



UNIVERSITÀ POLITECNICA DELLE MARCHE  
FACOLTÀ DI ECONOMIA “GIORGIO FUÀ”

---

Corso di Laurea triennale in Economia Aziendale

**BLOCKCHAIN, CRIPTOVALUTE E  
FINANZA DECENTRALIZZATA**

**BLOCKCHAIN, CRYPTOCURRENCIES AND DECENTRALIZED  
FINANCE**

Relatore di:  
Prof. Filippo Cossetti

Rapporto Finale di:  
Cristiano Massi

Anno Accademico 2020/2021

## **RINGRAZIAMENTI**

Prima di procedere con la trattazione, vorrei dedicare qualche riga a tutti coloro che mi sono stati vicini in questo percorso di crescita personale e professionale.

Un sentito grazie al mio relatore, il professor Cossetti Filippo, per la sua infinita disponibilità e tempestività ad ogni mia richiesta.

Ringrazio i docenti per il ruolo fondamentale svolto nel mio percorso formativo.

Un sentito ringraziamento va a tutti i miei amici e parenti che sono stati sempre presenti nel momento del bisogno.

Infine, un ringraziamento speciale ai miei genitori, a cui dedico questo traguardo, che senza di loro non avrei raggiunto, sostenendomi e incoraggiandomi in ogni mia scelta.

<b>1. INTRODUZIONE.....</b>	<b>3</b>
• 1.1 Storia.....	3
• 1.2 Cos'è la blockchain?.....	4
• 1.3 Cosa sono le criptovalute?.....	5
• 1.4 Cos'è la finanza decentralizzata? .....	5
• 1.5 Campi di applicazioni della finanza decentralizzata.....	6
<b>2. LA TECNOLOGIA BLOCKCHAIN .....</b>	<b>7</b>
• 2.1 Storia.....	7
• 2.2 Come funziona la blockchain? .....	8
<b>3. LE CRIPTOVALUTE .....</b>	<b>11</b>
• 3.1 Storia.....	11
• 3.2 Bitcoin .....	12
• 3.3 Differenze tra bitcoin e le valute fiat .....	14
• 3.4 Vantaggi e svantaggi di bitcoin: le opinioni degli addetti ai lavori .15	
• 3.5 Nuove criptovalute e blockchain .....	19
• 3.6 Le criptovalute come investimento .....	22
<b>4. DECENTRALIZED FINANCE .....</b>	<b>24</b>
• 4.1 Cos'è e come funziona la finanze decentralizzata?.....	24
• 4.2 Vantaggi e svantaggi della finanza decentralizzata .....	25
• 4.3 Differenze tra la finanza tradizionale, la CEFI e la DEFI .....	26
• 4.4 I principali strumenti finanziari della DEFI.....	27
<b>5. LENDING &amp; BORROWING .....</b>	<b>30</b>
• 5.1 Come funziona un prestito decentralizzato?.....	30
• 5.2 Caratteristiche del prestito .....	32
• 5.3 Rischi del prestito decentralizzato .....	34
• 5.4 Principali piattaforme per il lending DEFI .....	34
<b>6. DECENTRALIZED EXCHANGE .....</b>	<b>36</b>
<b>7. ORACOLI .....</b>	<b>38</b>
<b>8. NON FUNGIBLE TOKEN .....</b>	<b>39</b>
<b>9. CONCLUSIONI.....</b>	<b>40</b>
<b>10. BIBLIOGRAFIA .....</b>	<b>43</b>

# INTRODUZIONE

## Storia

“L’uomo è un animale sociale”. Questo concetto è stato espresso da Aristotele per spiegare il motivo che porta l’essere umano a unirsi in gruppi di persone, definita società, facendo sorgere dei problemi riguardo la convivenza con gli altri soggetti.

Fin dalle civiltà antiche si creò il problema di scambiare i beni tra altre persone.

Il primo metodo di scambio fu il baratto: che consisteva nel “pagare” un bene con un altro bene, creando così un rapporto di cambio.

Questa tipologia di pagamento però era molto complessa nella sua gestione per alcuni motivi: in primo luogo si doveva trovare l’accordo tra il compratore e il venditore per quale bene scambiare l’oggetto in questione, un altro problema era l’accordo sulle quantità da scambiare e infine il problema maggiore era che per ogni bene si doveva indicare il controvalore con qualunque altro bene presente in natura. Si passò così ad introdurre la moneta; ovvero un bene che ha valore intrinseco accettato da tutti, con cui poter acquistare qualunque cosa. Le monete erano composte da metalli preziosi come rame, oro e argento, i quali però erano molto pesanti e ingombranti.

Si decise così, di creare dei titoli di credito emessi dagli orafi che attestavano che una certa persona aveva depositato le sue monete presso quell’orafo e che il soggetto creditore con il titolo in mano poteva andare a ritirare la somma spettante iscritta nel documento: nascono così le banconote. In tempi più recenti, dopo la caduta del cambio aureo e l’introduzione delle monete a corso legale (monete fiat) che hanno la peculiarità di avere un valore fiduciario e non più intrinseco dato che non sono più monete forgiate con una grande quantità di metalli preziosi.

Oggi è presente questa tipologia di moneta, ma dato che ci troviamo in un'era altamente digitalizzata, si cerca di non stampare più moneta in modo fisico ma si tende ad aggiornare un saldo di un conto digitale, senza contare che l'attuale sistema economico si basa sul rapporto tra credito e debito che per la maggior parte di questa contabilità avviene all'interno di server centralizzati. Si è arrivati così alle monete digitali.

L'attuale sistema finanziario oggi, sta attraversando una grave crisi a livello globale, forse potremmo essere alla vigilia di un cambio del sistema economico proprio grazie alle nuove tecnologie come la blockchain e alle criptovalute, simile a quanto avvenuto con il passaggio dal baratto alle monete di metallo o tra il sistema a cambio aureo e le monete a corso legale.

Questo può avvenire anche grazie all'utilizzo della finanza decentralizzata, che consente la circolazione del denaro senza intermediari e in modo trasparente grazie alla blockchain.

## **Cos'è la blockchain?**

La blockchain, letteralmente catena di blocchi, fa parte di un più ampio sistema di tecnologie conosciute come Distributed Ledger<sup>1</sup>.

Infatti, la blockchain è formata da blocchi concatenati tra loro dove all'interno di essi sono presenti dei dati; nel caso delle criptovalute questi sono il denaro che viene scambiato da un soggetto ad un altro.

La blockchain può essere considerata quindi un grande libro mastro pubblico, in cui vengono annotate tutte le transazioni effettuate.

---

<sup>1</sup> Distributed Ledger: registro distribuito.

Questo registro è una rete formata dagli utilizzatori stessi che hanno una copia del registro costantemente aggiornata nel loro computer e sono proprio loro a validare le transazioni che si effettuano su di essa, data la mancanza di un ente centrale che svolga la funzione di garante o di intermediari finanziari.

### **Cosa sono le criptovalute?**

Le criptovalute sono monete completamente digitali utilizzate attraverso la tecnologia blockchain.

Proprio grazie a questa innovazione hanno la caratteristica di non essere emesse da un ente centrale che ne riconosce il valore: il loro valore è dato esclusivamente dall'incrocio di domanda e offerta.

Questa caratteristica, in aggiunta alla giovane età del mercato, rende il valore molto volatile.

Questo ha contribuito negli anni a far conoscere il mondo delle criptovalute come una nuova asset class di investimento molto speculativo.

Il vero obiettivo delle criptovalute però è quello di diventare un mezzo di pagamento a corso legale a tutti gli effetti.

Questo non è possibile fino a quando ci sarà una volatilità del valore elevata, dato che la caratteristica di una moneta deve essere quella della stabilità.

### **Cos'è la finanza decentralizzata?**

La finanza decentralizzata, in inglese Decentralized Finance (DEFI), è una forma sperimentale di sistema finanziario che non si basa su intermediari finanziari centrali come broker, exchange o banche ma utilizza invece smart contracts sulla blockchain.

Proprio gli smart contracts sono alla base dell'assenza di intermediari essendo tutto il sistema gestito in modo automatico, sono infatti protocolli informatici che facilitano, verificano, o fanno rispettare, la negoziazione o l'esecuzione di un contratto, permettendo talvolta la parziale o la totale esclusione di una clausola contrattuale.

La finanza decentralizzata è stata possibile grazie all'avvento della blockchain ma solo negli ultimi anni si è sviluppato un vero e proprio ecosistema, anche grazie all'aumento del denaro che circola in questo tipo di mercato.

### **Campi di applicazione della finanza decentralizzata**

La finanza decentralizzata negli ultimi anni ha visto aumentare il numero di società che si sono impegnate nello sviluppo, implementando strumenti economici sempre più utilizzati.

