LUISS

Dipartimento di Economia e Management

Cattedra: Finanza Aziendale

Decentralized Finance e applicazioni della blockchain sui servizi finanziari

RELATORE

Prof. Pierluigi Murro

CANDIDATO

Gaetano Tamburino - 247331

Anno Accademico: 2021/2022

INDICE

INTRODUZIONE

Una delle tecnologie più "dirompenti" in questo periodo è sicuramente la blockchain.
La blockchain è intesa da un punto di vista teorico, come un libro mastro digitale, che ha lo scopo di archiviare dati in "blocchi", ovvero una catena di registri. La forza di questa tecnologia si fonda sull'immutabilità dei dati raccolti, e l'opportunità di sviluppare applicazioni imponendo delle regole tramite degli smart contract. Tutto ciò è reso possibile dal codice informatico, il quale garantisce un sistema aperto (perché le informazioni contenute nei blocchi sono accessibili a tutti), neutrale, affidabile e sicuro.

Le applicazioni di questa tecnologia sono molte (e in continua crescita), ma concentreremo la nostra analisi sul mondo dei servizi finanziari decentralizzati, e il modo in cui sfruttano i vantaggi della blockchain per migliorare e innovare alcuni aspetti della finanza.
Ogni volta che abbiamo dovuto interagire da un punto di vista finanziario con altri soggetti, ci siamo serviti sempre di un intermediario finanziario, ovvero una terza parte fidata che garantisce trasparenza e mantenimento dell'integrità dell'intero sistema. La finanza decentralizzata sfrutta la potenza del codice, per superare la necessità di riporre fiducia su entità centrali, e aumentare l'accessibilità e l'efficienza dei mercati finanziari.

- Il primo capitolo ha uno scopo puramente introduttivo, spiegando da un punto di vista teorico il funzionamento della blockchain dalla sua nascita, associata al rilascio da parte di Satoshi Nakamoto del whitepaper sul Bitcoin. La prima moneta digitale e il suo "ecosistema" in generale, presentava alcuni limiti, dovuti al tipo di linguaggio utilizzato. Qualche anno dopo nacque Ethereum, una nuova piattaforma distribuita su blockchain, caratterizzata da una nuova forma di scripting: gli smart contract.

- Nel secondo capitolo passeremo alle applicazioni di questa tecnologia, focalizzando l'attenzione sull'aspetto oggetto di questa tesi, ovvero la DeFi (Decentralized Finance). Analizzeremo i principali servizi finanziari offerti dai principali protocolli e i loro vantaggi rispetto a quelli erogati da istituzioni centralizzate.

- Il terzo e ultimo capitolo parte da una dimostrazione, supportata da relativi dati, della portata di questo fenomeno per analizzare quanto capitale ha attratto fino a oggi. Parleremo delle stablecoin e il loro design innovativo, che permette di sfruttare i vantaggi offerti dalla decentralizzazione, senza sopportare i rischi di volatilità che coinvolgono pressoché tutte le criptovalute.

CAPITOLO 1 - Tecnologia della Blockchain e i primi ecosistemi

1.1 Blockchain

1.1.1Overview tecnica

Per capire cosa si intende per blockchain, è necessario comprendere il significato di "ledger digitale". Quest'ultimo è una sorta di database che registra tutti i dati delle transazioni che sono avvenute in un network peer-to-peer[1].

I ledger vengono utilizzati sin da tempi antichi, ma il suo scopo è sempre rimasto lo stesso. Ci sono state però delle evoluzioni nella tecnologia a supporto di esso, che hanno permesso di rimpiazzare gli obsoleti registri cartacei con innovativi archivi digitali. Dobbiamo però fare attenzione e non confondere un ledger con un database. Quest'ultimo infatti permette di inserire, rimuovere o modificare i dati, a differenza di un ledger che invece permette solamente l'aggiunta di nuovi dati. Questa caratteristica è di fondamentale importanza per garantire sicurezza e immutabilità nell'ecosistema della blockchain. Il punto però non è che i database verranno rimpiazzati; infatti, svolgono semplicemente funzioni diverse rispetto a una blockchain, e sono pensati per perseguire obiettivi del tutto distinti. Considerando che un database necessita di un sistema ad accesso controllato, possiamo partire individuando la principale novità che ha portato questa tecnologia, ovvero la possibilità di utilizzarla senza il bisogno di una terza parte fidata che garantisce la sicurezza.

All'interno della blockchain, un ledger digitale è strutturato come una catena di blocchi che hanno il compito di memorizzare informazioni. Ogni blocco è collegato al blocco precedente attraverso una funzione crittografica denominata come: "funzione di hash". Dalla concatenazione dei blocchi viene il nome "Blockchain" (catena di blocchi).

In base alla sua architettura, possiamo distinguere tre tipi di blockchain:

- Blockchain Pubbliche

  Questa tipologia è la più diffusa, in quanto più di tutte, fa leva sulla decentralizzazione. Non esiste una singola autorità ed è aperta a chiunque, senza possibilità di esclusione, per questo è anche chiamata **"permissionless"**. Tale apertura, consente a chiunque di poter verificare lo stato della blockchain e suggerire miglioramenti.

- Blockchain Private

  Dette anche **"permissioned"**, queste blockchain sacrificano un po' della decentralizzazione dando a una sola autorità la possibilità di mantenere un controllo sui permessi all'accesso.

[1] Un network peer-to-peer (p2p) è un tipo di rete di comunicazione, dove ogni nodo comunica direttamente con tutti gli altri, senza bisogno di mediazione.

- Consortium

  Questo modello “ibrido” distribuisce l’autorità tra i partecipanti del network, anziché ad una singola entità, come nel caso delle blockchain private, consentendo di mantenere alcuni dei vantaggi della decentralizzazione, la quale rappresenta il vero punto di forza di questa tecnologia.

1.1.2 Blocchi

Ma soffermiamoci sulla struttura e la funzione dei principali componenti di un blocco.
La sequenzialità dei blocchi è consentita, come detto prima, dalla crittografia hash, la quale permette di dare una prova matematica che non sono presenti alterazioni dei dati. In pratica, se qualcuno tenta di modificare, aggiungere, o eliminare alcune informazioni di un blocco, verrebbe immediatamente scoperto, in quanto l’hash del blocco cambierebbe, influenzando tutti i blocchi successivi (Figura 1.1).
L’hash è una funzione che viene utilizzata per mappare dati di dimensioni arbitrarie in dati di dimensioni fisse. Non esistono vincoli per la tipologia dell’input, che può andare da una transazione a un foglio di calcolo, ma l’output generato dalla funzione è caratterizzata da un numero finito di bit, e dunque, qualsiasi tipo di modifica nell’input (i dati presenti nel blocco), altera completamente l’hash.
Questo permette una notevole velocità nell’operazione di confronto dei dati, rispetto ad analizzare un intero file di informazioni.

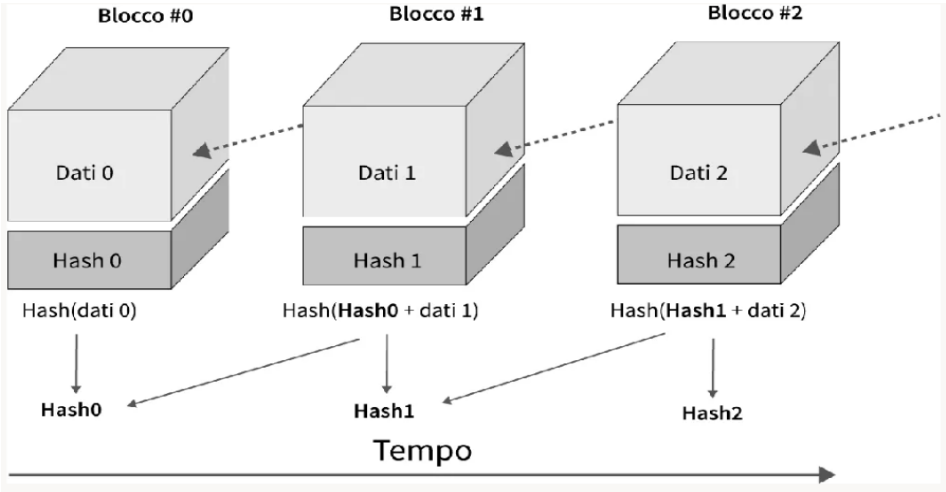

Figura 1.1
Struttura di un blocco e funzione di hash
Fonte: *Blockchain. Tecnologia e applicazioni per il business*, Hoepli (2019)

Per la maggior parte delle sue applicazioni, una blockchain necessità di un network sul quale essere distribuita. Per network si intende una rete di macchine connesse tra loro, con lo scopo di scambiarsi informazioni.
Tutte le macchine connesse alla rete sono "nodi" e in base alla loro autonomia distinguiamo **nodi completi** (full-node) da **nodi light** (light-node).
I primi sono capaci di archiviare (localmente) una copia dell'intera blockchain, in modo da verificare che non vi siano anomalie e propagare soltanto i blocchi validi, scartando quelli non validi. Utilizzare un full-node è il modo più sicuro e "diretto" per interagire con una blockcain, ma richiede il download dell'intera blockchain stessa e quindi può rivelarsi troppo dispendioso in termini di risorse.
I light-node, a differenza dei full che sono totalmente autonomi, ricevono solo una quantità limitata di dati da un nodo fidato, e di conseguenza, sono dipendenti dalla fiducia data dal full-node. Usare i nodi "light", inoltre, non richiede la memorizzazione dell'intera blockchain.

L'architettura del network di una blockchain è di tipo decentralizzata, ovvero non esiste un singolo punto di fallimento. La forza di questa tecnologia è la possibilità di distribuire e replicare le risorse nei nodi, permettendo a un'applicazione di essere eseguita da tutti i partecipanti, così da evitare la generazione di un singolo punto possibile di fallimento infrastrutturale; per "crollare" è necessario che cessino di operare tutti i nodi. Questi ultimi sono considerati tutti uguali in una blockchain, creando un'autorità decentralizzata, a differenza delle reti condizionate da autorità centralizzate che al contrario delle prime, sono contraddistinte dal potere di definire le regole del sistema.
Le "macchine" giocano quindi un ruolo fondamentale, e una delle ragioni che ha portato alla nascita della blockchain è stata proprio la ricerca di un sistema incorruttibile, privo di errori umani, che fa leva sulla determinazione a eseguire le regole dei full-node, a prescindere dalle decisioni di tutti gli altri nodi.

Come dovrebbe essere già abbastanza chiaro, una blockchain ripone si fonda sull'affidamento al codice, e non ha governanti (o autorità centrali). A questo punto potrebbero però sorgere delle domande, come ad esempio: Sulla base di cosa un nodo decide se un blocco è valido o meno? Chi decide se una transazione è valida?
Il responsabile di queste decisioni è il network. Gli attori principali sono i full-node e i **"miner"**, i quali hanno il compito di raggiungere una decisione, attraverso un processo di consenso. In una blockchain questo processo avviene in modo continuo, non in un istante preciso nel tempo, ed è cruciale ai fini delle verifiche sullo stato attuale di una blockchain.
I miner partecipano attivamente al processo di consenso., validando e raggruppando le transazioni in blocchi nuovi che vengono aggiunti alla catena, attraverso il cd processo di **mining**.
Questa fase fondamentale per raggiungere il consenso distribuito fu introdotta per la prima volta nel 2008, con il White Paper sul Bitcoin rilasciato da Satoshi Nakamoto.

1.2 Bitcoin

1.2.1 Il Proof of Work

Il protocollo di consenso che utilizza Bitcoin si basa sull'algoritmo Proof of Work (PoW), il quale consiste nella ricerca di un numero complesso da trovare e che richiede quindi un'elevata potenza computazionale, ma non appena trovato, risulterà estremamente facile verificarne la correttezza per tutti gli altri nodi.

