LUISS

RELATORE

CANDIDATO

A Mamma e Papà che nonostante le difficoltà hanno sempre creduto in me, supportandomi fino alla fine.

A me stesso, alla mia forza di volontà e alla voglia costante di superarsi.

INDICE

INTRODUZIONE

L'avvento della tecnologia è sempre più dinamico ai giorni nostri, entra a far parte delle nostre vite senza che ce ne accorgiamo come mezzo per migliorare la società e la nostra quotidianità. L'implementazione e la comprensione di una nuova tecnologia come la Blockchain in diversi settori può rappresentare un importante passo avanti per la società in termini sociali, ambientali ed economici rendendo più snello ed efficiente un sistema caratterizzato da un eccesso burocratico e il rischio di corruzione. Anche lo sviluppo di un sistema di commercio potrebbe aprire le porte verso un ulteriore rivoluzione del sistema monetario, che storicamente ha visto in sequenza bene tangibili come l'oro, banconote sostenute da quest'ultimo e infine banconote basate unicamente sulla fiducia, il tutto attraverso un'attenta supervisione delle banche che esercitano tutt'ora il controllo del denaro. A seguito di eventi e crisi passate che hanno scosso pesantemente l'ordine mondiale lasciando tutt'ora conseguenze, sono state inventate le criptovalute, un sistema di scambio peer to peer non tangibile e decentralizzato, governato direttamente dagli utenti, quindi caratterizzato dall' assenza di un'autorità centrale al controllo. Il percorso che sta accompagnando l'espansione della blockchain e delle criptovalute è spesso paragonato all'ascesa di internet, il quale ha portato ad un cambio radicale rivoluzionando il modo di vedere la realtà. Lo scopo dell'elaborato è di fare chiarezza e aiutare a comprendere l'attuale sviluppo tecnologico digitale rivoluzionario che stiamo vivendo, con un riguardo al passato, al presente e alle potenzialità future.

Nel Primo Capitolo vengono approfonditi i concetti di innovazione e i relativi processi come introduzione per comprendere la fase ciclica attuale della tecnologia blockchain. Quest'ultima viene definita dettagliatamente attraverso un approfondimento riguardo le strutture, il loro funzionamento e le applicazioni possibili in diversi settori. In particolare, con riguardo al settore finanziario è spiegata in maniera esaustiva la finanza decentralizzata, le attività svolte all'interno, i benefici e rischi che comporta.

Il Secondo Capitolo è caratterizzato da un cenno all'evoluzione della moneta per arrivare a definire gli odierni tipi di asset digitali, sia dal punto di vista giuridico

che tecnico, e più in particolare il funzionamento e lo sviluppo delle Blockchain e le relative Criptovalute Bitcoin ed Ethereum.

Nel Terzo Capitolo sono considerate e approfondite le prospettive future riguardo le proposte attuali di regolamentazione non ancora in vigore e i potenziali pericoli per la stabilità economica causate dall'assenza di direttive chiare nei confronti di tali innovazioni.

CAPITOLO 1: L'Innovazione e la Tecnologia Blockchain

Le innovazioni si percepiscono inizialmente come incerte e rischiose. Per superare l'incertezza, la maggior parte delle persone cerca altri simili che hanno già adottato la nuova idea. Il processo di diffusione si sviluppa grazie agli individui che per primi adottano un'innovazione e diffondono la parola[1]

1.1 Principi di un Innovazione Tecnologica e la sua Diffusione

Un'idea, una pratica o un oggetto percepito come nuovo da un individuo o da un'altra unità di adozione che altera e sposta lo stato di equilibrio precedentemente esiste è definibile Innovazione[2]. Dall'intervallo di tempo che parte dal suo primo utilizzo o scoperta, la novità percepita determina per l'individuo la sua reazione ad essa è considerata come un'innovazione. La novità di un'innovazione non deve implicare solo nuove conoscenze, si potrebbe essere a conoscenza di un'innovazione da tempo, ma non è tuttavia scontato lo sviluppo di un atteggiamento favorevole o sfavorevole nei suoi confronti, né la volontà di adozione o di rifiuto. L'Aspetto novità di un'innovazione può essere quindi espresso in termini di conoscenza, persuasione e decisione da adottare. Spesso ci si chiede come i primi utilizzatori di innovazione differiscono dai successivi adottanti, oppure come gli attributi percepiti di un'innovazione, il suo vantaggio competitivo influenzino il suo tasso di adozione. Non si deve presumere che la diffusione e l'adozione di tutte le innovazioni siano necessariamente auspicabili. In effetti, ci sono alcuni studi su innovazioni dannose e antieconomiche che generalmente non sono desiderabili né per l'individuo né per il suo sistema sociale né per l'ambiente[3]. Inoltre, la stessa innovazione può essere desiderabile per un utilizzatore in una situazione ma controproducente per un altro potenziale adottante in una situazione diversa. Far adottare una nuova idea, anche quando presenta evidenti vantaggi, è spesso molto difficile perché spesso è presente un ampio divario tra ciò che è noto e ciò che è effettivamente utilizzato. Molte innovazioni richiedono un periodo

[1] **Rogers Everett M.** Diffusion of Innovation, The Free Press. 2003.
[2] **Shumpeter Joseph Alois** Teoria dello sviluppo economico, Sansoni. 1971.
[3] **Rinnovabili.it** Nuove tecnologie:a Yale si studiano gli effetti indesiderati, Rinnovabili.it. 2020. https://www.rinnovabili.it/innovazione/nuove-tecnologie-impatti-ambientali-yale/

molto lungo, spesso alcuni anni, dal momento in cui diventano disponibili al momento in cui vengono ampiamente adottate[4]. Pertanto, un problema comune a molti individui e organizzazioni è come accelerare il tasso di diffusione di un'innovazione in modo da renderla disponibile e comprensibile a tutti. Ci sono infatti diverse difficoltà comuni che devono affrontare i programmi di diffusione. "La diffusione è un processo mediante il quale un innovazione è comunicato attraverso determinati canali nel tempo tra i membri di un sistema sociale"[5]

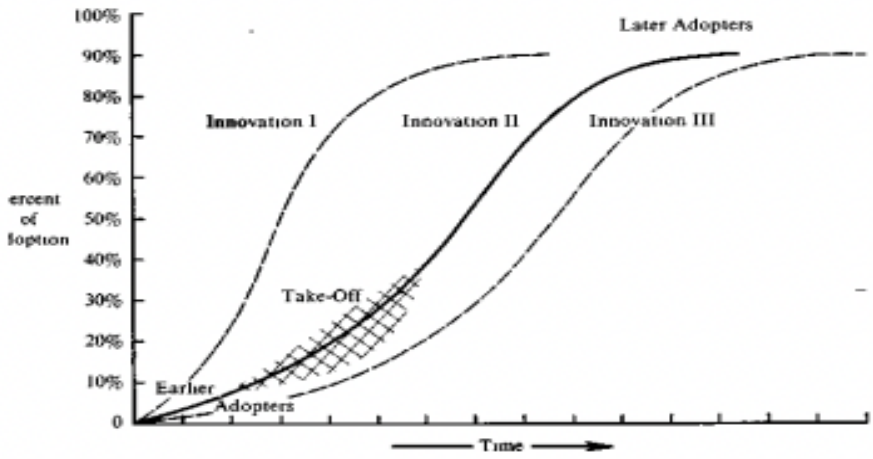


Figura: Processo di diffusione nella quale un'innovazione è comunicata attraverso determinati canali nel tempo attraverso alcuni membri del sistema sociale.

Pertanto, possiamo definire quattro elementi principali di un'innovazione tra i quali l'innovazione, i canali di comunicazione, il tempo e il sistema sociale[6]. Attraverso la comunicazione i partecipanti creano e condividono informazioni tra loro al fine di raggiungere una comprensione reciproca. Tale evento è solo una parte di un processo totale in cui le informazioni vengono scambiate tra gli individui. La diffusione è di fatto una comunicazione speciale, cui il contenuto presenta una novità e quest'ultima suggerisce il coinvolgimento di un certo grado di incertezza. Quest'ultima caratterizza significativamente l'avvento dell'innovazione e il grado in cui sono presenti un certo numero di alternative percepite rispetto al verificarsi di un evento relativo alla probabilità di queste alternative. Questa caratteristica

[4] **Cavicchioli Marco** La storia del Bitcoin, Cryptonomist. 2022, https://cryptonomist.ch/2022/05/15/storia-bitcoin-2/
[5] **Rogers Everett M.** Diffusion of Innovation. Cit. Pag. 12
[6] **Rogers Everett M.** Diffusion of Innovation. Cit. Pag. 10

implica una mancanza di prevedibilità, di struttura e di informazioni. L'informazione che rappresenta uno dei principali mezzi per ridurre l'incertezza può essere considerata come una "differenza di materia-energia che influisce sull'incertezza in una situazione in cui esiste una scelta tra un insieme di alternative"[7]. L'informazione e l'incertezza sono concetti chiave che ci aiutano a comprendere la diffusione delle innovazioni tecnologiche come un tipo di processo di comunicazione che porta ad un tipo di cambiamento, definito come il processo mediante il quale si verifica un'alterazione nella struttura e nella funzione di un sistema sociale. Quando nuove idee vengono inventate, diffuse e adottate o respinte, portano a determinate conseguenze, si possono verificare veri e propri cambiamenti in campo sociale. Esistono distinzioni in materia di diffusione, tra i quali troviamo il sistema di diffusione centralizzato e il sistema di diffusione decentralizzato[8].

In un sistema di diffusione centralizzato: le decisioni sul come, quando iniziare a diffondere un'innovazione, chi dovrebbe valutarla e attraverso quali canali sarà diffusa, sono prese da un piccolo numero di persone denominati funzionari o esperti a capo di un'agenzia di cambiamento.

In un sistema di diffusione decentralizzato: le decisioni sono maggiormente condivise da clienti e i potenziali adottanti. In questo caso le reti orizzontali tra i clienti sono il principale meccanismo attraverso il quale si diffondono le innovazioni. In questo sistema potrebbe non esserci bisogno di alcuna agenzia di cambiamento, i potenziali adottanti sono gli unici responsabili dell'autogestione della diffusione delle innovazioni in modo tale che nuove idee possano nascere dall'esperienza pratica di alcuni individui nel sistema cliente, piuttosto che provenire da attività formali di ricerca e sviluppo.

Per quanto riguarda il tempo, storicamente, ogni tecnologia ha un determinato ciclo di vita, infatti, è bene considerare l'innovazione in termini di prodotto ma soprattutto come processo. La caratteristica evolutiva è da attribuire ad alcune caratteristiche specifiche del settore, come le caratteristiche nella sua struttura fino

7 **Rogers, Everett M. and Kincaid, D. Lawrence.** Communication Networks: Toward a new paradigm for Research. The Free Press. 1988. Pag. 63
8 **Rogers Everett M.** Diffusion of Innovation. Cit. Pag. 333

o quelle che sono le diverse possibilità e difficoltà nell'ottenere un vantaggio competitivo. Un tentativo di spiegazione del fenomeno dell'innovazione di prodotto in coevoluzione con l'innovazione di processo è stato preso in considerazione spiegato attraverso un modello[9] che permette di seguire il ciclo di vita di una determinata tecnologia. In base a tale modello si possono distinguere due cicli di vita differenti:

Nel ciclo di prodotto, un'impresa cerca in primis la massimizzazione delle prestazioni, che poi vede seguire la massimizzazione delle vendite fino ad arrivare all'ultima alla minimizzazione dei costi giovando di un mercato educato.

Nel ciclo del Processo si parte dalla produzione non coordinata, per raggiungere una fase segmentata dove si prova a ridurre i costi fronteggiando la domanda di mercato crescente ed infine, una volta che il mercato si è stabilizzato, specializzarsi delle singole parti del processo[10].

Analizzando meglio il percorso della tecnologia, nel momento in cui entra nella prima volta nel mercato grazie agli "Innovators" trova solo alcuni utenti denominati "Early Adopters" portando con sé un processo produttivo poco standardizzato. Una volta che il mercato ha apprezzato tale prodotto e la domanda è aumentata, al crescere della stessa, si notano ulteriori entranti denominati "Early Makority", "Late Majority" ed infine i "Laggards''[11].

---

[9] **Utterback James M and Abernathy William J** A Dynamic Model of Process And Product Innovation, Omega Journal, 1975.

[10] **Utterback James M and Abernathy William J** A Dynamic Model of Process And Product Innovation. Cit.

[11] Gli "**INNOVATORS**" sono classificabili come entusiasti che sperimentano e presentano forti competenze tecniche, si stima che ricoprano circa il 2,5% del mercato.
Gli "**EARLY ADOPTERS**" sono definiti come coloro che grazie al loro status e credibilità, cercano di ottenere un vantaggio competitivo usufruendo e introducendo l'innovazione creando di fatto un trend che influenzi altre persone, si stima siano circa il 13,5% del mercato.
Con il termine "**EARLY MAJORITY**" viene chiamata la fetta di mercato che rappresenta circa il 34%, cerano rassicurazioni riguardo la stabilità e i rischi che li convincano ad adottare il cambiamento.
Vengono chiamati "**LATE MAJORITY**" gli abitudinari e poco inclini al cambiamento che solitamente si palesano nel momento in cui l'innovazione non è più considerata come tale, rappresentano il 34% circa del mercato. Identificati come "**LAGGARDS**", gli scettici tradizionalisti che comprendono circa il 16% del mercato, sono estremamente restii al cambiamento.
Moore Geoffrey A. Crossing the chasm: Marketing and selling disruptive products to mainstream customers, Harper Business an imprint of HarperCollins Publishers. 2014.

Come dal seguente grafico possiamo distinguere 3 fasi dell'innovazione: la "Fluid Phase", la "Transitional Phase" e la "Specific Phase" in riferimento al modello.

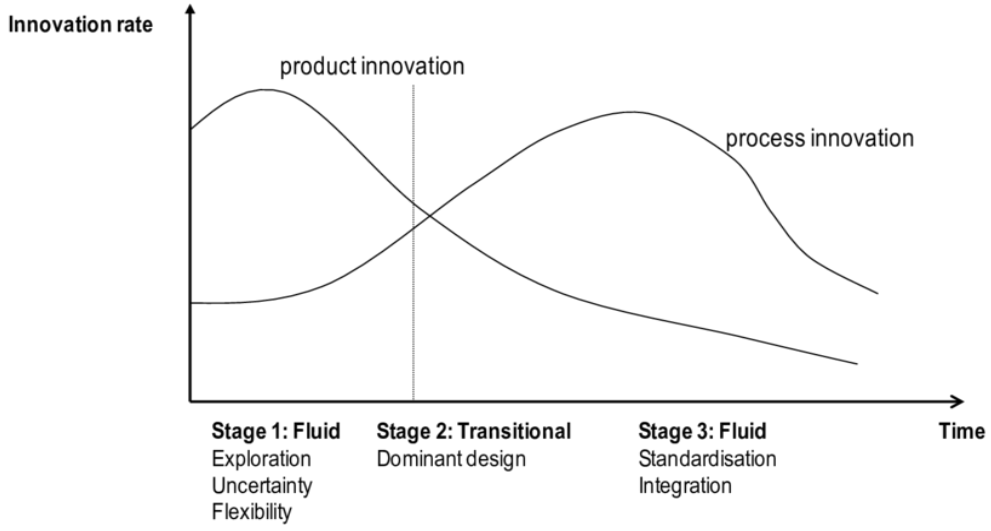


Figura: Rappresentazione Grafica dell'innovazione di prodotto e di processo caratterizzate da diverse fasi.

La **Fluid Phase** è guidata dalla massimizzazione delle performance, in quanto l'innovazione è considerata radicale poiché soddisfa un bisogno che il mercato non aveva mai espresso direttamente prima. Segue la **Transitional Phase** con massimizzazione delle vendite, si inizia a investire di più nelle tecnologie di processo che consentono la produzione su larga scala. Infine, la **Specific Phase**, caratterizzata dalla minimizzazione dei costi, ovvero dalla riduzione dell'investimento nella tecnologia di processo e di prodotto e la concentrazione verso l'offerta di più servizi e acquisizione di altre imprese cercando di far ripartire il ciclo tecnologico sperimentando nuove soluzioni non ancora esplicitate al mercato. È fondamentale considerare queste fasi perché una determinata combinazione di prodotto e processo vincente può portare alla soluzione architetturale che stabilisce un unico punto di riferimento per una classe di prodotto o processo.

1.2 Introduzione alla Blockchain

Nata da ormai 13 anni, la tecnologia blockchain rappresenta ad oggi un paradigma e modello di piattaforma la cui innovazione permette di dare nuove forme di interpretazione a tanti e diversi bisogni di imprese, organizzazioni e consumatori. Per diversi anni la Blockchain è stata sotto osservazione prevalente del mondo degli sviluppatori o per altri versi a coloro che avevano intravisto le potenzialità dal punto di vista finanziario, ma ad oggi si sta assistendo ad un importante salto di qualità in termini di diffusione della conoscenza di aspettative e di incentivi[12]. La blockchain sta entrando come è già accaduto in passato per internet, gradualmente nelle nostre vite, sottoforma di piattaforme che risolvono in un modo più moderno ed innovativo i nostri bisogni, quello delle imprese e delle pubbliche amministrazioni che erogano i servizi che utilizziamo tutti i giorni. Secondo Gartner[13] è possibile rendersi conto che tra il 2020 e il 2030 assisteremo con alle due fasi maggiormente profittevoli del ciclo di vita di un'innovazione tecnologica con riferimento alla Campana di Rogers[14] toccando di fatto la parte più alta della curva.

[12] **Ministero dello Sviluppo Economico** Blockchain e intelligenza artificiale: incentivi per imprese ed enti di ricerca. 2022, https://www.mise.gov.it/index.php/it/notizie-stampa/blockchain-e-intelligenza-artificiale-incentivi-per-imprese-ed-enti-di-ricerca.

[13] **Gartner** è una società per azioni multinazionale che si occupa di ricerca, consulenza strategica e analisi nel campo della tecnologia, https://www.gartner.com/en

[14] **La Campana di Rogers**, meglio nota come "Curva di adozione dell'innovazione" è un modello ideato da Everett M. Rogers per illustrare il modo in cui l'innovazione viene adottata dai differenti individui in un sistema sociale, https://www.insidemarketing.it/glossario/definizione/curva-di-rogers/

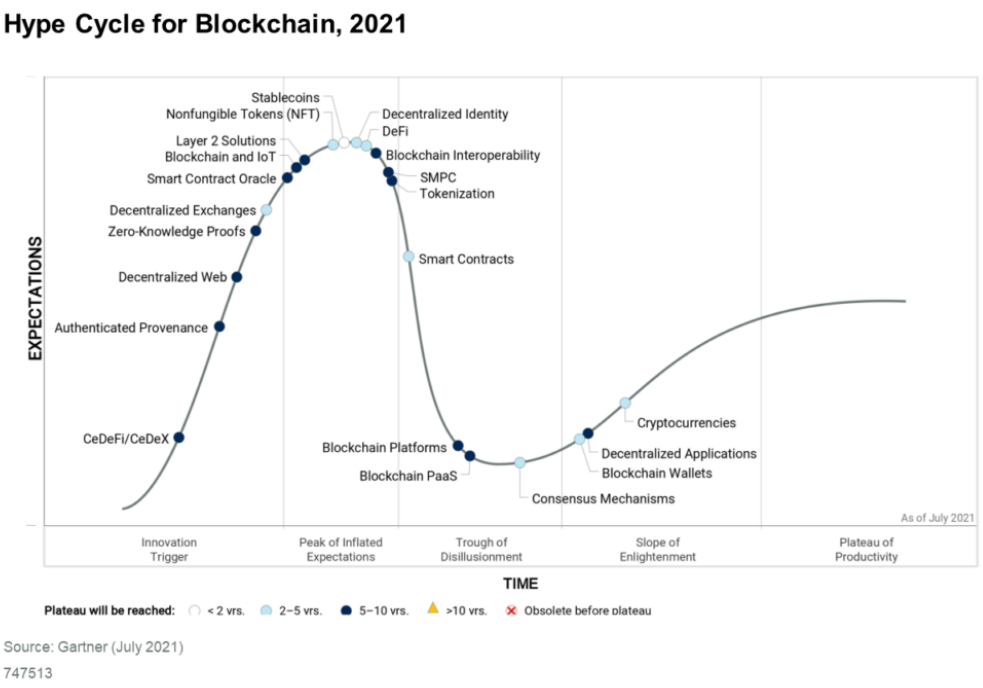


Figura: Previsione delle fasi della tecnologia emergente Blockchain stilato secondo la società Gartner.

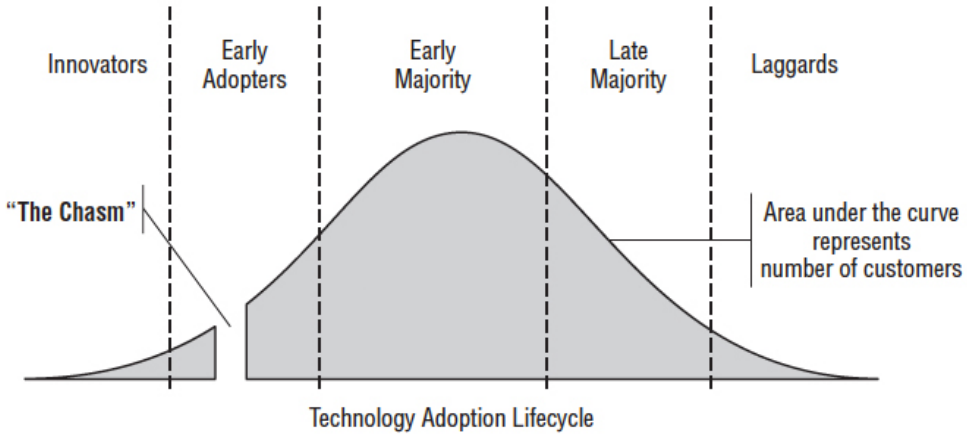


Figura: Curva di Rogers

Nell'arco del prossimo decennio è molto probabile che la blockchain raggiungerà lo stadio di maturità consentendole un'ampia adozione, se non capillare all'interno di numerosi settori. "Le ricompense per l'implementazione delle applicazioni blockchain nelle aziende sono semplicemente troppo alte per essere ignorate e sono

di gran lunga superiori ai costi"[15]. A differenza di altre innovazioni tecnologiche la Blockchain fa riferimento ad alcuni temi e concetti apparentemente molto diversi e lontani tra loro, che normalmente non associamo all'innovazione digitale come ad esempio: La fiducia, la responsabilità, la comunità e la decentralizzazione. In più accanto a questi ce ne sono altri che hanno una forte relazione con la tecnologia, ma che a loro volta non sono molto considerati e spesso trascurati come il tema della trasparenza, dell'immutabilità, della condivisione e della competizione nel raggiungimento di un risultato. La blockchain ha l'originalità come uno dei suoi ingredienti principali, il quale giustifica il tanto interesse e le tante aspettative. Questa tecnologia può essere letta e presentata da diversi punti di vista e prospettive, ne saranno esposte diverse affinché la si comprenda nella sua completezza ed essenza.

1.3 Distribuited Ledger Technology

Al fine di spiegare al meglio l'essenza della Blockchain, introduciamo il termine delle DLT, Distribuited Ledger Technology, una tecnologia che consente la registrazione e la conservazione di dati attraverso archivi multipli denominati "ledger" che può essere definito un registro distribuito, ovvero un sistema digitale per la registrazione di informazioni e dati correlati ognuno dei quali sono conservati e controllati da una rete di computer chiamati "Nodi". La Blockchain è la realizzazione della DLT, come evoluzione del Centralized Ledger e del Decentralized Ledger sino al Distributed Ledger.

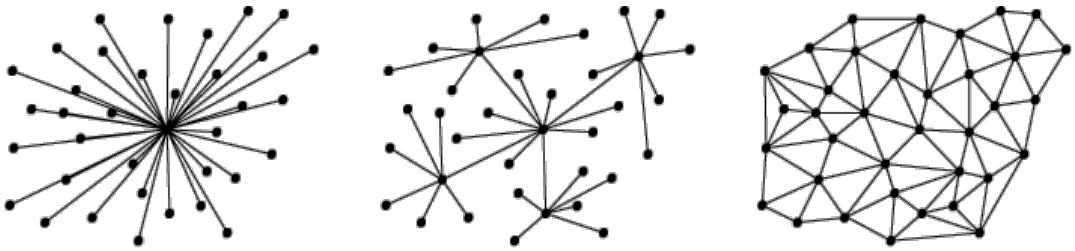
Il **Centralized Ledger** approccia una logica centralizzata, dove tutto deve essere gestito facendo riferimento ad una struttura**,** autorità o sistema centralizzato. "Nel registro centralizzato la fiducia è nell'autorità, nell'autorevolezza del soggetto o sistema che rappresenta il centro e che risulta a capo dell'organizzazione"[16].

