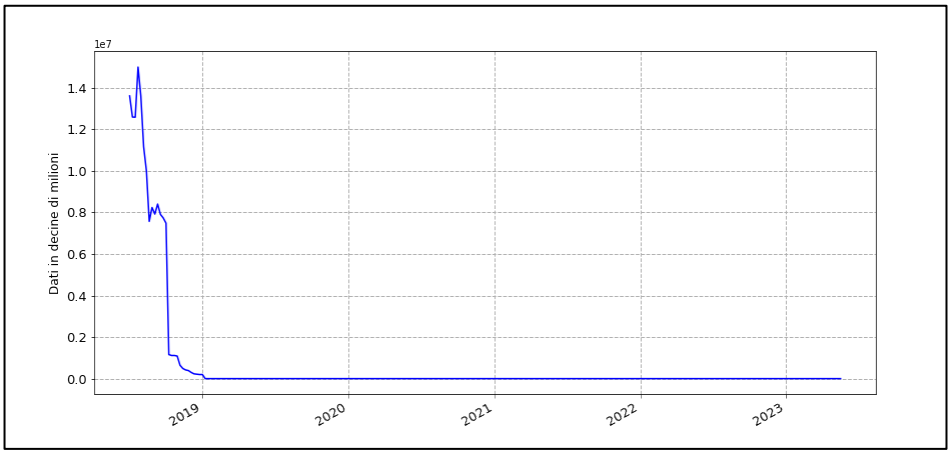


Figura 4.5: MarketCap/TVL ratio (luglio2018 - luglio 2023)

[109] Martin, Mike. "TVL vs Market Cap vs TVL Ratio: Crypto Metrics Explained." TastyCrypto, 2023. https://www.tastycrypto.com/blog/tvl-vs-market-cap/.

Per questo è stato necessario svolgere un'analisi più approfondita, suddividendo l'intervallo considerato in tre sottoperiodi:

- luglio 2018 – gennaio 2019: il rapporto passa da 14 milioni a poco meno di 500. Il settore cripto era ancora troppo giovane e caratterizzato da speculazioni e incertezza sul suo futuro, disincentivando potenziali utenti a depositare i propri risparmi nella piattaforma. La rapida discesa del rapporto tra Market Cap e TVL è stata causata dalla prima febbre da "oro digitale": nuovi utenti sono stati attirati da promesse di alti rendimenti, che hanno portato una grande affluenza di capitale all'interno dei protocolli rispetto alla loro valutazione di mercato, correggendo in soli sei mesi un'estrema sopravalutazione iniziale (Figura 4.6);

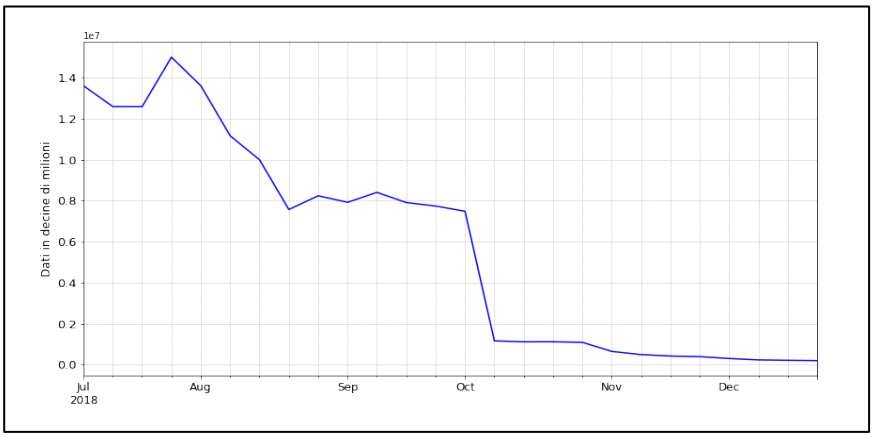


Figura 4.6: MarketCap/TVL ratio (luglio2018 – gennaio 2019)

- gennaio 2019 – novembre 2020: la frenesia speculativa iniziale si è attenuata e la DeFi inizia ad acquisire una reale fiducia da parte degli utenti, con una valutazione che diventa man mano più stabile e proporzionale al valore effettivamente bloccato nei protocolli. Solamente durante la Summer DeFi il rapporto scende del 85% in soli tre mesi, evidenziando la nascita di innovative dApp e un crescente interesse verso il settore (Figura 4.7);

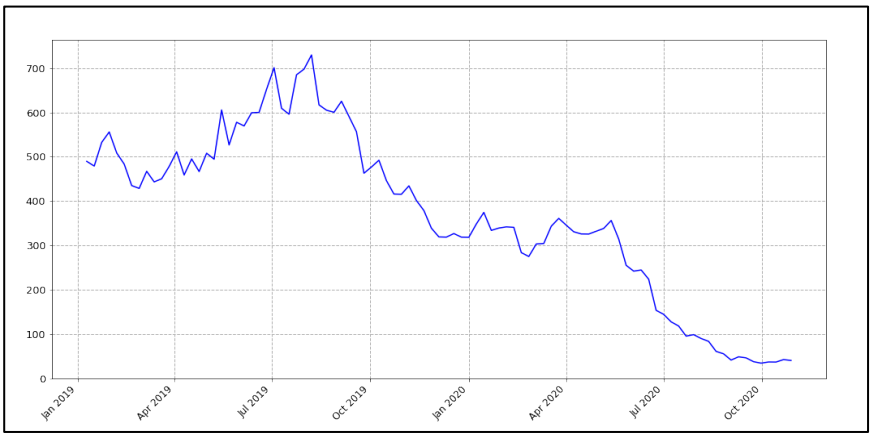


Figura 4.7: MarketCap/TVL ratio (gennaio 2019 – novembre 2020)

- novembre 2020 – giugno 2023: il rapporto inizia ad assestarsi su valori ancora più proporzionali (si passa da 90 a 25 in tre anni), suggerendo che il mercato inizia a credere che il settore sia valutato in modo equo rispetto al capitale bloccato. La relativamente leggera diminuzione del MarketCap/TVL ratio in un arco di tre anni è indicativa di un mercato sempre più maturo e di una comprensione approfondita delle dinamiche da parte degli investitori (Figura 4.8).

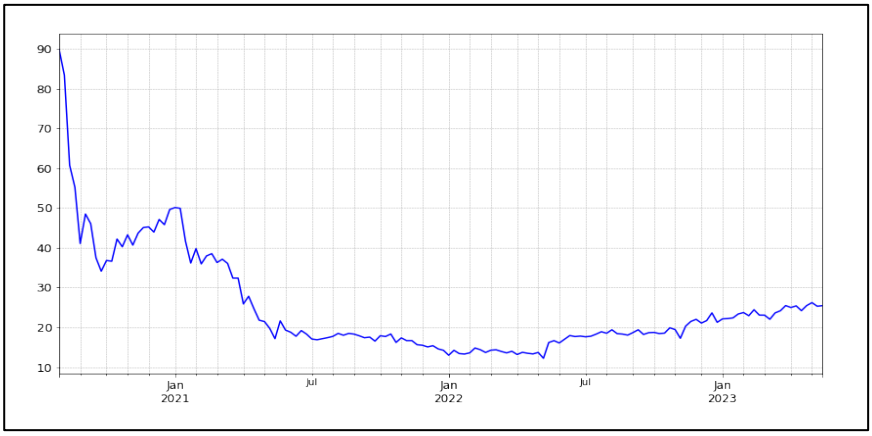


Figura 4.8: MarketCap/TVL ratio (novembre 2020 - giugno 2023)

Questi tre periodi hanno mostrato l'evoluzione del settore DeFi nella sua globalità, delineando chiaramente le diverse fasi della sua maturità. Durante la fase iniziale di sovrastima, dove, come spesso accade, l'emergere di una nuova tecnologia ha spinto il mercato verso valutazioni esagerate, si manifesta la natura entusiasta e speculativa di

molti investitori. Con l'avanzare del tempo, le innovazioni continue, la resilienza ad alcuni attacchi e la crescente accettazione da una porzione di utenti sempre maggiore hanno contribuito a rafforzare la fiducia e a ridurre la volatilità, portando ad una valutazione più equilibrata e in linea con i valori reali. L'ultima fase suggerisce che la percezione di rischio speculativo si è notevolmente ridotta e il mercato sembra aver gradualmente adattato le sue percezioni ai fondi effettivamente bloccati nei protocolli, portando il MktCap/TVL ratio ad un valore più sostenibile nel tempo, con gli stakeholder che ora vedono la DeFi sempre più come un pilastro solido e affidabile della finanza digitale.

