LUISS

Dipartimento di Impresa e Management

Cattedra di Economia Monetaria e Creditizia

DeFi: fondamenti, rischi e opportunità della finanza decentralizzata

Prof. Stefano Marzioni
RELATORE

Paolo Finili (matr. 229201)
CANDIDATO

Anno Accademico 2020/2021

INDICE

Introduzione

Stiamo vivendo un periodo difficile, di grande crisi e di forte incertezza. Il Covid ha stravolto le vite di tutti noi, mettendo a dura prova la nostra esistenza. La pandemia ha portato numerosi cambiamenti e nuove abitudini, che ci hanno costretto a rivalutare i progetti futuri e a modificare la nostra quotidianità. L'impossibilità di proiettarsi nel futuro e la rivoluzione delle routine e della realtà a cui eravamo abituati hanno provocato un senso di smarrimento che ha fatto vacillare le nostre certezze. Questo morboso desiderio di tornare alla normalità è un sintomo inequivocabile dell'impatto psicosociale del Coronavirus. Tuttavia, come diceva Einstein, la crisi porta progresso ed è nella crisi che sorgono l'inventiva, le scoperte e le grandi strategie. Ed è proprio in questo contesto che nasce la DeFi, la finanza decentralizzata.

Dopo la paura e la sfiducia iniziale che hanno portato gli investitori e i risparmiatori ad orientarsi verso beni rifugio, la successiva ripresa dei mercati ha spinto gli operatori a cercare rendimenti più elevati. La DeFi offre delle soluzioni innovative che hanno ottenuto un grande successo, come testimoniato dalla crescita esponenziale che ha avuto la DeFi in breve tempo. L'idea di una finanza decentralizzata in grado di ricreare i prodotti e i servizi della finanza tradizionale, ma senza l'intervento di intermediari e autorità, ha attirato numerosi investitori. Le opportunità della DeFi hanno suscitato l'interesse di molti ricercatori e imprenditori, che vedono nella DeFi delle potenzialità straordinarie. Si tratta di un affascinante connubio tra finanza e tecnologia che è soltanto nella sua fase iniziale, ma mostra già delle soluzioni significative, come ad esempio la possibilità per gli utenti di creare e vendere prodotti finanziari, oppure usufruire di servizi finanziari personalizzati totalmente diversi da quelli attualmente esistenti.

Dopo aver raccolto il materiale necessario per approfondire l'argomento, ho illustrato i principali rischi e opportunità della DeFi. Chiaramente, trattandosi di una realtà appena nata, bisogna sempre tener presente che è un ambiente in continua evoluzione, di conseguenza è ancora fortemente suscettibile agli stimoli esterni.

Nel primo capitolo si cerca di definire la DeFi, facendo chiarezza sul significato della decentralizzazione. Successivamente si analizza come funziona la DeFi, descrivendo la tecnologia blockchain che ne è alla base e che costituisce il pilastro fondamentale su cui è costruita la DeFi.

Il secondo capitolo mostra come sia concretamente possibile una finanza senza intermediari e senza autorità. Nello specifico si descrive il meccanismo attraverso il quale si raggiunge un accordo in una realtà decentralizzata, in cui sembra impossibile creare i presupposti necessari per instaurare un rapporto di fiducia indispensabile per la finanza. Nella fattispecie vedremo il ruolo svolto dagli smart contract in questo contesto.

Il terzo capitolo entra nel cuore della DeFi, analizzandone la struttura e le principali applicazioni pratiche più interessanti. In particolare, presenteremo opportunità e rischi delle varie piattaforme DeFi, illustrando i protocolli più validi e innovativi del settore.

Nel quarto ed ultimo capitolo affronteremo l'impatto del Covid sulla DeFi e la differenza tra il crollo del mercato di marzo 2020 e la recente crisi delle criptovalute di maggio 2021. Infine, concluderemo con una proiezione dei possibili scenari futuri alla luce degli sviluppi recenti, provando a prevedere le principali sfide che attendono la DeFi, sulla base degli attuali rischi e opportunità.

1. Che cos'è la finanza decentralizzata, come funziona e quali sono i suoi obiettivi

Immaginate di poter aprire un mutuo senza dover andare in banca, di scambiare criptoasset senza dover affidarsi a un broker, oppure di stipulare un contratto di assicurazione senza dover rivolgersi a una compagnia assicurativa. Se tutto ciò poteva sembrare soltanto un'utopia fino a qualche anno fa, oggi sta diventando una realtà concreta, quella della finanza decentralizzata (DeFi). Come spesso accade per le discipline emergenti, non esiste ancora una definizione ufficiale, universalmente riconosciuta. Secondo Forbes, la DeFi è un movimento che consente di ricreare nel mondo delle criptovalute tutti gli strumenti della finanza tradizionale in una architettura decentralizzata, posta cioè al di fuori del controllo di banche, imprese e istituzioni. DeFi pulse, sito che monitora e analizza i protocolli e i progetti DeFi, dà una definizione più tecnica, affermando che con il termine DeFi ci si riferisce all'insieme di asset digitali, smart contract finanziari, protocolli e app decentralizzate (DApps) costruiti su Blockchain. Fabian Schär, direttore del centro di finanza innovativa dell'Università di Basilea, in un articolo per la Federal Reserve Bank di Saint Louis, definisce la DeFi in maniera molto ficcante e concisa, come "un'infrastruttura finanziaria alternativa costruita su blockchain".

Alla luce di ciò, proviamo a ricavare una definizione sintetica partendo innanzitutto dai singoli termini: "finanza", "decentralizzata". La parola "finanza" deriva dal latino *finis* "fine, conclusione", da cui a sua volta proviene il termine medievale "finantia", che assumeva il duplice significato di "quietanza finale" e "definizione amichevole di una controversia". Successivamente, con il francese "finance", la parola ha preso il significato di "prestazione pecuniaria", "denaro contante", per poi essere utilizzata come sinonimo per definire gli affari in senso lato. Oggi la finanza è la disciplina che studia i processi con cui individui, imprese e istituzioni gestiscono i flussi monetari, quindi l'allocazione di denaro in base alle scelte di investimento e finanziamento. È l'aggettivo "decentralizzata" che attribuisce alla finanza una connotazione totalmente innovativa. Ma cosa significa effettivamente "decentralizzata" o "decentralizzazione"? Possiamo subito anticipare che non c'è una definizione chiara e univoca di questo termine. Lo stesso Vitalik Buterin fondatore di Ethereum, piattaforma decentralizzata per eccellenza, ha riscontrato questo problema, sostenendo che è probabilmente una delle parole definite in maniera peggiore. In effetti basterebbe una rapida ricerca per comprendere quanta confusione ci sia attorno a questa parola. Tony Sheng in un suo articolo sostiene che dovremmo addirittura "abolire" il termine, per farci capire come sia spesso utilizzato in modo improprio, ambiguo e fuorviante. Ciò è dovuto principalmente al fatto che il concetto di decentralizzazione è strettamente legato alla tecnologia blockchain su cui è incentrata la DeFi. Serve una profonda conoscenza della blockchain per poter comprendere il significato della decentralizzazione. Per il momento occorre solamente sapere che questa nuova forma di finanza non si basa più sugli intermediari finanziari, come broker, exchange o banche, bensì su blockchain. L'utilizzo di questa infrastruttura consente di replicare i principali servizi

finanziari (trading, borrowing, lending…) e strumenti finanziari (azioni, obbligazioni, derivati…) in maniera decentralizzata e immediata, ovvero senza il necessario intervento di intermediari o altre istituzioni.

1.1 DeFi VS finanza tradizionale

Nel mondo della finanza tradizionale esistono una serie di intermediari che svolgono un ruolo cruciale per il corretto funzionamento dei mercati finanziari. Gli intermediari finanziari, infatti, rendono possibile l'incontro tra domanda e offerta di risorse finanziarie, mettendo in comunicazione tra loro individui, imprese e istituzioni. Per questo motivo compiono una funzione rilevante nel ridurre i costi di transazione ed aumentare le probabilità di finalizzare tali transazioni. Spesso nelle transazioni economiche, gli intermediari aiutano le parti non soltanto a stabilire una connessione, ma anche ad instaurare un rapporto di fiducia, mediare durante la fase di negoziazione, cercare di trovare un accordo e farlo rispettare (Bellavitis, Chen, 2020). Tuttavia questi benefici derivanti dai servizi offerti dagli intermediari, attribuiscono a questi ultimi un potere tale da consentire loro di influenzare le transazioni per massimizzare i propri interessi (Cohen, 2019; Srnicek, 2017; Zuboff, 2019). Questo conflitto tra il bisogno di transazioni efficienti e la massimizzazione dell'utilità degli intermediari è particolarmente accentuato nei sistemi finanziari in cui le transazioni sono regolate da grandi istituzioni finanziarie.

Per comprendere meglio questo aspetto occorre capire in che modo gli istituti finanziari gestiscono le transazioni. Come spiegato nell'articolo di D.Zetsche, D.Arner e R.Buckley "Decentralized Finance (DeFi)", pubblicato sul *Journal of financial regulation*, nella finanza tradizionale la gestione delle transazioni avviene in maniera centralizzata. Quando i clienti effettuano un accesso locale a dei servizi come pagamenti, bancomat, risparmi, investimenti e assicurazione, questi servizi non sono forniti al punto di accesso. Piuttosto, le attività e i mercati finanziari si raggruppano tradizionalmente in punti di accesso locali, regionali e super-regionali/globali, detti "hubs". Questi servizi sono in sostanza forniti da un centro finanziario dove una sufficiente concentrazione di volumi e numeri di transazioni in un dato settore o servizio permette lo sviluppo di competenze e risorse. In base al settore o servizio in questione, le transazioni richieste vengono processate a livello locale, regionale o globale. Supponiamo ad esempio di voler effettuare un semplice bonifico internazionale per inviare 100 Euro dall'Italia agli Stati Uniti. Abbiamo un conto corrente bancario presso Intesa Sanpaolo, mentre il nostro beneficiario è correntista presso Bank of America. Per eseguire questo trasferimento, la banca italiana invierà una telecomunicazione SWIFT alla banca americana. SWIFT è un network che consente agli istituti finanziari di scambiarsi messaggi e inviare informazioni in maniera sicura e standardizzata. Una volta ricevuta questa richiesta di accredito, Bank of America provvederà a sottrarre 100 Euro dal conto che Intesa Sanpaolo ha presso Bank of America e li aggiungerà al conto corrente del beneficiario. Affinché questo meccanismo funzioni nella maniera più snella possibile, è necessario che ogni banca abbia dei conti correnti presso le principali banche estere. Nel caso in cui, invece, la banca dell'ordinante non abbia un conto corrente presso la banca del beneficiario, è

necessario l'intervento di un'altra banca, la banca intermediaria. Quest'ultima ha degli accordi bilaterali con entrambe le banche coinvolte, di conseguenza è in grado di fare da intermediario tra le due banche per portare a termine la transazione. Tornando al nostro esempio, qualora Intesa Sanpaolo non dovesse possedere un conto presso Bank of America, dovrebbe chiedere aiuto ad una terza banca, ipotizziamo Bnp Paribas, che, invece, dispone di un conto presso entrambe le banche. Bnp Paribas sottrae 100 Euro dal conto di Intesa Sanpaolo e li aggiunge su quello di Bank of America, che li accredita sul conto del beneficiario.

In questo viaggio finanziario si possono riscontrare diverse inefficienze in termini di tempo, rischi e costi di transazione. Infatti, l'esecuzione non è immediata, ma può richiedere del tempo: in media un bonifico SWIFT può impiegare dai 3 ai 7 giorni lavorativi. Nella fattispecie, però, un'inchiesta del Financial Times del 2018 ha osservato come i trasferimenti via SWIFT passino spesso attraverso diverse banche prima di raggiungere la loro destinazione finale, rendendoli lunghi, costosi e privi di trasparenza su quanto denaro arrivi effettivamente a destinazione. Chiaramente all'aumentare del numero di intermediari coinvolti aumenta la complessità e l'inefficienza del sistema: i tempi si dilatano, i costi di transazione crescono e anche i rischi connessi aumentano.

Finora abbiamo visto l'esempio di un bonifico, ma la parte più rilevante riguarda le transazioni *wholesale*, cioè quelle di importo notevole. Queste transazioni in genere sono regolate attraverso trasferimenti elettronici su reti interbancarie e le infrastrutture utilizzate vengono definite sistemi di pagamento. Il maggior rischio nei sistemi di pagamento *wholesale* è il cosiddetto rischio sistemico, ovvero il rischio che un intero sistema finanziario collassi. Le crisi bancarie hanno natura sistemica quando più fallimenti bancari appaiono tra loro collegati. Ciò è evidenziato da "co-movimenti simultanei e unidirezionali" che coinvolgono la maggior parte delle banche che costituiscono il sistema (Gualandri, Noera, 2014). Gli attuali sistemi di pagamento sono sufficientemente evoluti da ridurre la necessità di mantenere scorte in forma liquida, ma in compenso richiedono una concessione di credito. La funzione della tesoreria di una banca diventa, quindi, quella di ottimizzare la gestione giornaliera o infragiornaliera della liquidità, sulla base di interazioni strategiche tra banche. Come osservato da F. Bazzana e F. Debortoli nell'articolo *Il rischio sistemico in finanza: una rassegna dei recenti contributi in letteratura* i sistemi di pagamento possono essere fonte di rischio sistemico in due modi: trasmettendo direttamente i problemi di un membro agli altri, oppure procurando ai partecipanti dei danni inattesi derivanti da esposizioni finanziarie inaspettate. In merito a questo occorre fare una distinzione tra le due macrocategorie dei sistemi di pagamento: il regolamento netto periodico (RNP) e il regolamento lordo continuo (RLC).

Con il sistema RNP, i pagamenti vengono raggruppati ad intervalli di tempo prestabiliti, alcune ore o giorni, e, al momento del regolamento, vengono liquidate solo le posizioni nette. Il *net settlement* può essere bilaterale o multilaterale: nel primo caso i saldi debitori netti sono regolati nei confronti della rispettiva controparte, mentre nel secondo caso la fase di compensazione avviene attraverso un negoziatore centrale, di solito una *clearing house*. I costi di liquidità sono contenuti, ma fino al momento del *settlement* si resta esposti ad un rischio che cresce

all'aumentare del periodo di tempo prefissato. Questo sistema, infatti, implica un fabbisogno di liquidità relativamente basso, ma un rischio di credito piuttosto elevato, dovuto alla periodicità che comporta un ritardo tra *clearing* e *settlement*. Maggiore è lo scarto temporale tra *clearing* e *settlement*, maggiore è il rischio di credito. In caso di insolvenza di una singola banca, si potrebbe innescare una reazione a catena che coinvolge anche altre banche, compromettendo la stabilità dell'intero sistema. Per capire meglio tale meccanismo, supponiamo che ci sia un sistema RNP formato da tre banche A, B e C, le cui linee di credito sono descritte dalla seguente tabella:

	A	B	C	Debito totale
A	-	15	10	25
B	10	-	-	10
C	20	-	-	20
Credito totale	30	15	10	-
Credito netto	+5	+5	-10	-

Assumiamo per ipotesi che le riserve a disposizione di ciascun operatore siano pari a 2. Chiaramente la banca C con due sole unità di riserva, non è in grado di regolare le transazioni in sospeso. Inizia, quindi, il processo di *unwinding*, che consiste nel riaprire a ritroso tutte le operazioni svolte e conteggiare nuovamente le posizioni nette, escludendo l'operatore insolvente. Ricalcolando, dunque, le posizioni nette delle banche A e B emerge la seguente situazione:

	A	B	Debito totale
A	-	15	15
B	10	-	10
Credito totale	10	15	-
Credito netto	-5	+5	

Ora anche la banca A risulta insolvente, mettendo in crisi la stabilità del sistema. Abbiamo dimostrato come gli effetti negativi di una singola insolvenza possano essere amplificati, passando dal rischio di credito di un singolo istituto al rischio sistemico.

Con il sistema RLC, invece, le transazioni vengono regolate man mano che giungono le istruzioni di pagamento: ogni volta che c'è un *clearing*, c'è un *settlement*. Le transazioni sono immediate, quindi eventuali insolvenze emergono subito: questo riduce la probabilità di eventi sistemici, ma è estremamente costoso per gli intermediari partecipanti, che in ogni momento devono avere a disposizione fondi sufficienti. Di conseguenza nell'RLC serve molta più liquidità rispetto all'RNP e in caso di indisponibilità di riserve da parte di più intermediari potrebbero

esserci dei rischi per l'intero sistema. Tuttavia, questo porta più raramente all'insolvenza degli altri operatori, grazie all'intervento della banca centrale, che svolge un ruolo chiave in questo sistema di pagamento. Infatti, le banche commerciali che hanno riserve insufficienti per far fronte ai pagamenti, hanno accesso al credito della banca centrale. Questo da un lato riduce notevolmente il rischio sistemico, ma dall'altro richiede una regolamentazione e una vigilanza efficienti per scopi prudenziali. L'assunzione del rischio di credito da parte della banca centrale tende a deresponsabilizzare le banche, incoraggiando il loro *moral hazard*. Le banche, infatti, sono incentivate ad assumere dei rischi eccessivi, con la consapevolezza che la banca centrale effettuerà dei salvataggi per contenere gli effetti negativi di una singola insolvenza sul sistema. Subentrano così degli interessi secondari di massimizzazione dell'utilità da parte degli intermediari, che potrebbero minare l'efficienza dell'intero sistema.

La crisi del 2007-08 ha messo in evidenza tutta la fragilità e l'inefficienza della finanza tradizionale (Gualandri, Noera, 2014). Durante la crisi, infatti, si sono manifestate contemporaneamente le due componenti chiave del rischio sistemico: la prociclicità dei comportamenti finanziari (*time-varying risk*) e l'effetto aggregato delle interconnessioni interne al sistema finanziario (*cross-section risk*). La concessione incontrollata e smodata del credito, l'accumulo di eccessi di leverage espliciti ed impliciti e la trasformazione delle scadenze hanno completamente distorto la percezione del rischio: l'intero sistema finanziario era fondato su una struttura intrinsecamente fragile e vulnerabile, frutto di un eccessivo *moral hazard* (Borio, Lowe, 2002). La complessità delle interconnessioni tra istituti finanziari e la concentrazione del sistema hanno contribuito alla prociclicità, amplificandone la fragilità sistemica (Gai et al. 2011).

Possiamo affermare, quindi, che la crisi finanziaria del 2007-08 ha minato i due pilastri principali su cui si fonda la finanza tradizionale: la fiducia e la regolamentazione. La fiducia è un elemento essenziale per il regolare funzionamento dei mercati finanziari e per il corretto comportamento degli intermediari finanziari. Il *moral hazard* e il default potenziale ed effettivo di numerose rinomate banche d'affari hanno portato ad una crisi di fiducia, da cui scaturì ben presto una crisi di liquidità. Il default di Lehman Brothers provocò preoccupazioni e timori sulla solidità di altre banche, generando un diffuso sentimento di sfiducia verso questi istituti. L'improvviso aumento del rischio di insolvenza determinò una drastica riduzione della liquidità sui mercati interbancari e un aumento dei tassi di interesse a breve termine. La crisi apparve sempre più nella sua natura sistemica, con turbolenze senza precedenti che si estesero all'intero sistema finanziario, evidenziando un elevato grado di interconnessione che, per effetto dell'esposizione diretta o indiretta delle banche di diversi Paesi, ha innescato una reazione a catena che ha coinvolto tutto il mondo della finanza.

La crisi del 2007-08 ha così messo in discussione anche il secondo pilastro, quello della regolamentazione del sistema finanziario. Alla luce dei drammatici eventi provocati dalla crisi, sono state introdotte a livello globale delle misure più vincolanti e stringenti per aumentare i controlli e migliorare la qualità dell'assetto normativo.

Ancora oggi banche e imprese continuano a specializzarsi nell'ambito del *risk management*, per scardinare un sistema di incentivi distorto e deresponsabilizzante. Tuttavia, in finanza, quello della regolamentazione è un argomento molto complesso e intricato, che proprio dopo la crisi del 2007-08 ha destato un'attenzione crescente, che ha dato origine ad un dibattito tuttora aperto. Nell'epoca in cui viviamo, la tecnologia offre delle opportunità incredibili, in grado di rivoluzionare radicalmente ogni settore, incluso quello finanziario. Il problema normativo in ambito finanziario nasce in virtù del fatto che l'innovazione finanziaria consente di eludere l'attuale regolamentazione, rendendo presto obsoleti gli strumenti di controllo esistenti. Spesso l'innovazione è una diretta risposta alla regolamentazione. Sulla base delle nuove norme, si cerca di sfruttare la tecnologia emergente per variare il campo d'azione e muoversi al di fuori del quadro normativo. La regolamentazione è quindi spinta ad un'incessante rincorsa, estendendosi in pervasività e complessità. Se questa entropia regolamentare sia efficace a prevenire i rischi sistemici o se invece non finisca addirittura per amplificarli è una delle questioni sollevate dalla recente crisi ed ancora in attesa di risposta. Ma non è l'unica questione irrisolta. Come sottolineano D.Zetsche, D.Arner e R.Buckley , mentre molti sistemi finanziari si sono originariamente evoluti come forme di ordinamento privato o quadri di autoregolamentazione, nel tempo lo Stato ha assunto un ruolo crescente in risposta proprio ai fallimenti dell'ordinamento privato e dell'autoregolamentazione, che tendono a manifestarsi periodicamente in caso di crisi finanziarie. Chiaramente non esiste una formula risolutiva per bilanciare autoregolamentazione e intervento pubblico nei mercati. Ogni Stato è una realtà diversa, con diverse risorse a disposizione, quindi talvolta è necessario un intervento deciso da parte dello Stato, altre volte è più efficiente lasciar spazio all'autoregolamentazione. Il confine tra *deregulation* e *overregulation* può infatti risultare più labile di quanto si possa immaginare.

In questo contesto molto complesso, fatto di intermediari, istituzioni e autorità, si inserisce la DeFi che cerca di eliminare le inefficienze di un sistema fortemente centralizzato, attraverso una decentralizzazione della finanza che avviene per mezzo della tecnologia. Le nuove tecnologie sono potenzialmente in grado di ridurre notevolmente i rischi inerenti ai sistemi centralizzati della finanza tradizionale. Se poniamo la questione in questi termini, però, sembrerebbe che la DeFi sia soltanto una novità del mondo FinTech. Tuttavia, vi è una grande differenza tra DeFi e FinTech. La tecnologia finanziaria FinTech si limita a riprodurre e migliorare alcuni ruoli tradizionalmente svolti dalle grandi istituzioni finanziarie. In alcuni casi, la tecnologia digitale può ridurre i costi di transazione, espandere la portata delle transazioni e potenziare le transazioni peer-to-peer, stimolando una nuova ondata di innovazione nel FinTech (Chen et al., 2019). Anche se la FinTech ha ridotto la necessità di istituzioni finanziarie, non ha eliminato del tutto gli intermediari: spesso sostituisce un intermediario (ad esempio, un'istituzione finanziaria) con un altro (ad esempio, una società tecnologica). La decentralizzazione finanziaria DeFi, invece, permette di compiere un ulteriore passo in avanti che va a scardinare l'intero sistema finanziario: non solo riduce il rischio sistemico, velocizza le transazioni e garantisce una maggior trasparenza, ma i recenti

sviluppi della tecnologia blockchain stanno potenziando un nuovo paradigma incentrato sulla decentralizzazione e la disintermediazione. La tecnologia blockchain può eliminare la necessità di intermediari nelle transazioni finanziarie, in quanto è in grado di facilitare le transazioni peer-to-peer attraverso la fiducia "distribuita" e le piattaforme decentralizzate. Di conseguenza, questa tecnologia consente di aumentare sostanzialmente la portata e l'efficienza delle transazioni peer-to-peer senza intermediari e senza aumentare i costi di transazione. Grazie alla blockchain, i servizi finanziari diventano decentralizzati, innovativi, personalizzabili, senza confini, veloci e trasparenti. Questo nuovo paradigma è diverso da quello costruito sull'economia dei costi di transazione (TCE). In primo luogo, la TCE si concentra sull'opportunismo, mentre la DeFi è fondata sulla fiducia "distribuita" (Seidel, 2018), una forma di fiducia che "scorre lateralmente tra gli individui" senza relazioni di fiducia preesistenti (Botsman, 2017). La tecnologia blockchain può creare tale rapporto di fiducia distribuita, perché le transazioni registrate su una blockchain sono valide, immutabili e verificabili, in quanto vengono convalidate attraverso il consenso distribuito e sono protette da strumenti crittografici avanzati (Narayanan et al., 2016). Di conseguenza, una blockchain può servire come fonte comune di verità per le parti in transazione, facilitando le transazioni peer-to-peer in maniera efficiente e trasparente. In secondo luogo, la TCE riconosce i ruoli delle gerarchie e degli intermediari nella riduzione dei costi di transazione, mentre la DeFi si concentra sulla riduzione dei costi di transazione attraverso la decentralizzazione e la disintermediazione (Murray et al., 2019). Grazie a questi ultimi due elementi, la tecnologia blockchain può ridurre i costi associati alla ricerca, alla contrattazione e all'esecuzione di una transazione, mentre espande le possibilità di fare affari con utenti sparsi per il mondo, collegando le parti in modo diretto e innovativo (Cong, He, 2018). In sostanza si continua a usufruire dei benefici della riduzione dei costi di transazione e di gestione, pur senza dover ricorrere all'aiuto degli intermediari. A tal proposito, Accenture ha condotto un'analisi chiamata *Banking on blockchain,* da cui emergono tutte le potenzialità di questa tecnologia applicata al settore bancario. Nella fattispecie, questo studio ha riscontrato l'opportunità di lungo periodo per le banche di riorientare i sistemi finanziari, operativi e di rischio, su delle piattaforme basate sulla blockchain. Gli analisti di Accenture hanno confrontato i dati forniti da McLagan relativi a circa 50 indicatori dei costi operativi sostenuti dalle principali banche d'investimento, con l'Accenture High Performance Investment Bank, un modello sviluppato da Accenture stessa, che rappresenta la banca d'investimento "ideale". I risultati hanno evidenziato dei risparmi sostanziali in quattro aree principali: la trasparenza e la miglior qualità dei dati rendono il sistema più snello e questo può far risparmiare fino al 70% dei costi di rendicontazione finanziaria. In secondo luogo, un miglioramento delle identità digitali e del profiling dei clienti può ridurre i costi delle operazioni centralizzate del 50%. Inoltre, la trasparenza e la verificabilità delle transazioni possono recare un risparmio che va dal 30% al 50% circa sulla conformità normativa. Infine, anche a livello di operazioni di business, la riduzione o l'eliminazione di vari intermediari rendono il processo di *clearing* e *settlement* più efficiente ed efficace, con un risparmio potenziale pari al 50%. Nel complesso queste quattro componenti porterebbero ad un risparmio medio

annuale di circa il 30%. Anche il documento *The FinTech 2.0 paper: rebooting financial services* realizzato da Santander InnoVentures in collaborazione con Oliver Wyman e Anthemis Group dimostra come l'utilizzo della tecnologia blockchain sia in grado di ridurre i costi infrastrutturali delle banche attribuibili ai pagamenti internazionali, al trading di titoli e alla conformità normativa per un ammontare compreso tra i 15 e i 20 miliardi di dollari circa all'anno. Già nel 2016, il report annuale di McKinsey sul global banking sottolineava come la digitalizzazione dirompente fosse un elemento chiave che avrebbe eroso i profitti del settore bancario.