[15] **Litan Avivah** Hype cycle for blockchain 2021; More Action than Hype, Gartner Blog Web. 2021, https://blogs.gartner.com/avivah-litan/2021/07/14/hype-cycle-for-blockchain-2021-more-action-than-hype/.

[16] **Bellini Mauro** Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia. Blockchain4innovation. 2022, https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/.

Nel **Decentralized Ledger** troviamo invece una struttura di centralizzazione su base locale con dei satelliti organizzati che si relazionano a loro volta. In questo caso non c'è più un solo soggetto centrale bensì tanti soggetti centrali locali. "La fiducia nel caso delle Decentralized Ledger è delegata ad un soggetto centrale, ma in questo caso il più vicino"[17]. Le organizzazioni basate su Decentralized Ledger definiscono inoltre una governance che stabilisce delle forme di coordinamento di tipo centralizzato.

Il vero cambiamento è rappresentato dal **Distributed Ledger** dove non esiste più nessun centro e dove la logica di governance è strutturata attorno ad un nuovo concetto di fiducia reciproco fra tutti i soggetti dove nessuno ha la possibilità di prevalere e il processo decisionale passa rigorosamente attraverso un processo di costruzione del consenso comune.



Centralized **Decentralized** **Distribuited**

Figura: Rappresentazione grafica di Centralized, Decentralized e Distribuited Ledger

Sul piano giuridico l'Italia ha disciplinato le Tecnologie basate su registri distribuiti e Smart Contract meglio conosciute come "Distribuited Ledger Technology"[18], si definiscono infatti "Tecnologie basate su registi distribuiti, le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia

[17] **Bellini Mauro** Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia. Blockchain4innovation. 2022, Cit.
[18] Denominate anche "DLT".

verificabili da ciascun partecipante, non alterabili e non modificabili e che la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui l'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 Luglio 2014"[19]. Il Parlamento Europeo, in riferimento al tema valute virtuali[20], osserva come le tecnologie basate su DLT possono potenzialmente accelerare, decentrare, automatizzare e standardizzare dei processi basati sui dati ad un costo molto ridotto modificando di fatto le modalità di trasferimento delle attività e di tenuta dei registri in maniera più efficace, con conseguenze positive per il settore sia privato che pubblico coinvolgendo allo stesso tempo il prestatore di servizi, il supervisore e il legislatore. A rafforzare ciò, sempre il Parlamento Europeo, attraverso una "Risoluzione Sul Fintech"[21] ha espressamente chiamato in causa la Commissione europea a elaborare un piano d'azione globale in materia fintech che potesse contribuire a un sistema finanziario Europeo efficiente e competitivo.

1.3.1 Definizione di Blockchain e Casi d'uso

La Blockchain è definita come registro distribuito, decentrato e crittografato. "L'algoritmo"[22] che ne è alla base ha la funzione di tenere traccia di ogni singola transazione avvenuta all'interno del suo network. Infatti, il registro distribuito non è altro che un database da cui esistono tante copie, ognuna delle quali viene conservata in un nodo della rete. Il nome Blockchain deriva dal fatto che questo è un database suddiviso in blocchi, formando quindi una catena di blocchi a mano a mano che questi vengono creati. Tali blocchi devono essere riempiti di informazioni sottoforma di "Kb"[23] e ad intervalli di tempo vengono validati prima di chiudersi e

[19] *legge n. 12/2019 di conversione del decreto semplificazioni, D.L. n. 135/2018, Art. 8 Ter*

[20] **Parlamento Europeo** Risoluzione del Parlamento europeo del 26 maggio 2016 sulle valute virtuali (2016/2007(INI)). 2016, https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_IT.html

[21] **Parlamento Europeo** Risoluzione del Parlamento europeo del 17 maggio 2017 sulla tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario (2016/2243(INI)). 2017, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0211_IT.html

[22] Un **Algoritmo** è una strategia atta alla risoluzione di un problema, costituita da una sequenza finita di istruzioni, è un concetto cardine nella fase di programmazione dello sviluppo di un software, https://www.treccani.it/enciclopedia/algoritmo

[23] Kilobyte (**Kb**) è un unità di misura informatica del sistema internazionale, https://www.wikibit.it/k/cosa-significa-kb-kilobyte-563/

poter passare al blocco seguente. Più precisamente, nei blocchi saranno immessi dati relativi ad ogni transazione avvenuta in quel lasso di tempo, più altri dati di intestazione che garantiscono la continuità e preserva la sicurezza, poiché descrive il blocco in corso e quello precedente. Questo processo fa in modo che per modificare un solo blocco sia necessario modificare anche tutti quelli precedenti, rendendo di fatto l'operazione molto complessa. Poiché si tratta di una tecnologia distribuita e decentralizzata, non avremo mai un solo controllore, ma tanti quanti sono i nodi. Il risultato finale è un sistema aperto, neutrale, affidabile e sicuro, dove la nostra capacità di utilizzare e di avere fiducia nel sistema non dipendono dalle intenzioni di nessuno singolo individuo o singola istituzione. La blockchain può strutturare un'infrastruttura di pagamento, un sistema di monitoraggio della supply chain o di un gestore di identità digitale, ma è molto più di questo. Questa tecnologia ha le potenzialità per portare un nuovo livello di fiducia nelle applicazioni, introducendo un cambio di paradigma nelle modalità con cui esse vengono realizzate e dandoci l'opportunità di innovare liberamente. "La struttura soddisfa principalmente i concetti di decentralizzazione, la trasparenza e la tracciabilità, la sicurezza, l'immutabilità del registro, il consenso e la programmabilità"[24]. Sulla base di tali principi tale tecnologia potrebbe essere utilizzata come uno strumento di estrema fiducia che possa assumere un ruolo fondamentale che consenta lo sviluppo e la concretizzazione anche di una nuova forma di rapporto sociale, che grazie alla partecipazione di tutti sia in grado di garantire la possibilità di verificare, controllare e disporre di una totale trasparenza sugli atti e sulle decisioni, che vengono registrati in archivi che hanno la caratteristica di essere inalterabili, immodificabili ma soprattutto immuni da corruzione. Attualmente non è stata ancora coniata una vera e propria definizione universale di blockchain, pertanto è definita di volta in volta in base alle sue caratteristiche e alle esigenze che riesce a soddisfare. Inizialmente la blockchain è stata assimilata ai Bitcoin, in quanto la prima ad essere effettivamente rilevante, vista come un'innovazione nel mondo delle monete digitali, ma l'utilizzo di questa tecnologia come già accennato si può estendere a molte applicazioni. Ad esempio, le aziende di logistica utilizzano la

[24] **Bellini Mauro** Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia, Blockchain4innovation. 2022, Cit.

blockchain per tracciare le merci mentre si muovono attraverso la catena di approvvigionamento. Le Banche centrali del governo e la comunità finanziaria globale hanno testato e continuano a mettere alla tecnologia blockchain come base per lo scambio di valuta digitale, un esempio sono le Central Bank Digital Currencies[25]. Altri settori, tra cui la comunità legale e l'intrattenimento, stanno utilizzando la blockchain come base per gli Smart Contract[26] e altri meccanismi di trasferimento e protezioni dei diritti di proprietà intellettuale, sistema adottato recentemente da SIAE[27]. Come questi citati, molti settori stanno ora esplorando le applicazioni basate su blockchain come un modo sicuro ed economico per creare e gestire un database distribuito. Di conseguenza, la blockchain è sempre più vista come una soluzione per tracciare e condividere in modo sicuro anche i dati tra più entità aziendali.

1.3.2 Come funziona una Blockchain

Come detto la Blockchain è sostanzialmente una tecnologia di archiviazione progettata per rendere impossibile aggirare il sistema o falsificare i dati in esso archiviati, rendendolo così sicuro e immutabile. Ogni computer in una rete blockchain conserva una copia del registro per prevenire un singolo punto di errore e tutte le copie vengono aggiornate e convalidate contemporaneamente. La Blockchain differisce sostanzialmente dai database convenzionali nel modo in cui archivia e gestisce le informazioni. Invece di archiviare i dati in righe e colonne, tabelle e file come fanno i database tradizionali e archivia i dati in blocchi

[25] Per la Prima volta si è verificato un passaggio di monete digitali di banche centrali, le Central Bank Digital Currencies (**CBDC**), utilizzando una blockchain in pieno spirito bitcoin. Un Progetto ancora in fase di studio e valutazione da parte della Banca Centrale Europea per l'emissione dell'Euro Digitale o Il Dollaro digitale da parte della Federal Reserve, **Sgroi Maurizio** Così le banche centrali fanno prove generali di blockchain, Sole24Ore, 2021, https://www.econopoly.ilsole24ore.com/2021/10/06/banche-centrali-blockchain/

[26] **Smart Contract**, innovativi strumenti di automazioni che combinano protocolli informatici con le interfacce utente per formalizzare e rendere sicuri accordi tra le parti. **Intesa** Cosa sono gli smart contracts? Intesa. 2022, https://www.intesa.it/cosa-sono-gli-smart-contract-e-quali-sono-le-loro-applicazioni-pratiche/.

[27] La Società Italiana Degli Autori e Editori (**SIAE**), ha annunciato una partnership con una blockchain che i propri diritti di autore saranno rappresentati come asset digitali sulla DLT, abbracciando le opportunità offerte dalla tecnologia per proseguire la sua missione di protezione della creatività, **SIAE** Siae rappresenta i diritti degli autori con asset digitali: creati più di 4.000.000 di nft sull'infrastruttura blockchain di algorand. 2021, https://www.siae.it/it/iniziative-e-news/siae-rappresenta-i-diritti-degli-autori-con-asset-digitali-creati-pi%C3%B9-di-4000000.

concatenati digitalmente insieme. Più tecnicamente, una blockchain è gestita da computer appartenenti a una rete peer – to – peer anziché da un computer centrale come nei database tradizionali. Essa funziona infatti attraverso un processo multifase, che avviene come segue:

Un Partecipante autorizzato inserisce una transazione che deve essere autenticata dalla tecnologia, tale azione crea un blocco che rappresenta quella transazione o dati specifici, Il blocco viene inviato a ogni nodo di computer nella rete, I nodi autorizzati verificano la transazione e aggiungono il blocco nella blockchain esistente, l'aggiornamento viene distribuito sulla rete che finalizza la transazione.

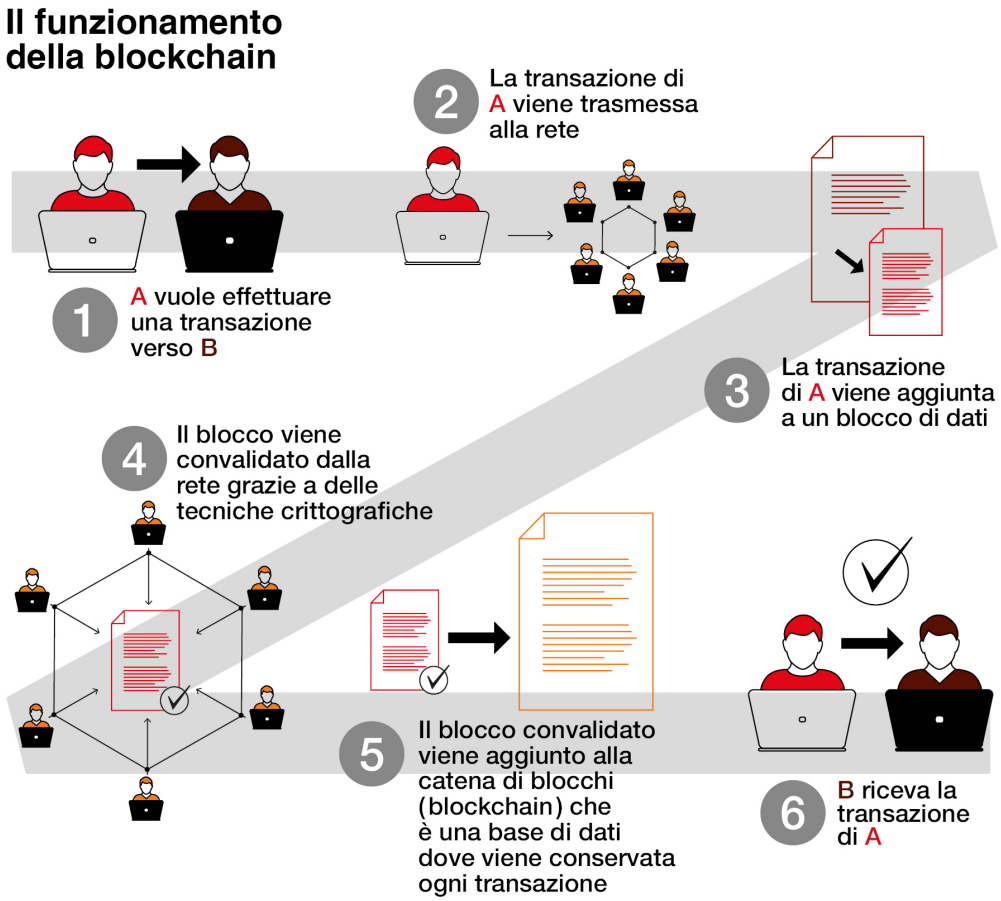


Figura: Processo di una transazione che avviene su una semplice Blockchain

Un registro semplice basato su blockchain è costituito da due tipi di record, singole transazioni e blocchi. Il primo blocco è costituito da un'intestazione e da dati relativi alle transazioni che avvengono entro un determinato periodo di tempo. Il

"Timestamp"[28] del blocco viene utilizzato per creare una stringa alfanumerica denominata "hash"[29]. Dopo che il primo blocco è stato creato, ogni blocco successivo nel libro mastro utilizza l'hash del blocco precedente per calcolare il proprio hash. Prima che un nuovo blocco possa essere aggiunto alla catena, la sua autenticità deve essere verificata mediante un processo computazionale chiamato validazione o consenso. A questo punto del processo blockchain, la maggior parte dei nodi della rete deve concordare che l'hash del nuovo blocco è stato calcolato correttamente. Il meccanismo di consenso garantisce che tutte le copie del libro mastro distribuito blockchain condividano lo stesso stato. Una volta che un blocco è stato aggiunto, può essere referenziato nei blocchi successivi, ma non può essere modificato. Se qualcuno tenta di sostituire un blocco, anche gli hash per i blocchi precedenti e successivi cambieranno e interromperanno lo stato condiviso del libro mastro. Quando il consenso non è più possibile, gli altri computer nella rete sono consapevoli che si è verificato un problema e non verranno aggiunti nuovi blocchi alla catena fino a quando il problema non sarà risolto. In genere, il blocco che causa l'errore verrà eliminato e il processo di consenso verrà ripetuto. Esistono di fatto diversi tipi di blockchain e sono classificate in base al fatto di essere pubbliche, cioè aperte o private, cioè chiuse.

1.3.3 Blockchain permissioned (Private)

La Blockchain Privata funziona su una rete chiusa e spesso centralizzata, dove l'autorizzazione a registrare le informazioni sui blocchi è quindi controllata da una singola entità o organizzazione. Ha la stessa architettura di decentralizzazione e peer-to-peer della blockchain pubblica ma su scala minore, il che aumenta le prestazioni rendendo di contro la fiducia più scarsa e debole rispetto a una blockchain aperta, questo perché è il nodo primario, o proprietario a prendere le decisioni. Quest'ultimo può introdurre a proprio piacimento policies o censurare la transazione restringendo l'uso della blockchain a sviluppatori e utilizzatori finali, i

[28] **Timestamp** è il termine con cui si fa riferimento ad un piccolo dato memorizzato in ogni blocco come seriale univoco e la cui funzione principale è determinare il momento esatto in cui il blocco è stato estratto e convalidato dalla rete, https://academy.bit2me.com/it/timestamp-blockchain/

[29] L'**Hash** è concetto fondamentale della crittografia e della struttura di una blockchain, tecnicamente è una funzione che da un input di una lunghezza arbitraria deriva una stringa di lunghezza predefinita, https://www.borsaitaliana.it/borsa/glossario/hash.html

quali possono fare affidamento unicamente sull'interfaccia fornita dagli operatori della blockchain per leggere e inviare transazioni. Anche la sicurezza più debole perché è più facile per un numero limitato di nodi dominare un meccanismo di consenso per convalidare le transazioni. "Le catene private sono più adatte a contesti aziendali, in cui un organizzazione vuole sfruttare la proprietà della blockchain senza rendere il proprio network accessibile all'esterno"[30]. rispetto alle blockchain di tipo permissionless oltre al fatto che si adeguano meglio alle strutture legislativa in corso. La maggior parte delle prime implementazioni blockchain di alto profilo sono su blockchain private. Il fattore umano rimarrà una vulnerabilità nelle blockchain private fino a quando non si riuscirà a ridurlo al minimo possibile e la condizione di difficile consultazione, questa caratteristica le rende infatti scarsamente accessibili a persone esterne al progetto, il set di nodi limitato infatti potrebbe suscitare preoccupazioni in quanto l'autenticazione dei valicatori introduce vulnerabilità nel sistema lasciando ampia possibilità di corruzione e manipolazione, mentre nel caso di permissionless blockchain, il processo di validazione è per natura neutra ed equidistante.

1.3.4 Blockchain permissionless (Pubblica)

La Blockchain pubblica, l'esempio più famoso è rappresentato da Bitcoin, non richiede l'autorizzazione per partecipare ed è trasparente e accessibile a chiunque vi partecipi, sono "aperte e non hanno proprietà"[31]. Non ci sono infatti restrizioni sulla consultazione degli scambi, la loro effettuazione e la possibilità di partecipare al meccanismo di consenso. È un ottimo ambiente di sviluppo per i ricercatori informatici, rendendo di fatto la blockchain supervisionata costantemente contrastando quelli che potrebbero essere problemi che potrebbero comprometterne la sicurezza. Questo diventa addirittura un incentivo, poiché molto spesso gli utilizzatori hanno un guadagno immediato nello scoprire le varie vulnerabilità e potendo sfruttare gli eventuali bug lucrandoci. Questo è inoltre il tipo di blockchain

[30] **Binance** Blockchain private, pubbliche e consorzi – qual è la differenza? Binance Accademy. 2021, https://academy.binance.com/it/articles/private-public-and-consortium-blockchains-whats-the-difference#private-blockchains.

[31] **Bellini Mauro** Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia. Blockchain4innovation. 2022, Cit.

in cui è spesso presente una Criptovaluta[32], dal modello permissionless è stata infatti realizzata la blockchain Bitcoin. È più lenta rispetto alla Blockchain Privata, questo perché per aprire il processo di consenso della blockchain a cosi tanti partecipanti rendere la verifica dei dati più elaborata, guadagnandoci in termini di sicurezza e da la possibilità ai partecipanti, gli utenti finali e sviluppatori di entrare e uscire dal protocollo in maniera semplice in quanto non sono presenti policies restrittive.

1.3.5 Blockchain Ibrida e Del consorzio

Combina gli aspetti delle blockchain pubbliche e private. Le organizzazioni possono usarlo per segmentare alcuni dati e transazioni dietro uno schema di autorizzazione mantenendo le connessioni al lato pubblico. I rischi per la sicurezza della blockchain e i problemi di integrità dei dati della blockchain privata sono mitigati non consentendo al proprietario di modificare le transazioni e le prestazioni tendono ad essere migliori di quelle di una blockchain pubblica. Gli utenti che si uniscono a una blockchain ibrida hanno privacy fino a quando non effettuano una transazione. La Blockchain del consorzio è molto simile alla blockchain privata, ma è controllata da un gruppo anziché da una singola entità. C'è meno vulnerabilità di sicurezza rispetto a quella tipica della blockchain privata, sebbene un nodo sia responsabile della convalida delle transazioni. "Questo tipo di blockchain è il più adatto in un contesto in cui le organizzazioni operano nello stesso settore e necessitano di un piano comune su cui eseguire le transazioni o tramettere informazioni sul settore con gli altri operatori"[33].

1.3.6 Vantaggi e Svantaggi della Blockchain

I principali **vantaggi** sono l'impossibilità o quasi di corrompere una blockchain, questo perché le informazioni sono condivise e continuamente riconciliate da migliaia e milioni, di computer. "Le transazioni possono essere più efficienti e

[32] Il termine **Criptovaluta** è una risorsa digitale che consente alle persone di effettuare transazioni tra loro poiché potrebbe essere utilizzata come mezzo di scambio. Inoltre, i proprietari di criptovalute archiviano le proprie risorse in un registro distribuito in un sistema di rete decentralizzata che registra le transazioni di vari utenti. **Aysan A.F., Demirtaş H.B. e Saraç M.** The Ascent of Bitcoin: Bibliometric Analysis of Bitcoin Research. Journal of Risk and Financial Management. 2021, https://doi.org/10.3390/jrfm14090427

[33] **Binance** Blockchain private, pubbliche e consorzi – qual è la differenza? Binance Accademy.2021, Cit.

meno costose rispetto ai sistemi transazionali non basati sulla DLT sebbene le blockchain, soprattutto quelle pubbliche possano soffrire di lentezza e inefficienza"[34]. È resiliente, ovvero non ci sono problemi se un nodo si interrompe perché tutti gli altri nodi hanno una copia nel libro mastro che mantiene la fiducia tra i partecipanti della rete. I blocchi confermati sono molto difficili da invertire, il che significa che i dati sono difficili da rimuovere o modificare. Può essere conveniente perché spesso riduce le spese associate alle transazioni eliminando intermediari e terze parti.

Per quanto riguarda gli **svantaggi**, soprattutto nelle blockchain pubbliche, ci sono domande sulla proprietà e su chi e responsabile quando insorgono problemi, ci sono dubbi sul fatto che le organizzazioni siano in grado o disposte a investire nell'infrastruttura necessaria per costruire, partecipare e mantenere una rete basata su blockchain, la modifica dei dati in una blockchain in genere richiede molto lavoro. Gli utenti devono tenere traccia delle proprie chiavi private per evitare di perdere i propri soldi. Lo spazio di archiviazione può crescere fino a diventare molto grande nel tempo, il che rischia la perdita di nodi se il libro mastro diventa troppo grande per essere scaricato dagli utenti.

Al centro dell'argomento blockchain è il trilemma relativo ai principi fondamentali della tecnologia ossia sicurezza, scalabilità e decentralizzazione. Il trilemma afferma che tutte le blockchain possono svolgere al meglio solo due delle caratteristiche appena citatate, trascurando di fatto l'altra che presenta spesso inefficienze. Per quanto riguarda Bitcoin, ad esempio, prevale la sicurezza e la decentralizzazione ma di contro è lenta a processare un elevato numero di transazioni. Si è pensato di risolvere questo disequilibrio portando direttamente fuori separando dalla blockchain principale la soluzione. Dei sistemi sono già in corso d'opera con lo sviluppo di protocolli come "Lighting Network"[35], un "layer

[34] **Pratt Mary K. e Gillis Alexander S.** TechTarget. Blockchain for businesses: The ultimate enterprise guide. 2021, https://www.techtarget.com/searchcio/definition/blockchain.

[35] **Lighting Network** (LN) è la soluzione che permette a Bitcoin di elaborare un maggior numero di transazioni senza sacrificare sicurezza e decentralizzazione, le transazioni infatti grazie a LN avvengono off-chain, quindi non registrate direttamente sulla blockchain, a parte la prima e l'ultima che servono come certifica del saldo per tutte le altre. **Guazzo Gianmarco** Bitcoin e trilemma della

2" [36] di Bitcoin che permette transazioni istantanee con a costi bassi, aumentando di fatto la scalabilità senza dover sacrificare la decentralizzazione e la sicurezza.

1.3.7 Smart Contract

La tecnologia blockchain oltre a registrare semplici dati come data, ora e i dettagli delle transazioni, possono anche ricoprire un ruolo più attivo. Incorporando un codice più complesso al auo interno, le transazioni possono essere eseguire in maniera automatica quando si verificano determinate condizioni. Ciò avviene mediante l'utilizzo di Smart Contract, "mezzi con cui gli sviluppatori, imprenditori, avvocati possono scrivere logiche personalizzate sottoforma di algoritmi che godono delle caratteristiche della Blockchain, ovvero l'immutabilità e la distribuzione causando di fatto l'automatica e irreversibile esecuzione delle clausole contrattuali trasposte in linguaggio informatico"[37]. Si definisce Smart Contract "un programma per elaboratore che opera su tecnologie basate su registri distribuiti la cui esecuzione vincola automaticamente duo o più parti sulla base di effetti predefiniti dalle stesse"[38]. Gli Smart Contact a esecuzione automatica, basati su questa funzionalità, sono ad oggi utilizzati in diversi progetti e in continuo sviluppo. Semplicemente i termini di un accordo tra due o più parti sono programmati sotto forma di codice informatico, un insieme di istruzioni che viene memorizzato in una blockchain. Quando sono soddisfatte le condizioni specifiche descritte accuratamente nel codice, vengono automaticamente avviate specifiche azioni, anch'esse definite precedentemente nel codice. Ad esempio, la richiesta di consegna di un prodotto potrebbe attivare un'istruzione di effettuare un pagamento. A sua volta, tale istruzione potrebbe potenzialmente attivare altre linee guida presenti in altri smart contract. Per rendere possibile la loro operatività, gli smart

---

blockchain: cosa è e possibile soluzione. Investire.biz. 2020, https://investire.biz/articoli/analisi-previsioni-ricerche/bitcoin-e-criptovalute/criptovalute-bitcoin-trilemma-blockchain-cosa-funzionamento-soluzione-lightning-network.