"Abbiamo proposto un sistema per le transazioni elettroniche non basato sulla fiducia. Abbiamo iniziato con il framework abituale delle valute basate su firme digitali, che prevede un forte controllo sulla proprietà, ma è incompleto non avendo modo di prevenire la doppia spesa. Per risolvere questo problema, abbiamo proposto una rete peer-to-peer che utilizza la proof-of-work per registrare una storia pubblica delle transazioni, la cui modifica diventa rapidamente impraticabile dal punto di vista computazionale per un utente malintenzionato se i nodi onesti controllano la maggioranza della potenza della CPU. La rete è robusta nella sua semplicità non strutturata. I nodi lavorano tutti insieme con poca coordinazione. Non hanno bisogno di essere identificati, dal momento che i messaggi non vengono instradati in qualche direzione particolare ma vengono solo consegnati su base "best effort". I nodi possono lasciare e ricongiungersi con la rete a piacimento, accettando la catena proof-of-work come prova di quello che è successo mentre erano assenti. Essi votano con la loro potenza di CPU, esprimendo la loro accettazione di blocchi validi mediante il lavoro che compiono sulla loro estensione e respingendo i blocchi non validi tramite il rifiuto di lavorare sugli stessi. Tutte le regole e gli incentivi necessari possono essere applicati mediante questo meccanismo di consenso." (Nakamoto; White Paper Bitcoin; 2008)

Così Satoshi Nakamoto concluse il paper, sottolineando come la vera forza del PoW sta nella sua garanzia di immutabilità. La Figura 1.2 aiuta a capire come funziona il processo di consenso da parte del network, di cui parlò il creatore di Bitcoin.

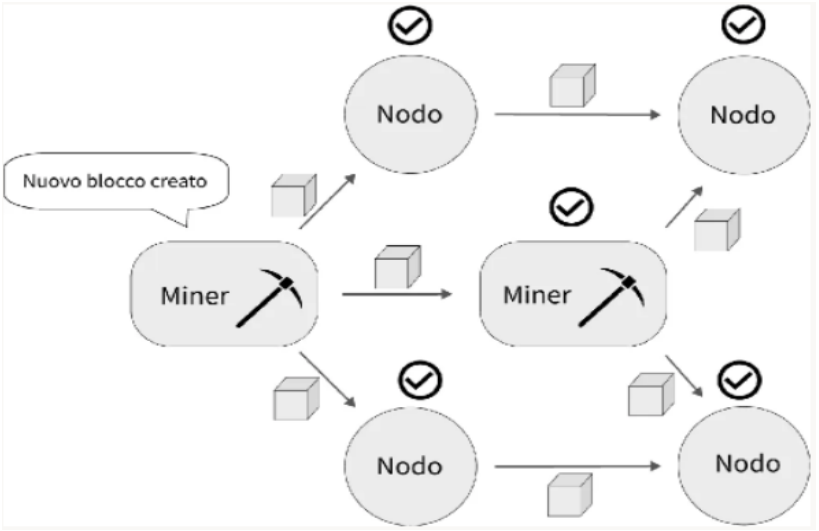

Figura 1.2

Validazione di un blocco

Fonte: *Blockchain. Tecnologia e applicazioni per il business*, Hoepli (2019)

In un processo di consenso, quando viene creato un blocco nel quale è inserita una transazione, il network verifica che i nuovi blocchi e le transazioni inserite siano valide e in caso, propagarli per la rete. Se un blocco non valido viene creato, cesserà subito di propagarsi non appena risulterà non valido ai nodi. Il PoW in particolare rende progressivamente più difficile (e costoso) modificare una transazione o modificare le informazioni in essa contenute, man mano che vengono generati nuovi blocchi. (Figura 1.3)

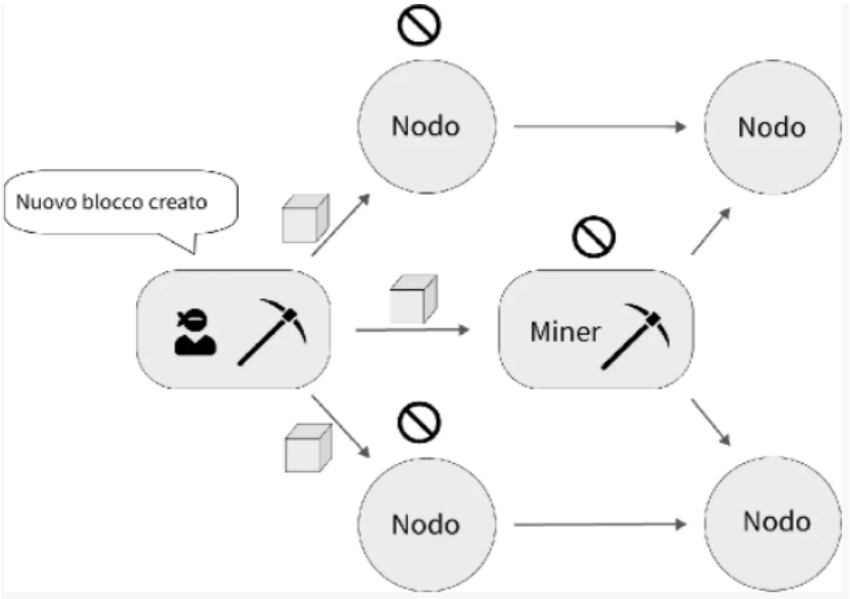

Figura 1.3
Interruzione propagazione del blocco
Fonte: *Blockchain. Tecnologia e applicazioni per il business*, Hoepli (2019)

I miner, per essere incentivati a continuare il loro importante lavoro ai fini della sicurezza del network, vengono ricompensati con le commissioni delle transazioni incluse nel blocco, e nuovi token che rappresentano monete digitali (criptovalute[2]).

1.2.2 Macro

La moneta virtuale generata, il BTC, è diversa dalle classiche valute che conosciamo. Se consideriamo una Banca Centrale, questa emette nuova moneta per fare prestiti e per finanziare la spesa dello stato, mentre con Bitcoin la nuova moneta va solamente a chi spende risorse (CPU) per aggiornare il ledger. Bitcoin è stato programmato per produrre un nuovo blocco all'incirca ogni dieci minuti, e che ogni blocco contenga delle

[2] Con il termine criptovaluta si fa riferimento a tutti gli asset digitali basati sulla tecnologia blockchain

ricompense (reward) di 50 monete per i primi quattro anni di attività del network, dimezzandosi ogni quattro anni.

La quantità di bitcoin creati è predeterminata e non può essere alterata. (Figura 1.4 e Figura 1.5)

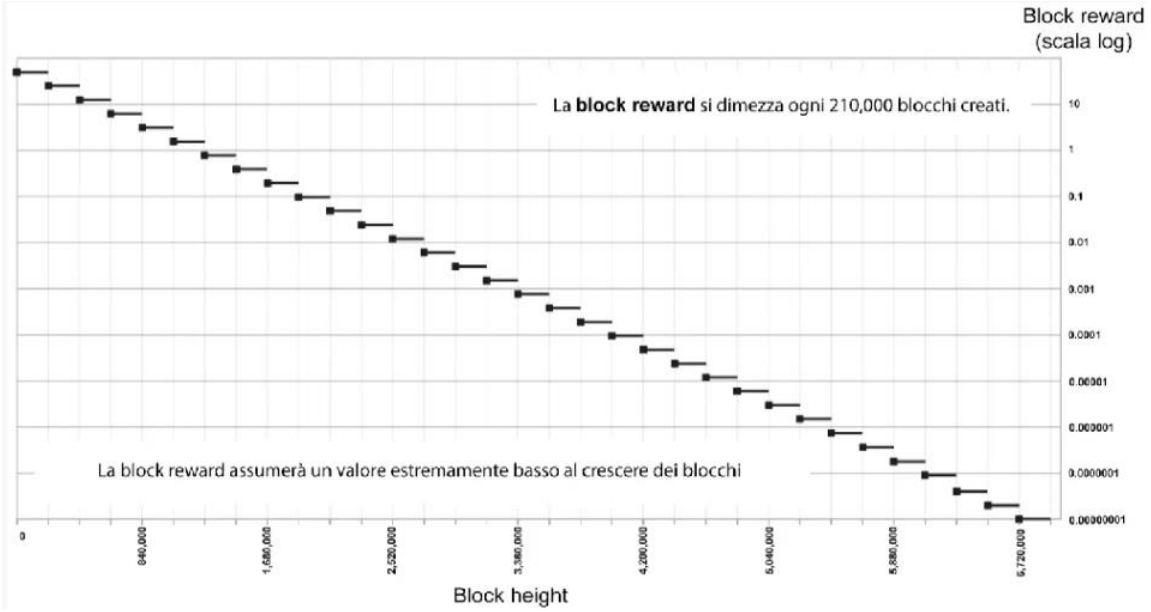

Figura 1.4

Bitcoin generati per nuovo blocco

Fonte: *Blockchain. Tecnologia e applicazioni per il business*, Hoepli (2019)

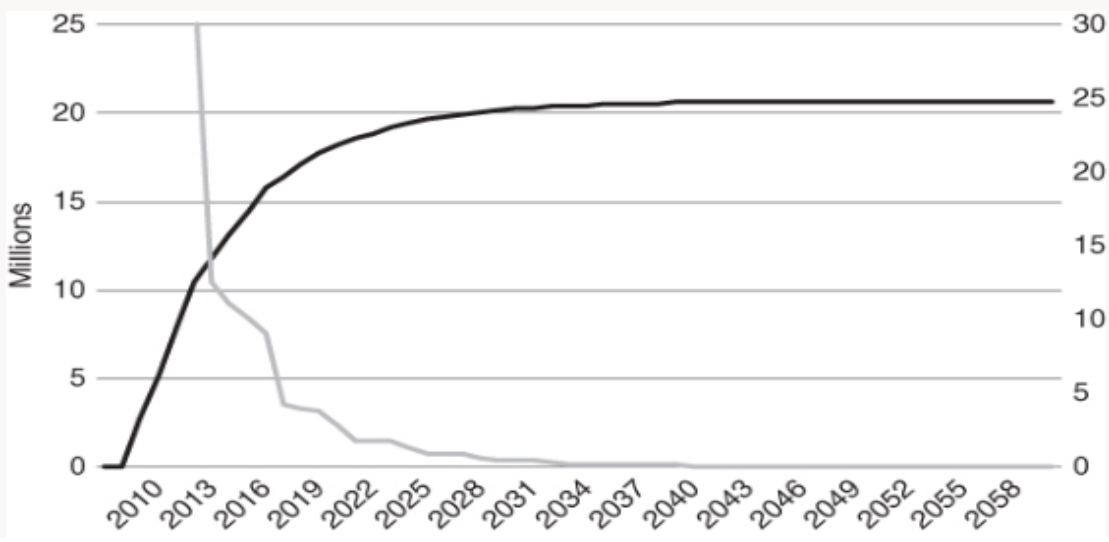

Figura 1.5

Andamento del numero di Bitcoin in circolazione

Fonte: *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, Wiley (2018)

Riassumendo, Nakamoto pianificò un tasso di crescita dell'offerta destinato a decrescere col tempo.
Quando nel 2009 ancora pressoché nessuno aveva mai utilizzato Bitcoin, il numero di nuove monete generato era ben più basso da quello previsto dall'algoritmo, in quanto i nuovi blocchi non sono "minati" esattamente ogni dieci minuti. Negli anni successivi è stato visto che all'aumentare dell'offerta totale (Total Supply), è stata riscontrata una varianza dalla "crescita teorica" proporzionalmente decrescente.
Mentre le tradizionali monete aumentano continuamente l'offerta, diminuendo di conseguenza il loro potere di acquisto, Bitcoin ha conosciuto una crescita enorme in termini di potere reale d'acquisto, nonostante la sua moderata crescita nell'offerta, dovuta al limite predisposto dall'algoritmo. Ad aumentare la forza dell'ecosistema e del progetto in sé, vi sono i minatori, i quali venendo ricompensati in BTC sul loro lavoro di verifica, hanno interesse a detenere la moneta e non venderla in quanto provocherebbero una diminuzione del prezzo.