4.4 DeFi vs Banche: confronto tassi d'interesse

I tassi d'interesse rappresentano un indicatore fondamentale dell'equilibrio tra domanda e offerta di capitali, influenzando decisioni di investimento, prestiti e risparmi. Nei sistemi finanziari tradizionali la decisione sui tassi d'interesse spetta ad entità centralizzate che in base a fattori macroeconomici e politiche monetarie stabiliscono il livello più adeguato al momento. Le dApp, invece, introducono un sistema decentralizzato, basato su protocolli algoritmici e contratti intelligenti, che opera in modo automatizzato. In questo mondo la determinazione dei tassi d'interesse è strettamente legata alla dinamica della domanda e dell'offerta in tempo reale: se su una piattaforma DeFi c'è una forte domanda di prestiti ma una scarsa fornitura di liquidità, i tassi d'interesse tendono ad aumentare, incentivando più depositi e viceversa.

Per condurre un'analisi comparativa tra i tassi d'interesse offerti dalle banche tradizionali e quelli disponibili sulle dApp, ci siamo basati sulla media mensile degli AAR (*Annualised Agreed Rate*), l'equivalente dei TAN in Italia[110], applicati dalle banche della zona Euro alla categoria famiglie e associazioni no profit. È stata selezionata questa quota di società perché rappresenta una vasta gamma di consumatori all'interno dell'area euro che potrebbe accedere ai servizi finanziari in modo decentralizzato.

[110] Elena Collina, Danilo Liberati, e Pasquale Maddaloni, *Handbook on the data published by the Bank of Italy*, "Bank interest rates", Bank of Italy, 3 Marzo 2023, https://www.bancaditalia.it/pubblicazioni/metodi-e-fonti-approfondimenti/metodi-fonti-2023/Methods-and-Sources_Bank-interest-rates.pdf?language_id=1.

In merito ai tassi sui prestiti abbiamo rivolto l'attenzione su quelli "al consumo", con l'intento di esplorare una tipologia di prestiti che risponde alle esigenze di finanziamento più urgenti e frequenti sia delle famiglie che delle istituzioni no profit, quali l'acquisto di beni quotidiani o la copertura di spese impreviste.

Per quanto riguarda i tassi sui depositi l'analisi si è concentrata su quelli con una scadenza concordata: i certificati di deposito (CD), cioè "non trasferibili che non possono essere convertiti in valuta prima di un termine fisso concordato o possono essere convertiti del termine, ma con un addebito di una penalità al titolare"[111].

Per dare una visione più ampia l'analisi ha considerato due intervalli temporali: uno a breve termine, inferiore ad un anno, e uno a medio termine.

Per entrambe le maturity è stato calcolato il margine d'interesse (spread) ed è stato messo a confronto con quello proposto dalle dApp Aave[112] e Compound[113], che rappresentano quasi il 50% del market cap complessivo delle piattaforme di lending. Come presentato nei capitoli precedenti i tassi d'interesse di queste piattaforme sono calcolati algoritmicamente considerando, oltre che la domanda e l'offerta per quello specifico token, anche il rischio associato, cioè la sua volatilità. Perciò, per svolgere un'analisi comparativa con la finanza tradizionale, sono stati analizzati i tassi dei pool di USDC, un token ad alta liquidità strettamente ancorato al dollaro.

Prima di immergerci nell'analisi comparativa è essenziale comprendere le differenze intrinseche tra i due tipi di tassi in esame. I tassi tradizionali sono, come detto, espressi come TAN, che rappresenta l'interesse calcolato su base annua senza tener conto della capitalizzazione composta. Invece, quelli del mondo DeFi, sono comunemente espressi come APY (*Annual Percentage Yield*), che tiene conto degli effetti della capitalizzazione composta, ossia degli interessi sugli interessi. In particolare, la maggior parte dei protocolli decentralizzati capitalizza i propri rendimenti in maniera continua. Per questo, per rendere più precisa possibile la nostra ricerca, abbiamo capitalizzato continuamente

---

[111] European Central Bank. "Definition: Deposit with agreed maturity." In *Guideline of the European Central Bank of 1 August 2007 on monetary, financial institutions and markets statistics (recast)*. Official Journal of the European Union No L 341, 27 Dicembre 2007. https://www.tariffnumber.com/info/abbreviations/11814.

[112] Dune, " Aave-v2-Ethereum Deposit & Borrow APY". Consultato il 4 settembre 2023. https://dune.com/queries/580512/1090585.

[113] Dune, "USDC Interest Rate on Compound". Consultato il 4 settembre 2023. https://dune.com/queries/1009795/1745172.

anche i tassi nominali tradizionali, in modo da effettuare confronti tra rendimenti calcolati allo stesso modo.

Dopo questa necessaria precisazione entriamo nel vivo dell'analisi, andando a vedere il comportamento dei tassi sui depositi delle banche della zona Euro e delle piattaforme decentralizzate negli ultimi due anni. L'andamento è mostrato in Figura 4.9 e, come ci aspettavamo, il rendimento offerto sul liquidity mining DeFi è più volatile, a causa della natura emergente delle criptovalute e della sensibilità del mercato DeFi a lanci di nuove applicazioni, notizie sul regolamento, fluttuazioni dei prezzi delle criptovalute e dinamiche di liquidità.

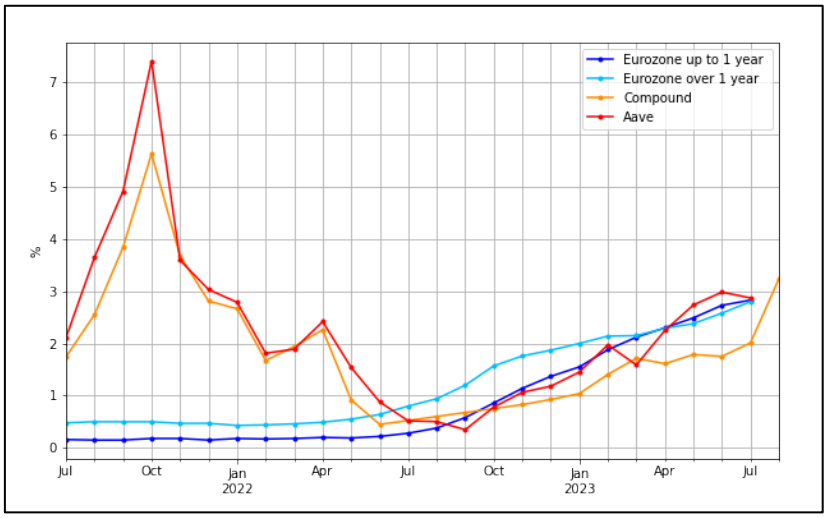


Figura 4.9: Confronto tassi sui depositi (pool USDC)[114,115]

Fino a giugno 2022 i tassi sulla liquidità immessa nei protocolli decentralizzati sono stati ampiamente superiori a quelli delle banche sui certificati di deposito, probabilmente a causa di una crescente domanda di liquidità, spinta da nuovi protocolli o farming di nuovi token. Tuttavia, il successivo allineamento dei tassi offerti da Aave e Compound con i

[114] European Central Bank, "Bank interest rates - deposits from households with an agreed maturity of over one year (new business) - euro area," https://data.ecb.europa.eu/data/datasets/MIR/MIR.M.U2.B.L22.K.R.A.2250.EUR.N, consultato il 4 settembre 2023.