[36] I **Layer 2** sono protocolli che consentono di migliorare notevolmente le performance dei layer 1 (Bitcoin, Ethereum ecc..) agendo come uno strato aggiuntivo che diminuisce il carico di lavoro allo strato principale, **The Crypto Gateway** Layer 0, layer 1 e layer 2: che cosa sono? TheCryptoGateway. 2022, https://thecryptogateway.it/layer-0-layer-1-layer-2/.

[37] **Boucher Philip** Come la tecnologia blockchain può cambiarci la vita. 2017, https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_IT.pdf.

[38] *Art.8-ter co. 2 D.L. 135/2018*

contract si servono di "oracoli"[39] che sono il principale driver di informazione al di fuori della blockchain, fornendo gli input all'interno. Molte applicazioni nel prossimo futuro interessano soprattutto il settore finanziario, come ad esempio i prestiti e i prodotti assicurativi che richiedono ingenti risorse manuali suscettibili di automatizzazione. Questi tipi di contratti possono rientrare in una miriade di applicazioni snellendo procedure ad oggi molto lente snellendo lunghe pratiche burocratiche. La blockchain Ethereum è una delle prime ad aver implementato un linguaggio di programmazione e una valuta propri, configurati specificamente per supportare gli smart contract, è infatti definita "Blockchain con un linguaggio di programmazione completo Turing integrato che può essere utilizzato per creare contratti che possono essere utilizzate per codificare funzioni arbitrarie di transazione di stato, [..] semplicemente scrivendo la logica in poche righe di codice"[40]. Ad oggi, la configurazione degli smart contract richiede un certo dispendio iniziale in termini di energie e spese che li rende più indicati per accordi di tipo ripetitivo piuttosto che per contratti una tantum. Data la loro natura molto specifica, non sono particolarmente indicati per situazioni soggette a cambiamenti sostanziali durante il periodo contrattuale. "Visto il livello di incertezza giuridica sarebbe in effetti prudente limitarne l'uso a relazioni e accordi relativamente consensuali che difficilmente daranno adito a controversie tra le parti"[41]. In effetti derivano da processi digitali e sono più efficienti quando le diverse condizioni e conseguenze delle clausole sono anch'esse di natura digitale e sono pertanto adatte per l'automazione relativo a questo ambiente. Riguardo ai potenziali impatti e sviluppi, poiché il libro mastro blockchain è immutabile, il codice concordato, quindi sostanzialmente un vero e proprio contratto concordato, può essere annullato o modificato solo nel rispetto dei termini già consentiti nel codice stesso. "I contratti tradizionali solitamente consentono di scegliere tra il pagamento di quanto dovuto

[39] Gli **Oracoli** sono servizi di terze parti che forniscono informazioni estere a Smart Contract, fungono da ponte tra la blockchain e il mondo esterno, **Binance** Gli Oracoli Blockchain Spiegati. Binance Accademy. 2020, https://academy.binance.com/it/articles/blockchain-oracles-explained.
[40] **Buterin Vitalik** Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2014, https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper__Buterin_2014.pdf.
[41] **Boucher Philip** Come la tecnologia blockchain può cambiarci la vita. Cit.

in base al contratto e la rescissione del contratto stesso con le conseguenze che ne derivano, tra cui anche azioni legali. Se invece il pagamento è automatizzato nel quadro di uno smart contract, tale scelta non è più possibile, la transazione viene eseguita automaticamente. Un'interpretazione radicale degli smart contract ridurrebbe il contratto al codice, riconoscendo di fatto il codice come la legge stessa: autonomo, auto-eseguibile e auto-applicabile"[42]. Questa posizione di si colloca effettivamente fuori dal controllo di strutture consolidate come per gli Stati nazionali e le altre giurisdizioni. Il codice in questo caso viene considerato come parte di legge e tutti gli errori o le vulnerabilità accidentali diventano parte del contratto. Sfruttare bug[43] per assumere il controllo di beni non sarebbe quindi considerato furto, poiché l'errore fa parte del codice. Di fatto i "contratti intelligenti possono essere sviluppati e implementati da persone malintenzionate pseudonime"[44]. L'obiettivo è collocare gli smart contract all'interno del più ampio ordinamento giuridico e come per i contratti cartacei imporre ulteriori requisiti e invalidare clausole sulla base dell'intenzione delle parti e del diritto nel suo complesso. Nonostante aumentino l'efficienza in diverse aree al momento "non sono strumenti in grado di sostituire una forma contrattuale tradizionale"[45]. Le Blockchain che includono un codice eseguibile presentano un ulteriore livello di complessità e azione il che significa la necessità di risorse per il mantenimento del sistema, che si traduce in costi più elevati, sia in termini monetari che energetici. Questo tipo di complessità, se associate all'ideologia del codice come legge potrebbe esporre infatti le blockchain a ulteriori vulnerabilità in termini di sicurezza. Nell'applicazione delle procedure giudiziarie tradizionali in materia smart contract potrebbero emergere nuove responsabilità dei governi, come l'arbitrato in caso di bug nel codice-contratto. Gli smart contract possono essere privi di flessibilità e incapaci di adattarsi a circostanze mutevoli o alle preferenze

[42] **Boucher Philip** Come la tecnologia blockchain può cambiarci la vita. Cit.
[43] Un'anomalia che porta il malfunzionamento di un software, tipicamente dovuto a un errore nella scrittura del codice.
[44] **Huang Yongfeng [et al.]** Smart Contract Security: A Software Lifecycle Prospective. IEEE, 2021, https://ieeexplore.ieee.org/document/8864988
[45] **Biscointi Avvocati** Smart Contract: opportunità, applicabilità e limiti giuridici. Biscointi Avvocati. 2022, https://www.studiobisconti.it/blog/smart-contract-opportunita-applicabilita-e-limiti-giuridici/.

delle parti, pertanto, per convertire i contratti in codice eseguibile, i programmatori dovrebbero assumersi maggiori responsabilità legali in termini di attuazione pratica. Questo tipo di circostanze impreviste richiedono un'interpretazione della corretta modalità di applicazione delle clausole contrattuali. "Il codice è semplicemente troppo rigido per consentire di determinare algoritmicamente tutti i contratti"[46]. Potrebbero rendersi necessarie modifiche del diritto contrattuale tradizionale per permettere l'evoluzione di queste tecnologie, in particolare per quanto riguarda le norme sulla tenuta della documentazione e altre per tenere conto della natura automatizzata e deterministica degli smart contract, così come la loro validità e applicabilità che al giorno d'oggi appare sempre più frequente[47].

1.3.8 La Finanza Decentralizzata (DeFi)

La Finanza Decentralizzata, comunemente conosciuta come DeFi, è un insieme di servizi finanziari open source, disponibili a tutti e trasparente, costruiti su una rete blockchain superiore attraverso l'uso degli smart contract che permettono lo scambio, il credito e il debito di criptovalute, il tutto senza intermediari e senza un server centrale che regga questo tipo di operazioni. Tra le piattaforme più importanti che permettono di usufruire di questi servizi troviamo Ethereum, dove gli utenti possono interagire facilmente attraverso applicazioni peer-to-peer e Decentralizzate (Dapps). Ethereum una piattaforma open-source globale e decentralizzata che ad oggi risulta come la Blockchain più utilizzata in ambito DeFi con "il più alto livello di denaro all'interno"[48] rispetto a tutte le altre Blockchain.

[46] **Boucher Philip** Come la tecnologia blockchain può cambiarci la vita. 2017, Cit.
[47] **Partz Helen** La banca centrale norvegese sceglie Ethereum per sviluppare la valuta digitale nazionale. Cointelegraph. 2022, https://it.cointelegraph.com/news/norwegian-central-bank-uses-ethereum-to-build-national-digital-currency

[48] Total Value Locked (TVL).

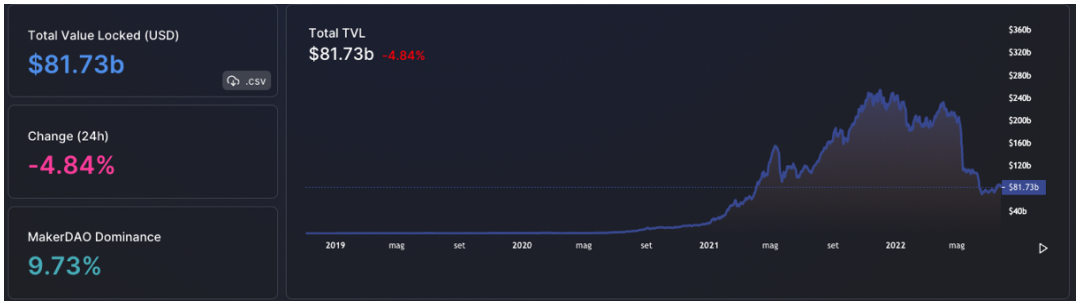


Figura: Rappresentazione Grafica del Total Value Locked in USD relativo alla somma di tutti i fondi presenti nei protocolli di Finanza Decentralizzata all'interno delle Blockchain esistenti.

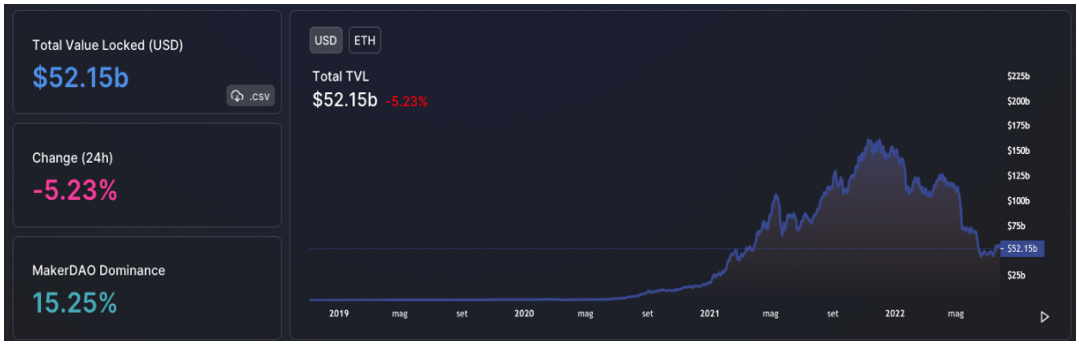


Figura: Rappresentazione Grafica del Total Value Locked in USD relativo unicamente ai fondi dei protocolli di Finanza Decentralizzata all'interno della Blockchain Ethereum.

Gli utenti possono connettersi a queste applicazioni decentralizzate attraverso un "wallet"[49] mantenendo il pieno controllo dei propri assets, tramite il proprio address e la chiave privata relativa, che non devono essere depositate sulla piattaforma, interagendo attraverso Dapp e Smart Contract. L'utilizzo della blockchain rende estremamente difficile che si verificano interruzione di servizi o hackeraggi di sistema oltre a ridurre considerevolmente i costi associati all'utilizzo dei servizi. Un ulteriore vantaggio è l'inclusività di una più ampia gamma di individui che solitamente sono privi di accesso ai servizi finanziari per via delle scelte operative degli intermediari e l'interoperabilità delle applicazioni DeFi che girano su blockchain pubbliche che hanno il potenziale di creare nuovi mercati finanziari, nuovi servizi e prodotti. Esistono numerose tipologie di piattaforme di Defi, esse

[49] Il **Wallet**, anche chiamato Portafoglio di Criptovalute serve ad archiviare le chiavi private per l'accesso ai fondi, mantenendo le criptovalute sicure e accessibili oltre a consentire all'utente di inviare e ricevere fondi, https://www.coinbase.com/it/learn/crypto-basics/what-is-a-crypto-wallet

possono essere costruite su blockchain diverse e hanno funzioni anche completamente differenti fra loro:

Piattaforme di Lending e Borrowing: Queste emettono attraverso "collateralizzazione"[50], uno o più asset che permettono la contrazione di un debito verso la piattaforma. Il prestito molto spesso è rilasciato sottoforma di Stablecoin, ovvero monete vincolate al prezzo di una "Moneta Fiat"[51] e quindi stabili rispetto alla fluttuazione di mercato, un esempio è USDT[52] denominata anche Theter, moneta virtuale che lavora attivamente per mantenere stabile la sua valutazione attraverso specifici meccanismi di mercato. Theter è collateralizzata con rapporto 1:1 dal Dollaro Americano. In queste Dapp, è possibile depositare i nostri asset e diventare creditori guadagnando un interesse annuo in percentuale in base alla quantità concessa. "Molto spesso la piattaforma per attirare l'utente a diventare creditore offre un incentivo definito liquidity mining erogando in aggiunta il suo token oltre all'interesse del credito per attrarre sempre più liquidità"[53]. La piattaforma ci permette anche di depositare i nostri asset per poter aprire una posizione di debito, vincolando parte delle nostre valute digitali alla piattaforma e prendere un prestito stablecoin pari solitamente a un rapporto ben preciso rispetto al nostro collaterale. La stablecoin emessa sarà pari al valore garantito dal collaterale a debito in base alla quotazione di quel momento. La piattaforma si protegge dall'insolvenza attraverso un sistema di "liquidazione"[54]. Alcune

[50] La finanza tradizionale definisce **Collateralizzazione** l'operazione contrattuale che effettua un soggetto obbligato ad eseguire una prestazione al fine di garantirla, la prestazione consiste nel sottoporre a vincolo uno specifico asset (Collaterale) che può essere venduto in danno del debitore, se questi non esegue la propria obbligazione, https://www.borsaitaliana.it/borsa/glossario/collateralizzazione.html

[51] In economia, la **Moneta Fiat** è definita come moneta cartacea inconvertibile, accettata come mezzo di pagamento in quanto dichiarata a corso legale (forzoso) dallo stato che la emette, indipendentemente dal suo valore intrinseco, https://www.treccani.it/enciclopedia/fiat-money/

[52] **USDT**, Denominato anche "Theter" è la Stablecoin più adottata e scambiata nel mondo delle criptovalute, ha aperto la strada al modello Stablecoin offrendo la stabilità e la semplicità delle Monete Fiat unita alla natura innovativa della tecnologia blockchain, https://tether.to/en/why-tether

[53] **The Crypto Gateway** Che cos'è la Decentralized Finance (DeFi)? 2022, https://thecryptogateway.it/tutorial-defi-finanza-decentralizzata/.

[54] Con il termine **Liquidazione** si intende il processo di chiusura forza della piattaforma riguardo una posizione debitoria di un utente che non è più in grado di soddisfare i requisiti di margine sul collaterale depositato, ciò avviene molto spesso si tratta di asset con un prezzo molto volatile, **Blockchain Media** Qual è la liquidazione delle criptovalute e cosa fare? 2022, https://blockchain-media.org/it/crypto-liquidation/.

piattaforme[55] della Defi svolgono quanto descritto ma senza di fatto emettere stablecoin, operando unicamente con una o più valute non stabili, ma altamente volatitli.

Decentralized Exchange o Exchange decentralizzati: Fondamentali per l'erogazione dei servizi DeFi, sono luoghi di scambio di criptovalute simili a Exchange decentralizzati come ad esempio Binance[56], con la differenza di non essere centralizzati ma decentralizzati. Ci permettono di scambiare i nostri asset senza doverci registrare tramite l'immissione di dati sensibili o tramite la procedura "Know your customer"[57]. Le piattaforme più utilizzate[58] utilizzano un metodo di scambio denominato Automatic Market Maker (AMM). Con esso l'utente non potrà mai impostare un acquisto pre-impostato come accade nelle piattaforme tradizionali ma dovrà acquistare al prezzo di mercato di quel preciso momento per poter effettuare lo scambio. Questi, inoltre, riescono a scambiare criptovalute grazie ai liquidity provider, ovvero coloro che forniscono liquidità alla piattaforma per permettere lo scambio e ricevere come guadagno una parte delle commissioni.

Combo farming e Yield Aggregator: Queste sono veri e propri aggregatori, monitorano e aggiornano costantemente i migliori rendimenti, interessi richiesti e dati dalle piattaforme combinandole fra loro trovando i migliori rendimenti presenti sul mercato in quel momento. È possibile utilizzare queste piattaforme depositando fondi al loro interno e allo stesso tempo utilizzare sia i loro smart contract che quelli di altre applicazioni decentralizzate collegate a questi aggregatori. Il più utilizzato fra gli yield aggregator è "Yearn Finance"[59]. Grazie a queste piattaforme i

[55] **AAVE** e **JustLend** (JST) sono le piattaforme prime in classifica per Total Value Locked, https://defillama.com/protocols/Lendig

[56] **Binance** è una piattaforma di scambio (Exchange) di criptovalute fondata nel 2017, nel maggio 2021 è stata definita come la più grande al mondo in termini di volume di scambi, https://www.binance.com/it

[57] **Know Your Customer** (KYC), è l'insieme di procedure attuate da alcuni istituti e professionisti per obbligo di legge volte ad acquisire dati certi e informazioni sull'identità dei loro clienti, le procedure sono racchiuse nella Direttiva Europea Antiriciclaggio AMLD, In Italia presenti nel *D.L 90/2017*. **Intesa** Che cos'è il KYC e perché adottarlo. 2022, https://www.intesa.it/che-cose-il-kyc-e-perche-adottarlo/.

[58] **Uniswap** (UNI) e **Curve** (CRV) sono le piattaforme prime in classifica per Total Value Locked, https://defillama.com/protocols/Dexes

[59] **Yearn Finance** (YFI) è la piattaforma decentralizzata con il primato di TVL che garantisce la massimizzazione dei profitti attraverso un servizio di aggregazione automatizzato, https://defillama.com/protocol/yearn-finance

rendimenti sono più alti ma di contro anche il rischio lo è, inoltre ad aumentare ulteriormente il rischio è il fatto che molto spesso gli interessi vengono pagati con il token[60] della piattaforma aggregatrice proprietaria esponendo l'utente a una volatilità elevata.

Piattaforme di strumenti Derivati: Piattaforme come "Synthetix"[61] Nascono con l'idea di permettere alle persone di creare prodotti derivati di qualsiasi tipo di asset e sono grado di creare degli asset sintetici di Materie Prime, Azioni e Criptovalute, tutto in maniera completamente decentralizzata, a basso costo e 24 ore su 24. Quando parliamo di prodotti sintetici o derivati parliamo di copie di beni digitali o fisici, che emulano il prezzo di tale asset. Il rischio è maggiore perché si va incontro al potenziale fallimento della piattaforma che sostiene il loro collegamento rendendo gli asset privi di valore. Il vantaggio principale risiede non nell'investimento ma bensì nella speculazione nel breve periodo a basso costo rispetto ai metodi tradizionali oltre a incentivare l'utente a rimanere all'interno del mondo decentralizzato.

Piattaforme di Assicurazione: Ci permettono di assicurare i nostri fondi all'interno di Smart Contract o addirittura all'interno di Piattaforme di Finanza Centralizzata. Rendono possibile sia ricoprire il ruolo di colui che assicura i fondi, sia di chi permette alla piattaforma di avere fondi da restituire a chi è stato frodato. Nella prima ipotesi l'utente dovrà pagare per assicurare i fondi, mentre nell'altra verremo pagati per detenere i nostri capitali all'interno di uno smart contact della piattaforma. Tutto ciò accade in protocolli come "Armor e Nexus Mutual"[62].

Ma la Finanza Decentralizzata per quanto possa sembrare remunerativa e sicura presenta molteplici rischi, tra i più comuni troviamo:

[60] Il termine **Token** è un altro termine tecnico per definire una "Critpovaluta" o "Crypto-Asset", https://www.coinbase.com/it/learn/crypto-basics/what-is-a-token

[61] **Synthetix** è un protocollo di liquidità decentralizzato in cima alla classifica per Total Value Locked che fornisce lo scambio di prodotti derivati agli utenti, https://defillama.com/protocol/synthetix

[62] **Armor** e **Nexus Mutual** sono i fornitori decentralizzati di servizi di assicurazione per eccellenza presenti sul territorio Defi, https://defillama.com/protocols/Insurance

Rug Pulls: L'utente malevolo sfruttando il basso valore di mercato e manipolando le "piscine di liquidità"[63] riempiendo un token della coppia presa di mira con tantissima liquidità, cosicché gli altri investitori, ingannati dalla mole di liquidità che suscita in loro sicurezza apparente, depositino denaro sottoforma di assets all'interno della pool. Colui che ha versato la maggior parte del capitale, notando l'aumento del prezzo dell'asset, vende interamente la sua parte, facendone crollare il prezzo e rendendolo privo di valore non permettendo alle persone che hanno investito il loro denaro di poter effettuare scambi. Un esempio di Rug Pull è avvenuto nel 2021, truffa che è costata circa 3 milioni di dollari agli investitori del Token denominato "Squid"[64].

Bug di Smart contract: In questo caso un hacker può sfruttare l'eventuale bug di uno smart contract a suo vantaggio per svuotare il contenuto monetario all'interno.

Flash Loans Attack: Questo è una tipologia di attacco in cui un esperto informatico malevolo sfrutta un prestito flash, cioè senza garanzia per manipolare a proprio vantaggio il prezzo di una valuta digitale all'interno di una piscina di liquidità. È molto frequente nei confronti di progetti della finanza decentralizzata[65].

Altri tipi: In quanto sistemi aperti, qualsiasi piattaforma o token potrebbe rivelarsi una truffa, qualsiasi smart contract potrebbe essere reindirizzato a favore di un truffatore, di conseguenza bisogna fare attenzione quando si approcciano progetti nuovi e token non molto famosi.

I macro obiettivi della Defi che sta perseguendo questi anni mediante l'utilizzo di DLT, Blockchain e Smart contract sono rendere i servizi finanziari accessibili a

---

[63] Le **Piscine di Liquidità** (Liquidity Pool) sono la colonna portante di molti Exchange Decentralizzati, gli utenti denominati "Liquidity Provider" aggiungono un valore uguale di due token in una pool per creare un mercato agevolando scambi prestiti, in cambio ricevono le commissioni degli scambi effettuati nella pool in proporzione alla loro quota della liquidità totale, **Binance** Cosa sono le pool di liquidità nella DeFi e come funzionano? 2020, https://academy.binance.com/it/articles/what-are-liquidity-pools-in-defi.

[64] **Cheng Amy** 'Squid Game'-inspired cryptocurrency that soared by 23 million percent now worthless after apparent scam. The Washington Post. 2021, https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/

[65] Un esempio di Flash loan Attack è stato osservato sulla piattaforma Cream Finance, **Bourgi Sam** Sembra che Cream Finance abbia subito un altro grave flash loan attack. Cointelegraph. 2021, https://it.cointelegraph.com/news/breaking-cream-finance-appears-to-have-suffered-major-loss-in-flash-loan-hack

chiunque dispenda di un dispositivo e di una connessione a internet e ridurre la necessita di un intermediario terzo. Questa innovazione ha lanciato una sfida al sistema tradizionale che vede "regole del mondo economico finanziario basate su relazioni contrattuali piuttosto che tecniche, in cui l'entità vigilata deve garantire la conformità da parte di tutti i fornitori di servizi ad essa collegati"[66]. Ad oggi la Finanza Decentralizzata è da considerare giovane ed ancora in evoluzione, non ha ancora potuto raggiungere il suo pieno potenziale a causa di problematiche come frodi, volatilità eccessiva e incertezza normativa. Sarà necessario una forte cooperazione internazionale e un approccio meno chiuso ma più flessibile da parte dei legislatori dei paesi leader e un impegno per l'ampia diffusione della cultura economico-tecnologica, soprattutto in paesi come l'Italia, per creare un approccio che possa far evolvere pienamente la DeFi a supporto dell'economia reale.

[66] **Buscema Salvatore** Finanza Decentralizzata – Problemi giuridici e tecnici. Cryptoavvocato. 2020 https://www.cryptoavvocato.it/articoli/finanza-decentralizza-problemi-giuridici-tecnici/.