Questi, altro non sono che gli stessi strumenti che esistono oggi nella finanza tradizionale, con la differenza che il tutto è gestito dagli smart contracts depositati sulla blockchain, senza l'ausilio degli intermediari finanziari classici, come ad esempio le banche.

Esistono differenti tipologie di blockchain in base all'servizio offerto: esempi di strumenti finanziari sono il lending decentralizzato, il DEX<sup>2</sup>, gli oracoli e più recentemente si sono affermate le piattaforme NFT (Non Fungible Token) relative al settore artistico.

Nelle pagine seguenti verranno approfondite le tematiche relative al mondo della blockchain, delle criptovalute fino ad arrivare a comprendere gli utilizzi della finanza decentralizzata.

---

<sup>2</sup> DEX: Scambio decentralizzato.

# LA TECNOLOGIA BLOCKCHAIN

## Storia

La blockchain, letteralmente “catena di blocchi”, è un registro digitale condiviso che non può essere alterato, ideata da dei ricercatori americani, Stuart Haber e W. Scott Stornetta<sup>3</sup>, per catalogare in modo digitale i documenti.

La blockchain si basa sulla crittografia dei dati contenuta in essi, che rendono il contenuto nascosto a chi non ha accesso ai dati.

La soluzione della cifratura viene individuata grazie all’uso di un computer che ha una potenza di calcolo molto più elevata di quella umana.

Grazie alla crittografia la blockchain viene sempre più considerata come un ottimo modo di scambiare dati, quindi anche denaro, tra più soggetti senza ricorrere a terze parti.

La blockchain in questi anni è stata utilizzata, oltre che come struttura per un sistema economico, anche per scopi più disparati, come strumento per la tracciabilità dei prodotti di una filiera produttiva oppure come mezzo di finanziamento per le società: attraverso le cosiddette ICO (Initial Coin Offering), entrate nel mondo delle criptovalute nel 2017 come equivalente delle IPO (Initial Public Offering ovvero offerta pubblica iniziale) del mercato azionario tradizionale. È inoltre possibile usare la blockchain per sottoscrivere un contratto, un prestito e recentemente si è affermata anche come validatore di opere d’arte digitali nel nuovissimo mondo degli NFT (Non Fungible Token).

---

<sup>3</sup> W. Scott Stornetta: fisico e matematico statunitense.



## **Come funziona la blockchain?**

La blockchain utilizza la crittografia che consiste nella cifratura del mittente, del destinatario e del contenuto del messaggio da inviare, in modo da far risultare il tutto anonimo.

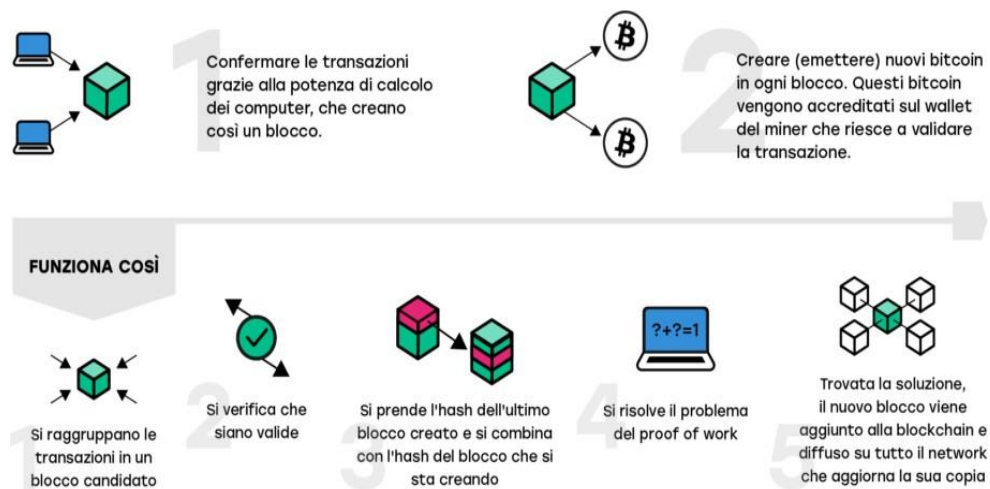
La cifratura avviene attraverso la crittografia a chiave pubblica e chiave privata: la chiave pubblica altro non è che l'identificativo del nostro portafoglio, con cui l'altro soggetto può identificarci, la chiave privata invece, è una sorta di password che serve sia per avere accesso ai fondi ma soprattutto viene utilizzata per codificare l'intero messaggio da inviare. Il risultato di questa codifica crea una stringa, chiamata hash, univoca e immutabile e contraddistingue la transazione e la lega a quella successiva.

La tecnologia blockchain viene considerata un mezzo sicuro per scambiare i dati o nel caso delle criptovalute denaro. Perché immutabile attraverso la concatenazione dei blocchi che avviene grazie all'hash, ovvero un valore che identifica univocamente la transazione: in ogni transazione oltre al suo hash è presente anche l'hash della transazione precedente, che diventa così immutabile dato che se si tenta di cambiare i dati di una transazione. L'hash cambierà a sua volta ed entrerà in contrasto con quello successivo e non verrà così memorizzato in tutti gli altri nodi della blockchain.

Non essendoci nessuna Banca Centrale o Stato a garantire il valore del denaro scambiato e la buona riuscita del trasferimento è stato necessario individuare un metodo per validare le transazioni.

Per fare ciò la blockchain utilizza il consenso distribuito, ovvero che la validazione della transazione deve essere accettata da tutti gli utilizzatori del sistema.

Questo avviene attraverso un protocollo informatico e una misura economica per disincentivare attacchi al sistema chiamato Proof-of-work (PoW), che consiste nel risolvere la cifratura della transazione attraverso la potenza di calcolo del computer. Le transazioni vengono raggruppate all'interno dei blocchi della catena: il primo che riesce a confermare il blocco riceve una ricompensa, che nel caso delle criptovalute è l'emissione di nuova moneta, questo fenomeno viene detto mining.



1. Fasi del processo di mining.

Questo metodo di lavoro è una delle forze di bitcoin: riesce a controllare la quantità di nuove monete emesse ed essendo queste un numero limitato crea deflazione e non inflazione.

Il PoW, però è anche alla base delle critiche rivolte a bitcoin: oltre ad essere un sistema di convalida lento, i detrattori di bitcoin lo reputano anche molto inquinante visto l'alto utilizzo di energia delle macchine di mining.

Per validare i dati all'interno delle blockchain oltre al protocollo Proof-of-Work, sono nati nuove modalità di convalida utilizzabili che hanno le caratteristiche di essere più veloci, efficienti ed economiche rispetto alla PoW. Queste sono:

- Proof-of-Stake (PoS): si basa sulla richiesta da parte del sistema di dimostrare che un determinato soggetto abbia un certo ammontare di

monete nel suo portafoglio, anche qui viene data una ricompensa che consiste in una quantità di nuova moneta emessa.

- Proof-of-Space: un nuovo metodo che sembrerebbe più ecologico, per validare le transazioni si basa anziché sulla potenza di calcolo di processori e schede video ma sullo spazio disponibile nei dischi di memoria del computer ideato da Bram Cohen<sup>4</sup>, inventore per protocollo di condivisione file P2P (persone to persone) BitTorrent.

L'utilizzo della Blockchain e della crittografia nell'economia ha dato inizio ad nuovo sistema economico-finanziario che è quello delle criptovalute.

---

<sup>4</sup> Bram Cohen: informatico e programmatore statunitense.

## LE CRIPTOVALUTE

### Storia

Le criptovalute come le conosciamo oggi, nascono il 18 agosto 2008 quando Satoshi Nakamoto lanciò il software open source di Bitcoin e pubblicò suo il whitepaper (ovvero un rapporto su cosa fosse bitcoin e l'obiettivo di tale progetto), indicando anche quali fossero le migliorie da apportare nel corso del tempo.

Tutt'oggi non conosciamo l'identità di Nakamoto, su cui però ci sono diverse teorie che lo identificano non in un solo individuo ma addirittura in un gruppo più ampio di persone.

Chiunque egli sia però è quasi sicuro sia stato influenzato da un movimento nato tra gli anni '80 e '90 del Novecento da un gruppo di attivisti libertari, ovvero il Cyberpunk<sup>5</sup>.

Alla base di questa idea vi era il concetto di un denaro completamente astratto e non controllato da un ente centrale e grazie alla crittografia era possibile, inoltre proteggerlo in maniera più efficace del sistema bancario tradizionale.

Per analizzare la portata di questo nuovo sistema economico dobbiamo analizzare il periodo in cui Satoshi ha lanciato bitcoin, ovvero nel 2008.

