LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Impresa e Management

Cattedra di Financial Market Analysis

Semantica del valore, modelli fattoriali e teoria del portafoglio nel mercato delle criptovalute

Relatore
Prof. Nicola Borri

Candidato
Federico Magnani
Matricola 231851

Anno Accademico 2020/2021

41206d6961206d61647265
2c20706572206176657 26d692069
6e7365676e61746f20696c206c696
e6775616767696f2064656c6c9261
6d6f726520652061206d696f20706
16472652c2070657220617665726
d6920646f6e61746f206c92617274
652064692063726564572652069
6e2073e920737465737369

INDICE

INDICE DELLE FIGURE

INDICE DELLE TABELLE

Introduzione

L'essere umano ha da sempre avvertito la necessità di organizzare la propria storia nello stesso modo con cui si prostra all'avvenire: dando risposta a domande e a stati di necessità. Cercando di immunizzare l'aspetto utilitaristico che inevitabilmente trapela da una simile dichiarazione, si coglie in tutta la sua amoralità quell'implicita "legge di mercato" che configura la *forma mentis* di qualsiasi individuo, indipendentemente dalla radici storiche e culturali di appartenenza. È in questo continuo ed ambivalente processo di ascolto e di risposta delle proprie esigenze che l'uomo ha saputo esprimere al meglio il proprio ingegno, applicandolo trasversalmente ad ogni ambito della propria esistenza, muovendosi in un equilibrio dinamico di invenzioni e scoperte che gli hanno permesso di collezionare guadagni di utilità anno dopo anno, generazione dopo generazione, secolo dopo secolo, anelando ad un indefinito stato di ottimalità paretiana, di "non ulteriore migliorabilità" del proprio essere: in altre parole all'estinzione dei propri bisogni, alla fine del proprio percorso evolutivo. Ecco, quindi, la ruota come risposta al bisogno del trasporto, la legge come risposta al bisogno del quieto vivere in collettività, la filosofia come risposta al proprio bisogno esistenziale, l'economia come risposta alla necessità di massimizzare l'utilità ricavabile da risorse limitate e deperibili. In quest'ottica, evoluzioni apparentemente distinte come quella tecnologica, dei sistemi giuridici e del pensiero filosofico ed economico si pongono in stati di reciproco condizionamento, assumendo i connotati di un'unica grande evoluzione scritta nel patrimonio genetico dell'essere umano.

Ed ecco quindi che l'uomo, abituato ad interfacciarsi con l'incertezza del futuro e alla mutabilità delle proprie esigenze, dando vita a nuove scoperte e poi ad innovazioni, è altrettanto abituato ad organizzare il proprio passato proprio alla luce di quelle stesse scoperte che, dal suo punto di vista, rappresentano i nodi cruciali del proprio "miglioramento" nel tempo. Per questo motivo, anche e soprattutto sotto un punto di vista didattico, le macrofasi storiche che caratterizzano la storia umana sono ricordate per le grandi scoperte che si sono susseguite, interpretando alla luce di esse i grandi cambiamenti che ne sono derivati. In un'ottica hegeliana c'è chi direbbe che l'evoluzione non sia un fenomeno lineare, consapevole del fatto che ogni sua fase sia intervallata da un cambiamento più o meno rilevante, ed ammettere che ciò avvenga con linearità vorrebbe dire commettere l'ingenuità intellettuale di non considerare l'inevitabile aspetto dirompente che caratterizza la natura intrinseca del cambiamento. Se si dovesse disegnare l'evoluzione, di certo la sua forma non sarebbe quella di una retta, piuttosto quella di una "spirale" orizzontale che pur mantenendo una direzione ed un verso risulterebbe incerta nella sua "intensità" e ciò impedirebbe di considerarla propriamente come una grandezza vettoriale. Il percorso evolutivo è una "sequenza ciclica" per il suo carattere dialettico e triadico: alternandosi tra fasi di tesi antitesi e sintesi, esso distrugge vecchi equilibri per crearne di nuovi, i quali sono destinati ad essere messi in discussione in un intervallo temporale indefinito ma marginalmente decrescente, inscenando così un teatro storico di vincitori e vinti del progresso che da sempre ha animato la sensibilità dei migliori

scrittori del passato, raccontando questo fenomeno ora come la "provvidenza dell'ingegno" ora come "l'ansia del miglioramento".

Come afferma Taylor[1] nella sua deposizione davanti alla commissione speciale della Camera dei Rappresentanti per spiegare i principi dell'Organizzazione Scientifica del Lavoro e per interpretare la diffidenza dei lavoratori a innovazioni che incrementassero la loro produttività, il cambiamento, pur presentandosi con innocua spontaneità, si verifica con una forza tale da rendersi inarrestabile rispetto a qualsiasi tentativo proattivo di opposizione, sia che si tratti di discredito mediatico o di rivoluzione violenta animata dagli esponenti di quel vecchio equilibrio, del "così è sempre stato", che sa di essere pericolosamente minacciato dal cambiamento.
Ora, che sia Karl Marx nella sua opera "Il Capitale" del 1867 a muovere l'invettiva contro la meccanizzazione del processo produttivo o che sia Jamie Dimon, amministratore delegato di JP Morgan, nel Gennaio 2018 a condannare Bitcoin e le altre criptovalute come l'enorme frode della modernità[2], il discorso non cambia: l'attacco incondizionato alle novità è indizio stesso del cambiamento in atto e dell'inevitabile polarizzazione tra vincitori e vinti che ne conseguirà: la vera sfida è a carico dei detrattori che, per sopravvivere, dovranno successivamente abbracciare il loro "nemico", cercando allo stesso tempo di salvarsi la faccia.
Dal 2010 ad oggi (2021) Bitcoin è stato dichiarato "morto" ben 404 volte[3] in una tendenza che ha trovato il suo picco nel 2017, in concomitanza con la prima fase "esplosiva" del suo prezzo, per poi decrescere fino a quasi azzerarsi nel periodo recente, nonostante il valore di mercato di questo asset sia il 193,63% superiore rispetto al picco registrato a dicembre 2017. Che sia stato dettato dalla consapevolezza di un'autentica minaccia o dal semplice disinteressamento di chi ha ritenuto divertente un confronto con i "tulipani del XXI secolo", il feroce attacco mediatico alle criptovalute è apparso sistematico ed incondizionato eppure, nonostante ciò, oggi Bitcoin è ai suoi massimi storici nel valore di mercato: si direbbe che il cambiamento, oggi vestito da criptovaluta, risponda al principio di azione e reazione.

