POLITECNICO DI TORINO

Corso di Laurea Magistrale in
Ingegneria Gestionale

Tesi di Laurea Magistrale

Criptovalute: visione macroeconomica e valutazione dell'efficienza come beni di investimento

Relatori
prof. Franco Varetto

Candidato
Mirko Vaia

Anno Accademico 2021-2022

Indice

1 INTRODUZIONE 4

2 CRIPTOVALUTE 5

2.1 DEFINIZIONE DI CRIPTOVALUTA 5

2.2 CARATTERISTICHE PRINCIPALI DELLE CRIPTOVALUTE 8

2.3 LE CRIPTOVALUTE E LA BLOCKCHAIN 10

2.4 ECOSISTEMA DELLE CRIPTOVALUTE 18

3 CRIPTOVALUTE E SISTEMI DI PAGAMENTO 20

3.1 EVOLUZIONE DELLE CRIPTOVALUTE COME METODO DI PAGAMENTO 21

3.2 VANTAGGI NELL'UTILIZZO DELLE CRIPTOVALUTE 23

3.3 SVANTAGGI NELL'UTILIZZO DELLE CRIPTOVALUTE 26

4 CRIPTOVALUTE E MONETA INTERNAZIONALE 28

4.1 INTRODUZIONE AL SISTEMA MONETARIO 28

4.2 L'EGEMONIA DEL DOLLARO E LA POSIZIONE DELLE CRIPTOVALUTE 30

5 CRIPTOVALUTE E LA POLITICA MONETARIA 35

5.1 LE BANCHE E IL MONITORAGGIO DELLE STABLECOIN 37

6 CRIPTOVALUTE: PROBLEMI DI CYBERSECURITY 42

6.1 E-COMMERCE ILLEGALE 42

6.2 RICICLAGGIO DI DENARO 45

6.3 FINANZIAMENTO AL TERRORISMO 46

6.4 VULNERABILITÀ E FURTI 47

6.5 MALWARE E CRYPTOLOCKING 52

6.6 CRYPTOJACKING 55

7 SOSTENIBILITÀ AMBIENTALE DELLE CRIPTOVALUTE 59

8 PRESENTAZIONE DELLE CRIPTOVALUTE E INDICI DI BORSA 68

8.1 BITCOIN 68

8.2 ETHEREUM 74

8.3 BINANCE COIN 78

8.4 LITECOIN 82

8.5 MONERO 84

8.6 S&P500 87

8.7 EUROSTOXX50 88

8.8 FTSE MIB 89
8.9 NASDAQ COMPOSITE 90
8.10 CAC 40 91

9 ANALISI DEI DATI 92

9.1 MERCATO EFFICIENTE 93
9.2 MODELLO RANDOM WALK 100
9.3 RANDOM WALK: UNIT ROOT TEST-TEST DICKEY-FULLER 102
9.4 VERIFICA DELL'EFFICIENZA DEBOLE 104
9.5 MODELLO DI MARKOWITZ: SELEZIONE DI PORTAFOGLIO 116
9.6 ANALISI DELLA CORRELAZIONE DEI DATI STORICI 125
9.7 CREAZIONE PORTAFOGLIO OTTIMO 132

10 CONCLUSIONE 145

11 BIBLIOGRAFIA & SITOGRAFIA 148

1 INTRODUZIONE

Il mercato delle criptovalute ha assunto una posizione di rilievo e non può più essere ignorato, ormai hanno cominciato a stimolare l'interesse di chiunque, dall'aziende ai consumatori fino ad arrivare alle banche centrali.

L'elaborato si pone l'obiettivo di analizzare il fenomeno delle criptovalute da due punti di vista: nella prima sezione si è deciso di utilizzare un approccio qualitativo, si sono studiati gli aspetti tecnici del fenomeno delle criptovalute, le dinamiche che ne controllano il funzionamento e poi possibili sviluppi dal punto di vista tecnologico. Inoltre, si è analizzato l'impatto che questo nuovo asset ha avuto e potrà avere in futuro sul sistema economico tradizionale, in particolare quali sono i possibili effetti del suo impiego come metodo di pagamento, sulle politiche monetarie e i possibili scenari di sviluppo delle valute digitali come moneta internazionale.

Successivamente si sono esposti i rischi legati alla cybersecurity e cybercriminalità che caratterizzano le criptovalute, si è ricercato come la diffusione delle valute digitali abbiamo incentivato la creazione di nuove tipologie di attacchi informatici e la crescita di organizzazioni criminali.

Infine, si sono illustrate le problematiche legate all'impatto ambientale delle principali criptovalute e alcune proposte innovative in quel settore.

Nella seconda sezione si è utilizzato un approccio quantitativo, si è valutata l'efficienza delle criptovalute come oggetto di investimento utilizzando i principi della teoria di Markowitz. Per effettuare queste valutazioni si sono utilizzate le serie storiche di cinque tra le principali criptovalute e cinque indici di borsa e si è analizzata la loro distribuzione in un portafoglio efficiente. L'eventuale assenza, o un valore relativamente basso, delle criptovalute dimostrerebbe la loro inefficienza come strumento di investimento.

2 CRIPTOVALUTE

In questo capitolo sono analizzate le principali caratteristiche delle valute digitali. In primo luogo, vengono presentate le idee generali da cui sono state progettate e le tecnologie implementate. Successivamente sono analizzate le varie componenti che formano l'ecosistema delle criptovalute.

2.1 Definizione di criptovaluta

L'avvento di Internet e la sua diffusione capillare è stata un driver di innovazione fondamentale per i servizi di ogni genere, compresi i servizi finanziari.

L'applicazione della tecnologia digitale al mondo della finanza ha reso possibile la nascita delle criptovalute, che nel corso degli ultimi hanno conquistato un ruolo sempre più importante sul panorama economico mondiale.

La definizione di criptovaluta non è ancora stata resa ufficiale da nessun ente a causa della costante evoluzione che le contraddistingue, quindi risulta difficile identificarla in modo univoco con una definizione che sia corretta e accettata in ogni sua sfumatura.

Perciò in questa sezione saranno presentate varie definizioni date dai principali enti, come le banche centrali, in modo da avere un quadro il più chiaro possibile su di esse.

Una prima possibile definizione è stata fornita dalla Banca centrale Europea (BCE) nel rapporto "Virtual Currency Schemes"[1] e "Virtual Currency Schemes-a further analysis"[2], dove si definisce una criptovaluta come una moneta virtuale non regolamentata che solitamente è rilasciata e controllata dagli stessi sviluppatori (*developer*), e usata ed accettata solamente tra i

[1] European Central Bank. 2012. VIRTUAL CURRENCY SCHEMES, OCTOBER 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[2] European Central Bank. 2015. Virtual currency schemes – a further analysis, Advance Access published 2015: doi:10.2866/662172

membri di una specifica "comunità virtuale" (*virtual community*). Successivamente sono state definite tre tipologie distinte di criptovalute:

1. *closed virtual currency schemes* (valute virtuali chiuse): questo tipo di valute virtuali non hanno alcun legame con l'economia reale e spesso sono chiamate *in game only*. Sono usate per acquistare beni e servizi virtuali all'interno di una specifica community virtuale e non possono essere usati al di fuori di essa. L'esempio proposto dal rapporto è quello delle valute all'interno dei giochi di ruolo online.
2. *Virtual currency schemes with unidirectional flows* (valute virtuali), questo tipo di valute possono essere acquistate, con un certo tasso di cambio, direttamente tramite moneta reale ma non possono essere ricambiate nella valuta reale. L'esempio descritto nel rapporto fa riferimento alle "Facebook Credits", valuta introdotta nel 2009 che permette agli utenti di comprare beni virtuali sulla piattaforma del socialnetwork.
3. *Virtual currency schemes with bidirectional flow*, gli utenti possono comprare e vendere la moneta virtuale con un tasso di cambio basato sulla propria valuta. Questo schema permette di comprare beni e servizi sia reali che virtuali. Il rapporto fa l'esempio di "Linden Dollars", una valuta virtuale rilasciata in un mondo virtuale, chiamato "Second Life", dove gli utenti possono creare i loro avatar personalizzati.

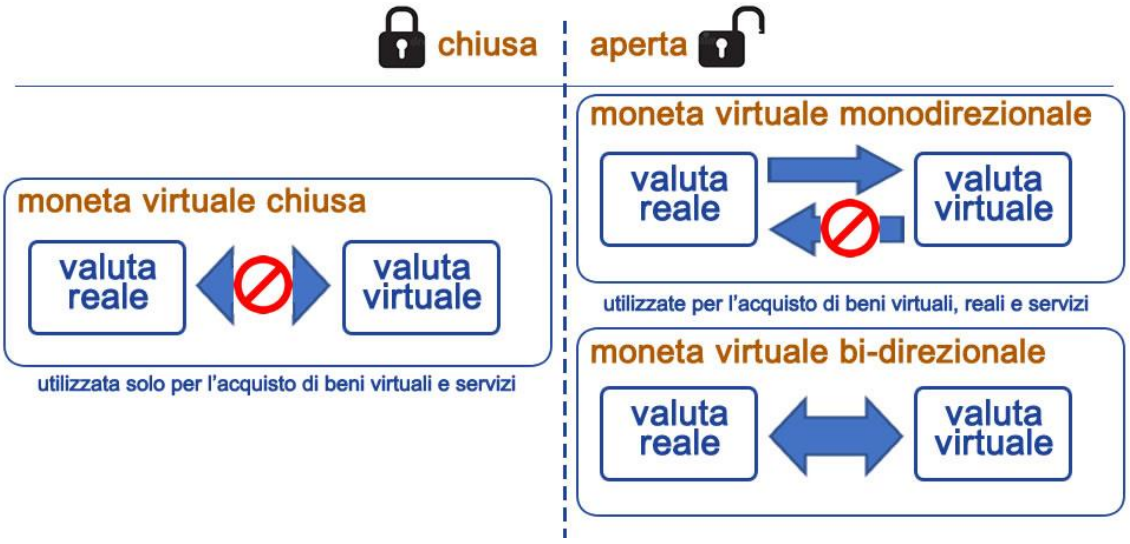


Figura 2.1. *Tipologie di monete virtuali. Fonte "https://civitas-schola.it/2021/08/29/criptovalute-cosa-sono-e-quali-rischi/"*

Questa classificazione, nel corso del tempo, è stata ampliata con ulteriori definizioni sempre basate sulle modalità di interazione con l'economia reale:

1. *real money like scheme*, queste valute virtuali sono acquistate ad un tasso di cambio, deciso dall'emittente, con moneta reale e possono essere utilizzate all'interno del sistema per acquistare beni e servizi. Un esempio di questo schema è il Bristol Pund, una valuta locale utilizzata nella città di Bristol emessa dalla "Bristol Pound Community interest Company" in collaborazione con una banca etica locale.
2. *Mutual credit scheme*, queste monete virtuali sono immesse nel sistema tramite scritture contabili e non acquistate tramite denaro reale. Al momento di un pagamento, una impresa che accetti questa moneta si vede iscritta nel conto corrente un credito in valuta virtuale e questo può essere usato per pagare dei fornitori che hanno aderito allo stesso sistema. Esempi di moneta che operano secondo questo schema sono Sardex e Piemex.[3]
3. *Discount Voucher*, questa tipologia di monete virtuali includono quelle monete locali che possono essere utilizzate per pagare una parte del controvalore di servizi e beni reali.

La Banca di Italia (BI) presenta una definizione nel paper "Questioni di Economia e Finanza-Aspetti economici e regolamentari delle cripto-attività"[4], secondo la quale le criptovalute, o cripto-attività, sono una rappresentazione del valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere traferita, memorizzata e

[3] Sardex è la prima moneta complementare nato nel 2009 in un piccolo paese della Sardegna, che si è sviluppata nell'ultimo decennio ad oggi può contare più di 3500 iscritti e un giro di affari di circa 140 milioni negli ultimi 5 anni. Grazie all'impulso causato da Sardex sono nate altre monete complementari in altre regioni italiane, tra cui Piemex in Piemonte.

[4] Gola, C. and Caponera, A. 2019. Aspetti economici e regolamentari delle "cripto-attività" (Economic and Regulatory Aspects of Crypto-Assets), *SSRN Electronic Journal*, Advance Access published 2019: doi:10.2139/ssrn.3432976

scambiata elettronicamente. L'articolo sottolinea come le criptovalute non sono "fiat money" ovvero moneta legale di stato.

Una ulteriore definizione utile ad inquadrare questi nuovi asset è presentata dalla BCE nel documento "BCE, bollettino economico- numero 5/2019- Aggiornamento sugli andamenti economici e monetari"[5], dove viene posta l'attenzione sull'aspetto economico societario e regolamentare delle criptovalute. Vengono definite come delle attività che, tramite l'uso della criptografia, sono registrate in forma digitale e non sono né una attività né una passività finanziaria nei confronti di un soggetto identificato. La caratteristica peculiare delle criptovalute di non essere un credito nei confronti di un soggetto comporta che il loro valore è stimato solo in base alla previsione di quanto saranno disposti a pagare gli utenti in futuro per le stesse attività.

2.2 Caratteristiche principali delle criptovalute

Al di là delle definizioni delle criptovalute date dalle varie istituzioni, per comprendere al meglio le valute digitali è necessario fare un approfondimento sul loro funzionamento, su quali sistemi basano la loro esistenza e quali sono le principali idee da cui sono state sviluppate.

Le criptovalute hanno tre elementi fondamentali:

1. il protocollo, ovvero una serie di regole definite attraverso codice informatico che specificano le modalità con cui si possono effettuare le transazioni.
2. Blockchain/distributed ledger Technologies (DLT)/Libro Mastro, un registro che conserva lo storico delle transizioni, in particolare esso non può essere modificato in alcun modo.

[5] 2022. *Bancaditalia.It*. https://www.bancaditalia.it/pubblicazioni/bollettino-eco-bce/2019/bol-eco-5-2019/bolleco-bce-5-2019.pdf.

3. Rete decentralizzata/Decentralized Network, una rete decentralizzata di partecipanti che possono interrogare e aggiornare il registro (Blockchain) secondo le regole definite dal protocollo.

Questi sono gli elementi che sorreggono l'intero sistema su cui si basano le criptovalute.
Ma per inquadrare il contesto da cui si sono sviluppate è necessario identificare i principali concetti che costituiscono le fondamenta teoriche delle valute digitali:

- La criptografia, cioè una serie di tecniche per rendere sicure informazioni e comunicazioni. Le criptovalute si basano sul sistema delle cosiddette "Chiavi pubbliche", in cui esiste una "chiave" che è scambiabile tra gli utenti e grazie a questo scambio che possono avvenire le transazioni. All'interno di questo sistema ci sono anche le "chiavi private" che non devono essere scambiate con gli altri utenti, esse fungono come una sorta di password e servono per mantenere sicura la proprietà/il possesso delle criptovalute e per confermare le transazioni effettuate.
- Trasparenza, principio cardine alla base della creazione delle criptovalute. Con essa si intende che qualunque transazione è *timestamped* nella blockchain, ovvero è memorizzato l'esatto momento in cui è stata realizzata, in questo modo si può sapere la provenienza e la cronologia delle transazioni dei proprietari delle criptovalute. Con il concetto di trasparenza si fa riferimento anche ad una altra caratteristica legata in modo diretto al sistema della blockchain, infatti i sopracitati protocolli sono *open source*[6] e possono essere modificati.
- Principio dell'incentivo, questa caratteristica si riferisce al funzionamento dei protocolli del consenso basati sulla "teoria dei giochi" in modo che tutti gli utenti siano incentivati a comportarsi così da riuscire a mantenere funzionante l'intero sistema. Un esempio pratico di questo principio è riscontrabile nel funzionamento del *mining* e del ruolo di incentivo dato dalla ricompensa in valuta digitale utilizzo da Bitcoin.

[6] Fa riferimento al fatto che il software utilizzato per i protocolli è open source, quindi il codice di quest'ultimi è stato creato per essere accessibile e perciò ogni utente può prendere questo codice modificarlo e distribuirlo secondo la sua volontà.

2.3 Le criptovalute e la blockchain

Per avere una comprensione più chiara sulle dinamiche che determinano il funzionamento delle criptovalute in questa sezione viene approfondito il rapporto tra le criptovalute e l'innovativa tecnologia blockchain.

Le basi teoriche della blockchain nascono dal concetto di libro mastro detto anche *Ledger*. La forma più semplice di organizzazione del *ledger* è il *Centralized ledger*, questa si basa sul rapporto centralizzato in cui esiste una struttura di riferimento che gestisce tutte le operazioni e in cui è riposta la fiducia. La Pubblica amministrazione e le banche, ad esempio, utilizzano questi sistemi e rappresentano, in quel contesto, la struttura di riferimento; essi controllano l'accesso alle informazioni contenute nel libro mastro. L'insieme di regole definito dall'autorità centrale viene definito *Governance*.

Come evoluzione del sistema centralizzato è stato creato il *Decentralized ledger*, anch'esso basato sulla logica della centralizzazione ma con più strutture centrali che operano a livello "locale". In sostanza, è la ripetizione del sistema centralizzato all'interno di un'unica rete con l'esistenza di collegamenti tra le strutture centrali. Anche queste organizzazioni si basano sulla fiducia che deve essere riposta nei vari soggetti centrali.

La struttura più rivoluzionaria è sicuramente la *Distributed Ledger*, dove non esiste più un vero centro di controllo e la logica della fiducia e della governance si basa sulla fiducia tra tutti i soggetti.

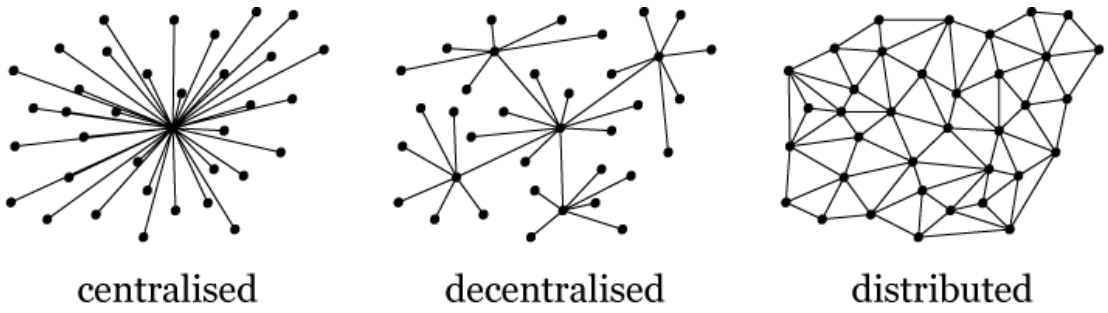
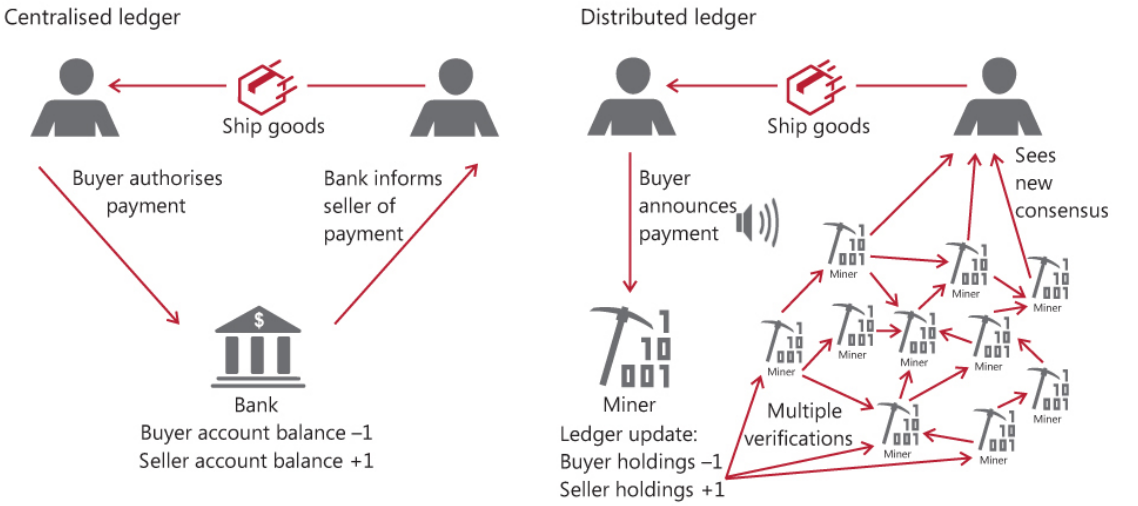


***Figura* 2.2.** *Rappresentazione grafica delle tipologie di ledger. Fonte"https://commons.wikimedia.org/"*

Valid transactions in a centralised ledger/bank account and in a permissionless cryptocurrency

Graph V.3



A buyer purchases a good from the seller, who initiates shipment upon perceived confirmation of the payment. If the payment takes place via bank accounts – ie via a centralised ledger (left-hand panel) – the buyer sends the payment instruction to their bank, which adjusts account balances debiting the amount paid from the buyer's account and crediting it to the seller's account. The bank then confirms payment to the seller. In contrast, if payment takes place via a permissionless cryptocurrency (right-hand panel), the buyer first publicly announces a payment instruction stating that the cryptocurrency holdings of the buyer are reduced by one, while those of the seller are increased by one. After a delay, a miner includes this payment information in a ledger update. The updated ledger is subsequently shared with other miners and users, each verifying that the newly added payment instruction is not a double-spend attempt and is authorised by the buyer. The seller then observes that the ledger including the payment instruction emerges as the one commonly used by the network of miners and users.

Source: Adapted from R Auer, "The mechanics of decentralised trust in Bitcoin and the blockchain", *BIS Working Papers*, forthcoming.

***Figura* 2.3**. *Rappresentazione di una registrazione di una transazione in un sistema centralizzato e in un sistema con un registro decentralizzato (nello specifico si fa riferimento al caso Bitcoin). Fonte "https://www.bis.org/publ/arpdf/ar2018e5.htm".*

Le *Distributed ledger Technologies* (DLT) sono dei sistemi che permettono di creare un registro crittografato di informazioni che sono controllabili, gestibili e accessibili in modo condiviso da più nodi della rete detto, un DLT viene anche definito "registro distribuito". La differenza fondamentale rispetto a un semplice database centrale con la possibilità di accesso condiviso tramite password, è che le DLT permettono la creazione di una cronologia delle transazioni immodificabile e non necessitano di una autorità terza affidabile.

Sono disponibili tre tipologie di DLT:

1. protocolli DLT "permissioned/privati", il gestore del protocollo può modificarlo e controllare il numero dei nodi. Inoltre, possono operare anche senza l'incentivo basato sulla creazione di token e il processo di minig.

2. Protocolli DLT "permissionless/pubblici", la gestione in questi protocolli è totalmente decentrata attraverso l'azione di soggetti specializzati.
3. Protocolli DLT "ibridi", hanno un sistema di validazione decentrato tramite i nodi, anche se non tutti abilitati dal gestore del protocollo, ma lasciano al gestore del protocollo il controllo.

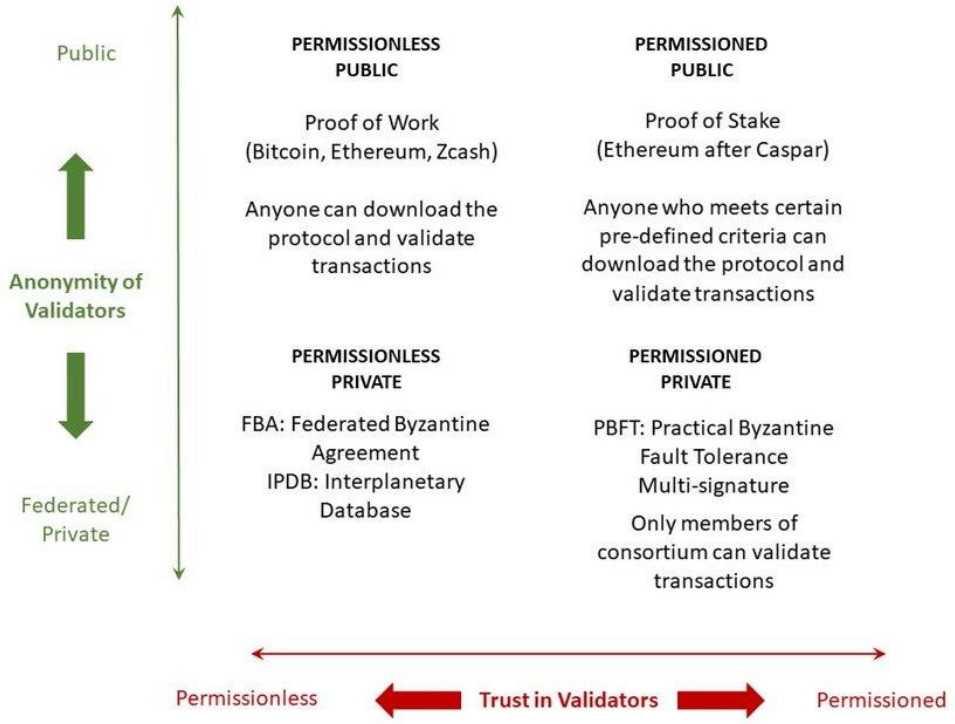


Figura 2.4. *Rappresentazione grafica delle tipologie di DLT in base alla fiducia e anonimato dei validator. Fonte" B. Varghese et al., "Realizing Edge Marketplaces: Challenges and Opportunities," in IEEE Cloud Computing, vol. 5, no. 6, pp. 9-20, Nov./Dec. 2018,";"https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/"*

Il protocollo Blockchain fa parte della famiglia delle *Distributed ledger Technologies* (DLT) ed è il protocollo su cui si basa la criptovaluta più famosa: "Bitcoin". La blockchain si può immaginare come una catena di blocchi collegati tra loro, ogni blocco rappresenta dei dati che non possono essere alterati a meno che non ci sia il consenso della maggioranza della rete. Ad ogni blocco sono associate una o più transizioni.

Componenti della blockchain

Per spiegare il funzionamento della Blockchain si fa riferimento al sistema creato contestualmente a Bitcoin, chiaramente quest'ultimo ha subito delle evoluzioni e degli adattamenti, nel corso del tempo, per poter ampliare i campi e metodi di applicazione.
I componenti principali della Blockchain sono:

- Nodi: sono coloro che partecipano alla blockchain e sono formati dai server di ognuno dei partecipanti e detengono una propria copia del registro ledger.
- Transazioni: costituiscono un insieme di dati e rappresentano gli oggetti di scambio.
- Blocco: è sostanzialmente un insieme di una o più transazioni che sono unite per essere processate secondo il metodo di verifica.
- Hash: è un algoritmo matematico che mappa dei dati in una stringa binaria di dimensione fissa in modo unidirezionale, ciò la rende una funzione criptografica che è difficile da invertire. Date le sue proprietà, applicata a funzioni criptografiche, è largamente utilizzata nell'ambito della sicurezza informatica.
- Algoritmo del consenso: utilizzato per gestire la creazione dei blocchi e il comportamento degli utenti. Gli utenti che vogliono aggiungere i blocchi nella catena devono fornire uno *stake,* cioè un valore generico che il *validator* deve mettere in gioco, in modo che gli incentivi siano bilanciati ed essi siano incentivati a comportarsi in modo onesto. L'esempio tipico di questi algoritmi sono i "Proof-of-Work", utilizzati nel sistema Bitcoin, originariamente nati per evitare attacchi informatici di tipo *Denial of Service*[7] . L'algoritmo funziona sulla risoluzione di un puzzle matematico in cui la soluzione è raggiungibile solo tramite il metodo *brute force*[8].

[7] Indica un malfunzionamento causato da un attacco informatico in cui l'aggressore provoca un esaurimento delle risorse della rete di un sistema informatico che fornisce un servizio ai client, in questo modo si impedisce agli utenti di accedere alla rete e al servizio attaccato. Esempi di questo tipo di attacco sono: "Mail bomb", "Ping of the death", ecc.

[8] Nel campo della sicurezza informatica questo algoritmo consiste nel verificare tutte le soluzioni possibili fino a trovarne una accettabile.

- Miners: sono nodi specializzati che, dopo aver creato un nuovo blocco, competono per la sua validazione cercando la risoluzione della "proof-of-work". L'algoritmo di consenso "PoW" consente ai miners di convalidare e aggiungere un nuovo blocco alla blockchain solo se gli altri sono concordi con la soluzione fornita.

Funzionamento della blockchain

Quando due utenti decidono di voler effettuare una transazione, questa viene creata nel sistema e comprende vari elementi:

1. L'indirizzo pubblico del ricevente.
2. Le informazioni relative alla transazione.
3. Le chiavi criptografiche relative alla transazione.

Le transazioni rimangono in sospeso sulla rete finché non vengono collezionate e raggruppate in un blocco di transazioni dai nodi di mining. Questa operazione è svolta dai miner che selezionano le transazioni da includere nel nuovo blocco e successivamente passano alla creazione di esso. In questa fase del processo questo nuovo blocco è definito "candidato" in quanto non ha ancora ricevuto una validazione completa, ad esso devono essere associate tutte le informazioni essenziali richieste dal sistema: il valore di Hash del blocco precedente, il timestamp, la Merkle root[9] e il Nonce[10].

[9] È una rappresentazione in forma ridotta del set di transazioni che sono presenti all'interno del blocco da confermare.

[10] È un numero casuale o pseudo-casuale che in criptografia viene utilizzato all'interno ne protocolli di autenticazione. In una rete blockchain, in combinazione con l'hash, viene utilizzato durante la Proof-of-Work come mezzi di controllo per evitare alterazioni dei blocchi e assicura la protezione da *replay attack*.

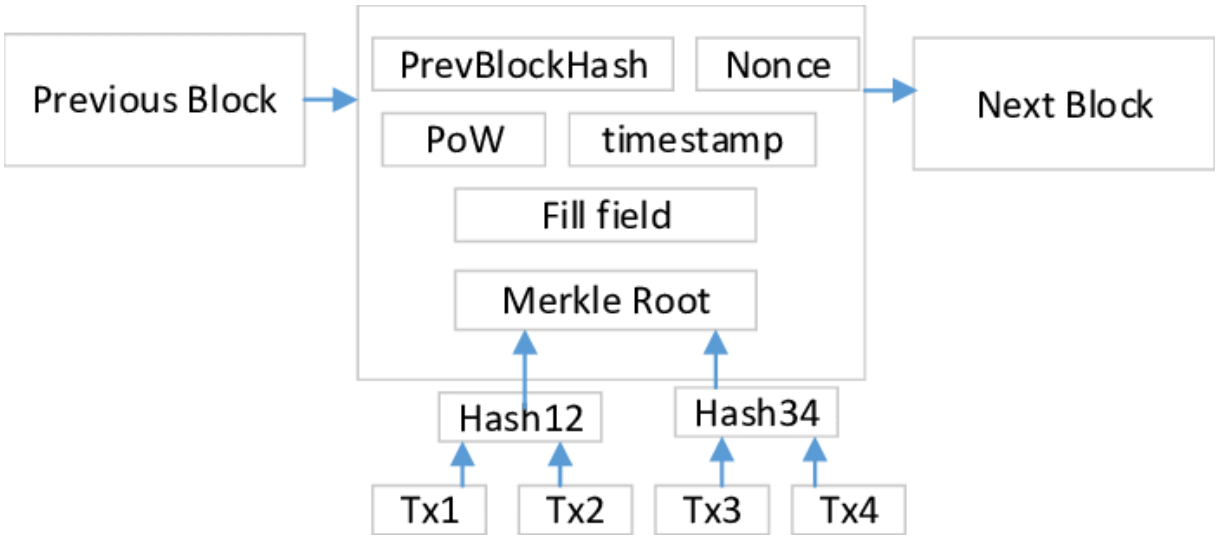


Figura 2.5. *Struttura di un blocco della catena. Fonte: Yang, X., Liu, J., and Li, X. 2019. Research and Analysis of Blockchain Data, https://www.researchgate.net/publication/334424125_Research_and_Analysis_of_Blockchain_Data (date last accessed February 27, 2022)*

Dopo che il blocco è stato creato, il miner deve eseguire la Proof-of-Work, ossia deve trovare la soluzione al puzzle criptografico eseguendo un processo di calcolo matematico per ogni blocco che ha formato. La soluzione della prova è nota come hash, ovvero una stringa costituita di numeri e lettere non invertibile. Ottenuto, quindi, l'hash valido dalla PoW, il miner trasmette questo risultato agli altri nodi della rete in modo che essi abbiano la possibilità di convalidarlo.

Gli altri nodi della rete verificheranno la legittimità e la soddisfazione dei requisiti richiesti dal sistema, è in questa fase che vengono effettuati i controlli a protezione del problema del *doublespending*[11]. Dopo che il blocco ottiene l'approvazione della rete, il miner che ha aggiunto il blocco ottiene, come ricompensa, una somma in valuta digitale.

Durante la fase di verifica i blocchi devono avere necessariamente le seguenti caratteristiche:

- Le transazioni contenute nel blocco devono essere valide.

[11] Il problema del *doublespending*, se non viene risolto, può compromettere l'intero sistema e protocollo di una moneta digitale, per questo motivo tutte le più importanti criptovalute presenti sul mercato lo hanno risolto. Il problema emerge quando in un sistema gli stessi fondi possono essere spesi, o inviati, a due utenti in contemporanea. Nei sistemi tradizionali sono le autorità centrali che controllano che non avvenga una doppia spesa.

- La dimensione del blocco deve soddisfare i limiti imposti dal sistema, nel caso di Bitcoin deve essere al massimo di 1-2MB.
- L'hash di intestazione del blocco deve essere inferiore al target.
- Il timestamp del blocco non deve superare le due ore nel futuro.
- L'intestazione del blocco deve contenere l'hash del blocco precedente e la *block height*, un numero che rappresenta la quantità di blocchi confermati nella catena.
- La prima transazione del blocco deve essere la *coinbase transaction*, che serve per far ricevere la ricompensa al miner.

Tutti i miner che avevano iniziato a competere per il blocco appena aggiunto alla catena dovranno avviare un nuovo processo per creare un nuovo blocco contenente altre transazioni. Quindi nel momento in cui un miner ottiene la risoluzione del problema criptografico, se nel frattempo sono stati aggiunti nuovi blocchi alla catena, l'hash trovato non avrà la corrispondenza con l'hash dell'ultimo blocco aggiunto e quindi sarà rifiutato dalla rete nella fase di verifica.

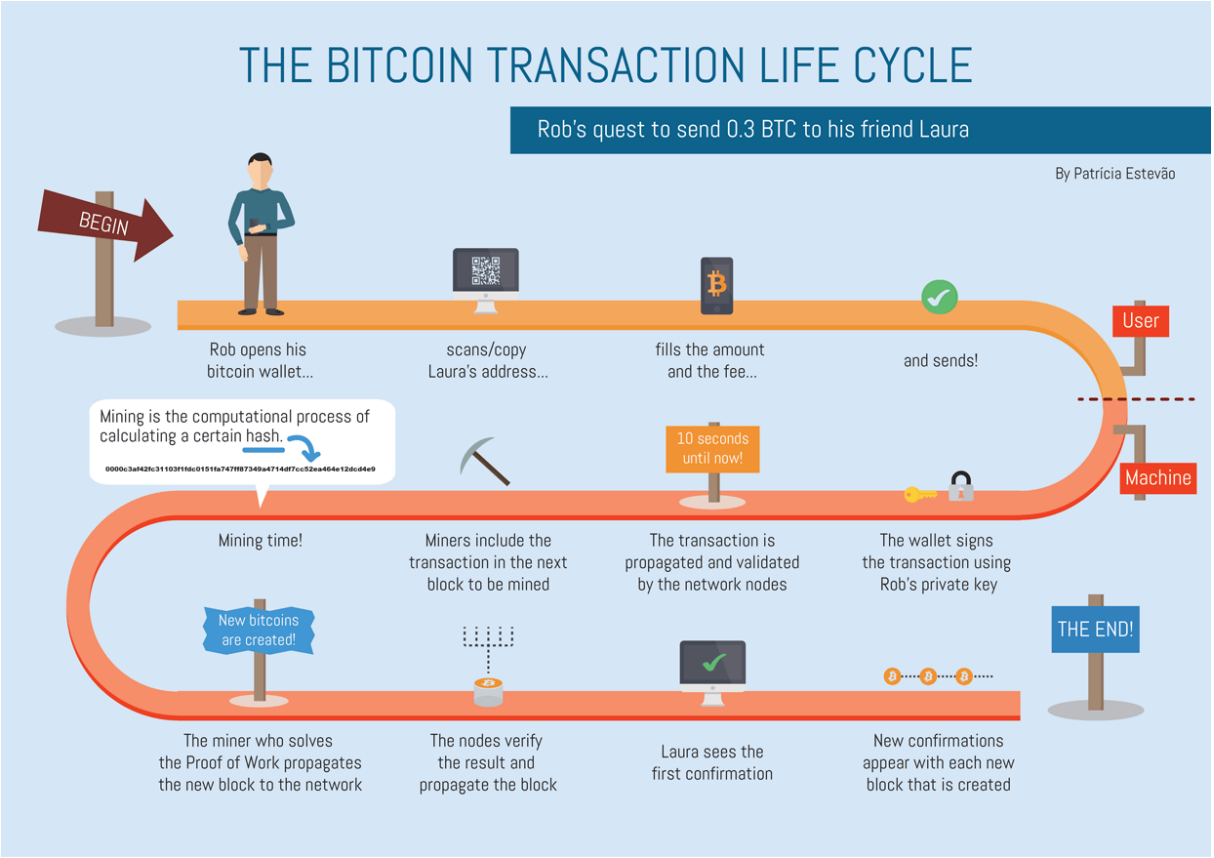


***Figura 2.5**. Schema di una transazione e creazione di un nuovo blocco nella blockchain. Fonte:" https://en.bitcoinwiki.org/wiki/File:Bitcoin-transaction-life-cycle.png".*

Caratteristiche della blockchain

Per concludere la visione di insieme della blockchain è necessario, quindi, individuare quali sono le sue caratteristiche essenziali profondamente legate alla natura della sua struttura. Questa analisi si basa sull'articolo di Roberto Garavaglia "Finalità, funzionamento e tipologia di utilizzi della Blockchain" contenuto nei "Quaderni di ricerca giuridica e della consulenza legale" pubblicato dalla Banca d'Italia[12]. Si individuano le seguenti caratteristiche:

[12] Banca d'Italia. 2019. *Banca d'Italia - N. 87 - Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, Bancaditalia.it, https://www.bancaditalia.it/pubblicazioni/quaderni-giuridici/2019-0087/index.html (date last accessed March 21, 2022)

- Decentralizzazione: ragione per cui si riesce garantire una certa robustezza e sicurezza distribuendo i dati e i ruoli tra una pluralità di nodi.
- Disintermediazione: l'eliminazione dei nodi centrali che gestiscono i processi in modo da semplificare il sistema.
- Programmabilità: la possibilità di poter programmare certe azioni al verificarsi di certe condizioni.
- Immutabilità: si riferisce all'impossibilità di modificare o manipolare una transazione dopo che è stata verificata e confermata nel registro condiviso.
- Verificabilità: si intende la sicurezza che ogni informazione scritta nel registro distribuito sia verificata e dalla facilità con cui è possibile consultare il distributed ledger.
- Accountability: la possibilità di sapere cosa sia scritto sul registro distribuito, chi l'abbia scritto e in quale momento.
- Tracciabilità: esiste la possibilità di conoscere la provenienza di ogni singolo elemento del registro.
- Trasparenza: il contenuto del registro distribuito è trasparente e visibile a tutti i nodi.

2.4 Ecosistema delle criptovalute

Nel documento redatto dalla BCE "Virtual Currency Scheme - a further analysis" 2015[13] si individuano gli attori principali e il loro ruolo all'interno dell'ecosistema delle criptovalute:

- Inventori/creatori: sono coloro che creano le valute virtuali e sviluppano tecnicamente parte della sua rete. Possono essere individui o organizzazioni e possono decidere di essere pubbliche o di mantenere sconosciuta la propria identità (come, ad esempio, è successo per Bitcoin).
- Emittenti: sono capaci di generare valute virtuali. In un sistema di valute centralizzato spesso sono anche coloro che amministrano il sistema e stabiliscono le regole di

[13] European Central Bank. 2015. Virtual currency schemes – a further analysis, Advance Access published 2015: doi:10.2866/662172

utilizzo e circolazione. Ma in un sistema decentralizzato, come ad esempio quello di Bitcoin, le monete possono essere create dai "miner" in modo automatico in base alle loro capacità e risultati.