In quel periodo si stava affrontando la crisi portata dall'esplosione della bolla dei titoli sui mutui sub-prime che investì gli Stati Uniti per poi allargarsi al mondo intero.

Inoltre, pochi anni dopo, nel 2011, l'Europa sarebbe stata travolta dalla crisi del debito sovrano. Satoshi infatti ha "inventato" bitcoin come sistema finanziario alternativo a quello attuale, cercando di sviluppare un progetto che avesse come punti di forza le debolezze di quello in vigore: la decentralizzazione e l'anonimato,

---

<sup>5</sup> Cyberpunk: movimento libertario nato all'inizio degli anni '90.

anche se quest'ultimo aspetto è difficilmente applicabile in un mondo completamente informatizzato e data la natura degli attuali Stati che giustamente o meno devono essere a conoscenza dei movimenti di denaro che avvengono sul loro suolo.

Grazie a bitcoin e alla blockchain, da 12 anni a questa parte il mondo della crittografia e della decentralizzazione non fa più parte di una cerchia ristretta di persone che appoggiano un movimento come il Cyberpunk, ma è stata adottata da milioni di persone e società che contribuiscono al suo continuo sviluppo.

## **Bitcoin**

Bitcoin è la prima e più famosa criptovaluta al mondo.

Bitcoin è un protocollo informatico per una moneta completamente digitale inventato nel 2008 da Satoshi Nakamoto per lo scambio sicuro di denaro tramite internet sfruttando la tecnologia blockchain. L'intenzione di bitcoin è quella di sostituire o quantomeno affiancare l'attuale sistema economico e monetario.

Essendo una nuova tecnologia e un nuovo sistema bitcoin ha delle caratteristiche principali che hanno il compito di renderlo più sicuro rispetto allo scambio di denaro tradizionale tramite internet.

Questo avviene grazie ad un protocollo informatico rigido utilizzato grazie alla tecnologia blockchain.

Il protocollo di bitcoin è open-source, ovvero chiunque può leggere e migliorare il funzionamento del sistema (ad esempio rendendolo più scalabile) ma è considerato rigido, ovvero immutabile, perché le sue caratteristiche fondamentali non sono



*2. Simbolo di Bitcoin.*

modificabili: il 12 giugno del 2021 è stato confermato uno dei più grandi aggiornamenti del sistema Bitcoin, il Taproot, che entrerà in vigore il prossimo novembre.

Alla base di bitcoin non c'è nessun ente emittente o garante; questo lavoro è svolto dalla blockchain che garantisce e convalida le transazioni attraverso il protocollo informatico Proof-of-Work (prova di lavoro) per validare le transazioni o più in generale i blocchi della catena, utilizzando la potenza di calcolo dei computer per decodificare la cifratura della transazione.

Chi per primo riesce a validare la transazione avrà in cambio una ricompensa che consiste in una somma di nuovi bitcoin "stampati".

Questo processo viene denominato mining, ovvero estrazione, giocando sulla similitudine tra un minatore che scava per trovare una l'oro.

Il bitcoin, come l'oro, è un bene scarso in natura, perché il protocollo ideato da Nakamoto prevede che esista un numero finito di bitcoin estraibili: 21.000.000. L'emissione di queste monete è controllata dall'algoritmo stesso: infatti ogni quattro anni la quantità di monete emesse come ricompensa per i miners si dimezzano dato che la potenza di calcolo dei computer tende ad aumentare.

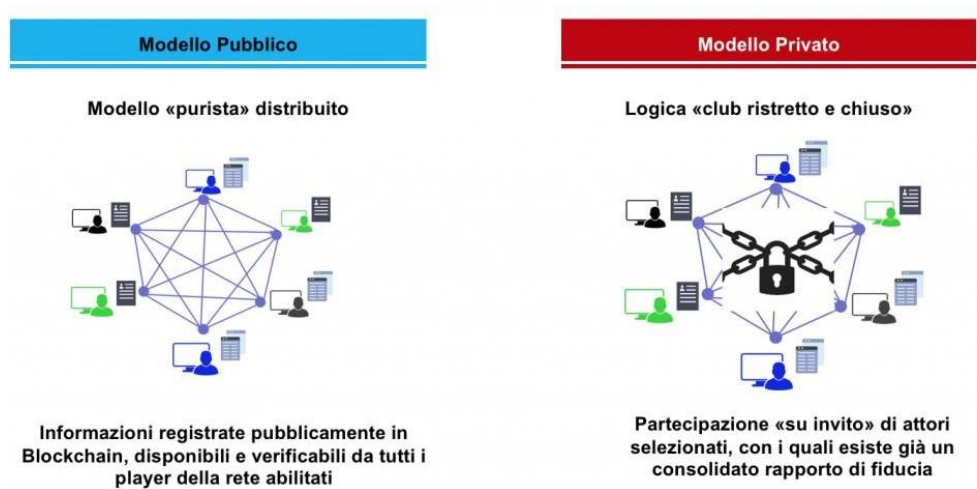
Questa viene denominata difficoltà di mining che viene misurata con un'unità di misura chiamata hashrate.

Ciò consente a bitcoin di essere una moneta deflazionistica, al contrario delle monete a corso legale che tendono ad inflazionarsi a causa della continua immissione nel mercato di moneta da parte delle banche centrali come stimoli all'economia.

## Differenze tra bitcoin e le valute fiat

Queste caratteristiche sono anche le differenze principali che si riscontrano con il sistema delle valute a corso legale:

- La prima differenza è data dall'ente emittente: le valute fiat sono emesse dagli Stati nazionali o dalle banche centrali, invece bitcoin e le altre criptovalute vengono “stampate” in base a un algoritmo chiamato mining;



### 3. Differenza di funzionamento tra sistema centralizzato e sistema decentralizzato.

- Non essendoci alcun ente, il controllo dell'intero sistema è nelle mani degli utilizzatori stessi, creando così un sistema completamente decentralizzato a differenza dell'euro o del dollaro;
- Oltre alla mancanza di un istituto centrale, manca anche la figura dell'intermediario bancario, dato che il denaro viene trasferito peer-to-peer (tra privati) e quindi non c'è nessuno che si occupi del servizio di custodia lasciando ai proprietari del denaro la libertà di gestire e tenere al sicuro la propria ricchezza;
- Un'altra caratteristica di bitcoin e delle criptovalute in generale è che sono frazionabili in una misura fino a 0.00000001 di un bitcoin, chiamato Satoshi

in onore del suo creatore; questa frazione corrisponde in pratica al centesimo di euro, ovvero la parte più piccola della moneta.

- La quantità di moneta stampabile è fissa e non può essere modificata (principio dell'immutabilità del sistema); nel caso di bitcoin questa quantità è indentificata a 21.000.000 di monete che verranno estratte in base ad un algoritmo che "paga" i miners (minatori) che convalidano le transazioni con nuove monete: la ricompensa viene dimezzata dal sistema ogni 4 anni circa, e una stima prevede che l'ultima frazione di bitcoin verrà estratta circa nel 2140;
- Il punto precedente è il motivo per cui bitcoin per natura è deflazionistico, o meglio, è meno inflazionistico delle attuali monete in circolazione (forse a livello economico il vero valore aggiunto di bitcoin), ovvero guadagna valore dato che non può essere stampato a piacimento, così come avviene con le monete comunemente usate oggi che a causa di politiche basate sull'immissione di denaro nel sistema che creano inflazione e quindi l'aumento dei prezzi e la diminuzione del potere d'acquisto dei consumatori.

### **Vantaggi e svantaggi di bitcoin: le opinioni degli addetti ai lavori**

Bitcoin e la blockchain come tutte le innovazioni ha dei pregi ma anche dei difetti. I principali pregi di bitcoin sono quelli elencati in precedenza, ad esempio la decentralizzazione e la natura deflazionistica.

Bitcoin è stato paragonato alle più grandi invenzioni della storia come internet (che molti dicevano essere non essenziale), o alla posta elettronica, i quali entrambi hanno cambiato la nostra vita.



A sostegno di bitcoin si sono espressi personaggi di rilievo del panorama mondiale e anche italiano: i primi a sostenere la causa sono stati i gemelli Winklevoss, che hanno avuto un ruolo importante nella creazione di Facebook, ceduta poi a Mark Zukemberg.

Si possono inoltre citare la senatrice americana Cynthia Lummis, ma anche uomini d'affari come Mike Novogratz, CEO di Galaxy Investment Partners, Tim Draper, Paul Tudor Jones. Nell'ultimo periodo però grazie hedge fund come Microstrategy o Black Rock hanno acquistato quantità enormi di bitcoin.

