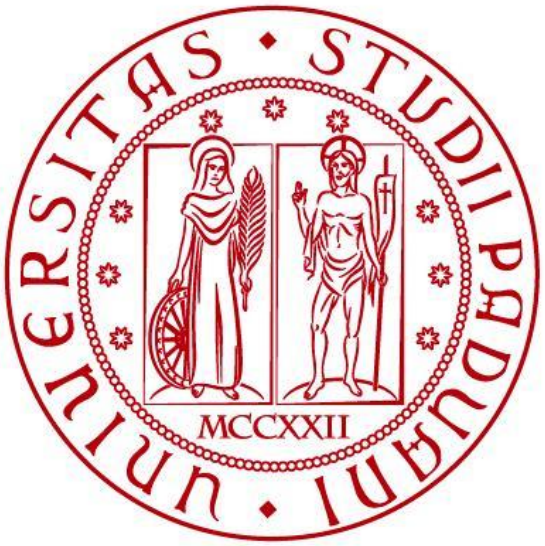


UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Scienze Statistiche

Corso di Laurea Triennale in
Statistica per l'Economia e l'Impresa

Analisi della profittabilità di strategie di trading applicate al mercato delle criptovalute

Relatore
Prof. Francesco Lisi

Candidato
Alberto De Simone
Matricola: 1198881

Anno Accademico 2022/2023

INDICE

1. INTRODUZIONE

Negli ultimi anni l'economia mondiale, soprattutto grazie all'evoluzione tecnologica ed informatica, ha visto sempre maggiori cambiamenti, in particolare l'introduzione di numerosi strumenti che sono andati ad aggiungersi al già complesso universo finanziario.
Un'importante novità, considerata una rivoluzione nel mondo digitale, è avvenuta nel 2009: la nascita della prima criptovaluta, il Bitcoin.
La crescente popolarità delle criptovalute ha suscitato un interesse considerevole nel mercato degli investimenti finanziari. Questo elaborato si propone di analizzare la profittabilità di strategie di trading applicate al mercato delle criptovalute, al fine di valutare l'efficacia di tali strategie nel generare rendimenti positivi.
Inizialmente, vengono descritti gli studi precedenti e i fatti storici relativi alle criptovalute. Si esplorano le strategie di previsione del prezzo e si approfondiscono le origini del fenomeno delle monete digitali.

La sezione seguente delinea l'universo delle criptovalute, concentrandosi nella prima parte sulla tecnologia blockchain e sulle sue caratteristiche chiave, come il registro distribuito digitale, la crittografia, la cybersecurity e gli algoritmi di consenso. Vengono anche esaminati i casi d'uso delle blockchain nel mondo reale, nonché le sfide legali, le considerazioni e le opportunità che rappresentano.
Un'attenzione particolare viene dedicata al Bitcoin e alla sua storia, comprese le origini attribuite a Satoshi Nakamoto, il limite di 21 milioni di unità, il processo di mining e l'evento dell'halving. Vengono inoltre analizzati modelli come lo Stock-to-Flow e il CBBI, oltre che le innovazioni portate dalla Lightning Network e dall'adozione di Bitcoin nel mondo.
Nel contesto delle altcoins, vengono esaminate criptovalute come Ethereum, considerata "l'argento digitale", le exchange coins, le "Ethereum Killer" coins, nonché l'applicazione delle criptovalute nell'Internet of Things, nel metaverso e nel settore degli NFT (Non-Fungible Token). Si esplorano anche le sinergie tra le criptovalute e l'intelligenza artificiale, gli oracoli e le stablecoin.

Nella sezione dedicata all'investimento in criptovalute, vengono analizzati i rischi e i vantaggi associati, le diverse tipologie di investimento e le modalità per condurre ricerche adeguate. Si illustra una strategia di investimento di successo, includendo l'individuazione del momento di ingresso ideale, la pianificazione di un approccio sostenibile, l'analisi fondamentale e il sentiment del mercato.

Si forniscono inoltre indicazioni sulla creazione di portafogli di criptovalute e sulla scelta di exchange e wallet affidabili.
In questa tesi vengono studiate le differenze del mercato delle criptovalute da quelli tradizionali, inoltre si analizzano dati storici sulle prestazioni di tale mercato e come questi possano essere utilizzati per formulare strategie di trading. La natura altamente volatile e complessa del mercato, combinata con i fenomeni di cluster, rende i tentativi di previsione più difficili e gli investimenti in criptovalute più rischiosi rispetto a quelli in altre attività finanziarie.
La ricerca esplora vari metodi per acquistare e vendere criptovalute nel tentativo di trarre profitto dai movimenti dei prezzi, proponendo l'utilizzo degli indicatori tecnici come strumenti per migliorare il processo decisionale e sviluppare strategie di trading efficaci.
Gli indicatori tecnici sono calcoli matematici basati sul prezzo, sul trend o su altre caratteristiche di un strumento finanziario, comunemente utilizzati dai trader per aiutare a identificare tendenze, modelli e potenziali opportunità di acquisto o vendita nel mercato delle criptovalute. Questi indicatori possono rivelarsi utili in una varietà di strategie di trading, tra quelli più diffusi nel mercato delle criptovalute vengono approfonditi i seguenti: le medie mobili (SMA, WMA, EMA), il Relative Strength Index (RSI), il Moving Average Convergence / Divergence (MACD) e le bande di Bollinger.

Successivamente, viene condotta un'analisi dettagliata della profittabilità delle strategie di trading. Sono descritti i passaggi per la raccolta dei dati, la visualizzazione grafica e l'analisi statistica, comprese le correlazioni tra le criptovalute.
Dopo aver scelto le criptovalute più influenti sul mercato, queste vengono utilizzate con gli indicatori tecnici precedentemente descritti e, in particolare, rappresentano gli asset sui quali vengono elaborate e analizzate alcune strategie di trading LONG e SHORT, basate sulle bande di Bollinger e sull'RSI.
Inoltre, vengono create delle strategie di HOLDing di lungo termine, mediante l'utilizzo di 3 differenti tipologie di Periodic Acquiring Cost (PAC), le quali vengono testate su tutte le criptovalute analizzate durante l'elaborato.
Dal confronto dei risultati delle diverse strategie di trading utilizzate vengono scelte le più efficaci, ovvero quelle maggiormente redditizie, valutando le implicazioni per trader e investitori. Infine, si discutono i limiti dello studio e si offrono prospettive per ulteriori ricerche in questo campo in continua evoluzione.

1.1 OBIETTIVI

Il prezzo di Bitcoin, come quello di altre criptovalute, è conosciuto per essere molto volatile e imprevedibile.
L'obiettivo di questo elaborato è analizzare la profittabilità di alcune strategie di trading applicate al mercato delle criptovalute, predisposto per queste metodologie essenzialmente per due ragioni:

1. la presenza di elevati livelli di volatilità;
2. la presenza di elevati livelli di correlazione tra le diverse monete digitali.

La volatilità degli asset finanziari esprime la caratteristica statistica delle serie storiche che tendono a discostarsi dal valore medio con maggiore ampiezza. Elevati livelli di volatilità possono essere interpretati come sintomo di un'instabilità del mercato, che può essere sfruttata attraverso strategie di trading.

È noto che la volatilità non è osservabile, quindi bisogna utilizzare metodologie efficienti che possano accuratamente cogliere tali movimenti dal prezzo. In questo elaborato viene effettuata un'analisi mediante il software RStudio, specificando determinate regole di trading, utilizzando delle strategie basate su alcuni indicatori tecnici, in particolare le Bollinger Band e l'RSI. Vengono anche elaborate delle strategie basate sull'HOLDing a lungo termine. Attraverso il raggiungimento di questi obiettivi, la tesi mira a fornire una comprensione approfondita delle strategie di trading nel contesto delle criptovalute e ad offrire un contributo significativo alla conoscenza nel settore.

1.2 STUDI PRECEDENTI E FATTI STORICI

Nella ricerca di strategie di trading proficue per il mercato delle criptovalute, sono stati condotti diversi studi precedenti che hanno esplorato l'applicazione di modelli e tecniche di previsione del prezzo, nonché l'analisi di fatti storici rilevanti.
Questi studi hanno cercato di trovare algoritmi efficaci e feature significative per migliorare la capacità di previsione, contribuendo a sviluppare una comprensione più approfondita dei movimenti del mercato delle criptovalute e delle possibili strategie per ottenere profitti.
Di seguito sono riportati alcuni esempi di ricerche precedenti e fatti storici significativi.

1.2.1 Strategie per la previsione di trend e prezzo

Nonostante la giovane età delle criptovalute, strategie di previsione del prezzo o del suo trend vengono vagliate già da diversi anni dato l'alto interesse speculativo e non suscitato da un panorama così fortemente volatile.
Alcuni di questi approcci si basano sull'utilizzo di tecniche di machine learning e data mining, che consentono di estrarre conoscenze dai dati storici e di adattare modelli predittivi.
Nel 2015, Joao Almeida et al. hanno condotto uno studio per prevedere il trend del prezzo di Bitcoin utilizzando reti neurali e dati storici di prezzo e volume.
I risultati hanno dimostrato che l'utilizzo delle reti neurali ha portato a guadagni superiori rispetto a una strategia di baseline che imitava il trend del giorno precedente. Inoltre, l'inclusione del volume di transazioni come feature aggiuntiva ha migliorato ulteriormente le performance.
Isaac Madan et al., nello stesso anno, hanno sviluppato sistemi di trading automatico basati su algoritmi di regressione, random forest e Support Vector Machine (SVM) per prevedere il prezzo o il trend di Bitcoin.
I risultati hanno mostrato un'alta accuratezza nella previsione del trend utilizzando regressione o random forest, mentre le SVM non hanno raggiunto prestazioni soddisfacenti. Inoltre, hanno evidenziato che l'aumento della frequenza di campionamento dei dati delle transazioni non aumentava l'accuratezza delle previsioni.

Huisu Jang et al. hanno condotto uno studio nel quale hanno utilizzato dati provenienti dalla blockchain e dalla macroeconomia, come il tasso di cambio di alcune valute legali rispetto al dollaro e il valore dei principali titoli azionari, per prevedere il prezzo intraday di Bitcoin. Utilizzando una rete neurale bayesiana, i ricercatori hanno ottenuto buoni risultati nella previsione della volatilità del prezzo.
Alex Greaves et al. hanno condotto uno studio sull'analisi dei movimenti di Bitcoin e dell'intera rete blockchain per cercare informazioni che potessero spiegare la crescente volatilità del prezzo. Hanno costruito un grafo orientato per identificare i principali investitori

e valutare l'influenza delle loro scelte sul mercato. Hanno utilizzato reti neurali per la previsione, ma hanno ottenuto risultati solo leggermente superiori al 50% di accuratezza.
Martina Matta et al. hanno studiato la correlazione del prezzo del Bitcoin con i volumi di tweet su Twitter e le tendenze di ricerca su Google. Hanno utilizzato l'analisi del sentiment per valutare la relazione tra le opinioni degli utenti e l'andamento del prezzo.
Young Bin Kim et al. hanno analizzato i dati dei forum online dedicati alle criptovalute, inclusi Bitcoin, Ethereum e Ripple, per misurare l'entità delle transazioni e valutare la correlazione con le fluttuazioni di prezzo.
Edwin Sin et al. hanno utilizzato reti neurali e algoritmi genetici per predire le variazioni del prezzo del Bitcoin. Hanno evidenziato l'importanza della selezione delle caratteristiche per migliorare l'accuratezza delle previsioni.

Arief Radityo et al. hanno confrontato modelli di previsione del prezzo di chiusura di Bitcoin utilizzando reti neurali e indicatori tecnici come la media mobile esponenziale. Hanno selezionato gli indicatori più efficaci per l'analisi.
Taiguara Melo Tupibnambàs ha sviluppato un classificatore associativo per le decisioni di acquisto o vendita di criptovalute, utilizzando algoritmi genetici per filtrare le regole decisionali. Ha utilizzato dati storici del prezzo con un time-frame di 15 minuti.
Nel 2016, Sean McNally et al. hanno confrontato l'efficacia delle tecniche di machine learning con l'analisi delle serie storiche basata sui modelli ARIMA nella previsione della direzione del prezzo del Bitcoin.
Hanno scoperto che le reti neurali hanno ottenuto un'accuratezza nettamente migliore rispetto ai modelli lineari stocastici, grazie alla loro capacità di riconoscere i trend nonostante la mancanza di stagionalità nei movimenti e l'alta volatilità.
Nel 2018, Seckin Karasu et al. hanno costruito modelli di SVM e regressione lineare per stimare il prezzo di chiusura del Bitcoin utilizzando dati giornalieri dal 2012 al 2018. Hanno utilizzato l'oscillatore Accumulazione/Distribuzione come indicatore tecnico per osservare gli effetti ciclici delle serie temporali.
Questo studio ha contribuito a comprendere meglio la correlazione tra diverse criptovalute e l'importanza di considerare i loro trend congiuntamente per acquisire informazioni chiave sulla loro evoluzione.

Muhammad Saad et al. hanno utilizzato metodi di machine learning per predire il prezzo di Bitcoin e hanno ottenuto ottimi risultati con un modello di regressione. Hanno selezionato le proprietà rilevanti dalla Blockchain pubblica di Bitcoin, filtrando le informazioni per concentrarsi sugli attributi con maggiore influenza sui cambiamenti di prezzo.
Hanno anche analizzato la correlazione tra le principali criptovalute calcolando il coefficiente di Pearson basato sui dati storici dei prezzi di mercato. Questa ricerca ha dimostrato l'importanza di una profonda analisi delle caratteristiche di input per migliorare l'accuratezza delle previsioni del prezzo.
Questi studi precedenti mostrano che l'utilizzo di tecniche di machine learning e data mining può fornire risultati promettenti nella previsione dei prezzi delle criptovalute. Tuttavia, è importante considerare che le criptovalute sono caratterizzate da una forte volatilità e da un contesto unico, che richiede approcci specifici per ottenere previsioni accurate.

1.2.2 Le origini delle criptovalute

Un primo accenno del concetto di criptovalute affonda le proprie radici nel lontano 1982 con la pubblicazione di un articolo di David Chaum intitolato “Blind Signature for Untraceable Payments”, nel quale venivano introdotte le “firme cieche” (“blind signatures”): una sorta di firma digitale che viene apposta sul messaggio prima che quest’ultimo venga aperto e letto. Nell’articolo erano spiegate le implicazioni pratiche di questo progetto nel settore dei pagamenti, che potevano realizzarsi senza la necessità di un controllo delle autorità e con l’adozione di forme anonime mediante l’utilizzo di pseudonimi.
Nel 1988 David Chaum pubblicò un giornale intitolato “The Dining cryptographers problem: unconditional sender and recipient untraceability”, nel quale per la prima volta venivano spiegati i concetti di “chiave pubblica” e “chiave privata”.
Il progetto di Chaum non ebbe una vera e propria realizzazione pratica, ma riuscì a ottenere l’interesse del movimento Cyberpunk: un gruppo di attivisti che vedevano nelle tecnologie informatiche e nella cibernetica degli strumenti utili per il cambiamento radicale nella società. Gli anarchici del movimento individuarono nel sistema di crittografia e cifratura pensato da Chaum uno strumento che potevano utilizzare alla loro lotta al potere; a tal punto da inserirlo nel manifesto dei Cripto – Anarchici del 1994.

Wei Dai, un membro del gruppo cyberpunk, grazie anche alle idee di Chaum, giunse ad un’idea concreta di criptovaluta, proponendo un sistema di interscambio di valore e stipulazione di contratti. Questi si basavano sull’uso di una moneta digitale che garantiva l’anonimato, la valuta in questione viene denominata “b-money”.
Wei Dai propose due protocolli nella sua presentazione di questo sistema di pagamento anonimo e distribuito:

1. Nel primo veniva presentato l’utilizzo di un proof of work, inteso come strumento per creare moneta online.
2. Nel secondo si spiegava come i partecipanti della rete erano in grado di verificare che il proprio importo non fosse stato soggetto a inflazione. Definiva anche le linee di partecipazione alla rete sostenendo che una somma di denaro era un requisito fondamentale per diventare server della rete, ma rischiava di essere perso se il server stesso si fosse rivelato “disonesto”.

Nonostante i notevoli progressi dell’Information Technology, il meccanismo teorizzato si scontrava con l’impossibilità di una sua implementazione pratica funzionale. Il problema riguardava principalmente il fenomeno della double spending: processo che consente di duplicare lo stesso token e spenderlo più volte.

Per la nascita ufficiale delle criptovalute bisogna aspettare fino al 18 agosto 2008 con la registrazione di bitcoin.org su “anonymousspeech.com”. Nell’ottobre dello stesso anno venne pubblicato online un white paper intitolato “Bitcoin A peer- to-peer electronic cash system”, contenente tutti i dettagli tecnici della criptovaluta che, ancora oggi, è ritenuta la più importante e, inoltre, proponeva per la prima volta l’idea di non tracciare la moneta, bensì le transazioni. Con la tracciabilità delle transazioni viene posto un freno al fenomeno della “double spending”, conferendo maggiore fiducia al sistema, infatti impedendo che gli stessi Bitcoin venissero utilizzati per transazioni differenti non era possibile creare moneta dal nulla.

Infine, l’avvento del mercato delle criptovalute risale solamente a poco più di 14 anni fa, era il mese di gennaio del 2009 quando Satoshi Nakamoto presentò il Bitcoin: la moneta virtuale per operare transazioni sicure su una rete peer-to-peer decentralizzata che garantisce anonimato e trasparenza grazie all’utilizzo di algoritmi crittografici.

2. L’UNIVERSO DELLE CRIPTOVALUTE

Le criptovalute sono nate sulla scia della crisi finanziaria globale del 2008 come una possibilità, per chi le detiene, di avere un controllo diretto sui propri risparmi, senza doversi affidare a banche, governi o altri servizi gestiti da intermediari finanziari.
Alcuni le vedono come un'alternativa al tradizionale denaro fiat, mentre altri come un investimento speculativo.
La vera innovazione portata da queste monete è l'uso della crittografia per controllare la creazione di nuove unità di valuta, per garantire transazioni finanziarie e per provare la proprietà di qualsiasi importo di valuta.
Queste monete sono risorse digitali progettate per essere mezzi di scambio, come Euro, Dollaro e Sterlina, basati su Internet e la loro particolarità è di essere state programmate con l’intento principale di scambiare informazioni digitali attraverso un processo basato sulla crittografia.
La finalità di questa “scrittura segreta”, basata su determinati algoritmi spesso molto complessi, risiede nel fatto che solo i destinatari delle informazioni sono in grado di leggere le stesse, evitando così che terzi soggetti riescano ad accedervi.
La resilienza della crittografia è garantita da una blockchain, che è un elenco di record chiamati blocchi, che non possono essere modificati retroattivamente una volta registrati. Le blockchain sono resistenti a modifiche dei dati perché si basano su una rete peer-to-peer che convalida ogni nuovo blocco.
In parole semplici, il sistema blockchain potrebbe assomigliare a un libro mastro aperto che registra transazioni verificabili tra le parti.

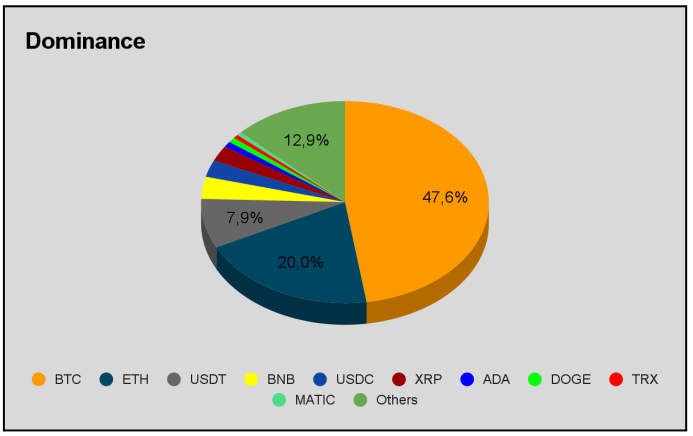
La blockchain promette di rendere le criptovalute decentralizzate. Mentre nelle economie centralizzate i governi controllano l'offerta di valuta stampando denaro, nei sistemi decentralizzati delle monete digitali, società e governi non possono controllarla. Inoltre, la maggior parte delle criptovalute è progettata per diminuire gradualmente la produzione di unità ponendo, in questo modo, un limite all'ammontare totale di quella valuta sul mercato.

Negli ultimi anni l’interesse circa la nuova tecnologia è stato in continua crescita e diverse nuove criptovalute sono state presentate sul mercato con l’intento di cavalcare l’onda rivoluzionaria del trend del momento.
Alcune copie della prima moneta hanno avuto origine da un vero e proprio distacco dalla blockchain di Bitcoin, detto hard fork. Dal momento che non sono ammesse modifiche del codice nativo, la creazione di una nuova moneta è l’unico modo per eseguire degli aggiornamenti consistenti. Il nuovo ramo viene creato esattamente come la blockchain da cui ha preso origine fino al punto di fork, ma le nuove transazioni non saranno più retrocompatibili.
Altre nuove valute digitali, non nate tramite hard fork, possono ugualmente essere considerate affini per diversi aspetti a quelle già ben consolidate.

Sono state sviluppate anche criptovalute che presentano nuove e distintive peculiarità, tali da renderle prodotti innovativi nel mercato.

Nel 2021, la capitalizzazione di mercato delle criptovalute ha superato la soglia di 2,8 bilioni (1 bilione = 1.000 miliardi) di USD (dollari USA), un aumento netto rispetto al valore raggiunto nel 2020 di 150 miliardi.
Sebbene il mercato sia composto da oltre 23.000 diverse criptovalute, le cinque più capitalizzate costituiscono più del 80% del totale, tra queste c'è un predominio di Ethereum, circa il 20% del totale, e di Bitcoin, più del 45%, che risulta dunque la più capitalizzata.

Grafico 1: Dominance delle 10 criptovalute più capitalizzate.



Il grafico 1 mostra la dominance, ovvero la percentuale di capitalizzazione di mercato delle criptovalute più dominanti, rispetto al totale. Dai valori riportati, si osserva immediatamente l'enorme influenza di BTC rispetto alla totalità del mercato (il 47,6% circa), ma anche il peso attribuito ad altre importanti monete digitali: ETH (19,9%), USDT (7,9%), BNB (3,5%) e USDC (2,7%).

2.1 LA BLOCKCHAIN

2.1.1 Registro distribuito digitale

La blockchain non è solo l'elemento più costruttivo e innovativo nel contesto delle criptovalute, ma anche una delle invenzioni più rivoluzionarie dell'era moderna.
Questo sistema è costruito su una complessa organizzazione di blocchi, che sono interconnessi e sicuri. Ogni blocco memorizza più transazioni convalidate ed è collegato al precedente tramite un hash, creando una catena di dati trasparente e immutabile.
Il timestamp associato a ciascun blocco aggiunge un ulteriore livello di sicurezza alla blockchain. Non solo convalida l'ora e la data di ogni transazione, ma garantisce anche che una volta registrata una transazione, non possa essere modificata o eliminata.
Questa caratteristica rende la blockchain ideale per la gestione della supply chain e la registrazione di transazioni che richiedono un elevato livello di trasparenza e sicurezza, come quelle finanziarie.
L'hash incluso in ogni blocco è quindi una componente fondamentale della sicurezza della blockchain. Questa funzione algoritmica non invertibile del computer identifica in modo univoco ogni blocco e crea una firma digitale che ne garantisce l'integrità.

Qualsiasi modifica al blocco altererebbe il suo hash, rendendo l'intera catena non valida. Questo rende la blockchain una tecnologia ideale per creare sistemi a prova di manomissione e identità digitali.

La blockchain rappresenta una tipologia di tecnologia chiamata registro distribuito (DLT) che permette la creazione di un database decentralizzato in cui è possibile archiviare numerose transazioni in un registro condiviso.
Questa rete si basa su una struttura elaborata che rende difficile la manipolazione o l'interruzione a causa della quasi impossibilità di apportare modifiche alle transazioni.
Con l'utilizzo di numerosi nodi si genera un unico archivio digitale, accessibile a tutti e che garantisce trasparenza e tracciabilità.
I DLT si riferiscono quindi a un insieme di sistemi che utilizzano un libro mastro distribuito per consentire l'accesso a più nodi di una rete. Forniscono, inoltre, un meccanismo di validazione basato sul concetto di consenso, distribuito in tutta la rete.
Le modalità di gestione del consenso, insieme alla logica di costituzione del registro, sono due dei principali punti di forza delle tecnologie di Distributed Ledger.

Uno dei vantaggi della tecnologia blockchain è che consente la creazione di una piattaforma trasparente e sicura per le transazioni senza la necessità di intermediari. Utilizzando algoritmi crittografici e meccanismi di consenso, fornisce un sistema decentralizzato che garantisce l'integrità e la trasparenza dei dati, rendendo difficile per gli attori malintenzionati manipolare il sistema.
Un’altra delle caratteristiche più notevoli della blockchain è la sua sicurezza. Dalla sua creazione nel 2009, sono stati fatti innumerevoli tentativi di hacking, ma nessuno ha avuto successo. Questo perché la blockchain è distribuita su un numero enorme di computer e ciò la rende praticamente inviolabile.
La sua rete, basata sul sistema P2P o "Peer-to-Peer", è composta da tanti computer con la stessa rilevanza, senza la presenza di un software centrale.

In sintesi, la blockchain si basa su cinque concetti fondamentali: trasparenza, sicurezza, immutabilità, decentralizzazione e consenso. Questi principi ne hanno fatto la declinazione digitale di un nuovo concetto di fiducia, che ha il potenziale per rivoluzionare la democrazia fornendo una piattaforma realmente distribuita per verificare, controllare e mantenere la trasparenza su azioni e scelte. La blockchain consente la creazione di archivi condivisi che sono inalterabili, immutabili e immuni dalla corruzione.
Sebbene sia spesso associata alle valute virtuali e ai pagamenti digitali, il suo valore va oltre la finanza, poiché ha il potenziale per essere utilizzata in diversi settori, dalla gestione della supply chain ai sistemi di voto, fornendo una piattaforma sicura e trasparente per la gestione delle transazioni e lo scambio di informazioni e dati.

Abbiamo visto come la crittografia, grazie all'utilizzo di algoritmi matematici per codificare i dati, sia in grado di proteggere le comunicazioni e le informazioni da accessi e manipolazioni non autorizzati, rendendole leggibili solo dalle parti autorizzate. Questa scrittura, infatti, è utilizzata in molte applicazioni, comprese le comunicazioni sicure su Internet, le transazioni elettroniche e le firme digitali.
Nel contesto della tecnologia blockchain, la crittografia svolge un ruolo fondamentale nel proteggere la rete e garantire l'integrità delle transazioni.
La blockchain utilizza due tipi di chiavi crittografiche: pubbliche e private.

Le chiavi pubbliche vengono utilizzate per ricevere transazioni e sono visibili a tutti sulla rete. Sono essenzialmente un indirizzo che altri utenti possono utilizzare per inviare criptovalute al proprio portafoglio.
Le chiavi private, invece, vengono utilizzate per firmare le transazioni e vengono mantenute segrete. Sono essenzialmente una lunga stringa di caratteri che viene utilizzata per dimostrare la proprietà di una particolare chiave pubblica.
Le chiavi private vengono generate in modo casuale e non dovrebbero mai essere condivise con nessuno, in quanto garantiscono l'accesso alle risorse digitali.
Quando un utente invia criptovalute alla chiave pubblica di un altro utente, il primo utilizza la propria chiave privata per firmare la transazione. L'algoritmo di hashing prende i dati della transazione e crea un hash univoco che rappresenta la transazione.
La chiave privata dell'utente viene quindi utilizzata per crittografare l'hash, creando la firma digitale, che viene trasmessa alla rete e verificata da altri nodi per garantire che l'utente disponga di fondi sufficienti per completare la transazione e che quest'ultima sia valida, ovvero sia stata inviata dal proprietario dell'indirizzo del portafoglio.
Le firme digitali forniscono un modo per garantire che le transazioni sulla blockchain siano sicure e a prova di manomissione. Qualsiasi tentativo di modificare i dati della transazione comporterà una firma non valida, avvisando la rete di potenziali frodi.

I merkle tree, noti anche come hash tree, sono un tipo di struttura dati utilizzata per organizzare e verificare in modo efficiente grandi quantità di dati. Nel contesto della blockchain, gli alberi Merkle vengono utilizzati per verificare l'integrità dei dati della transazione.
Gli alberi Merkle funzionano suddividendo un ampio set di dati in blocchi più piccoli e più gestibili. Ogni pezzo di dati viene sottoposto ad hashing, creando un valore hash univoco che rappresenta quel pezzo di dati. I valori hash vengono quindi combinati e sottoposti nuovamente a hash finché non rimane un solo hash root.
In una rete blockchain, l'hash radice di Merkle è incluso nell'intestazione del blocco insieme ad altri dati importanti come il timestamp e l'hash del blocco precedente. Questo crea una catena di blocchi che sono collegati tra loro utilizzando hash crittografici, da cui il nome "blockchain".

Tuttavia, come qualsiasi altra tecnologia, la blockchain non è immune da minacce per la sicurezza informatica.
In una rete blockchain, un attacco del 51% si verifica quando una singola entità o un gruppo di entità controlla più del 50% della potenza di calcolo nella rete. Ciò consente loro di manipolare i dati della transazione e potenzialmente raddoppiare la criptovaluta.
Un attacco Sybil avviene quando un utente malintenzionato crea più identità o nodi falsi in una rete blockchain. Questi nodi falsi possono essere utilizzati per manipolare l'algoritmo di consenso e interrompere la rete.
Gli attacchi di malware e phishing sono minacce informatiche comuni che possono prendere di mira gli utenti blockchain. Questi attacchi possono portare al furto di chiavi private, che possono concedere l'accesso alle risorse digitali di un utente.
Gli smart contract sono contratti auto eseguibili scritti in codice ed eseguiti su una rete blockchain. Tuttavia, se ci sono vulnerabilità nel codice, gli hacker possono sfruttarle e, potenzialmente, rubare risorse o interrompere la rete.

Insider threats si riferiscono al rischio di attacchi o violazioni dei dati dall'interno di un'organizzazione o di una rete. Gli addetti ai lavori con accesso a informazioni sensibili o risorse di rete possono potenzialmente causare danni significativi a una rete blockchain.

La protezione di una rete blockchain richiede quindi un approccio globale che comprenda varie best practice e misure di sicurezza.
La crittografia, come già visto, convertendo testo normale in testo cifrato, è fondamentale per la sicurezza blockchain e viene utilizzata per proteggere dati sensibili come chiavi private e transazioni.
L'autenticazione a più fattori (MFA), richiedendo agli utenti di fornire due o più forme di autenticazione per accedere a un sistema o a una rete, rappresenta una forma di sicurezza che può aiutare a prevenire l'accesso non autorizzato a una rete blockchain oltre che a proteggere i dati sensibili.
Gli algoritmi di consenso vengono utilizzati per garantire che tutti i nodi in una rete blockchain concordino sullo stato della rete e sono essenziali per prevenire attacchi come quelli del 51% e quelli double spending.
Anche gli aggiornamenti software eseguiti regolarmente sono molto utili per affrontare le vulnerabilità e migliorare la sicurezza di una rete blockchain.
Il controllo degli smart contract è il processo di revisione del codice dei contratti per identificare e affrontare le vulnerabilità. Controlli regolari degli smart contract possono aiutare a prevenire gli attacchi e proteggere la rete dalle violazioni della sicurezza.
In più, anche la gestione delle chiavi private è fondamentale per proteggere le transazioni blockchain. Fondamentale archiviarle in luoghi sicuri e proteggerle da password complesse e autenticazione a più fattori.

2.1.2 Algoritmi di consenso e casi d’uso nel mondo reale

Di fondamentale importanza è il concetto di Proof of Work (PoW), che è una delle idee alla base della tecnologia blockchain. Consente la creazione di un consenso distribuito ed elimina la necessità di terze parti per garantire la validità delle transazioni. Questo sistema mantiene un libro mastro privato, in cui vengono archiviati la cronologia delle transazioni e i saldi di ciascun conto.

Proof of Work è il primo algoritmo di consenso utilizzato in una rete blockchain. Questo processo richiede una notevole potenza di calcolo ed energia e viene utilizzato per confermare le transazioni e produrre nuovi blocchi nella catena.
Bitcoin, che utilizza l'algoritmo SHA-256, è un ottimo esempio di criptovaluta che utilizza PoW come algoritmo di consenso.
Con il PoW, i “miners” competono tra loro per risolvere un complesso problema matematico, noto come hash puzzle, al fine di aggiungere un nuovo blocco, contenente le transazioni confermate, alla blockchain. Sono premiati con nuovi BTC e commissioni di transazione quando hanno successo.