Con la fiducia distribuita e le piattaforme decentralizzate abilitate dalla tecnologia blockchain, gli imprenditori e gli innovatori hanno la possibilità di creare un sistema finanziario aperto, che ha un coinvolgimento limitato o nullo delle istituzioni finanziarie. Così facendo, intendono ridurre il costo delle transazioni, ampliare l'inclusione finanziaria, potenziare l'accesso aperto a tutti, incoraggiare l'innovazione e creare nuove opportunità di business (Financial Stability Board, 2019). Anche se questo movimento è ancora nelle sue fasi iniziali, mostra già il grande potenziale della tecnologia blockchain nel generare una nuova serie di modelli di business incentrati sulla decentralizzazione e la disintermediazione.

Entrando più nello specifico, Pasquale Sorgentone nel suo libro "Il futuro del valore" ci aiuta a sintetizzare le principali differenze tra la DeFi e la finanza tradizionale. In primo luogo, le attività operative non sono gestite da un'istituzione e dai suoi dipendenti, ma da regole codificate in un programma informatico, lo smart contract, che risiede su blockchain. Il codice programmatico dello smart contract è aperto, trasparente e immodificabile, e le transazioni sono pubbliche e pseudoanonime, tutte caratteristiche che aiutano a creare fiducia e consenso. Inoltre, i servizi della DeFi, detti "protocolli" o "blocchi base" (building blocks), sono componibili in modo tale da poter essere personalizzati per creare soluzioni a maggior valore aggiunto. La modularità dei protocolli garantisce un'elevata flessibilità sia per la creazione di prodotti sia per l'interfaccia utente. Il miglioramento dell'efficienza delle transazioni peer to peer e la sicurezza garantita da strumenti crittografici avanzati possono potenziare e velocizzare il processo di democratizzazione della finanza: tutti possono utilizzare protocolli DeFi e interagire attraverso gli smart contract. Infatti, nei Paesi in via di sviluppo, il sistema centralizzato della finanza tradizionale non garantisce a tutti l'opportunità di accedere ai servizi finanziari: la debolezza degli istituti finanziari e la mancanza di una regolamentazione efficiente rendono particolarmente problematico il corretto funzionamento dei mercati finanziari.

1.2 Come funziona

Per comprendere al meglio il concetto di decentralizzazione e le sue potenzialità in ambito finanziario, occorre conoscere la tecnologia alla base della DeFi. Innanzitutto, a livello macroscopico, Zetzsche, Arner e Buckley hanno individuato tre fattori chiave nel processo di evoluzione tecnologica che ha reso possibile la nascita della DeFi. Il primo è la legge di Moore, secondo la quale il numero di transistor per chip o per unità di area raddoppia

ogni due anni, mentre i costi si dimezzano, consentendo di aumentare in maniera esponenziale la capacità di processare dati. Mentre dal punto di vista tecnico tale legge sembrerebbe essere arrivata al suo limite, a livello concettuale la si può considerare ancora valida ai fini del nostro discorso, soprattutto se integrata con il secondo elemento: la legge di Kryder. Questa legge esamina l'archiviazione del disco rigido e afferma che la quantità di dati memorizzati per centimetro quadrato su un disco fisso raddoppierà ogni 13 mesi. Sebbene tale intervallo temporale stia in realtà aumentando (16-17 mesi circa), l'idea di fondo è che anche la capacità di archiviazione aumenta nel tempo, riducendo contestualmente i costi. Basti pensare a una semplice scheda di memoria che nel 2005 poteva contenere fino a massimo 128 MB, nel 2014 a parità di prezzo e di dimensioni aveva una capacità di 128 GB, che equivalgono a 128 000 MB. Il terzo e ultimo elemento è lo sviluppo della banda larga, che consente di ricevere e trasmettere informazioni in maggiori quantità, favorendo la costruzione di reti efficienti. Questi tre fattori insieme hanno reso possibile la virtualizzazione dell'hardware, che consiste nel fornire delle componenti hardware attraverso dei software: il software viene ospitato, aggiornato ed eseguito su server decentralizzati piuttosto che su ogni stazione di lavoro. Solo i dati che devono essere elaborati localmente (in condizioni di connessione online istantanea e banda sufficientemente larga) continuano ad essere elaborati localmente. Tra i vantaggi principali della virtualizzazione dell'hardware vi sono la gestione immediata delle risorse e la maggior flessibilità nella distribuzione e protezione delle applicazioni. Questo consente di creare un'architettura SaaS ("software as a service") che è alla base della DeFi. Dal modello SaaS, infatti, si è sviluppato il BaaS: "Blockchain as a Service". Il BaaS è un servizio fornito da terzi per agevolare l'utilizzo di soluzioni basate su cloud per costruire, ospitare e utilizzare le proprie app blockchain, gli smart contract e altre funzioni della blockchain. In questo modo il BaaS è in grado di risolvere una serie di problemi di efficienza, utilità e costi della DeFi, dovuti al fatto che la complessità tecnica della tecnologia sottostante costituisce una vera e propria barriera all'entrata. La possibilità di facilitare l'accesso e l'utilizzo degli strumenti tecnologici ha favorito lo sviluppo della DeFi.

Abbiamo citato, dunque, alcune delle radici tecnologiche su cui si fonda la DeFi. Zetzsche, Arner e Buckley le hanno ribattezzate con l'acronimo ABCD: Artificial intelligence (AI), Blockchain, Cloud e Data.

L'idea di base dell'AI è quella di un software che imita le funzioni cognitive umane, come l'apprendimento e il problem solving. L'AI utilizza i dati per trarre delle conclusioni sulla probabilità di un evento a partire dalla previa conoscenza delle condizioni relative all'evento: maggiore è il volume di dati, più perspicaci e precise saranno le inferenze tratte dai dati. Il *machine learning* è un sottoinsieme dell'AI che utilizza metodi statistici per migliorare progressivamente le prestazioni dei computer su un dato compito, in maniera autonoma, senza l'intervento dell'uomo. In pratica, l'apprendimento si ottiene attraverso un intenso "allenamento" con più cicli di feedback mediante i quali la macchina viene informata se ha superato o fallito un compito.

Per quanto riguarda il cloud computing applicato alla DeFi, ci si riferisce alla decentralizzazione della capacità del server. Invece di utilizzare un singolo server in un unico centro server (data center), i set di dati sono distribuiti su più centri server accessibili tramite Internet da vari utenti in tutto il mondo. Il cloud computing fa riferimento alla disponibilità, su richiesta, dell'archiviazione dei dati e della potenza di elaborazione, senza che gli utenti possiedano o controllino i server che forniscono questi servizi. Il cloud computing si basa su data center gestiti da fornitori commerciali che affittano ai clienti che lo richiedono un certo spazio per archiviare dati. Per garantire la stabilità del cloud nonostante la volatilità della domanda e dell'offerta di energia, e per diversificare contro i picchi di domanda, i fornitori di servizi cloud in genere collegano i centri server in diversi fusi orari, paesi e regioni economiche e incanalano la domanda in eccesso verso i server dove la capacità di elaborazione dei dati è più economica, a causa della minore domanda e minori costi energetici.

I dati sono al centro della maggior parte delle recenti innovazioni, che risultano dalla digitalizzazione di una gamma sempre più ampia di processi. È l'idea della "digitalizzazione di tutto" che è alla base delle teorie della quarta rivoluzione industriale. Il volume sempre maggiore di dati supporta sia l'analisi dati tradizionale sia gli approcci "Big Data". L'analisi dei Big Data si riferisce alla raccolta e l'elaborazione di una mole di dati troppo grande o troppo complessa per le applicazioni tradizionali di elaborazione dati. Le applicazioni Big Data si basano su metodi avanzati di analisi dati per rilevare correlazioni inaspettate, testare le correlazioni previste o determinare la probabilità di un modello predefinito.

La componente più caratterizzante dell'ABCD, però, è senza dubbio la blockchain, senza la quale la DeFi non sarebbe possibile. La blockchain è un *ledger* (libro mastro) digitale, decentralizzato e distribuito su un network, strutturato come una catena di registri, detti blocchi, responsabili dell'archiviazione dei dati, dalle transazioni a intere applicazioni digitali. Un *ledger* è un database in cui è possibile solamente aggiungere informazioni, sotto forma di nuovi blocchi, ma non si possono modificare o rimuovere i blocchi precedentemente aggiunti alla catena. 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 nessun individuo, nessun intermediario e nessuna istituzione. Dal punto di vista strutturale, quindi, alla base di una blockchain c'è un *ledger* digitale. La blockchain rientra, perciò, in un insieme ben più ampio che è quello della Distributed Ledgers Technology (DLT). Con la Distributed Ledgers Technology si entra nell'ambito dei database che fanno riferimento a un registro distribuito, ovvero gestito in modo tale da consentire l'accesso e la possibilità di effettuare modifiche da parte di più nodi di una rete. La condivisione dei dati si traduce in un database distribuito su una rete di server che funzionano tutti insieme come un unico libro mastro. I *ledgers* distribuiti sono caratterizzati dall'assenza di un'amministrazione e di un archivio centrale. Mentre un database tradizionale richiede un sistema di accesso controllato, in cui la gestione è affidata a terzi, una blockchain o una DLT possono essere utilizzate da parti sconosciute e non fidate in modo libero e aperto, senza la necessità di

alcuna forma di controllo. Di conseguenza, la blockchain e la DLT risultano molto utili in un settore come quello finanziario, in cui fiducia, sicurezza e trasparenza sono requisiti fondamentali. Ma ciò che rende la blockchain unica rispetto alle altre DLT è il raggruppamento e l'organizzazione in blocchi. I blocchi vengono collegati tra loro e protetti mediante crittografia, consentendo agli utenti solo di aggiungere dati al database distribuito. I dati, una volta registrati, non sono più modificabili o eliminabili. Ecco perché tutte le blockchain sono DLT ma non tutte le DLT sono blockchain.

Uno degli scopi principali della tecnologia blockchain è permettere a chiunque, in qualsiasi parte del mondo, di effettuare transazioni senza la necessità di affidarsi a un'istituzione centrale o a un intermediario. Per fare ciò, la blockchain deve essere distribuita su un network. Ogni macchina connessa alla rete della blockchain è un nodo. In base alla struttura della rete e al ruolo di ciascun nodo, si distinguono tre tipologie di rete: centralizzate, decentralizzate e distribuite. Vitalik Buterin, inventore di Ethereum, analizza il diverso grado di centralizzazione dal punto di vista di tre fattori diversi: architettura, autorità e logica.

A livello di architettura, una rete si definisce centralizzata se esiste al suo interno il cosiddetto "single point of failure", ossia un singolo punto centrale di errore che, se compromesso, impedirebbe all'intero sistema di funzionare correttamente. Ad esempio, un'applicazione web che comunica con un singolo server è considerata un sistema con un'architettura centralizzata (sistema client-server). Al contrario, in una rete decentralizzata le risorse sono distribuite e possibilmente replicate nei nodi della rete, in modo tale che un'applicazione possa essere eseguita da tutti i suoi partecipanti senza creare un singolo punto di fallimento (sistema peer to peer). Per quanto affermato finora, possiamo concludere che dal punto di vista dell'architettura una blockchain sia un sistema decentralizzato, poiché non esiste un singolo punto di fallimento.

Per quanto riguarda l'autorità, una rete centralizzata è sottoposta al controllo di un'autorità centrale che monitora i dati e vigila sulle operazioni degli utenti, e stabilisce le regole e i criteri di accesso al sistema. Facebook, Google, Amazon o un qualsiasi servizio home banking sono sistemi caratterizzati da un'autorità centrale. In una rete decentralizzata, invece, non esiste nessuna autorità e nessuno ha il controllo della rete. Di conseguenza, è facile dedurre che da questa prospettiva una blockchain pubblica sia un sistema decentralizzato, poiché non vi è alcuna autorità che ne detenga il controllo.

Infine, con riferimento alla logica, una rete logicamente centralizzata deve essere identificata in ogni istante da un singolo stato per funzionare correttamente. È necessario che tutti i partecipanti siano d'accordo su quale sia lo stato del sistema. Esiste quindi un unico stato logico sul quale tutti i partecipanti devono concordare. Un esempio può essere quello di un database globale in cui tutti i dati vengono salvati e mantenuti coerentemente. In una rete logicamente decentralizzata, invece, possono esistere diverse copie dei dati e qualsiasi nodo può modificare la propria copia senza alterare il normale funzionamento del sistema. Per esempio nel caso delle email, se io cancello

una mail che ho ricevuto nella mia casella di posta, non la elimino anche dalla casella di chi me l'ha inviata. Questo non è possibile in una blockchain, che pertanto è un sistema logicamente centralizzato, caratterizzato da un singolo stato logico, quindi l'intero sistema si comporta come se fosse un solo computer.

Ma la blockchain è anche una rete distribuita in cui i dati e le computazioni sono distribuiti su più nodi e ogni nodo ne possiede una copia. Questo serve a minimizzare i rischi e le complessità di gestione. Supponiamo che ci sia un registro centralizzato amministrato da una singola entità che contenga tutti i dati rilevanti. Una disposizione del genere comporta una serie di rischi. In primo luogo, se l'hardware che contiene il registro viene distrutto, il contenuto delle informazioni si perde definitivamente. In secondo luogo, dipendenti sleali dell'amministratore del database o amministratori poco affidabili possono manipolare il contenuto delle informazioni del registro. Terzo, un attacco informatico può portare a manipolazioni e perdite di dati. Le reti distribuite, invece, non possiedono un solo grande server o database, bensì vari data center sparsi in tutto il mondo.

L'accostamento di parole diverse, e talvolta in contrasto tra loro, associate alla medesima tecnologia può risultare destabilizzante e fuorviante. Con riferimento alla blockchain abbiamo utilizzato allo stesso tempo aggettivi come "decentralizzato", "centralizzato" e "distribuito". Questo ha contribuito ad alimentare il dibattito sul significato della decentralizzazione e in molti si sono chiesti se la DeFi sia effettivamente decentralizzata o meno alla luce della tecnologia sottostante che, come abbiamo visto, non è propriamente decentralizzata in senso assoluto. Piuttosto, esiste un diverso grado di decentralizzazione, tale per cui appare legittimo chiedersi in base a quali parametri un dato sistema possa definirsi più o meno decentralizzato.

Inizialmente, l'idea era quella di basarsi sul numero di nodi che fanno parte della rete. Tuttavia, tale metodo è stato ben presto abbandonato, in quanto un approccio puramente quantitativo si è rivelato insufficiente. Questo ha portato inevitabilmente a delle definizioni sempre più astratte, che hanno lasciato forse troppo spazio ad una libera interpretazione. Il Cambridge Center for Alternative Finance descrive la decentralizzazione come una caratteristica che emerge dai ruoli, dai comportamenti e dall'influenza degli attori su ogni livello di un ledger distribuito (protocollo, rete e dati). Alcuni sistemi DLT possono essere più centralizzati in alcuni aspetti per enfatizzare una specifica proprietà del sistema ritenuta desiderabile dagli utenti. Dato che ci possono essere casi in cui la centralizzazione di un determinato processo sarebbe particolarmente auspicabile per rendere un sistema più appetibile per i partecipanti, non è ragionevole - né fattibile in pratica - richiedere che tutti i livelli di un sistema siano completamente decentralizzati per poter essere classificati come DLT.

Alla luce di ciò, è possibile ricavare due caratteristiche fondamentali della decentralizzazione.

Innanzitutto è un concetto relativo, in quanto non esiste una linea chiara che separi la centralizzazione dalla decentralizzazione. Esistono solo diversi gradi di (de)centralizzazione che possono variare a seconda del sistema che consideriamo e in base alle diverse caratteristiche che analizziamo all'interno di uno stesso sistema. Come

abbiamo detto prima, la blockchain è un sistema decentralizzato dal punto di vista dell'architettura e dell'autorità, ma è logicamente centralizzato e al tempo stesso costruito su una rete distribuita.
La seconda caratteristica è che la (de)centralizzazione è un concetto dinamico, che è in grado di evolvere nel tempo. Un qualsiasi cambiamento in ambito tecnologico, economico o normativo potrebbe avere un impatto sul grado di (de)centralizzazione di un sistema. Ad esempio, una nuova legge o una variazione dei costi possono modificare il livello complessivo di (de)centralizzazione.

Alcuni detrattori di blockchain e delle criptovalute hanno cercato di screditare la DeFi facendo leva proprio sull'ambiguità del concetto di decentralizzazione e sulle sue caratteristiche. Molti sostengono, ad esempio, che vi sia una concentrazione di potere nelle mani di pochi sviluppatori di software e *miners*, che sono i nodi che partecipano attivamente al processo di consenso, che vedremo in seguito. A sostegno della loro tesi, questi autori riportano alcuni esempi come il caso del bug trovato nel software di Bitcoin nel 2018, noto come "inflation bug", che ha messo in crisi il mondo cripto. Il fatto che tale falla nel sistema sia stata scoperta e riparata da un ristretto gruppo di sviluppatori e *miners* esperti, è stato utilizzato come prova per dimostrare che la blockchain non è poi così decentralizzata come si dice. Tuttavia occorre puntualizzare in primo luogo che blockchain e Bitcoin sono due entità diverse: blockchain è la tecnologia che ha reso possibile la nascita della criptovaluta Bitcoin, ma le criptovalute sono solo uno dei tanti modi per utilizzare l'infrastruttura blockchain. Un bug nel software di una criptovaluta non intacca minimamente la validità dell'infrastruttura che ne è alla base. Un alunno che commette un errore nella dimostrazione di un teorema, non rende quel teorema privo di fondamento. Per fortuna c'è un insegnante che lo corregge. Analogamente sviluppatori e *miners* hanno svolto in questo caso lo stesso ruolo di un professore, con la differenza, però, che chiunque può diventare un *miner*: chiunque abbia a disposizione una potenza di calcolo sufficiente. Avere qualcuno in grado di correggere degli eventuali bug non è mai uno svantaggio, anzi. A tal proposito, basti pensare che ormai tutte le banche hanno un dipartimento di cybersecurity per difendersi da eventuali attacchi informatici, difatti la domanda di lavoro in questo campo è in netta crescita. Le banche spendono ogni anno delle cifre importanti per avere un servizio di sicurezza informatica, che però non sempre è aggiornato ed efficiente, o gestito da esperti. Oltretutto, tali servizi vengono forniti da società esterne specializzate, ma ciò non implica che le banche siano nelle mani di queste società. Allo stesso modo, non è possibile affermare che la blockchain sia di proprietà degli sviluppatori o dei *miners*, nonostante essi svolgano un ruolo fondamentale. Inoltre blockchain non necessita di alcun dipendente esperto di cybersecurity per monitorare e difendersi da eventuali attacchi hacker, in quanto la crittografia avanzata e il meccanismo di validazione e consenso lo rendono un sistema intrinsecamente più sicuro. Per completezza, però, è doveroso riconoscere che eventuali bug o attacchi informatici non aiutano certo a creare la fiducia necessaria che dei sistemi così complessi richiedono. Eppure, nella fattispecie, Bitcoin, che all'epoca dell'inflation bug passò da 5000 euro a 3000 euro

circa, oggi ha un valore che oscilla intorno ai 40 000 euro. Ciò a testimonianza del fatto che il problema è stato superato e qualcosa in termini di fiducia sta cambiando.

Un'altra critica che è stata mossa alla decentralizzazione in senso lato è che la mancanza di un'autorità implica che vi sia un'assenza di controllo tale da incentivare le attività illegali e illecite attraverso l'uso della blockchain. Lo stesso si diceva agli inizi di Internet. Tuttavia, sebbene molte persone continuino a fare un uso improprio di Internet, nessuno sostiene più che bisogna chiuderlo o che non lo si deve usare. È chiaro che sia necessaria una maggior regolamentazione per tutelare gli utenti meno esperti da eventuali frodi. La tecnologia comporta dei rischi, ma mentre nel settore bancario al rischio tecnologico si aggiunge quello sistemico, nel mondo DeFi il rischio maggiore è connaturato nella blockchain stessa. Come ogni innovazione tecnologica, anche la blockchain dovrà affrontare diverse insidie prima di arrivare alla sua fase di maturità e lungo questo percorso ci saranno sicuramente nuovi bug e altri problemi. La DeFi non è ancora una realtà perfetta, ma offre delle opportunità nuove e interessanti che la finanza tradizionale non propone.

1.3 Obiettivi

Prima di proseguire con l'analisi delle novità principali che può apportare la DeFi da un punto di vista più pratico, è opportuno definire gli obiettivi che la DeFi si prefigge, in modo tale da contestualizzare tale fenomeno all'interno della sua dimensione reale e potenziale. Si può già anticipare fin da subito che gli obiettivi sono particolarmente ambiziosi e il movimento DeFi è solo agli albori. Di conseguenza, è importante ai fini della nostra trattazione tenere presente non soltanto le possibilità concrete attualmente disponibili, ma anche le potenzialità inespresse che potrebbero manifestarsi in futuro.

Pasquale Sorgentone nel suo libro "Il futuro del valore" identifica come obiettivo generale della DeFi quello di consentire la gestione delle attività finanziarie in maniera aperta, autonoma e personalizzata, senza intermediari e senza confini. La DeFi in sintesi è un ambizioso tentativo di decentralizzare i principali casi di utilizzo finanziario tradizionale come trading, prestiti, investimenti, gestione patrimoniale, pagamenti e assicurazioni sulla blockchain. Tra gli obiettivi più specifici, infatti vi è ad esempio quello di poter ottenere prestiti quasi istantanei, senza la necessità di lunghi iter approvativi. Questo nasce dall'esigenza di agevolare l'accesso al credito, soprattutto nei Paesi meno sviluppati. Un altro target è quello di beneficiare di tassi di interesse superiori rispetto a quelli presenti attualmente nella finanza tradizionale. O ancora un altro proposito consiste nel facilitare l'emissione di azioni in maniera snella e veloce, apportando un cambiamento notevole per i mercati finanziari.

2. La fiducia nel mondo digitale: il consenso decentralizzato e il ruolo degli smart contract

Nel capitolo precedente abbiamo definito la DeFi come un ambiente aperto a tutti, privo di autorità e intermediari, e in grado di replicare i principali servizi finanziari offerti dalla finanza tradizionale, ma in maniera trasparente e decentralizzata. Appare legittimo chiedersi come ci si possa fidare di un sistema del genere che sembrerebbe non avere alcuna forma di controllo. In effetti quello della fiducia rappresenta uno dei problemi principali che si sono riscontrati agli inizi della blockchain e delle prime criptovalute. Fin dal principio, infatti, la questione più difficile da affrontare riguardava il problema della doppia spesa (*double spending*). Sostanzialmente consiste nell'accertarsi che la moneta digitale non venga spesa due volte. Nella finanza tradizionale con la moneta fisica questo rischio non sussiste per due motivi: il primo è che vige il controllo delle autorità e degli intermediari che autorizzano i pagamenti e vigilano sulla regolarità delle transazioni; mentre il secondo è dovuto all'impossibilità materiale di duplicare il denaro contante, al di là della contraffazione. Nel mondo digitale, invece, le informazioni si possono riprodurre con molta facilità. Si configura così la possibilità per un malfattore di poter inviare una copia del criptoasset in questione, mantenendo l'originale. In un sistema strutturalmente irreversibile e privo di un'autorità centrale, una frode del genere non sarebbe più risarcibile. In una blockchain, una volta creata una transazione valida non si può più tornare indietro: non è possibile modificare, eliminare o annullare una transazione. Ciò è dovuto al fatto che, come abbiamo visto prima, la blockchain è fondata su una logica centralizzata, tale per cui supporta l'esistenza di un singolo stato. Di conseguenza, ogni transazione modifica lo stato della blockchain in maniera permanente. Questo implica che in ogni singolo istante si deve avere contezza dell'ordine cronologico di tutte le transazioni effettuate fino a quel momento e devono risultare simultaneamente in un ledger distribuito, in modo tale che sia sempre aggiornato. Basterebbe un leggero ritardo per attuare la frode della doppia spesa, poiché si potrebbe impiegare lo stesso ammontare di criptoasset per effettuare due transazioni contemporaneamente, ma solo quella che raggiunge i server per prima sarebbe valida. Ovviamente questo rischio è tanto maggiore, quanto più si espande il network di utenti: una rete più ampia coinvolge più nodi e richiede, quindi, il funzionamento di più server. Per evitare che l'intero sistema collassi a causa di una semplice frode che fa leva su una discrepanza temporale di pochi secondi, è necessario l'aiuto di tutti gli utenti per raggiungere un accordo sull'effettivo stato della blockchain, che garantisca l'ordine cronologico delle transazioni in ogni dato istante di tempo. Tuttavia, sebbene a livello concettuale possa sembrare una problematica piuttosto semplice, in realtà è un'impresa ben più ardua che riguarda diversi ambiti disciplinari, dalla matematica all'informatica, passando per l'economia e la teoria del giochi. Si tratta di un problema di calcolo distribuito formulato per la prima volta nel 1982 dai matematici Leslie Lamport, Marshall Pease e Robert Shostak, noto come il problema dei generali bizantini. Immaginiamo che un gruppo di generali bizantini sia accampato fuori da una città nemica, circondandola. Dopo aver osservato il nemico, i generali devono decidere un piano comune per stabilire se attaccare o ritirarsi. Tuttavia, alcuni generali potrebbero essere dei traditori e ciò comprometterebbe l'esito del

piano. Inoltre, la questione diventa più complessa se assumiamo che i generali possano comunicare solamente attraverso dei messaggeri. Se ad esempio ci fossero cinque generali, due dei quali favorevoli ad attaccare e due contrari, il quinto, qualora fosse un traditore, potrebbe comunicare ai due favorevoli di voler attaccare e ai due contrari di voler ritirarsi, mettendo a repentaglio la strategia. Questa metafora allude chiaramente a ciò che accade concretamente in un sistema distribuito come una blockchain, in cui per analogia i generali sarebbero i nodi, i traditori simboleggiano i nodi maligni e i messaggeri rappresentano i canali di comunicazione. In un contesto particolarmente avverso e insidioso come questo, si deve trovare un modo per raggiungere un accordo.