Ma le criptovalute e la blockchain sono sempre più adottate anche da colossi bancari come PayPal, Visa e Martercard seguite da alcune banche commerciali, ad esempio UBS e società a livello mondiale come Walmart e quasi tutte le società tecnologiche come Microsoft, Amazon e Intel.

Il noto imprenditore Ray Dalio, inizialmente scettico, ha definito bitcoin “un’invenzione straordinaria simile all’oro”.

Nel nostro Paese una posizione più favorevole a bitcoin è stata presa dall’investitore Guido Maria Brera, che in una recente intervista ha affermato “Il bitcoin non ha punti deboli”.

In realtà come qualunque nuova tecnologia, anche bitcoin ha alcuni punti deboli, come ad esempio il costo eccessivamente alto per effettuare una transazione e la lentezza del sistema confrontato con il sistema centralizzato del denaro digitale di oggi.

Il concetto della lentezza però riguarda la blockchain di bitcoin, e dato che è un sistema ancora agli albori si sta cercando di velocizzare il tutto attraverso una maggiore scalabilità grazie al protocollo Lighting Network, che consentirebbe anche di diminuire il costo delle transazioni.

Essendo stato il precursore delle criptovalute, bitcoin da alcuni viene considerato obsoleto e non adatto a diventare un sistema finanziario dato che in questi dieci anni sono nate criptovalute basate su blockchain più performanti ed economiche, ad esempio quelle di Ethereum o Tron, ma questo non bloccherà la crescita di bitcoin che come detto dallo stesso Brera, “potrebbe diventare o è già diventato una riserva di valore” simile all’oro grazie alla sua scarsità.

Un altro aspetto che viene visto come un difetto delle criptomonete è quello di essere asset molto volatili e quindi non avere la caratteristica della stabilità richiesta da una moneta per essere utilizzata come mezzo di pagamento.

Un punto di forza di bitcoin da molte persone è visto come una debolezza: la sicurezza; non avendo un garante la ricchezza deve essere custodita dai singoli proprietari che potrebbero rischiare di perdere le credenziali di accesso ai fondi e non potervi più accedere, comportando la perdita della ricchezza in essi detenuta. Questi aspetti sono la risposta di quella schiera che non vede di buon occhio le criptovalute.

In primis da indicare come soggetti non amanti delle valute decentralizzate sono proprio le banche centrali che gestiscono il sistema economico e monetario attuale, come ad esempio la BCE, che sta cercando di sviluppare un euro digitale basato sulla blockchain: questo fenomeno verrà approfondito nella sezione dedicata alla finanza decentralizzata.

A causa di bitcoin l’alta finanza si è divisa: ci sono soggetti favorevoli come quelli citati in precedenza, ma ci sono anche chi non è attratto da questa nuova tecnologia: il nome più importante da fare in questo caso è quello dell’Hedge Fund per eccellenza Berkshire Hathaway fondata da Warren Buffet il quale si è detto più volte contrario a bitcoin e alle criptovalute in generale affermando di non

possederne e che non che acquisterà mai, perché secondo lui “fondamentalmente non valgono niente”.

Altri muovono a bitcoin la critica di essere uno schema Ponzi, ovvero uno schema piramidale che ha la caratteristica di far guadagnare di più chi entra per primo a spese di chi entra dopo di lui, questa tesi è sostenuta per esempio dall'economista e matematico Nassim Nicholas Taleb.

Altri economisti si sono espressi negativamente sul bitcoin e le criptovalute, come il premio Nobel Joseph Stiglitz che ha affermato che bitcoin non ha alcuna funzione lecita e che dovrebbe essere fermato perché non trasparente come il dollaro.

Altre persone criticano il sistema bitcoin per la grande quantità di energia che utilizza per il processo di estrazione e ciò produce un forte inquinamento, che forse è anche il principale problema della criptovaluta. Tralasciando che anche l'attuale sistema finanziario è informatizzato e posizionato all'interno di server che consumano moltissima energia, è vero bitcoin confrontando soprattutto le dimensioni dei due sistemi consuma molto di più. Questo problema è dato proprio dalla giovane età di bitcoin, che però in futuro potrà essere risolto almeno parzialmente con l'utilizzo di energia rinnovabile, come ad esempio quella solare, per alimentare il sistema, abbattendo così le emissioni di CO2 nell'aria dovute all'utilizzo di combustibili fossili; è da aggiungere però, che già oggi circa il 70% delle mining farm del mondo usa energia rinnovabile.

La caratteristica di pseudo-anonimità di bitcoin ha dato spazio alla critica più comune mossa a bitcoin, quella di essere uno strumento utilizzato per riciclare denaro illecito: infatti agli inizi veniva usato principalmente come fonte di finanziamento per attività illecite, ma che con il passare del tempo e l'utilizzo sempre più comune delle criptovalute questo utilizzo si è notevolmente ridotto.

## **Nuove criptovalute e blockchain**

Cavalcando l'onda del bitcoin sono nate centinaia di nuove monete digitali: oggi se ne contano circa 9000.

Tra queste la più importante dal punto di vista dell'utilizzo e dell'innovazione dopo bitcoin è Ethereum, che è anche la seconda criptovaluta più capitalizzata, ovvero con maggior valore. Ethereum è una blockchain decentralizzata simile a bitcoin sul quale girano altre monete, chiamati token, di altri progetti.

Anche Ethereum utilizza il sistema Proof-of-Work, anche se ultimamente si sta cercando di implementare un sistema di rete attraverso il Proof-of-Stake che risulta più veloce, meno costoso e meno dispendioso di energia. Proprio Ethereum ha dato inizio al fenomeno della finanza decentralizzata (in inglese Decentralized Finance, DEFI).

Il suo obiettivo è quello di creare un sistema finanziario indipendente gestito dagli smart contracts.

Grazie ad Ethereum sono nati progetti simili che hanno lo stesso obiettivo, dapprima basandosi sulla tecnologia già sviluppata e in seguito creando blockchain proprietarie con caratteristiche diverse da quella di Ether, la criptovaluta principale della piattaforma Ethereum.

Alcune di queste sono ad esempio Cardano, fondata da uno dei primi sviluppatori della rete Ethereum, basata su una blockchain nativa di tipo Proof-of-Stake e smart contracts e ha l'obiettivo di rendere la società più sicura, equa e trasparente. Come riporta il sito internet [www.coinmarketcap.com](http://www.coinmarketcap.com), che è il principale portale del settore dove si possono trovare informazioni relative al progetto e tenere sotto controllo l'andamento del mercato, la rete di Cardano viene utilizzata dalle aziende agricole per tracciare la filiera dei propri prodotti.

Un altro utilizzo di Cardano è quello di archiviare in modo sicuro le credenziali contro la contraffazione e di bloccare le merci contraffatte.

Una blockchain decentralizzata open-source tra le più usate è quella di Tron, il cui punto di forza è la scalabilità, infatti il team di sviluppo, tramite il whitepaper ha reso noto che la rete riesce ad eseguire fino a 2000 transazioni al secondo (TPS). La rete si basa principalmente sulla condivisione peer-to-peer di contenuti per l'intrattenimento, avendo anche acquistato uno dei servizi più noti in questo campo, ovvero Bittorrent.

Ultimo aspetto, ma non meno importante è quello che con la rete Tron è possibile creare DApps<sup>6</sup>, ovvero applicazioni decentralizzate per la gestione del denaro: ad esempio gestisce la parte finanziaria attraverso la creazione di token per l'industria videoludica.

Dato che questi ultimi anni sono stati caratterizzati dai social media non poteva mancare un progetto interessante in questo campo, sviluppato sulla blockchain di EOS: Voice; è un social network completamente decentralizzato. Chissà, questa potrebbe essere la nuova frontiera dei social!

Come erroneamente si pensa la blockchain di bitcoin, così come le altre sopra citate non sono anonime, ma vengono definite pseudo-anonime: ciò significa che è possibile risalire al soggetto che ha effettuato la transazione, questo perché le blockchain sono pubbliche ovvero nella transazione sono indicati gli indirizzi del mittente e del destinatario.

Ci sono criptovalute che per via del loro anonimato vengono definite privacy-coin, dato che il loro obiettivo principale è quello di mantenere l'anonimato dei suoi utilizzatori: esempi di queste blockchain sono Monero e Zcash.

---

<sup>6</sup> DApp: applicazione decentralizzata

Le criptovalute non vengono ancora riconosciute come metodi di pagamento a causa della loro volatilità.

Questo limite però viene colmato da una categoria di criptovalute dal valore stabile, chiamate stablecoin, che hanno una volatilità molto bassa del prezzo.

Queste possono essere ancorate a una qualunque valuta fiat; le principali si basano sul valore del dollaro e dell'euro.