1.2.3 Funzionalità

Date le sue caratteristiche, è giustificabile che la maggior parte considera il BTC più come un asset, piuttosto che come una semplice moneta. Nonostante ciò, esistono numerosi vantaggi nell'utilizzo del BTC come opzione di pagamento:

- Sicurezza dei dati: Bitcoin utilizza una blockchain pubblica [3], e questo permette a chiunque voglia, di visualizzare eventualmente tutte le transazioni collegate ad uno specifico indirizzo. L'indirizzo pubblico non contiene dirette informazioni sul suo proprietario. In pratica tutti fondi sono collegati a indirizzi, dai quali però risulta impossibile andare a ritroso per ottenere informazioni "private".
- Facilmente tracciabile: una volta che una transazione avviene, questa viene inserita nella catena e non può più essere cambiata. Risulta quindi estremamente più semplice e veloce rintracciare una transazione.
- Transazioni veloci: il trasferimento della moneta è pressoché istantaneo, non essendo richiesta la presenza di una terza parte (o intermediario). Non esistono dunque alcun vincolo sul luogo, la quantità (di moneta) e il momento in cui si voglia inviare/ricevere i bitcoin.
- Micropagamenti: i BTC possono essere scomposti fino a 1/100.000esimo. Questo rende facili anche pagamenti di piccole somme, e in più le commissioni sono quasi nulle.

[3] Una Blockchain pubblica (permissionless) è caratterizzata dall'assenza di un'autorità centrale. Ogni nodo ha stessi diritti e responsabilità, e chiunque voglia unirsi può farlo (rete aperta), senza distinzione in base al contenuto, destinazione e origine.

1.2.4 Proof of Work (PoW) vs Proof of Stake (PoS)

Tuttavia, molti ritengono ci siano modi migliori per raggiungere il consenso rispetto al Proof of Stake, in quanto questo sistema consuma una quantità massiccia di energia.
Emerge da un articolo pubblicato da "Harvard Business Review" nel 2021, che l'intero sistema del Bitcoin consuma attualmente circa 110 Terawatt Ora all'anno. L'energia elettrica utilizzata equivale allo 0,55% del consumo totale nel mondo, ed è paragonabile con i consumi elettrici annui di piccoli stati come la Malesia e la Svezia.
Il protocollo alternativo al PoW è il Proof of Stake (PoS), nel quale, a differenza di utilizzare potenza di calcolo per generare nuovi token vengono utilizzati i token stessi. Entrambi i protocolli perseguono lo stesso obiettivo (raggiungere il consenso nel network), ma il modo in cui lo fanno è diverso.
Nel Proof of Stake ci sono dei "validatori" che vengono alternati, e sono scelti sulla base delle quantità di token che possiedono. Mentre nel PoW i miner si occupano del processo di validazione, e vengono ricompensati sulla base del mining, nel protocollo Proof of Stake, ogni token corrisponde a un voto. In questo modo ciascun utente in possesso di un token può fare "staking", che si traduce in bloccare il proprio token fin quando il processo di validazione non è concluso, ricevendo in cambio il diritto di essere riconosciuto come validatore e ottenendo una ricompensa.

1.2.5 Bitcoin Script

Per essere trasferiti da un indirizzo all'altro, i Bitcoin richiedono a chi li traferisce, di rilasciare anche due elementi fondamentali:

- Una chiave pubblica: che dopo essere stata crittografata viene inserita nello script
- Una firma elettronica: per confermare che la chiave privata[4] corrisponda alla chiave pubblica che è stata fornita.

Durante un trasferimento di BTC, lo script permette la flessibilità di cambiare i parametri o quello che è necessario per effettuare la transazione.
Una delle principali criticità del linguaggio di script di Bitcoin, è che non può supportare molte funzioni. Queste mancanze vengono identificate come "Lack of Turing-completeness. Un linguaggio è Turing-complete se può essere usato per risolvere qualsiasi problema che ammetta soluzione.
Lo script di Bitcoin permette quindi un range limitato di funzionalità, e le transazioni possono risultare meno veloci se paragonate a progetti nati dopo che implementano la blockchain. Tuttavia, gli entusiasti di Bitcoin

[4] Le chiavi crittografiche si dividono in chiavi private e chiavi pubbliche. Mentre la chiave pubblica può essere condivisa con chiunque, le chiavi private sono segrete e rappresentano il punto di partenza dal quale viene calcolata la chiave pubblica. In questo modo si può beneficiare della "criptazione".

non tengono in considerazione questi aspetti come se fossero delle mancanze, bensì accettano di limitarsi alle funzioni possibili, in quanto vedono come vero punto di forza la pura decentralità dell'ecosistema.
Bitcoin ha creato una struttura per contratti elettronici, nella quale però le condizioni possono essere legate solamente al trasferimento di valore. Questo tipo di "Framework" ha aperto l'orizzonte verso potenziali transazioni subordinate a delle condizioni (come, ad esempio, alla ricezione del bene o servizio).

1.3 Ethereum

1.3.1Oltre il trasferimento di valore

Ogni sistema finanziario robusto necessita di servizi che vanno oltre il semplice trasferimento di valore, come ad esempio finanziamenti, prestiti ecc… Bitcoin a causa del suo Script non era adatto a questo tipo di applicazioni. Anziché semplicemente trasferire valore (monete) da una parte all'altra, gli script hanno il potenziale di subordinare questi trasferimenti all'eventualità che un determinato evento si verifichi o meno.
Nel 2015 il giovane programmatore Vitalik Buterin, lanciò un nuovo progetto basato sulla blockchain chiamato Ethereum, che deve riconoscere gran parte del suo successo al nuovo tipo di script "Turing-Complete" chiamato **Solidity**. Il nuovo linguaggio implementato in questa blockchain permette di svilupparci sopra un'applicazione del tutto personalizzabile, grazie all'utilizzo degli smart contract, creando il proprio token senza bisogno di creare una nuova blockchain.

1.3.2 Panoramica su Ethereum

Ethereum è una cd blockchain "generalizzata", in quanto non ha uno scopo predeterminato, ma può essere usata per sviluppare programmi attraverso la sopra-citata tecnologia degli **smart contract** che approfondiremo nel secondo capitolo.
A differenza di Bitcoin, l'ecosistema Ethereum non prevede una quantità massima di erogazione della sua valuta "ETH" (abbreviazione di Ether).
Dato che ogni transazione richiede una determinata quantità di risorse di calcolo, Ethereum chiede una commissione, che prenderà il nome di "Gas". I due parametri da considerare in una transazione sono: prezzo del gas, ovvero il numero di wei[5] da pagare, per unità di gas, e limite del gas che delinea la quantità massima di calcoli per blocco.

[5] Il "wei" rappresenta l'unità di misura di riferimento per il gas nella blockchain Ethereum: 1ETH = 10^18wei)

CAPITOLO 2 – Come la DeFi ha rivoluzionato i servizi finanziari

2.1 Le fondamenta della DeFi

2.1.1 Smart Contract

Uno smart contract è un "protocollo di transazione computerizzato che esegue i termini di un contratto" (Nick Szabo). La finalità di questo protocollo è automatizzare il soddisfacimento delle condizioni contrattuali, senza bisogno di un intermediario sul quale riporre la fiducia. In questo modo è possibile superare la tendenza all'inefficienza, lentezza e poca economicità dei servizi centralizzati caratterizzati dalla presenza di intermediari.

Gli smart contract usano una logica di tipo IFTTT (If This Then That) che risponde al verificarsi o meno di un determinato evento. Ad esempio, se un consumatore decidesse di acquistare un determinato prodotto/servizio al prezzo di 2 ETH a condizione che uno specifico evento si verifichi, lo smart contract eseguirà in modo autonomo l'azione (in questo caso lo scambio di valore) solo se la predeterminata condizione (evento) si concretizzi. Dall'altro lato ci sono coloro che si sono impegnati a trasferire il bene/servizio e a ricevere una somma in cambio della prestazione, sempre attraverso lo smart contract. (Figura 2.1)

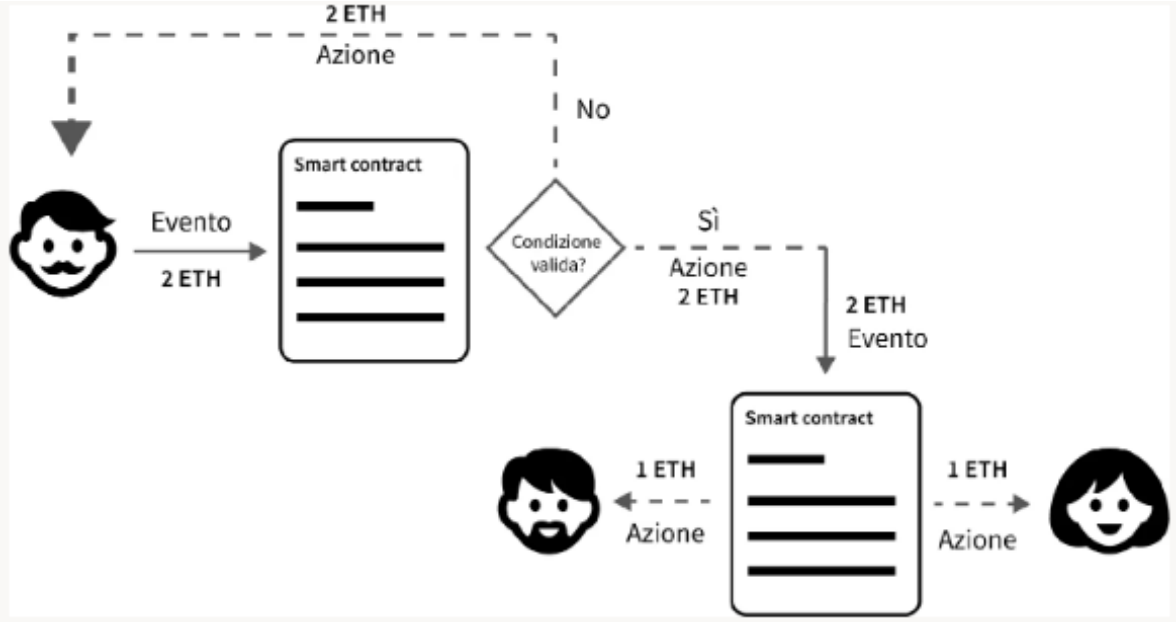

Figura 2.1

Il processo IFTTT

Fonte: *Blockchain. Tecnologia e applicazioni per il business*, Hoepli (2019)

La blockchain Ethereum, grazie alle tecnologie che implementava, divenne presto una forte calamita per programmatori, attirati dall'opportunità di sviluppare applicazioni.

L'intera struttura di Ethereum può essere ricollegata al controllo degli asset digital, i quali sono poi utilizzati per creare prodotti finanziari. Il meccanismo degli intermediari che forniscono servizi finanziari, è praticamente lo stesso, l'unica differenza è che gli stessi intermediari e regolatori devono verificare che i prodotti operino nel modo corretto. Nella finanza decentralizzata, invece, è il codice che assicura tutto questo. Dopo poco tempo, grazie all'innovativo sistema di raccolta di capitale chiamato Initial Coin Offering, cominciarono a prendere forma nuovi progetti che avevano l'aim di rivoluzionare il mondo della finanza, sfruttando le nuove tecnologie portate dalla blockchain. Nacque così il nuovo mondo della Decentralized Finance o DeFi.