2.1 Gli algoritmi del consenso: PoW vs PoS

Satoshi Nakamoto, il misterioso inventore di Bitcoin, è il primo che riesce a trovare una soluzione al problema della doppia spesa e a quello dei generali bizantini valida nell'ambito delle criptovalute. Nel suo manifesto, il celebre "white paper", Satoshi sostiene di aver elaborato un sistema di pagamento in grado di sostituire la fiducia riposta in un intermediario o in un'autorità, con degli strumenti di crittografia avanzata. La sua proposta si basa su due elementi: il *timestamp* e l'algortimo del consenso. Il *timestamp* consiste nell'apporre, su ogni blocco, data e ora per certificare il momento esatto in cui avviene la creazione del blocco. Ogni blocco è caratterizzato da una stringa alfanumerica detta *hash*. Si tratta di una funzione matematica in grado di trasformare un qualsiasi input di lunghezza variabile, in un output di lunghezza prestabilita. È una funzione deterministica, ovvero uno stesso input determina sempre lo stesso output, ed è unidirezionale, ossia per ogni output si può risalire all'input solo attraverso il metodo "brute force", cioè provando tutti i possibili input. Queste caratteristiche rendono la funzione di *hash* particolarmente utile in campo crittografico. Il *timestamp,* quindi, è come se mettesse un timbro su ogni nuovo blocco, che contiene non solo l'*hash* identificativo del nuovo blocco, ma anche l'*hash* di tutti i blocchi precedenti. In questo modo si certifica la reale esistenza dei dati fino ad un determinato momento e allo stesso tempo si garantisce l'immutabilità dei dati stessi, poiché qualora si voglia modificarli, anche un minimo cambiamento modificherebbe l'*hash*, andando ad impattare sull'intera catena. In altre parole, per alterare i dati di una transazione, bisogna alterare contestualmente i dati di tutta la catena, proprio perché ogni nuovo *hash* include anche tutti gli *hash* precedenti. In un registro pubblico distribuito come la blockchain, chiunque potrebbe accorgersi agevolmente di un tentativo di manomissione, perché sarebbe subito evidente e facilmente verificabile. Tutto ciò ha consentito a Satoshi di sviluppare un algoritmo del consenso in grado di risolvere il problema dei generali bizantini per raggiungere il consenso distribuito. Per implementare un sistema peer to peer che sia "Byzantine Fault Tolerant" (BFT), Satoshi ha programmato il cosiddetto protocollo Proof of Work (PoW). Il PoW consiste nella risoluzione di un problema matematico complesso, che richiede di trovare un determinato valore casuale, detto *nonce,* che, una volta eseguito come input di un algoritmo crittografico (SHA-256), restituisce un hash con un certo numero di bit a zero richiesti. Una soluzione, infatti, è ritenuta valida solo se soddisfa il

cosiddetto target di difficoltà, che si esplica nel numero di zeri con cui il nonce deve iniziare. Chiaramente, maggiore è il numero di zeri, maggiore è la difficoltà. La difficoltà viene aggiornata ogni 2016 blocchi, in base al tempo impiegato per crearli: al ritmo desiderato di un blocco ogni dieci minuti circa, per creare 2016 blocchi servirebbero due settimane di tempo. Se viene impiegato un tempo minore, la difficoltà viene aumentata, altrimenti sarà ridotta, al fine di mantenere il tempo di creazione di un blocco costante, onde evitare la trappola dell'inflazione. Il tempo dipende dal numero di tentativi calcolati al secondo, che viene chiamato hashrate. Ovviamente, l'hashrate dipende a sua volta dalla potenza di calcolo dei mezzi a disposizione: per avere un termine di paragone, basti pensare che una persona sarebbe in grado di calcolare un singolo hash a mano in circa 9-10 ore, mentre un ASIC, una macchina progettata appositamente per il mining, può calcolare oltre un trilione di hash al secondo.

Consideriamo ad esempio il Bitcoin, in cui un hash è un valore casuale compreso nell'intervallo $[0, 2^{256} - 1]$,che per convenzione definiamo come [0, M]. Affinché l'hash del blocco sia valido, deve valere la seguente ipotesi: Hash (Block) $\leq$ M/D, dove D $\in$[1, M] è proprio la soglia di difficoltà. L'unico modo per trovare la soluzione consiste nell'applicare il metodo "brute force", procedendo a tentativi attraverso il test di tutti i possibili input. Come avevamo accennato in precedenza, questo compito è affidato ai miners ed è un lavoro basato su probabilità e potenza di calcolo. Il periodo di tempo T(r) impiegato da un miner, che ha a disposizione un hardware capace di processare k operazioni al secondo, segue una distribuzione:

$$P \{ T(k) \leq t \} = 1 - \exp(-kt/D)$$

Consideriamo n miners di Bitcoin con un hashrate $k_1, k_2, \ldots, k_n$. Il periodo di tempo T è uguale al valore minimo delle variabili casuali $T(k_i)$, assumendo per ipotesi che il miner che trova la soluzione pubblichi subito il nuovo blocco per consentire agli altri miners della rete di verificarlo. In base alle proprietà della distribuzione esponenziale, anche T è distribuito in maniera esponenziale:

$$P \{ T \text{ def} = \min (T1, \ldots, Tn) \leq t \} = 1 - \exp(-t D \sum n^{i=1} k_i)$$

$$P \{ T = T_i \} = k_i / \sum n^{j=1} k_j$$

Quest'ultima equazione dimostra come il protocollo PoW sia equo: a parità di potenza di calcolo, due miners hanno le stesse probabilità di trovare la soluzione giusta, il cosiddetto golden hash. Una volta trovato, il golden hash viene trasmesso alla rete e verificato dagli altri miners. Sebbene sia molto difficile da trovare, risulta piuttosto facile verificarne la correttezza. Solo dopo aver ricevuto l'approvazione da parte di un numero di nodi ritenuto sufficiente (almeno 6 conferme nel caso di Bitcoin), il blocco viene considerato valido e i dati in esso contenuti diventano immutabili, in virtù delle proprietà crittografiche della funzione di hash e del timestamp. Occorre

sottolineare che il numero di conferme di una transazione sarebbe il numero di blocchi successivi a quello in cui viene inclusa la transazione. Questo meccanismo garantisce un livello di sicurezza che cresce all'aumentare dei blocchi creati. Sempre nel caso di Bitcoin, qualora si volesse per esempio manomettere una transazione inserita nel blocco numero 10, si dovrebbe ricalcolare il golden hash dei 6 blocchi successivi fino al numero 17, prima che altri miners riescano a minare il blocco 17, cioè prima di ricevere 6 conferme. Tutto ciò richiederebbe una potenza di calcolo enorme per poter completare la frode in solo 1 ora e 10 minuti circa (in Bitcoin viene creato approssimativamente un blocco ogni 10 minuti).

Abbiamo così chiarito quanto affermato precedentemente sul ruolo cruciale svolto dai miners che contribuiscono alla realizzazione di un sistema con delle caratteristiche fondamentali per creare la fiducia necessaria in ambito finanziario. Il lavoro dei miners unito alle proprietà intrinseche della blockchain dà origine a un sistema caratterizzato da una forte trasparenza, immutabilità dei dati e sicurezza nelle operazioni. Per questo motivo i miners vengono incentivati e valorizzati attraverso un sistema di ricompense, che ci proietta verso una nuova disciplina, detta cripto-economia. Come ci suggerisce il nome stesso, la cripto-economia consiste nella commistione della teoria economica e della crittografia: in un ambiente particolarmente ostile, la cripto-economia tenta di elaborare dei progetti che disincentivano dei comportamenti scorretti e disonesti, rendendoli più costosi rispetto all'osservanza delle regole. Questo è il risultato dell'unione tra crittografia e incentivi economici che garantisce un livello di fiducia e sicurezza accettabile per gli utenti. Nel caso del PoW gli incentivi possono essere di natura economica, come commissioni o ricompense monetarie, oppure decisionale, ad esempio la possibilità di scegliere di minare i blocchi più redditizi per un miner. Allo stesso modo eventuali comportamenti fraudolenti diventano particolarmente costosi in termini di elettricità e di hardware utilizzati per avere una potenza di calcolo considerevole. Tuttavia, l'introduzione dei cosiddetti token di governance da parte di alcune delle piattaforme decentralizzate più utilizzate ha suscitato qualche perplessità sull'effettiva efficacia del modello di incentivi e disincentivi nella cripto-economia. La principale preoccupazione consiste nel fatto che se da un lato un token nativo attenua il rischio di centralità, dall'altro i detentori di token non sono responsabili della regolamentazione come nei sistemi finanziari tradizionali e quindi potrebbero proporre aggiornamenti e iniziative per i loro interessi personali, piuttosto che per il bene degli utenti della piattaforma. Se ci sono milioni di dollari depositati in ETH sulla piattaforma e un piccolo numero di indirizzi accumula grandi quantità del token nativo in questione, questi utenti potrebbero compromettere il corretto funzionamento della piattaforma. Chiaramente il rischio si riduce all'aumentare del numero di utenti, poiché i criptoasset di maggior valore non sono concentrati nelle mani di pochi. Quindi si tratta di un rischio ridotto per le piattaforme più grandi, che possono permettersi di correre questo rischio dal momento in cui sono gli utenti stessi che si assumono i rischi finanziari e non finanziari delle piattaforme su cui operano. Il loro interesse principale consiste nel mantenere elevata la sicurezza della piattaforma che altrimenti si svaluterebbe.

Il protocollo PoW ha dimostrato nel corso degli anni di avere vari punti deboli. Tra le principali criticità, vi è senza dubbio l'enorme consumo di energia. Uno studio del Cambridge Center for Alternative Finance ha stimato che se la rete Bitcoin fosse uno Stato, si posizionerebbe al 29° posto per consumo di energia con circa 129 TWh, superando la Norvegia che consuma 124 TWh. Ciononostante, occorre sottolineare che è proprio l'elevato costo del mining a disincentivare le frodi e a rendere i dati sicuri e immutabili. Ma al di là di questo, è evidente che, se si considera che questi sono i dati relativi solamente a Bitcoin, il PoW non sembra essere un metodo sostenibile. Un'altra debolezza del PoW è che risulta vulnerabile al cosiddetto attacco del 51%. Se uno o più miner insieme riuscissero ad avere una potenza di calcolo tale da avere un hashrate superiore al resto del network, potrebbero manomettere le transazioni e convalidare i relativi blocchi prima che qualunque altro miner possa verificarli. Tuttavia, sempre per il sistema di incentivi sopraccitato, con una potenza di calcolo simile sarebbe più redditizio per un miner rispettare le regole, anziché violarle. Ciò non toglie, però, che questo attacco ha maggiori probabilità di successo in contesti più piccoli, con blockchain minori. Ma anche in questo caso va sottolineato che un attacco del genere svaluterebbe completamente la criptovaluta della piattaforma in questione, lasciando tutti a mani vuote.

Ad ogni modo, l'insostenibilità del PoW ha portato alla ricerca di algoritmi del consenso alternativi. Tra questi, il più utilizzato e promettente è il cosiddetto Proof of Stake (PoS). L'idea di fondo è piuttosto semplice: anziché basarsi sulla potenza di calcolo dei miners, la probabilità di creare un blocco e ricevere la ricompensa è proporzionale alla quota di criptoasset posseduta dall'utente. Un singolo stakeholder che ha una frazione p del numero totale di monete in circolazione, crea un nuovo blocco con probabilità p. Quindi anche il PoS è un protocollo altrettanto equo. Supponiamo ad esempio che ci siano quattro utenti A, B, C e D, che possiedono rispettivamente 40, 30, 20 e 10 Ether, la moneta di Ethereum. La probabilità di essere scelti come validatori sarà del 40% per A, del 30% per B, del 20% per C e del 10% per D. Gli utenti con le partecipazioni più alte nel sistema hanno più probabilità di essere selezionati come validatori e allo stesso tempo sono quelli che hanno più interesse a mantenere la rete sicura, poiché in caso di eventuali attacchi e frodi il valore della criptovaluta diminuirebbe. Il PoS presenta, quindi, alcuni vantaggi rispetto al PoW. Innanzitutto è più economico, in quanto non necessità della potenza di calcolo, ma si basa sulle quote possedute dagli utenti. Di conseguenza, non vi sono costi di elettricità e hardware. Inoltre, il PoS rende gli attacchi più costosi rispetto al PoW. Per organizzare un attacco del 51% , un attaccante esterno avrebbe bisogno di acquisire almeno il 51% della valuta, il che sarebbe particolarmente costoso per i criptoasset che hanno un valore alto. Oltretutto, analogamente al PoW, un attacco simile svaluterebbe completamente quel criptoasset vanificando gli elevati costi per sferrare l'attacco. Infine, uno dei disincentivi più comuni utilizzati nel PoS prevede, in caso di frode, la distruzione della quota messa in palio dal validatore per essere selezionato.

L'avvento del PoS ha diviso il mondo cripto in due fazioni: PoS vs PoW. Tuttavia, il PoS non è ancora così diffuso e questo crea un po' di scetticismo. Ethereum 2.0, il futuro aggiornamento di Ethereum, ha già preannunciato di

utilizzarlo e sarebbe la prima vera occasione per valutare il PoS applicato su larga scala. Molti dubitano che possa raggiungere gli stessi livelli di sicurezza del PoW. Ma in ogni caso PoW e PoS non sono gli unici algoritmi del consenso esistenti e magari in futuro si troverà una soluzione più sostenibile ed efficiente. Quel che è certo, però, è che il PoS o qualunque altro algoritmo futuro dovrà fare i conti con il cosiddetto trilemma della scalabilità. Con scalabilità si intende la capacità di un sistema di aumentare o ridurre le proprie prestazioni, in funzione delle necessità di chi lo richiede. In ambito blockchain, si tratta di elaborare e gestire un numero crescente di transazioni senza paralizzare il sistema e senza renderlo eccessivamente costoso. Questo rischio ha origine alla base di Ethereum, per cui le commissioni per le transazioni sono tanto più alte quanto maggiore è la richiesta di usare la blockchain. Quando c'è meno domanda per meno transazioni effettuate su Ethereum, il rischio è basso. Quando c'è un'alta domanda per un maggior numero di transazioni effettuate su Ethereum, il rischio è alto. La più grande componente del rischio di scalabilità è quanto sia imprevedibile sapere quando la rete blockchain di Ethereum sarà congestionata dagli utenti che inviano più transazioni del solito. Un'applicazione DeFi potrebbe non funzionare come previsto quando la rete è congestionata per un eccesso di domanda. Il solito Vitalik Buterin ha sollevato per primo la questione del trilemma della scalabilità, che si riferisce al trade-off di cui devono tener conto i progetti blockchain in termini di decentralizzazione, sicurezza e scalabilità. Il PoW garantisce un altissimo livello di sicurezza, un buon grado di decentralizzazione nonostante l'esistenza di mining pools e del rischio di attacco al 51%, ma secondo alcuni sarebbe necessario aumentare la scalabilità per elaborare un numero maggiore di transazioni al secondo. Da questo punto di vista, il PoS sembra essere in grado di aumentare il livello di scalabilità velocizzando il processo di conferma delle transazioni, ma desta qualche perplessità circa il livello di sicurezza e il grado di decentralizzazione, in virtù di un meccanismo che di fatto tende a privilegiare gli utenti che possiedono più criptoasset.

2.2 Il ruolo degli smart contract

Finora abbiamo parlato solo di transazioni e di come creare fiducia in un sistema decentralizzato. Ma se vogliamo ampliare gli orizzonti della finanza decentralizzata dobbiamo vedere come la DeFi è in grado di sostituire anche altre funzioni e servizi della finanza tradizionale, non solo le transazioni. A tal proposito dobbiamo introdurre un nuovo strumento: lo smart contract. Sebbene sia ormai considerato parte integrante delle blockchain e del mondo cripto, il concetto di smart contract è stato formulato ben prima del white paper di Satoshi Nakamoto (2008). Il termine smart contract comparve per la prima volta nel 1994 in un omonimo documento scritto dall'informatico statunitense Nick Szabo ed è stato poi elaborato e perfezionato dallo stesso autore tra il 1996 e il 1997. Il primo articolo del 1994 definisce lo smart contract come un protocollo informatico che esegue i termini di un contratto, con l'obiettivo generale di soddisfare le condizioni contrattuali comuni (termini di pagamento, garanzie, privacy e adempimento), minimizzare la necessità di fiducia negli intermediari e allo stesso tempo ridurre i costi di

transazione e il rischio di eventuali frodi. Szabo considera fin da subito i protocolli delle monete digitale, che non erano così diffuse all'epoca, come dei validi esempi di smart contract e intravede in questi protocolli il potenziale per sostituire un ampio spettro di titoli e servizi finanziari che va ben oltre le singole transazioni. In maniera quasi visionaria, Szabo vedeva negli smart contract l'opportunità per sviluppare nuove tipologie di business e creare soluzioni finanziarie personalizzate, grazie alla trasparenza e alla sicurezza garantite dai sistemi crittografici. Per quanto riguarda i nuovi business, Szabo cita il campo dell'Electronic Data Interchange (EDI), in cui gli elementi delle transazioni commerciali tradizionali (fatture, ricevute, ecc.) sono scambiati elettronicamente, a volte includendo la crittografia e la firma digitale. Per questo motivo, l'EDI può essere visto come un precursore primitivo degli smart contract, che però l'autore critica per mancanza di trasparenza. In ambito finanziario, invece, Szabo trova gli smart contract particolarmente utili per la standardizzazione e il trading degli asset sintetici, attività finanziarie ottenute dalla composizione di due diversi strumenti finanziari, uno dei quali è in genere costituito da uno strumento derivato. Si tratta di titoli complessi formati dalla combinazione di securities (come le obbligazioni) e derivati (opzioni e futures), la cui struttura può essere costruita su contratti standardizzati, che possono essere scambiati in maniera più facile e veloce, con bassi costi di transazione. Le attività sintetiche sono più flessibili e personalizzabili, adattandosi meglio alle diverse esigenze dei clienti, e permettono di costruire contratti che imitano altri contratti, al netto di alcune passività. Come esempio, Szabo riporta dei titoli sintetici che imitano i rendimenti delle azioni di società tedesche, senza richiedere il pagamento della tassa che gli stranieri devono pagare al governo tedesco per le plusvalenze in azioni tedesche. È importante notare che questi asset sintetici non conferiscono diritti di voto come gli originali, ma potrebbe essere possibile aggiungere protocolli di smart contract per trasferire anche i diritti di voto al titolo sintetico. Un recente articolo del Cointelegraph ha confermato quanto previsto da Szabo, preannunciando che, come vedremo in seguito, la competizione delle piattaforme per il mercato di asset sintetici sulla DeFi si sta facendo sempre più agguerrita.

Da questo punto di vista, possiamo dire che Szabo ha anticipato la nascita della DeFi, che non può prescindere dagli smart contract. Questo emerge ancora più chiaramente dagli articoli successivi, in particolare "Formalizing and Securing Relationships on Public Networks" del 1997, in cui Szabo chiarisce che l'idea alla base degli smart contract è quella di incorporare e automatizzare diversi tipi di clausole contrattuali direttamente attraverso l'hardware o il software, in modo tale da rendere un'eventuale violazione o inadempimento del contratto particolarmente costosa per il trasgressore. Se vogliamo questo non è altro che il principio cardine della sopraccitata cripto-economia. In merito a questo, Szabo paragona gli smart contract a un distributore automatico: entro una quantità limitata di perdita potenziale (l'importo in cassa dovrebbe essere inferiore al costo della violazione del sistema), la macchina prende le monete e, attraverso un semplice meccanismo, dispensa il resto e il prodotto secondo il prezzo visualizzato. Il distributore automatico è come se fosse un contratto al portatore: chiunque abbia monete può partecipare a uno scambio con il venditore. In questo senso, l'esecuzione del contratto

avviene in maniera automatica, in base all'avverarsi di certe condizioni. Il lockbox e altri meccanismi di sicurezza proteggono le monete immagazzinate e il contenuto dagli aggressori, in modo sufficiente per permettere una distribuzione redditizia dei distributori automatici in un'ampia varietà di aree. Analogamente, strumenti crittografici e disincentivi economici garantiscono un certo livello di sicurezza per gli smart contract. Un esempio concreto di smart contract affine alla similitudine del distributore automatico è il seguente: Tizio invia N unità di moneta digitale a Caio, solo se prima riceve M unità da Sempronio. Una volta che Tizio riceve M unità da Sempronio, Caio riceverà automaticamente N unità da Tizio, senza che sia necessario l'intervento di un'autorità per eseguire il regolare adempimento del contratto. Allo stesso modo, è ciò che si verifica ogniqualvolta inseriamo l'importo corretto per prendere uno snack o una bevanda al distributore automatico. Gli smart contract più comuni, infatti, seguono una logica IFTTT (If This Than That) in virtù della quale vengono eseguiti automaticamente al verificarsi di determinate condizioni.

Ma per vedere all'opera tutto il potenziale inespresso degli smart contract, bisognerà attendere lo sviluppo della blockchain. Come si può evincere da quanto detto finora, gli smart contract hanno trovato nella tecnologia blockchain terreno fertile per espandere i propri orizzonti, soprattutto nel settore finanziario. Blockchain, infatti, presenta tutte le caratteristiche necessarie in termini di fiducia e sicurezza per l'implementazione degli smart contract: da quelli più semplici, come i protocolli di scambio di moneta digitale, a quelli più complessi, relativi alle DApps (Decentralized Applications). Se pensiamo a Bitcoin, ad esempio, la piattaforma è in grado di supportare transazioni complesse, ma il linguaggio di scripting è troppo limitato per programmare delle DApps. Le blockchain di seconda generazione, invece, consentono di elaborare una vasta gamma di smart contract più articolati. Non a caso la blockchain di Ethereum è la più diffusa per lo sviluppo di smart contract, grazie ad un linguaggio di programmazione Turing-complete che gli consente di scrivere e personalizzare qualsiasi tipo di smart contract, anche quelli più avanzati. Gli smart contract, infatti, sono scritti in un linguaggio di programmazione che li rende chiari e trasparenti, privi di ambiguità. Al loro interno vengono definite tutte le regole e la logica necessaria affinché il contenuto del contratto venga eseguito automaticamente e in maniera decentralizzata: il cambiamento di stato della blockchain e il rispetto del vincolo contrattuale sono garantiti dal consenso del network, quindi dagli algoritmi del consenso trattati in precedenza. Se Bitcoin è la piattaforma che ha avuto più successo in termini di transazioni per le criptovalute, Ethereum è senza dubbio la blockchain di riferimento per quanto riguarda gli smart contract e le DApps. Ciò è dovuto principalmente al fatto che Vitalik Buterin in persona asserisce nel white paper di Ethereum che tale piattaforma nasce proprio con l'intento di consentire a chiunque di costruire delle DApps o scrivere degli smart contract attraverso il linguaggio di programmazione Turing-complete di Ethereum. A tal proposito, Buterin definisce gli smart contract come scatole crittografiche che contengono valore e che si aprono solo al verificarsi di determinate condizioni. In questo modo

Ethereum è diventata la più grande piattaforma di smart contract in termini di market cap, applicazioni disponibili e altre attività sviluppate.