CAPITOLO 2: La Moneta e le sue evoluzioni

"La moneta è indispensabile per il funzionamento di un sistema economico. Prima metallica, poi cartacea e ora addirittura elettronica, è lo strumento di pagamento comunemente usato per comprare ciò di cui gli individui, le organizzazioni e le società hanno bisogno. La sua evoluzione ha accompagnato lo sviluppo delle civiltà e di essa vi sono ampie tracce nella storia, anche la più lontana"[67]. In altre parole, il denaro è uno strumento utilizzato per scambiare valore in una comunità di persone che lo accetti come metodo di pagamento per beni e servizi prodotti oppure un deposito di ricchezza con cui conservare il potere d'acquisto da quando lo si ottiene a quando lo si spende. In sostanza qualunque oggetto può essere utilizzato come denaro, basti pensare al passato, dove si utilizzavano rocce e conchiglie per scambiare valore, questo perché ciò che dà valore al denaro, soprattutto ad oggi, è la fiducia. Il denaro che caratterizza il nostro mondo oggi è denominata moneta fiat, ovvero una moneta cartacea che la banca centrale può stampare senza restrizioni. Infatti, banche centrali come la Federal Reserve può creare nuova moneta e aumentarne l'offerta attraverso meccanismi economici svalutandola e rivalutandola rispettivamente attraverso politiche monetarie accomodanti o restrittive. Bitcoin come forma digitale di denaro, condivide alcune somiglianze con il denaro fiat a cui siamo abituati ma presenta delle differenze significative. La rivoluzione digitale sta sempre di più modificando gli aspetti del mondo della finanza, con un riguardo maggiore verso i sistemi dei pagamenti. Ci troviamo in una fase storica in cui si intensifica sempre di più la concorrenza tra i vari formati di denaro e il ruolo delle banche centrali sempre di più messo in discussione. L'innovazione tecnologica sta aprendo prospettive finora inesplorate per le istituzioni finanziarie, modificando e sviluppando soprattutto i concetti di transazione, proprietà e fiducia. Le criptovalute sfidano apertamente i tradizionali paradigmi legali e politici dei sistemi monetari controllati dallo stato, alimentando la competizione tra la fornitura di denaro privato e pubblico. A fronte della novità e dei sistemi di pagamenti digitalizzato dove monopolio delle banche centrali sembra non essere ormai assoluto come una volta,

[67] **Banca D'Italia** La Moneta e gli strumenti di pagamento alternativi al contante. Banca D'Italia, 2018.

l'intensificazione dell'azione e utilizzo delle criptovalute ha sollecitato e continua a sollevare preoccupazioni alle autorità che necessitano di esplorare nuove opportunità. "Molte banche stanno uscendo dalle proprie posizioni tradizionali per esplorare altri servizi che si basano sull'uso dei Bitcoin, tra questi c'è la possibilità di gestire e comprare criptovalute presso la banca"[68]. Le banche centrali difficilmente hanno valutato di riconsiderare il loro ruolo, sono infatti da sempre rimaste fedeli a una valuta monetaria fiat preferendo di non offrire alternative digitali, banconote o monete. E' sempre più vicina l'emissione di valuta digitale da parte delle banche centrali, il che con molta probabilità potrebbe segnare una definitiva svolta nell'evoluzione del denaro attraverso l'introduzione delle Central Banck Digital Currency, cogliendo l'opportunità per migliorare l'efficienza finanziaria moderna e introdurre un meccanismo innovativo con un riguardo verso l'inclusione finanziaria, come sta già accadendo in paesi come la Cina[69]. Allo stesso tempo vi sono preoccupazioni su come ciò potrebbe impattare sul sistema odierno e sulla sua stabilità.

1.4 Asset Digitale, Criptovaluta e Token

Un Asset Digitale è "Un asset che esiste esclusivamente in forma digitale o che è la rappresentazione digitale di un altro bene, laddove l'asset ha valore per uno stakeholder"[70]. Più tecnicamente un asset digitale è una sequenza di bit[71], ovvero unità che contengono e trasmettono informazioni che ha la caratteristica di essere distinguibile come un'unità discreta che si mantiene tale negli atti di scambio, così come si comportano gli asset fisici nel mondo non digitale. "Un asset digitale quindi definibile come tale se si presenta come inalterabile, durevole e non duplicabile, cioè con la quantità di informazione contenuta protetta da soluzioni crittografiche e da protocolli di sicurezza logica e fisica che ne garantiscano l'originalità e la

[68] **Spadafora Francisco** Banche, giocate d'anticipo: perché i crypto-asset sono un mercato da non sottovalutare. Ntt Data. 2021, https://it.nttdata.com/insights/blog/cryptoasset-banche.
[69] **Minenna Marcello** Cina: la grande crescita silenziosa dello Yuan digitale. Sole24Ore. 2022, https://www.ilsole24ore.com/art/cina-grande-crescita-silenziosa-yuan-digitale-AEufHqDB
[70] **International Organization for Standardization** ISO 22739:2020 Blockchain and distributed ledger technologies. 2020, https://www.iso.org/standard/73771.html.
[71] L'unità di misura della quantità di informazione.

conservazione" [72]. Solo seguendo queste condizioni possiamo attribuire ad un asset digitale un effettivo valore, proprio come succede con una banconota tradizionale che risulta infalsificabile e non duplicabile garantendo l'attendibilità del credito espresso nelle informazioni visive come valuta e importo. Il termine "Criptovaluta" è definito come "Rappresentazione digitale di valore, non emessa 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 e trasferita, archiviata e negoziata elettronicamente''[73]. "In altre parole per Criptovaluta si intende una moneta elettronica basata su blockchain"[74]. È una nuova forma di denaro digitale resa disponibile grazie agli sviluppi della crittografia. Ad introdurre questo concetto è stato Bitcoin nel 2008 permettendo agli utenti di poter inviare fondi a chiunque e ovunque nel mondo senza l'intervento di intermediari finanziari, ovvero un'autorità centrale come, ad esempio, una banca o un governo che può intervenire in una transazione tra mittente e destinatario, sorvegliando, censurando, annullando la transazione o convivendo i dati sensibili raccolti in ogni momento del processo. Con l'avvento delle criptovalute le transazioni collegano direttamente mittente e destinatario senza consentire a nessun altro l'accesso ai tuoi fondi e dove nessuno può dirti quali servizi puoi utilizzare. Tutto ciò avviene grazie alla tecnologia blockchain sulla base della quale operano le criptovalute attraverso tecniche crittografiche che tengono al sicuro i fondi dell'utente utilizzatore. Definiamo "Token" come "Una soluzione criptografica che consente la circolazione su rete telematica senza intermediazione di terzi di un asset digitale che incorpora o rappresenta un diritto soggettivo"[75]. "Una volta creato il registro delle transazioni vengono emessi i token, che vengono effettivamente scambiati tra gli utilizzatori della criptovaluta, ed i cui scambi saranno transazioni memorizzate sulla blockchain"[76]. La differenza sostanziale fra Criptovaluta e Token consiste che quest'ultimi non nascono con una loro blockchain, ma si appoggiano a una di quelle

[72] **Rampone Francesco** Token, asset digitali e ID I diritti soggettivi in chiave criptolegale. Associazione Blockchain Italia. 2020, https://associazioneblockchain.it/doc/token-asset-digitali-e-id-i-diritti-soggettivi-in-chiave-criptolegale/.
[73] *Art.1, comma 2, lett. Gg, D. LGS n° 90/2017*
[74] **Cavicchioli Marco** La Differenza tra Token e Criptovalute. 2018, https://medium.com/@marcocavicchioli/la-differenza-tra-token-e-criptovalute-596c9cb96bc5.
[75] **Rampone Francesco** Token, asset digitali e ID I diritti soggettivi in chiave criptolegale. Cit.
[76] **Cavicchioli Marco** La Differenza tra Token e Criptovalute. Cit.

già esistenti. Possiamo distinguere in 2 principali categorie di Token: I Security Token e gli Utility Token

Security Token: Rappresentano la titolarità di un'attività finanziaria, conferiscono sostanzialmente un diritto di credito a cui per legge o per contratto possono accedere altri diritti o situazioni giuridiche soggettive. Si suddividono a loro volta in Equity token e Asset Token. Gli **Equity Token** conferiscono al titolare di diritto a guadagni sulla base del capitale detenuto, derivanti ad esempio da un'applicazione o una piattaforma. Gli **Asset Token** invece attribuiscono l'esclusiva proprietà di un bene. Così come i titoli di credito come le obbligazioni o altre forme di prestito conferiscono al possessore il diritto alla prestazione indicati. È bene specificare che i token conferiscono il diritto che il Distribuited Ledger su cui sono implementati gli ha attribuito, per mezzo di Smart Contract.

Utility Token: Consentono di acquistare un determinato bene o servizio, conferendo al titolare un diritto di opzione per l'acquisto o somministrazione di cose o forniture di servizi che siano attuali o futuri, riservando quindi benefici e servizi premium a chi ne detiene. Anche questo tipo di token presenta delle sottocategorie: Voting token, Work Token e Consensus Token. I **Voting token** conferiscono diritto di voto di governance al titolare, come avviene nelle "DAO"[77]. I **Work token** attribuisce a chi compie determinate azioni o certi comportamenti una ricompensa. I **Consensus token** riconoscono una ricompensa di incentivazione ai nodi che garantiscono la convalida dei dati e il consenso del network. Quest'ultimo è osservabile in Bitcoin che garantisce a coloro che offrono una potenza di calcolo ingente una ricompensa sottoforma di nuovi bitcoin.

Sulla base delle definizioni appena riportate possiamo dedurre che un token è innanzi tutto un titolo digitale che rappresenta o incorpora un diritto in favore del

[77] Un **Organizzazione Autonoma Decentralizzata** (DAO) è un'organizzazione automatizzata tramite del codice e aperta a chiunque purché siano soddisfatti i requisiti di base. Nonostante sia creata da e gestita da una comunità è "autonoma", questo perché gli Smart Contract aiutano a gestire la maggior parte dei processi senza l'interferenza umana. Chi possiede il "Voting Token" di una DAO può proporre o votare riguardo cambiamenti di funzionamento della stessa. **Binance** Come creare una DAO? Binance Accademy. 2022, https://academy.binance.com/it/articles/how-to-create-a-dao.

suo possessore. Inoltre, assume questo tipo di valore in quanto non riproducibile e non falsificabile, ovvero in quanto basato sulla tecnologia DLT dove risulta un elemento digitale che consente l'effettivo scambio di valore su una rete telematica senza la necessità di intermediari. Ciò ne impedisce la duplicazione e modificazione, altrimenti si rischierebbe di considerarlo come una semplice messaggio poiché nulla impedisce che questo possa contenga una rappresentazione digitale di un diritto, ma la possibilità di alterare il messaggio da chiunque impedisce che ad esso possa attribuirsi valore. "Al fine di tutelare gli investitori, gli ordinamenti giuridici, al momento della valutazione dei cripto assets, saranno evidenziate le caratteristiche di investimento e il token, che sarà assoggettato alla disciplina prevista per le sue molteplici nomenclature"[78].

1.5 Il Principio: Bitcoin

Bitcoin: un sistema di moneta elettronica peer-to-peer

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Translated in Italian from bitcoin.org/bitcoin.pdf
by @terzim

Sommario. Una versione puramente peer-to-peer di denaro elettronico permetterebbe di spedire direttamente pagamenti online da un'entità ad un'altra senza passare tramite un'istituzione finanziaria. Le firme digitali offrono una soluzione parziale al problema, ma i benefici principali sono persi se una terza persona di fiducia è ancora richiesta per prevenire la doppia spesa. Proponiamo una soluzione al problema della doppia spesa mediante l'utilizzo di una rete peer-to-peer. La rete stampa un marcatore temporale sulle transazioni facendo hashing sulle stesse e incatenandole in una catena di proof-of-work basata sugli hash, formando una registrazione che non può essere modificata senza rifare la proof-of-work. La catena più lunga non solo serve come prova della sequenza di eventi ai quali si è assistito, ma anche come prova che essa proviene dal gruppo più grande di potenza CPU. Fintanto che la maggior parte della potenza CPU è controllata da nodi che non cooperano per attaccare la rete, questi genereranno la catena più lunga e supereranno gli utenti malintenzionati. La rete stessa richiede una struttura minimale. I messaggi sono trasmessi su base best effort, e i nodi possono lasciare e ricongiungersi con la rete a loro piacimento, accettando la catena proof-of-work più lunga come prova di quello che è avvenuto mentre erano non erano presenti.

[78] **Banca D'Italia** Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività. Banca D'Italia. 2022, https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-cripto.pdf

Figura: Rappresentazione Grafica del Sommario del Whitepaper originale di Bitcoin tradotto in lingua italiana

1.5.1 Storia di Bitcoin

Bitcoin fu inventato nel 2008 con la pubblicazione di un documento intitolato "Bitcoin: Un sistema di contanti elettronici peer-to-peer"[79]. Quest'ultimo aveva come obiettivo la creazione di un sistema di contanti elettronici completamente decentralizzato e non basato su un un'autorità centrale per l'emissione o regolamentazione di una valuta e la convalida delle transazioni. La rete Bitcoin è stata avviata a tutti gli effetti nel 2009, dopodiché nel 2011 Satoshi Nakamoto, identità tutt'ora sconosciuta, si è ritirato lasciando la responsabilità di sviluppare il codice e la rete a un gruppo di volontari in costante crescita. Tuttavia, nessuno di questi o altri esercita il controllo individuale sul sistema bitcoin, che opera sulla base di principi matematici completamente trasparenti, con codice open source e consenso tra i partecipanti. Questa invenzione ha generato conoscenze nei campi dell'informatica distribuita, dell'economia e dell'econometria dapprima sconosciute. Un'innovazione caratterizzante relativa a questa blockchain è l'implementazione dell'algoritmo di consenso Proof-Of-Work che fornisce sicurezza e resilienza per bitcoin aumentando nel tempo in modo esponenziale in termini di potenza arrivando a superare un potere di elaborazione combinata dei migliori supercomputer del mondo.

1.5.2 Che cos'è Bitcoin

Bitcoin è una raccolta di concetti e tecnologie che formano le basi per un nuovo ecosistema di denaro digitale. Le unità di valuta sono denominate "Bitcoin"[80] e vengono utilizzate per immagazzinare e trasferire valore tra i partecipanti del

[79] **Nakamoto Satoshi** Bitcoin: A Peer-to-Peer Electronic Cash System. 2008, https://bitcoin.org/bitcoin.pdf.

[80] I **Bitcoin** rispettano le caratteristiche di durata, portabilità, fungibilità, scarsità, divisibilità e riconoscibilità, piuttosto che far riferimento a proprietà fisiche (Oro e Argento) o avere fiducia nelle autorità centrali come le Valute a corso legale è gestito dalla matematica. Hanno un valore che proviene solo e direttamente dalle persone che li accettano come forma di pagamento; quindi, come per tutte le forme di denaro necessita di adesione e fiducia. **Bitcoin.org** Come sono creati i bitcoin? 2009, https://bitcoin.org/it/faq#come-vengono-creati-i-bitcoin.

Network Bitcoin. Gli utenti della rete comunicano tra loro utilizzando il protocollo bitcoin principalmente attraverso internet, sebbene possano essere utilizzate altre reti di trasporto. Il protocollo è caratterizzato da un software aperto, ovvero contenente un codice sorgente aperto a tutti, che può essere utilizzato su un'ampia gamma di dispositivi digitali, inclusi portatili e Smartphone, rendendo questa tecnologia facilmente accessibile. Gli utenti possono trasferire bitcoin sulla rete e possono fare tutto quello che permesso fare con l'utilizzo delle valute tradizionali che conosciamo, come vendere e acquistare beni o inviare denaro a persone o organizzazioni. I Bitcoin possono essere acquistati, venduti e scambiati con altre valute attraverso Exchange specializzati. In un certo senso bitcoin è considerato una forma perfetta di denaro per internet perché è veloce, economico, sicuro e senza confini. La principale differenza con le valute tradizionali è che quest'ultime non sono interamente digitali come lo è Bitcoin. Inoltre, Bitcoin è un sistema distribuito peer-to-peer e come tale non necessita e non usufruisce di un server centrale o un punto di controllo. La sua valuta rappresenta solo la prima applicazione di questa invenzione, questo protocollo è culmine di decenni di ricerca in crittografia e sistemi distribuiti che delle innovazioni chiave[81], che combinate fra loro rappresentano Bitcoin che consiste di: Un Network peer-to-peer decentralizzato, un Libro-mastro di transazioni pubblico (Blockchain), un insieme di regole per la convalida indipendente delle transazioni e l'emissione di valuta e un meccanismo per raggiungere un consenso globale decentrato sulla blockchain valida, nel caso di bitcoin l'algoritmo Proof Of Work.

1.5.3 Il Mining e il meccanismo di consenso Proof-Of-Work

In Bitcoin, viene utilizzato un tipo di algoritmo di consenso, denominato Proof-Of-Work, per confermare le transazioni e produrre i nuovi blocchi sulla catena. Come già spiegato un registro distribuito decentralizzato raccoglie ogni singola transazione effettuata dagli utenti, ma per essere considerate valide, devono essere prima approvate e organizzate in blocchi. Tale responsabilità ricade su nodi speciali chiamati "Miner" e l'intero processo è definito "Mining". L'algoritmo PoW

[81] **Antonopoulos Andreas M. and Masutti Riccardo** Mastering Bitcoin Indipendently Published. 2019, Pag. 48

incentiva i miner a competere fra loro nell'elaborazione degli scambi, ricevendo in cambio una ricompensa sottoforma di una nuova emissione di Bitcoin. Qualsiasi partecipante alla rete bitcoin, ovvero chiunque utilizzi un dispositivo che esegue un Bitcoin "Full Node''[82]. L'algoritmo incorporato regola la funzione di mining attraverso la rete. La difficoltà del processo che i minatori devono eseguire è regolata dinamicamente in modo tal che qualcuno ci riesca esattamente ogni 10 m, ricevendo nuovi bitcoin. Ciò avviene a prescindere da quanti minatori e quanta potenza di elaborazione siano in competizione in qualsiasi momento. Essenzialmente il bitcoin mining decentralizza le funzioni di emissione di valuta e di compensazione di una banca centrale e sostituisce la necessita di qualsiasi banca centrale. Il Protocollo dimezza inoltre la velocita con cui vengono creati nuovi Bitcoin circa ogni 4 anni e limita il numero di totale di bitcoin che verranno creati per un totale fissato a 21 milioni di monete. Si prevede che Bitcoin raggiungerà questo numero nel 2040[83]. A causa della diminuzione del tasso di emissione del bitcoin, nel lungo periodo, la valuta Bitcoin è deflazionistica, infatti, non può essere inflazionato stampando denaro nuovo oltre al tasso di emissione previsto come succede per le odierne Monete Fiat.

1.5.4 Pro e Contro Bitcoin in relazione alle Monete Fiat

Nonostante non ci sia alcun bene fisico che supporti il valore di questa moneta digitale la moneta Bitcoin ha mantenuto negli anni alto il suo valore, questo perché se si pensa al denaro nell'uso quotidiano, non ci sono più riserve di oro o altri asset che garantiscono il valore delle nostre banconote. Infatti, il denaro che prendiamo a prestito, spesso esiste solo come un numero su uno schermo, per via del sistema

[82] Un **Full Node** è un programma che convalida completamente transazioni e blocchi aiutando anche la rete accettando transazioni e blocchi da altri Full Node. **Bitcoin.org** What Is A Full Node? 2009, https://bitcoin.org/en/full-node#what-is-a-full-node.
[83] **Antonopoulos Andreas M. and Masutti Riccardo** Mastering Bitcoin. Cit. Pag. 47

bancario a riserva frazionaria[84]. Infatti tra i vantaggi[85] che caratterizzano e determinano il valore di Bitcoin troviamo:

La Libertà di Pagamento: La capacità di trasferire rapidamente grandi quantità di denaro, in tutto il mondo, senza la necessità di intermediari o vincoli quindi effettuare transazioni senza confini.

Le Commissioni: L'utente che decide di effettuare la transazione può decidere autonomamente la commissione da pagare in base alla sua esigenza di trasferire velocemente o meno i fondi. Commissioni elevate possono infatti incrementare la velocità di transazioni indifferentemente dalla quantità da inviare. Per colui che riceve non è prevista alcun tipo di commissione.

Rischi Contenuti, Controllo e Sicurezza: Le transazioni effettuate con Bitcoin sono sicure, non contengono dati sensibili o informazioni personali del cliente e sono irreversibili. Questo evita potenziali perdite proteggendo gli utenti da frodi. Gli utenti che utilizzano Bitcoin possono controllare totalmente le proprie transazioni anche in assenza di informazioni personali connesse offrendo protezione contro il furto d'identità.

Trasparente e Neutrale: La blockchain per definizione rende disponibili e di semplice consultazione tutte le informazioni relative alle attività in tempo reale, nessuno può censurarle o manipolarle in quanto Bitcoin è crittograficamente sicuro, il che garantisce la sua affidabilità in termini di dati e la sua neutralità, trasparenza e prevedibilità.

Bitcoin, sebbene non si l'unica rete a rendere possibile tutto questo, è considerata la più grande, sicura e popolare. La rete è formata da un numero di nodi elevato, bitcoin di fatto consente al maggior numero di persone di partecipare alla rete

[84] La **Riserva Frazionaria** è un sistema bancario che consente alle banche commerciali di trarre profitto prestando parte dei depositi dei propri clienti, conservando solo una piccola obbligatoria (frazione) di tali depositi come denaro reale disponibile per il prelievo, **Binance** Cos'è la Riserva Frazionaria? Binance Accademy. 2019, https://academy.binance.com/it/articles/what-is-fractional-reserve.

[85] **Vantaggi di Bitcoin, Bitcoin.org** Quali sono i vantaggi di Bitcoin? 2009, https://bitcoin.org/it/faq#quali-sono-i-vantaggi-di-bitcoin.

migliorando la sicurezza complessiva. Maggiore è il numero di nodi connessi al Distribuited Ledger e maggiore è il suo valore.