2.1.3 Un po' di storia

Poco dopo la nascita di Ethereum, numerosi nuovi progetti, cominciarono a preferire l'utilizzo di questa piattaforma, invece dei classici metodi di raccolta del capitale. Il processo che permette questo è chiamato ICO (Initial Coin Offering), ed è il metodo principale di raccolta fondi per il finanziamento di progetti basati sulla blockchain.

Una ICO consiste nella vendita di un token che rappresenta la partecipazione al progetto, in cambio di criptovalute o di denaro fiat (moneta a corso legale) con lo scopo di finanziare un progetto. La Figura 2.2 mostra quanto lo smart contract è importante in una ICO, in quanto gestisce la crowdsale, ricevendo il denaro fiat/criptovaluta, che gli investitori usano come metodo di pagamento, e distribuendo i token in maniera automatica.

Quando una società crea lo smart contract con il proprio token (solitamente basato sullo standard ERC 20[6]) stabilisce quantità massima (hard cap) e minima (soft cap) di token vendibili, prezzo di vendita, modalità di pagamento e di vendita.

[6] La maggior parte dei token basati su Ethereum si basano su questo "standard". Un token ERC 20 è in pratica uno smart contract che implementa le funzioni definite dallo standard ERC 20

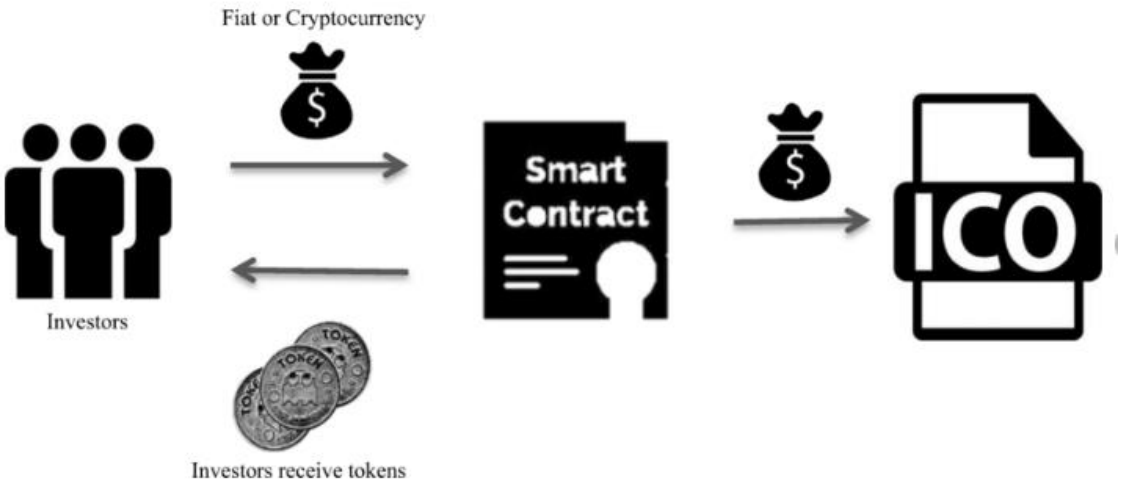

Figura 2.2

Processo di un'ICO

Fonte: https://www.researchgate.net/figure/The-ICO-process-and-generation-of-tokens_fig3_338845616

Solo nel 2017 ci sono state 552 ICO, attraverso le quali sono stati raggiunti in totale 7 miliardi di dollari raccolti, e circa un anno dopo il valore è aumentato più del 100% (Figura 2.3). Come accadde per la bolla "dot com", l'innovazione ha generato tanto scalpore, e molti progetti che nacquero non avevano nulla in più di qualche pagina di whitepaper a sostenere il progetto. L'euforia sulla nascita di nuovi progetti nel mondo blockchain ha fatto sì che molti di questi risultarono sopravvalutati.

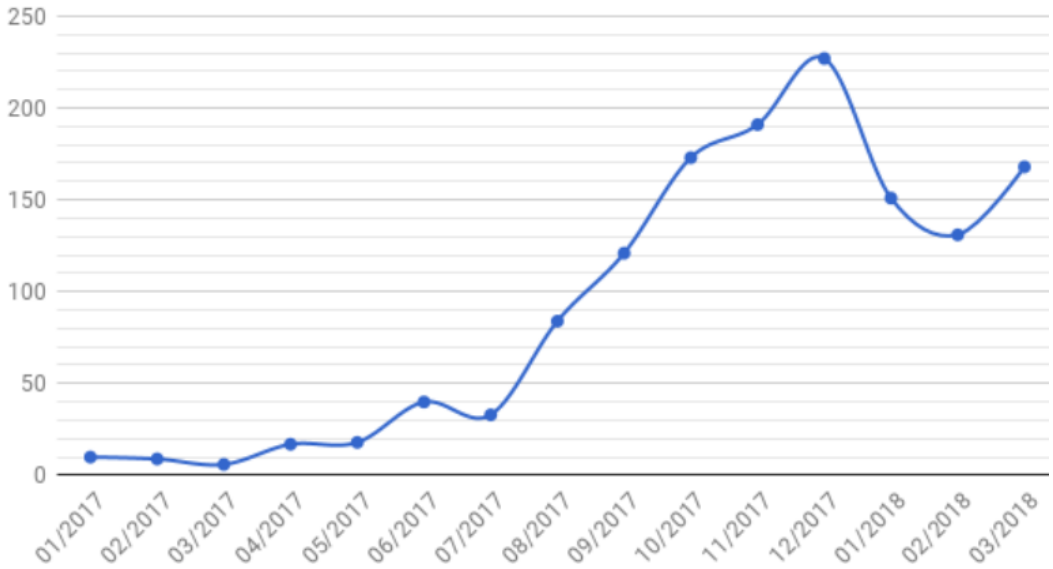

Figura 2.3

Numero di ICO dal 2017 a marzo 2018

Fonte: icodata

Nonostante la cattiva reputazione del periodo che prese il nome di "ICO mania" del 2017, alcuni protocolli emersi in questo periodo sono ancora tra le migliori applicazioni di finanza decentralizzata esistenti.

Tra le principali innovazioni portate dalla DeFi vi è il nuovo modello "user-to-contract". In pratica, a differenza del modello user-to-user, non serviva più interagire direttamente con un altro utilizzatore, bensì bastava farlo direttamente con uno smart contract, che conteneva dei fondi versati da molteplici utilizzatori. Il primo protocollo di finanza decentralizzata che dobbiamo ricordare è **MakerDAO**. Questo progetto, lanciato nel 2017, era basato sulla blockchain Ethereum, e permetteva agli utilizzatori di prendere a prestito la stablecoin[7] DAI, utilizzando come collaterale ETH, ovvero la criptovaluta nativa di Ethereum. Maker DAO fu la prima applicazione su blockchain che dava la possibilità a chiunque di prendere un prestito, senza bisogno di un'entità centralizzata, diventando così un'ispirazione per numerosi protocolli nati successivamente, come ad esempio Compound e Uniswap.
Dopo il periodo non troppo positivo dell'ICO mania, fu inevitabile un periodo caratterizzato da un trend ribassista dell'intero mercato. Il "bear market" aiutò però il mondo della DeFi a consolidarsi, spazzando via progetti che non avevano alcuna giustificazione di esistere in quanto non ben strutturati, o addirittura risultanti ancora inattivi dopo settimane o mesi dall'ICO.

2.2 Una nuova architettura dei servizi finanziari

2.2.1 Verso un miglioramento dell'efficienza

DeFi è l'abbreviazione di "decentralized finance" (finanza decentralizzata) e fa riferimento al sistema di generazione di servizi, simili a quelli offerti dagli intermediari, su una blockchain.

Per capire meglio il processo che porta allo sviluppo della finanza decentralizzata, è necessario soffermarci sulla struttura dell'ecosistema finanziario attuale. Lo scenario finanziario attuale è caratterizzato dalla presenza di centri economico/finanziari cruciali, come New York e Londra, che hanno la funzione di "hub operativo" per il settore dei servizi finanziari e influenzano l'attività economica. Questo modello di interdipendenza è replicato nel funzionamento delle società di servizi finanziari. Infatti, ognuna ha un headquarter, filiali, e partnership in molti casi in paesi diversi, ciascuno con il proprio ordinamento, generando complicazioni sulla regolamentazione esatta da applicare, e altri problemi legati alla giurisdizione finanziaria del paese. Questa infrastruttura dei servizi finanziari ha bisogno quindi di un funzionamento corretto dell'economia globale per funzionare. Dalla crisi finanziaria del 2008 che ha coinvolto tutto il mondo, è cresciuta l'attenzione sulle inefficienze e asimmetrie strutturali che hanno portato a una progressiva sfiducia nelle istituzioni finanziarie e la loro trasparenza.

[7] Una stable coin è un asset digitale il cui valore è ancorato (pegged) ad una moneta fiat, un paniere di monete fiat o altri asset con valore stabile.

La DeFi fa leva sulla potente tecnologia della blockchain per fornire alternative ai classici fornitori di servizi finanziari, innova servizi già esistenti o ne crea nuovi per migliorare l'efficienza dei mercati finanziari.

2.2.2 Tecnologie e caratteristiche

Dobbiamo ricordare che la maggior parte dei servizi DeFi opera sulla blockchain Ethereum grazie alle sue capacità e disponibilità di adozione da parte di sviluppatori. Successivamente abbiamo visto il ruolo cruciale che hanno gli smart contract, i quali controllano, analizzano, eseguono e documentano eventi e/o azioni rilevanti secondo un set di termini e regole predefiniti.
Adesso è necessario soffermarci su alcune tecnologie, oltre quelle già trattate precedentemente, che giocano un ruolo primario nell'ecosistema della DeFi:

- **Wallets**

  I wallet sono delle interfacce che servono agli utilizzatori per gestire i loro asset su blockchain. Quando l'utilizzatore possiede una chiave privata e ha il completo e esclusivo controllo dei suoi fondi si dice che possiete un "wallet non custodito"; viceversa se la chiave privata è gestita da un'altra entità si parla di "wallet custodito".

- **Dapps**

  Dapps sta per Decentralized Applications e fa riferimento alle applicazioni che combinano uno smart contract con un'interfaccia utente "fornt-end". Sono decentralizzate in quanto il controllo del criterio logico è codificato nello smart contract.

- **DAOs (Decentralized Autonomous Organizations)**

  Una "decentralized organization" indica un contesto dove gli stakeholder detengono la governance, esercitando i propri diritti decisionali tramite voto. Una DAO è inoltre un'entità autonoma, in quanto è in grado di eseguire azioni automaticamente, seguendo le regole dettate dagli smart contract.

- **Oracoli**

  Sono dei servizi ideati appositamente per connettere una blockchain con il mondo esterno[8] "nutrendo" lo smart contract con tutte le informazioni e i dati (ad esempio il prezzo di un'azione o di un token nativo di un'altra blockchain) che gli servono per effettuare una computazione.