Come sottolineato da Fabian Schär, per capire la novità degli smart contract, dobbiamo prima guardare alle normali applicazioni web basate su server. Quando un utente interagisce con una di queste applicazioni, non può osservare la logica interna dell'applicazione. Inoltre, l'utente non ha il controllo dell'ambiente di esecuzione. Il rischio che ci sia un tentativo di manipolazione del sistema è piuttosto elevato. Di conseguenza, l'utente deve fidarsi di chi gestisce l'applicazione. Gli smart contract mitigano entrambi i problemi e assicurano che un'applicazione venga eseguita come previsto. Il codice del contratto è memorizzato sulla blockchain sottostante e può quindi essere esaminato pubblicamente da chiunque abbia interesse. Il comportamento del contratto è deterministico e la sua esecuzione (sotto forma ad esempio di transazioni) viene elaborata da migliaia di partecipanti alla rete, garantendo la correttezza dell'adempimento. Quando l'esecuzione porta a cambiamenti di stato della blockchain, questi cambiamenti sono soggetti alle regole di consenso della rete e saranno protetti dagli strumenti crittografici relativi alla sicurezza della blockchain. Gli smart contract su Ethereum hanno accesso a un ricco set di istruzioni e risultano perciò molto flessibili e componibili, attraverso l'interazione di più codici diversi. Inoltre, possono contenere criptovalute e quindi assumere il ruolo di un "custode" o fungere da deposito, con criteri completamente personalizzabili per stabilire come, quando e a chi queste attività possono essere rilasciate. Si è così sviluppata una grande varietà di nuove applicazioni decentralizzate e fiorenti ecosistemi finanziari, il cui valore è in netta crescita.

Tuttavia, gli smart contract non sono del tutto privi di rischi. Il pericolo principale è il cosiddetto rischio di vulnerabilità, che consiste nella possibilità che un *attacker* possa trovare un modo per prosciugare letteralmente i fondi stanziati in uno smart contract a causa di un codice scritto in maniera errata o sfruttando dei vettori di attacco. Questi eventi purtroppo non sono ancora così rari come dovrebbero essere. Nella fattispecie esistono cinque tipi di vulnerabilità ricorrenti, che derivano dalla noncuranza degli sviluppatori, che non considerano il rischio e la sicurezza come parte imprescindibile della programmazione degli smart contract. In particolare ci sono tre vulnerabilità riconducibili ad errori di programmazione: codice rientrante, *unhandled exception* e *integer overflow*; e altre due causate da errori di validazione: *transaction order dependency* e *timestamp dependency*.

Il codice rientrante viene utilizzato in informatica per programmare sistemi multitasking. Un programma è detto rientrante se più compiti possono essere eseguiti simultaneamente in sicurezza su un sistema a processore singolo, dove una procedura rientrante può essere interrotta nel mezzo della sua esecuzione e poi essere eseguita di nuovo, "rientrando" appunto in modo sicuro prima che i compiti precedenti completino l'esecuzione. Un esempio di processo rientrante può essere l'invio di una e-mail. Un utente può iniziare a scrivere un'e-mail, salvarla come bozza, inviare un'altra e-mail e finire il messaggio più tardi. Questo è un esempio innocuo. Tuttavia, immaginate un sistema bancario online mal costruito per l'emissione di bonifici, dove il saldo del conto viene controllato solo

nella fase di inizializzazione. Un utente potrebbe cominciare a fare diversi bonifici senza effettivamente inviarne nessuno. Il sistema bancario confermerebbe che il conto dell'utente ha un saldo sufficiente per ogni singolo trasferimento. Se non ci fosse un controllo aggiuntivo al momento dell'effettivo invio, l'utente potrebbe quindi inviare tutte le transazioni e potenzialmente superare il saldo del suo conto, inviando più soldi di quanti ne abbia effettivamente. Negli smart contract avviene una situazione analoga. La rientranza consiste nello sfruttamento di una vulnerabilità del contratto, che si verifica quando un contratto cerca di inviare ETH prima di aver aggiornato il suo stato interno. Anziché comunicare con un indirizzo fidato, l'indirizzo di destinazione è un altro contratto non fidato, su cui viene eseguita una funzione per richiedere ETH diverse volte, prima che si compia il regolare adempimento del contratto "leale". In questo modo all'attaccante basta creare una funzione ricorsiva che intervenga sul contratto deviando la sua destinazione originaria corretta e spostando la transazione su un altro contratto fittizio. Tale operazione può essere ripetuta più volte, prosciugando lo smart contract iniziale. Sebbene oggi esistano diverse misure preventive per ridurre il rischio di subire tale attacco, quella del codice rientrante è forse una delle vulnerabilità che richiede maggiore attenzione da parte di tutti gli utenti, anche quelli più esperti.

L'*unhandled exception,* invece, è una vulnerabilità molto pericolosa per i principianti. In Ethereum, uno smart contract ha spesso bisogno di richiamare un altro smart contract per adempiere alle funzionalità richieste. Questo può avvenire o inviando le istruzioni ad un altro smart contract o facendo direttamente riferimento al contratto in questione menzionandolo all'interno di un unico contratto. In questo processo, possono essere sollevate delle eccezioni che fanno sì che il contratto possa terminare e ritornare al suo stato originale, e contemporaneamente restituire un valore falso all'utente che ha richiesto le operazioni, per avvertirlo delle anomalie riscontrate. Tuttavia, alcune operazioni di basso livello, quelle più semplici come "send", che viene usato per inviare ETH, non lanciano un segnale di eccezione in caso di fallimento, ma piuttosto riportano un valore booleano per indicare lo stato dell'operazione. Un classico esempio di *unhandled exception* è il cosiddetto contratto "King of the Ether". Un utente che esegue una funzione di trasferimento per diventare il nuovo proprietario di uno smart contract, potrebbe non essere consapevole dell'esito di altri movimenti relativi al suo portafoglio originale. Ad esempio potrebbe accadere che una transazione precedente fallisca e un contratto che ha ricevuto ETH inviati dallo stesso indirizzo utente potrebbe non riconoscere che la transazione è fallita, ma procedere comunque all'aggiornamento del contratto, effettuando il passaggio di proprietà. Questo bug è stato presto riconosciuto e segnalato dalla comunità di Ethereum per avvisare gli utenti e fornire loro gli strumenti per tutelarsi adeguatamente.

L'*integer overflow*, invece, è una vulnerabilità più frequente. Si tratta di una frode che sfrutta i limiti numerici del linguaggio di programmazione. Fondamentalmente è il caso in cui si fa memorizzare a una variabile intera un valore più grande del suo limite: per esempio un intero a 32 bit può memorizzare un valore compreso tra -2^{31} e $2^{31}-1$. Se si assegna alla variabile un valore al di fuori dall'intervallo, il suo valore diventerà qualcos'altro, in base a come quell'intero è rappresentato dal sistema. Ethereum supporta degli interi con un determinato livello di bit

per limitare le capacità di *storage* e ciò lo espone a dei rischi di *integer overflow*. Se a una variabile intera è assegnato un valore più grande di questo intervallo, il sistema restituisce come valore 0; se alla variabile viene assegnato un valore inferiore all'intervallo, viene resettata al valore massimo dell'intervallo. Per fortuna da ormai tre anni esistono delle funzioni correttive che neutralizzano questo bug, che ad oggi riguarda un numero limitato di token poco diffusi. Tuttavia, degli utenti meno esperti potrebbero non prendere le opportune precauzioni, mettendo a rischio tutte le operazioni che coinvolgono lo smart contract non protetto. Per questo motivo, sebbene la DeFi sia aperta a tutti, bisogna essere consapevoli dei rischi a cui si va incontro. Sarebbe opportuno che le piattaforme forniscano maggiori informazioni a riguardo per tutelare gli utenti ed aiutarli nella corretta stesura di uno smart contract.

Per quanto riguarda invece le vulnerabilità causate dal processo di validazione abbiamo il *transaction order dependency*, detto anche *front-running*. Questo meccanismo si realizza quando due transazioni dipendenti l'una dall'altra fanno riferimento ad uno stesso contratto e sono contenute in uno stesso blocco da validare. In blockchain, l'ordine in cui arrivano due transazioni, anche se dipendenti una dall'altra, è irrilevante. L'unica cosa che conta in un blocco è quanto è alta la commissione relativa alle transazioni. Se due transazioni sono identiche, quella che sarà pubblicata e minata per prima è quella che ha una commissione più alta. Questo implica ad esempio che se si invia una transazione, un attaccante può "rubare" la transazione e spacciarla come sua, inserendo lo stesso valore ma con una commissione più alta. Quando si invia una richiesta di registrazione di un dominio, l'attaccante può rubare la richiesta, emettere lo stesso nome di dominio e finalizzarlo prima che l'altra richiesta sia conclusa. Questo perché i miner valideranno prima le transazioni che offrono una commissione più alta. Attacchi del genere sono particolarmente diffusi sugli exchange decentralizzati. Se si invia una transazione dopo che l'attaccante ha cambiato lo stato del contratto, la richiesta sarà elaborata in un nuovo stato modificato dall'attaccante. Per esempio, se si piazza un ordine di acquisto a un prezzo più alto della migliore offerta, l'attaccante inserirà due transazioni: prima acquisterà al prezzo della migliore offerta e poi offrirà lo stesso bene in vendita a un prezzo leggermente più alto. Se la transazione "regolare" viene eseguita in un secondo momento, l'attaccante trarrà profitto dalla differenza di prezzo senza possedere effettivamente il bene. In questo caso oltre al rischio di vulnerabilità dello smart contract, emergono anche delle criticità nei confronti del sistema di incentivi della cripto-economia: le ricompense potrebbero spingere i miner a deviare il loro comportamento per seguire i loro interessi personali. Alcune piattaforme hanno introdotto delle misure preventive per mitigare questo rischio.

Infine, vi è il *timestamp dependency*. Si tratta di un tipo di vulnerabilità che si può verificare negli smart contract che utilizzano il timestamp come condizione per innescare l'esecuzione automatica del contratto. Il timestamp viene stabilito in base all'orario dei server di riferimento. Tuttavia questo può essere manipolato sfruttando la flessibilità del sistema che accetta un intervallo di massimo 15 minuti di tempo tra l'apposizione del timestamp sul blocco e la pubblicazione di quest'ultimo su blockchain. Questo concede ai miners fraudolenti la possibilità

di mettere il timestamp in base ai propri interessi, restando nel margine di 15 minuti. Se un miner ha interessi in uno smart contract, potrebbe voler apporre un valore di timestamp a lui favorevole per influenzare il valore di un asset sottostante che dipende dal timestamp. Per mitigare questo rischio, sono stati sviluppati degli strumenti che aumentano il controllo sui movimenti effettuati a intervalli di tempo ravvicinati. In ogni caso il passaggio al PoS metterebbe fine a queste ultime due vulnerabilità.

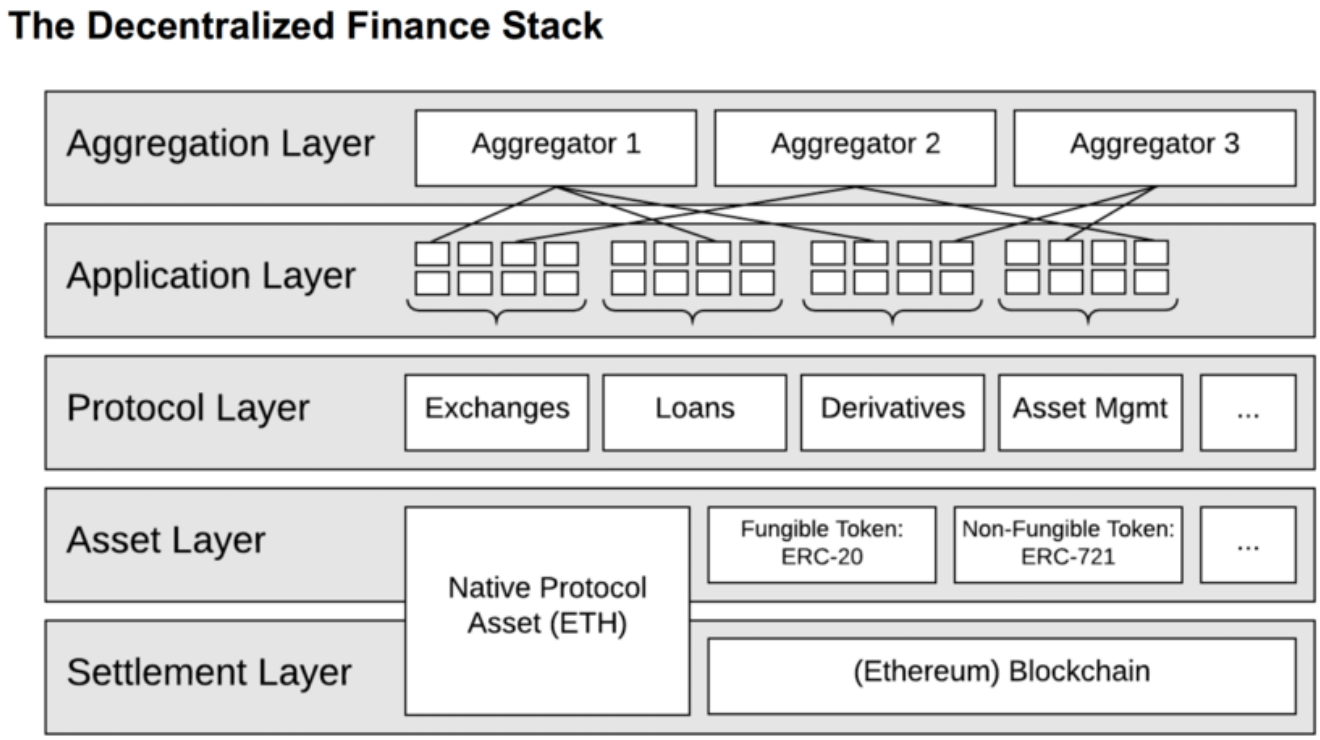
Abbiamo illustrato le principali criticità degli smart contract. Quando si ha a che fare con la tecnologia vi è sempre un grado di rischio intrinseco da dover valutare. Per gli addetti ai lavori può risultare più facile e immediato difendersi da questo tipo di vulnerabilità, ma per gli utenti meno esperti questi rischi possono rivelarsi molto pericolosi. Perciò, se da un lato è vero che l'apertura della DeFi offre delle opportunità rivolte a tutti, a cui chiunque può accedere, è altrettanto vero che prima di utilizzare delle nuove tecnologie bisogna essere consapevoli dei rischi che si possono incontrare, finanziari e non finanziari. Una regolamentazione che migliori gli obblighi di informazione per un utilizzo più sicuro dei servizi DeFi consentirebbe di rafforzare la tutela degli utenti. Abbiamo menzionato la possibilità di proteggere gli smart contract attraverso delle misure preventive e correttive, ma non tutti gli utenti sono al corrente di queste funzionalità e ciò li espone a dei rischi maggiori.

2.3 La struttura della DeFi

Con questo approfondimento abbiamo definito i due pilastri principali della DeFi: la tecnologia blockchain e gli smart contract. Questi due elementi sono accomunati da alcune caratteristiche principali su cui si fonda la DeFi. In primo luogo la decentralizzazione, che consente a chiunque di operare sulle piattaforme blockchain, utilizzare le DApps e scrivere smart contract, senza il necessario intervento di intermediari e autorità, in modo tale da velocizzare i tempi delle operazioni e ridurre i costi di transazione. Inoltre, sia per le transazioni blockchain, sia per le condizioni degli smart contract, le informazioni sono trasparenti e a disposizione degli utenti. In aggiunta, i dati su una blockchain, così come il codice programmatico degli smart contract, sono immutabili, quindi non si possono modificare. Tutto ciò è coadiuvato da un elevato standard di sicurezza garantito da strumenti crittografici avanzati. Ciascuno di questi aspetti contribuisce a creare la fiducia necessaria per effettuare transazioni e operazioni finanziarie, grazie soprattutto all'elaborazione degli algoritmi del consenso, che consentono di raggiungere un accordo in un sistema distribuito e decentralizzato. Se da un lato, infatti, la blockchain diventa sinonimo di decentralizzazione, dall'altro gli smart contract permettono di sviluppare delle applicazioni decentralizzate, le DApps, in grado di riprodurre e combinare in maniera personalizzata i vari servizi finanziari. Una volta definiti i cardini sui quali è incentrata la DeFi siamo in grado di comprendere la sua struttura.

La DeFi utilizza un'architettura a più livelli, in cui ogni strato ha uno scopo distinto. I livelli sono costruiti l'uno sull'altro in maniera gerarchica e creano un'infrastruttura aperta e altamente componibile che permette a tutti di utilizzare o combinare anche diverse parti dello *stack*. È fondamentale capire che le caratteristiche dei vari strati

hanno un impatto sui livelli sottostanti. Se consideriamo come parametro la sicurezza, per esempio, nel caso in cui la blockchain risultasse compromessa nel livello di *settlement*, tutti i livelli successivi non sarebbero sicuri. Allo stesso modo, se dovessimo utilizzare un *ledger* autorizzato come blockchain privata, qualsiasi sforzo di decentralizzazione sui livelli successivi sarebbe inefficace.



(Fonte: https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets)

Questo modello rielaborato da Fabian Schär propone un quadro concettuale per analizzare i vari strati in modo più dettagliato. Come mostrato nella figura, lo schema identifica cinque livelli distinti: a partire dal basso, troviamo il livello di *settlement*, il livello degli asset, il livello del protocollo, il livello delle applicazioni e il livello di aggregazione.

Il livello di *settlement* (Layer 1) consiste nel definire la blockchain di riferimento e il suo cosiddetto "native protocol asset" (ad esempio, Bitcoin [BTC] sulla blockchain Bitcoin e ETH sulla blockchain Ethereum). Questo permette alla rete di memorizzare le informazioni in modo sicuro e garantisce che qualsiasi cambiamento di stato sia conforme al suo set di regole. La blockchain può essere vista come la base per l'esecuzione di operazioni finanziarie senza intermediari e serve come livello di regolamento e risoluzione delle controversie.

Il livello degli asset (Layer 2) consiste in tutti gli asset che sono emessi al di sopra del livello di settlement. Questo include il native protocol asset così come qualsiasi asset aggiuntivo che viene emesso su questa blockchain (di solito indicati come token, che approfondiremo in seguito).

Il livello di protocollo (Layer 3) fornisce gli standard per casi d'uso specifici come exchange decentralizzati, mercati del debito, derivati e gestione degli asset. Questi standard sono di solito implementati come una serie di smart contract e protocolli altamente interoperabili, cui può accedere qualsiasi utente, anche attraverso le applicazioni DeFi. L'interoperabilità dei protocolli da un lato offre delle opportunità uniche nel mondo della finanza, grazie alla possibilità di comporre diversi servizi finanziari, rendendoli flessibili e personalizzabili, adatti alle esigenze degli utenti. Tuttavia, dall'altro lato questo potrebbe rivelarsi particolarmente rischioso per vari motivi. In primo luogo l'integrazione di diversi protocolli potrebbe non funzionare come previsto: ad esempio è capitato in passato che alcune piattaforme utilizzassero dei codici e dei token incompatibili gli uni con gli altri. Spesso le piattaforme DeFi integrano il codice di altre piattaforme con il proprio codice. Il rischio di questa procedura è che una piattaforma potrebbe non essere progettata correttamente per le integrazioni o i nuovi standard, quindi il codice sottostante fatto da un'altra piattaforma DeFi potrebbe non funzionare come dovrebbe. Inoltre, la composizione di protocolli con diversi gradi di sicurezza e di decentralizzazione potrebbe compromettere la validità dell'intero sistema composto. Il rischio di componibilità è il rischio che il corretto funzionamento di una piattaforma DeFi dipenda da quello di un'altra piattaforma. Se la componibilità coinvolge molte piattaforme, il rischio di componibilità può innescare una reazione a catena dagli effetti assimilabili a quelli di un rischio sistemico. Illustreremo in seguito degli esempi concreti a riguardo.

Il livello di applicazione (Layer 4) crea delle applicazioni per gli utenti per permettere loro di collegarsi ai singoli protocolli. L'interazione con gli smart contract avviene di solito attraverso un browser web front-end, che rende i protocolli più facili da usare. Nella figura si fa riferimento soprattutto alla blockchain di Ethereum, poiché ha introdotto un'innovazione particolarmente interessante che ha dato origine allo sviluppo della DeFi, in quanto ha reso possibile la programmazione delle DApps. Ethereum ha incorporato nella sua blockchain la cosiddetta "Ethereum virtual machine" (EVM), che permette a Ethereum di eseguire dei software per elaborare e processare asset digitali (monete, token…) che si trovano sulla sua blockchain. È da qui che deriva il termine "programmable money". Le applicazioni Ethereum sono fondamentalmente software per computer che programmano il funzionamento del denaro o di altri asset, con l'aiuto degli smart contract.

Il livello di aggregazione (Layer 5) è un'estensione del livello di applicazione. Gli aggregatori mettono insieme diverse applicazioni e protocolli, creando piattaforme incentrate sull'utente che può orientarsi più facilmente ed operare in maniera più agevole.. Di solito forniscono strumenti per confrontare e valutare i servizi, permettono

agli utenti di semplificare l'esecuzione di compiti complessi, collegandosi a diversi protocolli contemporaneamente e combinando le informazioni rilevanti in modo chiaro e conciso.

Come si può evincere dalla descrizione di questo modello concettuale, i livelli che meritano maggiore attenzione sono senza dubbio quelli degli assets, di protocollo e di applicazione. Dopo una breve introduzione alla tokenizzazione degli asset che caratterizza il layer 2, nel prossimo capitolo esamineremo i protocolli del layer 3 e le applicazioni più interessanti nel panorama DeFi (layer 4).

2.4 La tokenizzazione: la nuova moda per valorizzare qualsiasi cosa

Per avere un'idea del potenziale attualmente espresso dalla DeFi si potrebbe pensare al seguente esempio: attraverso delle DApps o dei DEXs è possibile comprare degli asset vincolati al dollaro americano, detti stablecoin, spostarli su una piattaforma di lending decentralizzata su cui guadagnare degli interessi e infine reinvestirli in dei liquidity pool, che sono dei fondi attraverso cui gli utenti possono immettere liquidità nel sistema in cambio di una ricompensa. Alla base di tutto ciò, vi è il processo di tokenizzazione. In principio, gli unici asset disponibili su blockchain erano le criptovalute e le uniche operazioni possibili erano delle semplici transazioni. Successivamente, lo sviluppo e la diffusione delle nuove tecnologie ha portato all'esplorazione di nuove possibilità, come quella di introdurre una vasta gamma di asset attraverso la tokenizzazione. Con questo termine si intende il procedimento mediante il quale vengono creati ed emessi sulla blockchain dei token che rappresentano dei beni reali, fisici o digitali. Questi token possono essere scambiati, prestati o venduti su delle DApps o DEXs, generalmente attraverso degli smart contract. Per questo motivo i token sono uno strumento fondamentale per la DeFi.

Al di là delle varie modalità tecniche di tokenizzazione, ciò che è più rilevante ai fini della nostra trattazione è la natura economica degli asset sottostanti ad un determinato token. Da questo punto di vista, la classificazione più diffusa suddivide i token in due categorie: i token fungibili e i token non fungibili (NFT). Si definisce fungibile un token che presenta due caratteristiche principali: divisibilità e intercambiabilità. In altre parole, un token è fungibile se lo si può frazionare in varie unità identiche fra loro, ciascuna con le medesime funzioni e proprietà, quindi intercambiabili. La maggior parte di questi token viene realizzata sulla blockchain di Ethereum tramite un modello di smart contract denominato ERC-20. In via residuale, i token non fungibili sono quelli caratterizzati da un certo grado di unicità, che li rende difficilmente indivisibili e di conseguenza non intercambiabili. La maggioranza degli NFT è creata sempre su Ethereum, ma a partire da un modello diverso, chiamato ERC-721.

I token fungibili possono essere a loro volta raggruppati in tre tipologie: i payment token, gli investment token e gli utility token. I payment token sono quelli che consentono di facilitare i pagamenti e gli scambi peer to peer, quindi non sono altro che le criptovalute. Gli investment token, invece, vengono utilizzati per investire in asset o

titoli finanziari. Infine, gli utility token sono quelli che conferiscono ai possessori il diritto all'uso di determinati prodotti o servizi.
Per quanto riguarda gli NFT, invece, si è soliti distinguere gli NFT scambiabili da quelli non scambiabili. Per fare un esempio di NFT unico nel suo genere, lo scorso 11 marzo la celebre casa d'aste Christie's ha venduto all'asta un'opera d'arte digitale, "Everydays: The First 5000 Days" dell'artista Beeple, per un valore di circa 69,2 milioni di dollari. Questo solo per far capire come la tokenizzazione sia un fenomeno molto ampio che non riguarda soltanto la finanza, ma che è potenzialmente estendibile a diversi ambiti, proprio in virtù del principio che teoricamente quasi qualsiasi bene può essere convertito in token.

Chiaramente, la nostra analisi sarà incentrata prevalentemente sui token fungibili, che sono quelli più rilevanti per la DeFi. Ma prima di procedere con lo studio dei vari protocolli del layer 3 e delle applicazioni più interessanti del layer 4, occorre introdurre un ultimo elemento che svolge un ruolo cruciale per incrementare la fiducia e l'affidabilità dei mercati nel mondo DeFi: le stablecoin. Si tratta di un particolare tipo di token fungibile il cui valore è vincolato a quello di una valuta fiat o di un asset esterno alla blockchain, oppure al valore dei criptoasset stessi. Viene definita moneta "stabile" in quanto il suo valore non risente dell'elevata volatilità tipica dei criptoasset. In questo modo si cerca di ridurre e mitigare uno dei problemi principali che ostacola lo sviluppo della DeFi e che è rappresentato proprio dalla volatilità. Inoltre, dal momento in cui chiunque può creare ed emettere token, quando qualcuno introduce dei token con la promessa, per esempio, di pagare interessi, dividendi, o prestare beni o servizi, il valore del token corrispondente dipenderà dalla credibilità e dalla fiducia riposte in questa promessa. Se un emittente non è disposto o non è in grado di soddisfare le aspettative, il token può diventare senza valore e si rischia di incorrere in delle frodi o truffe. Da questo punto di vista, molti autori hanno riscontrato una somiglianza con i derivati, poiché anche le stablecoin coinvolgono un determinato "sottostante", e la rischiosità del derivato dipende proprio dalla rischiosità del sottostante. In questo caso si potrebbero configurare dei rischi a livello informativo soprattutto per gli utenti meno esperti che, oltre a non avere le nozioni finanziarie per valutare la rischiosità del sottostante, potrebbero anche non essere in grado di reperire tutte le informazioni necessarie per individuare il sottostante. Molte piattaforme dovrebbero introdurre dei servizi di analisi per mostrare, anche per le operazioni interconnesse, la stessa trasparenza che c'è nelle operazioni singole.