- Miners: sono persone, spesso organizzate in gruppi, che utilizzano la potenza di calcolo dei loro computer per verificare e validare un blocco costruito con un sistema decentralizzato aggiungendolo al registro delle transizioni, la blockchain. Il loro ruolo è essenziale all'interno di un sistema decentralizzato perché, altrimenti non sarebbe possibile raggiungere gli standard di sicurezza e risolvere il problema del *doublespending*. I miners sono ricompensati ricevendo uno specifico ammontare di valute virtuali in modo automatico all'interno di un sistema decentralizzato e, inoltre, possono richiedere una *transaction fee* da chi ha iniziato la transazione.
- Processing service provider: serve per facilitare il trasferimento delle valute; nei sistemi decentralizzati VCS questo ruolo è in parte ricoperto dai miners.
- Utenti: sono gli utenti della rete che decidono di ottenere delle valute virtuali per acquistare beni o servizi reali o virtuali, per scambi di denaro, pagamenti tra persone, per fini di investimento e speculazione. Le modalità con cui si possono ottenere le criptovalute sono varie: ovviamente si possono comprare, ma possono essere ottenute anche come ricompensa per alcuna attività come sondaggi o promozioni. È possibile ottenerle anche generandole attraverso il processo di mining. Infine, chiaramente si possono ricevere come pagamento e donazione.
- Wallet providers: offrono un servizio denominato *digital wallet* che serve per conservare le proprie chiavi crittografiche delle monete virtuali e i codici di autenticazione delle transizioni; inoltre, offrono la possibilità di accedere ad una cronologia di tutte le transizioni effettuate. I wallet possono essere suddivisi in due macrocategorie: gli *hot wallet*, che possono consistere in un software messo a disposizione dell'utente che gli consente di ricevere e inviare criptovalute usando una applicazione, il tutto collegandosi ad una rete internet. I *cold wallet*, che offrono la possibilità di conservare in un luogo sicuro e non connesso alla rete le valute digitali.
- Exchages/scambia valute: hanno il ruolo di offrire dei servizi di trading e di conversione agli utenti quotando i tassi di cambio a cui si possono vendere o comprare

le valute virtuali con altre valute virtuali o attraverso valute reali. Questi *exchanges* possono essere di terze parti oppure affiliati agli emittenti.

- Piattaforme di trading: a differenza degli *exchanges*, non si occupano di comprare e vendere loro stesse le valute virtuali, hanno una funzione di mercato dando la possibilità ai compratori e venditori di valute virtuali di operare su una piattaforma dove poter raccogliere domanda e offerta.

3 CRIPTOVALUTE E SISTEMI DI PAGAMENTO

L'avvento delle criptovalute all'interno del mondo economico ha determinato l'avvio di una grande ondata di innovazione che, ad oggi, non si è ancora arrestata. La caratteristica per eccellenza delle criptovalute, che ne ha determinato il successo, è la loro decentralizzazione, derivata da un tentativo di svincolarsi dai classici intermediari.

La volontà di disintermediazione spinse nel 2008 un certo Satoshi Nakamoto, probabilmente uno pseudonimo, a pubblicare online "Bitcoin: a Peer-to-Peer Eletronic Cash system"[14], un documento dove spiega un metodo con cui era possibile creare e utilizzare una moneta digitale bypassando gli intermediari tradizionali. Questo documento non solo sancì la nascita della criptovaluta più famosa del momento, Bitcoin, ma fu anche un simbolo della volontà di cambiare un paradigma che ormai si era consolidato. Da allora il fenomeno dei Bitcoin, e in generale delle criptovalute, ha iniziato ad espandersi ed essere sempre più diffuso fino a diventare un fenomeno di massa.

[14] Nakamoto, S. 2008. *Bitcoin: a Peer-to-Peer Electronic Cash System*, date last accessed at bitcoin.org at https://bitcoin.org/bitcoin.pdf

In questo capitolo verrà trattato l'evoluzione delle criptovalute come metodo di pagamento, verranno valutati i passaggi fondamentali e quali sono i vantaggi e gli svantaggi di tale strumento.

Secondo l'articolo "L'anno delle criptovalute: è davvero una nuova età dell'oro?" [15] pubblicato su Econopoly, un blog del "IlSole24Ore", il 2021 sarà l'anno in cui l'adozione delle criptovalute esploderà definitivamente, come dimostrato anche dal numero di campagne di regolamentazione dei mercati fatte nell'ultimo periodo. Come dimostra un indice composito[16] creato dalla società "ChainAnalisys", l'utilizzo delle criptovalute è aumentato del 2500% (quindi di 25 volte) tra l'inizio del 2020 e la metà del 2021 con un picco a partire da gennaio 2021. In correlazione alla crescita dell'utilizzo delle criptovalute, nei paesi industrializzati con un'infrastruttura finanziari evoluta si è riscontrato un veloce sviluppo della finanza decentralizzata (DEFI), ovvero il tentativo di creare delle "piattaforme di negoziazione decentralizzate dei più comuni servizi finanziari" come, ad esempio, prestiti o depositi remunerati, servizi che sono forniti dagli intermediari tradizionali.

3.1 Evoluzione delle criptovalute come metodo di pagamento

Prendendo ad esempio Bitcoin come valuta digitale più famosa e diffusa, è possibile ripercorre le tappe dell'evoluzione dei metodi di pagamento tramite criptovalute e della loro diffusione. La famosa prima transazione utile ad acquistare un bene fisico è stata effettuata il 22 maggio 2010, 10.000 Bitcoin furono pagati in cambio di due pizze. All'epoca non esistevano metodi ufficiali o definiti per acquistare con la valuta digitale beni o servizi; perciò, le prime transazioni di Bitcoin erano negoziate da ogni persona tramite il forum Bitcoin forum secondo una sorta di baratto in cui venivano scambiate le criptovalute e monete legali.

Una ulteriore tappa fondamentale nella storia delle criptovalute è la fondazione di "BitPay", avvenuta nel 2011, che aveva l'ambizione di trasformare il modo in cui le persone potevano ricevere, scambiare, conservare e gestire i propri soldi. L'innovazione della società fu quella di

---

[15] Econopoly. 2022. *Blog | L'anno delle criptovalute: è davvero una nuova età dell'oro?*, Econopoly, https://www.econopoly.ilsole24ore.com/2022/01/21/criptovalute-bitcoin-moneta/ (date last accessed February 27, 2022)

[16] La costruzione dell'indice è basata sui valori del traffico registrato dalle reti decentralizzate.

essere tra i pionieri nell'adottare la blockchain nei processi di pagamento e fin dall'inizio ha deciso di voler rendere più facile e accessibile alle aziende accettare i bitcoin, e in generale le criptovalute come metodo di pagamento in modo da diventare uno tra i più grandi *bitcoin payment processor* nel mondo. BitPay offriva, sulla propria piattaforma online, varie possibilità di gestione delle proprie valute digitali, ossia la possibilità di gestire il proprio *wallet* e le proprie carte prepagate in modo da dare la possibilità di trasformare le valute digitali in dollari. Per comprendere la rapidità di espansione del fenomeno, ad ottobre 2012 BitPay aveva circa 1100 venditori attivi che attraverso la piattaforma accettavano bitcoin come valuta per i pagamenti online.

Dopo pochi mesi, lo scambio e la gestione delle criptovalute non rimasero esclusivamente in forma virtuale tramite i propri dispositivi, ma si decise di creare dei classici sportelli automatici in cui però fosse possibile gestire le proprie valute virtuali e in alcuni casi di poterle vendere per acquistare denaro contante nella propria moneta locale. Il primo ATM[17] in grado di offrire questi servizi fu installato nell'ottobre del 2013 in un coffee shop a Vancouver, Canada. Lo sportello non solo dava la possibilità di gestire le proprie valute digitali a chi già le possedeva, ma la Robocoin, società che si occupava dello sportello automatico, aveva previsto la possibilità di creare un proprio portafoglio e acquistare criptovalute direttamente dallo sportello utilizzando: un indirizzo mail, un documento di identità e un sistema di identificazione biometrico [18] installato direttamente sulla macchina. L'installazione dello sportello si dimostrò un successo dal momento che, in 30 giorni di operatività, lo sportellò effettuò 1500 transazioni e circa il 30% di queste erano state effettuate da utenti che non avevano mai utilizzato bitcoin.

L'ultimo grande passo che ha reso le criptovalute uno strumento di pagamento alla portata di tutti coincide con l'entrata di quest'ultime nel sistema di PayPal, società leader del settore dei servizi di pagamento digitale e di trasferimento di denaro attraverso internet. Nel 21 ottobre 2020 la società ha comunicato di essere pronta ad accettare pagamenti in criptovalute

---

[17] ATM, automated teller machine, è semplicemente l'acronimo di uso internazionale che fa riferimento allo sportello auomatico.

[18] Sistema informatico che garantisce l'identificazione di una persona basandosi su alcune caratteristiche fisiologiche. Fonte https://it.wikipedia.org/wiki/Sistema_di_riconoscimento_biometrico.

rendendo accessibile questa categoria di valute ad oltre 400 milioni di account. PayPal darà la possibilità a tutti i suoi utenti di poter utilizzare le criptovalute come strumento di pagamento e permetterà di poter acquistare e vendere le criptovalute in maniera semplice e sicura.
Il metodo di pagamento di PayPal mediante le criptovalute avviene in modo tale che, qualora un utente decidesse di utilizzare i propri fondi in valute digitali per effettuare una transazione di acquisto, il venditore incasserebbe l'importo in valuta legale. PayPal provvede a effettuare le conversioni tra criptovalute e moneta legale nel momento della transazione per all'ammontare dell'importo, in questo modo protegge il venditore affiliato ai suoi servizi dai rischi di fluttuazione delle criptovalute.

3.2 Vantaggi nell'utilizzo delle criptovalute

Sono stati individuati alcuni vantaggi nell'utilizzo delle criptovalute come metodo di pagamento:

- bassi costi di transazione: i pagamenti in criptovalute sono solitamente più economici, la commissione, a carico del mittente, varia in base all'entità della transazione. Le parte delle commissioni pagate dagli utenti vengono ricevute dai miner al termine della creazione di un blocco e spesso rappresentano una significativa parte del loro profitto. Quindi, l'utente è libero di scegliere tempi e costi per la transazione, ovviamente pagando una commissione più alta otterrà una elaborazione della transazione più veloce. Inoltre, gli utenti che usufruiscono delle piattaforme exchange, che semplificano molto le transazioni, dovranno pagare le transazioni alle piattaforme stesse, esse sono diversificate in base al servizio usufruito e alla criptovaluta interessata.
- Controllo e sicurezza: gli utenti hanno la possibilità di avere un controllo completo sulle transazioni e in questo modo non si ha la possibilità di ritirare denaro dal portafoglio del proprietario senza il suo consenso. I pagamenti effettuati con le criptovalute non trasmettono alcuna informazione personale, quindi, sono più protetti dai furti di identità. Oltre a ciò, data la natura criptografica delle transazioni tramite

chiave pubblica e privata non è possibile subire furti tramite clonazione dei dati, come può avvenire per le carte di credito.

- Neutralità e trasparenza: tutte le transazioni sono verificabili da ogni utente in qualunque momento. Il protocollo essendo criptato non può essere modificato né alterato da un singolo utente, quindi si ha la certezza che il sistema sarà sempre neutrale e trasparente.
- Svincolamento dai sistemi di pagamento tradizionali: data la natura decentralizzata delle criptovalute è possibile svincolarsi dai metodi tradizionali di pagamento come il denaro contante, le carte di credito, ecc. In questo modo non si è più soggetti ai loro limiti e alle regole imposte dalle autorità centrali dando la possibilità agli utenti di esplorare nuovi mercati.
- Facilità di accesso: per la creazione di un *wallet* non sono necessarie molte operazioni o strumenti, attraverso una connessione internet è possibile fare ciò in pochi minuti. Per richiedere l'apertura di un conto bancario in Italia, anche nel caso di una operazione *full digital*, le banche tradizionali migliori richiedono un tempo di attivazione di 48 ore e un numero di click tra i 70 e 80. I dati sono citati dall'articolo pubblicato dal IlSole24Ore "Meno di due giorni per aprire un conto con una banca fintech, ben 14 con una tradizionale."[19]
- Libertà nelle transazioni: tramite i sistemi forniti dalle criptovalute è possibile effettuare transazioni di qualunque ammontare, a qualunque persona e verso qualunque paese. Nessuna transazione può essere impedita o controllata quindi il livello di libertà fornito dalle valute digitali è chiaramente maggiore rispetto a quelle tradizionali.
- Anonimato/pseudo privacy: nonostante le transazioni siano accessibili a tutti gli utenti che appartengono alla rete, l'identità delle persone che effettuano le transazioni rimane

[19] Incorvati, L. 2021. *Meno di due giorni per aprire un conto con una banca fintech, ben 14 con una tradizionale*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/meno-due-giorni-aprire-conto-una-banca-fintech-ben-14-una-tradizionale-AD5i1IKB (date last accessed February 28, 2022)

protetta e inaccessibile. È descritto, però, come "pseudo anonimato" perché è possibile risalire all'indirizzo digitale della persona che effettuato la transazione ma non è possibile collegarlo a nessun dato identificativo di una persona.

3.3 Svantaggi nell'utilizzo delle criptovalute

I principali svantaggi analizzati nell'utilizzo delle criptovalute sono:

- volatilità: è sicuramente lo svantaggio principale delle criptovalute in quanto la maggior parte di esse è caratterizzata da una grande volatilità, rendendo il loro valore particolarmente imprevedibile.
- Possibilità di utilizzo: anche se in alcuni paesi le criptovalute stanno diventando legali e vengono riconosciute come moneta, nella maggior parte dei paesi non sono ancora accettate come metodo di pagamento. Questa criticità riguarda soprattutto i negozi fisici, in quanto i siti di e-commerce ormai sono tutti piuttosto disponibili ad accettare questo metodo di pagamento.
- Complessità: rispetto ai metodi tradizionali le criptovalute al momento richiedono una consapevolezza maggiore e delle competenze superiori, soprattutto per quanto riguarda la tecnologia sottostante le dinamiche che le coinvolgono, e quindi sicuramente, al momento, sono meno *user friendly*. Questa complessità si trasforma in una barriera all'ingresso per potenziali nuovi utenti rallentando la diffusione della criptovaluta come sistema di pagamento.
- Immaturità: essendo una tecnologia piuttosto innovativa ha ancora degli aspetti che risultano non completamente sviluppati e ottimizzati. Per alcuni potenziali utilizzatori, quindi, potrebbero ancora mancare dei servizi fondamentali che probabilmente presto verranno implementati.
- Problema di tassazione: data la peculiarità delle criptovalute di non avere bisogno di intermediari è sorto il problema di come si potesse gestire il pagamento delle tasse per non incorrere in problemi legali. In Italia, la normativa fiscale sulle criptovalute è basata su varie opinioni dell'Agenzia delle entrate e su delle sentenze dei tribunali e non su delle leggi chiare, in questo modo si possono creare delle discordanze e delle incomprensioni. Molti esperti del settore stanno sottolineando questo problema che

rischia ulteriormente di frenare la diffusione delle criptovalute in Italia, poiché molte persone hanno paura di commettere irregolarità.

- Problema reputazionale: le criptovalute sono state usate e vengono sfruttate, al momento, per compiere degli atti illeciti come riciclaggio di denaro, finanziamento al terrorismo, acquisti illeciti, eccetera, perciò le persone sono restie a adottarle e a utilizzarle per paura di essere giudicate e di rovinare la loro reputazione.
- Nessuna garanzia/assicurazione: tramite i mezzi tradizionali è possibile godere di alcuni diritti che garantiscono, fino ad una certa soglia, i risparmi degli utenti nel caso di fallimento della banca. I possessori di criptovalute non hanno garanzie in merito ad un possibile problema sistemico che potrebbe colpirle, questo aspetto aumenta i rischi nell'investire in questi asset e mette a rischio anche il semplice possesso di queste valute.

4 CRIPTOVALUTE E MONETA INTERNAZIONALE

In questo capitolo verrà analizzato l'impatto delle criptovalute sul sistema monetario tradizionale e la possibilità delle valute digitali di diventare una moneta internazionale.

4.1 Introduzione al sistema monetario

la moneta sostanzialmente nasce da una convenzione sociale, inizia ad essere fondamentale per lo sviluppo della società quando si ritenne necessario il superamento della "doppia coincidenza" negli scambi, ovvero quando non era più necessario barattare contestualmente due beni che sodisfacessero entrambe le parti. Non è l'unico motivo per cui si decise di utilizzare la moneta, l'utilizzo della moneta divenne fondamentale anche per superare il problema dei conflitti per i debiti e crediti nei confronti della società e per impedire che si creassero dissensi sul contributo di ognuno alla società.
La letteratura è concorde nel definire tre funzionali fondamentali che una moneta deve svolgere per essere definita tale:

- mezzo di pagamento: strumento attraverso il quale è possibile ottenere beni e servizi. Attraverso la consegna della moneta l'acquirente si libera da ogni obbligo nei confronti del venditore, allo stesso tempo il venditore accettandola riconosce il suo valore.
- Riserva di valore: rappresenta la funzione di poter conservare la possibilità di effettuare altri acquisti di beni e servizi in futuro. Sostanzialmente permette di traslare nel tempo una quota di ricchezza che si decide di non utilizzare immediatamente per lo scambio di beni e servizi in modo da averla comunque disponibile per il futuro.
- Unità di conto: fa riferimento alla funzione di rappresentare in modo numerico e convenzionale il valore di un bene o servizio. Inoltre, con l'utilizzo della moneta è possibile confrontare il valore di beni e servizi anche molto diversi tra loro in maniera omogenea, in questo modo si possono rendere più agevoli le decisioni economiche.

La prima forma di moneta che si creò nella società fu la cosiddetta moneta merce, detta anche *commodity money*, che era un mezzo di pagamento che aveva intrinsecamente un valore proprio, indipendente dal valore come strumento di pagamento. Questo tipo di moneta poteva essere di varie tipologie ma doveva rispettare alcune caratteristiche essenziali:

- Disponibilità: si richiede che sia disponibile per dare la possibilità di poterla diffondere negli scambi aumentando così la sua accettazione.
- Divisibilità: deve essere poter essere frazionata.
- Non deperibilità: grazie a questa caratteristica
- Verificabilità: deve essere facilmente verificabile la sua qualità in modo da ridurre le incertezze nelle transazioni.

Esempi di queste monete merce sono il tè, sale, vari metalli ecc.
Nella storia, con il crescere del numero degli scambi, i sistemi monetari dovettero affrontare un problema direttamente collegato alla natura delle materie prime: la loro carenza e difficoltà di approvvigionamento. Le materie prime per eccellenza, che hanno svolto il ruolo di "collaterale" della moneta merce, sono state i metalli preziosi (oro, argento, ecc.) che ben presto crearono non poche problemi ai sistemi monetari.
Il sistema con cui si cercò di ovviare a questo problema fu il cosiddetto "Gold standard", dove la moneta conteneva in percentuale il metallo prezioso ma affianco ad essa era possibile usare le banconote. Le banconote, stampate da una banca di emissione, potevano in qualunque momento essere convertite in oro ad un tasso fisso, perciò, le banche centrali, dovevano detenere comunque delle riserve di oro tali da coprire la circolazione del denaro cartaceo. La fiducia in questo sistema era data dal fatto che si pensava che basandosi sull'oro si sarebbe garantita una stabilità dei prezzi nel lungo periodo e un equilibrio nella bilancia dei pagamenti. Il principale vantaggio era che il valore delle monete non dipendeva dal rapporto domanda-offerta, ma semplicemente dalla quantità di oro delle stesse.
A causa dei vari eventi che hanno caratterizzato la storia del Novecento gli Stati Uniti, e di conseguenza tutti i più grandi paesi europei e asiatici, nel 1971 si decise di sospendere la convertibilità del dollaro in oro e quindi di sancire la fine del *gold exchange standard*. Dopo quella decisione quindi tutte le monete diventarono "monete fiat" o monete legali.
Una moneta legale ha un valore non dato dal fatto di avere come "collaterale" un metallo prezioso, ma il valore è dato dalla potenza economica e politica di chi le emette. La moneta

legale è emessa da una banca centrale e il suo valore è dato dal fatto che gli utilizzatori confidano che essa manterrà il valore stabile nel tempo. Accanto a questa moneta legale, detta anche "moneta pubblica", che consiste in forma fisica nelle banconote e monete e in forma di riserve bancarie, esiste la "moneta privata" che consiste nell'insieme dei depositi presso le banche.

In questo sistema le banche centrali hanno il monopolio sull'offerta di moneta in quanto sono le uniche entità autorizzate a emettere banconote e perché possono esercitare un controllo sulle monete digitali create dalle banche.

Dalla Seconda guerra mondiale, grazie alla supremazia degli Stati Uniti nel secolo scorso e alle numerose alleanze politiche, il dollaro è la valuta di riserva internazionale per eccellenza, ovvero una valuta che è conservata in quantità significative da istituzioni e governi come componente per le riserve di divise estere. Come dimostrazione di questa egemonia si può constatare che la maggior parte dei titoli finanziari in circolazione è in dollari, come anche e anche la maggioranza del commercio internazionale. Grazie a questa posizione dominante, tramite la Federal Reserve, ha la possibilità di influenzare il ciclo economico globale e allo stesso tempo supportare l'intero sistema nei momenti di crisi.

4.2 L'egemonia del dollaro e la posizione delle criptovalute

Nel 2020, a causa della crisi pandemica, l'egemonia del dollaro è stata messa in discussione dal momento che la valuta ha toccato il valore minimo dei due anni precedenti e ha subito la caduta peggiore degli ultimi 10 anni. Contestualmente a questo periodo il mercato delle criptovalute è cresciuto molto velocemente, spinto proprio dalla crisi pandemica; infatti, le misure delle banche centrali per salvare le economie globali hanno acceso l'interesse delle persone su strumenti finanziari alternativi come, ad esempio, l'utilizzo dei bitcoin e altre criptovalute come mezzo di copertura contro l'inflazione.

Considerando la situazione attuale, gli esperti sono scettici nell'immaginare il bitcoin, e valute digitali simili, come prossima moneta globale visti i difetti strutturali precedentemente discussi: alta volatilità, nessun inquadramento giuridico, nessuna garanzia riguardo la stabilità ecc.

Nell'articolo pubblicato dalla Banca di Italia "International Monetary System and Global Financial Cycles"[20] si analizza un'altra tipologia di criptovalute che, per le loro peculiarità, sarebbero, secondo la Banca d'Italia, più adatte a ricoprire il ruolo di moneta internazionale, ossia le cosiddette "Stablecoin".

Le Stablecoin sono una tipologia di criptovalute il cui prezzo è legato a delle monete legali, a delle commodity o anche ad altre criptovalute. Grazie a questa caratteristica riescono ad ottenere una stabilità maggiore rispetto alle criptovalute "tradizionali", come ad esempio Bitcoin, poiché possono essere collegate ad asset che non appartengono al mercato delle valute digitali, dunque le loro oscillazioni sono correlate solo a quelle degli asset sottostanti. Il successo di queste valute digitali deriva dalla possibilità di unire le qualità migliori delle valute digitali e tradizionali: l'elaborazione istantanea, la sicurezza e la privacy delle valute digitali e allo stesso tempo la stabilità e la bassa volatilità delle valute legali.

Le principali tipologie di stablecoin attuali sono:

- le stablecoin "commodity-backed", è stato riscontato che il loro valore è fissato ad una o più commodities e per esse è rimborsabile, quindi potenzialmente i possessori di queste valute digitali possono riscattare, al tasso di conversione, le loro stablecoin per ottenere gli asset sottostanti.
- Le stablecoin "fiat-backed", sono state le prime ad essere emesse sul mercato. Il loro valore si basa su una moneta legale, quindi sono negoziabili in borsa e possono essere rimborsate dall'emittente.
- Le stablecoin "cryptocurrency-backed", sono garantite da altre criptovalute in modo concettualmente assimilabile alle "fiat-backed", ma la particolarità di questo genere di stablecoin è che la collateralizzazione viene eseguita direttamente sulla blockchain attraverso degli *smart contract*. Questo maggiore grado di complessità, rispetto alle altre due tipologie, le espone ad dei rischi maggiori, come possibili bug

[20] HÉLÈNE REY International Monetary System and Global Financial Cycles. date last accessed at https://www.bancaditalia.it/pubblicazioni/lezioni-baffi/pblecture-14/Rey-2019.pdf

all'interno del codice degli *smart contract*, oltre a ciò le rendono meno desiderabili a causa della difficoltà di comprensione del meccanismo di garanzia.

- Le stablecoin "algorithmic backed", sono delle valute digitali in cui la stabilità dovrebbe essere garantita da un algoritmo che con l'emissione e il riacquisto di moneta cerca di stabilizzarne il prezzo. Un esempio di questo tipo di stablecoin è Ampleforth (AMPL).

A marzo 2020, con l'inizio della pandemia di COVID-19, si è verificato un enorme aumento della domanda delle stablecoin a causa della crisi generalizzata originata dal virus sui sistemi economici mondiali. La crisi dei mercati finanziari ha avuto degli effetti anche nel mondo delle valute digitali, ma colpendo in particolar modo le criptovalute "tradizionali" causando quindi una fuga degli utenti verso le stablecoin. Quest'ultime hanno svolto un ruolo di *Safe Haven* (attività rifugio), attività che in fasi di tensione dei mercati finanziari hanno una tendenza a non perdere il proprio valore, facendo fluire in questo mercato liquidi sia dal mondo finanziario tradizionale che dagli asset digitali.
Durante questo periodo si è posta quindi una maggiore attenzione sulle stablecoin e sono state oggetto di studio per un possibile sviluppo di un "dollaro digitale", infatti questi nuove valute digitali hanno ottenuto la liquidità che in tempi normali sarebbe stata destinata a dei conti correnti bancari in dollari, a dimostrazione di come abbiano soddisfatto le necessità degli operatori del settore: riserva di valore, stabilità e privacy.

Il ruolo di Diem

Nel 2019 Mark Carney, l'allora governatore della *Bank of England*, al simposio di *Jackson Hole*, organizzato dalla FED, aveva previsto Libra come una possibile futura moneta globale, individuando in essa le caratteristiche per mettere in discussione il ruolo del dollaro[21]. Da

[21] Joumanna Bercetche. 2019. *Bank of England keeps an "open mind" on Facebook's cryptocurrency Libra*, CNBC, https://www.cnbc.com/2019/06/21/bank-of-england-mark-carney-on-facebooks-libra-uk-digital-economy.html (date last accessed February 28, 2022)

allora il progetto "Libra" ha subito una trasformazione e un forte rebranding cambiando anche nome in Diem, in questo modo i creatori della valuta digitale hanno cercato di favorire l'approvazione delle autorità di regolamentazione che avevano evidenziato varie problematiche nel progetto iniziale.

Libra, conosciuta oggi come Diem, era stata ideata da una associazione di aziende, tra le quali spicca Facebook come principale sostenitore del progetto, che in un primo momento avevano pensato di creare una stablecoin garantita dalla parità con un paniere di asset con una bassa volatilità, con l'obiettivo di fornire l'accesso ad un sistema bancario anche a 1,7 miliardi di persone adulte che non hanno avevano mai avuto accesso a servizi bancari, il tutto grazie anche all'ecosistema di Facebook. Era stata pensata come una stablecoin basata su diverse monete nazionali (dollaro, euro ecc.) e governata da una associazione indipendente; con queste caratteristiche, gli sviluppatori, ambivano a creare una valuta digitale che riducesse drasticamente i costi delle transazioni e servizi, favorisse l'inclusione finanziaria e creasse dei sistemi di pagamento che si integrassero senza problemi con le politiche monetarie.

Il progetto iniziale, come descritto nel white paper rilasciato dalla associazione, ha dovuto subire varie modifiche per affrontare i problemi normativi che ne ostacolavano lo sviluppo, in particolare ci sono state quattro cambiamenti chiave:

1. Offrire una stablecoin basata sulla valuta singola oltre a quella multivaluta.
2. Migliorare la sicurezza dei sistemi di pagamento tramite un framework di conformità.
3. Rinunciare alla transizione futura ad un sistema permissionless per mantenere le proprietà economiche fondamentali.
4. Aumentare il livello di protezione nella progettazione del "Libra reserve".

Successivamente il progetto ha subito ulteriori modifiche, causate dalla forte volontà di ottenere la completa approvazione delle banche centrali e delle altre autorità che avevano ancora delle incertezze sullo sviluppo della valuta digitale, specialmente per quanto riguardava l'indebolimento del controllo della politica monetaria, i rischi legati alla privacy, e il pericolo del riciclaggio di denaro. L'ottenimento dell'approvazione delle autorità che regolano il sistema monetario è un passo fondamentale per cercare di creare una valuta digitale che possa diventare una moneta internazionale e per raggiungere la massima inclusività dei servizi finanziari, per questi motivi ogni scelta nella sua creazione è stata presa per accontentare tutte le pretese delle autorità.

Nella versione definitiva di Diem, si è deciso di creare una stablecoin basata non più su un paniere di valute ma solamente sul dollaro in rapporto 1 a 1, inoltre anche l'idea di un digital wallet di Facebook che doveva creare un sistema di pagamenti basato sulle applicazioni esistenti come "Facebook Messenger" e "WhatsApp" è stata abbandonata, l'associazione ha deciso di affidarsi a Novi Financial come partner per lo sviluppo del sistema di pagamento.
Durante l'evoluzione del progetto Diem, i suoi partecipanti hanno dovuto affrontare svariate difficoltà per riuscire ad ottenere l'approvazione delle autorità, riducendo le loro ambizioni e arrivando ad applicare delle limitazioni che sicuramente hanno snaturato l'idea iniziale del progetto. Inoltre, durante lo sviluppo molti grandi partner come PayPal, Mastercard, Visa ecc. hanno abbandonato il progetto, a dimostrazione di come anche un progetto su cui le previsioni erano positive non sembra potersi affermare come una nuova moneta internazionale. L'esempio di Diem dimostra come, ad oggi, le criptovalute non sembrano avere le caratteristiche necessarie per diventare la moneta internazionale come molti avevano previsto.

5 CRIPTOVALUTE E LA POLITICA MONETARIA

Le banche centrali, come la Banca Centrale Europea e la Federal Reserve, sono le istituzioni che si occupano di gestire la politica monetaria, quindi, prendono le decisioni per regolare l'offerta di moneta e il costo della moneta stessa. L'obiettivo delle politiche monetarie è mantenere la stabilità dei prezzi e cercare di sostenere le politiche economiche che mirano all'occupazione e alla crescita economica, per raggiungere questi obiettivi i policy maker utilizzano:

- Il tasso di interesse di riferimento, che consiste nel tasso che la banca centrale applica alle banche commerciali, questo influisce sul tasso di interesse legato alle attività di queste ultime e quindi influisce, seppur indirettamente, anche sui consumatori e investimenti delle imprese.
- L'offerta di moneta che viene influenzata attraverso l'acquisto e la vendita di titoli di stato, per esempio la banca centrale acquistando titoli di stato aumenta la quantità di moneta.

In questo sistema, ormai consolidato, si sono inserite le criptovalute che, data la loro natura decentralizzata, sembrano teoricamente destinate a cambiare il modo di operare della politica monetaria.

La BCE nel "Bollettino economico numero 5" del 2019[22] dichiarava che l'intero sistema finanziario avrebbe potuto sopportare i rischi collegati alle criptovalute, che avrebbero potuto avere un impatto sulla stabilità finanziaria e avere degli effetti sulla politica monetaria. Al tempo l'analisi evidenziava che i rischi erano contenuti e sotto controllo, ma che sarebbe stato

[22] 2022. *Bancaditalia.It*. https://www.bancaditalia.it/pubblicazioni/bollettino-eco-bce/2019/bol-eco-5-2019/bolleco-bce-5-2019.pdf.

necessario un monitoraggio continuo per poter intervenire con delle misure specifiche nel caso di possibili minacce all'equilibrio del sistema.

Nel documento vengono sottolineati le principali caratteristiche che potrebbero causare delle criticità all'interno del sistema economico, come ad esempio la mancanza delle criptovalute di un valore intrinseco che rende la loro valutazione difficile da realizzare. Successivamente si sottolinea, come già discusso precedentemente, come le criptovalute non soddisfino le proprietà necessarie per essere impiegate come moneta elettronica e strumenti finanziari e, in particolare, l'assenza di regolamentazione le espone a elevati rischi operativi. Inoltre, si evidenza come la natura decentralizzata e l'assenza di una autorità rende complicato il monitoraggio e l'identificazione di attività illegali e di far fronte problemi in materia di sicurezza informatica.

Nel documento si rimarcava che, in quel momento, non sembravano esserci le condizioni per organizzare attivamente delle misure per salvaguardare il sistema economico finanziario, in quanto la diffusione delle criptovalute era ancora sotto controllo e l'esposizioni delle banche nei confronti delle valute digitali erano limitate, ma comunque si delineavano degli scenari per comprendere le potenzialità del fenomeno. Nel bollettino si descrive uno scenario estremo in cui le operazioni di pagamento al dettaglio sono effettuate con le criptovalute, in queste condizioni le conseguenze sulla politica monetaria e sulla attività economica sarebbero significative: si causerebbe una completa inefficacia della fornitura di moneta e l'influenza della banca centrale sui tassi di interesse sarebbe nulla.

La quantità di monete in circolazione sarebbe indipendente dalla fornitura delle banche centrali, ma dipenderebbe unicamente dalla attività dei miners e dalle capacità del sistema. Un esempio di questa situazione, con le dovute proporzioni, è osservabile nel fenomeno della dollarizzazione delle economie in via di sviluppo, in questi sistemi, in cui se gran parte del sistema finanziario nazionale opera con una valuta estera, la politica monetaria per la valuta locale non ha più connessioni con l'economia reale.

Nell'articolo di Dong He "Monetary Policy in the Digital Age"[23], per quanto riguarda alla questione sul tasso di interesse, si fa riferimento alle teorie di B.Friedman secondo cui, in una circostanza del genere, la banca centrale potrebbe definire dei tassi di interesse che diventerebbero meno connessi o al limite disconnessi al tasso di interesse e al prezzo degli altri asset che interessano le transazioni dell'economia.

Dato l'attuale monopolio delle valute controllate delle banche centrali, per avere la possibilità di una completa sostituzione di criptovaluta ai danni di queste ultime servirebbe uno choc al sistema economico, come potrebbe essere un'esplosione dell'inflazione, ma anche in questo caso sembrerebbe più probabile la tendenza degli operatori economici di ricorrere ad altre valute rifugio meglio consolidate. In conclusione, gli scenari sopra descritti sono, ad oggi, da considerarsi come puramente teorici.

5.1 Le banche e il monitoraggio delle stablecoin

Nonostante la fiducia nella resistenza dei sistemi economici da parte delle autorità, la crescita delle valute digitali ha comunque reso necessario, per gli stati, l'inizio di una fase di monitoraggio e programmazione di misure di sicurezza, per evitare di perdere il controllo sulla stabilità economica. Attualmente l'attenzione delle banche centrali è rivolta verso le stablecoin, viste le loro caratteristiche peculiari rappresentano una minaccia più significativa rispetto alle criptovalute "tradizionali" come bitcoin; infatti, le loro particolarità le rendono un sostituto più adatto delle monete legali. Il rischio legato a queste valute digitali ha indotto "European Central Bank" a pubblicare il report "Stablecoins: implications for monetary policy financial stability, market infrastructure and payments and banking supervision in the euro area"[24], in cui l'istituzione analizza il fenomeno delle stablecoin e le sue possibili conseguenze

---

[23] He, D. 2018. *Monetary Policy in the Digital Age*, ResearchGate, https://www.researchgate.net/publication/334960925_Monetary_Policy_in_the_Digital_Age (date last accessed February 28, 2022)

[24] Echelpoel, F. van E., Chimienti, M. T., Adachi, M. M., Athanassiou, P., Balteanu, I., Barkias, T., Ganoulis, I., Kedan, D., Neuhaus, H., et al. 2020. Stablecoins: Implications for Monetary Policy, Financial Stability, Market Infrastructure and Payments, and Banking Supervision in the Euro Area, *SSRN Electronic Journal*, Advance Access published 2020: doi:10.2139/ssrn.3697295

sul sistema economico. Nell'articolo si evidenzia come il volume di scambio, *trading volume*, è aumentato dalla primavera del 2019, come conseguenza della pubblicazione del "Libra White Paper"[25] , successivamente è diminuito notevolmente a metà del 2020 ritornando a livelli preannuncio di Libra, per infine avere un ulteriore picco nel 2020 legato alla espansione del COVID-19[26] che ha causato crisi e oscillazione nei mercati finanziari. L'andamento del *trading volume* è osservabile nella Figura 5.1.

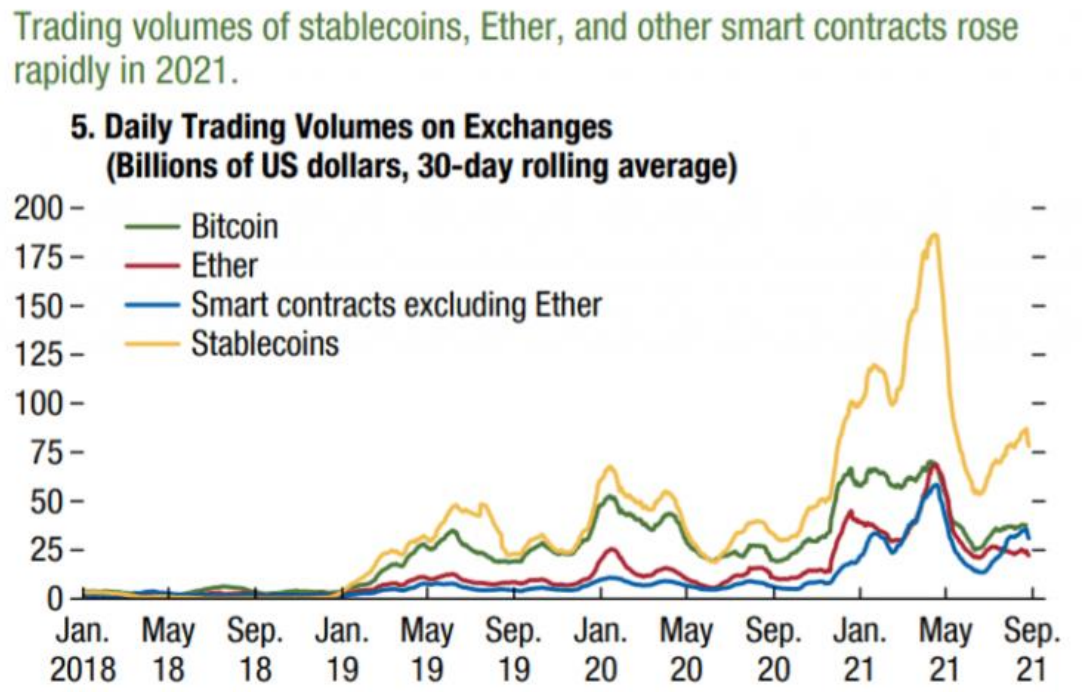


Figura 5.1. *Rappresentazione del trading volume in miliardi di dollari US di criptovalute tradizionali e stablecoin. Fonte "Bloomberg Finance L.P.; Bybt; CoinGecko; CryptoCompare; DeBank; and IMF staff calculations https://www.pymnts.com/cryptocurrency/2021/stablecoins-next-gen-payments-marching-toward-defi-adoption-europe/. Chapter 2 The Crypto Ecosystem and Financial Stability Challenges". In* Global Financial Stability Report, October 2021, *(USA: International Monetary Fund, 2021) accessed Feb 22, 2022, https://doi.org/10.5089/9781513595603.082.ch002*

[25] Documento ufficiale in cui vengono presentate le principali motivazioni che hanno portato allo sviluppo della criptovaluta, la *vision* dell'idea, le principali caratteristiche e le previsioni per il futuro.

[26] È un una patologia infettiva causata dal virus SARS-CoV-2. Individuata per la prima volta nell'autunno del 2019 in Cina, in poco tempo è diventata un'epidemia diffusa a livello globale.

Analizzando la portata del fenomeno e la sua importanza, gli autori del report delineano tre scenari possibili per il futuro delle Stablecoin:

1. Scenario in cui le Stablecoin sono percepite come non mature poiché non dimostrano sicurezza e facilità di uso tali per competere con i metodi di pagamento tradizionali. Sono utilizzate unicamente nello specifico mercato delle criptovalute o per bisogni specifici degli utenti.
2. Scenario in cui le Stablecoin riescono a moderare i principali rischi percepiti e appaiono convenienti, facili da usare e possono essere utilizzati come mezzo di pagamento per operazioni di norma non facilmente eseguibili con i metodi tradizionali, come ad esempio i pagamenti transfrontalieri.
3. In questo scenario le Stablecoin soddisfano la domanda di una valuta di riserva economica attraverso tassi di interesse accattivanti, inoltre sono garantite dalle istituzioni che godono di una certa reputazione quindi gli utenti sarebbero più propensi a sostituire il denaro contante e i loro depositi in valuta legale con le stablecoin.

Analizzando e confrontando i vari scenari e rapportandoli alla situazione attuale si evince che il primo scenario è la semplice continuazione dello stato attuale proiettato nel futuro. Il secondo scenario è stato teorizzato basandosi sul possibile sfruttamento, da parte delle stablecoin, delle debolezze o lacune mostrate da alcuni metodi di pagamento tradizionali come, ad esempio, la scarsa diffusione e adesione ai pagamenti istantanei. In questa situazione è stato ipotizzato che per svilupparsi potrebbero approfittare dei vantaggi derivati dalla loro natura, in modo da competere con i sistemi di pagamento attuali. Questo scenario appare probabile seppur di non facile realizzazione.

Il terzo scenario, dove si teorizza una sostituzione in larga scala della moneta legale con le stablecoin, sembra significativamente più improbabile rispetto al secondo, tenendo in considerazione lo stato attuale della realtà in cui persiste una elevata fiducia nei *regulator* e nei sistemi finanziari regolati.

Il report teorizza le implicazioni del secondo e terzo scenario sulla politica monetaria analizzando nello specifico la situazione dell'Euro Area, che è caratterizzata da un sistema

finanziario prevalentemente "*Bank based*"[27] e perciò un cambiamento nella composizione delle riserve bancarie e nella stabilità dei bilanci di quest'ultime può significativamente influenzare l'efficacia della politica monetaria.