Si è giunti ormai ad un mondo ormai globalizzato e orientato alla "digitalizzazione" dei rapporti interpersonali come espediente per il superamento di barriere geografiche, linguistiche e culturali. Questo cambiamento da un lato impone la ricerca di un rimedio in merito al "costo" fiduciario che inevitabilmente si sostiene nel momento in cui si insorge un'obbligazione con un contraente sconosciuto, specie se la prestazione è di natura

[1] *Udienze della Commissione speciale della Camera dei Deputati costituita per esaminare il Sistema d'organizzazione industriale del Taylor ed altri sistemi, in seguito della risoluzione 90 della Camera*. (Vol. III, pagg. 1377-1508);

[2] https://99bitcoins.com/jpmorgan-ceo-jamie-dimon-says-bitcoin-is-a-fraud/

[3] https://99bitcoins.com/bitcoin-obituaries/

immateriale, dall'altro offre l'incredibile opportunità di sviluppare progetti su scala globale, attraverso il contributo di persone provenienti da ogni parte del pianeta, secondo un approccio sempre più orientato alla condivisione delle informazioni e all'innovazione aperta.

È a partire da questi elementi che, indipendentemente dal rumore mediatico di fondo, si coglie la portata rivoluzionaria della tecnologia blockchain in tutte le sue declinazioni: l'utilizzo della crittografia asimmetrica come strumento idoneo a neutralizzare il "peso della fiducia" nei rapporti giuridici, sancendone al tempo stesso l'incontestabilità grazie alla loro registrazione presso un registro pubblico condiviso, sta costruendo un ecosistema fertile per la crescita di progetti che assumono portata globale sia per le risorse da cui attingono sia per i portatori di interesse a cui si riferiscono.

Allo stesso tempo ci si trova di fronte al primo caso di profonda ibridazione tra una tecnologia emergente, potenzialmente rivoluzionaria, ed i mercati finanziari. La possibilità di beneficiare economicamente di un'innovazione ha sempre previsto la necessità di investire denaro in società private ad essa collegate. Alla fine del XX secolo, chi desiderava investire in "Internet" aveva bisogno di acquistare le *securities* emesse da società come Microsoft o Apple, beneficiando soltanto attraverso loro del cambiamento in atto. Le criptovalute rappresentano invece un esempio di "tokenizzazione" dell'innovazione, permettendo ai risparmiatori di investire direttamente nella tecnologia stessa e massimizzando il beneficio derivante dalla sua crescita ed adozione. In questi termini, le criptovalute rappresentano un'opportunità di investimento totalmente inedita che necessita di un approfondimento per valutare l'applicabilità o meno degli approcci tradizionali utilizzati nell'analisi dei mercati finanziari.

È quindi necessario studiare le componenti strutturali delle blockchains prese in esame al fine di ricomporre la cornice valoriale delle relative criptovalute: in questo modo si è in grado di inferirne il paradigma del valore ed accorgersi di come esso possa avere natura "reale" pur riferendosi ad asset tipicamente immateriali. Quindi, una volta inquadrato concettualmente l'argomento, si potrà procedere all'applicazione di modelli fattoriali riferiti all'asset-pricing, elaborandone eventualmente di nuovi, per capire quali siano le determinati o gli elementi di condizionamento dei rendimenti delle criptovalute, in modo tale da intuire come avvenga la determinazione del loro valore di mercato. Infine, attraverso la costruzione di portafogli che permettano di osservare gli effetti della diversificazione, si potrà valutare se le criptovalute rappresentino o meno un'appetibile opportunità di investimento per soggetti tipicamente avversi al rischio, seguendo gli schemi tipici della *Modern Portfolio Theory* inaugurata da Harry Markowitz.

CAPITOLO 1

LE CRIPTOVALUTE: UNO SGUARDO D'INSIEME

1.1 La rilevanza dell'onere fiduciario

Da sempre l'uomo per vivere al meglio intrattiene rapporti quotidiani, economici e non, con altri individui per procacciarsi le risorse di cui ha bisogno (siano esse beni, informazioni, moneta etc.) alienando le proprie il più delle volte, seguendo coerentemente la modellizzazione fornita dalla teoria dell'utilità in merito al saggio marginale di sostituzione.

In maniera quasi inconsapevole, il perpetrarsi di transazioni quotidiane guidate solo da principi amoralmente egoistici, vincolati solo dalla coerenza degli individui con i propri gusti (le funzioni di utilità per l'appunto) e con le proprie risorse, è indirizzato al raggiungimento di un equilibrio efficiente nell'accezione di "ottimale allocazione delle risorse". Con questo ci si riferisce ad una situazione in cui le risorse hanno modo di esprimere il massimo potenziale dell'utilità che possono generare, proprio in ragione del fatto che la transazione con cui avviene il loro scambio si conclude solo nel caso in cui entrambe le parti ne beneficiano, e per beneficiarne è necessario che la perdita di utilità dovuta all'alienazione di una propria risorsa sia compensata in maniera più che proporzionale dall'incremento di utilità dovuto all'acquisizione di una nuova.

Ora, in una situazione-limite di meccanismi economici perfetti, il problema di massimizzazione vincolata dell'utilità degli individui verrebbe risolto efficacemente attraverso la quotidiana interazione economico-sociale: in questo modello se si vertesse in uno stato di necessità e si avesse qualcosa desiderato da altri individui da dare in cambio, la transazione per procacciarsi le risorse idonee a placare i propri bisogni avverrebbe con efficacia e velocità, senza che la transazione stessa sia responsabile di perdite di utilità nel trasferimento delle risorse. In altre parole, in un mondo ideale il passaggio di risorse tra i contraenti avverrebbe senza "barriere" dettate dalla difficoltà di trovare una controparte, dai costi "monetari" dovuti allo scambio, dalla lentezza del trasferimento di risorse, piuttosto che dalla diffidenza rispetto all'autenticità dei prodotti ottenuti o all'affidabilità della controparte. Nel concreto però, tutte queste barriere sono soltanto alcuni esempi di costi di transazione che gravano nei rapporti economici degli individui, vincolandoli ad uno stato di subottimalità rispetto a quello che si otterrebbe in loro assenza. Questa situazione evidenzia spesso l'insufficienza della modellizzazione economica, a causa della debolezza delle assunzioni che ne sanciscono la validità, nel cercare di raggiungere l'ottimalità paretiana anche nelle dinamiche reali.