Non tutte le applicazioni su blockchain che sfruttano queste tecnologie sono però categorizzabili come progetti DeFi. I protocolli di finanza decentralizzata sono solo quelli sviluppati su blockchain pubbliche che offrono la funzionalità degli smart contract (ad esempio Ethereum), e eseguono le transazioni sulla base delle regole impostate dal protocollo stesso. Un aspetto caratterizzante è il totale controllo sugli asset emessi o gestiti dalla DeFi, sui quali non è prevista l'espropriazione o la custodia da parte di terzi.
È importante non confondere ciò che fanno alcuni exchange centralizzati (ad esempio Binance), i quali, pur offrendo alcuni servizi decentralizzati, applicano una custodia sugli asset digitali e non possono quindi essere identificati come DeFi. Infine, un'altra peculiarità che merita di essere citata è la tipologia di architettura aperta, programmabile e componibile. L'ampia disponibilità del codice sottostante e l'API (Public Application Programming Interface) insieme, possono essere **composti e programmati** dinamicamente per la creazione di nuovi strumenti e servizi finanziari (Figura 2.4). Ad esempio, è possibile utilizzare una stablecoin come base per un derivato che ha come collaterale (garanzia) un prestito.

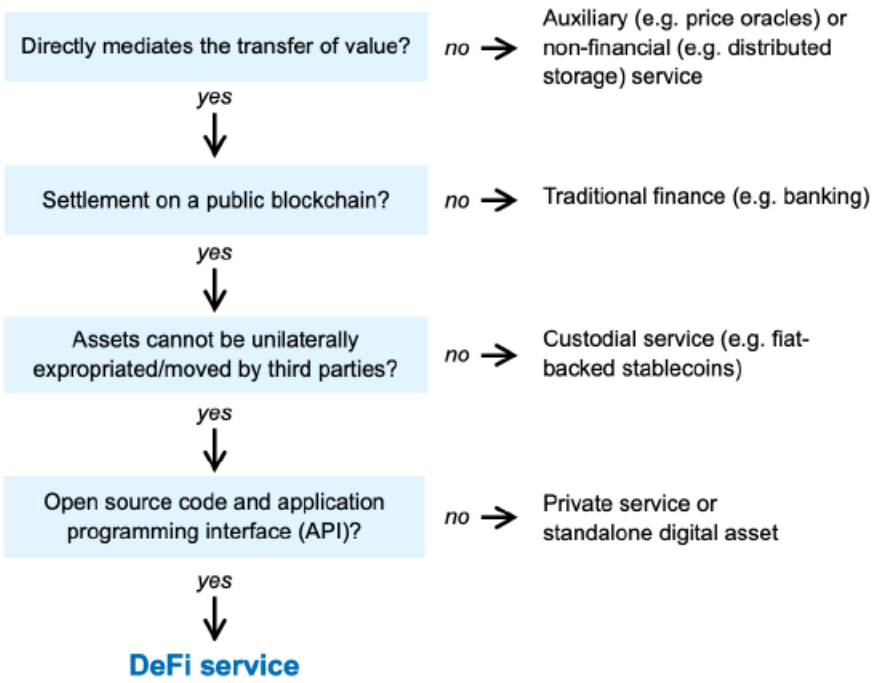

Figura 2.4

Classificazione della DeFi

Fonte: https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf

[8] Gli smart contract sono eseguiti in un ambiente isolato che non interagisce con tutto quello che sta al di fuori della sua blockchain

2.2.3 Governance

Ogni organizzazione necessita di un modello efficiente di governance, fondamentale per il perseguimento degli obiettivi e per assicurarsi che tutti gli stakeholder siano in grado di interagire con la struttura in modo sicuro e affidabile.

Gran parte dei protocolli DeFi utilizza strutture che danno incentivi basati sui token per raggiungere obiettivi di liquidità e di governance. Parlando di liquidità, solitamente il protocollo incentiva il detentore degli asset a "bloccarli" in una pool, ricevendo in cambio dei pagamenti nell'asset che ha bloccato oppure **governance token** (Figura 2.5). I token bloccati servono soprattutto a dare liquidità al protocollo o per essere utilizzati come collaterale per qualche servizio di DeFi, ma possono essere utilizzati per molteplici funzioni come, ad esempio, a pagare le commissioni di liquidazione che guadagnano i market maker in percentuale all'operazione.

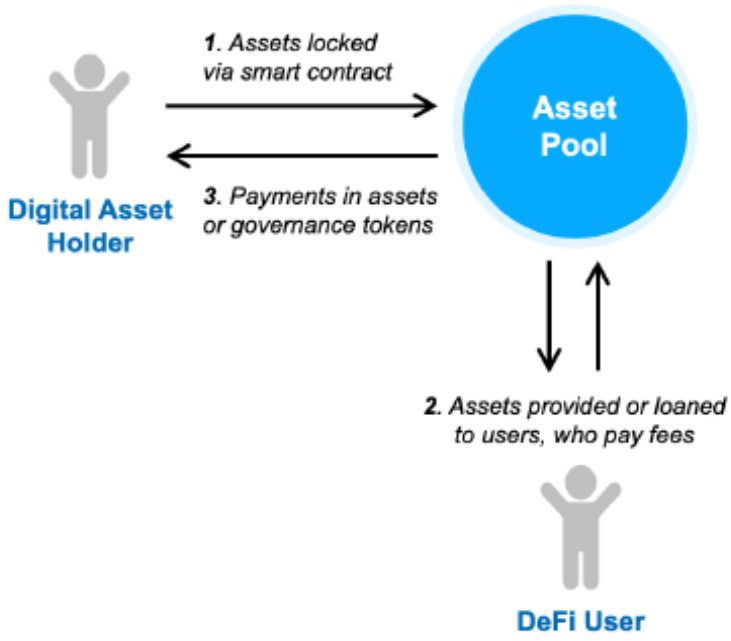

Figura 2.5

Modello a incentivi della DeFi

Fonte: https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf

Abbiamo visto che una delle caratteristiche più importanti della DeFi, è la componibilità e programmabilità della sua architettura. Questo aspetto ha permesso di integrare strutture che ottimizzano i ritorni dal capitale bloccato muovendo i fondi automaticamente attraverso i servizi di DeFi (**yield farming**). Il valore del token utilizzato è legato al livello di attività del progetto, e molto spesso concede diritti di governance sul protocollo

di DeFi, permettendo di votare sulle proposte dei cambiamenti che si propongono di applicare oppure su specifici parametri come, ad esempio, i tassi di interesse.

Il "modello a incentivi" creato dalla DeFi è fondamentale per assicurarne il suo corretto funzionamento, e a supportare questo, i token coprono un ruolo importante innescando un meccanismo che tende a decentralizzare sempre di più i servizi di DeFi: più gli sviluppatori cedono il loro potere sulle decisioni ai possessori dei token, più il loro potere sul protocollo decresce (massimizzando la decentralizzazione)

2.3 I servizi della DeFi

2.3.1 Stablecoin

La DeFi copre un'ampia gamma di servizi, mantenendo i suoi criteri di **componibilità**, **minimizzazione della fiducia** e **programmabilità** dei servizi finanziari. Oltre ai servizi ausiliari che abbiamo già visto come oracoli e wallet, è importante ritornare sul concetto di stablecoin. Quest'ultime danno la possibilità di separare i rendimenti offerti dal protocollo DeFi (e tutti gli altri suoi vantaggi), dai rischi di volatilità dei normali asset digitali.

Le stablecoin hanno il compito di mantenere un valore, ancorato a qualche asset (comunemente il dollaro o altre monete fiat) e il loro "design" può essere di due tipi: "non-custodial" e "custodial". Le prime quando utilizzano gli smart contract per assemblare e liquidare i collaterali attraverso criptovalute o altri asset, prendono il nome di "Asset-Backed Stablecoin" (ad esempio USDC e USDT). Alcune invece, le cd "Algorithmic Stable" cercano di mantenere il peg attraverso una dinamica espansione e contrazione dell'offerta del token originario del protocollo DeFi.

Le stable "custodite" utilizzano come riserva delle valute fiat o asset liquidi. Non sono considerate un servizio DeFi, in quanto sono centralizzate e rimettono la loro fiducia sull'entità che le custodisce.

2.3.2 Credito

Nella forma classica di erogazione dei prestiti, le banche gestiscono lo spread tra i tassi di interesse che paga ai depositanti e i tassi che riceve dai mutui. Al contrario, nei protocolli DeFi che offrono questo servizio (tra cui Compound e Aave che vedremo nel terzo capitolo), vengono raggruppati i token in delle pool soggette a un tasso di interesse determinato dal rapporto tra offerta e prestiti.
Quando un soggetto presta capitale ad un protocollo di DeFi riceve in cambio dei token nativi di quella piattaforma, i quali rappresentano il capitale prestato più uno specifico tasso di interesse. Inoltre, non esiste il

concetto di “spread” in quanto i tassi di prestito e crediti sono lì stessi (al netto dei costi di transazione che sono generalmente pagati da chi offre il servizio).
A differenza dei servizi erogati da istituzioni centralizzate, entrambe le parti (creditori e debitori) mantengono piena custodia sui loro asset e sono liberi di liquidarli in qualsiasi momento.

2.3.3 DEX (Exchange Decentralizzati)

In un ecosistema finanziario ben strutturato, gli exchange giocano un ruolo fondamentale. Di solito un exchange centralizzato sono necessari operatori che salvaguardano i fondi, forniscono un’accurata stima dei prezzi, ma sopratutto per effettuare una transazione, è necessario l’incontro tra chi vuole vendere e chi vuole comprare (un determinato titolo azionario ad esempio).

Gli exchange DeFi, puntano a decentralizzare tutte queste operazioni. Le transazioni sono processate automaticamente dagli smart contract con una logica peer to peer, oppure attingendo a dei pool di token. Mentre la prima logica è molto simile al meccanismo “order book” già da tempo utilizzato, la seconda si distacca totalmente facendo leva sugli “automated market makers” (AMMs) che basano il prezzo sulla liquidità disponibile sul trade. Le piattaforme più famose come Uniswap o PancakeSwap utilizzano il metodo di scambio AMM, e i cd “Liquidity Provider” permettono che gli scambi avvengano, dando liquidità alla piattaforma. In pratica qualsiasi detentore di asset digitali può bloccare i suoi fondi sul DEX, e ricevere parte delle commissioni di transazioni sullo scambio. (Figura 2.6)

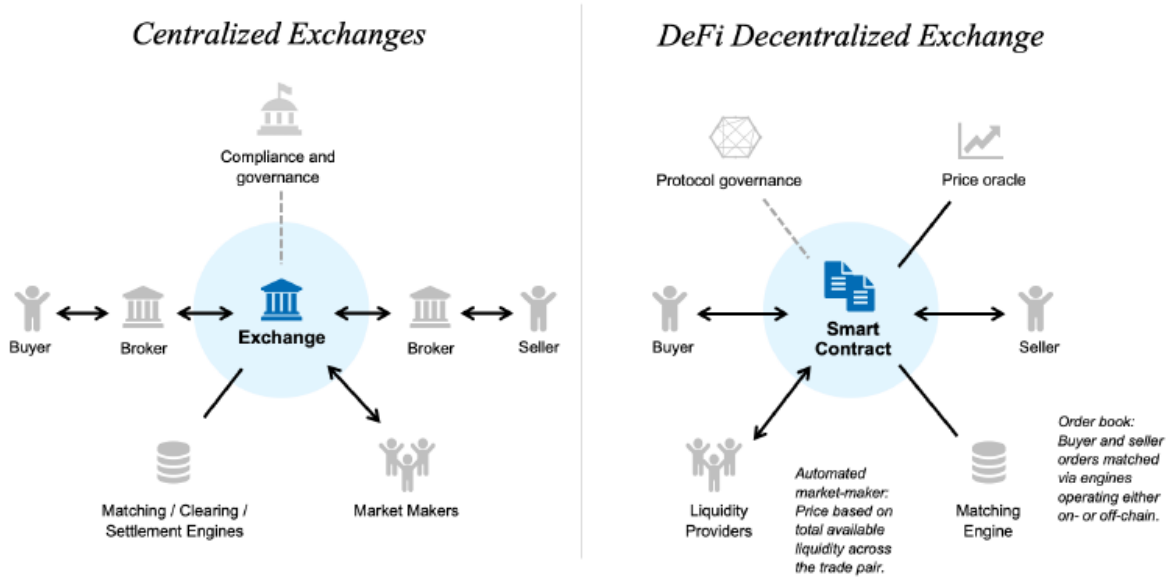

Figura 2.6
Exchange Decentralizzati vs Exchange Centralizzati
Fonte: https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf

CAPITOLO 3 - Una concreta alternativa al tradizionale sistema bancario

3.1 Quanto vale la DeFi?

3.1.1 Total Value Locked

Come abbiamo visto nei capitoli precedenti, la crisi finanziaria del 2008 ha generato un sentimento di sfiducia verso il sistema bancario, e questo ha portato un gran numero di persone a cercare soluzioni nelle tecnologie emergenti del settore finanziario, come la DeFi.
Possiamo riassumere i benefici della finanza decentralizzata in 4 driver: trasparenza, accessibilità, sicurezza e programmabilità.
Il mondo della DeFi rappresenta un importante cambiamento nel modo in cui le persone interagiscono con la finanza e i suoi servizi, come disse il CTO (Chief Technology Officier) della divisione crypto di Robinhood, Johann Kerbrat in un'intervista di Fortune "By removing middlemen, DeFi prompted access to create a fluid, global financial system open to everyone, with no barriers".
Tra le barriere a cui auspica Kerbrat possiamo pensare ai depositi minimi imposti per aprire un conto di risparmio ad esempio, e le tasse aggiuntive sul mantenimento. Nei protocolli DeFi non esistono requisiti di questo genere, e nemmeno "screening" sulla legittimità del cliente e della sua stabilità finanziaria, che sono classici delle procedure KYC (know your customer) sulle quali si basa l'intera struttura dei servizi finanziari erogati da entità centralizzate.

A questo punto, potrebbe venire spontanea la domanda: "Quanto è diffusa la finanza decentralizzata?"
Per rispondere a questa domanda, è opportuno utilizzare un indicatore molto importante per conoscere il peso (in termini economici) di questo fenomeno: il Total Value Locked (TVL).
Il "Total Value Locked" è l'importo aggregato di fondi bloccati nei protocolli di finanza decentralizzata. Molte volte viene utilizzato per confrontare la quota di mercato di un singolo protocollo rispetto agli altri, ma ai fini della nostra analisi ci limiteremo a osservarlo come un indicatore di interesse sui progetti DeFi. Il grafico riportato nella Figura 3.1 mostra la grandezza del mercato, esprimendola sottoforma di valore totale bloccato nelle varie blockchain che supportano applicazioni di DeFi (Dapps).

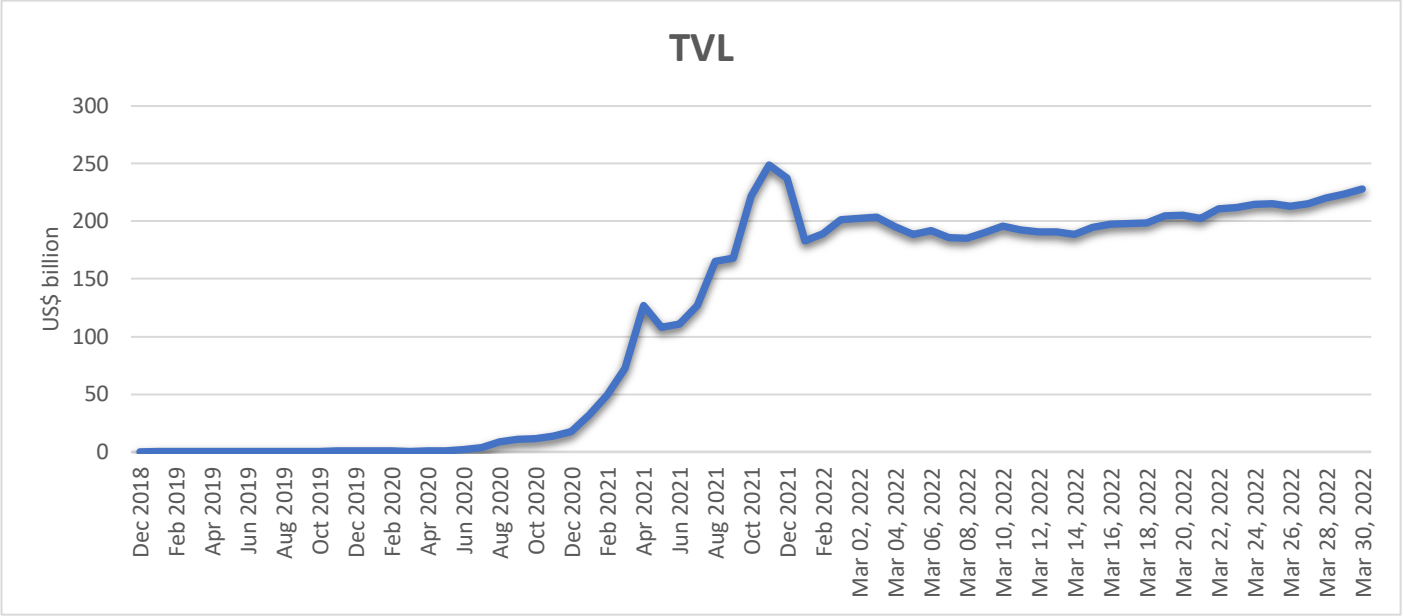

Figura 3.1

Total Value Locked

Fonte: DeFi Llama

Nonostante quello della DeFi sia ancora un mercato emergente, come possiamo vedere dal grafico, già dagli inizi del 2021 i vari protocolli avevano raggiunto i 50 miliardi di dollari raccolti, valore che è radoppiato nel giro di pochi mesi, fino a raggiungere il picco di 200 miliardi a Novembre 2021.

Nei precedenti capitoli abbiamo approfondito i vantaggi della blockchain Ethereum e la dirompente tecnologia degli smart contract, che hanno questa piattaforma il principale framework sul quale sviluppare protocolli di finanza decentralizzata. Il valore aggregato dei progetti sviluppati su Ethereum, occupa quindi una fetta importante sul totale della TVL dei protocolli DeFi (circa il 90%). (Figura 3.2)

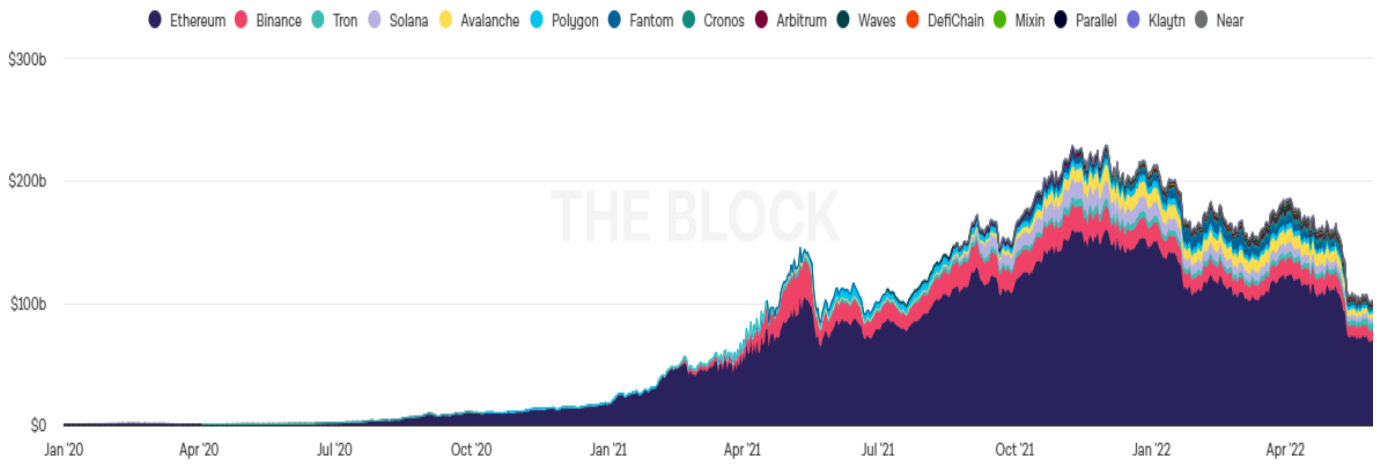

Figura: 3.2

TVL per blockchain

Fonte: DeFi Llama

3.1.2 Aave e Compound

Sono molti i progetti che hanno portato esistenti servizi finanziari nella blockchain, ognuno, in base alle sue caratteristiche, sfruttando alcuni vantaggi dati appunto dalla disintermediazione. Nonostante ciò, molti progetti hanno sperimentato con successo servizi totalmente nuovi, che con i classici intermediari sarebbero stati impensabili.
Tra il 2018 e il 2019 vennero rilasciati numerosi progetti sulla piattaforma Ethereum, tra i quali **Compound**. Questo protocollo però, conobbe un'enorme attenzione qualche anno dopo, nel periodo che prese il nome di "Defi Summer". In questi mesi ci fu un particolare interesse verso un nuovo meccanismo, incorporato per la prima volta dal protocollo Compound: il **liquidity mining** (o yield farming). Tramite il suo token nativo "COMP", i possessori ottenevano poteri di governance e importanti incentivi di liquidità che spinsero sempre più risparmiatori a "coltivare" il loro token, beneficiando delle ricompense che offriva il protocollo. Da quel momento numerosi progetti sfruttarono quest'architettura a incentivi per attirare maggiore liquidità possibile. Lo yield farming si basa dunque sul modello AMM visto nel secondo capitolo, dove i fornitori di liquidità sono ricompensati con le commissioni che vengono pagate sulle transazioni, in proporzione alla loro quota nel pool.

Nel 2020, dopo il successo di Compound, venne rilasciato **Aave,** un protocollo di finanza decentralizzata basato sulla blockchain Ethereum dove gli utilizzatori possono prestare (lending) e prendere a prestito (borrowing) un ampio numero di diverse criptovalute. Il meccanismo del servizio offerto, analogo a quello di Compound, sembra molto simile ai tradizionali modelli di erogazione di prestito, in quanto posso prestare criptovalute guadagnando interessi o prendere capitale a prestito pagandoli.
Di gestire tutti questi asset e i vari accordi (deals) se ne occupano gli smart contract. A differenza delle banche o istituzioni finanziarie in generale, non è necessario rimettere la fiducia (e pagare) su questi ultimi affinché il mio capitale venga protetto.
Aave utilizza un algoritmo per stabilire i tassi, basandosi sul tasso di utilizzo del protocollo stesso. Ad esempio, se non ci sono abbastanza criptovalute rimaste nel pool, i tassi di interesse saranno elevati per incentivare la gente a depositare, viceversa se troppe poche criptovalute vengono utilizzate (ovvero prese a prestito dal pool) i tassi diminuiranno affinché più persone saranno invogliate a prende a prestito.
Prendere a prestito su Aave può essere un'ottima strategia nel caso in cui detengo una posizione lunga, e ho bisogno di liquidità per fare degli investimenti, senza però vendere l'asset (le criptovalute) in quanto significherebbe chiudere quella posizione.
Prima di prendere a prestito, il protocollo richiede un asset da utilizzare come collaterale, e la quantità depositata sarà determinante per il quantitativo massimo che può essere preso a prestito. Inoltre, è possibile decidere a monte se si vuole applicare un tasso fisso o variabile.