La classificazione delle stablecoin avviene sulla base del collateral (garanzia) posto a supporto delle stablecoin. Si è soliti distinguere tra stablecoin con collateral "on-chain" e quelle con collateral "off-chain", a seconda se la garanzia si trovi nella blockchain o nel mondo reale.
Come abbiamo anticipato nella definizione, le stablecoin con collateral off-chain sono quelle supportate da valuta fiat o da asset esterni alla blockchain. Questa tipologia di stablecoin è particolarmente diffusa poiché può sfruttare il vantaggio di essere più familiare e confortevole per gli utenti, che restano in contatto con delle risorse fisiche del mondo reale o con i mercati finanziari tradizionali. Nel primo caso, infatti, le stablecoin vengono emesse in

base a un rapporto prestabilito vincolato a una determinata valuta legale. L'esempio più famoso è quello della moneta USDC, che è ancorata al dollaro americano secondo un rapporto 1 : 1.
Nella seconda categoria, invece, le stablecoin sono legate ad asset esterni alla blockchain, in genere commodities o altri prodotti scambiati nei mercati finanziari tradizionali. Una delle stablecoin più diffuse è la Digix Gold Token (DGX), il cui valore è pari a quello di un grammo d'oro.
In entrambi i casi, però, bisogna tenere presente che, seppur stabili, queste stablecoin non sono prive di rischio. I rischi principali derivano dalla dipendenza da un'altra entità centrale e dalla necessità di effettuare dei controlli regolari per assicurarsi che il collaterale sottostante sia effettivamente disponibile in ogni momento. Questo processo può essere costoso e, in molti casi, non del tutto trasparente. USDC, ad esempio, è gestito da una piattaforma centralizzata, Circle, con cui si deve instaurare un certo grado di fiducia. Gli utenti devono fidarsi che USDC mantenga stabilmente la parità col dollaro, e Circle deve fidarsi dei propri utenti affinché non compiano attività illecite. Infatti, Circle ha il potere di controllare tutti i movimenti sulla piattaforma e, se dovesse individuare delle transazioni sospette, ha il diritto di chiudere l'account dell'utente e ritirare tutti gli USDC del suo portafoglio. Si tratta di un rischio di centralità di cui gli utenti devono essere consapevoli. Nel caso di Digix, invece, l'oro che funge da collaterale si trova in un caveau a Singapore e viene controllato ogni tre mesi per monitorare se le riserve auree corrispondono effettivamente alla capitalizzazione di Digix. Anche in questo caso gli utenti devono fidarsi di un'entità centralizzata e ciò li espone ad un rischio di centralità: se dovesse venir meno la corrispondenza con le riserve auree, l'intero sistema di garanzie sarebbe a rischio fallimento.

Contrariamente, le stablecoin con collateral on-chain, quelle supportate da criptoasset sulla blockchain, presentano diversi vantaggi, in quanto sono altamente trasparenti e ulteriormente garantiti dagli smart contract. Tuttavia, come si può facilmente intuire, tutelarsi da eventuali fluttuazioni di valore attraverso degli strumenti caratterizzati da un'elevata volatilità può sembrare un controsenso. Non sarebbe ragionevole basarsi su un rapporto 1 : 1 con il valore del criptoasset sottostante se quest'ultimo è soggetto a forti oscillazioni di prezzo. In effetti, per superare questa contraddizione, è stato necessario ricorrere a delle soluzioni tecnicamente più complesse come quella adottata da Maker per creare la stablecoin Dai. Maker è una piattaforma per smart contract basata sulla blockchain di Ethereum, che garantisce e stabilizza il valore del Dai attraverso un sofisticato sistema dinamico di collateralized debt position (CDP). Il Dai utilizza principalmente ETH come collaterale on-chain per creare un Dai token decentralizzato ancorato al valore di 1 USD. Poiché non c'è un token nativo legato all'USD su Ethereum, i token Dai devono essere sostenuti da un altro asset. Ogni volta che qualcuno vuole emettere nuovi token Dai, deve prima bloccare abbastanza ETH come garanzia sottostante, depositandoli in una CDP attraverso uno smart contract fornito dal protocollo Maker. Siccome il tasso di cambio USD/ETH non è fisso, le CDP sono sempre collateralizzate per eccesso, cioè il valore del collaterale da depositare deve essere maggiore del debito. Questo meccanismo viene definito "over-collaterization" ed è utilizzato per contrastare la volatilità del sottostante.

Se il valore del collaterale ETH sottostante scende sotto la soglia minima del 150 per cento del valore di Dai in circolazione, lo smart contract metterà all'asta il collaterale per cancellare il debito in Dai.

La principale criticità di questo sistema risiede nella mancanza di diversificazione degli asset sottostanti, che si basano solamente su Ethereum. Avere la possibilità di detenere diversi tipi di criptoasset come collateral, consentirebbe di ridurre ulteriormente la volatilità. In futuro si pensa che la nuova generazione di stablecoin, sarà basata su degli algoritmi che modificano automaticamente l'offerta di stablecoin in base alla domanda, come se fosse una sorta di banca centrale automatizzata, che stabilizza il valore delle stablecoin senza ricorrere ad alcuna forma di collateral. In attesa degli sviluppi futuri, attualmente MakerDAO ha avviato una ricerca per espandere le categorie di criptoasset accettati come collateral. Una strategia che però ha destato qualche perplessità. In particolare, la decisione di introdurre l'utilizzo di USDC come collateral ha fatto storcere il naso ai fautori della DeFi: il fatto che l'USDC sia centralizzato comprometterebbe il grado di decentralizzazione della piattaforma, esponendola a un rischio di centralità. Tuttavia si tratta di un modo facile e veloce per testare l'idea di un multi-collateral Dai, un Dai coperto da più tipologie di collateral. In questo caso il rischio di centralità non ricade su tutti gli utenti, ma solo sui possessori dei token nativi di MakerDAO, i MKR. Se un CDP garantito da USDC viene decollateralizzato, allora i MKR saranno automaticamente coniati per coprire la perdita e questo svaluterà i MKR esistenti. Poiché i detentori di MKR sono coloro che hanno votato per decidere di usare il collaterale USDC come garanzia, sono loro gli unici a correre il rischio di svalutazione dell'MKR, senza intaccare il valore del Dai degli altri utenti. È per questo che stanno facendo attenzione a bilanciare il rischio e il beneficio, limitando la quantità consentita di collaterale USDC. Torneremo più avanti sull'argomento, ma possiamo già anticipare che alla luce dei recenti accadimenti questa scelta si è rivelata vincente, poiché ha consentito al Dai di reggere l'urto del più grande crollo del mercato cripto avvenuto a maggio 2021.

3. App ed exchange decentralizzati: la DeFi in azione

La nostra epoca sarà ricordata come l'era di Internet: non è ormai una novità che stiamo assistendo a un'evoluzione della rete che procede a un ritmo sempre più veloce, supportata da uno sviluppo tecnologico senza precedenti. La stessa Internet, che da molti era considerata agli inizi solo una bolla speculativa, un posto pericoloso pervaso da truffe, frodi e malfattori di ogni genere, è diventata parte integrante della nostra vita.

Tim Berners-Lee, inventore del World Wide Web, ha sempre sostenuto che la sua invenzione fosse più un'innovazione sociale, che tecnologica. Ha dichiarato in diverse occasioni di aver immaginato il web come una piattaforma aperta che avrebbe permesso a tutti, ovunque, di condividere informazioni, accedere alle opportunità e collaborare attraverso i confini geografici e culturali. In effetti la storia è andata in questa direzione, ma il progresso tecnologico ci pone continuamente dinanzi a nuove sfide e nuove possibilità, talvolta rivoluzionarie. Chiunque oggi può accedere ai potenti mezzi che ci offrono il web e Internet, per implementare anche le idee più folli, che fino a poco tempo fa erano impensabili. Sono state proprio le menti più visionarie della storia recente a dare vita a delle invenzioni che hanno avuto un impatto strabiliante sulla nostra quotidianità. L'Internet of Value e il Web 3.0 sembrano avere tutte le caratteristiche per stravolgere il futuro prossimo della nostra società. Ma facciamo un passo indietro.

3.1 Internet of Value e Web 3.0

In principio, vi era l'Internet dell'informazione, il cosiddetto Web 1.0, che era formato da una serie di portali e siti web che riportavano e pubblicavano principalmente informazioni. I contenuti erano di natura statica, "only read web", gli utenti potevano solo usufruire passivamente delle informazioni, con limitate possibilità di interazione. Questa fase si è protratta fino ai primi anni 2000, quando con lo sviluppo di software e connessioni più veloci, si è passati a un Internet incentrato sull'utente, l'Internet della condivisione, detto Web 2.0. Il passaggio da "read-only" a "read-write" ha consentito di creare soluzioni in grado di interagire attivamente con l'utente, che è diventato così il protagonista di un Web su misura per lui. Da questo punto di vista, l'avvento dei social media è stato senza dubbio determinante per incrementare la partecipazione degli utenti, dando loro la possibilità di creare, condividere e commentare informazioni e contenuti. Grazie al Web 2.0 la base utenti si è allargata a tal punto da generare una mole enorme di dati molto preziosi per i colossi del Web. Lo studio di questi Big Data permette loro di influenzare i nostri comportamenti, attraverso pubblicità e servizi ad hoc per noi, sulla base delle nostre ricerche e delle nostre abitudini. Ed è in questo contesto che prende forma il Web 3.0.

Tale espressione è stata coniata dal web designer Jeffrey Zeldman agli inizi del 2006, in piena fase Web 2.0. Come si può facilmente immaginare, questo ha dato luogo ad un lungo dibattito tuttora acceso ed attuale. Basti pensare che oggi si parla già di Web 4.0 senza che il 3.0 sia effettivamente concluso, anzi. Il concetto di Web 3.0 si è evoluto nel tempo. Nato inizialmente come critica verso il Web 2.0, il 3.0 è stato spesso associato nel recente

passato all'idea alquanto criptica di Web semantico. Dovrebbe trattarsi di un potenziamento dell'attuale World Wide Web, per abilitare i computer a leggere e processare molte più informazioni, in base ad una logica più evoluta di quella corrente, per portare la qualità della ricerca ad un livello superiore. Non sappiamo ancora quanto questa idea sia effettivamente praticabile, né se sia così necessaria o rivoluzionaria. È per questo che, con l'arrivo di blockchain, il Web 3.0 ha cominciato ad assumere una connotazione totalmente diversa. La blockchain, infatti, presenta tutte le caratteristiche necessarie per contrastare molti difetti del Web 2.0, dei quali gli utenti sono sempre più consapevoli, attenti ed esigenti. Innanzitutto in termini di privacy, gli utenti di una blockchain sono gli unici proprietari dei dati: spetta a loro decidere quali dati condividere e con chi, in maniera chiara, trasparente e sicura. La decentralizzazione della blockchain inverte così il paradigma del Web 2.0, restituendo agli utenti la proprietà dei loro dati. Inoltre, per il processo di democratizzazione avviatosi con lo sviluppo di queste tecnologie, l'accesso alle risorse di blockchain è aperto a tutti, senza alcuna forma di censura o discriminazione.

Il Web 3.0 si configura, quindi, come un modello decentralizzato basato su due elementi fondamentali, che denotano un cambiamento radicale della gestione dei dati. Il primo riguarda il modo in cui i dati vengono raccolti: non più in maniera verticale, ovvero in modo tale per cui ogni applicazione possiede e gestisce i dati a sua disposizione, bensì in modo orizzontale, cioè attraverso delle blockchain che contengono dei dati specifici forniti dagli utenti stessi e ai quali le varie applicazioni hanno accesso. L'altro pilastro riguarda il valore dei dati, che viene remunerato attraverso un sistema volto a scardinare l'attuale economia dell'attenzione e ci proietta verso il cosiddetto Internet of value. Invece di estrarre valore dai dati dei loro utenti, le reti Web 3.0 ridistribuiscono valore creando delle opportunità per gli utenti. In questo modo i protocolli del Web 3.0 capovolgono essenzialmente la struttura di incentivi economici dell'internet di oggi, sulla falsariga della sopraccitata cripto-economia. Negli ultimi anni, abbiamo visto un'esplosione cambriana di applicazioni Web 3.0, dal prestito decentralizzato alle soluzioni di pagamento mobile, dai servizi di codifica video agli scambi pubblicitari decentralizzati. Questi progetti sono incentrati sugli individui, i quali mettono a disposizione le loro risorse per creare servizi e prodotti aperti, che non esisterebbero senza gli utenti. Il loro contributo è fondamentale per il successo delle applicazioni ed è per questo che la protezione degli utenti e dei loro dati diventa un principio imprescindibile. Se avranno successo, questi progetti potrebbero aprire la strada a nuovi business che proteggono i singoli utenti e permettono ai creatori di catturare valore dalle loro invenzioni. Il Web 3.0 - il nuovo internet - potrebbe rovesciare gli attuali modelli di business basati sulla pubblicità e restituire parte del valore creato agli utenti stessi, come ricompensa del loro contributo.

Tutto ciò è possibile grazie alle DApps, le applicazioni decentralizzate. Le app che utilizziamo abitualmente sono centralizzate, ovvero sono costruite su dei server di proprietà di una determinata azienda. Possono essere a pagamento o gratuite, ma in generale si mantengono grazie alla vendita degli spazi pubblicitari e dei dati degli utenti, che vengono gestiti per targetizzare l'advertising. Le DApps, invece, sono applicazioni eseguite su reti

decentralizzate peer to peer, su cui non vi è un "single point of failure", in quanto nessun singolo nodo ha il totale controllo della DApp. Il codice sorgente è di tipo open source e per evitare che vi siano tentativi di manomissione si utilizzano gli algoritmi del consenso e gli smart contract. Il contributo di tutti coloro che aiutano a mantenere in esecuzione una determinata DApp viene premiato attraverso dei criptoasset interni alla DApp stessa, che in genere possono essere spesi su quella DApp per ottenere dei particolari servizi. Ma anche gli utenti finali possono essere coinvolti attraverso degli incentivi di vario genere. Per comprendere meglio questo meccanismo di redistribuzione del valore nell'Internet of value, riportiamo due esempi particolarmente significativi.

Il primo è quello di Brave, un browser che fa della privacy e della protezione dati il suo principale punto di forza. In base alle preferenze dell'utente, Brave è in grado di bloccare qualsiasi pubblicità, annuncio, cookie e tracker. Se invece gli utenti decidono di guardare annunci e pubblicità, Brave distribuisce il 70% delle entrate derivanti da tali annunci direttamente agli utenti sotto forma di BAT, Basic Attention Token, un criptoasset che può essere speso su diverse piattaforme, oppure scambiato o convertito in valuta fiat sugli exchange che lo supportano. In questo modo Brave inverte il principio dell'economia dell'attenzione, remunerando gli utenti che scelgono di vedere le pubblicità. Per completezza, Brave ha dichiarato a febbraio 2021 di aver superato quota 25 milioni di utenti attivi al mese.

L'altro esempio è quello di Steemit, un social media che ricompensa gli utenti con il criptoasset Steem per pubblicare post, commentarli e condividerli. Vengono premiati anche i cosiddetti curatori che reagiscono ai post, poiché il loro contributo è fondamentale per combattere le fake news e mantenere sicuro l'ambiente. Anche in questo caso, quindi, il valore viene redistribuito agli utenti sulla base della loro partecipazione.

3.2 Protocolli e applicazioni

Come abbiamo visto in precedenza, la maggior parte delle DApps sono costruite sulla blockchain di Ethereum attraverso smart contract e protocolli. Il livello di protocollo (layer 3) è quello che stabilisce gli standard e le regole per governare specifici compiti o attività. In parallelo con le istituzioni del mondo reale, il livello di protocollo costituisce un insieme di principi e regole che tutti i partecipanti in una data industria hanno concordato di seguire come prerequisito per operare nel settore. I protocolli DeFi sono interoperabili, il che significa che possono comunicare tra loro per costruire un servizio o un'applicazione personalizzati. Il livello di protocollo fornisce liquidità all'ecosistema DeFi attraverso le principali attività che compongono il mondo DeFi. Di seguito la tabella stilata da DeFiPrime, piattaforma che presta servizi di analisi dei prodotti DeFi, riporta tutte le categorie dei protocolli che compongono il panorama DeFi:

Sulla base di quanto affermato all'inizio, ci soffermeremo solo sui progetti più innovativi dal punto di vista finanziario e quelli più rilevanti economicamente. Dal momento in cui abbiamo dichiarato a più riprese che la DeFi offre un'alternativa al settore bancario, senza però coinvolgere banche e altre istituzioni, analizzeremo come la DeFi sostituisce alcuni servizi essenziali offerti dalle banche tradizionali, quali, ad esempio, depositi e prestiti. Inoltre, come si può notare nella seguente figura, la piattaforma DeFiPulse ci mostra che i progetti più importanti per "Total Value Locked" (TVL), appartengono alle categorie di protocollo lending & borrowing (più propriamente detto "protocol for loanable funds") e decentralized exchange (DEXs), che esamineremo successivamente.

DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
1.	Maker	Ethereum	Lending	$9.87B	5.11%
2.	Aave	Ethereum	Lending	$9.19B	0.56%
3.	Compound	Ethereum	Lending	$8.00B	-8.25%
4.	Polygon	Ethereum	Payments	$6.33B	9.92%
5.	Curve Finance	Ethereum	DEXes	$6.02B	3.03%
6.	Uniswap	Ethereum	DEXes	$5.70B	3.82%
7.	InstaDApp	Ethereum	Lending	$4.99B	-4.32%
8.	yearn.finance	Ethereum	Assets	$3.36B	-19.92%
9.	SushiSwap	Ethereum	DEXes	$3.30B	4.19%
10.	Liquity	Ethereum	Lending	$2.33B	0.30%

(fonte: DeFiPulse, dati aggiornati al 20/05/2021)

3.3 Savings & staking

Iniziamo allora a vedere in che modo è possibile depositare una certa somma di criptoasset sulla DeFi per accrescere i propri risparmi e guadagnare degli interessi che sono ben più alti rispetto ai tassi odierni. D'altronde ricordiamo che quello di ottenere degli interessi maggiori rispetto alla finanza tradizionale è proprio uno degli obiettivi della DeFi. Ciononostante, occorre precisare che il concetto di conto deposito non è molto consono al mondo DeFi, poiché in linea di principio non ci dovrebbe essere alcun interesse a mantenere fermi i propri criptoasset in un conto deposito. Vi sono molti altri investimenti e opportunità più redditizi e con un rischio minore o uguale. Per questo motivo, per riprodurre tale servizio offerto dal banking tradizionale, vi sono diversi protocolli DeFi che hanno permesso di sviluppare piattaforme e DApps originali che, in alcuni casi, non si limitano a compiere la funzione di deposito, ma propongono delle soluzioni innovative che si integrano anche con altri protocolli DeFi, sfruttandone la loro interoperabilità.

In primo luogo, come si può facilmente intuire, il protocollo che rimane più fedele alla versione originale dei depositi bancari è senza dubbio quello degli "alternative savings". Tra i progetti più interessanti in questo ambito menzioniamo Dharma, una piattaforma basata sulla blockchain di Ethereum che mette in comunicazione il tuo portafoglio di criptoasset col tuo bank account tradizionale, attraverso i principali exchange decentralizzati come Uniswap o DApp di lending & borrowing come Compound, che vedremo in seguito. Attraverso Dharma è possibile anche collegare la propria carta di credito per depositare la somma desiderata e convertirla in stablecoin su cui matureranno gli interessi, che possono arrivare fino a un Annual Percentage Rate (APR) del 7%.

Un'altra piattaforma che funziona in modo analogo, ma con un maggior grado di decentralizzazione, è Linen. A differenza di Dahrma, Linen è completamente svincolato dalla finanza tradizionale e il tasso di interesse viene calcolato automaticamente attraverso l'algoritmo di Compound che si basa sulla domanda di prestiti e crediti. Ci sono stati picchi di APR tra il 6% e il 7% e minimi intorno allo 0,4%.

In generale, si può affermare che i tassi di interesse sui depositi siano comunque superiori a quelli offerti dal settore bancario tradizionale, poiché la struttura dei costi è molto più snella, sia in termini di costi del personale e di infrastruttura, sia per quanto riguarda i costi di transazione e di gestione del cliente. Tuttavia, la funzione di alternative savings può comportare dei rischi elevati dovuti principalmente all'interazione con altri protocolli da cui dipendono queste piattaforme. Sembrerebbe più ragionevole investire direttamente su Compound anziché passare da altre piattaforme che risulterebbero solamente più complesse e rischiose, e meno trasparenti. È per questo motivo che agli alternative savings si affiancano altri protocolli che si sposano meglio con la filosofia decentralizzata della DeFi.

Un protocollo simile, ma molto più congeniale all'ecosistema DeFi, è ad esempio quello dello "staking". Lo staking è uno dei casi d'uso della DeFi più semplici ed è spesso uno dei primi modi in cui molti possessori di asset digitali si espongono alla finanza decentralizzata. Questo servizio supporta le blockchain che utilizzano l'algoritmo Proof-of-Stake (PoS), attraverso delle infrastrutture come *staking pool* o *staking as a service*: gli utenti depositano i propri criptoasset in questi fondi, fornendo la liquidità necessaria per partecipare al meccanismo del consenso tramite PoS, e in cambio ricevono degli interessi su quei fondi come ricompensa per il loro contributo. Avevamo riscontrato tra i limiti del PoS proprio il costante bisogno di liquidità, indispensabile per avviare il sistema di validazione. Questo servizio non solo riesce a mitigare questa problematica incentivando la partecipazione, ma somiglia a tutti gli effetti ad un conto deposito in una banca tradizionale, poiché consente a chiunque di far maturare gli interessi sui propri "depositi" partecipando allo staking.
Le principali piattaforme di staking funzionano più o meno tutte allo stesso modo, le uniche differenze riguardano le blockchain supportate e i tassi di interesse offerti, che possono raggiungere dei livelli notevoli, in base alle dimensioni del blocco da validare. Tuttavia questo servizio risulta essere piuttosto limitato in quanto il PoS non è ancora così diffuso, né sicuro. I principali rischi dei protocolli di staking sono gli stessi dell'algoritmo del PoS e riguardano quindi l'effettivo grado di scalabilità, sicurezza, decentralizzazione e il rischio di un attacco del 51%. Gli interessi così alti sullo staking sono proprio dovuti principalmente ai limiti e all'incertezza del PoS al suo stato attuale.

3.4 Asset management

A proposito di rendimenti elevati non possiamo non citare uno dei progetti più interessanti del panorama DeFi nell'ambito dell'asset management: Yearn.Finance (YFI). Lanciato sul mercato a luglio 2020, in meno di un anno Yearn.Finance ha raccolto oltre 3 miliardi di dollari, entrando così nella top ten delle piattaforme DeFi più grandi al mondo. Si tratta di una *suite* di prodotti DeFi che consente l'aggregazione di prestiti e la generazione di rendimenti elevati sulla blockchain di Ethereum. L'attività principale che è possibile attuare attraverso questi prodotti è il cosiddetto "yield farming", un metodo utilizzato dagli investitori per guadagnare dei rendimenti più elevati del normale investendo i propri criptoasset: a un eventuale apprezzamento del valore di mercato dei criptoasset si aggiungono gli interessi maturati sui criptoasset investiti. Finora sembrerebbe molto simile ai protocolli sopra descritti. Tuttavia, mentre nei depositi o nello staking si stanziano delle risorse che restano ferme nel tempo, le principali strategie di yield farming consistono nel monitorare le varie piattaforme e DApps sul mercato DeFi per investire in quelle che offrono un ritorno migliore. Questo metodo risulta, quindi, piuttosto complesso e rischioso: bisogna stare sempre in allerta per evitare dei crolli improvvisi o delle mancate opportunità di guadagno. Ovviamente, è necessaria una certa esperienza per muoversi nel mercato DeFi con notevole agilità e destrezza, poiché passare da una piattaforma all'altra comporta dei costi all'entrata e all'uscita e tutto ciò potrebbe rivelarsi inefficiente. Yearn.Finance ci permette di risolvere questo problema attraverso il suo protocollo

decentralizzato che è in grado di eseguire un fenomeno così complesso come lo yield farming in maniera automatica. Sostanzialmente, Yearn.Finance riesce ad individuare autonomamente i protocolli più redditizi del momento tra quelli a sua disposizione, per poi investirci i criptoasset depositati dall'investitore. Tutto questo avviene attraverso i tre prodotti principali creati da YFI che sono: Vault, Earn e Zap.

I Vault sono dei capital pool che generano automaticamente il rendimento in base alle opportunità presenti sul mercato. I Vault consentono agli utenti di beneficiare dei vantaggi dello yield farming, automatizzando la generazione di rendimento e il processo di ribilanciamento, spostando automaticamente il capitale in base alle opportunità di mercato che si presentano. Gli utenti finali inoltre non hanno bisogno di avere una conoscenza approfondita dei protocolli sottostanti coinvolti, poiché avviene tutto in maniera autonoma e trasparente. Per questo motivo i Vault rappresentano una strategia di investimento passiva.

Earn è il primo prodotto lanciato da YFI ed è un aggregatore di prestiti. I fondi vengono allocati automaticamente tra tre delle principali piattaforme di lending dYdX, AAVE e Compound in base a come variano i tassi di interesse su questi protocolli. Gli utenti possono depositare in questi aggregatori di prestiti degli smart contract tramite la pagina Earn. Questo prodotto ottimizza completamente il processo di maturazione degli interessi per gli utenti finali per garantire che stiano ottenendo i più alti tassi di interesse del momento tra le tre piattaforme citate.