Proof of Stake (PoS) è un algoritmo di consenso che sta guadagnando popolarità come alternativa più ecologica e scalabile a Proof of Work (PoW) nel mondo blockchain.

A differenza del PoW, nel PoS i validatori (o staker) vengono scelti per creare un nuovo blocco in base alla quantità di criptovalute che detengono e sono disposti a utilizzare come garanzia, in un processo chiamato staking.
Ciò riduce significativamente il consumo di energia e consente la realizzazione di una rete più scalabile, questo viene fatto per incentivare il buon comportamento e penalizzare quello malevolo, poiché i validatori possono perdere le loro criptovalute in stake se agiscono in modo dannoso.
Nel complesso, PoS è uno sviluppo entusiasmante che risolve alcuni dei limiti di PoW. Ha il potenziale per diventare un algoritmo di consenso più sostenibile ed efficiente, in quanto elimina la necessità di mining ad alta intensità energetica e incoraggia una maggiore partecipazione da parte dei membri della comunità.
Inoltre, diverse tipologie di algoritmi PoS vengono sviluppati e implementati in varie reti blockchain. Ogni variante ha caratteristiche e vantaggi unici, come maggiore sicurezza, scalabilità ed efficienza.

Il consenso BFT (Byzantine Fault Tolerance) è un meccanismo tollerante ai guasti utilizzato nelle reti distribuite per garantire consenso e coerenza tra i nodi, anche quando alcuni sono difettosi o dannosi.
BFT funziona utilizzando un processo di voto tra un insieme di nodi fidati per confermare le transazioni e aggiungerle alla blockchain. Per raggiungere questo consenso, i nodi comunicano tra loro, scambiandosi informazioni e utilizzando un insieme di regole per determinare quali transazioni siano valide.
Il meccanismo BFT non richiede grandi quantità di potenza di calcolo per convalidare le transazioni, a differenza del PoW. Può anche raggiungere velocità di transazioni più elevate rispetto al PoW, poiché ogni nodo può convalidare le transazioni in modo indipendente senza attendere che altri nodi completino i propri calcoli.
BFT è notevolmente sicuro contro gli attacchi, infatti è progettato per tollerare comportamenti dannosi da un massimo di un terzo dei nodi della rete.
Il consenso BFT può essere altamente decentralizzato, poiché i nodi possono venire aggiunti o rimossi dalla rete senza influire sul meccanismo di consenso generale. Ciò è in contrasto con il PoS, dove il numero di validatori è limitato dalla quantità di stake che detengono nella rete.

Il meccanismo di consenso PoA (Proof of Authority) è un altro tipo di algoritmo di consenso utilizzato nelle blockchain. Si basa su un gruppo di validatori o nodi pre-approvati che hanno l'autorità per convalidare le transazioni e creare nuovi blocchi.
Il PoA è progettato per essere più veloce ed efficiente dal punto di vista energetico rispetto ad altri meccanismi di consenso, come il Proof of Work (PoW). È anche più sicuro rispetto, ad esempio, al Proof of Stake (PoS).
Il consenso PoA è particolarmente utile per le reti blockchain autorizzate in cui i validatori sono conosciuti e affidabili.

PoH (Proof of History) è un nuovo meccanismo di consenso sviluppato dalla blockchain di Solana (SOL). È progettato per fornire una fonte temporale verificabile e sicura per la rete, consentendo un'elaborazione rapida delle transazioni.
PoH funziona creando un record storico di timestamp che può essere facilmente verificato da altri nodi della rete. Ciò consente un meccanismo di consenso rapido ed efficiente in grado di scalare per gestire elevati volumi di transazioni.

Tendermint è stato introdotto per la prima volta dalla rete Cosmos ed è ora ampiamente utilizzato in molte altre reti blockchain. Utilizza un'architettura a due livelli che separa il consenso e l'elaborazione dell'applicazione. Il livello di consenso è responsabile della conferma delle transazioni e dell'aggiunta alla blockchain, mentre il livello dell'applicazione gestisce la logica aziendale della blockchain.
Tendermint è un'implementazione dell'algoritmo di consenso Byzantine Fault Tolerance (BFT). Mentre sia BFT che Tendermint hanno obiettivi simili di raggiungere il consenso nei sistemi distribuiti, anche in presenza di nodi difettosi o dannosi, ci sono alcune differenze tra loro.
Con il BFT, ogni nodo viene trattato allo stesso modo e non esiste un nodo leader specifico che abbia più potere di altri. Al contrario, Tendermint ha un nodo leader designato, noto come "set di convalida", che è responsabile della proposta di nuovi blocchi e del coordinamento del processo di consenso.
Nel BFT ogni nodo invia in modo indipendente una proposta e il consenso viene raggiunto attraverso più turni di votazione. Con Tendermint il leader del set di validatori propone un blocco, che viene poi votato dagli altri nodi del validatore; se più di due terzi dei validatori concordano, il blocco viene aggiunto alla catena.

Passando alla parte pratica, la tecnologia blockchain ha il potenziale per migliorare l'efficienza, la trasparenza e la sicurezza in diversi settori.
Nel settore dei servizi finanziari, la blockchain offre un sistema di pagamento più sicuro ed efficiente. Può semplificare i processi di negoziazione, riducendo i tempi e i costi associati alla compensazione e al regolamento, aumentando la trasparenza e diminuendo i rischi per gli istituti finanziari. Inoltre, la blockchain può automatizzare transazioni finanziarie tramite smart contract, migliorare la gestione delle risorse finanziarie fornendo un registro trasparente e semplificare i pagamenti transfrontalieri.

Nel settore della gestione della supply chain, la blockchain può automatizzare processi come il pagamento delle fatture e il monitoraggio dell'inventario, riducendo errori e aumentando la produttività. Inoltre, aiuta a tracciare e verificare pratiche sostenibili e previene la vendita di prodotti contraffatti.

Nel settore sanitario, la blockchain offre un sistema sicuro ed efficiente per l'archiviazione e la condivisione delle cartelle cliniche, migliorando la privacy dei pazienti e riducendo il rischio di violazioni dei dati. Facilita l'interoperabilità tra sistemi sanitari, migliorando la qualità delle cure e diminuendo gli errori medici. La blockchain può gestire le sperimentazioni cliniche, tracciare il ciclo di vita dei farmaci e facilitare la telemedicina.

Nel campo dei sistemi di voto, la blockchain offre un processo più trasparente ed efficiente. Cripta i voti e crea un registro decentralizzato e immutabile di ogni transazione, garantendo la sicurezza e l'integrità del processo elettorale. Permette ai votanti di tracciare il proprio voto e assicurarsi che sia stato registrato correttamente, prevenendo interferenze e frodi. Elimina la necessità di conteggi manuali dei voti e riduce i costi delle elezioni. Fornisce risultati immediati, riducendo i tempi di attesa.

Nella beneficenza, la blockchain migliora la trasparenza e l'efficienza nel monitoraggio e nella distribuzione delle donazioni, permette donazioni transfrontaliere più economiche ed

efficienti, automatizza la distribuzione delle donazioni e consente modelli di governance decentralizzati. Con l'evoluzione della tecnologia, si prevede che la blockchain si integri sempre più con l'intelligenza artificiale e il machine learning per migliorare ulteriormente la gestione delle donazioni e il monitoraggio dell'impatto.
Altri casi d'uso rilevanti sono i seguenti:

- Gestione della proprietà intellettuale: la blockchain può fornire un registro sicuro e immutabile della proprietà del copyright, automatizzare il processo di licenza e pagamento delle royalty e prevenire la contraffazione.
- Settore immobiliare: la blockchain semplifica il trasferimento della proprietà, permette la creazione di smart contract per l'esecuzione automatica dei termini di vendita o locazione e migliora la valutazione della proprietà.
- Gestione delle identità: la blockchain offre modalità sicure e decentralizzate per la verifica, la gestione e la condivisione delle informazioni personali, consentendo alle persone di mantenere il controllo delle proprie identità e prevenire frodi.
- Scambio di energia: la blockchain facilita lo scambio peer-to-peer di energia, monitora la produzione e il consumo di energia rinnovabile e ottimizza la domanda e l'offerta di energia.

2.1.3 Sfide, considerazioni e opportunità

Gli aspetti normativi e legali della blockchain sono considerazioni importanti per qualsiasi individuo o organizzazione che intenda impegnarsi in attività legate alla blockchain.
La tecnologia blockchain è un campo relativamente nuovo e in rapida evoluzione, che presenta sfide normative e legali uniche per molti paesi e giurisdizioni in tutto il mondo.
Una delle maggiori sfide è la mancanza di chiarezza su come le leggi e i regolamenti esistenti si applicano alla tecnologia blockchain.
Poiché la blockchain è una tecnologia decentralizzata e transfrontaliera, può essere difficile determinare quale legge della giurisdizione si applica a una particolare transazione o attività blockchain.
Di conseguenza, molti paesi e organismi di regolamentazione sono ancora in procinto di sviluppare nuove normative specifiche per la blockchain.

Altri aspetti normativi e legali della blockchain sono i seguenti:

- Privacy dei dati: la blockchain può esporre i dati personali poiché sono visibili a chiunque abbia accesso alla rete, quindi è necessario adottare misure di protezione dei dati.
- Applicabilità degli smart contract: questi contratti possono incontrare ostacoli nell'applicazione delle leggi tradizionali a causa delle loro caratteristiche codificate.
- Requisiti AML e KYC: le normative anti-riciclaggio e di identificazione del cliente sono necessarie per prevenire l'uso illecito delle transazioni blockchain.
- Proprietà intellettuale: la blockchain solleva questioni sulla proprietà dei dati archiviati e dei diritti di proprietà intellettuale ad essi associati.
- Responsabilità: la mancanza di un'autorità centrale rende difficile determinare la responsabilità in caso di controversie o errori di transazione.

È importante che le aziende e gli individui considerino attentamente questi problemi e si assicurino di rispettare le leggi e i regolamenti pertinenti, al fine di ridurre al minimo il rischio di controversie o errori sulla blockchain.

Uno dei principali punti di forza della tecnologia blockchain è la sua capacità di rivoluzionare il modo in cui archiviamo, condividiamo e gestiamo i dati. Fornendo una piattaforma affidabile e trasparente per le transazioni digitali, senza la necessità di intermediari, permette di creare registri digitali sicuri e a prova di manomissione. Queste sue caratteristiche hanno portato a numerose approvazioni e investimenti da parte di varie società, tra cui Daimler, Carrefour e Nasdaq.

Tuttavia, la tecnologia blockchain deve affrontare anche diverse sfide ed è importante valutare e gestire attentamente rischi e benefici del suo utilizzo, implementando adeguate misure di salvaguardia per garantire la protezione delle informazioni sensibili.
Nonostante i potenziali benefici, le fluttuazioni delle criptovalute hanno indebolito la fiducia degli investitori nella tecnologia blockchain, evidenziando la necessità di criptovalute stabili e regolamentate. La corsa globale per regolamentare il settore è in corso, poiché i paesi competono per cogliere le opportunità offerte dalla tecnologia blockchain affrontando i rischi associati alle asimmetrie informative e alle attività illegali.
Man mano che la tecnologia continua a svilupparsi e a maturare, diventa fondamentale superare le sfide che la blockchain deve affrontare, come le questioni normative e le preoccupazioni sulla privacy dei dati, al fine di realizzare appieno il suo potenziale. Più organizzazioni adottano la blockchain ed esplorano i suoi potenziali usi, più è probabile che assisteremo a continue innovazioni e sviluppi in questo campo entusiasmante e in rapida crescita.

2.2 BITCOIN

2.2.1 Il protocollo Bitcoin

Il 3 Gennaio 2009 avviene il lancio ufficiale di Bitcoin nel mercato: viene creato il primo blocco di 50 BTC, il Genesis Block. Questo viene anche chiamato blocco zero e contiene una frase che riporta il titolo di un articolo sulla front page del “Financial Times”: “Chancellor on brink of second bailout for banks”. A questo titolo sono stati attribuiti 2 significati:

1. Definire il giorno in cui è stato creato il primo blocco, dato che contiene le informazioni di questo articolo uscito nella stessa data del lancio di Bitcoin;
2. Introdurre uno degli obiettivi della criptomoneta, in quanto in quel periodo ci si trovava nel pieno della crisi economica mondiale e si valutava un possibile secondo aiuto alle banche mediante l’applicazione del “quantitative easing.” Uno degli scopi fondamentali di tale invenzione era proprio prendere le distanze da un sistema che si era rivelato fallimentare, causando ingenti danni economici alle whales ma anche ai piccoli investitori retails.

A più di 14 anni di distanza da tale pubblicazione, non è ancora nota l’identità del padre del Bitcoin; infatti l’autore del cosiddetto “Bitcoin White Paper” si è firmato sotto lo pseudonimo Satoshi Nakamoto.
Nel corso degli anni sono state formulate diverse ipotesi su chi potesse celarsi dietro a questo celebre e misterioso personaggio ma, nonostante l’impegno di ricercatori e autorità provenienti da numerosi paesi del mondo, nessuno è ancora in grado di poter dire né chi sia il creatore di tale strumento, né se esiste davvero qualcuno che muove i fili del sistema valutario digitale.

Una giornalista di nome Leah McGrath scrisse nel 2014, sulla rivista “Newsweek”, di aver scoperto l’identità di Satoshi Nakamoto, ma la persona interessata negò ogni tipo di coinvolgimento.
L’anno successivo uscì la notizia che il vero creatore fosse un imprenditore australiano di nome Craig Wright, anche grazie alle dichiarazioni dell’uomo si pensò di aver risolto questo mistero; Wright pubblicò online un post che diceva “Satoshi è morto, ma siamo solo all’inizio”. L’uomo però non riuscì a produrre le prove crittografiche della sua identità e, anche a causa di una serie di incongruenze, non riuscì a dimostrare la sua versione.
Al giorno d’oggi esistono solo alcune idee sull’identità e sul luogo in cui potrebbe trovarsi tale figura. Grazie a delle analisi effettuate da Stefan Thomas, programmatore svizzero e membro della comunità Bitcoin, sugli orari di pubblicazione di ogni post di network firmato da Satoshi Nakamoto, si deduce che fosse americano per via di una totale assenza di pubblicazioni dalle ore 23 alle ore 5 di mattina (orario di Greenwich).

Da questi elementi si possono trarre due conclusioni:

1. Bitcoin ha avuto il merito di fare da apripista nel settore ed è stato proprio grazie al lavoro dei creatori della criptovaluta che, successivamente, sempre più monete digitali sono state create ed adottate in tutto il mondo.
2. Sarà molto complesso risolvere l’enigma dell’identità di Satoshi Nakamoto, anche perché si sostiene che tale persona, o gruppo, sia in possesso di più di 1 milioni di Bitcoin, situazione che potrebbe metterlo troppo in esposizione.

La fornitura totale di Bitcoin è limitata a 21 milioni di monete. Questo massimale è stato stabilito da Satoshi Nakamoto nel white paper originale.
La ragione di questo limite è imitare la scarsità di oro e altri metalli preziosi, che sono limitati nell'offerta e, quindi, hanno un relativo valore.
Il limite di 21 milioni è integrato nel protocollo Bitcoin e non può essere modificato. Nei 14 anni trascorsi dalla creazione di Bitcoin sono state estratte oltre 19,3 milioni di monete (quasi il 93%) con poco meno di 1,7 milioni ancora da estrarre.
Ciò significa che l'offerta totale di Bitcoin alla fine raggiungerà (quasi) il suo limite e, quando questo avverrà, non verranno più creati nuovi Bitcoin. Prima di assistere a tale evento, però, dovranno passare circa altri 120 anni; le cause di questa enorme differenza temporale per l’estrazione, rispetto alla stessa estrazione nel periodo già trascorso, sono spiegate successivamente.

Il data mining è il processo di estrazione di informazioni utili da un ampio set di dati.
Nell'ambito di Bitcoin, il data mining si riferisce al processo di utilizzo di software specializzati e potenti computer per risolvere complessi problemi matematici o algoritmi al fine di convalidare e aggiungere nuove transazioni alla blockchain di Bitcoin. I “miners” vengono ricompensati con Bitcoin appena coniati per aver risolto i suddetti problemi e mantenuto l'integrità della blockchain.
E’ anche noto come "Bitcoin mining" ed è il processo fondamentale ed imprescindibile mediante cui vengono creati nuovi Bitcoin e aggiunti all'offerta esistente, mantenendo la rete stabile e sicura.
Si può considerare come il centro dati di Bitcoin, ad eccezione del fatto che è stato progettato per essere totalmente decentralizzato, infatti i miners operano in tutte le nazioni senza che nessun individuo abbia il controllo della rete.

Il termine “minare” Bitcoin viene usato perché il processo per ottenerli ricorda il lavoro delle miniere: richiede l’estrazione e crea lentamente nuova moneta, un po’ come veniva fatto in passato con l’oro o altri metalli preziosi.
Mining è, quindi, anche il processo attraverso il quale i Bitcoin vengono immessi nel sistema, ai cosiddetti miners vengono pagate delle fee come commissioni delle nuove monete create, questo serve essenzialmente per due scopi:

1. Distribuire nuove monete in maniera decentralizzata.
2. Aggiungere sicurezza al sistema.

Uno dei principali obiettivi del processo di mining è permettere ai nodi della rete Bitcoin di raggiungere un consenso sicuro e a prova di manomissione.

Esistono 3 metodi per partecipare all’attività di Bitcoin mining:

1. Il solo mining viene eseguito individualmente e il miner utilizza le proprie risorse per risolvere problemi matematici e convalidare le transazioni sulla blockchain di Bitcoin. L'attuale elevata competitività del settore richiede investimenti significativi negli hardware e nella potenza di calcolo per questa specifica alternativa.
2. Il pool mining è un'attività collettiva in cui più soggetti uniscono le proprie risorse, mettendo a disposizione la propria potenza di calcolo, suddividendo i profitti in proporzione al contributo fornito.
3. Il cloud mining consente alle persone di partecipare all'attività di mining senza possedere fisicamente i dispositivi hardware necessari. Attraverso il cloud mining è possibile affittare una certa quantità di potenza computazionale e fare propri i profitti, in cambio di un canone di locazione.

I server necessari per compiere tali operazioni hanno un costo di acquisto rilevante e comportano un consumo di corrente davvero non indifferente, dato che lavorano per ben 24 ore al giorno, 7 giorni su 7, a cui vanno aggiunte delle spese necessarie a non causare surriscaldamenti dei computer.
Per fare fronte a questo problema, i più grandi centri che si occupano di mining si stanno spostando sempre di più in paesi con minori costi della manodopera e dell’elettricità, come l’Europa dell’est o la Cina.

Il mercato del mining sta divenendo sempre meno conveniente, principalmente per il continuo aumento dei costi connessi a tali attrezzature e, soprattutto, della sempre maggiore riduzione di Bitcoin ottenibile mediante tale processo.
Il numero massimo di BTC in circolazione non potrà mai superare quota 21 milioni. Una volta raggiunta quella soglia la produzione, il mining, si arresterà.

L’estrazione della criptovaluta avviene per mano dei cosiddetti miners che, per questo lavoro, vengono ricompensati proprio con Bitcoin. Con l’halving la loro ricompensa viene semplicemente dimezzata, quindi il numero di BTC immessi sul mercato diminuisce, il valore di questi ultimi, di conseguenza, tende ad aumentare.
Grazie all’halving di Bitcoin i “ritmi di produzione” vengono quindi rallentati, il che impedisce l’immediato raggiungimento di quota 21 milioni e rende il prezzo meno esposto a rischi di deprezzamento.

In pratica, ogni 10 minuti circa vengono creati nuovi Bitcoin. Per i primi quattro anni dalla loro nascita, la quantità di nuovi Bitcoin emessi ogni 10 minuti era di 50. Ogni quattro anni, tale numero si dimezza e il giorno in cui questo accade viene chiamato «halving» o «halvening». Nel 2012, la quantità di nuovi Bitcoin emessi ogni 10 minuti è scesa da 50 a 25. Nel 2016 è scesa da 25 a 12,5. Nell'ultimo halving dell'11 maggio 2020, la quantità è scesa da 12,5 a 6,25 BTC per blocco.

Il dimezzamento di Bitcoin è programmato in base all'altezza del blocco, non alla data. L'halving avviene ogni 210.000 blocchi e il dimezzamento del 2024 avverrà nel blocco 840.000. Sulla base di questo, si stima che il quarto halving avverrà, probabilmente, tra marzo 2024 e maggio 2024. L'attuale ricompensa per un blocco di Bitcoin è di 6,25 BTC per blocco, quando il blocco 840.000 verrà raggiunto nel 2024, questa scenderà a 3,125 BTC. Attraverso il meccanismo dell'halving, l'offerta di Bitcoin subisce un forte ridimensionamento incidendo direttamente sulle dinamiche inerenti la costituzione del prezzo. Questo perché dovrebbe teoricamente esserci meno spinta dal lato dell'offerta, stimolando quindi maggiormente la salita del prezzo.

Occorre però fare una precisazione: il valore di Bitcoin non è matematicamente impostato per una crescita perenne e incondizionata come molti pensano. Questo perché, affinché il prezzo continui a salire, deve mantenersi almeno costante la domanda di Bitcoin. Qualora non sia presente quest'ultimo ingrediente, non sarà sufficiente la conclusione del processo di halving a far salire il prezzo di BTC.
Ciò che in passato ha veramente spinto il prezzo verso l'alto, facendo registrare a Bitcoin rendimenti da record, non è stato quindi esclusivamente il processo legato all'halving, ma la forte spinta nel lato della domanda scaturita proprio dall'incentivo derivante da un dimezzamento della produzione.

In passato, gli eventi di halving di Bitcoin sono stati seguiti da aumenti di prezzo graduali e significativi nel tempo, culminati in un anno e mezzo circa. L'ipotesi più probabile è che, durante l'halving del prossimo anno, l'azione rialzista dei prezzi si ripeterà in base agli halving passati di luglio 2016 e aprile 2020.

In seguito a ciascun halving, il prezzo ha poi segnato nuovi massimi:

1. Durante l'halving di novembre 2012 il prezzo di BTC era pari a circa $12, mentre dodici mesi dopo aveva superato il prezzo di $1.100;
2. Durante l'halving di luglio 2016 il prezzo di BTC era intorno ai $650, per poi arrivare nell'anno successivo ad un prezzo pari a quasi $20.000;
3. Durante l'halving di maggio 2020 il prezzo di BTC si aggirava tra $8.500 e gli $8.600 e, poco più di un anno dopo, registrò il nuovo massimo storico: $69.000.

Tabella 1: Dati relativi ai 3 cicli degli halving passati.

FEATURES	1ST HALVING	2ND HALVING	3RD HALVING
DATE	28 November 2012	9 July 2016	11 May 2020
BLOCK NUMBER	210.000	420.000	630.000
BTC FOR EACH BLOCK	50 BTC -> 25 BTC	25 BTC -> 12.5 BTC	12.5 BTC -> 6.25 BTC
PRICE VALUE	$12	$650	$8.600
TOP CYCLE DATE	4 December 2013	17 December 2017	10 November 2021
TOP CYCLE PRICE	$1.140	$19.700	$69.000
GAIN HALVING-TOP	9.300%	2.900%	700%
BOTTOM CYCLE DATE	14 January 2015	15 December 2018	9 November 2022
BOTTOM CYCLE PRICE	$150	$3.100	$15.700
LOSS TOP-BOTTOM	86%	84%	77%
GAIN *BOTTOM-TOP	38.000%	13.000%	2.100%

La tabella 1 mostra alcuni dati riguardanti i 3 halving passati e i relativi cicli di mercato: data dell'halving, numero del blocco di Bitcoin corrispondente all'halving, quantità di Bitcoin per ogni blocco, il prezzo di Bitcoin al momento dell'halving, la data e il valore raggiunti al top del ciclo, il profitto dall'halving al top del ciclo, la data e il valore raggiunti al bottom del ciclo, la perdita dal top al bottom del ciclo e, infine, il guadagno dal bottom del ciclo precedente al top di quello successivo. Le celle in rosso si riferiscono al fatto che, essendo l'attuale ciclo non ancora terminato, potrebbe verificarsi un nuovo bottom di mercato. Da questi numeri è facilmente osservabile una ciclicità dei movimenti successiva agli halving: prima un trend rialzista, di durata massima di un anno e mezzo, poi un trend ribassista, che dovrebbe estinguersi nell'arco di 12 mesi. Nonostante l'alternarsi di mercati bulls e bears, il movimento alla base di Bitcoin rimane estremamente rialzista. Sebbene sia presente un evidente rallentamento della curva di crescita, la tabella mostra anche una diminuzione delle perdite, fattori dovuti probabilmente alla maggiore stabilità che sta ottenendo Bitcoin e, in generale, l'intero mercato delle criptovalute
Nonostante la storia presenti andamenti ciclici e ripetitivi, è importante tenere sempre a mente che le performance passate non sono garanzia di risultati futuri.

2.2.2 Modelli per Bitcoin

Il modello stock to flow (S2F) è un framework per analizzare il valore di un asset scarso, come l'oro o il Bitcoin, basato sulla relazione tra il suo stock esistente (la quantità totale già prodotta) e il suo flusso annuale (la quantità prodotta ogni anno).

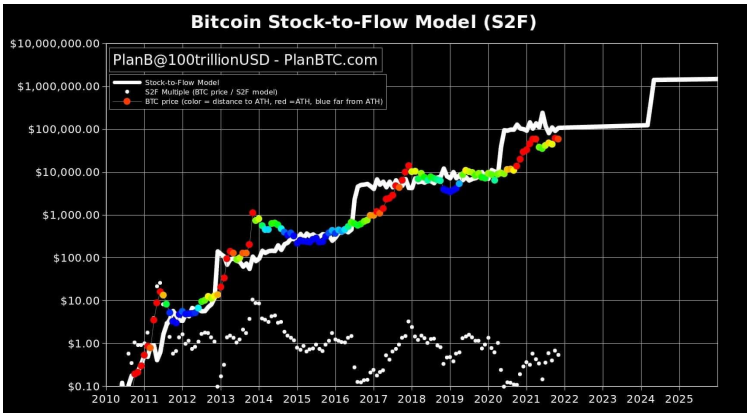
Il modello S2F prevede che il valore di un asset dovrebbe essere direttamente proporzionale al suo rapporto stock/flusso, con un rapporto più alto che implica un valore più alto. Prendendo in esame l'oro, per esempio, nella storia sono state estratte circa 190.000 tonnellate fino ad oggi. Questa quantità, la fornitura totale, può anche essere chiamata stock. Si stima, inoltre, che circa 2.500/3.000 tonnellate di oro vengono estratte ogni anno, tale quantità si può chiamare il flow.
Il rapporto tra queste due quantità è un valore che ci viene fornito da quante nuove unità di una data risorsa entrano nel mercato ogni anno, in relazione alla fornitura totale. Maggiore è il rapporto Stock to Flow, meno sarà la nuova fornitura che entra nel mercato in relazione al totale.

Un asset con un rapporto S2F più alto dovrebbe, in teoria, mantenere il suo valore in modo efficace nel lungo termine.
Al contrario, i beni di consumo e i prodotti industriali hanno generalmente un rapporto Stock to Flow basso; dato che il loro valore deriva tipicamente dalla loro distruzione o consumo, le scorte (lo stock) sono sufficienti solo a coprire la domanda. Queste risorse generalmente non hanno un alto valore come proprietà, quindi, hanno la tendenza a non risultare buoni asset di investimento.
Si premette che la scarsità da sola non implica che una risorsa sia preziosa, l'oro non è così raro dato che ne abbiamo già 190.000 tonnellate; un bene è prezioso perché la produzione annuale rispetto alla fornitura esistente è relativamente esigua e costante, stando al rapporto Stock to Flow.

Storicamente l'oro ha avuto il rapporto Stock to Flow maggiore tra tutti i metalli preziosi. Se si riprendono i dati sull'oro citati nel paragrafo precedente e si divide la fornitura totale di 190.000 tonnellate per 3.500 si ottiene un rapporto Stock to Flow circa di ~54. Tale dato indica che ci vorranno circa 54 anni per minare 190.000 tonnellate di oro al tasso di produzione attuale (chiaramente l'oro non finirà tra 54 anni in quanto, molto probabilmente, il prezzo aumenterà in modo da stabilizzare domanda e offerta).
Il diamante è il secondo con un SF pari a 19. L'argento e il palladio hanno SF appena superiore a 1, mentre quello del platino è pari a 0.4.

Questo modello tratta i Bitcoin come se fossero risorse naturali, come l'oro e l'argento, definiti spesso come risorse che fungono da riserva di valore.
Se si paragona Bitcoin all'oro emergono delle somiglianze: è relativamente costoso da produrre e scarso, con una fornitura massima limitata a 21 milioni di unità, tale fornitura è definita a livello del protocollo, elemento che rende il flow completamente prevedibile (grazie agli halving).
La combinazione di queste proprietà crea una risorsa digitale scarsa con caratteristiche profondamente valide per mantenere un valore consistente a lungo termine.
La formula dello Stock to Flow applicata a Bitcoin è su base mensile e il valore va da dicembre 2009 a febbraio 2026. C'è però un accorgimento che deve essere aggiunto alla formula del modello finale. Si stima che durante il primo anno di vita di Bitcoin, il 2009, Satoshi Nakamoto abbia minato circa 1 milione di Bitcoin i quali, ad oggi, non sono mai stati spostati su un altro wallet. Non si sa se questi siano stati persi oppure Satoshi stia ancora aspettando per venderli, ma la certezza è che non sono mai stati spostati. Si dovrà togliere quindi 1 milione di unità dalle 21 totali.

Grafico 2: Bitcoin Stock-to-Flow model live chart, fonte “charts.bitbo.io”.



Nel modello, riportato nel grafico 2, sono stati usati valori e assi logaritmici per la capitalizzazione di mercato, poiché questa si estende su 8 ordini di grandezza (da 10.000 a 100 miliardi di dollari). Con l’utilizzo di valori logaritmici, lo S2F mostra una sorprendente relazione lineare tra ln(SF) e ln(capitalizzazione di mercato).
Ci sono comunque fattori esterni quali regolamentazioni, hack e altre notizie che possono influire sul modello, per questo motivo abbiamo un $R^2 = 95\%$ e non superiore.
L’attuale fornitura in circolazione di Bitcoin è pari a più di 19 milioni di unità, mentre la nuova fornitura è pari a circa 0,7 milioni per anno. Al momento della scrittura, il rapporto S2F di bitcoin si aggira attorno a 54,8. Bitcoin è però caratterizzato dagli halving, infatti a maggio del 2020, quando è avvenuto effettivamente l’halving, lo S2F è salito a ~44.7, molto vicino all’oro. Il prossimo halving, nel 2024, dovrebbe alzare il numero a 113 anni poiché verrà nuovamente dimezzata l’offerta.

Bitcoin risulta essere il primo bene digitale scarso che il mondo abbia mai conosciuto: è scarso come l’oro, ma può essere inviato attraverso Internet. Questa scarsità di Bitcoin ha, quindi, un valore che il modello Stock to Flow permette di esprimere.
Vale la pena notare che il modello S2F è stato controverso, con alcuni analisti che sostengono che semplifica eccessivamente i fattori che determinano il valore di Bitcoin e potrebbe non essere un predittore affidabile del suo prezzo.

Esistono diversi modelli e indici che sono stati sviluppati per studiare i movimenti del prezzo di Bitcoin sotto diversi aspetti. Alcuni di questi sono stati raggruppati e utilizzati per sviluppare uno score di fiducia, che risulta utile per capire in quale fase dei cicli di mercato rialzista e ribassista di Bitcoin ci si trova.
Questo score, chiamato CBBI, o ColinTalksCrypto Bitcoin Bull Run Index, utilizza un'analisi avanzata in tempo reale di nove metriche per fornire informazioni sullo stato attuale dei cicli di mercato di Bitcoin.
Le metriche utilizzate dal CBBI sono le seguenti:

1. Pi Cycle Top Indicator - storicamente efficace nell'identificare i massimi del ciclo di mercato entro 3 giorni; utilizza la media mobile a 111 giorni e un multiplo della media mobile a 350 giorni.
2. Grafico RUPL/NUPL - questa metrica è derivata dal valore di mercato (prezzo corrente di Bitcoin moltiplicato per il numero di monete in circolazione) e dal valore

realizzato (prezzo di ogni Bitcoin quando è stato spostato l'ultima volta). Sottraendo il valore realizzato dal valore di mercato si ottiene il profitto/perdita non realizzato.