La più famosa è USD Tether, che è ancorata al dollaro americano: questo vuol dire che 1 USDT equivale ad 1 \$.

Le stablecoin però non vengono considerate vere e proprie criptovalute, perché per ogni moneta digitale emessa deve esistere la stessa quantità in dollari in un fondo che generalmente è quello della società emittente.

Questo meccanismo rende le monete stabili come una digitalizzazione delle valute fiat.

Le stablecoin però, non funzionano tutte allo stesso modo. Ci sono infatti, delle monete che sono a tutti gli effetti delle criptovalute decentralizzate gestite interamente della blockchain.

La più importante e innovativa di queste è DAI, creata da una delle prime società dedite alla finanza decentralizzata, MakerDAO<sup>7</sup>.

DAI funziona in modo completamente diverso e totalmente indipendente dalla società che lo ha lanciato, ovvero attraverso la blockchain e gli smart contract.

Dai utilizza la teoria dei giochi e incentivi economici bilanciati per sostenere il suo valore di 1 \$.

“In termini più tecnici, tutto si riduce al trading di margine utilizzando la posizione di debito collaterale (CDP).

---

<sup>7</sup> MakerDAO: organizzazione decentralizzata.

Il CDP è un contratto intelligente che supporta gli utenti a ricevere DAI.

Funziona efficacemente come uno strumento di debito con un tasso di interesse.

L'utente di CDP ha registrato garanzie in eccesso rispetto al valore del prestito al fine di garantire la propria posizione debitoria.

Quando un singolo Dai scende al di sotto di 1 \$, i meccanismi di tariffazione del contratto intelligente incentivano gli utenti ad aumentare il prezzo.

Quando un Dai vale più di 1 \$, gli incentivi funzionano al contrario. In una di queste occasioni, gli attori razionali possono fare soldi a causa delle oscillazioni dei prezzi.

Più Dai si discosta dalla media, migliori sono gli incentivi per riportare il prezzo a 1 \$".

Le stablecoin hanno accentuato la funzione di pagamento delle criptovalute e per contrastare questo fenomeno in forte crescita, le banche centrali hanno deciso di sviluppare le proprie monete in forma digitale sfruttando la blockchain, le cosiddette Central Bank Digital Currencies (CBDC).

Queste però sono più simili alle stablecoin basate sul sottostante in dollari che a delle vere e proprie criptovalute dato che le blockchain nel caso delle CBDC non sono decentralizzate, ma centralizzate facendo venir meno l'utilità di una blockchain trasparente, non differenziandosi molto dall'attuale sistema finanziario dato che la maggior parte del denaro in circolazione è già digitale e il contante copre una percentuale minima.

## **Le criptovalute come investimento**

Una delle caratteristiche delle criptovalute è la volatilità del loro prezzo essendo un prodotto tecnologico recente e a causa delle dimensioni non molto grandi del mercato risultato molto speculative.

Grazie a questa diffusa speculazione sono molte le persone che hanno fatto fortuna con bitcoin, specialmente i giovani nati a cavallo tra gli anni '90 e i primi anni 2000; i cosiddetti millennials.

Nel 2009 un bitcoin valeva meno di 0,01\$ e il suo massimo lo ha raggiunto qualche mese fa arrivando a toccare 65000\$ che lo rende l'asset più performante della storia.



4. Grafico del prezzo di Bitcoin dal 2013 al 28 maggio 2021 (fonte: <https://coinmarketcap.com/currencies/bitcoin/>).

Recentemente Goldman Sachs ha definito le criptovalute come una nuova asset class, lanciando dei contratti futures proprio su bitcoin.

Bitcoin ancora oggi, purtroppo, viene visto solamente dal punto di vista speculativo, ma che potrebbe portare a una rivoluzione finanziaria.



## DECENTRALIZED FINANCE

### **Cos'è e come funziona la finanza decentralizzata?**

Dopo l'avvento delle grandi multinazionali dell'informatica e del commercio via internet, negli ultimi anni si è sentito il bisogno di proteggere i propri dati in rete attraverso una più diffusa decentralizzazione.

La blockchain e le criptovalute hanno contribuito allo sviluppo di sistemi sempre più decentralizzati.

Il primo passo è stato quello della condivisione di file tra utenti finali, il cosiddetto peer-to-peer, per poi cercare di rendere meno controllabile da poche persone la finanza, si è arrivati così al concetto di finanza decentralizzata denominata in inglese Decentralized Finance o semplicemente DEFI.

La finanza decentralizzata è il movimento che sfrutta le reti decentralizzate per trasformare i vecchi protocolli finanziari in protocolli affidabili e trasparenti senza intermediari.

Questo nuovo tipo di finanza non prevede quindi la presenza di intermediari o enti che gestiscano i rapporti di denaro tra i soggetti: il tutto viene mosso dalle cosiddette Dapps, ovvero Decentralized Applications formate da diversi smart contracts.

Questo concetto consente di ridurre i costi di gestione e commissioni: si pensi a quelle persone che hanno necessità di mandare del denaro ai parenti che si trovano in un altro Stato che devono sostenere commissioni elevatissime anche per piccole somme di denaro; con la DEFI e l'utilizzo delle criptovalute questo è possibile.

La finanza decentralizzata ha anche l'obiettivo di rendere accessibili quegli strumenti che necessitano di un conto corrente bancario a chi non ha la possibilità di averne uno, dato che circa 2 miliardi di persone non ne possiedono uno.

La finanza decentralizzata è un'innovazione molto recente e ancora in fase di sviluppo ma potrebbe essere considerata come una nuova frontiera della finanza tradizionale o più semplicemente affiancarsi ad essa.

## **Vantaggi e svantaggi della finanza decentralizzata**

La finanza decentralizzata ha dei vantaggi e degli svantaggi.

Alcuni dei vantaggi però, a volte possono diventare dei punti deboli di questa tecnologia.

Il primo punto a favore è la decentralizzazione che consente di ridurre costi degli intermediari, ma se mal gestita la decentralizzazione può causare molti danni.

Un esempio può essere un exchange che se centralizzato espone al rischio di un attacco hacker per derubare i soldi degli utilizzatori, ma se l'exchange è decentralizzato il rischio è dato dalla possibilità di perdere le chiavi di accesso al portafoglio online.

Un altro vantaggio è quello di dare una vera libertà finanziaria, ad esempio ad un'azienda che vuole cercare finanziamenti da tutto il pianeta, ma che potrebbe trasformarsi in un contro qualora questa libertà venisse usata da criminali.

Uno svantaggio che presto potrebbe diventare un punto di forza per la DEFI è la sicurezza: oggi, esclusi i progetti con maggiore capitalizzazione, non risultano molto sicuri, ma considerando la velocità di questo settore a svilupparsi presto la sicurezza di questi protocolli potrebbe essere equiparata a quella delle grandi multinazionali; basti pensare a bitcoin che più soggetti lo utilizzano più diventa sicuro.

Un ultimo vantaggio molto importante è la velocità delle transazioni.

## **Differenze tra la finanza tradizionale, la CEFI e la DEFI**

Grazie all'avvento della blockchain si è sviluppata la finanza decentralizzata che ancora è in fase sperimentale e attualmente concede un'alternativa a quella classica; tra le due ci sono sostanziali differenze.

La finanza tradizionale si basa su istituzioni come le banche o intermediari che gestiscono i rapporti tra soggetti o che danno garanzia a tutto il sistema, ma che non hanno un alto grado di trasparenza.

La finanza decentralizzata si basa sulla trasparenza di tutto il sistema e contemporaneamente sulla riservatezza dei dati personali.

Come visto in precedenza, la finanza tradizionale ha dei punti deboli che la DEFI cerca di arginare: infatti quest'ultima non ha bisogno di intermediari perché il tutto viene gestito dalla tecnologia blockchain grazie agli smart contracts.

Nel sistema tradizionale un normale contratto utilizza terminologia legale per specificare i termini della relazione tra le entità che stipulano il contratto, uno smart contract utilizza codice informatico.

Ciò consente inoltre di avere una minore quantità di burocrazia che consente di velocizzare i processi finanziari, al momento però, a discapito di una sicurezza meno elevata rispetto al sistema classico.

Come finanza alternativa a quella tradizionale non vi è solo la DEFI, ma esiste anche la CEFI (Centralized Finance) ovvero finanza centralizzata che si differenzia da entrambe.

La CEFI è costituita da quelle aziende che forniscono servizi attraverso la blockchain e le criptovalute ma non hanno la caratteristica della decentralizzazione.

La CEFI ha quindi i pro e i contro sia della DEFI che della finanza tradizionale, come ad esempio la custodia dei fondi dei clienti.