Nel secondo scenario l'utilizzo delle stablecoin come metodo di pagamento, secondo l'articolo, ridurrebbe le entrate delle banche ottenute dalle fee e dalle commissioni intaccando la loro redditività, sebbene ciò non cambierebbe in modo significativo la loro condizione finanziaria. Invece, nel caso previsto dal terzo scenario gli effetti sarebbero significativamente più impattanti dal momento che le banche dovrebbero passare a delle risorse più costose per finanziare i loro depositi, di conseguenza crescerebbero i costi per accedere al credito delle famiglie e delle piccole imprese.

Successivamente si analizza l'influenza delle stablecoin sulla domanda di liquidità della banca centrale, ossia la politica della Banca Centrale Europea sui tassi del mercato monetario: un livello di sostituzione delle banconote ipotizzato nel secondo scenario potrebbe ridurre la domanda di liquidità della BCE, ma non ne limiterebbe necessariamente la capacità di influenzare i tassi del mercato monetario a breve termine, considerando che le riserve di stablecoin verosimilmente verrebbero investite in asset denominati in euro, e quindi reagirebbero alle variazioni dei tassi di riferimento. Nel caso del terzo scenario si prevederebbe una influenza più rilevante sulla domanda di liquidità della banca centrale e, quindi, avrebbe un effetto maggiore sull'orientamento della Banca Centrale Europea sui tassi di riferimento.

Un ultimo aspetto analizzato nel paper è relativo alla possibilità di realizzazione del terzo scenario e il conseguente aumento di domanda di attività sicure. Nel caso in cui i detentori di depositi passassero dai depositi bancari alle stablecoin, la domanda di asset sicuri potrebbe aumentare se queste avessero come collaterali gran parte di queste attività. Si sottolinea che, in quel caso, sarebbe preoccupante per la BCE il caso in cui anche in altri paesi dei depositi non in euro venissero su larga scala da stablecoin denominate in euro considerando che queste dovrebbero avere come collaterali degli asset altamente sicuri in euro.

---

[27] Nel sistema bank-based le banche hanno un ruolo centrale come fonte di finanziamento delle imprese, la maggior parte delle imprese utilizzano i prestiti per finanziare i loro investimenti. In questo sistema le banche provano a creare dei rapporti stretti con le imprese, sempre mediante prestiti a lungo termine e tassi di interesse vantaggiosi per clienti con alta reputazione.

L'aumento della domanda di attività sicure potrebbe influenzare il tasso di cambio, la curva dei rendimenti privi di rischio[28], i prezzi generali delle attività e la valutazione dei collaterali, con potenziali conseguenze nella trasmissione della politica monetaria ai prezzi. In aggiunta, ci potrebbero essere conseguenze sulle potenzialità della politica monetaria che potrebbero essere diminuite a causa di una riduzione dei numeri di titoli disponibili per operazioni di politica monetaria. Infine, nell'articolo si evidenzia come, considerando solo gli scenari più plausibili, l'impatto stimato sui tassi risk free di una domanda addizionale di asset sicuri in euro sarebbe ridotto.

[28] Risk free yield curve.

6 CRIPTOVALUTE: PROBLEMI DI CYBERSECURITY

Le caratteristiche principali delle criptovalute, come l'essere decentralizzate e l'assenza di autorità centrali e policy, le rendono particolarmente interessanti per l'attività criminali come il furto, le frodi, il riciclaggio di denaro ecc. Inoltre, lo sviluppo e la loro diffusione hanno incentivato i cybercriminali a sviluppare degli attacchi informatici che le sfruttassero per approfittarsi delle loro vittime. In questo capitolo sono presentate le principali attività illegali e i problemi di cybersecurity collegate alle criptovalute.

6.1 E-commerce illegale

Le potenzialità delle criptovalute furono chiare fin dall'inizio ai cybercriminali più lungimiranti; infatti, nel 2011 venne creato "Silk Road" un sito di e-commerce dove avveniva la compravendita di beni illegali e dove le transazioni venivano condotte utilizzando la valuta Bitcoin. Il caso di "Silk road" non è un evento isolato, ma è diventato un simbolo di questo mercato nero operante sul web a cui potenzialmente chiunque, ormai, potrebbe accedervi. Esistono parecchi esempi di queste tipologie di siti, tipicamente situate su una *darknet*[29], e tutti ovviamente ambiscono a poter svolgere le proprietà attività illegali cercando di evitare ogni possibile monitoraggio da parte delle autorità. Principalmente sono due gli strumenti fondamentali usati per raggiungere tale scopo: in primo luogo, per accedere a questi siti è necessario utilizzare dei software, ad esempio TOR[30], che permettono una comunicazione anonima attraverso internet, in questo modo si rendono più difficoltose le attività di monitoraggio del traffico web da parte delle autorità. In secondo luogo, si è reso necessario trovare un metodo di pagamento che garantisse, per quanto possibile, anch'esso di evitare

[29] Rete telematica privata alla quale ci si può connetter solo attraverso programmi o applicazioni specifiche.

[30] È un software nato per proteggere la privacy degli utenti rendendo anonime le loro comunicazioni, i dati degli utenti non passano direttamente dal client al server ma attraversano i server di Tor che agiscono come una rete di router creando un circuito virtuale crittografato a strati.

scoperti e tracciati dalle forze dell'ordine; in questo contesto la natura anonima e decentralizzata delle criptovalute le rende particolarmente adatte per portare a termine le transazioni.

In particolare, nel caso di Silk Road, il gestore del sito decise di utilizzare Bitcoin come valuta per effettuare le transazioni sulla piattaforma, il sistema di pagamento del sito permetteva agli utenti registrati di creare e gestire i loro "wallet", questi ultimi erano direttamente conservati sui server di Silk Road. Quando un utente decideva di effettuare un acquisto, la somma di bitcoin corrispondente al prezzo veniva trasferita su un conto di garanzia gestito da Silk Road in modo che esso si potesse assicurare che la transazione avvenisse in modo corretto prima di effettuare effettivamente lo scambio di denaro. Quando la transazione veniva conclusa i Bitcoin veniva traferiti dal conto di garanzia al portafoglio del venditore. Come ulteriore garanzia per mantenere l'anonimato durante i pagamenti venivano usati dei "Tumbler", ovvero dei servizi che innescano una serie di false transazioni create in modo randomico e collegate in modo complesso alla transazione reale del sito, in modo da rendere molto più complicato risalire agli effettivi scambi di criptovaluta avvenuti sul sito.

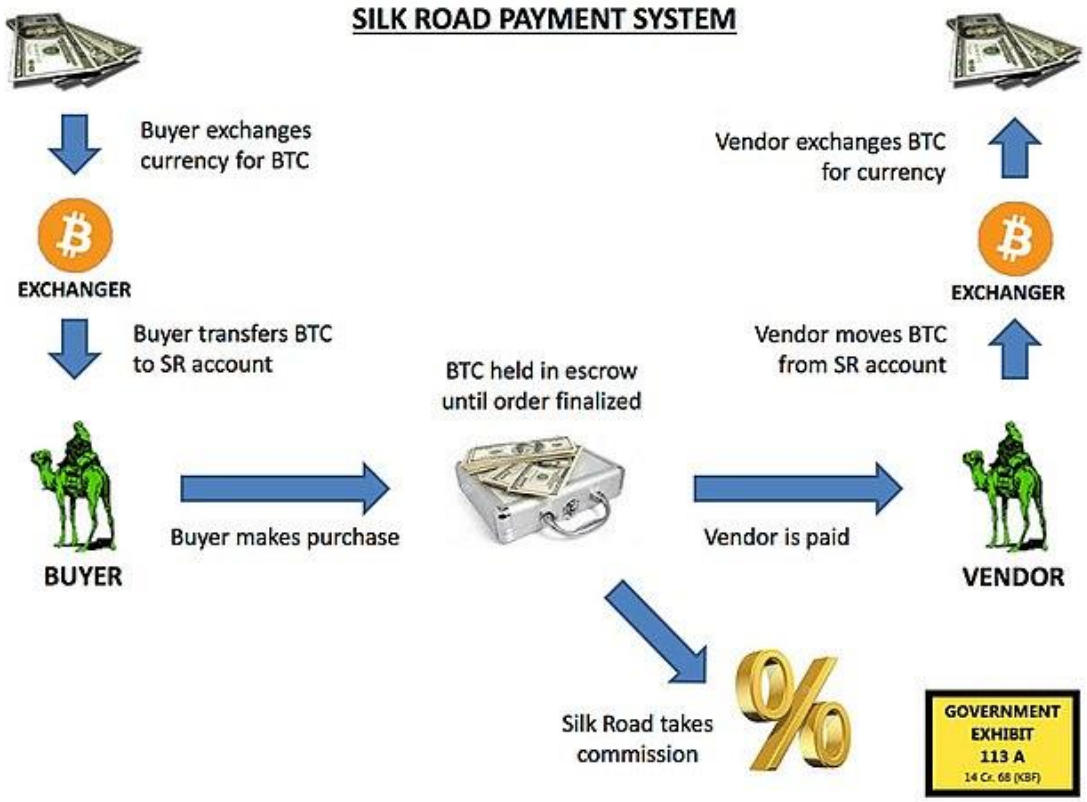


Figura 6.1. *Schema del sistema di pagamento utilizzato sul sito "Silk Road". Fonte https://it.wikipedia.org/wiki/Silk_Road#/media/File:Silk_road_payment.jpg*

Il sito fu chiuso dal FBI il 13 ottobre del 2013, dalle analisi dell'autorità si stima che il sito, nei due anni e mezzo di attività, abbia fatturato più di 9.5 milioni di bitcoin e accumulato circa 600 mila bitcoin di commissioni. Il dipartimento di Giustizia sequestrò circa 173 mila bitcoin, per un valore di 33,6 milioni di dollari[31].

I dati mostrano chiaramente l'importanza del fenomeno e hanno portato le autorità a intensificare le indagini in questo genere di attività e hanno allertato le istituzioni che continuano ad avvisare gli investitori circa la loro pericolosità. Anche Christine Lagarde, presidente della Banca Centrale Europea, si è esposta in merito a questo utilizzo delle

[31] Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website. 2013. FBI, https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website (date last accessed March 17, 2022)

criptovalute, ha sottolineato come abbiano incentivato l'attività di alcuni "*funny business*" e altre attività di riciclaggio di denaro[32].

6.2 Riciclaggio di denaro

Le criptovalute hanno incentivato e aperto ulteriori orizzonti anche al fenomeno del *CyberLaundering*, ossia la nuova frontiera del riciclaggio di denaro che si basa sull'utilizzo di tecnologie informatiche e telematiche. Con la diffusione delle valute digitali è stato possibile sviluppare una nuova modalità di riciclaggio di denaro, che la letteratura definisce "riciclaggio totalmente digitale", a differenza del "riciclaggio digitale strumentale"[33] il denaro "sporco" è già in forma digitale e quindi tutte le fasi del riciclaggio sono effettuate online, in modo che il riciclatore possa non avere alcun contatto con il contante. Come sottolineato nell'articolo "Cyberlaundering e valute digitali. La lotta al riciclaggio nell'era della distributed Economy"[34] l'utilizzo delle criptovalute crea una sinergia con gli aspetti vantaggiosi generali delle pratiche di riciclaggio online rendendo più agevole e sicuro il movimento di capitali, infatti la riduzione dei tempi di transazione e la possibilità degli scambi "peer to peer", dati dall'utilizzo di un sistema decentralizzato, facilitano significativamente il trasferimento del denaro e la possibilità di non dover obbligatoriamente passare da una autorità terza, gravata da obblighi di antiriciclaggio, lo rendono sicuramente più sicuro.

---

[32] Staff, R. 2021. *ECB's Lagarde calls for regulating Bitcoin's "funny business,"* U.S., https://www.reuters.com/article/us-crypto-currency-ecb-idUSKBN29I1B1 (date last accessed March 1, 2022)

[33] Il "riciclatore di denaro" procede all'acquisto delle criptovalute utilizzando del denaro ottenuto in modo illecito. In questo caso le valute digitali sono usate come mezzo per semplificare la fase di placement.

[34] M. Croce | Cyberlaundering e valute virtuali. 2021. www.sistemapenale.it, https://www.sistemapenale.it/it/articolo/cyberlaundering-valute-virtuali-la-lotta-al-riciclaggio-nellera-della-distributed-economy (date last accessed March 1, 2022)

I vantaggi nell'utilizzo delle criptovalute hanno effetto in tutte le fasi del riciclaggio di denaro ma in particolare nella fase di "layering", in questa fase le valute virtuali vengono traferite ad altri indirizzi appartenenti al criminale in modo da rendere scollegate la somma di denaro e le attività illecite. Per ovviare alla possibilità di rintracciare le operazioni sulla blockchain, durante queste operazioni si utilizzano dei servizi di "mixing", quest'ultimi frammentano la somma di denaro "sporco" e la indirizzano verso altri conti "bounce" tramite i quali vengono create molteplici operazioni fittizie intermedie, infine il denaro viene indirizzato verso un deposito di uscita. In questo modo si rende molto più complicato un eventuale tracciamento delle operazioni da parte delle autorità. Successivamente, grazie alle caratteristiche delle criptovalute, è possibile concludere la procedura di riciclaggio semplicemente scambiando il denaro su una piattaforma exchange.

6.3 Finanziamento al terrorismo

Le criptovalute, dopo la loro diffusione, sono diventate uno degli strumenti più utilizzati per il finanziamento del terrorismo, in particolar modo quello islamico. Le cellule collegate al terrorismo internazionale si sono mobilitate nel capire e utilizzare alcune criptovalute per sfruttarne le caratteristiche principali, ovvero l'anonimato e la difficile tracciabilità, con queste sono stati in grado di potenziare e semplificare il finanziamento delle loro attività tramite raccolte fondi sul "Dark web" o l'organizzazione di campagne di crowdfunding sui vari social media. Il fenomeno è tutt'ora in crescita dal momento che su varie piattaforme spiccano numerosi gruppi in cui si effettuano richieste di finanziamento a tali attività, tra i tentativi più recenti si può citare il caso "al-Sadaqah", parte di un gruppo situato in Siria che ha organizzato una campagna di raccolta fondi tramite social media, in cui era richiesto che il denaro venisse inviato tramite bitcoin.

Le potenzialità delle criptovalute hanno aumentato la diffusione del fenomeno, la non tracciabilità ha facilitato ai terroristi la fase di richiesta del finanziamento, dando la possibilità di renderlo esplicito senza dover creare dei sistemi per celarlo. Inoltre, le persone, oltre a sentirsi più sicure grazie all'anonimato offerto dalle criptovalute, sono più propense a inviare il denaro vista la possibilità di evitare di pagare le commissioni agli "infedeli" vista la natura decentralizzata delle valute digitali. Con il passare del tempo e l'esplosione del fenomeno, le

criptovalute non sono più l'oggetto misterioso a cui si possono avvicinare solo gli esperti, ma sono diventate sempre più diffuse e *userfriendly*, perciò possono essere gestite da chiunque, rendendo insospettabili i soggetti radicalizzati e aumentando la velocità della loro diffusione per fini terroristici. Un caso emblematico, riportato nell'articolo "Finanziamento al terrorismo internazionale e paradisi fiscali" di Luca Sammuri, fu quello di Zoobia, tecnica di laboratorio priva di competenze informatiche, che donò 62 mila dollari in bitcoin a delle società fantasma usate dall'Isis per finanziare le loro attività.

Il primo utilizzo, su grossa scala, delle criptovalute per finanziare attività terroristiche avvenne nell'ottobre 2017 quando "al-Qaeda"[35], sul web magazine "AlHaqiqa", invitò a donare bitcoin per supportare le loro attività, questo episodio è stato particolarmente significativo poiché contribuì alla completa affermazione dell'utilizzo delle valute digitali come strumento di finanziamento al terrorismo. Queste associazioni criminali hanno continuato a seguire l'evoluzione delle criptovalute sfruttando quelle che si adattano maggiormente alle loro esigenze. A dimostrazione di ciò, di recente, hanno scelto di utilizzare delle valute digitali alternative che offrissero un maggiore livello di anonimato come "Monero"[36], diventata ormai nota per il suo utilizzo collegato ad attività illegali. In conclusione, a livello europeo si sta cercando di regolamentare gli snodi dove fluiscono le criptovalute come gli exchange e i wallet provider, quest'ultimi dovranno assumere un ruolo più centrale nella lotta al terrorismo, dovranno potenziare le attività di monitoraggio per cercare di individuare le transazioni di natura sospetta e segnalarle alle autorità competenti.

6.4 Vulnerabilità e furti

Esiste un'altra tipologia di criticità collegata alle criptovalute, nello specifico alla sicurezza informatica delle piattaforme di exchange e dei servizi di wallet, che causa un effetto diretto ai loro possessori.

---

[35] Organizzazione terroristica fondata sul finire degli anni '80 del ventesimo secolo, responsabile di molteplici attacchi terroristici contro obiettivi civili come l'11 settembre a New York.

[36] Criptovaluta creata nel 2014 che si contraddistingue per l'attenzione data alla tutela della privacy ottenuta grazie all'applicazione di un meccanismo di per rendere anonime collegato all'uso del protocollo "Cryptonote".

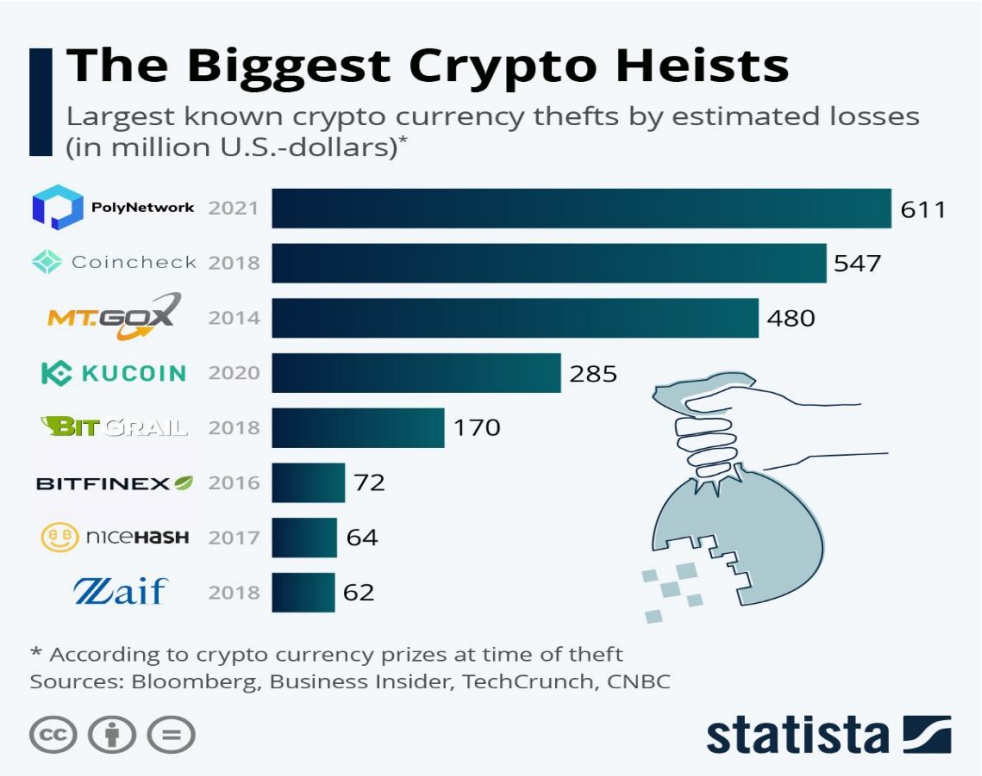


Figura 6.2. *Confronto in milioni di dollari dei principali furti di criptovalute. Fonte" Zandt, F. 2021. Infographic: The Biggest Crypto Heists, Statista Infographics, https://www.statista.com/chart/12707/largest-known-crypto-currency-thefts/ (date last accessed February 22, 2022)*".

Durante la diffusione delle valute digitali, le principali piattaforme exchange hanno dovuto affrontare numerosi problemi di cybersicurezza, spesso questi eventi si sono sviluppati come veri e propri furti di criptovalute dai loro siti con conseguente danno anche agli utenti che usufruivano del loro servizio.

Nel 2014 "Mt.Gox", all'epoca l'exchange più famoso e utilizzato al mondo, subì un attacco hacker nel quale furono rubati tutti i bitcoin presenti sui conti dei clienti, si parla di circa 850 mila bitcoin, che al tempo avevano un valore di circa 473 milioni di dollari ma che ad oggi varrebbero oltre 9 miliardi di dollari. I bitcoin furono sottratti ad oltre 25 mila utenti che, in un primo momento, non furono rimborsati. Successivamente, furono recuperati circa 200 mila bitcoin e da allora ci furono una serie di vicissitudini legali che hanno portato il tribunale di Tokyo ad approvare un piano di suddivisione dei bitcoin recuperati solo nel dicembre 2020.

Un altro evento che ha scosso il mondo delle criptovalute è il furto avvenuto a Coincheck. Essa è una piattaforma che offre un servizio di wallet e di exchange con sede a Tokyo, nata nel 2014, in pochi anni è riuscita a diventare una delle più note piattaforme exchange del Giappone,

attirando l'attenzione di altre società come "Monex Group"[37] che l'ha acquisita per 33 milioni di dollari nel 2018. Pochi mesi prima, precisamente a Gennaio 2018, ha subito un attacco hacker in cui furono rubati circa 500 milioni di Nem[38] , per un valore di circa 530 milioni di dollari. Le indagini hanno rivelato che gli hacker penetrarono le difese della azienda tramite delle mail infette inviate ad alcuni membri dello staff e, successivamente, riuscirono ad entrare in possesso delle loro chiavi private e ad accedere agli hot wallet.

Appena si accorsero di aver subito questo attacco, sospesero le contrattazioni sui bitcoin e impedirono il ritiro dei fondi da parte dei clienti, questo evento ebbe conseguenze particolarmente importanti sulle criptovalute coinvolte. La società, poco dopo l'attacco, dichiarò che avrebbe rimborsato circa il 90% degli oltre 250 mila utenti coinvolti nel furto, utilizzando denaro proveniente dai propri fondi, per una somma pari a 426 milioni di dollari. Poco dopo l'accaduto furono intervistati dei clienti di Coincheck che affermarono di essere rimasti increduli e che non avrebbero mai pensato che una situazione del genere si sarebbe potuta configurare con una legislazione sviluppata come quella giapponese. Pochi mesi più tardi la società iniziò a risarcire i propri clienti in base alle promesse fatte poco dopo il furto.

Attacchi informatici di questo genere sono avvenuti anche in periodi recenti: l'11 agosto 2021, un hacker, sfruttando una debolezza del sistema, ha rubato più di 600 milioni di dollari in criptovalute dalla piattaforma Polynetwork[39] , traferendo i token nei suoi portafogli. A differenza delle altre vicende questa ha avuto un risvolto diverso, in seguito all'evento la società, dopo aver dichiarato l'accaduto, ha fatto un annuncio su Twitter, in cui richiedeva di poter iniziare un dialogo con l'hacker per trattare la restituzione delle monete virtuali. Dopodiché l'hacker ha deciso di iniziare a restituire il bottino e in poco tempo Polynetwork riuscì a rientrare in possesso della maggior parte del denaro, anche se per una rimanente parte, pari a 200 milioni di dollari, entrambe le parti hanno dovuto trovare un compromesso:

---

[37] È una società, con sede a Tokyo, che offre servizi finanziari online.

[38] È una piattaforma blockchain e un criptovaluta *peer-to-peer*. Sviluppata per introdurre nuove caratteristiche nella tecnologia blockchain, come l'algoritmo del consenso *Proof-of-Importance*, è stata rilasciata nel 2015 e nel 2017 è stata tra le prime 10 criptovalute al mondo per capitalizzazione.

[39] Poly Network è un una piattaforma di finanza decentralizzata (DeFi) che permette l'interoperabilità tra diverse blockchain consentendo di scambiare i token tra di esse.

Polynetwork ha promesso una somma pari a 500 mila dollari a "Mr.White Hat", soprannome dell'hacker, per aver individuato una falla nel loro sistema di sicurezza e un posto di lavoro come "chief security advisor".

Infine, l'hacker ha deciso di riconsegnare tutta la somma prelevata illecitamente e, successivamente, Polynetwork ha subito iniziato le procedure per restituire le somme ai suoi utenti.

Dalle indagini effettuate della società SlowMist[40], si è scoperto, infine, che l'hacker ha sfruttato una debolezza nel codice di una funzione per "richiamare i contratti".

Alla luce di questo evento, Ferdinando Ametrano, fondatore di CheckSig, in una intervista rilasciata al "Sole24ore" sottolinea come ormai queste situazioni si verificano in troppi casi a causa, secondo il suo parere, dell'inefficienza del codice dell'infrastrutture. Inoltre, sottolinea che il software di queste piattaforme è spesso "formalmente non verificato", perciò si crea il rischio che siano lasciate delle debolezze aggredibili dai malintenzionati[41].

La particolare dinamica che ha caratterizzato il furto a Polynetwork ha suscitato numerose preoccupazioni e perplessità: in una intervista alla BBC[42] Katie Paxton-Fear, *hacker white hat* e docente presso la "Manchester Metropolitan University", ha dichiarato che il modo in cui questa società si è riferita hacker definendolo *white hat*[43] è deludente, poiché nelle sue azioni non ha seguito nessun principio del *white hat hacking.* Anche Charlie Steele, partner di Forensic

[40] È una società specializzata in servizi di *cybersecurity* specializzata nell'ecosistema blockchain.

[41] Carlini, V. 2021. *Assalto hacker alla piattaforma Poly Network: rubati 600 milioni in cripto asset*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/il-piu-grande-assalto-hacker-finanza-decentralizzata-rubati-600-milioni-cripto-asset-AEFnoOc (date last accessed March 2, 2022)

[42] Tidy, J. 2021. *Crypto hacker offered reward after $600m heist*, BBC News, https://www.bbc.com/news/business-58193396 (date last accessed February 22, 2022)

[43] Il white hat è un hacker che utilizza le sue conoscenze e capacità nell'ambito della programmazione e della sicurezza informatica per introdursi in sistemi informatici e segnalare ai proprietari i problemi nei sistemi di sicurezza. Queste figure si contrappongono a coloro che violano penetrano i sistemi di sicurezza illegalmente, anche senza un profitto personale.

Risk Alliance[44] ed ex funzionario del Dipartimento di Giustizia e dell'FBI, ha espresso delle perplessità in merito all'accaduto, ha sottolineato che le società private non hanno alcuna autorità per promettere l'immunità da procedimenti penali, perciò comportamenti come quelli di Polynetwork creano un importante precedente in quest'ambito e rischiano di creare degli squilibri nel sistema giudiziario.

Dalle dinamiche degli attacchi hacker precedentemente descritti, è possibile notare un certo grado di sistematicità dovuta, generalmente, al non completo sviluppo dei sistemi di sicurezza della finanza decentralizzata. La vulnerabilità di queste piattaforme rende ragionevole prevedere la possibilità di altri attacchi di questa portata in futuro, alimentando i timori e le perplessità degli utenti circa la solidità di questi strumenti.

Per quanto riguarda la sicurezza delle criptovalute in sé sembrerebbe essere più elevata e sufficiente a scongiurare attacchi diretti ai loro sistemi, grazie alla sicurezza integrata nel sistema blockchain, alla natura decentralizzata e al lavoro di supervisione della comunità.

In conclusione, è evidente come, al momento, i sistemi di finanza decentralizzata non possano offrire un livello di sicurezza comparabile a quello dei sistemi tradizionali. L'aspetto più significativo di queste problematiche è il trattamento della tutela degli utenti di questi sistemi, sebbene in molti casi le piattaforme siano riuscite a restituire le somme sottratte, appare evidente che le procedure non siano univoche e sono create in base alla policy dell'azienda creando incertezze su modalità e tempi di rimborso, esplicativo è stato il caso di "Mt.Gox".

Il costo della decentralizzazione, componente chiave delle criptovalute, si riscontra in queste occasioni dove si evidenzia una mancanza di un sistema di tutele a sostegno degli utenti e investitori, tutele che negli ambienti tradizionali regolamentati sono assicurate: ad esempio nel caso di fallimento di una banca esiste un sistema di protezione dei risparmi che impone al sistema nazionale di rimborsare i risparmi fino al limite imposto per legge; nel caso di un *wallet* di criptovalute non esiste una copertura statale, neanche forma di garanzia o assicurazione.

[44] Società leader del mercato globale nel settore della consulenza, specializzata nel *forensic accountig* e data analytics.

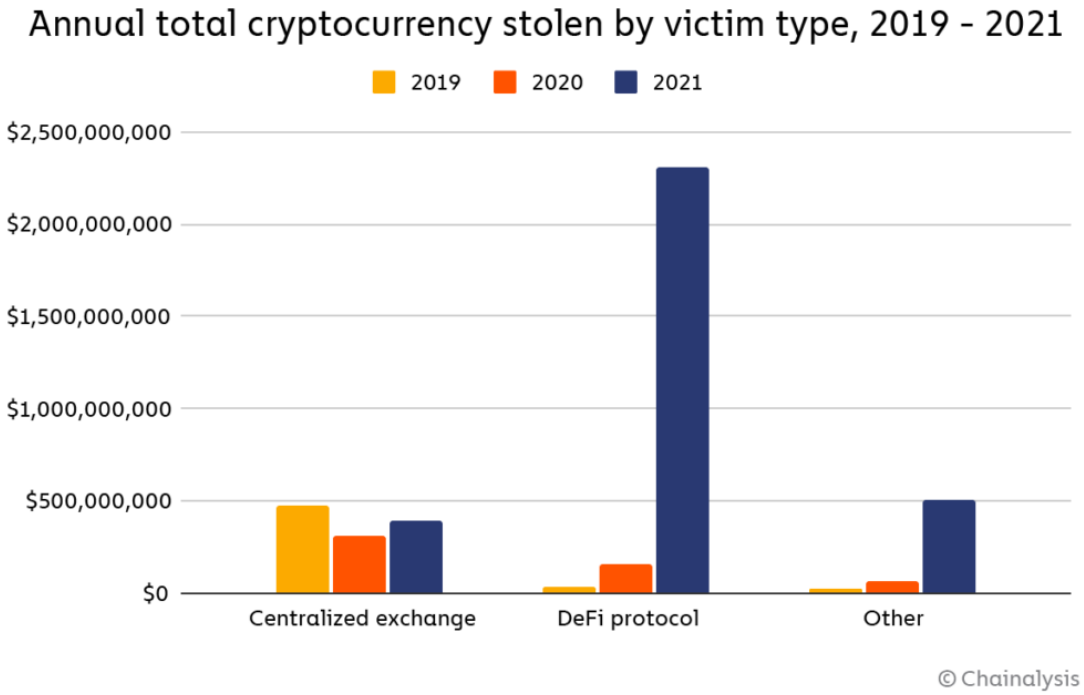


***Figura 6.3**. Il grafico mostra le quantità annuali di criptovaluta rubate divise in base alla tipologia di vittime del furto. Fonte "https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/".*

6.5 Malware e cryptolocking

Le caratteristiche delle criptovalute hanno causato la creazione e la rapida diffusione di una ulteriore forma di frode informatica basata su un attacco Ransomware. Il Ransomware è una tipologia di Malware che opera limitando o impedendo l'accesso al dispositivo che viene infettato, solitamente possono impedire all'utente di utilizzare il sistema chiedendo un riscatto per poterlo sbloccare oppure opera cifrando dei file e, successivamente, viene richiesto un riscatto per riportarli nella forma originaria. Nel 2013 si diffuse il famoso "Cryptolocker", tra i primi ransomware che usava i bitcoin per incassare denaro e mantenere l'anonimato in tutta sicurezza, a causa della sua particolare complessità molti analisti lo descrivevano come molto difficile da eliminare, rendendolo particolarmente temuto. Questo ransomware si è diffuso in modo significativo e, grazie al suo particolare modus operandi, riuscì a estorcere circa tre milioni di dollari prima che le autorità statunitensi riuscissero ad isolarlo.

Figura 6.4. *Schema di funzionamento di un ransomware con l'utilizzo di criptovalute, Internet of things and ransomware: Evolution, mitigation and prevention - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/How-crypto-Ransomware-Work_fig5_341719300 [accessed 9 Dec, 2021]*

Con l'esplosione della pandemia di COVID-19 si è notato un aumento di questo tipo di attacchi tanto è vero che qualcuno parla anche di una pandemia digitale, infatti, secondo i dati di Accenture[45], l'attività di intrusione informatica a livello globale è aumentata del 125% nella prima metà del 2021 rispetto all'anno precedente. È stato dimostrato che i principali responsabili di tale aumento di attività sono i ransomware; l'FBI ha dichiarato la presenza di un aumento del 62% degli attacchi ransomware nel periodo sopracitato e ciò viene confermato anche dai dati riportati dall'azienda "Allianz", società europea di servizi assicurativi, che ha visto aumentare i sinistri del 50% tra il 2019 e 2020, evidenziando un trend in crescita. Oltre alle cause specificatamente legate al periodo storico, la sempre più diffusa adozione e accettazione delle criptovalute, come Bitcoin, ha sicuramente avuto un ruolo fondamentale nell'aumento di questi numeri, ma ha comportato anche un cambiamento di paradigma in questo genere di attacchi informatici.

[45] Multinazionale operante nel settore della consulenza.

Si ipotizza che la facilità con cui le aziende e i singoli cittadini possano operare con le criptovalute ha creato un incentivo a propendere di limitarsi a pagare il riscatto invece di cercare risolvere il problema cercando di riprendere il controllo dei sistemi informatici. Emblematico è stato il caso di "Jbs", impresa brasiliana leader nel settore della lavorazione della carne, che ha scelto di pagare 11 milioni di dollari in bitcoin di riscatto per sbloccare i propri sistemi informatici colpiti da un attacco ransomware. L'opzione di pagare il riscatto può sembrare, sul momento, una scelta ragionevole dal punto di vista economico, ma alimenta un sistema di organizzazioni criminali, favorendo la loro evoluzione, e provoca un aumento delle possibilità di attacchi futuri. Secondo il rapporto "Chainanalysis 2021 Crypto Crime Report"[46], analizzando gli introiti di criptovalute derivanti da attacchi ransomware nel 2020 si nota un aumento del 300%, questo dimostra la tendenza dei cybercriminali ad abbandonare gli attacchi informatici che mirano per lo più ad infliggere danni al sistema e a sabotarlo, per preferire gli attacchi ransomware che mirano ad estorcere denaro alla vittima. I dati del report di Sophos[47] "State of Ransomware"[48] del 2021, rendono evidente come rispetto al 2020, in cui su 5400 aziende interviste il 51% dichiarava di aver subito un attacco ransomware, gli attacchi sono scesi fino al 37% a dimostrazione dell'evoluzione degli attacchi; l'azienda sottolinea un cambiamento fondamentale nel comportamento dei criminali, che, al momento, avrebbero una tendenza a non effettuare più attacchi automatizzati su larga scala, ma a scegliere le loro vittime in modo più mirato, studiando le loro debolezze. Inoltre, Sophos precisa che con questo modus operandi nonostante il numero di attacchi sia diminuito il danno potenziale degli attacchi targettizzati sia molto più alto.

Oltre a ciò, emerge l'aumento della propensione delle vittime di questi attacchi a pagare il riscatto per riottenere i propri dati: rispetto al 2020, dove solo il 26% dei partecipanti al sondaggio dell'azienda aveva pagato, nel 2021 il numero è salito al 32%. Nello studio si è

---

[46] The Chainalysis 2021 Crypto Crime Report. 2021. Chainalysis.com, https://go.chainalysis.com/2021-Crypto-Crime-Report.html (date last accessed March 2, 2022).

[47] Sophos è una società leader mondiale nel settore della cybersecurity next-gen, è principalmente focalizzata sulla fornitura di sicurezza ad organizzazioni e imprese.

[48] Ransomware Report: Sophos State of Ransomware Report 2021. 2021. Sophos.com, https://secure2.sophos.com/en-us/content/state-of-ransomware (date last accessed March 2, 2022).

riuscito a stimare che il costo medio per rimediare ad un attacco Ransomware è quasi duplicato, passando dal 0.76 milioni di dollari a 1.85 milioni di dollari.
Il Dipartimento del tesoro americano ha emesso vari comunicati in cui si sottolinea la criticità del fenomeno degli attacchi ransomware e dichiara di avere avviato una serie di azioni per l'eliminazione delle organizzazioni criminali e degli scambi di valute digitali atte a riciclare i riscatti. L'autorità rimarca il ruolo degli *exchange* di criptovalute definendole un elemento critico, poiché le valute digitali sono un mezzo che facilita i pagamenti dei riscatti dei ransomware e le attività di riciclaggio di denaro associate ad essi, perciò ha già intrapreso delle azioni di controllo e sanzionamento verso alcuni *exchange* di criptovalute, come dimostra il caso di SUEX, con l'accusa di aver supportato scambi di denaro collegate a queste attività.

6.6 Cryptojacking

Un'ultima tipologia di problematica riscontrata nell'ecosistema delle criptovalute è relativa alla cybersicurezza, nello specifico riguarda una tipologia di crimine informatico che è emersa in modo significativo solamente negli ultimi anni e che è intrinsecamente collegata alla struttura delle criptovalute, e in particolare all'attività di Mining. La probabilità di risolvere i problemi criptografici da parte del miner è direttamente proporzionale alla capacità computazionale dell'hardware, al contempo più hardware viene utilizzato per questa attività e più sarà necessario consumare energia per alimentarlo e, di conseguenza, si verifica un aumento dei costi energetici facendo diventare il tradeoff tra il costo dell'energia e il guadagno dato dal mining sempre meno vantaggioso. Attorno al 2017 ci fu un'esplosione delle criptovalute sia per quanto riguarda la capitalizzazione sia la diffusione, rendendo sempre più appetibile intraprendere l'attività di mining, questo contesto incentivò la diffusione dei "Cryptojacking malware".
Il cryptojacking è un software malevolo che mira a utilizzare la potenza computazionale delle vittime per estrarre le criptovalute senza il loro consenso, in questo modo si eliminano i costi operativi dell'energia elettrica ed è possibile creare delle reti di calcolatori in modo da ottenere una notevole potenza di calcolo. Ovviamente le vittime di questi attacchi subiranno un notevole diminuzione delle prestazioni del proprio device e, allo stesso tempo, pagheranno gli extracosti per l'energia elettrica.

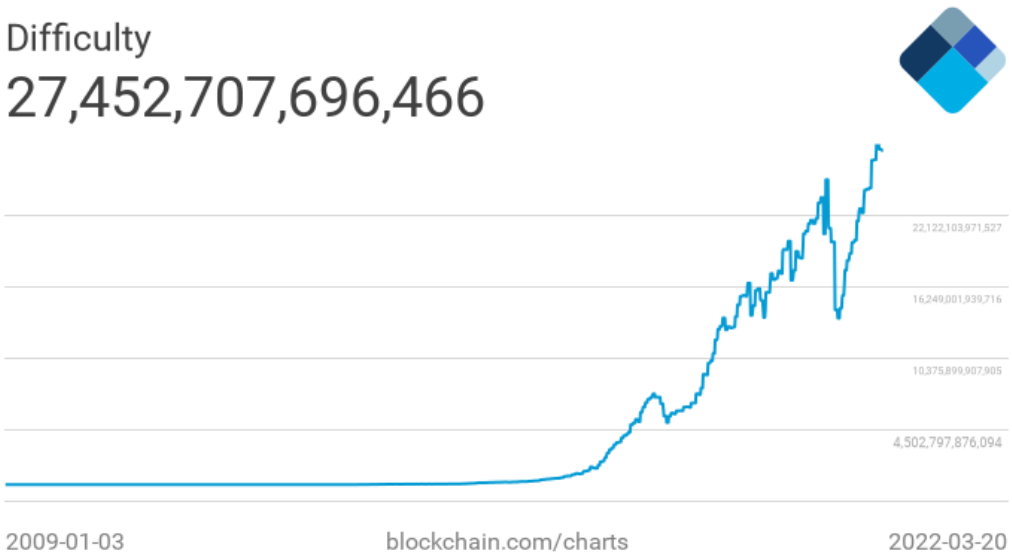


Figura 6.5 *Grafico dell'andamento della Bitcoin difficulty. Fonte" Blockchain.com, https://www.blockchain.com/charts/difficulty" (date last accessed March 21, 2022).*

Le criptovalute, nello specifico si utilizza Bitcoin come valuta di riferimento, sono progettate in modo che la rete produca un nuovo blocco in media ogni 10 minuti, il metodo di ricalibrazione per mantenere questo parametro consiste nella continua regolazione dell'hash target, più basso è quest'ultimo più ripetizioni della funzione hash dovranno essere completate per poter ottenere un risultato valido e, quindi, maggiore è la "difficoltà" della criptovaluta. Come si può notare dal grafico relativo alla "difficulty" di Bitcoin, Figura 6.6, l'aumento della diffusione delle criptovalute e dei minatori ha fatto esplodere il valore di quest'ultima negli ultimi due anni, incentivando l'attività illecite che hanno creato uno strumento per poter risolvere il problema della potenza di calcolo sfruttando la potenza di calcolo delle vittime.

Gli attacchi di cryptojacking possono avvenire in vari modi:

- con i classici metodi utilizzati da altri malware, come un link inviato tramite mail di phishing che al momento del click causa il download del codice di *cryptominig* che viene caricato direttamente sul dispositivo.
- Metodo "drive by criptomining" / "Browser based cryptojacking", questo si basa sull'integrazione di un codice JavaScript in una pagina web e procede alla generazione delle criptovalute sfruttando macchine che visitano la pagina. In questi casi l'intento

delle pagine web rimane celato, in più il codice è creato in modo che per quanto l'utente ritenga che le finestre del browser siano state chiuse almeno una di esse rimane aperta per continuare a sfruttare la potenza di calcolo della vittima[49].