3. Rapporto RHODL - misura il rapporto tra la quantità di Bitcoin detenuta dagli investitori a lungo termine e la quantità totale di Bitcoin in circolazione.
4. Puell Multiple - analizza i ricavi del mining di Bitcoin e li confronta con la media storica.
5. Media mobile a 2 anni - questa metrica attenua la volatilità dei prezzi dei Bitcoin su un periodo di due anni.
6. Bitcoin Trolololo Trend Line - misura il tasso di crescita medio del prezzo di Bitcoin nel tempo.
7. MVRV Z-Score - calcola il valore di mercato diviso per il valore realizzato di Bitcoin e lo confronta con la sua media storica.
8. Rischio di riserva - misura la fiducia dei detentori a lungo termine di Bitcoin analizzando la quantità di monete posseduta.
9. Woobull Top Cap vs. CVDD - questa metrica utilizza alcuni modelli predittivi basati su diversi parametri (prezzo, investitori, rete, ecc.)

Grafico 3: CBBI historical chart, fonte “colintalkscrypto”.

Come è osservabile dal grafico 3, l'indice CBBI fornisce un punteggio di fiducia, da 0 a 100, che indica se ci si sta avvicinando alla parte superiore o inferiore di un ciclo di Bitcoin. Modellato sui cicli storici del mercato, con particolare attenzione ai massimi relativi del 2013 e del 2017, ha come scopi i seguenti: identificare correttamente le caratteristiche del massimo di un ciclo e fornire preziose informazioni agli investitori di Bitcoin.

2.2.3 Innovazione e adozione

Il Lightning Network è un protocollo di pagamento layer 2 costruito sulla blockchain di Bitcoin. Consente transazioni più veloci, economiche e private, permettendo agli utenti di effettuare pagamenti tramite canali off-chain garantiti da smart contract.

Il Lightning Network è stato proposto per la prima volta nel 2015 da Joseph Poon e Thaddeus Dryja come soluzione al problema della scalabilità di Bitcoin. L'idea alla base è quella di togliere la maggior parte delle transazioni Bitcoin dalla blockchain principale ed elaborarle, invece, attraverso una rete di canali di pagamento.

Questi canali off-chain vengono creati tra due parti che desiderano effettuare transazioni frequenti tra loro. Una volta stabilito il canale di pagamento, le parti possono effettuare operazioni tra loro istantaneamente e senza bisogno di conferma sulla blockchain di Bitcoin. Una volta che le due parti hanno concluso la transazione, possono chiudere il canale di pagamento e il saldo finale viene regolato sulla blockchain di Bitcoin.

Inoltre, il Lightning Network consente agli utenti di instradare i pagamenti attraverso più canali di pagamento. In questo modo, due utenti che non dispongono di un canale di pagamento diretto tra di loro, possono comunque effettuare transazioni tra loro indirizzando il pagamento attraverso altri canali sul Lightning Network.

La sicurezza del Lightning Network si basa sulla sicurezza della blockchain sottostante, che nel caso di Bitcoin è garantita da una Proof of Work. I pagamenti lampo sono protetti da smart contract, che assicurano che vengano eseguite solo transazioni valide. Inoltre, il Lightning Network consente agli utenti di connettersi direttamente tra loro, aggirando gli intermediari, riducendo il rischio di attacchi.
In termini di privacy, le transazioni del Lightning Network sono private per impostazione predefinita, non vengono trasmesse alla blockchain e solo i partecipanti possono vederne i dettagli. Tuttavia, ci sono alcuni problemi di privacy con questa rete, come la possibilità di collegare più transazioni Lightning allo stesso utente.

Questi i molteplici vantaggi forniti dall’utilizzo del Lightning Network:

- Commissioni basse e rapidi tempi di transazione che consentono di inviare piccole quantità di Bitcoin, chiamate microtransazioni; aprendo nuovi casi d'uso come servizi pay-per-use o contenuti in streaming.
- Transazioni quasi istantanee, il che le rende ideali per operazioni al dettaglio o altre situazioni in cui è richiesto un pagamento rapido.
- Trading peer-to-peer senza la necessità di intermediari, rendendo possibile lo scambio diretto di risorse come opere d’arte digitale.
- Permette di inviare e ricevere pagamenti transfrontalieri in modo rapido ed economico.
- Opportunità per la rete Bitcoin di gestire molte più transazioni al secondo di quanto sarebbe in grado di fare senza, migliorandone la scalabilità.

Il progressivo utilizzo del Lightning Network, renderà probabile l’emergere di nuovi casi d'uso, espandendo ulteriormente le possibilità di questa entusiasmante tecnologia.
Bitcoin ha fatto enormi progressi dalla sua nascita nel 2009: dall'essere una sconosciuta valuta digitale utilizzata da una manciata di appassionati di tecnologia, a rappresentare un fenomeno globale che ha catturato l'attenzione di investitori, regolatori e consumatori. Tuttavia, nonostante la sua popolarità, Bitcoin deve ancora affrontare diverse sfide che ne limitano l'adozione di massa da parte di governi e aziende; che è sempre stata un argomento controverso nella comunità delle criptovalute.

Anche se durante il 2022 il prezzo del Bitcoin ha raggiunto il valore più basso degli ultimi due anni, l'adozione della criptovaluta tra i commercianti è cresciuta.
La prova di ciò può essere trovata nei dati di coinmap.org, che riportano un aumento del 7% del numero di esercizi commerciali che accettano Bitcoin tra gennaio 2022 e gennaio 2023.

L'hash rate è la misura della potenza computazionale della rete Bitcoin, fornisce un'altra metrica importante da considerare quando si esamina l'adozione di Bitcoin.
L'arrivo di nuovi operatori nel settore del mining porta ad un aumento della difficoltà e, quindi, dell'hash rate che nel 2023 si trova ad un livello superiore rispetto al bull market del 2020-2021, nonostante il prezzo della criptovaluta sia diminuito.

Durante il 2022, diversi paesi in tutto il mondo hanno compiuto passi importanti verso una maggiore adozione di Bitcoin e delle tecnologie decentralizzate.

Una delle iniziative più importanti nel 2022 è stata il Lugano Plan B Forum, sponsorizzato da Tether Operations Limited e dalla Città di Lugano, per facilitare l'adozione di Bitcoin nella città più popolosa della Svizzera. L'evento si è tenuto il 28 ottobre 2022 e ha portato trenta aziende ad accettare Bitcoin come metodo di pagamento.
Il Plan B Forum ha obiettivi ancora più ambiziosi, tra cui estendere l'uso di Bitcoin al pagamento delle tasse e trasformare Lugano in una città crypto-friendly. Il sindaco di Lugano ha dichiarato di puntare a rendere la città un luogo dove nascono professionalità e startup legate alla blockchain.
Questa iniziativa rappresenta una grande opportunità per promuovere l'adozione di Bitcoin nel continente europeo, partendo da uno dei principali centri finanziari mondiali.

Il 27 aprile 2022, la Repubblica Centrafricana ha seguito le orme di El Salvador affermandosi come il secondo paese al mondo ad adottare Bitcoin come valuta ufficiale; il 4 luglio ha anche lanciato la sua CBDC (Sango Coin).
L'elevata prevalenza di Bitcoin in Africa è probabilmente dovuta agli alti tassi di inflazione che caratterizzano le economie della maggior parte dei paesi del continente e alla dipendenza dalle rimesse estere. Inoltre, l'Africa ha la più grande concentrazione di individui senza conti bancari.

Anche Bitcoin Island, situata a Boracay nelle Filippine, ha visto un'adozione significativa di Bitcoin. Pouch, l'azienda dietro il progetto, ha implementato una vasta campagna di adozione sull'isola, convertendo più di 100 attività commerciali locali che ora accettano Bitcoin come mezzo di pagamento.
Le Filippine sono il secondo paese al mondo per l'adozione di criptovalute, dietro solo al Vietnam.

El Salvador è probabilmente il paese più all'avanguardia nell'adozione di Bitcoin, avendolo adottato come moneta a corso legale nel 2021. Il 17 novembre 2022, il Ministro dell'Economia di El Salvador ha presentato un nuovo disegno di legge che conferma il piano del governo di raccogliere 1 miliardo di dollari per la costruzione di " Bitcoin City".
I "Bitcoin bond", gli strumenti che verranno utilizzati per raccogliere finanziamenti, erano stati introdotti dal presidente Bukele già nel 2021. Quando i bond saranno finalmente lanciati, rappresenteranno il primo esempio di obbligazioni emesse su blockchain.

La speranza è che questo possa diventare realtà nel 2024, ispirando altri stati ad adottare la finanza decentralizzata.

Nel complesso, l'adozione di Bitcoin ha continuato a crescere ed evolversi negli ultimi anni, con il 2022 che è stato un anno particolarmente significativo per la criptovaluta.
Nonostante un calo del prezzo di Bitcoin, i suoi fondamentali rimangono solidi e il numero di utenti che adottano la criptovaluta continua a crescere rapidamente. Questa evoluzione è particolarmente evidente nei paesi emergenti, dove gli alti tassi di inflazione e la mancanza di accesso ai servizi bancari tradizionali ne hanno favorito l'impiego.

In conclusione, è probabile che la tendenza verso una maggiore adozione di tecnologie decentralizzate, incluso Bitcoin, continui nei prossimi anni.
Man mano che più individui e aziende si sentono a proprio agio con queste tecnologie e i quadri normativi diventano più chiari, potremmo assistere ad un'integrazione ancora più diffusa delle criptovalute nella vita di tutti i giorni.

2.3 LE ALTCOINS

Parlando di monete digitali, viene data sempre maggiore attenzione al Bitcoin, essendo questo il primo per capitalizzazione e, come già detto, per anzianità.
Va detto però che il mondo delle criptovalute, in poco più di dieci anni, ha subito una crescita esponenziale, con la nascita di moltissimi strumenti digitali diversi tra di loro. Ad oggi si contano svariate migliaia di criptovalute differenti, che prendono il nome di "Altcoins", intese come alternative realizzate dopo il successo di Bitcoin. A volte pretendono di andare a sostituirsi a Bitcoin, correggendone eventuali problematiche, altre volte vengono progettate e utilizzate in ambiti e con finalità completamente diverse da BTC.

Il mondo delle Altcoins si è sviluppato in maniera notevole e, pertanto, è davvero difficile conoscerlo esaustivamente, ma il suo studio è utile principalmente per tre motivi:

1. Maggiore margine di sviluppo a livello tecnologico rispetto al Bitcoin.
2. Prezzo di mercato inferiore.
3. Possibilità di studiare le nuove monete dalla loro "nascita" e di controllarne il continuo sviluppo.

Volendo fare un'analisi delle altre valute digitali che in questi anni si sono ritagliate uno spazio sempre maggiore, va premesso che sono molto distanti dalla realtà del Bitcoin, che resta il leader assoluto nel mercato delle monete digitali. In più, è doveroso aggiungere che la performance di tutte le altre monete è fortemente correlata a quella del Bitcoin. Partendo da queste considerazioni, vediamo alcune delle altre migliori criptovalute degli ultimi anni.

2.3.1 Ethereum e le top altcoins

Ethereum è una piattaforma blockchain decentralizzata e open source che consente la creazione di applicazioni decentralizzate (DApps) e smart contract. Proposta per la prima volta nel 2013 da Vitalik Buterin, programmatore e appassionato di criptovalute, negli anni è diventata una delle reti blockchain più grandi e conosciute al mondo.
Ethereum viene spesso definita "argento digitale" rispetto allo status di Bitcoin come "oro digitale". Questa analogia si basa sull'idea che, proprio come l'argento è un metallo prezioso

e ampiamente utilizzato, ma meno prezioso dell'oro, Ethereum è una piattaforma blockchain ampiamente utilizzata, ma meno preziosa di Bitcoin. Tuttavia, a differenza dell'argento, Ethereum è progettato per essere più versatile e adattabile, con l'obiettivo di consentire la creazione di nuove e innovative applicazioni decentralizzate.

Una delle caratteristiche chiave di questa piattaforma è l'utilizzo di smart contract: contratti auto eseguiti, in base ai termini dell'accordo, tra acquirente e venditore, scritti direttamente in righe di codice sulla blockchain. Ciò elimina la necessità di intermediari e consente transazioni peer-to-peer affidabili.
Un altro aspetto importante di Ethereum è il suo supporto per le DApps: applicazioni che girano su una rete decentralizzata, piuttosto che su un singolo server controllato da un'autorità centrale. Ciò consente una maggiore sicurezza e trasparenza, nonché la possibilità di accedere alle applicazioni da qualsiasi parte del mondo.

Ethereum utilizza l'algoritmo di consenso chiamato Proof of Stake (PoS).
Nell'implementazione del PoS di Ethereum, la criptovaluta messa in staking è chiamata ether, i partecipanti che mettono in stake i propri ether sono chiamati validatori e sono responsabili della verifica delle transazioni e della creazione di nuovi blocchi nella blockchain.
L'algoritmo PoS in Ethereum funziona selezionando in modo casuale i validatori per creare blocchi e convalidare le transazioni. La probabilità di essere selezionato come validatore è proporzionale alla quantità di ether messa in stake.
Una volta selezionati, i validatori sono responsabili della creazione e della convalida di nuovi blocchi. Vengono ricompensati con commissioni di transazione e una certa quantità di ether appena coniato per ogni blocco che creano. Tuttavia, se un validatore si comporta in modo dannoso o tenta di manipolare il sistema, può perdere l'ether in stake come penalità.
Utilizzando il PoS, Ethereum mira a ridurre la propria impronta di carbonio e rendere la rete più sostenibile a lungo termine.

I token nativi degli exchange di criptovalute, noti anche come exchange coin, sono token specifici di un particolare exchange di criptovalute. Queste monete digitali vengono utilizzate per pagare le commissioni delle transazioni sulle piattaforme e, solitamente, offrono numerosi vantaggi, come commissioni di negoziazione scontate, diritti di voto sulle decisioni della piattaforma o sconti su servizi di terze parti. Alcuni esempi di exchange coin includono Binance Coin (BNB) sull'exchange Binance e Cronos (CRO) sull'exchange Crypto.com.
Le exchange coins sono diventate sempre più popolari negli ultimi anni, in quanto permettono agli utenti sia di ridurre le commissioni di scambio che di essere maggiormente coinvolti nella gestione dell'exchange. Possono anche essere utilizzate come un semplice investimento nel mercato delle criptovalute; detenere queste monete è sintomo di una fiducia relativa allo sviluppo e l'espansione del loro exchange nativo, perciò una crescita delle suddette piattaforme di scambio comporterebbe un aumento di valore della criptovaluta da loro coniata.

Binance Coin è il token nativo dell'exchange di criptovalute Binance, è stato creato per aiutare a finanziare lo sviluppo dell'ecosistema Binance e per fornire agli utenti sconti e altri vantaggi sulla piattaforma dedicata.

BNB ha diverse caratteristiche chiave che la rendono una criptovaluta unica e preziosa. Per esempio:

1. Sconti sulle commissioni di trading - gli utenti di Binance che detengono BNB nei loro conti ricevono sconti sulle commissioni di trading quando usano BNB per pagarle. Questo incentiva gli utenti a detenere BNB e utilizzare la piattaforma Binance.
2. Token Burn - Binance utilizza una parte dei suoi profitti per riacquistare e "bruciare" i token BNB, riducendo l'offerta totale di BNB e aumentandone la scarsità e il valore nel tempo.
3. Casi d'uso diversificati - Binance sta espandendo il suo ecosistema per includere una vasta gamma di prodotti e servizi oltre al semplice trading di criptovalute.
4. Riserva di liquidità - Binance è un exchange vasto che offre un'ampia gamma di coppie di trading e un'importante riserva di liquidità; ciò rende BNB un'opzione di investimento interessante per trader che cercano stabilità nel proprio portafoglio.

BNB ha ottenuto buoni risultati sin dal suo lancio ed è stata una delle criptovalute con le migliori prestazioni in termini di crescita di prezzo e valore dell'asset.
Binance Coin (BNB) utilizza un meccanismo di consenso noto come Proof of Stake Authority (PoSA), che è una combinazione di Proof of Stake (PoS) e delegated Byzantine Fault Tolerance (dBFT).

Cronos è una criptovaluta creata nel 2018 da Crypto.com, una società fintech con sede a Hong Kong, con lo scopo di essere utilizzata come utility token per la piattaforma di Crypto.com stessa.
Detenendo CRO nel proprio portafoglio, gli utenti possono ottenere benefici come ricevere sconti sulle commissioni di trading e accedere a servizi esclusivi. Inoltre, CRO viene utilizzato come valuta nativa per la Cronos Chain, una blockchain ad alte prestazioni che consente transazioni veloci ed economiche.
Il valore di CRO è strettamente legato al successo della piattaforma Crypto.com: poiché la piattaforma continua a crescere e ad attrarre più utenti, si prevede che la domanda di CRO aumenterà, aumentandone il prezzo.
CRO utilizza un meccanismo di consenso ibrido che incorpora il Delegated Proof of Stake (DPoS) con il Proof of Authority (PoA).

"Ethereum killer" è un termine usato per descrivere una criptovaluta o una piattaforma blockchain che ha il potenziale per superare Ethereum in termini di popolarità, utilizzo o tecnologia. Ethereum è attualmente una delle piattaforme blockchain più popolari e utilizzate e ha una comunità ampia e attiva di sviluppatori e utenti.
Ci sono diversi progetti che sono stati soprannominati "Ethereum killer" dai media o dalla comunità delle criptovalute, come Cardano, Polkadot e Solana. Questi progetti hanno le loro caratteristiche e casi d'uso unici e mirano a migliorare alcuni dei limiti di Ethereum, come la scalabilità o la funzionalità degli smart contract. Tuttavia, è importante notare che "Ethereum killer" è un termine usato più a scopo di marketing e non è ancora chiaro se qualcuno di questi progetti sarà in grado di superare Ethereum in termini di popolarità, utilizzo o tecnologia nel prossimo futuro.

Cardano è una piattaforma decentralizzata per lo sviluppo e l'esecuzione di smart contract e DApps. È stata fondata nel 2015 ed è stata sviluppata da IOHK (Input Output Hong Kong), una società di ricerca e sviluppo.
Cardano utilizza un meccanismo di consenso PoS chiamato Ouroboros.
Una delle caratteristiche uniche di Cardano è l'architettura multistrato con due livelli: il Cardano Settlement Layer (CSL) e il Cardano Computation Layer (CCL). Il CSL gestisce il trasferimento della criptovaluta nativa della piattaforma, ADA, mentre il CCL consente l'esecuzione di smart contract e DApps. Ciò consente una maggiore flessibilità e aggiornamenti alla piattaforma senza compromettere la criptovaluta sottostante.
Il rigoroso processo di verifica formale a cui la piattaforma è stata sottoposta garantisce che il codice sia matematicamente provato per funzionare come previsto. Questo rende Cardano una delle piattaforme blockchain più sicure sul mercato.

Polkadot è una piattaforma decentralizzata che consente l'interoperabilità di più blockchain. Fondata nel 2016 dalla Web3 Foundation, è rapidamente diventata uno dei progetti blockchain più promettenti sul mercato.
Uno degli aspetti chiave di Polkadot è la sua architettura multi-chain, che consente il trasferimento continuo di dati e risorse tra diverse reti blockchain, abbattendo le barriere tra sistemi blockchain isolati e consentendo la comunicazione cross-chain. Ciò apre nuove possibilità per applicazioni e servizi decentralizzati che possono operare su più blockchain.

Polkadot ha una struttura di governance unica che consente alla sua comunità di prendere decisioni sulla direzione futura e sullo sviluppo della piattaforma. Questo le conferisce la flessibilità necessaria per evolversi e rispondere alle mutevoli condizioni del mercato e alle esigenze degli utenti.
Polkadot utilizza un modello di sicurezza condiviso, in cui la sicurezza della rete è fornita da più parachain (catene parallele) anziché da una singola chain; ciò le dà una scalabilità che consente velocità di transazione più elevate e costi inferiori rispetto alle tradizionali piattaforme blockchain.

Il protocollo di Solana è stato progettato per facilitare la creazione di DApps e migliorare la scalabilità combinando il consenso PoH (Proof of History) e PoS; creato per servire sia i piccoli utenti che i clienti aziendali, promette bassi costi di transazione pur garantendo elevata scalabilità ed elaborazione rapida. Solana ha molto colpito per le sue impressionanti velocità e performance, attirando l'interesse istituzionale e diventando un rivale di Ethereum. Nel settembre 2021, Solana è salita al settimo posto nella classifica CoinMarketCap, con un aumento del prezzo di oltre il 700% da metà luglio 2021. Tuttavia, la rete è stata afflitta da ripetute interruzioni e il suo ecosistema è stato accusato di favorire gli investitori in capitale di rischio con tokenomics ingiusti.

2.3.2 Sinergie con altri settori

L'Internet of Things (IoT) si riferisce all'interconnessione di dispositivi e apparecchi fisici di uso quotidiano attraverso Internet. Questi dispositivi, da smartphone e dispositivi domestici intelligenti ad attrezzature e veicoli industriali, sono dotati di sensori e software che consentono loro di raccogliere e condividere dati, utilizzabili per migliorare l'efficienza, l'automazione e la connettività.

La tecnologia IoT può essere utilizzata in un'ampia gamma di settori, tra cui produzione, trasporti, assistenza sanitaria e agricoltura, per migliorare le operazioni e il processo decisionale.
Questo settore è ancora nelle sue prime fasi di sviluppo, ma sta rapidamente avanzando e diventando sempre più integrato nella vita di tutti i giorni.
L'Internet of Things (IoT) e le criptovalute sono due tecnologie separate, ma hanno il potenziale per essere combinate al fine di creare soluzioni innovative. Esistono già numerosi progetti sul mercato che stanno lavorando all'integrazione di IoT e criptovalute, tra questi si distinguono VeChain e IOTA.

Man mano che la tecnologia continua ad avanzare, l'integrazione di IoT e criptovalute diventerà probabilmente più diffusa, portando a nuove ed entusiasmanti possibilità per automatizzare e proteggere vari aspetti del nostro modo di vivere, come la convenienza, l'efficienza e la sostenibilità.

VeChain è una piattaforma blockchain focalizzata sulla gestione della supply chain e della logistica, che utilizza la tecnologia RFID per tracciare i prodotti attraverso la supply chain e fornire dati in tempo reale sulla posizione e l'autenticità dei prodotti stessi. Avviata nel 2015 e lanciata nel giugno 2016, VeChain mira a utilizzare la governance distribuita e la tecnologia Internet of Things (IoT) per creare un ecosistema che risolva alcuni dei principali problemi con la gestione della supply chain, un settore che prima della blockchain era rimasto poco mutato nel corso dei decenni. L'utilizzo di una tecnologia trasparente senza un punto di debolezza o controllo consente una maggiore sicurezza, efficienza e facilità di tracciabilità dei prodotti in una determinata supply chain, riducendo al contempo i costi grazie all'automazione affidabile.
Il modello di VeChain si rivolge quindi alle aziende che cercano di ridurre l'attrito della supply chain e dare un'impressione più trasparente ai clienti.

VET è un token PoS, quindi è necessaria una potenza di elaborazione relativamente bassa per ottenere la sicurezza della rete e mantenere il consenso degli utenti.
VeChain presenta anche una funzione diversa, la PoA (Proof of Authority), che coinvolge gli operatori di masternode dell'autorità che mantengono il protocollo nel proprio interesse secondo le regole stabilite dall'organizzazione madre, la VeChain Foundation.

IOTA è un registro distribuito con una grande differenza: in realtà non è una blockchain. La sua tecnologia è conosciuta come Tangle: un sistema di nodi che conferma le transazioni. Fondamentale è come offra velocità molto maggiori rispetto alle blockchain convenzionali e un'impronta ideale per l'ecosistema di Internet of Things in continua espansione.
Dato che non esiste una blockchain, non ci sono miners e quindi non ci sono costi. Molte reti consolidate vedono aumentare i costi quando la congestione si intensifica, ma IOTA mira a fornire un throughput illimitato con una spesa minima.

Con il tempo, l'obiettivo di IOTA è quello di diventare la piattaforma di riferimento per l'esecuzione di transazioni tra dispositivi IoT. Poiché le stime suggeriscono che potrebbero esserci 20,4 miliardi di dispositivi di questo tipo entro il 2024, questo ecosistema potrebbe portare ad un grande successo.

Il nome più tecnico di Tangle è Directed Acyclic Graph e, come spiegato da Sønstebø in un post sul blog nel 2015: "IOTA non deve essere considerata una moneta alternativa (altcoin) per le criptovalute esistenti come Bitcoin, piuttosto è un'estensione del crescente ecosistema blockchain. È pensato per lavorare in sinergia con queste altre piattaforme per formare coesione e relazioni simbiotiche. IOTA è progettato per fornire una soluzione che nessun'altra crittografia fa: microtransazioni efficienti, sicure, leggere e in tempo reale senza commissioni».

Metaverso e NFT (Non-Fungible-Token) sono entrambi legati al mondo degli asset digitali e la loro applicazione alle criptovalute sta diventando sempre più popolare.
Un metaverso è un mondo virtuale in cui gli utenti possono interagire, creare e possedere risorse digitali, come immobili, opere d'arte e oggetti da collezione. Le criptovalute possono essere utilizzate come mezzo di scambio all'interno di questi mondi virtuali, consentendo agli utenti di acquistare e vendere risorse digitali ed effettuare altre transazioni. Alcuni metaversi popolari includono Decentraland e The Sandbox, i quali sono basati sulla tecnologia blockchain, consentendo trasparenza e sicurezza nelle transazioni.
Gli NFT, d'altra parte, sono un tipo di risorsa digitale che rappresenta la proprietà di un oggetto unico, come un'opera d'arte digitale o da collezione. Sono creati utilizzando la tecnologia blockchain, che consente di verificarne l'unicità e l'autenticità. Gli NFT possono anche essere utilizzati nei metaversi, per rappresentare la proprietà di risorse virtuali, come immobili virtuali o oggetti da collezione virtuali.
L'uso di NFT e metaversi insieme alle criptovalute consente un nuovo livello di proprietà e valore per le risorse digitali, ed è un'area che sta registrando una crescita e un'innovazione significative. Grazie allo sviluppo continuo e inesorabile della tecnologia e della comprensione di questi concetti, si prevede che la loro applicazione nell’universo delle criptovalute continuerà ad espandersi.

Decentraland è una piattaforma di realtà virtuale che utilizza la tecnologia blockchain per creare un mondo virtuale decentralizzato e di proprietà degli utenti, i quali possono creare, sperimentare e monetizzare contenuti e applicazioni sulla piattaforma.
Decentraland ha avuto origine dopo un'ICO da 24 milioni di dollari condotta nel 2017. Il mondo virtuale ha lanciato la sua closed beta nel 2019 e ha aperto al pubblico nel febbraio 2020. Da quel momento gli utenti hanno creato un'ampia gamma di esperienze sui loro appezzamenti di LAND, inclusi giochi interattivi, vaste scene 3D e una varietà di altre esperienze interattive.

Il mondo virtuale di Decentraland è open-source e consente piena libertà creativa. Gli utenti possono creare tutto ciò che desiderano, come giochi, spazi sociali, contenuti educativi e altro ancora. La piattaforma dispone anche di un livello sociale integrato, che consente agli utenti di interagire e comunicare tra loro nel mondo virtuale.
Decentraland punta a creare una piattaforma di realtà virtuale decentralizzata che offra agli utenti il pieno controllo sulle proprie esperienze e risorse virtuali. E’ pensata per creatori di contenuti, aziende e privati che cercano un nuovo mezzo artistico, opportunità di business o una fonte di intrattenimento.
In sintesi, Decentraland mira a consentire nuove forme di attività economica e a permettere agli utenti di monetizzare la propria creatività ed esperienze in modi non possibili nei mondi virtuali centralizzati.

Anche The Sandbox è una piattaforma di gioco virtuale decentralizzata costruita sulla blockchain di Ethereum. A differenza di Decentraland, che consente agli utenti di creare qualsiasi tipo di esperienza desiderino all'interno della piattaforma, The Sandbox è più focalizzato sulle esperienze di gioco, con uno studio di sviluppo di giochi integrato, che rende il processo di creazione di giochi ed esperienze più accessibile e intuitivo.
The Sandbox ha la peculiarità innovativa di incorporare elementi di gioco, come le missioni, con l'utilizzo di una criptovaluta chiamata SAND.
Oltre alle funzionalità di gaming, The Sandbox si concentra anche sull'interazione tra comunità e giocatori. Il gioco ha un solido sistema sociale, che consente ai giocatori di formare gruppi, collaborare a progetti ed esplorare i reciproci mondi.
Nel complesso, The Sandbox è un gioco unico e coinvolgente che offre infinite possibilità di creatività, esplorazione e interazione con la comunità. Il suo uso della criptovaluta e l'economia guidata dai giocatori lo rendono una rivoluzione nel settore del gaming.

L'intelligenza artificiale (AI) e le criptovalute sono due delle tecnologie più entusiasmanti e in rapida evoluzione del nostro tempo, queste hanno il potenziale per trasformare le industrie e cambiare il modo in cui interagiamo con il mondo.
L'intelligenza artificiale, il campo dell'informatica dedicato alla creazione di macchine intelligenti in grado di apprendere, ragionare e risolvere problemi come gli esseri umani, ha applicazioni in una vasta gamma di settori: da sanità e finanza a trasporti e logistica.

L'intersezione di AI e criptovalute è un'area di ricerca e sviluppo entusiasmante e in rapida evoluzione, con il potenziale per sbloccare nuove possibilità per entrambe le tecnologie.
L'intelligenza artificiale può migliorare le capacità delle reti blockchain e fornire soluzioni a sfide complesse nel settore delle criptovalute, mentre le criptovalute possono creare nuovi mercati per prodotti e servizi basati sull'intelligenza artificiale, incentivando lo sviluppo di soluzioni innovative ai problemi del mondo reale.
Queste tecnologie vengono combinate in diversi modi: dall'uso dell'intelligenza artificiale per ottimizzare le prestazioni della blockchain all'utilizzo delle criptovalute per creare nuovi mercati per prodotti e servizi basati sull'intelligenza artificiale.
Alcuni dei casi d'uso più entusiasmanti per l'intelligenza artificiale e le criptovalute sono l'analisi predittiva, il rilevamento delle frodi e i sistemi finanziari autonomi. L'intelligenza artificiale e le criptovalute hanno quindi il potenziale per rivoluzionare i settori e guidare l'innovazione in un'ampia gamma di campi.

The Graph è un protocollo di indicizzazione che consente agli utenti di interrogare i dati di reti come Ethereum utilizzando API aperte chiamate subgraph.
GRT ha una comunità ampia e in crescita, inclusi oltre 3.000 subgraph distribuiti tra migliaia di sviluppatori per varie DApps.
Per garantire la sicurezza economica di The Graph Network e l'integrità dei dati interrogati, i partecipanti utilizzano GRT, che è un token di lavoro bloccato da indicizzatori, curatori e deleganti per fornire servizi di indicizzazione e stabilità alla rete.
The Graph ha creato un livello di dati aperto sopra le blockchain e i sottografi sono API aperte che consentono agli utenti di estrarre i dati dalla blockchain nel modo più semplice ed efficiente.
Qualsiasi società di analisi può creare un'applicazione per interrogare i dati del sottografo indicizzati da The Graph.

SingularityNET è una piattaforma basata su blockchain che consente agli utenti di creare, condividere e monetizzare facilmente i servizi di intelligenza artificiale attraverso il suo mercato AI accessibile a livello globale.
Gli utenti possono navigare, testare e acquistare un'ampia gamma di servizi AI utilizzando l'utility token nativo della piattaforma: AGIX.
SingularityNET è la prima piattaforma che consente agli sviluppatori di vendere i propri strumenti e librerie di intelligenza artificiale, mentre gli acquirenti possono testare qualsiasi servizio AI fornito sul mercato prima di effettuare il pagamento.
La piattaforma presenta anche una vasta comunità di specialisti di AI attraverso il portale Request for AI (RFAI), che consente ai clienti di commissionare un nuovo strumento di intelligenza artificiale, mentre gli sviluppatori possono guadagnare token AGIX soddisfando queste richieste.
Il token AGIX è supportato dall'algoritmo di consenso PoS di Ethereum e da una rete di validatori. SingularityNET ha accennato alla possibilità di passare a un'altra blockchain in futuro e ha recentemente annunciato la sua esplorazione del lancio sulla blockchain di Cardano.
L'obiettivo finale di SingularityNET è sviluppare "intelligenza generale avanzata" o “intelligenza artificiale a livello umano e oltre”.
Il team della piattaforma ha aperto la strada allo sviluppo di un'intelligenza artificiale nota come Sophia, il "robot più espressivo del mondo".
SingularityNET ha anche collaborato con Hanson Robotics per sviluppare Awakening Health, che mira a sfruttare l'intelligenza artificiale per scopi sanitari.