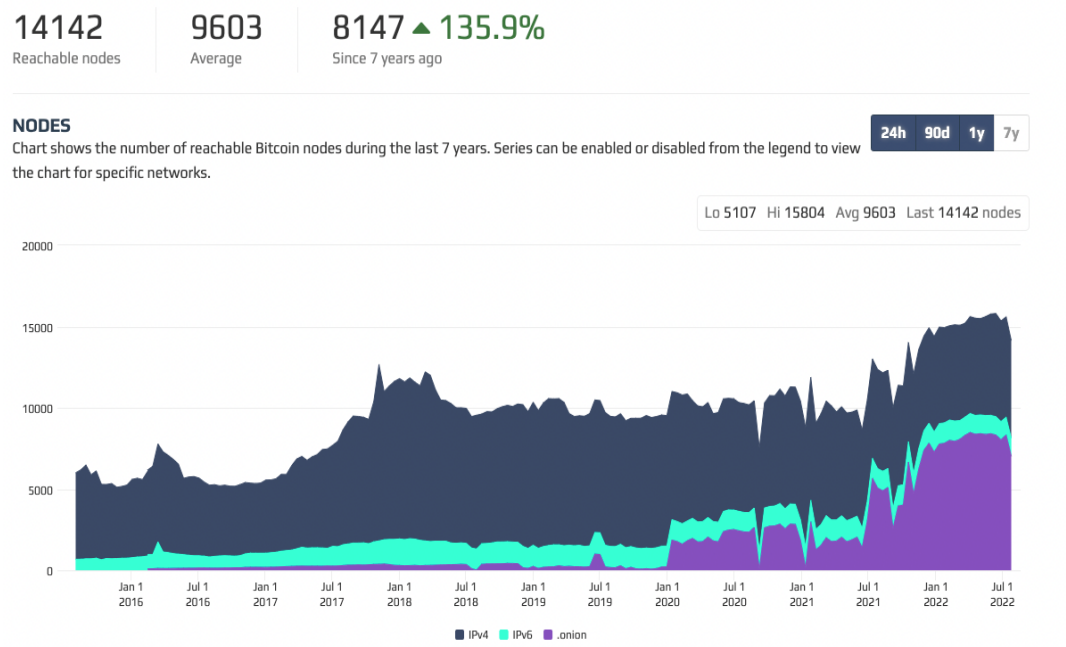
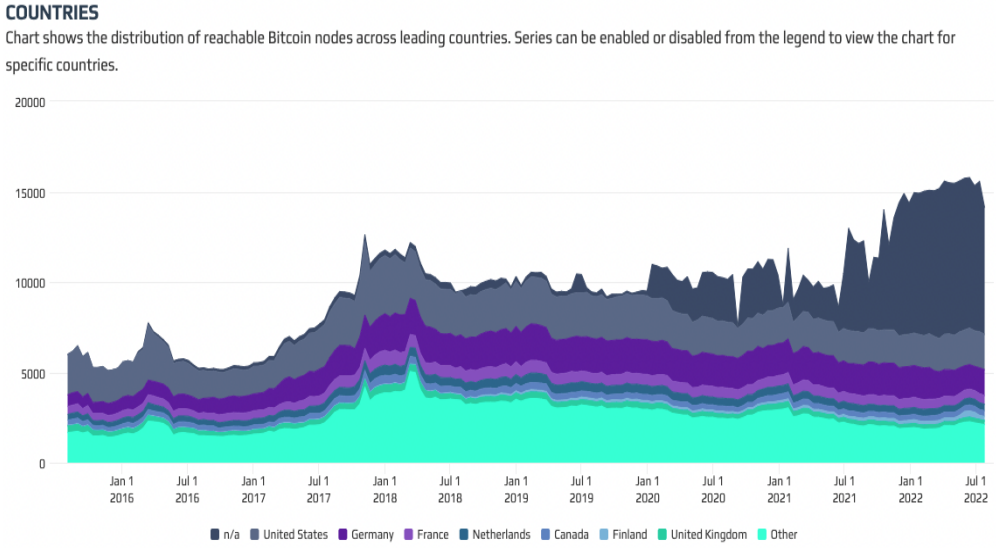


Figura: Rappresentazione Grafica del numero dei nodi della rete Bitcoin totali attivi degli ultimi 7 anni.[86]



[86] https://bitnodes.io/dashboard/7y/

Figura 1: Rappresentazione Grafica della distribuzione geografica dei nodi della rete Bitcoin totali attivi degli ultimi 7 anni.[87]

Un database centralizzato sarebbe suscettibile ad attacchi informatici e interruzioni, infatti, non è raro riscontrare problemi usando una carta di credito per via di problemi legati a server. Un network come quello di Bitcoin, gestito da migliaia di utenti in tutto il mondo lo rende più efficiente e sicuro. Nonostante la decentralizzazione sia un enorme vantaggio, il creatore ha voluto portare gli utenti a collaborare attraverso il meccanismo di consenso Proof-Of-Work che premia il comportamento positivo dei partecipanti. La rete fa particolarmente attenzione nel rispetto del concetto di fiducia che è parte essenziale per qualsiasi oggetto o prodotto di valore. Nelle operazioni di bitcoin c'è più fiducia intrinseca rispetto ad altri sistemi e asset che utilizziamo quotidianamente. Tuttavia, gli utenti della rete non devono fidarsi l'uno dell'altro. Devono solo fidarsi della tecnologia sottostante, che nel tempo si è dimostrata affidabile, sicura e con un codice sorgente aperto a chiunque. Per questo Proof-Of-Work è efficiente, è un meccanismo trasparente che chiunque può verificare. Controllare, è facile da vedere il valore di bitcoin che nasce generando un consenso privo di errori. La mancanza di fiducia nella banca centrale è un avvenimento che si trasforma molto spesso in disastri per la nazione e per la valuta di riferimento. In termini di protezione dei propri fondi, non esistono molte altre opzioni che garantiscono la stessa sicurezza di bitcoin, se depositati correttamente nel wallet di custodia, i fondi saranno al sicuro e anche gratuitamente. Nei paesi sviluppati, ad esempio, la sicurezza fino ad un certo grado è garantita dalle banche ma in altri paesi, le istituzioni finanziarie non sono in grado di fornire la loro protezione verso coloro che detengono grandi somme di denaro. L'offerta massima di emettibile di Bitcoin è limitata a 21.000.000[88] ed è costruita all'interno del framework della blockchain, infatti sono creati ad un tasso decrescente e prevedibile, una volta raggiunto quel numero non ci saranno più Bitcoin disponibili.

[87] https://bitnodes.io/dashboard/7y/

[88] L'emissione di Bitcoin cessa ad un totale di **21 Milion**i, **Bitcoin.org** Economia. 2009 https://bitcoin.org/it/faq#economia.

Bitcoin non è ancora perfetto, gli svantaggi[89] che ad oggi lo caratterizzano sono:

Il Basso Grado di Accettazione: Nonostante la costante crescita dei nodi sono ancora poche le persone e le aziende consapevoli del funzionamento e valore di Bitcoin, per beneficiare degli effetti della rete è necessario che il bacino di utenti adottanti aumenti.

L'alta Volatilità: A causa della fase primordiale dell'innovazione, il valore totale di tutti i bitcoin in circolazione è molto piccolo, pertanto anche piccoli eventi o attività speculative potrebbero variarne significativamente il prezzo.

Lo Sviluppo Continuo: La versione finale di Bitcoin è ancora da vedere, ad oggi nuovi strumenti sono in sviluppo per rendere bitcoin più accessibile e sicuro alle masse.

1.5.5 Bitcoin Come riserva di valore

Alla luce di tutte le caratteristiche riportate, Bitcoin sembra essere una buona scelta per essere usata come una riserva di valore e diversificare il proprio portafoglio. Questa Criptovaluta, infatti, sta guadagnando di anno in anno una reputazione come alternativa moderna e como oro digitale rispetto a opzioni più tradizionali come Metalli preziosi, dollari statunitensi e titoli di stato. Questo perché presenta delle caratteristiche che sono comunemente tipiche delle riserve di valore:

Essere in grado il Mantenere Valore Nel Tempo: Bitcoin fino a quando ci saranno dei computer che manterranno la rete sarà durevole al 100%, inoltre non può essere distrutto come il denaro fisico o i metalli preziosi.

Come valuta digitale Bitcoin è incredibilmente Portatile: tutto ciò di cui un utente ha bisogno è una connessione Internet e le chiavi private per accedere ai propri fondi disponibili da qualsiasi luogo.

Ogni Bitcoin è Divisibile in "Satoshi"[90]: consente di fatto agli utenti di effettuare transazioni di qualsiasi grandezza.

---

[89] **Svantaggi di Bitcoin**, **Bitcoin.org** Quali sono i vantaggi di Bitcoin? Cit.
[90] Un **Satoshi** è la più piccola unità di un Bitcoin, 1 BTC = 100.000.000.

Possedere la caratteristica di Fungibilità: Un Bitcoin o Un Satoshi è intercambiabile con un altro e questo consente di utilizzare la criptovaluta come scambio di valore con altre persone a livello globale.

La sua Scarsità: In fase di programmazione l'emissione di Bitcoin è limitata e alcuni milioni già emessi sono stati persi per sempre, il che rende l'offerta di Bitcoin caratterizzata da 21.000.000 di BTC rispetto alle valute fiat inflazionistiche, dove l'offerta aumenta o diminuisce a piacere di un autorità centrale.

Un'ampia Accettabilità: l'adozione di BTC come metodo di pagamento per privati e aziende e l'industria blockchain continua a crescere ogni giorno

Nonostante ciò, ad oggi Bitcoin, agli occhi del mercato dimostra altro e non rientra in una categoria facilmente identificabile, basta considerare la relazione tra bitcoin e i mercati tradizionali. Sin dal primo lancio di bitcoin i mercati sono stati in una costante tendenza rialzista, di fatto è ancora presto considerare questa criptovaluta come una riserva di valore paragonabile ad asset storicamente validi come l'oro, nonostante bitcoin abbia avuto performance migliori in termini percentuali negli ultimi anni. Non è da escluderne la possibilità in futuro in quanto alcuni parametri stanno lentamente cambiando, come per l'appunto la correlazione con l'indice più capitalizzato, Nasdaq100.

1.5.6 Correlazione Bitcoin e Nasdaq

Negli ultimi anni e recentemente, abbiamo osservato il prezzo di BTC aumentare e diminuire drasticamente insieme agli altri titoli, soprattutto tech, considerando la politica restrittiva e quindi l'aumento dei tassi di interesse per fronteggiare l'aumento dei prezzi al consumo.

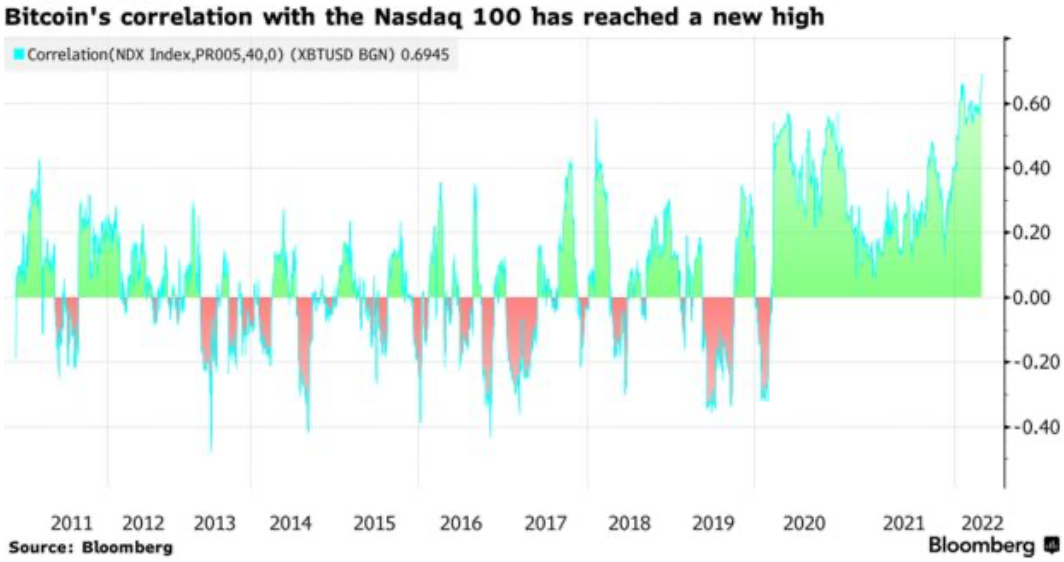


Figura: Rappresentazione Grafica relativa alla correlazione tra Bitcoin e Nasdaq100 degli ultimi 10 anni.

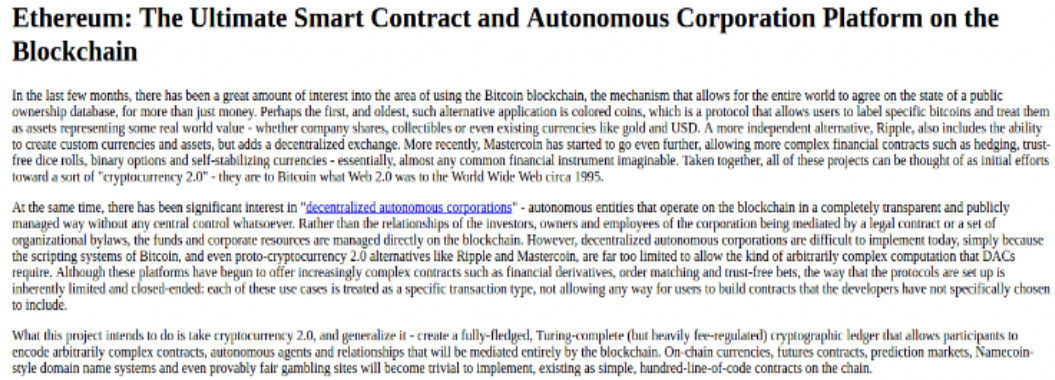
Figura: Rappresentazione Grafica relativa alla correlazione tra Bitcoin e Nasdaq100 dell'ultimo anno (Giugno 2021 – Giugno 2022).

Prendiamo come riferimento la correlazione al Nasdaq, indice tecnologico per eccellenza, con una capitalizzazione di circa 31.46 Miliardi[91], come si può evincere dal primo grafico la correlazione fra i due è molto alta, soprattutto negli ultimi anni.

[91] **Capitalizzazione Totale di Mercato di Nasdaq100**, https://www.nasdaq.com/nasdaq-100

Dall'inizio della pandemia, bitcoin ha avuto la tendenza a muoversi nella stessa direzione di Nasdaq in seguito alla politica monetaria espansiva che ha generato forti acquisti in settori ad alto valore tecnologico, considerati come settori a rischio. Nel secondo grafico invece è riportata la loro correlazione attuale, che dopo un periodo di correlazione molto elevata, si nota una discreta. le prospettive ritraggono Bitcoin sulla strada per diventare un bene rifugio paragonabile all'oro e quindi un buon candidato per contrastare l'inflazione anche se è un asset ancora troppo giovane, poco conosciuto, poco compreso e non regolamentato. Ad oggi la quota di mercato di Bitcoin equivale a poco meno del 3,5%[92] di quella dell'oro, in crescita costante.

1.6 Ethereum 1.0



Ethereum: The Ultimate Smart Contract and Autonomous Corporation Platform on the Blockchain

In the last few months, there has been a great amount of interest into the area of using the Bitcoin blockchain, the mechanism that allows for the entire world to agree on the state of a public ownership database, for more than just money. Perhaps the first, and oldest, such alternative application is colored coins, which is a protocol that allows users to label specific bitcoins and treat them as assets representing some real world value - whether company shares, collectibles or even existing currencies like gold and USD. A more independent alternative, Ripple, also includes the ability to create custom currencies and assets, but adds a decentralized exchange. More recently, Mastercoin has started to go even further, allowing more complex financial contracts such as hedging, trust-free dice rolls, binary options and self-stabilizing currencies - essentially, almost any common financial instrument imaginable. Taken together, all of these projects can be thought of as initial efforts toward a sort of "cryptocurrency 2.0" - they are to Bitcoin what Web 2.0 was to the World Wide Web circa 1995.

At the same time, there has been significant interest in "decentralized autonomous corporations" - autonomous entities that operate on the blockchain in a completely transparent and publicly managed way without any central control whatsoever. Rather than the relationships of the investors, owners and employees of the corporation being mediated by a legal contract or a set of organizational bylaws, the funds and corporate resources are managed directly on the blockchain. However, decentralized autonomous corporations are difficult to implement today, simply because the scripting systems of Bitcoin, and even proto-cryptocurrency 2.0 alternatives like Ripple and Mastercoin, are far too limited to allow the kind of arbitrarily complex computation that DACs require. Although these platforms have begun to offer increasingly complex contracts such as financial derivatives, order matching and trust-free bets, the way that the protocols are set up is inherently limited and closed-ended: each of these use cases is treated as a specific transaction type, not allowing any way for users to build contracts that the developers have not specifically chosen to include.

What this project intends to do is take cryptocurrency 2.0, and generalize it - create a fully-fledged, Turing-complete (but heavily fee-regulated) cryptographic ledger that allows participants to encode arbitrarily complex contracts, autonomous agents and relationships that will be mediated entirely by the blockchain. On-chain currencies, futures contracts, prediction markets, Namecoin-style domain name systems and even provably fair gambling sites will become trivial to implement, existing as simple, hundred-line-of-code contracts on the chain.

Figura: Rappresentazione Grafica del Whitepaper di Ethereum.[93].

1.6.1 Storia di Ethereum

Proposta da un giovane sviluppatore di nome Vitalik Buterin, nel 2014 in un blog post intitolato "Ethereum: The Ultimate Smart Contract and Decentralized Application Platform"[94]. Ethereum si è presentata come approfondimento dell'idea introdotta da bitcoin per applicarla a qualsiasi tipo di applicazione mirando a

[92] **Rapporto tra Capitalizzazione di Mercato dell'Oro con la Capitalizzazione di Mercato di Bitcoin**, https://companiesmarketcap.com/assets-by-market-cap/
[93] **Buterin Vitalik** Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Cit.
[94] https://vitalik.ca/general/2017/09/14/prehistory.html

scoprire se la tecnologia blockhain ha utilizzi validi al di fuori dei limiti di progettazione intenzionali della rete Bitcoin, il quale presenta limitato insieme di transazione, tipo di dati e dimensione di archiviazione dei dati, il che non permettono una programmabilità semplice e flessibile ma una semplice "valutazione vero/falso delle condizioni di spesa"[95]. Nonostante lo sviluppo del protocollo e una trasformazione radicale dei concetti di denaro e valuta, bitcoin non permetteva di eseguire determinate applicazioni limitando alcune delle potenzialità della blockchain. Una nuova blockchain pubblica era l'unica soluzione per quei progetti che necessitavano di maggiore libertà e flessibilità. Al momento della fondazione la destinazione d'uso della blockchain Ethereum non era intenzionalmente definita, in modo tale che potesse supportare un'ampia varietà di applicazioni blockchain decentralizzate attraverso una programmazione sicura e deterministica. L'attenzione si è sempre più spostando verso quelle applicazioni basate su blockchain che rappresentano valute e strumenti finanziari personalizzati, la proprietà di un dispositivo fisico sottostante, risorse non fungibili come nomi di un dominio e applicazioni più complesse che comportano la presenza di risorse digitali controllate direttamente da codice che regola regole arbitrarie come gli Smart Contract o addirittura nuovi modelli organizzativi come le DAO[96].

1.6.2 Che cos'è Ethereum

Definita come il "computer del mondo"[97], Ethereum intende fornire le proprie funzionalità attraverso un linguaggio di programmazione esaustivo denominato "Turing-complete" [98], in altri termini questa blockchain si definisce come un computer decentralizzato che, con tempo e risorse sufficienti, potrebbe potenzialmente eseguire qualsiasi applicazione. Ethereum, "può essere utilizzato per creare contratti (Smart Contract), i quali a loro volta possono essere utilizzati per codificare funzioni di transizione di stato arbitrarie, permettendo agli utenti di

[95] **Antonopoulos Andreas M. and Wood Gavin** Mastering Ethereum [Book]. - [s.l.] : O'Reilly Media. 2018. Pag. 2

[96] **Ethereum.org** Decentralized autonomous organizations (DAOs).Ethereum.org. 2022, https://ethereum.org/en/dao/#what-are-daos.

[97] **Antonopoulos Andreas M. and Wood Gavin** Mastering Ethereum. Cit. Pag. 8

[98] In informatica si definisce **Turing Complete** una macchina che, con il tempo e la memoria sufficienti insieme alle istruzioni necessarie può risolvere qualsiasi tipo di calcolo, non importa quanto complesso, https://academy.binance.com/en/glossary/turing-complete

creare un sistema scrivendo la logica in poche righe di codice"[99]. Solo il tempo e l'immaginazione può limitare i tipi di applicazioni che potrebbero essere implementate su questa blockchain. Ethereum è più simile a un mercato di servizi finanziari, giochi, social network e altre app che rispettano la privacy dell'utente e abboliscono la censura fornendo verificabilità, trasparenza e neutralità. Utilizza il modello blockchain per sincronizzare memorizzare i cambiamenti di stato del sistema, insieme a una criptovaluta denominata "Ether" per misurare e limitare i costi delle risorse di esecuzione, non è controllato da nessuna entità e utilizza il meccanismo di consenso Proof-Of-Work come Bitcoin sfruttando il processo di Mining ma con alcune differenze. Il mining garantisce che la blockchain venga aggiornata seguendo regole e consentendo al network senza un'organizzazione centrale. Esiste l'esclusiva partecipazione decentrata e la cooperazione della comunità, la rete infatti fa uso di nodi gestiti da volontari, privati o aziende in ogni parte del mondo, che dedicano la propria potenza computazionale alla risoluzione di un enigma crittografico fornendo una resilienza unica a tutta l'infrastruttura di rete, rendendo meno vulnerabile all'hacking o agli arresti del sistema. Ciò che fanno effettivamente è "l'hashing"[100] di un set di transazioni in sospeso, insieme ad altri dati. Per fare in modo che il blocco sia considerato valido la hash deve essere inferiore a un valore definito dal protocollo e i miner per competere fra loro devono riuscire a generare hash il più velocemente possibile, la loro potenza è misurata in un'unità di misura denominata "Hash Rate"[101]. Maggiore è l'hash rate sul network, più difficile sarà l'enigma da risolvere. Una volta trovata è facile per gli altri partecipanti controllare la validità. Il network Ehereum, come per bitcoin distribuisce una ricompensa come incentivo per incentivare i miner a svolgere il loro operato e di conseguenza proteggere il network. Ethereum introduce il concetto di "Gas"[102] per mitigare il rischio di far eseguire all'infinito un contratto con lo

[99] **Buterin Vitalik** Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Cit.
[100] Con il termine **Hashing** si intende il processo che genera un output di dimensione fissa partendo da un input di dimensione variabili, **Binance** Cos'è l'Hashing. Binance Accademy. 2019, https://academy.binance.com/it/articles/what-is-hashing.
[101] Per **Hash Rate** si intende la velocità con cui opera hardware di mining per calcolare un hash di blocco valido, https://academy.binance.com/en/glossary/hash-rate
[102] Il termine **Gas** si riferisce ad un'unità di misura che indica la quantità di sforzo di calcolo necessaria per eseguire operazioni specifiche sulla rete Ethereum, più precisamente il Gas o

stesso codice da un nodo (SPAM), il che richiederebbe troppe risorse e porterebbe il sistema al crollo. In sostanza, è un meccanismo di commissioni collegato alle transazioni che vogliono essere effettuate dagli utenti e si collega all'incentivo verso i nodi validatori, che motivati dal profitto ignoreranno le transazioni con una commissione troppo bassa privilegiando la partenza di quelle con una commissione più elevata. La criptovaluta Ether (Eth) con la quale vengono ricompensati i Miner è diversa dal gas utilizzato per far partire la transazione, il quale viene comunque pagato in Ether. dall'utente. Il prezzo medio del gas è deciso dai nodi validatori, se il network risulta intasato e molti utenti cercano di effettuare transazioni, il prezzo del gas aumenterà, mentre se la rete risulta essere libera allora il prezzo sarà basso. Il gas, quindi, misura la potenza computazionale necessario per eseguire uno Smart Contract, anche in base alla sua complessità. Grazie a questo "modello"[103] Ethereum dal suo lancio nel 2015 non ha mai subito un solo momento di inattività, ad oggi ci sono migliaia di nodi sparsi per il mondo che autonomamente eseguono la rete rendendola per decentralizzazione seconda solo a Bitcoin. Sono diverse le attività costruite su questa blockchain, essa grazie al suo sistema di prestiti, prodotti di risparmio e una connessione a internet, rende le attività bancarie accessibili a tutti in un mondo in cui oramai è necessario presentare sempre più garanzie per poter accedere a servizi finanziari. L'utilizzo della blockchain come succede anche con bitcoin, non necessita di tutte le informazioni degli utilizzatori, infatti, si basa su un'economia basata sul valore piuttosto che sulla sorveglianza come accade per i sistemi tradizionali. La rete non permette il controllo di un governo o azienda specifica, è impossibile l'impedimento di ricezione, invio di pagamenti e utilizzo dei servizi interni. Gli utenti hanno una garanzia integrata e sicura riguardo allo spostamento dei propri fondi accordato preventivamente e tutte le applicazioni costruite sulla Blockchain Ethereum hanno uno stato globale condiviso, possono essere costruite a vicenda e sviluppate da chiunque ne abbia le capacità portando di fatto miglioramenti costanti da cui tutti possono trarne beneficio. Ad oggi Ethereum conta circa "±2970 progetti costruiti su esso, + 71 Milioni di Wallet con

Carburante si riferisce alla commissione richiesta per far si che una transazione su Ethereum vada a buon fine, https://ethereum.org/it/developers/docs/gas/

[103] **Binance** Cos'è Ethereum? Binance Accademy. 2020, https://academy.binance.com/it/articles/what-is-ethereum.

all'interno la cripotovaluta "Ether", +50,5 Milioni di Smart Contract in esecuzione, $ 11,6 Trilioni di dollari scambiati all'interno del network nel 2021, $ 3,5 Miliardi di dollari guadagnati dai creatori e sviluppatori della blockchain e circa +1,679 Milioni di transazioni completate proprio in questo momento dagli utenti"[104]. La rete, nonostante le grandi cifre sopra riportate è ancora in uno stato giovane e in fase di continuo sviluppo e miglioramento, basta notare i casi d'uso che vengono scoperti continuamente nel tempo e che soltanto ultimamente aziende, artisti, musicisti, scrittori, videogiocatori e rifugiati hanno cominciato a comprendere e utilizzare Ethereum come soluzione alternativa e innovativa per conseguimento dei propri interessi.

1.7 Ethereum 2.0

Ethereum 2.0 è un aggiornamento del network Ethereum che promette dei miglioramenti significativi alla struttura, le funzionalità e all'esperienza dell'utente nella piattaforma. Sono infatti sorte delle "Problematiche relative alla Scalabilità"[105] e al consumo eccessivo di energia elettrica non permetterebbero un sostenibile sviluppo di questa tecnologia. Alcuni aggiornamenti più importanti includono la transizione dall'algoritmo Proof-Of-Work a Proof-Of-Stake, l'introduzione delle Shard Chain e una nuova blockchain organizzatrice chiamata Beacon Chain. Dal lancio di Ethereum 1.0, gli utenti utilizzatori sono cresciuti costantemente e con loro sviluppo di nuove Dapp.

[104] **Ethereum.org** What is Ethereum? The foundation for our digital future. Ethereum in numbers. 2022, https://ethereum.org/en/what-is-ethereum/.