- Gli attacchi *cryptojacking-cloud*, quest'ultimi hanno inizio con l'ottenimento delle chiavi di accesso ai servizi cloud, di solito di grandi organizzazioni. Ottenuto l'accesso gli hacker utilizzano le capacità computazionali del server per minare le criptovalute, questo causa un danno economico considerevole sulle vittime, poiché a loro viene addebitato il costo dell'utilizzo dei servizi cloud necessario per effettuare i calcoli per il mining.

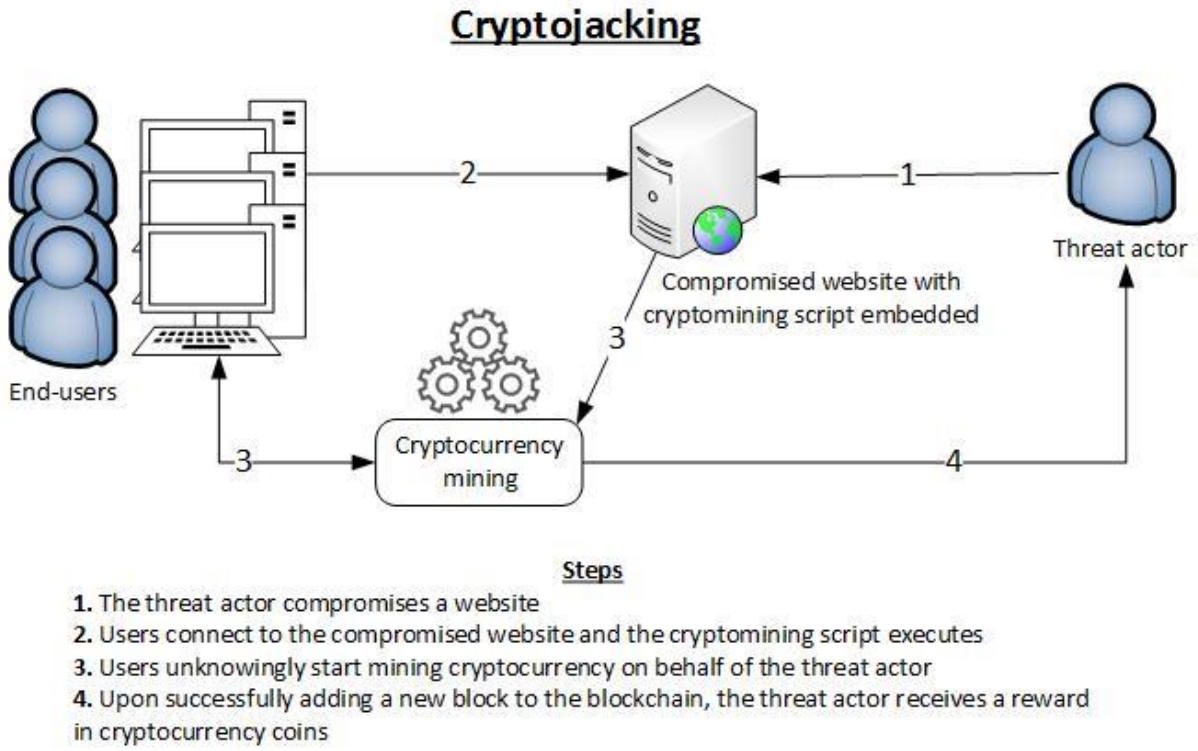


***Figura 6.6**. Schema di funzionamento di un malware Cryptojacking. Fonte" Cryptojacking - Cryptomining in the browser. 2017. ENISA, https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser (date last accessed March 21, 2022)*

[49] Normalmente vengono utilizzati dei pop-under dimensionati in modo da nascondersi sotto la barra delle applicazioni o dell'orologio. Fonte https://it.malwarebytes.com/cryptojacking/.

7 SOSTENIBILITÀ AMBIENTALE DELLE CRIPTOVALUTE

Nel seguente capitolo saranno analizzati alcuni aspetti critici delle criptovalute rispetto alle tematiche della sostenibilità ambientale.

L'aumento di quantità di energia per l'attività di minig di alcune criptovalute, Bitcoin in primis, non desta solo preoccupazione per la possibile esplosione di attività illegali legate ai cybercriminali, ma pone l'attenzione sul problema della sostenibilità ambientale delle criptovalute. Secondo il "Bitcoin Energy Consumption Index" di Digiconomist[50] il consumo di energia annuale stimato di Bitcoin è di 201,70 TWh, una quantità paragonabile al consumo di energia elettrica della Thailandia e una *carbon footprint* simile a quella della Repubblica Ceca. La stima fatta dal "Cambridge Centre for Alternative Finance"[51] è di circa 122 TWh all'anno, paragonabile all'energia elettrica spesa per l'estrazione dell'oro in un anno.

[50] Digiconomist. 2022. *Bitcoin Energy Consumption Index - Digiconomist*, Digiconomist, https://digiconomist.net/bitcoin-energy-consumption/ (date last accessed March 2, 2022).

[51] CCAF Digital Tools - Cambridge Centre for Alternative Finance. 2021. Ccaf.io, https://ccaf.io/ (date last accessed March 2, 2022).

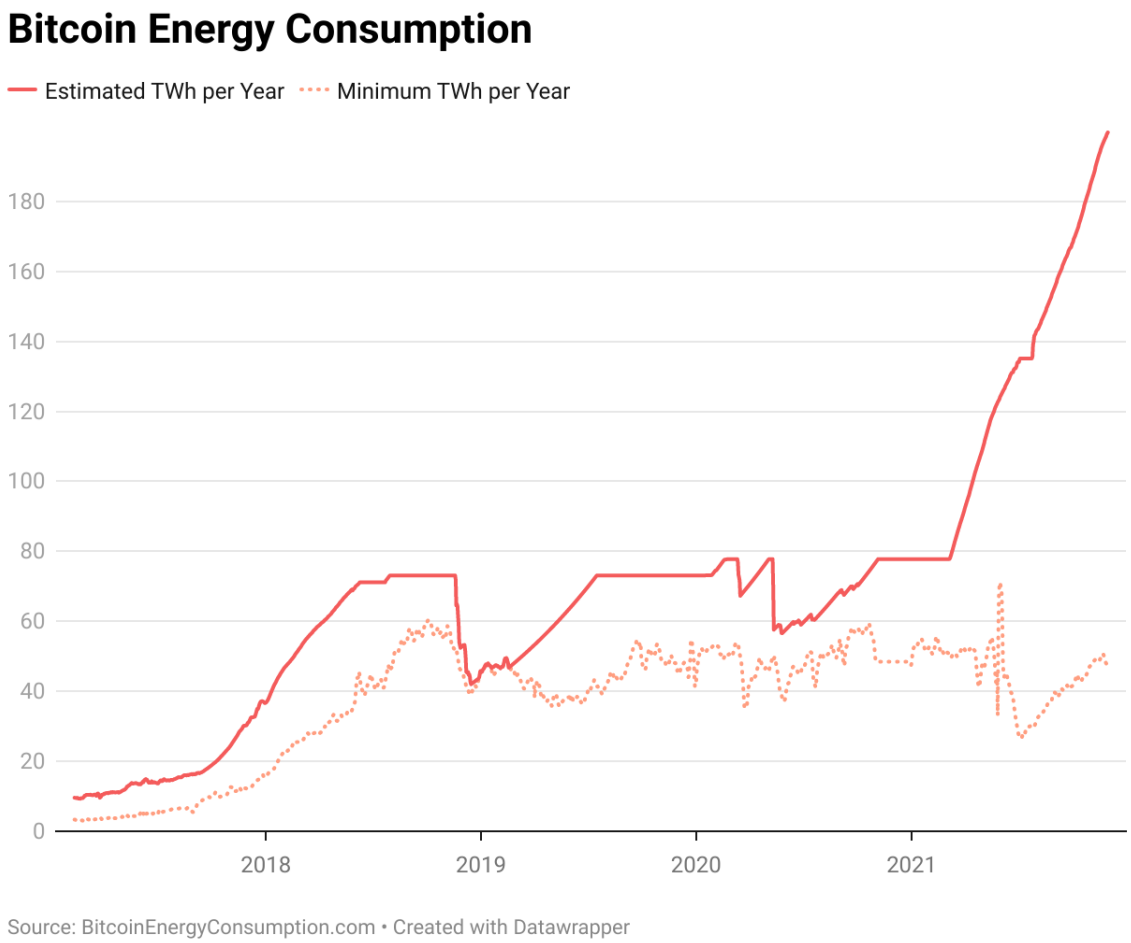


Figura 7.1. *Rappresentazione dell'consumo energetico stimato di Bitcoin. Fonte:*" Digiconomist. 2022. Bitcoin Energy Consumption Index - Digiconomist, Digiconomist, https://digiconomist.net/bitcoin-energy-consumption/ (date last accessed February 22, 2022)"

La quantità di energia necessaria per il sostentamento del sistema delle criptovalute, come già detto, è aumentata a causa dell'aumento della complessità dei puzzle criptografici che i miner devono risolvere per ottenere la loro ricompensa. Se nel 2011 si potevano utilizzare dei semplici computer desktop per estrarre le criptovalute, ad oggi sono necessari dei dispositivi specializzati che necessitano di investimenti elevati, spazi significativi e dei sistemi di raffreddamento particolarmente efficienti per contrastare il surriscaldamento dell'hardware. Queste barriere all'ingresso hanno causato un consolidamento di 7 grandi gruppi che si occupano di mining e che rappresentano circa l'80% della potenza di calcolo della rete, questo accentramento di potere ha indotto questi gruppi ad avviare e creare delle mining farm nei paesi dove è possibile ottenere l'energia elettrica a basso costo.

Secondo alcuni modelli esposti nell'articolo "Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China"[52], il consumo annuale dell'energia dell'intera "Bitcoin industry" cinese avrebbe avuto un picco nel 2024 con un livello pari a 269.59 TWh, consumo che è comparabile a quello dell'Italia e, contestualmente, l'emissione di anidride carbonica dovuta ai bitcoin avrebbe avuto un picco al valore di 130.50 milioni di tonnellate all'anno. Secondo la stima del modello, l'emissione dell'industria del mining di bitcoin si sarebbe posizionata al decimo posto tra i maggiori settori industriali della Cina e avrebbe contribuito al 5% delle emissioni della Cina per la produzione dell'energia elettrica.
Come descritto nell'articolo, ad aprile 2021 circa il 75% delle mining pool avevano sede nel territorio cinese, questa concentrazione era causata da un basso costo dell'energia elettrica e dalla possibile vicinanza con industrie specializzate nella produzione di componenti hardware. Di conseguenza, la Cina ha dovuto intervenire in modo da tenere sotto controllo una possibile minaccia alle sue politiche di riduzione delle emissioni di CO2.
Secondo le previsioni eseguite dagli autori, in base alle loro simulazioni, il trend delle emissioni causate dal sistema della blockchain di bitcoin avrebbero rischiato di diventare una considerevole minaccia per il conseguimento dei risultati previsti dagli "Accordi di Parigi"[53], secondo i quali la Cina sarebbe tenuta diminuire le emissioni di carbonio di una considerevole quantità. Nell'articolo venivano analizzati possibili scenari in base alle politiche attuate dalla Cina per regolamentare questo fenomeno e diminuire le emissioni, ciò che emerge è che la risosta più efficace sarebbe stata la "site regulation" in cui i miner di bitcoin sono incentivati a spostare le loro mining pool in zone della Cina ricche di centrali idroelettriche, in modo da poter sfruttare il basso costo dell'energia in surplus a disposizione in quelle aree. Questa politica, secondo le analisi degli autori, avrebbe potuto abbassare notevolmente il picco di

[52] Jiang, S., Li, Y., Lu, Q., Hong, Y., Guan, D., Xiong, Y., and Wang, S. 2021. Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China, *Nature Communications*, vol. 12, no. 1.

[53] Accordo sottoscritto il 12 dicembre 2015 dagli stati membri della "United Nations Framework Convention on Climate Change- UNFCCC" riguardo alla riduzione di emissioni di gas serra e alla finanza a partire dal 2020.

emissioni di carbonio rispetto a tutte le altre alternative studiate come la "carbon tax" o la regolamentazione all'accesso a questo tipo di settore.

A giugno 2021 la Cina ha deciso di vietare il mining delle criptovalute, Meng Wei, portavoce della commissione nazionale per lo sviluppo e la riforma, ha affermato che l'industria del mining di criptovalute, a causa del suo elevato consumo di energia e la conseguente emissione di carbonio, non avrebbe avuto un effetto positivo sullo sviluppo tecnologico e industriale del paese. Inoltre, ha sottolineato come l'evoluzione spregiudicata di questa industria non è in linea con gli obiettivi da loro fissati come lo sviluppo sociale ed economico di alta qualità e soprattutto con il risparmio energetico e la riduzione delle emissioni.

Questa decisione da parte del governo cinese ha drasticamente cambiato la distribuzione geografica dei siti di estrazione di criptovalute, dal momento che la Cina è passata da controllare il 75% del mining globale al non contribuire più ufficialmente a questa attività, questo evento ha scatenato una migrazione dei miner verso altri paesi che hanno la possibilità di offrire energia a basso costo come fatto dalla Cina negli anni passati. I dati prodotti dal "Cambridge Center for Alternative Finance" mostrano che la ridistribuzione della potenza di calcolo utilizzata per il mining ad agosto 2021, si nota che la maggior parte è situata negli U.S.A con circa il 35% della potenza, mentre gli altri due grandi paesi in cui si sono insediate le mining pool sono stati il Kazakistan (18%) e la Russia (11%).

Sulla base degli studi fatti sul caso cinese, questa ridistribuzione desta delle preoccupazioni da parte delle autorità per quanto riguarda l'impatto ambientale, in quel caso l'utilizzo dell'energia in eccesso delle centrali idroelettriche era stata eletta come l'unica possibile alternativa per tenere sotto controllo le emissioni di CO2, ma questo non può avvenire in Kazakistan dove, secondo i dati del "US Department of Commerce"[54], l'87% dell'elettricità del paese è prodotta da combustibili fossili, in primis il carbone. Perciò la scelta della Cina di vietare ufficialmente l'attività di mining nel suo territorio ha esacerbato il problema delle emissioni a livello globale.

---

[54] Tidy, J. 2021. *US leads Bitcoin mining as China ban takes effect*, BBC News, https://www.bbc.com/news/technology-58896545 (date last accessed March 2, 2022).

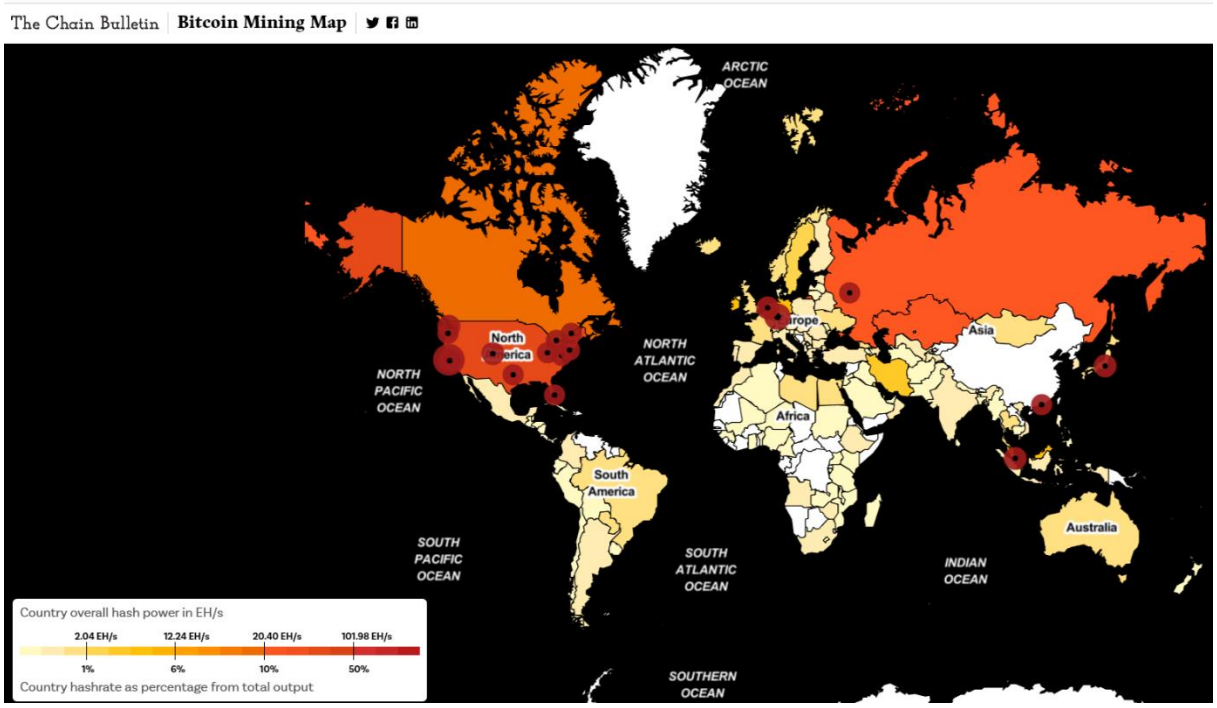


***Figura* 7.2.** *Mappa che mostra la distribuzione geografica dell'hashpower. Fonte:" https://chainbulletin.com/bitcoin-mining-map/" e https://www.openstreetmap.org/copyright.*

Nell'articolo "Renewable Energy Will Not Solve Bitcoin's Sustainability Problem" di Alex de Vries[55], utilizza il caso cinese per evidenziare alcune problematiche circa la sostenibilità dell'ecosistema di Bitcoin anche in uno scenario in cui vengano utilizzate delle fonti di energia rinnovabili. Lo studio fa riferimento all'utilizzo dell'energia idroelettrica delle regioni del Sichuan e Yunnman nel periodo in cui era possibile effettuare l'attività di mining, e dimostra quanto non sia efficace per rendere il settore del mining di bitcoin sostenibile. In primo luogo, l'autore afferma che essendo la rete elettrica di quelle regioni non di alta qualità l'esportazione di energia da fonti rinnovabili da quella regione risultava molto inefficiente e, il basso costo dell'energia in surplus avrebbe potuto spingere aziende molto energivore a spostarsi in quella regione facendo concorrenza ai miner. Inoltre, viene sottolineato che la produzione di energia

[55] de Vries, A. 2019. Renewable Energy Will Not Solve Bitcoin's Sustainability Problem, *Joule*, vol. 3, no. 4, 893–98.

da centrali idroelettriche è molto influenzata dalla stagionalità, si specifica che durante la stagione delle piogge la produzione di energia elettrica è circa tre volte maggiore rispetto alla stagione secca e perciò si creerebbe uno squilibrio di bisogno energetico colmabile solo attraverso altre fonti di energia, molto probabilmente dal carbone. Infine, si definisce un caso in cui i miner potrebbero temporaneamente sfruttare il surplus energetico di quelle regioni aumentando la domanda di energia elettrica base, nelle stagioni secche questa extra-domanda dovrebbe essere colmata da altre fonti il che potrebbe creare un incentivo per la costruzione di nuovi centrali a carbone per soddisfarla.

Un'altra componente che rende l'industria dei bitcoin una possibile minaccia per la riduzione delle emissioni a livello globale è osservabile nel problema dei rifiuti elettronici generati da Bitcoin. Dallo studio "Bitcoin's growing e-waste problem"[56] di Alex De Vries, si evince come l'intero sistema generi circa 30.7 mila tonnellate di rifiuti elettronici all'anno, la principale causa di questi dati è il costante aggiornamento a cui devono essere sottoposti i macchinari per l'attività di mining. Quest'ultime diventano obsolete molto velocemente, poiché tra i grandi *player* di questo settore avviene una continua competizione a sviluppare e distribuire hardware per il mining sempre più efficiente, in modo da ottenere un vantaggio competitivo.

[56] de Vries, A. and Stoll, C. 2021. Bitcoin's growing e-waste problem, *Resources, Conservation and Recycling*, vol. 175, 105901.

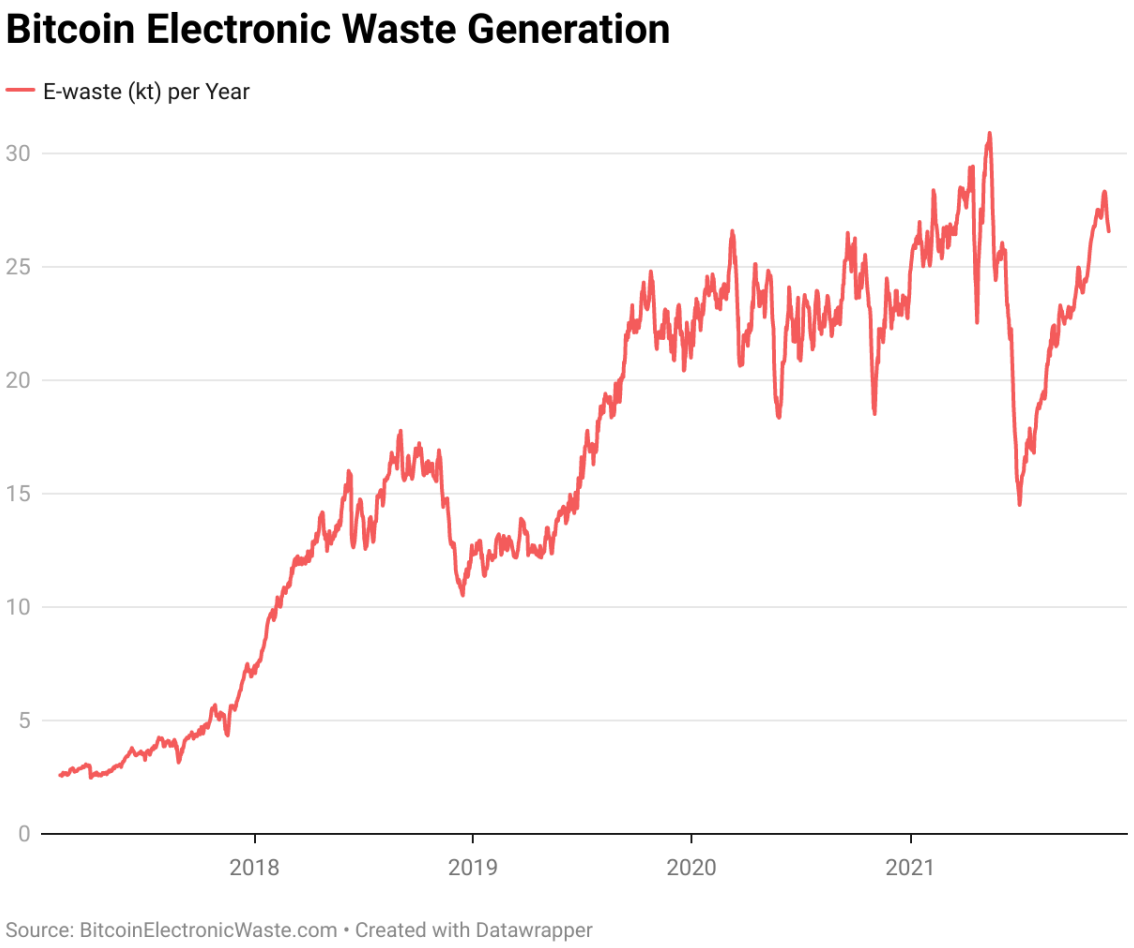


Figura 7.2. *Generazione di rifiuti elettronici in Ktonnellate all'anno. Fonte "https://digiconomist.net/bitcoin-electronic-waste-monitor/".*

Nello studio si stima che i calcolatori utilizzati per l'estrazione di bitcoin hanno una durata media di 1.29 anni, dopodiché vengono ritenuti non più redditizi in modo ottimale e, quindi, vengono sostituiti provocando una continua creazione di rifiuti elettronici.

Il problema è strettamente legato anche agli strumenti utilizzati per il mining poiché, con lo sviluppo del settore, è ormai consolidato l'impiego di ASIC[57], chip prodotti e ottimizzati per un uso specifico e che quindi non possono essere utilizzati per altri compiti; questo ne rende difficile, se non impossibile, il riutilizzo aumentando sensibilmente lo spreco di queste componenti.

Confrontando la generazione di rifiuti elettronici per transazione di bitcoin con altri metodi più tradizionali, ad esempio Visa, si evidenzia una sostanziale differenza legata alle esigenze

[57] Acronimo di Application Specific Integrated Circuit.

costruttive dei sistemi di gestione delle transazioni, che per Visa consistono in *Data center* caratterizzati da un minor tasso di riciclo rispetto ai mining pool.

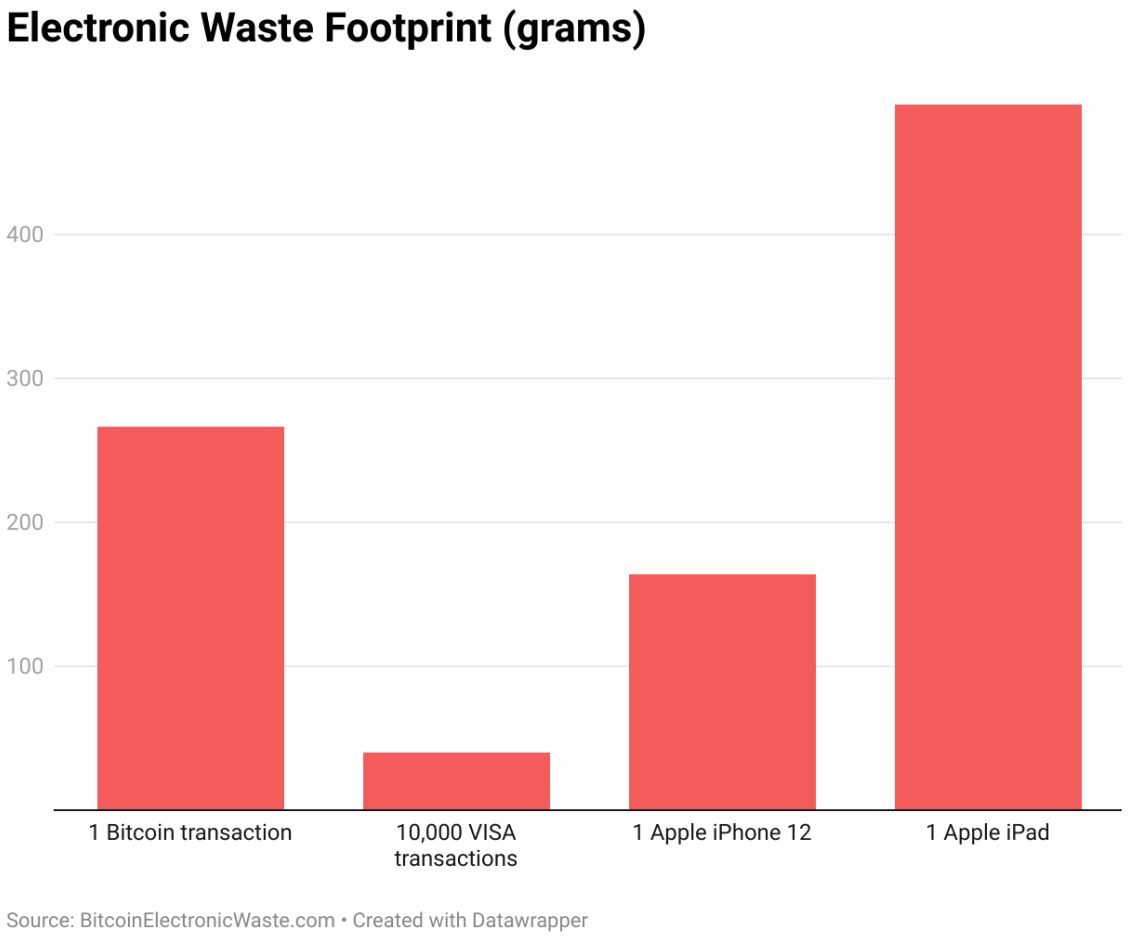


Figura 7.3. *Confronto dei rifiuti elettronici generati (in grammi) in relazione ai prodotti (in questo caso prodotti Apple) e servizi offerti (transazioni di Visa e Bitcoin). Fonte " https://digiconomist.net/bitcoin-electronic-waste-monitor/".*

Ogni 10000 transazioni, Visa produce 40 grammi di rifiuti elettronici, invece una singola transazione in bitcoin ne produce circa 306.

Oltre a considerare le emissioni per la continua produzione e approvvigionamento delle componenti elettroniche utilizzate dalle mining pool, è necessario considerare anche l'impatto dovuto allo smaltimento e il riciclo di questi rifiuti sull'ambiente. Uno scorretto smaltimento di questi rifiuti comporta un rilascio incontrollato nell'ambiente di sostanze nocive che possono creare gravi danni all'ambiente, è sufficiente pensare al solo rilascio di metalli pesanti nelle acque quali e quante conseguenze potrebbero generare. Inoltre, il non rispetto dei protocolli di sicurezza nello smaltimento dei rifiuti può mettere a rischio la salute dei

lavoratori e delle popolazioni limitrofe ai centri di smaltimento. Esistono numerose pubblicazioni che hanno evidenziato la correlazione tra la presenza di siti di smaltimento di questo genere di rifiuti con la maggior comparsa di problemi al sistema respiratorio, danni al cervello ecc.

Per cercare di creare delle alternative migliori dal punto di vista della sostenibilità ambientale sono state progettate delle criptovalute che hanno una intrinseca vocazione verso l'ecosostenibilità o che cercano una resa migliore rispetto alle criptovalute tradizionali, di seguito sono presentate alcune valute digitali con queste caratteristiche:

- Solari coin, una criptovaluta nata per incentivare la produzione di energia solare; i produttori di energia solare registrati possono ottenere 1 Solarcoin ogni 1MWh prodotto verificato dal sistema.

- Bitcoin green, creata dall'idea di realizzare una valuta digitale che fosse più sostenibile e scalabile rispetto a Bitcoin. Il metodo utilizzato nella ricerca di raggiungere l'obiettivo è stato quello di utilizzare un algoritmo del consenso più efficiente rispetto allo "proof-of-work", che è alla base dei problemi ambientali derivati da Bitcoin, ovvero è stato scelto di utilizzare un algoritmo "proof-of-stake". Questo metodo consente di evitare di utilizzare la risoluzione di problemi criptografici altamente energivori, difatti consente ai proprietari di usare i loro token come collaterali, quindi una persona può estrarre criptovalute in base alla numero di monete che detiene.

- Iota, valuta digitale che utilizza un ulteriore algoritmo del consenso che consente di utilizzare meno energia elettrica per la sua estrazione. Quest'ultima utilizza "Fast Probabilistic Consensus" per il consenso e si basa solo in parte sulla "proof-of-work". In questo caso il concetto di mining viene eliminato in modo da rendere disponibili fin da subito le valute, tutti questi fattori rendono questa criptovaluta molto più efficiente dal punto di vista energetico consentendole di utilizzare solo 0.11 Wh di energia a transazione, valore che risulta simile a quello di reti finanziarie più consolidate come VISA e Masatercard.

8 PRESENTAZIONE DELLE CRIPTOVALUTE E INDICI DI BORSA

Nel seguente capitolo vengono presentate le criptovalute e gli indici di borsa[58] oggetto di studio.

Si è deciso di scegliere cinque criptovalute in base alla loro importanza e al loro valore di capitalizzazione di mercato, con il vincolo di una disponibilità di dati delle quotazioni di almeno quattro anni.

8.1 Bitcoin

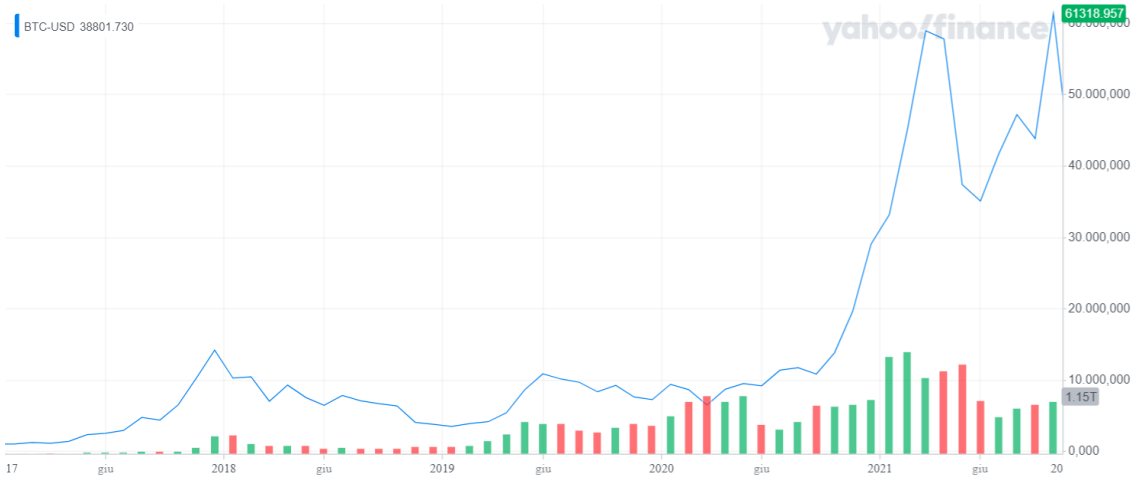


Figura 8.1. *Prezzo di Bitcoin. Fonte "https://it.finance.yahoo.com/".*

[58] Gli indici azionari hanno la funzione di rappresentare il valore di un paniere di titoli, i movimenti dell'indice sono una approssimazione della variazione del valore dei titoli all'interno del portafoglio. Le modalità con cui vengono calcolati gli indici sono molteplici e variano a seconda del modo in cui viene assegnato il peso ai titoli del paniere, possono essere ponderati in modo proporzionale alla capitalizzazione in borsa, in base al prezzo in base alla sostenibilità ecc.

È la criptovaluta con la capitalizzazione di mercato maggiore e la più famosa e diffusa al mondo, solitamente descritta semplicemente come una moneta virtuale decentralizzata e anonima che non è controllata da nessun governo o alcuna entità legale che non può essere convertita in oro o in altre commodity. Dato il continuo riferimento a questa valuta digitale nelle sezioni precedenti, si è deciso di evidenziare solo alcuni aspetti salienti non trattati in precedenza.

Storia della valuta

Questa valuta digitale nasce contestualmente alla pubblicazione del *white paper* dal titolo "Bitcoin: A Peer-to-Peer Eletronic Cash System" scritto da Satoshi Nakamoto, avvenuta nel 2008. In questo documento viene descritto come poter utilizzare una rete *peer-to-peer* per creare, come viene affermato nella parte conclusiva del documento, "*a system for electronic transactions without relying on trust*". Successivamente il 3 gennaio del 2009 venne creato il primo blocco della rete bitcoin, il cosiddetto blocco genesi o blocco 0.

Una delle persone più importanti per i primi momenti di vita della criptovaluta, oltre a Satoshi Nakamoto, fu Hal Finney, programmatore informatico statunitense, fu uno dei primi utilizzatori e sostenitori come dimostrato dal fatto che effettuò il download del software di bitcoin il giorno stesso in cui fu rilasciato. Entrò nella storia di Bitcoin diventando il primo utente che a ricevere una transazione in bitcoin, questa fu eseguita con il creatore della criptovaluta il 12 gennaio 2009.

Il primo pagamento con bitcoin avvenne il 22 maggio 2010, giorno in cui Laszlo Hanyecz spese 10.000 bitcoin per pagare due pizze ordinate da una pizzeria locale, all'epoca quella somma di bitcoin aveva un valore di circa 40$ ma ad oggi varrebbe circa 400 milioni di dollari. La transazione non avvenne in modo diretto dal momento che la criptovaluta non era ancora accettata come metodo di pagamento, Hanyecz face una richiesta sul *Bitcointalk*[59] facendo

[59] Creato da Satoshi Nakamoto il 17 novembre 2009, è un forum dove si riuniscono tutte le persone interessate alla criptovaluta, a sostenerla e a partecipare al suo sviluppo. Il ruolo del forum fu fondamentale per lo sviluppo delle prime versioni di Bitcoin e della blockchain, su quel sito web i primi sviluppatori e Satoshi Nakamoto si scambiarono idee e opinioni fino a delineare le caratteristiche di Bitcoin così come è conosciuta oggi.

pagare le pizze ad un utente in cambio delle criptovalute sopracitate. Questo evento ha avuto un impatto talmente significativo nella comunità di Bitcoin da promuovere una ricorrenza chiamata "Bitcoin Pizza Day", in cui si commemora il primo acquisto di un bene attraverso una valuta virtuale.

Il 9 febbraio 2011, la criptovaluta raggiunge il valore di 1 dollaro su MtGox, questo valore è simbolico poiché di fatto in quel momento la valuta digitale raggiunge la parità con il dollaro, da quel momento il valore di bitcoin avrà una crescita molto rapida arrivando a raggiungere il suo picco massimo ad aprile 2021 con un valore di 64800 $.

Il 17 settembre 2021, El Salvador è diventato il primo paese al mondo ad affiancare bitcoin alla moneta nazionale, in questo caso il dollaro. Il presidente del paese, Nyib Bukele, ha spinto per questa manovra con l'obiettivo di rilanciare l'economia, dando una spinta ai consumi e aumentando l'inclusione finanziaria, considerato lo scarso utilizzo dei cittadini dei servizi bancari principali. Non è stata fatta una transizione completa e radicale dal dollaro alla valuta digitale, gli stipendi e le pensioni sono ancora pagate in dollari e gli operatori economici e gli esercizi commerciali non sono obbligati ad accettare bitcoin, ma hanno l'obbligo di indicare tutti i prezzi in entrambe le valute.

Limite di supply

Un elemento fondamentale che caratterizza questa criptovaluta è che il numero di bitcoin che è possibile creare attraverso il processo del mining è limitata dalle regole di mining imposte dal suo creatore: il processo di creazione di bitcoin è strutturato in modo che la generazione di un blocco nella blockchain, con l'avanzare del tempo e del numero di valute create, sarà ricompensata con sempre meno valute digitali fino al punto in cui potranno essercene al massimo 21 milioni. Secondo Andreas M.Antonopoulos, importante divulgatore e esperto di criptovalute, la cifra di 21 milioni è un "limite asintotico", perciò il numero totale di bitcoin tenderà verso quella cifra senza mai effettivamente raggiungerla.

La data prevista per il raggiungimento del limite massimo della criptovaluta è stimata a circa il 2140, da quel momento gli scenari sono di difficile previsione poiché il sistema non è ancora del tutto sviluppato, anche alla luce delle deviazioni hanno caratterizzato bitcoin dalle intenzioni originali. Uno dei possibili scenari prevederebbe una trasformazione del sistema e del funzionamento della criptovaluta, tra questi si potrebbe ipotizzare un cambiamento nel

protocollo tale da poter superare il limite dei 21 milioni. Questo scenario sembra essere improbabile poiché si andrebbe a cambiare uno dei principali motivi che spingono ad investire nella valuta digitale, ovvero la sua scarsità. Perciò i *miner*, i quali sarebbero i primi interessati ad aumentare il limite per non modificare il loro sistema di guadagno, potrebbero vedere i loro ricavi drasticamente diminuiti a causa della diminuzione dei prezzi della valuta dovuta ad una offerta più alta.

In uno scenario in cui viene raggiunto il limite, le ricompense dall'attività di mining non sarebbero sufficienti a coprire i costi operativi, si potrebbe affermare che non esisterebbe più alcuna ricompensa in quel contesto. I minatori potrebbero rendere la loro attività redditizia solo in caso di un controllo delle transazioni, se la criptovaluta venisse usata come riserva di valore i miner potrebbero richiedere delle commissioni elevate in modo da poter ottenere dei guadagni. Nel caso, invece, di utilizzo delle criptovaluta come mezzo di scambio le commissioni dovrebbero rimanere ad un livello ragionevole in modo da rendere possibile l'uso della valuta digitale nelle transazioni quotidiane.