Nel mondo della blockchain e delle criptovalute, gli oracoli svolgono un ruolo fondamentale nel facilitare la comunicazione tra i sistemi on-chain e off-chain. In termini semplici, un oracolo è un feed di dati che collega una blockchain al mondo esterno.
Gli oracoli consentono agli smart contract di accedere ai dati del mondo reale ed eseguire le loro funzioni predefinite in base alle informazioni ricevute. Ciò consente la creazione di DApps in grado di interagire con fonti esterne di informazioni, come dati di mercato, previsioni meteorologiche e dati finanziari, tra gli altri.
Gli oracoli forniscono una funzione cruciale nell'ecosistema crittografico, consentendo alle DApps di funzionare con l'accuratezza e l'affidabilità delle applicazioni centralizzate, senza compromettere la natura decentralizzata della tecnologia blockchain.

Chainlink è un layer decentralizzato che collega smart contract a feed di dati esterni, eventi e metodi di pagamento off-chain. La rete è stata fondata nel 2017 ed è cresciuta fino a diventare uno dei principali attori nel campo dell'elaborazione dei dati.
Chainlink consente agli utenti di diventare operatori di nodi e guadagnare entrate contribuendo all’esecuzione dell'infrastruttura di dati necessaria per il successo delle blockchain.
Chainlink utilizza un'ampia raccolta di operatori di nodi per alimentare collettivamente le reti decentralizzate live, che attualmente assicurano miliardi di valore per le principali applicazioni DeFi come Synthetix, Aave, Compound e altre.
La società ha anche stretto partnership con diverse organizzazioni mainstream come AccuWeather, FedEx, FlightStats e Associated Press.

Chainlink utilizza un algoritmo di consenso Proof-of-Reserve (PoR), una versione modificata del Proof-of-Stake (PoS), che consente alla rete di verificare l'esistenza di riserve detenute dagli operatori del nodo.

2.3.3 Stablecoins

Per far sì che l'intero mondo delle criptovalute non venisse considerato dalla maggior parte degli investitori esclusivamente come un semplice investimento speculativo, caratterizzato da forti rialzi o ribassi in tempistiche molto brevi, sono state prese diverse iniziative, tra le più importanti c'è sicuramente la creazione delle Stablecoins. Queste sono delle criptovalute, nate in tempi molto recenti, che vogliono eliminare la volatilità del prezzo, garantendo al contempo un'operatività il più possibile simile a quella dei mercati tradizionali.

Le stablecoins sono quindi degli assets che godono delle proprietà di riserva di valore e unità di conto, diversamente da tutte le altre criptomonete, e al pari della moneta legale. Per poter soddisfare la caratteristica della stability, queste si legano ad altre risorse, come una valuta tradizionale o a una materia prima, senza comunque vincolarsi ad alcuna banca centrale. Inoltre queste monete cercano di riprodurre la stabilità della valuta cartacea tradizionale, garantendo tutte le caratteristiche principali delle criptovalute, ovvero trasferimenti veloci, sicuri ed economici per i suoi utenti, i quali possono usufruirne ovunque nel mondo con una semplice connessione ad internet.

Esistono 5 tipologie di stablecoin:

1. La prima è quella delle stablecoins collaterali in valuta fiat: questa si basa sul fatto che una certa quantità di moneta in corso legale, come il dollaro, venga depositata a garanzia dell'emissione delle stablecoins, che sono rilasciate in proporzione uno a uno rispetto a tale moneta legale. Sebbene questo metodo sia solido, richiede la centralizzazione e può risultare costoso. Alcuni esempi sono USDT e USDC.

2. Nelle stablecoins di secondo tipo (come DAI) il collaterale è invece sostenuto da altre criptovalute e non da dollari o oro, con questa modalità tutto può restare sulla blockchain e non c'è bisogno di un'autorità centrale. Il problema è che le criptovalute sono instabili, il che significa che le garanzie fluttueranno. Per risolvere quindi questo problema la stablecoin viene sovra-garantita, mediante depositi maggiori del sottostante, per fare in modo che possa assorbire le fluttuazioni dei prezzi nel collaterale. Tuttavia, in caso di un evento finanziario imprevedibile, a causa del quale la criptovaluta sottostante perderebbe tutto il suo valore, anche la stablecoin collasserebbe e le perdite sarebbero addirittura maggiori.

3. Poi esistono le stablecoins "non collateralizzate", cioè senza garanzie (come FRAX). Queste si basano sulla fiducia: chi le acquista crede che il prezzo rimarrà fisso. In pratica queste monete sono gestite algoritmicamente per mantenere il loro valore attraverso meccanismi di domanda e offerta. Se il prezzo supera un dollaro, l'offerta di moneta aumenta per riportarlo in basso, quando il prezzo è inferiore a un dollaro, l'offerta diminuisce.

4. Anche le stablecoin algoritmiche non sono supportate da alcun asset fisico, infatti hanno un meccanismo unico per mantenere il loro valore. Queste criptovalute utilizzano smart contract e oracoli per regolare l'offerta e il valore.

5. Infine esistono le rappresentazioni digitali di una valuta fiat emessa e sostenuta da una banca centrale, queste stablecoins vengono chiamate Central Bank Digital Currency (CBDC)

Volendo fare un focus sulla storia del mercato, le stablecoins sono diventate maggiormente utilizzate nella seconda metà del 2018, rappresentando una proposta sempre più interessante, in particolare per gli investitori timorosi della volatilità dei prezzi delle criptovalute tradizionali.

Una stablecoin perfettamente funzionante potrebbe davvero essere qualcosa di importante per il mercato delle criptovalute, ma da un punto di vista rivolto ai profitti, al momento non ci sono molte ragioni per utilizzare una stablecoin, soprattutto nel lungo termine, principalmente per via dei bassi rendimenti. Esistono inoltre diversi problemi di fiducia relativi all'investimento in una stablecoin, tra questi ci sono la credibilità di chi emette tali strumenti e la sicurezza della blockchain sottostante.

3. INVESTIRE IN CRIPTOVALUTE

Investire in criptovalute è diventato un modo sempre più popolare tra le persone per ottenere un'esposizione nella classe di asset digitali. L'investimento in criptovalute può essere effettuato attraverso una varietà di mezzi, come l'acquisto e la detenzione della valuta, l'investimento in una società correlata alla criptovaluta o l'utilizzo di derivati come futures o opzioni. Il trading di criptovalute, d'altra parte, è l'acquisto e la vendita della valuta su piattaforme online. Questo può essere fatto attraverso un exchange di criptovalute, dove le persone possono acquistare e vendere utilizzando valute fiat o altre monete digitali.
Il trading di criptovalute offre anche un livello di anonimato, poiché non sono necessarie informazioni personali per aprire un conto di trading, ma significa anche che esiste un rischio maggiore di frode. È importante ricercare la reputazione di un exchange e utilizzare un wallet sicuro per conservare le proprie risorse.

Il valore delle criptovalute può essere molto volatile e il mercato è ancora relativamente nuovo e non ben compreso da molti investitori. Questo lo rende un investimento altamente speculativo e che richiede un elevato livello di tolleranza al rischio. E' essenziale eseguire ricerche approfondite e comprendere i rischi prima di investire. E' anche importante rimanere aggiornati con le ultime notizie e gli sviluppi nel mercato delle criptovalute per prendere decisioni ponderate. Inoltre, ci sono numerose leggi che riguardano il trading di criptovalute che variano in base al paese, quindi gli investitori dovrebbero essere consapevoli di quali regolamenti vigono nella loro area.

3.1 PIANO DI INVESTIMENTO DI SUCCESSO

3.1.1 Prima di investire

La popolarità delle criptovalute è cresciuta rapidamente negli ultimi anni, con molti investitori che le vedono come un'opportunità di investimento potenzialmente redditizia. Il valore delle criptovalute può aumentare rapidamente, portando a profitti significativi per gli investitori che hanno acquistato a basso prezzo.
Le monete digitali offrono anche il potenziale per la diversificazione, in quanto ne esistono di diverse tipologie e non sono direttamente legate ai mercati finanziari tradizionali.
Investire in criptovalute può anche fornire una copertura contro l'inflazione, poiché molte valute digitali hanno un'offerta limitata, che può aiutare a proteggere dalla svalutazione delle valute tradizionali.
Inoltre, la capacità di trasferire e archiviare valute digitali al di fuori dei sistemi bancari tradizionali può fornire una maggiore privacy finanziaria e protezione contro l'intervento del governo.

Tuttavia, ci sono anche rischi associati all'investimento in criptovalute.
Il mercato è altamente volatile e i prezzi possono fluttuare rapidamente, portando a perdite significative per gli investitori che non hanno un'elevata tolleranza al rischio.
Anche le criptovalute sono soggette a rischi normativi, poiché i governi di tutto il mondo stanno ancora cercando di capire come regolamentarle e tassarle.
Inoltre, la sicurezza delle valute digitali crea preoccupazione, in quanto possono essere vulnerabili a hacking e frode.
Gli investitori dovrebbero fare attenzione a cercare e scegliere exchange affidabili e wallet sicuri per conservare i propri beni.
Rispetto agli investimenti tradizionali, come azioni e obbligazioni, l'investimento in criptovalute è ancora un mercato relativamente nuovo e non testato. È importante comprendere i rischi e le opportunità unici associati alle criptovalute e considerare attentamente la propria strategia prima di investire.
Nel complesso, investire in criptovalute può essere un'opportunità di investimento potenzialmente gratificante ma ad alto rischio, che richiede una conoscenza approfondita del mercato e la volontà di assumersi dei rischi.

Le criptovalute offrono varie opzioni e strategie di investimento da considerare, tra cui:

- HOLDing: comporta l'acquisto di criptovalute e il loro mantenimento per un periodo a lungo termine, con l'aspettativa di venderle quando il prezzo è aumentato in modo significativo.
- Trading attivo: comporta l'acquisto e la vendita frequenti di criptovalute per trarre profitto dalle fluttuazioni dei prezzi. Il day trading, lo swing trading e lo scalping sono alcune strategie di trading comuni.
- Mining: comporta l'utilizzo da parte dei miners della potenza dei sistemi di calcolo per risolvere complessi problemi matematici, convalidando le transazioni sulla blockchain e guadagnando ricompense sotto forma di nuove criptovalute.
- Initial Coin Offerings (ICO): comporta l'investimento in criptovalute di nuova emissione, solitamente a un prezzo scontato durante le fasi iniziali del progetto.

La media del costo (PAC) è una tecnica di investimento popolare che prevede l'investimento di una quantità fissa di denaro in criptovalute a intervalli regolari, indipendentemente dalle condizioni di mercato. Questa strategia aiuta gli investitori a evitare la tentazione di cronometrare il mercato e può portare a rendimenti più consistenti nel tempo.
In sintesi, investire in criptovalute offre varie opzioni e strategie di investimento da considerare, a seconda della tolleranza al rischio e degli obiettivi di investimento dell'investitore.
Le strategie a lungo termine prevedono l'acquisto e la detenzione di criptovalute, mentre le strategie a breve termine si concentrano sulla realizzazione di profitti rapidi dalle fluttuazioni dei prezzi. La media del costo in dollari e altre tecniche di investimento possono aiutare gli investitori a gestire il rischio e massimizzare i rendimenti.

Quando si considera di investire in criptovalute, è importante condurre ricerche approfondite per prendere decisioni strategiche ponderate.
L'analisi fondamentale comporta lo studio della tecnologia sottostante, del team di sviluppo e del mercato complessivo per una particolare criptovaluta. Questo tipo di analisi aiuta gli investitori a comprendere il potenziale a lungo termine dell'asset.
L'analisi tecnica del mercato è un comune metodo pensato per aiutare gli azionisti ad aprire posizioni profittevoli. Si tratta di un'analisi fondata sulla convinzione che lo studio dell'andamento storico di prezzo e volume possa racchiudere quasi tutte le informazioni utili per prevedere gli sviluppi futuri.
L'andamento del prezzo sul mercato azionario infatti segue sempre dei trend, per questa ragione il passato può essere visto come preludio di ciò che avverrà in futuro, di fondamentale importanza è la corretta identificazione della ciclicità dei movimenti.

Gli investitori possono anche analizzare gli indicatori economici, come i tassi di inflazione e i tassi di interesse, per capire come possono influire sul valore delle criptovalute.
Seguire notizie e pubblicazioni finanziarie può fornire approfondimenti sulle tendenze del mercato, sui cambiamenti normativi e su altri fattori che possono influire sul valore delle criptovalute.
Esistono vari strumenti e risorse di investimento online, come piattaforme di trading e strumenti di analisi di mercato, che possono fornire informazioni preziose agli investitori.
Gli investitori possono anche ricercare i settori e le applicazioni che le criptovalute potrebbero interrompere, come la finanza, il settore immobiliare e la gestione della supply chain.
Esaminare i bilanci e gli indici può fornire ulteriori informazioni sulla salute finanziaria e sulle prestazioni delle società legate alle criptovalute e del mercato in generale.
Nel complesso, condurre una ricerca approfondita è essenziale quando si investe in criptovalute. Una combinazione di più tecniche di analisi, oltre a tenere il passo con le tendenze del mercato e gli sviluppi del settore, può aiutare a prendere decisioni ponderate e gestire il rischio.

3.1.2 Entry point ottimale

Quando si tratta di investire in criptovalute, trovare un buon entry point è fondamentale per massimizzare i rendimenti e minimizzare i rischi.
Il value investing è una strategia che prevede l'identificazione di asset sottovalutati e l'investimento in essi nella speranza che il loro vero valore venga infine riconosciuto dal

mercato. Quando si tratta di criptovalute, gli investitori di valore cercano monete che abbiano una forte tecnologia sottostante, un team di sviluppo dedicato e un solido tasso di adozione. Un modo per identificare le criptovalute sottovalutate è condurre un'analisi fondamentale, che verrà approfondita in seguito.

Il timing del mercato prevede l'acquisto e la vendita di risorse in base alle tendenze e ai movimenti del mercato. Sebbene possa essere difficile cronometrare il mercato, alcuni investitori tentano di farlo per massimizzare i rendimenti.
Nel settore delle criptovalute, la tempistica del mercato può essere difficile a causa della volatilità del mercato. I prezzi possono fluttuare selvaggiamente in un breve lasso di tempo, rendendo difficile prevedere quando acquistare o vendere. Tuttavia, tenere d'occhio le tendenze e le notizie del mercato può aiutare gli investitori a identificare potenziali opportunità di acquisto quando i prezzi sono bassi e di vendita quando i prezzi sono alti.

La tolleranza al rischio si riferisce alla disponibilità di un individuo ad assumersi il rischio per ottenere rendimenti potenzialmente più elevati. Quando si investe in criptovalute, è importante comprendere i potenziali rischi coinvolti e determinare la propria tolleranza al rischio.
Le criptovalute sono note per la loro volatilità, che può comportare guadagni o perdite ingenti in un breve lasso di tempo. Gli investitori con una tolleranza al rischio più elevata potrebbero essere a loro agio nell'investire in criptovalute, mentre quelli con una tolleranza al rischio inferiore potrebbero preferire investire in asset più stabili.

Gli obiettivi di investimento si riferiscono agli obiettivi generali di un investitore per il proprio portafoglio di investimenti. Nel mercato delle criptovalute ci sono una varietà di obiettivi di investimento da considerare, come la crescita o il reddito.
Gli investitori con un obiettivo di crescita potrebbero essere interessati a investire in criptovalute che hanno un forte potenziale di crescita a lungo termine. Coloro che hanno un obiettivo di reddito potrebbero essere interessati a investire in criptovalute che pagano dividendi o offrono un flusso costante di reddito.

L'orizzonte temporale si riferisce al periodo di tempo durante il quale si prevede di detenere una certa risorsa. Gli investitori dovrebbero considerare il proprio orizzonte temporale e scegliere asset in linea con i propri obiettivi di investimento.
Gli investitori a breve termine potrebbero essere interessati a investire in criptovalute con potenziale di guadagni rapidi, mentre gli investitori a lungo termine potrebbero preferire detenere attività per diversi anni nella speranza di realizzare guadagni significativi a lungo termine.

La diversificazione è una strategia che prevede la diffusione degli investimenti su una varietà di attività, cercando di ridurre al minimo il rischio e bilanciare potenziali perdite e guadagni in tutto il portafoglio.
Bisognerebbe investire in diverse categorie di criptovalute che presentano specifiche tecnologie sottostanti e casi d'uso, come l’Internet of Things e l’intelligenza artificiale, in modo da mitigare il rischio complessivo.
Gli investitori dovrebbero considerare quanti fondi del loro portafoglio di investimenti complessivo sono disposti ad allocare nel mercato delle criptovalute, basandosi sui propri obiettivi di investimento, tolleranza al rischio e orizzonte temporale.

Infine, è consigliato bilanciare regolarmente il proprio portafoglio di criptovalute per garantire che rimanga allineato con i propri obiettivi. Ciò significa vendere alcune criptovalute che potrebbero aver guadagnato più valore e investire in altre che potrebbero avere un maggiore potenziale di crescita.

In sintesi, costruire una strategia di investimento sostenibile, per aumentare le possibilità di successo, richiede un'attenta pianificazione e una valutazione continua. Alcuni step fondamentali da seguire sono i seguenti:

1. Fare le proprie ricerche (DYOR) - prima di investire in qualsiasi criptovaluta, avere la dovuta diligenza e fare ricerche approfondite sul progetto d'interesse. Considerare fattori come la tecnologia, il team, la comunità e i casi d'uso per valutarne il potenziale di successo a lungo termine.
2. Definire gli obiettivi di investimento - considerare gli obiettivi finanziari e la tolleranza al rischio quando si sviluppa una strategia di investimento.
3. Determinare la asset allocation - decidere quanto del portafoglio si vuole allocare alle criptovalute e ad altre classi di asset.
4. Creare un portafoglio diversificato - la diversificazione è la chiave per gestire il rischio in qualsiasi portafoglio di investimenti. Prendere in considerazione l'idea di investire in diverse categorie di criptovalute e altri asset, in linea con gli obiettivi di investimento, in modo da distribuire il rischio e ridurre l'impatto della volatilità del mercato.
5. Impostare un budget e rispettarlo - determinare quanto si è disposti a investire e stabilire un tetto massimo per gli investimenti.
6. Investire a lungo termine (HODL) - i mercati delle criptovalute possono essere molto volatili a breve termine, quindi è importante investire con una visione a lungo termine. Concentrarsi su progetti con solidi fondamentali e una visione chiara per il futuro.
7. Rimanere aggiornati - il mercato delle criptovalute è in continua evoluzione, quindi è importante rimanere aggiornati con le ultime notizie, tendenze e cambiamenti normativi. Seguire fonti di notizie affidabili e canali social per rimanere in pari.
8. Gestire le emozioni - i mercati delle criptovalute possono essere altamente emotivi, con i prezzi che fluttuano rapidamente in risposta a notizie e speculazioni. È necessario rimanere disciplinati e non lasciare che le proprie emozioni guidino le decisioni di investimento.
9. Monitorare e adattare una strategia - valutare regolarmente il portafoglio di investimenti e apportare le modifiche necessarie per assicurarsi che rimanga allineato con gli obiettivi di investimento.

Ci sono molte risorse disponibili per ulteriore apprendimento e ricerca nel mercato delle criptovalute. Si può anche prendere in considerazione la possibilità di partecipare a conferenze e incontri, leggere pubblicazioni di settore e white paper e interagire con la comunità delle criptovalute.

3.1.3 Analisi fondamentale e sentiment del mercato

In sintesi, investire in criptovalute può rivelarsi un'impresa complessa e rischiosa, di enorme importanza è condurre un'analisi fondamentale prima di prendere qualsiasi decisione di investimento.

Ciò significa che bisogna comprendere lo scopo sottostante e i casi d'uso di una particolare criptovaluta, infatti alcune sono progettate per settori specifici, come la finanza decentralizzata (DeFi), i token non fungibili (NFT) o l'Internet of Things (IoT). Considerare anche se la criptovaluta abbia o meno un caso d'uso chiaro e praticabile e se risolva un problema del mondo reale.
Il successo di un progetto dipende spesso dalla forza e dall'esperienza del suo team.
E' importante ricercare i background dei membri chiave del team, compresa la loro esperienza nel settore, i progetti precedenti su cui hanno lavorato e qualsiasi altra informazione rilevante. Inoltre, si rivela utile studiare la trasparenza e lo stile di comunicazione del team, nonché il loro impegno nel progetto.

La tecnologia alla base di una criptovaluta è un altro fattore fondamentale da considerare prima di investire, valutandone la qualità e l'affidabilità, nonché eventuali aggiornamenti o innovazioni recenti. Inoltre, è importante considerare eventuali potenziali problemi di scalabilità o sicurezza che potrebbero influire sulla visione a lungo termine della criptovaluta.
La capitalizzazione di mercato e il volume degli scambi di una criptovaluta possono fornire preziose informazioni sulla sua popolarità e liquidità. E' importante considerare se la criptovaluta abbia una capitalizzazione di mercato e un volume di scambi sufficientemente grandi da renderla valida per fornire liquidità per l'acquisto e la vendita.

Anche il tasso di adozione e la popolarità di una criptovaluta possono essere un buon indicatore del suo potenziale a lungo termine. Considerare il livello di supporto e coinvolgimento, nonché eventuali partnership o approvazioni degne di nota, porta a nozioni fondamentali per il futuro investimento. Inoltre, è importante valutare il livello di adozione mainstream e come la criptovaluta viene utilizzata da aziende o individui in scenari reali.
Il mercato delle criptovalute è altamente competitivo ed è importante considerare il livello di concorrenza, analizzando se la criptovaluta abbia caratteristiche o vantaggi unici rispetto alle sue concorrenti.
L'analisi fondamentale può quindi aiutare gli investitori a identificare le criptovalute che hanno il potenziale per una crescita a lungo termine, piuttosto che quelle che stanno semplicemente cavalcando un ciclo di hype a breve termine.

Gli investimenti in criptovalute sono influenzati da diversi fattori, tra cui il sentimento del mercato e il comportamento delle comunità di investitori. Comprendere il ruolo di questi due elementi risulta determinante per elaborare strategie di investimento nel mercato in rapida evoluzione delle criptovalute.
Il sentimento del mercato si riferisce allo stato d'animo o all'atteggiamento generale degli investitori nei confronti di un particolare asset o settore. Nel mercato delle criptovalute, il sentiment può essere influenzato da una varietà di fattori, tra cui notizie, cambiamenti normativi e sviluppi tecnologici. Di fondamentale importanza è monitorare il sentimento del mercato al fine di identificare le tendenze e anticipare i potenziali movimenti.

Un elemento che ha un impatto sul sentimento e sulla comunità sono i pregiudizi psicologici e l'investimento emotivo. Questi pregiudizi possono indurre gli investitori a prendere decisioni irrazionali basate su emozioni come la paura o l'avidità, piuttosto che su una solida analisi e ricerca. È necessario essere consapevoli di questi pregiudizi e adoperarsi per ridurre al minimo il loro impatto sulle proprie decisioni di investimento.

Un altro concetto rilevante per comprendere il sentimento è la finanza comportamentale, ovvero lo studio di come i pregiudizi cognitivi influiscono sulle decisioni finanziarie. La finanza comportamentale può aiutare ad identificare modelli di comportamento che potrebbero avere un impatto sul mercato delle criptovalute, in modo da elaborare strategie più ponderate.

Anche i social media possono avere un impatto significativo sul sentimento e sulla comunità nel mercato delle criptovalute. Le piattaforme come Twitter, Reddit e Telegram sono ampiamente utilizzate dagli appassionati di criptovalute per discutere di notizie, condividere approfondimenti e analisi e speculare sui movimenti dei prezzi.
In conclusione, quando si investe in criptovalute, è importante effettuare un'analisi fondamentale, studiando: i casi d'uso, il team e la leadership, la tecnologia e l'innovazione, la capitalizzazione e il volume, il tasso di adozione e la popolarità, la concorrenza e l'ambiente normativo; in modo da elaborare strategie ponderate e ridurre il rischio di perdite nel volatile mercato delle criptovalute.

3.2 PORTAFOGLI PER CRIPTOVALUTE

Un portafoglio di criptovalute è un portafoglio digitale utilizzato per detenere, inviare e ricevere valute digitali come Bitcoin ed Ethereum. Questi portafogli utilizzano chiavi pubbliche e private per visualizzare e gestire le criptovalute dell'utente. Le chiavi pubbliche vengono utilizzate per ricevere criptovalute, mentre le chiavi private permettono di autorizzare le transazioni e accedere alle risorse digitali del proprietario.
Esistono due tipologie di sistemi per comprare e detenere criptovalute: gli exchange e i wallet. Sebbene entrambi svolgano un ruolo importante nell'ecosistema delle criptovalute, è fondamentale comprendere le differenze e come utilizzarli correttamente.

3.2.1 Exchange e wallet

Un exchange di criptovalute è una piattaforma che consente alle persone di acquistare e vendere criptovalute utilizzando diversi metodi:

1. Eseguendo uno scambio da una valuta ad un'altra, indipendentemente che sia una normale criptovaluta o una moneta fiat.
2. Comprandola direttamente utilizzando una propria carta di credito o debito.
3. Prima ricaricando il proprio saldo tramite bonifico bancario, poi acquistandola con il suddetto saldo.

Questi exchange fungono da mercato per investitori e trader per scambiare criptovalute. L'exchange, solitamente, addebita una commissione per ogni transazione, che può essere una percentuale dell'operazione o un importo fisso. Gli exchange possono anche differire nei tipi di criptovalute che supportano e nelle coppie di trading che offrono, infatti alcuni si concentrano su un insieme specifico di criptovalute, mentre altri offrono un'ampia varietà di risorse digitali. Inoltre, certi exchange offrono funzionalità di trading avanzate come il trading a margine, che consente agli utenti di fare trading con la leva finanziaria.
Gli exchange possono essere centralizzati (CEX) o decentralizzati (DEX). Quelli appartenenti alla prima categoria sono di proprietà e gestiti da una società e, in genere, richiedono agli utenti di passare attraverso un processo Know Your Customer (KYC) e Anti-Money Laundering (AML) per conformarsi alle normative.

Due tra gli exchange centralizzati tra i più popolari sono Crypto.com e Binance.

Crypto.com è una società con sede a Hong Kong che offre una varietà di servizi finanziari incentrati sulle criptovalute. Questi includono un wallet mobile per detenere e scambiare criptovalute, una carta di debito Visa che consente agli utenti di spendere le proprie criptovalute nel mondo reale e una piattaforma per acquistare, vendere e guadagnare interessi su una varietà di risorse digitali.

La società gestisce anche una criptovaluta nativa: CRO, che viene utilizzata per accedere alle funzionalità premium sulla piattaforma e premiare gli utenti per il loro coinvolgimento. Crypto.com ha stretto partnership con varie società, personaggi e eventi in molti settori oltre quello delle criptovalute.
Alcune di queste partnership, oltre la già citata VISA, includono:

- 2022 FIFA World Cup in Qatar, l'evento sportivo calcistico più popolare al mondo, ispirandosi al quale ha anche creato 10.000 NFT unici insieme a Coca Cola.
- Anschutz Entertainment Group (AEG) sulla denominazione dello Staples Center, l'iconica arena di Los Angeles, che dal 25 dicembre 2021 ha cambiato nome in Crypto.com Arena in cambio di 700 milioni di dollari. Si tratta di uno dei più grandi accordi sui diritti di denominazione nella storia degli Stati Uniti, a dimostrazione che le criptovalute sono diventate un fenomeno di grande popolarità.
- F1 Miami Grand Prix, di cui è partner principale per 9 anni.
- LeBron James e la LeBron James Family Foundation (LJFF), associazione benefica della stella NBA a cui è legato il programma educativo I Promise, che prevede l'implementazione dell'offerta educativa grazie alla piattaforma online Web3.
- Matt Damon e Water.org, fondato dalla star del cinema, per portare acqua potabile e servizi igienico-sanitari alle persone bisognose, grazie a donazioni all'organizzazione no-profit e lanciando iniziative per incoraggiare gli utenti di Crypto.com in tutto il mondo a sostenere la causa.

Binance è un exchange leader di criptovalute fondato nel 2017 con sede a Malta. In pochi anni è rapidamente cresciuto fino a diventare uno degli exchange più grandi al mondo per volume di transazioni.
Binance offre un'ampia varietà di risorse digitali per il trading, possiede anche una sua criptovaluta nativa: Binance Coin (BNB), che viene utilizzata per pagare le commissioni delle transazioni e accedere alle funzionalità premium sull'ecosistema Binance. Fornisce inoltre agli utenti una piattaforma con interfaccia user-friendly per l'acquisto, la vendita e il trading di criptovalute, nonché per guadagnare interessi dalle loro risorse digitali.
Oltre alla sua attività principale di exchange, Binance gestisce anche diverse altre attività, tra le quali:

- Binance Smart Chain (BSC), una blockchain sviluppata da Binance stesso per l'esecuzione di smart contract e il supporto di applicazioni decentralizzate (dApp).
- Binance Launchpad, che supporta nuovi progetti blockchain raccogliendo fondi per progetti innovativi e portando nuovi token sul mercato.
- Binance Charity, un ramo filantropo che utilizza la tecnologia blockchain per aumentare la trasparenza e l'efficienza nelle donazioni dirette a cause di beneficenza verificate.

E ha stretto molte partnership rilevanti come:

- TravelbyBit: un servizio di prenotazione di viaggi che consente agli utenti di prenotare voli e hotel utilizzando le criptovalute.
- Tokenomica: una piattaforma di titoli digitali che permette agli utilizzatori di emettere, gestire e scambiare asset tokenizzati.
- AERGO: una blockchain open source che mira a fornire un'infrastruttura sicura e ad alte prestazioni per applicazioni di livello aziendale.
- Elrond Network: una blockchain ad alto potenziale che mira a fornire transazioni veloci, sicure e scalabili per applicazioni decentralizzate, utilizzando un nuovo meccanismo di consenso chiamato Secure Proof of Stake (SPoS).

Gli exchange decentralizzati, d'altra parte, vengono eseguiti su una blockchain e consentono un maggiore anonimato, non facendo affidamento su un'autorità centrale per detenere e gestire i fondi degli utenti, i quali mantengono il controllo dei propri fondi e commerciano direttamente tra loro, ma possono avere un volume di scambi inferiore e spread più elevati. Alcuni exchange decentralizzati tra i più popolari includono Uniswap e PancakeSwap.
Uniswap è un exchange decentralizzato costruito sulla blockchain di Ethereum. È uno dei principali protocolli di market maker automatizzati (AMM) nel mondo della finanza decentralizzata (DeFi).

Uniswap consente agli utenti di scambiare criptovalute direttamente dai loro wallet, senza la necessità di un intermediario o di un exchange centralizzato. Ciò consente agli utenti di avere il pieno controllo delle proprie risorse e di operare in un ambiente affidabile e decentralizzato.
Uniswap opera utilizzando pool di liquidità per coinvolgere acquirenti e venditori. La piattaforma incentiva gli utenti a fornire liquidità alle pool premiando con una parte delle commissioni di negoziazione generate dalla piattaforma. Questo crea un sistema autosufficiente che consente agli utenti di fare trading con spread bassi e liquidità elevata. L'uso da parte della piattaforma di smart contract e infrastrutture decentralizzate consente il trading 24 ore su 24, 7 giorni su 7 ed elimina la necessità di una terza parte fidata.

