Università
Ca'Foscari
Venezia

Corso di Laurea
Magistrale

in Economia e
Finanza

Tesi di Laurea

Blockchain e Finanza:

Smart contract e
applicazioni di un nuovo
concetto di fiducia

Relatore
Ch. Prof. Antonella Basso

Laureando (***)
Alessio Cendron
Matricola 863726

Anno Accademico
2021 / 2022

Desidero ringraziare i miei genitori, i quali mi hanno supportato durante tutti gli anni di studio. Ringrazio anche tutte le persone che mi sono state vicine nei momenti in cui mi serviva supporto morale. Infine, desidero ringraziare la Professoressa Antonella Basso per avermi aiutato nella stesura della tesi.

ABSTRACT

Sono passati diversi anni dalla nascita della blockchain e si potrebbe ritenere una realtà ormai affermata.

L'obiettivo del mio studio è comprendere la tecnologia blockchain e osservare come questa abbia rivoluzionato il mondo, in primis quello della finanza.

Il mio interesse per il mondo blockchain e le criptovalute risale a poco più di un anno fa dove, parlando con un amico, mi iniziai a domandare per quale motivo delle valute elettroniche potessero raggiungere un valore così grande. Fu così che iniziai ad addentrarmi in questo mondo che mi permetterei di definire in stato di "beta testing". Da studente di Economia e Finanza sono sempre stato attratto dal mondo della finanza e, nonostante il mondo delle criptovalute sia ancora agli albori, c'è molto da imparare. Il valore che sta dietro le criptovalute è dovuto alla tecnologia che portano: Bitcoin nasce per soppiantare la finanza tradizionale ed Ethereum per diventare "il computer del mondo" dove si può costruire qualsiasi applicazione. La tecnologia Blockchain nasce nel periodo della crisi finanziaria del 2008, dove si sono verificati tanti salvataggi di banche. L'impotenza dovuta al fatto di "non sentirsi padroni del proprio destino" di quel periodo ha portato Satoshi Nakamoto verso la ricerca di una soluzione permanente. I registri sono delle basi fondamentali della società e ci hanno accompagnato nel corso della storia mappando relazioni economiche e sociali. Il punto debole dei registri è la necessità di fiducia nei confronti di chi lo scrive. La novità che porta la blockchain e la tecnologia Distributed Ledger è l'assenza dell'autorità centrale, vista la distribuzione dei registri su una rete ad accesso libero, composta da utenti posti allo stesso livello.

L'elaborato verte sullo studio della tecnologia blockchain, con particolare attenzione a Bitcoin e ad Ethereum, che sono le criptovalute più importanti. Al termine della presentazione sulla tecnologia blockchain e su come questa ha rivoluzionato il concetto di fiducia, definiremo gli smart contract e come essi essere applicabili al mondo della finanza. In questa tesi l'obiettivo è presentare la tecnologia blockchain, riconoscere l'innovazione portata e come possa essere una solida base per il cambiamento della finanza per come la conosciamo ora.

INDICE

INTRODUZIONE

Quando nascono nuove tecnologie esse possono avere un impatto importante sul modus operandi delle aziende: si possono offrire servizi e prodotti nuovi, aumentare le entrate, abbassare i costi e riorganizzare le strutture. Le imprese già presenti nel settore dove si sviluppano le nuove tecnologie, se risultassero lente nel cogliere le nuove opportunità o nel porre barriere all'entrata, potrebbero essere soppiantate da dei nuovi operatori "migliori" nello sfruttare le innovazioni.

Una rivoluzione tecnologica potrebbe portare a un cambiamento radicale dell'intero sistema sociale. La nascita della blockchain ha tutte le carte in regola per essere una tecnologia che stravolge l'intero sistema economico e la società.

Rivoluzioni tecnologiche

Nel passato alcune innovazioni hanno delineato alcune delle più grandi rivoluzioni in campo economico e societario: le rivoluzioni industriali, la rivoluzione ferroviaria, la rivoluzione petrolifera. Ognuna ha mutato la struttura industriale, portato nuove forme di energia e influenzato il modo di organizzarsi della società. Nell'attuale momento storico ci troviamo in una rivoluzione delle comunicazioni e delle informazioni caratterizzata dall'intensità, dalla connettività, dalla specializzazione e globalizzazione.

Generalmente si individuano tre pilastri caratterizzanti questi stadi: costi significativamente più bassi, nuovi metodi di comunicazione, infrastrutture e logistica migliorate. L'abbassamento del costo dei fattori di produzione genera delle tensioni nei mercati, spesso delle bolle e dei crolli finanziari, che portano alla richiesta di una revisione delle istituzioni. Ogni rivoluzione tecnologica porta con sè una serie di principi di buon senso che cambiano a seconda di come operano le imprese e le società. Inoltre, conducono ad un nuovo paradigma tecno-economico, con diverse strutture dei costi, diverse opportunità di innovazione, e organizzazioni basate su principi differenti.

Introduzione alla blockchain

La blockchain apporta innovazioni potenzialmente rivoluzionarie in diversi ambiti industriali, infatti dalla sua prima applicazione nel campo delle valute virtuali, si è

capito che essa poteva essere implementata anche come registro distribuito e trasparente per altre applicazioni, grazie ad un network non gerarchico, alla crittografia e all'ingegneria del software. Questo potrebbe condizionare i vari business model attuali andando a produrre nuovi oggetti o servizi per le industrie interessate.

La Distributed Ledger Technology riduce significativamente i costi operativi dato che può evitare duplicazioni o inefficienze nel controllo e coordinamento attraverso un libro mastro che opera a livello industriale, tagliando così i costi sistemici dovuti a processi come il controllo incrociato fra i libri e i database posseduti.

La conseguente digitalizzazione e archiviazione in modo sicuro delle informazioni di qualsiasi attività consente alle organizzazioni di identificare e tenere traccia delle loro proprietà. Nuovi metodi di registrazione delle obbligazioni e trasferimento di valore con contratti programmabili sono stati sviluppati utilizzando blockchain (Ethereum, per esempio, è una piattaforma decentralizzata incentrata sullo sviluppo di smart contract). Il potenziale della tecnologia che supporta la blockchain può estendersi anche ad un nuovo scenario, dove fiducia o intermediari necessari che operano in un monopolio gerarchico sono uniti o sostituiti da una struttura consensuale maggiormente aperta su base comunitaria.

Lo sviluppo di blockchain e delle tecnologie associate offre anche la possibilità di registrare in tempo reale accessi e transazioni, rendendo le operazioni più rapide ed economiche, ad esempio l'assicurazione dell'auto potrebbe essere basata sia sullo stato del veicolo che del conducente, con un costo che varia a seconda del comportamento, dei prezzi e dell'avversione al rischio. Si potrebbe arrivare così ad un'economia programmabile legata agli smart contracts, basata su reti decentralizzate e agenti che richiedono sempre meno il coinvolgimento umano, operando come organizzazioni autonome distribuite in grado di offrire una vasta gamma di prodotti e servizi.
L'esempio lampante di un registro operativo è Bitcoin, applicazione della blockchain entrata a pieno regime nel mondo dei servizi finanziari. Il libro mastro condiviso offre un costo di funzionamento inferiore nell'ambito delle strutture e della governance esistenti, fornendo la possibilità di ridurre i costi e la complessità a livello di sistema. La creazione di moneta non è più una prerogativa esclusiva di responsabilità da parte dei governi nazionali, inoltre si è abilitato un ulteriore sviluppo con la possibilità di aggiungere informazioni su attributi specifici (ad esempio attività o contratti fisici)

generando così molteplici casi d'uso che potrebbero migliorare la nostra vita di tutti i giorni.

Approccio dell'industria finanziaria

La blockchain è stata messa sotto i riflettori per la prima volta nel 2008 grazie al modello Bitcoin, rete che gestisce la compravendita dell'omonima moneta digitale attiva tramite il consenso automatizzato dei suoi utenti.
Questa nuova tecnologia sembra abbia suscitato la stessa reazione al pubblico che ebbe Internet nei suoi primi anni, permettendo la registrazione e gestione di risorse attraverso registri distribuiti, database di risorse che possono essere condivisi attraverso una rete in diverse aree geografiche e istituzioni. Le attività gestite attraverso tali registri potranno essere di natura finanziaria, legale, aziendale o elettronica e la loro sicurezza è garantita dall'utilizzo di chiavi e firme crittografiche.

I metodi attuali di gestione di dati e di operazioni finanziarie coinvolgono grandi sistemi informatici situati all'interno di singole istituzioni. La comunicazione fra essi coinvolge reti di messaggistica che aggiungono costi e complessità, inoltre questi sistemi essendo per lo più centralizzati presentano un unico punto centrale di fallimento, che non garantisce la continuità di sistema in caso di guasto. I dati processati attraverso questi modelli, infine, risultano spesso non sincronizzati, non aggiornati o semplicemente imprecisi e più vulnerabili ad attacchi informatici rispetto alla blockchain.

Attraverso concetti come chiavi pubbliche e private, modelli di rete peer to peer, protocolli di criptovaluta, registri distribuiti, la blockchain può potenzialmente scatenare un'ondata di creatività e innovazione in svariati settori industriali mettendo in discussione parametri economici tradizionali del mondo moderno come moneta, fiducia, scambio di valore. Attualmente alcuni degli istituti bancari più importanti sono attivi nello sviluppo di soluzioni che coinvolgono l'utilizzo della blockchain, riconoscendo la sua utilità per il futuro del settore in particolare per quanto riguarda usi interni e collaborazioni fra più partner.

CAPITOLO I:
DLT, BLOCKCHAIN E CRIPTOVALUTE

In questo capitolo andremo a scoprire la tecnologia Blockchain, con un occhio di riguardo a Bitcoin. Per comprendere questa tecnologia è necessario conoscere le caratteristiche di un Distributed Ledger e, dopo una breve spiegazione, potremo avanzare nello studio dettagliato di tutto il suo potenziale. Bitcoin e le criptovalute sono parte dei protagonisti principali della ricerca perchè non si può più ignorare un mercato del valore di 3 trilioni di dollari, è importante avere una visione completa di questo mondo.

1.1 La base della blockchain: Distributed Ledger Technology

Il termine "ledger" letteralmente fa riferimento alla parola "registro, libro mastro", dunque uno strumento di archiviazione di informazioni qualsiasi. I sistemi DLT rappresentano dunque un nuovo sviluppo nell'utilizzo dei ledger, è una tecnologia peer-to-peer[1] che sfrutta Internet come strumento per la condivisione di dati attraverso dei registri distribuiti lungo la rete[2]. Il network è composto dai vari peer (che da ora in poi chiameremo anche "nodi"), situati geograficamente in tutto il mondo, il cui compito è garantire la sicurezza del protocollo contro possibili attacchi informatici. La decentralizzazione dei registri è il punto cardine della tecnologia, le informazioni sono archiviate seguendo algoritmi di consenso distribuito che permettono di tenere tutti i ledger aggiornati simultaneamente. La tecnologia DLT elimina l'autorità centrale e l'archiviazione dei dati avviene eliminando la discrezionalità dell'uomo. L'eliminazione di intermediari è sicuramente un lato positivo di questo modello, d'altro canto abbiamo una notevole diminuzione della privacy perché le informazioni possono essere viste e verificate da tutti. La collaborazione tra i nodi è volta all'obiettivo di verificare collettivamente i dati e registrarli. Le operazioni di controllo e archiviazione in un sistema centralizzato sono svolte dall'unica autorità presente; invece, il lavoro collettivo dei

[1] Un modello di architettura di rete informatica basata sulla parità dei nodi (peer), essi possono essere allo stesso tempo sia client sia server.
[2] Ministero dello sviluppo economico, *Tecnologie Distributed Ledger*, disponibile a https://uibm.mise.gov.it/index.php/en/lotta-alla-contraffazione/servizi-per-imprese-e-consumatori/tecnologie-anticontraffazione/sot-servizio-orientamento-tecnologie-anticontraffazione/tecnologie-distributed-ledger

partecipanti di un sistema DLT aumenta la capacità di informazioni elaborabili simultaneamente, rendendo il sistema più veloce e riducendo i costi complessivi[3]. Lo sviluppo di una rete dove ogni utente è alla pari degli altri porta ad un aumento esponenziale della sicurezza, dato che per modificare i dati e corromperli sarebbe necessario possedere il controllo della maggior parte dei nodi della rete per avere la maggioranza di potere decisionale. Le due caratteristiche più importanti dei Distributed Ledger sono quindi:

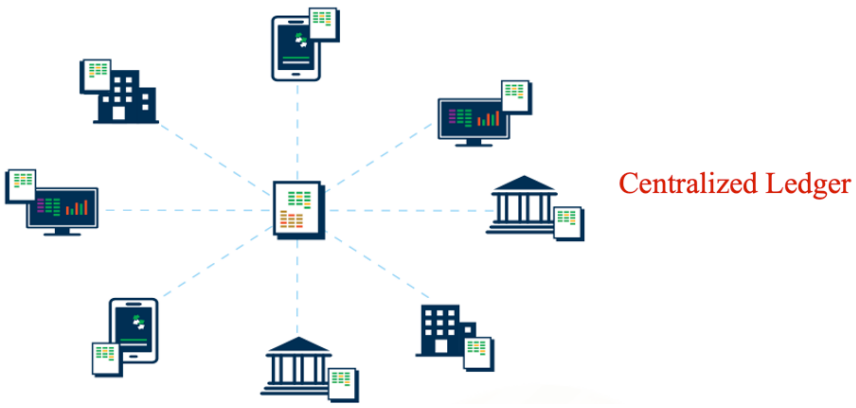
1- la possibilità di raccogliere, archiviare e scambiare informazioni attraverso una rete digitale tra vari partecipanti, senza l'ausilio di una figura governativa o la fiducia nella controparte.
2- L'eliminazione del problema del double-spending (nel caso di utilizzo della tecnologia come infrastruttura di pagamento): non posso spendere più volte lo stesso token.[4]

1.1.1 La governance prima dei Distributed Ledger

La governance è l'insieme dei principi, regole e procedure che tengono unite la gestione e il governo di una qualsiasi entità riguardante un collettivo[5].
Prima della nascita dei DLT, il sistema veniva definito Centralized ledger.
In questo apparato, il processo di registrazione di dati viene svolto da un'autorità centrale che compila il registro e lo aggiorna sistematicamente. Il punto di forza di questo modello sta nella fiducia che viene sistematicamente dalla comunità in un unico punto di riferimento, l'autorità centrale. La debolezza del sistema Centralized ledger è il rischio di essere impossibilitati ad archiviare i dati nel registro per varie cause (un sovraccarico della rete, un attacco hacker), perdendo quindi fiducia da parte dei partecipanti della rete. Come vediamo nella Figura 1.1, tutti i partecipanti della rete fanno riferimento ad unico registro redatto e controllato da una singola autorità centrale.

[3] World Bank Group, *Distributed Ledger Technology (DLT) and Blockchain,* disponibile a https://openknowledge.worldbank.org/handle/10986/29053
[4] Blockchain4Innovation, *Valuta elettronica utilizzata in un dato sistema DLT*, disponibile a *https://www.blockchain4innovation.it/criptovalute/token-cose-come-viene-utilizzato/*
[5] Enciclopedia Treccani, *governance,* definizione disponibile a https://www.treccani.it/enciclopedia/governance_%28Dizionario-di-Economia-e-Finanza%29/

Figura 1.1. Rappresentazione grafica di un sistema a registro centralizzato



Fonte: Immagine tratta da World Bank Group, *Distributed Ledger Technology (DLT) and Blockchain,* disponibile a https://openknowledge.worldbank.org/handle/10986/29053

1.1.2 La governance dopo l'avvento dei DLT

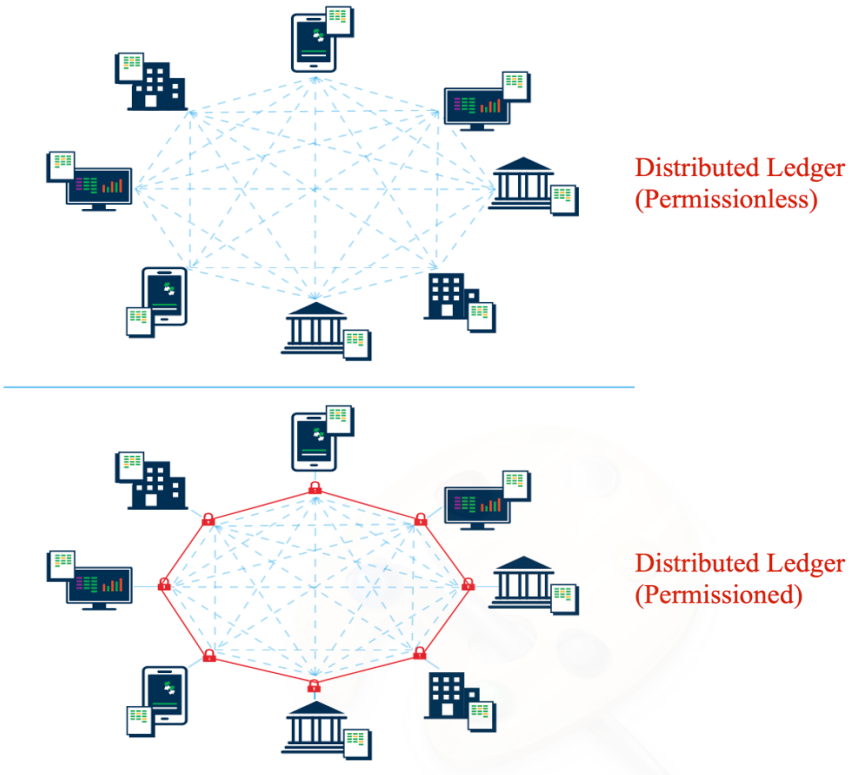
I sistemi DLT possono essere distinti in due categorie che differiscono radicalmente dal punto di vista della governance:

- Permissionless: network decentralizzato, utilizzo di un software aperto a tutti per unirsi alla rete e partecipare alla archiviazione di dati nel ledger. Nella rappresentazione in Figura 1.2 possiamo notare che ogni nodo possiede una propria copia del ledger e in caso uno decida di apportare delle modifiche deve mandarli al vaglio di tutti i partecipanti.
- Permissioned: network con un'autorità centrale che controlla gli accessi e funge da regolatore. In Figura 1.2 ne viene ritratto un tipico esempio, per poter modificare il ledger è necessaria l'autorizzazione di un'entità centrale.

Entrambe le due tecnologie portano pro e contro e non è possibile al momento definire quale sia la migliore. Svolgendo un'analisi più dettagliata, si può notare come i sistemi possano essere applicati in settori diversi. La struttura permissionless porta al massimo la sicurezza del sistema attraverso l'utilizzo della crittografia e degli algoritmi, rendendosi così attraente ai partecipanti, e questi vengono incentivati al rispetto delle regole per il

funzionamento del registro. Nel sistema permissionless un nodo qualsiasi partecipante al network può validare le transazioni e trasmetterle agli altri anche senza consenso distribuito. I sistemi permissioned sono avvantaggiati dal punto di vista del controllo dell'identità dei partecipanti e della privacy, dato che è presente un'autorità centrale; quest'ultima si prende la responsabilità di giudicare affidabili i nodi partecipanti e sceglie quali rendere validatori attraverso l'uso di algoritmi. Un DLT permissioned si allontana maggiormente dagli ideali di decentralizzazione portati da questa tecnologia.

Figura 1.2. Rappresentazione grafica di un sistema a registro distribuito permissionless e uno permissioned



Fonte: Immagine tratta da World Bank Group (2017), *Distributed Ledger Technology (DLT) and Blockchain,* disponibile a https://openknowledge.worldbank.org/handle/10986/29053

1.2 La Blockchain

La tecnologia blockchain è universalmente definita come "un registro distribuito" su una rete peer-to-peer per lo scambio di informazioni o di valori. È un protocollo discendente direttamente dallo sviluppo della DLT basato sulla possibilità di interazione tra i nodi, i quali hanno il compito di validare le transazioni e archiviarle nel registro distribuito sotto forma di "blocchi"[6]. È conosciuta principalmente per l'utilizzo nel protocollo Bitcoin e nelle altre criptovalute, ma i suoi sviluppi vanno ben oltre l'essere solo un'infrastruttura di pagamento. L'essere sempre online garantisce una reperibilità massima dei servizi e dimostra di rimediare al "single point of failure[7]", eliminandolo definitivamente. La facilità di accesso alla rete per il pubblico rende la decentralizzazione ancor più evidente: maggiore è il numero di utenti, maggiore sarà quest'ultima. La sicurezza e la trasparenza offerte dalla blockchain sono il maggiore punto di forza che attraggono un numero di utenti in costante aumento. A differenza dei database classici, nella blockchain non si possono modificare le informazioni scritte e archiviate in precedenza sul registro distribuito, le transazioni avvenute sono irreversibili. Il registro digitale a cui si fa riferimento è contenuto all'interno di blocchi uniti in una lunga catena ed è distribuito a tutti gli utenti del network. DLT e blockchain hanno possibilità di sviluppo al di fuori del settore finanziario: ci sono applicazioni e servizi di identità digitale, archiviazione decentralizzata di flussi di beni e materiali in una supply chain e molto altro ancora. L'avvento della blockchain porta alla rivoluzione del concetto di "fiducia": tutti i giorni ci imbattiamo in sistemi basati su persone o entità singole che hanno il potere di decidere per una comunità intera, creando quindi un rischio di inefficienza per vari motivi[8]. L'individuo nell'utilizzo di sistemi a registro distribuito si trova con un potere decisionale pari a quello di tutti gli altri utenti, ci si sente parte di un collettivo e, talvolta, è permesso condividere anche il proprio punto di vista. In breve, la tecnologia blockchain porta chiunque abbia intenzione di partecipare a un network ad avere fiducia nel sistema, fondato su calcoli matematici. La differenza con i sistemi classici Distributed Ledger sta nella struttura a blocchi concatenati indissolubilmente in sequenza: questo si traduce

[6] Il blocco è l'unità fondamentale della blockchain
[7] Il single point of failure è il punto vulnerabile di un dato sistema che, in caso di disservizi, porterebbe a gravi anomalie o alla cessazione dell'esistenza. – definizione liberamente tratta da IBM, *Single point of failure, disponibile* a https://www.ibm.com/docs/he/tsafm/4.1.0?topic=p-single-point-failure-spof
[8] Rischi di corruzione o di attacchi di attori malevoli.

nell'impossibilità di un nodo qualsiasi di modificare il registro distribuito contenuto in un blocco validato, dato che dovrebbe ricostruire la catena e raggiungere nuovamente il consenso ottenuto sulla catena precedente.

1.2.1 Caratteristiche

Le caratteristiche principali della tecnologia blockchain sono:

- Decentralizzazione e disintermediazione: le informazioni vengono registrate su una lunga catena e distribuite tra i vari partecipanti del network, senza ausilio di alcun'entità centrale;
- Unicità: il registro distribuito è unico e disponibile a tutti i nodi, non ci sono altre versioni;
- Trasparenza: il contenuto della blockchain è disponibile a tutti in qualsiasi momento, è possibile tracciare qualsiasi movimento;
- Immutabilità: le informazioni contenute nei blocchi non sono modificabili;
- Programmabilità delle operazioni: attraverso l'utilizzo di smart contract[9] è possibile prestabilire azioni da compiere in base al verificarsi di determinati eventi.[10]

1.2.2 Due architetture di blockchain

Classifichiamo le blockchain in due categorie, possono differire in base all'apertura al pubblico di lavorare alla validazione dei blocchi o dalla tipologia di consenso che vige. Studieremo il sistema:

- Permissioned (privata): è una rete chiusa dove la "creazione" dei blocchi e la validazione viene svolta solo dalle figure prestabilite. Nella Tabella 1 troviamo riassunti i vantaggi e gli svantaggi di questo sistema. La decentralizzazione si definisce "parziale" dato che, nonostante i nodi siano distribuiti, ci si trova di fronte a delle restrizioni decise da un gruppo privato. L'utilizzo di una rete privata

[9] Vedi capitolo 2
[10] Garavaglia, R. (2021), *Conoscere la blockchain,* Hoepli, Milano

favorisce un aumento della privacy e si rende più flessibile a possibili aggiornamenti.

Tabella 1. Riassunto di vantaggi e svantaggi di una blockchain Permissioned

VANTAGGI	SVANTAGGI
- La decentralizzazione, anche se parziale, favorisce l'utilizzo del sistema in molti settori grazie alla diminuzione dei costi - Privacy, in una rete privata serve l'autorizzazione per accedere ai dati - Possibilità di modificare la configurazione a seconda delle necessità - Velocità e scalabilità, visto l'utilizzo di pochi nodi per consenso e validazione dei blocchi	- Rischio di corruzione alto, vista la poca decentralizzazione - Le regole di consenso distribuito possono essere cambiate dai proprietari della blockchain, col rischio di infrangere l'immutabilità della catena. - Poca trasparenza, le persone esterne non possono accedere ai dati

- Permissionless (pubblica): è una rete liberamente accessibile a chiunque. Come vediamo riassunto nella Tabella 2, non è presente alcuna restrizione e non si necessita di alcun requisito per partecipare al network anzi, si viene incentivati a farne parte mettendo a disposizione la propria potenza computazionale per validare i blocchi. Il fatto di essere letteralmente "senza restrizioni" permette l'entrata e l'uscita in qualsiasi momento da parte dei partecipanti. Essendo una rete aperta, non è possibile escludere nessuno e la cooperazione di tutti gli utenti

è volta alla verifica delle operazioni che avvengono, limitando la possibilità di attacchi informatici.

Tabella 2. Riassunto di vantaggi e svantaggi di una blockchain Permissionless

VANTAGGI	SVANTAGGI
- Decentralizzazione che estende il network a tutti coloro che vogliano parteciparvi - Alto trasparenza, ognuno può consultare le informazioni contenute nei blocchi - Resistenza alla censura, nessuno può permettersi di escludere qualcun altro dal network - Alta sicurezza, per attaccare una blockchain si necessita almeno del 51% della potenza computazionale totale della rete per operare un attacco informatico e riuscire a corrompere il sistema di validazione.	- Poca efficienza energetica, data la grandezza del network e l'intenzione di condividere tra tutti la propria potenza - Meno privacy, tutti possono vedere le informazioni che vogliono - Meno scalabilità, a causa della necessità di hardware potenti

La tipologia di blockchain permissioned potrebbe essere attrattiva per delle istituzioni che vorrebbero interessarsi a questa tecnologia, dato che sarebbe più facilmente adeguabile a strutture legislative, scontrandosi però con l'ideale dell'eliminazione dell'intermediario. Questa tipologia di network potremmo vederla utilizzata nel campo della privacy e della

sicurezza[11]. L'obiettivo di raggiungere la decentralizzazione viene rispettato con successo dalle blockchain permissionless, vista l'estromissione del fattore umano e la sostituzione di questo con un protocollo pubblicamente disponibile, reso funzionante da una rete di computer indipendenti. Quest'altra tipologia di network si trova ottima per un possibile sviluppo nel settore finanziario. La struttura permissioned potrebbe incontrare un disinteressamento dei nodi validatori o potrebbe subire più facilmente un attacco hacker, eventi quasi impossibili in una rete permissionless[12].

1.3 Le criptovalute

L'espressione della tecnologia blockchain attualmente più conosciuta è rappresentata dalle criptovalute. Il termine in sé fa intendere lo stretto legame con la crittografia su cui si basa la blockchain e sono il primo esempio dell'Internet of value. Le criptovalute sono la rappresentazione digitale di un asset non emesso da banche centrali né altre autorità centralizzate, l'obiettivo per cui son state create è, infatti, il raggiungimento della decentralizzazione. Le caratteristiche della tecnologia blockchain unite alle criptovalute sono giunte all'eliminazione del cosiddetto "problema del double spending"[13], evento che può verificarsi facilmente dato che nel mondo digitale è semplice ottenere la duplicazione di dati. Il problema della doppia spesa viene evitato per la prima volta al di fuori del mondo centralizzato, senza coinvolgere alcuna terza parte. Ad oggi le criptovalute sono circa 20000[14] e sono tutte derivate da Bitcoin, ognuna di esse cerca di risolvere un problema differente. Nello specifico, la struttura della blockchain delle criptovalute è un network del tipo permissionless: questa struttura incentiva la sicurezza, dato che è presente una quantità illimitata di nodi che validano le transazioni, e sono incentivati a farlo con maggiore interesse data la possibilità di guadagno di una ricompensa in criptoasset. Le criptovalute sono asset digitali che possono essere scambiati liberamente e il loro valore segue le logiche classiche del mercato di domanda e offerta.

---

[11] Cointelegraph, *Permissioned blockchain vs. permissionless blockchain: Key differences,* disponibile a https://cointelegraph.com/blockchain-for-beginners/permissioned-blockchain-vs-permissionless-blockchain-key-differences

[12] Lai, R. e Kuo Chuen, D. L. (2018), *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2,* Academic Press

[13] Il double-spending è una situazione in cui esiste più di una copia digitale di qualcosa che dovrebbe essere unico" – Chiap, G. (2019*, Blockchain: tecnologie e applicazioni per il business,* Hoepli Editore, Milano

[14] Dato ricavabile dall'home page del sito https://coinmarketcap.com

1.3.1 Bitcoin

"Una versione puramente peer-to-peer di denaro elettronico consentirebbe di inviare pagamenti online direttamente da un attore a un altro senza passare attraverso istituzioni finanziarie[15]", così lo descrive il suo fondatore (o fondatori dato che è uno pseudonimo) Satoshi Nakamoto.

Bitcoin è la prima criptovaluta (ticker: BTC o XBT) decentralizzata che utilizza un registro distribuito tra i nodi partecipanti al network, i quali tengono traccia delle transazioni e sfruttano la crittografia per l'emissione di nuova moneta. La rete Bitcoin permette il possesso e il trasferimento attraverso Internet utilizzando dei "wallet" digitali. Il non essere centralizzato e la struttura peer-to-peer escludono qualsiasi entità dal controllo e impedendo così il blocco della rete. Erroneamente si accosta il termine "anonimo" a Bitcoin[16], ma non è corretto: il protocollo, in linea con le caratteristiche della blockchain, è trasparente e qualsiasi trasferimento resta visibile in eterno; ciò che non è visibile è l'intestatario del wallet, perché è permesso usare uno pseudonimo.[17]

1.3.1.1 Storia di Bitcoin e della valuta elettronica

La prima volta che si sentì parlare di valuta elettronica, o criptovaluta, fu nel 1982 in uno scritto di David Chaum denominato "Blind signatures for untraceable payments[18]" dove descrisse le caratteristiche che avrebbe dovuto avere una valuta al fine di preservare la privacy degli utilizzatori attraverso l'uso della crittografia. Il suo scritto venne ripreso da un gruppo di programmatori chiamati Cyberpunk nei paper e manifesti pubblicati all'inizio degli anni '90.
La moneta elettronica avrebbe dovuto dare la possibilità di nascondere dei messaggi prima che arrivassero al destinatario con l'obiettivo di: eliminare il rischio di

[15] Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System,* https://bitcoin.org/bitcoin.pdf
[16] Comandini, G.L. (2020), *Da zero alla luna,* Dario Flaccovio Editore, Palermo
[17] Successivamente in questo elaborato vedremo perché la differenza tra pseudonimato e anonimato è così importante
[18] Chaum, D. (1982), *Advances in Cryptology Proceedings of Crypto,* disponibile a https://chaum.com/wp-content/uploads/2022/01/Chaum-blind-signatures.pdf

manomissione di pagamenti da parte di terzi, rendere possibile avere una prova del pagamento e interrompere l'uso dei mezzi di pagamento in caso di frodi.[19]

L'idea di David Chaum venne ripresa da Satoshi Nakamoto, pseudonimo di una persona (o un gruppo di persona) di cui non si è ancora scoperta l'identità, quando il 31 ottobre 2008 pubblicò un white paper[20] dove spiegava la sua idea di valuta digitale. Bitcoin non è niente altro che una delle infinite possibilità di utilizzo della tecnologia blockchain, risulta però essere il primo progetto e il più popolare.