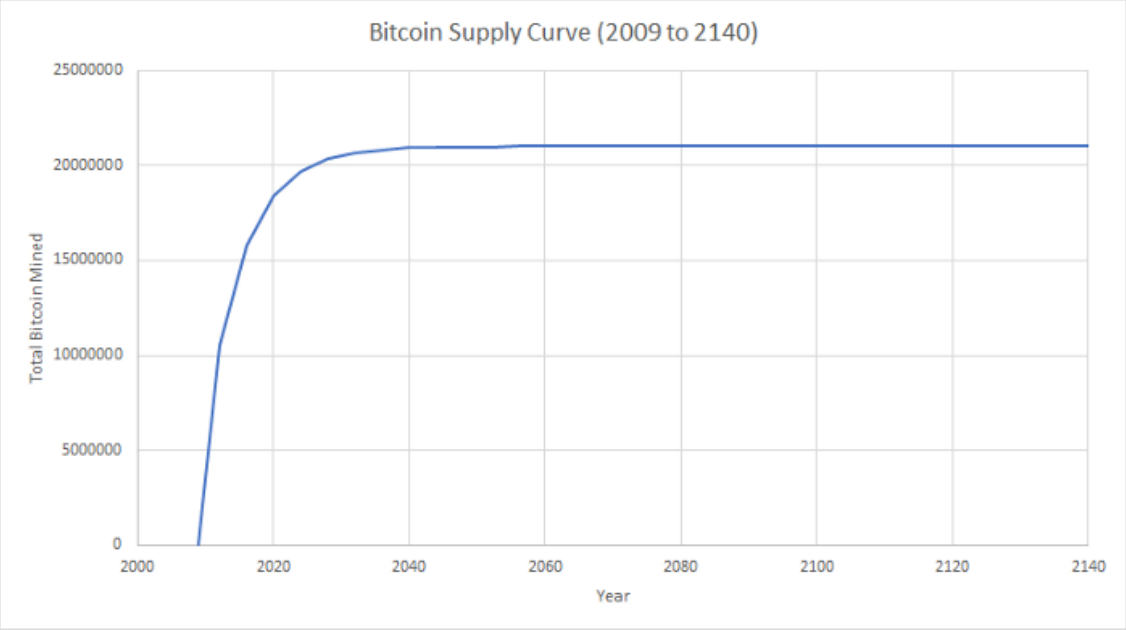


***Figura 8.2**. Quantità di bitcoin estratti dal 2009 fino alla possibile data di raggiungimento del limite massimo. Fonte" https://medium.com/@billygarrison.btc/what-the-bitcoin-halving-is-and-how-to-witness-it-8c6f13173b65".*

Bitcoin ETF

Gli ETF, acronimo di *Echange Traded Funds*, sono "fondi o SICAV a basse commissioni di gestione negoziati in Borsa come le normali azioni. Si caratterizzano per il fatto di avere come unico obiettivo quello di replicare fedelmente l'andamento e quindi il rendimento di indici azionari, obbligazionari o di materie prime" (ETF (Exchange Traded Fund) Borsa Italiana, 2022). Questi fondi forniscono agli investitori la possibilità di poter diversificare i loro investimenti senza possedere le attività. Una caratteristica comune agli ETF tradizionali è che questi sono collegati a dei panieri molto ampi di attività che hanno una caratteristica che li accomuna, un esempio tipico è il focus sulla sostenibilità, consentendo dunque di poter diversificare molto facilmente i loro investimenti.

Il 19 ottobre 2021 è stato creato il primo ETF sui bitcoin, l'autore di questo lancio è stata la società *Proshare*, un gruppo creato nel 2006 specializzato nella fornitura di servizi finanziari, la quale ha ottenuto un ottimo successo di fatto avendo lanciato il secondo ETF più scambiato al debutto.

L'ETF sui bitcoin consente agli investitori di poter investire nel settore della valuta digitale bypassando il sistema di negoziazione di bitcoin che potrebbe risultare complicato e non *user-friendly* per i non esperti del settore. Oltre a ciò, gli investitori andrebbero incontro ad una ulteriore semplificazione poiché non saranno tenuti a eseguire procedure complesse di archiviazione e di messa in sicurezza necessarie per poter detenere delle criptovalute.

Si possono evidenziare ulteriori vantaggi nell'esistenza degli ETF sui bitcoin, attraverso di essi, infatti, si evita di gestire in prima persona gli scambi di criptovaluta e, quindi, di poter semplicemente acquistare e vendere l'ETF rimanendo all'interno del sistema degli scambi e mercati tradizionali. Inoltre, data la natura degli ETF, essi permettono la possibilità, assente nel caso di bitcoin e delle altre criptovalute, di poter vendere allo scoperto delle azioni dell'ETF nel caso prevedessero una discesa del prezzo di bitcoin in futuro.

Principali caratteristiche

Le principali caratteristiche di bitcoin sono:

- Decentralizzazione: alla base delle idee di Nakamoto era sicuramente centrale l'idea di ottenere l'indipendenza da qualsiasi autorità in modo che qualunque persona potesse partecipare attivamente al processo di mining e alla verifica delle transazioni.
- Anonimato: con il sistema utilizzato da bitcoin l'indirizzo del *wallet* non può essere collegato a nessuna informazione personale, a differenza dei canali tradizionali in cui le autorità, ad esempio le banche, necessitano di ogni dettaglio personale per fornire i loro servizi. Ovviamente questa particolare caratteristica può supportare attività illecite come il riciclaggio di denaro e la compravendita di oggetti illegali.
- Trasparenza: ogni singola transazione è registrata all'interno della blockchain, perciò ogni persona, in qualunque momento, può visionare tutte le transizioni. In aggiunta, teoricamente sarebbe possibile risalire ad ogni transazione effettuata da un particolare utente e sapere quanto denaro è presente nel suo portafoglio, ma, come descritto precedentemente, sarebbe impossibile identificare la persona collegata al suo indirizzo Bitcoin.
- Velocità: è possibile effettuare pagamenti e scambi di denaro in modo quasi immediato anche per pagamenti internazionali, risulta quindi molto più veloce rispetto ai metodi tradizionali.
- Irreversibilità: questa caratteristica corrisponde alla impossibilità di riottenere i bitcoin dopo averli inviati a meno che il destinatario non li rispedisca effettuando una ulteriore transazione, in questo modo la ricezione del pagamento è assicurata.

8.2 Ethereum

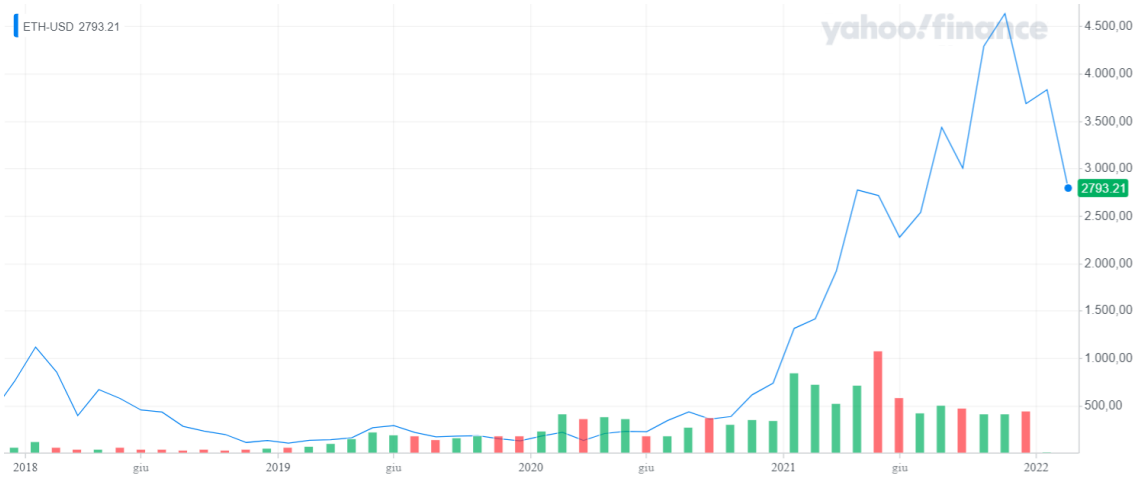


Figura 8.3. *Prezzo di Ethereum. Fonte "https://it.finance.yahoo.com/".*

L'intento dei suoi creatori era quello di creare una piattaforma che si distaccasse dai protocolli precedenti che miravano a offrire funzionalità per settori o applicazioni specifiche, i creatori del progetto Ethereum volevano cercare di creare una rete di criptovalute molto flessibile in modo da dare la possibilità di creare delle applicazioni specifiche per ogni scopo realizzabile. Il servizio offerto dai suoi sviluppatori consisteva nel creare un protocollo migliore su cui altre applicazioni decentralizzate potessero basarsi offrendo una scalabilità ed efficienza maggiore rispetto alle altre.

Una delle caratteristiche fondamentali e alla base della sua innovatività è il linguaggio di scripting progettato per essere libero da più restrizioni possibili, l'unico vincolo è l'esistenza di un sistema di pagamento, ma nella pratica qualunque tipo di regola può essere pianificata. Il linguaggio di scripting fornito da Ethereum è "turing completo", così un programmatore potrebbe creare qualunque tipo di *smartcontract* o transazioni che possono essere definite matematicamente.

il sistema Ethereum e la moneta Ether

Ethereum adotta un sistema *account based* per la validazione delle transazioni, l'autorizzazione all'esecuzione di quest'ultime è collegata al saldo di ether di ogni account. Esistono due tipologie di account:

- Account "Externally Owned", chiamati anche "EOA", a questi è associata una chiave privata[60] e hanno la possibilità di generare delle transazioni.
- *Contract account*, essi non possono generare delle transazioni e non hanno associata alcuna chiave privata.

Entrambe le tipologie di account hanno un indirizzo e un saldo di ether e possono mandare o ricevere ether.

Ether è la moneta digitale di Ethereum, nel sistema ad ogni transazione è richiesto il pagamento di una commissione, riscossa dai *miner*, per convalidare una trasmissione, queste sono pagate in unità denominate Gas. Questa unità è stata creata poiché gli sviluppatori di Ethereum decisero di assegnare dei valori costanti alle possibili operazioni che possono essere eseguite tramite il sistema, in modo tale che ogni operazione nel sistema Ethereum avesse un valore in Gas stabilito e costante, in base al costo computazionale, e quindi non possa venire alterato dalle oscillazioni del valore di Ether. In questo modo gli sviluppatori hanno potuto scindere il prezzo della moneta virtuale, caratterizzata da una naturale volatilità, e il costo computazionale delle operazioni svolte dal sistema. Con questa importante distinzione che divide il costo computazionale e il valore in ether delle operazioni, in base al prezzo in quel momento, gli sviluppatori hanno aiutato a rendere utilizzabile il sistema indipendentemente dal momento storico e, quindi, dal valore di ether.

Oltre all'unità Gas, che è il valore di gas legato al valore di costo computazionale di una specifica operazione ma che non ha di per sé un valore monetario, è necessario utilizzare anche il prezzo del gas per caratterizzare una operazione. Il prezzo del gas è il prezzo che si sceglie di pagare per ogni unità di gas dell'operazione, costituendo, in base all'operazione, la commissione detta anche *Gas fee.* Attraverso la commissione è possibile gestire il livello di priorità che si vuole assegnare all'operazione, se si è disposti a pagare un valore maggiore per ogni unità di gas utilizzato saranno i *miner* più veloci che si incaricheranno di validare la transazione.

[60] È una chiave criptografica utilizzata in un sistema di criptografia asimmetrica, essa non deve essere scambiata con nessun altro utente della rete poiché fondamentale per il funzionamento del sistema che unicamente il legittimo proprietario la conosca.

Per facilitare la gestione del carico computazionale della rete di Ethereum esistono dei limiti al numero di unità di Gas che la rete può gestire in un certo istante, i limiti sono stabiliti in base all'operazione: per quanto riguarda una transazione il limite imposto è di circa 21000 unità di Gas; il valore limite per gli *smart contracts* è molto più alto dal momento che questi possono avere più o meno complessità nelle loro interazioni e questo implica un livello di unità gas maggiore, il limite è solitamente tra le 130.000 e le 145.000 unità; è stato fissato anche il limite massimo per un blocco della blockchain, il suo valore dovrebbe essere circa 8 milioni di unità di Gas, perciò i *miner* hanno la consapevolezza di poter includere tutte le transazioni, *smart contracts* e interazioni possibili purché il livello totale di unità di Gas rientri in tale limite. Con questo meccanismo, le ricompense dei *miner* sono costitute da due parti: una parte fissa che è data dalla generazione di un blocco che è pari a 2 Ether, la parte restante è costituita dalle commissioni corrisposte al *miner* in base alle unità di Gas delle operazioni, ogni unità di Gas ha un prezzo in Gwei, ovvero i decimali di Ether, perciò è possibile stabilire questa parte variabile calcolando semplicemente il prodotto tra prezzo di una unità di gas e il numero di unità.

La nascita di Ethereum coincide con l'uscita del *white paper* di Ethereum avvenuta nel 2014, in cui si delineavo le particolarità più innovative del suo sistema e l'ambizione di creare un sistema *general purpose*[61], da quel momento il team di fondatori di Ethereum ha iniziato a lavorare alla rete finché, nel 2015, è stato messo a punto "Olympic" l'ultimo prototipo prima del rilascio al pubblico. Luglio 2015 ha segnato il lancio ufficiale della piattaforma Ethereum con la creazione del blocco genesi.

Dal gennaio 2016 il protocollo Ethereum riusciva ad elaborare 25 transazioni al secondo, un numero molto limitante se confrontato con piattaforme di pagamento consolidate, come Visa che riesce ad elaborare 45.000 transazioni al secondo, questi dati, dunque, fecero nascere dei dubbi sulla potenziale scalabilità della piattaforma. Durante il 2016, Ethereum è riuscito a crescere in modo significativo attirando l'interesse della stessa Visa per il suo sistema.

A partire dal gennaio 2018, Ethereum è diventata la seconda criptovaluta per capitalizzazione del mercato, dietro a Bitcoin, e attualmente mantiene ancora quella posizione, ciò dimostra

[61] In ambito informatico fa riferimento alla caratteristica di non essere specializzato ma di essere flessibile e adattabile per molti impeghi.

come la solidità e l'innovatività del suo sistema siano stati particolarmente apprezzati dal mercato.

Ethereum e NFT

Il sistema di Ethreum è alla base di una nuova tecnologia che sta diventando sempre più conosciuta ed utilizzata, tanto da causare la creazione di un nuovo mercato in rapida ascesa in cui, ad oggi, si possono contare più di 500 mila venditori e acquirenti e si registrano scambi che superano il milione di dollari. La tecnologia su cui si fonda tutto ciò sono gli NFT, acrononimo di *non-fungible token*, delle unità di dati uniche e non interscambiabili conservate su una blockchain. Quest'ultimi sono degli asset criptografici caratterizzati da un codice di identificazione univoco e da dei metadata che li contraddistinguono gli uni dagli altri. A differenza delle criptovalute che sono dei token fungibili, in quanto possono essere scambiati poiché sono definiti dal proprio valore e possono essere sostituiti, gli NFT non possono reciprocamente intercambiabili in quanto solitamente sono utilizzati per rappresentare la proprietà di oggetti unici.

Gli NFT sono token unici e indivisibili utilizzati per assegnare o rivendicare la proprietà di qualsiasi oggetto unico digitale, costituito semplicemente da dati, che sia tracciabile utilizzando la blockchain di Ethereum principalmente. I token, infatti, sono stati creati utilizzando lo standard di Ethereum ERC-721 e ERC-1155.

I token di questo tipo possono avere un proprietario alla volta, essi vengono coniati tramite degli *smart contract* secondo gli standard sopracitati; le informazioni create tramite il processo di "conio" vengono registrate sulla blockchain.

Ad oggi, questi token sono utilizzati per una vasta gamma di scopi, ma sicuramente l'ambito principale è l'arte digitale. In questo particolare contesto si è creato un nuovo mercato dove i creatori di contenuti digitali riescono a vendere le loro opere senza l'invadente intermediazione del mercato tradizionale, grazie a ciò riescono a guadagnare in modo diretto e, grazie alla particolare flessibilità degli NFT, possono anche decidere di inserire delle *royalty* sui futuri scambi dell'oggetto.

Gli NTF sono entrati in contatto anche con il mondo della finanza decentralizzata, difatti sono nate delle applicazioni che offrono la possibilità di prendere in prestito del denaro utilizzando questi token come garanzie. Possono essere offerti o sottoscritti dei prestiti la cui garanzia è

costituita da un oggetto digitale, ad esempio, la cui proprietà è documentata da un NFT, in questo modo nel caso non sia rimborsato il prestito il token verrà inviato direttamente al prestatore. Questi scenari sono facilitati dal fatto che grazie alla particolarità del sistema di Ethereum, infatti sia il mondo degli NFT che quello della finanza decentralizzata utilizzano la stessa infrastruttura.

8.3 Binance Coin

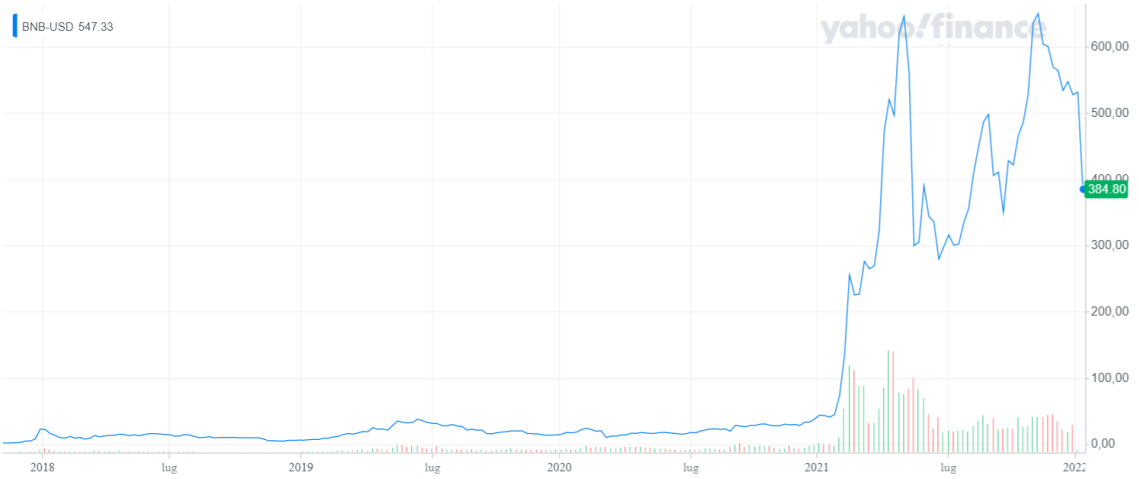


Figura 8.4. *Prezzo di Binance Coin. Fonte "https://it.finance.yahoo.com/".*

Binance è un exchange di criptovalute nato nel 2017, in un breve lasso di tempo è riuscito a crescere fino a diventare nel 2018 la più grande piattaforma di exchange di criptovalute con capitalizzazione di mercato di 1.3 miliardi. Nonostante, ad oggi, la concorrenza nel settore sia più forte rimane comunque una delle piattaforme più importanti del mercato.

La piattaforma dal 2017 ha continuato ad essere aggiornata con l'aggiunta di nuove funzionalità, come l'incubatore per le start up e il software per lanciare le ICO; tra gli aggiornamenti più significativi è necessario evidenziare la creazione della criptovaluta Binance coin.

Binance coin si inserisce nel sistema di Binance per accedere ai servizi che la piattaforma offre ad un prezzo ridotto. I progettisti della criptovaluta decisero di basare la loro creazione sulla blockchain di Ethereum, garantendosi la possibilità di utilizzare una struttura consolidata e particolarmente sofisticata dal punto di vista tecnologico e, inoltre, di poter sfruttare la peculiare flessibilità che la caratterizza. Effettuando la ICO nell'ecosistema di Ethereum,

Binance coin è da considerarsi come se fosse un progetto a sé stante e, quindi, tramite la piattaforma Binance, può essere scambiata con altre criptovalute e in alcuni casi convertita in denaro.

Binance ha lanciato L'ICO a giugno 2017, raccogliendo 15 milioni di dollari e distribuendo in modo proporzionato le 200 milioni unità di criptovaluta tra il pubblico, i *business angels* e la piattaforma stessa che necessitava di monete virtuali per rendere possibili le operazioni di exchange.

A marzo del 2018 Binance ha deciso di lanciare la sua nuova blockchain con il nome "Binance Chain", cercando di creare un mercato alternativo per la realizzazione e lo scambio di risorse in modo decentralizzato. Essa utilizza il sistema del consenso sviluppato da "Tendermint", che sfrutta un algoritmo basato sul PoS.

il processo di "burn"

Il processo di *burn* delle criptovalute è un metodo per cui vengono eliminate delle valute digitali dalla circolazione in modo da ridurne il numero in uso. In particolare, i token vengono inviati ad un *wallet* sconnesso dal sistema di transazioni, ad esclusione della ricezione di monete. Il portafoglio in questione è considerabile esterno alla rete e, quindi, i token al suo interno non possono essere in alcun modo riutilizzati. Questi indirizzi, a cui è associato il wallet, sono chiamati *eater* o *burner* e, a differenza dei portafogli "normali", che possiedono un chiave privata per accedere ai token immagazzinati, essi ne sono sprovvisti a rimarcare il fatto che i token una volta inviati a questo portafoglio sono virtualmente eliminati.

Il concetto di *coin burn* può essere effettuato attraverso varie procedure, in base al sistema sulla quale è basata la criptovaluta, in particolare Binance coin ha effettuato delle *coin burn* periodiche utilizzando una funzione di uno *smart contract* nota come funzione di *burn*. Gli eventi di burn, per Binance coin, sono schedulati per avvenire ogni trimestre fino "bruciare" il 50% del totale delle monete create, quindi 100˙000˙000 criptovalute. La quantità eliminata ogni trimestre varia in base al volume di scambi effettuati in quel periodo.

Questi processi di rimozione delle criptovalute, generalmente, sono effettuati dagli sviluppatori stessi, come nel caso di Binance coin, poiché l'offerta ridotta della moneta dovrebbe aumentarne il prezzo creando un vantaggio per i suoi proprietari. Ovviamente la conseguenza di un *burn* non è così diretta, in quanto il possibile effetto dipende dalla

percezione degli investitori e dai potenziali investitori, inoltre il modo in cui i nuovi valori di domanda-offerta possano influenzarne il prezzo non è facilmente calcolabile. È possibile paragonare questa pratica con il meccanismo del *buy-back* per i mercati tradizionali, in quanto è possibile evidenziare delle caratteristiche comuni tra le due azioni, sia dal punto di vista del processo che delle conseguenze.

Inoltre, attraverso questo processo è stato creato un algoritmo del consenso chiamato Proof-of-Burn, in cui si utilizza la rimozione di alcuni token dal sistema per raggiungere il consenso e aggiungere un nuovo blocco alla catena.

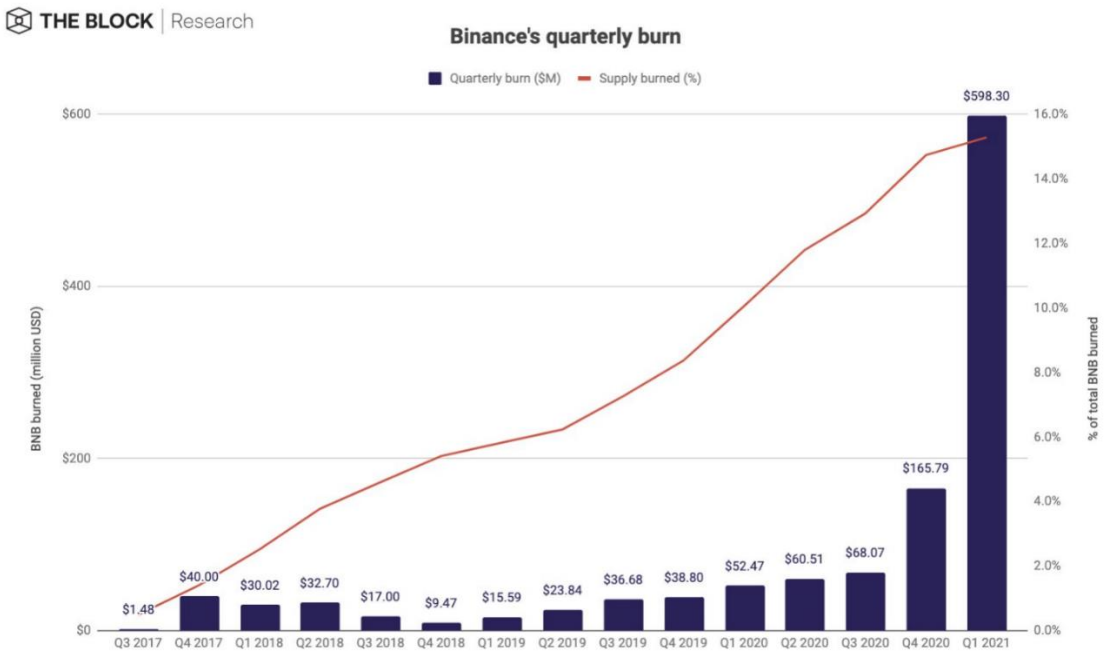


Figura 8.5. *Valore delle monete (in milioni di dollari) "bruciate" in ogni trimestre da Binance Coin. Fonte "https://www.theblockcrypto.com/linked/101912/binance-15th-quarterly-bnb-burn-token-highest-ever"*

Binance smart chain

Binance Smart Chain (BSC) è una blockchain che funziona parallelamente alla Binance chain, ma a differenza di essa è più ottimizzata per gestire le funzionalità degli *smart contract* e

garantisce la compatibilità con la "Ethereum Virtual Machine" [62]. In questo modo gli sviluppatori hanno cercato di mantenere intatto il *throughput* della Binance chain e allo stesso tempo inserire nell'ecosistema tutte le potenzialità degli *smart contract.* È necessario specificare come queste due blockchain cooperino, ma allo stesso tempo siano anche indipendenti, ossia la BSC potrebbe funzionare anche nel caso in cui la Binance chain andasse *offline*.

La compatibilità con la "Ethereum Virtual Machine" ha facilitato la progettazione di questa nuova blockchain visto che fin dall'inizio ha potuto utilizzare, come supporto, i tool di Ethereum, ciò rende anche più semplice e immediato il trasferimento di progetti dal suddetto sistema.

BSC utilizza un algoritmo del consenso appartenente al gruppo Proof-of-Stake, in particolare è chiamato Proof-of-Staked Authority, in quanto combina caratteristiche anche del Proof-of-Autority (POA). Come in quest'ultimi, nell'algoritmo del consenso di BSC esistono alcuni nodi chiamati *validator*, essi si occupano di verificare e validare transazioni e blocchi della catena, operando come "moderatori" del sistema. A differenza del POW e POS, i *validator* mettono in gioco la loro reputazione per ottenere e mantenere la loro posizione, infatti per ottenere tale carica essi devono rendere pubblica la loro identità. L'incentivo nel comportarsi in modo onesto e collaborativo deriva, appunto, dall'evitare un possibile danno reputazionale, dalle ripercussioni legali o alla più diretta perdita del ruolo di validatore. Inoltre, è bene specificare che l'operato di ogni *validator* è controllato dagli altri, che hanno eguale potere e capacità di contestare una transazione.

I validatori in questo sistema vengono rieletti ogni 24 ore, per candidarsi è necessario mettere in gioco la propria reputazione e una quantità di BNB, coloro che offriranno la maggiore quantità di criptovaluta diventeranno *validator*. Anche in questo nuovo sistema i BNB sono utilizzati come mezzo di pagamento per le commissioni.

A livello di performance questo sistema si presenta come un considerevole competitor rispetto alle altre blockchain; a livello di scalabilità, infatti, le sue prestazioni sono notevoli, è sufficiente osservare che il tempo medio di aggiunta di un nuovo blocco alla catena è di soli tre secondi.

---

[62] Elemento della blockchain di Ethereum che consente di eseguire una grande varietà di funzioni e istruzioni, grazie a ciò è possibile implementare programmi e gli *smart contracts* per aumentare le funzionalità della blockchain.

Inoltre, presenta dei vantaggi anche dal punto di vista economico dal momento che le commissioni sono inferiori rispetto alla concorrenza.

8.4 Litecoin

Figura 8.6. *Prezzo di Litecoin. Fonte "https://it.finance.yahoo.com/".*

È una criptovaluta nata nel 2011, dall'idee di Charlie Lee e dei suoi collaboratori, con lo scopo di migliorare alcune caratteristiche della più famosa Bitcoin. In sostanza, l'obiettivo di tale progetto era di creare una valuta digitale con una generazione dei blocchi più veloce, con commissioni più economiche e pagamenti più veloci.

Storia della valuta

Nel 2011 alcuni utenti avevano cominciato a manifestare una certa preoccupazione riguardo al processo di mining di Bitcoin, all'epoca era ormai effettuato solamente tramite GPUs e perciò si potevano creare alte barriere all'ingresso per questa attività. Per ovviare a questo

problema, in quel periodo, iniziarono ad essere sviluppate delle valute digitali alternative a Bitcoin, come ad esempio Tenebrix o Fairbrix[63], caratterizzate da un metodo di mining differente. Proprio dallo sviluppo di Fairbrix, nasce Litecoin, la quale ha ereditato completamente l'algoritmo di mining di Fairbrix, ma concepisce comunque un limite di massimo di monete come Bitcoin.

Il lancio ufficiale di Litecoin è avvenuto nel 2013, al momento della *release* il valore della criptovaluta era di 4.30$.

Durante il suo sviluppo, per via di alcune caratteristiche simili a Bitcoin, è stata usata come ambiente di testing per progetti innovativi e nuove features potenzialmente implementabili nell'ecosistema di entrambe le valute digitali, ad esempio SegWit, the Lightning Network ecc.

Caratteristiche della criptovaluta

Una delle sostanziali differenze rispetto a Bitcoin riguarda la generazione dei blocchi della catena, questa operazione, nel caso di Litecoin, richiede circa il 75% di tempo in meno in media, il che rende la fase di convalida delle transazioni significativamente più veloce. Questo miglioramento è ottenuto attraverso un cambiamento nel protocollo rispetto a Bitcoin, infatti, quest'ultimo utilizza una funzione di hash "SHA-256", invece Litecoin utilizza la funzione "Scrypt". Entrambi questi algoritmi si basano sulla Proof-of-Work, ma l'utilizzo della funzione di "Scrypt" la rendono meno dispendiosa in termini di risorse e inoltre rende possibile creare blocchi inferiori a 1 MB. Ad oggi la potenza necessaria per l'attività di mining di Litecoin non è ancora molto alta.

Un altro problema che i creatori di Litecoin hanno cercato di risolvere era relativo alla scalabilità, le transazioni potenzialmente elaborabili da Bitcoin sono risultate notevolmente limitanti per le ambizioni a cui aspirano le criptovalute in generale. C.Lee e i suoi collaboratori sono riusciti a migliorare questo aspetto passando dalle 7 elaborazioni al secondo di Bitcoin, alle 56 di Litecoin. Come già descritto in precedenza, queste prestazioni non sono ancora comparabili rispetto ad altre soluzioni di pagamento consolidate sul mercato.

L'emissione di monete è stata aumentata rispetto a Bitcoin, il numero massimo di token di Litecoin è di 84 milioni; oltre a ciò, è stata modificata anche la soglia per la riduzione di monete

[63] Criptovaluta creata da Charlie Lee nel 2011.

per ogni blocco: il numero di blocchi necessari per dimezzare l'emissione è 4 volte superiore rispetto a Bitcoin, per Litecoin avviene ogni 840.000 blocchi mentre per Bitcoin ogni 210.000.

8.5 Monero

Figura 8.7. *Prezzo di Monero. Fonte "https://it.finance.yahoo.com/".*

Questa criptovaluta nasce nel 2014 sulla base dei principi di non associabilità e non tracciabilità, ovvero l'idea di non poter collegare due transazioni e di non poter determinare fonte e destinazione dei fondi. Il suo nome iniziale era BitMonero, successivamente venne denominata semplicemente Monero[64].

Storia della valuta

Il progetto ebbe origine su un *thread* sul forum "Bitcointalk" nel 2014, in cui un utente mostrava le caratteristiche del suo progetto chiamato "BitMonero", ma inizialmente non riscosse molto successo tra i membri della comunità. Molti utenti evidenziarono delle problematiche nella prima versione del progetto, perciò si creò un team di sviluppatori che decise di migliorare gli aspetti più critici del progetto per renderlo interessante agli occhi della community.

[64] Monero in esperanto significa "moneta".

Questo gruppo creò, poco tempo dopo, la ormai celebre criptovaluta Monero, quest'ultima dal 2014 è stata continuamente aggiornata con l'obiettivo di migliorarne le performance senza snaturarne i principi.

Caratteristiche

Data la sua attenzione alla privacy, la sua flessibilità e facilità di programmazione ebbe una rapida crescita dal 2014, diventando una delle criptovalute più importanti del mercato.
Le principali caratteristiche su cui è basato l'intero progetto Monero sono:

- La privacy: è sicuramente uno dei capisaldi della criptovaluta e il segno distintivo rispetto ai competitor; molte sue funzioni, algoritmi e protocolli sono stati sviluppati ad hoc per assicurarne la massima integrità.
- La sicurezza: gli sviluppatori sottolineano come per loro sia fondamentale ottenere la fiducia a riguardo delle transazioni con Monero, perciò hanno sviluppato e continuano ad aggiornare il sistema di sicurezza del protocollo. Questo aspetto è legato alla privacy e alla criptografia utilizzata nel sistema.
- Il decentramento: caratteristica comune alle altre criptovalute.

L'alto livello di privacy, principio cardine di Monero, è raggiunto grazie all'applicazione di sofisticate tecniche criptografiche, la più nota è la tecnica delle "firme ad anello". Attraverso questo metodo si combina l'indirizzo di un mittente con un gruppo di altri indirizzi, in questo modo la difficoltà di tracciare la transazione cresce in modo esponenziale.
Inoltre, per aumentare ulteriormente il livello di privacy, viene applicato un altro concetto denominato "indirizzi invisibili", secondo cui gli indirizzi utilizzati nelle transazioni vengono generati in modo che sia impossibile scoprire i veri indirizzi di destinazione e del mittente per utenti che sono semplici osservatori nella rete e non rappresentano né il destinatario né il mittente.
Infine, per completare il quadro dei sistemi di protezione della privacy implementanti in Monero, è necessario citare anche l'implementazione di un metodo "zero-knowledge-proof", per la precisione chiamato "Bulletproofs", che garantisce la riuscita della transazione senza che sia svelato il suo valore.

In ultima analisi, si è deciso di sottolineare una ulteriore caratteristica che differenzia Monero dalle altre criptovalute, ovvero l'algoritmo alla base del sistema di mining, il "Crypto Night", un algoritmo di tipo Proof-of-Work progettato per funzionare su CPU di PC "normali", disincentivando l'utilizzo di GPU o hardware specializzato ASIC.

8.6 S&P500

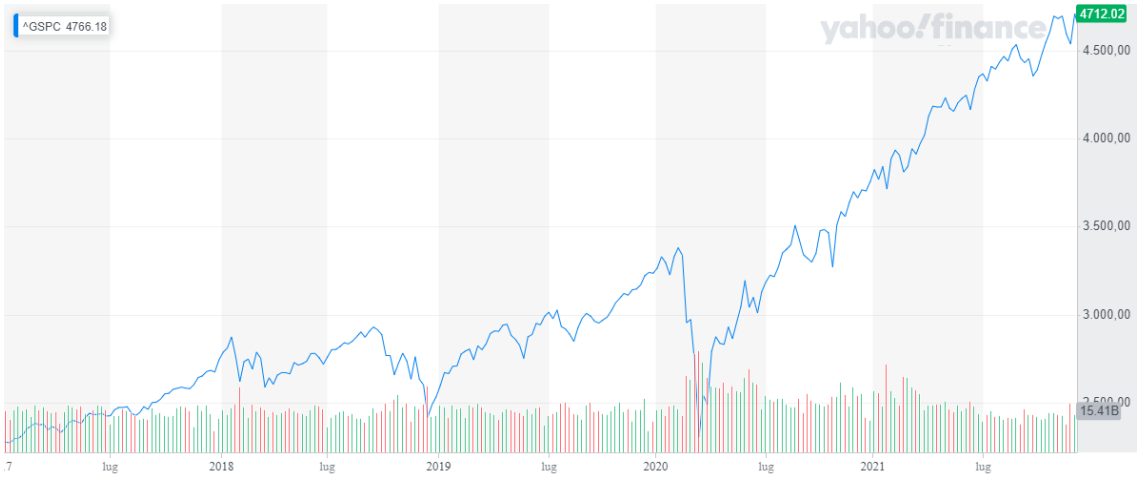


Figura 8.8. *Prezzo dell'indice S&P500. Fonte "https://it.finance.yahoo.com/".*

Lo Standard & Poor's 500 è uno dei più importanti indici azionari nordamericani, venne creato da Standard & Poor's, società statunitense che effettuata ricerche finanziarie e analisi su titoli azionari e obbligazionari e tra le prime tre agenzie di *rating* al mondo, nel 2016 viene calcolato dal 4 marzo 1957[65] grazie alla tecnologia contemporanea.

Esso è un paniere di 500 titoli azionari di società quotate a New York, selezionato da un apposito comitato secondo determinati parametri come, ad esempio, la provenienza dagli Stati Uniti d'America, una capitalizzazione di almeno 11,2 miliardi di dollari, eccetera. Dal 2005 è stato introdotto un nuovo metodo di selezione basato sulla capitalizzazione flottante[66], questa riforma non ha causato grandi cambiamenti poiché, a differenza del contesto europeo, le aziende del suddetto indice con un flottante inferiore alla capitalizzazione totale rappresentano una minoranza non significativa. Il metodo di selezione lo contraddistingue questo indice da altri indici simili come il Fortune 500 o il Down Jones.

---

[65] Prima del 1957, vista la mancanza di tecnologie, come i calcolatori, che potessero renderne agevole il calcolo, l'indice conteneva solo 90 titoli.

[66] Il flottante fa riferimento alla parte di capitale sociale che può essere liberamente scambiata sul mercato secondario, ad esempio non vengono considerati i titoli vincolati per oltre 6 mesi, i titoli detenuti dagli Stati, da azionisti legati da patti di sindacato ecc.

I dieci titoli che raggiungono circa il 21% del totale e quindi hanno maggior peso nel paniere sono: Apple, Microsoft Corp, Amazon, Berkshire Hathaway, Johnson & Johnson, JP Morgan Chase, Facebook, Exxon Mobil, Alphabet C e Alphabet A.

8.7 Eurostoxx50

***Figura 8.9**. Prezzo dell'indice Eurostoxx50. Fonte "https://it.finance.yahoo.com/".*

È l'indice azionario che rappresenta l'andamento dei 50 titoli societari a maggiore capitalizzazione tra i paesi dell'Eurozona, comprendente una rappresentazione dei principali settori industriali della suddetta area. Venne introdotto il 26 febbraio 1998 dalla Stoxx Limited, una joint venture formata da Dow Jones & Company, Deutsche Boerse e SWX Group.

8.8 FTSE MIB

Figura 8.10. *Prezzo dell'indice FTSEMIB. Fonte "https://it.finance.yahoo.com/".*

È il più importante indice azionario della Borsa Italiana, il nome è un acronimo di "Financial Times Stock Exchange Milano Indice di Borsa".

Il paniere è composto dalle azioni delle 40 società italiane, anche nel caso abbiano la sede legale fosse all'estero, con maggiore capitalizzazione, flottante e liquidità. Le componenti vengono revisionate ogni tre mesi.

L'indice di riferimento italiano è nato nel 1992 con COMIT30, in seguito, nel 1994, la Borsa Italiana ha ottenuto i diritti sull'indice rinominandolo Mi30. Dal 2003 al 2009 è stato quotato l'indice S&P Mib, subentrando al Mib30, che in quegli anni era stato creato da una partnership tra Standard & Poor's e la Borsa Italiana, successivamente è stato sostituito dal primo giugno 2009 dall'indice FTSE MIB. Quest'ultimo è stato utilizzato in seguito alla creazione della holding "London Stock Exchange Group", ovvero l'aggregazione della Borsa Italiana e la Borsa di Londra.

8.9 NASDAQ composite

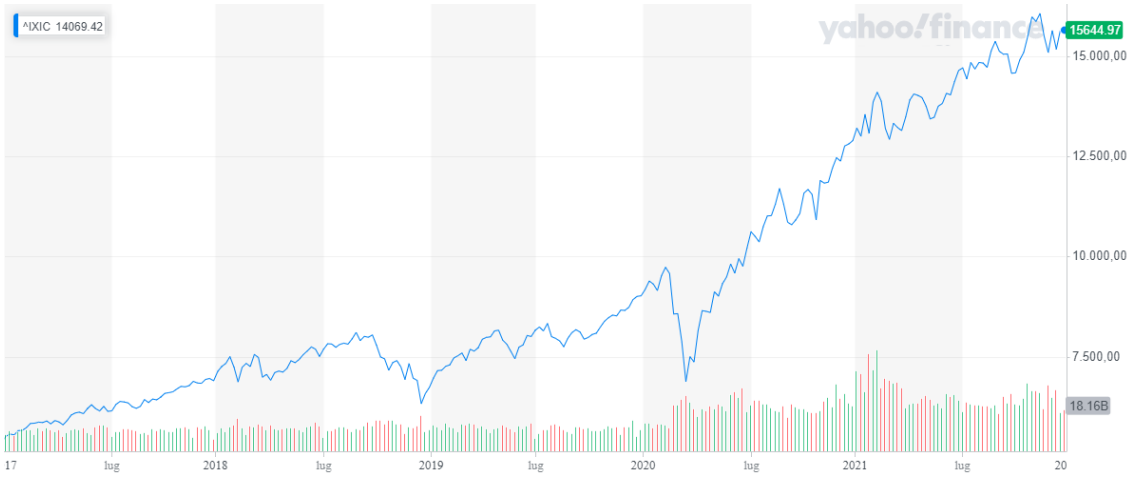


Figura 8.11. *Prezzo dell'indice Nasdaq. Fonte "https://it.finance.yahoo.com/".*

È un indice composto da più di 3000 titoli quotati sul mercato azionario NASDAQ. Il NASDAQ, acronimo di National Association of Securities Dealers Automated Quotation, è l'indice dei principali titoli tecnologici della borsa americana, tra titoli possiamo trovare Microsoft, Apple, Facebook Amazon eccetera. Questa borsa valori è stata istituita a New York il 5 febbraio 1971, in un primo momento era solo un sistema di quotazione e non forniva gli strumenti per eseguire delle operazioni. Successivamente il NASDAQ ha preso in carico tutte le operazioni che fino ad allora erano state eseguite *over the counter*, nonostante ci siano comunque ancora titoli che vengono negoziati in tal modo.