PancakeSwap è un DEX costruito sulla rete Binance Smart Chain (BSC). È un exchange automatizzato di market maker (AMM), simile a Uniswap, che consente una facile fornitura di liquidità e basse commissioni di negoziazione. L'exchange consente agli utenti di scambiare un'ampia varietà di token basati su Binance Smart Chain, tra cui Binance Coin (BNB) e Binance USD (BUSD).
Una delle caratteristiche chiave di PancakeSwap sono le sue pool che consentono agli utenti di fornire liquidità a una specifica coppia di token e guadagnare una quota delle commissioni di trading generate da quella coppia; in modo simile alla funzione offerta da altri DEX come Uniswap.
PancakeSwap ha anche una funzione "farming", che consente agli utenti di bloccare per un certo periodo di tempo i propri token per guadagnare ricompense sotto forma di un nuovo token, in modo tale da aiutare ad aumentare la liquidità complessiva della piattaforma.
Inoltre, PancakeSwap ha un'interfaccia intuitiva e un wallet integrato che consente agli utenti di gestire facilmente i propri fondi ed effettuare operazioni. Presenta anche basse commissioni grazie alla rete Binance Smart Chain ed è uno dei DEX più popolari nell'ecosistema Binance.

È importante effettuare ricerche approfondite e confrontare i diversi exchange prima di utilizzarne uno.
Infine, è necessario utilizzare un wallet sicuro per archiviare le proprie risorse.
Anche un wallet di criptovalute è un portafoglio digitale utilizzato per archiviare, inviare e ricevere valute digitali, ma a differenza degli exchange centralizzati, nei quali le chiavi private dei portafogli sono detenute dell'azienda proprietaria del relativo exchange, nei wallet quelle stesse chiavi sono disponibili solo all'utilizzatore, aumentando esponenzialmente la sicurezza.

I wallet di criptovalute possono essere classificati in tre tipologie: software, hardware e paper. I software wallet sono portafogli digitali che possono essere scaricati come app o accessibili tramite un sito web e che vengono eseguiti su un dispositivo; mentre i portafogli hardware sono dispositivi fisici progettati per archiviare offline le chiavi private e, quindi, le criptovalute di un utente. I paper wallet sono essenzialmente stampe delle chiavi private e pubbliche di un utente.
Quando si sceglie un portafoglio di criptovalute è importante considerare il tipo di portafoglio, la sicurezza, la facilità d'uso, la proprietà e l'accessibilità.

- Sicurezza: fattore critico nella scelta di un portafoglio di criptovalute. I portafogli hardware sono considerati i più sicuri in quanto non sono connessi a Internet e sono meno inclini all'hacking. Anche i portafogli software sono sicuri, ma sono più suscettibili a hacking e malware.
- Facilità d'uso: la facilità d'uso può variare notevolmente tra i diversi tipi di portafogli. I portafogli software tendono ad essere i più facili da usare, invece i portafogli hardware potrebbero risultare più difficili per alcuni utenti.
- Proprietà: con un portafoglio software, gli utenti hanno il pieno controllo delle proprie chiavi private e hanno la proprietà completa delle proprie risorse. Con i portafogli hardware, gli utenti hanno un controllo limitato sulle loro chiavi private e le loro risorse sono archiviate sul dispositivo hardware.
- Accessibilità: l'accessibilità di un wallet può dipendere dalla tipologia e dalla piattaforma che lo supporta. I portafogli software sono accessibili da qualsiasi dispositivo con una connessione Internet, mentre i portafogli hardware sono limitati al dispositivo su cui sono archiviati.

Alcuni esempi di wallet di criptovalute includono Trust Wallet, Metamask e Ledger.
Trust Wallet è un wallet mobile di criptovalute che consente agli utenti di archiviare, gestire e trasferire in modo sicuro criptovalute. È progettato con particolare attenzione alla sicurezza e alla privacy e offre funzionalità come il backup delle chiavi private, l'autenticazione biometrica e l'integrazione di wallet hardware. Trust Wallet è open-source, il che significa che il suo codice è pubblicamente disponibile per la revisione e la verifica, aumentandone la trasparenza e la sicurezza. Trust Wallet supporta anche le DApps e consente agli utenti di interagire con l'ecosistema della DeFi, compreso lo staking: processo di bloccare una certa quantità di una particolare criptovaluta per supportare la rete e guadagnare ricompense.

MetaMask è un wallet di criptovalute e un'estensione del browser che semplifica l'interazione degli utenti con le DApps, consentendo agli utenti di archiviare e gestire in modo sicuro i propri token e fornendo un'interfaccia semplice e intuitiva per effettuare transazioni.
MetaMask supporta le DApps costruite su reti come Ethereum e Binance Smart Chain, ma anche molte altre. Con MetaMask, gli utenti hanno il pieno controllo delle proprie chiavi

private, garantendo la sicurezza delle proprie risorse. L'estensione del browser è disponibile su Chrome, Firefox, Brave e Edge, rendendola accessibile a una vasta gamma di utenti e permettendo a più persone possibile di partecipare al web decentralizzato.

Un portafoglio Ledger è un tipo di hardware wallet utilizzato per archiviare in modo sicuro le criptovalute. Ledger, un marchio ben noto nel mondo delle criptovalute, offre una gamma di prodotti come Ledger Nano S e Ledger Nano X, che funzionano come dispositivi di cold storage per risorse digitali. I portafogli sono dotati di un chip sicuro e di una semplice interfaccia per l'utente, che li rende un'opzione accessibile e affidabile.
I portafogli Ledger sono considerati uno dei metodi più sicuri per archiviare le criptovalute, poiché le chiavi private sono archiviate offline e protette dai tentativi di hacking. Inoltre, Ledger fornisce un'app complementare che consente agli utenti di gestire facilmente le proprie risorse crittografiche, visualizzare i saldi e la cronologia delle transazioni e, anche, effettuare transazioni.
La regola principale di tutte le tipologie di wallet è mantenere le proprie chiavi private sicure e protette, poiché la perdita dell'accesso ad esse può comportare la perdita delle proprie risorse digitali.

La scelta del giusto exchange di criptovalute è una decisione importante per qualsiasi trader o investitore di criptovalute, avendo molti fattori da considerare.
Uno degli elementi più importanti da valutare quando si sceglie un exchange è la sicurezza. Queste piattaforme sono spesso prese di mira dagli hacker, quindi è fondamentale sceglierne una che disponga di solide misure di sicurezza. Ciò include funzionalità come l'autenticazione a due fattori (2FA), la conservazione a freddo dei fondi e regolari controlli di sicurezza.
Un altro criterio importante sono le opzioni di pagamento. Exchange diversi offrono differenti metodi di pagamento, come bonifici bancari, carte di credito e PayPal.
Anche l'interfaccia utente e l'assistenza clienti sono fattori rilevanti da considerare. Un'interfaccia user-friendly può semplificare il trading e la gestione delle criptovalute, mentre un'assistenza clienti reattiva può fornire aiuto e guida quando necessario.
Quando si sceglie un exchange, è anche necessario considerare i diritti legali. Paesi diversi hanno leggi e regolamenti differenti in materia di criptovalute, quindi è importante utilizzarne uno conforme alle leggi della propria giurisdizione.
Infine, può essere utile leggere recensioni e valutazioni di diversi exchange prima di prendere una decisione. Questo può dare un'idea delle esperienze di altri utenti, inclusi eventuali problemi o preoccupazioni che potrebbero aver riscontrato durante l'utilizzo.

3.2.2 Sicurezza e trend emergenti

Gli exchange non sono immuni da rischi di sicurezza informatica, che possono portare al furto di fondi, tra quelli più significativi associati agli exchange di criptovalute c'è l'hacking. Gli hacker possono sfruttare le vulnerabilità nel software, nell'infrastruttura o nei protocolli di sicurezza dell'exchange per ottenere l'accesso non autorizzato agli account degli utenti e rubare i loro fondi.
Per mitigare questo problema, gli exchange possono implementare solide misure di sicurezza, come l'autenticazione a due fattori (2FA), la crittografia e i portafogli multi-firma. Possono anche condurre regolari controlli di sicurezza e test di penetrazione per identificare e affrontare le vulnerabilità.

Nonostante queste misure, gli exchange hanno sofferto casi di hacking e furto. Ad esempio, nel 2018, l'exchange giapponese Coincheck è stato violato, provocando il furto di oltre 500 milioni di dollari in criptovaluta. Allo stesso modo, nel 2019, l'exchange canadese QuadrigaCX è fallito dopo aver perso l'accesso a $190 milioni di fondi dei clienti.
Per proteggere i propri fondi sugli exchange, è essenziale sceglierne uno affidabile e consolidato con una solida esperienza di sicurezza. Si consiglia inoltre di abilitare la 2FA e di archiviare le proprie risorse digitali in un wallet hardware, invece che lasciarle nell'exchange.

Gli exchange di criptovalute sono suscettibili alla volatilità del mercato e ai rischi di liquidità, che possono influenzare il valore e la disponibilità delle criptovalute. Inoltre, l'industria delle criptovalute non è immune da truffe e frodi, che possono comportare perdite finanziarie per gli investitori.La volatilità del mercato si riferisce alle fluttuazioni rapide e imprevedibili del valore delle criptovalute, le quali sono spesso soggette a speculazioni, che possono portare a significative oscillazioni dei prezzi. I rischi di liquidità alludono alla disponibilità economica di acquirenti e venditori per una particolare criptovaluta, che può influire sulla facilità e sulla velocità del trading.
Per mitigare questi problemi, è consigliabile scegliere exchange consolidati con volumi di scambio elevati e una vasta gamma di criptovalute. Inoltre, gli investitori dovrebbero essere preparati a tollerare un certo livello di volatilità e rischio di liquidità quando investono in criptovalute.

Anche le truffe e le frodi sono comuni nel settore delle criptovalute. Queste possono assumere varie forme, come false offerte iniziali di monete (ICO), schemi Ponzi e truffe di phishing. Le ICO scam coinvolgono società fraudolente che vendono criptovalute false agli investitori, mentre gli schemi Ponzi prevedono il pagamento di investitori precedenti con fondi di nuovi investitori.
Gli exchange di criptovalute sono anche soggetti a vari rischi normativi e legali, tra cui implicazioni fiscali, legislazione internazionale e regolamentazione nazionale. L'impatto delle leggi sulla sicurezza degli exchange può porre sfide significative per la conformità e la gestione del rischio.
Le implicazioni fiscali si riferiscono al trattamento fiscale delle criptovalute e al loro trading. In molte giurisdizioni, le criptovalute sono considerate attività o materie prime e sono soggette all'imposta sulle plusvalenze. Gli investitori dovrebbero consultare dei professionisti fiscali per comprendere i loro obblighi durante il trading di criptovalute.

La regolamentazione degli exchange varia ampiamente tra i paesi. Alcuni hanno adottato un approccio normativo permissivo, mentre altri hanno implementato normative severe o addirittura vietato del tutto le criptovalute. In alcuni casi, la legislazione internazionale, come la Financial Action Task Force (FATF), ha influenzato le normative nazionali sulle criptovalute.La regolamentazione nazionale può porre sfide significative per gli exchange. La conformità ai requisiti normativi, come le normative antiriciclaggio (AML) e know-your-customer (KYC), può essere costosa e richiedere molto tempo.
I rischi normativi e legali possono anche derivare da cambiamenti nel contesto legale e normativo. Ad esempio, le modifiche alle leggi o ai regolamenti fiscali sul trading di criptovalute possono influire sul valore e sulla disponibilità delle criptovalute.
Per mitigare i rischi normativi e legali, gli exchange di criptovalute devono rimanere aggiornati con i cambiamenti nell'ambiente legale e normativo e implementare solidi programmi di conformità e gestione del rischio.

Infine, gli exchange dovrebbero coinvolgere le autorità di regolamentazione e i responsabili politici per sostenere leggi che promuovano l'innovazione e proteggano gli investitori.

Gli exchange di criptovalute hanno fatto molta strada dai primi giorni di Bitcoin, con un numero crescente di investitori e istituzioni che adottano risorse digitali come investimento. Il futuro degli exchange è promettente, con diverse tendenze e sviluppi emergenti che stanno rivoluzionando l'universo delle criptovalute.
La DeFi e gli exchange decentralizzati (DEX) stanno emergendo come un trend significativo nell'intero settore. DeFi si riferisce a un nuovo sistema finanziario basato sulla tecnologia blockchain, che offre servizi finanziari decentralizzati come prestiti e scambi senza intermediari. I DEX sono una componente essenziale dell'ecosistema DeFi, forniscono una piattaforma per il trading peer-to-peer di criptovalute. L'ascesa di DeFi e DEX offre agli investitori maggiore flessibilità e controllo sui propri asset, nonché la possibilità di commissioni più basse.
L'adozione istituzionale delle criptovalute è un'altra tendenza significativa nel settore delle criptovalute. Grandi istituzioni finanziarie, inclusi hedge fund, gestori patrimoniali e banche, stanno iniziando a investire in criptovalute. È probabile che questa adozione istituzionale aumenti la domanda di criptovalute e guidi la liquidità nei mercati delle risorse digitali.

Anche gli sviluppi tecnologici, come l'ascesa dell'interoperabilità blockchain, degli smart contract e degli atomic swap, stanno plasmando il futuro degli exchange di criptovalute. L'interoperabilità blockchain consente a diverse blockchain di comunicare e interagire tra loro, dando luogo ad un trasferimento continuo di risorse su reti diverse. Gli smart contract permettono l'esecuzione automatica di contratti tra parti senza intermediari, mentre gli atomic swap mettono a disposizione lo scambio di criptovalute tra diverse blockchain senza la necessità di un exchange centralizzato.
In conclusione, le prospettive per il futuro degli exchange di criptovalute sono positive, con una crescente adozione da parte di investitori, istituzioni e governi. Gli anni a venire degli exchange saranno modellati da tendenze emergenti come DeFi, adozione istituzionale e sviluppi tecnologici.

3.3 STRATEGIE DI TRADING

3.3.1 Dal mercato finanziario al trading di criptovalute

Mercato finanziario è un termine usato per descrivere il mercato in cui vengono acquistati e venduti strumenti finanziari come azioni, obbligazioni, valute e materie prime. Questi mercati possono essere suddivisi in due categorie principali: il mercato primario e il mercato secondario. Il mercato primario è il luogo in cui i nuovi titoli vengono emessi al pubblico per la prima volta, mentre il mercato secondario è il luogo in cui i titoli esistenti vengono acquistati e venduti.
Il mercato azionario è un ottimo esempio di mercato finanziario. È qui che le azioni delle società quotate in borsa vengono acquistate e vendute. Altri esempi includono il mercato obbligazionario, il mercato valutario e il mercato delle materie prime. Questi mercati forniscono ad aziende, investitori e trader l'opportunità di acquistare e vendere attività finanziarie, gestire i rischi e raccogliere capitali. I mercati finanziari svolgono un ruolo cruciale nell'economia fornendo liquidità, facilitando l'allocazione efficiente delle risorse e promuovendo la crescita economica.

I rendimenti finanziari, invece, si riferiscono ai guadagni o alle perdite generati da un investimento in un determinato periodo di tempo. Questi rendimenti possono presentarsi sotto forma di apprezzamento del capitale, dividendi o interessi.
Diversi tipi di investimenti hanno rendimenti attesi diversi, ad esempio le azioni tendono ad avere rendimenti più elevati ma anche un rischio più elevato, mentre le obbligazioni tendono ad avere rendimenti inferiori ma anche un rischio inferiore.
I rendimenti finanziari possono essere misurati in diversi modi, come il rendimento nominale, il rendimento reale, il rendimento annualizzato e il rendimento totale. È importante considerare anche il rischio insito in qualsiasi investimento e l'orizzonte temporale nella valutazione dei rendimenti generati da un investimento.

Molti studi sulle proprietà delle serie di rendimenti finanziari hanno dimostrato che questi mostrano tre proprietà statistiche che sono presenti in molte, se non in tutte, le serie finanziarie.
Tali proprietà vengono chiamate i tre fatti stilizzati delle serie di rendimenti finanziari:

1. Volatility clusters
2. Code grasse
3. Dipendenza non lineare

La prima proprietà si basa sull'osservazione che grandi cambiamenti o, allo stesso modo, piccoli cambiamenti, tendono a raggrupparsi tra di loro, per questo motivo capita spesso di osservare molti giorni di alta volatilità seguiti da molti giorni di bassa volatilità.
La seconda proprietà è basata sul fatto che le serie finanziarie occasionalmente presentano dei rendimenti positivi o negativi molto elevati e questo fa sì che le code siano più grasse di una normale avendo valori estremi elevati.
Infine, la dipendenza non lineare è da attribuire a come i rendimenti multivariati si relazionano tra di loro. Se i rendimenti sono linearmente dipendenti, la correlazione descrive come si muovono insieme. Se invece sono caratterizzati da una dipendenza non lineare, la correlazione tra i diversi rendimenti dipende dalla grandezza dei risultati. Ad esempio, si è spesso osservato che le correlazioni sono più basse in bull markets che in bear markets, mentre tendono a raggiungere il 100% durante le crisi finanziarie.
Le analogie del trading online in criptovalute con il mercato finanziario non mancano: proprio come avviene per gli investimenti in azioni, il trader spera di ottenere un guadagno vendendo o acquistando gli asset in suo possesso a un prezzo più vantaggioso rispetto a quello dell'operazione precedente.

L'obiettivo dell'investitore sta nell'indovinare, o comunque avvicinarsi, alla previsione del trend futuro e guadagnare:

1. Dalla salita del prezzo, usando la strategia long-selling (LONG);
2. Dalla discesa del prezzo, mediante gli investimenti short-selling (SHORT).

Nel primo caso si ottiene un profitto positivo acquistando un titolo a ribasso e rivendendolo una volta che il relativo prezzo è salito, il guadagno è la differenza tra il prezzo di vendita e quello di acquisto, al netto delle tasse.
La tecnica SHORT, invece, è puramente speculativa e consiste nella vendita allo scoperto: il trader vende dei titoli avuti in prestito e scommette sulla discesa del prezzo, in modo da poter avere comunque un margine di ritorno nonostante la diminuzione del controvalore dell'oggetto su cui si ha investito.

Ricerche di strategie per massimizzare i guadagni nel mercato azionario vengono studiate da decenni, ma non è immediato comprendere se tali soluzioni siano valide anche per il mercato delle criptovalute in cui la variabilità dei tassi di rendimento sembra senza apparenti limiti, in cui l'opportunità di un alto guadagno è tangibile tanto quanto una possibile ingente perdita.
Per poter comprare o vendere criptovalute è sufficiente aprire un portafoglio su uno dei diversi exchange online e acquistare, ad esempio con valuta FIAT, la moneta digitale che potrà a sua volta essere scambiata con altre criptovalute. A differenza di altri sistemi di pagamento tradizionali, le transazioni in criptovalute sono irreversibili e avvengono direttamente tra il portafoglio del venditore e dell'acquirente senza che sia necessario l'intervento o la supervisione di terze parti.

La scelta di investire in criptovalute con il solo scopo di guadagno è essenzialmente una scommessa sul prezzo futuro della moneta. Proprio come avviene per gli investimenti in azioni, il trader spera di ottenere un guadagno nel breve o lungo termine rivendendo gli asset in suo possesso a un prezzo più vantaggioso rispetto a quello al momento dell'acquisto, traendo così profitto dalla compravendita.
Il valore di mercato di una criptovaluta può venire influenzato da un elevato numero di fattori, alcuni di questi sono elementi da non sottovalutare anche per il trading di azioni, come ad esempio il rapporto tra domanda e offerta e il sentimento di mercato, altri sono invece prettamente legati a questo specifico prodotto, come la difficoltà di mining o le utility case della moneta.
L'obiettivo di molte analisi sugli investimenti, in primo luogo in borsa, è proprio riuscire a progettare una buona linea di azione sul mercato, eventualmente misurando anche l'andamento degli elementi citati precedentemente. Di norma l'investitore segue una strategia di trading che pilota l'ingresso e l'uscita sul mercato generando segnali di acquisto e vendita.

Le strategie di trading nel mercato delle criptovalute possono variare notevolmente e sono basate su una serie di diversi fattori. Alcune tra le strategie più utilizzate sono le seguenti:

- HOLDing: detenere una certa criptovaluta, di cui si è studiato il progetto e in cui si ripone fiducia per un possibile sviluppo futuro, per un lungo periodo di tempo nella speranza che il suo valore aumenti.

- Analisi tecnica: utilizzare grafici e indicatori tecnici come medie mobili, RSI e MACD per studiare le tendenze del mercato e fare previsioni sui futuri movimenti dei prezzi.

- Arbitraggio: sfruttare le differenze di prezzo tra le diverse borse per acquistare a basso prezzo e vendere ad un prezzo superiore.

- Day trading: acquistare e vendere in un breve lasso di tempo, spesso lo stesso giorno, nel tentativo di trarre profitto dai movimenti di prezzo a breve termine.

- Trading algoritmico: utilizzare un programma per computer per eseguire automaticamente operazioni basate su determinate regole o algoritmi.

- Pair Trading: acquistare i titoli sottovalutati e vendere quelli sopravvalutati; verrà trattato in maniera dettagliata successivamente.

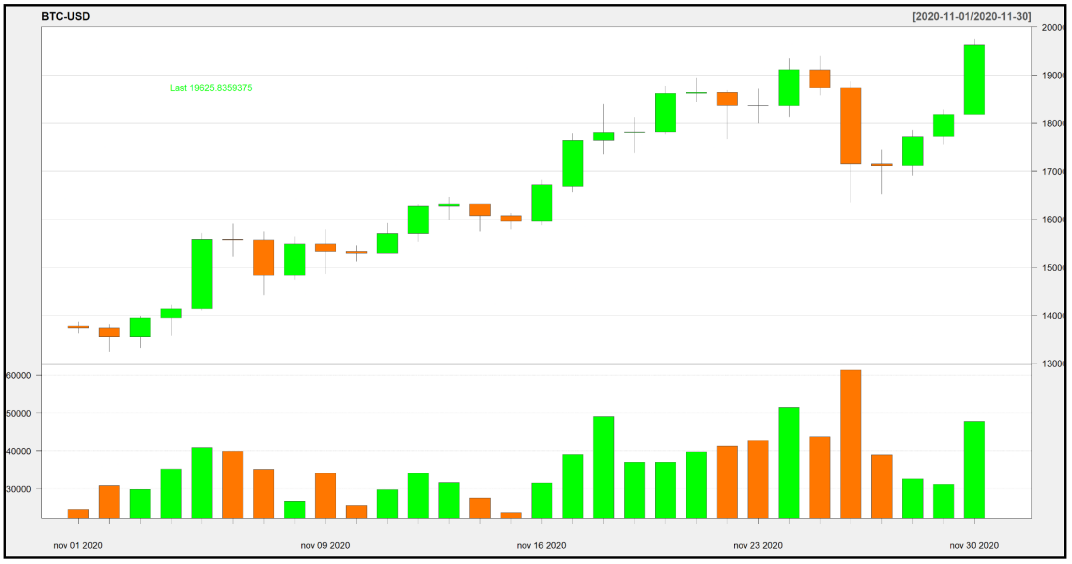
- Trading basato su news: basato su eventi di notizie che muovono il mercato, come annunci di partnership, nuovi sviluppi normativi e altri eventi significativi.

- Swing Trading: strategia in cui le posizioni vengono mantenute per diversi giorni, sfruttando la volatilità e le oscillazioni del mercato.

- Scalping: strategia in cui le posizioni vengono mantenute per un tempo molto breve, di solito solo pochi minuti o secondi, per trarre profitto da piccoli movimenti di prezzo.

È importante tenere presente che le performance passate delle strategie non garantiscono risultati futuri e che i mercati delle criptovalute sono ancora altamente speculativi e volatili. Per visualizzare e interpretare il trend del prezzo di mercato analizzando i dati storici in un determinato intervallo temporale si possono utilizzare le Candele Giapponesi (candlestick): rappresentazione grafica del prezzo di apertura, prezzo massimo, prezzo minimo e prezzo di chiusura di un bene nel periodo considerato. Oltre a questi valori viene generalmente considerato anche il volume delle transazioni in modo da dare un peso all'entità dei movimenti.

Grafico 4: 01/11/2020-30/11/2020 'BTC-USD' chart, generato con RStudio.



Il grafico 4 rappresenta i prezzi di Bitcoin durante il mese di novembre 2020. Il corpo della candela è una misura dell'oscillazione tra prezzo di apertura e chiusura, la figura è verde se l'escursione è positiva, mentre è rossa se la chiusura è in perdita. La barra sottile che taglia in verticale ogni candela tocca il massimo e il minimo del relativo periodo.

Si noti che, a differenza di quanto accade per il mercato azionario, le piattaforme di trading online in criptovalute sono sempre accessibili 24 ore su 24 e 7 giorni su 7, pertanto non esiste una condizione intrinseca di orario di apertura o di chiusura, come invece è per la giornata di borsa.

3.3.2 Indicatori tecnici

L'analisi tecnica del mercato è un comune metodo pensato per aiutare gli azionisti ad aprire posizioni profittevoli. Si tratta di un'analisi fondata sulla convinzione che lo studio dell'andamento storico di prezzo e volume possa racchiudere quasi tutte le informazioni utili per prevedere gli sviluppi futuri.
L'andamento del prezzo sul mercato azionario infatti segue sempre dei trend, per questa ragione il passato può essere visto come preludio di ciò che avverrà in futuro, di fondamentale importanza è la corretta identificazione della ciclicità dei movimenti.

Il calcolo di indicatori statistici a partire dai dati passati può essere associato all'analisi tecnica in modo da offrire un supporto quantitativo nella ricerca di pattern ricorrenti. I dati storici di prezzo (open, close, high, low) e volume sono osservati a prescindere dal periodo storico di riferimento e possono essere considerati la chiave rappresentativa dell'evoluzione del mercato nel breve termine.
Gli indicatori statistici, calcolati su intervalli di tempo più o meno ampi, permettono uno sguardo ad un livello più dettagliato consentendo la comprensione di diverse informazioni. Gli indicatori leading, o primari, suggeriscono una prossima inversione di trend, gli indicatori lagging, invece, si muovono in ritardo e fanno luce sulla situazione del mercato solamente dopo l'arresto del trend, in modo da analizzare l'effetto del movimento su un titolo o un bene. Esistono molte tipologie di indicatori le cui funzioni possono essere riassunte in macro categorie. Il confronto di segnali forniti da indicatori di categorie diverse consente una valutazione maggiormente esaustiva, una tendenza confermata da indicatori di tipo diverso gode infatti di una elevata affidabilità.

L'obiettivo delle medie mobili è misurare la direzione e la forza di un trend, calcolando la media del prezzo in un periodo prestabilito, per mettere in evidenza la tendenza del mercato. Il valore medio viene visto come il riferimento rispetto al quale osservare l'andamento del mercato e cogliere il cambiamento del trend rispetto all'intervallo temporale considerato. Nel caso in cui i prezzi si muovano sopra la media, si parla di movimento rialzista e il segnale da intendere è un avviso di acquisto. Se invece i prezzi scendono al di sotto della media, il segnale è di vendita perché ci si trova in un momento di trend ribassista. Infine il mercato è detto laterale se le oscillazioni di prezzo non sono predominanti in nessun verso.
Le medie mobili sono indicatori di tipo "trend following" proprio perché seguono l'andamento del prezzo, questa loro caratteristica implica sempre un leggero ritardo nei segnali generati. Inoltre la scelta dell'ampiezza del periodo di osservazione è lasciata all'analista, per questa ragione i segnali derivanti da questo indicatore non sono mai esenti da una interpretazione soggettiva.

Data una serie storica Y_t, t=1,2,...,N di una variabile aleatoria dal tempo 1 al tempo T siano:

1. m_1 il numero dei periodi precedenti a t;
2. m_2 il numero dei periodi successivi a t;
3. θ_i Il peso da attribuire all'i-esimo valore osservato.

Si definisce media mobile al tempo t il valore:

- $mm_t = \frac{1}{k} * \sum_{i=-m1}^{m2} \theta_i y_{t+i}$;

dove $m_1 + m_2 + 1 = \mathrm{k}$ è il periodo o l'ordine della media mobile.
Una media mobile può essere classificata come:

1. Semplice, se i pesi θ_i sono tutti uguali a $\frac{1}{k}$, cioè equivale alla media semplice aritmetica;
2. Centrata, se $m_1 = m_2$;
3. Simmetrica, se è centrata e se $\theta_{i-m} = \theta_{i+m} \ \forall \ \mathrm{i} \leq \mathrm{m} \leq m_1 = m_2$;

Con il termine "mobile" ci si riferisce al fatto che ogni volta che si aggiungerà un nuovo prezzo, il più vecchio non verrà più considerato.
Per quanto riguarda il grafico, la media mobile è utile perché mette in rilievo la direzione del trend attenuando le fluttuazioni del prezzo che possono confondere nell'interpretazione del grafico stesso.

Il calcolo della media mobile funziona in modo semplice: dato un tempo t il numero delle osservazioni rimane costante in tale tempo, mentre il valore della media viene aggiornato attraverso un algoritmo che procede eliminando di volta in volta il valore più vecchio (utilizzato per il calcolo relativo al tempo $t - 1$) e introducendo quello più recente.
Le tipologie di media mobile più utilizzate sono la media mobile semplice, la media ponderata e la media esponenziale. Differiscono tra loro in base alla formula del calcolo che può risultare più o meno sensibile alla variazione di prezzo.

La Single Moving Average (SMA), anche chiamata media aritmetica, è un indicatore mediamente utilizzato dagli analisti.
Questo tipo di media viene spesso criticata da molti in quanto assegna la stessa importanza ad ogni singolo dato: in una media mobile a 100 periodi l'ultimo valore ha la stessa importanza (peso) del primo valore.
Detti quindi $C_1,\ldots,C_N$ i prezzi di chiusura, la SMA si calcola tramite la seguente formula:

- $\mathrm{SMA} = \frac{1}{N} * \sum_{i=1}^{N} C_i$;

Dal punto di vista grafico questa corrisponde a una curva che attraversa le candele del grafico e ne indica il trend corrente (uptrend, downtrend ecc.).

Un altro utilizzo della media mobile semplice è quello dell'"incrocio": infatti basta prendere in considerazione due SMA differenti, una di breve periodo (solitamente quelle a 25 o 50 periodi) e una di lungo periodo (solitamente quella di 200 periodi) e si va ad analizzare cosa succede una volta che avviene un loro incrocio. Se l'incrocio tra la curva della SMA(200) e la SMA(50) volge verso l'alto (golden cross), si tratta di un'indicazione che il trend del prezzo del titolo o della criptovaluta sottostante è in salita; è quindi consigliato aprire posizioni long (buy). In caso contrario, se l'incrocio tra le due SMA appena citate volge verso il basso (death cross), c'è da aspettarsi un downtrend; è quindi utile considerare posizioni short (sell).

La Weighted Moving Average, WMA, è utilizzata per ovviare al problema delle medie mobili semplici riguardo al peso da assegnare ai valori presi in considerazione; si dà maggior peso ai prezzi più recenti, in quanto si presuppone che essi esprimano meglio le informazioni disponibili al mercato rispetto ai prezzi meno recenti.

Per quanto riguarda la determinazione dei pesi, nel calcolo delle medie ponderate al valore del giorno t viene assegnato un peso pari a t, alla chiusura del giorno $t - 1$ viene assegnato un peso pari a $t - 1$, e così via.
Facendo in questo modo si dà più peso agli ultimi valori; il totale verrà poi diviso per la somma dei multipli; ad esempio, nel caso di 10 periodi sarà diviso per 1+2+3+ …. +10=55

- $\mathrm{WMA} = (C_1 * 1 + C_2 * 2 + \ldots + C_N * \mathrm{N}) / (1+2+...+\mathrm{N})$;

La Exponential Moving Average, EMA, rappresenta un ulteriore miglioramento rispetto alla media mobile semplice, in quanto supera le limitazioni legate alla ponderazione uniforme dei dati. In sostanza, l'EMA riesce a catturare in modo più accurato le variazioni di prezzo più recenti, rendendola una scelta preferibile per coloro che desiderano una visione più dinamica e reattiva del mercato.