Aave ha inoltre introdotto un particolare nuovo servizio che prende il nome di:" **Flash Loan**". Questo tipo di finanziamento può essere usato per sfruttare opportunità di arbitraggio sull'ecosistema delle crypto. I flash loan, non richiedendo un collaterale da depositare, hanno una durata di pochi secondi: praticamente è come se dovessi ripagare il prestito durante la stessa transazione fatta per ottenerlo. Questo meccanismo sembra essere poco intuitivo, ma proviamo a fare un esempio per capire meglio. Consideriamo che un investitore nota che un determinato token ha un certo prezzo sul DEX A e un prezzo maggiore nel DEX B, a quel punto sarà utile sfruttare un Flash Loan per approfittare dell'opportunità di arbitraggio, e quindi il risparmiatore agirà in questo modo: ottiene il prestito, acquista il token nel primo DEX e lo rivende ad un prezzo più alto su un altro, torna il capitale che aveva preso in prestito e si tiene il guadagno. La caratteristica distintiva di questo tipo di operazione, è che avviene tutto in un'unica transazione grazie a uno smart contract.

3.2 Stablecoin

3.2.1 settori principali della finanza decentralizzata

I servizi di Aave e Compound rientrano nella categoria "Lending" che occupa una porzione molto rilevante (in termini di capitale bloccato) nel mondo della DeFi (Figura 3.3), posizionandosi infatti secondo solo dopo gli Exchange decentralizzati.
Nello scorso capitolo ci siamo soffermati ad analizzare quali sono i principali segmenti in cui opera la finanza decentralizzata. Possiamo quindi raffinare l'analisi generale sul TVL fatta precedentemente, per capire quali sono i settori che attraggono più capitale. Per finalità dimostrative, il grafico si ferma soltanto a 5 segmenti, ma i servizi che copre la DeFi sono molti di più e, soprattutto, in continua espansione.

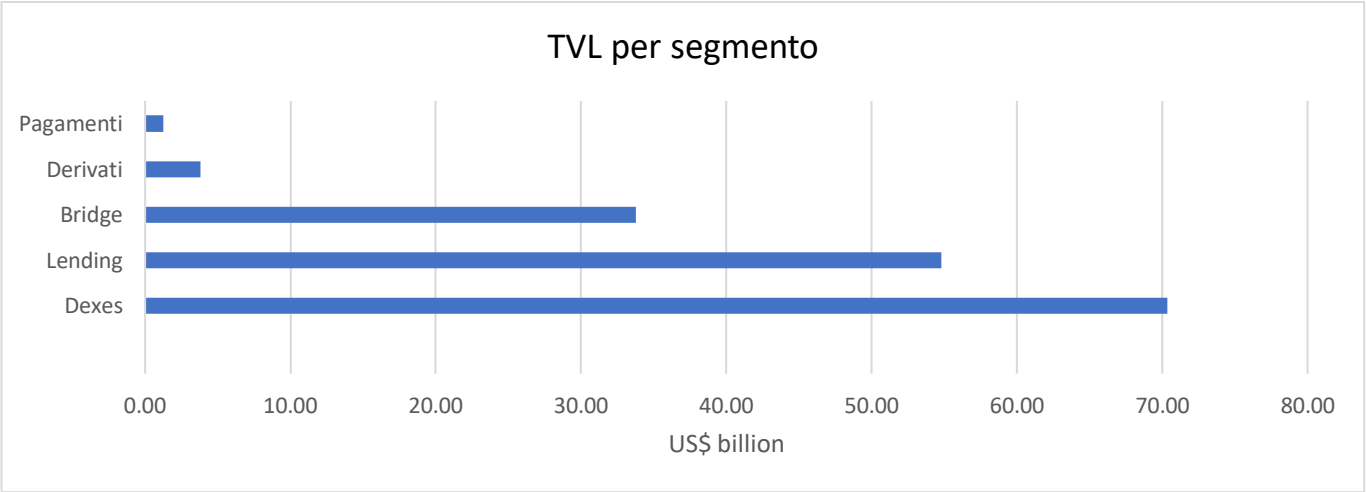

Figura 3.3
TVL per segmento
Fonte: Statista

Oltre ai principali segmenti (Lending e Dexes), occupano una porzione notevole i "bridge". Abbiamo visto che esistono più di una blockchain, e ognuna ha le sue caratteristiche e particolarità, regole e modelli di governance diversi. I bridge sono delle connessioni che consentono il trasferimento di token e/o dati da una blockchain all'altra. In pratica consentono la condivisione di valore tra le varie chain (che altrimenti resterebbero isolate), abbattendone le barriere che rappresentano un limite per la decentralizzazione.

Un'altra categoria di servizi che deve essere citata è quella dei derivati. Come nella finanza tradizionale, anche nel mondo delle criptovalute si possono utilizzare strumenti derivati: ovvero dei prodotti finanziari sintetici il cui valore dipende dall'andamento dell'asset sottostante.
Proporzionalmente al rischio che deriva dall'utilizzo di questi strumenti, il capitale bloccato è inferiore rispetto agli altri servizi della DeFi.
Durante gli anni, è stato riscontrato un elevato interesse per le **stablecoin**, che abbiamo introdotto nel secondo capitolo. Dato il livello di rischio relativamente basso e le opportunità date dai protocolli di lending, hanno attratto molto capitale, imponendoci quindi di ritornare sull'argomento per un'analisi più approfondita.

3.2.2 Il caso di Terra

Nel secondo capitolo è stato introdotto il concetto di stablecoin e i benefici ad esse associati. Va sottolineato che le stablecoin non sono tutte uguali, ma cambiano in funzione di come sono strutturate (ad esempio Asset-Backed e Algorithmic).
Nonostante, come detto prima, possono essere considerate un'ottima scelta per chi voglia sfruttare alcuni dei benefici della DeFi senza sopportare i rischi di volatilità, sembrerebbe di essere ancora lontani da una concreta alternativa alle valute emesse dalle banche centrali.

Poche settimane fa, una delle Algorithmic stablecoin più diffuse "Terra USD" (UST) ha perso il peg con il dollaro, facendo collassare l'intera blockchain sulla quale era sviluppata: Terra. La particolarità di questo network decentralizzato era rappresentata dall'attenzione data alle stablecoin, principalmente quella nativa dell'ecosistema (UST), affiancate da altre crypto che rappresentavano altre valute tradizionali come l'euro, lo yen e il dollaro canadese ad esempio.
La crypto nativa di questo ecosistema è Luna, che gioca un ruolo di fondamentale importanza per garantire il buon funzionamento della blockchain Terra, e cruciale per il mantenimento del peg di UST al dollaro americano. Questa stablecoin algoritmica si basa sull'interdipendenza tra il token nativo LUNA e la stable stessa (UST). Esiste una regola per cui 1 UST può essere scambiato per 1 euro di LUNA. Se UST scende sotto il dollaro, molte più persone saranno invogliate ad acquistare sfruttando l'arbitraggio. L'algoritmo di Terra,

brucia gli UST scambiati con i LUNA per diminuire automaticamente l'offerta, e di conseguenza ristabilizzare la parità di UST con il dollaro, viceversa se UST supera il valore del dollaro ci sarà maggiore convenienza a comprare LUNA e rivenderlo a un prezzo più alto (facendo aumentare l'offerta di UST e provocando una contrazione del prezzo).

Questo meccanismo però aveva un presupposto dietro affinché tutto funzionasse come previsto, ovvero che la liquidità del sistema rimanesse li. Gran parte di questa liquidità era concentrata su Anchor Protocol, il principale protocollo di DeFi della blockchain Terra. Questa applicazione è riuscita ad attrarre ingenti quantità di capitale grazie all'elevato APY[9] (intorno al 20%) sul deposito di UST.
Anchor però utilizzava un modello basato sul periodico rifornimento della yield reserve, e l'interesse che offriva era quindi dinamico. A partire dal 6 maggio, è stata riscontrata una perdita del peg in poche ore (Figura 3.4), e di conseguenza la riserva di depositi su anchor ha cominciato a diminuire, passando in poco tempo da 17 a 14 miliardi di dollari. Una decrescita della riserva come questa ha portato con sé un abbassamento dell'APY, spingendo ancora più persone a ritirare i loro fondi per spostarli su piattaforme più profittevoli.

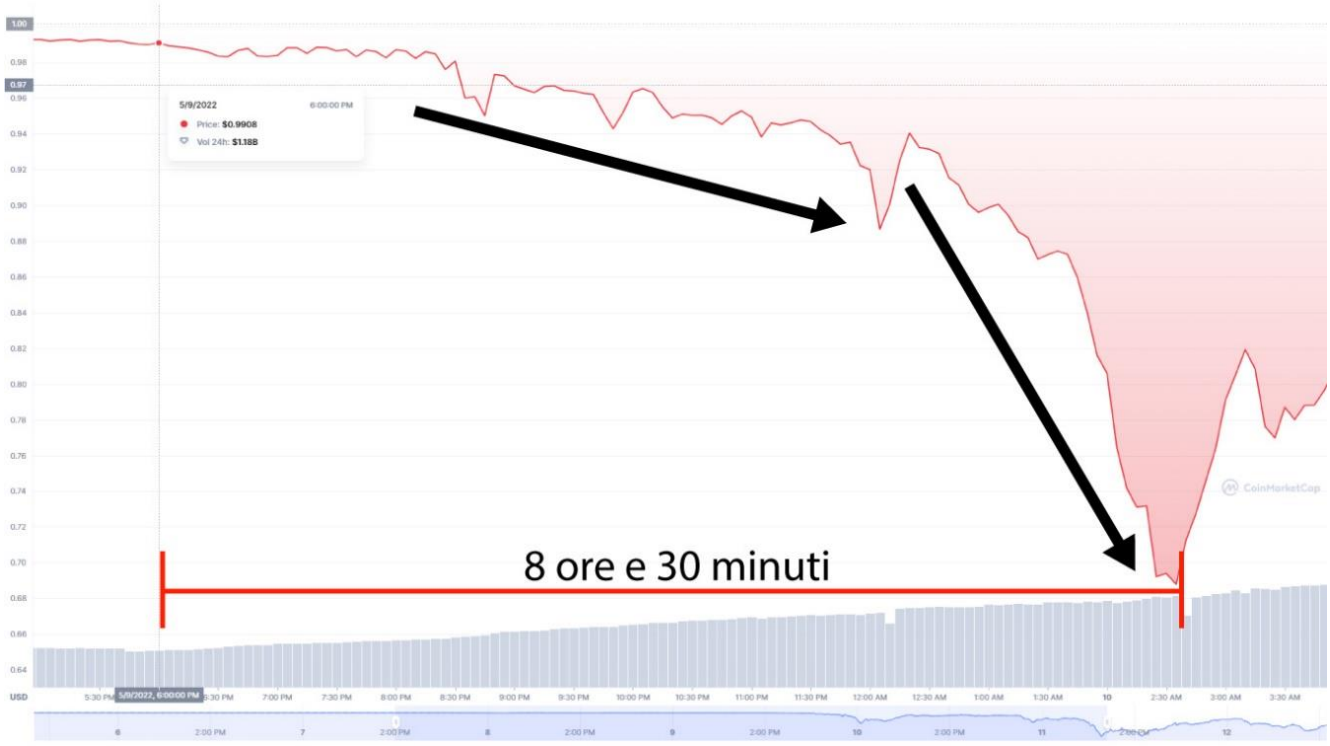

Figura 3.4
Perdita del peg di UST
Fonte: Coinmarketcap

[9] Acronimo di "Annual Percentage Yield", ovvero il tasso composto di rendimento annuo.

Nel frattempo, a causa dell'elevato sell-off, UST iniziò a scostarsi dal dollaro, e LUNA di pari passo perdeva valore passando da 57 a 28 dollari. Come spesso succede, gli investitori furono sopraffatti dal lato emotivo e innescarono una vera e propria "bank run". Purtroppo, data la scarsa regolamentazione attuale nel settore, non ci furono limiti alla picchiata dell'ecosistema; non possono infatti essere bloccati degli "sportelli bancomat" o essere imposti limiti sull'eccesso di ribasso.