[105] Il **Problema della Scalabilità** sorge a causa dei limiti fissati sul numero delle transazioni che possono essere elaborate all'interno della blockchain, per impedire che il database arrivi a dimensioni troppo grandi. Infatti, se i blocchi sono troppo pesanti, non è possibile trasmetterli rapidamente attraverso il network. A causa di ciò un network molto popolato come Ethereum risulta spesso intasato, il che causerà un aumento delle commissioni per far si che le transazioni vengano incluse in tempi ragionevoli. **Binance** Scalabilità Blockchain - Sidechain e Canali di Pagamento. Binance Accademy. 2020 https://academy.binance.com/it/articles/blockchain-scalability-sidechains-and-payment-channels#the-blockchain-scalability-problem.

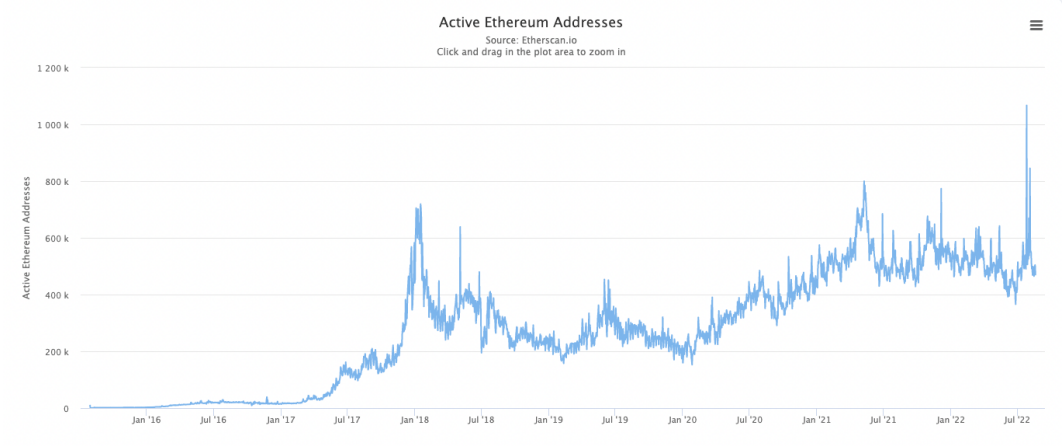


Figura: Rappresentazione Grafica del numero giornaliero di indirizzi unici attivi operanti sul Network Ethereum dal 2016 al 2022(Luglio)[106].

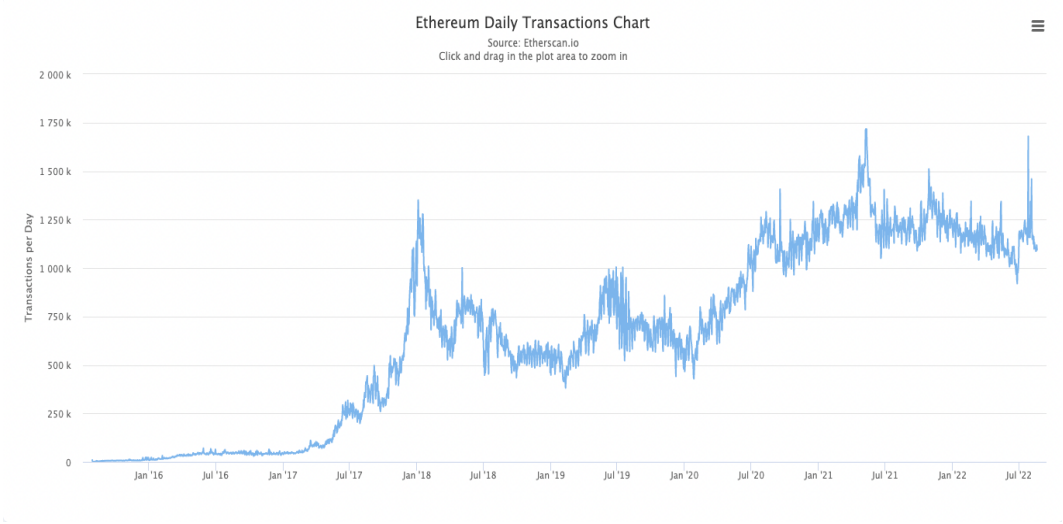


Figura: Rappresentazione Grafica delle Transazioni totali giornaliere effettuate su Network Ethereum dal 2016 al 2022(Luglip)[107].

[106] https://etherscan.io/chart/active-address
[107] https://etherscan.io/chart/tx

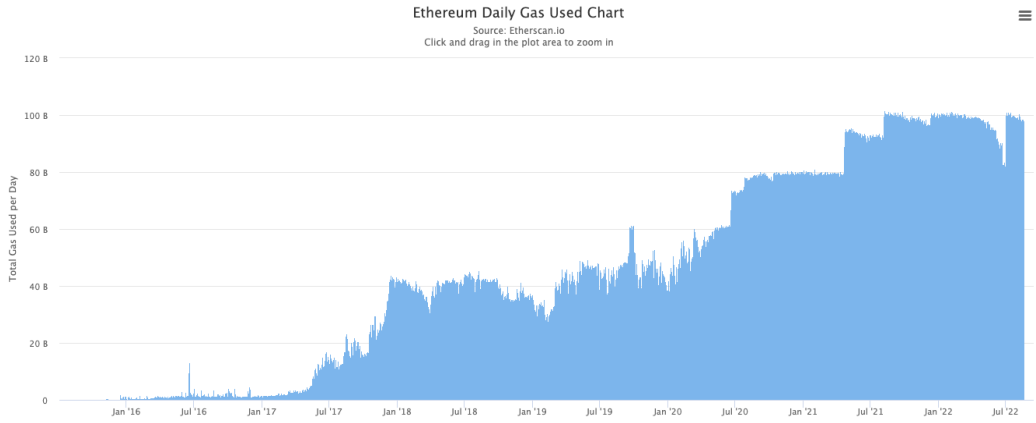


Figura: *Rappresentazione Grafica del "gas" utilizzato giornalmente sul Network Ethereum dal 2016 al 2022(Luglio)*[108].

Mentre il numero di transazioni sul network di Ethereum aumentava anche il costo ad esse associato sotto forma di Gas. Per sopportare un grande numero di transazioni come ci si aspetta nel prossimo futuro grazie a una potenziale adozione di massa, la piattaforma necessitava di aggiornamenti o implementazioni che avrebbero risolto la questione scalabilità e la problematica del consumo energetico.Le Blockchain regolate dall'algoritmo di consenso Proof-of-Work consumano una quantità di energia elettrica molto ingente in quanto richiede una potenza di calcolo sempre maggiore man mano che la blockchain cresce. Consultando i dati riportati dal "Bitcoin Energy Consumption Index", Bitcoin "consuma nel 2022 circa 139,35 TeraWatt-ore (TWh) di energia elettrica"[109] che corrisponde a circa lo "0,57%"110 del consumo totale annuale di elettricità mondiale.

[108] https://etherscan.io/chart/gasused
[109]**Digiconomist** Bitcoin Energy Consumption Index. 2022 https://digiconomist.net/bitcoin-energy-consumption.
[110] **% del Consumo Totale Elettrico di Bitcoin rispetto al Totale Mondiale**, ottenuto calcolando il rapporto del consumo energetico di Bitcoin e il dato relativo al consumo elettrico mondiale del 2019. https://www.statista.com/statistics/280704/world-power-consumption/

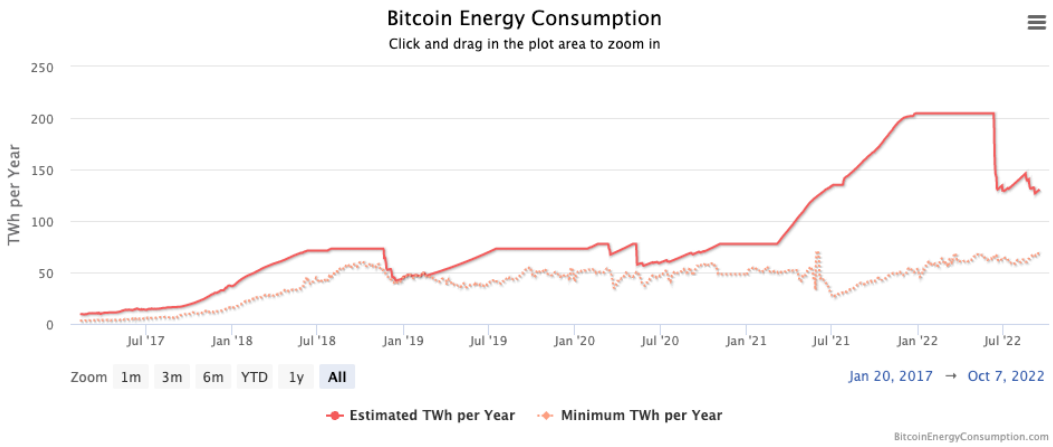


Figura: *Rappresentazione Grafica del consumo energetico annuo misurato in TeraWatt-ore (TWh) da parte del Network Bitcoin dal 2017 al 2022(Settembre)*[111].

Per quanto riguarda Ethereum secondo i dati riportati dal Ethereum energy Consumption Index sono state usate a luglio circa un totale di 85,67 TeroWatt-Ora (TWh) di energia elettrica[112] che corrispondeva a circa lo 0,36%[113] del consumo totale annuale di elettricità nel mondo, mentre ad oggi con il ridimensionamento avvenuto con successo con l'evento Ethereum Merge[114] ad Ethereum 2.0, le emissioni sono quasi azzerate rendendo di fatto Ethereum una tecnologia green.

[111] **Digiconomist** Bitcoin Energy Consumption Index. Cit.
[112] **Digiconomist** Ethereum Energy Consumption Inde. 2022, https://ethereumenergyconsumption.com/.
[113] **% del Consumo Totale Elettrico di Ethereum rispetto al Totale Mondiale**, ottenuto calcolando il rapporto del consumo energetico di Ethereum e il dato relativo al consumo elettrico mondiale del 2019. https://www.statista.com/statistics/280704/world-power-consumption/
[114] **Battaglia Alberto** Ethereum Merge: l'evento crypto dell'anno è andato in porto. We Wealth. 2022, https://www.we-wealth.com/news/fintech/blockchain/ethereum-merge-l-evento-crypto-dell-anno-e-andato-in-porto

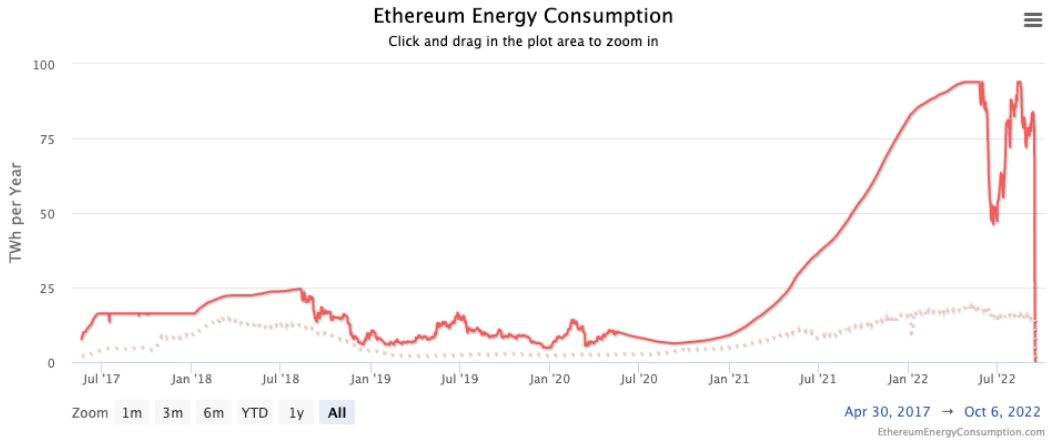


Figura: *Rappresentazione Grafica del consumo energetico annuo misurato in TeraWatt-ore (TWh) da parte del Network Ethereum dal 2017 al 2022(Settembre)*[115].

La sfida più grande per Ethereum è migliore scalabilità senza al contempo intaccare negativamente la decentralizzazione e la sicurezza del network, caratteristiche molto importanti e impattanti.

1.7.1 Proof-Of-Stake, Sharding e La Beacon Chain

Negli ultimi anni è emerso un nuovo algoritmo di consenso chiamato Proof-Of-Stake attraverso il quale, poter convalidare le transazioni e partecipare al processo di "forgiatura" dei blocchi, i nodi validatori devono necessariamente bloccare una certa quantità di monete sul network al posto di utilizzare potenza di calcolo derivante da hardware. Questo processo è definito "Stake"[116] e riduce di gran lunga il consumo di energia necessario e migliora la scalabilità anche se può risultare meno accessibile a utenti che non dispongono di una quantità sufficiente di criptovalute. L'algoritmo "PoS"[117] segue un processo di selezione pseudo-casuale per individuare i validatori all'interno di un gruppo di nodi. Il sistema utilizza una combinazione di tre fattori per evitare la centralizzazione:

[115] **Digiconomist** Bitcoin Energy Consumption Index. Cit.
[116] Con il termine **Stake** o Staking, si intende l'atto di bloccare criptovalute, sostenendo la sicurezza e le operazioni di un network blokchain per ricevere ricompense, **Binance** Cos'è lo Staking? Binance Accademy. 2019, https://academy.binance.com/it/articles/what-is-staking.
[117] Proof-of-Stake

La ricchezza del nodo validatore: L'ammontare delle monete detenute e bloccate dal nodo in determina le possibilità di essere selezionato come prossimo validatore e ricevere la ricompensa.

Elemento di randomizzazione: Denominata anche "Randomized Block Selection"[118], nella quale i validatori delle transazioni vengono selezionati tra i vari nodi esistenti attraverso una combinazione tra il valore di hash più basso e lo stake più alto.

L'età dello staking: Chiamata anche "Coin Age Selection"[119] , i nodi sono scelti in base al tempo di staking del token di riferimento. La selezione viene calcolata prendendo il numero dei giorni a partire dal quale le monete sono state messe in staking e moltiplicato per il numero totale di monete in staking. Una volta creato un nuovo blocco, questo parametro viene azzerato in modo tale da impedire che i grandi nodi presenti da tempo dominino la blockchain.

Quando un nodo viene scelto per creare il blocco successivo, verificherà se le transazioni del blocco sono valide per poi firmare il blocco e aggiungerlo alla blockchain. Come ricompensa, il nodo riceve le commissioni di transazione dal blocco e alcune ricompense in monete. Per quanto riguarda il meccanismo con cui vengono convalidate le transazioni, ogni criptovaluta che utilizza questo algoritmo di consenso ha un'impostazione ben precisa e metodi combinati per raggiungere la migliore combinazione possibile per la propria rete e i suoi utenti. Se un nodo vuole smettere di forgiare nuovi blocchi, l'importo messo in staking e le ricompense guadagnate verranno rilasciate dopo un determinato periodo, così per dare alla rete il tempo di verificare che non vi siano blocchi con dati falsi aggiunti alla blockchain da questo nodo.

I "vantaggi principali"[120] di questo algoritmo sono principalmente:

[118] Randomized Block Selection, **Binance** What Is Proof of Stake (PoS)? Binance Accademy. 2018, https://academy.binance.com/en/articles/proof-of-stake-explained.
[119] Coin Age Selection, **Binance** What Is Proof of Stake (PoS)? Cit.
[120] Vantaggi Proof-Of-Stake, **Binance** What Is Proof of Stake (PoS)? Cit.

L'adattabilità: la PoS risulta essere versatile alla maggior parte delle applicazioni blockchain.

La Decentralizzazione: più utenti sono incoraggiati a eseguire i nodi perché la gestione risulta più conveniente, risultando di fatto come un incentivo alla partecipazione con il processo di randomizzazione.

Efficienza in termini di spesa ed energia consumata: il costo della partecipazione è attribuito a quello economico relativo allo staking mentre nel proof of work il costo è principalmente di tipo computazionale.

La scalabilità: molto elevata perché non c'è bisogno di macchine fisiche per generare consenso e aggiungere nuovi validatori alla rete è più economico, semplice e accessibile.

La Sicurezza: Motivata dallo staking, la sicurezza spinge il nodo selezionato a validare a non elaborare transazioni fraudolente. Se la rete dovesse rilevarne una, allora il nodo perderà parte della sua quota in staking e il diritto a partecipare in futuro alla rete. Quindi finché l'importo in staking è maggiore delle ricompense potenziali allora perderebbe più di quanto guadagnerebbe se intraprendesse un'attività illecita.

Gli "svantaggi"[121] sono:

L'accessibilità: Per fare staking è necessario un ammontare del token nativo di una blockchain e ciò richiede spesso un acquisto ingente del token tramite un Exchange.

51% attack"[122]: C'è una maggior probabilità di centralizzazione e abusi di potere nel caso il prezzo del token del protocollo in questione crolli significativamente, o che la blockchain abbia una bassa capitalizzazione di mercato permettendo l'acquisto di più del 50% del "token circolante" riuscendo di fatto a controllare e potenzialmente compromettere la rete.

[121] Svantaggi Proof-Of-Stake, **Binance** What Is Proof of Stake (PoS)? Cit.
[122] **Binance** Cos'è un 51% Attack? Binance Accademy. - 2018. - https://academy.binance.com/it/articles/what-is-a-51-percent-attack.

In Ethereum 2.0, detenendo un minimo di Eth, precisamente 32, impegnarli e metterli in stake un utente può diventare a tutti gli effetti un validatore della blockchain e venire pagato per confermare transazioni. Per permettere il ciò sono necessari degli aggiornamenti che introdurranno implementazioni alla struttura:

Le Shard Chain: Introdotte attraverso un aggiornamento multifase denominato "Sharding"[123] migliorano la scalabilità e la capacità di Ethereum, forniscono dei livelli di archiviazione dati aggiuntivi e più economici e "Rollup"[124] per memorizzare i dati e consentono a soluzioni Layer 2 di offrire commissioni di transazione contenute sfruttando al contempo la sicurezza della blockchain principale Ethereum. Un nodo su Ethereum conserva una copia dell'intero network, scaricando, computando, archiviando ed elaborando ogni singola transazione dalla nascita di Ethereum e questo rallenta tutto il sistema. L'implementazione delle shard chain ridurrà la congestione della rete e aumentando il numero di transazioni al secondo creando nuove catene chiamate shard, che contengono solo un sottoinsieme specifici di un'intera blockchain.

La Beacon Chain: Una nuova blockchain che svolgerà un ruolo centrale in Ethereum 2.0, si assicurerà che le shard chain rimangano sincronizzate tra loro, scambiando informazioni, coordinando di fatto il network. Senza di essa, non sarebbe possibile l'implementazione dell'algoritmo di consenso Proof-of-Stake. "Il suo ruolo è una componente fondamentale per la sicurezza, la sostenibilità e la scalabilità di Ethereum"[125].

In assenza di un aggiornamento di questo tipo, Ehtereum, nel lungo periodo con molta probabilità sarebbe surclassata da altre blockchain emergenti e rischierebbe di perdere la posizione di piattaforma per smart contract leader nell'ecosistema crypto.

---

[123] **Ethereum.org** Shard chain. Ethereum.org. 2022, https://ethereum.org/it/upgrades/sharding/.

[124] I **Rollup** di ethereum hanno la funzione di raccogliere in unico blocco molte transazioni, rendendo la rete molto più veloci, **Cacioppoli Vincenzo** Il ruolo dei rollup sulla scalabilità di Ethereum. Cryptonomist. 2022. https://cryptonomist.ch/2022/08/05/ruolo-rollup-scalabilita-ethereum/

[125] **Ethereum.org** La Beacon Chain. Ethereum.org. 2022, https://ethereum.org/it/upgrades/beacon-chain/#main-content .

CAPITOLO 3: Nuove Prospettive e Pericoli per la Stabilità economica

A fronte delle potenzialità offerte dalla digitalizzazione, il settore finanziario ne sta sempre di più usufruendo. In particolare, l'utilizzo delle criptovalute e le attività che ne derivano possono generare rischi di vario genere, compromettendo potenzialmente la stabilità del sistema finanziario a causa dell'interdipendenza dei soggetti che vi partecipano, regolamentati e non regolamentati, e della mancanza di strumenti di controllo che possono limitare eventuali eventi sfavorevoli. La deregolamentazione riguardo questo mondo è ancora marcata, sono in corso infatti a livello internazionale ed europeo i lavori per disegnare un nuovo insieme di regole e di controlli per questi prodotti e per i relativi ecosistemi, che per entrare in vigore a tutti gli effetti avrà sicuramente bisogno ancora tempo. Negli anni l'elevata crescita, il numero e le oscillazioni del valore delle criptovalute hanno dato luce a episodi di crisi di operatori, "truffe"[126], incidenti informatici o difetti alla base delle tecnologie che hanno portato ingenti perdite, un esempio recente è il fallimento della stablecoin algoritmica Terra-Usd[127] che ha causato il collasso di un ecosistema del valore di circa 60 Miliardi replicando le conseguenze, questa volta nel mercato delle criptovalute, seppur di portata decisamente inferiore, a quanto successo nel mercato tradizionale con il crollo finanziario del 2008. L'estrema volatilità e continua adozione[128] di questi asset ha sollevato non poche preoccupazioni delle principali autorità. Fra queste, la Banca d'Italia e la Federal Reserve, interessate al

[126] Una molto impattante è da attribuire a Bitfinex nel 2016, Exchange di criptovalute al quale sono stati rubati circa 119.756 Bitcoin per un controvalore ad oggi di circa $ 633 Milioni di Dollari, **Travia Niccolò** Il "caso" Bitfinex: attacco hacker o semplice frode, che c'è da sapere. Agenda Digitale. 2019, https://www.agendadigitale.eu/documenti/il-caso-bitfinex-attacco-hacker-o-semplice-frode/

[127] Il fallimento della Stablecoin algoritmi UST che aveva una riserva di garanzia non stabile, è stato causato dalla perdita dell'ancoraggio al Dollaro che ha portato al collasso di tutto l'ecosistema e conseguenze per tutto il mercato delle criptovalute, accentuando l'interesse e il bisogno secondo le autorità di un adeguata regolamentazione. **Davies Pascale** Spiegazione del crollo della stablecoin Terra Luna: è questo il momento del crollo finanziario della criptovaluta del 2008? Euronews.next 2022, https://www.euronews.com/next/2022/05/12/terra-luna-stablecoin-collapse-is-this-the-2008-financial-crash-moment-of-cryptocurrency.

[128] La tendenza a fluttuare delle criptovalute in brevi periodi di tempo aggrava l'influenza di bias cognitivi legati all'interpretazione delle informazioni in condizioni di incertezza, come pregiudizi di eccesso di ottimismo. **Davola Antonio** Bias Cognitivi e Contrattazione Standardizzata: Quali tutele per i consumatori? Contratto e Impresa. 2017.

controllo prudenziale sugli intermediari vigilati, alla sorveglianza sul regolare funzionamento del sistema dei pagamenti, alla stabilità monetaria finanziaria, al contrasto dei furti e riciclaggio di denaro[129], al finanziamento del terrorismo e la tutela della clientela. L'attenzione richiamata è quella degli intermediari vigilati (Exchange) e quelli che operano negli ecosistemi decentralizzati, anche come utenti, con riguardo alle opportunità e ai rischi derivanti dall'utilizzo di tali tecnologie nella finanza e riguardo attività e servizi relativi a emissione, custodia, scambio, prestiti e servizi di pagamento. Per questi enti è necessario evidenziare e definire i volti per alcuni profili rilevanti, per attenuare i rischi connessi con l'impiego e l'operatività delle tecnologie decentralizzate e delle cripto attività. In merito a ciò è avanzata la volontà di alcuni obblighi relativi alla raccolta dati degli utenti, procedure Know Your Customer[130]. Secondo la Banca d'Italia: "l'elemento qualificante in questo caso si trova nel fattore tecnologico che è in grado di far interagire diversi attori di sistema anche in mancanza di relazioni dirette"[131]. La forte connessione fra gli sviluppatori degli algoritmi con schemi e accordi i quali contribuiscono a trasferimenti di valore costituisce la ragione per cui le banche centrali osservano e monitorano attentamente affinché la stabilità finanziaria e monetaria non venga intaccata. Il comunicato della Banca D'Italia evidenzia che "i rischi finanziari ai quali espone la tecnologia di cui stiamo parlando non sono diversi da quelli della finanza tradizionale, troviamo infatti il rischio di credito, di mercato, operativo, cibernetico e di liquidità accrescendone però la rilevanza in materia di stabilità finanziaria derivante dal rischio operativo all'interno di un ecosistema decentralizzato, del rischio riguardo le vulnerabilità dell'innovazione DLT, dal rischio cibernetico e frodi legati alla presenza di soggetti non regolati che agiscono in maniera autonoma, dalla presenza di strumenti e paradigmi tecnologici

[129] **Carlini Vittorio** Cripto, nella finanza decentralizzata è boom di furti e riciclaggio. Sole24Ore 2022, https://24plus.ilsole24ore.com/art/cripto-finanza-decentralizzata-e-boom-furti-e-riciclaggio-AEhU6LmB

[130] **Barbieri Giacomo** Cosa sta facendo la Ue per regolamentare le criptovalute. La Repubblica. 2022.
https://www.repubblica.it/tecnologia/2022/04/25/news/gli_sforzi_di_regolamentazione_delle_crypto_in_ue_spiegati_per_bene-346309419/

[131] **Banca D'Italia** Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanzaecripto-attività Banca D'Italia 2022,
https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-cripto.pdf

non regolamentati, dall'assenza di standard di settore di riferimento e dalla dimensione transazionale del fenomeno che rende difficile la regolamentazione all'interno delle singole giurisdizioni"[132]. Quindi il rapido sviluppo di tecnologie può incidere sulla stabilità del sistema finanziario in virtù della connessione e intraprendenza tra i soggetti coinvolti che operano in un contesto che è privo di regole e controlli, pertanto, è necessario definirne i rischi:

Il rischio di Credito: Si presuppone che la controparte "non sia in grado di adempiere integralmente ai propri obblighi di debito alla scadenza o in qualsiasi momento durante la durata dell'esposizione debitoria"[133]. Nelle criptovalute non è presente una valutazione del rischio come per il sistema tradizionale per cui si è assistito a crisi che hanno comportato l'impossibilità per alcune società di prestito di adempiere ai propri obblighi debitori, un esempio è la società di prestito Celsius[134].