Rispetto alla Media Mobile Pesata, è necessario definire un parametro (detto fattore decadimento), compreso tra 0 e 1, il quale consente di attribuire, in modo progressivo e esponenziale, un peso maggiore ai valori più recenti, senza però annullare del tutto il peso dei valori meno recenti. Il coefficiente è calcolato nel seguente modo:

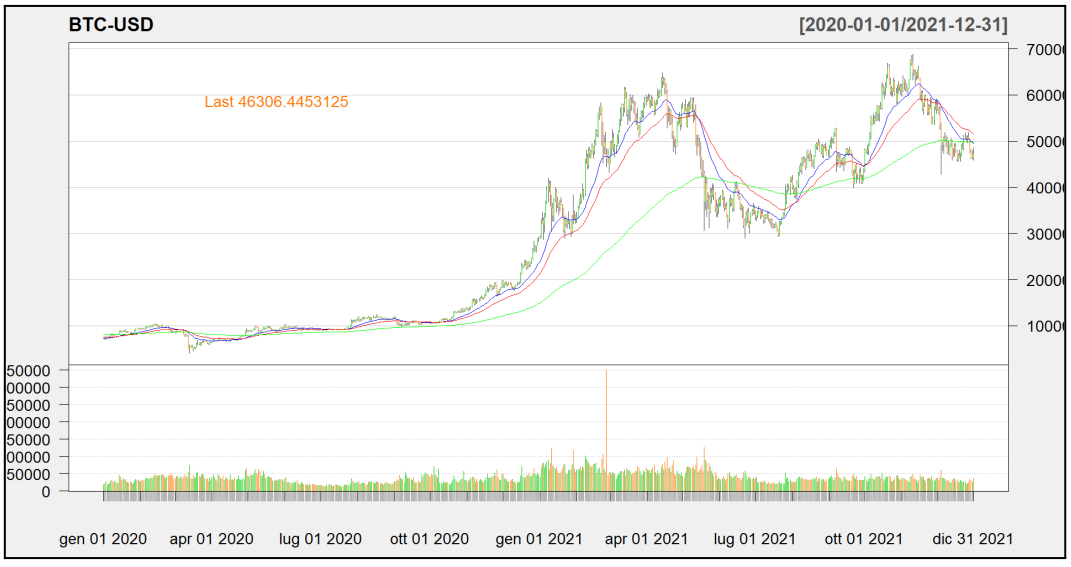
- $\boldsymbol{\alpha} = \frac{2}{N+1}$;

dove N è il numero dei periodi temporali.
La formula completa per calcolare l'EMA è la seguente:

- $EMA = (P_C - EMA_{i-1}) * \boldsymbol{\alpha} + EMA_{i-1}$;

Dove Pc si riferisce al prezzo di chiusura nel periodo attuale e EMA_{i-1} si riferisce al valore della Media Mobile Esponenziale nel periodo precedente.

Grafico 5: 01/01/2020-31/12/2021 'BTC-USD' chart, generato con RStudio.



Il grafico 5 mostra i prezzi di Bitcoin dal 1/1/2020 al 31/12/2021 e l'applicazione di 3 EMA: EMA26 (linea blu), EMA50 (linea rossa) e EMA200 (linea verde). Se si fa un confronto tra Media Mobile Semplice e Media Mobile Esponenziale si può dire che quest'ultima reagisce in maniera più rapida alle variazioni della tendenza del prezzo.
Dal grafico possiamo notare un'altra differenza: oltre al fatto che l'EMA segue con più accuratezza i prezzi, si vede anche che essa cambia pendenza più rapidamente.

Quindi l'EMA è la media mobile più sensibile a variazioni immediate del trend; e può essere rappresentativa anche di un intervallo di tempo molto lungo, senza per questo perdere la sua reattività.

Con l'acronimo MACD (Moving Average Convergence/Divergence, ovvero convergenza e divergenza di medie mobili) si intende un oscillatore di analisi tecnica utilizzato per studiare l'andamento dei prezzi dei mercati finanziari nel tempo, in modo da prevedere le tendenze future. Questo oscillatore è stato studiato e sviluppato da Gerard Appeal alla fine del 1970 e si basa su medie mobili esponenziali. Successivamente, nel 1986, Thomas Aspray ideò un'implementazione di tale oscillatore, ovvero il MACD istogramma.

Grafico 6: 01/01/2021-31/12/2021 'BNB-USD' chart, generato con RStudio.

Il grafico 6 mostra l'applicazione dell'indicatore MACD ai prezzi di BNB durante il 2021. Per costruire questo indicatore sono necessarie tre medie mobili esponenziali, sul grafico però vengono visualizzate solo due linee dato che una coppia delle tre appena citate è utilizzata unicamente per calcolare la loro differenza. La prima media mobile, quella più veloce, viene calcolata a 12 periodi, mentre quella più lenta è a 26 periodi. Queste due medie vengono sottratte tra loro, la relativa differenza sarà quindi rappresentata graficamente da una sola linea. Per la generazione di segnali si è introdotta una terza linea, un'altra media mobile esponenziale, solitamente a 9 periodi, della precedente differenza. Abbiamo quindi:

- $MACD = EMA_{12} - EMA_{26}$;

dove EMA sta per media mobile esponenziale;

- $SignalLine = EMA_{9}[MACD]$;

cioè una media mobile esponenziale della linea di MACD.
Il MACD permette l'individuazione di differenti segnali: il più importante tra questi si genera in seguito all'incrocio della linea della MACD e la Signal Line. Un incrocio rialzista (dal basso verso l'alto) tra queste due linee sarà un segnale di acquisto, al contrario, un incrocio ribassista (dall'alto verso il basso) indicherà un segnale di vendita.

Il Relative Strength Index (RSI) è un indicatore di forza relativa, sviluppato dall'ingegnere meccanico John Welles Wilder e pubblicato nel suo libro " New Concepts in Technical Trading System" del 1978.
Tale indicatore è utilizzato per identificare la forza interna di un asset finanziario in un intervallo di tempo, misurando la velocità e il peso della direzione dell'andamento del prezzo, in modo tale da anticipare la possibile inversione di un trend e evidenziare zone di ipercomprato e ipervenduto.

Il relative Strength Index è calcolato come:

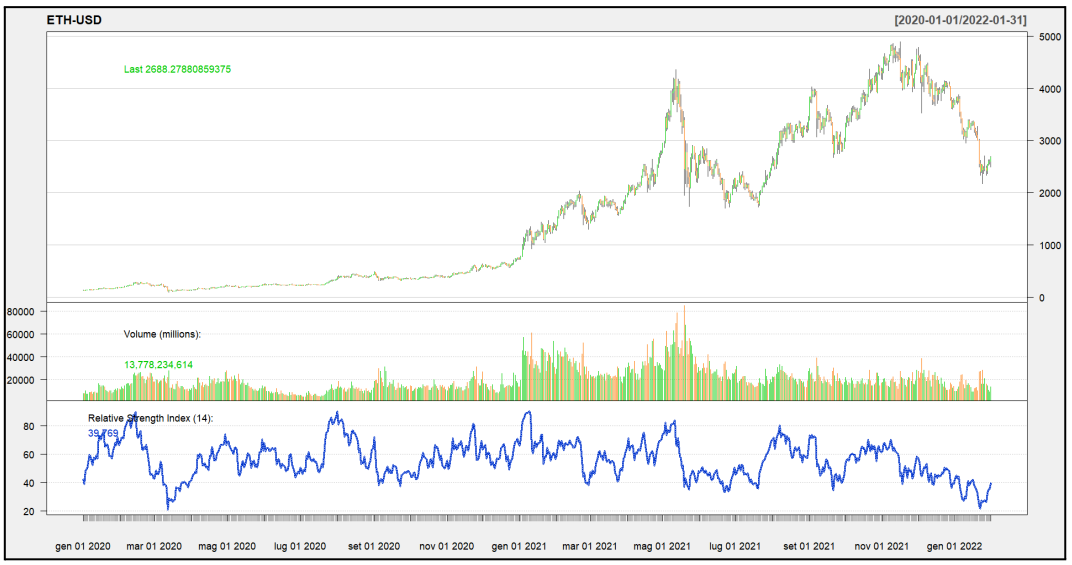
- $\mathrm{RSI} = \frac{100}{1+RS}$;

Dove RS è il rapporto tra la media delle variazioni positive e la media delle variazioni negative fatte segnare dal prezzo del titolo nel periodo "N":

- $\mathrm{RS} = \frac{MV_p}{MV_n}$;

In particolare, per "media delle variazioni positive" si intende la media delle differenze, tra i valori di apertura e chiusura del prezzo, negli ultimi periodi rialzisti compresi in N; viceversa, per "media delle variazioni negative" si intende la differenza, tra i valori di apertura e chiusura del prezzo, negli ultimi periodi ribassisti compresi in N.
La costruzione matematica di questo oscillatore necessita quindi di un solo parametro, cioè il numero di periodi che si vuole considerare. La scelta del numero riguardo al valore di "N" risulta di fondamentale importanza, dato che all'aumentare del numero di periodi diminuisce il numero di falsi segnali, ma si ha anche una minore reattività. Nel suo libro Wilder consiglia l'utilizzo di un valore di n periodi uguale a 14.

Grafico 7: 01/01/2020-31/01/2022 'ETH-USD' chart, generato con RStudio.



Il grafico 7 mostra l'applicazione dell'indicatore RSI ai prezzi di ETH da gennaio 2020 a gennaio 2022. Questo indicatore presenta una banda d'oscillazione costante, da 0 a 100, che permette una comparazione dei valori con alcuni livelli costanti prestabiliti, con lo scopo di individuare le fasi di ipercomprato e ipervenduto.
Segnali di ipercomprato si evincono da un RSI superiore a 70, mentre di ipervenduto è ravvisabile da un RSI inferiore a 30; si possono scegliere soglie più rigide per azzerare i falsi segnali. Anche la linea mediana del 50 va considerata, ma pur sempre in subordine rispetto

ai valori 30 e 70. Molto importanti e interessanti sono anche le divergenze rialziste o ribassiste in relazione al corso dei prezzi sul grafico.

Le bande di Bollinger prendono il nome dal loro ideatore John Bollinger, un analista tecnico americano, che le ha formalizzate nel libro del 2002 “Bollinger on Bollinger Bands”.
Questo indicatore di analisi tecnica è costituito da 3 bande:

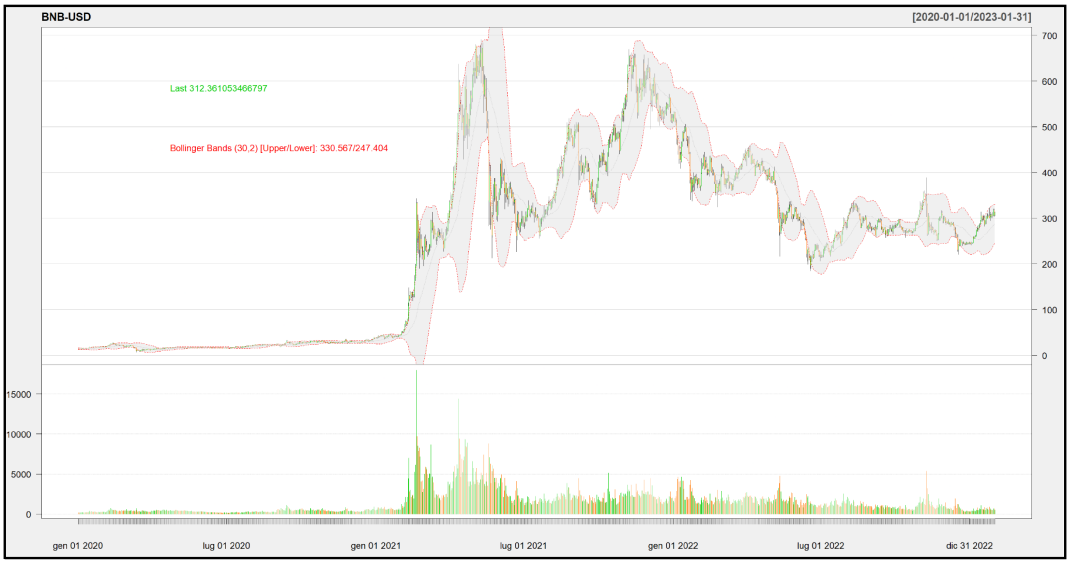
- LC: linea centrale;
- LI: linea inferiore;
- LS: linea superiore;

La banda centrale è una media mobile, tipicamente quella a 20 giorni. La banda superiore rappresenta la deviazione standard del prezzo del titolo al di sopra della media mobile, mentre quella inferiore rappresenta la deviazione standard del prezzo del titolo al di sotto della media mobile.
Da un punto di vista matematico è possibile calcolare questi tre valori:

- $LC_t = \frac{1}{N} * \sum_{i=0}^{N-1} P_{t-i}$;
- $LI_t = LC_t + \frac{m}{N}\sqrt{\sum_{i=0}^{N-1} (P_{t-i} - LC_t)^2}$;
- $LS_t = LC_t + \frac{m}{N}\sqrt{\sum_{i=0}^{N-1} (P_{t-i} - LC_t)^2}$;

Dove “N” indica il valore dei periodi e “m” il numero di dati utilizzati per calcolare la deviazione standard.

Grafico 8: 01/01/2020-31/01/2023 ‘BNB-USD’ chart, generato con RStudio.



Il grafico 8 mostra i prezzi di BNB durante l’arco degli anni 2020 e 2021, ai quali vengono aggiunte le bande di Bollinger. L’idea alla base di questo indicatore è che i prezzi tendono a rimanere all'interno delle bande superiore e inferiore e che i cambiamenti nella volatilità possono essere rilevati dai cambiamenti nella distanza tra le bande.

Le Bande di Bollinger, da un punto di vista grafico, si presentano come tra linee tracciate all'interno e intorno alla serie storica dei prezzi, linee che possono guidare l'investitore nelle sue decisioni strategiche.
Questo indicatore viene utilizzato spesso per identificare potenziali punti di acquisto e vendita e per aiutare a valutare se il prezzo corrente di un titolo è ipercomprato o ipervenduto.

4. ANALISI DELLA PROFITTABILITA'

4.0.1 Step da seguire

Uno degli scopi di questa lunga fase di studio è stata la scelta selettiva delle features realmente influenti sui movimenti di mercato e di cui dover quindi tenere conto per l'elaborazione di strategie efficaci. Queste caratteristiche includono dati storici di prezzo, volumi di scambio e applicazioni nei vari settori. Una volta scelte le criptovalute per l'analisi, vengono raccolti i dati corrispondenti per un periodo di tempo significativo. È importante considerare le monete digitali che sono rilevanti per le strategie di trading in esame e assicurarsi di avere un periodo di tempo sufficiente per valutare le performance.
I dati sono messi a disposizione da Yahoo Finance, ottenuti da CryptoCompare, che permette il download di dati aggregati estratti dalle maggiori piattaforme di scambio.

Nella fase preliminare, vengono raccolte informazioni sulle criptovalute di interesse, tra cui Bitcoin (BTC), Ethereum (ETH) e Binance Coin (BNB). Vengono anche visualizzati i grafici dei prezzi storici e calcolate le statistiche di base.
Poi, viene effettuata un'analisi delle correlazioni tra le criptovalute considerate, utilizzando i dati storici dei loro prezzi, in modo tale da trovare le monete digitali più influenti nel mercato, che verranno utilizzate nelle strategie di trading. Vengono calcolate le matrici di correlazione e vengono visualizzate graficamente le correlazioni con un'heatmap.

Successivamente, vengono applicate alcune strategie di analisi tecnica alle criptovalute considerate. In particolare, vengono calcolati diversi indicatori tecnici come la media mobile semplice (SMA), la media mobile esponenziale (EMA), il Moving Average Convergence Divergence (MACD), le Bollinger Bands e il Relative Strength Index (RSI); con gli ultimi due di questi vengono sviluppate delle strategie di trading LONG e SHORT.
A questo punto, vengono elaborate e valutate delle strategie di HOLDing, che consistono nel mantenere le criptovalute a lungo termine senza effettuare continue operazioni di trading attivo.

Infine, dopo aver simulato le diverse strategie, è necessario valutare e confrontare le performance prodotte. Ciò viene effettuato attraverso l'utilizzo delle seguenti metriche finanziarie: numero di trade, somma dei rendimenti, media dei rendimenti e profitto medio annuo. In particolare, la media dei rendimenti (o rendimento medio per trade) rappresenta la metrica più significativa, in quanto permette una migliore comparazione tra le diverse strategie di trading elaborate.

4.1 ANALISI PRELIMINARI

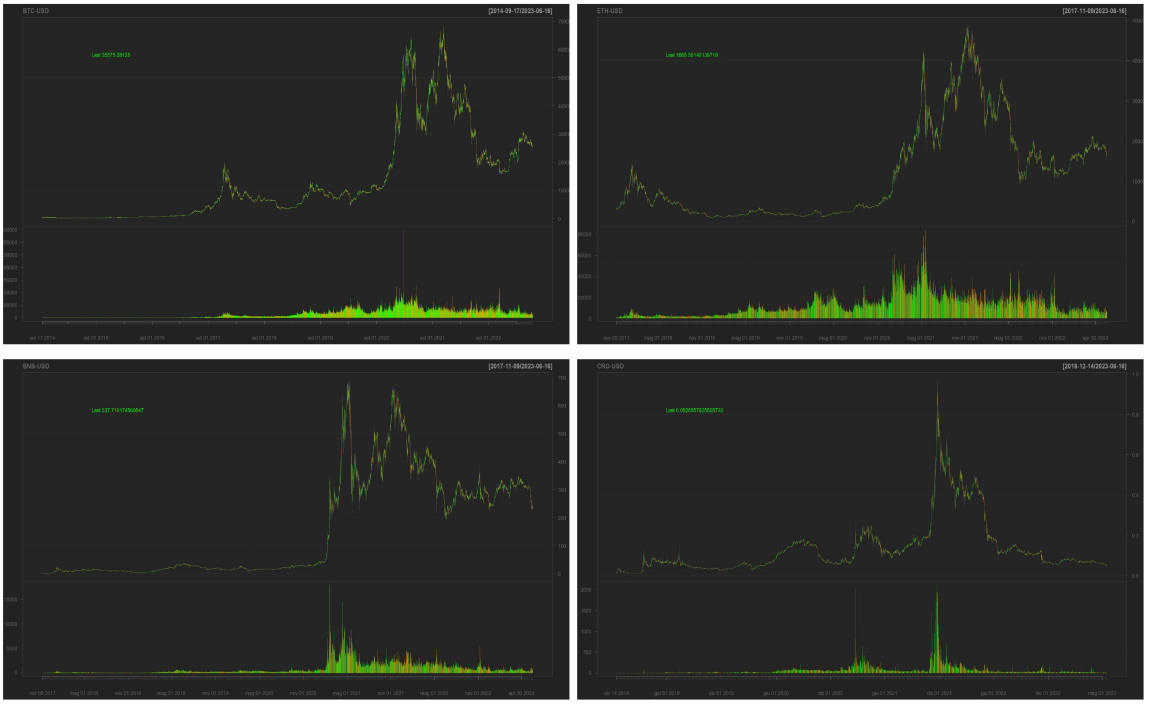
Questo primo paragrafo di analisi preliminare riguarda principalmente l'utilizzo di diversi pacchetti e funzioni in R per eseguire analisi e visualizzazioni generali dei dati raccolti relativi alle criptovalute descritte precedentemente. Il basket di monete digitali selezionate è composto quindi da: Bitcoin (BTC), Ethereum (ETH), Binance Coin (BNB), Cronos (CRO), Cardano (ADA), Polkadot (DOT), Solana (SOL), VeChain (VET), iOTA (MIOTA), Decentraland (MANA), The Sandbox (SAND), The Graph (GRT), SingularityNET (AGIX) e Chainlink (LINK). I pacchetti caricati offrono una serie di funzionalità per l'analisi finanziaria e la manipolazione dei dati.

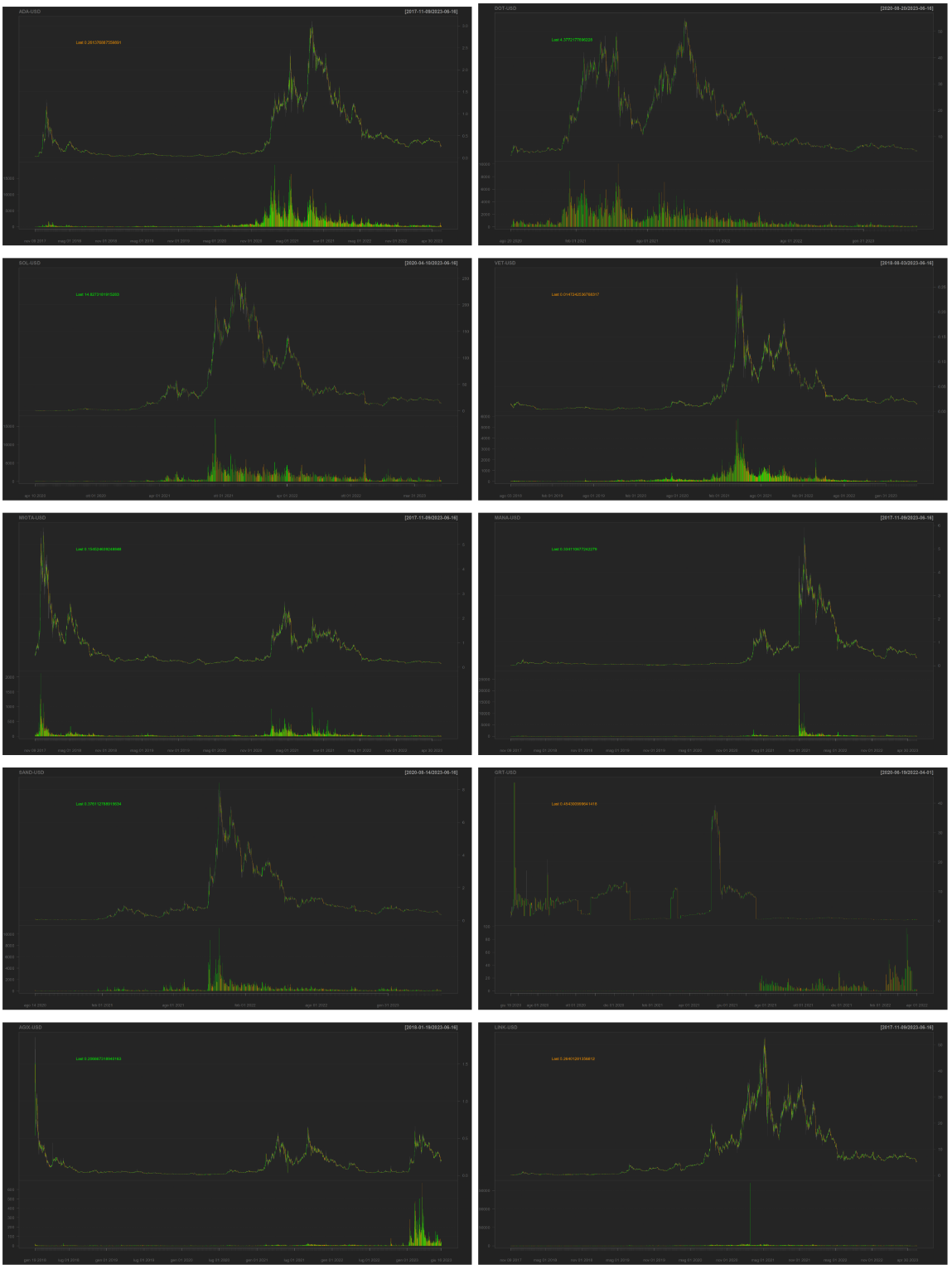
Viene creata una raccolta di dati relativi alle criptovalute scelte utilizzando la funzione getSymbols(), del pacchetto "quantmod", che recupera i dati storici delle monete digitali da Yahoo Finance.
Vengono scaricati tutti i dati disponibili relativi a prezzo e volume, per l'intervallo di tempo più ampio possibile. Nello specifico, ogni elemento si riferisce a un preciso giorno dell'anno ed a una determinata valuta ed è definito per i seguenti attributi:

- Prezzo di apertura;
- Prezzo massimo;
- Prezzo minimo;
- Prezzo di chiusura;
- Volume, riferito alle transazioni in uscita.

Successivamente, vengono mostrati alcuni grafici a linee per visualizzare i dati dei prezzi delle criptovalute. La funzione chartSeries(), del pacchetto "quantmod", viene utilizzata per creare questi grafici.

Grafici 9-22: 'BTC-USD', 'ETH-USD', 'BNB-USD', 'CRO-USD', 'ADA-USD', 'DOT-USD', 'SOL-USD', 'VET-USD', 'MIOTA-USD', 'MANA-USD', 'SAND-USD', 'GRT-USD', 'AGIX-USD', 'LINK-USD' charts, generati con RStudio.





Dall’osservazione dei grafici 9-22 appaiono subito evidenti i diversi movimenti di prezzo delle varie criptovalute. Da questa prima visualizzazione, le monete digitali sembrerebbero poco correlate le une con le altre, sebbene alcune presentino dei tratti in comune; bisogna effettuare ulteriori analisi. Dopo l’osservazione dei grafici, vengono estratti i prezzi di chiusura di Bitcoin (in USD), che vengono salvati in un vettore denominato price_BTC. Viene quindi utilizzata la funzione basicStats(), del pacchetto "fBasics", che fornisce una sintesi di tutte le statistiche descrittive della serie dei prezzi di Bitcoin.

La skewness dà un'indicazione di quanto la distribuzione si concentri intorno alla propria media. In particolare, nel caso in esame, la skewness è prossima allo 0, con un valore approssimativo di 1,42. Una skewness positiva, anche se di poco, rappresenta una situazione negativa in quanto va a significare che la distribuzione delle performance giornaliere si concentra a sinistra della media.

La kurtosis, invece, è un indice che misura lo spessore delle code di una funzione di densità. Se il coefficiente di kurtosis è minore di 0, la curva si definisce platicurtica, cioè più piatta di una normale, e sta a significare che la dispersione dei valori intorno alla propria media è molto ampia. Se il coefficiente di kurtosis è maggiore di 0, come in questo caso (1,05), la curva si definisce leptocurtica e i valori della distribuzione sono concentrati intorno alla media. La leptocurtosi è fenomeno comune a quasi tutte le serie storiche dei rendimenti di asset finanziari.
Infine, vengono creati ulteriori vettori di prezzi per tutte le altre criptovalute.

4.1.1 Correlazioni tra criptovalute

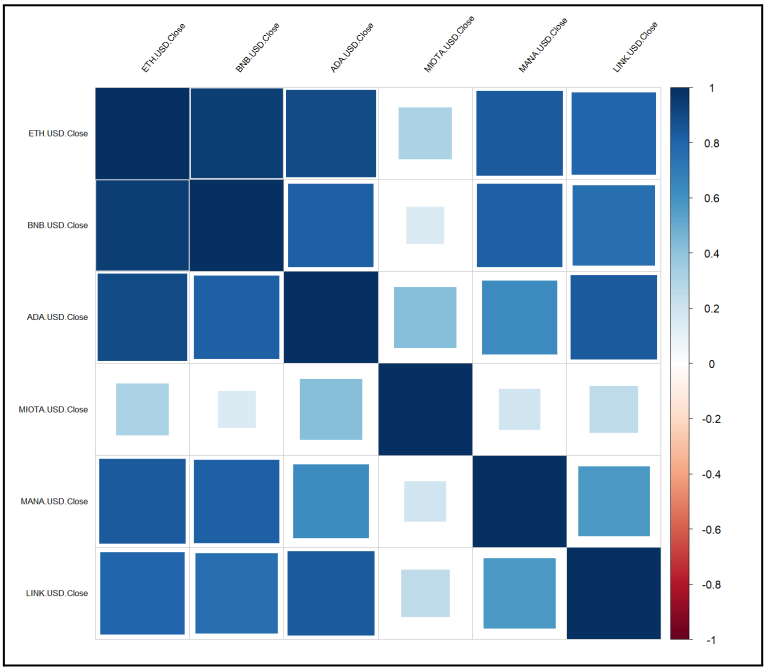
Per la caratteristica di persistenza di alti livelli di volatilità presente sul mercato delle monete digitali, in questa analisi si è deciso di utilizzare il prezzo di chiusura giornaliero come prezzo della criptovaluta, poiché esso incorpora tutte le attività del giorno.
Un altro argomento di cui si è già parlato sono gli alti livelli di correlazione presenti sul mercato delle criptovalute. La correlazione indica la tendenza che hanno due variabili (X e Y) a variare insieme, ovvero, a covariare.

I periodi ribassisti di BTC nel 2018 e nel 2022 hanno portato inevitabili perdite anche per le più importanti criptovalute presenti nel mercato, giustificando l'idea di una possibile correlazione tra esse. Le principali altcoins hanno seguito, nel periodo di studio considerato, un andamento analogo, seppure con intensità diverse. La causa fondamentale di un così simile andamento di mercato della maggioranza delle monete digitali è la forte correlazione che c'è tra questi stessi strumenti ed il "market mover", ossia il Bitcoin.

Analizziamo ora la matrice delle correlazioni, la quale può risultare un buon indicatore approssimativo per identificare la relazione tra asset finanziari.
Inizialmente, viene valutata la lunghezza delle dimensioni delle osservazioni per le diverse criptovalute utilizzando la funzione length(). Questa fornisce il numero di elementi in ciascun vettore di prezzi, come ad esempio p per Bitcoin, p_E per Ethereum e p_B per Binance Coin. Come era già stato possibile osservare dai grafici 9-22, la maggior parte delle serie storiche delle monete digitali in esame hanno differenti lunghezze.

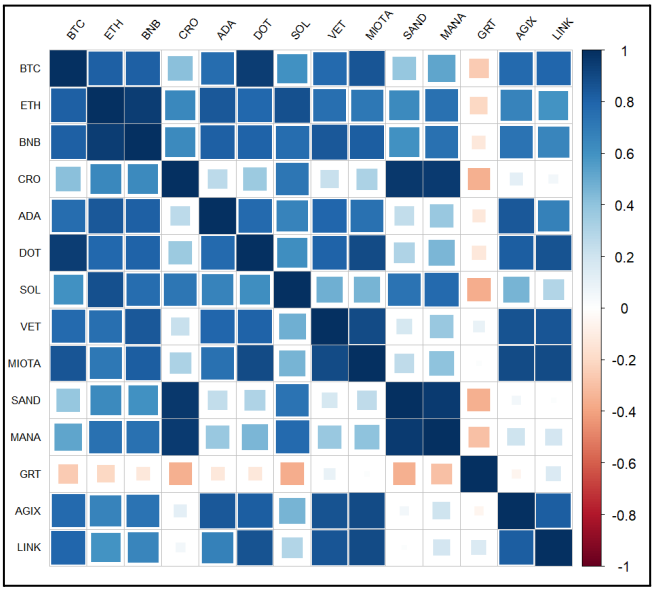
Quindi, viene calcolata la matrice di correlazione utilizzando la funzione cor() applicata ai vettori dei prezzi delle criptovalute selezionate, ovvero le monete digitali con lo stesso numero di osservazioni. I vettori vengono combinati utilizzando la funzione cbind() e la matrice di correlazione risultante viene assegnata alla variabile cor. Questa matrice viene poi visualizzata utilizzando la funzione corrplot(), del pacchetto "corrplot", che crea un grafico delle correlazioni con colori e stili specifici.

Grafico 23: ‘ETH-USD’, ‘BNB-USD’, ‘ADA-USD’, ‘MIOTA-USD’, ‘MANA-USD’, ‘LINK-USD’ heatmap, generata con RStudio.



Il grafico 23 mostra un’elevata correlazione tra tutte le criptovalute considerate (con lo stesso numero di osservazioni), ad eccezione di MIOTA. Le più correlate risultano ETH e BNB, le quali presentano tutte correlazioni superiori allo 0.75 (ad eccezione che con MIOTA).
Successivamente, viene definito un periodo di analisi, utilizzando le variabili startDate e endDate per indicare la data di inizio e fine del lasso di tempo scelto. Vengono quindi acquisiti i dati delle criptovalute selezionate utilizzando la funzione getSymbols() con le date specificate; i dati vengono assegnati a variabili come BTC per Bitcoin e ETH per Ethereum. Dopo, viene calcolata una nuova matrice di correlazione utilizzando i dati delle criptovalute nel periodo specificato. La procedura è simile a quella descritta in precedenza, con l'utilizzo della funzione cor() e la creazione di un grafico delle correlazioni utilizzando corrplot().

Grafico 24: ‘BTC’, ‘ETH’, ‘BNB’, ‘CRO’, ‘ADA’, ‘DOT’, ‘SOL’, ‘VET’, ‘MIOTA’, ‘SAND’, ‘MANA’, ‘GRT, ‘AGIX’, ‘LINK’ heatmap, generata con RStudio.