Nel 1998 il NASDAQ è diventato il primo mercato azionario degli Stati Uniti a fare trading online, lo slogan di tale operazione è stato "the stock market for the next hundred years", a sottolineare l'importanza ottenuta da questo mercato.

Il NASDAQ composite è un indice ponderato per la capitalizzazione, il calcolo di questo indice è basato sulla somma pesata dei prodotti delle quotazioni di chiusura dei titoli, tale somma viene divisa per un fattore al fine di ridurne l'ordine di grandezza. Le componenti dell'indice vengono selezionate sulla base di vari parametri, ad esempio l'essere quotati esclusivamente sul mercato borsistico NASDAQ.

8.10 CAC 40

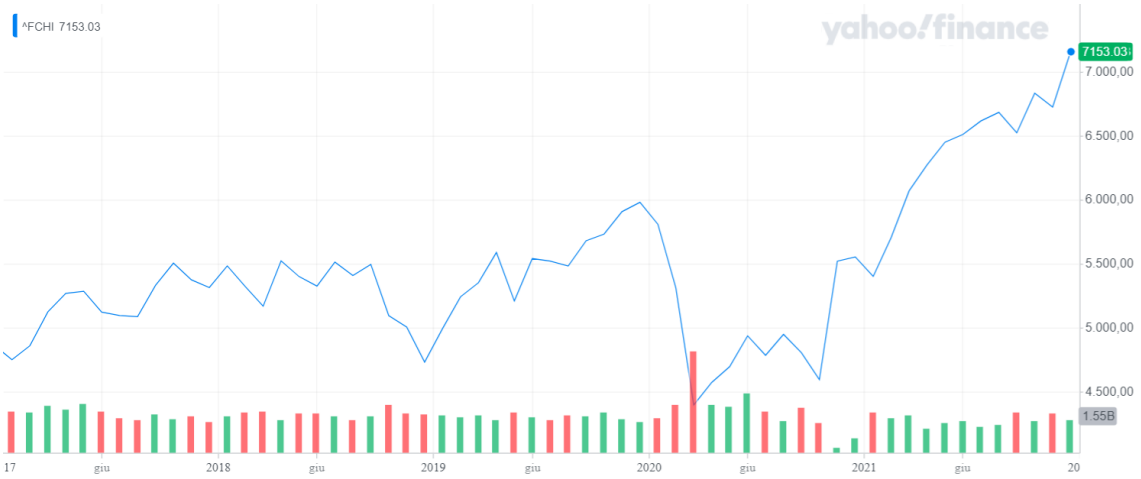


Figura 8.12. *Prezzo dell'indice CAC 40. Fonte "https://it.finance.yahoo.com/".*

È il principale indice della borsa francese e tra i principali in Europa, comprende i 40 titoli francesi o esteri, quotati presso la Euronext, con la maggiore capitalizzazione flottante.
Dal 2003 viene costruito il paniere di 40 titoli da un elenco di titoli a maggior capitalizzazione flottante della Borsa di Parigi. Anche in questo caso per la selezione dei titoli sono imposti una serie di vincoli per la selezione.
Tra i principali titoli del paniere sono compresi: LVMH, L'Oreal, Carrefour, ecc.

9 ANALISI DEI DATI

Degli indici e delle criptovalute sono state raccolte le serie storiche di dati, principalmente dal sito "Yahoo Finance"[67]: per ogni serie è stato preso in considerazione il valore di chiusura del mercato tra i valori possibili.

Sulla base delle serie storiche sono stati calcolati i log-rendimenti:

$$log\left(\frac{P_t}{P_{t-1}}\right) \tag{9. 1}$$

Il termine al numeratore è la quotazione all'istante t, invece a denominatore è presente la quotazione al periodo t-1.

Secondo la letteratura, in particolare "The Econometrics of Financial Markets" Campbell, Lo e MacKinlay[68], ci sono, in particolare, due ragioni per preferire l'utilizzo dei rendimenti anziché dei prezzi: la prima ragione è legata alla chiarezza informativa dei rendimenti. In secondo luogo, le serie dei rendimenti sono più facilmente gestibili, rispetto a quelle dei prezzi, poiché dotate di proprietà statistiche particolari come la stazionarietà e la ergodicità[69].

[67] Yahoo Finanza - Mercato azionario in tempo reale, quotazioni e notizie di economia e finanza. 2021. @yahoo_italia, https://it.finance.yahoo.com/ .

[68] Campbell, John Y., Lo, Andrew W. and MacKinlay, A. Craig. *The Econometrics of Financial Markets*. Princeton: Princeton University Press, 2012. https://doi.org/10.1515/9781400830213.

[69] Proprietà statistica di un processo aleatorio, che indica una certa regolarità in media del processo stesso. (Treccani.it, 2012).

9.1 Mercato efficiente

In questo capitolo sono presentati i concetti della teoria alla base dell'efficienza del mercato e le relative espressioni fondamentali

Quando si analizza il concetto di efficienza dei mercati finanziari si fa riferimento a tre concetti fondamentali:

1. Efficienza allocativa-funzionale: questo aspetto riguarda la capacità di trasferire le risorse finanziarie e i rischi così da raggiungere gli obiettivi in modo ottimale dai diversi operatori del mercato. Il mercato stabilisce il prezzo delle attività in base al flusso dei rendimenti attesi in futuro e del loro rischio intrinseco. Relativamente a questo concetto di efficienza è collegata la capacità del mercato di offrire ai diversi operatori la quantità e il tipo di beni desiderati in ogni circostanza futura, tramite lo smobilizzo delle attività possedute o l'impegno a consegnare attività in futuro quando ricorrano specifiche condizioni. Questa caratteristica dell'efficienza del mercato vien definita *full-insurance efficency. (Varetto, slide "Mercati e strumenti finanziari").*
2. Efficienza tecnico-operativa: questa caratteristica è legata alla capacità del mercato di funzionare con i costi di transazione minimi, in tempi brevi e riuscendo a soddisfare gli ordini di vendita e acquisto di qualunque importo. *(Varetto, slide "Mercati e strumenti finanziari").*
3. Efficienza informativa: questo tipo di efficienza concerne la capacità del mercato di raccogliere, analizzare e diffondere le informazioni rilevanti per gli operatori che effettuano gli scambi. In questo genere di contesto è impossibile poter guadagnare dagli scambi decisi analizzando le informazioni pubbliche e quindi disponibili a tutti. La possibilità di guadagno nasce dal possesso di informazioni private, coloro che ne dispongono sono chiamati *Insider*, e in questa circostanza l'efficienza informativa risulta particolarmente fondamentale. *(Varetto, slide "Mercati e strumenti finanziari").*

Per quanto riguarda la teoria dell'economia generale, il concetto di efficienza è stato identificato con l'ipotesi della concorrenza perfetta, ovvero da uno stato di assenza di costi di transazione e di altre imperfezioni del mercato e dall'impossibilità degli operatori di poter

influenzare la formazione dei prezzi e dal poter guadagnare con dei tassi superiori a quelli del profitto normale.

La teoria dell'economia finanziaria si è formata sulla base dell'ipotesi fondamentale che l'informazione sia istantaneamente disponibile a tutti gli operatori e che sia distribuita in modo uniforme tra di loro, questo concetto è riassumibile nell'idea della "informazione perfetta": ogni operatore ottiene le stesse informazioni nello stesso momento senza distinzioni.

Dall'idea di informazione perfetta deriva che l'equilibrio competitivo del mercato riconosce la possibilità di ottenere l'allocazione ottimale delle risorse, dal punto di vista dell'economia del benessere. I prezzi assumono il ruolo fondamentale di punto di riferimento per le decisioni allocative dei risparmiatori, imprese e operatori del mercato. Riassumendo è possibile affermare che le decisioni vengono prese sulla base dei prezzi osservati sul mercato.

I prezzi assumono il ruolo di aggregatori di informazioni, le quali sono disperse tra i vari operatori, e agiscono nel modo più efficiente possibile.

L'incertezza, nella condizione in cui essa sia comune a tutti gli operatori, aumenta la complessità del processo di decisione e allocazione delle risorse senza però alterarne le conclusioni di fondo.

La presenza di differenze sistematiche, non transitorie, nelle quantità e qualità dell'informazione tra i vari operatori ha la possibilità di far crollare le conclusioni dell'economia finanziaria neoclassica e influenzano l'allocazione delle risorse, derivante da un processo di ricerca dell'equilibrio di mercato, rendendola non ottimale. L'esistenza di informazioni asimmetriche tra gli operatori appartiene a quest'ultima eventualità e implica una violazione radicale dell'ipotesi dei mercati efficienti.

La relazione tra informazione ed efficienza del mercato è stata al centro di numerose analisi teoriche ed econometriche, nella maggior parte dei casi focalizzate sullo studio del comportamento dei prezzi e dei rendimenti azionari.

L'economia finanziaria ha evidenziato come in un mercato efficiente i movimenti dei prezzi siano casuali. Questa casualità ha creato una percezione del mercato finanziario simile a quella di un casinò, in cui l'investimento in titoli è paragonabile al gioco d'azzardo e gli investitori diventano dei semplici giocatori, le cui perdite e profitti sono dovuti solamente alla fortuna.

L'economia finanziaria, dopo il susseguirsi di studi e teorie, è giunta alla conclusione che in un mercato efficiente i prezzi delle attività si muovono in modo causale. La casualità dei

movimenti dei prezzi sarebbe la dimostrazione di un mercato finanziario che elabora in modo efficiente l'informazione disponibile agli operatori, i prezzi quindi riflettono le valutazioni e analisi effettuate dagli operatori e il peso e significato che attribuiscono alle informazioni disponibili. In questo contesto teorico le variazioni dei prezzi del mercato sarebbe causate unicamente scoperta di nuove informazioni, ma il processo di rivelazione di queste nuove informazioni è causale per definizione, se l'arrivo di nuove informazioni non fosse causale e quindi prevedibile in qualche modo, quest'ultime sarebbero anticipate dagli operatori stessi e quindi incluse nella formazione dei prezzi, perdendo di fatto la caratteristica di novità, in quanto le informazioni veramente nuove non possono essere anticipate dagli operatori. In conclusione, se i prezzi di un mercato efficiente si modificano solo in base alla scoperta di nuove informazioni, se esse si manifestano secondo una sequenza casuale allora le variazioni dei prezzi devono essere casuali.

Eugene Fama, Professore di finanza alla scuola economica di dell'università di Chicago, è lo studioso che per definizione viene accostato allo studio dell'efficienza dei mercati. Nel gennaio 1965 venne pubblicato sul "Journal of Business"[70] la tesi di dottorato di Fama intitolata "The Behavior of Stock Market Prices"[71]. Nella sua tesi l'autore, sosteneva che dato l'utilizzo di una grande quantità di risorse da parte di società che operavano nel settore del *brokeraggio* con lo scopo di effettuare analisi sui trend nell'industria, sugli effetti delle variazioni dei tassi, sui bilanci delle aziende eccetera, gli analisti delle società avrebbero dovuto avere la capacità di battere un generico portafoglio titoli con le stesse caratteristiche di rischio.

Nella tesi si afferma che in qualunque situazione l'analista ha il cinquanta percento di probabilità di battere il mercato e, soprattutto, non avrebbe la possibilità di batterlo sistematicamente. Secondo l'autore, l'analista contribuisce a mantenere il mercato efficiente: ipotizzando una situazione in cui tutti gli investitori detenessero un portafoglio costituito da indici azionari, si creerebbero delle opportunità per i traders professionisti per ottenere dei vantaggi da quella situazione. Ma sarebbe proprio un eventuale movimento dei traders verso

---

[70] Rivista accademica, pubblicata dall'università di Chicago, specializzata in tutti i campi accademici legati all'economia.

[71] Fama, Eugene F. "The Behavior of Stock-Market Prices." *The Journal of Business* 38, no. 1 (1965): 34–105. http://www.jstor.org/stable/2350752.

tali opportunità a fare scomparire il vantaggio, confermando quindi la "Teoria dei mercati efficienti" di E.Fama.

Le teorie di Fama confermavano le famose "Random Walk Theory" dei prezzi azionari, introdotte con Louis Bachelier[72] e sviluppate in ultima analisi da Paul Samuelson[73] nel 1965. Fama, con i suoi articoli, aggiunse a queste teorie un approccio più rigoroso dal punto di vista statistico-matematico definendo così una rivoluzione nell'ambito della finanza.

Il *Journal of Finance* nel 1970 pubblicò un articolo di E.Fama intitolato "Efficient Capital Markets: A Review of Theory and Empirical Work"[74], in cui l'autore ha formalizzato la famosa definizione di mercato finanziario efficiente: un mercato finanziario in cui i prezzi riflettono sempre pienamente le informazioni disponibili è definito efficiente.

Per comprendere al meglio la definizione di Fama e renderla operativamente verificabile sul piano empirico, si rende necessario precisare i due concetti fondamentali: l'informazione disponibile e pienamente incorporati. È possibile sviluppare ciò utilizzando un approccio classico facendo riferimento agli *excess return:*

- ε_{t+1} : excess return.
- Φ_t : insieme delle informazioni disponibili agli operatori al tempo t.
- P_t : prezzo al tempo t.
- $E[P_t]$: prezzo atteso al tempo t.
- r_{t+1}: rendimento al tempo t+1.

[72] Matematico e statistico francese, famoso per i suoi studi sui processi stocastici "Moti Browniani" e la loro applicazione per la valutazione delle *stock option*, per questi motivi è considerato il padre della matematica finanziaria.

[73] Economista statunitense che contribuì alla formazione della "Efficient Market Hypothesis", in particolar modo con l'articolo "Proof that Properly Anticipated Prices Fluctuate Randomly".

[74] Fama, Eugene F. "Efficient Capital Markets: A Review of Theory and Empirical Work." *The Journal of Finance* 25, no. 2 (1970): 383–417. https://doi.org/10.2307/2325486.

$$\varepsilon_{t+1} = \frac{P_{t+1} - P_t}{P_t} - \frac{E[P_{t+1}|\Phi_t] - P_t}{P_t} = \frac{P_{t+1} - E[P_{t+1}|\Phi_t]}{P_t}$$

(9. 2)

$$\varepsilon_{t+1} = r_{t+1} - E[r_{t+1}|\Phi_t] = ex\ ante - ex\ post$$

(9. 3)

Se Φ_t è completamente incluso nei prezzi attesi allora risulta impossibile progettare una strategia di investimento finanziario che abbia un *excess return* atteso maggiore di zero. Nel caso in cui Φ_t contenesse le informazioni necessarie per ottenere un rendimento in eccesso atteso in t+1 allora quella informazione sarebbe già inclusa nel prezzo di P_t e non in P_{t+1}.
E.Fama ha formalizzato il concetto di "informazione completamente incorporata nei prezzi" attraverso tre modelli:

1. Modello del Fair-Game: secondo questo modello l'aspettativa su ε_{t+1} , ovvero il rendimento atteso in eccesso, viene specificata in modo diretto senza alcuna considerazione sul modello che genera i rendimenti attesi. Nel modello viene esplicitato che nel lungo periodo gli scostamenti tra i rendimenti effettivi e quelli attesi sono nulli; perciò, risulta che le informazioni comprese in Φ_t non sono utili al fine di generare rendimenti attesi in eccesso sistematicamente positivi.

$$E[\varepsilon_{t+1}|\Phi_t] = 0$$

(9. 4)

2. Modello Martingala: con questo approccio vengono analizzate e modellate le proprietà statistiche delle serie temporali dei prezzi o rendimenti azionari. Secondo questo modello l'uso efficiente delle informazioni sottende che il prezzo atteso futuro sia pari al prezzo corrente P_t moltiplicato per (1+rendimento atteso):

$$E[P_{t+1}|\Phi_t] = P_t \cdot (1 + E[r_{t+1}|\Phi_t])$$

(9. 5)

Perciò esplicitando il prezzo corrente P_t:

$$P_t = \frac{E[P_{t+1}|\Phi_t]}{1 + E[r_{t+1}|\Phi_t]}$$

(9. 6)

Perciò il prezzo corrente corrisponde al valore attuale del futuro prezzo atteso $E[P_{t+1}|\Phi_t]$, scontato al tasso di rendimento atteso congruo per il rischio $1 + E[r_{t+1}|\Phi_t]$, chiamato *properly discounted*. Questo è anche la definizione stessa di un processo statistico Martingala, ovvero un processo definito secondo le proprie osservazioni passate. Secondo la definizione, una variabile statistica segue un processo dinamico Martingala rispetto a Φ se il valore attesa futuro condizionale, data la sequenza di Φ, è pari al suo valore corrente.
La nozione generale di Martingala:

$$E[Y_{t+1}|Y_0, \dots, Y_t] = Y_t$$

(9. 7)

Ritornando alla definizione del modello applicato al prezzo o ai rendimenti azionari è possibile affermare che il prezzo atteso scontato del tasso sopracitato è una martingala, a differenza del solo prezzo atteso che non lo è.
Il solo prezzo atteso $E[P_{t+1}|\Phi_t]$ è definibile come una *Submartingala*, poiché ci si aspetta che cresca al tasso di rendimento atteso.
Un processo stocastico è un *Submartingala* se:

$$E[Y_{t+1}|Y_0, \dots, Y_t] > Y_t$$

(9. 8)

3. Modello Random Walk: con questo approccio è definita l'intera forma della distribuzione statistica dei rendimenti in eccesso, a differenza dei due approcci precedentemente illustrati che specificano solo il valore atteso e non consideravano gli altri momenti della distribuzione. Il susseguirsi delle variazioni dei prezzi segue un processo *random walk* se sono identicamente e indipendentemente distribuite (I.I.D).

   È necessario chiarire che dal punto di vista economico l'ipotesi del *random walk* non implica che le variazioni successive dei prezzi siano puramente casuali, ovvero senza ragione economica. I prezzi variano poiché lo stato delle cose varie continuamente: l'impresa si evolve, le condizioni ambientali cambiano e di conseguenza cambia anche la percezione degli operatori e le loro valutazioni a riguardo delle caratteristiche dell'impresa. Perciò è possibile quindi affermare che la conoscenza degli operatori è in continua evoluzione a causa dell'arrivo di nuove informazioni e la revisione del contenuto di quelle passate. Quindi l'ipotesi del *random walk* afferma dato un certo istante, la variazione dei prezzi nel momento successivo è casuale allo stato delle informazioni in quel momento. Il prezzo attuale riflette in modo completo lo stato attuale della conoscenza delle informazioni, cioè corrisponde al valore attuale atteso della media della distribuzione dei prezzi del prossimo periodo considerando le informazioni date oggi.

   I processi *random walk* sono detti *memoryless* (senza memoria), ciò significa che la conoscenza degli stati passati del sistema non è utile per fare delle previsioni sugli stati futuri: tale proprietà, nel contesto di prezzi e rendimenti azionari, comporta che la conoscenza dei prezzi passati e dei rendimenti passati non è utilizzabile per predire prezzi e rendimenti futuri.

   In termini statistici con il modello del *random walk* il rendimento atteso è costante ed il rendimento atteso in eccesso ha media nulla, con identica varianza e altri momenti superiori in ciascun periodo futuro, ovvero la funzione di densità

$f(\varepsilon_{t+1})$ è identica per ogni t. Il rendimento atteso è il *drift* (deriva) del processo *random walk*, ovvero l'elemento la cui presenza implica che la media degli incrementi sia diversa da 0.

Se il processo di formazione dei prezzi segue un *random walk* implica che il valore atteso dei *capital gains* è nullo, perciò l'unico determinante del valore atteso delle quotazioni azionarie è il valore attuale del flusso di dividendi pagati dalle imprese ed ai suoi determinanti.

Formalizzando il concetto di "informazione disponibile", E.Fama ha teorizzato tre forme di efficienza del mercato basandosi sul contenuto di informazioni progressivamente crescente:

- Efficienza in forma debole (*weak form*): l'informazione è limitata alla serie storica dei prezzi azionari passati, che è il dato pubblico più diffuso e facilmente ottenibile dagli operatori. Non è possibile creare delle strategie di trading con un rendimento atteso superiore a quello del mercato basandosi solo sull'informazione contenuta nella serie storica dei prezzi.
- Efficienza in forma semi-forte (*semi-strong form*): l'informazione comprende l'insieme di tutti i dati pubblicamente disponibili, quindi sono incluse le notizie stampa, i bilanci, i dati macroeconomici, i dati finanziari, i dati di settori, ecc.
- Efficienza in forma forte (*strong form*): l'informazione comprende l'intero insieme dei dati includendo anche quelli non pubblicamente disponibili, le cosiddette *insider information*.

9.2 Modello random walk

La seguente introduzione ad alcuni modelli dei processi randomici è basata sulla trattazione del manuale di econometria "*The Econometrics of Financial Markets*", Campbell, J., Lo, A. & MacKinlay[75]. In questo capitolo si presentano una serie di modelli alla base del processo di verifica dell'efficienza di mercato degli oggetti finanziari analizzati.

[75] Campbell, John Y., Lo, Andrew W. and MacKinlay, A. Craig. *The Econometrics of Financial Markets*. Princeton: Princeton University Press, 2012. https://doi.org/10.1515/9781400830213.

Nel testo sono presentati tre modelli dei processi randomici:

- *Randomwalk 1: IZD increments.*
- *Randomwalk 2: indepent increments.*
- *Randomwalk 3: uncorrelated increments*.

Per lo sviluppo di questo elaborato si è deciso di trattare e verificare solamente il primo modello: *Randomwalk 1*. Utilizzando questo modello si cerca di verificare l'efficienza debole del mercato delle criptovalute e degli indici di borsa.

Nella forma più semplice del modello del Random walk si assume che gli incrementi siano indipendenti e identicamente distribuiti (IID), in questo caso la dinamica di p_t segue l'espressione:

$$p_t = \mu + p_{t-1} + \varepsilon_t \qquad \varepsilon_t \sim I.I.D.(0, \sigma^2)$$

(9. 9, 9.10)

Dove μ è il rendimento atteso[76] e ε_t è l'incremento al tempo t. L'espressione $I.I.D.(0, \sigma^2)$ evidenzia che ε_t sono indipendenti e identicamente distribuiti con media pari a 0 e varianza pari a σ^2.
L'indipendenza non implica solamente l'assenza di correlazione tra gli incrementi, ma anche qualunque funzione non lineare applicata agli incrementi.

[76] Definito anche *drift*.

9.3 Random walk: unit Root test-test Dickey-Fuller

Per verificare l'ipotesi del random walk, tra le possibili alternative, è stato scelto di utilizzare test del tipo "Unit Root Test" per andare a testare la non stazionarietà delle serie temporali, condizione necessaria per un processo random walk.

$$X_t = \mu + X_{t-1} + \epsilon_t$$

(9. 11)

$$Y_t = \phi Y_{t-1} + \mu + \epsilon_t$$

(9. 12)

Per verificare che Y_t ha una radice è necessario che ϕ=1. Di seguito è presentata l'ipotesi nulla:

$$\begin{cases} H_0 : \phi = 1 \\ H_1 : \phi \neq 1 \end{cases}$$

(9. 13)

Tale modello di solito è parametrizzato nel seguente modo:

$$Y_t - Y_{t-1} = \phi Y_{t-1} - Y_{t-1} + \mu + bt + \epsilon_t$$

(9. 14)

$$Y_t - Y_{t-1} = (\phi - 1) Y_{t-1} + \mu + bt + \epsilon_t$$

(9. 14)

Dato $\gamma = \phi$-1 è possibile riscrivere l'espressione come:

$$\Delta Y_t = \gamma Y_{t-1} + \mu + bt + \epsilon_t$$

(9. 15)

Questa parametrizzazione permette di effettuare il test di Dickey-Fuller, che rientra nella categoria dei test di radici unitarie, per valutare l'esistenza di un trend nelle variabili della regressione.

L'ipotesi nulla da verificare diventa:

$$\begin{cases} H_0: \gamma = 0 \\ H_1: \gamma \neq 0 \end{cases}$$

(9. 16)

Per valutare l'efficienza del mercato delle criptovalute si è deciso di applicare un modello di regressione lineare semplice:

$$Y_t = \beta_0 + \beta_1 Y_{t-1} + \varepsilon$$

(9. 17)

Dove la Y_t corrisponde all'osservazione del log-rendimento al tempo t e β_1 è la pendenza della retta di regressione.

Mentre $\beta_0$rappresenta l'intercetta della retta di regressione, l'ultimo termine dell'espressione, ε, indica l'errore di regressione, questo fattore include varie distorsioni che possono influenzare il valore della Y, in particolare i fattori omessi, ovvero altri fattori diversi dalla variabile X che influenzano il valore della Y.

L'espressione della ipotesi nulla del test può essere formulata nel seguente modo:

$$\begin{cases} H_0: \beta_1 = 0 \\ H_1: \beta_1 \neq 0 \end{cases}$$

(9. 18)

Se non è possibile rifiutare l'ipotesi nulla, $\beta_1 = 0$, il termine autoregressivo ha radice unitaria, e quindi si avrebbe la conferma del *random walk* del processo in esame. Alla luce di questi risultati si andrebbe a verificare l'efficienza debole del mercato. Inoltre, viene effettuato un controllo della significatività tramite il calcolo della statistica t pari a $t = \frac{\beta_1 - \widehat{\beta_1}}{Errorestandard}$, con $\widehat{\beta_1}$ pari a 0.

Per effettuare il test si è deciso di analizzare, oltre al valore del coefficiente β_1 , anche il valore del coefficiente di determinazione lineare, R^2 , un indice che misura il legame tra la variabilità dei dati e il modello statistico utilizzato. R^2 rappresenta la frazione variabilità di Y spiegata dalla variabile X, dal punto di vista matematico è definita dalla seguente espressione:

$$R^2 = 1 - \frac{RSS}{TSS} = 1 - \frac{\sum_{i=1}^{n}(y_i - \hat{y})^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2}$$

(9. 19)

È nota anche una ulteriore espressione di R^2:

$$R^2 = \frac{ESS}{TSS} = \frac{\sum_{i=1}^{n}(\hat{y_i} - \bar{y})^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2}$$

(9. 20)

L'espressione a numeratore, ESS [77] , indica la devianza spiegata dal modello, invece l'espressione a denominatore, TSS[78], rappresenta la devianza totale.
Analizzando il valore di R^2, applicato al modello di regressione descritto in precedenza, è possibile dedurre la correlazione tra i log-rendimenti al tempo t e al tempo t-1. Secondo la teoria del mercato efficiente, queste due variabili non dovrebbero essere correlate, quindi il valore target del test è di R^2 pari a 0 o comunque tendente a tale valore.

9.4 Verifica dell'efficienza debole

In questa sezione vengono presentati i risultati dell'applicazione del modello e del test, descritto in precedenza, per verificare che le serie storiche dei dati delle criptovalute rispettano l'efficienza in forma debole del mercato.

[77] *Explained Sum of Squares*

[78] *Total Sum of Squares*

I risultati dell'analisi di regressione, effettuata tramite il software *Excel*, sono presentanti in una tabella contenente i valori più significativi.

Durante l'analisi di regressione e del test sono state fatte alcune assunzioni:

1. È stato considerato un Lag temporale di un periodo, nel caso in esame di 1 giorno. Si studia la correlazione tra il log-rendimento al tempo t e al tempo t-1.
2. È stato scelto un livello di significatività pari a α=5%.

Analisi efficienza del mercato: Bitcoin

I dati presi in considerazione fanno riferimento al periodo 31/12/2016 al 31/12/2021, con 1827 osservazioni.

Tabella 9.1.

Bitcoin	**Intercetta**	Y_{t-1}
Coefficienti	0.00216964	-0.03152094
Errore standard	0.00099077	0.02340703
Stat t	2.18985568	-1.34664419
Valore di significatività	0.02866104	0.17826225
R al quadrato	0.00099377	
R al quadrato corretto	0.00044577	

Dai risultati dell'analisi di regressione effettuata tramite il software *Excel*, è possibile verificare se Bitcoin rispetta il grado di efficienza debole.

In primo luogo, si può notare che il valore del coefficiente, che nell'espressione precedente abbiamo indicato come β_1, è assimilabile al valore nullo. Questa conclusione viene verificata anche dal valore di significatività, detta anche *p-value*, che assume un valore di circa 17,83%, sicuramente maggiore rispetto al livello di confidenza del 5%, permettendoci di affermare di non poter rifiutare l'ipotesi che il valore del coefficiente sia nullo.

Analizzando l'R^2 si può constatare come anch'esso sia prossimo allo zero, il che implica l'assenza di correlazione tra i rendimenti in t e in t-1.

Considerando, dunque, questi risultati è possibile affermare che il processo è a radice unitaria, quindi i log-rendimenti nei due periodi considerati non sono correlati, confermando l'ipotesi di un grado di efficienza debole del mercato.

Analisi efficienza del mercato: Ethereum

I dati presi in considerazione fanno riferimento al periodo 9/11/2017 al 31/12/2021, con 1514 osservazioni. La data di riferimento iniziale è la prima in cui sono disponibili le osservazioni del prezzo per questa criptovaluta.

Tabella 9.2.

Ethereum	**Intercetta**	Y_{t-1}
Coefficienti	0.001743262	-0.051339801
Errore standard	0.001353042	0.025684939
Stat t	1.288401823	-1.998829024
Valore di significatività	0.197803502	0.045805837
R al quadrato	0.002638923	
R al quadrato corretto	0.001978419	

Nel caso di Ethereum, il valore del coefficiente β_1 risulta maggiore rispetto al caso di Bitcoin, e il valore del p-value risulta essere minore del valore livello di confidenza usato nel test, 4.58%<5%, quindi non possiamo accettare l'ipotesi nulla e affermare che il valore del coefficiente sia pari a 0.

Considerando il valore di R^2, 0.002638923, si potrebbe affermare una possibile approssimazione al valore zero e quindi l'assenza di correlazione tra i log-rendimenti in t e in t-1.

Perciò se si considerasse il solo test sul valore di R^2 sarebbe possibile affermare l'efficienza debole della valuta digitale Ethereum.

Analisi efficienza del mercato: Binance Coin

I dati presi in considerazione fanno riferimento al periodo 9/11/2017 al 31/12/2021, con 1514 osservazioni. La data di riferimento iniziale è la prima in cui sono disponibili i dati per questa criptovaluta.

Tabella 9.3.

Binance Coin	**Intercetta**	Y_{t-1}
Coefficienti	0.00373938	-0.00039725
Errore standard	0.00161168	0.02571041
Stat t	2.32016711	-0.01545101
Valore di significatività	0.02046457	0.98767441
R al quadrato	0.00000016	
R al quadrato corretto	-0.00066209	

In questo caso la tendenza verso il valore nullo del valore del coefficiente del termine autoregressivo è evidente, sia per il valore assoluto del coefficiente, sia per del *p-value* di circa il 99%.

il valore di R^2, dato il suo valore significativamente basso, è praticamente approssimabile al valore zero.

In virtù di questi risultati è possibile concludere che l'efficienza debole della valuta virtuale Binance Coin.

Analisi efficienza del mercato: Litecoin

I dati presi in considerazione fanno riferimento al periodo 31/12/2016 al 31/12/2021, con 1827 osservazioni.

Tabella 9.4.

Litecoin	**Intercetta**	Y_{t-1}
Coefficienti	0.00193703	-0.01545040
Errore standard	0.00142934	0.02341581
Stat t	1.35519767	-0.65982745
Valore di significatività	0.17552248	0.50944791
R al quadrato	0.00023876	
R al quadrato corretto	-0.00030965	

I risultati dell'analisi di regressione, per l'applicazione del test di Dickey-Fuller, sono molto simili a quelli di Bitcoin. Il valore di β_1 è assimilabile allo zero, inoltre considerando il valore di significatività, pari a circa il 51%, si esclude la possibilità di poter rifiutare l'ipotesi nulla $\beta_1 = 0$.

Il valore di R^2 è prossimo al valore nullo confermando, quindi, la non correlazione tra i log-rendimenti in t e t-1.

È possibile concludere, alla luce dei risultati esposti, che Litecoin rispetta un grado di efficienza debole dei mercati.

Analisi efficienza del mercato: Monero.

I dati presi in considerazione fanno riferimento al periodo 9/11/2017 al 31/12/2021, con 1514 osservazioni. La data di riferimento iniziale è la prima data in cui sono disponibili i dati per questa criptovaluta.

Tabella 9.5.

Monero	**Intercetta**	Y_{t-1}
Coefficienti	0.00057413	-0.15133664
Errore standard	0.00143917	0.02538949
Stat t	0.39893241	-5.96060091
Valore di significatività	0.68999942	0.00000000
R al quadrato	0.02298810	
R al quadrato corretto	0.02234107	

il valore del coefficiente β_1 assume il valore più alto tra le criptovalute analizzate, inoltre se si considerasse il valore di significatività, che assume un valore quasi nullo, non si può accettare l'ipotesi nulla che β_1 sia pari a zero.

Il valore di R^2, nonostante anch'esso sia il valore maggiore tra le valute digitali osservate, risulta essere sufficientemente basso da poter considerare nulla la correlazione tra i log-rendimenti in t e t-1.

In conclusione, considerando il valore di R^2, seppur con le dovute considerazioni, è possibile affermare che è stata verificata l'efficienza debole di Monero.

Analisi efficienza del mercato: S&P500

I dati presi in considerazione fanno riferimento al periodo 31/12/2016 al 31/12/2021, con 1259 osservazioni.

Tabella 9.6.

S&P500	**Intercetta**	Y_{t-1}
Coefficienti	0.00073647	-0.24036648
Errore standard	0.00033447	0.02741018
Stat t	2.20192107	-8.76923970
Valore di significatività	0.02785242	0.00000000
R al quadrato	0.05778014	
R al quadrato corretto	0.05702877	

Il valore del coefficiente β_1 non è particolarmente basso da poter affermare che può essere assimilabile al valore zero, osservando il valore di significatività e confrontandolo con il livello di confidenza, 0.057780141<0.05 è evidente che non si può accettare l'ipotesi nulla.

Il valore di R^2 non è estremamente basso, ma, con le dovute accortezze, possiamo considerarlo sufficientemente basso da approssimarlo al valore zero per poter affermare l'assenza di correlazione tra i log-rendimenti in t e t-1. Tenendo in considerazione l'R^2, è possibile verificare l'ipotesi di efficienza debole dell'indice S&P500.

Analisi efficienza del mercato: Eurostoxx50

I dati presi in considerazione fanno riferimento al periodo 31/12/2016 al 31/12/2021, con 1255 osservazioni.

Tabella 9.7.

Stoxx50	**Intercetta**	Y_{t-1}
Coefficienti	0.00021384	-0.02781354
Errore standard	0.00033380	0.02826382
Stat t	0.64062988	-0.98406885
Valore di significatività	0.52188051	0.32527194
R al quadrato	0.00077350	
R al quadrato corretto	-2.5247E-05	

Il valore del coefficiente del termine di autoregressione β_1 risulta tendente al valore nullo, per verificare tale ipotesi è necessario osservare il valore del p-value, il quale risulta essere molto superiore al valore soglia del 5%. Quindi è possibile affermare che non è possibile rifiutare l'ipotesi nulla e quindi il valore del coefficiente non è significativamente diverso da zero.
Il valore di R^2 , praticamente approssimabile al valore zero, conferma l'ipotesi descritta in precedenza, perciò è possibile affermare che il processo è a radice unitaria e la correlazione tra i log-rendimenti al tempo t e t-1 è nulla. Con questo test è stata verificata il grado di efficienza debole per l'indice di Eurostoxx50.

Analisi efficienza del mercato: FTSEMIB

I dati presi in considerazione fanno riferimento al periodo 31/12/2016 al 31/12/2021, con 1269 osservazioni.

Tabella 9.8.

FTSEMIB	**Intercetta**	Y_{t-1}
Coefficienti	0.00028344	-0.07376830
Errore standard	0.00037760	0.02803947
Stat t	0.75063165	-2.63087305
Valore di significatività	0.45301397	0.00862006
R al quadrato	0.00544176	
R al quadrato corretto	0.00465555	

Il valore del coefficiente β_1 sembra apparentemente prossimo allo zero, ma il valore di significatività è minore del livello di confidenza α=5%, perciò non è possibile accettare l'ipotesi nulla per cui β_1 dovrebbe essere significativamente uguale a zero.

Il valore assunto da R^2 è tale da poterlo assimilare al valore nullo; perciò, si può affermare che la correlazione tra i log-rendimenti in t e in t-1 non sia presente.

Il valore di R^2 permette quindi di effettuare una veloce verifica del rispetto del grado di efficienza debole dell'indice FTSEMIB.

Analisi efficienza del mercato: NASDAQ

I dati presi in considerazione fanno riferimento al periodo 31/12/2016 al 31/12/2021, con 1258 osservazioni.

Tabella 9.9.

NASDAQ	**Intercetta**	Y_{t-1}
Coefficienti	0.00103024	-0.22346641
Errore standard	0.00037958	0.02752152
Stat t	2.71418861	-8.11969831
Valore di significatività	0.00673492	0.00000000
R al quadrato	0.04994926	
R al quadrato corretto	0.04919164	

In questo caso il valore del coefficiente β_1, come nel caso di S&P500, assume un valore che non consente una approssimazione al valore zero immediata. Il valore del p-value tendente allo zero dimostra come non possiamo accettare l'ipotesi nulla che β_1 sia pari a zero.

R^2 assume un valore non estremamente basso, ma è possibile considerarlo comunque sufficiente per poter considerare la correlazione tra i log-rendimenti in t e in t-1 non correlati.

Anche nel caso dell'indice Nasdaq è possibile affermare che è verificata l'efficienza debole.

Analisi efficienza del mercato: CAC40

I dati presi in considerazione fanno riferimento al periodo 31/12/2016 al 31/12/2021, con 1280 osservazioni.

Tabella 9.10.

CAC	**Intercetta**	Y_{t-1}
Coefficienti	0.00029850	-0.00058329
Errore standard	0.00032939	0.02799397
Stat t	0.90622100	-0.02083624
Valore di significatività	0.36498998	0.98337954
R al quadrato	3.40242E-07	
R al quadrato corretto	-0.00078336	

Il valore assunto dal coefficiente β_1 è approssimabile al valore nullo, per confermare questa ipotesi è necessario osservare il valore del p-value, il quale risulta molto l'oltre la soglia di non accettazione, 98%>5%, perciò non è possibile rifiutare l'ipotesi nulla, ovvero che il valore di β_1 sia significativamente uguale a zero.

Anche il valore di R^2 , praticamente prossimo allo zero, conferma la non correlazione tra i log-rendimenti in t e in t-1, perciò si conferma che il processo sia a radice unitaria.

I risultati dimostrano che il grado di efficienza debole per l'indice CAC è stato verificato.

9.5 Modello di Markowitz: selezione di portafoglio

Harry Markowitz pubblicò nel 1952 "Portfolio Selection", un articolo destinato a rivoluzionare la teoria della selezione dei portafogli finanziari[79]. Nell'articolo l'autore illustrava il metodo per poter costruire un portafoglio finanziario che fosse caratterizzato da un alto rendimento e al contempo dal valore di rischio più basso possibile, ovvero l'autore cercò di ottenere l'ottimizzazione del rendimento di un portafoglio agendo su parametri principali: il profitto e la rischiosità.

Nell'articolo si definiscono queste due grandezze dimostrando che da un punto di vista matematico-probabilistico potevano essere modellate nel seguente modo:

- il profitto del portafoglio è modellizzato tramite il valore atteso del rendimento $E[R_\Pi]$.
- Il rischio è modellizzato tramite la varianza del rendimento $Var[R_\Pi] = \sigma^2_{R_\Pi}$.

Il modello viene anche chiamato "modello media-varianza" proprio per la scelta dell'autore delle misure di profitto e rischio, la scelta è stata fatta per la semplicità di calcolo e attinenza con la realtà che modellizzano.

La teoria di Markowitz si basa sui seguenti assunti fondamentali:

- Gli investitori sono avversi al rischio e perciò cercano di minimizzare la volatilità massimizzando i rendimenti.
- Il mercato è perfettamente concorrenziale e l'asimmetria informativa è assente.
- I costi di transazione e le imposte sono trascurabili.
- Gli investitori sono razionali e avversi al rischio, il loro comportamento cerca di massimizzare la loro funzione di utilità una volta fissato un budget.
- Il portafoglio viene considerato su un unico periodo temporale, quindi l'orizzonte temporale è uniperiodale.

[79] Markowitz, Harry. "Portfolio Selection." *The Journal of Finance* 7, no. 1 (1952): 77–91. https://doi.org/10.2307/2975974.

- I rendimenti assumono una distribuzione normale e sono indipendenti e identicamente distribuiti.

Il concetto fondamentale introdotto dalla "teoria del portafoglio" di Markowitz è la correlazione possibile tra i titoli collegata alla rischiosità del portafoglio stesso, fino ad allora si erano considerati le caratteristiche dei titoli, ovvero rendimento e rischiosità, senza tenere presente i rapporti tra di essi, quindi la rischiosità di un portafoglio composto da *N* titoli diversi era calcolata semplicemente come la media ponderata delle rischiosità di ogni titolo. Markowitz afferma che per la costruzione del portafoglio ottimo sia necessario considerare anche la correlazione tra i titoli costituenti il portafoglio e questo si riflette sulla valutazione della sua diversificazione: un portafoglio verrà considerato diversificato solo nel caso i suoi titoli non abbiano un alto grado di correlazione e quindi in questi casi si potrà ottenere "l'effetto diversificazione" tale per cui si ottiene una riduzione del rischio di portafoglio, o nel caso estremo in cui vi sia una perfetta correlazione negativa tra i titoli "l'eliminazione del rischio". Il rendimento del portafoglio composto da *N* titoli per Markowitz, quindi, dipende più dalle covarianze tra i vari titoli anziché rispetto alle varianze dei singoli titoli.
Il modello, come affermato dall'autore, si sviluppa in due fasi:

1. nella prima parte viene costruita la "frontiera efficiente", ovvero l'individuazione di quei portafogli che in termini di rendimento e varianza dominano gli altri, quindi sono ottimi paretiani.