Questo accade perché l'individuo concreto non gode della perfetta informazione di cui gode l'individuo teorico: l'individuo concreto è costretto in uno stato di razionalità limitata che gli impedisce di conoscere con esattezza ogni aspetto rilevante della transazione che si appresta a concludere o delle possibili transazioni alternative che potrebbe concludere. Pertanto, ogni individuo decide valutando in maniera più o meno corretta il bagaglio informativo di cui dispone e spesso l'acquisizione di ulteriori informazioni è soggetta a costi che appesantiscono il beneficio ricavato dalla transazione, arrivando talvolta persino a comprometterlo: il risultato

è uno scambio di risorse che nel migliore dei casi si conclude in maniera imperfetta e congenitamente viziata a causa della mancata opportunità di considerare transazioni alternative, rimaste inconoscibili, che sarebbero state potenzialmente più convenienti. In questo dilemma kierkegaardiano dello scambio, i costi di transazione giocano un ruolo fondamentale poiché, laddove non esistessero, la situazione sarebbe sicuramente più vicina all'ottimo teorico.

Tra tutti i costi di transazione ne esistono alcuni dettati dall'aspetto tecnico del trasferimento da imputare tanto alla natura dei beni scambiati quanto alla tecnologia dello scambio (ragion per cui, pur presentando comunque qualche costo di transazione, la moneta negli scambi si è rivelata una tecnologia vincente rispetto al baratto in termini di frazionabilità e quantificazione del valore, nonché di sostituzione della duplice corrispondenza degli interessi dei contraenti con l'unico interesse del compratore), ma ne esistono altri da imputare inevitabilmente allo stato di razionalità limitata in cui verte ciascun contraente e questa tipologia di costi, a differenza dei primi, oltre a determinare una perdita di utilità nello scambio possono essere anche potenzialmente pregiudizievoli per il perfezionamento stesso dello scambio. Tra questi, i costi di ricerca possono essere significativi nella misura in cui le parti debbono investire il proprio tempo o il proprio denaro in un'attività, la ricerca appunto, di cui non è garantito un risultato efficace (l'individuazione della migliore controparte), ma più dei costi di ricerca sono i costi di natura fiduciaria ad essere particolarmente onerosi per le controparti poiché, oltre ad essere potenzialmente pregiudizievoli della transazione stessa, sopravvivono anche a seguito dello scambio materiale in quell'implicito rapporto contrattuale che periste tra le parti (banalmente si pensi alla spesa aggiuntiva per una garanzia, su un prodotto che si acquista, come quantificazione del costo fiduciario che altrimenti verrebbe "naturalmente" sostenuto a transazione compiuta)

Lo studio della razionalità limitata, ma soprattutto dei costi transattivi di natura fiduciaria che emergono da essa, nonché delle distorsioni del comportamento economico che gli sono imputabili, meritano un approfondimento rigoroso in virtù delle implicazioni che hanno. I contesti di razionalità limitata condizionano visceralmente le decisioni economiche degli individui segnando, in definitiva, delle importanti distorsioni a livello sistemico. Generalmente, la mancata consapevolezza da parte di un contraente di ogni elemento imputabile alla controparte e rilevante per la transazione produce effetti distorsivi tanto nella fase antecedente quanto nella fase successiva rispetto al momento di conclusione dello scambio.

Con "selezione avversa", infatti, si fa riferimento a quella situazione di subottimalità che si verifica nella ricerca della controparte, ossia prima ancora del verificarsi stesso della transazione: si tratta di una fase caratterizzata dalla diffidenza dettata dal rischio del rischio di trovarsi di fronte un cattivo contraente che non assolverà le prestazioni nei tempi, nei modi o nella specie prevista dall'obbligazione comunemente accordata. Questo rischio rappresenta un disincentivo a concludere le transazioni e la carenza di scambi si riverbera nell'incompletezza del mercato. La selezione avversa, descritta efficacemente dal modello "*Market for lemons"* di George A. Akerlof prendendo come esempio l'incompletezza del mercato di auto usate, è spesso