Come è possibile osservare dalla matrice di correlazione, la maggior parte delle criptovalute presenta valori superiori alla media, quindi è possibile affermare che, almeno nel breve periodo, esiste una correlazione. In particolare, BTC presenta valori superiori allo 0.6 rispetto a 9 delle 13 altcoins in esame (fanno eccezione CRO, SAND, MANA e GRT). ETH e BNB presentano valori superiori allo 0.6 con, rispettivamente, 11 e 12 differenti altcoins, risultando le due monete digitali maggiormente correlate con le altre.
Tra le criptovalute meno correlate troviamo CRO, SAND e MANA con solamente 5 valori sopra lo 0.6. La meno correlata, che presenta solo 3 valori positivi, risulta GRT.
Inoltre, è possibile notare che spesso le monete digitali appartenenti allo stesso settore presentano delle elevate correlazioni. VET e MIOTA, legate all'Internet of Things, mostrano una correlazione di 0.89, mentre SAND e MANA, appartenenti al mondo di metaversi e NFT, presentano un valore di 0.96.

Dai risultati ottenuti si può confermare ciò che è stato detto fino ad ora: tra le varie criptovalute vi è un'elevata correlazione. È fondamentale però chiarire che questa relazione non è statica, ma tende a variare nel tempo: infatti, generalmente, la correlazione tra diverse classi di asset e mercati aumenta in periodi di elevata volatilità.

4.2 STRATEGIE DI ANALISI TECNICA

Partendo dai risultati ottenuti precedentemente, è stata presa la scelta di utilizzare le criptovalute BTC, ETH e BNB per elaborare le strategie di trading, in quanto rappresentano le monete digitali con maggiore influenza nel mercato.
In questa fase iniziale, i dati relativi al prezzo di Bitcoin vengono usati per il calcolo di determinati indicatori tecnici. Come già anticipato, alcuni indicatori assumono valori relativi limitati in un intervallo preciso, altri invece sono una misura assoluta, fanno parte di quest'ultima tipologia le medie mobili.

La prima sezione del codice fornito riguarda l'applicazione delle medie mobili (SMA, EMA e WMA) al grafico dei prezzi di Bitcoin. Le medie mobili sono indicatori ampiamente utilizzati nell'analisi tecnica per identificare le tendenze di prezzo e generare segnali di trading, maggiori saranno le lunghezze dei periodi presi in considerazione e più sarà lento il movimento della curva della media.

Inizialmente, viene creato un grafico del prezzo di Bitcoin nel periodo compreso tra gennaio 2020 e dicembre 2021, utilizzando la funzione chartSeries. Successivamente, vengono aggiunte le medie mobili semplici utilizzando la funzione addSMA con i rispettive finestre temporali di 26, 50 e 200 periodi. Le medie mobili semplici vengono calcolate come la media aritmetica dei prezzi di chiusura nel periodo specificato (grafico 25).
Dopo, vengono visualizzate le medie mobili pesate (WMA) con finestre temporali di 10 e 20 periodi, calcolate utilizzando la funzione addWMA. Viene creato un nuovo grafico del prezzo di Bitcoin durante l'anno 2021 (grafico 26).
Infine, vengono visualizzate le medie mobili esponenziali (EMA) con finestre temporali di 26, 50 e 200 periodi, calcolate utilizzando la funzione addEMA. Viene creato un altro grafico del prezzo di Bitcoin nel periodo compreso tra gennaio 2020 e dicembre 2021 (grafico 5).

Grafico 25: 01/01/2020-31/12/2021 'BTC-USD' chart, generato con RStudio.

Grafico 26: 01/01/2021-31/12/2021 'BTC-USD' chart, generato con RStudio.

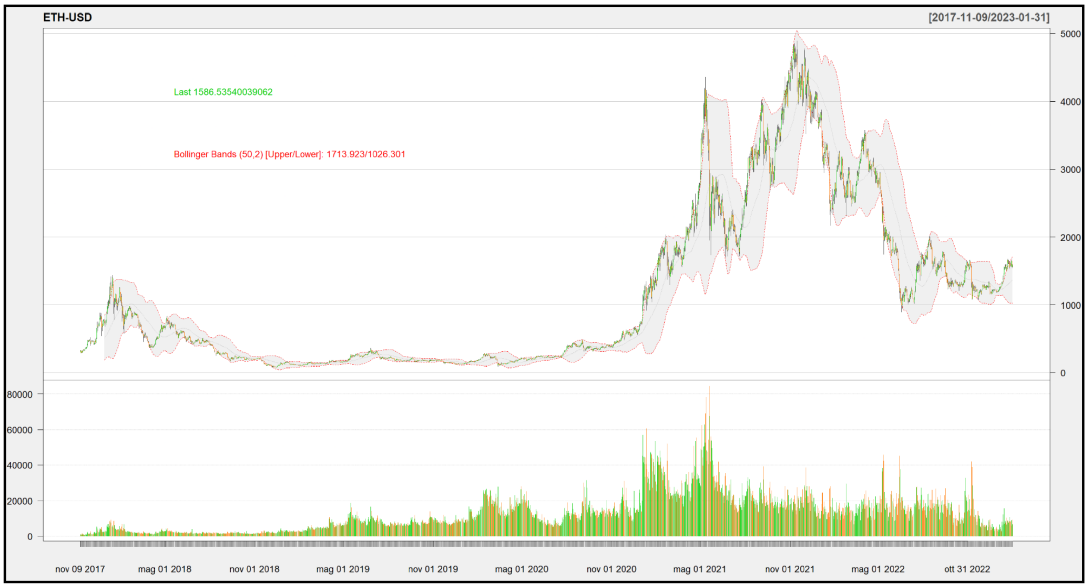
Come possiamo notare nel grafico 25, la curva rossa, ovvero la SMA200, segue molto "in ritardo" l'andamento del prezzo di Bitcoin, a differenza delle curve blu (SMA26) e verde (SMA50), che sono più reattive. Per quanto riguarda il grafico 26, si è voluto sperimentare il movimento delle medie mobili prendendo in considerazione intervalli temporali più brevi, per capire che differenze troviamo. In effetti, osservando l'andamento dei prezzi sul grafico, si nota una maggior reattività delle Medie Mobili nei confronti del prezzo di Bitcoin.
L'obiettivo di questi grafici è fornire una rappresentazione visiva delle medie mobili e delle tendenze di prezzo di Bitcoin. Le diverse finestre temporali e le differenti tipologie di medie mobili consentono di osservare le variazioni nel comportamento del prezzo nel corso del tempo e di identificare eventuali segnali di trading.

In questo elaborato le medie mobili verranno utilizzate per formulare strategie di trading mediante altri indicatori tecnici, ritenuti più precisi ed affidabili, e non come unici generatori di segnali.

La funzione fBBands è stata definita per calcolare le bande di Bollinger. Prende in input il prezzo dell'asset, la finestra temporale n (nel caso in esame uguale a 30) e il numero di deviazioni standard sd (nel caso in esame uguale a 2) per determinare la larghezza delle bande. Utilizza la funzione SMA per calcolare la media mobile semplice del prezzo nel periodo specificato, poi vengono calcolate le deviazioni standard basate sui dati precedenti. Le bande superiori e inferiori vengono calcolate aggiungendo e sottraendo il prodotto della deviazione standard e del numero di deviazioni standard specificato dalla media mobile. Successivamente, vengono eseguiti i calcoli per l'asset specifico. Viene creato un grafico, utilizzando la funzione chartSeries, per visualizzare i dati storici del prezzo dell'asset e le bande di Bollinger sovrapposte (Grafici 27,28,8).

Grafico 27: 01/01/2020-31/01/2023 'BTC-USD' chart, generato con RStudio.

Grafico 28: 09/11/2017-31/01/2023 'ETH-USD' chart, generato con RStudio.



Il grafico 27 rappresenta i prezzi di BTC da gennaio 2020 a dicembre 2022, mentre il grafico 28 mostra i prezzi di ETH da novembre 2017 a gennaio 2023. A queste due serie sono state aggiunte le rispettive bande di Bollinger.
Come già accennato, questo indicatore consiste in tre linee. Le due bande, superiore e inferiore, funzionano da supporto e resistenza dinamica. Come è osservabile dai grafici, uno dei principali problemi delle bande di Bollinger riguarda le fasi di trend del mercato. In tali fasi può succedere che i prezzi corrono lungo tutta la banda, così che l'investitore chiuda l'operazione di vendita in modo prematuro e apra troppo presto l'operazione di acquisto.

La strategia di trading viene implementata nelle funzioni fBB_long e fBB_short, che usano le bande di Bollinger calcolate e il prezzo dell'asset come input.
La strategia di trading LONG si basa sulla condizione che il prezzo scenda al di sotto della banda inferiore e, successivamente, superi la banda superiore. Quando ciò accade, viene registrato il prezzo di apertura dell'asset (Open Price Long) e il prezzo di uscita (Exit Price Long. Viene calcolato anche il guadagno percentuale.

La strategia di trading SHORT, invece, si basa sulla condizione che il prezzo salga al di sopra della banda superiore e, in un secondo momento, scenda al di sotto della banda inferiore. Quando ciò accade, viene registrato il prezzo di apertura della posizione short (Open Price Short) e il prezzo di uscita (Exit Price Short). Anche qui viene calcolato il guadagno percentuale, ma in modo negativo poiché si tratta di una posizione short.

I risultati delle strategie di trading vengono registrati in data frame separati per ciascuna criptovaluta (BTC, ETH, BNB) utilizzando la funzione rem_zero per rimuovere eventuali righe con valori nulli o zeri. Vengono quindi calcolati il numero di trade effettuati, la somma dei guadagni percentuali, la media dei guadagni percentuali e il profitto medio annuo.

Tabella 2: Profitti strategia LONG con le Bollinger Bands.

Strategia LONG	BTC	ETH	BNB
Numero di trade	41	34	32
Somma profitti	770,23%	948,35%	796,5%
Media profitti	18,79%	27,89%	24,89%
Profitto medio annuo	110,03%	189,67%	159,3%

La strategia LONG, riassunta nella tabella 2, mostra solo valori positivi, con dei profitti medi per operazione che vanno dal 18,8% (BTC) al 27,9% (ETH). Anche i numeri dei trade effettuati sono sufficientemente alti, il minimo è rappresentato dalle 32 operazioni nella strategia applicata a BNB.
Infine, le somme dei guadagni permettono di valutare la profittabilità di questa strategia a lungo termine, ovvero dalla nascita delle criptovalute analizzate, mostrando degli ottimi risultati: 770,2% (BTC), 948,3% (ETH) e 796,5% (BNB).

Tabella 3: Profitti strategia SHORT con le Bollinger Bands.

Strategia SHORT	BTC	ETH	BNB
Numero di trade	39	30	31
Somma profitti	565,88%	564,72%	646,08%
Media profitti	14,51%	18,82%	20,84%
Profitto medio annuo	80,84%	112,94%	129,21%

I risultati della strategia SHORT, riportati nella tabella 3, si rivelano molto simili a quelli della strategia LONG. Per ogni criptovaluta, le operazioni effettuate sono almeno 30 e la media dei profitti, tutti positivi, va dal 14,5% (BTC) al 20,8% (BNB).
Quindi, una prima differenza vede BNB essere la criptovaluta più profittevole per questa strategia, in quella LONG era ETH. Inoltre, si osservano dei guadagni minori a livello generale, con le somme dei profitti che non superano il 646,1%; valore inferiore ad ogni guadagno totale della strategia LONG.

In conclusione, il codice implementa una strategia di trading basata sulle bande di Bollinger per le criptovalute BTC, ETH e BNB. Vengono calcolate le bande di Bollinger e, successivamente, vengono identificati i punti di ingresso e di uscita per le posizioni LONG e SHORT in base alle condizioni specificate. I risultati delle strategie di trading vengono quindi analizzati per valutare la loro profittabilità.

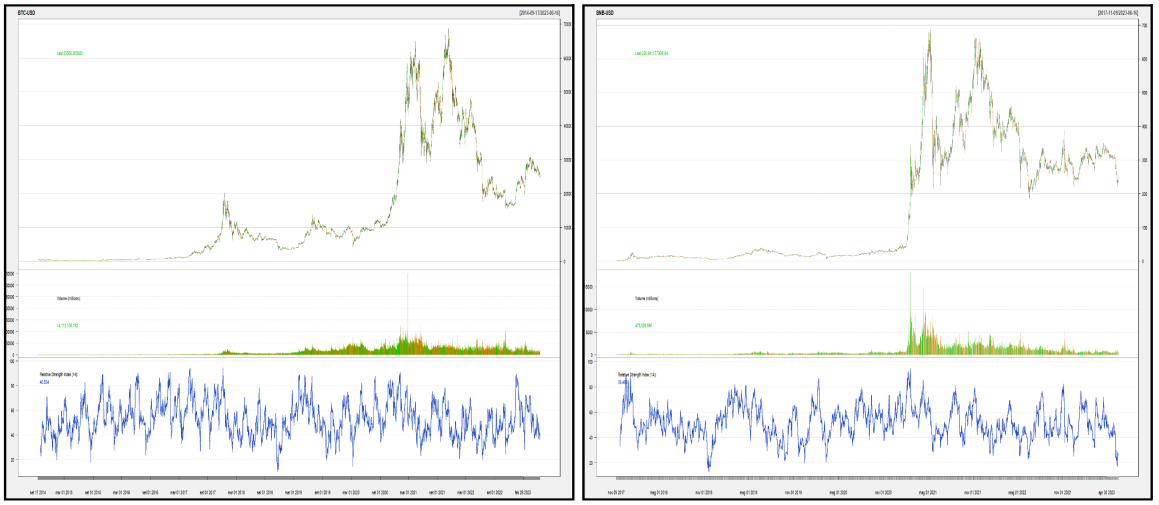
Le righe di codice fornite rappresentano l'implementazione dell'indicatore Relative Strength Index (RSI) e la definizione di due strategie di trading basate sull'RSI per gli asset BTC, ETH e BNB.
L'RSI è un indicatore di analisi tecnica utilizzato per valutare la forza e la direzione di un trend dei prezzi, viene calcolato confrontando i guadagni medi durante i periodi rialzisti con le perdite medie durante i periodi ribassisti. Il Relative Strength Index assume valori in un intervallo tra zero e cento: se l'indicatore va al di sopra dei 70 ci si trova in una zona di ipercomprato, mentre al di sotto dei 30 si è in una zona di ipervenduto.

La funzione fRSI è stata definita per calcolare l'RSI a partire dai dati dei prezzi e dal periodo di osservazione specificato. Questa funzione calcola le variazioni positive (U) e le variazioni negative (D) dei prezzi, quindi calcola l'RSI utilizzando la formula classica dell'RSI:

- $RSI = AvgUp/(AvgUp + AvgDown) * 100$

Vengono calcolati gli RSI per BTC, ETH e BNB utilizzando la funzione "fRSI" appena definita. I risultati vengono quindi visualizzati graficamente con l'aiuto della libreria "quantmod" in R.
Viene tracciato il grafico del prezzo delle criptovalute con sovrapposto l'indicatore RSI calcolato con finestra di osservazione di lunghezza 14 e tipologia di media esponenziale (grafici 29, 7, 30).

Grafici 29-30: 01/09/2014-31/12/2022 ‘BTC-USD’, 01/11/2017-31/5/2023 ‘BNB-USD’ charts, generati con RStudio.



Il grafico 29 rappresenta la serie di BTC, da settembre 2014 a dicembre 2022, mentre il grafico 30 mostra il movimento dei prezzi di BNB, da novembre 2017 a maggio 2023; ai quali è stato aggiunto l'indicatore RSI. Da una prima visualizzazione, è facilmente osservabile come i segnali prodotti devono essere monitorati molto attentamente, in quanto non forniscono un’indagine esaustiva. Infatti, in certe fasi di “ipercomprato”, durante i quali un mercato è rialzista, questi segnali possono dilungarsi per molto tempo, così come può avvenire nelle fasi di “ipervenduto”, durante un mercato ribassista.

Successivamente, viene definita la strategia di trading "LONG" utilizzando l'RSI. La funzione "fRSI_long" prende come input l'RSI calcolato e il vettore dei prezzi e restituisce una matrice che contiene i punti di ingresso, uscita e il guadagno percentuale per le operazioni "LONG" basate sull'RSI. La funzione fRSI_long esegue una strategia di trading identificando i punti in cui l'RSI scende al di sotto di una soglia di 40 e risale al di sopra di 90. Vengono effettuati i calcoli per BTC, ETH e BNB e i risultati vengono visualizzati in tabelle separate. Viene anche calcolata la somma dei guadagni e la media dei guadagni per ciascuna coppia di valute, nonché il profitto medio annuo.
In un secondo momento, viene definita la strategia di trading "SHORT" utilizzando l'RSI. La funzione "fRSI_short" prende come input l'RSI calcolato e il vettore dei prezzi e restituisce una matrice che contiene i punti di ingresso, uscita e il guadagno percentuale per le operazioni "SHORT" basate sull'RSI. La funzione fRSI_short esegue una strategia di trading identificando i punti in cui l'RSI sale al di sopra di una soglia di 80 e scende al di sotto di 20. Vengono effettuati i calcoli per BTC, ETH e BNB e i risultati vengono visualizzati in tabelle separate.

Tabella 4: Profitti strategia LONG con l’RSI.

Strategia LONG	BTC	ETH	BNB
Numero di trade	11	7	4
Somma profitti	91,82%	25,84%	53,91%
Media profitti	8,35%	3,69%	13,48%
Profitto medio annuo	13,12%	5,17%	10,78%

La strategia LONG, riassunta nella tabella 4, mostra dei risultati molto differenti rispetto ad entrambe le strategie con le bande di Bollinger. Infatti, il numero di trade va da 4 (BNB) a 11 (BTC), mentre i profitti medi vanno da 3,7% (ETH) a 13,5% (BNB); valori notevolmente minori rispetto a quelli prodotti dalle strategie precedenti.
Nonostante le performance inferiori, anche questa strategia presenta solo risultati positivi.

Tabella 5: Perdite strategia SHORT con l'RSI.

Strategia SHORT	BTC	ETH	BNB
Numero di trade	14	12	8
Somma profitti	-239,21%	-180,42%	-636,89%
Media profitti	-17,09%	-15,03%	-79,61%
Profitto medio annuo	-34,17%	-36,08%	-127,38%

Come è subito visibile dalla tabella 5, la strategia SHORT con l'RSI è l'unica a mostrare solo risultati negativi, qualunque siano i valori dell'RSI scelti come soglie (es.90-40, 80-30, 70-30, 70-20, ecc).
Il numero di operazioni è leggermente maggiore rispetto alla strategia LONG, con un massimo di 14 (BTC), ma rimane ben distante rispetto alle performance prodotte dalle strategie con le bande di Bollinger.
Le perdite medie sono relativamente basse per BTC e ETH, rispettivamente 17,1% e 15%, ma quella di BNB arriva a -79,6%.

In conclusione, questo paragrafo illustra l'applicazione dell'RSI come indicatore di trading per le criptovalute BTC, ETH e BNB. La strategia "LONG" mostra risultati di guadagno leggermente positivi, mentre la strategia "SHORT" non produce profitti, ma solo perdite.

Infine, viene applicato l'indicatore MACD (Moving Average Convergence Divergence) alle criptovalute Bitcoin (BTC), Ethereum (ETH) e Binance Coin (BNB). Come si è anticipato nella definizione dell'indicatore MACD, questo non permette di capire dove si troveranno i massimi e i minimi che il prezzo raggiungerà, ma è molto utile per comprendere la direzione che il trend prenderà.

La funzione "fMACD" definita consente di calcolare il MACD utilizzando tre parametri: m1, m2 e m3, che rappresentano rispettivamente il periodo di calcolo per la media mobile esponenziale (EMA) rapida, la EMA lenta e il periodo di calcolo per il segnale MACD.
Il MACD stesso viene calcolato sottraendo la EMA lenta dalla EMA rapida, mentre il segnale viene calcolato come EMA del MACD stesso. Il risultato viene restituito in una matrice che contiene i valori del MACD e del segnale.

Successivamente, viene calcolato il MACD per BTC, ETH e BNB utilizzando la funzione "fMACD". I risultati vengono visualizzati attraverso grafici che mostrano il prezzo delle criptovalute sovrapposto al MACD e al segnale (grafici 31,32,6).

Grafico 31: 01/01/2021-31/12/2021 ‘BTC-USD’ chart, generato con RStudio.

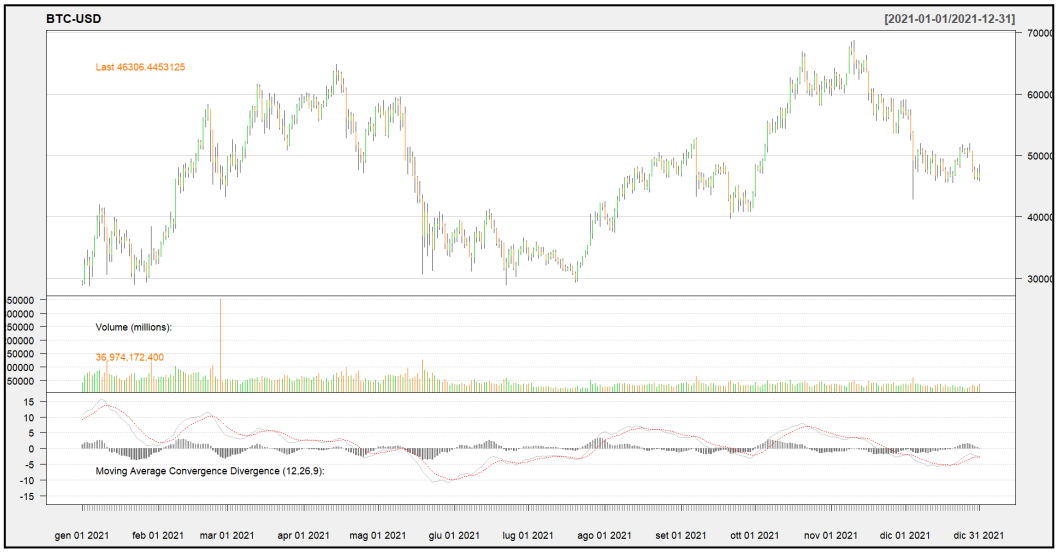
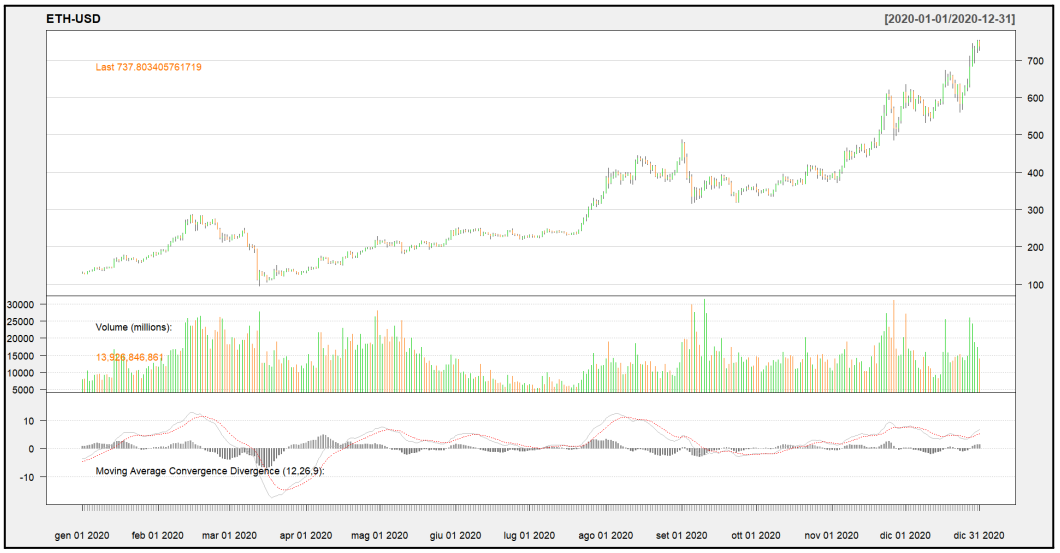


Grafico 32: 01/01/2020-31/12/2020 ‘ETH-USD’ chart, generato con RStudio.



I grafici 31 e 32 mostrano, rispettivamente, i prezzi di BTC durante il 2021 e ETH durante il 2020, ai quali viene aggiunto l’indicatore MACD. In questo caso si può evidenziare come gli incroci al rialzo e al ribasso delle linee MACD e EMA9 coincidano con movimenti rialzisti e ribassisti del prezzo delle criptovalute in esame.

Tuttavia, è importante notare che il MACD da solo non è un segnale di trading sufficientemente affidabile. Rispetto ad altri indicatori di analisi tecnica, come le bande di Bollinger e l'RSI, il MACD può essere meno preciso nella generazione di segnali di trading. Mentre le bande di Bollinger forniscono informazioni sulla volatilità dei prezzi e l'RSI identifica le situazioni di ipercomprato e ipervenduto, il MACD si concentra sull'intersezione tra le due linee del MACD e dell’EMA. Questo può portare a segnali meno chiari ed è validato dal fatto che, quando ci sono stati movimenti rialzisti o ribassisti del prezzo di Bitcoin, anche l’indicatore MACD è stato molto ampio nei suoi movimenti.

In conclusione, queste ultime righe di codice mostrano l'applicazione del MACD come indicatore di trading per le criptovalute BTC, ETH e BNB. Tuttavia, è importante considerare l'inadeguatezza del MACD come unico indicatore di trading e la sua minore precisione rispetto ad altri indicatori come le bande di Bollinger e l'RSI.

4.3 STRATEGIE DI HOLDING

Questa sezione descrive l'implementazione di una strategia di trading di "holding" utilizzando la funzione "fHODL", basata sull'acquisto di un asset e sulla sua detenzione a lungo termine, senza eseguire operazioni di acquisto o vendita in base a indicatori tecnici.

La funzione "fHODL" prende come input il prezzo della criptovaluta e calcola i profitti ottenuti attraverso la strategia di "holding". La matrice "HODL" viene inizializzata con valori nulli e, successivamente, viene popolata con i prezzi di apertura della posizione e i guadagni in percentuale, per ogni periodo di tempo. In questo caso specifico vengono utilizzate tutte le criptovalute analizzate nel corso dell'elaborato (BTC, ETH, BNB, CRO, ADA, DOT, SOL, VET, IOTA, MANA, SAND, AGIX e LINK), ad eccezione di GRT che è stata l'unica a presentare una correlazione negativa. La strategia di "holding" viene implementata con una frequenza di acquisto ogni 30, 90 e 180 giorni.
Successivamente, vengono calcolati gli indicatori di performance per la strategia di "holding" per ogni criptovaluta analizzata: numero di trade, somma dei profitti totali e media dei profitti per ogni trade.

Tabella 6: Profitti strategia HODL con PAC ogni 30 giorni.

Strategia HODL (PAC ogni mese)			
Criptovaluta	**Numero di trade**	**Somma dei profitti**	**Media dei profitti**
BTC	86	228.253,1%	2.654,1%
ETH	51	26.069,73%	511,17%
BNB	42	83.406,47%	1.985,87%
CRO	11	994,13%	90,38%
ADA	36	11.512,4%	319,79%
DOT	2	74,37%	37,18%
SOL	14	12.035,15%	859,65%
VET	26	4.317,86%	166,07%
MIOTA	68	-3.864,64%	-56,83%
MANA	41	26.023,6%	634,72%
SAND	9	4.824,31%	536,03%
AGIX	52	22.532,92%	433,33%
LINK	33	29.447,52%	892,35%

Tabella 7: Profitti strategia HODL con PAC ogni 90 giorni.

Strategia HODL (PAC ogni 3 mesi)			
Criptovaluta	**Numero di trade**	**Somma dei profitti**	**Media dei profitti**
BTC	21	19.166,73%	912,7%
ETH	17	8.625,75%	507,4%
BNB	15	32.348,29%	2.156,55%
CRO	4	298,15%	74,54%
ADA	11	3.945,35%	358,67%
DOT	1	60,02%	60,02%
SOL	5	4.396,9%	879,38%
VET	9	1.457,37%	161,93%
MIOTA	22	-1.321,11%	-60,05%
MANA	14	9.998,86%	714,2%
SAND	3	1.441,89%	480,63%
AGIX	18	8.099,39%	449,97%
LINK	11	10.242,57%	931,14%

Tabella 8: Profitti strategia HODL con PAC ogni 180 giorni.

Strategia HODL (PAC ogni 6 mesi)			
Criptovaluta	**Numero di trade**	**Somma dei profitti**	**Media dei profitti**
BTC	15	39.466%	2.631,07%
ETH	8	4.374,27%	546,78%
BNB	7	20.441,62%	2.920,23%
CRO	2	258,04%	129,02%
ADA	6	2.430,05%	405,01%
DOT	1	60,02%	60,02%
SOL	2	2016,91%	1008,46%
VET	4	633,92%	158,48%
MIOTA	12	-698,03%	-58,17%
MANA	7	5.900,99%	842,99%
SAND	2	655,74%	327,87%
AGIX	10	4.303,84%	430,38%
LINK	6	5.382,02%	897%

Le tabelle 6,7 e 8 mostrano i risultati dell'applicazione delle 3 strategie: tutte portano a profitti ad eccezione dell'applicazione con MIOTA, che mostra solo perdite. Diverse monete digitali mostrano profitti medi simili con tutti e 3 i PAC, le medie di questi, per le criptovalute in questione, sono le seguenti: 521,8% (ETH), 162,2% (VET), -58,3% (MIOTA), 437,9% (AGIX) e 906,8% (LINK). BNB risulta essere la criptovaluta più profittevole, infatti è la prima per profitti medi sia con il PAC ogni 6 mesi (2.920,2%) sia con quello ogni 3 (2.156,6%), invece è seconda con quello mensile (1.985,9%) dietro a BTC (2.654,1%). Quest'ultimo, essendo la prima moneta digitale, è anche quella che presenta il numero maggiore di trade (86 con il PAC mensile), con conseguente media delle somme dei profitti pari a 95.628,3%.

È importante notare che la strategia di "holding", generalmente, porta a profitti significativi rispetto alle strategie di trading basate su indicatori tecnici, come nel caso del calcolo dei rendimenti per le criptovalute scelte. I risultati mostrano somme e medie dei profitti significativamente superiori rispetto alle strategie di trading basate su indicatori tecnici. Questo evidenzia il fatto che, nella maggior parte dei casi, mantenere un asset a lungo termine senza eseguire numerose operazioni di acquisto o vendita risulta essere più redditizio rispetto alle strategie di trading attive basate su indicatori tecnici. Tuttavia, è importante considerare che i risultati possono variare a seconda delle condizioni di mercato e dell'asset specifico preso in considerazione.

5. CONSIDERAZIONI E CONCLUSIONI

Nel corso di questa tesi di laurea sono stati esplorati diversi aspetti del mercato delle criptovalute, comprese le strategie di previsione del prezzo, le caratteristiche della tecnologia blockchain e il potenziale offerto da svariate monete digitali come Bitcoin ed Ethereum. Inoltre, sono state sviluppate diverse strategie di trading basate sull'analisi tecnica e confrontate con alcune strategie di HOLDing.
L'obiettivo principale di questo elaborato è stato identificare le caratteristiche influenti nei movimenti di mercato e sviluppare strategie efficaci per ottenere rendimenti positivi.

Attraverso una ricerca accurata e l'analisi dei dati storici, è emerso che il mercato delle criptovalute presenta un enorme potenziale di investimento. Le monete digitali sono state in grado di generare profitti significativi nel corso degli anni, grazie a una crescita esponenziale dei prezzi e a una sempre maggiore accettazione a livello globale.
Nella fase di analisi della profittabilità, sono stati seguiti diversi passaggi. Innanzitutto, sono state selezionate le criptovalute da includere nell'analisi, sono state raccolte informazioni su di loro e sono stati calcolati grafici dei prezzi storici e statistiche di base. Successivamente, è stata condotta un'analisi delle correlazioni tra le criptovalute considerate utilizzando i dati storici dei loro prezzi. Sono state calcolate le matrici di correlazione e visualizzate graficamente con una heatmap.
Dall'analisi preliminare è emerso che le criptovalute considerate presentano movimenti di prezzo diversi, ma la maggior parte mostra tratti comuni. Sono state trovate forti correlazioni tra molte di esse, con Bitcoin, Ethereum e Binance Coin che svolgono un ruolo significativo come "market movers". Sono state identificate anche correlazioni elevate tra criptovalute appartenenti allo stesso settore.