Sebbene Vault e Earn sembrino due prodotti molto simili, vi sono delle differenze importanti. La prima è che Earn supporta solo depositi per stablecoin e wBTC (la stablecoin di Bitcoin), mentre Vault supporta una gamma più ampia di attività, tra cui menzioniamo ETH, LINK e token LP. Di conseguenza, Earn distribuisce i fondi solo ad una manciata di protocolli di prestito, mentre Vault distribuisce i fondi ad una più vasta selezione di protocolli. Inoltre, le strategie Earn sono più o meno fisse e preimpostate, mentre delle nuove strategie Vault possono essere proposte dagli utenti e implementate attraverso un processo di voto, basato su un protocollo del consenso molto simile al PoS. Il risultato finale è che Vault ha generalmente un rischio e un rendimento più alto rispetto a Earn, a causa del coinvolgimento di più opzioni di yield farming.

Ma al di là delle varie differenze, il meccanismo in fin dei conti è analogo: i token che vengono depositati su Yearn.Finance, sono trasformati in yTokens, che vengono periodicamente ribilanciati automaticamente in modo da essere composti dai token dei servizi DeFi più redditizi. Gli yToken sono semplicemente rappresentazioni della liquidità fornita. Se un utente deposita DAI, riceverà yDAI in cambio. Tuttavia, l'importo depositato sarà diverso da quello rappresentato dagli yToken. Questo perché gli yToken rappresentano una quota di un pool, il cui valore è in continua evoluzione.

È in questo contesto che viene in aiuto il terzo prodotto, lo Zap, che permette agli utenti di fare "zapping" tra i diversi pool di liquidità disponibili su Curve.Finance, un exchange decentralizzato. Inoltre consente di fare trading su Curve.Fi per scambiare in modo facile e veloce token in cambio di stablecoin. Attualmente gli utenti possono utilizzare cinque stablecoin (BUSD, DAI, USDC, USDT, TUSD) e "zappingare" in uno dei due pool (y.curve.fi

o busd.curve.f) su Curve, oppure, in alternativa, in una delle cinque stablecoin di base. È un prodotto complesso, ma fondamentale per contrastare eventuali crisi di liquidità.

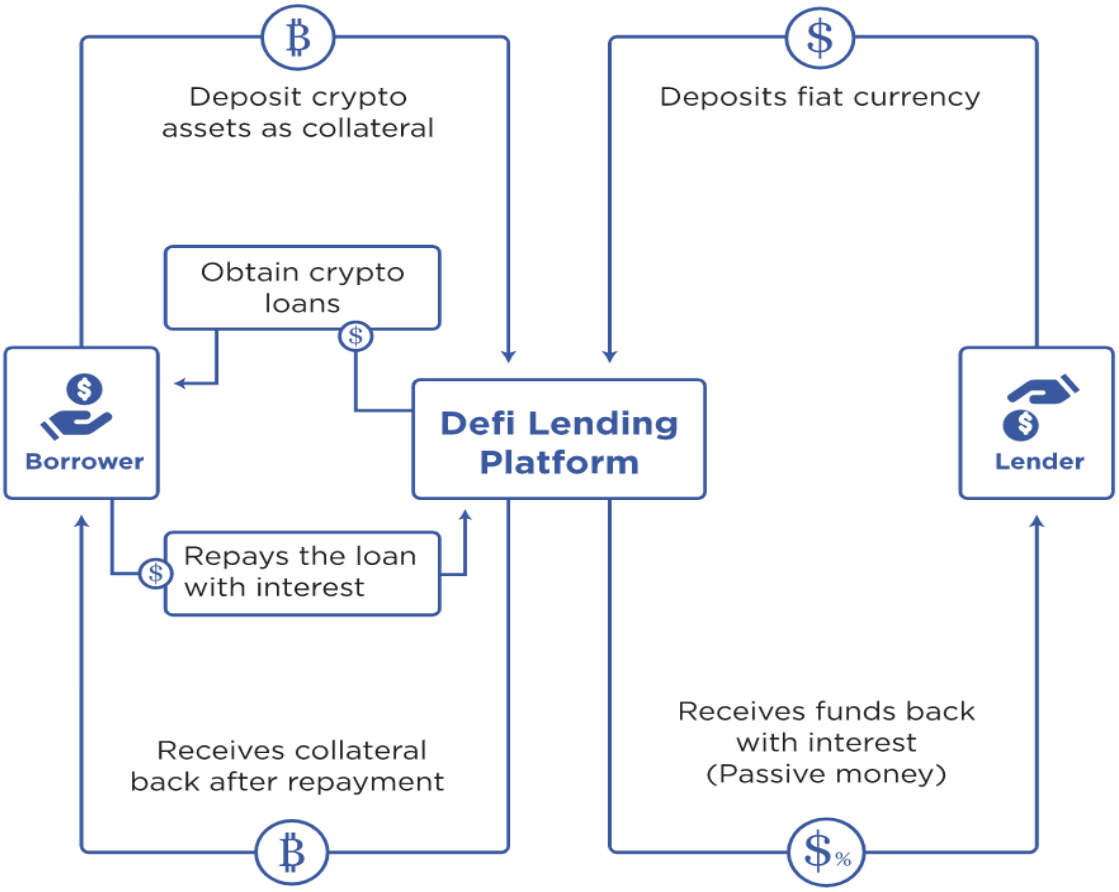
Per quanto possa essere affascinante, il fenomeno dello yield farming, anche se automatizzato, resta una pratica altamente rischiosa ed è per questo che offre un premio per il rischio così elevato. C'è il solito rischio di correlazione che esiste tra i vari token DeFi e gli altri protocolli: se un token crolla, la correlazione potrebbe far crollare l'intero castello di carte e rendere i token privi di valore. L'interdipendenza di queste piattaforme DeFi aumenta il rischio di componibilità in quanto la caduta di un token potrebbe portare alla caduta di altri token, compromettendo la stabilità delle piattaforme coinvolte. Pertanto, il fallimento di un protocollo di riferimento da cui dipendono molti token legati l'uno all'altro, causerebbe uno shock per tutti gli altri protocolli, contagiando anche il resto della DeFi. Da questo punto di vista, sarebbe un rischio assimilabile al rischio sistemico della finanza tradizionale.

3.5 Lending & borrowing

Fino a questo momento abbiamo sempre menzionato con riferimento ai protocolli precedenti, le piattaforme di lending & borrowing. Questo perché i prestiti sono una parte essenziale dell'ecosistema DeFi, come si può evincere dal fatto che tra le prime dieci piattaforme DeFi per Total Value Locked (TVL), cinque appartengono proprio alla categoria di lending & borrowing. Nel mondo DeFi, infatti, c'è una grande varietà di protocolli che permettono alle persone di prestare e prendere in prestito criptovalute, stablecoin e più in generale token di ogni tipo. Le piattaforme di prestito decentralizzate sono aperte a tutti, chiunque può accedere per prendere in prestito denaro o fornire liquidità per guadagnare interessi. Come tali, i prestiti DeFi sono completamente "senza permesso" e non dipendono da relazioni di fiducia. Non serve passare per lunghi iter burocratici per accedere a un mutuo o per ottenere un prestito, ma è possibile farlo direttamente tra individui peer to peer in modo decentralizzato, senza intermediari. A primo impatto può sembrare folle o eccessivamente rischioso, quindi analizzeremo come funziona questo protocollo e quali garanzie fornisce, alla luce del *modus operandi* delle principali piattaforme di questo settore.

Nella finanza tradizionale prima di erogare un prestito occorre instaurare un rapporto di fiducia: nessuno presterebbe denaro senza avere sufficienti garanzie per riaverlo indietro, possibilmente con gli interessi. Le piattaforme di prestito Defi hanno l'obiettivo ambizioso di offrire prestiti di criptovalute senza basarsi su un rapporto fiducia, cioè senza intermediari, per permettere agli utenti di mettere a disposizione i loro criptoasset per fornire liquidità al sistema. Un mutuatario può ottenere direttamente un prestito attraverso una piattaforma decentralizzata, nota come P2P lending. Allo stesso tempo, il prestatore può guadagnare interessi attraverso una sorta di yield farming passivo, senza sforzi e con rischi minori. La tecnologia blockchain consente alla DeFi di sfruttare tutte le sue caratteristiche, che si sposano perfettamente con l'esigenza di concedere credito a degli

sconosciuti, senza l'intervento di intermediari e autorità. Come abbiamo già visto nel secondo capitolo, la blockchain offre una completa trasparenza per poter trasferire denaro senza coinvolgere alcuna terza parte. Non serve sottoscrivere documenti lunghissimi che possono nascondere tra le pagine finali spiacevoli clausole che potrebbero rendere il prestito impossibile da rimborsare per il debitore. Questa tecnologia fornisce le garanzie necessarie in termini di sicurezza, grazie a strumenti crittografici avanzati e agli smart contract, che certificano l'immutabilità dei dati, mantenendo un ambiente accessibile a tutti e privo di censura o disparità di trattamento. Il prestito sulla DeFi offre dei benefici sia ai prestatori che ai prenditori, attraverso un servizio più veloce e democratico rispetto a quello tradizionalmente proposto dalle banche, permettendo ai prestatori di guadagnare tassi di interesse più elevati, e ai prenditori di accedere al credito più facilmente. Inoltre, a seconda delle preferenze e delle esigenze, gli utenti possono sfruttare le stablecoin per stabilizzare il valore dei criptoasset, ancorandoli ad esempio alla valuta fiat. La seguente immagine tratta da Leeway Hertz, impresa che si occupa dello sviluppo dei software, riassume molto chiaramente il procedimento del lending & borrowing decentralizzato e introduce un concetto chiave di questo settore: il collateral.



Quando si ottiene un prestito da una banca, sono sempre richieste delle garanzie associate a quel prestito. Per esempio, se si chiede un prestito per acquistare un'auto, l'auto stessa è una garanzia: se il cliente smette di pagare il prestito, la banca sequestra il veicolo. Lo stesso vale per il sistema decentralizzato, con la sola differenza che il

sistema è anonimo e non coinvolge alcuna proprietà fisica come garanzia. Per ottenere un prestito, il mutuatario deve offrire qualcosa di più prezioso dell'importo del prestito. Gli smart contract vengono utilizzati per depositare questa quantità di valuta per un valore maggiore rispetto all'importo del prestito. Le garanzie sono disponibili in un'ampia varietà, poiché qualsiasi token può essere utilizzato come collateral. Dal punto di vista tecnico, per proteggere il prestatore e impedire che il debitore scappi con i soldi, ci sono due approcci distinti: il primo si basa sul concedere un credito sotto la condizione che il prestito deve essere rimborsato atomicamente, ovvero l'esecuzione deve essere o totale o nulla, mai parziale; mentre il secondo approccio, più diffuso e affermato, consiste nel concedere prestiti solo se completamente garantiti da un collaterale.

Nel primo caso il mutuatario riceve i fondi, li usa e li ripaga, tutto all'interno della stessa transazione blockchain. Supponiamo che il mutuatario non abbia restituito i fondi (più gli interessi) alla fine del ciclo di esecuzione della transazione. In questo caso, la transazione non sarà valida e tutti i suoi risultati (incluso il prestito stesso) saranno annullati. Questi sono i cosiddetti prestiti flash e sono un'applicazione molto interessante, ma ancora altamente sperimentale. I prestiti flash possono essere impiegati solo in applicazioni che sono regolate atomicamente e interamente on-chain e questo li rende uno strumento efficiente per l'arbitraggio e la ristrutturazione del portafoglio. Per questo motivo i prestiti flash hanno tutte le potenzialità per diventare una parte essenziale dei prestiti DeFi, ma attualmente sono troppo rischiosi. I prestiti flash consentono di prendere in prestito una grande somma di denaro senza alcuna garanzia, per sfruttare le opportunità di arbitraggio. Fondamentalmente, si approfitta dell'illiquidità dei DEXs utilizzando strategie di trading per gonfiare i prezzi degli asset su cui speculare per guadagnare così profitti immediati.

Nel secondo caso, invece, il collaterale è bloccato in uno smart contract e viene rilasciato solo quando il debito viene rimborsato. Le piattaforme di prestito collateralizzato esistono in tre varianti: *collateralized debt position* (CDP), *pooled collateralized debt markets* e *P2P collateralized debt markets*. La differenza tra le posizioni di debito collateralizzate e i mercati del debito è che le prime implicano l'utilizzo di nuovi token appositamente creati, mentre i mercati del debito utilizzano token già esistenti e richiedono, quindi, una perfetta corrispondenza tra domanda e offerta di credito.

Per quanto riguarda le CDP, gli utenti possono creare posizioni di debito collateralizzate ed emettere nuovi token da prendere in prestito. Per poter creare questi token, l'utente deve bloccare come garanzia dei criptoasset in uno smart contract. Il numero di token che possono essere creati dipende da tre elementi: il prezzo target dei token generati, il valore dei criptoasset che vengono utilizzati come garanzia e il rapporto di collateralizzazione obiettivo. I token creati sono essenzialmente prestiti completamente collateralizzati che non richiedono una controparte e permettono all'utente di ottenere liquidità mantenendo l'esposizione al mercato attraverso la garanzia. Il prestito può essere utilizzato per il consumo, permettendo alla persona di soddisfare il suo bisogno di liquidità o per acquisire ulteriori criptoasset per sfruttare la leva finanziaria.

Per illustrare il concetto, approfondiamo l'esempio fatto in precedenza per la stablecoin di MakerDAO, il protocollo decentralizzato che viene utilizzato per emettere appunto i Dai. Nella classifica di DeFiPulse, Maker si trova al primo posto per TVL, a testimonianza del fatto che svolge un ruolo chiave per l'ecosistema DeFi, come se fosse una banca decentralizzata. Vediamo allora più nello specifico come funziona Maker, quali servizi e opportunità offre, e quali sono i suoi limiti e rischi allo stato attuale. In primo luogo, l'utente deposita ETH in uno smart contract classificato come posizione di debito collateralizzato (CDP). Successivamente, ha luogo l'esecuzione del contratto per creare e ritirare un certo numero di Dai e bloccare gli ETH depositati come garanzia. Questo processo attualmente richiede un rapporto di collateralizzazione minimo del 150%, il che significa che per ogni 100 USD di ETH bloccati nel contratto, l'utente può creare al massimo 66,66 Dai. Questo meccanismo di over-collateralization serve per stabilizzare il Dai, cercando di mantenere la parità col dollaro nonostante l'elevata volatilità del mercato.

Per chiudere un CDP ed estinguere il prestito, il debitore deve restituire i Dai ricevuti in prestito più gli interessi maturati e le commissioni di stabilità. Lo smart contract sottoscritto permette di effettuare tutto ciò in maniera automatica e decentralizzata, restituendo al debitore i fondi bloccati a garanzia solo una volta che il debito è stato ripagato. Se non riesce a ripagare il debito, o se il valore del collaterale scende sotto la soglia del 150%, il prestito è a rischio e lo smart contract inizierà a liquidare il collaterale ad un tasso potenzialmente scontato, il Dai Saving Rate (DSR) e il debitore perde così i fondi posti a garanzia. Il DSR è un tasso variabile che serve a stabilizzare il mercato di Dai adeguando autonomamente la domanda all'offerta, in funzione dei token Maker (MKR) in circolazione. I pagamenti degli interessi e le commissioni di liquidazione sono parzialmente utilizzati per "bruciare" MKR, diminuendo così l'offerta totale di MKR. In questo modo l'MKR si apprezza e in cambio i detentori di MKR si assumono il rischio residuo di shock estremi negativi del prezzo dell'ETH, che possono portare a una situazione in cui il collaterale è insufficiente a mantenere il vincolo di stabilità col dollaro. In questo caso, nuovi MKR saranno creati e venduti ad un tasso scontato. Dal momento in cui i titolari di MKR si assumono tale rischio, dovrebbe essere nel loro interesse mantenere un sistema sano.

I principali limiti e rischi di questo sistema sono quelli che avevamo già individuato in precedenza: l'impossibilità di poter diversificare i criptoasset utilizzati come collateral e l'inefficienza dell'accesso al capitale causato dall'over-collateralization. Per risolvere almeno parzialmente tali questioni, MakerDAO ha già annunciato recentemente il passaggio ad un sistema multi-collaterale, con l'obiettivo di rendere il protocollo più scalabile permettendo di mettere come garanzia una varietà più ampia di criptoasset.

Per quanto concerne i mercati del debito collateralizzato, invece, non è possibile creare nuovi token, ma solo prendere in prestito criptoasset già esistenti messi a disposizione da qualcun altro. Per ovvie ragioni, questo approccio richiede di dover incontrare una controparte con preferenze opposte. In altre parole, affinché qualcuno possa prendere in prestito ETH, ci deve essere un'altra persona disposta a prestare ETH. Per mitigare il rischio di

controparte e proteggere il prestatore, i prestiti devono essere completamente garantiti, e il collaterale è bloccato in uno smart contract, proprio come nel caso precedente.

L'incontro tra domanda e offerta, cioè tra prestatori e mutuatari, può avvenire in vari modi. Le principali categorie sono due: il P2P e i pool. L'abbinamento P2P significa che la persona che fornisce la liquidità presta i criptoasset a specifici mutuatari. Di conseguenza, il prestatore inizierà a guadagnare interessi solo quando riuscirà a trovare qualcuno a cui prestare i propri criptoasset. Il vantaggio di questo approccio è che le parti si accordano privatamente stipulando uno smart contract con cui vengono stabiliti i tempi e le modalità di restituzione della somma, e i tassi di interesse sono fissi.

I prestiti in pool, invece, utilizzano tassi d'interesse variabili che dipendono dalla relazione tra domanda e offerta. I fondi di tutti i mutuatari sono aggregati in un unico pool di prestiti basato su smart contract e i prestatori iniziano a guadagnare interessi quando depositano i loro fondi nel pool. I tassi di interesse sono una funzione del tasso di utilizzo del pool: quando la liquidità è prontamente disponibile, i prestiti saranno economici; quando invece è molto richiesta, i prestiti diventeranno più costosi. I pool di prestiti hanno quindi il vantaggio di essere generalmente più liquidi e più flessibili.

Nel mondo DeFi esiste una grande varietà di protocolli di prestito appartenenti a quest'ultima categoria. Alcuni dei più popolari sono Aave e Compound, che infatti si collocano rispettivamente al secondo e al terzo posto della classifica di DeFiPulse in base al TVL. Si tratta di due piattaforme molto simili basate sulla blockchain di Ethereum. Entrambe concedono prestiti in pool a tassi di interesse calcolati tramite un algoritmo in base a domanda e offerta di liquidità. Attualmente possiamo affermare che Aave è più flessibile, in quanto offre più possibilità a livello di asset coinvolti e modalità di prestito. Tuttavia, la competizione e la velocità di innovazione sono talmente elevate, che è difficile prevedere gli sviluppi futuri.

Quel che è certo è che i servizi DeFi di lending & borrowing sono tra i più interessanti nel panorama DeFi e offrono delle alternative particolarmente valide rispetto alla finanza tradizionale. Tuttavia, se da un lato è innegabile che favoriscano l'accesso al credito, accelerino i tempi per l'erogazione dei prestiti e rendano l'intero processo molto più snello e trasparente rispetto alla finanza tradizionale, dall'altro lato è altrettanto vero che i rischi relativi a tali pratiche sono piuttosto elevati, così come i rendimenti. Il rischio principale riguarda proprio l'utilizzo del collateral e l'intero sistema di garanzie: in caso di momentanei crash del mercato cripto o di continua volatilità negativa, si potrebbe abbassare notevolmente il rapporto di collateralizzazione mettendo potenzialmente a rischio l'intera piattaforma. Supponiamo, ad esempio, che un utente blocchi ETH come collateral in un contratto MakerDAO per emettere stablecoin Dai. Ipotizziamo, inoltre, che i Dai siano bloccati in uno smart contract per un prestito su Compound, in modo da far maturare gli interessi su un nuovo token, detto cDai. I token cDai vengono successivamente spostati in un pool di liquidità su UniSwap ETH/cDai, insieme ad alcuni ETH, permettendo all'utente di ritirare token UNI-cDai che rappresentano una quota del pool di liquidità. Al crescere

degli smart contract sottoscritti, il rischio potenziale aumenta. Se uno qualsiasi degli smart contract coinvolti in questa sequenza fallisce, i token UNI-cDai potrebbero potenzialmente diventare senza valore. Questi scenari danno origine ai cosiddetti token "wrapper", cioè la costruzione artificiosa di un token sopra all'altro, che crea delle interdipendenze che possono complicare i progetti, compromettendone la trasparenza e la validità, ma soprattutto li espongono a dei rischi finanziari molto alti. Se la DeFi continua a crescere facendo affidamento su un protocollo di riferimento come quello di MakerDAO, nel caso in cui il Dai fallisse, questo esporrebbe tutte le piattaforme e DApps che si basano sul Dai a rischio fallimento. A causa della cosiddetta "evaporazione del collateral", che provocherebbe una crisi di liquidità per il Dai, molte posizioni sulle piattaforme di lending potrebbero risultare scoperte e fallire per via del fallimento di altre piattaforme. Questo rientra nel rischio di componibilità menzionato in precedenza, che a seconda della portata della crisi e del numero di piattaforme coinvolte, potrebbe sfociare in un rischio sistemico.

3.6 Decentralized Exchange: DEXs

Con exchange decentralizzati (DEXs) si intende una tipologia di exchange in cui vengono eseguite le principali operazioni di un exchange tradizionale in maniera decentralizzata e "non custodial", ovvero le chiavi private dei portafogli restano sotto il controllo degli utenti. Ad oggi, maggio 2021, esistono più di 10.000 criptovalute quotate in borsa, per un market cap complessivo di circa €1,15 T. Ma mentre la maggior parte di esse ha un valore economicamente irrilevante in termini di market cap e volume di scambi, per quelle più diffuse c'è bisogno di un marketplace dove le persone possano comprare e vendere in sicurezza. Questo permette ai proprietari di tali asset di riequilibrare l'esposizione secondo le loro preferenze in termini di rischio/rendimento per ottimizzare le allocazioni di portafoglio.

Attualmente, gli scambi di criptoasset sono condotti prevalentemente attraverso exchange centralizzati. Gli exchange centralizzati sono relativamente efficienti e forniscono un punto di incontro tra domanda e offerta, tra il mondo blockchain e quello tradizionale. Hanno infatti il grande vantaggio di essere più familiari per gli utenti, più facili e intuitivi da utilizzare. Inoltre, consentono di effettuare diverse tipologie di ordini, dagli stop loss al trading automatico, oltre ad agevolare il margin trading, qualora l'utente voglia esporsi ad un maggior rischio per cercare rendimenti più alti. Infine, possiamo dire che non presentano alcun difetto in termini di velocità e scalabilità, poiché sono in grado di supportare un gran numero di richieste ed operazioni. Tuttavia hanno un grave problema: per essere in grado di negoziare su un exchange centralizzato, i trader devono prima depositare i loro criptoasset presso l'exchange, affidandogli le chiavi private del proprio portafoglio. In questo modo gli utenti perdono l'accesso diretto ai loro beni e devono fidarsi dell'operatore di borsa. Gli operatori di borsa disonesti o non professionali potrebbero gestire in maniera errata gli asset. Inoltre, gli scambi centralizzati hanno per definizione un single point of failure e ciò li espone costantemente alle minacce di attacchi hacker da parte di terzi

malintenzionati. Infine, il controllo normativo relativamente basso intensifica entrambi i problemi e ci sono stati numerosi casi di account bloccati senza un valido motivo. Di conseguenza, non è una sorpresa che alcuni exchange centralizzati di criptovalute abbiano perso i fondi dei clienti che hanno avvertito l'urgenza di una maggior trasparenza.

I protocolli di scambio decentralizzati cercano di mitigare queste problematiche rimuovendo il requisito della fiducia. Gli utenti non devono più depositare i loro fondi su un exchange centralizzato, bensì rimangono in controllo esclusivo dei loro criptoasset durante l'intero processo delle operazioni di trading. L'esecuzione di tali operazioni finanziarie avviene atomicamente attraverso uno smart contract, il che significa che sono eseguite in una transazione indivisibile, mitigando il rischio di credito della controparte. A seconda delle modalità di implementazione, lo smart contract può assumere ruoli aggiuntivi, rendendo effettivamente obsoleti molti servizi offerti dagli intermediari, come i servizi di deposito a garanzia e le stanze di compensazione della controparte centrale (CCP). La trasparenza intrinseca garantita dalla tecnologia blockchain rende l'ambiente più sicuro e resistente ad eventuali tentativi di manipolazione del mercato. Basti pensare al fenomeno del *wash trading*, attraverso il quale vengono effettuate numerose operazioni di compravendita al solo scopo di generare dei volumi fittizi. Così facendo si dà l'impressione che ci sia un mercato in fermento e in questo modo si giustificano determinati livelli di prezzo che sono in realtà artificiali. Secondo uno studio di TokenInsight, su 24 exchange centralizzati solo quattro dichiarano i volumi effettivi; dei restanti, dieci falsificano i loro volumi addirittura fino al 70%, mentre gli altri dieci alterano circa il 50% dei volumi. Lo studio è stato ulteriormente approfondito e certificato anche da altri autori, testimoniando l'inaffidabilità di alcuni exchange centralizzati per mancanza di trasparenza. Tuttavia, si potrebbe obiettare che nulla vieta di fare wash trading anche sulle piattaforme decentralizzate DEXs. Infatti, un articolo di due ricercatori dell'Università tecnica di Berlino ha riscontrato l'esistenza di tale fenomeno anche in alcuni DEXs, in particolare su due piattaforme: EtherDelta e IDEX. A tal proposito, però, è doveroso precisare alcuni limiti e debolezze di questo studio. In primo luogo, mentre negli exchange centralizzati sono le piattaforme stesse a influenzare il mercato riportando dati falsati, nel caso di EtherDelta e IDEX sono stati gli utenti ad effettuare operazioni di mercato ingannevoli. Ma questo fa parte delle speculazioni fraudolente che avvengono quotidianamente anche sui mercati tradizionali sotto gli occhi delle autorità vigilanti. Inoltre, questo studio non prende in considerazione tutte le tipologie di DEXs, ma esamina solo due piattaforme dello stesso tipo che, peraltro, non rappresentano più i DEXs moderni: si tratta di una piattaforma ormai obsoleta (EtherDelta) e un'altra (IDEX) che da quando è stata aggiornata nel 2019 ha ridotto drasticamente il fenomeno del wash trading, grazie all'integrazione di protocolli Know Your Customer (KYC) che hanno introdotto un maggior controllo sulla verifica delle identità digitali nel mondo cripto. Non è un caso, infatti, che queste piattaforme non siano più tra i DEXs più utilizzati.