Il rischio di Liquidità: La controparte in questo caso "non dispone di fondi sufficienti per adempiere ai propri obblighi finanziari alla scadenza, ma potrebbe farlo in futuro"[135].

Il rischio Operativo: Si intende "il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni"[136]

Il rischio Cibernetico: Conosciuto anche come rischio informatico rappresenta "la violazione di sicurezza che comporta accidentalmente o in modo illecito la

---

[132] **Banca D'Italia** Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività . Cit.
[133] **Rischio di Credito**, https://www.borsaitaliana.it/borsa/glossario.html
[134] Celsius Network, società di prestiti in criptovalute, ha presentato istanza di protezione dal fallimento, ultimo anello di una reazione a catena innescata di una sorta di reazione a catena innescata dal crac della stablecoin algoritmica Terra-Luna, che ha travolto e affondato l'hedge fund cripto Three Arrow Capital. **Culicchi Roberto** Le criptovalute gettano le famiglie sul lastrico: il caso Celsius e la necessità di un intervento legislativo. Network Digital 360. 2022, https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/le-criptovalute-gettano-le-famiglie-sul-lastrico-il-caso-celsius-e-la-necessita-di-un-intervento-legislativo/
[135] **Rischio di Liquidità**, https://www.borsaitaliana.it/borsa/glossario/rischio-di-liquidita-.html -
[136] **Banca D'Italia** Recepimento della nuova regolamentazione prudenziale internazionale. Rischi Operativi.Banca D'Italia. 2006,
https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2006/basilea2/Doc_Cons_Rischi_operativi.pdf

distruzione, la perdita, la modifica o la divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati"[137], è un rischio di tipo operativo associato a perdite economiche inflitte, un esempio può essere lo spegnimento improvviso del Server, furto di dati sensibili, oppure per quanto riguarda gli ecosistemi blockchain, errori nello smart contract.

Il rischio di Mercato: È il rischio in cui incorre l'investitore in seguito ad effetti imprevedibili riguardo "il valore di mercato di attività e passività prodotti da variazioni dei tassi di interesse, dei tassi di cambio e da altri prezzi delle attività"[138].

Il rischio Reputazionale: Rispecchia la possibilità che la pubblicità negativa, la percezione pubblica o gli eventi incontrollabili abbiano un impatto negativo sulla reputazione.

Questi tipi di rischi sono concetti distinti ma spesso correlati. In un sistema finanziario con intermediari finanziari che hanno la responsabilità di facilitare i processi di pagamento, compensazione o regolamento e talvolta anche di garantire il regolamento di una transazione per conto dei propri clienti o partecipanti, gran parte di questo rischi è assunto e gestito centralmente dall'intermediari attraverso, per esempio, il rispetto del requisito che gli obblighi di pagamento siano completamente prefinanziati o quelli che mitigano e gestiscono i rischio consentendo la pubblicazione di garanzie a scarti di garanzia ragionevoli. La finanza decentralizzata espone l'investitore a dei rischi a volte sconosciuti, in assenza di tutela del depositante gli utenti possono perdere tutto l'investimento a cause di crolli improvvisi, frodi e chiavi private perse oltre alle difficoltà di attribuire le responsabilità verso una gestione che risulta decentralizzata. in tutto il mondo si stanno diffondendo sempre nuove iniziative e proposte di regolamentazione che creino un ambiente chiaro favorevole allo sviluppo di un sistema con un grande potenziale sia per i paesi già sviluppati che per paesi che non dispongono di mezzi e che beneficerebbero di tali sistemi che ne aumenterebbero la competitività. Ad oggi "i regulators delle economie avanzate […] stanno

[137] GDPR - *Regolamento Europeo 679/2016, Art. 4 Comma 12 "Violazione dei dati Personali"*
[138] **Rischio di Mercato**, https://www.borsaitaliana.it/borsa/glossario/rischio-di-mercato.html-

rapidamente riorientando il focus sul tema della finanza decentralizzata"[139]. Anche l'impatto ambientale delle nuove tecnologie ad oggi è tenuta sotto stretta osservazione, infatti si prospetta nell'interesse verso dei parametri ESG (Environmental, Sociale, Governance) di un adattamento, che renda sostenibile e in linea con la realtà odierna, l'utilizzo di blockchain come Bitcoin che fanno utilizzo del meccanismo di consenso Proof Of Work. Riguardo le pratiche di mining, infatti, si è riscontrato negli ultimi anni uno spostamento verso paesi dove vengono utilizzate fonti di energia rinnovabili e pratiche di utilizzo di energia che altrimenti andrebbe sprecata oltre al crescente sviluppo e utilizzo di ecosistemi basati su protocolli di consenso Proof Of Stake, "le criptovalute a basso impatto ambientale sono possibili e rappresentano una svolta concreta"[140].

1.8 Regolamentazione in Europa: MiCA e DORA

In **Europa**, è stata discussa una la strategia inerente alla finanza digitale definita dalla commissione europea a settembre del 2020, in tale occasione sono state pubblicate due proposte legislative: Il Markets in Crypto Assets Regualtion[141] (MiCAR), e il "Digital Operational Resilence Act"[142] (DORA).

1.8.1 MICA

La Commissione Europea il 24 settembre 2020 ha adottato un nuovo dettagliato pacchetto di finanza digitale contenente misure con l'obiettivo di trasformare l'economia europea nei prossimi anni a fronte delle nuove necessità. Il contenuto

[139] **Minenna Marcello** Criptovalute: perché il 2022 sarà l'anno dei regulators. Sole24Ore. 2021, https://www.ilsole24ore.com/art/criptovalute-perche-2022-sara-l-anno-regulators-AEN03wo
[140] **Web ToEmotion** Cambiamenti climatici tra ESG e criptovalute [Online]. 2022, https://blog.web2emotions.com/sostenibilita/cambiamenti-climatici-tra-esg-e-criptovalute/.
[141] **Commissione Europea** Regolamento del Parlamento Europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937. 2020, https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0008.02/DOC_1&format=PDF.
[142] **Commissione Europea** Regolamento del Parlamento Europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014. 2020, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0595&from=EN.

di questo pacchetto mira a migliorare la competitività dei settori Fintech e Tecnologici del continente, ridurre i rischi e garantire la stabilità finanziaria assicurando al contempo l'accesso ai consumatori di prodotti più innovativi mantenendo intatta la loro protezione. Il nuovo quadro normativo include una proposta legislativa completa riguardo il tema Criptovalute, denominata Market In Crypto Asset (MiCa), sviluppata per aiutare a semplificare la tecnologia del registro distribuito e la regolamentazione delle risorse virtuali nell'Unione Europea con attenzione verso la sicurezza di investitori e utenti che ne fanno utilizzo. MiCA è un documento di circa 168 pagine, diviso in 9 sezioni, concepito da un processo iniziato nel 2018, periodo coincidente all'intenso interesse pubblico e di investitori verso le Criptovalute, dalle autorità di regolamentazione europee, in particolare sono state incaricate "l'Autorità bancaria europea"[143] (EBA) e "l'Autorità Europea degli strumenti finanziari e dei Mercati"[144] (ESMA) che hanno riscontrato una molteplicità di criptovalute non rientranti nei criteri della legislazione UE sui servizi finanziari, rendendo di conseguenza i consumatori e l'integrità del mercato in generale vulnerabili a potenziali pericoli. Infatti, i consumatori ad oggi non godono di particolari diritti di risarcimento o protezione, con l'introduzione di MiCA i fornitori di servizi cripto dovranno rispettare requisiti rigorosi per proteggere i portafogli dei consumatori e diventare responsabili in caso di perdita nelle cripto attività degli investitori. La Proposta coprirà anche ogni abuso di mercato connesso a qualsiasi tipo di servizio concesso, con particolare riguardo verso la manipolazione di mercato e l'abuso di informazioni privilegiate. L'obiettivo finale di MiCA è quindi fornire certezza del diritto per i cripto asset non coperti dalla vigente legislazione UE sui servizi finanziari e stabilire regole uniformi per gli emittenti di Stablecoin e i fornitori di servizi di criptovalute. Questi, infatti, se superati volumi di mercato significativi saranno soggetti a obblighi, come la

[143] **L'Autorità Bancaria Europea** (EBA) è un'autorità indipendente dell'UE, che opera per assicurare un livello di regolamentazione e di vigilanza prudenziale efficace e uniforme nel settore bancario europeo. Gli obiettivi generali sono assicurare la stabilità finanziaria nell'UE e garantire l'integrità, l'efficienza e il regolare funzionamento del settore bancario. https://www.eba.europa.eu/languages/home_it

[144] **L'Autorità Europea degli Strumenti Finanziari e Dei Mercati** (ESMA) è un'autorità indipendente dell'UE che contribuisce a salvaguardare la stabilità del sistema finanziario dell'UE rafforzando la protezione degli investitori e promuovendo mercati finanziari stabili e ordinati. https://www.esma.europa.eu/about-esma/esma-in-brief

fornitura di un "Whitepaper"[145] e il rispetto di rigidi requisiti di conformità definiti dall'UE proporzionati ai rischi dei servizi forniti. Per le società emettenti di stablecoin, si richiederà la costituzione di una riserva che sia sufficientemente liquida e con un rapporto rigorosamente 1 a 1 e in gran parte sotto forma di depositi. Ogni titolare di stablecoin, in questo modo, potrà chiedere in qualsiasi momento un rimborso all'emittente gratuitamente perché norme che disciplinano il funzionamento della riserva garantiranno la liquidità minima adeguata. La regolamentazione delle stablecoin in questo modo da possibilità ad una possibile coesistenza con le CBDC[146]. Sarà inoltre limitato per preservare la sovranità monetaria attuale, lo sviluppo di token collegati ad attività non basati su una valuta non europea, quale mezzo di pagamento ampiamente diffuso. Per quanto riguarda i fornitori di servizi di criptovalute, saranno concesse attività se rispettato il requisito di persona giuridica con sede legale in uno stato membro dell'UE con annessa autorizzazione ufficiale come Fornitore di servizi all'autorità competente dello stato membro in cui hanno sede legale. Chi offrirà servizi operativi nel mercato del cripto sarà tenuto anche a dichiarare informazione sulla loro impronta ambientale e climatica, l'Autorità Europea degli strumenti finanziari e dei mercati elaborerà progetti di norme tecniche riguardanti il contenuto, le metodologie e la presentazione delle informazioni relative agli effetti negativi sull'ambiente e sul clima, con l'introduzione di norme minime di sostenibilità obbligatorie, limitando significativamente l'impatto ambientale derivante dalle Cripto attività (Es. Consumo di Energia derivante dal PoW). La proposta potrebbe rappresentare una minaccia per il mercato delle criptovalute, soprattutto per la Finanza Decentralizzata (DEFI) ma potrebbe anche permettere il godimento di vantaggi del mercato interno europeo dei servizi finanziari, ora non possibili a causa della mancanza di normative, che impedisce l'attribuzione alle società di criptovalute di licenze europee per operare, come avviene invece nei servizi finanziari tradizionali. "Entro il 2024, L'UE dovrebbe mettere in atto un quadro completo che consenta

[145] Documento inteso come guida e rilasciato per spiegare un concetto o la soluzione ad un problema specifico, solitamente è redatto e rilasciato da una persona o entità con autorità in materia per attirare potenziali investitori, https://academy.bit2me.com/it/que-es-un-whitepaper/

[146] **Graziani Alessandro** Stablecoin contro valute digitali delle Banche centrali? No, sarà coesistenza. Sole24Ore. 2021, https://24plus.ilsole24ore.com/art/stablecoin-contro-valute-digitali-banche-centrali-no-sara-coesistenza-AEHqMX1

l'adozione della tecnologia di contabilità distribuita (DLT) e delle criptovalute nel settore finanziario…"[147]

1.8.2 DORA

Durante la riunione della Commissione Europea del 2020 ha avuto luogo anche la proposta "Digital Operational Resilience Act" riguardante ogni stato membro appartenente all'UE. L'obiettivo è il rafforzamento della resilienza operativa digitale all'interno del settore finanziario armonizzando la legislazione esistente e integrando le lacune mitigando il rischio posto dalle crescenti vulnerabilità, causate dalla crescente interconnettività del settore finanziario, far fronte al cambiamento del profilo di rischio causato dall'adozione di servizi finanziari digitali, riconoscere e affrontare la dipendenza da terzi alla base della stabilità del settore finanziario e adottare un approccio di vigilanza unico e coerente alla resilienza operativa unico in tutto il mercato. "Resilienza operativa digitale significa la capacità di un'entità finanziaria di costruire, assicurare e rivedere la propria integrità operativa da un punto di vista tecnologico garantendo, direttamente o indirettamente, attraverso l'uso di servizi di fornitori ICT terzi, l'intera gamma di ICT capacità correlate necessarie per affrontare la sicurezza della rete e dei sistemi informativi di cui fa uso un'entità finanziaria e che supportano la fornitura continua di servizi finanziari e la loro qualità"[148]. Tutto ciò usufruendo dell'introduzione di un regime di sorveglianza sui fornitori ICT critici come ad esempio le risorse cloud, analisi dei dati e revisione contabile, temi che interessano anche e soprattutto coloro che prestano servizi funzionali alla gestione delle cripto attività. Per quanto riguarda la gestione del rischio delle ICT, il documento si basa in gran parte sulle linee guida dettate dall'Autorità Bancaria Europea con attenzione verso il rischio di questi sistemi e sulla loro sicurezza, definendo come gestire i rischi in ogni fase del loro ciclo di vita, enfatizzando il ruolo dell'alta direzione e ampliando i requisiti per

[147] **Commissione Europea** Regolamento del Parlamento Europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937. Cit.
[148] **Commissione Europea** Regolamento del Parlamento Europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014. Cit.

includere una strategia di resilienza digitale, come l'obbligo informativo e di segnalazione incidenti. DoRa richiede inoltre che le imprese abbiamo una strategia anche sul rischio ICT di terzi e la limitazione di uso di terze parti al di fuori dell'Unione Europea.

1.9 Regolamentazione negli USA: Responsible Financial Innovation Act.

Fin dalla nascita delle criptovalute, negli anni si sono susseguite proposte di regolamentazione della materia ancora in via di sviluppo e perfezionamento, poiché lo strumento da regolare per sua stessa natura non prevede di essere regolamentato. La nuova tecnologia se adottata nella maniera corretta, potrebbe portare un vantaggio competitivo ed economico non indifferente verso il paese che meglio gestirà la regolamentazione. Per la rete "il concetto di Estero non esiste"[149], scambi commerciali di beni acquistati con le criptovalute possono avvenire anche in diverse nazioni e la valuta spedita e ricevuta si troverà sempre e solo sulla rete. È proprio per questo che la tassazione potrebbe essere molto difficile da attuare con i sistemi tradizionali attuali, risultati inadeguati. Le blockchain ad oggi presenti e conosciute sono caratterizzate da completa tracciabilità, più di ogni altro strumento umano inventato finora. È nota inoltre l'esistenza di Blockchain di nicchia definite "alternative" che hanno caratteristiche specifiche che rendono l'anonimato possibile, queste molto spesso vengono usate nel dark web ma sono caratterizzato da un uso molto limitato e cercano di essere costantemente contrastate dalle autorità, un esempio è Tornato Cash[150], blockchain utilizzata a scopo criminale. Ad oggi è dimostrato che "le che coinvolgono indirizzi illeciti rappresentano solo lo

[149] **Bellicini Bernardo and Comandini Gian Luca** Il Punto Su... La Fiscalità delle Criptovalute tra Rischi di Evasione, Problemi di Tracciabilità e Future Prospettive. Pacini Giuridica. 2022, https://www.rivistadirittotributario.it/2022/03/02/il-punto-su-la-fiscalita-delle-criptovalute-tra-rischi-di-evasione-problemi-di-tracciabilita-e-future-prospettive/

[150] Si pensa che Tornado Cash sia stato sviluppato per aggirare le leggi antiriciclaggio. **Cavicchioli Marco** Tornado Cash: punito perché creato per scopi criminali. Cryptonomist. 2022, https://cryptonomist.ch/2022/08/18/tornado-cash-punito-perche-creato-per-scopi-criminali/

0,15%, del volume delle transazioni di criptovaluta nel 2021"[151], ciò rafforza infatti il concetto di blockchain come uno strumento sicuro e migliore di alcuni odierni.

Le regole secondo l'imposizione del KYC (Know Your Costumer), sempre più stringenti verso gli Exchange di criptovalute, risultano essere illogiche e improbabili di attuazione in quanto sistemi come Bitcoin risultano essere tutt'altro che strumenti di evasione per l'occultamente di fondi illeciti, in quanto per definizione il sistema è tracciabile ed è facile risalire retroattivamente a tali transazioni e provenienza. Ad oggi è chiaro che siamo a un punto di non ritorno, in quanto il valore aggiunto di questa rivoluzionaria tecnologia e applicazioni sembra non essere più trascurabile. I Casi d'uso, l'effettivo L'utilizzo e lo sviluppo è sempre più frequente, basta notare la crescita di interesse per concetti fino a qualche anno fa sconosciuti o impensabili come il metaverso, ancora in via di sviluppo e lontano dalle aspettative ma sotto stretta osservazione dei regulators, in particolare l'UE[152]. Cittadini, Aziende, Istituzioni e Banche Centrali stanno cercando di governare questo tipo di tecnologia che deve il suo attuale successo proprio all'assenza di una governance centralizzata. La Maggior parte delle criticità e i problemi sollevati sono stati frutto di ignoranza tecnica in materia, di paura insita nell'indole umana per ogni nuovo paradigma e di pigrizia mentale di cambiamento e adattamento ad un futuro che, grazie a questa tecnologia potrebbe essere realmente più sicuro trasparente ed efficiente.

1.9.1 Responsible Financial Innovation Act.

Negli USA è stato introdotto un disegno di legge bipartisan di 69 pagine presentato al senato da Kiristen Gillibrand (Politica e avvocata statunitense) e Cynthia Lummis (Senatrice per lo stato Wyoming), che prevede di creare un quadro normativo completo per le risorse digitali negli stati uniti risolvendo le problematiche sorte questi ultimi anni. Il Documento è denominato Responsible Financial Innovation

[151] **Chainalysis** Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity. Chainalysis. 2022, https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/

[152] **Anastasio Paolo** La Commissione Ue guarda al metaverso: proposta di regolamento europeo nel 2023. Key4Biz. 2022, https://www.key4biz.it/la-commissione-ue-guarda-al-metaverso-proposta-di-regolamento-europeo-nel-2023/416083/.

Act. e si rivolge alla giurisdizione della "Security and Exchange Commission"[153] (SEC) Degli stati uniti e dalla "Commodity Futures Trading Commission"[154] (CFTC), trattamento fiscale delle risorse digitali, regolamentazione delle Stablecoin e coordinamento tra agenzie. La proposta del disegno delinea una guida per classificare le criptovalute, concentrandosi al contempo su flessibilità, innovazione, trasparenza e protezione dei consumatori al fine di integrare le risorse digitali nella legge esistente fornendo chiarezza alle autorità di regolamentazione e al settore nel suo insieme. Più nel dettaglio Il Responsible Financial Innovation Act. chiamato anche Lummis-Gillibrand propone: "la creazione di uno standard chiaro per determinare quali risorse digitali sono merci e quali sono titoli, esaminandone accuratamente lo scopo e i diritti e poteri che trasmette all'acquirente, fornendo al contempo chiarezza e struttura alle società di asset digitali e la possibilità di determinare i loro obblighi normatici e dare alle autorità di regolamentazione i giusti mezzi per far rispettare le leggi già vigenti. Definizione chiare, al fine di attuare in modo coerente le regolamentazioni e permetterne la conoscenza e la comprensione da parte di tutti gli americani. Assegnazione delle regolamentazioni all'autorità di regolamentazione CFTC in tema di asset simili a materie prime. Requisiti di riserva al 100% per le Stablecoin, permettendo il riscatto in cambio del valore in dollari equivalente in qualsiasi momento, per un'accurata protezione di consumatori e mercati e per agevolare lo sviluppo di un sistema basato su Stablecoin che potrebbe fornire al consumatore un mezzo di pagamento più rapido e sicuro. Creazione di un comitato consultivo con il compito di studiare continuamente il settore in rapida evoluzione formulando raccomandazione e sviluppando principi guida, responsabilizzare e consigliare i legislatori sugli sviluppi tecnologia. Una particolare attenzione all'educazione dei consumatori con la costituzione di un'imposizione verso i fornitori di servizi di risorse digitali di requisiti di divulgazione per un'idonea comprensione del prodotto e dei rischi ad esso connessi. Riferire e analizzare costantemente il consumo di energia nel settore

[153] La **Securities and Exchange Commission** (SEC) è l'ente federale statunitense che ha come missione di proteggere gli investitori, mantenere il mercato sicuro, ordinato ed efficiente e facilitare la formazione di capitale. https://www.sec.gov/about.shtml

[154] La **Commodity Futures Trading Commission** ha la missione di promuovere l'integrità, la resilienza e la vivacità dei mercati dei derivati statunitensi attraverso una solida regolamentazione. https://www.cftc.gov/About/AboutTheCommission

delle risorse digitali, trovando al contempo modi migliori, come la riduzione dello spreco energetico e l'utilizzo di energie rinnovabili con cui alimentare le attività di estrazione di valuta virtuale (Es. Bitcoin con il Meccanismo PoW). Sviluppo di un'organizzazione di autoregolamentazione da parte di CFTC e SEC che possa svolgere un ruolo di collaborazione con le autorità di regolamentazione consentendo una maggiore efficienza, agilità e una certa supervisione. Incarico alla CFTC e SEC per la creazione di una guida completa e basata sui principi di sicurezza informatica per gli intermediari di asset digitali, creando degli standard solidi. Il disegno di legge agli stessi indirizza le autorità di regolamentazione appropriate a studiare il potenziale di identificazione e mitigazione delle minacce, operazioni di sicurezza, auditing e test. il documento suggerisce l'introduzione di un sandbox consentendo alle aziende crittografiche di testare nuovi prodotti su scala e durata limitate e controllate, per aiutare lo sviluppo dell'innovazione, l'attenzione alla creazione di una struttura praticabile per la tassazione delle risorse digitali, chiarendo i trattamenti fiscali di diversi attori e azioni relative al settore e condurre analisi di potenziali opportunità e rischi associati all'investimento dei risparmi pensionistici in risorse digitali, per non limitare le opportunità ai consumatori di beneficiare della crescita del settore garantendo al contempo sicurezza[155].

[155] **Lummis Cynthia and Gillibrand Kiristen** Lummis-Gillibrand Responsible Financial Innovation Act. 2022, https://www.congress.gov/bill/117th-congress/senate-bill/4356/text.