La nascita di Bitcoin non avviene in un momento casuale, ma nei mesi immediatamente successivi alla crisi finanziaria del 2008 e dei numerosi bailout delle banche.

Il 3 gennaio 2009 nasce il "genesis block", il blocco 0 della catena, dove troviamo scritta la frase "il cancelliere sta per effettuare un secondo salvataggio per le banche". Il messaggio rilasciato da Satoshi Nakamoto sul blocco genesi era quello di criticare il sistema finanziario vigente a quel tempo, riprendendo appunto il titolo del Times di quel giorno.[21]

Solo dopo anni la tecnologia blockchain si conquistò le prime pagine dei giornali a causa di eventi negativi accaduti legati alla criminalità.

Dopo una prima regolamentazione dell'EBA per l'antiriciclaggio e per il contrasto del terrorismo, finalmente si giunse a un interesse di tipo diverso nei confronti della blockchain e dal 2015 in poi si ebbe un susseguirsi di grandi entità finanziarie mondiali che iniziavano a studiare e sviluppare il proprio futuro di questa nuova tecnologia.

1.3.1.2 Decentralizzazione vs centralizzazione

Il sistema centralizzato tradizionale prevede intermediari, è centralizzato proprio perché si basa su qualcuno che autorizza come la banca, il circuito della carta di credito, Paypal, Satispay e tutti coloro che sono appunto intermediari finanziari. Immaginiamo di dover mandare un bonifico a qualcuno: entro sull'online banking, dispongo il bonifico, la banca verifica se è possibile, una volta approvato lo invia all'altra banca e una volta svolti i controlli, lo accredita al destinatario. Di fatto, abbiamo avuto il bisogno di due

[19] Basile, A. (2019), *Blockchain: la nuova rivoluzione industriale,* Dario Flaccovio Editore, Palermo

[20] Un white paper è un documento che informa il lettore in merito alla filosofia della risoluzione di un determinato problema, è il primo documento che i ricercatori dovrebbero leggere.

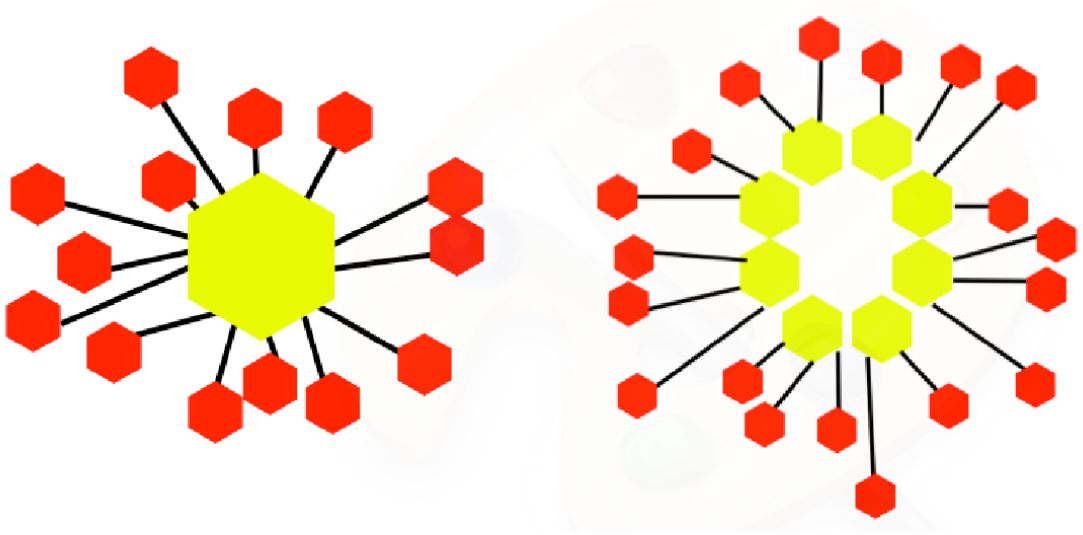
[21] Antonopoulos, A. M. (2014), *Mastering Bitcoin,* O'Reilly Media

approvazioni di entrambe le banche e questo richiede generalmente un giorno di tempo, oltre ai costi (il bonifico istantaneo elimina il problema delle tempistiche, ma aumenta i costi). È possibile che il sistema della banca sia offline per vari motivi, creando un disservizio che non mi permette di spendere il denaro, questa conseguenza è dovuta all'affidamento a un'unica istituzione centralizzata. Immaginando di dover utilizzare la carta di credito si introducono ulteriori intermediari, ovvero il circuito della carta, che dovranno svolgere lo stesso iter del bonifico e di conseguenza il processo aumenta ulteriormente i costi. Nel caso ci fosse la necessità di inviare dei soldi all'estero le tempistiche aumentano e oltretutto si affrontano ulteriori costi come il tasso di cambio, che presenta sempre delle commissioni. In conclusione, si potrebbe dire che il sistema centralizzato risulta inefficiente dato che ha dei costi elevati e se un intermediario smettesse di funzionare non si potrebbe più disporre del proprio denaro.

In un sistema decentralizzato si ha un insieme di nodi distribuiti in giro per il mondo e grazie alla struttura paritaria possiamo interagire con tutti: se un nodo a cui mi rivolgo risultasse offline, potrei rivolgermi a un altro e farmi validare la transazione, riuscendo a far arrivare il denaro al destinatario in tempi brevissimi. Questa velocità è dovuta alla possibilità di rivolgersi a più nodi validatori, che citavamo prima, e si ottiene un notevole abbassamento dei costi, viene eliminato così il single point of failure. Nelle criptovalute le transazioni sono borderless, quindi io che dispongo un pagamento non mi trovo a dover pagare delle commissioni in base alla locazione geografica del mio destinatario.

I due tipi di sistemi possono essere rappresentati come in Figura 1.3, possiamo notare che le relazioni in un sistema decentralizzato sono distribuite lungo una rete di nodi e abbiamo una reale visione dell'eliminazione del single point of failure.

Figura 1.3. Rappresentazione di una rete centralizzata e una decentralizzata



Fonte: liberamente rivisitato da Binance Academy, *Centralizzazione vs decentralizzazione,* disponibile a https://www.binance.com/it/blog/from-cz/centralizzazione-vs-decentralizzazione-301982828007075840

1.3.1.3 La crittografia

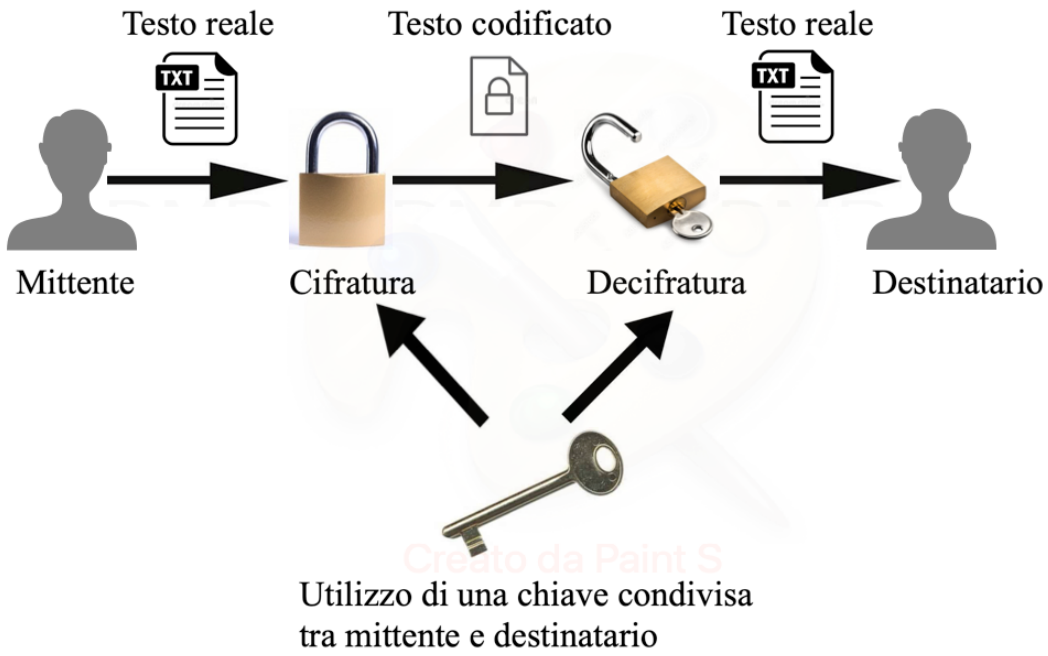
La crittografia (dal greco "scrittura nascosta") è quel processo con cui delle informazioni vengono trasformate in modo tale da essere illeggibili a terzi non autorizzati. Solo il destinatario può decriptare i dati e accedere alle informazioni nel formato originale.[22] La trasformazione da messaggio "reale" a quello "codificato" si chiama cifratura, l'inverso si chiama decifratura. La crittografia è la **base della protezione dei dati** ed è il modo più semplice e importante per garantire che le informazioni di un sistema informatico **non possano essere rubate e lette** da malintenzionati. Ad oggi questa scienza utilizza algoritmi matematici che agiscono sul messaggio originale, trasformandolo. La conversione del messaggio si basa su una "chiave segreta" (che rappresenta il linguaggio crittografico) che garantisce la sicurezza del processo se nota solo agli autorizzati, a differenza dell'algoritmo che non deve essere necessariamente esserlo.

a) *Crittografia Simmetrica*

[22] Tratto da kaspersky.it, *La crittografia nella protezione dei dati*, disponibile a https://www.kaspersky.it/blog/limportanza-della-crittografia-nella-protezione-dei-dati/949/

La crittografia tradizionale si definisce "simmetrica": il linguaggio di cifratura dei messaggi è la stesso di quello di decifratura, nella Figura 1.4 si può vedere il meccanismo di funzionamento. Uno scambio di un'informazione testuale tra due individui è schematizzabile come in Figura 1.4, il processo di cifratura e decifratura avviene attraverso la stessa chiave[23].

Figura 1.4. Esempio di invio di un messaggio attraverso il metodo di crittografia simmetrica



Fonte: ispirato da Javaboss.it, *Crittografia in Java,* disponibile a https://www.javaboss.it/crittografia-in-java/

Il problema nell'utilizzo di questo tipo di crittografia deriva dal fatto che i due interlocutori devono scambiarsi la chiave vedendosi fisicamente dato che non utilizzano un canale per la trasmissione dei messaggi sicuro. Un esempio di questo tipo di crittografia deriva dai tempi degli antichi romani con il famoso "cifrario di Cesare"[24].

b) Crittografia Asimmetrica

[23] Comandini, G.L. (2020), *Da zero alla luna,* Dario Flaccovio Editore, Palermo
[24] Un sistema crittografico primitivo ideato da Giulio Cesare – da Young Platform, *Crittografia: Cesare, Enigma e la Blockchain***,** disponibile a https://academy.youngplatform.com/blockchain/storia-crittografia-cesare-enigma-blockchain/

L'utilizzo di un'unica chiave sia per la cifratura che per il processo inverso rendono il meccanismo poco sicuro, negli anni Settanta si è giunti alla soluzione del problema. La crittografia asimmetrica, o "a chiave pubblica", è ampiamente utilizzata su internet ed è fondamentale nella tecnologia blockchain. Il sistema prevede l'impiego di due chiavi: una privata, che l'individuo custodisce e non deve diffondere, e una pubblica, derivata matematicamente dalla precedente e che può essere diffusa[25]. La chiave pubblica viene generata facilmente da quella privata, ma l'inverso non può accadere (nemmeno con il bruteforcing[26]). La criptazione del messaggio mandato dal mittente avviene tramite l'utilizzo della chiave pubblica del destinatario ed è decifrabile solo con la chiave privata di quest'ultimo, in Figura 1.5 è illustrato il meccanismo. Attraverso l'utilizzo della crittografia asimmetrica solo il destinatario può decifrare il messaggio, ma un attore esterno potrebbe modificarlo anche senza comprenderlo. Questo problema può essere ovviato attraverso l'uso di algoritmi, nella blockchain e nelle criptovalute si utilizza la funzione di hashing.

[25] Garavaglia, R. (2021), *Conoscere la blockchain,* Hoepli, Milano

[26] È un metodo utilizzato dagli hacker per poter scoprire password e chiavi di accesso di un individuo. Generalmente l'individuo che attacca provando tutte le parole più comuni per poi passare a linguaggi più complicati. – tratto da Kaspersky.com, *Brute Force Attack: Definition and Examples*, disponibile a https://www.kaspersky.com/resource-center/definitions/brute-force-attack

Figura 1.5. Esempio di invio di un messaggio attraverso il metodo di crittografia asimmetrica

Fonte: liberamente rivisitato da Cyberment.it, *Crittografia un tassello fondamentale nella sicurezza informatica,* disponibile a https://cyberment.it/sicurezza-informatica/crittografia-un-tassello-fondamentale-nella-sicurezza-informatica/

c) In Bitcoin

L'utilizzo della crittografia asimmetrica in Bitcoin e nelle criptovalute risulta di importanza vitale: senza di essa sarebbe possibile alterare la blockchain o spendere il denaro di un altro utente. Bitcoin si basa su uno schema di firma digitale basato su un algoritmo a curva ellittica (ECDSA) per garantire la sicurezza all'utente. La crittografia nelle valute elettroniche deve garantire tre proprietà:

- Autenticazione: una chiave privata è collegata a uno e un solo utente. Se c'è una firma digitale, l'utente in possesso della chiave privata ha inequivocabilmente dimostrato di aver inviato il messaggio;
- Integrità: un messaggio non può essere modificato, altrimenti si invalida la firma;
- Non ripudio: non è possibile negare di aver firmato una transazione.

Avevamo citato ci fosse la possibilità di subire una manomissione, di una terza parte, del messaggio inviato a un destinatario. La risoluzione di questo problema viene affidata alla funzione di hash e all'impronta digitale. La funzione di hash è un algoritmo crittografico che consente di convertire un messaggio (input) di lunghezza arbitraria in una stringa alfanumerica di lunghezza fissata (digest o impronta digitale)[27]. Le principali caratteristiche di questa funzione sono 3:

- lo stesso input restituisce sempre lo stesso output (digest),
- una modifica qualsiasi nell'input genera un output completamente diverso,
- dall'output non si può risalire all'input, a meno di usare il metodo brute-forcing (tentare tutte le combinazioni), per cui si dice funzione unidirezionale.

Le caratteristiche appena descritte sono dimostrate in Figura 1.6 e in Figura 1.7, dove vengono ottenuti due digest completamente diversi nonostante l'input vari solo di un carattere inserito.

L'irreversibilità della funzione dovrebbe garantire la corrispondenza biunivoca tra digest e messaggio originale, anche se c'è la possibilità che due messaggi diversi ci restituiscano lo stesso digest (fenomeno chiamato collisione[28]).

Esistono vari algoritmi di hash, in Bitcoin si utilizza il Secure Hash Algorithm (SHA-256) che restituisce un digest di 256 bit.

Figura 1.6. Creazione di un digest inserendo la parola "laurea" come input

[27] Garavaglia, R. (2021), *Conoscere la blockchain,* Hoepli, Milano

[28] Non è mai successo ad ora per gli algoritmi come lo SHA-256: c'è la remota possibilità dato che il numero di messaggi possibili è maggiore al numero di digest generabili.

Fonte: Tool online per la simulazione dell'algoritmo SHA-256, https://emn178.github.io/online-tools/sha256.html

Figura 1.7. Creazione di un digest inserendo la parola "laurea?" come input

Fonte: Tool online per la simulazione dell'algoritmo SHA-256, https://emn178.github.io/online-tools/sha256.html

1.3.4 Address, wallet, transazioni e Timestamp

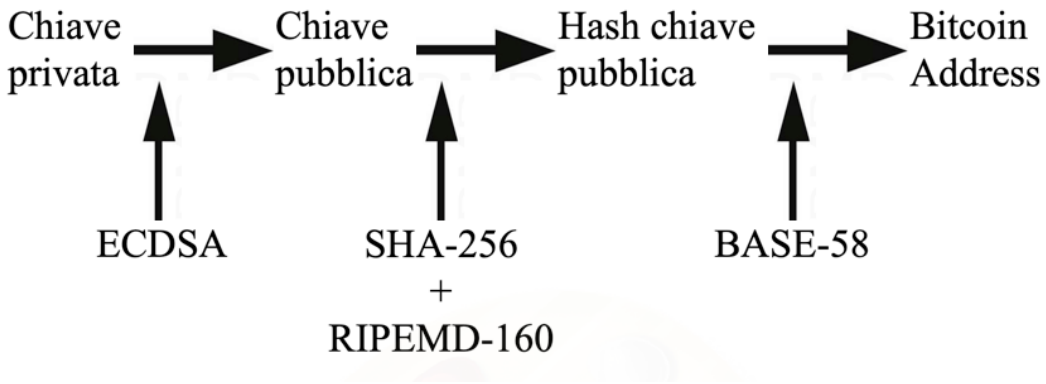
1.3.4.1 Address

Quando si tratta il mondo blockchain, per essere identificati si utilizzano gli indirizzi come identificatori per le transazioni. La generazione di un address passa attraverso numerosi calcoli matematici: partendo dalla coppia di chiavi generata con ECDSA da un numero casuale[29], si può trasformare la chiave pubblica tramite le funzioni di hash

[29] La chiave privata in Bitcoin è una stringa derivante da un numero casuale compreso tra 1 e 1,158 x 10^77 e la chiave pubblica deriva da essa attraverso la crittografia a curva ellittica.

RIPEMD-160 e BASE-58 (la prima trasforma la chiave e l'altra codifica il valore trovato in una stringa alfanumerica)[30].

Figura 1.8. Processo di generazione di un Bitcoin Address con i relativi algoritmi necessari



Fonte: liberamente rivisitato da BitcoinWiki, *Indirizzo Bitcoin,* disponibile a https://it.bitcoinwiki.org/wiki/Indirizzo_Bitcoin

1.3.4.2 Wallet

Nonostante il nome lo suggerisca, la traduzione corretta è "portachiavi", in quanto i wallet custodiscono la coppia di chiavi, quella privata e quella pubblica. Lo definiamo portachiavi perché le criptovalute sono sulla blockchain, non sono all'interno del portachiavi, e posso interagirci solo se sono in possesso della coppia di chiavi che ne dimostra l'effettiva proprietà. Esistono più categorie di wallet:

- Il software wallet: sono applicazioni che conservano la chiave privata e pubblica e risultano sempre connesse ad Internet;
- L'hardware wallet: il salvataggio delle chiavi avviene presso un'unità fisica, si pongono come alternativa più sicura rispetto alla tipologia "software". L'aumento di sicurezza consiste nel fatto che l'unità fisica risulta offline finchè non viene utilizzata insieme ad un altro dispositivo.
- Multisignature wallet: è un wallet che per essere utilizzato necessita di più di una chiave privata per autorizzare una transazione. Esistono tipi di portachiavi multisig di tipo n-of-n, dove n rappresenta il numero di chiavi private e queste

[30] Comandini, G.L. (2020), *Da zero alla luna,* Dario Flaccovio Editore, Palermo

vengono richieste tutte come conferma di una transazione, oppure di tipo m-of-n, dove n rappresenta il numero totale di chiavi private e ne viene richiesta almeno una quantità m (pari o inferiore ad n) per l'autorizzazione delle operazioni[31].

1.3.4.3 Transazioni

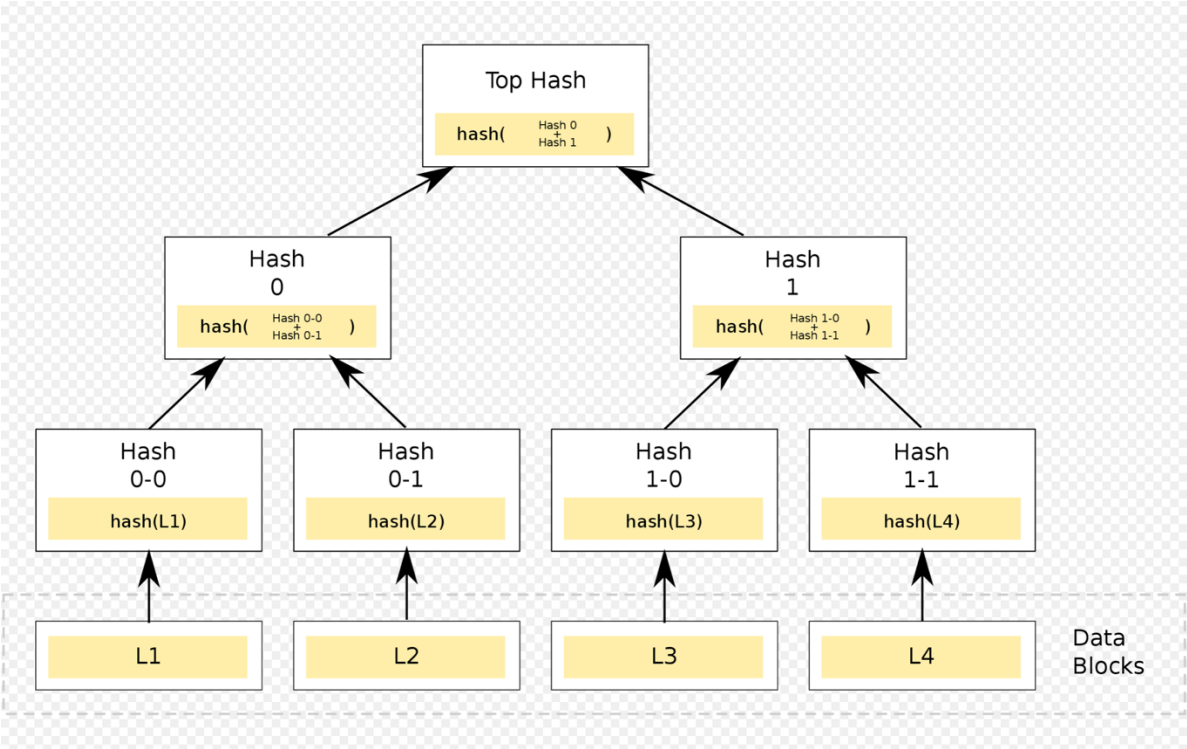
Nota la struttura base della blockchain, si possono analizzarne più concretamente le funzioni osservando lo svolgimento di una transazione. Una transazione è il trasferimento di informazioni (o di valore) e viene trascritta sulla blockchain, la procedura rappresenta la più grande differenza dai sistemi di pagamento tradizionali. Lo svolgimento dell'operazione avviene senza la presenza di un'entità centrale e la sicurezza è basata sul funzionamento delle funzioni crittografiche precedentemente presentate. La struttura della blockchain permette a tutti gli utenti di visualizzare l'ordine cronologico delle transazioni, al fine di poter riconoscere se un utente è veramente in possesso di una quantità di valore necessaria al trasferimento. Il processo di controllo della disponibilità dell'asset avviene applicando ricorsivamente la funzione di hash a un numero di transazioni, la verifica avviene seguendo uno schema Merkle Tree[32]. Il Merkle Tree, come vediamo nella figura 1.10, è uno schema in cui vengono raggruppati i dati, nella blockchain e non solo, che permette di ottenere un'archiviazione delle transazioni più efficiente e sicura. La funzionalità principale dell'albero di Merkle è l'efficienza, come citato in precedenza, dato che per verificare una transazione non necessito di scaricare l'intera blockchain. In ogni blocco si trova la radice dell'albero di Merkle (o Merkle Root) che mi permette di verificare un set di transazioni contemporaneamente, senza dover controllarle una per volta. Il beneficio derivante dal Merkle Tree non è solo questo, infatti, offre maggior sicurezza, incatenando le transazioni tra loro, e lo spazio occupato sulla blockchain è inferiore[33].

[31] Bitstamp.net, *What is a multisig wallet?,* disponibile a https://www.bitstamp.net/learn/security/what-is-a-multisig-wallet/

[32] La struttura ad albero di Merkle permette di raccogliere un maggior numero di transazioni e quindi garantisce una maggiore velocità al processo. – Binance Academy, *Merkle Trees and Merkle Roots explained,* disponibile a https://academy.binance.com/en/articles/merkle-trees-and-merkle-roots-explained

[33] Bitcoin Wiki, *Merkle tree*, disponibile a https://it.bitcoinwiki.org/wiki/Albero_Merkle

Figura 1.10. Rappresentazione di un Albero di Merkle



Fonte: immagine tratta da Bitcoin Wiki, *Merkle tree*, disponibile a https://it.bitcoinwiki.org/wiki/Albero_Merkle

L'eliminazione del problema del double-spending è il frutto dell'attività della rete di partecipanti che controlla e convalida le transazioni, tutto questo iter elimina il rischio di controparte. La componente fondamentale di una transazione sono gli UTXO (unspent transaction output): nella blockchain la quantità disponibile di valuta è riconosciuta come una quantità ancora non spesa. Gli UTXO vengono tracciati dai nodi e attribuiti ai vari proprietari. Un utente in possesso di criptovaluta non è detto sia in possesso di un UTXO equivalente al totale del saldo del proprio wallet, spesso accade che il corrispettivo del saldo sia sparpagliato in più UTXO[34]. Nel wallet del mittente è contenuta la chiave privata che andrà a firmare le transazioni e fornisce una prova della provenienza degli UTXO disponibili. In particolare, una transazione è composta di:

[34] Per esempio, se disponiamo di 1 BTC nel nostro wallet, questo potrebbe essere la somma di: un UTXO di 0.3 BTC e uno da 0.7 BTC

a) input: composto da address, prova crittografica degli UTXO disponibili al mittente e la Scriptsig[35];
b) fee: rappresenta il costo della transazione. Oltre ad avere un costo base definito dal network, si può aggiungere "una mancia libera" per assicurarsi una maggiore velocità nell'inserimento della propria transazione nel blocco[36];
c) output: composto da address del destinatario, valore inviato in UTXO, la marcatura temporale (o timestamp[37]) e il "change" (il resto).

I tre elementi appena descritti sono facilmente visualizzabili in Figura 1.11. Gli UTXO inseriti nell'input vengono consumati nel corso dell'operazione e se la quantità che uso è maggiore al costo totale, ovvero l'output più le fee, mi verrà restituito un secondo output, il change. Al momento dell'input non si conosce ancora la quantità di UTXO disponibile al mittente, è necessario andare a recuperare sulla blockchain le precedenti transazioni. L'utilizzo degli UTXO ha lo scopo di mantenere la sicurezza e ottimizza la validazione delle transazioni. Ogni qualvolta che una data transazione viene inserita in un blocco viene detta confermata, perché una transazione si dica confermata è necessario attenderne sei[38]. Qualsiasi transazione viene definita irreversibile almeno dopo sei blocchi per questioni probabilistiche: maggiore è il numero di blocchi successivi, minore è la possibilità per un attore malevolo di andare ad alterare la catena. Esiste un tipo di transazione speciale chiamata "coinbase transaction" (Figura 1.12), essa è la prima transazione in ogni blocco e rappresenta la ricompensa ricevuta dal miner per il lavoro svolto, la validazione delle operazioni[39].

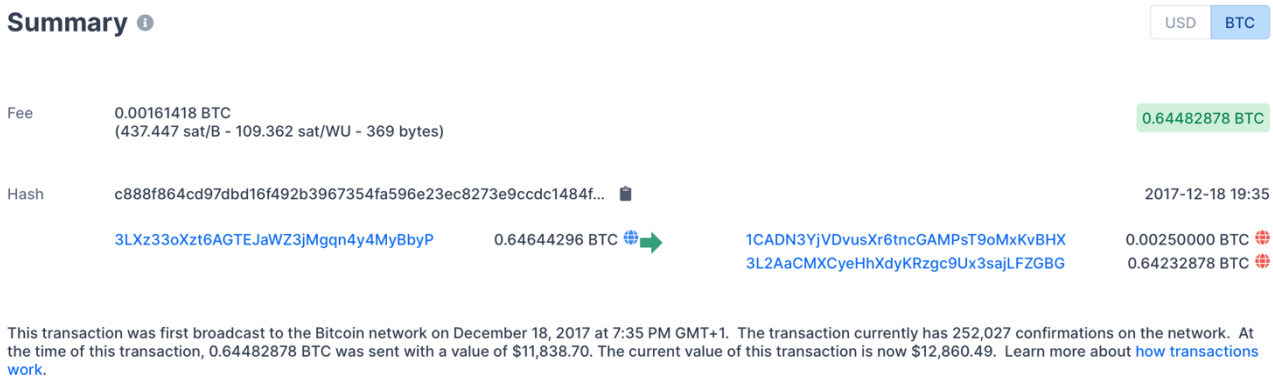
1.3.4.4 Timestamp

Il timestamp è la marcatura temporale, si potrebbe paragonarlo a un timbro che possiamo porre su un documento. Nella blockchain la marcatura temporale è di fondamentale importanza perché è essenziale avere un ordine cronologico nella sequenza di blocchi; dunque, può riconoscere quando viene stipulato uno smart contract oppure quando viene

[35] Uno script che permette di "sbloccare" gli UTXO e quindi renderli spendibili- Comandini, G.L. (2020), *Da zero alla luna,* Dario Flaccovio Editore, Palermo
[36] Saranno analizzate in dettaglio nella sezione dedicata al Mining e Proof of Work.
[37] Spiegato nel paragrafo 1.3.4.4
[38] Quando si riceve dei BTC, si possono spendere solo dall'ora successiva: 6 blocchi per 10 minuti all'uno.
[39] Vedi paragrafo 1.6.2

svolta effetivamente una transazione. L'apposizione del timestamp ad un blocco ne attesta inequivocabilmente l'esistenza in quel preciso momento.

Figura 1.11. Schermata rappresentante una transazione: input e fee a sinistra; i due output e timestamp a destra.



Fonte: schermata ottenuta grazie all'utilizzo del sito Blockchain.com, il quale permette di verificare autonomamente lo stato di una transazione, lo stato dei blocchi o anche verificare la quantità di Bitcoin presente in un wallet

Figura 1.12. Schermata rappresentante la Coinbase transaction: output diretto al miner

Fonte: schermata ottenuta grazie all'utilizzo del sito Blockchain.com, il quale permette di verificare autonomamente lo stato di una transazione, lo stato dei blocchi o anche verificare la quantità di Bitcoin presente in un wallet

1.4 Struttura e funzionamento della blockchain

I dati della blockchain sono salvati ordinatamente in una lunga catena di blocchi legati l'uno all'altro da una prova matematica, l'hash, generata con l'utilizzo della crittografia. Il blocco è l'unità funzionale che contiene i dati inclusi nel registro distribuito, è finalizzato in una quantità di tempo prestabilita (prendendo per esempio Bitcoin si tratta di 10 minuti, altre blockchain hanno altre tempistiche). Ogni qual volta viene aggiunto un blocco alla catena esso viene propagato all'interno del network e collegato al precedente attraverso la funzione di hash; quindi, percorrendo all'indietro il percorso si giungerebbe al blocco 0, il cosiddetto "genesis block".

Ogni blocco appartenente a una blockchain qualsiasi contiene all'interno dei dati, con una dimensione massima decisa dal protocollo, e l'hash del blocco precedente; un cambiamento dell'hash di un blocco comporterebbe all'alterazione di tutti i successivi e si potrebbe subito scoprire il problema.

La funzione di hash quindi funge da "identità digitale" di un determinato file, in quanto attraverso l'analisi della sola stringa derivante da questa funzione è possibile comprendere lo stato dell'intera blockchain[40].