richiamata nel contesto dei mercati finanziari enfatizzando l'importanza del circuito indiretto nella corretta allocazione delle risorse. Infatti, la concessione di un prestito o di qualsiasi altra forma di finanziamento prevede sempre la valutazione del premio al rischio della controparte al fine di determinare le migliori condizioni contrattuali e questa attività, nel caso in cui avvenisse unicamente nel circuito diretto, risentirebbe notevolmente di costi informativi che potrebbero sancire il mancato trasferimento di capitale da risparmiatori a operatori potenzialmente in grado di far fruttare quel capitale, causando così una mancata allocazione efficiente delle risorse e la generale incompletezza dei mercati finanziari. In altre parole, se si intende investire il proprio denaro concedendo un finanziamento ad una controparte, si avrà difficoltà a stabilire un congruo tasso di interesse da applicare all'operazione proprio perché non si saprà con quale certezza il debitore sarà disposto o sarà in grado di ripagare e remunerare il proprio debito. Pertanto, poiché l'incertezza nell'*an* e nel *quando* della riscossione del proprio credito incrementa il rischio patito dal creditore, per remunerare questo rischio aggiuntivo egli esigerà un tasso di interesse adeguato che sarà quindi più alto per debitori dalla cattiva reputazione, o dall'infelice situazione patrimoniale e reddituale, e più basso per buoni debitori. In altre parole, il creditore avrà interesse a discriminare il tasso di interesse richiesto dopo aver effettuato la valutazione del rischio di controparte, in un processo definito "valutazione del merito creditizio". Ammettendo il caso in cui il creditore goda di completa informazione conoscendo ogni aspetto rilevante del debitore, allora la valutazione del merito creditizio avverrebbe con efficacia ed il costo dell'indebitamento verrebbe considerato congruo anche dal debitore che accetterebbe quindi di concludere la transazione. Tuttavia, in contesti ordinari, gli aspetti rilevanti del debitore rimangono estranei al creditore il quale, pur di non abbandonarsi ad un "atto di fede" nel concedere il proprio denaro, non sarà in grado di discriminare correttamente il premio al rischio tra diversi debitori. La soluzione più semplice sarebbe quella di proporre un unico tasso di interesse che vada a riflettere il rischio di controparte mediamente osservato nella platea degli investitori: in questo modo però i buoni debitori, caratterizzati da un rischio di controparte particolarmente contenuto, non riterranno congruo il "costo" del loro debito e decideranno di non indebitarsi uscendo, in un certo senso, dal mercato; al contrario, il tasso di interesse "medio" avrà un effetto magnetico su tutti i cattivi debitori consapevoli che il costo di quel debito stia sovrastimando la loro integrità debitoria, e pertanto costoro si affanneranno a ricevere denaro a quel tasso di interesse. Poiché il rischio di controparte è marginalmente crescente rispetto all'uscita dal mercato di buoni debitori e alla persistenza di cattivi debitori, accade che il rischio medio di controparte (e di conseguenza il tasso di interesse applicato) aumenta progressivamente, arrivando al fallimento del mercato causato dalla sola sopravvivenza di pessimi debitori e quindi dall'assenza di volontà di investire i propri soldi concedendoli in finanziamento. Come osserviamo, il manifestarsi del costo fiduciario nella fase preliminare della transazione può impedire la conclusione stessa dello scambio, e gli esempi sono molteplici anche nel quotidiano: quante volte si è rinunciato a comprare un prodotto su eBay proprio a causa di perplessità riferite all'inserzionista o all'autenticità del prodotto venduto? Ora, che si vada a pagare un'agenzia di rating per ottenere informazioni che promettono di essere oggettive e funzionali alla valutazione del rischio di

controparte o che si vada a pagare per un servizio di certificazione dell'autenticità di un prodotto che si va ad acquistare c'è poca differenza: in entrambi i casi la selezione avversa subordina la conclusione di una transazione alla monetizzazione del costo fiduciario che, a causa delle limitate risorse informative, si rivela indissolubilmente legato ad essa.

Al contrario, uno stato di asimmetria informativa e di conseguente onere fiduciario da parte di anche un solo contraente si traduce, a transazione compiuta, in una persistente incertezza rispetto all'integrità del proprio credito a causa del compimento di atti, potenzialmente pregiudizievoli a riguardo, posti in essere dal debitore. Questo si traduce in un onere di monitoraggio da parte del creditore e di complessivo irrigidimento del rapporto contrattuale (vedasi le clausole di *protective covenant* di molti contratti obbligazionari), elementi che vanno a pesare sul vantaggio reciproco della transazione. Pertanto, è evidente ancora una volta come il carattere fiduciario che inevitabilmente caratterizza il rapporto tra le parti si ramifichi in un insieme aperto di costi in termini monetari, temporali e di controllo.

Come evidenziato dal modello di Diamond, la presenza di una terza parte che ora assiste le parti nello scambio, ora diventa essa stessa controparte di entrambi i contraenti, agendo come vero *man in the middle*, si è rivelata fino ad oggi una soluzione efficace rispetto all'incompletezza del mercato dovuta a selezione avversa ed azzardo morale, decretando a tutti gli effetti la superiorità del circuito indiretto rispetto al circuito diretto dei sistemi finanziari, almeno in termini di minimizzazione delle frizioni finanziarie. Pur essendo la più efficace, essa non è esente da inefficienze che comunque si verificano, pur essendo queste relativamente infime rispetto ai guadagni di utilità derivanti da tale soluzione. Tuttavia, esistono dei costi, monetari o informativi, tanto nell'attività di consulenza e di assistenza offerta dagli intermediari broker quanto nell'attività di negoziazione diretta svolta dagli intermediari dealer, soprattutto in termini di bilanciamento del potere contrattuale delle parti se si pensa al confronto tra il numero complessivo di unità in deficit e la notevole concentrazione di intermediari finanziari in grado di concedere loro questi finanziamenti. Lungi dal considerare "fatali" queste perdite di efficienza per il sistema corrente, quantomeno esse aprono alla possibilità che il circuito indiretto dei sistemi finanziari non sia destinato ad essere l'unica ed imperitura soluzione ai problemi di selezione avversa e azzardo morale. E va anche sottolineato come il circuito indiretto, pur minimizzandone gli effetti, di certo non va ad eliminare quei costi di natura fiduciaria prima riferiti a coloro che nel circuito diretto avrebbero agito come uniche controparti dirette, ossia i singoli privati, e che ora si rivolgono a coloro che, nel circuito indiretto, si propongono nell'attività di brokeraggio o di negoziazione diretta, ossia gli intermediari finanziari. Molte delle grandi crisi, ultima quella del 2008, hanno dimostrato come la persistenza dell'elemento fiduciario, seppur quiescente nei suoi effetti, possa essere indizio di una fragilità strutturale del circuito indiretto del sistema finanziario, soprattutto in contesti di conflitto di interesse in cui vertono intermediari dalle attività polivalenti. E questa fragilità è nota agli stessi legislatori nazionali e sovrannazionali, come nel caso del legislatore europeo, che già a partire dal 2004 con la direttiva MiFID (direttiva 2004/39/EC), entrata in vigore a partire dal 2007, avvertì l'esigenza di regolamentare il "*detrimental conflict of interest*" degli

intermediari finanziari attraverso una disciplina arricchita successivamente dalla direttiva MiFID II (direttiva 2014/65/UE). Aldilà del conflitto di interesse, gran parte della vigilanza prudenziale e informativa sancita dal Comitato di Basilea attraverso gli accordi di Basilea I, Basilea II, Basilea III e prossimamente di Basilea IV ha evidenziato la necessità di neutralizzare le barriere informative che separano gli intermediari dalle autorità di vigilanza e dal pubblico di risparmiatori, richiedendo il soddisfacimento da parte dei primi di requisiti patrimoniali, di solvibilità, di trasparenza e di *disclosure* proprio per scongiurare situazioni di azzardo morale dettate da un'eccessiva assunzione di rischi.