[115] European Central Bank, "Bank interest rates - deposits from households with an agreed maturity of up to one year (new business) - euro area," https://data.ecb.europa.eu/data/datasets/MIR/MIR.M.U2.B.L22.F.R.A.2250.EUR.N, consultato il 4 settembre 2023.

tassi tradizionali suggerisce una normalizzazione, causata da una maggiore diffusione, una minore necessità di attrarre liquidità o una convergenza verso modelli di business più sostenibili.

Per quanto riguarda i tassi sui prestiti, come mostrato in figura 4.10, la situazione è notevolmente diversa.

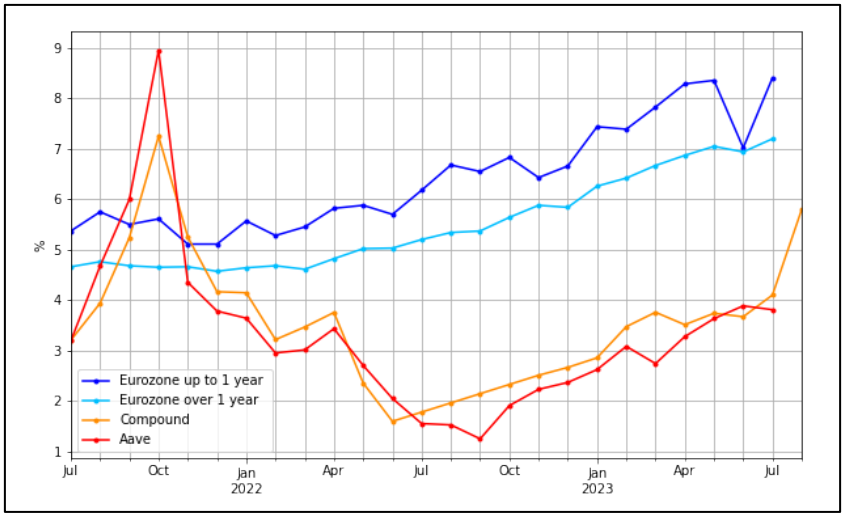


Figura 4.10: Confronto tassi sui prestiti (pool USDC)[116,117]

Negli ultimi due anni i lending rates DeFi hanno superato quelli tradizionali solo nell'autunno 2021; da allora, hanno registrato un marcato calo, posizionandosi decisamente al di sotto dei livelli tradizionali.

Il declino dei tassi DeFi può essere spiegato con una crescente competizione tra le piattaforme o un eccesso di liquidità, dovuto a un numero crescente di utenti che desiderano depositare piuttosto che prendere a prestito, portando le piattaforme ad esercitare una pressione al ribasso sui loro tassi per liberarsi delle riserve in eccesso. È utile ricordare che spesso i *supply rates* e i *borrow rates* delle applicazioni decentralizzate sono, come ampiamente spiegato nel caso di Compound, legati da una relazione matematica ed è per questo che ci aspettiamo che si muovano approssimativamente

[116] European Central Bank. "Bank interest rates - loans to households for consumption & other purposes with an original maturity of up to one year - euro area." Consultato il 5 settembre 2023 https://data.ecb.europa.eu/data/datasets/MIR/MIR.M.U2.B.A25.F.R.A.2250.EUR.O.

[117] European Central Bank. "Bank interest rates - loans to households for consumption & other purposes with an original maturity of over one & up to five years - euro area." Consultato il 5 settembre 2023. https://data.ecb.europa.eu/data/datasets/MIR/MIR.M.U2.B.A25.I.R.A.2250.EUR.O.

insieme. È interessante notare che nell'ultimo anno, nonostante le differenze di valore, la traiettoria dei tassi DeFi ha seguito un andamento simile a quello dei tassi bancari, suggerendo una certa correlazione tra le dinamiche del mercato centralizzato e decentralizzato.

Concludiamo l'indagine con l'aspetto più interessante della nostra ricerca: confrontare i margini d'interesse nei due diversi contesti. Considerando le due piattaforme prese in esame, Aave e Compound, si osserva che gli spread sono risultati in media inferiori del 3,5% rispetto ai loro corrispettivi tradizionali (Figura 4.11).

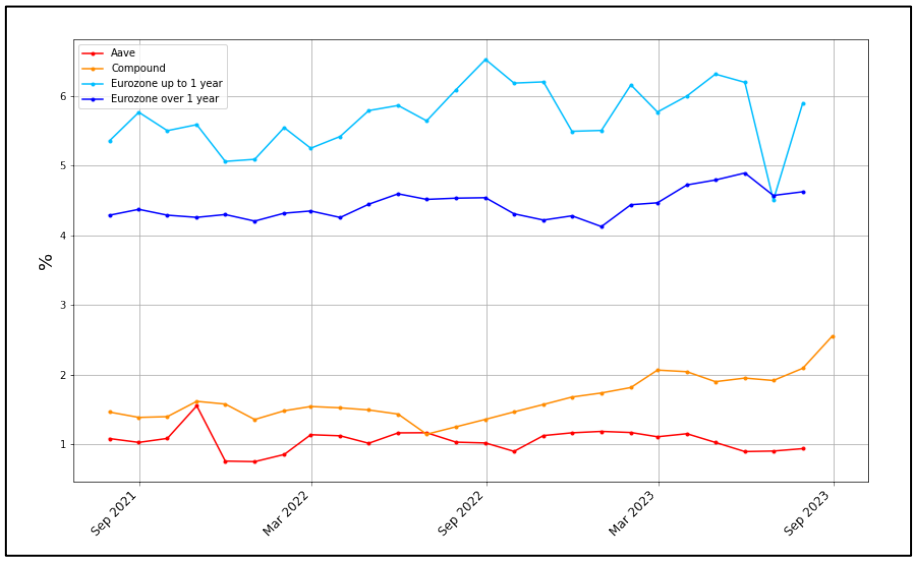


Figura 4.11: Confronto spreads (pool USDC)

La motivazione principale è senza dubbio quella relativa al fatto che le piattaforme DeFi, essendo basate su smart contract e operando in modo automatizzato, tendono ad avere costi operativi (*brick-and-mortar costs*) inferiori rispetto alle banche tradizionali, potendosi permettere spread più contenuti. Inoltre l'ambiente DeFi è relativamente giovane e le piattaforme, operando in un mercato aperto e trasparente in cui gli utenti possono facilmente spostare la loro liquidità, potrebbero dover lottare fra loro per attrarre liquidità e clienti.

Oltre ciò non bisogna dimenticare l'ulteriore incentivo che molte di queste piattaforme DeFi offrono: la distribuzione di token di governance. Piattaforme come Aave e Compound, ad esempio, ricompensano i loro utenti non solo con tassi di interesse competitivi, ma anche distribuendo i loro token nativi, rispettivamente AAVE e COMP.

Questi token, oltre a rappresentare un potenziale guadagno per i detentori grazie alle dinamiche di mercato, conferiscono, come già spiegato, anche diritti di voto all'interno della governance della piattaforma ed essendo offerti sia in caso di depositi che di prestiti contribuiscono ulteriormente ad assottigliare lo spread.