Il blocco è suddiviso in due parti:

- l'header: all'interno si trovano più gruppi di dati:
    - il numero del blocco,
    - l'hash blocco precedente,
    - Merkle root[41],
    - il timestamp[42],
    - nonce[43],
- il body: all'interno si trovano le informazioni (o transazioni) registrate nel blocco.[44]

[40] Chiap, G. (2019*, Blockchain: tecnologie e applicazioni per il business,* Hoepli Editore, Milano

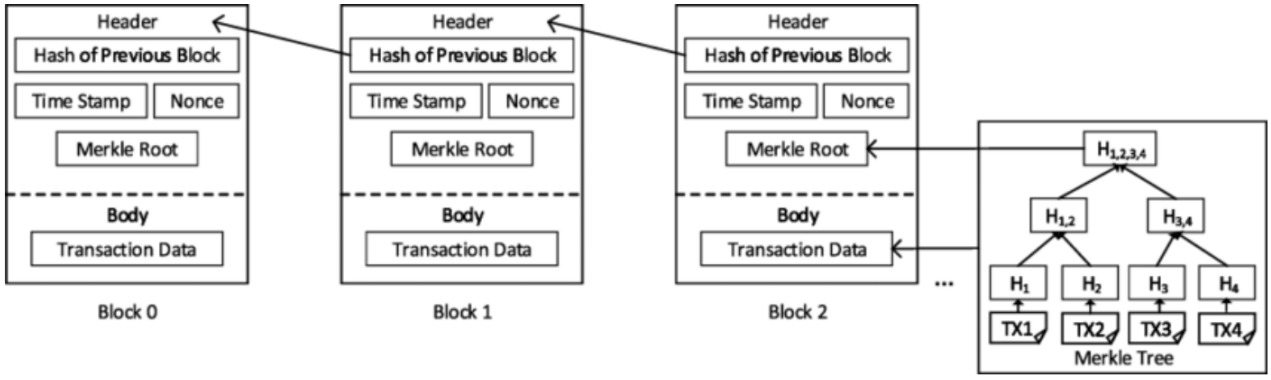
[41] è il campo che ha come valore il risultato della root transaction: un'applicazione ricorsiva della funzione di hashing a un insieme di transazioni, questo permette di dare la certezza della validità di un maggior numero di transazioni contemporaeamente.

[42] Riferimento temporale, ovvero il momento in cui viene creato il blocco. Vedi sezione successiva

[43] Valore casuale necessario alla creazione del blocco

[44] Antonopoulos**,** A. M. (2014), *Mastering Bitcoin***,** O'Reilly Media

Figura 1.13. Struttura di un blocco con rappresentazione del Merke Root



Fonte: immagine tratta dal capitolo 5 del libro di Liang, C.-Y. (2020), *Dynamic spectrum management*, Springer Nature, Singapore, disponibile a https://link.springer.com/content/pdf/10.1007/978-981-15-0776-2.pdf

Ogni blocco ha un solo "genitore", ma è possibile che da esso possano discendere più "blocchi figli", a causa dei fork[45].

La decentralizzazione è uno degli obiettivi alla base di questa tecnologia, affinchè sia un obiettivo raggiungibile occorre avere una rete distribuita e non dipendente da un'autorità centrale. Qualsiasi macchina collegata alla rete viene definita "nodo" e sfrutta dei canali di comunicazione, Internet generalmente, al fine di scambiare informazioni con gli altri utenti. Conosciamo due tipi di nodi:

- Full node (nodo completo): possiede una copia completa della blockchain, scaricata e archiviata nel disco locale. Il suo compito è di controllare che ogni blocco non contenga anomalie, e nel caso ci siano di rifiutarlo. Un nodo completo è indipendente, dato che possiede tutti i dati della blockchain salvati in locale.
- Nodo light: non possiede una copia della blockchain scaricata in locale, riceve solo i dati che gli vengono inviati da un nodo completo fidato.[46]

Affinché il sistema peer to peer funzioni, i nodi devono essere sempre online e aggiornare la blockchain in tempo reale[47].

[45] Ne parleremo nei prossimi paragrafi
[46] Tratto da Binance Academy, *Cosa sono i nodi?* , disponibile https://academy.binance.com/it/articles/what-are-nodes
[47] Tratto da Blockchain Media, *Cosa sono i nodi blockchain e Bitcoin?,* disponibile a https://blockchain-media.org/chto-takoe-blockchain-i-node-bitcoin

1.5 L'importanza dello pseudonimato in Bitcoin

Sin dal principio, Bitcoin viene associato a criminalità e riciclaggio di denaro data la sua natura e visti i suoi precedenti. L'obiettivo di Bitcoin e della blockchain nel settore finanziario è di rendere tutto trasparente e tracciabile, non di essere utenti anonimi su un network. La rete Bitcoin consente ai partecipanti di creare un proprio nome utente deciso liberamente, che ne rende possibile l'identificazione. Vista l'intenzione di incentrare questo elaborato sulle innovazioni portate dalla tecnologia blockchain era necessario fare un appunto sulla questione, supportando il tema con degli eventi accaduti negli anni passati. Nell'agosto del 2016 all'exchange Bitfinex, ai tempi il più utilizzato al mondo, furono rubati circa 120 mila BTC attraverso un attacco hacker e inviati ad un singolo wallet. Nel corso degli anni le indagini delle FBI si sono svolte tracciando, grazie alle caratteristiche della blockchain, tutte le transazioni in uscita da quel wallet giungendo al risultato sperato. A febbraio 2022 viene arrestata una coppia con l'accusa del riciclaggio dei BTC rubati, nonostante tentativi di creazione di identità false e numerosi altri escamotage. L'ente federale americano seguì i tentativi della coppia di riuscire a "pulire" il denaro spendendo somme che non potessero creare sospetto in più siti del dark-web. Sebbene i loro accorgimenti fossero corretti, la storia giunse al termine con il recupero di circa 90 mila BTC, tuttora in custodia del governo americano[48]. L'episodio è un passo importante per la storia delle criptovalute e della blockchain, nel tentativo di limitare il più possibile le attività criminali.

1.6 Il consenso distribuito

Il consenso distribuito ha lo scopo di mettere d'accordo i nodi su un'unica versione della blockchain, si potrebbe definire come il "garante" della fiducia e della sicurezza riposta nel sistema. In un sistema peer-to-peer dove i nodi comunicano tra loro è necessaria un'ottima coordinazione, solo così si riesce a mantenere la velocità e la scalabilità del network. Lo scopo degli algoritmi di consenso è riuscire a conciliare il network su un

[48] Chow, A.R. (2022), *Inside the Chess Match That Led the Feds to $3.6 Billion in Stolen Bitcoin,* The Time, disponibile a https://time.com/6146749/cryptocurrency-laundering-bitfinex-hack/

unico stato della blockchain, riconoscendo le possibili frodi. Nelle blockchain più conosciute gli algoritmi di consenso utilizzati sono: Proof-of-Work, Proof-of-Stake, Proof-of-Authority, Proof-of-History, Proof-of-Elapsed-Time, Proof-of-Capacity.

1.6.1 Il problema dei generali bizantini e la soluzione al problema del double spending

Il Double-Spending è quando un individuo effettua due acquisti simultaneamente utilizzando la stessa somma di denaro, con l'intento di truffare i venditori[49]. Per un sistema decentralizzato come Bitcoin e le criptovalute, non permettere il problema della doppia spesa risulta più complicato, dato che non c'è un'autorità centrale che fa da garante sulle transazioni. In modo analogo al problema del double spending, fu ideato nel 1982 un enigma informatico simile. Il problema dei Generali Bizantini vuole mettere in evidenza le difficoltà di comunicazione che possono crearsi in un gruppo di generali bizantini. L'enigma consiste nel riuscire ad accordare i generali sulla decisione di attaccare la città nemica o ritirarsi, una volta fatta la scelta non è possibile cambiarla. I generali possono comunicare solamente tramite un messaggero. L'obiettivo è il raggiungimento del consenso tra i generali: serve l'accordo sul da farsi per coordinarsi al meglio, in caso non tutti eseguissero la stessa direttiva ci sarebbe un fallimento. La sfida posta dal problema dei Generali Bizantini riguarda la possibilità di manomissione del messaggio, di un possibile arrivo in ritardo oppure lo smarrimento. In aggiunta, è presente il rischio che uno o più generali possano falsificare il messaggio per confondere gli altri. Il problema dei Generali Bizantini ha dato vita al concetto di Byzantine Fault Tolerance (BFT). La Byzantine fault tolerance è la proprietà di un sistema che riesce a resistere alla classe di fallimenti che derivano dal Problema dei Generali Bizantini. Un sistema BFT è in grado di continuare ad operare anche se alcuni nodi falliscono o agiscono in modo disonesto[50].

La Blockchain risolve il problema utilizzando gli algoritmi di consenso distribuito e li tratteremo nella continuazione di questo capitolo, partendo dall'algoritmo Proof-Of-Work che viene utilizzato in Bitcoin.

---

[49] Young Platform, *Bitcoin: come funziona il Double Spending?,* disponibile a https://academy.youngplatform.com/blockchain/bitcoin-come-funziona-double-spending/

[50] Gatti, M. (2019), *Il problema dei generali Bizantini e la soluzione di Bitcoin,* disponibile a https://cryptonomist.ch/2019/08/04/problema-generali-bizantini-soluzione-bitcoin/

1.6.2 Mining

Il mining è il processo con cui vengono creati i nuovi blocchi aggiunti alla catena attraverso l'ausilio dell'algoritmo Proof-of-Work e permette il raggiungimento del consenso distribuito. L'attività di mining consente al network di validare le transazioni, aggregate in blocchi che verranno successivamente aggiunti alla blockchain. I nodi che partecipano al mining si definiscono "miner": il nome del processo e degli attori vuole riferirsi al processo estrattivo dell'oro. Nelle blockchain permissionless, come le criptovalute, i miner vengono ricompensati con le commissioni derivanti dalle transazioni che validano; in quelle permissioned l'attività di mining viene svolta dall'autorità centralizzata.

La creazione di un blocco è il frutto di numerose fasi:

1. Scelta delle transazioni, raccolte dalla transaction pool, da inserire in un nuovo blocco. La transaction pool è un insieme di transazioni già validate dai nodi, ma non ancora inserite in un blocco. La scelta viene effettuata seguendo un ordine non casuale, gli individui che pagano fee più alte[51] avranno la priorità e i loro trasferimenti saranno effettuati prima.
2. Verifica delle transazioni incluse nel blocco per controllarne la validità.
3. Selezione del blocco più recente nel ramo più lungo della catena e inserimento dell'hash di tale blocco in quello in fase di creazione.
4. Tentativo di chiudere il blocco cercando il nonce.
    - Nel caso di successo, il nuovo blocco viene aggiunto alla catena e propagato al network.
    - Nel caso fosse trovato da un altro miner, verranno effettuati i controlli di validità al suo blocco proposto. Se risulta valido viene aggiunto ad una copia locale della Blockchain e condiviso in rete, altrimenti viene scartato e le transazioni che vi erano state inserite vengono immesse nuovamente nel transaction pool[52].

[51] Ricordiamo che le fee sono composte di una tariffa base più un'offerta libera fatta ai miner.
[52] Antonopoulos, A. M. (2014), *Mastering Bitcoin,* O'Reilly Media

1.6.2.1 Proof-Of-Work

Il Proof-Of-Work dimostra la "fatica", intesa come potenza computazionale utilizzata, nella ricerca di un numero computazionalmente difficile da trovare, il nonce, consumando energia e creando una versione della blockchain che deve essere accettata dal network. Ogni miner compete nel raggiungimento della soluzione dell'enigma per la creazione del blocco attuale. La competizione termina nel momento in cui un miner riesce risolvere il problema di calcolo e propaga al network il blocco minato. Il Proof of Work è risolto mediante il bruteforcing, il quale rende impossibile prevedere quale utente troverà la soluzione prima degli altri. La "difficoltà target" nella ricerca del nonce è regolata con il l fine di poter controllare la velocità di estrazione di blocchi. In Bitcoin la difficoltà viene modificata ogni circa due settimane, a seconda della quantità di potenza di calcolo disponibile nell'intero network (hashrate). L'importanza di mantenere costante la velocità di creazione nei blocchi è dovuta dalla possibile creazione di biforcazioni della catena, nel caso si proceda troppo velocemente, oppure di un'eccessiva lentezza nella validazione di transazioni in caso contrario. I minatori devono scegliere quali transazioni includere nel blocco che stanno estraendo dalla transaction pool: questo è un problema di ottimizzazione rispetto alla dimensione del blocco.
Le transazioni sono ordinate in base alla quantità di fee pagate. Potrebbe verificarsi il rifiuto di alcuni miner di includere un numero eccessivo di transazioni perché comporterebbe a un aumento di tempo per la risoluzione del blocco, quindi il rischio di non essere i primi a presentare la proof of work. Una volta che il miner riesce a validare il blocco, presenta la Proof-of-Work agli altri nodi del network e, solo dopo il raggiungimento del consenso distribuito, viene propagato. In Bitcoin, e nelle altre criptovalute che utilizzano questo algoritmo di consenso, il primo miner a risolvere il proof of work e a proporre il blocco nuovo, riceve una ricompensa nella criptovaluta della blockchain di riferimento. La quantità di valuta elargita viene creata e viene distribuita al miner attraverso la transazione "Coinbase".

Bitcoin presenta una caratteristica molto particolare, Satoshi Nakamoto ha voluto creare una sorta di deflazione controllata nel corso degli anni. Ogni 4 anni circa avviene l'halving, le ricompense di ogni blocco vengono ridotte del 50%, fino al raggiungimento

dell'offerta massima di 21 milioni di BTC e si suppone questo avvenga intorno all'anno 2140.[53]

1.6.2.2 Mining pool

Una mining pool è l'unione di più miners che puntano ad aumentare la propria potenza computazionale (hash power) attraverso la collaborazione. Formando un pool è più probabile riuscire a validare un blocco e la redditività aumenta: è meglio ricevere più ricompense minori costantemente che riceverne una grande, sempre che succeda, una volta sola. Ogni miner appartenente alla pool ha entrate in base alla propria percentuale di hash power su quella totale al netto di una trattenuta del gestore. Il vantaggio di questa unione di miner consta anche nella possibilità di non dover conservare la copia integrale della blockchain, ma è sufficiente ricevere dal gestore della pool l'header del blocco e iniziare la ricerca del nonce.

1.6.2.3 Attacchi al sistema Bitcoin

Nonostante l'utilizzo di algoritmi come l'ECDSA e lo SHA-256, rinomati per la sicurezza, la minaccia di incorrere nel problema del double-spending è sempre alta e potrebbe compromettere l'intero funzionamento della blockchain. Il più conosciuto degli attacchi a una blockchain è il cosiddetto "51% attack" e per poterlo attuare serve possedete almeno il 51 % dell'hashrate del network. Nel caso un attore malevolo possedesse questa enorme quantità di potenza di calcolo potrebbe falsificare e validare le transazioni a proprio piacimento validando solo i blocchi che gli interessano. La forza del sistema Bitcoin consta nell'essere una rete accessibile a tutti e quindi, risulta molto estesa. Nel caso si verificasse, un 51% attack comporterebbe per l'ecosistema Bitcoin un crollo del valore e quindi risulterebbe poco conveniente appropriarsi di una valuta di poco valore.

1.6.2.4 Pro e contro del Proof-of-Work

L'algoritmo di consenso Proof-of-Work garantisce l'immutabilità della blockchain, dato che maggiori sono le conferme che una transazione riceve, minore diventa la possibilità

[53] Crypto Italia, *Come è stato scelto il limite di 21 milioni di Bitcoin?,* disponibile a https://cryptoitalia.org/mai-limite-21-milioni-btc/

che un agente malevolo riesca a modificarla. L'utente deciso a manomettere la catena dovrebbe essere in possesso di un'enorme quantità di energia. L'energia che consuma la proof of work comporta un sistema poco sostenibile nel corso del tempo, è una condizione però che è necessario accettare per garantire l'immutabilità del network. Molto spesso le blockchain che utilizzano la Proof-Of-Work sono notevolmente difficili da scalare, anche se il problema è facilmente risolvibile attraverso varie soluzioni off-chain. Il problema della scalabilità, dunque, potrebbe essere risolto eseguendo delle transazioni al di fuori della blockchain. La soluzione porta a dei vantaggi, come l'istantaneità e la drastica riduzione delle commissioni; d'altro canto, svolgendo operazioni al di fuori della blockchain non si beneficia dello stesso livello di sicurezza. In Bitcoin per ovviare al problema si utilizza il Lightning network[54], protocollo che si sta espandendo esponenzialmente in tutto il mondo, che velocizza (come suggerisce il nome) notevolmente i pagamenti utilizzando la criptovaluta. Il mantenimento della sicurezza della blockchain viene garantito dai miner che partecipano al network. In questo periodo, visto il grande aumento del costo dell'energia, in particolare in certe aree geografiche, risulta poco profittevole partecipare all'attività di mining, potremmo definire questo fenomeno come una "discriminazione".

1.6.2.5 Impatto ambientale del mining di Bitcoin

Durante gli anni l'attività di mining è stata presa di mira da numerose testate giornalistiche per via del consumo di energia. Quando nacque Bitcoin, l'attività estrattiva veniva svolta mediante l'utilizzo di CPU e GPU; con l'evoluzione della tecnologia mineraria si è arrivati alla nascita degli ASIC, dispositivi nati con una potenza di calcolo migliore dei precedenti e che utilizzano un quantitativo di energia nettamente inferiore. Un altro punto a favore del mining è la nascita di numerose aziende private che sono entrate nel settore, alcune quotandosi al NASDAQ, e quindi alla ricerca di profitti maggiori dovendo rispettare numeri criteri ESG[55]. Nonostante siano nati i dispositivi ASIC e le aziende quotate al NASDAQ rispettino i criteri ESG, non si può chiudere gli occhi di fronte al consumo elettrico e alle emissioni di CO2. Il network Bitcoin consuma circa 100 Twh[56] in un anno e, secondo delle stime, nel 2021 avrebbe emesso circa 57

[54] Spiegata in paragrafo 1.8
[55] Comandini, G.L. (2020), *Da zero alla luna,* Dario Flaccovio Editore, Palermo
[56] Dato fornito dal Bitcoin Energy Consumption Index dell'Università di Cambridge. Disponibile a https://ccaf.io/cbeci/index

milioni di tonnellate di carbonio, si dovrebbero piantare più di 284 milioni di alberi per essere definiti "carbon neutral"[57].

1.6.3 Proof-of-Stake

Il Proof-of-Stake (POS) è il secondo protocollo più importante per il raggiungimento del consenso distribuito, la differenza con l'algoritmo POW è il fatto che vengono premiati dei validatori[58] che vengono scelti in base allo stake[59] in loro possesso della valuta di riferimento della blockchain. Gli utenti in possesso di valuta possono bloccare temporaneamente i token, avviando il processo di staking, per ricevere come ricompensa la possibilità di diventare una validatore, ottenendo potere di voto e guadagnare dalle fee. Maggiore è la quantità di stake, maggiore è la possibilità di validare i blocchi. Esistono più tipi di algoritmi POS: il più conosciuto nel mondo delle criptovalute è il TENDERMINT BFT[60]. Viene scelto casualmente il produttore del prossimo blocco in base alla percentuale di potere di voto, il produttore raggruppa le transazioni nel blocco e successivamente le propaga al network che procede al voto. Affinché un blocco venga accettato dal network e aggiunto alla catena deve ricevere almeno 2/3 di voti positivi, successivamente il validatore riceve la ricompensa[61]. La POS si definisce algoritmo di consenso asincrono perché non è necessario che tutti i nodi siano attivi, si necessita solo del voto a favore dei 2/3. Nel caso il validatore proponesse un blocco non valido, o anche se fosse spesso offline, subirebbe una sorta di "punizione":

- slashing, il validatore perde una parte dei token in suo possesso;
- jailing, il validatore viene rimosso dal proprio ruolo per un tempo determinato o anche definitivamente.

In alcune blockchain se il validatore decidesse di smettere di svolgere il suo lavoro e riprendere le sue valute serve aspettare una discreta quantità di giorni. Questo motivo è un ottimo deterrente per chi intende di validare un blocco malevolo e sperare di riuscire a ritirare il proprio stake prima di subire lo slashing, nei giorni dove si effettua l'unstake probabilmente gli altri validatori si accorgerebbero del blocco non valido.
Nella proof of stake è necessario fare distinzione tra due figure:

---

[57] Paolini, M. (2022), *Bitcoin e mining: qual è il loro impatto ambientale*, disponibile a https://quifinanza.it/green/bitcoin-mining-impatto-ambientale/640370/
[58] Coloro che confermano le transazioni.
[59] Quantità di valuta in possesso.
[60] Non a caso nel nome è incluso l'acronimo BFT con il significato di Byzanthine fault tolerant.
[61] Garavaglia, R. (2021), *Conoscere la blockchain,* Hoepli, Milano

- il validator, per esserlo si necessita di una grande quantità di coin. L'hardware che permette di far funzionare il programma di validazione deve essere sempre online e ha dei requisiti minimi in base alla blockchain.
- il delegator, colui che delega il proprio stake a un validator e gli concede il proprio diritto di voto in cambio di ricompense, al netto di una commissione per la delega.

Il delegator deve scegliere a che validator affidarsi, nel caso ne scegliesse uno con intenzioni malevole subirebbe uno slashing proporzionale. Il potere di voto non serve solo alla possibilità di validazione dei blocchi, ma anche per avere più influenza sulle decisioni di governance. I validator possono votare le proposte per modifiche o aggiornamenti del protocollo, è necessario superare un quorum per passare all'implementazione della proposta. Il rischio di questo algoritmo di consenso è di essere troppo centralizzato, visto che chi possiede un maggior numero di token ha più potere di voto. E' interesse degli sviluppatori della chain distribuire il più possibile il voting power, incentivando la delegazione ai validatori meno "importanti". Altro fattore importante per mantenere la decentralizzazione è rendere possibile diventare validatore a tutti, senza necessitare di hardware troppo costosi e non accessibili a tutti.

1.6.4 Differenze tra Proof-of-Work e Proof-of-Stake

Il punto più critico di un algoritmo di consenso distribuito viene denominato Sybil Resistance[62] e non c'è un metodo che riesca a inibirlo definitivamente, l'obiettivo della blockchain è renderlo poco conveniente ad un attaccante:

- incoraggiare gli utenti del network a raggiungere un consenso distribuito partecipando con hash power o voting power[63],
- punendo chiunque tenti di comportarsi in mala fede,
- incentivando i partecipanti a comportarsi bene con ricompense.

Nel Proof-of-Work si ha una dipendenza dall'hash power totale, nella Proof-of-Stake dal voting power. Le transazioni nel Proof-of-Stake dipendono dai voti positivi pari almeno al 66% complessivo, se qualcuno riuscisse ad accumulare almeno il 33% potrebbe bloccare il processo di consenso e rischiare di bloccare la creazione dei blocchi. Nel Proof-of-Work si dipende esclusivamente da chi presenta la blockchain più lunga e quindi

[62] Il Sybil attack è un attacco malevolo effettuato utilizzando un gran numero di account con lo scopo di prendere il controllo della blockchain.
[63] Rispettivamente Proof-of-Work e Proof-of-Stake

maggiore è il numero di conferme, maggiore è la probabilità di riuscire ad avere le transazioni non più invertibili.

Il mining disincentiva gli utenti intenzionati nella creazione di blocchi malevoli perché verrebbero subito scoperti dai nodi, il risultato ottenuto sarebbe lo spreco di energia. Per poter attuare un 51% attack sulla blockchain Bitcoin si è stimato un costo di circa 8.6 miliardi di dollari per gli hardware necessari e in aggiunta un costo pari a 20 milioni di dollari al giorno di costo dell'energia[64]. La decentralizzazione nel mining è più facilmente mantenibile dato che non è fondamentale la quantità di coin che i nodi hanno a disposizione: nel 2017 era stata proposta una modifica al protocollo di Bitcoin denominata Segwit2x, con lo scopo di aumentare la dimensione dei blocchi, e nonostante il supporto di grandi detentori della coin non è stata accettata. Il Proof-of-Stake non previene quanto il mining le possibilità di fork frequenti, dato che si potrebbe mettere in staking su entrambe le chain e così facendo ottenere più ricompense. Il rischio di corruzione nel Proof-of-Work è più basso, dato che non basta il 33% del totale del network per ottenere il potere di "censurare" i blocchi successivi[65].

Il Proof-of-Work consuma molta energia e l'impatto ambientale è notevole, soprattutto se si vuole evitare il 51% attack. Restare al passo con la tecnologia negli hardware per il mining implica ulteriori costi, che potrebbero essere sostenibili solo da entità con maggiori disponibilità economiche[66]. Nel mining non è fattibile bloccare gli operatori malevoli permanentemente visto che si opera in anonimo; nel Proof-of-Stake, invece, si può operare lo slashing e il rischio di perdere i propri token frena gli attori malevoli. In momenti di grande congestione di transazioni le fee delle blockchain POW aumentano, dato che i miner si trovano nella situazione di dover svolgere un carico di lavoro maggiore della media. L'aumento delle fee di transazione, allo stesso tempo, è un metodo di difesa verso gli attacchi DDoS[67], rendendo irragionevole inviare numerose richieste di transazione per mandarlo in tilt. I vantaggi del Proof-of-Stake sono il notevole risparmio

[64] Il costo dell'energia utilizzato nel calcolo è di 0.1177 KWh, ovvero il costo medio stimato negli USA a giugno 2022. Tratto da Kraken Intelligence (2022), *Proof-of-Work vs Proof-of-*Stake, disponibile a https://kraken.docsend.com/view/58b6xidjxk44xedc

[65] Garavaglia, R. (2021), *Conoscere la blockchain,* Hoepli, Milano

[66] Ad oggi negli USA è una tendenza in ascesa la nascita di azienda di mining.

[67] "Un attacco DDoS invia molteplici richieste alla risorsa Web aggredita, allo scopo di superare la capacità del sito Web di gestire più richieste e impedirgli quindi di funzionare correttamente." – tratto da Kaspersky.it, *Cosa sono gli attacchi DDos? ,* disponibile a https://www.kaspersky.it/resource-center/threats/ddos-attacks

energetico, si stima una riduzione del 99.9% rispetto all'attività di mining[68], e non si necessita di un continuo bisogno di migliorare gli hardware. I validatori Proof-of-Stake possono rimuovere gli attaccanti permanentemente dal network e penalizzarli togliendoli quantità di coin in possesso. Le blockchain Proof-of-Stake sono più scalabili e le barriere all'entrata sono quasi totalmente eliminate; d'altro canto, il Proof-of-Work è stato testato per maggior tempo e risulta essere meno centralizzato, quindi ha una migliore BFT[69].
In conclusione, si potrebbe affermare che un algoritmo di consenso non può sostituire l'altro, la scelta di uno sviluppatore dipende esclusivamente dall'utilizzo che intende farne. La scelta tra Proof-of-work e Proof-of-Stake per gli sviluppatori di una blockchain varia a seconda dell'obiettivo da raggiungere: il primo permette il mantenimento di un livello di sicurezza e decentralizzazione maggiore, l'altro offre la possibilità di operare su una chain più scalabile e dunque, più efficiente.

1.6.5 Gli altri algoritmi di consenso

Proof-of-Authority: rappresenta un meccanismo di consenso basato sull'esclusività dell'autorizzazione di alcuni nodi alla convalidazione dei blocchi. In questo protocollo prevale l'importanza dell'identità del validatore, che viene controllata da un soggetto terzo, portando a una sorta di centralizzazione.[70]
Proof-of-Elapsed-Time: è un meccanismo di consenso basato sulla richiesta di un partecipante qualsiasi di assumere il ruolo di validatore mediante regole prescritte nel protocollo. La probabilità di essere scelti dal network è casuale e indipendente da qualsiasi fattore. L'algoritmo genera un timer di durata casuale, allo scadere di questo viene scelto il validatore del blocco successivo. Questo sistema è nettamente meno costoso in termini energetici del Proof-of-Work, dato che il lavoro di validazione viene svolto da un nodo per volta, ed è più facilmente accessibile visto l'abbattimento delle barriere all'entrata.[71]

[68] Tratto da Kraken Intelligence (2022), *Proof-of-Work vs Proof-of-*Stake, disponibile a https://kraken.docsend.com/view/58b6xidjxk44xedc
[69] 50% rispetto al 33%
[70] Tratto da Binance Academy, *La Proof of Authority Spiegata,* disponibile a https://academy.binance.com/it/articles/proof-of-authority-explained
[71] Tratto da The Cryptonomist, *Proof-of-Elapsed-Time, l'algoritmo di consenso basato sul tempo,* disponibile a https://cryptonomist.ch/2019/06/15/proof-of-elapsed-time-poet/

Proof-of-History: è un meccanismo basato su il Verifiable Delay Function[72] che rende molto più accessibile partecipare alla validazione di blocchi, alleggerendo l'intera blockchain e più scalabile.[73] La mancanza del timestamp viene soppiantata da un certo numero di passaggi sequenziali per collocare le transazioni in ordine.
Proof-of-Capacity: è un'altra alternativa al Proof-of-Work che utilizza una funzione di hash più complessa e lenta da calcolare. I partecipanti al network possono precomporre la funzione crittografica presso i propri hard disk, si presenta anche questa come un'alternativa eco-friendly.[74]

1.7 I fork della Blockchain

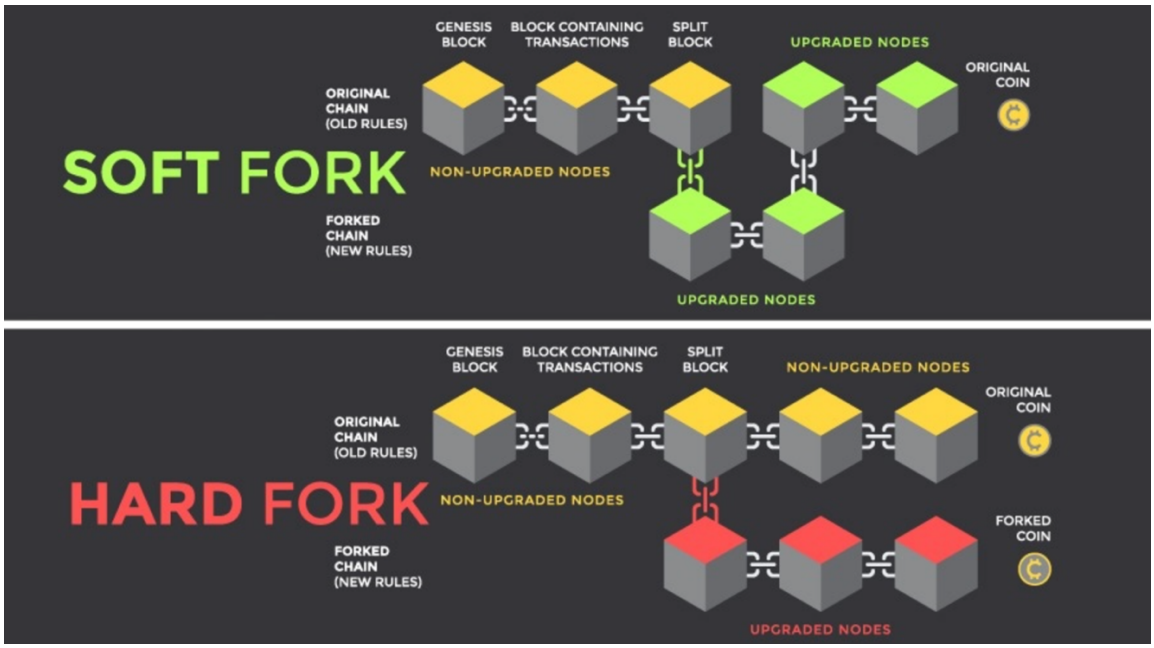
Un fork è una modifica del codice originario di un protocollo che porta a conseguenze diverse in base alle situazioni in cui si crea. Il fork comporta la modifica del codice originario e l'operazione può essere svolta in modi diversi:

- Fork regolare: è il temporaneo dissenso tra i nodi sulla cronologia delle transazioni, senza alcun cambio alla struttura della catena. Accade quando due o più miner risolvono il blocco nello stesso momento e, a causa della latenza del network, non tutti i nodi riceverebbero la stessa versione della blockchain. In breve, questa situazione si traduce in una divisione temporanea. Non esistendo alcuna autorità centrale per risolvere il contenzioso si necessiterà dell'attesa della creazione del blocco successivo a una delle due catene, quella che risulterà più lunga sarà quella scelta da tutti i miner.
- Soft fork: sono effettuati per introdurre nuove funzionalità alla blockchain, comporta la modifica delle regole della blockchain. I miner potranno continuare a svolgere la loro attività se saranno conformi al nuovo regolamento. Il risultato di un soft fork è una catena unica, quindi, i nuovi blocchi sono compatibili con quelli vecchi. Generalmente un soft fork viene attuato per ottimizzare un protocollo[75].