Quando si chiede il rating di una società, si postula che la sua determinazione sia avvenuta secondo criteri obiettivi ed inconfutabili; quando si apre un conto corrente bancario, si postula che il denaro depositato sia e sarà sempre alienabile e prelevabile; quando si accetta un pagamento in moneta fiduciaria emessa da una terza parte, si postula la solvibilità dell'emittente o del suo garante. In tutti questi "postulati" con cui si perfezionano le transazioni quotidiane, per quanto impercettibili e apparentemente remoti negli effetti non augurabili, albergano i costi fiduciari a carico di almeno uno dei due contraenti: l'intermediazione fiduciaria non elimina il costo fiduciario, semplicemente ne muta le fattezze.

Parte della fortuna dell'intermediazione finanziaria risiede nel vizio "infrastrutturale" del sistema finanziario, ossia nel fatto che l'infrastruttura stessa dei sistemi di circolazione del capitale, allo stato attuale, non sia in grado di istruire al meglio le unità che vi operano, costringendole ad uno stato di sistematica penuria informativa da cui discendono le subottimalità evidenziate sino ad ora. In altre parole, gli intermediari finanziari sono un ottimo fertilizzante sintetico per un terreno che altrimenti rimarrebbe arido ed infruttifero.

Ma cosa accadrebbe se l'infrastruttura, autonomamente, permettesse ai suoi operatori di ampliare il bagaglio informativo a loro disposizione in modo tale che, lungi dal raggiungere una situazione di perfetta informazione, si vadano a ridurre gli elementi di asimmetria informativa in cui si insinuano i costi di natura fiduciaria ora rivolti alla generica controparte, ora rivolti allo stesso intermediario? Cosa accadrebbe se un contraente fosse consapevole delle effettive disponibilità economiche della controparte alla luce della concatenazione di transazioni autenticate che hanno anticipato quello scambio? Cosa accadrebbe se vi fosse reciproca certezza in merito al perfezionamento simultaneo di prestazioni digitali? Indubbiamente si assisterebbe ad una generale rivalutazione del circuito diretto dei sistemi finanziari, facendo diminuire il potere assoluto goduto allo stato attuale dal circuito indiretto, innescando così un percorso di disintermediazione fiduciaria in cui, tanto nell'offerta quanto nella domanda di capitali, unità in surplus ed unità in deficit beneficerebbero di possibili alternative rispetto a quelle proposte dalla tradizionale e centralizzata intermediazione finanziaria. L'esistenza di alternative genera concorrenza, portando potenzialmente ad un definitivo incremento di utilità nel sistema. Banche ed altri intermediari potrebbero patire la concorrenza della finanza decentralizzata (anche detta DeFi) ed elaborare, alla luce di essa, un nuovo ventaglio di offerta più accomodante per le esigenze dei propri clienti, magari servendosi gli stessi strumenti dell'infrastruttura-competitor.

1.2 La Blockchain

La tecnologia che, allo stato attuale, si propone come la soluzione più promettente per l'eliminazione dell'onere fiduciario tra i contraenti, senza prevedere l'intromissione di terze parti, è detta "*Blockchain*". Questa nuova tecnologia nasce da un'originale combinazione di ambiti disciplinari trasversali tra loro, come l'informatica, la crittografia e l'economia monetaria, permettendo la realizzazione di un'infrastruttura dinamica tanto nella crescita quanto nel potenziale applicativo.

1.2.1 L'isola di Yap

Per avere un'idea iniziale dei principi della blockchain, può risultare utile richiamare un esempio storico, evidenziando come questa tecnologia trovi il suo archetipo secoli addietro[4]. Nel 1400 gli abitanti di Yap, un'isola in Micronesia, avviarono un sistema monetario costruito intorno al "Rai", una moneta merce consistente in una pietra calcarea forata al centro che veniva estratta a Palau, un'isola distante 400 chilometri. In qualità di moneta merce e priva di un garante esterno, il valore nominale del Rai era ancorato al suo valore reale e quindi l'autoreferenzialità della moneta faceva sì che le pietre di maggiori dimensioni avessero un valore altrettanto maggiore. Il problema di questo meccanismo risiedeva nel fatto che le transazioni quotidiane richiedessero il trasporto di un notevole peso nel corso della giornata, inficiando sulla funzione di questa pietra come intermediario degli scambi. Per questo motivo, come accadde nella storia monetaria occidentale con il tramonto delle monete d'oro, si avvertì l'esigenza di definire un'infrastruttura monetaria che facilitasse gli scambi e che potenziasse la natura della moneta come numerario del sistema.

Tuttavia, se il modello occidentale si caratterizzò per un'infrastruttura centralizzata segnata dal passaggio da moneta merce a moneta segno, quindi da moneta segno a moneta legale e fiduciaria, in cui prima lo Stato e poi soggetti privati si sono proposti come necessari intermediari fiduciari per garantire l'efficacia del sistema, gli isolani di Yap mantennero un'infrastruttura decentralizzata basata sull'annotazione di transazioni a favore o a debito presso un unico grande registro, aggiornato periodicamente e collettivamente, di cui ciascun isolano manteneva una copia. Questo meccanismo da un lato azzerava il costo transattivo associato al trasporto del Rai, poiché permetteva di concludere transazioni reali senza prevedere il materiale passaggio di moneta, dall'altro impediva che il potere di acquisto degli individui fosse subordinato al rischio di furto, smarrimento o distruzione della pietra in quanto elemento materiale, proprio perché la loro disponibilità di spesa sarebbe emersa dalle annotazioni note a tutti presso il grande registro condiviso. In altre parole, una volta immesso nel sistema ed essendo stato accreditato all'abitante che l'aveva estratto, il Rai in quanto tale perdeva qualsiasi utilità per l'individuo poiché, anche nel caso in cui fosse stato materialmente rubato, il ladro non avrebbe beneficiato di alcun potere d'acquisto ulteriore rispetto a quello che sarebbe emerso dalle transazioni

[4] Comandini, Gianluca. *Da Zero alla Luna. La Blockchain: quando, come, perché sta cambiando il mondo*. Flaccovio, 2020;

"pubbliche" concluse in passato a suo favore. In sintesi, si era costruita un'infrastruttura monetaria in cui la semantica del valore monetario non veniva associato alla componente materiale e visibile della singola moneta, ma alla componente immateriale, conoscibile e condivisa dello storico delle transazioni monetarie, causando un definitivo distaccamento tra l'immateriale potere d'acquisto ed il materiale strumento di pagamento. È su questo differente paradigma che si è in grado di apprezzare la natura infrastrutturale della blockchain, tanto nella sua forma più arcaica (come sistema di pagamenti) quanto nelle sue forme più evolute.