L'ascesa delle dApp ha rivoluzionato il modo in cui i tassi d'interesse sono determinati. Spostandosi da un modello centralizzato top-down a uno decentralizzato bottom-up, dove l'ultima parola è dei clienti, si sono generate sempre più nuove opportunità per il cambiamento e l'efficienza del sistema finanziario. Sebbene gli inferiori margini inferiori della DeFi possano suggerire maggiore efficienza e competizione, questo ambiente decentralizzato porta con sé sia opportunità che sfide. Da un lato, eliminando gli intermediari, riduce potenzialmente le commissioni e democratizza l'accesso ai servizi finanziari, dando anche voce in capitolo agli utenti nella determinazione di determinati parametri del sistema, inclusi i tassi d'interesse. D'altro canto, mentre nella TradFi le banche offrono un certo grado di protezione per i depositi e una relativa stabilità, nella DeFi gli utenti devono navigare in un ambiente più imprevedibile, dove i tassi possono fluttuare drasticamente in brevi periodi di tempo e in un sistema dove gli algoritmi giocano un ruolo centrale. Piccoli errori o vulnerabilità tecniche possono avere effetti amplificati e un margine d'interesse ridotto potrebbe limitare la capacità di una piattaforma di assorbire gli shock o di compensare adeguatamente per i rischi assunti.

Appendice capitolo 4 - Codice di programmazione Python

Codice paragrafo 4.2

```
# Importo i dati e le librerie necessarie

import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns

tvl: pd.DataFrame = pd.read_excel("/Users/lorenzostagi/Desktop/DATI/tvldefi.xlsx")
tvl['Date'] = pd.to_datetime(tvl['Date'])
tvl.set_index('Date', inplace=True)

mktcap_sett: pd.DataFrame = pd.read_excel("/Users/lorenzostagi/Desktop/DATI/mktdefi.xlsx")
mktcap_sett['Date'] = pd.to_datetime(mktcap_sett['Date'])
mktcap_sett.set_index('Date', inplace=True)

# Resemple il TVL per ottenere la media settimanale

tvl_sett = tvl.resample('W-WED').last()

# Elimino eventuali non valori

tvl_sett.dropna(inplace=True)
mktcap_sett.dropna(inplace=True)

# Testo la stazionarietà delle serie tramite il Augmented Dickey-Fuller test

from statsmodels.tsa.stattools import adfuller
tvl_adf = adfuller(tvl_sett)
mktcap_adf = adfuller(mktcap_sett)
print("p-value TVL:",tvl_adf[1])
print("p-value MktCap:",mktcap_adf[1])

p-value TVL: 0.5036270400064333
p-value MktCap: 0.5216109288095491
```

Entrambi i p-value sono abbondantemente maggiori dei livelli di significatività del 1%, 5% e 10%, per cui rigettiamo l'ipotesi nulla di non stazionarietà.

```
# Differenzio le serie per renderle stazionarie

tvl_diff = tvl_sett['TVL'].diff().dropna()
mktcap_diff = mktcap_sett['MktCap'].diff().dropna()

# Eseguo nuovamente il test di Dicekey-Fuller

tvl_adf = adfuller(tvl_diff)
mktcap_adf = adfuller(mktcap_diff)
print("p-value TVL:",tvl_adf[1])
print("p-value MktCap:",mktcap_adf[1])

p-value TVL: 0.02791262755673959
p-value MktCap: 5.092332232967229e-08
```

A livelli di significatività del 5% e 10% posso rigettare l'ipotesi nulla, per cui entrambe le serie sono stazionarie ad un livello di significatività di almeno il 5%.

```
# Calcolo il coefficiente di correlazione

coeff_corr = tvl_diff.corr(mktcap_diff)

print('Coefficiente di correlazione TVL-MktCap:', coeff_corr)
```

```
Coefficiente di correlazione TVL-MktCap: 0.733647602228519

# Creo un DataFrame combinando le due serie

tvl_mktcap_diff = pd.DataFrame({
    'TVL': tvl_diff,
    'MktCap': mktcap_diff
})

# Normalizzo le serie per averle nella stessa scala

from sklearn.preprocessing import StandardScaler
ss = StandardScaler()
tvl_mktcap_norm_array = ss.fit_transform(tvl_mktcap_diff)

# Converto l'output normalizzato nuovamente in un DataFrame

tvl_mktcap_norm = pd.DataFrame(tvl_mktcap_norm_array, columns=['TVL', 'MktCap'], index=tvl_diff.
index)

# Plotto il grafico a dispersione

plt.figure(figsize=(10, 6))
sns.regplot(x="TVL", y="MktCap", data=tvl_mktcap_norm, color="blue", line_kws={"color": "red"})
plt.grid(True)
plt.xlabel('TVL Normalizzato')
plt.ylabel('MktCap Normalizzato')
plt.close()

# Testo la causalità del Market Cap sul TVL tramite il Granger Casusality test

from statsmodels.tsa.stattools import grangercausalitytests
tvl_mktcap_diff = tvl_mktcap_diff.dropna()
max_lag = 4 # Per comodità verifico l'ipotesi su un lags di 4 settimane
gc_test = grangercausalitytests(tvl_mktcap_diff, maxlag=max_lag, verbose=True)

Granger Causality
number of lags (no zero) 1
ssr based F test:         F=13.6101 , p=0.0003  , df_denom=249, df_num=1
ssr based chi2 test:   chi2=13.7741 , p=0.0002  , df=1
likelihood ratio test: chi2=13.4109 , p=0.0003  , df=1
parameter F test:         F=13.6101 , p=0.0003  , df_denom=249, df_num=1

Granger Causality
number of lags (no zero) 2
ssr based F test:         F=8.1187  , p=0.0004  , df_denom=246, df_num=2
ssr based chi2 test:   chi2=16.5673 , p=0.0003  , df=2
likelihood ratio test: chi2=16.0435 , p=0.0003  , df=2
parameter F test:         F=8.1187  , p=0.0004  , df_denom=246, df_num=2

Granger Causality
number of lags (no zero) 3
ssr based F test:         F=8.4721  , p=0.0001  , df_denom=243, df_num=3
ssr based chi2 test:   chi2=26.1484 , p=0.0000  , df=3
likelihood ratio test: chi2=24.8693 , p=0.0000  , df=3
parameter F test:         F=8.4721  , p=0.0000  , df_denom=243, df_num=3

Granger Causality
number of lags (no zero) 4
ssr based F test:         F=8.0162  , p=0.0000  , df_denom=240, df_num=4
ssr based chi2 test:   chi2=33.2671 , p=0.0000  , df=4
likelihood ratio test: chi2=31.2248 , p=0.0000  , df=4
parameter F test:         F=8.0162  , p=0.0000  , df_denom=240, df_num=4
```

I p-value sono minori del livello di confidenza del 5% per tutti e 4 i lags, ciò significa che informazioni passate del MktCap forniscono informazioni significative sull'andamento futuro del TVL.

```
# Testo la causalità del TVL sul MarketCap

tvl_mktcap_diff_invertito = tvl_mktcap_diff[['MktCap', 'TVL']] # Inverto l'ordine delle colonne
```

```
gc_test_invertito= grangercausalitytests(tvl_mktcap_diff_invertito, maxlag=max_lag, verbose=True
)

Granger Causality
number of lags (no zero) 1
ssr based F test:         F=1.1620  , p=0.2821  , df_denom=249, df_num=1
ssr based chi2 test:   chi2=1.1760  , p=0.2782  , df=1
likelihood ratio test: chi2=1.1732  , p=0.2787  , df=1
parameter F test:         F=1.1620  , p=0.2821  , df_denom=249, df_num=1

Granger Causality
number of lags (no zero) 2
ssr based F test:         F=1.6733  , p=0.1898  , df_denom=246, df_num=2
ssr based chi2 test:   chi2=3.4145  , p=0.1814  , df=2
likelihood ratio test: chi2=3.3915  , p=0.1835  , df=2
parameter F test:         F=1.6733  , p=0.1898  , df_denom=246, df_num=2

Granger Causality
number of lags (no zero) 3
ssr based F test:         F=2.5080  , p=0.1595  , df_denom=243, df_num=3
ssr based chi2 test:   chi2=7.7407  , p=0.1517  , df=3
likelihood ratio test: chi2=7.6233  , p=0.1545  , df=3
parameter F test:         F=2.5080  , p=0.1595  , df_denom=243, df_num=3

Granger Causality
number of lags (no zero) 4
ssr based F test:         F=3.5695  , p=0.0875  , df_denom=240, df_num=4
ssr based chi2 test:   chi2=14.8135 , p=0.0751  , df=4
likelihood ratio test: chi2=14.3896 , p=0.0762  , df=4
parameter F test:         F=3.5695  , p=0.0675  , df_denom=240, df_num=4
```