In seguito, sono stati applicati diversi indicatori di analisi tecnica alle criptovalute selezionate, come le medie mobili, il Moving Average Convergence Divergence (MACD), le Bollinger Bands e il Relative Strength Index (RSI). Sono state sviluppate strategie di trading LONG e SHORT utilizzando le ultime due di queste tecniche, che hanno dimostrato di essere strumenti utili per prendere decisioni di investimento nel breve termine, al fine di sfruttare le tendenze al rialzo e al ribasso dei prezzi delle criptovalute.
Tuttavia, è importante notare che l'efficacia di tali strategie può variare in base alle condizioni di mercato e alla precisione degli indicatori utilizzati, essendo suscettibili a falsi segnali. Alcune di queste possono generare profitti consistenti, mentre altre possono risultare meno affidabili o, persino, portare a perdite.

Inoltre, sono state elaborate alcune strategie di HOLDing, che hanno dimostrato di offrire risultati considerevoli nel lungo termine. Mantenere le criptovalute per un periodo consistente, senza effettuare operazioni di trading attivo, ha consentito di beneficiare di maggiore stabilità e rendimenti positivi nel corso del tempo. Ciò è dovuto al fatto che le criptovalute tendono a mostrare un'alta volatilità e fluttuazioni significative nel breve termine, ma generalmente registrano apprezzamenti significativi nel lungo periodo. Pertanto, questo approccio si basa sulla fiducia nella crescita e nell'adozione a lungo termine delle criptovalute scelte, come dimostrato dalla storia di successo di Bitcoin.
Tuttavia, è importante sottolineare che il mercato delle criptovalute è altamente volatile e soggetto a rischi significativi, pertanto una gestione attenta e una continua valutazione delle strategie di trading sono essenziali per ottenere risultati positivi.
Per valutare e confrontare le performance prodotte dalle diverse strategie, sono state utilizzate le seguenti metriche finanziarie: il numero di trade, la somma dei rendimenti, la media dei rendimenti e il rendimento medio annuo. La media dei profitti è stata considerata come metrica più significativa, in quanto permette una migliore comparazione tra le diverse strategie di trading sviluppate.

In conclusione, l'analisi della profittabilità delle strategie di trading applicate al mercato delle criptovalute ha evidenziato l'importanza di considerare le caratteristiche influenti nel mercato e di adottare strategie efficaci. Questa tesi ha fornito una panoramica completa del mercato delle criptovalute e delle strategie di trading adottate in questo settore. Le strategie di analisi tecnica possono essere efficaci nel breve termine, ma richiedono un'analisi accurata delle condizioni di mercato e la scelta adeguata degli indicatori. D'altra parte, le strategie di HOLDing offrono una prospettiva di investimento a lungo termine e forniscono risultati più stabili e consistenti nel tempo.

APPENDICE: CODICE IN RSTUDIO

###ANALISI PRELIMINARI

```
# Pacchetti necessari
library("quantmod")
library(TTR)
library("tseries")
library("fBasics")
library(tidyverse)
library(tidymodels)
library(corrplot)

#Funzione “rem_zero”
rem_zero <- function(data){
  #data$price==0 #controllo prezenza zeri nei valori
  remove.zero1 <- (data[,1]>0)
  remove.zero2 <- (data[,2]>0)
  new_data <- data %>% slice( which(remove.zero1)) #rimozione dati con valori uguali a
zero
  new_data <- new_data %>% slice( which(remove.zero2))
  return(new_data)
}

## Raccolta dati e grafici generali
crypto <- c("BTC-USD","ETH-USD","BNB-USD","CRO-USD","ADA-USD",
"DOT-USD","SOL-USD","VET-USD","MIOTA-USD","MANA-USD",
"SAND-USD","GRT-USD","AGIX-USD","LINK-USD")
getSymbols(na.omit(crypto),src = "yahoo")
#BTC
chartSeries(`BTC-USD`)  #Elemento 'BTC-USD' contenente valori dei prezzi di apertura,
massimo, minimo, chiusura, volume e chiusura corretta
head(`BTC-USD`,n=3)
#ETH
chartSeries(`ETH-USD`)
#Exchange coins
chartSeries(`BNB-USD`)
chartSeries(`CRO-USD`)
#"Ethereum killer" coins
chartSeries(`ADA-USD`)
chartSeries(`DOT-USD`)
chartSeries(`SOL-USD`)
#IoT
chartSeries(`VET-USD`)
chartSeries(`MIOTA-USD`)
#Metaverse
chartSeries(`MANA-USD`)
chartSeries(`SAND-USD`)
#AI
```

```
chartSeries(`GRT-USD`)
chartSeries(`AGIX-USD`)
#Oracle
chartSeries(`LINK-USD`)

## Prezzi delle criptovalute
#BTC
p<-(`BTC-USD`)
price_BTC <-  p[,4] #vettore dei valori dei prezzi di chiusura di BTC
colnames (price_BTC) <- c('price_BTC')
View(price_BTC)
basicStats (price_BTC)
#Prezzi delle altcoins
p_E<-(`ETH-USD`)
p_B<-(`BNB-USD`)
p_A<-(`ADA-USD`)
p_C<-(`CRO-USD`)
p_D<-(`DOT-USD`)
p_O<-(`SOL-USD`)
p_V<-(`VET-USD`)
p_I<-(`MIOTA-USD`)
p_M<-(`MANA-USD`)
p_S<-(`SAND-USD`)
p_G<-(`GRT-USD`)
p_X<-(`AGIX-USD`)
p_L<-(`LINK-USD`)

## Esempi grafici
#BTC
chartSeries(`BTC-USD`,
        subset='2017-01::2023-01',
        theme=chartTheme('white'))
#Grafico a linee anno 2021
chartSeries(`BTC-USD`,
        type="line",
        subset='2021',
        theme=chartTheme('white'))
#Grafico a barre mese di gennaio anno 2020
chartSeries(`BTC-USD`,
        type="bar",
        subset='2020-01',
        theme=chartTheme('white'))
#Candlestick mese di novembre anno 2020
chartSeries(`BTC-USD`,
        type="candlesticks",
        subset='2020-11',
        up.col = 'green',
        down.col = 'red',
```

```
        theme=chartTheme('white'))
#ETH
chartSeries(`ETH-USD`,
        subset='2017-01::2023-01',
        theme=chartTheme('white'))
#Candlestick mese di novembre anno 2021
chartSeries(`ETH-USD`,
        type="candlesticks",
        subset='2021-11',
        up.col = 'green',
        down.col = 'red',
        theme=chartTheme('white'))
#BNB
chartSeries(`BNB-USD`,
        subset='2020-01::2023-01',
        theme=chartTheme('white'))
#Candlestick mese di gennaio anno 2021
chartSeries(`ETH-USD`,
        type="candlesticks",
        subset='2021-1',
        up.col = 'green',
        down.col = 'red',
        theme=chartTheme('white'))
#Grafico a linee anno 2021
chartSeries(`BNB-USD`,
        type="line",
        subset='2021',
        theme=chartTheme('white'))
```

##CORRELAZIONI

```
#Elenco dimensioni osservazioni
length(p)
length(p_E)
length(p_B)
length(p_C)
length(p_A)
length(p_D)
length(p_O)
length(p_I)
length(p_V)
length(p_M)
length(p_S)
length(p_G)
length(p_X)
length(p_L)
#Correlazioni tra osservazioni con la stessa dimensione
cor <- cor(cbind(p_E[,4], p_B[,4], p_A[,4], p_I[,4], p_M[,4], p_L[,4]))
cor
```

```
corrplot(cor, method = "square",  tl.srt = 50, tl.col = "black", tl.cex = 0.6, title = "Correlazione
tra criptovalute", mar=c(0,0,1,0))

## Correlazioni in un dato periodo
#Periodo di analisi
startDate= as.Date("2020-09-01")
endDate= as.Date("2022-04-01")
#Dati delle criptovalute
getSymbols(crypto, from = startDate, to = endDate)
btc<-(`BTC-USD`)
eth<-(`ETH-USD`)
bnb<-(`BNB-USD`)
cro<-(`CRO-USD`)
ada<-(`ADA-USD`)
dot<-(`DOT-USD`)
sol<-(`SOL-USD`)
vet<-(`VET-USD`)
iota<-(`MIOTA-USD`)
sand<-(`SAND-USD`)
mana<-(`MANA-USD`)
grt<-(`GRT-USD`)
agix<-(`AGIX-USD`)
link<-(`LINK-USD`)
#Analisi delle correlazioni
cor <- cor(cbind(btc[,4], eth[,4], bnb[,4], cro[,4], ada[,4], dot[,4], sol[,4], vet[,4], iota[,4],
sand[,4], mana[,4], grt[,4], agix[,4], link[,4]))
rownames(cor)<-(c('BTC','ETH','BNB','CRO','ADA','DOT','SOL','VET','MIOTA','SAND','MANA'
,'GRT','AGIX','LINK'))
colnames(cor)<-(c('BTC','ETH','BNB','CRO','ADA','DOT','SOL','VET','MIOTA','SAND','MANA','
GRT','AGIX','LINK'))
cor
corrplot(cor, method = "square",  tl.srt = 50, tl.col = "black", tl.cex = 0.6, title = "Correlazione
tra criptovalute", mar=c(0,0,1,0))
```

###STRATEGIE DI ANALISI TECNICA

```
#Raccolta di tutti i dati disponibili delle 3 criptovalute che verranno utilizzate: BTC, ETH,
BNB
getSymbols ("BTC-USD")
getSymbols ("ETH-USD")
getSymbols ("BNB-USD")

## Calcolo di alcuni indicatori tecnici di Bitcoin
#Calcolo della media mobile semplice (SMA)
sma <- na.omit(SMA(price_BTC, n = 20))
View(sma)
#Calcolo della media mobile esponenziale (EMA)
ema <- na.omit(EMA(price_BTC, n = 50))
View(ema)
```

```
#Calcolo delle Bollinger Bands per Bitcoin
bbands <- na.omit(BBands(price_BTC))
View(bbands)
#Calcolo del Relative Strength Index (RSI)
rsi <- na.omit(RSI(price_BTC, n = 14))
View(rsi)
#Calcolo del Moving Average Convergence Divergence (MACD)
macd <- na.omit(MACD(price_BTC))
View(macd)
```

##BTC CON LE MEDIE MOBILI

```
#BTC con medie mobili semplici
chartSeries(`BTC-USD`,
        subset='2020-01::2021-12',
        theme=chartTheme('white'))
addSMA(n=26,on=1,col = "blue")
addSMA(n=50,on=1,col = "green")
addSMA(n=200,on=1,col = "red")

#BTC con medie mobili pesate
chartSeries(`BTC-USD`,
        subset='2021-01::2021-12',
        theme=chartTheme('white'))
addWMA(n=10,on=1,col = "blue")
addWMA(n=20,on=1,col = "red")

#BTC con medie mobili esponenziali
chartSeries(`BTC-USD`,
        subset='2020-01::2021-12',
        theme=chartTheme('white'))
addEMA(n=26,on=1,col = "blue")
addEMA(n=50,on=1,col = "red")
addEMA(n=200,on=1,col = "green")
```

##CRIPTOVALUTE CON LE BOLLINGER BANDS

```
#Funzione per creare le bande di bollinger
fBBands <- function (price,n,sd){
  mavg <- SMA(price,n)
  sdev <- rep(0,n)
  N <- nrow(price)
  for (i in (n+1):N){
    sdev[i]<- sd(price[(i-n+1):i])
  }
  sdev <- sqrt((n-1)/n)*sdev
  up <- mavg + sd*sdev
  down <- mavg - sd*sdev
  bb <- cbind(down, mavg, up)
  colnames(bb) <- c("down", "mavg", "up")
```

```
  return(na.omit(bb))
}
#BTC
BTC_bands <-fBBands(Cl(p),n=30,sd=2)
head(BTC_bands,n=5)
tail(BTC_bands,n=5)
chartSeries(`BTC-USD`,
            subset='2020-01::2023-01',
            theme=chartTheme('white'))
addBBands(n=30,sd=2)
#ETH
ETH_bands <-fBBands(Cl(p_E),n=30,sd=2)
head(ETH_bands,n=5)
tail(ETH_bands,n=5)
chartSeries(`ETH-USD`,
            subset='2017-01::2023-01',
            theme=chartTheme('white'))
addBBands(n=30,sd=2)
#BNB
BNB_bands <-fBBands(Cl(p_B),n=30,sd=2)
head(BNB_bands,n=5)
tail(BNB_bands,n=5)
chartSeries(`BNB-USD`,
            subset='2020-01::2023-01',
            theme=chartTheme('white'))
addBBands(n=30,sd=2)

## STRATEGIA DI TRADING: LONG CON LE BOLLINGER BANDS
fBB_long <- function(bands,price){
  n <- basicStats(bands)[1,1]
  LONG_bb <- matrix(rep(0,1500),ncol=3)
  colnames(LONG_bb)<-c("Open Price Long","Exit Price Long","Gain in %")
  i<-2
  j<-1
  dn <- as.numeric(bands$down)
  dn <- as.matrix(dn,ncol=1)
  up <- as.numeric(bands$up)
  up <- as.matrix(up,ncol=1)
  for(i in 1:n){
    if(price[i,3] < dn[i]){
      LONG_bb[j,1] <- dn[i]
    }
    if(price[i,2] > up[i]){
      LONG_bb[j,2] <- up[i]
      LONG_bb[j,3] <- (LONG_bb[j,2]-LONG_bb[j,1])/LONG_bb[j,1]*100
      j<-j+1
    }
  }
```

```
  return(LONG_bb)
}
#BTC
data_bb_long <- data.frame(fBB_long(BTC_bands,p))
data_bb_long <-rem_zero(data_bb_long)
View(data_bb_long)
dim(data_bb_long)[1]
sum(data_bb_long$Gain.in..)
mean(data_bb_long$Gain.in..)
sum(data_bb_long$Gain.in..)/7
#ETH
data_bb_long<-data.frame(fBB_long(ETH_bands,p_E))
data_bb_long_ETH <-rem_zero(data_bb_long)
View(data_bb_long_ETH)
dim(data_bb_long_ETH)[1]
sum(data_bb_long_ETH$Gain.in..)
mean(data_bb_long_ETH$Gain.in..)
sum(data_bb_long_ETH$Gain.in..)/5
#BNB
data_bb_long<-data.frame(fBB_long(BNB_bands,p_B))
data_bb_long_BNB <-rem_zero(data_bb_long)
View(data_bb_long_BNB)
dim(data_bb_long_BNB)[1]
sum(data_bb_long_BNB$Gain.in..)
mean(data_bb_long_BNB$Gain.in..)
sum(data_bb_long_BNB$Gain.in..)/5

## STRATEGIA DI TRADING: SHORT CON LE BOLLINGER BANDS
fBB_short <- function(bands,price){
  n <- basicStats(bands)[1,1]
  SHORT_bb <- matrix(rep(0,1500),ncol=3)
  colnames(SHORT_bb)<-c("Open Price Short","Exit Price Short","Gain in %")
  i<-2
  j<-1
  dn <- as.numeric(bands$down)
  dn <- as.matrix(dn,ncol=1)
  up <- as.numeric(bands$up)
  up <- as.matrix(up,ncol=1)
  for(i in 1:n){
    if(price[i,2] > up[i]){
      SHORT_bb[j,1] <- up[i]
    }
    if(price[i,3] < dn[i]){
      SHORT_bb[j,2] <- dn[i]
      SHORT_bb[j,3] <- -(SHORT_bb[j,2]-SHORT_bb[j,1])/SHORT_bb[j,1]*100
      j<-j+1
    }
  }
```

```
  return(SHORT_bb)
}
#BTC
data_bb_short<-data.frame(fBB_short(BTC_bands,p))
data_bb_short <-rem_zero(data_bb_short)
View(data_bb_short)
dim(data_bb_short)[1]
sum(data_bb_short$Gain.in..)
mean(data_bb_short$Gain.in..)
sum(data_bb_short$Gain.in..)/7
#ETH
data_bb_short<-data.frame(fBB_short(ETH_bands,p_E))
data_bb_short_ETH <-rem_zero(data_bb_short)
View(data_bb_short_ETH)
dim(data_bb_short_ETH)[1]
sum(data_bb_short_ETH$Gain.in..)
mean(data_bb_short_ETH$Gain.in..)
sum(data_bb_short_ETH$Gain.in..)/5
#BNB
data_bb_short<-data.frame(fBB_short(BNB_bands,p_B))
data_bb_short_BNB <-rem_zero(data_bb_short)
View(data_bb_short_BNB)
dim(data_bb_short_BNB)[1]
sum(data_bb_short_BNB$Gain.in..)
mean(data_bb_short_BNB$Gain.in..)
sum(data_bb_short_BNB$Gain.in..)/5
```

##CRIPTOVALUTE CON L'RSI

```
#Funzione per creare l'RSI
fRSI <- function (price,n){
  N <- length(price)
  U <- rep(0,N)
  D <- rep(0,N)
  index <- rep(NA,N)
  Lprice <- Lag(price,1)
  for (i in 2:N){
    if (price[i] >= Lprice[i]){
      U[i] <- price[i] - Lprice[i]
    } else{
      D[i] <- Lprice[i]- price[i]
    }
    if (i>n){
      AvgUp <- mean(U[(i-n+1):i])
      AvgDown <- mean(D[(i-n+1):i])
      index[i] <- AvgUp/(AvgUp+AvgDown)*100
    }
  }
  rsi <- reclass(index, price)
```

```
  return(na.omit(rsi))
}
#BTC
BTC_rsi <- fRSI(Cl(p), n=14)
tail(BTC_rsi,n=5)
chartSeries(`BTC-USD`,
          theme=chartTheme('white'))
addRSI(n=14,maType="EMA")
#ETH
ETH_rsi <- fRSI(Cl(p_E), n=14)
tail(ETH_rsi,n=5)
chartSeries(`ETH-USD`,
          theme=chartTheme('white'))
addRSI(n=14,maType="EMA")
#BNB
BNB_rsi <- fRSI(Cl(p_B), n=14)
tail(BNB_rsi,n=5)
chartSeries(`BNB-USD`,
          theme=chartTheme('white'))
addRSI(n=14,maType="EMA")

## STRATEGIA DI TRADING: LONG CON L'RSI
fRSI_long <- function(rsi,price){
  n <- basicStats(rsi)[1,1]
  LONG_rsi <- matrix(rep(0,2400),ncol=3)
  colnames(LONG_rsi)<-c("Open Price Long","Exit Price Long","Gain in %")
  j<-1
  index <- as.numeric(rsi[,1])
  index <- as.matrix(index,ncol=1)
  for(i in 1:n){
    if(index[i] < '40'){
      LONG_rsi[j,1] <- (price[i,3]+price[i,2])/2
    }
    if(index[i] > '90'){
      LONG_rsi[j,2] <- (price[i,3]+price[i,2])/2
      LONG_rsi[j,3] <- (LONG_rsi[j,2]-LONG_rsi[j,1])/LONG_rsi[j,1]*100
      j<-j+1
    }
  }
  return(LONG_rsi)
}
#BTC
data_rsi_long<-data.frame(fRSI_long(BTC_rsi,p))
data_rsi_long <-rem_zero(data_rsi_long)
View(data_rsi_long)
dim(data_rsi_long)[1]
sum(data_rsi_long$Gain.in..)
mean(data_rsi_long$Gain.in..)
```

```
sum(data_rsi_long$Gain.in..)/7
#ETH
data_rsi_long<-data.frame(fRSI_long(ETH_rsi,p_E))
data_rsi_long_ETH <-rem_zero(data_rsi_long)
View(data_rsi_long_ETH)
dim(data_rsi_long_ETH)[1]
sum(data_rsi_long_ETH$Gain.in..)
mean(data_rsi_long_ETH$Gain.in..)
sum(data_rsi_long_ETH$Gain.in..)/5
#BNB
data_rsi_long<-data.frame(fRSI_long(BNB_rsi,p_B))
data_rsi_long_BNB <-rem_zero(data_rsi_long)
View(data_rsi_long_BNB)
dim(data_rsi_long_BNB)[1]
sum(data_rsi_long_BNB$Gain.in..)
mean(data_rsi_long_BNB$Gain.in..)
sum(data_rsi_long_BNB$Gain.in..)/5

## STRATEGIA DI TRADING: SHORT CON L'RSI
fRSI_short <- function(rsi, price) {
  n <- basicStats(rsi)[1, 1]
  SHORT_rsi <- matrix(rep(0, 2400), ncol = 3)
  colnames(SHORT_rsi) <- c("Open Price Short", "Exit Price Short", "Gain in %")
  j <- 1
  index <- as.numeric(rsi[, 1])
  index <- as.matrix(index, ncol = 1)
  for (i in 1:n) {
    if (index[i] > '80') {
      SHORT_rsi[j, 1] <- (price[i, 3] + price[i, 2]) / 2
    }
    if (index[i] < '20' && SHORT_rsi[j, 1] != 0) {
      SHORT_rsi[j, 2] <- (price[i, 3] + price[i, 2]) / 2
      SHORT_rsi[j, 3] <- -((SHORT_rsi[j, 2] - SHORT_rsi[j, 1]) / SHORT_rsi[j, 1]) * 100
      j <- j + 1
    }
  }
  SHORT_rsi <- SHORT_rsi[1:j - 1, ]
  return(SHORT_rsi)
}
#BTC
data_rsi_short<-data.frame(fRSI_short(BTC_rsi,p))
data_rsi_short <-rem_zero(data_rsi_short)
View(data_rsi_short)
dim(data_rsi_short)[1]
sum(data_rsi_short$Gain.in..)
mean(data_rsi_short$Gain.in..)
sum(data_rsi_short$Gain.in..)/7
#ETH
```

```
data_rsi_short<-data.frame(fRSI_short(ETH_rsi,p_E))
data_rsi_short_ETH <-rem_zero(data_rsi_short)
View(data_rsi_short_ETH)
dim(data_rsi_short_ETH)[1]
sum(data_rsi_short_ETH$Gain.in..)
mean(data_rsi_short_ETH$Gain.in..)
sum(data_rsi_short_ETH$Gain.in..)/5
#BNB
data_rsi_short<-data.frame(fRSI_short(BNB_rsi,p_B))
data_rsi_short_BNB <-rem_zero(data_rsi_short)
View(data_rsi_short_BNB)
dim(data_rsi_short_BNB)[1]
sum(data_rsi_short_BNB$Gain.in..)
mean(data_rsi_short_BNB$Gain.in..)
sum(data_rsi_short_BNB$Gain.in..)/5
```

##CRIPTOVALUTE CON IL MACD

```
#Funzione per creare il MACD
fMACD <- function(price, m1, m2, m3){
  MACD <- EMA(price, m1) - EMA(price, m2)
  signal <- EMA(MACD, m3)
  output <- cbind(MACD, signal)
  colnames(output) <- c("MACD", "signal")
  return(na.omit(output))
}
#BTC
BTC_macd <- fMACD(Cl(p), 12, 26, 9)
View(BTC_macd)
chartSeries(`BTC-USD`, subset = '2021-01::2021-12', theme = chartTheme('white'))
addMACD(fast = 12, slow = 26, signal = 9, type = "EMA")
#ETH
ETH_macd <- fMACD(Cl(p), 12, 26, 9)
View(ETH_macd)
chartSeries(`ETH-USD`, subset = '2020-01::2020-12', theme = chartTheme('white'))
addMACD(fast = 12, slow = 26, signal = 9, type = "EMA")
#BNB
BNB_macd <- fMACD(Cl(p), 12, 26, 9)
View(BNB_macd)
chartSeries(`BNB-USD`, subset = '2021-01::2021-12', theme = chartTheme('white'))
addMACD(fast = 12, slow = 26, signal = 9, type = "EMA")
```

###STRATEGIE DI HOLDING

```
#Strategia di HOLDing con PAC
fHODL <- function(price){
  n <- basicStats(price)[1,1]
  HODL <- matrix(rep(0,500),ncol=2)
  colnames(HODL)<-c("Open Price HODL","Gain in %")
  j<-1
```

```
  for(i in seq(from = 1, to = n, by = 90)){    #by=30 (per il PAC ogni mese);
                                               #by=180 (per il PAC ogni 6 mesi);
    HODL[j,1] <- (price[i,2]+price[i,3])/2
    HODL[j,2] <- ((price[n,2]+price[n,3])/2-HODL[j,1])/HODL[j,1]*100
    j<-j+1
  }
  return(HODL)
}
#BTC
data_hodl<-data.frame(fHODL(p))
data_hodl_BTC <-rem_zero(data_hodl)
View(data_hodl_BTC)
dim(data_hodl_BTC)[1]
sum(data_hodl_BTC$Gain.in..)
mean(data_hodl_BTC$Gain.in..)
#ETH
data_hodl<-data.frame(fHODL(p_E))
data_hodl_ETH <-rem_zero(data_hodl)
View(data_hodl_ETH)
dim(data_hodl_ETH)[1]
sum(data_hodl_ETH$Gain.in..)
mean(data_hodl_ETH$Gain.in..)
#BNB
data_hodl<-data.frame(fHODL(p_B))
data_hodl_BNB <-rem_zero(data_hodl)
View(data_hodl_BNB)
dim(data_hodl_BNB)[1]
sum(data_hodl_BNB$Gain.in..)
mean(data_hodl_BNB$Gain.in..)
#CRO
data_hodl<-data.frame(fHODL(p_C))
data_hodl_CRO <-rem_zero(data_hodl)
View(data_hodl_CRO)
dim(data_hodl_CRO)[1]
sum(data_hodl_CRO$Gain.in..)
mean(data_hodl_CRO$Gain.in..)
#ADA
data_hodl<-data.frame(fHODL(p_A))
data_hodl_ADA <-rem_zero(data_hodl)
View(data_hodl_ADA)
dim(data_hodl_ADA)[1]
sum(data_hodl_ADA$Gain.in..)
mean(data_hodl_ADA$Gain.in..)
#DOT
data_hodl<-data.frame(fHODL(p_D))
data_hodl_DOT <-rem_zero(data_hodl)
View(data_hodl_DOT)
dim(data_hodl_DOT)[1]
```

```
sum(data_hodl_DOT$Gain.in..)
mean(data_hodl_DOT$Gain.in..)
#SOL
data_hodl<-data.frame(fHODL(p_O))
data_hodl_SOL <-rem_zero(data_hodl)
View(data_hodl_SOL)
dim(data_hodl_SOL)[1]
sum(data_hodl_SOL$Gain.in..)
mean(data_hodl_SOL$Gain.in..)
#VET
data_hodl<-data.frame(fHODL(p_V))
data_hodl_VET <-rem_zero(data_hodl)
View(data_hodl_VET)
dim(data_hodl_VET)[1]
sum(data_hodl_VET$Gain.in..)
mean(data_hodl_VET$Gain.in..)
#IOTA
data_hodl<-data.frame(fHODL(p_I))
data_hodl_IOTA <-rem_zero(data_hodl)
View(data_hodl_IOTA)
dim(data_hodl_IOTA)[1]
sum(data_hodl_IOTA$Gain.in..)
mean(data_hodl_IOTA$Gain.in..)
#MANA
data_hodl<-data.frame(fHODL(p_M))
data_hodl_MANA <-rem_zero(data_hodl)
View(data_hodl_MANA)
dim(data_hodl_MANA)[1]
sum(data_hodl_MANA$Gain.in..)
mean(data_hodl_MANA$Gain.in..)
#SAND
data_hodl<-data.frame(fHODL(p_S))
data_hodl_SAND <-rem_zero(data_hodl)
View(data_hodl_SAND)
dim(data_hodl_SAND)[1]
sum(data_hodl_SAND$Gain.in..)
mean(data_hodl_SAND$Gain.in..)
#AGIX
data_hodl<-data.frame(fHODL(p_X))
data_hodl_AGIX <-rem_zero(data_hodl)
View(data_hodl_AGIX)
dim(data_hodl_AGIX)[1]
sum(data_hodl_AGIX$Gain.in..)
mean(data_hodl_AGIX$Gain.in..)
#LINK
data_hodl<-data.frame(fHODL(p_L))
data_hodl_LINK <-rem_zero(data_hodl)
View(data_hodl_LINK)
```

dim(data_hodl_LINK)[1]
sum(data_hodl_LINK$Gain.in..)
mean(data_hodl_LINK$Gain.in..)

Bibliografia

1. Antonopoulos A. M. (2017). Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media.

2. Binance (2017). Binance Coin Whitepaper.
   Disponibile all'indirizzo:
   https://www.exodus.com/assets/docs/binance-coin-whitepaper.pdf

3. Butterin V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform.
   Disponibile all'indirizzo: https://ethereum.org/it/whitepaper/

4. Chiu J. e Koeppl T. (2017). The Economics of Cryptocurrencies-Bitcoin and Beyond. Journal of Economic Perspectives.
   Disponibile all'indirizzo: https://www.bis.org/events/eopix_1810/chiu_paper.pdf

5. Comandini G. L. (2020). Da zero alla luna. Dario Floccovio Editore.

6. Contaldo A. e Campara (2019). Blockchain, criptovalute, smart contract, industria 4.0. Registri digitali, accordi giuridici e nuove tecnologie. Pisa: Pacini Giuridica.

7. Crypto.com (2018). Crypto.com Chain Whitepaper.
   Disponibile all'indirizzo: https://whitepaper.cronos.org/

8. Elder A. (2014). Trading for a Living: Psychology, Trading Tactics, Money Management. Wiley.

9. Ellis S. , Juels A. e and Nazarov S. (2017). ChainLink. A Decentralized Oracle Network.
   Disponibile all'indirizzo: https://research.chain.link/whitepaper-v1.pdf

10. Grigoletto M. , Pauli F. e Ventura L. (2017). Modello lineare. Teoria e applicazioni con R.

11. Input Output Hong Kong "IOHK" (2017). Why we are building Cardano.
    Disponibile all'indirizzo: https://whitepaper.io/document/581/cardano-whitepaper

12. Lisi F. e Di Fonzo T. (2005). Serie storiche economiche. Analisi statistiche e applicazioni.

13. Lo A. W. (2018). Adaptive Markets: Financial Evolution at the Speed of Thought. Princeton University Press.

14. Nakamoto S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Disponibile all'indirizzo: https://bitcoin.org/bitcoin.pdf

15. Popov S. (2018). The Tangle. Version 1.4.2. Disponibile all'indirizzo: https://whitepaper.io/document/3/iota-whitepaper

16. Ordano E. , Meilich A. , Jardi Y. e Araoz M. (2017). Decentraland: A blockchain-based virtual world. Disponibile all'indirizzo: https://decentraland.org/whitepaper.pdf

17. SingularityNET Foundation (2019). SingularityNET. A Decentralized, Open Market and Network for AIs. Version 2.0. Disponibile all'indirizzo: https://public.singularitynet.io/whitepaper.pdf

18. Tal Y. , Ramirez B. e Pohlmann J. (2018). The Graph: A Decentralized Query Protocol for Blockchains. Disponibile all'indirizzo: https://raw.githubusercontent.com/graphprotocol/research/master/papers/whitepaper/the-graph-whitepaper.pdf

19. Tapscott D. e Tapscott A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.

20. The Sandbox Team (2020). The Sandbox. Play. Create. Own. Govern. Earn. Disponibile all'indirizzo: https://installers.sandbox.game/The_Sandbox_Whitepaper_2020.pdf

21. VeChain Foundation (2023). Web3 for Better. Whitepaper 3.0. Disponibile all'indirizzo: https://www.vechain.org/assets/whitepaper/whitepaper-3-0.pdf

22. Vigna P. e Casey M. J. (2016). The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order. St. Martin's Press.

23. Wood G. (2016). Polkadot: Vision for a Heterogeneous Multi-chain Framework. Disponibile all'indirizzo: https://assets.polkadot.network/Polkadot-whitepaper.pdf

24. Yakovenko A. (2020). Solana: A new architecture for a high performance blockchain v0.8.13. Disponibile all'indirizzo: https://solana.com/solana-whitepaper.pdf

Sitografia

1. https://cryptorivista.com/insight/tech/
2. https://www.investopedia.com
3. https://www.pandslegal.it/tecnologie-ict/smart-contracts/
4. https://cryptonomist.ch

5. https://www.consob.it/web/investor-education/criptovalute
6. https://bitcoin.org/it/
7. https://ethereum.org/en/
8. https://www.internet4things.it
9. https://www.tradingonline.it/investire
10. https://www.sciencedirect.com
11. https://it.cointelegraph.com
12. https://www.coindesk.com/
13. https://onlinelibrary.wiley.com/journal/15406261
14. https://bitcoinmagazine.com/
15. https://lightning.network/#intro
16. https://colintalkscrypto.com/cbbi/
17. https://charts.bitbo.io/stock-to-flow/
18. https://coinmarketcap.com/it/
19. https://it.tradingview.com/chart/
20. https://coinmap.org/