[72] Concetto crittografico che permette di non utilizzare il timestamp tradizionale, ma semplicemente di utilizzare un ordine sequenziale e definito.
[73] Blockchain Consensus Encyclopedia, *Proof-of-History,* disponibile a https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-capacity-space/proof-of-history
[74] Tratto da The Cryptonomist, *Proof of Capacity (PoC): l'algoritmo di consenso che sfrutta l'hard disk,* disponibile a https://cryptonomist.ch/2019/08/17/proof-of-capacity-hard-disk/
[75] Coinbase, *What is a fork?,* disponibile a https://www.coinbase.com/it/learn/crypto-basics/what-is-a-fork

- Hard fork: è il cambiamento radicale delle regole e non retrocompatibile, comporta la biforcazione della catena in due nuove e distinte. Questa divisione della catena comporta il dissenso tra i vari nodi, alcuni vorranno operare sul vecchio protocollo e altri su quello nuovo[76].

Figura 1.14. Rappresentazione di un soft fork e di un hard fork



Fonte: immagine tratta da Finance Magnates, *Soft Fork vs Hard Fork: what are the differences?* disponibile a https://www.financemagnates.com/cryptocurrency/education-centre/soft-fork-vs-hard-fork-what-are-the-differences/

1.8 Scalabilità

Bitcoin nel corso della sua storia ha sollevato molte questioni in merito alla scalabilità. Nel 2017, in un periodo di bolla speculativa, la richiesta di transazioni on-chain era altissima e questo causò un aumento fino a 50 US$ di fee di transazione. Come spiegato nel paragrafo precedente, fu effettuato un soft fork denominato SegWit2x. L'aggiornamento del protocollo modificava la dimensione dei blocchi, prima con un limite massimo di 1MB, permettendo la validazione di blocchi di grandezza fino a 2MB. È stato proposto ancor prima, nel 2015, un protocollo di pagamento chiamato Lightning Network: un sistema che consente il trasferimento di BTC istantaneamente, riducendo nettamente i costi di transazione. Questo aggiornamento, anche se è stato proposto prima

[76] Da Cointelegraph, *Cos'è una hard fork,* disponibile a https://it.cointelegraph.com/bitcoin-cash-for-beginners/what-is-hard-fork

di Segwit2x, è solo in questo periodo in fase di testing avanzata e permette di gestire le transazioni off-chain, regolando i saldi dei wallet solo in un secondo momento. Per effettuare un pagamento bisogna disporre di un wallet con all'interno una certa quantità di valuta e le transazioni avvengono creando un canale tra mittente e destinatario: il valore di BTC scambiato viene segnato in una specie di smart contract, che si risolverà definitivamente solo quando verrà chiuso il canale e trasferita la quantità decisa in precedenza. Il miglioramento che vuole portare Lightning Network è rendere la rete Bitcoin utile per gli scambi di piccola entità, perché in periodi di alta congestione si potrebbe pagare delle commissioni eccessivamente alte e rendere insensato effettuare delle transazioni. Per esempio, per inviare 1$, si potrebbe arrivare a pagare 1$.

1.9 Bitcoin come mezzo d'investimento

Bitcoin nasce come rete per i pagamenti e come moneta, citando Satoshi Nakamoto. L'investimento in BTC è sempre stato considerato speculativo. Man mano che la tecnologia blockchain si è espansa nel mondo, con particolare attenzione agli ultimi anni dopo il COVID-19, si è notato un aumento della correlazione con gli indici americani, in particolare con NASDAQ e S&P500. Bitcoin viene considerato da molti fanatici un bene rifugio, lo definiscono "l'oro digitale", ma la realtà dei fatti è un'altra, per quanto visto finora

Figura 1.15. Correlazione tra Bitcoin e indice S&P500

Fonte: Finbold, *Bitcoin correlation with the S&P reaches a new all-time-high,* disponibile a https://finbold.com/bitcoin-correlation-with-the-sp-500-reaches-a-new-all-time-high/

Nonostante la grande correlazione momentanea coi mercati tradizionali (Figura 1.15) , il motivo per decidere di speculare su asset digitali come le criptovalute è la grande volatilità presente: ricordiamo che il prezzo di BTC nel 2009 al lancio era di 0.1$, a novembre 2021 ha raggiunto un massimo storico di 69.000$. I rendimenti notevoli riportati dall'asset digitale sono rappresentati in Grafico 1.1.

Grafico 1.1 Bitcoin e il suo andamento del prezzo in scala logaritmica, timeframe mensile

Fonte: schermata acquisita da Tradingview

Capitolo II:
ETHEREUM: SMART CONTRACT E ALTRI UTILIZZI

Il processo di adozione della blockchain a livello mondiale è basato sulla fiducia che si sta creando su questa tecnologia e pian piano si sta espandendo in ogni settore. La versatilità della blockchain non è dovuta a Bitcoin, che presenta una possibilità di programmazione limitata, ma ad Ethereum. Ethereum è una piattaforma nata con lo scopo di permettere a qualsiasi sviluppatore di costruire applicazioni e di operare liberamente sulla sua blockchain open-source. In questo capitolo studieremo il binomio "smart contract e Ethereum" partendo da una breve introduzione ai primi, passando per un'analisi della piattaforma e infine concludendo con la comprensione delle potenzialità che hanno insieme.

2.1 Smart contract

Il termine "smart contract" è definito da Nick Szabo "un protocollo di transazione digitale che esegue i termini di un contratto"[77] ed è un'espressione nata intorno agli anni '90. Si potrebbe tradurre letteralmente in "contratto intelligente", in quanto un contratto è un accordo tra due o più parti che viene utilizzato come vincolo legale. La parola "smart" potrebbe rivelarsi fuorviante[78], dato che non esiste al momento un programma che ragiona in autonomia e dotato di razionalità, ma si riferisce allo svolgimento automatico di un'azione prestabilita. Il rischio di controparte viene minimizzato a causa della natura dei contratti intelligenti: essi tendono a svolgere automaticamente le azioni prescritte nel programma nel momento in cui si presentano le condizioni prefissate. Come vedremo nel paragrafo successivo, la tecnologia blockchain ha permesso lo sviluppo delle applicazioni dei contratti intelligenti, non si tratta più di sola teoria. La forma più comune di smart contract è denominata IFTTT (if this than that), ovvero al verificarsi di una condizione viene eseguita un'azione predeterminata[79]. I contratti scritti o gli accordi verbali al giorno d'oggi rispondono a leggi molto severe, durante la stipulazione talvolta è necessaria la

[77] Szabo, N. (1994), *Smart contracts*, disponibile a https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
[78] data la traduzione in "intelligente"
[79] Lai, R. e Kuo Chuen, D. L. (2018), *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2,* Academic Press

presenza di un notaio e non sono facilmente accessibili a tutti. I vantaggi per cui gli smart contract sono stati ideati sono molteplici:

- grande abbattimento di costi e di tempi perché si realizza autonomamente su una rete distribuita di computer, non centralizzata;
- il linguaggio non lascia spazio all'interpretazione;
- sono disponibili in qualsiasi momento sulla blockchain;
- una volta che il contratto viene depositato sulla blockchain, non è più modificabile.

L'ultimo punto appena citato, l'irreversibilità, potrebbe essere inteso anche come un limite dei contratti intelligenti. Di fatto, nel caso le parti intendano sciogliere il vincolo contrattuale si troverebbero bloccati, a meno che non sia inserita una funzione nel codice del contratto che ne permetta l'autodistruzione. Un altro punto critico è la complessità nella scrittura di smart contract molto complessi, far comprendere certe clausole in modo errato alla macchina potrebbe diventare letale. Per questa difficoltà nella personalizzazione di alcuni contratti, ad ora questa tecnologia è più facilmente applicabile nel caso in cui ci siano accordi standardadizzati.

2.1.1 Nascita degli smart contract

Gli smart contract, come detto poco fa, non sono una novità portata dalla blockchain, ma sono la realizzazione di un'idea già concepita verso la fine del millennio precedente. La prima idea rudimentale di contratto intelligente potremmo ritrovarla intorno agli anni '70, quando si necessitava di un sistema per la gestione delle licenze dei software. Il problema oggi lo definiremmo molto semplice, serviva un programma che permettesse la gestione delle chiavi digitali: una volta scaduto il tempo di utilizzo del software e, non rinnovato il pagamento della quota, il servizio cessava di funzionare. Il vero e proprio ultimo tassello prima dell'arrivo alla tecnologia degli smart contract è rappresentato dai Ricardian Contract. Questo tipo di contratti si interpone tra le due parti di uno scambio e ne verifica la legittimità, creando un documento legalmente accettabile dai tribunali.[80] I

[80] Levi, S.D., Lipton, A. B. (2018) , *An Introduction to Smart Contracts and Their Potential and Inherent Limitations,* Harvard law school on corporate governance, disponibile a https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/#4

Ricardian contract creavano un passaggio tra il linguaggio umano e il linguaggio informatico, le caratteristiche principali sono:

a) Sono rilasciati da degli emittenti;
b) Sono gestiti dagli emittenti e conservati dai detentori;
c) Sono comprensibili a chiunque li legga e allo stesso tempo anche dai software;
d) Hanno apposte delle firme digitali;
e) Portano le informazioni del server con le chiavi necessarie;
f) La sicurezza e l'unicità è confermata da identificatori.[81]

La principale differenza tra questo tipo di contratti e gli smart contract sta nell'attenzione posta dai primi nell'automatizzare la parte legale del contratto, i secondi intendono invece automatizzare l'intero processo. Negli smart contract, il procedimento che inizia con l'intesa delle parti fino all'adempimento del contratto viene svolto in assenza dell'essere umano. I primi prototipi di smart contract vennero fatti da un esperto di crittografia degli anni '90, Nick Szabo. L'idea dell'esperto si basava sul tentativo di creare un sistema di gestione digitale di particolari oggetti all'accadere di certe condizioni. L'esempio teorizzato da Szabo fu un semplice distributore di bevande: al verificarsi dell'inserimento di una quantità di denaro decisa in precedenza, viene erogata una determinata bevanda. L'erogazione della bevanda al consumatore è "l'esecuzione del contratto"[82]. Le teorie di Szabo vennero pubblicate nel 1996 e rappresentarono la base di partenza di un nuovo sviluppo del pensiero economico nel commercio online. L'esperto crittografo non poté fare altro che teorizzare i contratti intelligenti, dato che la tecnologia a fine anni '90 non era ancora abbastanza sviluppata da poter costruire una piattaforma utile allo sviluppo di questi. Gli smart contract necessitano di modelli necessari per raggiungere l'automazione nei processi di scrittura e esecuzione, per scriverli serve un linguaggio preciso al fine di eliminare il rischio di interpretazioni sbagliate o i possibili errori[83]. L'avvento della blockchain ha portato con sé le varie caratteristiche definite nel capitolo precedente: un sistema sicuro e affidabile, disintermediato. Le premesse della tecnologia portata da Satoshi Nakamoto parvero il terreno perfetto a un giovane programmatore al tempo ancora diciannovenne, Vitalik Buterin, per lo sviluppo di una piattaforma di riferimento per lo sviluppo di smart contract: Ethereum.

---

[81] The Ricardian Contract, Ian Grigg- https://iang.org/papers/ricardian_contract.html
[82] Basile, A. (2019), *Blockchain: la nuova rivoluzione industriale,* Dario Flaccovio Editore, Palermo
[83] https://www.blockchain4innovation.it/mercati/legal/smart-contract/blockchain-smart-contracts-cosa-funzionano-quali-gli-ambiti-applicativi/

2.2 La piattaforma Ethereum

Ethereum è la seconda blockchain permissionless più conosciuta dopo Bitcoin, l'asset nativo è Ether (ticker: ETH). È necessario detenere Ether se si vuole interagire con smart contract o applicazioni decentralizzate[84] e il suo valore segue le logiche di mercato, può essere considerato un investimento[85]. Il progetto Ethereum nasce da un'idea di Vitalik Buterin nel 2013, quando venne rilasciato il white paper; gli sviluppi successivi vennero condivisi mediante uno yellow paper[86]. La prima versione venne rilasciata nel 2015 e venne presentata come una piattaforma informatica per la creazione di smart contract. Dal concetto di registri distribuiti ora si passa a una macchina virtuale utilizzabile a livello mondiale, chiunque può accedere e allo stesso tempo essere indipendente. Bitcoin rappresenta la miglior soluzione come sistema di pagamento, Ethereum è una blockchain programmabile dove è possibile costruire applicazioni di vario tipo. La rete è un sistema peer-to-peer basato sull'utilizzo di Ether sia per la produzione di smart contract sia per il compenso che viene elargito agli utenti.

2.2.1 Nascita di Ethereum

Ethereum nasce in un periodo dove le potenzialità della blockchain, grazie a Bitcoin, erano già ben riconosciute e si cercava di trovare nuove soluzioni ancor più rivoluzionarie. Chiunque fosse interessato alla creazione di nuovi protocolli avrebbe dovuto scegliere se costruire sulla blockchain Bitcoin, poco scalabile e limitata dal punto di vista della programmabilità, oppure dare luce a una nuova blockchain. L'ideatore di Ethereum è Vitalik Buterin, un giovane programmatore ancora teenager, che ancor prima di concepire la propria piattaforma propose uno sviluppo agli sviluppatori di un altro protocollo: Mastercoin[87]. L'invito del giovane programmatore era di aggiornare radicalmente il linguaggio utilizzato. L'idea venne scarta considerandola non sostenibile

[84] Chiamate Dapp
[85] Tratto da CME group, *Defining Ether and Ethereum,* disponibile a https://www.cmegroup.com/education/courses/introduction-to-ether/defining-ether-and-ethereum.html
[86] Il white paper di Ethereum include la filosofia, la tecnologia alla base e le possibili applicazioni. Lo yellow paper è un documento tecnico che vuole essere più analitico sulla tecnologia che si utilizza. – tratto da Coinsquare, *Whitepaper Versus Yellowpaper: What is the Difference?,* disponibile a https://news.coinsquare.com/learn-coinsquare/whitepaper-versus-yellowpaper-difference/
[87] Un protocollo esistente all'epoca che permetteva l'utilizzo di smart contract.

nel lungo periodo, nonostante il team del protocollo ne fosse rimasto stupito. Il rifiuto non fermò Buterin nel proseguimento della creazione della piattaforma per smart contract e nel corso del dicembre 2013 condivise il white paper di Ethereum: una nuova blockchain programmabile e decentralizzata per la gestione di contratti intelligenti con l'utilizzo di un linguaggio Turing. Il riconoscimento in rete arrivò presto, con aiuti da programmatori di fama mondiale, come Gavin Wood. L'aiuto di Gavin Wood, in particolare, fu essenziale per Vitalik Buterin nell'obiettivo di perfezionare l'idea di quello che oggi come conosciamo come Ethereum. Il progetto dei due programmatori mirava a diventare una blockchain generica, che permettesse a chiunque di utilizzarla e di programmare senza dover avviare nuovi algoritmi di consenso, nuove reti, nuove blockchain. I fondatori di Ethereum hanno lavorato per anni al miglioramento della loro invenzione e il 30 luglio 2015 venne estratto il primo blocco della catena. Questa data viene definita come il giorno in cui il computer del mondo iniziò a servire la popolazione.

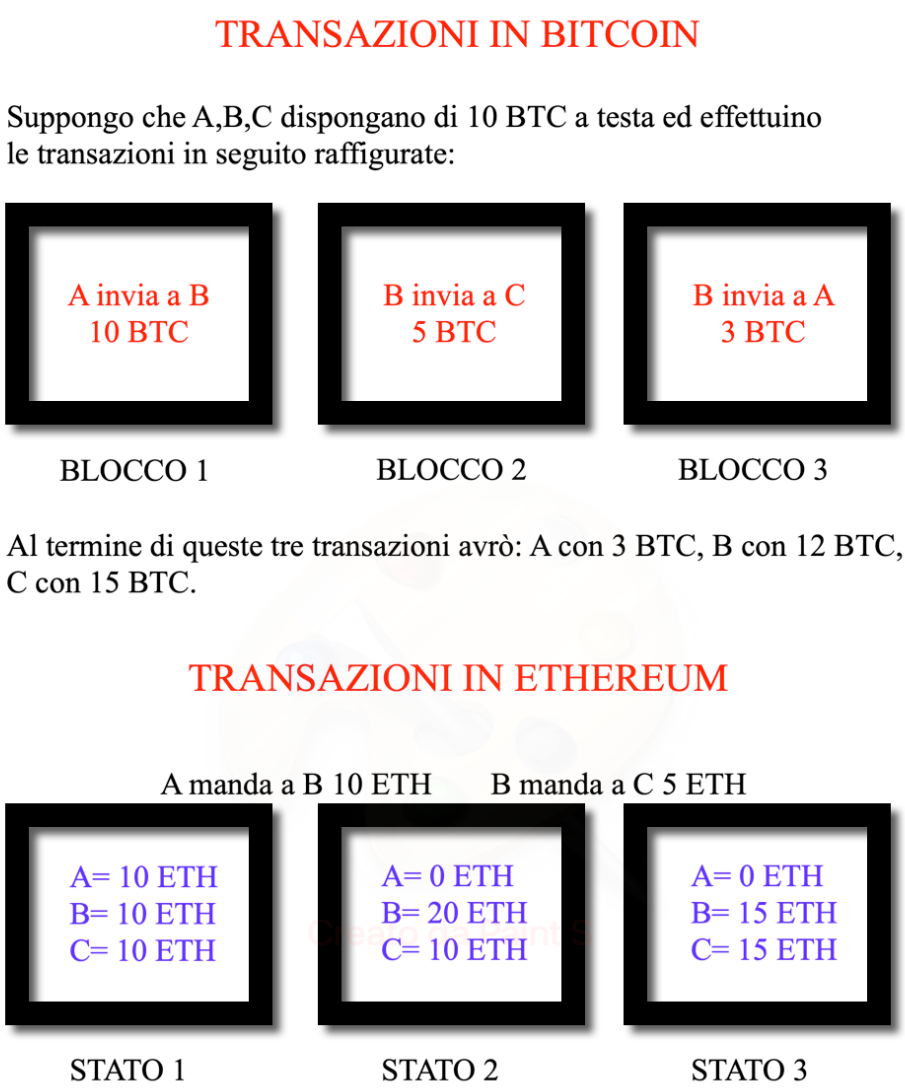
2.2.2 Struttura della blockchain di Ethereum

La blockchain di Ethereum permette sia di effettuare transazioni che di sviluppare e eseguire applicazioni decentralizzate, gli smart contract. L'algoritmo di consenso è tuttora Proof-of-Work, anche se gli sviluppatori stanno lavorando al passaggio a Proof-of-Stake. Il mining di Ethereum presenta qualche differenza rispetto a quello di Bitcoin: la logica alla base è la stessa, ma l'algoritmo per trovare il nonce dei blocchi necessità di più memoria. Ogni blocco viene minato ogni circa 12 secondi e gestisce circa 2-300 transazioni totali all'interno di esso, con un throughput di 15-20 al secondo[88]. Anche la blockchain Ethereum risulta poco scalabile, a causa del tempo eccessivo di elaborazione delle transazioni, gli ideali alla base vanno in contrasto con questo problema. Le transazioni non si basano sugli UTXO come su Bitcoin, Ethereum si definisce "state-machine": le transazioni raggruppate in un blocco vanno a eseguire un cambiamento di stato sulla blockchain, come vediamo nella Figura 2.1. Lo stato è un insieme di dati raggruppati in una radice di Merkle, con una struttura modificata rispetto a quella di Bitcoin, che contiene tutti i collegamenti tra gli account tramite la funzione di hashing. Uno stato è prima del blocco e uno è dopo. Tutti i nodi miner della blockchain trovano l'accordo sul world state della blockchain in un determinato momento e alla chiusura di ogni blocco viene trovato un unico consenso sul nuovo stato. Si definisce world state

[88] Numero di transazioni gestite al secondo

perché definisce lo stato di qualsiasi cosa facente parte del mondo Ethereum: i wallet, quanto posseggono, chi ha effettuato qualcosa, lo stato degli smart contract e le transazioni[89].

Figura 2.1. Rappresentazione del cambiamento di stato e contrapposizione con il funzionamento di Bitcoin



Fonte: liberamente rivisitato e integrato con la parte riguardante Bitcoin da Bitcoininsider.org, *Getting Deep Into Ethereum: How Data Is Stored In Ethereum?,* disponibile a https://www.bitcoininsider.org/article/34603/getting-deep-ethereum-how-data-stored-ethereum

[89] Garavaglia, R. (2021), *Conoscere la blockchain,* Hoepli, Milano

2.2.3 Un linguaggio Turing-complete

Il linguaggio di scripting utilizzato da Ethereum prende il nome dal matematico inglese Alan Turing. Il matematico inglese sosteneva che un giorno si sarebbe riusciti ad ottenere delle macchine che attraverso la loro potenza di calcolo avrebbero potuto risolvere qualsiasi problema. Una macchina viene detta Turing-complete quando può risolvere qualsiasi problema. Bitcoin venne creato con l'intenzione di non risolvere altri problemi al di fuori della creazione di una valuta elettronica decentralizzata, infatti viene definito Turing-incomplete. Ethereum è stato concepito dagli sviluppatori con lo scopo di poter utilizzare qualsiasi programma, anche quelli non ancora conosciuti, attraverso l'uso della dovuta energia e di tempo[90].

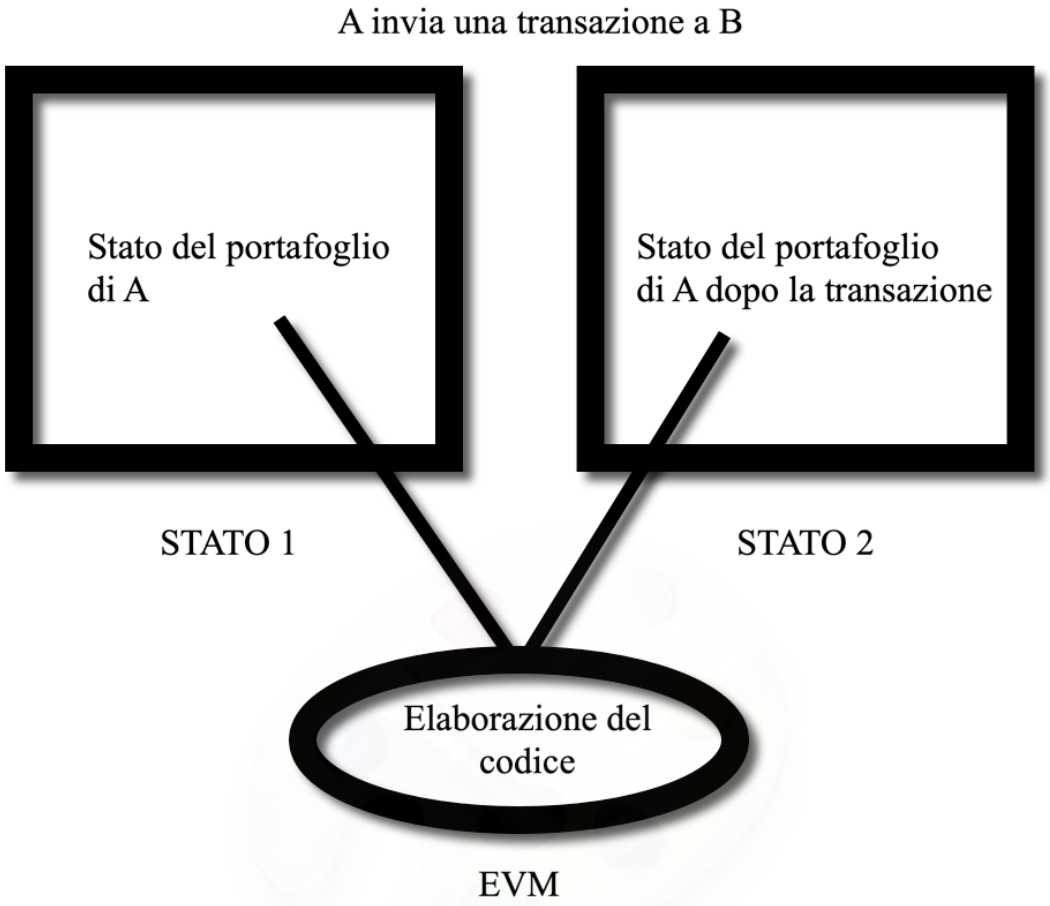
2.2.4 L'EVM

Ethereum esegue i programmi in una macchina virtuale denominata EVM[91], un centro di calcolo separato dal network che garantisce l'esecuzione degli smart contract allo stesso modo in ogni nodo[92]. La funzione principale dell'EVM è l'occuparsi dell'aggiornamento degli stati, come si può vedere nella Figura 2.2: quando mando la transazione, l'EVM elabora il codice e esegue il contratto, quindi poi elabora lo stato. Il linguaggio di scrittura dei programmi di Ethereum è Solidity. L'importanza di Ethereum è la ricerca di una combinazione tra una macchina e un programma scritto su Blockchain, dando vita al Distributed Computing[93]. La flessibilità della piattaforma nell'eseguire qualsiasi codice a cui venga sottoposta potrebbe creare problemi di sicurezza e un possibile spreco di risorse. Il problema dello spreco di risorse è dovuto dall'esecuzione di ogni contratto intelligente inserito in blockchain e, come dimostrò Turing, non si sa l'effettiva durata di

[90] Binance academy, *Turing complete*, disponibile a https://academy.binance.com/en/glossary/turing-complete
[91] Ethereum Virtual Machine
[92] Ethereum.org, *Macchina virtuale Ethereum,* disponibile a https://ethereum.org/it/developers/docs/evm/
[93] In italiano la traduzione è "calcolo distribuito. È un sistema composto da più computer che collaborano e comunicano tra loro, con un obiettivo comune. – IBM.com, *What is distributed computing?,* disponibile a https://www.ibm.com/docs/en/txseries/8.2?topic=overview-what-is-distributed-computing

un programma finché questo non viene fatto partire. La soluzione è data dall'utilizzo del gas, il quale ha la funzione di essere il "carburante" per l'esecuzione degli smart contract.

Figura 2.2. Rappresentazione del ruolo dell'EVM



Fonte: ispirato da Ethereum.org, *Macchina virtuale Ethereum,* disponibile a https://ethereum.org/it/developers/docs/evm/

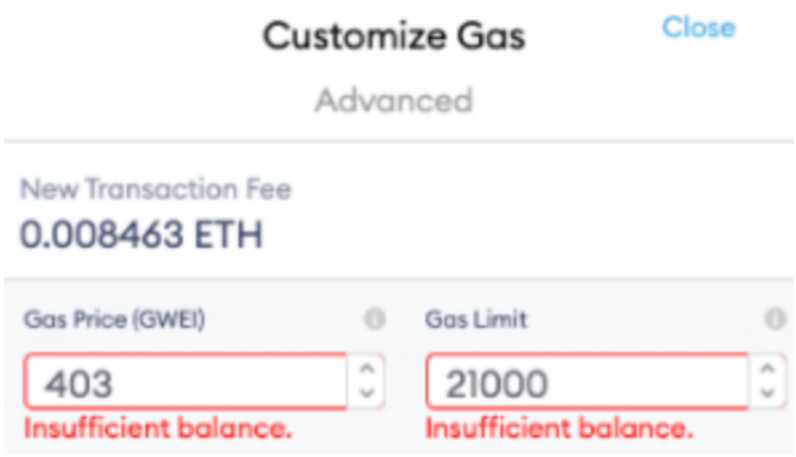
2.2.5 Il gas

L'introduzione del gas, inteso come carburante, ha reso sicuro il network e incentiva i miner a convalidare i blocchi[94]. Il gas viene pagato da chi richiede l'utilizzo della potenza di calcolo di Ethereum, è misurato in wei (1 ETH= 10^{18} wei), più spesso per comodità in gwei (1 gwei= 10^{9} wei), e si utilizzano gli Ether per il pagamento. Il prezzo del gas può variare in base alla congestione della rete, quindi alla domanda, e alle decisioni dei

[94] Ethereum.org, *Gas e commissioni,* disponibile a https://ethereum.org/it/developers/docs/gas/

miner[95]. Al momento dell'invio di una transazione si affronta il pagamento delle commissioni, come si vede nella Figura 2.3 e ci si relaziona con: un parametro "gas limit", ovvero la massima quantità di gas (in gwei) che si intende impiegare nella transazione o nell'esecuzione del contratto, e "gas price", quanto son disposto a pagare il gas per unità. Il gas è essenziale per l'esecuzione dei contratti e, l'EVM, nel caso non si inserisse una quantità adatta nel riquadro "gas limit", bloccherebbe l'operazione. Se venisse esaurito il gas prima del termine del lavoro, la transazione non verrebbe completata. I blocchi di Ethereum hanno dimensioni variabili e dipendenti dalla quantità di gas limite richiesta dai miner, questa possibilità è stata introdotta con l'aggiornamento "London" dell'agosto 2021. La necessità di gas varia in base alla funzione che chiedo di svolgere all'EVM: una transazione semplice generalmente ha un costo basso, la creazione di uno smart contract richiederebbe una quantità importante di gas. È possibile che uno smart contract si autodistrugga nel caso diventi inutile la sua esistenza, questa funzione è stata ideata per non occupare potenza di calcolo e deve essere inserita nel codice.

Figura 2.3. Schermata di setting dei parametri del gas in un hot wallet



Fonte: schermata di personalizzazione del pagamento del gas. Ottenuta utilizzando Metamask, un software wallet

2.2.6 Differenze di struttura con Bitcoin

Abbiamo menzionato la presenza di una differenza di utilizzo del Merkle Root in Ethereum, essa si trova nell'intestazione del blocco sia per la blockchain di Bitcoin sia per quella di Ethereum. Nella blockchain di Ethereum, troviamo una radice di Merkle più

[95] Esattamente come in Bitcoin

estesa, viene definita “radice di stato”, e contiene tutti i dati riguardanti lo stato corrente della catena[96]; in Bitcoin si trovava solo l’hash dell’albero con i riferimenti di tutte le transazioni. I full-node sono i nodi che contengono l’intera storia della blockchain salvata in locale, partecipano alla validazione dei blocchi, alla verifica degli stati e propagano i dati al resto della rete. I light-node non posseggono l’intera storia della blockchain, ma richiedono solo gli header dei blocchi ai nodi completi, e dato che non necessitano di sistemi computazionali avanzati, sono definiti “leggeri”. In Ethereum, i light-node hanno accesso alla radice di stato e possono verificare più velocemente i dati ricevuti, alleggerendo il lavoro dei full-node.