Molto probabilmente un attacco speculativo è ciò che ha colpito l'ecosistema Terra, con l'obiettivo di far perdere il peg di UST e guadagnare dalle posizioni short. Questo però non giustifica la struttura del progetto, in quanto avrebbe dovuto essere immune a questi tipi di attacchi. Nel giro di 3 giorni, sono bastate 2 ondate ribassiste a dare il colpo di grazia all'intero ecosistema, facendo scendere UST a 30 centesimi di dollaro (peg ormai impossibile da riprendere) e LUNA con impressionanti perdite del -98/99%. (Figura 3.5)

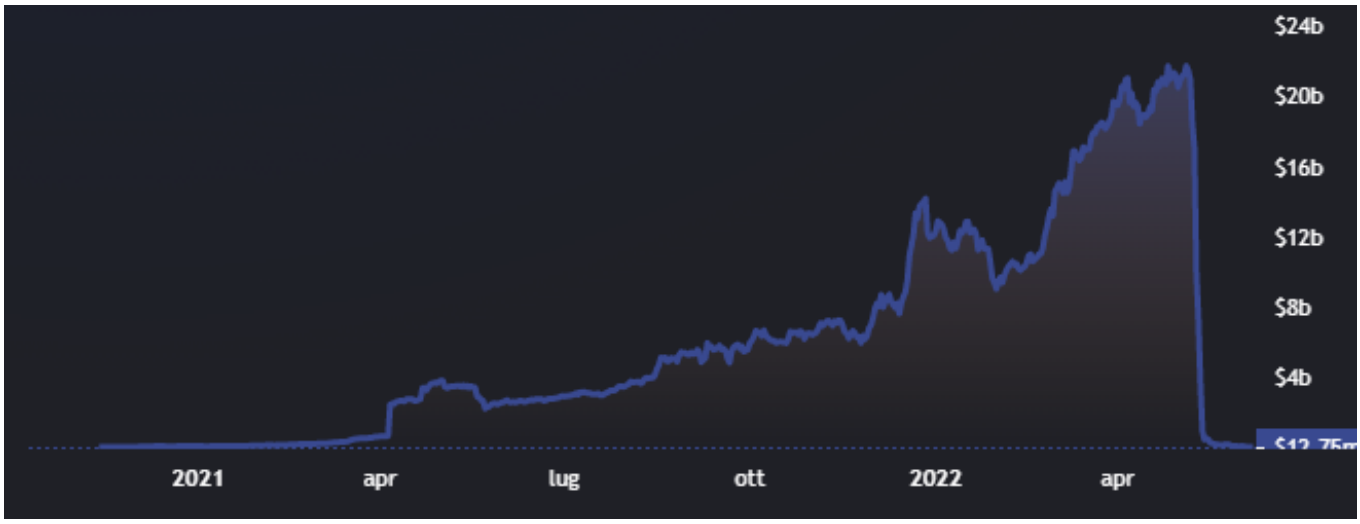

Figura 3.5
Terra TVL
Fonte: Defi Llama

3.2.3 Quali sono i rischi?

Il collasso dell'ecosistema Terra ha causato un brutto colpo all'intero settore delle criptovalute che sta attraversando un periodo di trend negativo, generando in particolare un sentimento condiviso di sfiducia nei confronti della DeFi in generale.
Nonostante nel mondo della finanza ci sono sempre dei rischi da supportare per ottenere un determinato rendimento, a prescindere dalla tipologia dell'asset, va comunque detto che le stablecoin, in particolare quelle coperte da valute tradizionali, risultano essere molto meno rischiose rispetto ad altri asset o valute digitali.

Consideriamo ad esempio USDC, la stablecoin di Circle e Coinbase. Il suo punto di forza (e stabilità) è la copertura 1:1 con il dollaro americano. Questa crypto è molto trasparente, ed è "auditata" periodicamente, in modo da tenere tutti aggiornati sull'effettiva disponibilità delle riserve, anche se non è chiaramente specificato se questi fondi sono detenuti al sicuro, su un solo conto piuttosto che diversi sparsi nel mondo. Questo però non deve per forza preoccuparci, in quanto anche le classiche banche operano in questa direzione, mantenendo una riserva "parziale" in modo da utilizzare il resto dei fondi per investimenti. Anche questo tipo di stablecoin può essere soggetto a leggeri "depeg" ma solitamente sono capaci di riagganciare la parità in poco tempo.
Andando in ordine di rischiosità, subito dopo le stablecoin asset-backed troviamo quelle coperte da altre stablecoin o criptovalute in generale. In questo caso, conviene monitorare di tanto in tanto lo stato degli asset che coprono queste monete digitali, e qualora servisse, essere pronti ad intervenire di conseguenza. La categoria chiaramente più pericolosa è quella delle stablecoin algoritmiche come Terra USD (UST), le quali non hanno riserve.

CONCLUSIONI

Concludendo, possiamo dire che la DeFi deve ancora fare dei passi avanti per diventare un possibile rimpiazzo per il sistema finanziario centralizzato in generale e l'erogazione dei servizi.
Nonostante l'enorme crescita di questo mercato emergente, e i traguardi raggiunti in termini di trasparenza e accessibilità, è sicuramente necessaria una regolamentazione ben costruita su questo mondo, che sia capace di proteggere i protocolli dagli attacchi, e minimizzare la diffusione di progetti scarsi, pur mantenendo le sue peculiarità e la decentralizzazione (caratteristica più importante). Sicuramente, oltre alla regolamentazione, è richiesto anche un progresso nella tecnologia, in modo da gestire i rischi in modo più efficiente, e di conseguenza migliorare l'attrazione di capitale del settore.

Dall'altro lato, qualora la DeFi non ottenesse risvolti positivi, siamo sempre stati fortunati di aver potuto comprendere le opportunità che derivano dall'implementazione della blockchain nei servizi finanziari. Anche se in modo diverso, perdendo gran parte dei benefici della decentralizzazione, esistono sostanzialmente due possibilità per implementare questa tecnologia nell'industria finanziaria:

- Utilizzando come collaterali per i prestiti dei prodotti basati sulla blockchain

Abbiamo visto che il segmento che ha ottenuto più successo insieme agli Exchange decentralizzati è quello dei prestiti (piattaforme lending & borrowing). Molte applicazioni sfruttano la possibilità di "collateralizzare" i prestiti con asset basati sulla blockchain (ad esempio delle criptovalute), traendone numerosi vantaggi in termini di valutazione e controllo.
Questi asset sono considerati infatti come veri e propri investimenti, e danno la possibilità di avere una stima sempre affidabile sul loro valore semplicemente controllando il prezzo di mercato. I benefici che trae chi emette il prestito non si limitano alla semplicità di calcolo del valore di questi asset usati come collaterale, ma va considerata anche la velocità di un'eventuale liquidazione rispetto a quella applicata sui beni immobili, tipicamente usati come garanzia. Quest'ultimi sono anche più complicati da tenere sotto controllo durante la durata del prestito, mentre dei "crypto-asset" sono facilmente tracciabili sulla blockchain pubblica, che registra qualsiasi transazione e/o movimento.
In questo modo chi eroga il prestito può raggiungere mercati che prima sarebbero stati troppo rischiosi a causa dei problemi di valutazione visti sopra, aumentando così anche l'accessibilità al capitale per i risparmiatori che vogliono ottenere un prestito, specialmente in aree meno sviluppate dove le opportunità di indebitarsi sono minori.

- Creando blockchain private (permissioned)

Questa alternativa vede sacrificare i vantaggi dati dalla decentralizzazione, tipici delle blockchain pubbliche. La sostanziale differenza con questo tipo di blockchain sta appunto nella selezione all'accesso (da cui l'aggettivo "permissioned"), e che di solito il controllo non è distribuito come nelle blockchain pubbliche, ma è riservato a uno o pochi soggetti. Come disse il creatore di Ethereum Vitalik Buterin: "L'idea che esista un solo modo di utilizzare la blockchain è completamente sbagliata, ed entrambe le categorie hanno i loro vantaggi e svantaggi". Nel nostro caso, una blockchain privata offre l'opportunità alle banche di rendere più fluido il trasferimento di capitale da creditori a debitori. Permettono inoltre maggiore rapidità e costi notevolmente minori nella fase della raccolta di informazioni sui debitori, che sono imposte dalla legge.

Il grafico della Figura 3.6 dimostra la crescita continua dell'adozione di tecnologie blockchain nel settore bancario, e prevede che per il 2026 la spesa su questa tecnologia superi addirittura i 200 miliardi di dollari.

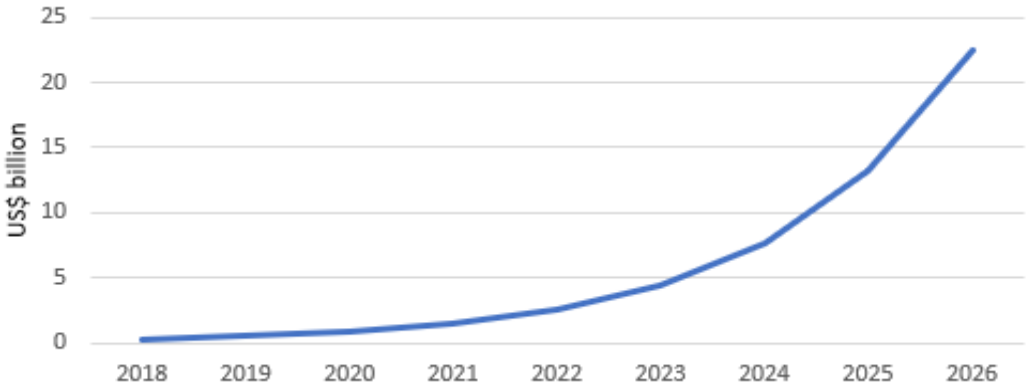

Figura 3.6

Spesa sulla tecnologia blockchain nel settore dei servizi finanziari

Fonte: Statista

I benefici nell'implementazione della blockchain nell'industria finanziaria sono condivisi da tutti gli stakeholder, ovviamente incluse le stesse istituzioni finanziarie. Tra i minori costi derivanti da una standardizzazione dei processi e la collaborazione tra le istituzioni finanziari nelle diverse parti del mondo che permette la blockchain, non è più tempo di essere scettici e distaccati.

Adesso è quindi il momento per le autorità governative, di mettersi a lavorare insieme per facilitare l'espansione della tecnologia blockchain, nel settore finanziario, in un modo sicuro, e in grado di garantire solide protezioni ai consumatori.

BIBLIOGRAFIA/SITOGRAFIA

Chiap, Ranalli, Bianchi., *Blockchain. Tecnologia e applicazioni per il business*, Hoepli (2019)

Antonopoulos., *Mastering Bitcoin*, O'Reilly Media (2014)

Ammous., *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, Wiley (2018)

Martino, Bellavitis, DaSilva., *Blockchain and initial coin offerings (ICOs): a new way of crowdfunding*, IBS (2019)

https://bitcoin.org/bitcoin.pdf.

https://www.bitcoinblockhalf.com

https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume

https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

https://www.pwc.ch/en/insights/digital/defi-defining-the-future-of-finance.html

https://coinmarketcap.com/alexandria/article/what-is-decentralized-finance

https://finematics.com/history-of-defi-explained/

https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf

https://docs.aave.com/faq/swap-and-repay-with-collateral-v2

https://www.repubblica.it/tecnologia/blog/decrypto/2022/05/16/news/tutti_giu_per_terra-349771023/