CONCLUSIONE

Dal lavoro di tesi e dalle analisi effettuate è emersa l'importanza di conoscere e approfondire giorno per giorno lo sviluppo blockchain, che non ha ancora espresso come innovazione, il suo massimo potenziale, ma che è sulla buona strada per dimostrarlo, in prospettiva delle sue crescenti applicazioni e dell'interesse di adattamento normativo, avanzato dai più importanti paesi mondiali. Stiamo infatti assistendo ad una radicale rinnovamento in vari settori, come i sistemi logistici o di raccolta dati e in particolare quello finanziario, che vede oggi come protagonisti assoluti di una vera e propria rivoluzione la blockchain e le criptovalute. Il nuovo sistema basato registri distribuiti e decentralizzati sta aiutando a risolvere delle inefficienze che hanno da sempre caratterizzato il mondo finanziario, comportando diversi benefici non di poco conto per gli utenti, soprattutto coloro che non hanno la fortuna di vivere in paesi con un sistema finanziario sviluppato e moderno. I vantaggi principali sono la completa tracciabilità e trasparenza con il conseguente aumento del grado di fiducia degli utilizzatori, sentimento in declino proprio nei confronti delle istituzioni bancarie a causa delle recenti crisi, la velocità e i bassi costi di transazione che permettono pagamenti diretti e più efficienti e un completo controllo delle finanze possedute attraverso la gestione di un wallet personale. Le criptovalute hanno permesso la nascita della finanza decentralizzata, in proporzione molto piccola rispetto alla finanza tradizionale, ma che si sta evolvendo e migliorando costantemente grazie ai vantaggi che offre e alla collaborazione di tutti i partecipanti. Tali sviluppi hanno richiamato l'attenzione dei sistemi finanziari tradizionali, che avvertendo un cenno di concorrenza sono immediatamente ricorsi alla ricerca di un rinnovamento interno provando addirittura ad implementare servizi giovando dei benefici della blockchain e delle criptovalute proponendo di fatto un nuovo sistema, ancora in via di sviluppo basato sulle Central Bank Digital Currencies. Sono molte anche le difficoltà da superare per adattare al meglio queste grandi innovazioni permettendone un'adozione più significativa. Ad oggi sono ricorrenti casi di fallimenti, errori e truffe dei fornitori di questi nuovi servizi a discapito degli utenti. Questo probabilmente è dovuto per ora, all'inadeguatezza della attuale formazione finanziaria attuale e dall'utilizzo di preesistenti norme finanziarie tradizionali e alla mancanza di linee guide chiare che informino, e

tutelino gli utilizzatori di questi nuovi servizi. Per aspirare ad una adozione significativa le criptovalute hanno bisogno di una maggiore comprensione e una regolamentazione non eccessivamente rigida e restrittiva ma flessibile e accomodante, permettendo così i giusti margini per un sano sviluppo. Le proposte di regolamentazione attuali di USA ed Europa sembrano voler accogliere l'innovazione, probabilmente, visto il grande interesse fra il pubblico, per aggiudicarsi un vantaggio competitivo prima di tutti gli altri. Il successo di tali strumenti sarà deciso da coloro che decideranno di farne utilizzo nella propria quotidianità contribuendo al miglioramento e alla realizzazione di un nuovo metodo di scambio, ancora immaturo ma unico nel suo genere.

BIBLIOGRAFIA

Anastasio Paolo La Commissione Ue guarda al metaverso: proposta di regolamento europeo nel 2023. Key4Biz. 2022, https://www.key4biz.it/la-commissione-ue-guarda-al-metaverso-proposta-di-regolamento-europeo-nel-2023/416083/.

Antonopoulos Andreas M. e Masutti Riccardo Mastering Bitcoin. Indipendently Published, 2019.

Antonopoulos Andreas M. e Wood Gavin Mastering Ethereum. O'Reilly Media, 2018.

Aysan A.F., Demirtaş H.B. e Saraç M. The Ascent of Bitcoin: Bibliometric Analysis of Bitcoin Research. Journal of Risk and Financial Management, 2021. https://doi.org/10.3390/jrfm14090427

Banca D'Italia Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività. Banca D'Italia, 2022. https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-cripto.pdf

Banca D'Italia La Moneta e gli strumenti di pagamento alternativi al contante. Banca D'Italia, 2018.

Banca D'Italia Recepimento della nuova regolamentazione prudenziale internazionale. Rischi Operativi. Banca D'Italia, 2006. https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2006/basilea2/Doc_Cons_Rischi_operativi.pdf

Barbieri Giacomo Cosa sta facendo la Ue per regolamentare le criptovalute. La Repubblica. 2022. https://www.repubblica.it/tecnologia/2022/04/25/news/gli_sforzi_di_regolamentazione_delle_crypto_in_ue_spiegati_per_bene-346309419/

Battaglia Alberto Ethereum Merge: l'evento crypto dell'anno è andato in porto. We Wealth, 2022. https://www.we-wealth.com/news/fintech/blockchain/ethereum-merge-l-evento-crypto-dell-anno-e-andato-in-porto

Bellicini Bernardo e Comandini Gian Luca Il Punto Su... La Fiscalità delle Criptovalute tra Rischi di Evasione, Problemi di Tracciabilità e Future Prospettive. Pacini Giuridica, 2022. https://www.rivistadirittotributario.it/2022/03/02/il-punto-su-la-fiscalita-delle-criptovalute-tra-rischi-di-evasione-problemi-di-tracciabilita-e-future-prospettive/

Bellini Mauro Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia. Blockchain4innovation. 2022. https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/.

Binance Gli Oracoli Blockchain Spiegati. Binance Accademy. - 2020. - https://academy.binance.com/it/articles/blockchain-oracles-explained.

Binance Bitcoin è una Riserva di Valore? 2020. https://academy.binance.com/it/articles/is-bitcoin-a-store-of-value.

Binance Blockchain private, pubbliche e consorzi – qual è la differenza? Binance Accademy. 2021. https://academy.binance.com/it/articles/private-public-and-consortium-blockchains-whats-the-difference#private-blockchains.

Binance Come creare una DAO?Binance Accademy. 2022. https://academy.binance.com/it/articles/how-to-create-a-dao.

Binance Cosa sono le pool di liquidità nella DeFi e come funzionano? [Online]. 2020. https://academy.binance.com/it/articles/what-are-liquidity-pools-in-defi.

Binance Cos'è Ethereum? Binance Accademy. 2020. https://academy.binance.com/it/articles/what-is-ethereum.

Binance Cos'è la Riserva Frazionaria? Binance Accademy. 2019. https://academy.binance.com/it/articles/what-is-fractional-reserve.

Binance Cos'è l'Hashing Binance Accademy. 2019. https://academy.binance.com/it/articles/what-is-hashing

Binance Cos'è lo Staking? Binance Accademy. 2019. https://academy.binance.com/it/articles/what-is-staking.

Binance Cos'è un 51% Attack? Binance Accademy. 2018. https://academy.binance.com/it/articles/what-is-a-51-percent-attack.

Binance Scalabilità Blockchain - Sidechain e Canali di Pagamento. Binance Accademy. 2020. https://academy.binance.com/it/articles/blockchain-scalability-sidechains-and-payment-channels#the-blockchain-scalability-problem.

Binance What Is Proof of Stake (PoS)? Binance Accademy.2018. https://academy.binance.com/en/articles/proof-of-stakeexplained

Biscointi Avvocati Smart Contract: opportunità, applicabilità e limiti giuridici Biscointi Avvocati. - 2022. - https://www.studiobisconti.it/blog/smart-contract-opportunita-applicabilita-e-limiti-giuridici/.

Bitcoin.org Come sono creati i bitcoin? 2009. https://bitcoin.org/it/faq#come-vengono-creati-i-bitcoin.

Bitcoin.org Economia. 2009. https://bitcoin.org/it/faq#economia.

Bitcoin.org Quali sono i vantaggi di Bitcoin? 2009. https://bitcoin.org/it/faq#quali-sono-i-vantaggi-di-bitcoin.

Bitcoin.org What Is A Full Node? 2009. https://bitcoin.org/en/full-node#what-is-a-full-node.

Blockchain Media Qual è la liquidazione delle criptovalute e cosa fare? 2022. https://blockchain-media.org/it/crypto-liquidation/.

Boucher Philip Come la tecnologia blockchain può cambiarci la vita. 2017. https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_IT.pdf.

Bourgi Sam Sembra che Cream Finance abbia subito un altro grave flash loan attack. Cointelegraph, 2021. https://it.cointelegraph.com/news/breaking-cream-finance-appears-to-have-suffered-major-loss-in-flash-loan-hack

Buscema Salvatore Finanza Decentralizzata – Problemi giuridici e tecnici. Cryptoavvocato. 2020. https://www.cryptoavvocato.it/articoli/finanza-decentralizza-problemi-giuridici-tecnici/.

Buterin Vitalik Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2014. https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

Cacioppoli Vincenzo Il ruolo dei rollup sulla scalabilità di Ethereum. Cryptonomist, 2022. https://cryptonomist.ch/2022/08/05/ruolo-rollup-scalabilita-ethereum/

Carlini Vittorio Cripto, nella finanza decentralizzata è boom di furti e riciclaggio Sole24Ore, 2022.

Cavicchioli Marco La Differenza tra Token e Criptovalute. 2018. https://medium.com/@marcocavicchioli/la-differenza-tra-token-e-criptovalute-596c9cb96bc5.

Cavicchioli Marco Tornado Cash: punito perché creato per scopi criminali. Cryptonomist, 2022. https://cryptonomist.ch/2022/08/18/tornado-cash-punito-perche-creato-per-scopi-criminali/

Cavicchioli Marco La storia del Bitcoin, Cryptonomist. 2022, https://cryptonomist.ch/2022/05/15/storia-bitcoin-2/

Chainalysis Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity. Chainalysis, 2022. https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/

Cheng Amy 'Squid Game'-inspired cryptocurrency that soared by 23 million percent now worthless after apparent scam. The Washington Post. 2021. https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/

Coinbase Cos'è un token? 2022. https://www.coinbase.com/it/learn/crypto-basics/what-is-a-token.

Commissione Europea Regolamento del Parlamento Europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937. 2020. https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0008.02/DOC_1&format=PDF.

Commissione Europea Regolamento del Parlamento Europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014.2020. https://eur-lex.europa.eu/legal content/IT/TXT/PDF/?uri=CELEX:52020PC0595&from=EN.

Culicchi Roberto Le criptovalute gettano le famiglie sul lastrico: il caso Celsius e la necessità di un intervento legislativo. Network Digital 360, 2022. https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/le-criptovalute-gettano-le-famiglie-sul-lastrico-il-caso-celsius-e-la-necessita-di-un-intervento-legislativo/

Davola Antonio Bias Cognitivi e Contrattazione Standardizzata: Quali tutele per i consumatori? Contratto e Impresa. 2017.

Davies Pascale Spiegazione del crollo della stablecoin Terra Luna: è questo il momento del crollo finanziario della criptovaluta del 2008? Euronews.next. 2022. https://www.euronews.com/next/2022/05/12/terra-luna-stablecoin-collapse-is-this-the-2008-financial-crash-moment-of-cryptocurrency.

Digiconomist Bitcoin Energy Consumption Index. 2022. https://digiconomist.net/bitcoin-energy-consumption.

Digiconomist Ethereum Energy Consumption Index. 2022. https://ethereumenergyconsumption.com/

Ethereum.org Decentralized autonomous organizations (DAOs). Ethereum.org. 2022. https://ethereum.org/en/dao/#what-are-daos

Ethereum.org La Beacon Chain. Ethereum.org. - 2022. - https://ethereum.org/it/upgrades/beacon-chain/#main-content .

Ethereum.org Shard chain. Ethereum.org. 2022. https://ethereum.org/it/upgrades/sharding/

Ethereum.org What is Ethereum? The foundation for our digital future. Ethereum in numbers. 2022. https://ethereum.org/en/what-is-ethereum/

Graziani Alessandro Stablecoin contro valute digitali delle Banche centrali? No, sarà coesistenza. Sole24Ore, 2021. https://24plus.ilsole24ore.com/art/stablecoin-contro-valute-digitali-banche-centrali-no-sara-coesistenza-AEHqMX1

Guazzo Gianmarco Bitcoin e trilemma della blockchain: cosa è e possibile soluzione. Investire.biz. 2020. https://investire.biz/articoli/analisi-previsioni-ricerche/bitcoin-e-criptovalute/criptovalute-bitcoin-trilemma-blockchain-cosa-funzionamento-soluzione-lightning-network.

Huang Yongfeng [et al.] Smart Contract Security: A Software Lifecycle Perspective. IEEE, 2021.

International Organization for Standardization ISO 22739:2020 Blockchain and distributed ledger technologies. 2020. https://www.iso.org/standard/73771.html.

Intesa Che cos'è il KYC e perché adottarlo. Intesa. 2022. https://www.intesa.it/che-cose-il-kyc-e-perche-adottarlo/.

Intesa Cosa sono gli smart contracts? Intesa. 2022. https://www.intesa.it/cosa-sono-gli-smart-contract-e-quali-sono-le-loro-applicazioni-pratiche/.

Litan Avivah Hype cycle for blockchain 2021; More Action than Hype. Gartner Blog Web. 2021. https://blogs.gartner.com/avivah-litan/2021/07/14/hype-cycle-for-blockchain-2021-more-action-than-hype/.

Lummis Cynthia e Gillibrand Kiristen Lummis-Gillibrand Responsible Financial Innovation Act. 2022. https://www.congress.gov/bill/117th-congress/senate-bill/4356/text.

Minenna Marcello Cina: la grande crescita silenziosa dello Yuan digitale. Sole24Ore, 2022. https://www.ilsole24ore.com/art/cina-grande-crescita-silenziosa-yuan-digitale-AEufHqDB

Minenna Marcello Criptovalute: perché il 2022 sarà l'anno dei regulators. Sole24Ore, 2021. https://www.ilsole24ore.com/art/criptovalute-perche-2022-sara-l-anno-regulators-AEN03wo

Ministero dello Sviluppo Economico Blockchain e intelligenza artificiale: incentivi per imprese ed enti di ricerca. 2022. https://www.mise.gov.it/index.php/it/notizie-stampa/blockchain-e-intelligenza-artificiale-incentivi-per-imprese-ed-enti-di-ricerca.

Moore Geoffrey A. Crossing the chasm: Marketing and selling disruptive products to mainstream customers. Harper Business an imprint of HarperCollins Publishers, 2014.

Nakamoto Satoshi Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. https://bitcoin.org/bitcoin.pdf.

Parlamento Europeo Risoluzione del Parlamento europeo del 17 maggio 2017 sulla tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario (2016/2243(INI)). 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0211_IT.html

Parlamento Europeo Risoluzione del Parlamento europeo del 26 maggio 2016 sulle valute virtuali (2016/2007(INI)). 2016. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_IT.html

Partz Helen La banca centrale norvegese sceglie Ethereum per sviluppare la valuta digitale nazionale. Cointelegraph, 2022. https://it.cointelegraph.com/news/norwegian-central-bank-uses-ethereum-to-build-national-digital-currency

Pratt Mary K. e Gillis Alexander S. Blockchain for businesses: The ultimate enterprise guide. Techtarget.2021. https://www.techtarget.com/searchcio/definition/blockchain.

Rampone Francesco Token, asset digitali e ID I diritti soggettivi in chiave criptolegale. Associazione Blockchain Italia. 2020. https://associazioneblockchain.it/doc/token-asset-digitali-e-id-i-diritti-soggettivi-in-chiave-criptolegale/.

Rinnovabili.it Nuove tecnologie: a Yale si studiano gli effetti indesiderati. Rinnovabili.it, 2020. https://www.rinnovabili.it/innovazione/nuove-tecnologie-impatti-ambientali-yale/

Rogers Everet M. e Kincaid D. Lawrence Communication Networks: Toward a new paradigm for Research.The Free Press, 1988.

Rogers Everett M. Diffusion of Innovation. The Free Press, 2003.

Sgroi Maurizio Così le banche centrali fanno prove generali di blockchain. Sole24Ore, 2021. https://www.econopoly.ilsole24ore.com/2021/10/06/banche-centrali-blockchain/

Shumpeter Joseph Alois Teoria dello sviluppo economico. Sansoni, 1971.

SIAE Siae rappresenta i diritti degli autori con asset digitali: creati più di 4.000.000 di nft sull'infrastruttura blockchain di algorand. 2021. https://www.siae.it/it/iniziative-e-news/siae-rappresenta-i-diritti-degli-autori-con-asset-digitali-creati-pi%C3%B9-di-4000000.

Spadafora Francisco Banche, giocate d'anticipo: perché i crypto-asset sono un mercato da non sottovalutare. Ntt Data. 2021. https://it.nttdata.com/insights/blog/cryptoasset-banche.

The Crypto Gateway Che cos'è la Decentralized Finance (DeFi)? 2022. https://thecryptogateway.it/tutorial-defi-finanza-decentralizzata/.

The Crypto Gateway Layer 0, layer 1 e layer 2: che cosa sono? TheCryptoGateway. 2022. https://thecryptogateway.it/layer-0-layer-1-layer-2/.

Travia Niccolò Il "caso" Bitfinex: attacco hacker o semplice frode, che c'è da sapere. Agenda Digitale, 2019. https://www.agendadigitale.eu/documenti/il-caso-bitfinex-attacco-hacker-o-semplice-frode/

Utterback James M e Abernathy William J A Dynamic Model of Process And Product Innovation. Omega Journal, 1975.

Web ToEmotion Cambiamenti climatici tra ESG e criptovalute. 2022. https://blog.web2emotions.com/sostenibilita/cambiamenti-climatici-tra-esg-e-criptovalute/.

SITOGRAFIA

https://24plus.ilsole24ore.com/art/cripto-finanza-decentralizzata-e-boom-furti-e-riciclaggio-AEhU6LmB

https://24plus.ilsole24ore.com/art/stablecoin-contro-valute-digitali-banche-centrali-no-sara-coesistenza-AEHqMX1

https://academy.binance.com/en/articles/proof-of-stake-explained

https://academy.binance.com/en/glossary/hash-rate

https://academy.binance.com/en/glossary/turing-complete

https://academy.binance.com/it/articles/blockchain-oracles-explained

https://academy.binance.com/it/articles/blockchain-scalability-sidechains-and-payment-channels#the-blockchain-scalability-problem.

https://academy.binance.com/it/articles/how-to-create-a-dao

https://academy.binance.com/it/articles/private-public-and-consortium-blockchains-whats-the-difference#private-blockchains

https://academy.binance.com/it/articles/what-are-liquidity-pools-in-defi

https://academy.binance.com/it/articles/what-is-a-51-percent-attack.

https://academy.binance.com/it/articles/what-is-ethereum.

https://academy.binance.com/it/articles/what-is-fractional-reserve.

https://academy.binance.com/it/articles/what-is-hashing.

https://academy.binance.com/it/articles/what-is-staking.

https://academy.bit2me.com/it/que-es-un-whitepaper/

https://academy.bit2me.com/it/timestamp-blockchain/

https://associazioneblockchain.it/doc/token-asset-digitali-e-id-i-diritti-soggettivi-in-chiave-criptolegale/

https://bitcoin.org/en/full-node#what-is-a-full-node

https://bitcoin.org/it/faq#come-vengono-creati-i-bitcoin.

https://bitcoin.org/it/faq#economia.

https://bitcoin.org/it/faq#quali-sono-i-vantaggi-di-bitcoin.

https://bitnodes.io/dashboard/7y/

https://blockchain-media.org/it/crypto-liquidation/

https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/

https://blog.web2emotions.com/sostenibilita/cambiamenti-climatici-tra-esg-e-criptovalute/.

https://blogs.gartner.com/avivah-litan/2021/07/14/hype-cycle-for-blockchain-2021-more-action-than-hype/.

https://companiesmarketcap.com/assets-by-market-cap/

https://cryptonomist.ch/2022/05/15/storia-bitcoin-2/

https://cryptonomist.ch/2022/08/18/tornado-cash-punito-perche-creato-per-scopi-criminali/

https://defillama.com/protocol/synthetix

https://defillama.com/protocols/Dexes

https://defillama.com/protocols/Insurance

https://defillama.com/protocols/Lendig

https://digiconomist.net/bitcoin-energy-consumption.

https://doi.org/10.3390/jrfm14090427

https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper__Buterin_2014.pdf.

https://ethereum.org/en/dao/#what-are-daos.

https://ethereum.org/en/what-is-ethereum/.

https://ethereum.org/it/developers/docs/gas/

https://ethereum.org/it/upgrades/beacon-chain/#main-content .

https://ethereum.org/it/upgrades/sharding/

https://ethereumenergyconsumption.com/

https://etherscan.io/chart/active-address

https://etherscan.io/chart/gasused

https://etherscan.io/chart/tx

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0595&from=EN.

https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0008.02/DOC_1&format=PDF.

https://ieeexplore.ieee.org/document/8864988

https://investire.biz/articoli/analisi-previsioni-ricerche/bitcoin-e-criptovalute/criptovalute-bitcoin-trilemma-blockchain-cosa-funzionamento-soluzione-lightning-network.

https://it.cointelegraph.com/news/norwegian-central-bank-uses-ethereum-to-build-national-digital-currency

https://it.nttdata.com/insights/blog/cryptoasset-banche

https://medium.com/@marcocavicchioli/la-differenza-tra-token-e-criptovalute-596c9cb96bc5

https://tether.to/en/why-tether

https://thecryptogateway.it/layer-0-layer-1-layer-2/.

https://thecryptogateway.it/tutorial-defi-finanza-decentralizzata/

https://vitalik.ca/general/2017/09/14/prehistory.html

https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/le-criptovalute-gettano-le-famiglie-sul-lastrico-il-caso-celsius-e-la-necessita-di-un-intervento-legislativo/

https://www.agendadigitale.eu/documenti/il-caso-bitfinex-attacco-hacker-o-semplice-frode/

https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2006/basilea2/Doc_Cons_Rischi_operativi.pdf

https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-cripto.pdf

https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-cripto.pdf

https://www.binance.com/it

https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/

https://www.borsaitaliana.it/borsa/glossario.html

https://www.borsaitaliana.it/borsa/glossario/collateralizzazione.html

https://www.borsaitaliana.it/borsa/glossario/hash.html

https://www.borsaitaliana.it/borsa/glossario/rischio-di-mercato.html

https://www.cftc.gov/About/AboutTheCommission

https://www.coinbase.com/it/learn/crypto-basics/what-is-a-crypto-wallet

https://www.coinbase.com/it/learn/crypto-basics/what-is-a-token

https://www.congress.gov/bill/117th-congress/senate-bill/4356/text.

https://www.cryptoavvocato.it/articoli/finanza-decentralizza-problemi-giuridici-tecnici/

https://www.eba.europa.eu/languages/home_it

https://www.econopoly.ilsole24ore.com/2021/10/06/banche-centrali-blockchain/

https://www.esma.europa.eu/about-esma/esma-in-brief

https://www.euronews.com/next/2022/05/12/terra-luna-stablecoin-collapse-is-this-the-2008-financial-crash-moment-of-cryptocurrency.

https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_IT.html

https://www.europarl.europa.eu/doceo/document/TA-8-2017-0211_IT.html

https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_IT.pdf.

https://www.gartner.com/en

https://www.ilsole24ore.com/art/cina-grande-crescita-silenziosa-yuan-digitale-AEufHqDB

https://www.ilsole24ore.com/art/criptovalute-perche-2022-sara-l-anno-regulators-AEN03wo

https://www.insidemarketing.it/glossario/definizione/curva-di-rogers/

https://www.intesa.it/che-cose-il-kyc-e-perche-adottarlo

https://www.intesa.it/cosa-sono-gli-smart-contract-e-quali-sono-le-loro-applicazioni-pratiche/

https://www.iso.org/standard/73771.html

https://www.iso.org/standard/73771.html

https://www.key4biz.it/la-commissione-ue-guarda-al-metaverso-proposta-di-regolamento-europeo-nel-2023/416083/.

https://www.mise.gov.it/index.php/it/notizie-stampa/blockchain-e-intelligenza-artificiale-incentivi-per-imprese-ed-enti-di-ricerca.

https://www.nasdaq.com/nasdaq-100

https://www.repubblica.it/tecnologia/2022/04/25/news/gli_sforzi_di_regolamentazione_delle_crypto_in_ue_spiegati_per_bene-346309419/

https://www.rinnovabili.it/innovazione/nuove-tecnologie-impatti-ambientali-yale/

https://www.rivistadirittotributario.it/2022/03/02/il-punto-su-la-fiscalita-delle-criptovalute-tra-rischi-di-evasione-problemi-di-tracciabilita-e-future-prospettive/

https://www.sec.gov/about.shtml

https://www.siae.it/it/iniziative-e-news/siae-rappresenta-i-diritti-degli-autori-con-asset-digitali-creati-pi%C3%B9-di-4000000.

https://www.statista.com/statistics/280704/world-power-consumption/

https://www.statista.com/statistics/280704/world-power-consumption/

https://www.studiobisconti.it/blog/smart-contract-opportunita-applicabilita-e-limiti-giuridici/

https://www.techtarget.com/searchcio/definition/blockchain.

https://www.treccani.it/enciclopedia/fiat-money/

https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/

https://www.we-wealth.com/news/fintech/blockchain/ethereum-merge-l-evento-crypto-dell-anno-e-andato-in-porto

https://www.wikibit.it/k/cosa-significa-kb-kilobyte-563/