2.2.7 Account e indirizzi

Nella piattaforma creata da Vitalik Buterin esistono due tipi di account:

- EOA (Externally owned account): sono dei conti detenuti da persone che ne possiedono le chiavi private, e permettono lo scambio di token. Le chiavi private degli EOA sono generate da un numero casuale e, come in Bitcoin, la chiave pubblica viene calcolata attraverso l’algoritimo ECDSA da quella privata. Il saldo dell’account è salvato su ogni Merkle Root e si aggiorna ad ogni chiusura di blocco.
- Associati a smart contract: sono dei conti controllati da un programma che, una volta ricevuta una transazione o un messaggio, svolgono determinate azioni prefissate.

Entrambe le tipologie di account sono generalmente collegate ad indirizzi che iniziano con “0x”, questi ultimi sono generati dalla chiave pubblica creando una stringa di 20 byte[97].

2.3 Altri utilizzi di Ethereum

Ethereum permette numerosi utilizzi che vanno oltre alla speculazione, grazie all’utilizzo di smart contract, infatti, si possono creare applicazioni decentralizzate e tanto altro.

[96] Quindi il saldo dei conti, la situazione riguardanti gli smart contract e i codici necessari alla memorizzazione dei dati.
[97] Comandini, G.L. (2020), *Da zero alla luna,* Dario Flaccovio Editore, Palermo

2.3.1 Cos'è un token?

La traduzione letterale "gettone" potrebbe portare in inganno, il significato di token può variare in base all'ambito trattato. Nel mondo delle criptovalute è possibile ottenere token in due modi diversi:

- creando una nuova criptovaluta attraverso l'elaborazione di un nuovo protocollo[98];
- emettendo token su un'altrui blockchain di riferimento, come Ethereum, attraverso la creazione di uno smart contract.

Un token viene identificato come un asset digitale progettato su una blockchain attraverso la scrittura di uno smart contract che riconosce i diritti del proprietario. La tokenizzazione è il processo con cui si sceglie di collegare un bene reale, come una moneta o altri beni materiali, e lo si collega ad un contratto intelligente. La maggior parte dei token conosciuti sono lanciati sulla piattaforma di Ethereum e grazie alla costruzione su di essa possono sfruttarne le caratteristiche, in particolare la sicurezza. Una transazione quando si invia un token basato su una blockchain altrui è generalmente più costosa rispetto allo spostamento di token nativo (come ETH nella rete Ethereum), la causa di questo è il bisogno di interagire con lo smart contract che controlla il token. Esistono diversi tipi di token:

- Utility token: sono valute che hanno un'utilità all'interno del progetto a cui si decide di partecipare. Possono servire per ricevere determinati servizi, per accedere ad applicazioni e non vengono comprati per speculazione, dato che il token non segue il valore del progetto. L'emissione di questa categoria di token non è regolamentata e il rischio di frodi resta sempre altissimo;
- Security token: rappresenta una quota di partecipazione in un progetto, generalmente un investimento del genere è fatto per generare un profitto. Rappresenta il valore del progetto ed è regolamentato secondo le leggi locali[99];
- Fiat-pegged token: sono la rappresentazione digitale di valute "fiat" e il loro valore è garantito da riserve in beni quali denaro contante o commodities. Nel

[98] A volte questa categoria di token viene denominata "coin"
[99] Ad esempio, negli USA l'organo regolamentatore è la SEC

mondo delle criptovalute questa categoria di token viene chiama "stablecoin" e sono diventate una realtà sempre più presente.

- Governance token: rappresentano una quota di partecipazione che dà il diritto di voto nelle organizzazioni decentralizzate, come le DAO, che vedremo successivamente[100].

I vantaggi della tokenizzazione risultano essere molteplici e il mondo della finanza ha iniziato a valutarli più attentamente. La forza di questo processo è nel rendere liquido un mercato che per definizione non lo è, sfruttando la velocità e la sicurezza offerti dalla tecnologia blockchain.

2.3.2 I fiat-pegged token: le Stablecoins

Le stablecoin sono delle criptovalute che rappresentano la tokenizzazione di altri beni reali, come oro o le valute fiat. Il termine in sé ci fa intendere che il valore non oscilla e non subisce l'effetto della volatilità, questi sono i motivi per cui l'avvento di questa categoria di token era necessario. La creazione delle stablecoins era necessaria per poter offrire ulteriori opportunità, oltre alla speculazione, per chi volesse entrare nel mercato; infatti, l'utilizzo di queste permise di utilizzare i propri wallet come un vero e proprio "conto deposito" con un saldo stabile, usato anche per eludere il sistema normativo vigente nel mondo bancario. Perché una stablecoin possa essere definita tale deve assicurarsi di mantenere la conversione con l'asset che intende rappresentare. La logica di domanda/offerta viene eliminata, il valore del token resta ancorato a un bene reale[101]. Per garantire la stabilità del prezzo si creano delle riserve in valuta tradizionale o in commodities, al fine di mantenere un livello minimo di liquidità. L'innovazione portata dalle stablecoin ha alla base la solidità del valore del denaro fiat, aggiunta alle opportunità di sicurezza, velocità e allo pseudonimato della tecnologia blockchain. Esistono più tipologie di stablecoin:

- Fiat-collateralized: le riserve sono costituite da denaro contante in rapporto 1:1. Il loro valore resta sempre ancorato alla valuta di riferimento e nel caso di minime

[100] Basile, A. (2019), *Blockchain: la nuova rivoluzione industriale,* Dario Flaccovio Editore, Palermo

[101] Coscia, E. (2018), *Stablecoins: cosa sono e perché sono così importanti,* disponibile a https://www.fintastico.com/it/blog/stablecoin-cosa-sono-perche-sono-cosi-importanti/

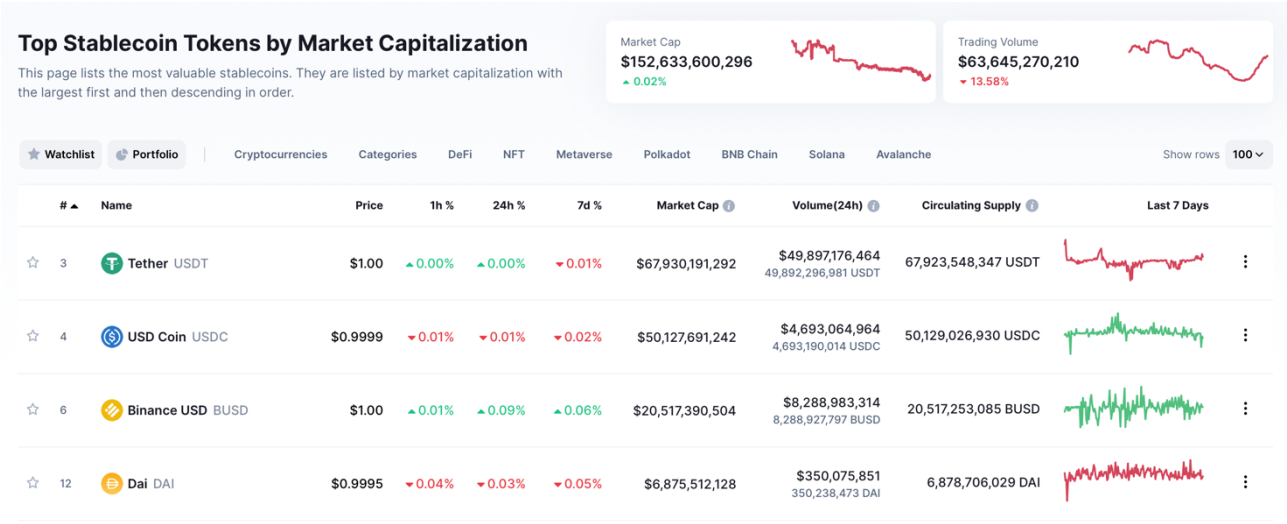
oscillazioni, gli operatori del mercato effettueranno arbitraggio per riportare il tutto alla normalità[102].

- Crypto-collateralized: le riserve sono costituite da altre criptovalute, e vista la volatilità del mercato, in un maggiore quantità rispetto al valore dei token emessi. Questo fenomeno viene denominato sovracollateralizzazione, permette di riuscire a mantenere il valore stabile anche in caso di oscillazioni importanti del valore delle riserve.
- Algoritmiche: questo tipo di token stabili è quello nato più recentemente e necessita di essere ancora collaudato bene. Le riserve vengono sostituite da degli algoritmi combinati a smart contract che si occupano della gestione della supply. I contratti intelligenti operano come un'autorità centrale e mantengono il valore ancorato al bene di riferimento: se il prezzo del token fosse più alto si aumenterebbe l'offerta; al contrario, in caso il valore fosse più basso la si diminuirebbe.

L'utilizzo di stablecoin è diventato sempre più elevato nel mercato delle criptovalute grazie alla possibilità di sfuggire alla finanza centralizzata e alla volatilità. Le stablecoin presenti nella Figura 2.4 sono le più capitalizzate. le prime tre sono di tipo fiat-collateralized e l'ultima è crypto-collateralized. Nella Figura 2.5 si può notare come la percentuale di capitalizzazione di mercato[103], delle stablecoin citate in precedenza, sia in costante aumento dal 2018 e come nei periodi di grossa volatilità esse siano un rifugio spesso preferito dagli investitori. Ancora oggi, le stablecoin sono una novità non ancora a causa della mancanza di trasparenza di alcune società, come nel caso di USDT e USDC, che tuttora non rilasciano audit[104] da emittenti attendibili. Nonostante i vantaggi portati da questi token siano molti e li abbiamo appena descritti, i rischi dovuti alla mancanza di regolamentazioni sono da non sottovalutare, pertanto è necessario svolgere uno studio approfondito se si vuole utilizzarne[105].

[102] Da Blockchain.com (2018)*, Shining light on The State of Stablecoins,* disponibile a https://medium.com/blockchain/shining-light-on-the-state-of-stablecoins-1a92c9172043
[103] Viene calcolata utilizzando la market cap di un token in rapporto alla market cap totale. Nel caso della Figura 2.5 vengono sommate le market cap dei tre token e messi in rapporto alla market cap totale delle criptovalute.
[104] Documenti che attestano la presenza di reserve, i controlli son fatti da revisori contabili.
[105] Da Binance Academy, *Cosa sono le stablecoin?, disponibile a https://academy.binance.com/it/articles/what-are-stablecoins*

Figura 2.4. Schermata con i dati rilevanti sulle stablecoin più utilizzate presenti nel mercato.



Fonte: schermata acquisita da Coinmarketcap.com

Figura 2.5. Dominanza di mercato di USDT, USDC, DAI. BUSD non può essere inserita a causa della carenza di dati.

Fonte: schermata acquisita da Tradingview.com

2.3.3 I token in Ethereum

Nell'ecosistema Ethereum è possibile creare token sfruttandone la sicurezza e potendoli conservare all'interno dei propri wallet. La possibilità di utilizzare la tecnologia smart contract è fondamentale per la creazione dei token ERC-20 (Ethereum Request for Comment[106]) dato che questi ultimi non sono presenti negli account, ma esistono all'interno del contratto. Ad oggi ERC-20 è lo standard dei token dell'ecosistema Ethereum e nello smart contract devono essere scritte sei funzioni fondamentali che una volta dato il relativo comando restituiscono:

- *Total supply*: l'offerta totale di token contenuti nel contratto;
- *BalanceOf* : il saldo di token in un dato indirizzo;
- *Transfer:* il trasferimento di token da un indirizzo ad un altro;
- *Allowance:* dà l'accesso al contratto ai prelievi di token;
- *Transfer from:* il trasferimento di un token verso un indirizzo, questi non devono essere obbligatoriamente proprietà di un utente*;*
- *Approve:* rende programmabile il limite massimo di prelievo di token da parte di uno smart contract[107].

Nel mondo Ethereum è presente un altro standard, denominato ERC-721, che presenta la possibilità di tokenizzare beni reali come opere d'arte o altri beni non fungibili. Un bene così denominato non permette la sostituzione con altri facenti parte della stessa specie[108], sono più semplicemente conosciuti come NFT's (non-fungible tokens). L'introduzione di questo nuovo standard nel mondo blockchain ha permesso l'inserimento di un'idea nuova, basata sull'unicità e sulla rarità dei token. Questo mondo permette una discreta semplicità nel processo di verifica della proprietà attraverso le chiavi e rende possibili grandi sviluppi in futuro per settori dove il valore viene rappresentato dall'impossibilità di replicare certi beni, come quello musicale o artistico.

---

[106] Vengono chiamati ERC-20 perché l'acronimo indicherebbe il nome del protocollo per i miglioramenti alla rete Ethereum, il 20 si riferisce al numero della proposta. - Tratto da Young Platform, *ERC-20*, disponibile a https://youngplatform.com/glossary/erc20/

[107] Garavaglia, R. (2021), *Conoscere la blockchain*, Hoepli Editore, Milano

[108] Da Enciclopedia Treccani, *infungibile*, disponibile a https://www.treccani.it/vocabolario/infungibile/

2.3.4 Le applicazioni decentralizzate (Dapp)

Una Dapp è il risultato di un'interazione di più smart contract che forniscono la base decentralizzata, elemento che più la differenzia dalle applicazioni tradizionali. Se si dovesse "sovraccaricare" di funzioni un solo contratto intelligente si potrebbe creare un sistema inefficiente; infatti, le Dapp ne utilizzano uno per ogni funzione diversa. Le applicazioni decentralizzate sono composte da:

- Backend: è composto da più smart contract, ognuno ha funzioni diverse. È possibile rimuovere e sostituire uno smart contract in caso di bug.
- Frontend: l'interfaccia che si presenta all'utente, generalmente di facile comprensione per l'utente medio;
- Archivio dati: ogni utente memorizza le proprie interazioni compiute nella Dapp nella blockchain.

Gli sviluppatori sono incentivati allo sviluppo di applicazioni, dato che non è necessario pagare commissioni alte né dover rendere pubblica la propria identità, al pubblico è noto solo lo pseudonimo a cui è collegato l'account blockchain. Ad oggi, le tipologie di Dapp sono molteplici: si possono realizzare exchange decentralizzati, piattaforme di pubblicità, giochi e quanto altro si voglia senza alcun limite. La nascita delle Dapp vuole colmare alcuni disagi creati dalle applicazioni centralizzate: il più grande vantaggio è il totale controllo dei dati personali, la sicurezza è garantita dalla struttura, l'accesso è aperto a tutti e gratuito. Possiamo affermare che le applicazioni decentralizzate sono strutture essenziali che permettono l'interazione con la tecnologia blockchain ed offrono una vasta gamma di strumenti finanziari, o non, in sicurezza.

2.3.5 Le ICO e le sue evoluzioni

Una ICO (Initial Coin Offering) è letteralmente la "prima offerta di un token al pubblico" e potremmo paragonarla in parte a una IPO e in parte al crowdfunding. La ICO non necessita di regolamentazioni per l'offerta al pubblico né tantomeno distribuisce quote azionarie, ma coin o utility token. In un'offerta di token al pubblico il tutto viene gestito attraverso smart contract, il quale si occupa della gestione delle vendite e si rende essenziale per ottenere la fiducia. Gli organizzatori di una ICO sono solitamente aziende che hanno bisogno di fondi per procedere nella realizzazione del progetto, condiviso in

rete e pubblicizzato nei white paper. I vantaggi di ottenere "la quotazione" nel mondo blockchain teoricamente dovrebbero esserci sia per gli organizzatori della ICO, sia per coloro che decidono di destinare dei fondi all'acquisto di token. La parola "teoricamente" scritta in precedenza è di grande importanza, è necessario ricordare che il mondo blockchain non offre garanzie contro truffe; infatti, negli anni precedenti si sono verificati spesso eventi negativi per gli investitori dovuti ad errori nella scrittura degli smart contract, talvolta voluti, oppure truffe legate all'insider trading. Noti i rischi, è essenziale dire che questa struttura di offerta al pubblico rende possibile a ogni individuo la partecipazione a qualsiasi progetto. In una ICO non è necessario rispettare limiti temporali né ottenere autorizzazioni da autorità centrali, favorendo lo sviluppo dei progetti con fondi ottenibili velocemente. La struttura di una ICO può essere divisa in più fasi:

1. nascita dell'idea e esposizione al pubblico;
2. creazione di un white paper, il quale ha la funzione di promuovere il progetto spiegandone le caratteristiche;
3. condivisione del white paper e ricerca di eventuali partnership a scopo di marketing;
4. creazione dello smart contract: stabilendo la quantità massima vendibile (hard cap) nella ICO, la minima (soft cap) per poter intraprendere il progetto e il prezzo;
5. lancio della ICO: invio del denaro (in criptovaluta o fiat) allo smart contract, effettuato il trasferimento il proprio indirizzo riceve la quantità di token, la fine della ICO avviene allo scadere del tempo fissato o al raggiungimento della quantità massima vendibile.

   Se non si raggiungesse il soft cap, il progetto potrebbe essere abbandonato oppure avere ritardi sul programma;
6. sviluppo del progetto, in caso di risultato positivo del processo.

L'investitore o lo speculatore interessato a una ICO può ottenere ottimi profitti visto il prezzo fissato dall'azienda e non ancora in balia della logica di domanda/offerta. Anche la piattaforma Ethereum si è finanziata attraverso questo metodo di crowdfunding nel 2014, un Ether era venduto ad un prezzo fisso che si aggirava intorno ai $0,30 e i $0,40. Per buona parte del 2017, giornalmente venivano effettuate ICO, finché enti regolatori come la SEC non hanno iniziato a notare dei tentativi di raggirare le norme. Il fenomeno

si è pian piano eclissato a causa della grande percentuale di truffe, portando gli investitori verso lidi più sicuri come le STO (Security Token Offering). Gli exchange centralizzati (definiti CEX, Centralized Exchange) e decentralizzati (definiti DEX, Decentralized Exchange), vista la fiducia in essi riposta dai partecipanti del mondo blockchain, decisero di dare vita alle IEO e alle IDO[109]. Sia le prime che le seconde sono la realizzazione di un rapporto di simbiosi: le startup possono ottenere fondi ed essere garantite dalle ricerche condotte da team di tecnici sovvenzionati dagli exchange, questi ultimi il profitto lo ottengono dal pagamento di commissioni e da una percentuale di token.

2.3.6 Le DAO

Una DAO (Decentralized Autonomous Organization) è un'organizzazione autonoma decentralizzata che sfrutta la tecnologia blockchain attraverso l'utilizzo di molteplici smart contract. L'utilizzo dei contratti intelligenti favorisce l'impossibilità di trasgredire le regole della governance in un mondo decentralizzato, per questo viene definita una struttura autonoma. Una DAO agisce attraverso l'utilizzo di programmi codificati, fondati sull'utilizzo della blockchain, e nella totale assenza di sistemi gerarchici. Per partecipare a un'organizzazione autonoma si necessita di alcuni titoli che attestano la possibilità di entrata: gli utility token o i governance token, questi garantiscono solitamente il diritto di voto. La DAO permette la creazione di un sistema perfettamente democratico e autonomo dove chiunque abbia interesse, e possiede i token che permettono di votare, può incidere sul percorso di sviluppo di un progetto. Le regole possono essere cambiate, modificando quindi il contratto, solo se la modifica viene proposta all'interno della DAO e viene votato positivamente dalla community. Lo smart contract può essere cambiato nel caso vengano scoperti errori nella scrittura che rendono, di fatto, l'organizzazione vulnerabile ad attacchi malevoli[110]. Nelle DAO token-based per potervi partecipare si necessita solo del possesso del token di governance, acquistabile in exchange decentralizzati, e dunque, non ha barriere all'entrata. Nelle DAO share-based vengono effettuate delle "selezioni", per entrarvi bisogna fare una proposta alla community in cui si offre un tributo, in termini di lavoro o token. In questa struttura decentralizzata manca un possibile responsabile nel caso vengano violate delle norme o nel caso succeda qualcosa di negativo, motivo per cui

[109] IEO: Initial Exchange Offering, IDO: Initial Dex Offering
[110] Come nel caso di The DAO che viene riportato nel paragrafo 2.4

si celano ancora molte domande dietro questa organizzazione di governance[111]. Si possono riassumere le differenze tra un'azienda tradizionale e una DAO come in Tabella 2.1.

Tabella 2.1 DAO e aziende tradizionali a confronto

DAO	Azienda tradizionale
- Organizzazione decentralizzata fondata sui possessori di governance token - Le regole sono scritte su uno smart contract - L'identità dei possessori di governance token è gestita dallo smart contract di riferimento - La proprietà dei governance token è regolata dallo smart contract di riferimento	- Organizzazione societaria fondata su una struttura gerarchica - Le regole seguono le leggi locali - L'identità dei possessori di quote è nota - La proprietà di una quota è certificata da un contratto o da un titolo di credito

Fonte: tabella ispirata da Binance Academy, *Le Decentralized Autonomous Organization (DAO)*, disponibile a https://academy.binance.com/it/articles/decentralized-autonomous-organizations-daos-explained

In conclusione, una DAO potrebbe rappresentare uno sviluppo futuro della governance nel mondo delle società, garantisce la sicurezza e la democrazia. Ad ora, questa struttura organizzativa è ancora in fase di sviluppo e per vedere future applicazioni nelle aziende tradizionali necessita di numerosi miglioramenti.

2.4 L'importanza di non fare errori negli smart contract: The DAO attack

Nell'aprile 2016 ci fu una ICO per ottenere i token DAO, durata 28 giorni e vennero raccolti 150 milioni di dollari in Ether, fu un successo. La raccolta avvenne attraverso uno smart contract che associava gli account ai token, come abbiamo spiegato in

[111] Chiap, G. (2019)*, Blockchain: tecnologie e applicazioni per il business,* Hoepli Editore, Milano

precedenza, e nel caso un utente avesse voluto successivamente uscire dall'organizzazione necessitava solo di richiamare una funzione scritta nel codice. Nella scrittura del contratto era stato fatto un errore che potremmo definire banale: al momento del prelievo per uscire dalla DAO non veniva azzerato immediatamente il saldo del wallet, questo permise di ritirare i fondi anche senza averne effettivamente depositati[112]. Qualche utente si accorse della vulnerabilità e lo denunciò, il tempo di fare una proposta alla community e di applicarla però sarebbe stato in ogni caso più di quanto ne potesse servire a un attaccante. L'attacco avvenne a giugno 2016, pochi mesi dopo la nascita della DAO, e furono rubati fondi per 70 milioni di dollari in Ether. Lo sviluppatore della piattaforma Ethereum, Vitalik Buterin, propose un soft fork per risolvere la situazione congelando i fondi. In risposta, gli arrivò una lettera aperta anonima dove veniva spiegato che non c'era stato alcun furto o violazione di leggi, in quanto lo smart contract era stato rispettato[113]. La community si divise tra chi sosteneva le ragioni dell'attaccante e chi no, la soluzione venne scelta dagli utenti del network. Fu scelto l'hard fork e la blockchain venne biforcata cambiando il blocco dov'era avvenuto l'attacco, nacquero molte discussioni e si parlò molto di una tendenza alla centralizzazione. Questo caso mise in luce lo stato ancora di gioventù della struttura DAO e i rischi che comporta la scrittura errata di uno smart contract.

2.5 Una possibilità di interazione col mondo reale: gli oracoli

Gli oracoli nella storia antica rappresentavano un punto di collegamento tra gli dèi e l'essere umano, essi potevano rispondere a tutte le domande a cui l'essere umano non poteva trovare risposta. Lo stesso compito lo svolgono gli oracoli blockchain. L'utilizzo della blockchain e degli smart contract può essere limitato dalla disponibilità di dati "on-chain", è necessario un ponte con il mondo "off-chain". È doveroso ricordare che la funzione degli oracoli non è una fonte di dati, essi risultano essere coloro che reperiscono le informazioni e le controllano, solo successivamente le propagano agli smart contract . Conosciamo più tipi di oracoli in base alle funzioni, al dove reperiscono le informazioni e alla decentralizzazione o meno.

[112] Tratto dall'articolo di Siegel, D. (2016) , *Understanding The DAO hack for journalists,* disponibile a https://pullnews.medium.com/understanding-the-dao-hack-for-journalists-2312dd43e993

[113] Basile, A. (2019), *Blockchain: la nuova rivoluzione industriale,* Dario Flaccovio Editore, Palermo

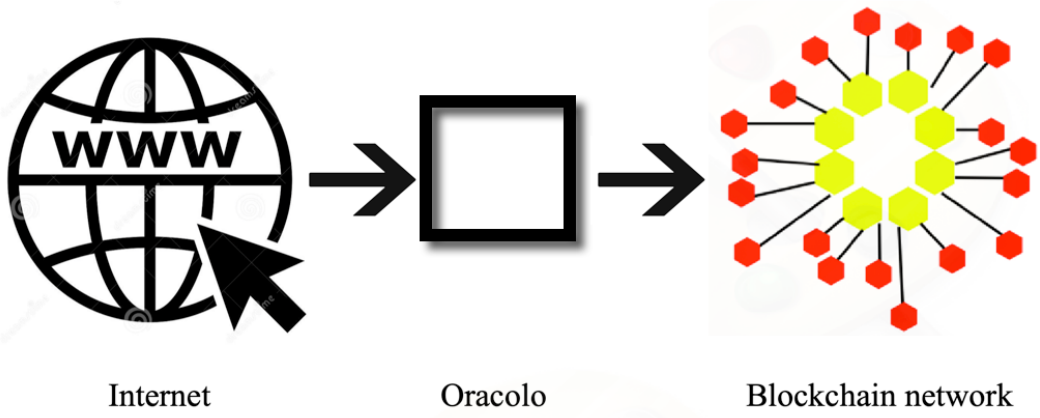
2.5.1 Oracoli in entrata e in uscita

Permettono lo scambio di informazioni tra la blockchain e il mondo reale. Gli oracoli in entrata portano le informazioni dall'esterno all'interno, quelli in uscita fanno l'operazione contraria.

2.5.1.1 Oracoli software

Sono gli oracoli che interagiscono con informazioni recuperate da più siti web, server o database, come dimostra la Figura 2.6. L'essere online permette una comunicazione diretta con gli smart contract in tempo reale. Questo genere di oracoli permette la lettura di parametri come i tassi di cambio di valute o i prezzi di asset.

Figura 2.6. Funzionamento di un oracolo software



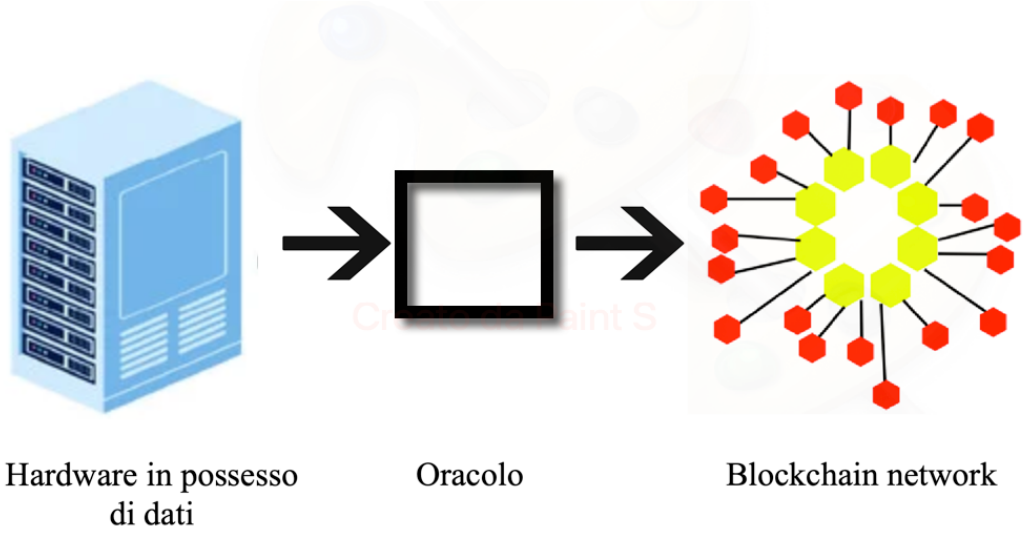
Fonte: liberamente rivisitato da AQOOM, *Blockchain for Novices series: what are Oracles?,* disponibile a https://medium.com/@AQOOM/blockchain-for-novices-series-what-are-oracles-8683737cf9ef

2.5.1.2 Oracoli hardware

Certi tipi di smart contract necessitano di interazioni col mondo fisico, la loro funzione è la possibilità di mettere a disposizione questi dati agli smart contract. Questa categoria

permette la comprensione di alcuni dati non recuperabili online essenziali per determinati tipi di smart contract, come si vede nella figura 2.7[114].

Figura 2.7. Funzionamento di un oracolo hardware



Fonte: liberamente rivisitato da Caldarelli, G. (2022), *Overview of Blockchain Oracle Research,* disponibile a https://www.mdpi.com/1999-5903/14/6/175/htm

2.5.2 La decentralizzazione

Un oracolo centralizzato comporta il rischio di cadere nel Single Point of Failure, tutto quello che la tecnologia blockchain cerca di evitare. Gli oracoli decentralizzati mirano alla totale eliminazione del concetto di fiducia anche se non è effettivamente realizzabile, il consenso viene distribuito tra vari partecipanti. Gli smart contract reperiscono le informazioni da più oracoli, l'effettiva dimostrazione di un mondo basato sulla distribuzione dei dati.

2.5.2.1 Un pilastro del mondo decentralizzato: Chainlink

Chainlink rappresenta una rete di oracoli decentralizzati che dà la possibilità di creare un'infrastruttura indipendente e sicura nel mondo blockchain. Questo protocollo

[114] Larchevêque, E. (2016), *Hardware Oracles: bridging the Real World to the Blockchain,* disponibile a https://bravenewcoin.com/insights/hardware-oracles-bridging-the-real-world-to-the-blockchain

rappresenta il primo progetto che è riuscito a far interagire il mondo esterno con il mondo on-chain attraverso una rete di smart contract ed è l'oracolo decentralizzato più conosciuto nella rete Ethereum. Chainlink funziona attraverso una rete di nodi che seguono eventi reali da cui ricavano informazioni da inviare agli smart contract. Essendo una rete di più nodi che svolgono lo stesso lavoro, il consenso è raggiunto quando la stessa risposta è indicata da più utenti e questi vengono ricompensati ricevendo il token LINK. Oltre a essere un oracolo che riceve dati dall'esterno, permette anche la comunicazione di dati tra più blockchain vista il collettivo impiego del protocollo.