I p-value sono maggiori del livello di confidenza del 5% per tutti e 4 i lags, ciò significa che informazioni passate del TVL non forniscono informazioni significative sull'andamento futuro del MktCap

Codice paragrafo 4.3

```python
# Importo i dati e le librerie necessarie

import pandas as pd
import numpy as np
import matplotlib.pyplot as plt

tvl: pd.DataFrame = pd.read_excel("/Users/lorenzostagi/Desktop/DATI/tvldefi.xlsx")
tvl['Date'] = pd.to_datetime(tvl['Date'])
tvl.set_index('Date', inplace=True)
mktcap: pd.DataFrame = pd.read_excel("/Users/lorenzostagi/Desktop/DATI/mktdefi.xlsx")
mktcap['Date'] = pd.to_datetime(mktcap['Date'])
mktcap.set_index('Date', inplace=True)
mktcap['MktCap'] = mktcap['MktCap'] * 1e9 # Converto MktCap da miliardi a unità base
dati = tvl.merge(mktcap, left_index=True, right_index=True)

# Calcolo l'andamento del MarketCap/TVL ratio nel tempo

dati['MktCap/TVL ratio'] = dati['MktCap'] / dati['TVL']
print(dati)
```

```
                    TVL        MktCap  MktCap/TVL ratio
Date
2018-07-04  2.056829e+04  2.800200e+11      1.361416e+07
2018-07-11  2.072903e+04  2.610800e+11      1.259490e+07
2018-07-18  2.361935e+04  2.973300e+11      1.258840e+07
2018-07-25  2.054309e+04  3.082000e+11      1.500261e+07
2018-08-01  2.050041e+04  2.790600e+11      1.361241e+07
...                  ...           ...               ...
2023-04-19  5.246460e+10  1.269420e+12      2.419574e+01
2023-04-26  4.813422e+10  1.226270e+12      2.547605e+01
```

```
2023-05-03  4.758705e+10  1.247460e+12      2.621428e+01
2023-05-10  4.714914e+10  1.192890e+12      2.530036e+01
2023-05-17  4.654239e+10  1.185080e+12      2.546238e+01

[254 rows x 3 columns]

# Plotto tutta la serie storica

plt.figure(figsize=(14,7))
dati['MktCap/TVL ratio'].plot(color='blue', linewidth=1.5)
#plt.title('Serie storica MktCap/TVL ratio')
plt.ylabel('Dati in decine di milioni',fontsize=12)
plt.xlabel('')
plt.xticks(fontsize=13)
plt.yticks(fontsize=13)
plt.grid(True, which='both', linestyle='--', linewidth=1)
plt.close() # Impedisco la visualizzazione del grafico

# Plotto la serie storica del MktCap/TVL ratio da lug 2018 a gen 2019

dati_gen2019 = dati[dati.index < '2019-01-01']
plt.figure(figsize=(14,7))
dati_gen2019['MktCap/TVL ratio'].plot(color='blue', linewidth=1.5)
#plt.title('Serie storica del MktCap/TVL ratio (lug 2018 - gen 2019)')
plt.ylabel('Dati in decine di milioni', fontsize=13)
plt.xlabel('',fontsize=12)
plt.xticks(fontsize=12)
plt.yticks(fontsize=13)
plt.grid(True, which='both', linestyle='--', linewidth=0.5)
plt.close()

## Plotto la serie storica del MktCap/TVL ratio da gen 2019 a ott 2020

data_gen2019_ott2020 = dati[(dati.index >= '2019-01-03') & (dati.index <= '2020-10-31')]
plt.figure(figsize=(14,7))
data_gen2019_ott2020['MktCap/TVL ratio'].plot(color='blue', linewidth=1.5)
#ax.xaxis.set_major_formatter(mdates.DateFormatter('%b %Y'))
#plt.title('Serie storica del MktCap/TVL ratio (gen 2019 - ott 2020)')
plt.ylabel('')
plt.xlabel('')
plt.xticks(fontsize=12, rotation=45)  # ho aggiunto una rotazione per rendere le date più leggib
ili
plt.yticks(fontsize=13)
plt.grid(True, which='both', linestyle='--', linewidth=1)
plt.close()

# Plotto la serie storica del MktCap/TVL ratio da nov 2020 a giu 2023

dati_nov2020_giu2023 = dati[dati.index >= '2020-07-30']
plt.figure(figsize=(14,7))
dati_nov2020_giu2023['MktCap/TVL ratio'].plot(color='blue', linewidth=1.5)
#plt.title('Serie storica del MktCap/TVL ratio (nov 2020 - giu 2023)'
plt.ylabel('')
plt.xlabel('')
plt.xticks(fontsize=12)
plt.yticks(fontsize=13)
plt.grid(True, which='both', linestyle='--', linewidth=0.5)
plt.close()
```