CEFI e DEFI condividono lo stesso obiettivo ossia fornire l'accesso ai mercati ed ai servizi finanziari alle persone ovunque nel mondo, ad esempio a persone che si trovano sotto un regime dittatoriale o che non hanno accesso ai canali finanziari tradizionali, tramite l'utilizzo delle criptovalute.

La differenza tra questi due sistemi è data dal metodo che utilizzano per raggiungere lo scopo comune: con la CEFI gli utenti si affidano alle persone che sono dietro a un business che hanno il potere di eseguire le operazioni; con la DEFI invece, gli utenti si affidano alla tecnologia, ed è essa che regola l'intero funzionamento del sistema.

## **I principali strumenti finanziari della DEFI**

La finanza decentralizzata ha sostanzialmente gli stessi strumenti della finanza tradizionale che però vengono utilizzati attraverso gli smart contracts della blockchain e le criptovalute.

Come detto in precedenza la DEFI è gestita in modo autonomo dalla blockchain che utilizza gli smart contracts per regolare i rapporti economico-finanziari.

Questo può avvenire grazie a quegli strumenti appositamente creati per ogni esigenza finanziaria: si chiamano Dapps, ovvero Decentralized Applications.

Per creare questi strumenti finanziari esistono dei protocolli DEFI appositi: uno di questi è 0X.

In DEFI è anche possibile creare delle organizzazioni governate con regole digitali e controllate direttamente dagli azionisti: queste sono le DAO (Decentralized Autonomous Organizations), organizzazione autonome decentralizzate.

Nel mondo della Blockchain sono presenti anche tutti quegli strumenti che risultano essere utilizzati maggiormente dai chi opera attraverso la finanza tradizionale:

questi sono ad esempio la richiesta di prestiti attraverso piattaforme specifiche, la possibilità di effettuare acquisti istantaneamente attraverso progetti come il Lightning Network di Bitcoin o piattaforme che consentono di assicurarsi senza che siano presenti intermediari come le assicurazioni.

In questo ambito sono presenti anche le stablecoin, che sono delle criptovalute dal valore stabile che consentono di effettuare acquisti senza il rischio di avere una volatilità del prezzo molto elevata. Queste monete, per non far fluttuare il loro prezzo vengono ancorate ad un paniere molto ampio contenente altre valute titoli e metalli preziosi.

Sono presenti anche dei protocolli che consentono di depositare fondi come in un conto risparmio: questi sfruttano lo staking della tecnologia Proof-of-Stake che consente di avere in piccolo ritorno economico sotto forma di interesse potendo scegliere se vincolare o meno il denaro; il primo caso però, viene effettuato attraverso lo yield farming.

Attraverso la finanza decentralizzata è possibile anche effettuare operazioni di investimento attraverso exchange decentralizzati, ovvero senza un'autorità centrale.

Si possono effettuare previsioni su eventi futuri, utilizzare la tecnica del margin trading attraverso broker decentralizzati o comprare derivati.

Nell'ultimo anno è fiorente anche il mercato dell'arte digitale attraverso gli NFT (Non Fungible Token).

L'acquisto di derivati e di opere d'arte è possibile non solo in riferimento esclusivo al mondo blockchain (on-chain), ma si possono scambiare anche beni e servizi reali (off-chain) attraverso la tokenizzazione dei beni reali attraverso un nuovo strumento: gli oracoli.

Essendo le criptovalute per definizione anonime o pseudo-anonime è complesso risalire al proprietario di un fondo ma per motivi di antiriciclaggio e per venire incontro alle istituzioni, la DEFI è riuscita a decentralizzare anche il processo di identificazione che viene usato quando si vuole avere accesso ai servizi bancari tradizionali.

In seguito, verranno analizzati alcuni degli strumenti più utilizzati.

## LENDING & BORROWING

La nostra economia si basa principalmente sul credito e sul debito.

Anche nella finanza decentralizzata è possibile chiedere o concedere un prestito, la differenza sostanziale è quella che il denaro non viene erogato da un ente ma gli smart contracts gestiscono in modo automatico questi rapporti, questo viene chiamato lending decentralizzato.

### **Come funziona un prestito decentralizzato?**

Il prestito attraverso piattaforme decentralizzate, come quelli concessi dagli istituti finanziari centralizzati, ha bisogno di una garanzia in grado di assicurare al creditore che il debito venga ripagato.

Il debitore è generalmente una persona che ha bisogno di liquidità e quindi chiede un prestito alla piattaforma, che essendo decentralizzata viene gestita da smart contracts e quindi la possiamo definire una DApp.

Le piattaforme che permettono di prestare denaro nel panorama DeFi si distinguono in due tipologie: la prima fa riferimento a quelle che permettono di prestare denaro generando nuovi assets nelle quali a seguito del deposito di un collaterale a garanzia viene generata una stablecoin ancorata generalmente al prezzo del dollaro.

Così facendo si crea uno strumento finanziario che ha un valore stabile, collateralizzando un asset volatile come la criptovaluta, senza che l'intervento di un intermediario possa bloccare il processo: questo viene definito CDP (Collateral Debt Position).

L'erogatore sarà quindi direttamente uno smart contract che a fronte della garanzia del collaterale potrà emettere una quantità infinita di debito.

La seconda possibilità consiste nel prendere in prestito asset già esistenti e presenti dentro una pool di liquidità.

In questo caso, l'individuo che richiede il prestito prende dei fondi che già esistono, non si ha dunque il processo di generazione.

Si tratta quindi di un modello più simile a quello del sistema bancario, con l'unica differenza che per prendere il prestito occorre lasciare un collaterale più alto di quello che è il debito. Il livello di sicurezza è allora maggiore.

Se da un lato si ha un lender che inserisce dentro un pool (riserva di liquidità) le somme che ha intenzione di prestare, dall'altro si ha un borrower, richiedente il prestito.

Chiuso il prestito, il borrower riavrà indietro il collaterale messo a garanzia, sul quale però saranno calcolati gli interessi destinati al lender.

Un'altra figura importante interna a queste piattaforme è quella dei keeper, che verificano la collateralizzazione cosicché quando il valore della garanzia va al di sotto di una certa soglia, il prestito viene liquidato e il debito sanato. In questo modo, il lender rientra dal proprio prestito. Sono proprio i keeper che comprano i collateral in caso di liquidazione.

Dal punto di vista del creditore invece, si possono semplicemente depositare delle stablecoin in eccesso o inutilizzate e ricevere degli interessi dalla piattaforma che gestisce quindi la linea di credito-debito e i rispettivi interessi maturati.

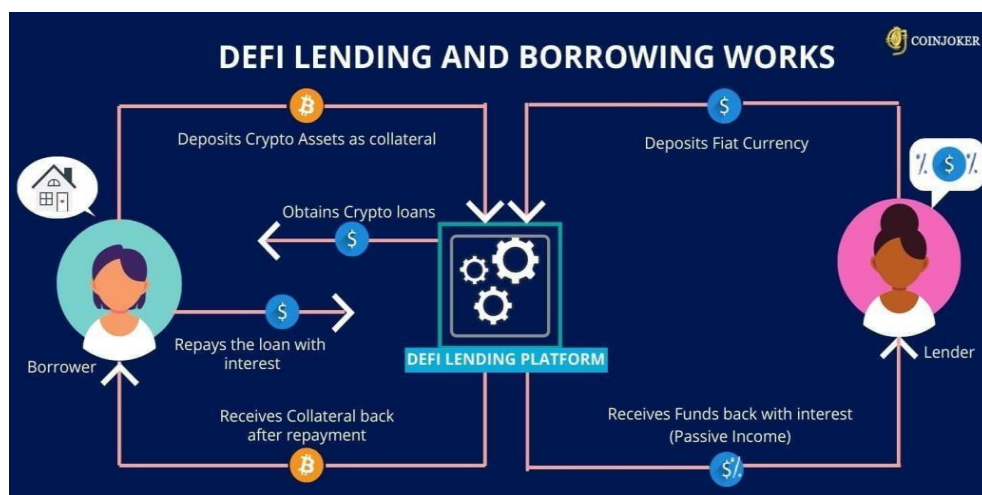
Oltre a gestire i fondi, queste piattaforme possiedono anche una riserva di liquidità per garantire il prelievo in qualsiasi momento.

Questo meccanismo consente di concedere prestiti a chi ha bisogno di denaro, prendendolo da chi ne ha in eccesso, cercando di redistribuire la ricchezza in maniera efficace e senza perdita di benessere.



A questo sistema è stata mossa la critica di creare denaro dal nulla, ma ciò non è corretto, dato che come descritto sopra il debito deve essere coperto da una garanzia o un sottostante.