2. Nella seconda fase, definita dall'autore soggettiva, si ricerca il portafoglio che massimizza la funzione di utilità dell'investitore e che si trova sulla frontiera efficiente individuata nella prima fase. La "soggettività" nasce dalla funzione di utilità dell'investitore che risulta essere legata alle sue decisioni.

Definizione rischio e rendimento del portafoglio

In questa sezione sono presentate le definizioni e il modello di portafoglio ottimo e di frontiera efficiente.

Dato un insieme di asset che costituiscono il portafoglio Π, e dato il rendimento dell'i-esimo asset, R_i, e il peso dell'i-esimo asset, ω_i , il valore atteso del rendimento del portafoglio, R_Π è calcolato nel seguente modo:

$$E[R_\Pi] = \sum_{i=1}^{n} \omega_i \, \mu_i$$

(9. 21)

Per i successivi passaggi è necessario definire i rendimenti e i pesi degli asset del portafoglio in forma vettoriale. Viene definito il vettore dei pesi degli asset del portafoglio $\Omega = \{\omega_i, \dots, \omega_n\}$ e il vettore dei rendimenti medi degli asset del portafoglio $\Theta = \{\mu_1, \dots, \mu_n\}$.

Il valore atteso del rendimento del portafoglio può essere riscritto nella seguente forma:

$$E[R_\Pi] = \Omega \times \Theta^T$$

(9. 22)

Con Θ^T si intende il vettore dei rendimenti medi Θ trasposto.

Per definire il rischio del portafoglio è necessario calcolarne la varianza, il primo passo è definire la matrice varianza-covarianza Σ:

$$\Sigma = \begin{bmatrix} \sigma_{11} & \cdots & \sigma_{1n} \\ \vdots & \ddots & \vdots \\ \sigma_{n1} & \cdots & \sigma_{nn} \end{bmatrix}$$

(9. 23)

- $\sigma_{ij} = Cov(R_i, R_j) = E[(R_k - \mu_k) \cdot (R_j - \mu_j)]$ sono le covarianze dei rendimenti R_i *e* R_j, rispettivamente i rendimenti del i-esimo e j-esimo asset.
- $\sigma_{ii} = Var(R_k) = \sigma_i^2$ sono le varianze del rendimento i-esimo che costituiscono la diagonale principale della matrice.

Con questi elementi è possibile definire la varianza del portafoglio:

$$Var[R_\Pi] = \sigma_\Pi^2 = \sum_{k=1}^{n} \omega_k^2 \cdot \sigma_k^2 + 2 \sum_{k<j=1}^{n} \omega_k \cdot \omega_j \cdot \sigma_{kj} = \Omega \cdot \Sigma \cdot \Omega^T$$

(9. 24)

Con Ω^T vettore dei pesi del portafoglio trasposto.

Costruzione della frontiera efficiente

Il primo passaggio nello sviluppo del modello di Markowitz è quello di costruire la frontiera efficiente, per individuarla è necessario risolvere uno dei problemi di ottimizzazione vincolata:

$$\begin{cases} \max_{\omega_1,\dots,\omega_n} E[R_\Pi] \\ \sigma_\Pi^2 = \tilde{\sigma} \\ \sum_{i=1}^{n} \omega_i = 1 \end{cases} \quad [1] \qquad \begin{cases} \min_{\omega_1,\dots,\omega_n} (\sigma_\Pi^2) \\ E[R_\Pi] = \tilde{R} \\ \sum_{i=1}^{n} \omega_i = 1 \end{cases} \quad [2]$$

Il primo sistema rappresenta un problema di ottimizzazione vincolata i cui viene massimizzato il rendimento atteso del portafoglio, $E[R_\Pi]$, con una rischiosità fissata a priori $\tilde{\sigma}$.

Il secondo sistema rappresenta il problema di ottimizzazione vincolata in cui si minimizza la rischiosità del portafoglio[80], σ_Π^2 , dopo aver fissato un rendimento del portafoglio, detto rendimento target $\tilde{R}$.

Seguendo la trattazione viene scelto di minimizzare la volatilità, ossia di risolvere il problema di ottimizzazione vincolata [2], ottenendo la forma analitica della frontiera efficiente con n titoli rischiosi.

Si riscrive il problema di ottimizzazione in forma vettoriale:

- e = vettore colonna dei rendimenti degli n titoli;

[80] Pari alla varianza del portafoglio.

- u = vettore unità a n componenti;
- Ω = vettore colonna delle quote;
- $\Omega^T \cdot e$ = vincolo di rendimento;
- $\Omega^T \cdot u$ = vincolo di bilancio;
- μ = rendimento atteso;
- Σ = matrice della varianza e covarianza di ordine n[81];

$$\begin{cases} min\ \frac{1}{2}\ \sigma_{\Pi}^{2} = \frac{1}{2}\ \Omega^{T} \cdot\ \Sigma\ \cdot\ \Omega \\ \Omega^T \cdot e = \mu \\ \Omega^T \cdot u = 1 \end{cases}$$

(9. 25)

Il problema di ottimo vincolato viene risolto con la funzione lagrangiana:

$$L = \frac{1}{2}\Omega^T \cdot \Sigma \cdot \Omega - \lambda_1(\Omega^T \cdot e - \mu) - \lambda_2(\Omega^T \cdot u - 1)$$

(9. 26)

Da questa equazione è possibile ricavare l'espressione analitica che lega il rendimento atteso μ alla varianza del portafoglio, ovvero l'equazione della frontiera efficiente.
L'equazione della frontiera efficiente, rappresentata nel piano (σ;μ), è una parabola con asse orizzontale e concavità rivolta verso destra.

[81] $\Sigma = \begin{bmatrix} \sigma_{11} & \cdots & \sigma_{1n} \\ \vdots & \ddots & \vdots \\ \sigma_{n1} & \cdots & \sigma_{nn} \end{bmatrix}$

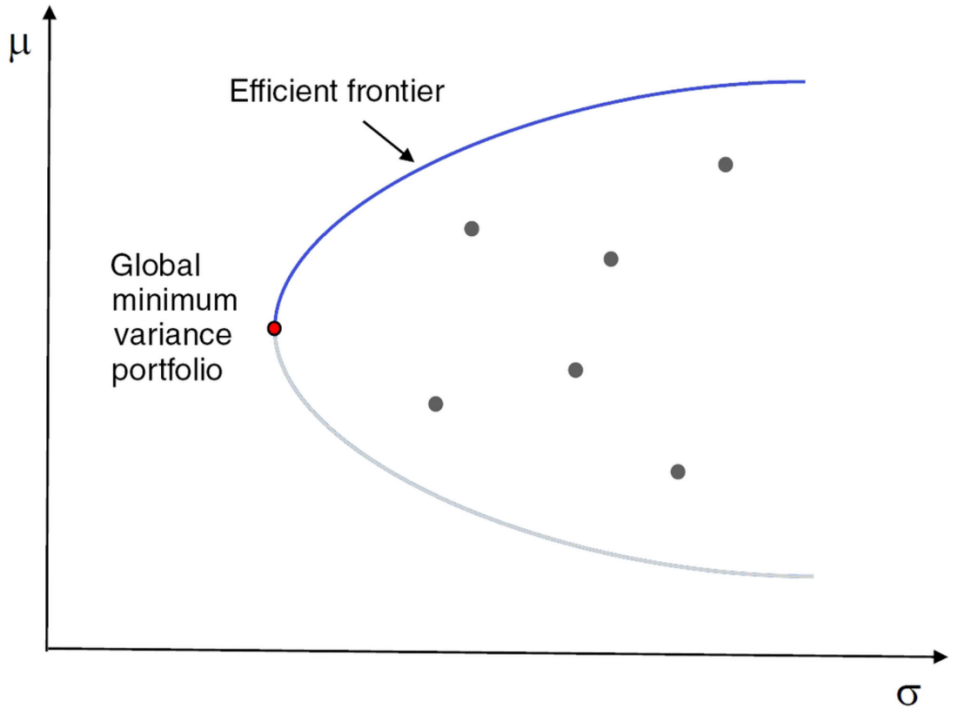


***Figura 9.1**. Esempio di frontiera efficiente. Fonte "Golosnoy, V., Gribisch, B., and Seifert, M. I. 2021. Sample and realized minimum variance portfolios: Estimation, statistical inference, and tests, WIREs Computational Statistics, Advance Access published May 4, 2021: doi:10.1002/wics.1556".*

Nell'analisi sopradescritta è necessario ricordare che i risultati presentati si riferiscono ad un caso generale in cui sono permesse le vendite allo scoperto o short selling, operazione finanziaria che consiste nella vendita di strumenti finanziari non posseduti con successivo riacquisto (Borsaitaliana.it, 2018)[82]. Per costruire un modello che comprenda lo scenario in cui non è possibile effettuare questo tipo di operazioni bisogna aggiungere un ulteriore vincolo all'equazione di ottimizzazione vincolata [2].

[82] Short Selling: cos'è e come funziona - Borsa Italiana. 2018. Borsaitaliana.it, https://www.borsaitaliana.it/notizie/sotto-la-lente/short-selling.htm (date last accessed March 5, 2022).

Il problema di ottimizzazione in assenza di vendite allo scoperto assume la forma:

$$\begin{cases} min_{\omega_1,\dots,\omega_n}(\sigma_\Pi^2) \\ E[R_\Pi] = \tilde{R} \\ \omega_i \geq 0 \\ \sum_{i=1}^{n} \omega_i = 1 \end{cases}$$

(9. 9)

Il vincolo, $\omega_i \geq 0$, aggiunto al sistema impone che i pesi dei titoli del portafoglio devono essere positivi.

Portafoglio ottimo

In questa sezione viene affrontata la seconda fase del modello, in cui bisogna selezionare il portafoglio ottimo tra quelli che costituiscono la frontiera efficiente trovata nella sezione precedente. Nella fase di selezione del modello si deve far riferimento alla funzione di utilità del decisore, è necessario massimizzare l'utilità attesa, la quale deve considerare l'avversione al rischio dell'investitore. La funzione di utilità attesa dovrà essere espressa secondo i parametri del modello, ossia attraverso media e varianza:

- U= funzione di utilità;
- σ^2 =varianza;
- μ = media;
- γ= coefficiente di avversione al rischio. Quest'ultimo viene scelto in maniera arbitraria e rappresenta la propensione al rischio dell'investitore.

$$U(\mu, \sigma) = \mu - \gamma \cdot (\mu^2 + \sigma^2)$$

(9. 10)

Il modello utilizza una funzione di utilità quadratica, inoltre si osserva che all'aumentare del coefficiente di avversione al rischio γ i portafogli tendono verso il titolo risk free, ovvero al portafoglio privo di rischio.

Successivamente si definiscono le curve di indifferenza, funzioni che, fissato un livello di utilità, sono composte da diverse combinazioni di μ e σ che garantiscono all'investitore la medesima utilità. I portafogli appartenenti alla stessa curva di indifferenza sono equivalenti per il decisore per quanto riguarda l'avversione al rischio e queste corrispondono a quei portafogli che massimizzano la sua funzione di utilità.

$\overline{U}$=livello di utilità.

Le curve di indifferenza sono descritte dalla seguente equazione:

$$U(\mu, \sigma) = \overline{U}$$

(9. 11)

Le curve di indifferenza presentano le seguenti caratteristiche:

- le curve posizionate più in alto sono caratterizzate da un maggiore livello di utilità $\overline{U}$;
- le curve sono convesse $\frac{\partial U}{\partial \mu} > 0$ e $\frac{\partial U}{\partial \sigma} < 0$;
- maggiore è l'avversione al rischio γ, maggiore è la convessità delle curve.

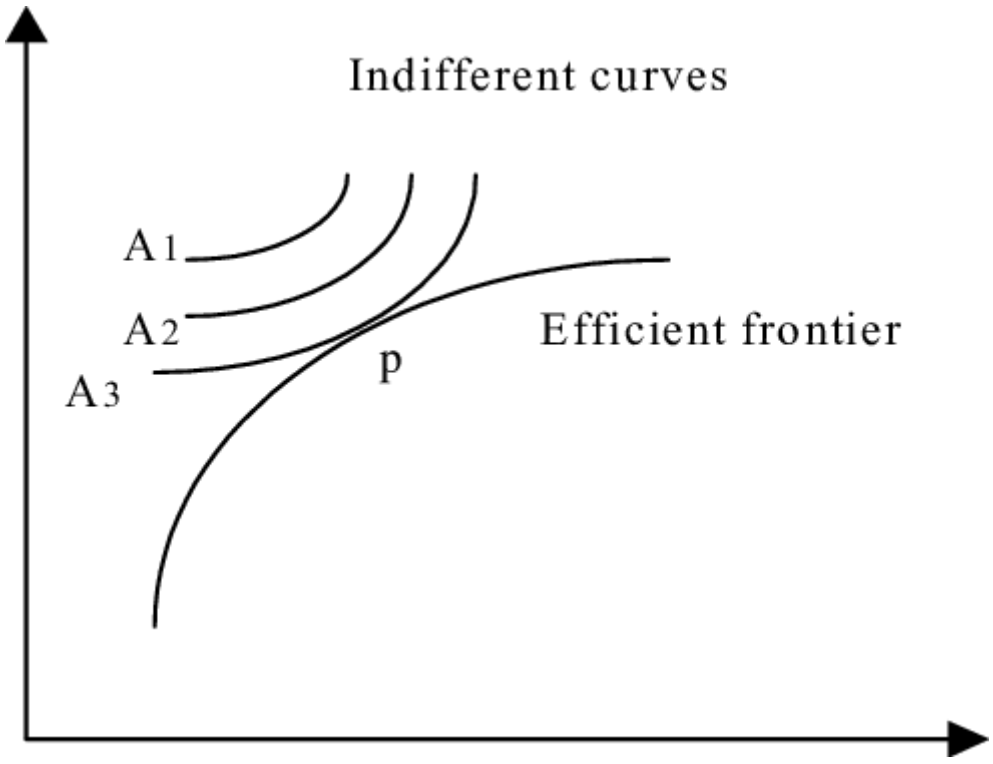


Figura 9.2. *Frontiera efficiente e curva di indifferenza. Fonte "Tanaka, Hideo & Guo, Peijun. (1999). Possibilistic data analysis for operations research". Sito: "https://www.researchgate.net/figure/The-efficient frontier_fig17_266308727".*

Per individuare il portafoglio ottimo è necessario massimizzare la funzione di utilità attesa trovando il punto di tangenza tra la frontiera efficiente e la curva di indifferenza che soddisfa il valore di $\overline{U}$.

La soluzione trovata dal modello di Markowitz sarà un portafoglio composto da *N* titoli che minimizza il rischio provando allo stesso tempo di massimizzare la funzione di utilità, questo si ottiene grazie all'effetto diversificazione, cioè sfruttando le correlazioni tra i titoli per avere un portafoglio con un livello di rischio più basso possibile. I coefficienti di correlazione negativi sono cruciali nella riduzione del rischio complessivo del portafoglio.

9.6 Analisi della correlazione dei dati storici

Per applicare il modello di Markowitz è necessario analizzare la correlazione tra i dati presi in esame.

La misurazione della correlazione tra due variabili casuali viene effettuata calcolando il coefficiente di correlazione lineare di Pearson, che misura il grado di relazione lineare tra le misure. L'indice di correlazione di Pearson viene indicato con il simbolo ρ_{xy} che indica il coefficiente tra le generiche variabili x e y.

L'indice di correlazione è determinato dalla seguente formula:

$$\rho_{xy} = \frac{\sum_{i=1}^{N}(x_i - \bar{x}) \cdot \sum_{i=1}^{N}(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - x^2) \cdot \sum_{i=1}^{N}(y_i - y^2)}}$$

(9. 12)

La precedente equazione può essere riformulata nel seguente modo:

$$\rho_{xy} = \frac{cov(x, y)}{\sqrt{\sigma_2^x \sigma_2^y}}$$

(9. 13)

Dai log rendimenti è stata creata la matrice varianza-covarianza di ordine n, rappresentata da Σ:

$$\Sigma = \begin{bmatrix} \sigma_{11} & \cdots & \sigma_{1n} \\ \vdots & \ddots & \vdots \\ \sigma_{n1} & \cdots & \sigma_{nn} \end{bmatrix}$$

(9. 14)

- $\sigma_{ij} = Cov(R_i, R_j) = E\left[(R_k - \mu_k) \cdot (R_j - \mu_j)\right]$ è la covarianza tra il k-esimo titolo e il j-esimo titolo.

- $\sigma_{ii} = Var(R_k) = \sigma_i^2$ è la varianza dell'i-esimo titolo, esse costituiscono la diagonale principale della matrice varianza-covarianza.

Markowitz introdusse nella sua teoria il concetto di correlazione tra i titoli applicato alla creazione di un portafoglio ottimo, nello specifico ha introdotto il concetto di decorrelazione, fondamentale anche per la diversificazione.
Secondo la teoria di Markowitz, per ottenere un portafoglio ideale, è necessario che i titoli non siano perfettamente correlati, ovvero che il coefficiente di correlazione sia minore di 1.
In base al valore dell'indice di correlazione di Pearson è possibile descrivere tre scenari:

1. Se $\rho_{xy} < 0$ i titoli x e y sono correlati negativamente.
2. Se $\rho_{xy} = 0$ i titoli x e y sono incorrelati.
3. Se $\rho_{xy} > 0$ i titoli x e y sono correlati positivamente.

Nel caso in cui la correlazione tra i titoli del portafoglio sia inferiore a 0, ossia nel caso in cui siano correlati negativamente, la diversificazione tra i titoli permette di minimizzare il rischio del portafoglio titoli, questo implica che il rischio del portafoglio è inferiore a quello medio dei titoli che lo compongono.
Di seguito sono presentate le analisi della correlazione e della covarianza in base a tre scenari:

1. Scenario in cui si analizzano solamente le criptovalute.
2. Scenario in cui si analizzano solamente gli indici di borsa
3. Scenario in cui si analizza il sistema costruito sia dagli indici di borsa sia dalle criptovalute.

È necessario sottolineare come non è stato possibile utilizzare le stesse serie storiche di dati utilizzati per l'analisi dei *Random Walk*, poiché le sequenze dei trading day presentavano alcune differenze. Questa mancanza di corrispondenza è dovuta alla diversa gestione delle chiusure nei weekend delle borse e alle feste nazionali e internazionali che possono essere diverse in base alla posizione geografica delle borse.
Per gli indici di borsa si sono individuati i giorni in cui i dati sul valore di chiusura dell'asset fossero disponibili per ogni indice analizzato. Il processo di adeguamento delle serie storiche

ha provocato all'eliminazione di alcuni dati in modo da non creare uniformità, alla fine di questa attività sono state ottenute serie di 1219 dati.

L'analisi dell'insieme di criptovalute e indici di borsa ha richiesto un'uniformità tra tutti i dati, quindi, sono state uniformate le serie storiche di entrambi i gruppi. Alla fine di tale processo sono state ottenute delle serie storiche, con data di partenza dei prezzi pari a 9/11/2017, di 1008 dati.

Analisi matrice covarianza e correlazione indici di borsa

In questa sezione vengono presentate e analizzate le matrici di varianza-covarianza e di correlazione delle serie storiche degli indici di borsa.

***Tabella 9.11**. Matrice varianza-covarianza degli indici di borsa*

	S&P500	Euro Stox50	FTSEMIB	CAC 40	NASDAQ
S&P500	0.00014998	0.00009333	0.00010056	0.00009271	0.00016015
Euro Stox50	0.00009333	0.00014356	0.00014757	0.00014140	0.00009101
FTSEMIB	0.00010056	0.00014757	0.00018970	0.00014466	0.00009824
CAC 40	0.00009271	0.00014140	0.00014466	0.00014511	0.00008861
NASDAQ	0.00016015	0.00009101	0.00009824	0.00008861	0.00019262

***Tabella 9.12**. Matrice di correlazione degli indici di borsa.*

	S&P500	*Euro Stox50*	*FTSEMIB*	*CAC 40*	*NASDAQ*
S&P500	1				
Euro Stox50	0.64	1			
FTSEMIB	0.60	0.89	1		
CAC 40	0.63	0.98	0.87	1	
NASDAQ	0.94	0.55	0.51	0.53	1

Alla matrice di correlazione, Tabella 10.12, è stata applicata una formattazione condizionale per evidenziare un'alta correlazione, tendente al valore 1, con il colore rosso e un a bassa correlazione, tendente al valore -1, con il colore verde.

Le correlazioni più alte si hanno tra due gruppi distinti: gli indici "europei", ovvero FTSEMIB, CAC 40 e Eurostox50, e gli indici statunitensi, S&P500 e NASDAQ. Le correlazioni tra indici appartenenti allo stesso gruppo sono piuttosto alte, fino a valori quasi pari ad 1.
Al contrario, le correlazioni tra gli indici appartenenti a gruppi diversi assumono un valore medio, tra il 0.64 e il 0.51.

Analisi matrice covarianza e correlazione Criptovalute

In questa sezione vengono presentate e analizzate le matrici di varianza-covarianza e di correlazione delle serie storiche delle criptovalute.

***Tabella 9.13**. Matrice varianza-covarianza delle criptovalute*

	Bitcoin	**Ethereum**	**Binance Coin**	**Monero**	**Litecoin**
Bitcoin	0.00174139	0.00169610	0.00170084	0.00171999	0.00180838
Ethereum	0.00169610	0.00277246	0.00213466	0.00218769	0.00248327
Binance Coin	0.00170084	0.00213466	0.00391621	0.00219109	0.00225885
Monero	0.00171999	0.00218769	0.00219109	0.00321297	0.00234855
Litecoin	0.00180838	0.00248327	0.00225885	0.00234855	0.00330747

***Tabella 9.14**. Matrice di correlazione delle criptovalute.*

	Bitcoin	**Ethereum**	**Binance Coin**	**Monero**	**Litecoin**
Bitcoin	1				
Ethereum	0.77	1			
Binance Coin	0.65	0.65	1		
Monero	0.73	0.73	0.62	1	
Litecoin	0.75	0.82	0.63	0.72	1

Anche per questa matrice, Tabella 10.14, è stata usata la stessa formattazione condizionale per evidenziare i valori di correlazione tre le criptovalute. In questo caso non si evidenziano

correlazioni particolarmente alte, a differenza degli indici di borsa, l'unica correlazione che un valore particolarmente superiore è quella tra Ethereum e Litecoin.
È possibile notare che Binance coin ha i valori di correlazione più bassi della matrice.

Analisi matrice covarianza e correlazione con indici e criptovalute

In questa sezione vengono presentate e analizzate le matrici di varianza-covarianza e di correlazione delle serie storiche degli indici di borsa e delle criptovalute.
Per una maggior chiarezza grafica è stato deciso di presentare la matrice di correlazione e covarianza utilizzando i simboli azionari (tickers) degli indici e delle criptovalute (Tabella 10.15).

Tabella 9.15.

Asset	**Simbolo azionario**
Euro Stox50	STOXX50E
Nasdaq	IXIC
FTSEMIB	FTSEMIB.MI
S&P500	SPX
CAC 40	FCHI
Bitcoin	BTC
Ethereum	ETH
Binance Coin	BNB
Monero	XMR
Litecoin	LTC

A causa delle dimensioni della matrice varianza-covarianza si è deciso di dividerla in due parti:

	STOXX50E	IXIC	FTSEMIB.MI	SPX	FCHI
STOXX50E	0.000164	0.000106	0.000168	0.000109	0.000162
IXIC	0.000106	0.000225	0.000114	0.000189	0.000103
FTSEMIB.MI	0.000168	0.000114	0.000212	0.000118	0.000164
SPX	0.000109	0.000189	0.000118	0.000177	0.000109
FCHI	0.000162	0.000103	0.000164	0.000109	0.000165
BTC	0.000140	0.000169	0.000173	0.000150	0.000135
ETH	0.000196	0.000251	0.000239	0.000228	0.000188
BNB	0.000197	0.000258	0.000230	0.000231	0.000193
XMR	0.000159	0.000204	0.000189	0.000178	0.000153
LTC	0.000166	0.000215	0.000203	0.000191	0.000160

	BTC	ETH	BNB	XMR	LTC
STOXX50E	0.000140	0.000196	0.000197	0.000159	0.000166
IXIC	0.000169	0.000251	0.000258	0.000204	0.000215
FTSEMIB.MI	0.000173	0.000239	0.000230	0.000189	0.000203
SPX	0.000150	0.000228	0.000231	0.000178	0.000191
FCHI	0.000135	0.000188	0.000193	0.000153	0.000160
BTC	0.002494	0.002399	0.002431	0.002439	0.002505
ETH	0.002399	0.004106	0.003177	0.003025	0.003469
BNB	0.002431	0.003177	0.006124	0.003335	0.003158
XMR	0.002439	0.003025	0.003335	0.004515	0.003138
LTC	0.002505	0.003469	0.003158	0.003138	0.004642

***Tabella 9.16**. Matrice varianza-covarianza.*

	STOXX50E	IXIC	FTSEMIB.MI	SPX	FCHI	BTC	ETH	BNB	XMR	LTC
STOXX50E	1									
IXIC	0.55	1								
FTSEMIB.MI	0.90	0.52	1							
SPX	0.64	0.94	0.61	1						
FCHI	0.98	0.53	0.88	0.63	1					
BTC	0.22	0.23	0.24	0.23	0.21	1				
ETH	0.24	0.26	0.26	0.27	0.23	0.75	1			
BNB	0.20	0.22	0.20	0.22	0.19	0.62	0.63	1		
XMR	0.18	0.20	0.19	0.20	0.18	0.73	0.70	0.63	1	
LTC	0.19	0.21	0.20	0.21	0.18	0.74	0.79	0.59	0.69	1

***Tabella 9.17**. Matrice di correlazione tra indici di borsa e criptovalute.*

In primo luogo, è necessario evidenziare che le differenze rispetto alle matrici precedenti sono dovute alle modifiche dei dati per avere uniformità sulle date dei valori degli indici e delle criptovalute.

La formattazione condizionale è la stessa utilizzata per le matrici precedenti.

Le correlazioni tra gli indici di borsa e le criptovalute sono piuttosto bassi, con un valore medio che è circa 0.21.

9.7 Creazione portafoglio ottimo

Per la creazione del portafoglio ottimo si è deciso di utilizzare il software Matlab.

I portafogli sono stati ottimizzati minimizzando il valore di rischio del portafoglio, e fissando un rendimento target, nello specifico è stato fissando al valore pari a quello del portafoglio equi ponderato.

Gli scenari studiati sono tre: nel primo viene analizzato un portafoglio formato dalle sole criptovalute in modo da capire le potenzialità delle singole valute digitali; nel secondo scenario vengono analizzati solamente gli indici di borsa; infine, nel terzo scenario viene analizzato l'insieme delle criptovalute e degli indici di borsa per valutare la loro efficienza come strumento di investimento in un mercato in cui sono presenti asset tradizionali.

Se il portafoglio ottimo del terzo scenario fosse caratterizzato dalla presenza di una quota di una specifica criptovaluta implicherebbe un certo grado di efficienza come strumento di investimento.

Si sottolinea che i dati utilizzati per effettuare tale analisi hanno subito lo stesso processo di uniformazione già spiegato nell'analisi della correlazione e covarianza.

Portafoglio ottimo con sole criptovalute

Portafoglio ottimo con mix di criptovalute in assenza di short selling

Tabella 9.18.

Asset	**Composizione portafoglio**
Bitcoin	87.19%
Ethereum	2.45%
Binance Coin	10.36%
Litecoin	0.00%
Monero	0.00%
Rendimento target	0.00149658
Deviazione standard ottenuta	0.04192953

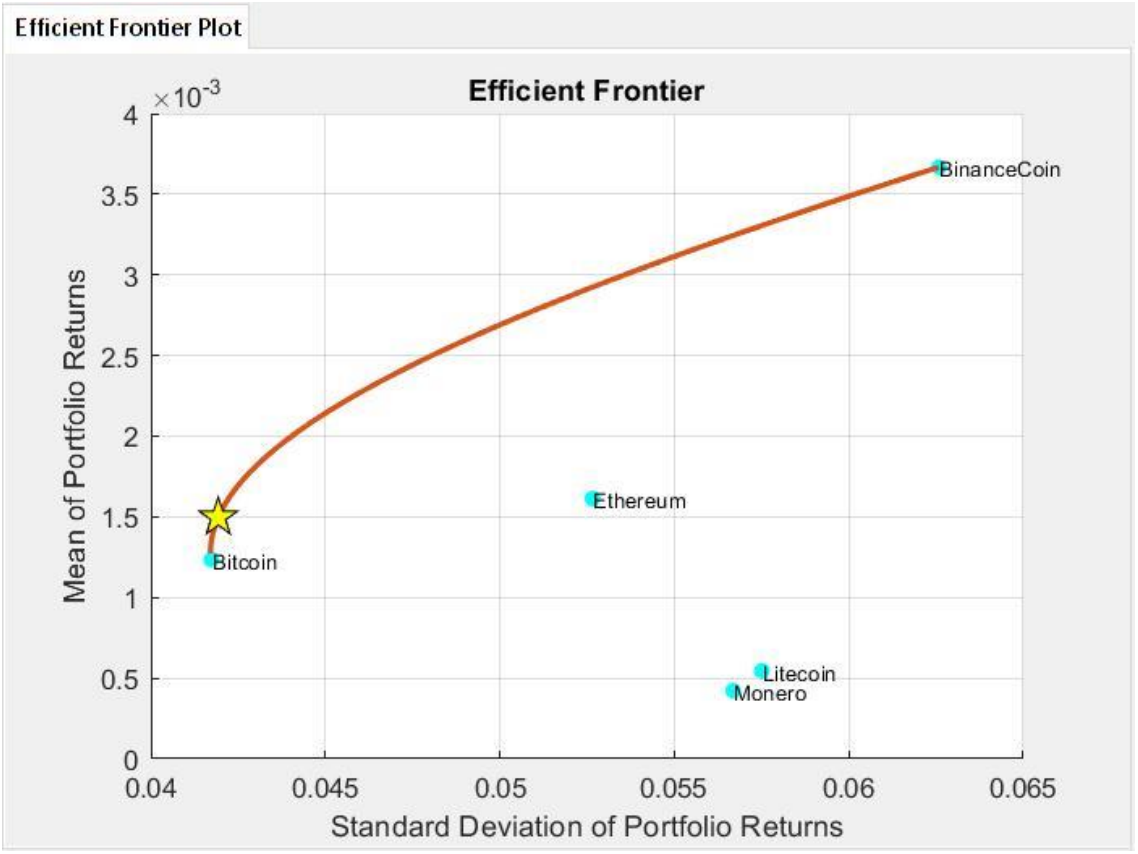


***Figura 9.3**. Frontiera efficiente con criptovalute in assenza di short selling.*

Il rendimento target, fissato come rendimento del portafoglio equiponderato, è pari a 0.0014965800718166.

Il portafoglio ottimo individuato sulla frontiera efficiente è rappresentato da una stella gialla. Come si può notare dalla composizione del portafoglio il mix è composto da sole tre criptovalute: Bitcoin, Ethereum e Binance Coin. In particolare, la maggior parte della quota è costituita dalla sola Bitcoin.

Portafoglio ottimo con mix di criptovalute con short selling

Tabella 9.19.

	Composizione del portafoglio
Bitcoin	97.27%
Ethereum	11.42%
Binance Coin	5.04%
Litecoin	-13.09%
Monero	-0.63%
Rendimento target	0.00149658
Deviazione standard ottenuta	0.04161747

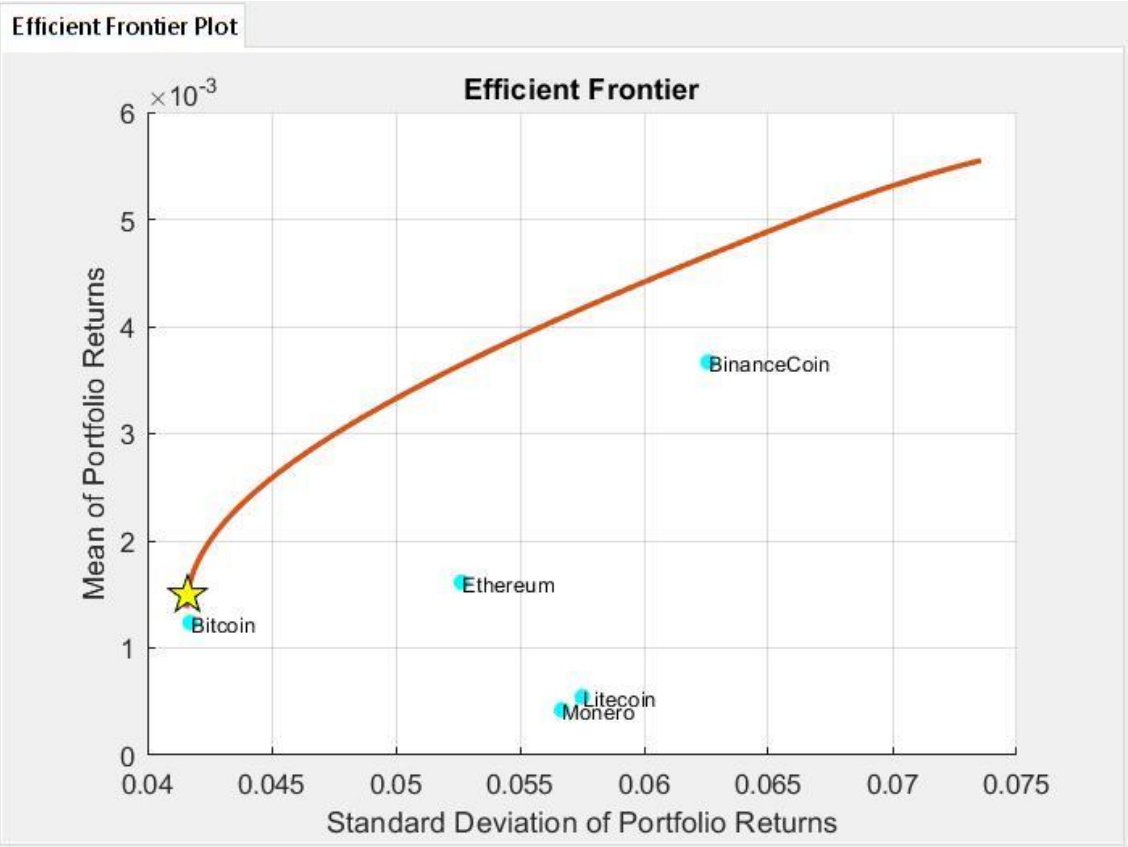


Figura 9.4. *Frontiera efficiente con criptovalute con short selling.*

Il rendimento target è uguale al caso precedente, pari al rendimento del portafoglio equiponderato.

Come si può notare si ha una posizione lunga sulle prime tre criptovalute, invece per Monero e Litecoin si ha una posizione corta, evidenziato dal valore negativo in tabella.

Grazie alla possibilità delle vendite allo scoperto è possibile ottenere lo stesso rendimento ma con un rischio minore, infatti la deviazione standard è caratterizzata da una diminuzione del 0.74%. La logica di questo effetto è evidente nel caso delle valute digitali Monero e Litecoin, esse non comparivano nella composizione del portafoglio in assenza dello *short selling*, invece in questo caso vengono utilizzate assumendo una posizione corta su di esse e ottenendo una diminuzione della rischiosità.

Portafoglio ottimo con i soli indici

Portafoglio ottimo con mix di indici di borsa in assenza di short selling

Tabella 9.20.

Asset	**Composizione del portafoglio**
S&P500	50.51%
Eurostoxx 50	7.59%
FTSE MIB	0.00%
NASDAQ	0.00%
CAC	41.89%
Rendimento target	0.00045838
Deviazione standard ottenuta	0.01095248

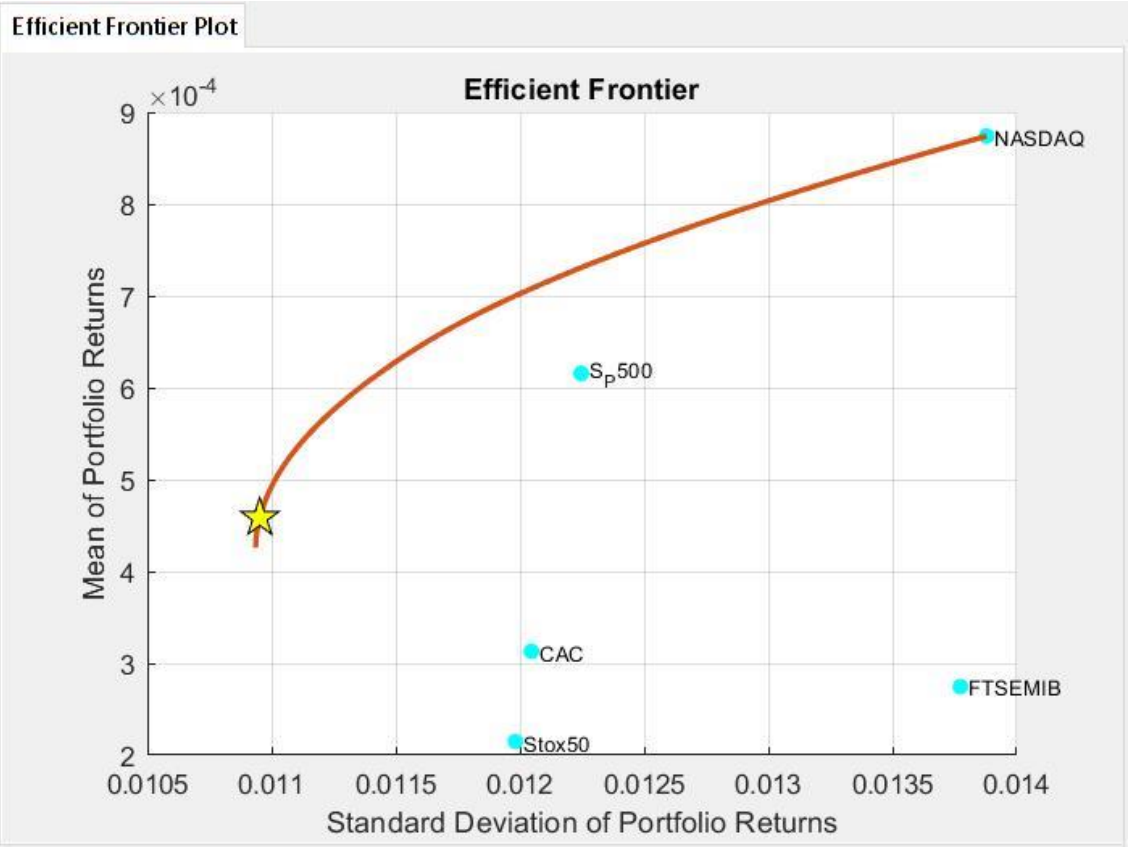


Figura 9.5. *Frontiera efficiente con indici di borsa in assenza di short selling.*

Il portafoglio ottenuto è composto da soli tre indici, l'indice FTSEMIB e il NASDAQ hanno una percentuale pari a zero nella composizione del portafoglio.

La deviazione standard ottenuto è pari a 0.010952482, confrontando i valori del portafoglio comprendente le criptovalute si evidenzia un rendimento minore a fronte di una rischiosità anch'essa minore.

Portafoglio ottimo con mix di indici di borsa con short selling

Tabella 9.21.