2.6 Ethereum 2.0

Ethereum è una piattaforma all'avanguardia che ambisce a sviluppi costanti e continui al fine di migliorare l'esperienza degli utenti. Il problema più determinante che viene riscontrato è l'insostenibilità della blockchain che utilizza l'algoritmo di consenso Proof-of-Work, a causa di questo viene consumata, infatti, una quantità eccessiva di energia. Sono presenti ulteriori problemi dovuti alla scalabilità della blockchain e altri riguardanti la privacy nelle transazioni. Gli sviluppatori da anni stanno sviluppando molteplici aggiornamenti al fine di risolvere tutti i problemi in un passaggio ad Ethereum 2.0. Il problema del costo delle gas fee nell'ultimo periodo è aumentato a tal punto che progressivamente la piattaforma viene rimpiazzata da altre blockchain, limitandone l'adozione dei clienti meno abbienti. Oltre alla poca convenienza dell'utilizzo di Ethereum, è necessario rendere la rete più versatile per un aumento di utenti in futuro che porterebbe a un maggior volume di transazioni. Il problema della scalabilità è stato risolto finora dall'utilizzo di blockchain layer 2[115], ovvero catene separate con i relativi protocolli che sfruttano la sicurezza e la decentralizzazione di Ethereum. La creazione di un secondo livello consente la diminuzione del carico di transazioni della blockchain principale, la quale riceverà poi le prove delle transazioni effettuate dal protocollo layer 2[116]. L'utilizzo di layer 2 non è una soluzione temporanea, quando si passerà totalmente ad Ethereum 2.0 continuerà ad essere utile per mantenere la rete non congestionata. Il processo, denominato anche "Serenity" è diviso in tre fasi:

[115] La traduzione di "layer" è "livello"
[116] Da Ethereum.org, *Cos'è il livello 2?*, disponibile a https://ethereum.org/it/layer-2/

- Fase 0: il “Merge”, consiste nel passaggio al Proof-of-Stake ed è lo sviluppo più importante e renderà la blockchain del 99.9% più efficiente[117] spostando il ruolo di validatore in mano ai detentori di Ether. Questa fase è in attuazione in questo periodo di fine 2022.
- Fase 1: lo “sharding”, prevede l’implementazioni di blockchain frammentate, che permetteranno di rendere la blockchain più scalabile e l’utilizzo di più shard di catena che si relazionano con una “Beacon chain”, la catena centrale, per la gestione dei dati. Il periodo di attuazione non è ancora definito con precisione, tra i sei e i dodici mesi dopo il Merge.

Questo grande sviluppo di Ethereum favorirà l’essere più green, d’altro canto la validazione dei blocchi sarà in mano ai più grandi possessori di Ether. Serenity porterà un grande cambiamento nella politica monetaria di emissione del token: la riduzione del tasso di inflazione di Ether calerà del 90%, dato che le rewards date ai miner erano notevolmente più alte. Si stima che considerando il burning delle gas fee, introdotto nel 2021 dall’EIP-1559[118], combinato alla nuova politica di emissione con il Proof-Of-Stake possa portare a una situazione in cui il token ETH sia deflattivo. Il burn delle gas fee è la distruzione di una parte delle commissioni pagate nelle transazioni, così facendo si riesce a limitare l’offerta del token. Nei periodi dove vengono fatte molte transazioni nella rete Ethereum vengono bruciati più token, dato che sono pagate più gas fee dagli utenti. Nella Figura 2.8 si nota come in un periodo di mercato ribassista, come quello che si sta vivendo da fine 2021, comporti un minore utilizzo della blockchain Ethereum, riducendo il numero di token bruciati.

[117] Dato tratto da Ethereum.org, *Consumo energetico di Ethereum,* disponibile a https://ethereum.org/it/energy-consumption/
[118] Ethereum Improvement Proposal

Figura 2.8. Dati sul tasso di inflazione di Ether con la Proof-of-Work.

Fonte: schermata acquisita da Ultrasound.money

2.7 Gli Ether come mezzo di investimento

Ethereum rappresenta la miglior piattaforma disponibile ad ora per la creazione e lo sviluppo di smart contract. Nonostante abbiamo definito Ether come una coin, potremmo definirlo utility token perché sono necessari per poter operare sulla blockchain. Gli Ether, come i Bitcoin, sono distribuiti come ricompensa per i miner; ma a differenza di Bitcoin, l'offerta massima di Ether non è bloccata e l'inflazione dovuta alla creazione di nuovi token viene regolata seguendo dei principi deterministici, con la tendenza all'abbassarsi progressivamente. Dopo l'aggiornamento EIP-1559, probabilmente il più importante, il protocollo ha modificato radicalmente il tasso di inflazione: una percentuale delle commissioni pagate nelle transazioni viene "burnata", ovvero eliminata per sempre dalla blockchain; quindi, maggiori sono gli scambi sulla rete, più cala l'offerta. Il valore di un Ether è stato molto volatile nel tempo, è necessario considerare che il prezzo alla ICO era di $0,3/$0,4 e ha raggiunto un picco verso fine 2021 di $4800, come si vede nel grafico 2.2. Ethereum, come Bitcoin, dopo il crash dovuto dal COVID-19 si trova fortemente correlato al mercato tradizionale.

Grafico 2.2. Ethereum e il suo andamento del prezzo in scala logaritmica, timeframe mensile

Fonte: schermata acquisita da Tradingview.com

CAPITOLO III:

APPLICAZIONI DELLA TECNOLOGIA BLOCKCHAIN E SMART CONTRACT

In questo capitolo affronteremo gli sviluppi della tecnologia blockchain e degli smart contract non solo nella finanza decentralizzata, ma anche nel settore bancario e assicurativo.

3.1 La finanza decentralizzata: la DeFi

La finanza decentralizzata è stata definita dal giornale Forbes[119] un movimento che consente di ricreare la finanza tradizionale, con tutti gli strumenti annessi, nel mondo decentralizzato della blockchain e delle criptovalute. La finanza decentralizzata nasce per dare la possibilità di usufruire di servizi finanziari, normalmente erogati da banche o istituti finanziari, senza la presenza di un intermediario. Le Dapp permettono la realizzazione di una struttura decentralizzata fondata su una moltitudine di smart contract, i quali potremmo definirli come l'unità fondamentale della DeFi. La possibilità di avere l'automazione nell'erogazione di servizi, la programmazione di sviluppi futuri rendono possibile il concetto di "moneta programmabile". La DeFi nasce su Ethereum e sbarca su altre blockchain date le difficoltà create dal costo delle gas fee per la clientela retail, uno con un capitale ridotto si troverebbe mangiato il wallet dalle commissioni[120].

3.1.1 DeFi vs finanza tradizionale

La principale differenza, decantata dal mondo blockchain, certamente riguarda l'assenza di intermediari nel mondo della DeFi. Nella finanza tradizionale essi aiutano a far incontrare gli interessi tra la domanda e l'offerta dei vari attori che vi partecipano, questo comporta dei costi. Nelle transazioni che si compiono attraverso istituzioni finanziarie gli intermediari rendono possibile l'incontro tra le parti al fine di creare anche un rapporto di fiducia nella negoziazione degli accordi. L'operare sfruttando la presenza di grandi

[119] Curry, B., Napoletano, E. (2022), *What Is DeFi? Understanding Decentralized Finance,* disponibile a https://www.forbes.com/advisor/investing/cryptocurrency/defi-decentralized-finance/

[120] Coinbase.com, *Cos'è la finanza decentralizzata (DeFi)?,* disponibile a https://www.coinbase.com/it/learn/crypto-basics/what-is-defi

istituzioni comporta l'accentuarsi di costi di transazioni o altro. Infatti, in una struttura centralizzata, come il settore bancario, i costi sono dovuti dalla presenza di intermediari in qualsiasi operazione che potremmo voler svolgere. Prendiamo come esempio l'invio di un bonifico estero verso gli USA utilizzando il sistema SWIFT:

- Nel caso la banca del mittente abbia un conto presso la banca del destinatario è solo sufficiente inviare una comunicazione per spostare i fondi dal conto della prima a quello del destinatario.
- Nel caso la banca del mittente non disponga di un conto presso la banca del destinatario è necessario interpellare un ulteriore intermediario che svolgerà la stessa operazione spiegata al punto precedente.

Resta presente il rischio sistemico, possibile tra le banche nel caso di pagamenti di grandi somme di denaro[121]. Le banche operano con diversi sistemi di pagamento che necessitano di grandi posizioni di credito. Conosciamo il regolamento netto periodico (RNP) e il regolamento lungo continuo (RLC):

Il RNP consiste nella regolazione dei pagamenti periodica. Supponendo di avere un credito verso A e un debito verso C, regolo il pagamento con quest'ultimo solo dopo aver ricevuto i soldi da A. Nel caso del RLC invece è presente una clearing house che si occupa della compensazione, più il tempo tra clearing e settlement è basso più il rischio di credito si abbassa. RLC è un sistema che comporta meno disponibilità di liquidità, ma necessita di poco tempo di scarto tra clearing e settlement. Il sistema RNP è più esposto al rischio sistemico perché se dovessero verificarsi delle insolvenze su una banca potrebbe esserci una reazione a catena. Invece, il Regolamento Lungo Continuo permette di scoprire subito la nascita di insolvenze e limita notevolmente il rischio sistemico, a fronte dello svantaggio di dover trattenere maggior liquidità per operare. Solitamente, le banche commerciali hanno accesso al credito disponibile presso le banche centrali e questo

[121] Masciantonio, S., Zaghini, A. (2017), *N. 1153 - Un'analisi delle misure di rischio sistemico e di importanza sistemica durante la crisi finanziaria globale*, disponibile a https://www.bancaditalia.it/pubblicazioni/temi-discussione/2017/2017-1153/index.html?com.dotmarketing.htmlpage.language=102&dotcache=refresh

potrebbe comportare il moral hazard, dove le prime tendono a sovraesporsi consapevoli dell'aiuto della banca centrale.

La crisi finanziaria del 2007-2008 ha messo in evidenza tutti i problemi del sistema bancario dell'epoca, si sono manifestate tutte le cose che potevano creare un effetto sistemico. L'aumento delle posizioni debitorie aveva un effetto di leva enorme e non ha portato alla luce il problema che si stava creando e il rischio che si stava correndo. Il 2007 è stato un momento topico che ha portato la sfiducia nel sistema finanziario e la fiducia è essenziale per poter operare in un mercato. Il default di Lehman Brothers provocò un crollo generale della fiducia e il rischio di insolvenza portò a una crisi di liquidità. La regolamentazione nel sistema finanziario era necessaria, le banche hanno iniziato a specializzarsi nel risk management. Tuttavia, col progredire delle tecnologie è sempre più facile eludere le regole; quindi, la regolamentazione è sempre alla rincorsa[122].

Questo è il contesto che ha portato alla nascita della blockchain, delle criptovalute e ha creato i presupposti per la nascita della DeFi.

La DeFi è un sistema aperto a chiunque abbia le capacità di sviluppare applicazioni o di interagire con i prodotti disponibili su esso, a differenza della finanza tradizionale che non permette l'accesso al sistema dal momento che non è possibile conoscere il codice sorgente. Un'architettura aperta è più attrattiva, di fatto attira più persone al proprio interno favorendo il progresso del sistema. La finanza tradizionale è meno efficiente a causa della presenza di vari intermediari per qualsiasi operazione da svolgere, abbiamo visto il caso del bonifico estero in precedenza. Un discorso analogo è applicabile ai pagamenti con le carte: è necessaria la comunicazione tra le banche, le quali sono intermediate da Visa. La DeFi, attraverso gli smart contract, tende verso l'ottimizzazione del processo, aumentando le velocità e riducendo i costi. La finanza decentralizzata è governata dagli utenti, vedi il sistema delle DAO che porta a una maggiore velocità e un'apertura all'aggiornamento. Nei paesi in via di sviluppo la DeFi ha avuto una grande espansione a causa della sfiducia nei governi e nei sistemi centralizzati; inoltre, le spese per l'apertura e la gestione di un conto bancario erano insostenibili[123].

[122] De Candia, A. (2021), *Le origini della DeFi*, disponibile a https://cryptonomist.ch/2021/01/01/origini-defi/
[123] Garavaglia, R. (2021), *Conoscere la blockchain,* Hoepli, Milano

3.1.2 Come opera il consenso

Il dubbio sul fatto se riporre la fiducia su un settore così innovativo e giovane non è facilmente eliminabile dalla mente di chi si interessa alla DeFi. Nei capitoli precedenti abbiamo trattato il problema del double-spending, cosa che nella finanza tradizionale viene sconfitto dalle autorità garanti che vigilano sull'osservanza delle regole nelle transazioni. Abbiamo visto come la blockchain possa debellare lo stesso problema grazie ai propri fondamentali: l'irreversibilità e l'utilizzo dei timestamp. I protocolli di consenso coinvolgono gli utenti a partecipare all'aumento della sicurezza, mettendo a disposizione la potenza computazionale nel caso della Proof-of-Work o la propria quantità di valuta nel caso della Proof-Of-Stake[124].

3.1.3 Gli smart contract nella DeFi e i rischi

Per comprendere l'importanza dei contratti intelligenti nella DeFi è utile citare Nick Szabo, quando in uno dei suoi trattati marca il concetto di automatizzazione e incorporazione delle clausole contrattuali attraverso apparecchi digitali, in modo tale da non renderne possibile la violazione[125]. La blockchain rende possibile la visualizzazione dei codici di uno smart contract e permette la disamina del funzionamento ancor prima di doversi fidare e utilizzarlo, azione non possibile sulle applicazioni web che utilizziamo tutti i giorni. Le funzionalità degli smart contract sono varie e le istruzioni che possono ricevere sono limitate solo dalla capacità di riuscire a tradurre il codice in un linguaggio leggibile dalla macchina[126].

3.1.4 Obiettivi e rischi della DeFi

La DeFi vuole offrire tutti i servizi che normalmente ci vengono offerti dalle istituzioni finanziarie, dalla banca all'assicurazione. Ciò che si è prefissato il settore della finanza decentralizzata è la creazione di un luogo dove è possibile usufruire di tutti i servizi che

[124] Condemi, J. (2020), *DeFi: cos'è la finanza decentralizzata e come sta cambiando il mercato delle criptovalute,* disponibile a https://www.blockchain4innovation.it/mercati/defi-cose-la-finanza-decentralizzata-e-come-sta-cambiando-il-mercato-delle-criptovalute/
[125] Szabo, N. (1997), *Formalizing and Securing Relationships on Public Networks,* disponibile a http://myinstantid.com/szabo.pdf
[126] Comandini, G.L. (2020), *Da zero alla luna,* Dario Flaccovio Editore, Palermo

vengono offerti dalle banche, le assicurazioni o gli altri intermediari[127]. Il settore non presenta barriere all'ingresso, è necessario di disporre di un wallet, e fornisce una vasta gamma di prodotti che vengono gestiti con automazione dalla blockchain e dà la possibilità di personalizzazione. La DeFi attrae soprattutto gli abitanti dei paesi con un'economia emergente o chi è desideroso di otttenere dei rendimenti migliori rispetto al sistema tradizionale.

Per quanto concerne i rischi degli smart contract, abbiamo citato nel capitolo precedente come sia possibile la presenza di vulnerabilità, bug o exploit, nella scrittura dei codici e che ci sono hacker che "lavorano" alla ricerca di questi errori al fine di trarne vantaggio. Durante il boom della DeFI degli ultimi anni spesso ci si poteva imbattere in smart contract programmati da attori malevoli che, vista la mancanza di dimestichezza dei novellini del settore, nel caso accettati riuscivano a svuotare il wallet di tutti i token. Si sono verificati anche casi dove, durante il periodo delle ICO in particolare[128], venivano creati token con alla base dei contratti carenti di funzioni fondamentali come la possibilità di renderli non vendibili (Honey pot). Rischio rugpull, ovvero la rimozione della liquidità di un token da parte del team di sviluppo, spesso si verifica con la vendita di grandi quantità di token allo scopo di ottenere grandi profitti[129]. Un rischio da non sottovalutare è quello di "Liquidity crunch", ovvero troppa poca liquidità in un protocollo, che comporta l'abbandono graduale della piattaforma.

3.1.5 La struttura della DeFi

Da un lato abbiamo quindi la tecnologia blockchain, che permette la creazione di una struttura efficiente e trasparente; dall'altro troviamo i contratti intelligenti, che permettono la creazione di prodotti appetibili ai consumatori. La DeFi ha un'architettura a più livelli, ognuno ha uno scopo differente ed è di fondamentale importanza per il layer superiore. I livelli della struttura sono basati su:

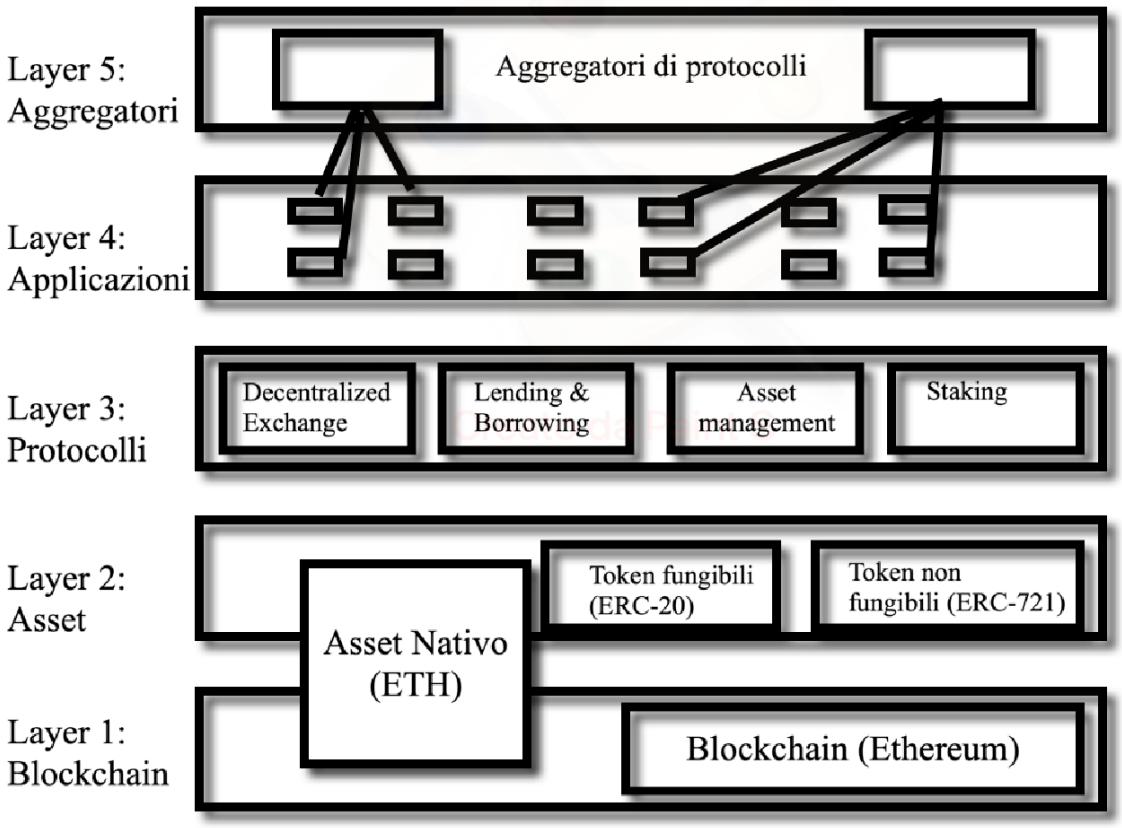
[127] Sorgentone, P. (2020), *Il Futuro del Valore: Blockchain, Cryptoasset e Finanza Decentralizzata,* pubblicazione indipendente da editori
[128] Comandini, G.L. (2020), *Da zero alla luna,* Dario Flaccovio Editore, Palermo
[129] Binance Academy, *Rug pull,* disponibile a https://academy.binance.com/en/glossary/rug-pull

- Layer 1: la blockchain di riferimento, come Ethereum, e sul relativo token nativo, come ETH[130];
- Layer 2: qui troviamo tutti i token della blockchain, comprendendo quello nativo, fungibili e non fungibili;
- Layer 3: in questo livello si trovano gli standard per la costruzione di applicazioni come exchange, piattaforme di lending & borrowing, asset management, piattaforme che permettono lo staking.
- Layer 4: su questo livello si trovano costruite le applicazioni decentralizzate che si collegano direttamente ai protocolli, si presentano all'utente con un'interfaccia tendenzialmente user-friendly;
- Layer 5: questo è un livello superiore e più complesso, ha lo scopo di unire vari protocolli aiutando ancor di più l'utente.

Il livello 1 è quello che dà la direzione a tutta la struttura e se fosse compromesso in un parametro, come la sicurezza, pregiudicherebbe anche i livelli sovrastanti. La figura 3.1 ci aiuta a comprendere meglio l'importanza di una base solida, intesa come blockchain, per costruire un ecosistema stabile e duraturo. Nella figura sono stati riportati tra parentesi degli esempi nel mondo Ethereum.

[130] Basile, A. (2019), *Blockchain: la nuova rivoluzione industriale,* Dario Flaccovio Editore, Palermo

Figura 3.1. Rappresentazione della struttura a livelli della DeFi.



Fonte: ispirato da Schär, F. (2020), *Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets,* disponibile a https://www.researchgate.net/publication/340061422_Decentralized_Finance_On_Blockchain-_and_Smart_Contract-based_Financial_Markets

3.1.6 Che servizi offre la DeFi?

I protocolli sono per costruzione interoperabili, non raramente accade che vengano integrati tra loro per creare servizi progressivamente più innovativi. I servizi di base, come vediamo nella Figura 3.1 sono il lending & borrowing, la possibilità di scambiare i token nei DEX, la gestione di capitali oppure il deposito e lo staking.

3.1.6.1 Lending & borrowing

Una piattaforma di lending & borrowing, permette la possibilità di accedere a prestiti o di concedere la propria liquidità al fine di ricevere un interesse sul deposito. La finanza

tradizionale offre lo stesso servizio, la differenza consta nella presenza della burocrazia e nei tassi di interesse[131]. Nella DeFi si possono aprire prestiti senza il controllo di un intermediario, non è necessario creare rapporti di fiducia con chi deve erogarmi la liquidità. Queste piattaforme cercano di far incontrare gli interessi di tutti gli utenti, solo così si può costruire un'applicazione che dura nel tempo. Grazie alla trasparenza della blockchain e alla chiarezza degli smart contract è possibile accedere a prestiti in tempi brevi e senza dover creare rapporti di fiducia con un intermediario, non vi è possibilità di censura. Per poter accedere ad un prestito bancario tradizionale vengono chieste delle garanzie su dei beni in nostro possesso; nel mondo blockchain avviene lo stesso, con la differenza che intestatario del prestito figura solo il nome che ho attribuito al mio account e le garanzie sono composte da altri token. Esistono due strategie di prestitiutilizzate dai protocolli:

1. Il prestito collateralizzato, che è completamente coperto da garanzie di valore pari o superiore, queste sono sotto forma di token che vanno bloccati in uno smart contract e non ritornano al proprietario fino alla totale restituzione del debito.
2. I Flash Loan, che sono operazioni complesse effettuate solo da operatori esperti e permettono di ricevere grandi somme di denaro senza alcun deposito di garanzie. Nel corso della stessa transazione viene erogato il credito, senza il deposito di collaterale, e ripagato. Questo tipo di prestiti viene utilizzato per sfruttare opportunità di arbitraggio presenti negli exchange decentralizzati, dovute a discrepanze di prezzo[132]. I prestiti "flash" sono ancora nelle prime fasi di sviluppo e sono utilizzati da degli attori malevoli che vogliono sfruttarne le debolezze presenti[133].

A loro volta, i prestiti collateralizzati hanno più modalità di realizzazione. Il primo metodo, il più semplice, è l'accordo peer-to-peer dove le parti si accordano privatamente e creano uno smart contract ad hoc in base alle esigenze.

Il secondo metodo consiste nell'utilizzo di "pool", ovvero l'aggregazione della liquidità di tutti i prestatori. I tassi di interesse pagati da coloro che richiedono il prestito sono

[131] Crowell, B. (2020), *I prestiti crypto spiegati semplicemente*, disponibile a https://it.cointelegraph.com/explained/crypto-lending-simply-explained
[132] Aave.com, *Flash Loans,* disponibile a https://docs.aave.com/faq/flash-loans
[133] Deer, M. (2022), *What are flash loans in DeFi?,* disponibile a https://cointelegraph.com/explained/what-are-flash-loans-in-defi

variabili in base alla domanda e all'offerta disponibile: se l'erogazione del credito è molto richiesta, i tassi pagati salgono; quando la richiesta è bassa, i tassi scendono. L'utilizzo di pool di liquidità rende il mercato del debito più liquido e flessibile. Queste piattaforme di prestiti hanno un sistema di gestione dei debiti degli utenti basandosi sul loan-to-value (LTV), la soglia varia tra i vari protocolli. Nel caso di raggiungimento della soglia scatta la liquidazione, questo comporta la vendita forzata del collaterale del prestito e la piattaforma riesce a evitare di subire perdite. Di solito il LTV si aggira intorno al 50-65%, il valore potrebbe sembrare relativamente basso, ma è una scelta obbligata vista la volatilità del mercato delle criptovalute. Un protocollo tra i più utilizzati su Ethereum che utilizza questo sistema è Aave. Nasce come piattaforma di lending & borrowing con l'obiettivo di una creazione di un vero e proprio mercato di prestiti decentralizzato dove poterne trarre un guadagno. Nella Figura 3.2 vediamo a sinistra il nostro deposito e a destra il nostro debito. La schermata offre un servizio con dei parametri spiegati come "borrowing power" che rappresenta quanto ho preso in prestito rispetto alla disponibilità totale che avevo e l'health factor che è una valutazione sulla sicurezza del mio debito. L'interfaccia offre anche un dato che è l'Annual Percentage Yield (APY), ovvero il tasso d'interesse composto sui depositi e sui prestiti, questi due differiscono di un valore necessario al pagamento di commissioni e spese varie della piattaforma. Nel mondo della DeFi si può essere incentivati a chiedere prestiti, quest'operazione si chiama "liquidity mining", e si verifica quando una piattaforma vuole attirare liquidità al proprio interno, offrendo una ricompensa al borrower[134]. Questo fenomeno avviene anche nel nostro caso nella Figura 3.2 e si può vedere sotto all'APY; infatti, il token che abbiamo depositato come collaterale ci verrà riconsegnato, nel momento in cui estingueremo il debito, con degli interessi calcolati con un tasso d'interesse annuale, l'Annual Percentage Rate (APR).

[134] Binance Academy, *Cosa sono i pool di liquidità nella DeFi e come funzionano?,* disponibile a https://academy.binance.com/it/articles/what-are-liquidity-pools-in-defi

Figura 3.2. Dashboard di Aave dopo aver depositato del collaterale sotto forma di Matic (un token ERC-20) per ricevere 1 USDC.

Fonte: schermata acquisita da https://app.aave.com/

La terza tipologia di prestiti collateralizzati viene definita “minting di stablecoin” ed è l’operazione con cui depositando del collaterale ricevo una valuta stabile creata dalla piattaforma. Il protocollo più conosciuto che offre questo servizio si chiama MakerDAO, il nome suggerisce il tipo di governance decentralizzata. La piattaforma è sviluppata sul token Maker, il quale regola l’emissione della stablecoin crypto-collateralized DAI. L’utente intenzionato a ricevere un prestito deposita i propri token a garanzia della posizione con un rapporto di almeno il 150%: quindi se fossi intenzionato a ricevere $100 di DAI dovrei bloccare almeno $150 di ETH, o qualsiasi altra criptovaluta, e se il collaterale dovesse scendere sotto il 150% scatterebbe la liquidazione della mia posizione. La strategia attuata da MakerDAO con la creazione di una stablecoin completamente decentralizzata, perché non necessita di riserve nel mondo reale, rappresenta la massima espressione di DeFi. Questa tipologia di prestiti, solitamente, viene svolta per ottenere della liquidità un token che possiedo senza venderlo, quindi beneficiando di un eventuale aumento del prezzo. La liquidità ottenuta posso usarla per effettuare margin trading o attuare numerose strategie che la finanza decentralizzata permette.

3.1.6.2 I Decentralized Exchange: DEX

I DEX sono la piattaforma per lo scambio di token decentralizzata e operarci non comporta l’affidamento delle nostre chiavi private ad un exchange centralizzato. L’utente medio utilizza i Centralized Exchange (CEX), che non presentano alcun difetto strutturale e sono molto user friendly. I DEX nascono per essere completamente decentralizzati, per garantire maggiore sicurezza e lo pseudonimato sulle operazioni. La principale differenza

tra DEX e CEX è data dal fatto che nei CEX noi concediamo le nostre chiavi private alla piattaforma; nei DEX invece, sono al sicuro all'interno dei nostri wallet[135]. I DEX possono essere divisi in due categorie:

- Decentralized order book exchange: sono luoghi di scambio dove è possibile vendere o comprare token al prezzo desiderato e l'order book può essere on-chain o off-chain. Nel primo tipo di order book è presente uno smart contract che gestisce la creazione di limit order, o la cancellazione di essi, attraverso il pagamento di gas fee. Nel secondo tipo, il più utilizzato, si utilizzano delle terze parti centralizzate che si occupano del fornire liste ordinate con gli ordini segnati. I market maker piazzano i limit order, questi vengono aggregati in un order book dalle terze parti e successivamente, quando un utente trova un ordine che soddisfa le proprie richieste, viene effettuato lo scambio.
- Automatic Market Maker: il loro funzionamento è basato sulla costruzione di liquidity pool, dove si trovano coppie di asset. Questi pool sono riempiti da utenti che mettono a disposizione i propri token, ricevendo in cambio un pagamento di commissioni generate dagli scambi. Quando io decido di operare su questo tipo di exchange e invio la richiesta di swap, uno smart contract richiede all'oracolo la quotazione degli asset e un altro si occupa di ritirare il token dal pool di liquidità per inviarlo al mio wallet.

Con il tempo gli exchange decentralizzati hanno iniziato ad offrire sempre più servizi. Si può operare:

- trading a margine, c'è la possibilità di utilizzare una leva finanziaria;
- trading di derivati, utilizzando futures a scadenza oppure opzioni;
- trading di asset sintetici, ovvero comprare o vendere token che mimano il prezzo di commodities, stocks o indizi azionari.

[135] Cointelegraph.com, *What are decentralized exchanges, and how do DEXs work?,* disponibile a https://cointelegraph.com/defi-101/what-are-decentralized-exchanges-and-how-do-dexs-work

Le prime due tipologie di operazioni sono offerte da DEX che combinano le funzionalità di piattaforme di lending & borrowing e la terza viene realizzata attraverso l'utilizzo di oracoli.

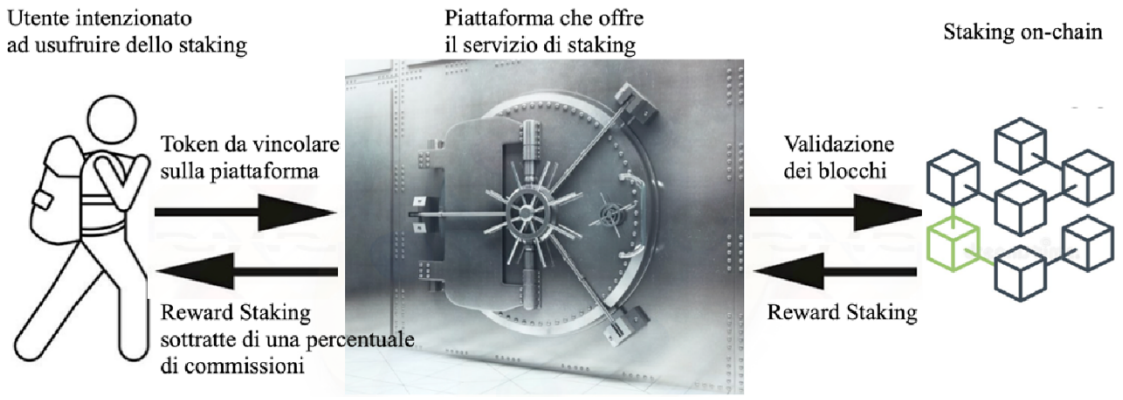
I punti deboli dei DEX sono la velocità e il rischio di una crisi di liquidità che creerebbe lo slippage[136], che è il fenomeno in cui lo scambio non si verifica al prezzo indicato ad inizio transazione.