L'unico svantaggio potrebbe essere che i prestiti possono essere richiesti da chi ha già una quantità di denaro da vincolare, potendo creare sempre più disparità sociali ma anche il sistema del credito tradizionale è nato secondo questo principio, il quale però è regolato dall'uomo che ha causato ingenti danni all'economia attraverso questo strumento, come ad esempio la crisi dei mutui SubPrime<sup>8</sup> del mercato azionario americano.



5. Struttura del prestito decentralizzato.

## Caratteristiche del prestito

Quando ci si rivolge a uno smart contract per chiedere o concedere un prestito si devono prima identificare le caratteristiche che esso deve avere: in base ad esse si decide quale piattaforma utilizzare.

<sup>8</sup> Crisi dei mutui SubPrime: crisi finanziaria nel settore immobiliare scoppiata alla fine del 2006 negli Stati Uniti.

La prima differenza, come descritto sopra è quella tra un prestito con l'utilizzo di un CDP o di una riserva di liquidità.

Una caratteristica delle piattaforme di prestito da tenere in considerazione è quella che esse possono essere Custodial o Non-Custodial:

- La prima identifica una piattaforma centralizzata che detiene le chiavi private dei portafogli per i clienti fornendo sicurezza e backup per le risorse, in questo modo non si avrà il pieno controllo di esse;
- La seconda identifica invece una piattaforma decentralizzata che un detiene le chiavi dei clienti, i quali hanno il pieno possesso dei loro fondi con il rischio però di essere gli unici responsabili della gestione e perdita perenne dei fondi.

“Un’ulteriore distinzione è la fonte dei prezzi, cioè il modo di fornire alla piattaforma il prezzo del collaterale.

Il prezzo può essere dato da un ente centrale, con il risultato di avere un single point of failure, o può essere ottenuto in maniera decentralizzata.

La tempestività nel fornire i prezzi è fondamentale per il buon funzionamento del sistema, poiché quando il collaterale va sotto una certa soglia si rende necessario chiamare il margin call per segnalare la non più sana posizione.

Quest’ultima va risanata per evitare che la piattaforma vada in default.

Quando una posizione di debito è dichiarata non sana, i keeper acquistano il collaterale e inseriscono la differenza necessaria a risanare la posizione.

Il sistema è aperto a chiunque possa comprare il collaterale, abbattendo così il rischio del di default della piattaforma.

Allo stesso tempo può essere chiuso con la liquidità recuperata in maniera centralizzata dalla stessa piattaforma.

Le piattaforme possono essere open source, hanno quindi un codice aperto e leggibile a tutti o viceversa avere un codice proprietario, non aperto e quindi non conosciuto dagli utenti”.

## **Rischi del prestito decentralizzato**

Essendo il prestito decentralizzato uno strumento nuovo, si possono incorrere in alcuni rischi. Perciò si devono valutare alcuni aspetti.

Innanzitutto, si deve controllare se lo smart contract è open source, quindi se effettivamente è decentralizzato e trasparente, in seguito è da valutare l’audit della piattaforma ospitante, per non incorrere in mancanza a livello di sicurezza.

Sono presenti poi dei rischi che possono riguardare il collaterale nel caso di momentanei crash del mercato delle criptovalute o di continua volatilità negativa, e che potrebbero abbassare il rapporto di collateralizzazione mettendo potenzialmente a rischio la piattaforma e il sistema.

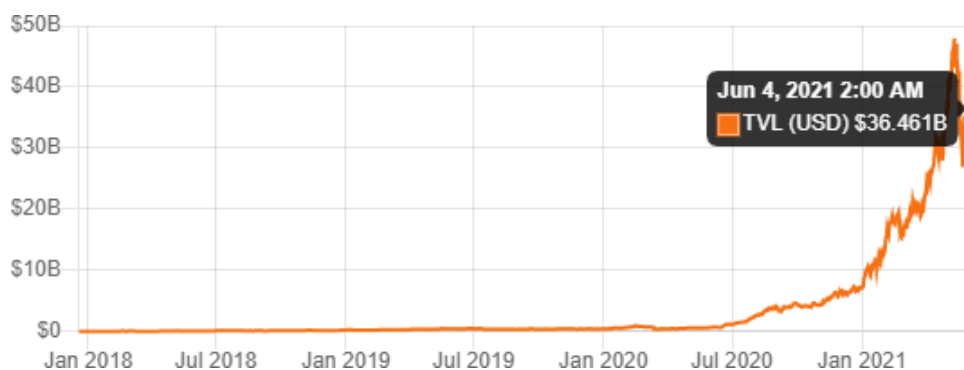
I rischi normativi sono invece dei rischi esterni alla piattaforma, dovuti all’eventuale intervento di un regolatore.

Infine esistono i rischi tecnici, vale a dire quelli legati al disegno della piattaforma. Ogni piattaforma ha infatti i suoi punti di forza e di debolezza a seconda della sua struttura.

## **Principali piattaforme per il lending DEFI**

La finanza decentralizzata è una tecnologia molto recente, ma in pochi anni sono molte le aziende che hanno contribuito alla crescita esponenziale di questo settore. In figura si può vedere in dollari la quantità di denaro bloccata su piattaforme che concedono prestiti in modo decentralizzato: in data 4 giugno 2021 risultano essere

vincolati più di 36 miliardi di dollari, con una crescita esponenziale dalla metà del 2020.



6. Dollari bloccati su piattaforme di prestito decentralizzato ([www.defipulse.com](http://www.defipulse.com)).

La piattaforma di maggiore utilizzo in questo ambito è Aave, con circa il 10% del valore complessivamente bloccato.

Questo sistema di prestito è costruito sul protocollo Ethereum attraverso una serie di smart contracts.

In particolare, il prestito avviene tramite il protocollo Aave che supporta oltre 17 criptovalute.

Un'altra piattaforma da nominare è Maker, che è anche piattaforma che gestisce, sempre in modo decentralizzato, la stablecoin DAI, uno dei progetti più all'avanguardia nel campo delle criptovalute stabili.

Altre piattaforme importanti sono Compound, Liquidity and Band Protocol.

Tutte queste piattaforme operano sia sulle blockchain proprietarie sia su quella di Ethereum, che risulta essere un riferimento dell'intero mercato DEFI sia perché è la seconda criptovaluta per capitalizzazione, sia perché risulta essere una delle blockchain tra le più innovative, scalabili e trasparenti.

## DECENTRALIZED EXCHANGE

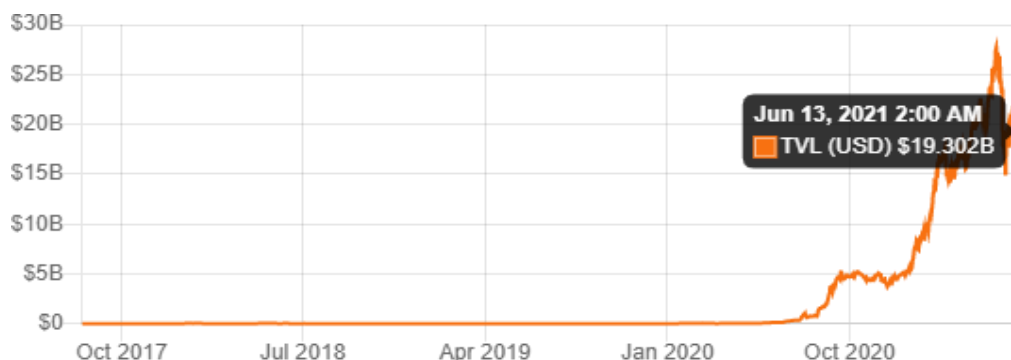
Come detto in precedenza le criptovalute sono uno strumento molto recente, ma in questi 12 anni si sono fatti passi da gigante per cercare di rendere più accessibile questo settore.

All'inizio le persone che scambiavano bitcoin si conoscevano in rete su forum specifici, con il passare del tempo sono nati i primi siti di scambio, chiamati exchange.

Gli exchange sono dei siti dove si può contrattare il prezzo di un qualsiasi asset finanziario: una sorta di borsa digitale.

Nel mondo della blockchain, un aspetto importante è quello della decentralizzazione e così sono nati i primi exchange decentralizzati, che danno numerosi vantaggi rispetto a quelli tradizionali.

Un primo vantaggio è che i DEX sono completamente autonomi e gli ordini vengono gestiti dagli smart contracts che registrano tali ordini sulla blockchain, generalmente quella di Ethereum, donando la caratteristica della trasparenza. Un'altra caratteristica degli exchange decentralizzati è quella che consente al cliente di evitare procedure di registrazione complesse.



7. Denaro bloccato su Exchange decentralizzati (fonte: [www.defipulse.com](http://www.defipulse.com)).

I DEX consentono inoltre di evitare di cedere alla società che gestisce la piattaforma il denaro dei clienti; infatti, questi operano secondo lo schema peer-to-peer, senza far passare il denaro dalla piattaforma, ma direttamente tra le parti operanti.