1.2.2 Il meccanismo *trustless* dell'infrastruttura

Tecnicamente, la blockchain è un'infrastruttura di rete *peer-to-peer* che assolve le funzioni di un *database* distribuito tra tutti i partecipanti (*nodes*) della rete.

Essa prevede la concatenazione in ordine cronologico di blocchi di dati che vengono autenticati (entrando quindi a far parte di questa infrastruttura) mediante un protocollo di validazione condiviso tra tutti i nodi della rete. Questo protocollo di validazione condiviso è spesso definito "algoritmo di consenso" o "protocollo di consenso". I "dati" contenuti all'interno di questi blocchi concatenati vengono detti "transazioni" (*transactions*) e, contrariamente a ciò che suggerirebbe il nome, non necessariamente assumono una connotazione economica, poiché con esse si intende qualsiasi esecuzione di un programma informatico sulla blockchain. Infatti, salvo il caso in cui il programma si limiti alla sola "lettura" di dati già presenti su questa rete, ciò che definisce una transazione è l'ingresso di nuovi dati o lo spostamento di dati preesistenti tra un utente ed un altro, ossia, genericamente, qualsiasi modifica dello "status quo" di questo grande registro distribuito che è la blockchain, sia essa l'estrazione di nuova criptovaluta, il trasferimento di criptovaluta esistente, il passaggio di determinati diritti o la registrazione di qualsiasi altra informazione.

Esistono blockchain, infatti, come quella di Ethereum, che espandono l'impiego di questa infrastruttura oltre i confini di un semplice sistema di pagamento, permettendo agli indirizzi della rete di realizzare transazioni digitali (in senso lato) invocando le funzioni informatiche di librerie distribuite dette "*smart contracts"*. Gli smart contracts, attraverso le stesse funzioni che ospitano e che vengono invocate da parte delle transazioni che se ne servono, definiscono uno *standard,* ossia un insieme di regole coincidente con il dominio di possibilità della categoria di transazioni che li riguarda. Potremmo dire che una *transaction* stia ad uno *smart contract* esattamente come un contratto giuridico stia al relativo istituto: se un contratto d'appalto viene stipulato senza rispettarne il relativo standard, ossia l'insieme di regole fondamentali che ne definisce la validità (ad esempio, il rispetto delle norme imperativa in materia urbanistica), il contratto sarà nullo o annullabile a seconda della decisione del giudicante; allo stesso modo, se una transazione che si riferisce ad un certo smart contract invocherà funzioni diverse da quelle previste dallo stesso o utilizzerà parametri diversi da quelli previsti ed ammessi, la transazione non potrà essere tecnicamente eseguita sulla rete venendo quindi automaticamente rigettata senza coinvolgere la discrezionalità di alcuna terza parte. In ogni caso, gli smart contracts rappresentano l'insieme aperto di possibilità inerenti al potenziale applicativo della blockchain: dalla

tokenizzazione dei diritti al mercato dell'arte. Per mezzo degli smart contracts è possibile realizzare i c.d. *token*, ossia "gettoni" digitali diversi dalla criptovaluta nativa della blockchain presso la quale gli stessi smart contracts sono depositati, che attribuiscono al portatore gli stessi diritti e le stesse facoltà riconosciute dallo smart contract a cui si riferiscono, sia anche la sola "titolarità" unica ed esclusiva sul token stesso, in ottica autoreferenziale. Servendosi degli *standard* ERC-20 ed ERC-677 ad esempio, le tipologie di smart contract più comuni per i token fungibili presenti sulla blockchain Ethereum, sono stati avviati importanti progetti che promettono di integrare il mondo *off-chain* con quello *on-chain* come i tokens ChainLink (LINK) o Tether (USDT), mentre standard come ERC-751, ERC-1155 ed i relativi token infungibili (*NFT, Non-Fungible-Token*) stanno lentamente rivoluzionando il concetto dell'arte e di qualsiasi forma di apprezzamento del concetto di "unicità".

Tipicamente, qualsiasi criptovaluta non è altro che una registrazione a favore di un certo indirizzo (*wallet*) all'interno di questo database, definendo così lo "spendibile" di quell'indirizzo nei confronti degli altri indirizzi della rete. Ovviamente, nel caso in cui la somma a proprio favore venisse trasferita ad un altro indirizzo, il proprio indirizzo verrebbe nettato della somma trasferita una volta convalidata la transazione da parte dei *full nodes* della rete: il coinvolgimento della crittografia asimmetrica garantisce questo funzionamento impedendo che un indirizzo possa disporre nuovamente della criptovaluta precedentemente alienata (fenomeno del c.d. *double spending*).

Comprando un Bitcoin quindi, si compra semplicemente una scrittura a proprio favore all'interno del registro-blockchain ed è in questo senso che si coglie il carattere intangibile delle criptovalute in generale. L'intuizione di questo meccanismo sta nell'utilizzo della crittografia asimmetrica tanto nel concretarsi delle transazioni quanto nel processo di validazione dei blocchi, in modo tale da prevenire fenomeni di contraffazione di questo libro mastro (come il fenomeno di *double spending* precedentemente accennato).

Un indirizzo, presso il quale vengono depositate le criptovalute, nasce a partire da due chiavi: una chiave privata ed una chiave pubblica; la chiave privata è un numero casuale di 256 cifre rappresentato in forma esadecimale, motivo per cui appare come una stringa alfanumerica di 64 caratteri[5].

La chiave pubblica viene generata a partire dalla chiave privata attraverso la *moltiplicazione a curva ellittica* (ECDSA-512 nel caso di Bitcoin), ossia un tipo di trasformazione non-lineare che impedisce di risalire alla sequenza alfanumerica della chiave privata conoscendo quella pubblica.