3.1.6.3 Staking

Lo staking è supportato solo sulle blockchain che utilizzano l'algoritmo di consenso Proof-Of-Stake. Gli utenti che hanno a disposizione una determinata quantità di token possono depositarli e vincolarli per un periodo minimo di tempo per ottenere degli interessi[137]. Il servizio di staking ha più vantaggi: contribuisce a migliorare la sicurezza della blockchain, si ha il diritto di validare i blocchi e, non sempre, conferisce il diritto di voto. Su alcune blockchain è possibile praticare il "liquid staking", che consiste nel classico deposito vincolato dei token, con la differenza che mi viene restituito un derivato del mio token. La possibilità di mantenere liquidità per fare altre operazioni aiuta il network a crescere e dei volumi più alti sono più attraenti per nuovi utenti. Questa soluzione è stata accolta come un'innovazione decisiva per il mondo DeFi perché porta con sé numerosi vantaggi, sia per l'utente sia per i validatori e il network. Dal punto di vista di possessore del token posso avere una migliore gestione del capitale, piuttosto che tenerlo fermo sul wallet lo utilizzo per partecipare al consenso del network e con il derivato opero su altri protocolli. I validatori guadagnano dal liquid staking perché, dato che favorisce gli utenti a farlo, e avendo stake più grandi possono validare i blocchi con più facilità; invece, il network diventa più utilizzato e liquido[138].

[136] Garavaglia, R. (2021), *Conoscere la blockchain,* Hoepli, Milano
[137] Da Kraken.com, *Panoramica dello staking on chain su Kraken,* disponibile a https://support.kraken.com/hc/it/articles/360037682011-Panoramica-dello-staking-On-chain-su-Kraken
[138] Campaci, E. (2021), *Come funziona il liquid staking,* disponibile a https://youngplatform.com/blog/news/come-funziona-liquid-staking/

Figura 3.3. Illustrazione del sistema generale di staking offerto dalla DeFi.



Fonte: ispirato da Becker, S. (2022), *Guide to Crypto Staking: What It Is, How It Works, and How to Get Started,* disponibile a https://www.sofi.com/learn/content/crypto-staking/

3.1.6.4 Gestione del capitale

La DeFi, soprattutto nel periodo di grande espansione tra il 2020-21, si è popolata di persone alla ricerca di rendimenti elevati. L'operazione di ricerca del rendimenti migliori potrebbe rivelarsi complessa e, soprattutto, rischiosa. Questi furono i presupposti che portarono alla nascita dei primi protocolli di asset management, dove si è distinto Yearn.Finance. Il funzionamento di questo era basato sull'aggregazione di più piattaforme di lending & borrowing per riuscire ad ottenere profitti maggiori individuando le opportunità migliori presenti nel mondo della finanza decentralizzata. Il protocollo offre più prodotti distinti che differiscono in base alla possibilità di supportare token o stablecoin. Al momento del deposito in uno dei tre prodotti d'investimento viene restituito un token denominato con un prefisso "y" che rappresenta una quota del pool. Al momento del prelievo verrà restituito il token per dimostrare di possedere quella partecipazione al pool[139].

3.1.6.5 Un nuovo settore della DeFi: le assicurazioni

Supponiamo di essere molto esposti nella finanza decentralizata e di utilizzare delle piattaforme "esotiche" per cercare dei rendimenti alti. È possibile comprare delle

[139] Yearn.finance, *Overview,* disponibile a https://docs.yearn.finance/getting-started/products/yvaults/overview

coperture pagando un premio per ottenere un abbassamento del rischio contro uno dei vari rischi possibili, come il rischio di hack o di bug di smart contract e il rischio di perdita di valore della stablecoin rispetto al bene a cui son legate. Nel caso avvenga una delle cose comprese nel contratto per cui sono coperto si richiede il rimborso dimostrando di aver subito la perdita attraverso la presentazione del proprio address e lì avviene il controllo delle transazioni sulla blockchain, grazie alla trasparenza[140]. Nel caso avvenisse un errore nella valutazione del nostro rimborso è possibile ricorrere in appello, lì subentra un team dedicato con un supporto legale per rivedere la decisione. Esistono delle assicurazioni dette algoritmiche, che funzionano tramite utilizzo di oracoli, e sono più complesse da applicare. Nel caso si verifichi la condizione per cui gli assicurati devono ricevere il rimborso, l'operazione viene svolta automaticamente, non è necessario fare la richiesta all'assicurazione, e più velocemente rispetto alle piattaforme[141].

Si può anche svolgere il ruolo dell'assicuratore, ovvero fornire il proprio capitale nel protocollo che svolge la copertura degli assicurati, ricevendo una parte del pagamento dei premi. L'operazione può rivelarsi profittevole se non si verificasse l'evento negativo per cui si trova il rimborso dei danneggiati. Utilizzare le piattaforme di assicurazione comporta sempre il rischio di hack degli smart contract.

3.1.7 Da dove arrivano i rendimenti offerti dai protocolli DeFi?

Prendendo l'esempio di Aave, se ho della liquidità ferma, posso depositarla perché sia data a chi ne ha bisogno. Il borrower chiede un prestito perché potrebbe volere operare strategie profittevoli su altri protocolli, vuole ottenere liquidità da un asset illiquido pagando un piccolo tasso di interesse o fare margin trading. Dunque, si incontrano gli interessi dei due attori. Come vediamo nella Figura 3.4 il lender riceve una quota di interesse che è una parte di quella che paga il borrower, la piattaforma riceve un compenso, ed è un rendimento sicuramente più alto di un conto di deposito bancario. Un

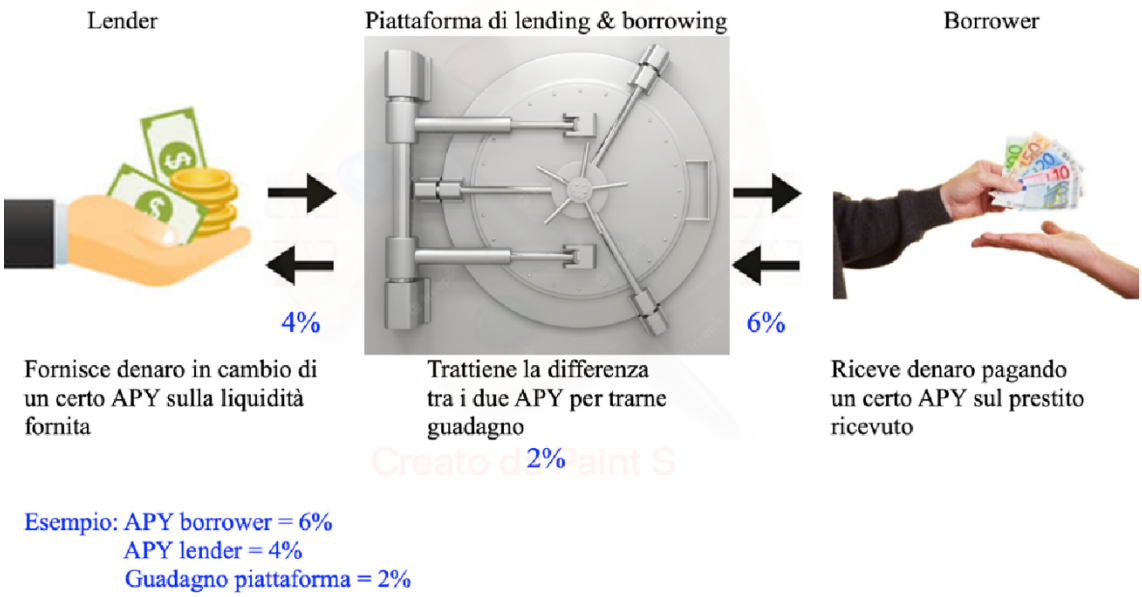
---

[140] Basile, A. (2019), *Blockchain: la nuova rivoluzione industriale,* Dario Flaccovio Editore, Palermo

[141] Sorgentone, P. (2020), *Il Futuro del Valore: Blockchain, Cryptoasset e Finanza Decentralizzata,* pubblicazione indipendente da editori

rendimento più alto è commisurato anche al rischio della DeFi. La differenza tra interessi pagati e ricevuti è usata per mantenere la piattaforma, il team che ci lavora e incentivare il liquidity mining. La piattaforma dona della liquidità agli utenti che la utilizzano: posso ricevere soldi per usare la Dapp, essa ottiene profitti dalle commissioni pagate e la liquidità nel protocollo aumenta. Questo meccanismo è una sorta di loop a feedback positivo, che favorisce tutti i partecipanti del sistema. Nei periodi di nascita delle piattaforme avvengono i liquidity mining, spesso si viene pagati per effettuare dei prestiti, questo perché più aumenta il valore bloccato più gli utenti sono attirati ad usare la piattaforma.

Figura 3.4. Illustrazione del modello di funzionamento di una piattaforma di lending & borrowing

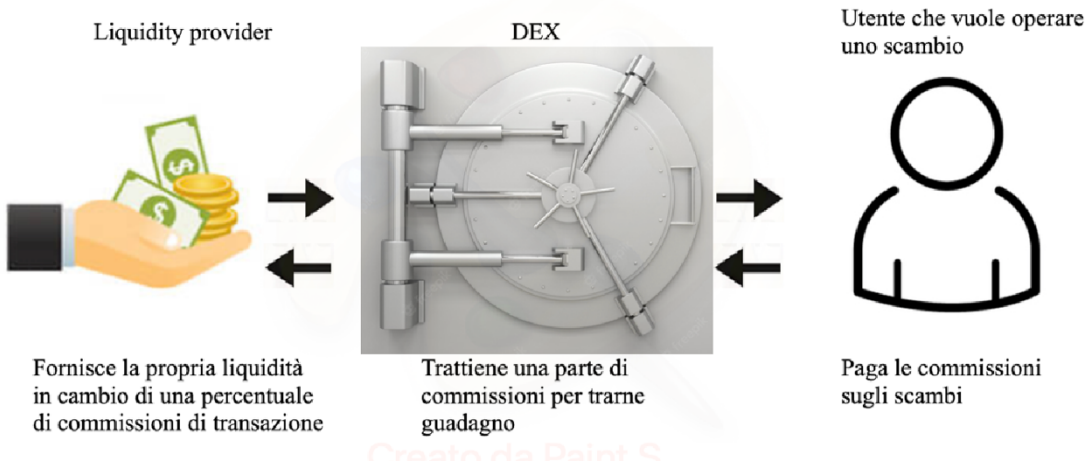


Fonte: Yield.app, *Defi lending & borrowing guide,* disponibile a https://blog.yield.app/post/defi-lending-and-borrowing-guide

Prendendo l'esempio di un qualsiasi Automatic Market Maker DEX, posso fornire liquidità ai pool di token. Nel caso un utente voglia scambiare i propri Ether per una stablecoin è necessario che qualcuno abbia dato liquidità ad un pool con i token corrispondenti. Le commissioni dei DEX sono generalmente basse ed una parte di queste viene offerta al liquidity provider, come vediamo nella Figura 3.5. Il vantaggio

dell'utilizzo di queste piattaforme è la possibilità di ottenere un guadagno a tutti gli attori, se non fosse così la finanza decentralizzate perderebbe il motivo di esistere.

Figura 3.5. Illustrazione del funzionamento dei DEX



Fonte: liberamente ispirato da BeInCrypto.com, *How liquidity provider tokens works*, disponibile a https://beincrypto.com/learn/lp-tokens/

3.2 Interazione tra la finanza tradizionale e la blockchain

La blockchain non è solo criptovalute, da anni si stanno sviluppando applicazioni della tecnologia per il settore bancario e assicurativo.

3.2.1 Il settore bancario

La blockchain ha introdotto la possibilità di effettuare gli scambi evitando l'intermediazione di qualsiasi istituzione. Questo fenomeno ha indotto grandi banche mondiali, alcune banche centrali incluse, a studiare una soluzione per lo sfruttamento della tecnologia sia nella creazione di criptovalute che in altri campi di applicazione[142]. Le caratteristiche della blockchain sono state viste sia come possibili antagoniste sia come possibilità di sviluppo futuro per l'abbattimento di costi, la sicurezza e l'aumento della velocità. Accenture High Performance Investment Bank ha svolto un'analisi dei costi nel

[142] Chiap, G. (2019), *Blockchain: tecnologie e applicazioni per il business,* Hoepli Editore, Milano

caso di utilizzo della tecnologia blockchain. Secondo il report, si può risparmiare circa il 70% sulla rendicontazione bancaria, creando un sistema di identità digitali e dei profili dei clienti on-chain si ridurrebbe il costo di gestione della clientela del 50%. A livello di clearing e settlement, si risparmierebbe pure li potenzialmente il 50%. Per quanto riguarda la trasparenza e la verificabilità, il risparmio stimato è del 30%. In totale insieme si puo ridurre i costi di circa il 30%[143].

3.2.1.1 Corda

Corda è una piattaforma che sfrutta i benefici della tecnologia blockchain senza l'utilizzo del sistema a blocchi[144] ed è sviluppata dall'azienda R3, con il fine della riduzione dei costi vari delle banche e delle aziende[145]. Il sistema è già stato adottato da più di 200 banche nel mondo al fine di essere in linea con i criteri del settore e con leggi imposte dagli enti regolatori. Inoltre, permette alle banche e alle aziende di operare privatamente tra controparti legalmente identificate su un'unica rete con applicazioni da sviluppatori indipendenti. Corda, a differenza della blockchain di Bitcoin e delle altre criptovalute, non necessita del timestamp e potrebbe essere definita come un sistema liberamente ispirato dalla creazione di Satoshi Nakamoto. Corda è stato sviluppato per:

- essere scalabile perché deve supportare numerose transazioni al giorno dovute alla grande quantitià di aziende che utilizzano il network;
- rendere le varie applicazioni utilizzabili anche con versioni diverse;
- interoperabile per permettere la coesistenza di più applicazioni e possibilmente integrarle tra loro.

Il network definisce numerosi parametri per il meccanismo di consenso su cui nodi sono accordati per mantenerne la stabilità. In Corda non è necessario un algoritmo di consenso perché non esistono blocchi da validare né costi di transazione con cui retribuire un eventuale miner. Le transazioni utilizzano lo stesso sistema di Bitcoin, gli UTXO, e avvengono in seguito a una proposta inviata dal mittente, verso un destinatario, che la

[143] Accenture.com, disponibile a https://www.accenture.com/us-en/insights/blockchain/banking-on-blockchain
[144] Basile, A. (2019), *Blockchain: la nuova rivoluzione industriale,* Dario Flaccovio Editore, Palermo
[145] Comandini, G.L. (2020), *Da zero alla luna,* Dario Flaccovio Editore, Palermo

firma. Svolti questi passaggi, delle figure note come "notai" svolgono il ruolo di validazione e finalizzazione dello scambio, che avviene istantaneamente.

3.2.1.2 Hyperledger Fabric

Hyperledger costituisce le fondamenta di progetti basati sulla tecnologia blockchain di tipo permissioned. Il primo progetto è stato chiamato Fabric e risulta essere il più flessibile perché consente la creazione di applicazioni adatte a vari settori. L'architettura di Hyperledger è a livelli, ognuno dei quali permette l'elaborazione di operazioni diverse: interconnessione tra nodi, utilizzo di smart contract, comunicazione tra i nodi, archiviazione dei dati e mantenimento della sicurezza[146]. Per entrare nel network è necessario ottenere lo status di membro, per cui è necessaria l'identificazione, erogata da un ente controllore. La tecnologia di Hyperledger mira ad essere utilizzata nel settore finanziario per l'interoperabilità, la velocità e la sicurezza.

3.2.1.3 Quorum

Quorum è una blockchain permissioned sviluppata da JP Morgan, derivata da Ethereum per poterne sfruttare le caratteristiche principali. In aggiunta, essendo privata, aumenta notevolmente la scalabilità del network e introduce un alto livello di privacy. Quorum favorisce la creazione di reti private di ogni azienda interessata, sfruttando la popolarità della blockchain su cui è fondata. Il linguaggio di programmazione di Ethereum è ampiamente conosciuto in rete ed è quindi appetibile a nuovi utenti per lo sviluppo di applicazioni. JP Morgan ha sviluppato questa piattaforma al fine di agevolare il proprio business come banca, aumentandone l'efficienza e la sicurezza.

3.2.2 Settore assicurativo

La tecnologia blockchain si pone come possibile sviluppo anche per il settore assicurativo. L'utilizzo di un network decentralizzato e l'utilizzo della crittografia potrebbe mettere fine a vari problemi che affliggono le compagnie portando a:

- maggiore efficienza nella gestione delle identità dei clienti e dei relativi dati;

[146] Chiap, G. (2019), *Blockchain: tecnologie e applicazioni per il business,* Hoepli Editore, Milano

- un abbassamento dei costi e automazione dei processi;
- un possibile utilizzo degli smart contract per la gestione dei reclami.

3.2.2.1 B3i

Alcune multinazionali, come Allianz, Zurich, Swiss Re e altre, hanno costituito la Blockchain Insurance Industry Initiative[147] (B3i) che mira allo studio e allo sviluppo del settore assicurativo su blockchain con l'utilizzo di smart contract in direzione dei tre obiettivi citati qui sopra. B3i Fluidity è la soluzione trovata ed è un network permissioned costruito per offrire ai partner un luogo più sicuro per operare le transazioni e facilitare i rapporti tra le compagnie di assicurazione, cercando di eliminare il problema del costo di gestione dell'enorme mole di dati. Lo scambio di informazioni e le transazioni vengono validati attraverso un sistema di nodi identificati dalla rete. L'obiettivo che si ricerca con questa piattaforma è il raggiungimento di un'efficienza tale che le persone autorizzate possano accedere ai contenuti necessari nel minor tempo possibile. L'automazione dei processi garantita dall'utilizzo di smart contract aiuta il mercato delle assicurazioni a raggiungere un livello di sicurezza maggiore rispetto alla presenza del rischio dell'errore umano.

3.2.2.2 Poleecy

Poleecy è una startup italiana di insurtech che si occupa di offrire ai clienti servizi di assicurazione temporanea basati sull'utilizzo di blockchain di tecnologia Hyperledger e di smart contract. L'obiettivo è dare la possibilità ai clienti in qualsiasi momento di sottoscrivere una polizza alle migliori condizioni possibili. L'azienda mira a proporre polizze ad hoc per ogni situazione in cui può incorrere un possibile cliente, garantendo l'istantaneità dell'attuazione grazie agli smart contract. La firma dei contratti di microassicurazione è basata sulla crittografia asimmetrica e viene salvata su blockchain, che essendo permissioned, è popolata di utenti identificati.

---

[147] Chiap, G. (2019)*, Blockchain: tecnologie e applicazioni per il business,* Hoepli Editore, Milano

CAPITOLO IV:
L'APPROCCIO DELLA MASSA VERSO LA BLOCKCHAIN E LE REGOLAMENTAZIONI IMPOSTE DAI REGOLATORI

La finanza comportamentale studia il comportamento delle persone poste di fronte ad alcune scelte economiche e finanziarie[148]. Tutte le ipotesi fondate sulla teoria economica classica implicano la presenza dell'uomo come essere razionale. La razionalità attribuita all'attore economico stabilisce la capacità di gestire un paniere di scelte da compiere e l'ordine in cui farlo, l'intelligenza di massimizzare la soddisfazione personale e l'intelligenza per svolgere un'analisi accurata delle situazioni. Nel nostro studio abbiamo affrontato lo studio di una tecnologia in rapida espansione nel mondo moderno, la blockchain. Essa ha avuto il potere di scuotere il mondo della finanza, e non solo, creando nuove opportunità.

4.1 Un forte disincentivo all'utilizzo della blockchain

In un mondo non regolamentato, come quello delle criptovalute, accade spesso che il principale utilizzo venga fatto da persone che cercano di eludere le forze dell'ordine. Fin dalla nascita Bitcoin ha dato la possibilità di nascondersi dietro a pseudonimi e di rendersi non rintracciabili, fa parte della sua struttura. Nel febbraio 2011 nacque un mercato anonimo, Silk Road, in una parte nascosta di internet definita "deep web" che garantiva un servizio nascosto attraverso l'utilizzo di un software "Tor". Silk Road permetteva agli utenti di effettuare attività di compravendita di droghe, documenti falsi, prodotti contraffatti o la possibilità di ingaggiare sicari. La moneta utilizzata negli scambi era Bitcoin, nota per la riservatezza che poteva garantire. Al momento della scoperta dell'FBI di questo mondo sommerso e delle attività criminali che vi erano all'interno, vi fu un gran rigetto della tecnologia dietro a Bitcoin. L'episodio di Silk Road non è l'unico a dimostrare un forte utilizzo per scopi malevoli la blockchain. Dal 2009 ad oggi, capita spesso di leggere su importanti testate giornaliste articoli che incriminano le criptovalute per l'essere un ottimo aiuto per i malfattori e fonte di truffe per gli utenti, come il caso dell'hack di Bitfinex citato nel primo capitolo. La criminalità non è l'unico fattore che

[L] Legrenzi, P. (2006), *Psicologia e investimenti finanziari,* EdiText, Torino

tende a condannare la blockchain, lo è anche l'ecosostenibilità. Infatti, Bitcoin e il suo algoritmo di consenso funzionante sul consumo di energia sono da lungo tempo presi di mira. Secondo dati risalenti a settembre 2021, il consumo annuo della Proof-Of-Work è di circa 100 TWh[149] e rappresenta un consumo pari a quello dell'Olanda[150].
Esistono molti altri miti diffusi nella popolazione mondiale che attribuiscono a Bitcoin e alla sua tecnologia di essere solo una bolla speculativa, di non essere un sistema sicuro o soprattutto l'attribuzione di essere inutile per il mondo reale[151].

4.1.1 Due modelli per l'analisi di una possibile adozione della tecnologia blockchain

Ho scelto per quest'analisi due teorie che studiano la diffusione e l'accettazione di una nuova tecnologia.
Secondo la teoria Technology Acceptance Model (TAM), che rappresenta un ottimo modello di analisi del comportamento umano, un individuo ha bisogno di scontrarsi con due fattori: l'utilità della nuova tecnologia e la facilità d'uso[152]. L'utilità di una tecnologia può essere interpretata come vantaggio personale nello sfruttamento di essa, la facilità d'uso invece rappresenta la semplicità nell'approcciarsi e servirsi delle funzionalità nuove[153]. È possibile utilizzare anche dell'Innovation Diffusion Theory (IDT), una teoria applicata alle novità tecnologiche. Questo modello analizza i comportamenti in merito alla scelta di inglobare nella propria vita quotidiana o di rifiutare un'innovazione basandosi sulle credenze degli individui. Secondo il modello IDT, l'accettazione di una novità si basa su cinque concetti: compatibilità, vantaggio che può portare, complessità

[149] Dato fornito dal Bitcoin Energy Consumption Index dell'Università di Cambridge. Disponibile a https://ccaf.io/cbeci/index
[150] Battaglia, A. (2021), *Bitcoin: quanta energia consuma il mining, i dati aggiornati,* Wall Street Italia, 27 settembre 2021, disponibile a https://www.wallstreetitalia.com/bitcoin-quanta-energia-consuma-il-mining-i-dati-aggiornati/
[151] Da Coinbase.com, *I 7 miti Bitcoin più importanti,* disponibile a https://www.coinbase.com/it/learn/crypto-basics/7-biggest-bitcoin-myths
[152] Lee, Y., Kozar, K.A., Larsen, K. (2003), *The Technology Acceptance Model: Past, Present, and Future,*
disponibile a https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3217&=&context=cais&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.it%252Fscholar%253Fq%253Dtechnology%252Bacceptance%252Bmodel%2526hl%253Dit%2526as_sdt%253D0%2526as_vis%253D1%2526oi%253Dscholart#search=%22technology%20acceptance%20model%22
[153] Marikyan, D. & Papagiannidis, S. (2022) *Technology Acceptance Model: A review*, TheoryHub Book, disponibile a http://open.ncl.ac.uk

d'uso, potenzialità e la possibilità di essere compresa[154]. Combinando queste due possibilità si può avere una visione generale della possibilità di adozione della blockchain nella vita di tutti i giorni.

4.1.1.1 L'Analisi

Partiremo dai rischi che possono essere percepiti dagli utilizzatori di Bitcoin e del network sottostante.

Agli inizi della storia della prima criptovaluta i rischi percepiti potevano essere fondati in primis sull'abilità di rimanere in vita come protocollo nel corso degli anni, la possibilità poteva essere quella di una fine prematura a causa di qualche bug. Tuttavia, il valore di Bitcoin in quel periodo era molto vicino allo zero e poteva rappresentare un investimento molto speculativo con un gran rapporto di rischio/rendimento. Il problema riguardante la sicurezza era molto sentito soprattutto negli anni 2009-2010, si verificavano frequentemente truffe ai danni di utenti che venivano attaccati da virus e, data l'impossibilità di poter mettere al sicuro le proprie criptovalute, si rifiutavano di investire in un qualcosa che poi avrebbero probabilmente perso. Un altro fattore di rischio percepito era la difficoltà nel riuscire a interagire con la rete per poter comprare qualche unità di Bitcoin, rendendo il processo di adozione eccessivamente complesso. Man mano che gli anni passavano, gli enti regolatori hanno iniziato a notare l'ascesa parabolica del prezzo della criptovaluta, anche dovuto alla grande richiesta da parte della comunità e iniziarono a imporre delle prime regole da seguire: il processo per la conoscenza del cliente (KYC) e per l'antiriciclaggio (AML).

L'imposizione delle prime regolamentazioni e alcuni miglioramenti imposti dagli sviluppatori attraverso i fork, hanno reso pian piano più facile accedere alla rete e questo guadagnò l'interesse di una piccola parte della popolazione. L'individuo poteva valutare i possibili utilizzi e i vantaggi che poteva trarne. Nell'ultimo decennio i protocolli open source hanno iniziato a diventare più popolari perché non comportavano dei costi all'entrata, Bitcoin facendo parte di questa categoria aumentò la propria notorietà. Lo

[154] Wani, T., Ali, S. (2015), *Innovation Diffusion Theory,* Journal of General Management Research, Vol. 3, Issue 2, July 2015, disponibile a https://www.academia.edu/17960774/Innovation_Diffusion_Theory_Review_and_Scope_in_the_Study_of_Adoption_of_Smartphones_in_India?bulkDownload=thisPaper-topRelated-sameAuthor-citingThis-citedByThis-secondOrderCitations&from=cover_page

studio del whitepaper di Bitcoin[155] e le evidenze riscontrate dai cosiddetti "early adopters" dimostravano come potesse aumentare la libertà degli individui sia per l'eliminazione degli intermediari sia per la possibilità di trasferire denaro liberamente a costi limitati. Dal punto di vista di coloro che volevano arricchirsi attraverso questa tecnologia, Bitcoin rappresentava un mezzo estremamente interessante a causa della politica monetaria di emissione del token e per la volatilità del prezzo. Dopo tredici anni dalla nascita di questo protocollo si può affermare che la tecnologia blockchain sta prendendo piede nel settore finanziario particolarmente, ma non solo.

4.1.2 Gli errori cognitivi negli investimenti in criptovalute

La finanza comportamentale suddivide le distorsioni dalla razionalità dell'uomo in bias cognitivi e euristiche. I bias cognitivi sono delle deviazioni che la nostra mente crea a causa di convinzioni errate[156]. Le euristiche, al contrario dei bias, sono scorciatoie di pensiero che l'essere umano applica per dare risposte semplici di fronte a problemi complessi. Questi meccanismi vengono utilizzati dal nostro corpo per permetterci di operare più velocemente e per proteggerci[157].

Nell'ottica investimenti, in criptovalute come tutti gli altri strumenti finanziari, sono fortemente influenzati da questi atteggiamenti.

Un grande bias cognitivo che impedisce di investire nelle criptovalute è lo "status-quo bias". Questa è una distorsione mentale che comporta un forte interesse nel mantenere il proprio capitale allo stato attuale, sovrappesando le perdite e non tenendo conto delle possibilità di guadagno.

Un comportamento operato dall'uomo è l'effetto gregge che porta ad un rifiuto degli investimenti in criptovalute è stato l'essere fortemente condizionato dalla pubblicità negativa operata in più riviste di attualità dove nei cicli ribassisti di mercato Bitcoin veniva dichiarato fallito, solo nel 2018 si scrisse novanta volte "Bitcoin is dead"[158]. L'effetto gregge si verifica anche nel caso contrario, ovvero nell'affidarsi alla massa per la scelta degli investimenti da compiere; per esempio, quando nel 2017, dopo una grande

[155] Disponibile a https://bitcoin.org/bitcoin.pdf
[156] Legrenzi, P. (2006), *Psicologia e investimenti finanziari,* EdiText, Torino
[157] Kahneman, D., Tversky, A. (2013), *Handbook of the fundamentals of financial decision making: part I,* World Scientific Publishing Co. Pte. Ltd., Singapore
[158] Chang, S. (2018), *Bitcoin "dead" 90 times in 2018*, disponibile a https://finance.yahoo.com/news/bitcoin-died-90-times-2018-120041001.html

salita parabolica dei prezzi, molti sono accorsi a effettuare acquisti di criptovalute. Il risultato è stato lo scoppio della bolla, che lasciò molti nuovi investitori in perdita per molto tempo. L'effetto gregge viene chiamato anche Fear of Missing Out (FOMO)[159].

L'euristica della rappresentatività è il giudizio fatto da un individuo che viene formulato sulla base di stereotipi. Questo è applicabile nel nostro caso, in quanto è possibile perdere l'opportunità di rendimenti molto interessanti a causa di tutti i retroscena che hanno condizionato i primi anni della storia delle criptovalute, gli hack e le truffe. Se l'investitore ha vissuto il periodo della bolla dot-com può notare diverse analogie con Bitcoin e può esserne negativamente influenzato.

L'overconfidence degli investitori può essere affiancata al bias dell'eccessivo ottimismo. Questi due tendenze comportamentali conducono alla sottostima dei rischi, dovuta a un'eccessiva sicurezza nei rendimenti positivi e nelle proprie abilità. Questa condotta dell'uomo può essere condizionata dall'effetto gregge, un esempio che possiamo farne risale a poco tempo fa: nei mesi di ottobre e novembre 2021 le criptovalute stavano avendo dei rialzi molto accentuati, che ingannarono gli investitori, convinti di raggiungere determinate soglie di prezzo nonostante la presenza di numerosi indicatori che indicavano il contrario[160].

Anche l'euristica dell'ancoraggio può influenzare l'individuo nell'elaborazione della decisione di investimento o meno. Nel momento in cui sto parlando, i mercati stanno vivendo un momento ribassista iniziato molti mesi fa: l'investitore prende solo il lato negativo della cosa e preferisce aspettare momenti migliori, non sfruttando l'occasione di poter entrare a prezzi migliori[161]. In periodi come questo, il possibile investitore guarda solo la performance di breve periodo e non considera l'evoluzione del prezzo nell'arco di un periodo più grande.

---

[159] Calderòn, O. B. (2018), *Herding behavior in cryptocurrency markets,* Universitat Autònoma de Barcelona Department of Applied Economics, disponibile a https://arxiv.org/pdf/1806.11348.pdf

[160] Gardenal, G., Rigoni, U. (2016), *Finanza comportamentale e gestione del risparmio,* Giappichelli Editore, Torino

[161] Almansour, B. (2020), *Cryptocurrency market: a behavioral finance perspective,* Journal of Asian Finance Economics and Business, disponibile a https://www.researchgate.net/publication/346565632_Cryptocurrency_Market_Behavioral_Finance_Perspective

4.1.3 Le criptovalute come mezzo di investimento oggi

Dal periodo dopo lo scoppio della pandemia le criptovalute sono diventate molto più popolari. Non ci si meraviglia più quando si vede che un exchange è sponsorizzato sulle reti televisive che guardiamo tutti i giorni o diventa partner di squadre nella maggioranza degli sport. Sempre nello stesso periodo, sono nati i "fan token". Questa categoria di token rappresenta una collaborazione tra l'exchange emittente e una società sportiva al fine di ottenere entrambe un guadagno, offrendo agli interessati la possibilità di speculare su possibili eventi futuri o di detenerle a scopo di intrattenimento.