Codice paragrafo 4.4

```
# Carico i dati e le librerie necessarie

import pandas as pd
import matplotlib.pyplot as plt
import matplotlib.dates as mdates
```

```
loans_upto1 = pd.read_excel("/Users/lorenzostagi/Desktop/DATI/loans_to1.xlsx")
loans_upto1.set_index('DATE', inplace=True)

deposit_upto1 = pd.read_excel("/Users/lorenzostagi/Desktop/DATI/deposit_to1.xlsx")
deposit_upto1.set_index('DATE', inplace=True)

loans_over1 = pd.read_excel("/Users/lorenzostagi/Desktop/DATI/loans_1to5.xlsx")
loans_over1.set_index('DATE', inplace=True)

deposit_over1 = pd.read_excel("/Users/lorenzostagi/Desktop/DATI/deposit_over1y.xlsx")
deposit_over1.set_index('DATE', inplace=True)

tassi_euro = pd.concat([loans_upto1, deposit_upto1,loans_over1, deposit_over1], axis=1)
tassi_euro = tassi_euro['2021-07-31':'2023-07-31']

tassi_euro.index = pd.to_datetime(tassi_euro.index)

aave_apy = pd.read_excel("/Users/lorenzostagi/Desktop/DATI/aave_apy.xlsx")
aave_apy['DATE'] = pd.to_datetime(aave_apy['DATE'])
aave_apy.set_index('DATE', inplace=True)
aave_apy = aave_apy[aave_apy['token'] == 'USDC'] # Filtro per il token USD coin
aave_apy.index = aave_apy.index.tz_localize(None) # Converto le date nello stesso formato dei ta
ssi eurozona
aave_apy = aave_apy.resample('M').mean() # Resample la serie in mensile
aave_apy = aave_apy['2021-07-31':'2023-07-31'] # Filtro le date che mi interessano

comp_apy = pd.read_excel("/Users/lorenzostagi/Desktop/DATI/Compound_apy.xlsx")
comp_apy.set_index('DATE', inplace=True)
comp_apy.index = pd.to_datetime(comp_apy.index)
comp_apy = comp_apy.sort_index(ascending=True)
comp_apy = comp_apy['2021-07-31':'2023-07-31']

# Calcolo gli spread dell'eurozona

spread_euro_upto1 = loans_upto1['loans_upto1'] - deposit_upto1['deposit_upto1']
spread_euro_over1 = loans_over1['loans_over1'] - deposit_over1['deposit_over1y']

spread_euro = pd.DataFrame({
    'Up to 1 year spread Europe': spread_euro_upto1,
    'Over 1 year spread Europe': spread_euro_over1
})
spread_euro = spread_euro.loc['2021-07-31':'2023-07-31']
spread_euro.index = pd.to_datetime(spread_euro.index)

# Calcolo gli spread DeFi

spread_comp = comp_apy['compound_borrow_apy'] - comp_apy['compound_supply_apy']
spread_aave = aave_apy['aave_borrow_apy'] - aave_apy['aave_deposit_apy']

spread_defi = pd.DataFrame({
    'Spread Aave': spread_aave,
    #'stable_spread_aave': spread_defi_stable,
    'Spread Compound': spread_comp
})
spread_defi.index = pd.to_datetime(spread_defi.index)

spreads = pd.concat([spread_defi, spread_euro], axis=1)
spreads.index = pd.to_datetime(spreads.index)
spreads = spreads.loc['2021-07-31':'2023-07-31']

# Plotto i tassi sui depositi

fig = plt.subplots(figsize=(10, 6))
tassi_euro['deposit_upto1'].plot(label='Eurozone up to 1 year', color='blue', marker='.')
tassi_euro['deposit_over1y'].plot(label='Eurozone over 1 year', color='deepskyblue', marker='.')
comp_apy['compound_supply_apy'].plot(label='Compound', color='orange', marker='.')
aave_apy['aave_deposit_apy'].plot(label='Aave', color='red', marker='.')
plt.title("Confronto tassi sui depositi", fontsize=12, fontweight='bold')
plt.ylabel("%")
plt.xlabel('')
plt.legend()
```

```
plt.grid(True, which='both')
#plt.show()
plt.close()

# Plotto i tassi sui prestiti

fig = plt.subplots(figsize=(10, 6))
tassi_euro['loans_upto1'].plot(label='Eurozone up to 1 year', color='blue', marker='.')
tassi_euro['loans_over1'].plot(label='Eurozone over 1 year', color='deepskyblue', marker='.')
comp_apy['compound_borrow_apy'].plot(label='Compound', color='orange', marker='.')
aave_apy['aave_borrow_apy'].plot(label='Aave', color='red', marker='.')
plt.title("Confronto tassi sui depositi", fontsize=12, fontweight='bold')
plt.ylabel("%")
plt.xlabel('')
plt.legend()
plt.grid(True, which='both')
#plt.show()
plt.close()

# Plotto gli spreads

plt.figure(figsize=(14, 8))
spreads['Spread Aave'].plot(label='Aave', color='red', marker='.')
spreads['Spread Compound'].plot(label='Compound', color='orange', marker='.')
spreads['Up to 1 year spread Europe'].plot(label='Eurozone up to 1 year', color='deepskyblue', m
arker='.')
spreads['Over 1 year spread Europe'].plot(label='Eurozone over 1 year', color='blue', marker='.'
)
plt.title('Confronto spread: DeFi vs TradFi (pool USDC)', fontsize=16, fontweight='bold')
plt.xlabel('')
plt.ylabel('%')
plt.legend()
plt.grid(True, which='both')
#plt.show()
plt.close()
```

CONCLUSIONI

Nel corso degli ultimi 50 anni il mondo della finanza ha vissuto molte "prime volte", segnando un'evoluzione costante e significativa del sistema economico. Dalla nascita delle prime monete fiat, alla digitalizzazione dei servizi bancari, fino all'avvento delle criptovalute, ogni tappa di questo percorso ha contribuito a plasmare la situazione finanziaria attuale. Il futuro si chiama DeFi, una promessa rivoluzionaria che ridisegnando il modo in cui interagiamo con il nostro denaro offre notevoli vantaggi rispetto alla finanza tradizionale sotto gli aspetti di decentralizzazione, accessibilità, efficienza e interoperabilità.

La finanza tradizionale mostra aspetti di inefficienza che penalizzano il consumatore medio, mentre la DeFi, per merito della sua automazione contrattuale, gli consente di utilizzare al meglio le soluzioni che offre. La decentralizzazione permette ai prodotti finanziari di essere di proprietà collettiva della comunità, senza un controllo dall'alto verso il basso, e garantire l'accesso a questi nuovi servizi a tutte le persone è di fondamentale importanza per prevenire un aumento del divario di ricchezza.

Nel corso di questa tesi abbiamo esplorato una vasta gamma di servizi finanziari, tra cui prestiti, depositi, scambi, obbligazioni e derivati. Il concetto di ancoraggio con monete reali, come USDC o DAI, è cruciale per la DeFi. Se si potesse stabilire una solida e affidabile correlazione di queste stablecoin a valute tradizionali, allora la porta sarebbe spalancata per emulare e trasferire la maggior parte dei servizi finanziari tradizionali in questo nuovo sistema. Mentre la tecnologica progredisce e il mondo si adatta, emergeranno nuovi e altri servizi, ampliando ulteriormente le potenzialità e le opportunità in questo settore in rapida crescita.

Inoltre la DeFi, tramite i token di governance, può persino distribuire direttamente valore agli utenti per incentivarne la crescita. In pratica, non si tratta solo di fornire servizi finanziari in modo decentralizzato, ma anche di ricompensare gli utenti per la loro fiducia e partecipazione, accelerando così la crescita e l'adozione su larga scala di queste piattaforme. Questo modello economico, in cui gli utenti sono sia consumatori che beneficiari diretti dei profitti generati, rappresenta un netto distacco dai sistemi finanziari tradizionali e potrebbe ridefinire le aspettative sulla distribuzione del valore nel settore finanziario. Grazie all'infrastruttura condivisa e alle sue interfacce, la DeFi permette una

radicale interoperabilità che supera di gran lunga ciò che il tradizionale sistema finanziario può offrire. Questa capacità di integrare e interagire con vari protocolli e piattaforme consente una fluidità e una flessibilità senza precedenti nelle transazioni e negli scambi, abbattendo le barriere che una volta limitavano l'interazione tra differenti servizi e prodotti finanziari.

Rischi come la scalabilità e le vulnerabilità degli smart contract affliggono tutta la DeFi e superarli sarà fondamentale per il raggiungimento dell'adozione di massa, altrimenti i benefici di questa rivoluzione saranno limitati solo ai soggetti più ricchi se la tecnologia sottostante non può servire l'intera popolazione. Inevitabilmente, superare tali sfide potrebbe compromettere alcuni dei vantaggi intrinseci alla DeFi, come una minore interoperabilità su una blockchain "spezzettata" (*sharded*). Similmente ad Internet e ad altre tecnologie dirompenti, i benefici e la portata miglioreranno nel tempo, tuttavia lo smart contract risk non verrà mai eliminato del tutto, ma la capacità degli sviluppatori e programmatori derivata dall'esperienza riuscirà a mitigare tali ostacoli.

Se la futura regolamentazione nel settore DeFi sarà concepita e attuata in maniera equilibrata, tenendo conto delle esigenze di questo ecosistema, e se gli investitori istituzionali entreranno nel settore con una visione costruttiva e collaborativa, allora ci troveremo di fronte a una vera e propria rivoluzione del settore finanziario. Presumendo che la DeFi si realizzi completamente, le società finanziarie che non saranno in grado di adattarvisi potrebbero rimanere indietro. Man mano che l'ambiente normativo diventerà più chiaro e i rischi saranno meglio affrontati, queste aziende dovrebbero iniziare a integrare i loro servizi con la blockchain e la DeFi e quelle che integreranno la tecnologia e sosterranno la regolamentazione locale con successo emergeranno come vincitori.

La convergenza tra l'innovazione decentralizzata e gli attori tradizionali potrebbe dare luogo a un sistema finanziario più inclusivo, efficiente e resiliente. Tuttavia, è fondamentale che questa evoluzione avvenga salvaguardando sia le libertà e le promesse della DeFi, sia le necessità di protezione e sicurezza degli investitori.

Da quella fatidica estate del 2020 sono passati tre anni e la tecnologia e l'adozione delle dApp, accompagnata da nuovi rischi e sfide, non ha mai smesso di crescere. Sarà fondamentale osservare come il settore si svilupperà e si adatterà nel tempo per realizzare pienamente la promessa di una rivoluzione decentralizzata, in cui il potere e il controllo

finanziario vengono restituiti nelle mani degli individui, ridefinendo il modo in cui concepiamo e interagiamo con il mondo finanziario.