Quindi, inserendo la chiave pubblica all'interno di un algoritmo di hash (RipeMD 160 nel caso di Bitcoin) si ottiene una stringa ridotta, definendo così l'indirizzo del wallet sulla rete; si potrebbe concepire un algoritmo di hash come un "tritacarne" in cui, in maniera similare alla moltiplicazione a curva ellittica, l'unidirezionalità dell'algoritmo rende infinitesima la probabilità di successo nel risalire all'input iniziale (la chiave pubblica, o l'ipotetico "pezzo di carne") a partire dall'output finale (l'indirizzo del wallet, o l'ipotetico "macinato").

[5] https://cryptonomist.ch/2019/07/13/bitcoin-chiavi-indirizzi/

La crittografia asimmetrica è di fatto il vero "garante" dell'autenticità della transazione che, nel caso di Bitcoin, si articola nella fase di *firma* della transazione da parte del mittente e di *verifica dell'autenticità* da parte del ricevente. La fase di firma[6] prevede prima la sintesi del messaggio (ossia dei dati da trasferire) in un hash mediante l'utilizzo di un omonimo algoritmo (SHA-256 nel caso di Bitcoin), quindi la generazione della "firma digitale" attraverso l'impiego di una funzione di *encrypting* che prenderà come argomenti l'hash del messaggio e la chiave privata del wallet da cui proviene la transazione; completato questo passaggio, il mittente invierà all'indirizzo del wallet del destinatario il messaggio, la firma digitale e la propria chiave pubblica. La verifica dell'autenticità avviene sottoponendo nuovamente il messaggio allo stesso algoritmo di hash precedentemente utilizzato dal mittente e decriptando la firma digitale utilizzando la chiave pubblica ricevuta, in modo tale da ricostruire l'hash del mittente. In questo modo si potrà confrontare l'hash generato dall'*hashing* del messaggio con quello ottenuto decriptando la firma digitale usando la chiave pubblica del mittente: se i due hash sono identici, allora questo certifica tanto l'autenticità del messaggio (che non sarà stato alterato in fase di trasmissione) quanto l'autenticità del mittente, poiché altrimenti sia per la corruzione del messaggio, sia per l'utilizzo di una chiave pubblica diversa da quella del mittente, il secondo hash generato risulterà completamente diverso da quello ricevuto.

$$\begin{cases} M = messaggio \\ S = firma\ digitale \\ K_{pubb} = chiave\ pubblica\ del\ mittente \\ K_{priv} = chiave\ privata\ del\ mittente \\ H(x) = hashing\ di\ x \\ Add = indirizzo\ del\ ricevente \end{cases}$$

Firma (mittente)

1) Hashing del messaggio da parte del mittente: $H = H(M)$

2) Firma digitale del mittente: $S = encrypting(H; K_{priv})$

Transazione

$M + S + K_{pubb} \rightarrow Add$

Verifica(destinatario)

1) Hashing del messaggio da parte del destinatario: $H_{Add} = H(M)$

2) Ricostruzione dell'hash del mittente : $H' = decrypting(S; K_{pubb})$

3) Confronto dei due hash: $H' = H_{Add} \leftrightarrow transazione\ autentica$

Quindi la transazione, dopo essere stata validata, entra a far parte di un blocco di transazioni in attesa di essere trascritto sulla rete mediante il meccanismo di validazione dei blocchi previsto per quella blockchain.

[6] http://www.10bitcoin.it/firma-transazione-bitcoin/

1.2.3 I principali protocolli di consenso

I protocolli più famosi per la validazione dei blocchi sono Proof-of-Work (PoW) e Proof-of-Stake (PoS), protocolli di consenso ideati originariamente come misure di prevenzione contro i c.d. "*Sybil attacks*" ma impiegati rispettivamente per la blockchain di Bitcoin e di Ethereum. La validazione dei blocchi è anche detta "mining", termine che fa riferimento al fatto che con tale meccanismo avvenga anche la generazione di nuova criptovaluta (o meglio, la generazione di una prima transazione di una futura cronologia di transazioni) a favore dei nodi validatori, al fine di remunerarli per i costi sostenuti tanto per le attrezzature quanto per l'energia elettrica inevitabilmente spesa in questo processo, creando così un incentivo per la partecipazione alla rete in qualità di *full node* contribuendo positivamente alla sicurezza generale dell'infrastruttura. Se l'accesso al processo di validazione dei blocchi è libero, ossia se chiunque abbia capacità di calcolo da prestare alla rete ha anche la possibilità di entrarne a far parte in qualità di *full node,* allora la blockchain si dirà "*permissionless*", altrimenti, nel caso in cui l'accesso al meccanismo di validazione dei blocchi sia subordinato al placet da parte di alcuni nodi "principali" della rete, allora la blockchain si dirà "*permissioned*": è chiaro che il significato più ampio della decentralizzazione viene colto da blockchain di tipo *permissionless* e che, al contrario, le blockchain di tipo *permissioned* non siano lontane dai meccanismi tradizionali di *data storaging* o comunque di piattaforme governate centralmente. Di fatto quindi, la definizione di un certo protocollo di validazione dei blocchi implica necessariamente la scelta di una certa frequenza di registrazione delle transazioni (che si tradurrà in una specifica velocità della rete), di un certo grado di decentralizzazione, nonché di un certo meccanismo di emissione "monetaria" riferito alla criptovaluta in questione.

Tanto nella PoW quanto nella PoS, gli archetipi di funzionamento di entrambi i meccanismi potrebbero definirsi di natura "smithiana" essendo basati sull'amorale ed egoistica ricerca al profitto perseguita dagli individui, in questo caso, dai *miners* (nodi validatori). In entrambi i casi, infatti, la sicurezza e l'efficienza della rete è definita a partire dalla concorrenza presente tra ciascun miner nel tentativo di aggiudicarsi la validazione del blocco di transazioni, in modo da appropriarsi del premio che ne deriva: ciò che diverge tra i due modelli è la variabile di competizione con cui si espleta questo processo di validazione.