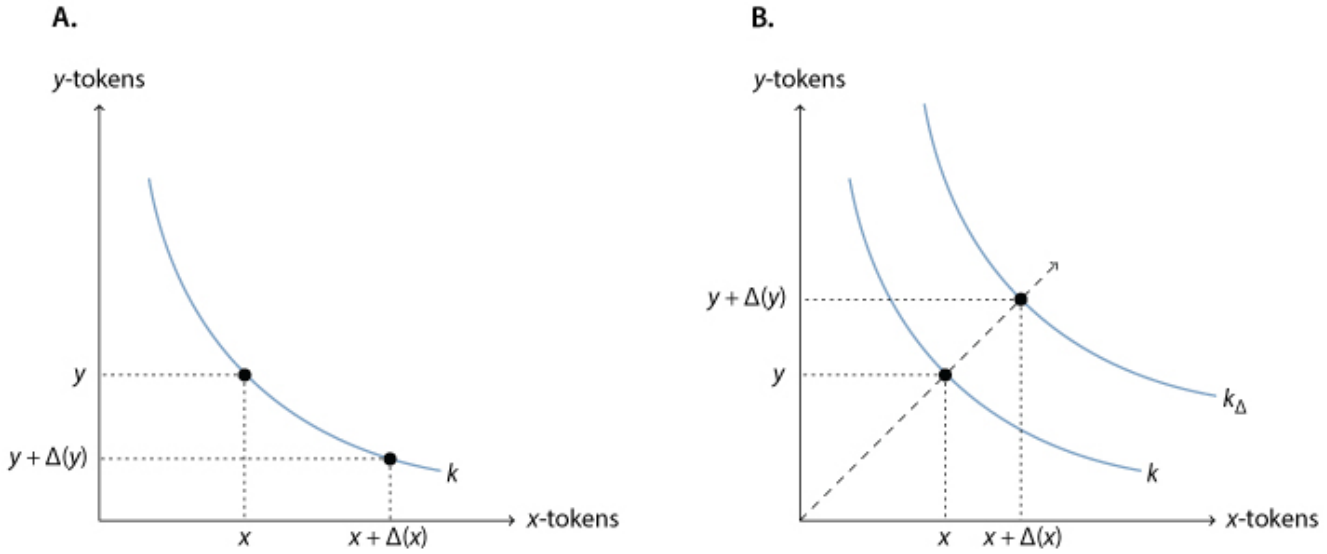
I primi exchange decentralizzati, come appunto EtherDelta, sono stati impostati in maniera rigida per compartimenti stagni, nel senso che erano isolati dal resto dell'ecosistema DeFi. Gli scambi non avevano liquidità condivisa, portando a volumi di transazioni relativamente bassi e grande divario tra domanda e offerta. Le alte commissioni di rete, così come i processi macchinosi e lenti per spostare i fondi tra questi exchange decentralizzati, hanno reso inutili le presunte opportunità di arbitraggio.
Più recentemente, invece, c'è stato uno spostamento verso protocolli di exchange aperti. Questi progetti cercano di semplificare l'architettura degli exchange decentralizzati fornendo degli standard su come realizzare gli scambi di asset attraverso pool di liquidità condivisi. In questo modo è stato possibile sfruttare l'interoperabilità dei protocolli DeFi, che sono stati integrati negli exchange per poter scambiare o liquidare token quando necessario, riequilibrando il sistema.
Analizziamo ora i vari tipi di protocolli di exchange decentralizzati, alcuni dei quali non sono tali in senso stretto, ma sono stati inclusi nell'analisi in quanto svolgono lo stesso compito.

La prima categoria è quella dei *decentralized order book exchange*, che sono caratterizzati dall'utilizzo di smart contract per il regolamento delle transazioni, ma differiscono significativamente tra loro per il modo in cui gli order book sono ospitati. All'interno di questa categoria, infatti, si distinguono due tipologie di order book: quelli on-chain, cioè ospitati su blockchain, e quelli off-chain.
Gli order book on-chain hanno il vantaggio di essere interamente decentralizzati. Ogni ordine è memorizzato all'interno di uno smart contract in maniera trasparente e automatizzata, non richiede, quindi, l'utilizzo di infrastrutture aggiuntive o di host esterni, forniti da terze parti. Lo svantaggio di questo approccio, però, è che ogni singola azione richiede una transazione blockchain. Pertanto, è un processo costoso e lento per il quale anche la sola dichiarazione dell'intenzione di iniziare a fare trading si traduce in commissioni di rete. Considerando la volatilità dei mercati, le cancellazioni di ordini sono piuttosto frequenti e questo svantaggio diventa ancora più costoso e marcato. Gli utenti devono pagare per ogni aggiornamento degli order book sulla rete, aspettare che la rete raggiunga il consenso sui loro aggiornamenti, e poi attendere la conferma sicura degli aggiornamenti. Di conseguenza, le blockchain più lente e con tariffe più alte sono meno favorevoli per ospitare un registro degli ordini on-chain.
Per questo motivo, molti protocolli di scambio decentralizzati si basano su order book off-chain e usano la blockchain solo come livello di regolamento. Gli order book off-chain sono ospitati e aggiornati da terze parti centralizzate, di solito chiamate *relayer*. Esse forniscono agli acquirenti le informazioni di cui hanno bisogno per selezionare l'ordine che vorrebbero piazzare. Sebbene questo approccio introduca effettivamente alcuni componenti e dipendenze centralizzate nel sistema, il ruolo dei relayer è molto limitato. I relayer non hanno mai il controllo dei fondi e non eseguono gli ordini. Si limitano solo a fornire delle liste ordinate con le relative

quotazioni aggiornate e possono addebitare una commissione per questo servizio. L'apertura del protocollo assicura che ci sia concorrenza tra i relayer e mitiga le potenziali dipendenze.

Il protocollo dominante che utilizza questo approccio è chiamato 0x. Gli scambi su questa piattaforma avvengono attraverso un processo formato da tre fasi. Nella prima fase, i maker inviano ordini di acquisto e vendita direttamente a un relayer, e il relayer aggrega tutti gli ordini ricevuti nel suo order book. Nel secondo step i taker scoprono gli ordini dei maker consultando gli order book del relayer. Infine, quando un taker trova un ordine soddisfacente, compilerà l'ordine inviando le informazioni richieste ai sensi del protocollo 0x tramite uno smart contract. Dato che tutti i relayer utilizzano il protocollo 0x per regolamento, un relayer può scegliere di condividere i suoi order book anche con altri relayer per avere maggiore liquidità, sbloccando così gli order book con più ordini. Chiaramente alla base di questo tipo di protocolli ci deve essere un certo grado di fiducia nei confronti del relayer, dal momento in cui si parla di un sistema ibrido, con un minor grado di decentralizzazione.

La seconda categoria riguarda i market maker automatici, più nello specifico i Constant Function Market Maker (CFMM). Si tratta di uno smart contract-liquidity pool che detiene come riserva almeno due criptoasset e permette a chiunque di depositare token di un tipo per poter ritirare token dell'altro tipo. Per determinare il tasso di scambio, i liquidity pool sono basati su degli smart contract che utilizzano delle variazioni del cosiddetto "costant product model", un modello in cui il prezzo relativo è espresso in funzione del rapporto di riserva di token depositati. La prima implementazione è stata proposta da Hertzog, Benartzi e Benartzi (2017). Adams (2018) ha semplificato il modello, mentre Zhang, Chen e Park (2018) hanno fornito una prova formale del concetto, che è stato successivamente approfondito anche da altri autori per verificarne la validità in casi complessi con più di due token. Nel nostro caso riportiamo la versione sintetica di Fabian Schär.



(Fabian Schär: Visualizzazione grafica del Liquidity Pool Token Reserves nel Constant Product Model)

Nella sua forma più semplice, il constant product model può essere espresso come $xy = k$, dove x e y rappresentano le riserve dei due tipi di token depositati negli smart contract, mentre k è una constante. Se vogliamo mantenere il rapporto costante, quando qualcuno effettua uno scambio, abbiamo

$$(x + \Delta x) \cdot (y + \Delta y) = k$$

Da cui si ottiene

$$\Delta y = (k/(x + \Delta x)) - y$$

Di conseguenza, Δy diminuisce per ogni $\Delta x > 0$, come si può facilmente evincere dall'andamento decrescente del grafico. Infatti, ogni scambio corrisponde a un movimento lungo la curva di riserva di token, che è appunto convessa, come mostrato nella figura di sinistra. Il liquidity pool utilizzato in questo modello non può esaurirsi, poiché i token diventeranno via via più costosi al diminuire delle riserve: quando l'offerta di uno dei due token tende a zero, il prezzo relativo tende all'infinito.

È importante sottolineare che i pool di liquidità basati su smart contract non si affidano a delle stime dei prezzi fornite da servizi esterni (i cosiddetti oracoli). Ogni volta che il prezzo di mercato di un bene si sposta, chiunque può utilizzare l'opportunità di arbitraggio e scambiare token con uno smart contract, fino a quando il prezzo del pool di liquidità converge al prezzo corrente di mercato. La differenza tra domanda e offerta implicita nel modello del prodotto costante (più una piccola commissione di trading) può portare all'accumulo di fondi aggiuntivi. Chiunque fornisca liquidità riceve dei token che rappresentano una quota del pool e gli permettono di partecipare al pool e di riscattare eventuali interessi proporzionali alla quota, attraverso un meccanismo autoincentivante. La fornitura di liquidità si traduce, infatti, in un k crescente ed è raffigurato nella figura di destra. Esempi importanti di protocolli di pool di liquidità basati su smart contract sono UniSwap, Balancer e Curve.

La terza categoria consiste nell'aggregare le riserve di liquidità attraverso uno smart contract che permette ai grandi fornitori di liquidità di connettersi e pubblicizzare i prezzi per delle specifiche coppie di scambio. Un utente che vuole scambiare il token x con il token y può inviare una richiesta di scambio tramite smart contract. Lo smart contract confronterà automaticamente i prezzi di tutti i fornitori di liquidità, accetterà la migliore offerta per conto dell'utente ed eseguirà lo scambio. Agisce come un gateway tra gli utenti e i fornitori di liquidità, garantendo la migliore esecuzione e la liquidazione completa.

Rispetto al caso precedente dei pool di liquidità basati su smart contract, con l'aggregazione delle riserve i prezzi non sono determinati all'interno dello smart contract, ma sono stabiliti dai fornitori di liquidità. In questo caso i prezzi non dipendono dalle riserve di token disponibili, bensì direttamente dai prezzi offerti dai fornitori di liquidità. Questo approccio funziona bene se c'è un'offerta relativamente ampia. Tuttavia, se c'è una concorrenza limitata o nulla per una data coppia di scambi, l'approccio può risultare rischioso e potrebbe sfociare in rischi di collusione o addirittura in una fissazione monopolistica dei prezzi. Come contromisura, i protocolli di aggregazione delle riserve di solito hanno alcuni meccanismi di controllo centralizzati, come prezzi massimi o un

numero minimo di fornitori di liquidità. In alcuni casi, i fornitori di liquidità possono partecipare solo dopo un determinato controllo, come ad esempio la verifica KYC (know your customer). L'implementazione più nota di questo modello è il Kyber Network.

In ultima analisi vi sono i protocolli peer-to-peer, chiamati anche protocolli over-the-counter (OTC), che forniscono un'alternativa ai classici modelli di exchange o di pool di liquidità. In genere si basano su un approccio a due fasi, dove i partecipanti possono cercare sulla rete le controparti che vorrebbero scambiare una data coppia di criptovalute e poi negoziare il tasso di cambio bilateralmente. Una volta che le due parti sono d'accordo su un prezzo, lo scambio viene eseguito on-chain tramite smart contract. Inoltre, si possono usare indicizzatori off-chain per trovare la controparte. Questi indicizzatori assumono il ruolo di una directory in cui le persone possono pubblicizzare la loro intenzione di fare uno scambio specifico. Si noti che questi indicizzatori servono solo a stabilire una connessione: i prezzi sono comunque negoziati P2P. AirSwap è l'implementazione più popolare di protocollo P2P decentralizzato.

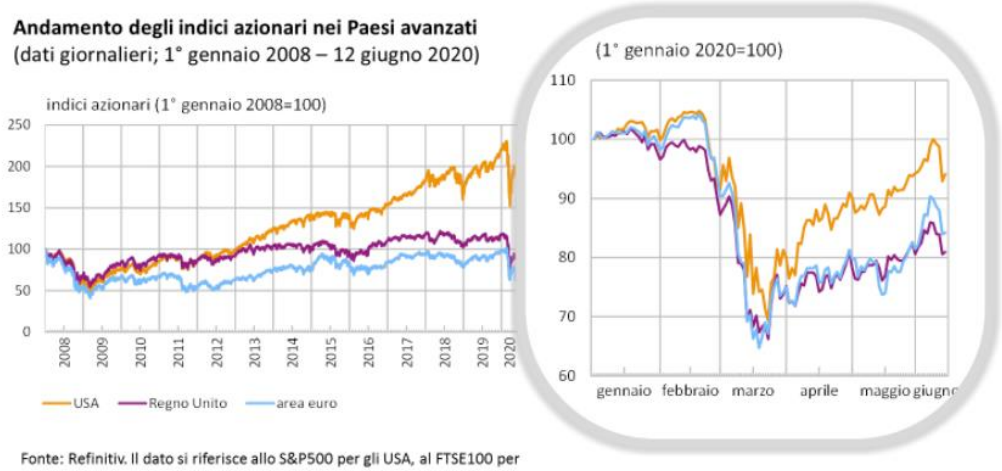
Possiamo concludere dicendo che gli exchange decentralizzati offrono un’alternativa valida nel mondo cripto soprattutto in termini di sicurezza, in quanto consentono agli utenti di mantenere le proprie chiavi private, restando in controllo dei loro criptoasset senza dover delegare la gestione di tali risorse agli exchange. Tuttavia, le principali criticità dei DEXs risiedono nelle eventuali crisi di liquidità, che possono rendere piuttosto complicato l’incontro tra domanda e offerta alla base del trading, e nella scalabilità, che può rallentare l’esecuzione delle varie operazioni. Ciononostante, ciascuna tipologia di DEX offre una soluzione diversa per cercare di mitigare questi problemi, fornendo una varietà di opportunità che ha attratto numerosi investitori.

4. Pandemia e crisi finanziaria: che impatto ha avuto il Covid sulla DeFi

È più di un anno ormai che stiamo affrontando una pandemia che ha sconvolto le vite di ognuno di noi, cambiando radicalmente le nostre abitudini e la nostra quotidianità. Individui, imprese e istituzioni si stanno riorganizzando per adeguarsi alle misure di prevenzione necessarie per contrastare gli effetti del Covid. Il virus ha contagiato diversi settori, dalla sanità all'istruzione, dal turismo al mondo dello sport, mettendo in ginocchio l'economia mondiale. Data l'attualità degli eventi, è doveroso sottolineare che ci sono numerose questioni tuttora irrisolte e che qualsiasi valutazione è basata su degli studi fondati su dati parziali, poiché in molti casi non si ha e non si può avere ancora il quadro generale della situazione. Analizzare un fenomeno durante la sua manifestazione è un compito particolarmente difficile, poiché la continua evoluzione dei dati e degli scenari ci porta a dover prendere delle decisioni in condizioni di totale imprevedibilità degli sviluppi futuri. Abbiamo assistito a un susseguirsi di teorie e opinioni, anche autorevoli, che in tempi brevi non sono più state ritenute valide o attendibili, poiché smentite proprio dalla mutevolezza della realtà. In questo periodo è tornata in voga l'espressione "vivere in un mondo VUCA", richiamando la teoria manageriale di Bennis e Nanus, che sottolinea la difficoltà di pianificare una strategia vincente in un ambiente caratterizzato da: volatilità (*volatility*), incertezza (*uncertainty*), complessità (*complexity*) e ambiguità (*ambiguity*). Il Covid è stato spesso associato anche al concetto di "cigno nero", riprendendo la teoria sviluppata dal matematico Nassir Taleb per descrivere l'impatto di eventi imprevedibili, che hanno degli effetti rilevanti e che solo in un secondo momento vengono razionalizzati in modo improprio e ritenuti prevedibili. L'obiettivo dell'autore non è cercare di prevedere eventi prevedibili, bensì tentare di costruire delle basi solide e robuste per mitigare eventuali shock negativi. A tal proposito, Taleb muove delle dure critiche al sistema finanziario, da lui considerato troppo fragile e vulnerabile in caso di "cigni neri". Sebbene molti studiosi, tra cui Taleb stesso, non condividano la scelta di associare il Covid a un cigno nero, poiché non lo reputano un evento così imprevedibile dal punto di vista teorico, le sue conseguenze pratiche sono talmente gravi e pervasive che lo si può ritenere un cigno nero a tutti gli effetti. Non è un caso, infatti, che i principali programmi stilati da istituzioni e imprese per pianificare la ripartenza economica contengano i termini "robustness" (robustezza) o "resilience" (resilienza), due parole chiave utilizzate da Taleb nel suo saggio. Questo a testimonianza del fatto che il fenomeno Covid ha messo in evidenza tutte le fragilità di un sistema economico-finanziario che non era pronto ad assorbire gli effetti negativi di uno shock di tale portata. Ecco come quella che inizialmente era una crisi sanitaria, è diventata presto una crisi economica: le misure precauzionali insufficienti hanno portato a un inevitabile lockdown che ha causato una crisi produttiva. L'interruzione della produzione ha determinato uno shock negativo dell'offerta al quale si è aggiunto anche un calo della domanda, provocato dalla riduzione dei consumi dovuta alla diminuzione del reddito disponibile. In questo contesto sono emerse tutte le caratteristiche di un ambiente VUCA, in cui regna l'incertezza e l'imprevedibilità, e ciò si traduce in una mancanza di fiducia che si è abbattuta sui mercati finanziari. La crisi finanziaria si è manifestata all'inizio come una crisi di liquidità, che

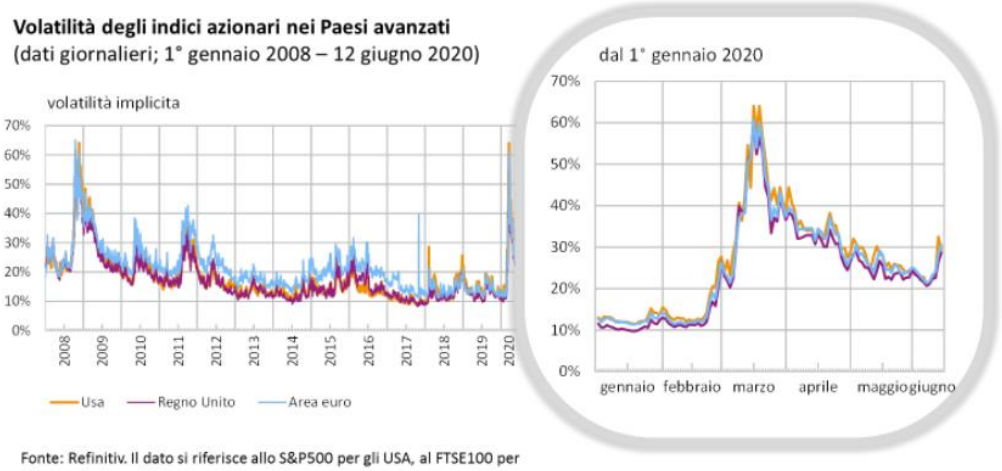
ha costretto la maggior parte delle economie sviluppate a intraprendere una politica monetaria espansiva. Ma l'andamento negativo dei mercati ha coinvolto anche le banche e i principali istituti di credito, che hanno subito un aumento del tasso di insolvenza, che ha portato ad una restrizione dell'erogazione di nuovi prestiti. La seguente immagine mostra il crollo e la volatilità dei mercati azionari nel periodo più acuto della crisi.

Andamento degli indici azionari nei Paesi avanzati
(dati giornalieri; 1° gennaio 2008 – 12 giugno 2020)



Fonte: Refinitiv. Il dato si riferisce allo S&P500 per gli USA, al FTSE100 per il Regno Unito e all'EuroStoxx50 per l'area euro.

Volatilità degli indici azionari nei Paesi avanzati
(dati giornalieri; 1° gennaio 2008 – 12 giugno 2020)



Fonte: Refinitiv. Il dato si riferisce allo S&P500 per gli USA, al FTSE100 per il Regno Unito e all'EuroStoxx50 per l'area euro.

4.1 L'impatto del Covid sui criptoasset

Cerchiamo di analizzare ora come hanno reagito i criptoasset e come si pongono rispetto al mercato tradizionale. Come da prassi, utilizzeremo Bitcoin come termometro per misurare il mercato dei criptoasset, poiché è l'unico che ha una capitalizzazione di mercato tale da poter essere confrontato con gli asset class tradizionali. Uno studio condotto da VanEck col supporto dei dati di Morningstar evidenzia tre aspetti fondamentali. Il primo è che il Bitcoin ha mantenuto per la maggior parte della sua storia una correlazione molto bassa con gli asset class tradizionali, prossima allo zero. La seguente tabella mette a confronto la correlazione che c'è tra Bitcoin e gli indici dei mercati azionari/obbligazionari e le commodities, come il petrolio e l'oro. Le dinamiche di prezzo del Bitcoin e i suoi elevati rendimenti, lo hanno storicamente reso uno strumento attraente per la diversificazione del

portafoglio.

Correlation 2/1/2012 to 12/31/2020	S&P 500	U.S. Bonds	Bitcoin	Gold	U.S. Real Estate	Oil	Emerging Market Currencies
S&P 500	–	-0.25	0.01	0.02	0.73	0.34	0.30
U.S. Bonds	-0.25	–	0.02	0.28	0.04	-0.15	0.10
Bitcoin	0.01	0.02	–	0.00	0.01	0.03	-0.01
Gold	0.02	0.28	0.00	–	0.09	0.08	0.27
U.S. Real Estate	0.73	0.04	0.01	0.09	–	0.20	0.29
Oil	0.34	-0.15	0.03	0.08	0.20	–	0.22
Emerging Market Currencies	0.30	0.10	-0.01	0.27	0.29	0.22	–

Source: Morningstar. Data as of 12/31/2020. US Bonds is measured by the Bloomberg Barclays US Aggregate Index; Bitcoin is measured by the MVIS CryptoCompare Bitcoin Index; Gold is measured by the S&P GSCI Gold Spot Index; U.S. Real Estate is measured by the MSCI US REIT Index; Oil is measured by the Brent Crude oil spot price, Emerging Market Currencies is measured by the Bloomberg Barclays EM Local Currency Government Index.

Un secondo elemento importante è dato da un'altra tabella che mette in evidenza come il coefficiente di correlazione tra Bitcoin e gli asset class tradizionali sia aumentato nel 2020, raggiungendo il suo picco più alto, pur restando basso in termini assoluti.

Calendar Year Correlation to Bitcoin	2020	2019	2018	2017	2016	2015	2014	2013
S&P 500	0.22	-0.09	0.04	-0.01	-0.01	0.01	-0.03	-0.12
U.S. Bonds	0.07	0.00	-0.03	0.04	0.04	-0.06	0.04	0.10
Gold	0.34	0.14	-0.02	0.01	0.07	0.04	-0.08	-0.04
U.S. Real Estate	0.17	-0.09	-0.03	0.04	-0.03	0.01	0.01	-0.10
Oil	0.23	0.02	0.00	0.06	0.03	0.00	0.00	-0.03
Emerging Market Currencies	0.25	-0.02	0.07	-0.04	-0.07	-0.04	-0.03	-0.07

Source: Morningstar

Questo aumento di correlazione può essere il risultato della diffusione e adozione di Bitcoin, come evidenziato dai volumi record di trading, l'aumento degli scambi OTC e un numero crescente di reti di pagamento che permettono l'acquisto e la vendita di Bitcoin e di asset digitali sulle loro reti.

Analizziamo allora l'andamento del Bitcoin durante la pandemia, distinguendo tre momenti principali: il crollo del mercato a marzo 2020, la ripresa dei mercati nella seconda parte del 2020 e i recenti sviluppi del 2021. Nelle

seguenti immagini abbiamo confrontato il Bitcoin (linea blu), con gli indici S&P 500 (linea gialla) e NASDAQ (linea azzurra), e con l'oro (linea arancione).

Durante la prima fase, si può notare come il Bitcoin sia l'asset che ha subito più duramente il crollo dei mercati, con picchi negativi del -60% circa. Male anche gli indici di mercato col NASDAQ che ha registrato un calo massimo del -16,68% e S&P 500 è arrivato fino a -19,65%. L'unico asset che ha attutito l'impatto negativo è stato l'oro, che ha riportato un minimo del -3,22%.