Uno svantaggio degli exchange decentralizzati è la limitata disponibilità di asset da scambiare, ma con il passare del tempo e il crescente interesse di questo settore, porteranno i DEX ad avere maggiori asset disponibili.

Sono poi presenti anche exchange ibridi: hanno la caratteristica di archiviare gli ordini all'interno di un server centralizzato di proprietà della società, ma gli scambi avvengono in maniera decentralizzata.

I DEX, per esempio hanno già integrato la funzione cross-chain, ovvero riescono ad effettuare scambi anche di monete basate su blockchain differenti, facendole a tutti gli effetti a comunicare tra esse.

Negli ultimi anni sono nate molte blockchain dedicate agli exchange decentralizzati, alcune di queste sono: Curve Finance, Uniswap, Pankaswap, Sushiswap e DDex.

## ORACOLI

Fin dall'inizio la blockchain poteva eseguire richieste provenienti solo dal suo interno. Contemporaneamente al collegamento tra blockchain diverse, si è sviluppato un modo per farle comunicare con il mondo esterno.

Questo processo avviene attraverso gli oracoli che sono degli applicativi che consentono di mandare informazioni del mondo esterno (off-chain) all'interno della blockchain (on-chain) e viceversa.

Gli oracoli ampliano i campi di applicazione degli smart contracts, ad esempio, attraverso il loro utilizzo è possibile contrattare materie prime come l'oro anche su blockchain utilizzando criptovalute.

Gli oracoli possono avere diverse caratteristiche, sono classificati in:

- Fonte: i dati possono provenire da un software o da un hardware;
- Direzione delle informazioni: come affermato in precedenza le informazioni possono essere in entrata o in uscita dalla blockchain;
- Fiducia: un oracolo può essere sia centralizzato che decentralizzato.

Gli oracoli blockchain sono strumenti molto recenti che in futuro potranno essere fondamentali per l'utilizzo della blockchain e delle criptovalute nella vita quotidiana.

## NON FUNGIBLE TOKEN

Per evidenziare il continuo sviluppo della blockchain è da citare anche il recentissimo settore negli NFT (Non Fungible Token), ovvero “gettone non fungibile”.

Questi token hanno la qualità di non avere la caratteristica della fungibilità, che si trova alla base di ogni moneta: infatti ad esempio, un'unità di bitcoin è uguale all'altra, non si differenziano.

I token non fungibili invece, sono unici, rivendicano la proprietà di un asset reale digitalizzato.

Gli NFT sono riusciti nell'arduo compito di creare qualcosa di unico e non riproducibile nel mondo digitale.

Questo nuovo settore è particolarmente esploso nell'ultimo anno, specialmente nel campo dell'arte, sono moltissimi infatti, gli artisti che hanno deciso di pubblicare una loro opera in NFT.

Per esempio, il famosissimo ma anonimo street-artist Banksy, ha bruciato una sua opera che ha aveva prima digitalizzato e poi ne ha creato un NFT, che ha venduto per una cifra vicina ai 280.000 dollari pagati con la criptovaluta Ethereum.

Con questa mossa il quadro si è rivalutato di circa tre volte.

Banksy non è l'unico ad aver usufruito della tecnologia NFT: anche la NBA ha venduto un brevissimo video di pochi secondi di una schiacciata, o come il cantante The Weeknd ha venduto una sua canzone come NFT, insieme a lui anche moltissime star americane hanno fatto lo stesso.

Quello della crypto-art basato su NFT è un mercato sperimentale che un giorno potrebbe affiancare quello tradizionale.



## CONCLUSIONI

Concludendo, posso affermare che la tecnologia blockchain e le criptovalute sono un'innovazione recente che però hanno già, velocemente, cambiato il modo di vedere la finanza e l'economia.

Quella della finanza decentralizzata potrebbe essere una rivoluzione al pari di quella delle banconote o di internet.

Le criptovalute sono ancora una piccola realtà che in pochi anni è arrivata alle orecchie dei grandi dell'economia, come banche e Stati che però, finora, si sono limitate e demonizzare questo settore, forse per disconoscenza o forse per convenienza.

Dal mio punto di vista, posso affermare che se le criptovalute venissero capite e accettate da chiunque utilizzi una carta di credito, si potrebbe immaginare facilmente che il sistema tradizionale possa vedersi diminuire l'uso dei loro servizi.

Senza contare l'immenso potere che hanno, avendo a disposizione i dati e il denaro dei risparmiatori per i loro investimenti che con il tempo, sono diventati tossici, si pensi al crack della Lehman Brothers del 2008 a causa dei titoli sui mutui subprime.

Se la blockchain venisse utilizzata come nuovo standard per un sistema economico alternativo, le banche di risparmio e tutti gli altri intermediari non avrebbero più senso di esistere.

Le criptovalute e la blockchain sono il metodo di resettare tutto il sistema, non senza degli effetti collaterali, per poi ricominciare con una mentalità non più volta al mero guadagno da parte dell'alta finanza.

Queste nuove tecnologie cercano di migliorare molti aspetti dell'economia tradizionale che con il passare del tempo, sono passati dall'essere pregi a difetti: si pensi ad esempio alla centralità che una volta era considerata un punto di forza per

l'economia e che le criptovalute hanno stravolto completamente o anche alla trasparenza delle operazioni che cerca di combattere il riciclaggio di denaro ma indirettamente anche la corruzione.

Nello specifico, bitcoin è nato per combattere l'inflazione che sta legando il mondo intero a causa delle scelte degli Stati.

La blockchain si rivolge anche a tutte quelle persone che sono state relegate ai margini della società economico-finanziaria e che non possono permettersi un conto corrente bancario.

Tutte queste idee, a mio parere, sono un ottimo punto di partenza per cercare di migliorare un sistema economico che negli ultimi anni non sta godendo di buona salute.

Oggi, per quelli che ne hanno sentito parlare, le criptovalute e la blockchain sono solo delle frodi, oppure vengono viste, come tutti i settori emergenti, ancora dal punto di vista speculativo: sono nel mondo delle criptovalute ormai da quattro anni, non nascondo, che me ne sono interessato, con curiosità, per lo stimolo di facili guadagni ma col il passare del tempo, ho imparato a comprendere questo settore, augurandomi che un giorno si possa capire a pieno la potenzialità delle criptovalute, della blockchain e della finanza decentralizzata che, essendo basate sulla tecnologia, sono pressoché infinite.

Spero vivamente che si possa al più presto passare ad una economia sana, trasparente, equa ed inclusiva affinché milioni di persone nel mondo che vivono in condizioni di estrema povertà possano avvantaggiarsene.

## BIBLIOGRAFIA

- Chi è W Scott Stornetta, 2021;
- Cos'è Chia Coin, l'alternativa green al bitcoin, Pierandrea Ferrari, 7 maggio 2021;
- Il movimento Cyberpunk: le origini delle criptovalute, Riccardo Santilli, 27 settembre 2019;
- Whitepaper Bitcoin, Satoshi Nakamoto, 18 agosto 2008;
- Svolta bitcoin: da novembre debutta Taproot, Mariangel Tessa, 18 giugno 2021;
- Che cosa succederà quando tutti i bitcoin saranno minati?, 2021;
- Intervista a Guido Maria Brera sul canale Youtube Marco Montemagno, 26 aprile 2021;
- Dal bitcoin “veleno per topi” di Buffet al dietrofront delle grandi banche d'affari, 24 maggio 2021;
- Taleb: Bitcoin volatile, ricorda lo schema Ponzi, Naomi Ferraris, 27 aprile 2021;
- Premio Nobel per l'economia Joseph Stiglitz: "Credo che dovremmo fermare le criptovalute", Helen Partz, 6 maggio 2019;
- Come funziona la Stablecoin DAI?, Ross Evans, 8 ottobre 2019;
- Grafico bitcoin da <https://coinmarketcap.com/currencies/bitcoin/>;
- CEFI VS DEFI – Non confondere finanza centralizzata con decentralizzata, Filippo Angeloni;
- Le caratteristiche delle piattaforme di lending nella DeFi, Mirko Silvestri, 31 luglio 2020;
- Grafici DEFI on-chain da <https://defipulse.com/>;

- Gli Oracoli Blockchain Spiegati;
- Bruciano quadro di Banksy e lo rivendono tramite NFT al quadruplo, Lorenzo Ferrero, 17 marzo 2021;
- Why a LeBron James GIF Sold for \$210,000, 4 aprile 2021;
- The Weeknd annuncia il lancio del suo primo NFT, Andrea Santillo, 2 aprile 2021.