Asset	**Composizione del portafoglio**
S&P500	51.39%
Eurostoxx 50	16.44%
FTSE MIB	-11.95%
NASDAQ	0.25%
CAC	43.86%
Rendimento target	0.00045838
Deviazione standard ottenuta	0.01092704

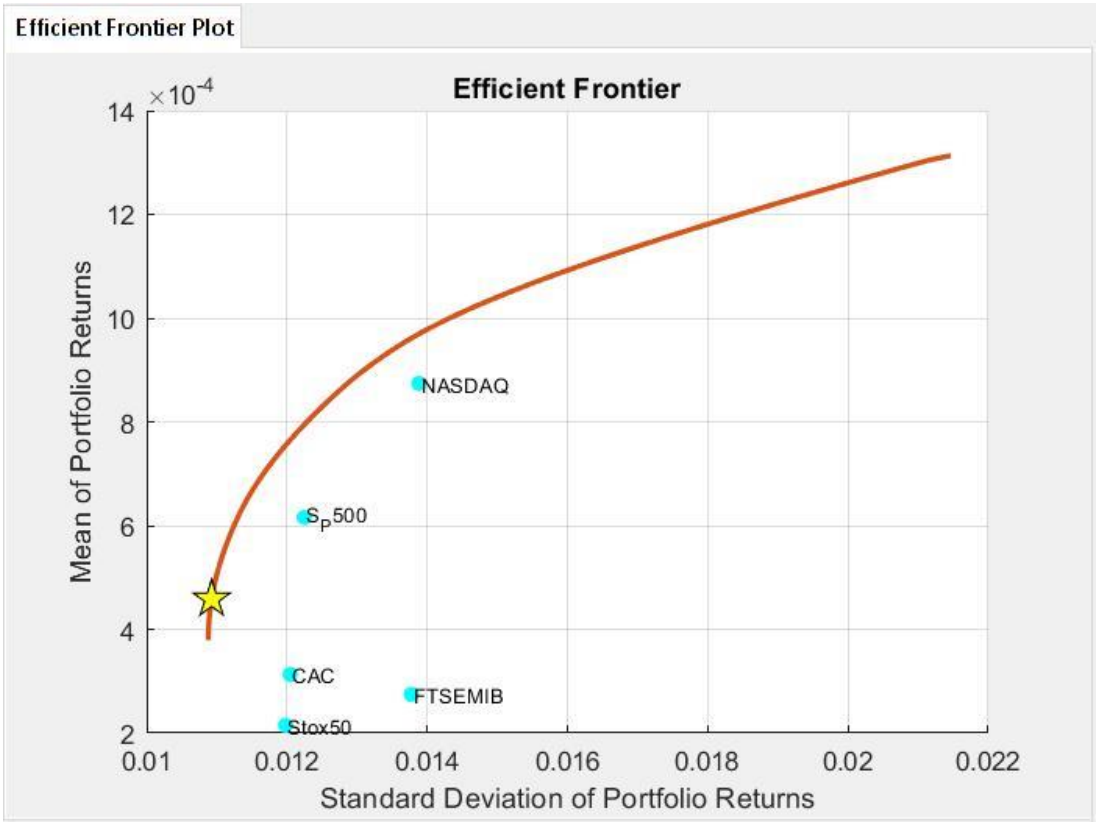


***Figura 9.6**. Frontiera efficiente con indici di borsa con short selling.*

Rimuovendo il vincolo dell'assenza di vendite allo scoperto la composizione del portafoglio varia notevolmente, risultano quattro posizioni lunghe ed una posizione corta sull'indice FTSEMIB.

Le differenze tra i due casi riguardano principalmente l'indice NASDAQ, che in questo caso assume un valore positivo di circa 0.25%, e le variazioni di FTSEMIB e Eurostoxx50, il primo assume un valore negativo pari a circa 11.95%, il secondo è caratterizzato da un aumento del 8.85% della quota rispetto al caso precedente.

Queste variazioni sono causate dalla possibilità di vendita allo scoperto dei titoli, questa comporta una migliore allocazione dei titoli del portafoglio, infatti, come si vede dalla deviazione standard del portafoglio, a parità di rendimento si ha un livello di rischiosità minore di circa lo 0.23%.

Portafoglio ottimo con indici e criptovalute

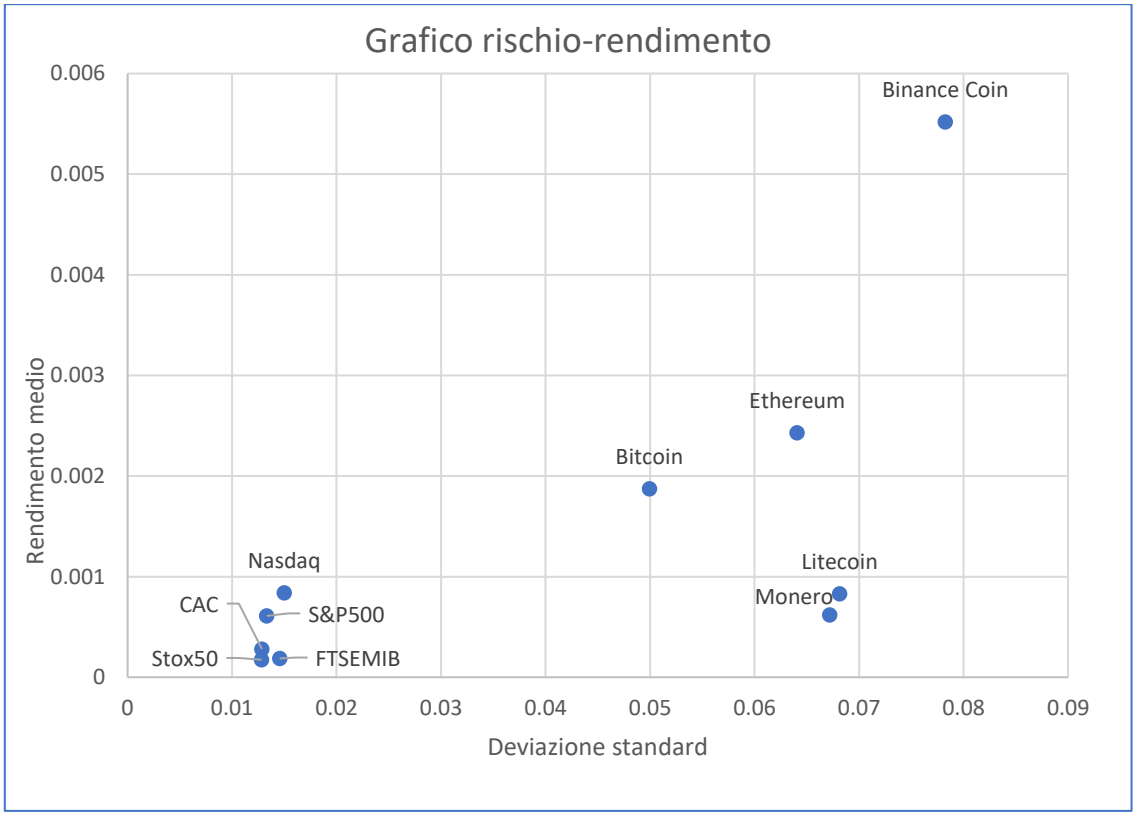


***Figura 9.7**. Grafico rischio-rendimento delle criptovalute e indici di borsa.*

Prima di presentare i portafogli ottimi si è deciso di analizzare il grafico rischio-rendimento. Si individua un comportamento diverso tra il gruppo delle criptovalute e quello degli indici di borsa: il primo è caratterizzato da una rischiosità più elevata rispetto al secondo e da una tendenza ad avere un rendimento medio maggiore, in particolar modo Binance Coin, Ethereum e Bitcoin. Inoltre, si evidenzia una maggiore dispersione delle criptovalute rispetto agli indici di borsa che hanno un rendimento medio e una rischiosità simile.

Portafoglio ottimo in assenza di short selling

Tabella 9.22.

Asset	**Composizione del portafoglio**
S&P500	0.00%
Eurostoxx 50	74.36%
FTSE MIB	0.00%
NASDAQ	13.43%
CAC	0.00%
Bitcoin	0.00%
Ethereum	0.00%
Binance Coin	12.21%
Litecoin	0.00%
Monero	0.00%
Rendimento target	0.00133626
Deviazione standard ottenuta	0.01709743

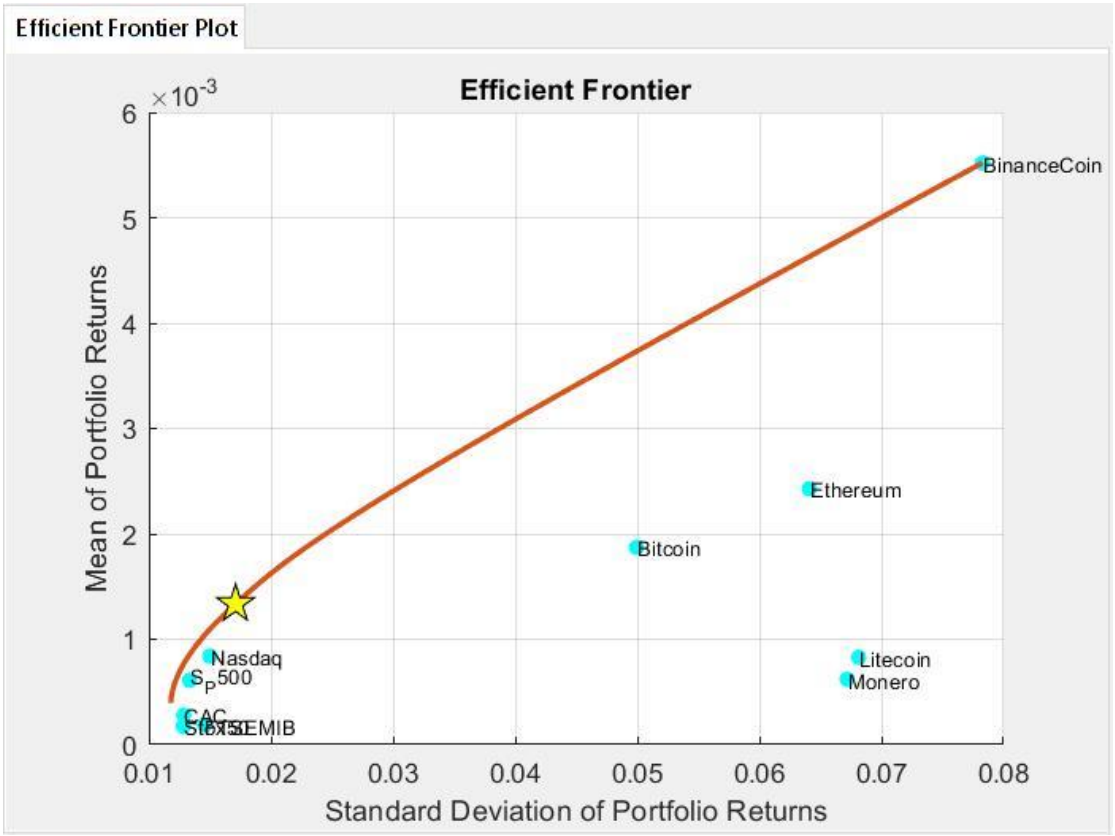


***Figura 9.8**. Frontiera efficiente nello scenario con criptovalute e indici di borsa senza short selling.*

In questa sezione è presentata la frontiera efficiente e la composizione del portafoglio ottimo costituito dall'insieme di criptovalute e degli indici presentati in precedenza. L'analisi è stata effettuata imponendo un rendimento target, pari al portafoglio equi ponderato, e ottimizzando in modo da minimizzare il rischio, cioè la deviazione standard.

I risultati ottenuti, nel caso di assenza di short selling, dimostrano come il portafoglio è composto da soli tre elementi: Eurostoxx50, NASDAQ e Binance Coin. La composizione è formata principalmente dagli indici, con l'88% del totale, rispetto alle criptovalute che hanno un peso del solo 12%.

Questo è un primo segnale che fa intuire un certo grado di inefficienza delle criptovalute come strumento di investimento.

Portafoglio ottimo con short selling

Tabella 9.23.

Asset	**Composizione del portafoglio**
S&P500	-52.91%
Eurostoxx 50	59.80%
FTSE MIB	-15.73%
NASDAQ	100.00%
CAC	3.38%
Bitcoin	9.65%
Ethereum	2.75%
Binance Coin	9.51%
Litecoin	-7.56%
Monero	-8.89%
Rendimento target	0.00133626
Deviazione standard ottenuta	0.01485006

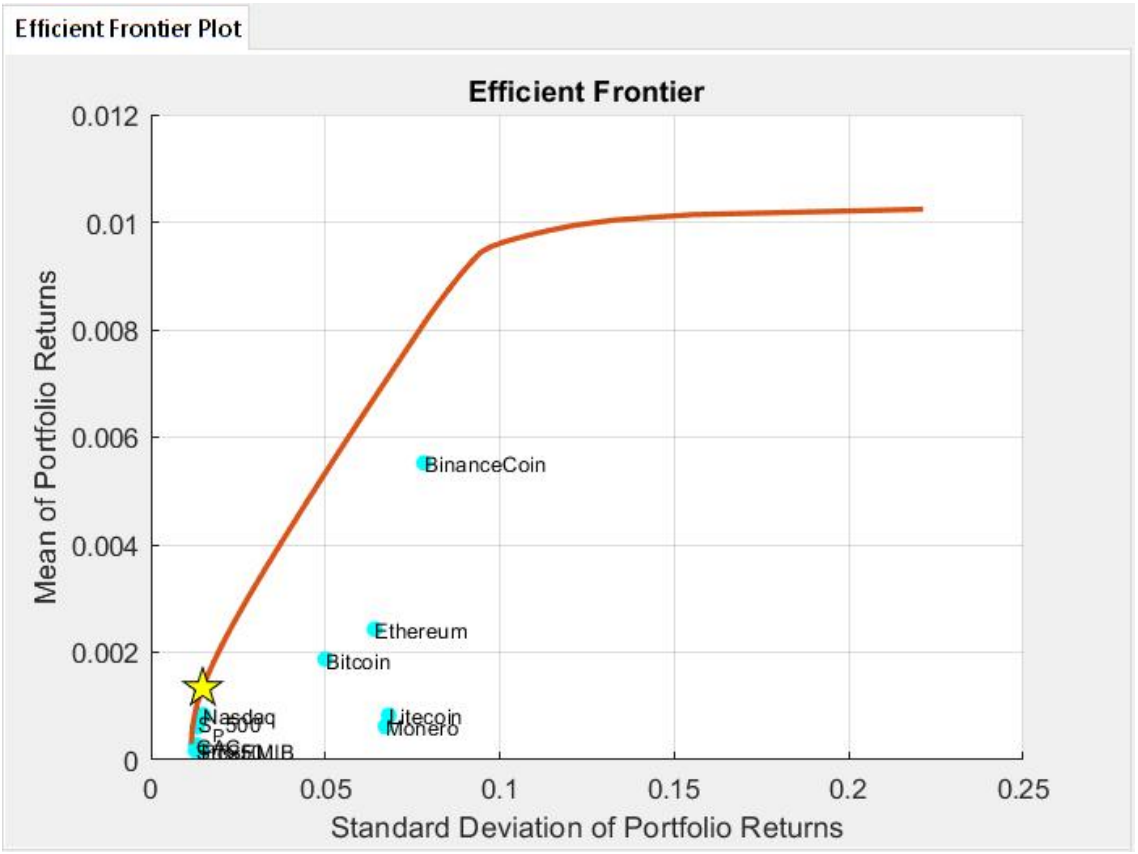


***Figura 9.9**. Frontiera efficiente con criptovalute e indici di borsa con short selling.*

Analizzando i risultati in modo generale, il CAC assume un valore positivo rispetto al caso precedente in cui aveva un valore nullo. Gli altri due indici che non comparivano nel portafoglio ottimo, S&P500 e FTSEMIB, assumono un valore negativo, quindi una posizione corta.

Per quanto riguarda le criptovalute assumono valore positivo: Bitcoin, Ethereum e Binance Coin; quest'ultima ha una diminuzione di partecipazione di circa il 22%.

Su Litecoin e Monero è necessario assumere, in questo scenario, una posizione corta; invece, nel caso precedente non erano comprese nel mix di portafoglio ottimo.

I risultati ottenuti confrontando i due gruppi, indici e criptovalute, in questo caso risultano ancora più evidenti: le criptovalute che hanno un valore positivo, quindi con una posizione lunga, hanno un valore relativamente basso rispetto agli indici. Considerando la somma dei pesi dei due gruppi è possibile notare che gli indici costituiscono il 95% del portafoglio, a dimostrazione, tenendo conto dei limiti del modello e delle assunzioni effettuate, una relativa inefficienza delle criptovalute come strumento di investimento.

10 CONCLUSIONE

L'elaborato ha messo in evidenza l'innovatività portata dalla creazione delle criptovalute, esse sono state progettate con l'intenzione di creare uno strumento finanziario rivoluzionario che potesse cambiare il sistema finanziario. L'analisi dell'impatto delle valute digitali sul sistema economico ha mostrato i punti di forza e di debolezza di quest'ultime e ha rivelato quali sono le più grandi problematiche che, nel prossimo futuro, potrebbero compromettere il loro sviluppo. Nonostante l'importante diffusione raggiunta e una consapevolezza sempre maggiore da parte degli utenti, le grandi autorità, come le banche centrali, invitano a mantenere un certo grado di attenzione nei confronti delle valute digitali e dichiarano di non considerarle ancora una vera e propria minaccia per il sistema tradizionale.

Le criticità riguardati la cybersecurity e i cybercrimini mostrano la presenza di un grado di pericolosità significativo, inoltre la varietà dei profili di rischio e l'assenza di un sistema di tutela consolidato dimostrano una maggiore esposizione rispetto ai metodi tradizionali.

L'impatto ambientale delle maggiori criptovalute, come Bitcoin ed Ethereum, non può essere trascurato, specie in un momento cruciale per la transizione ecologica. La riduzione delle emissioni per il sostentamento della loro infrastruttura è fondamentale per renderle compatibili con le politiche e le misure adottate dai maggiori paesi per la lotta al cambiamento climatico. Per ottenere dei risultati soddisfacenti le criptovalute principali dovrebbero apportare significative modifiche ai loro sistemi di estrazione, ma, al momento, non esistono iniziative a riguardo, alimentando le perplessità delle autorità circa il loro ruolo nel sistema economico mondiale.

L'analisi dell'efficienza delle criptovalute, utilizzando gli indici di borsa come benchmarking, ha dimostrato la loro inefficienza come beni di investimento, nel caso di un portafoglio con un rendimento target pari alla media dei rendimenti e una rischiosità minima. Questo risultato, seppur con le dovute semplificazioni, dimostra che la loro volatilità è determinante e avvalora i timori delle autorità circa lo loro pericolosità per il sistema economico, come dichiarato da Alessandra Perrazzelli, Vicedirettrice generale della Banca d'Italia, all'Assiom Forex "Se non opportunamente controllate possono in prospettiva comportare eventuali tensioni sui mercati finanziari, specie nel caso si debba procedere a vendite significative di attività finanziarie" (ANSA).

Le criptovalute, ad oggi, presentano delle criticità evidenti che ne limitano lo sviluppo e alimentano lo scetticismo e la diffidenza da parte delle autorità centrali, ma hanno decisamente definito una nuova visione di moneta che non può più essere ignorata, come dimostra l'attività delle banche centrali per la creazione delle Central Bank Digital Currency (CBDC). Questi progetti sono la declinazione delle valute digitali effettuata dalle banche centrali che hanno l'ambizione di sfruttare le potenzialità delle criptovalute decentralizzate, ma rimanendo legate alle valute legali dei vari paesi e al sistema di regolamentazione tradizionale. Le CBDC, secondo le autorità, costituirebbero la base per garantire la stabilità finanziaria e monetaria facendo coesistere nel mondo digitale sia il denaro privato e sovrano. Inoltre, con il loro consolidamento si otterrebbe una maggiore riservatezza nei pagamenti digitali, è noto che le società private, sfruttando una regolamentazione che non riesce a stare al passo dell'innovazione tecnologica, utilizzano le informazioni contenute nelle transazioni elettroniche per monetizzarle. Questo utilizzo improprio delle informazioni con una valuta digitale emessa da una banca centrale sarebbe scongiurato, una istituzione pubblica non avrebbe alcun interesse nello sfruttare i dati dei pagamenti, perciò si otterrebbe un livello di privacy ancora maggiore, aspetto che per gli utenti, secondo i sondaggi condotti dalla BCE, risulterebbe tra i più importanti. Oltre a ciò, il progetto delle CBDC si pone l'obiettivo di utilizzare le informazioni riguardanti le transazioni solo per scopi consentiti, nello specifico contrastare le attività illegali, aspetto particolarmente critico delle criptovalute.

La progettazione di queste valute è in fase di discussione da parte delle maggiori autorità, ma la complessità ne sta rallentando la realizzazione. L'obiettivo è di migliorare l'efficienza del sistema economico finanziario, ma, contemporaneamente, è necessario non stravolgere il funzionamento del sistema finanziario, quindi è fondamentale costruire uno strumento che non spiazzi completamente le soluzioni private di pagamento e, allo stesso tempo, soddisfi le esigenze degli utenti.

Date le difficoltà e l'importanza di queste decisioni i tempi per il rilascio di questi strumenti potrebbero essere dilatati, come dimostrano le parole di Fabio Panetta, membro dell'Executive Board della BCE, che ha dichiarato che è previsto l'inizio di una fase realizzativa e di sviluppo di una moneta digitale europea nel 2023, con una durata del progetto pari a tre anni.

In conclusione, si può affermare che nonostante la crescita dell'interesse verso le criptovalute e il grande fermento intorno a questo fenomeno, i difetti e le criticità mostrate ne evidenziano

i limiti e rendono difficili le previsioni a proposito del loro futuro e del progresso dei progetti presenti oggi. L'attenzione dei regulators e le dichiarazioni in merito alle CBDC da parte delle maggiori autorità mondiali aumentano l'incertezza del ruolo delle criptovalute nel prossimo futuro, ma è evidente che l'innovazione tecnologica introdotta dalle valute digitali e dalle tecnologie sottostanti, in particolar modo la tecnologia blockchain, ha posto le basi per una nuova rivoluzione del mondo finanziario.

11 BIBLIOGRAFIA & SITOGRAFIA

European Central Bank. 2015. Virtual currency schemes – a further analysis, Advance Access published 2015: doi:10.2866/662172

European Central Bank. 2012. VIRTUAL CURRENCY SCHEMES, OCTOBER 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Le criptovalute. 2018. Consob.it, https://www.consob.it/web/investor-education/criptovalute

Il fenomeno delle Monete Virtuali: opportunità per Telecom Italia | Notiziario Tecnico TIM. 2021. Telecom Italia Corporate, https://www.gruppotim.it/tit/it/notiziariotecnico/numeri/2014-1/capitolo-6.html

Colucci, K. and Moiso, C. Il fenomeno delle monete Virtuali: opportunità per Telecom Italia:, https://www.gruppotim.it/content/dam/telecomitalia/it/archivio/documenti/Innovazione/MnisitoNotiziario/2014/1-2014/capitolo-06/cap06.pdf

Reutzel, B. 2021. *What is cryptocurrency? Here's what you need to know about blockchain, coins and more*, CNBC, https://www.cnbc.com/select/what-is-cryptocurrency/

Bollettino economico. date last accessed February 16, 2022, at https://www.bancaditalia.it/pubblicazioni/bollettino-eco-bce/2019/bol-eco-5-2019/bolleco-bce-5-2019.pdf

Gola, C. and Caponera, A. 2019. Aspetti economici e regolamentari delle "cripto-attività" (Economic and Regulatory Aspects of Crypto-Assets), *SSRN Electronic Journal*, Advance Access published 2019: doi:10.2139/ssrn.3432976

https://it.wikipedia.org/wiki/Blockchain

https://it.wikipedia.org/wiki/Proof-of-work

https://it.wikipedia.org/wiki/Hashcash

Blockchain Explained: How does a transaction get into the blockchain? | Euromoney Learning. 2016. Euromoney.com, https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain

Blockchain: cos'è, come funziona e applicazioni oggi (2021). 2021. Blockchain 4innovation, https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/

https://it.wikipedia.org/wiki/Proof-of-work

Proof of work: cos'è e le differenze con il PoS - Blockchain 4innovation. 2020. Blockchain 4innovation, https://www.blockchain4innovation.it/criptovalute/blockchain-cosa-sono-i-protocolli-pow-e-pos-e-a-cosa-servono/

https://it.wikipedia.org/wiki/Funzione_crittografica_di_hash#Proof-of-Work

https://it.wikipedia.org/wiki/Metodo_forza_bruta

Nakamoto, S. 2008. Bitcoin: a Peer-to-Peer Electronic Cash System:, date last accessed at bitcoin.org at https://bitcoin.org/bitcoin.pdf

Cos'è la tecnologia blockchain? - IBM Blockchain | IBM. 2022. Ibm.com, https://www.ibm.com/it-it/topics/what-is-blockchain

V. Cryptocurrencies: looking beyond the hype. date last accessed at https://www.bis.org/publ/arpdf/ar2018e5.pdf

Redazione. 2021. *Criptovalute: perché il 2022 sarà l'anno dei regulators*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/criptovalute-perche-2022-sara-l-anno-regulators-AEN03wo

European Central Bank. 2021. *Financial Stability Review, November 2021*, European Central Bank, https://www.ecb.europa.eu/pub/financial-stability/fsr/html/ecb.fsr202111~8b0aebc817.en.html

CoinMarketCap. 2021. *A Look Back in Time: Bitcoin Price History and Events Timeline*, CoinMarketCap Alexandria, https://coinmarketcap.com/alexandria/article/bitcoin-price-history-and-events-timeline

BitPay Commemorates 10 Years as Leading Blockchain Payment Processor. 2021. Businesswire.com, https://www.businesswire.com/news/home/20210604005137/en/BitPay-Commemorates-10-Years-as-Leading-Blockchain-Payment-Processor

https://en.wikipedia.org/wiki/Bitcoin_ATM

Wagner, K. 2013. *World's First Bitcoin ATM Opens In Vancouver, Canada*, Mashable, https://mashable.com/archive/bitcoin-atm-2

Simonetta, B. 2014. *Arriva il primo bancomat di bitcoin*, Il Sole 24 ORE, https://st.ilsole24ore.com/art/tecnologie/2014-02-05/arriva-primo-bancomat-bitcoin-175513.shtml?uuid=ABmWUgu

Soldavini, P. 2020. *PayPal apre alle criptovalute: il bitcoin sarà accettato per i pagamenti*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/paypal-apre-criptovalute-bitcoin-sara-accettato-i-pagamentii-ADxnOSx

PayPal e le criptovalute: che prospettive si aprono e quali sono i vantaggi per gli utenti - Pagamenti Digitali. 2020. Pagamenti Digitali, https://www.pagamentidigitali.it/esperti-e-analisti/paypal-e-le-criptovalute-come-funziona-e-quali-sono-i-vantaggi-per-gli-utenti/

Incorvati, L. 2021. *Meno di due giorni per aprire un conto con una banca fintech, ben 14 con una tradizionale*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/meno-due-giorni-aprire-conto-una-banca-fintech-ben-14-una-tradizionale-AD5i1IKB

Cos'è il Bitcoin? 2022. Cointelegraph, https://it.cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin

Cau, E. 2021. *In Italia pagare le tasse sui bitcoin è complicato - Il Post*, Il Post, https://www.ilpost.it/2021/04/23/bitcoin-criptovalute-tasse/

Banca d'Italia. 2012. *Banca d'Italia - Le funzioni della moneta e le proposte di "moneta fiscale,"* Bancaditalia.it, https://www.bancaditalia.it/media/views/2017/moneta-

fiscale/index.html#:~:text=Dal%20punto%20di%20vista%20economico,economiche%20e%20gli%20accordi%20contrattuali.

Alessandro Guerani. 2019. *Blog | Piccola storia della moneta, fra miti e realtà*, Econopoly, https://www.econopoly.ilsole24ore.com/2019/04/07/piccola-storia-moneta/

Terraciano, T. 2020. *Davvero il dollaro è al tramonto come valuta di riserva mondiale?*, Econopoly, https://www.econopoly.ilsole24ore.com/2020/08/19/dollaro-valuta-riserva/

Yakubowski, M. 2021. *Nel 2020, Bitcoin si è dimostrato una riserva di valore affidabile? Le risposte degli esperti*, Cointelegraph, https://it.cointelegraph.com/news/did-bitcoin-prove-itself-to-be-a-reliable-store-of-value-in-2020-experts-answer

HÉLÈNE REY International Monetary System and Global Financial Cycles. date last accessed February 16, 2022, at https://www.bancaditalia.it/pubblicazioni/lezioni-baffi/pblecture-14/Rey-2019.pdf

https://en.wikipedia.org/wiki/Stablecoin

Safe haven asset - Glossario Finanziario - Borsa Italiana. 2022. Borsaitaliana.it, https://www.borsaitaliana.it/borsa/glossario/safe-haven-asset.html

Soldavini, P. 2019. *Ecco Libra, criptovaluta di Facebook: garantita da asset reali*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/ecco-libra-criptovaluta-facebook-sara-aperta-e-garantita-asset-reali-pagamenti-istantanei-ACyCYDS

Minenna, M. 2021. *Il dollaro digitale è già qui (ed è privato)*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/il-dollaro-digitale-e-gia-qui-ed-e-privato-AENyFfJ

Sorrentino, R. 2019. *Carney propone una "Libra globale" per superare l'egemonia del dollaro*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/carney-propone-una-libra-globale-superare-l-egemonia-dollaro-ACLbl5f

Maci, L. 2020. *Da Libra a Diem: cos'è, come funziona e cosa aspettarsi dalla criptovaluta di Facebook*, Economyup, https://www.economyup.it/fintech/libra-facebook-cose-come-funziona-e-cosa-aspettarsi-dalla-criptovaluta-di-cui-tutti-parlano/

The Diem Association. 2022. Diem.com, https://www.diem.com/en-us/

Valsania, M. 2020. *Facebook: dalle ceneri di Libra nasce Diem, legata al dollaro*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/facebook-ceneri-libra-nasce-diem-legata-dollaro-ADeGGo5

Claeys, G., Demertzis, M., and Efstathiou, K. 2018. Cryptocurrencies and monetary policy, Econstor.eu, Advance Access published 2018: doi:http://hdl.handle.net/10419/208013

Occasional Paper Series Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

Echelpoel, F. van E., Chimienti, M. T., Adachi, M. M., Athanassiou, P., Balteanu, I., Barkias, T., Ganoulis, I., Kedan, D., Neuhaus, H., Pawlikowski, A., Philipp, G., Poignet, R., Sauer, S., Schneeberger, D., et al. 2020. Stablecoins: Implications for Monetary Policy, Financial Stability, Market Infrastructure and Payments, and Banking Supervision in the Euro Area, *SSRN Electronic Journal*, Advance Access published 2020: doi:10.2139/ssrn.3697295

He, D. 2018. Crypto assets may one day reduce demand for central bank money, date last accessed at https://www.imf.org/external/pubs/ft/fandd/2018/06/central-bank-monetary-policy-and-cryptocurrencies/he.pdf

Ron, D. and Shamir, A. How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?

https://it.wikipedia.org/wiki/Tor_(software)#Descrizione.

Look, C. 2021. *Lagarde Blasts Bitcoin's Role in Facilitating Money Laundering*, Bloomberg.com, https://www.bloomberg.com/news/articles/2021-01-13/lagarde-blasts-bitcoin-s-role-in-facilitating-money-laundering

M. Croce | Cyberlaundering e valute virtuali. 2021. www.sistemapenale.it, https://www.sistemapenale.it/it/articolo/cyberlaundering-valute-virtuali-la-lotta-al-riciclaggio-nellera-della-distributed-economy

Sammuri, L Finanziamento al terrorismo internazionale e paradisi fiscali

Criptovalute: cos'è Monero, quanto conviene utilizzarlo - Blockchain 4innovation. 2020. Blockchain 4innovation, https://www.blockchain4innovation.it/criptovalute/criptovalute-cose-monero-quanto-conviene-utilizzarlo/

Cacioppoli, V. 2021. *Ultima chiamata per i creditori di Mt Gox*, The Cryptonomist, https://cryptonomist.ch/2021/10/08/ultima-chiamata-per-i-creditori-di-mt-gox/

https://en.wikipedia.org/wiki/Coincheck#cite_note-7

Shane, D. 2018. *$530 million cryptocurrency heist may be biggest ever*, CNNMoney, https://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html

Simonetta, B. 2021. *Ransomware inarrestabili. Ecco quanto costa la pandemia digitale*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/ransomware-inarrestabili-ecco-quanto-costa-pandemia-digitale-AEh86Kr

Annunziata, M. 2020. *Ransomware e criptovalute: due facce della stessa medaglia*, Treccani, l'Enciclopedia italiana, https://www.treccani.it/magazine/atlante/societa/Ransomware_criptovalute.html

Treasury Takes Robust Actions to Counter Ransomware. 2021. U.S. Department of the Treasury, https://home.treasury.gov/news/press-releases/jy0364

-"SoK: Cryptojacking Malware", Ege Tekiner, Abbas Acar, A. Selcuk Uluagac, Engin Kirda, Ali Aydin Selcuk, 2021.

Il cryptojacking – Una duplice minaccia sempre più diffusa: l'accoppiata cryptojacker-ransomware. 2016. Acronis.com, https://www.acronis.com/it-it/articles/cryptojacking/

Malwarebytes. 2018. *Cryptojacking – Cos'è e come funziona.*, Malwarebytes, https://it.malwarebytes.com/cryptojacking/

Sophoslabs, S., Managed, T., and Response. 2020. Navigating cybersecurity in an uncertain world:, date last accessed at https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf

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

Cambridge Bitcoin Electricity Consumption Index (CBECI). 2020. Ccaf.io, https://ccaf.io/cbeci/index/comparisons

Bitcoin Uses More Electricity Than Many Countries. How Is That Possible? 2022. *The New York Times*

Digiconomist. 2021. *Bitcoin's growing e-waste problem - Digiconomist*, Digiconomist, https://digiconomist.net/bitcoins-growing-e-waste-problem/

Digiconomist. 2021. *Bitcoin Electronic Waste Monitor - Digiconomist*, Digiconomist, https://digiconomist.net/bitcoin-electronic-waste-monitor/

Jiang, S., Li, Y., Lu, Q., Hong, Y., Guan, D., Xiong, Y., and Wang, S. 2021. Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China, *Nature Communications*, vol. 12, no. 1

de Vries, A. 2019. Renewable Energy Will Not Solve Bitcoin's Sustainability Problem, *Joule*, vol. 3, no. 4, 893–98

Kim, C. 2020. *The Rise of ASICs: A Step-by-Step History of Bitcoin Mining*, @coindesk, https://www.coindesk.com/tech/2020/04/26/the-rise-of-asics-a-step-by-step-history-of-bitcoin-mining/

McGregor, G. 2021. *China already banned crypto mining. Now it's cracking down on any holdouts*, Fortune, https://fortune.com/2021/11/17/china-bitcoin-mining-ban-crypto-holdouts-ether-solana-price/

The 28 Most Sustainable Cryptocurrencies for 2022 - LeafScore. 2021. LeafScore, https://www.leafscore.com/blog/the-9-most-sustainable-cryptocurrencies-for-2021/

Bitcoin: cos'è, come funziona e a cosa serve - Blockchain 4innovation. 2021. Blockchain 4innovation, https://www.blockchain4innovation.it/bitcoin/bitcoin-cose-come-funziona-e-a-cosa-serve/

Whitepaper Ethereum | ethereum.org. 2022. ethereum.org, https://ethereum.org/it/whitepaper/

Non-fungible tokens (NFT) | ethereum.org. 2020. ethereum.org, https://ethereum.org/en/nft/

Accademia Bit2Me. 2020. *Cos'è il gas in Ethereum?*, Bit2Me Academy,https://academy.bit2me.com/it/cos%27%C3%A8-il-gas-in-Ethereum/

History of Ethereum in Timeline - Popular Timelines. 2013. populartimelines.com, https://populartimelines.com/timeline/Ethereum

Applebaum, S., Jain, T., and Samani, K. MULTICOIN CAPITAL BINANCE COIN ($BNB) Analysis and Valuation: date last accessed February 17, 2022, at https://assets.ctfassets.net/qtbqvna1l0yq/4XdZJHThSHWvk1NV2Tt9ZD/21a23e0d8e2937bb6a4a1f1ba057b5ad/Binance_Analysis.pdf

https://en.wikipedia.org/wiki/Binance

Binance Academy. 2018. *What Is a Coin Burn?*, Binance Academy, https://academy.binance.com/en/articles/what-is-a-coin-burn

Reiff, N. 2022. *What Is Cryptocurrency Burning?*, Investopedia, https://www.investopedia.com/tech/cryptocurrency-burning-can-it-manage-inflation/

Khatri, Y. 2021. *Binance destroys $595 million worth of BNB tokens in its largest-ever burn*, The Block, https://www.theblockcrypto.com/linked/101912/binance-15th-quarterly-bnb-burn-token-highest-ever

Eurostoxx 50. 2021. Money.it, https://www.money.it/+Eurostoxx50+

https://it.wikipedia.org/wiki/Euro_Stoxx_50

https://it.wikipedia.org/wiki/FTSE_MIB

https://it.wikipedia.org/wiki/London_Stock_Exchange_Group

https://en.wikipedia.org/wiki/Nasdaq

https://it.wikipedia.org/wiki/NASDAQ_Composite

https://it.wikipedia.org/wiki/NASDAQ_Composite

Chen, J. 2022. *What Is the Nasdaq Composite Index?*, Investopedia, https://www.investopedia.com/terms/n/nasdaqcompositeindex.asp

Cos'è l'indice borsistico NASDAQ Composite? 2012. Strategie-bourse.com, https://www.strategie-bourse.com/it/indice-nasdaq-composite.html

La Teoria del Mercato Efficiente - Eugene F. Fama. 2019. Performancetrading.it, https://www.performancetrading.it/Documents/Uomini/SF_Mercato_Fama.htm

Profit, N. 2021. *Bitcoin Was First Used To Buy Pizza. Other Interesting Tidbits*, NDTV.com, https://www.ndtv.com/business/the-first-bitcoin-transaction-was-for-buying-pizzas-more-interesting-tidbits-inside-2512643

Scozzari, C. 2021. *El Salvador è il primo Paese dove il bitcoin è moneta legale. Il presidente Bukele ne ha comprati per 21 milioni di dollari*, La Stampa, https://www.lastampa.it/economia/2021/09/07/news/el-salvador-e-il-primo-paese-dove-il-bitcoin-e-moneta-legale-il-presidente-bukele-ne-ha-comprati-per-21-milioni-di-dollari-1.40677014/

Reiff, N. 2022. *Bitcoin ETFs Explained*, Investopedia, https://www.investopedia.com/investing/bitcoin-etfs-explained/

Mastrodonato, L. 2021. *Bitcoin, il primo etf basato sul prezzo è stato lanciato a Wall Street - Wired*, Wired Italia, https://www.wired.it/economia/finanza/2021/10/21/bitcoin-etf-finanza-borsa-new-york/

Hayes, A. 2022. *What Happens to Bitcoin After All 21 Million Are Mined?*, Investopedia, https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/

Singh, J. 2021. *Can Bitcoin's hard cap of 21 million be changed?*, Cointelegraph, https://cointelegraph.com/explained/can-bitcoins-hard-cap-of-21-million-be-changed

Bit2Me Academy. 2018. *What is Litecoin (LTC)?*, Bit2Me Academy, https://academy.bit2me.com/en/what-is-litecoin-ltc-cryptocurrency/

https://en.wikipedia.org/wiki/Litecoin

Litecoin Price, Chart & History. 2019. Coinhouse, https://www.coinhouse.com/litecoin-price/#:~:text=Litecoin%20was%20created%20by%20Charlie%20Lee%20in%20October%202011.&text=The%20creator%20of%20Litecoin%2C%20Charlie,popular%20in%20the%20crypto%20market.

Frankenflied, J. 2022. *What Is Litecoin (LTC)?*, Investopedia, https://www.investopedia.com/terms/l/litecoin.asp#citation-7

Accademia Bit2Me. 2019. *Cos'è Monero (XMR)?*, Bit2Me Academy, https://academy.bit2me.com/it/cos%27%C3%A8-la-criptovaluta-monero-xmr/

About Monero. 2014. getmonero.org, The Monero Project, https://www.getmonero.org/resources/about/

The Complete History of Monero (XMR). 2014. Coinloan.io, https://coinloan.io/article/the-complete-history-of-monero-xmr/

Markowitz, H. 1952. Portfolio Selection, *The Journal of Finance*, vol. 7, no. 1, 77–91

Masala, G.B., and M., Micocci. *Manuale di matematica finanziaria. Metodi e strumenti quantitativi per il risk management*.Carocci, 2012.

Campbell, John Y., Lo, Andrew W. and MacKinlay, A. Craig. "The Econometrics of Financial Markets". The Econometrics of Financial Markets, Princeton: Princeton University Press, 2012.

Massimiliano Carrà. 2019. *Teoria di Markowitz: ecco cosa è e a cosa serve*, Money.it, https://www.money.it/Teoria-di-Markowitz-ecco-cos-e-a-cosa-serve-costruzione-portafoglio#:~:text=Ecco%20cosa%20%C3%A8%20e%20a%20cosa%20serve%20la%20teoria%20di%20Harry,rischio%20e%20massimizzi%20il%20rendimento&text=rendimento%20atteso%3A%20quanto%20l'investitore,o%20pi%C3%B9%20titoli%20nel%20futuro.

Yahoo Finanza - Mercato azionario in tempo reale, quotazioni e notizie di economia e finanza. 2022. https://it.finance.yahoo.com/

FTSE MIB Index. 2022. Wsj.com, https://www.wsj.com/market-data/quotes/index/IT/MTAA/I945/historical-prices (date last accessed February 17, 2022)

Giorgi, G. 2021. *Monete digitali e banche centrali, convergenze e sfide*, Il Sole 24 ORE, https://www.ilsole24ore.com/art/monete-digitali-e-banche-centrali-convergenze-e-sfide-AELFNyp (date last accessed February 21, 2022)

European Central Bank. 2022. *Central bank digital currencies: defining the problems, designing the solutions*, European Central Bank, https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220218_1~938e881b13.en.html (date last accessed March 11, 2022)

Ringraziamenti

Ringrazio prima di tutto il professore Franco Varetto per la disponibilità che mi ha concesso, per la professionalità che ha dimostrato, per la passione che mi ha trasmesso in ogni spiegazione e per avermi sopportato e supportato in un momento così cruciale della mia vita.

Ringrazio la mia famiglia per il supporto e l'amore dimostratomi ogni giorno.

Un ringraziamento speciale va dato a Michele, Diego, Giacomo, Pamela, Carlo, Angela e Tobia per avermi tenuto compagnia e tirato su il morale nei momenti più bui.

Agli amici di sempre e a quelli più recenti, grazie.