BIBLIOGRAFIA

Abdulhakeem, S. A., & Hu, Q. L. "Powered by Blockchain Technology, DeFi (Decentralized Finance) Strives to Increase Financial Inclusion of the Unbanked by Reshaping the World Financial System." *Modern Economy* 12 (2021): 1-16.

Capriglione, F., & Semeraro, G. *Manuale di diritto bancario e finanziario*. Giuffrè, 2019.

Chetty, R., Hendren, N., Kline, P., e Saez, E. "Where is the Land of Opportunity? The Geography of Intergenerational Mobility in the United States." *National Bureau of Economic Research* (2014).

Chiap, G., Ranalli, J., & Bianchi, R. *Blockchain: Tecnologia e applicazioni per il business*. Hoepli, 2019.

Collina E., Liberati D., Maddaloni P., *Handbook on the data published by the Bank of Italy, "Bank interest rates"*, Bank of Italy, 3 Marzo 2023.

Corbae, D., D'Erasmo, P. "Rising bank concentration." *National Bureau of Economic Research* (2020).

Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*. Washington DC: World Bank, 2018.

Di Orio, G., Brito, G., Maló, P. "Semantic Interoperability Framework for Digital Finance Applications." In: Soldatos, J., Kyriazis, D. (eds) *Big Data and Artificial Intelligence in Digital Finance*. Springer, Cham, 2022.

Dirk Andreas Zetzsche, Douglas W. Arner, & Ross P. Buckley. "Decentralized Finance (DeFi)." *Journal of Financial Regulation* 6 (2020): 172–203.

eHealth Governance Initiative. *Discussion Paper on Semantic and Technical Interoperability*, 2012.

Felsenthal, M., & Hahn, R. "Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows." 2018.

Harvey, C.R., Ramachandran, A., & Santoro, J. DeFi and the Future of Finance. Wiley, 2021.

Hicks, J. *A Contribution to the Theory of the Trade Cycle*. Oxford: Clarendon Press, 1950.

Mell, Peter & Grance, Timothy. "The NIST Definition of Cloud Computing." *National Institute of Standards and Technology*, 2011.

Ratha, D., Plaza, S., Kim, E.J., Chandra, V., Kurasha, N., and Pradhan, B. *Migration and Development Brief 38: Remittances Remain Resilient But Are Slowing*. KNOMAD–World Bank, Washington, DC, 2023.

Schär, F. "Decentralized Finance: On Blockchain and Smart Contract based Financial Markets." Center for Innovative Finance, University of Basel, 8 marzo 2020.

Shiller, Robert J. 1993. "Measuring Asset Values for Cash Settlement in Derivative Markets: Hedonic Repeated Measures Indices and Perpetual Futures." *The Journal of Finance* 48 (3).

SITOGRAFIA

Aave. “Credit Delegation”. https://docs.aave.com/developers/guides/credit-delegation.

Aquaro, D. "Smart Contract: Cosa sono e come funzionano le clausole blockchain." Il Sole 24 Ore, 2019. https://www.ilsole24ore.com/art/smart-contract-cosa-sono-e-come-funzionano-clausole-blockchain-ACsDo2P.

Banca d'Italia. "Avvertenza sulle valute virtuali," 2015. https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/index.html.

Banca d'Italia. L’Unione Bancaria. https://www.bancaditalia.it/compiti/vigilanza/unione-europea/index.html.

BCE. "Payments statistics: 2021." 2021. https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2021~956efe1ee6.en.html.

Binance Academy. "Impermanent Loss Explained." https://academy.binance.com/it/articles/impermanent-loss-explained.

Bit2Me. 2022. "Cos'è il lock-up e il vesting?." https://support.bit2me.com/it/support/solutions/articles/35000194500-cos-è-il-lock-up-e-il-vesting-.

Borsa Italiana. "Differenza tra token fungibili e token non fungibili." https://www.borsaitaliana.it/notizie/sotto-la-lente/differenza-tra-token-fungibili-e-token-non-fungibili.htm.

BrightNode. "La storia del progetto MakerDAO." BrightNode, 2021. https://brightnode.io/it/la-storia-del-progetto-makerdao/.

Bruce Scheneir. "There's no good reason to trust blockchain technology." *Wired*, 2019. https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/.

Cervi, C. "Ethereum passa al proof-of-stake: dopo lo stop al mining, cosa cambia?" *Money.it*, 2023. https://www.money.it/ethereum-passa-al-proof-of-stake-dopo-stop-al-mining-cosa-cambia.

Cheng, Evelyn. 2018. "Japanese cryptocurrency exchange loses more than $500 million to hackers." *CNBC*, 26 Gennaio. https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html.

CoinMarketCap, Global Cryptocurrency Chart – Total Cryptocurrency Market Cap, https://coinmarketcap.com/charts/. Consultato il 5 settembre 2023.

Compound. “Distribute COMP to Users”. 15 Giugno 2020. https://compound.finance/governance/proposals/7.

Compound. "Governance." https://docs.compound.finance/v2/governance/.

Compound. "Whitepaper." 2019. https://compound.finance/documents/Compound.Whitepaper.pdf.

CONSOB. "Criptovalute." https://www.consob.it/web/investor-education/criptovalute.

CONSOB. "Dal baratto alla finanza." https://www.consob.it/web/investor-education/dal-baratto-alla-finanza.

Crabb, Jon. 2022 “DeFi Design Tips: Volume One." Medium. https://medium.com/@JonCrabb/defi-design-tips-volume-one-6507512f9c98.

Curve, https://dao.curve.fi.

Dargahwala, T., & Riedl, E. "How interoperability can solve and scale financial inclusion." Mastercard, 2021. https://www.mastercard.com/news/media/vrhj0cxo/how-interoperability-can-solve-and-scale-financial-inclusion.pdf.

DeFi Llama, All protocols, https://defillama.com. Consultato il 3 settembre 2023.

DeFiLlama, Stablecoin Market Cap. https://defillama.com/stablecoins. Consultato il 20 luglio 2023.

Dexilon, 2022, “Problem of Scaling DeFi”. https://dexilon.io/company-and-product/problems-of-scaling-defi/.

Duggan, Wayne. 2023. "Che cos’è Ethereum 2.0? Ecco spiegato il Merge." Forbes, 18 febbraio. https://www.forbes.com/advisor/it/investire/criptovalute/merge-ethereum/.

Dune, “Aave-v2-Ethereum Deposit & Borrow APY”. Disponibile su: https://dune.com/queries/580512/1090585. Consultato il 4 settembre 2023.

Dune, Defi users over time, https://dune.com/rchen8/defi-users-over-time.

Dune, “USDC Interest Rate on Compound”. Disponibile su: https://dune.com/queries/1009795/1745172. Consultato il 4 settembre 2023.

dYdX. “A Standard for decentralized Margin Trading and Derivatives”, 2017. https://whitepaper.dydx.exchange.

Federal Deposit Insurance Corporation. "Deposit insurance at a glance." https://www.fdic.gov/resources/deposit-insurance/brochures/documents/deposit-insurance-at-a-glance-english.pdf.

Focus.it. "Quando è stata inventata la moneta?" 2022. https://www.focus.it/cultura/storia/quando-e-stata-inventata-la-moneta.

Forbes Advisor. "Interchange fees: How they work and affect credit card rewards." 2022. https://www.forbes.com/advisor/business/interchange-fees/.

Forbes. "Best Online Banks Of 2023." 2023. https://www.forbes.com/advisor/banking/best-online-banks/.

Garavaglia, Roberto. 2023. "Cripto-asset: MiCAR approvato dal Parlamento europeo." PagamentiDigitali.it, 20 aprile. https://www.pagamentidigitali.it/esperti-e-analisti/cripto-asset-micar-approvato-dal-parlamento-europeo/#MiCA_e_DeFi.