4.2 Il riciclaggio nelle criptovalute

Una nuova tecnologia nel mondo finanziario comporta la considerazione della creazione di nuove possibilità di riciclaggio. È un dato di fatto che le criptovalute vengano utilizzate anche con scopi illeciti, abbiamo citato il caso di Silk Road in precedenza, e le loro caratteristiche intrinseche favoriscono l'utilizzo di esse per eludere la legge. Le regolamentazioni antiriciclaggio che sono state imposte nel corso degli anni stanno man mano cercando di limitare il fenomeno, con la speranza di riuscire ad eliminarlo definitivamente. Prima di svolgere un'analisi delle regolamentazioni ad ora vigenti è utile capire quali caratteristiche delle criptomonete siano la loro propensione a diventare mezzi invitanti per riciclare denaro. Le caratteristiche di cui parliamo sono:

1. Accettabilità: è diventato possibile acquistare beni e servizi senza dover convertire le criptovalute in valuta fiat. Se non è necessario trasferire il proprio denaro illecito in un conto bancario, o in qualsiasi altro deposito tracciabile, l'unico freno che può essere posto al riciclaggio di denaro è la ancora bassa accettazione di pagamenti in criptovalute.
2. Impossibilità di congelamento dei fondi: le autorità di vigilanza non possono confiscare le criptovalute rappresentanti il denaro sporco se sono detenute nel network decentralizzato. L'accesso ai fondi detenuti sui wallet non-custodial è possibile solo possedendo la chiave privata. È possibile congelare i fondi solo

quando le criptovalute sono detenute in exchange centralizzati, come è successo a febbraio 2022 con Kraken[162].

3. Pseudonimato: abbiamo presentato la differenza con l'anonimato nel Capitolo 1. L'utilizzo di pseudonimi non aiuta nell'identificazione delle controparti coinvolte in uno scambio, si può tenere solo traccia della transazione. Inoltre, è possibile utilizzare più wallet per aggirare un possibile controllo.
4. Flessibilità e commissioni di transazione: i costi dei trasferimenti di criptovalute nella blockchain sono irrisori, solitamente, grazie all'eliminazione degli intermediari. La mancanza di una figura posta tra mittente e destinatario comporta un'ulteriore difficoltà per le autorità. Utilizzando la rete peer-to-peer è possibile riciclare denaro facendo più scambi in direzione di destinatari diversi.
5. Irreversibilità: è un incentivo al riciclaggio perché anche se fosse scoperta un'attività di compravendita illecita o una frode non sarebbe possibile rimborsare i malcapitati. Dopo che la transazione viene confermata sui blocchi, le autorità sono impossibilitate alla revoca.
6. Velocità dei trasferimenti: gli scambi di criptovalute sono monitorabili solo dopo l'effettivo avvenimento.

4.2.1 Le ultime disposizioni in materia di regolamentazioni

Le regolamentazioni riguardanti le criptovalute al momento sono ancora lacunose e in continua evoluzione, analizzeremo le ultime normative emanate a livello italiano e europeo.

4.2.1.1 In Italia

Il 17 febbraio 2022 è stato emanato il decreto del Ministero dell'Economia e delle Finanze riguardante le modalità in cui gli exchange e i wallet provider devono operare sul suolo italiano.

[162] Kelly, L. (2022), *Kraken "Cannot Protect You" From Canadian Government Freezing Crypto: CEO,* disponibile a https://decrypt.co/93243/kraken-cannot-protect-you-from-canadian-government-freezing-crypto-ceo

La normativa è frutto di un lungo percorso e aspira alla regolamentazione degli erogatori di servizi finanziari che utilizzano valute virtuali. La definizione di "valuta virtuale" data dal MEF è la seguente "la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente"[163]. Nel decreto il Legislatore intende comprendere gli exchange di criptovalute e coloro che concedono il servizio di custodia delle chiavi crittografiche private di portafogli all'interno della categoria dei cambiavalute, facendoli sottostare alla V direttiva antiriciclaggio UE 2018/843. La prima conseguenza riguarda l'iscrizione al registro dei cambiavalute presso l'OAM[164]. Il decreto nei primi due articoli definisce chi può essere definito un erogatore di servizi o un wallet provider e le finalità per cui sono utilizzati. Nella parte centrale, dall'articolo tre al sei, si trattano:

- L'obbligo di iscrizione alla sezione speciale del registro per prestatori di servizi relativi a valute digitali e servizi di portafoglio digitale;
- Le tempistiche per iscriversi al registro;
- Le modalità d'invio dei dati relativi ai fruitori dei servizi e la periodicità dell'invio. Le informazioni richieste sono in merito all'identificazione dei clienti, noto come servizio Know Your Costumer (KYC).
- La cooperazione con le forze dell'ordine italiane nel segnalare operazioni sospette e l'obbligo di collaborare durante delle possibili indagini delle forze dell'ordine[165].

4.2.1.2 La fiscalità in Italia

La dichiarazione delle criptovalute è ancora un tema che crea molti dubbi agli investitori. Qualsiasi sia il fine della detenzione di valute virtuali, ai fini di monitoraggio è richiesta la dichiarazione nel modello 730 nel quadro RW, ovvero la stessa sezione riguardante le valute estere, dove va indicato il controvalore in euro al 31 dicembre del periodo di

[163] Gazzetta Ufficiale, 17 febbraio 2022, numero 40, Roma, 17 febbraio 2022
[164] "è l'Organismo competente in via esclusiva ed autonoma per la gestione degli Elenchi degli Agenti in attività finanziaria e dei Mediatori creditizi", è stato istituito con il decreto legislativo 13 agosto 2010, n.141. – OAM, *Cosa fa l'OAM,* disponibile a https://www.organismo-am.it/cosa-fa-l-oam
[165] Gazzetta Ufficiale, 17 febbraio 2022, numero 40, Roma, 17 febbraio 2022

riferimento[166]. Al momento, per la legge italiana non si è imponibili di tassazione fino al momento della conversione in valuta legale o per l'attività di compravendita di qualsiasi tipo di bene. La tassazione viene imposta al momento della cessione in caso di plusvalenza, solo se il valore del portafoglio dell'investitore ha superato per almeno sette giorni consecutivi la cifra di 51.645,69 €. In caso di minusvalenze, o cessioni da parte di individui che non superano la giacenza media di 51.645,69 € per sette giorni consecutivi, persiste solo l'obbligo di dichiarazione[167].

4.2.2 In Europa

Il Parlamento europeo ha annunciato il 30 giugno 2022 l'accordo provvisorio su un nuovo regolamento in relazione ai mercati delle cripto-attività (MiCA)[168]. L'insieme di regole MiCA nascono con il fine di fare chiarezza in materia di servizi finanziari offerti nel mondo digitale e, in collaborazione col regolamento DLT[169], forniscono le linee guida per chi opera su piattaforme a registro distribuito. Il MiCA mira al controllo degli utility token e, in particolare, delle stablecoins; il regolamento DLT disciplina la negoziazione di strumenti finanziari nei vari protocolli blockchain[170].

Come citato a inizio capitolo, ad ora non esistono regolamenti riguardanti gli scambi che avvengono nei vari servizi di finanza decentralizzata. Il regolamento MiCA, differentemente da quello DLT, deve ancora essere approvato ma rappresenta una grande implementazione di controlli per la sicurezza dell'investitore. L'approccio sarà particolarmente incentrato sulle stablecoin, data la loro importanza sempre crescente, e l'intenzione è quella di renderle controllate dall'EBA, l'Autorità bancaria europea.

---

[166] Agenzia delle Entrate, Interpello 788/2021, disponibile a https://www.agenziaentrate.gov.it/portale/documents/20143/3930262/Risposta+788+del+2021.pdf/01995188-b1a7-bdcb-6116-760577456538

[167] Dott. Pescosolido, J. (2021), *Criptovalute- Tassazione ed obblighi di monitoraggio fiscale (RW),* disponibile a https://www.fiscoetasse.com/approfondimenti/14140-criptovalute-tassazione-ed-obblighi-di-monitoraggio-fiscale-rw.html

[168] Fulco, D. (2022), *Cripto-attività, ecco cosa cambia col Regolamento MICA: obiettivi, perimetro, prossimi step, disponibile a* https://www.agendadigitale.eu/cittadinanza-digitale/cripto-attivita-ecco-cosa-cambia-col-regolamento-mica-obiettivi-perimetro-prossimi-step/

[169] Gazzetta Ufficiale dell'Unione europea, 30 maggio 2022, Regolamento UE 2022/858, L. 151/1, 2 giugno 2022

[170] Fulco, D. (2022), *Cripto-attività, ecco cosa cambia col Regolamento MICA: obiettivi, perimetro, prossimi step, disponibile a* https://www.agendadigitale.eu/cittadinanza-digitale/cripto-attivita-ecco-cosa-cambia-col-regolamento-mica-obiettivi-perimetro-prossimi-step/

4.2.3 Il caso della criptovaluta Terra (LUNA)

Terra Money è un protocollo costruito su blockchain sviluppato da Terraform Labs, fondata da Do Kwon. La blockchain di Terra utilizza l'algoritmo di consenso Proof-of-Stake, totalmente indipendente dal mondo Ethereum, fondato sul token nativo LUNA. Il token LUNA funge da token di governance, essendo Terra una DAO, è necessario per il pagamento delle commissioni delle transazioni e viene utilizzato per lo staking. All'interno dell'ecosistema era stata creata una stablecoin algoritmica ancorata al valore del dollaro chiamata TerraUSD (UST). Su Anchor Protocol era possibile depositare i propri UST ottenendo una rendita di circa il 20% APY, i rendimenti così alti resero molto popolare l'utilizzo della stablecoin per questo fine. Per mantenere il valore del dollaro lo smart contract di UST opera il "mint and burn", ovvero la creazione e la distruzione, utilizzando il token LUNA. Quando si verificava un eccesso di domanda per la stablecoin, causandone il distaccamento dal valore di 1$, si poteva scambiare 1$ di LUNA ottenendo un profitto privo di rischi e riportando il valore di UST al dollaro. Nel caso il valore della stablecoin fosse sceso sotto al dollaro era comunque possibile scambiarlo con 1$ di LUNA, riducendone così l'offerta[171]. Il meccanismo ha retto finché ci sono stati arbitraggisti pronti a riportare il valore di UST al dollaro. Il giorno 8 maggio 2022 il protocollo ha subito un attacco, che viene attribuito a due colossi della finanza tradizionale: Blackrock e Citadel[172]. La strategia sarebbe stata la richiesta di un prestito per un quantitativo di 100.000 BTC ad un exchange per poi scambiarne 25.000 in UST. La grande quantità di liquidità di UST prelevata per lo scambio e la vendita istantanea, combinata alla vendita dei restanti 75.000 BTC, ha causato un panic selling generale del mercato. Gli investitori di UST iniziarono una sorta di "bank run" ritirando la stablecoin da Anchor Protocol, il quale non aveva la liquidità disponibile a pagare i prelievi, si stima siano stati prelevati oltre cinque miliardi di dollari in breve tempo[173]. Il prezzo di LUNA crollò del 100% e UST di circa il 90%, furono spazzati 60 miliardi di dollari dal

[171] Young Platform, *Cosa sta succedendo a UST e a Terra (LUNA)?, disponibile a* https://youngplatform.com/blog/news/cosa-sta-succedendo-terra-luna-ust/
[172] Martellucci, E. (2022), *Cosa è successo veramente a Terra LUNA e UST?,* disponibile a https://cryptonomist.ch/2022/05/12/cosa-successo-terra-luna-ust/
[173] Erlich, S., *Unstable Stablecoin: How Crypto's Crash Broke The Buck For TerraUSD,* disponibile a https://www.forbes.com/sites/stevenehrlich/2022/05/10/unstable-stablecoin-how-cryptos-crash-broke-the-buck-for-terrausd/?sh=46d45e006ff4

mercato[174]. I presunti attaccanti avrebbero poi ripagato il prestito ottenendo un grosso profitto dalla differenza del prezzo, prima dell'attacco BTC era quotato a circa 31.000$, nelle due settimane successive è sceso intorno ai 20.000$. Il fondatore del protocollo Terra fece la proposta di hard fork e la DAO si espresse positivamente, ma era una soluzione che non poteva far tornare i guadagni alle persone. La fiducia nella DeFi crollò in seguito all'attacco e molti investitori, che ingenuamente, si fecero attrarre dalla rendita del 20% perdendo tutti i propri risparmi[175], sono stati riportati anche dei casi di suicidio[176]. La polizia sudcoreana, paese d'origine del fondatore di Terra, per mesi cercò di ottenere delle risposte in merito al coinvolgimento nel crollo. Al momento, Do Kwon risulta scomparso, ma ancora attivo sul suo account twitter, nonostante continui ad affermare il contrario. La polizia sudcoreana, con la complicità di un servizio di analisi on-chain, ha chiesto il fermo a due exchange di due wallet collegati al fondatore di Terra contenenti circa 60 milioni di dollari in Bitcoin. Inoltre, l'Interpol ha emanato la richiesta "red notice", la quale sarebbe una richiesta a tutti gli organi di polizia mondiale di localizzare e arrestare temporaneamente Do Kwon in attesa di estradizione[177].

4.2.4 Il blocco di Tornado Cash

Tornado Cash è una Dapp sviluppata su Ethereum che permette di aumentare la privacy delle transazioni rendendole anonime. Proteggere i dati di chi trasferisce valore all'interno della blockchain non è illegale, ma dal momento che viene usato a fini criminali va contro l'etica. Il protocollo permette di depositare i fondi in dei pool, riuscendo a "far perdere le tracce" delle transazioni precedenti, eludendo la trasparenza

[174] Soon, W. (2022), *Some crypto investors say TerraUSD and Luna's $60 billion crash pushed them to the brink and led to thoughts of self-harm,* disponibile a https://www.businessinsider.com/terrausd-luna-60-billion-crash-sparks-fears-suicide-self-harm-2022-6?r=US&IR=T

[175] Wolfe, N. (2022), *Crypto investors contemplate SUICIDE and hide from friends seeking revenge for losing their life savings as currency crashes to zero,* disponibile a https://www.dailymail.co.uk/news/article-10823197/Terra-Luna-crypto-crash-investors-suicidal-friends-seek-retribution-millions-lost.html

[176] Yahoo News, *Luna crashes below $3 after S. Korea issues arrest warrant for Terraform Labs founder Do Kwon,* disponibile a https://news.yahoo.com/luna-crashes-below-3-korea-200957950.html

[177]Rociola, A. (2022), *La Corea del Sud ha chiesto all'Interpol l'arresto del creatore della criptovaluta Terra-Luna,* 19 settembre 2022, disponibile a https://www.repubblica.it/tecnologia/2022/09/19/news/do_kwon_interpol_red_notice_criptovalute_terra_luna-366314155/

dei dati on-chain. Durante il 2022 è stato sollevato il caso dalle autorità statunitensi e l'8 agosto 2022 il sito è stato oscurato a tutti gli americani; inoltre, sono stati bloccati gli indirizzi collegati a scambi operati sul protocollo sospettati di riciclaggio di denaro sporco. Il dipartimento del Tesoro americano stima che siano stati riciclati più di 7 miliardi di dollari all'interno della Dapp[178]. Il maggior contributore al codice di Tornado Cash è stato arrestato nei Paesi Bassi con l'accusa di favoreggiamento al riciclaggio e di reati finanziari[179].

[178] Ponciano, J. (2022), *Treasury Sanctions Ethereum-Based Tornado Cash For Allegedly Helping To Launder More Than $7 Billion*, disponibile a https://www.forbes.com/sites/jonathanponciano/2022/08/08/treasury-sanctions-ethereum-based-tornado-cash-for-allegedly-helping-to-launder-more-than-7-billion/?sh=192c84f93f97

[179] Giordano, M. T., Capaccioli, S. (2022), *Il caso Tornado Cash alza il livello dello scontro su privacy e criptovalute,* disponibile a https://www.wired.it/article/tornado-cash-privacy-criptovalute/

CONCLUSIONI

Nel corso dell'ultimo ventennio la tecnologia ha fatto passi da gigante. All'inizio degli anni duemila, il cellulare era la più grande rivoluzione che si fosse potuta vedere, oggi è la normalità. L'adozione di massa di Internet, che è diventato disponibile all'intera popolazione mondiale e si evolve in continuazione. L'evoluzione dei cellulari, divenuti "smartphone", che con un solo input ci permettono una miriade di azioni. In questo periodo sono nate anche la blockchain e le criptovalute: saranno adottati dalla popolazione mondiale come Internet e gli smartphone? Per quanto ne sappiamo ora, tutto è possibile. Al momento, la blockchain è ancora in fase di studio per le future applicazioni alle aziende di tutti i settori, in questa tesi abbiamo dato particolare importanza agli sviluppi nel settore finanziario. Abbiamo studiato anche le criptovalute, potranno un giorno affermarsi? Bitcoin e i suoi ideali di decentralizzazione hanno attirato l'attenzione del grande pubblico e, anche, degli enti regolatori. La regolamentazione per le criptovalute è ancora in una fase primordiale e le leggi esistenti ad ora sono lacunose e, talvolta, poco comprensibili dall'uomo medio. La sostenibilità dell'algoritmo di consenso di Bitcoin è discutibile e non passa giorno in cui non si possa leggere un articolo di qualche giornalista che condanna lo spreco di energia dovuto al Proof-Of-Work. L'innovazione che ha portato al settore finanziario è degna di nota, ma per restare in questo settore è necessario venga adottato dal mondo intero. Perché avvenga questo fenomeno è necessario trovare un compromesso sull'energia consumata, soprattutto in un periodo di crisi energetica mondiale, come quella che stiamo vivendo. Personalmente, credo fermamente in questa tecnologia e credo nel mondo digitale. Sono convinto che, con i dovuti compromessi, tra un decennio farà parte delle nostre vite.

BIBLIOGRAFIA

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

Basile, A. (2019), *Blockchain: la nuova rivoluzione industriale,* Dario Flaccovio Editore, Palermo

Chiap, G. (2019)*, Blockchain: tecnologie e applicazioni per il business,* Hoepli Editore, Milano

Comandini, G.L. (2020), *Da zero alla luna,* Dario Flaccovio Editore, Palermo

Garavaglia, R. (2021), *Conoscere la blockchain,* Hoepli, Milano

Gazzetta Ufficiale dell'Unione europea, 30 maggio 2022, Regolamento UE 2022/858, L. 151/1, 2 giugno 2022, https://www.gazzettaufficiale.it

Gardenal, G., Rigoni, U. (2016), *Finanza comportamentale e gestione del risparmio,* Giappichelli Editore, Torino

Kahneman, D., Tversky, A. (2013), *Handbook of the fundamentals of financial decision making: part I,* World Scientific Publishing Co. Pte. Ltd., Singapore

Lai, R. e Kuo Chuen, D. L. (2018), *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2,* Academic Press

Legrenzi, P. (2006), *Psicologia e investimenti finanziari,* EdiText, Torino

Sorgentone, P. (2020), *Il Futuro del Valore: Blockchain, Cryptoasset e Finanza Decentralizzata,* pubblicazione indipendente da editori

SITOGRAFIA

Accenture.com, https://www.accenture.com/us-en/insights/blockchain/banking-on-blockchain

Agenzia delle Entrate, Interpello 788/2021, disponibile a https://www.agenziaentrate.gov.it/portale/documents/20143/3930262/Risposta+788+del+2021.pdf/01995188-b1a7-bdcb-6116-760577456538

Battaglia, A. (2021), *Bitcoin: quanta energia consuma il mining, i dati aggiornati,* Wall Street Italia, 27 settembre 2021, disponibile a https://www.wallstreetitalia.com/bitcoin-quanta-energia-consuma-il-mining-i-dati-aggiornati/

[1] Da Coinbase.com, *I 7 miti Bitcoin più importanti*

Binance Academy, *Merkle Trees and Merkle Roots explained,* disponibile a https://academy.binance.com/en/articles/merkle-trees-and-merkle-roots-explained

Binance Academy, *Rug pull,* disponibile a https://academy.binance.com/en/glossary/rug-pull

Binance Academy, *Cosa sono i pool di liquidità nella DeFi e come funzionano?,* disponibile a https://academy.binance.com/it/articles/what-are-liquidity-pools-in-defi

Binance Academy, *Cosa sono i nodi?* , disponibile https://academy.binance.com/it/articles/what-are-nodes

Binance Academy, *La Proof of Authority Spiegata,* disponibile a https://academy.binance.com/it/articles/proof-of-authority-explained

Binance Academy, *Turing complete*, disponibile a https://academy.binance.com/en/glossary/turing-complete

Binance Academy, *Cosa sono le stablecoin?, disponibile a https://academy.binance.com/it/articles/what-are-stablecoins*

Bitcoin Wiki, *Merkle tree*, disponibile a https://it.bitcoinwiki.org/wiki/Albero_Merkle

Bitstamp.net, *What is a multisig wallet?,* disponibile a https://www.bitstamp.net/learn/security/what-is-a-multisig-wallet/

Blockchain.com (2018)*, Shining light on The State of Stablecoins,* disponibile a https://medium.com/blockchain/shining-light-on-the-state-of-stablecoins-1a92c9172043

Blockchain Media, *Cosa sono i nodi blockchain e Bitcoin?,* disponibile a https://blockchain-media.org/chto-takoe-blockchain-i-node-bitcoin

Blockchain Consensus Encyclopedia, *Proof-of-History,* disponibile a https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-capacity-space/proof-of-history

Blockchain4Innovation, *Valuta elettronica utilizzata in un dato sistema DLT*, disponibile a *https://www.blockchain4innovation.it/criptovalute/token-cose-come-viene-utilizzato/*

Campaci, E. (2021), *Come funziona il liquid staking,* disponibile a https://youngplatform.com/blog/news/come-funziona-liquid-staking/

Chaum, D. (1982), *Advances in Cryptology Proceedings of Crypto,* disponibile a https://chaum.com/wp-content/uploads/2022/01/Chaum-blind-signatures.pdf

Chow, A.R. (2022), *Inside the Chess Match That Led the Feds to $3.6 Billion in Stolen Bitcoin,* The Time, disponibile a https://time.com/6146749/cryptocurrency-laundering-bitfinex-hack/

CME group, *Defining Ether and Ethereum,* disponibile a https://www.cmegroup.com/education/courses/introduction-to-ether/defining-ether-and-ethereum.html

Coscia, E. (2018), *Stablecoins: cosa sono e perché sono così importanti,* disponibile a https://www.fintastico.com/it/blog/stablecoin-cosa-sono-perche-sono-cosi-importanti/

Coinbase, *What is a fork?,* disponibile a https://www.coinbase.com/it/learn/crypto-basics/what-is-a-fork

Cointelegraph, *Permissioned blockchain vs. permissionless blockchain: Key differences,* disponibile a https://cointelegraph.com/blockchain-for-beginners/permissioned-blockchain-vs-permissionless-blockchain-key-differences

Cointelegraph.com, *What are decentralized exchanges, and how do DEXs work?,* disponibile a https://cointelegraph.com/defi-101/what-are-decentralized-exchanges-and-how-do-dexs-work

Cointelegraph, *Cos'è una hard fork,* disponibile a https://it.cointelegraph.com/bitcoin-cash-for-beginners/what-is-hard-fork

Coinmarketcap, https://coinmarketcap.com

Condemi, J. (2020), *DeFi: cos'è la finanza decentralizzata e come sta cambiando il mercato delle criptovalute,* disponibile a https://www.blockchain4innovation.it/mercati/defi-cose-la-finanza-decentralizzata-e-come-sta-cambiando-il-mercato-delle-criptovalute/

Coinsquare, *Whitepaper Versus Yellowpaper: What is the Difference?,* disponibile a https://news.coinsquare.com/learn-coinsquare/whitepaper-versus-yellowpaper-difference/

Crypto Italia, *Come è stato scelto il limite di 21 milioni di Bitcoin?,* disponibile a https://cryptoitalia.org/mai-limite-21-milioni-btc/

De Candia, A. (2021), *Le origini della DeFi*, disponibile a https://cryptonomist.ch/2021/01/01/origini-defi/

Ethereum, https://ethereum.org/en/

Enciclopedia Treccani, *infungibile*, disponibile a https://www.treccani.it/vocabolario/infungibile/

Enciclopedia Treccani, *governance,* definizione disponibile a https://www.treccani.it/enciclopedia/governance_%28Dizionario-di-Economia-e-Finanza%29/

Erlich, S., *Unstable Stablecoin: How Crypto's Crash Broke The Buck For TerraUSD,* disponibile a https://www.forbes.com/sites/stevenehrlich/2022/05/10/unstable-stablecoin-how-cryptos-crash-broke-the-buck-for-terrausd/?sh=46d45e006ff4

Fulco, D. (2022), *Cripto-attività, ecco cosa cambia col Regolamento MICA: obiettivi, perimetro, prossimi step, disponibile a* https://www.agendadigitale.eu/cittadinanza-digitale/cripto-attivita-ecco-cosa-cambia-col-regolamento-mica-obiettivi-perimetro-prossimi-step/

Giordano, M. T., Capaccioli, S. (2022), *Il caso Tornado Cash alza il livello dello scontro su privacy e criptovalute,* disponibile a https://www.wired.it/article/tornado-cash-privacy-criptovalute/

Kraken.com, *Panoramica dello staking on chain su Kraken,* disponibile a https://support.kraken.com/hc/it/articles/360037682011-Panoramica-dello-staking-On-chain-su-Kraken

Gatti, M. (2019), *Il problema dei generali Bizantini e la soluzione di Bitcoin,* disponibile a https://cryptonomist.ch/2019/08/04/problema-generali-bizantini-soluzione-bitcoin/

IBM, *Single point of failure, disponibile* a https://www.ibm.com/docs/he/tsafm/4.1.0?topic=p-single-point-failure-spof

IBM.com, *What is distributed computing?,* disponibile a https://www.ibm.com/docs/en/txseries/8.2?topic=overview-what-is-distributed-computing

kaspersky.it, *La crittografia nella protezione dei dati*, disponibile a https://www.kaspersky.it/blog/limportanza-della-crittografia-nella-protezione-dei-dati/949/

Kaspersky.it, *Cosa sono gli attacchi DDos? ,* disponibile a https://www.kaspersky.it/resource-center/threats/ddos-attacks

Kelly, L. (2022), *Kraken "Cannot Protect You" From Canadian Government Freezing Crypto: CEO,* disponibile a https://decrypt.co/93243/kraken-cannot-protect-you-from-canadian-government-freezing-crypto-ceo

Kaspersky.com, *Brute Force Attack: Definition and Examples*, disponibile a https://www.kaspersky.com/resource-center/definitions/brute-force-attack

Kraken Intelligence (2022), *Proof-of-Work vs Proof-of-*Stake, disponibile a https://kraken.docsend.com/view/58b6xidjxk44xedc

Larchevêque, E. (2016), *Hardware Oracles: bridging the Real World to the Blockchain,* disponibile a https://bravenewcoin.com/insights/hardware-oracles-bridging-the-real-world-to-the-blockchain

Levi, S.D., Lipton, A. B. (2018) , *An Introduction to Smart Contracts and Their Potential and Inherent Limitations,* Harvard law school on corporate governance, disponibile a https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/#4

Lee, Y., Kozar, K.A., Larsen, K. (2003), *The Technology Acceptance Model: Past, Present, and Future,*
disponibile a
https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3217&=&context=cais&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.it%252Fscholar%253Fq%253Dtechnology%252Bacceptance%252Bmodel%2526hl%253Dit%2526as_sdt%253D0

%2526as_vis%253D1%2526oi%253Dscholart#search=%22technology%20acceptance%20model%22

Masciantonio, S., Zaghini, A. (2017), *N. 1153 - Un'analisi delle misure di rischio sistemico e di importanza sistemica durante la crisi finanziaria globale*, disponibile a https://www.bancaditalia.it/pubblicazioni/temi-discussione/2017/2017-1153/index.html?com.dotmarketing.htmlpage.language=102&dotcache=refresh

Marikyan, D. & Papagiannidis, S. (2022) *Technology Acceptance Model: A review*, TheoryHub Book, disponibile a http://open.ncl.ac.uk

Ministero dello sviluppo economico, *Tecnologie Distributed Ledger*, disponibile a https://uibm.mise.gov.it/index.php/en/lotta-alla-contraffazione/servizi-per-imprese-e-consumatori/tecnologie-anticontraffazione/sot-servizio-orientamento-tecnologie-anticontraffazione/tecnologie-distributed-ledger

Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System,* https://bitcoin.org/bitcoin.pdf

Paolini, M. (2022), *Bitcoin e mining: qual è il loro impatto ambientale*, disponibile a https://quifinanza.it/green/bitcoin-mining-impatto-ambientale/640370/

Ponciano, J. (2022), *Treasury Sanctions Ethereum-Based Tornado Cash For Allegedly Helping To Launder More Than $7 Billion*, disponibile a https://www.forbes.com/sites/jonathanponciano/2022/08/08/treasury-sanctions-ethereum-based-tornado-cash-for-allegedly-helping-to-launder-more-than-7-billion/?sh=192c84f93f97

Rociola, A. (2022), *La Corea del Sud ha chiesto all'Interpol l'arresto del creatore della criptovaluta Terra-Luna,* 19 settembre 2022, disponibile a https://www.repubblica.it/tecnologia/2022/09/19/news/do_kwon_interpol_red_notice_criptovalute_terra_luna-366314155/

Szabo, N. (1994), *Smart contracts*, disponibile a https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Soon, W. (2022), *Some crypto investors say TerraUSD and Luna's $60 billion crash pushed them to the brink and led to thoughts of self-harm,* disponibile a https://www.businessinsider.com/terrausd-luna-60-billion-crash-sparks-fears-suicide-self-harm-2022-6?r=US&IR=T

The Cryptonomist, *Proof-of-Elapsed-Time, l'algoritmo di consenso basato sul tempo,* disponibile a https://cryptonomist.ch/2019/06/15/proof-of-elapsed-time-poet/

The Cryptonomist, *Proof of Capacity (PoC): l'algoritmo di consenso che sfrutta l'hard disk,* disponibile a https://cryptonomist.ch/2019/08/17/proof-of-capacity-hard-disk/

Università di Cambridge, disponibile a https://ccaf.io/cbeci/index

Wani, T., Ali, S. (2015), *Innovation Diffusion Theory,* Journal of General Management Research, Vol. 3, Issue 2, July 2015, disponibile a https://www.academia.edu/17960774/Innovation_Diffusion_Theory_Review_and_Scope_in_the_Study_of_Adoption_of_Smartphones_in_India?bulkDownload=thisPaper-topRelated-sameAuthor-citingThis-citedByThis-secondOrderCitations&from=cover_page

World Bank Group, *Distributed Ledger Technology (DLT) and Blockchain,* disponibile a https://openknowledge.worldbank.org/handle/10986/29053

Yahoo News, *Luna crashes below $3 after S. Korea issues arrest warrant for Terraform Labs founder Do Kwon,* disponibile a https://news.yahoo.com/luna-crashes-below-3-korea-200957950.html

Yearn.finance, *Overview,* disponibile a https://docs.yearn.finance/getting-started/products/yvaults/overview

Young Platform, *Crittografia: Cesare, Enigma e la Blockchain***,** disponibile a https://academy.youngplatform.com/blockchain/storia-crittografia-cesare-enigma-blockchain/

Young Platform, *Bitcoin: come funziona il Double Spending?,* disponibile a https://academy.youngplatform.com/blockchain/bitcoin-come-funziona-double-spending/

Young Platform, *ERC-20*, disponibile a https://youngplatform.com/glossary/erc20/