L'effetto panico si è abbattuto più duramente proprio sul Bitcoin, colpevole di non avere meccanismi di protezione tipici degli asset tradizionali, come la sospensione del titolo per eccesso di ribasso, oppure il divieto di vendite allo scoperto. Inoltre, non c'è nessuna autorità o istituzione centralizzata in grado di rassicurare i mercati o annunciare comunicati e iniziative per diffondere fiducia. Infine, se a ciò si aggiunge la possibilità per Bitcoin di fare trading 7 giorni su 7, si spiega l'elevata volatilità, con dei cali notevoli proprio nei fine settimana, quando i mercati tradizionali erano chiusi.

Tuttavia, nella seconda fase di ripresa dei mercati, Bitcoin ha mostrato grande resilienza, con delle performance di gran lunga superiori al resto dei mercati. Infatti, Bitcoin non solo ha recuperato molto velocemente i livelli pre-pandemia, ma ha addirittura raggiunto nuovi massimi, come si può notare in questo grafico che va da ottobre a dicembre 2020.

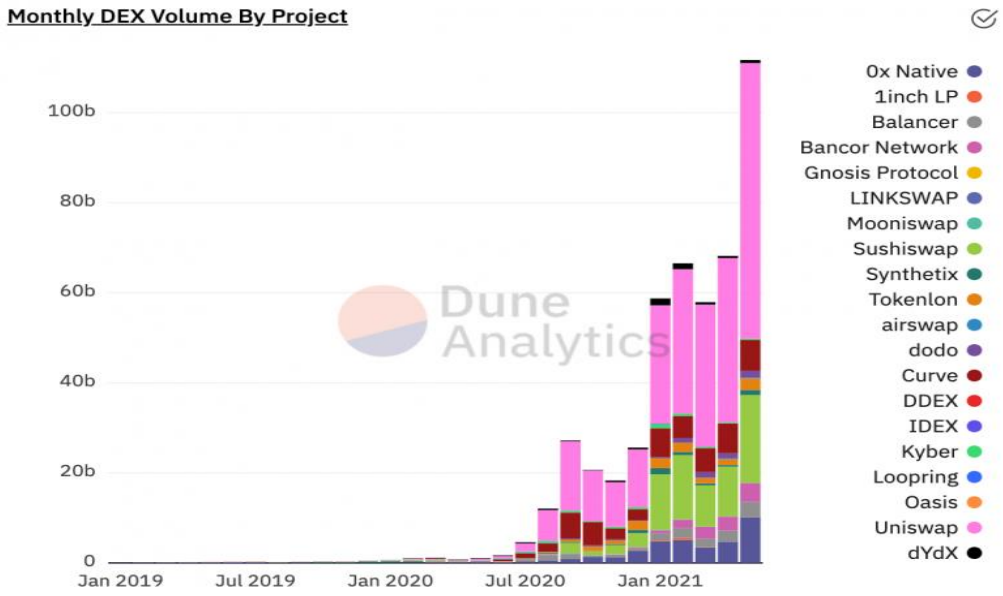
Non è una caso che un report di Goldman Sachs del 21 maggio 2021 inizi a considerare le criptovalute come un nuovo asset class. La stessa banca d'affari che fino a poco tempo fa sminuiva e ridicolizzava il settore dei criptoasset, adesso sta mostrando un maggiore interesse verso il mondo cripto, proprio alla luce della crescente capitalizzazione nonostante le recenti difficoltà.

La terza ed ultima fase in esame mostra gli sviluppi di Bitcoin nell'ultimo trimestre, da marzo a maggio 2021. In quest'ultimo mese, Bitcoin ha subito il peggior ribasso della sua storia, come si può osservare nel seguente grafico. Tutto ebbe inizio il 12 maggio, quando Elon Musk ha fatto dietrofront sulle sue precedenti dichiarazioni e ha annunciato tramite Twitter la sospensione della possibilità di pagare le auto Tesla in Bitcoin, poiché il mining tramite PoW è considerato troppo inquinante e poco sostenibile. Musk sembra esser rimasto sorpreso da questo fatto che è ormai alla luce del sole da tempo e lo abbiamo anche analizzato in merito ai limiti del PoW. Tuttavia, questo suo tweet ha scatenato una prima ondata ribassista, a cui si sono aggiunti altri due cali provocati dall'opposizione della Cina al mercato delle criptovalute. Stando a quanto riportato pubblicamente, il governatore della Banca popolare cinese ha tenuto una riunione con le principali istituzioni finanziarie cinesi per comunicare loro il divieto di fornire servizi con transazioni in criptovaluta e di effettuare qualsiasi attività di finanziamento legata alle criptovalute. Probabilmente lo scopo principale è quello di promuovere in futuro il renminbi digitale. Si è manifestato il cosiddetto rischio normativo, che tanto preoccupa gli investitori del mondo cripto. Consiste nel rischio che qualsiasi protocollo DeFi possa essere influenzato dai governi con leggi che limitano il funzionamento di un protocollo DeFi o con leggi che potrebbero addirittura chiudere o vietare i protocolli DeFi. Al di là delle

opinioni più disparate che sono state espresse in merito alla regolamentazione, i fatti ci suggeriscono che tale rischio sia reale ed è effettivamente in grado di influenzare la fiducia sui mercati, almeno nel breve periodo. Gli effetti di lungo periodo dipendono ovviamente dal tipo di regolamentazione che sarà adottata nei vari Paesi.

Le vendite da parte degli investitori cinesi sono state accolte come un chiaro segnale negativo dal mercato, che ha registrato la più grande ondata di vendite nella storia del Bitcoin, per un totale di 2,56 miliardi di dollari di perdite nette per i trader. Tuttavia, rispetto alle crisi precedenti, ci sono delle differenze importanti. In primo luogo i comportamenti delle varie categorie di trader sono state divergenti: uno studio de *Il Sole 24 Ore* ha dimostrato che mentre i piccoli risparmiatori vendevano in preda al panico, i grandi investitori ne hanno approfittato per comprare a prezzi scontati Oltre l'80% di coloro che hanno liquidato la loro posizione avevano comprato Bitcoin non più di sei mesi prima del crollo. Le vendite sono state effettuate prevalentemente da trader novizi e da trader indebitati. Questo scenario ha dato luogo a delle opportunità speculative, che hanno provocato un rimbalzo quasi immediato, come si può notare dall'andamento a "W" del grafico nella parte finale. Per completezza, riportiamo che in quest'ultima settimana di maggio 2021 il valore di Bitcoin sta oscillando intorno ai 36.000 dollari, ma con un Crypto Fear & Greed Index pari a 21/100, a testimonianza del fatto che la paura non è ancora passata e Bitcoin potrebbe scendere ulteriormente nel breve periodo. Come spesso accade nel mondo cripto, il trend ribassista di Bitcoin si è riversato anche su tutte le altre criptovalute, che stanno registrando dei cali notevoli in questo periodo. Nonostante ciò, un aspetto interessante che sta emergendo in questa crisi riguarda la *dominance* di Bitcoin: sebbene l'elevata volatilità renda particolarmente difficile effettuare un'analisi ciclica, alcuni analisti di mercato

sostengono che la struttura dell'ultimo ciclo della dominance di Bitcoin sia fortemente ribassista. Questo significa che tutte le altre criptovalute, le cosiddette altcoin, dovrebbero acquistare nel futuro prossimo un maggior potere nei confronti di Bitcoin e colmare almeno parzialmente un gap attualmente molto elevato in termini di market cap. Infine, una nota positiva in questo periodo buio per il mondo cripto riguarda gli attuali volumi scambiati, che sono di gran lunga superiori rispetto a quelli delle precedenti crisi, anche del crash di marzo 2020. Questo implica che ci sia stato un maggior assorbimento delle vendite da parte del mercato, che ha consentito di evitare ulteriori danni almeno nel breve periodo. Ovviamente, i volumi sono stati scambiati sugli exchange centralizzati e sui DEXs. Non a caso, proprio a maggio 2021 in piena crisi Bitcoin, i DEXs hanno registrato un totale di scambi per un valore record di oltre 10 miliardi di dollari, come rappresentato in questo grafico di Dune Analytics:



4.2 La reazione della DeFi

Analizziamo ora come ha reagito la DeFi alla prima vera crisi delle cripto da quando la DeFi è nata. Abbiamo esaminato il grado di correlazione tra Bitcoin e il resto degli asset tradizionali, e poi l'influenza di Bitcoin sul resto del mondo cripto. Cerchiamo di capire se c'è una correlazione anche con la DeFi e che tipo di impatto può avere Bitcoin sulla DeFi. Occorre premettere che uno studio del genere non è affatto semplice, in quanto non si può effettuare una comparazione diretta dei movimenti sul mercato di Bitcoin e della DeFi, che ha una struttura composita, formata da vari protocolli. Tuttavia, valuteremo i due momenti più significativi che mostrano le caratteristiche principali della relazione tra i due mercati.

A fine 2020, mentre Bitcoin registrava aumenti del +42,35%, molte DApps e piattaforme DeFi erano in netto calo. L'elevata volatilità che accomuna i due mercati portava gli investitori più esperti a sfruttare le opportunità di mercato: utilizzare gli alti rendimenti della DeFi per reinvestirli poi in Bitcoin, con ritorni potenzialmente ancora più elevati. Ciononostante, una delle peculiarità della DeFi è quella di offrire una vasta gamma di servizi

e protocolli, tale per cui all'interno della stessa DeFi è possibile diversificare per mitigare il rischio. Tra Bitcoin e Altcoin abbiamo visto che c'è una correlazione più evidente, che non offre molte opportunità di diversificazione, in quanto la dominance di Bitcoin è ancora significativa: nessun altcoin cresce quanto Bitcoin e se Bitcoin crolla tira giù anche le altcoin. Questo non vale per la DeFi, in cui al netto delle interdipendenze e interoperabilità dei protocolli, ogni protocollo ha un proprio andamento. Tale concetto diventa lampante se si analizza il recente crollo delle cripto di maggio 2021.

Come abbiamo ripetuto più volte, la maggior parte dei progetti DeFi è basato sulla blockchain di Ethereum e utilizza l'ETH come valuta di riferimento per eseguire transazioni sulla rete. Il recente ribasso di Bitcoin si è riversato su tutte le altcoin, Ether compresa. La maggior parte dei token DeFi ha rispecchiato l'elevata correlazione tra DeFi e ETH, che ha provocato un crollo del -42% del valore totale bloccato negli smart contract rispetto al picco massimo della DeFi. Ciononostante, ci sono stati tre elementi principali che hanno difeso la DeFi da un tracollo pari o peggiore di quello subito dal mondo cripto. Il primo riguarda un meccanismo analogo a quello descritto in merito al rialzo di Bitcoin a fine 2020: mentre in quel periodo il trend rialzista di Bitcoin portava gli investitori a spostare il proprio denaro dalla DeFi al Bitcoin, a maggio 2021 si è verificato il processo inverso. Il ribasso del Bitcoin ha spinto la comunità delle criptovalute a cercare alternative valide sulla DeFi, con gli investitori che hanno diversificato i loro portafogli speculando su promettenti progetti DeFi, acquistando token a prezzi scontati sui vari DEXs e reinvestendoli in strategie di yield farming sulle piattaforme di lending & borrowing. Il secondo aspetto, infatti, riguarda proprio i volumi di trading, con UniSwap leader assoluto del settore DEXs con circa 5.7 miliardi di dollari in volume di trading giornaliero nel momento di massima crisi. Inoltre, nonostante il crollo del mercato, le varie piattaforme decentralizzate hanno registrato un numero crescente di nuovi utenti proprio nel giorno del crash e nelle settimane a seguire. Infine, il terzo ed ultimo aspetto che ha rafforzato la DeFi durante la crisi riguarda le stablecoin. Nonostante la complessità e l'elevato livello di rischio intrinseco alla struttura delle stablecoin, queste ultime hanno reagito bene all'urto dei mercati, in particolar modo il Dai. L'offerta di Dai è riuscita ad autobilanciarsi perfettamente con la domanda e il meccanismo di over-collateralization ha consentito di mantenere stabile la parità col dollaro, nonostante le intemperie sui mercati. Si tratta di un risultato che non è stato affatto scontato, anzi. Durante il crollo di marzo 2020 il Dai non aveva dato gli stessi segnali di stabilità, mostrando evidenti problemi di scalabilità. Quando il prezzo di ETH è crollato del 43% in poche ore, molte CDP sono state liquidate poiché non rispettavano più il rapporto di over-collateralization. Le opportunità di arbitraggio sono state sfruttate al massimo dai trader esterni che hanno effettuato numerose operazioni che hanno congestionato la piattaforma per gli utenti interni. Molte posizioni sono state liquidate gratuitamente: 8,32 millioni di dollari in ETH sono stati venduti a fronte di offerte da 0 Dai, proprio perché gli utenti non riuscivano ad accedere per garantire ulteriormente le loro posizioni. Secondo il team di ricerca whiterabbit, su 3.994 transazioni di liquidazione, 1.462 (36,6%) sono state realizzate con uno sconto del 100%.

Ecco perché la performance del Dai durante il crash di maggio assume un significato ancora più importante, poiché a distanza di poco più di un anno, si è riusciti a migliorare la validità della piattaforma che ha assorbito un crollo addirittura maggiore di quello di marzo. Come avevamo anticipato, la scelta di accettare USDC come collaterale si è rivelata vincente e un multi-collateral Dai è senza dubbio la strada da seguire.

Conclusione

Attualmente la DeFi resta ancora una nicchia di mercato con ampi margini di crescita. Si presenta come alternativa alla finanza tradizionale, ma ovviamente per volumi e capitalizzazione non si può neanche pensare che possa essere in grado di soppiantarla. Tuttavia offre delle soluzioni concrete per creare un ambiente finanziario aperto a tutti, trasparente e immutabile, che non richiede alcun rapporto di fiducia con terze parti, intermediari e autorità. L'utilizzo della tecnologia blockchian e degli smart contract ha consentito di riprodurre i principali prodotti e servizi della finanza tradizionale in maniera decentralizzata. L'interoperabilità dei protocolli ha permesso lo sviluppo di strumenti innovativi e personalizzabili a seconda delle esigenze degli utenti. Tra le opportunità che hanno riscontrato il maggior successo ricordiamo i prestiti flash, l'introduzione delle stablecoin, lo yield farming automatizzato, i DEXs. Queste novità hanno avuto un impatto notevole nel mondo della finanza soprattutto in un periodo storico che a partire dalla crisi del 2008 ha visto crescere la sfiducia verso banche e intermediari finanziari. Il bisogno da parte degli investitori e dei risparmiatori di beneficiare di rendimenti più elevati, prestiti istantanei e transazioni più veloci ha trovato una risposta concreta in un ambiente accessibile e trasparente come la DeFi.

A fronte dei vantaggi e delle grandi potenzialità espresse dalla DeFi finora, si devono tener presente anche determinati rischi finanziari e non finanziari. I principali rischi finanziari sono gli stessi della finanza tradizionale, con particolare attenzione all'alta volatilità tipica del mondo cripto e alla pericolosità di eventuali crisi di liquidità, i cui effetti negativi possono essere più accentuati nella DeFi rispetto alla finanza tradizionale. Ma se da un lato gli elevati guadagni rispecchiano effettivamente un premio per il rischio, dall'altro lato molte opportunità nascondono delle insidie legate ai rischi non finanziari, che diventano particolarmente pericolosi soprattutto per gli utenti meno esperti. A tal proposito rammentiamo le vulnerabilità degli smart contract, che se scritti senza le opportune funzioni correttive, possono presentare dei bug che li espongono a rischio attacco. L'interoperabilità, che permette agli utenti di interagire con diversi protocolli per creare un servizio o un prodotto finanziario su misura per lui, può celare dei rischi di componibilità: a livello progettuale i protocolli potrebbero rivelarsi incompatibili e non funzionare come previsto; a livello operativo, invece, si potrebbero comporre dei prodotti complessi costruiti su una catena di token relativi a diverse piattaforme, creando delle interdipendenze che possono originare, in caso di fallimento, un rischio sistemico per le piattaforme coinvolte. Da questo punto di vista si corre il rischio di imbattersi in prodotti finanziari poco trasparenti che nascondono al loro interno altri token di altre piattaforme. Per questo motivo abbiamo menzionato dei rischi a livello informativo che potrebbero compromettere parzialmente la trasparenza del sistema.

Quando si ha a che fare con una nuova tecnologia si è attratti dalle nuove tendenze, ma bisogna essere consapevoli anche dei rischi. La DeFi è ancora al suo stato iniziale e la sua crescita fa ben sperare per il pieno sviluppo delle sue potenzialità, ma ciò comporta anche che potrebbero emergere ulteriori rischi. Gran parte di questi rischi sono già stati risolti, basti pensare a tutte le funzionalità che sono state introdotte per correggere molti bug degli smart

contract. Tuttavia il futuro è imprevedibile, ma la DeFi può dimostrarsi una valida alternativa anche in situazioni di grande incertezza, come quella che stiamo affrontando.

Quel che è certo, è che il suo futuro non può prescindere dalla risoluzione di due annose questioni: la scalabilità e la regolamentazione. La prima dipende molto dai risultati e dal successo del nuovo Ethereum 2.0, che metterà finalmente alla prova l'algoritmo del consenso PoS e vedremo se sarà in grado di risolvere in maniera sostenibile il trilemma della scalabilità, soppiantando definitivamente l'inquinante metodo del PoW. Per quanto riguarda la seconda, invece, passa tutto per la volontà dei legislatori dei vari Paesi, a seconda dell'approccio normativo che adotteranno. Il dibattito in merito è ancora molto aperto: secondo alcuni si opterà per una politica restrittiva fortemente limitante, che porterà alla chiusura della DeFi e di tutto il modo cripto. Secondo altri, invece, si sceglierà una regolamentazione più flessibile per tutelare gli utenti e portare maggiore serenità nel panorama DeFi, contribuendo positivamente alla sua espansione.

Se questi problemi saranno risolti, la DeFi potrà dare luogo ad un nuovo paradigma, costituendo una finanza decentralizzata solida, aperta e trasparente.

Bibliografia

Alharby, M., & Moorsel, A. V. (2017) *Blockchain-based Smart Contracts: A Systematic Mapping Study.* S.e.

Ante, L., Fiedler, I., & Le Pennec, G. (2021) *Wash trading at cryptocurrencies exchanges.* Finance Research Letters.

Arner, D. W., Buckley R. P., & Zetzsche, D. A. (2020) *Decentralized finance.* Journal of Financial Regulation.

Arnett, M., Delmolino, K., Kosba, A., Miller, A., & Shi, E. (2016) *Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab.* International Conference on Financial Cryptography and Data Security.

Bazzana, F., & Debortoli, F. (2002) *Il rischio sistemico in finanza: una rassegna dei recenti contributi in letteratura.* Alea Tech Reports.

Bekiros, S., & Lahmiri, S. (2020) *The impact of COVID-19 pandemic upon stability and sequential irregularity of equity and cryptocurrency markets.* Chaos, solitions & fractals.

Bellavitis, C., & Chen, Y. (2020) *Blockchain disruption and decentralized finance: The rise of decentralized business models.* Journal of Business Venturing Insights.

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

Borio, C., & Lowe, P. (2002) *Asset prices financial and monetary stability: exploring the nexus.* BIS Working Papers.

Botsman, R. (2017) *Who Can You Trust?: How Technology Brought Us Together and Why It Might Drive Us Apart.* PublicAffairs.

Bünzli, F., Dan, A., Drachsler-Cohen, D., Gervais, A., Tsankov, P., & Vechev, M. (2018) *Securify: Practical Security Analysis of Smart Contracts*. The 2018 ACM SIGSAC Conference.

Buterin, V. (2017) *The meaning of decentralization.* Medium.

Chen, C., Liu, L., & Zhao, N. (2020) *Fear Sentiment, Uncertainty, and Bitcoin Price Dynamics: The Case of COVID-19.* Emerging Markets Finance and Trade.

Chen, M.A., Wu, Q., & Yang, B. (2019) *How valuable is FinTech innovation?.* Review of Financial Studies.

Chohan, U. W. (2021) *The Double Spending Problem and Cryptocurrencies.* SSRN.

Chu, D. H., Hobor, A., Luu, L., Olickel, H., & Saxena, P. (2016) *Making smart contracts smarter.* In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security.

Cohen, J.E. (2019) *Between Truth and Power: The Legal Constructions of Informational Capitalism.* Oxford University Press.

Cong, L. W., & He, Z. (2018) *Blockchain disruption and smart contracts.* National bureau of economic research.

Cong, L. W., Li, X., Tang, K., & Yang, Y. (2021) *Crypto wash trading.* SSRN.

Corbet, S., Goodell, J. W., Gunay, S., & Kaskaloglu, K. (2021) *Are DeFi tokens a separate asset class from conventional cryptocurrencies?* SSRN.

Dannen, C. (2017) *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners.* Apress.

Gai, P., Haldane, A., & Kapadia, S. (2011) *Complexity, concentration and contagion.* Journal of Monetary Economics.

Gervais, A., Gudgeon, L., Harz, D., Livshits, B., & Perez, D. (2020) *The decentralized financial crisis.* 2020 Crypto Valley Conference on Blockchain Technology (CVCBT)

Gervais, A., Livshits, B., Qin, K., & Zhou, L. (2020) *Attacking the defi ecosystem with flash loans for fun and profit.* S.e.

Goodell, J. W., & Goutte, S. (2021) *Co-movement of COVID-19 and Bitcoin: Evidence from wavelet coherence analysis.* Finance Research Letters.

Gualandri, E., & Noera, M. (2014) *Rischi sistemici e regolamentazione macroprudenziale.* Iris Unimore.

Gudgeon, L., Knottenbelt, W. J., Perez, D., & Werner, S. M. (2020) *DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency.* S.e.

Jalan, A., Matkovskyy, R., & Yarovaya, L. (2020) *The Effects of a 'Black Swan' Event (COVID-19) on Herding Behavior in Cryptocurrency Markets: Evidence from Cryptocurrency USD, EUR, JPY and KRW Markets.* Journal of international financial markets, institutions and money.

Jarboui, A., Mnif, E., & Mouakhar, K. (2020) *How the cryptocurrency market has performed during COVID 19? A multifractal analysis.* Finance Research Letters.

Kim, J. M., Kim, S. T., & Kim, S. (2020) *On the relationship of Cryptocurrency Price with US Stock and Gold Price Using Copula Models.* MDPI.

Lamport, L., Pease, M., & Shostak, R. (1982) *The byzantine generals problem.* ACM transactions on programming languages and systems.

Lin, L. X. (2019) *Deconstructing decentralized exchanges.* Stanford journal of blockchain law & policy

Livshits, B., & Perez, D. (2019) *Smart contract vulnerabilities: Does anyone care?.* S.e.

Murray, A., Kuban, S., Josefy, M., & Anderson, J. (2019) *Contracting in the smart era: the implications of blockchain and decentralized autonomous organizations for contracting and corporate governance.* Academy of Management Perspectives.

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System.* S.e.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press.

Saleh, F. (2018) *Volatility and Welfare in a Crypto Economy.* McGill University.

Schär, F. (2020) *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial markets.* Federal Reserve Bank of St. Louis.

Schutte, J., State, R., & Torres, C. F. (2018) *Osiris: Hunting for integer bugs in ethereum smart contracts*. In Proceedings of the 34th Annual Computer Security Applications Conference.

Seidel, M.-D.L. (2018) *Questioning centralized organizations in a time of distributed trust*. Journal of Management Inquiry.

Shuwar, R., & Vashchuk, O. (2018) *Pros and cons of consensus algorithm proof of stake. Difference in the network safety in proof of work and proof of stake.* S.e.

Sorgentone, P. (2020) *Il futuro del valore: blockchain, cryptoasset e finanza decentralizzata.* (2. Ed.) Pubblicazione indipendente.

Srnicek, N. (2017) *Platform Capitalism.* Polity Press.

Sun, T., & Yu, W. (2020) *A formal verification framework for security issues of blockchain smart contracts.* MDPI.

Szabo, N. (1994) *Smart contracts.* S.e.
Szabo, N. (1997) *Formalizing and Securing Relationships on Public Networks.* S.e.

Victor, F., & Weintraud, A. M. (2021) *Detecting and quantifying wash trading on decentralized cryptocurrencies exchanges.* S.e.

Vidal-Tomas, D. (2021) *Transitions in the cryptocurrency market during the COVID-19 pandemic: A network analysis.* Finance Research Letters.

Walch, A. (2019) *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems.* Oxford University Press.

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Public Affairs.

Ringraziamenti

Questo lavoro è solo l'ultimo di un lungo percorso durato tre anni, un viaggio fatto di alti e bassi, ricco di esperienze e sfide stimolanti. Ho superato ostacoli che credevo insormontabili, ho incontrato compagni straordinari e ho imparato a conoscermi meglio. Guardandomi indietro mi chiedo come abbia fatto ad affrontare l'ansia e la paura, ma ora che sto pensando alle persone da ringraziare, ho capito da dove viene la mia determinazione, la mia ambizione, la mia resilienza.

Allora ringrazio innanzitutto la mia famiglia che ha sempre creduto in me e mi ha sostenuto in ogni momento. Mio fratello è sempre stata un'ancora e un esempio, un punto di riferimento e una guida. I nonni e le nonne, che mi hanno trasmesso il valore della formazione e l'importanza della cultura. Un grande abbraccio a una persona speciale che mi protegge dall'alto e fa sempre il tifo per me.

Ringrazio i miei amici più cari e i miei compagni di avventura, con cui ho condiviso gioie e dolori. Mi hanno aiutato a crescere e ho imparato tanto da ognuno di loro. Ci siamo sostenuti a vicenda e insieme abbiamo raggiunto traguardi importanti.

Un grazie speciale a Susanna: in lei e per lei ho trovato la forza per dare sempre il massimo. Mi è stata vicina nei momenti difficili, e non era facile, ma è anche stata sempre il primo pensiero dopo ogni esame superato.

Spero vivamente che ogni sacrificio che ho fatto e che farò servano per costruire qualcosa di bello.

Grazie a tutti, di cuore.