Geeksforgeeks. "Reentrancy Attack in Smart Contracts." https://www.geeksforgeeks.org/reentrancy-attack-in-smart-contracts/.

Gennai, Andrea. "Derivati, la montagna sale a 620mila miliardi (e supera il pre Lehman)." Il Sole 24 Ore, 18 dicembre 2022. https://www.ilsole24ore.com/art/derivati-montagna-sale-620mila-miliardi-e-supera-pre-lehman-AEL7eqPC.

Gillis, A.S. & Bernsteiun, C. "Blockchain dApp (decentralized application)." TechTarget. 2022. https://www.techtarget.com/iotagenda/definition/blockchain-dApp.

Ethereum.org. "Gas e commissioni." Ultima modifica 10 luglio 2023. https://ethereum.org/it/developers/docs/gas/.

Ethereum.org. "Oracles." Ultima modifica 17 luglio 2023. https://ethereum.org/it/developers/docs/oracles/.

European Central Bank, "Bank interest rates - deposits from households with an agreed maturity of over one year (new business) - euro area." https://data.ecb.europa.eu/data/datasets/MIR/MIR.M.U2.B.L22.K.R.A.2250.EUR.N.

European Central Bank, "Bank interest rates - deposits from households with an agreed maturity of up to one year (new business) - euro area." https://data.ecb.europa.eu/data/datasets/MIR/MIR.M.U2.B.L22.F.R.A.2250.EUR.N.

European Central Bank, "Bank interest rates - loans to households for consumption & other purposes with an original maturity of up to one year - euro area." https://data.ecb.europa.eu/data/datasets/MIR/MIR.M.U2.B.A25.F.R.A.2250.EUR.O.

European Central Bank, "Bank interest rates - loans to households for consumption & other purposes with an original maturity of over one & up to five years - euro area." https://data.ecb.europa.eu/data/datasets/MIR/MIR.M.U2.B.A25.I.R.A.2250.EUR.O.

European Central Bank. "Guideline of the European Central Bank of 1 August 2007 on monetary, financial institutions and markets statistics (recast)." Official Journal of the European Union No L 341, 27 Dicembre 2007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:341:0001:0232:EN:PDF.

Kehl, F. "Credit card processing fees: how much will they cost your business & how can you lower them?" 2023. https://www.merchantmaverick.com/the-complete-guide-to-credit-card-processing-rates-and-fees/.

King, N. "The App Connecting the GCC's Low Paid Workers with Bank Accounts." 2017. https://gulfbusiness.com/the-app-connecting-the-gccs-low-paid-workers-with-bank-accounts/.

MakerDAO. "Chiusura di Emergenza." Whitepaper, 2020. https://makerdao.com/it/whitepaper/#chiusura-di-emergenza.

MakerDAO. "Governance del Protocollo Maker." Whitepaper, 2020. https://makerdao.com/it/whitepaper/#governance-del-protocollo-maker.

MakerDAO. "Il Protocollo Maker." Whitepaper, 2020. https://makerdao.com/it/whitepaper/#il-protocollo-maker.

Martin, Mike. "TVL vs Market Cap vs TVL Ratio: Crypto Metrics Explained." TastyCrypto, 2023. https://www.tastycrypto.com/blog/tvl-vs-market-cap/.

Medium. 2021. "Exploiting a Smart Contract without Security Vulnerabilities: Analysis of True Seigniorage Dollar Attack Event." 17 Marzo. https://certik.medium.com/exploiting-a-smart-contract-without-security-vulnerabilities-analysis-of-true-seigniorage-dollar-c319dce45783.

Nexus Mutual. https://nexusmutual.io.

Pereira, Ana Paula. "Factory pool di Curve Finance exploitate per oltre 47 milioni di dollari a causa di una reentrancy vulnerability." Cointelegraph Italia, 31 luglio 2023. https://it.cointelegraph.com/news/curve-finance-pools-exploited-over-24-reentrancy-vulnerability.

Porcelli, Andrea. "Il Total Value Locked (TVL) nel mondo delle crypto: una panoramica sul 2023." Cryptonomist, 24 giugno 2023, https://cryptonomist.ch/2023/06/24/tvl-mondo-crypto-panoramica-2023/.

Portal Cripto. “Che cos’è l’indicatore TVL DeFi?”. 28 settembre 2021. https://portalcripto.com.br/it/o-que-e-tvl-indicador-defi/.

Portale, V. & Fracassi, J. "Dentro la rivoluzione: la finanza DeFi e i nuovi business model." Il Sole 24 Ore. 10 dicembre 2021. https://www.ilsole24ore.com/art/dentro-rivoluzione-finanza-defi-e-nuovi-business-model-AEb27ZUB.

PricewaterhouseCoopers. "DeFi: Defining the future of finance." PwC Switzerland. https://www.pwc.ch/en/insights/digital/defi-defining-the-future-of-finance.html.

Raiffeisen.it. "Quando e dove è stato inventato il denaro?" https://www.raiffeisen.it/it/sapere-finanziario/dettaglio/quando-e-dove-e-stato-inventato-il-denaro.html.

Rooney, K. "Plaid valuation tops $13 billion in first funding after a scrapped $5.3 billion merger with Visa." CNBC, 2021. https://www.cnbc.com/2021/04/07/plaid-hits-13point4-billion-valuation-in-the-wake-of-scrapped-visa-deal.html.

Roose, K. "What Are DAOs?" The New York Times. 18 marzo 2022. https://www.nytimes.com/interactive/2022/03/18/technology/what-are-daos.html.

Sergeenkov, Andrey. 2021 "What Is Smart Contract Risk?" Crypto Basics; https://coinmarketcap.com/alexandria/article/what-is-smart-contract-risk.

Stadelmann, Kadan. 2023. "I legislatori puntano ora a una regolamentazione dedicata alla DeFi." Cryptonomist, 9 aprile. https://cryptonomist.ch/2023/04/09/i-legislatori-regolamentazione-dedicata-alla-defi/.

Sveriges Riksbank. "History." n.d. https://www.riksbank.se/en-gb/about-the-riksbank/history/.

Synthetix. “Litepaper”, 2023. https://docs.synthetix.io/synthetix-protocol/the-synthetix-protocol/synthetix-litepaper.

Techopedia. "Legacy system definition." https://www.techopedia.com/definition/6815/legacy-system.

The World bank. "Personal remittances received (% of GDP)." 2022. https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS.

Trabucchi, M. "Con la prima DAO riconosciuta in Italia si sperimenta l'azienda decentralizzata." Il Sole 24 Ore, 11 ottobre 2022. https://www.ilsole24ore.com/art/con-prima-dao-riconosciuta-italia-si-sperimenta-l-azienda-decentralizzata-AEXVnU7B.

Treccani. "banca." http://www.treccani.it/enciclopedia/banca.

Treccani, "Legge di Moore," *Enciclopedia della Scienza e della Tecnica*, 2008. https://www.treccani.it/enciclopedia/legge-di-moore_(enciclopedia-della-scienza-e-della-tecnica)/.

Treccani. "SAN GIORGIO, banco di." n.d. https://www.treccani.it/enciclopedia/san-giorgio-banco-di_%28Enciclopedia-Italiana%29/.

UBS. "The history of the credit card." 2019. https://www.ubs.com/ch/it/private/accounts-and-cards/information/magazine/2019/the-history-of-the-credit-card.html.

Uniswap. “Introducing Uniswap v3”, 2021. https://blog.uniswap.org/uniswap-v3.

Uniswap. "Uniswap V3 Core." 2021. https://uniswap.org/whitepaper-v3.pdf.

"Yield Farming," Google Trends, https://trends.google.it/trends/explore?date=today%205-y&q=yield%20farming&hl=it.

Yield Protocol. “Introduction”. https://docs.yieldprotocol.com/#/.