Nel caso della Proof-of-work, la competizione tra i miners avviene sulla *velocità* e quindi, in definitiva, sulla *forza computazionale* (*hash power*) delle macchine impiegate nel mining, definendo così un protocollo di validazione particolarmente energivoro su larga scala. I miners, infatti, per validare i blocchi, sottopongono ad uno stesso algoritmo di hash il contenuto del blocco in attesa di essere validato (ossia le transazioni), l'hash del blocco precedente (ovviamente già validato) ed un numero randomico, detto *nonce*, che viene fatto variare al fine di ottenere (prima degli altri miners) un hash avente uno specifico numero di zeri inziali. Nel caso di Bitcoin, il numero di zeri iniziali che viene richiesto per la convalida di un blocco è variabile ed è direttamente proporzionale all'*hash power* complessivamente prestato alla rete, poiché l'aggiunta di uno zero inizialmente richiesto nell'hash intensifica notevolmente lo sforzo computazionale complessivamente impiegato: la

variabilità dello sforzo computazionale è servile al fatto di rendere costante la frequenza di validazione dei blocchi, in modo tale che vengano validati blocchi ogni 10 minuti indipendentemente da quanto sia intensa la partecipazione al potere computazionale della rete (ad oggi il numero di zeri iniziali richiesti nell'hash è 19). Inoltre, la PoW di Bitcoin prevede ogni quattro anni il c.d. fenomeno di *halving* ossia di dimezzamento del premio di validazione di ciascun blocco di transazioni (ad oggi è di 6.5 BTC per blocco convalidato) al fine di massimizzare la distanza temporale dall'estrazione di tutti i 21 milioni di Bitcoin (si potrebbe definire un'applicazione concreta del "Paradosso di Zenone" ma facendone il limite matematico si prevede che tutti I Bitcoin saranno estratti intorno al 2140[7]).

L'onere computazionale marginalmente crescente ed il dimezzamento periodale del premio di validazione è causa di una rapida obsolescenza delle macchine da mining, apprezzando al tempo stesso il valore reale di Bitcoin essendo quest'ultimo "sempre più difficile" da estrarre sia rispetto all'aumento della partecipazione alla rete (in termini di maggiore concorrenza e di maggiore capacità computazionale richiesta) sia rispetto al passare del tempo. La velocità di crescita del valore di mercato di Bitcoin rispetto all'incremento del suo valore reale definisce la presenza o meno di economie di scala nell'attività di mining e di conseguenza l'incentivo a partecipare sul "lato dell'offerta" (in senso lato) di questa criptovaluta.

Il protocollo di validazione è detto appunto "Proof-of-Work" proprio in ragione del fatto che la prova di validazione del blocco sia data dalla capacità computazionale spesa efficientemente per la validazione stessa, ed è sulla base di questo stesso principio che la blockchain condivisa tra tutti i blocchi (e quindi la blockchain considerata appunto come "vera") sia quella più lunga in termini di blocchi convalidati: il protocollo di convalida quindi si rivela anche un protocollo di sicurezza in ragione del fatto che un nodo malevolo, ossia un nodo che ha interesse a validare una o più transazioni che si distaccano da quelle storicamente osservate (in modo tale, ad esempio, da portare avanti una blockchain in cui venga figurato che sul proprio indirizzo siano riconosciuti 1.000.000 BTC, quando in realtà non si sono mai verificati transazioni passate che l'hanno reso possibile), per poter riuscire nel suo intento ha bisogno di possedere *sistematicamente* una capacità computazionale maggiore o uguale al 51% dell'intero hash power della blockchain.

Il rischio del c.d. "*51% attack*" quindi si rende marginalmente decrescente all'aumentare della partecipazione alla blockchain, ed è in tal senso che si capisce il significato per cui diventare *full node* implichi inevitabilmente il fatto di contribuire "passivamente" alla sicurezza generale dell'infrastruttura.

Bisogna sottolineare anche il fatto che, laddove il nodo malevolo riuscisse a raggiungere per un breve intervallo il 51% della potenza complessiva della rete, questo non sarebbe sufficiente per garantire la validazione del blocco a proprio vantaggio, poiché nella fase di registrazione della blockchain-malevola presso gli altri nodi, accadrebbe che nel frattempo gli altri nodi ordinari continuerebbero a validare i blocchi della blockchain principale che, diventando più lunga di quella malevola, la andrebbe a sostituire.

[7] https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/#:~:text=This%20effectively%20lowers%20Bitcoin's%20inflation,until%20around%20the%20year%202140.

Il pericolo di un "*51% attack*" per blockchain basate su PoW appare particolarmente remoto analizzando il potere computazionale delle macchine correnti, ma l'avvento del *quantum computing* e quindi di macchine con potere computazionale drasticamente più alto di quelle attuali può rappresentare una minaccia per questo protocollo.
Tradizionalmente la PoW viene considerata come il protocollo di validazione più decentralizzato in assoluto, e così è stato agli inizi della blockchain, permettendo a chiunque fosse disposto ad impiegare la CPU del proprio computer o economiche schede elettroniche designate di guadagnare autonomamente dall'attività di mining. Allo stato attuale però, l'onere computazionale richiesto da questa attività si traduce in costi proibitivi di macchine che nel medio termine diverranno già obsolete, motivo per cui attualmente l'unica possibilità per ottenere profitti dall'attività di mining è quella di impiegare le proprie macchine costose in "*mining pools*" registrandole, insieme ad altri utenti, presso medesimi nodi-miner, spartendo gli eventuali premi di criptovaluta che ne deriveranno insieme agli altri partecipanti del "pool", proporzionalmente alla capacità computazionale che ciascuno avrà fornito al nodo. Questo porta inevitabilmente a fenomeni di concentrazione sul versante della validazione che tradiscono in parte lo spirito di decentralizzazione che caratterizza l'ortodossia-blockchain, esponendo al tempo stesso la sicurezza della rete

Per quanto riguarda la PoS invece, la variabile di competizione ed al tempo stesso strumento di decentralizzazione è la criptovaluta stessa. Questo meccanismo di consenso prevede infatti che i nodi validatori vengano scelti sulla base dell'ammontare di criptovaluta che ciascuno di essi mette in "*staking*", ossia di criptovaluta che viene "congelata" all'interno dell'infrastruttura. Il principio è semplice: maggiore è la quantità di criptovaluta che viene bloccata da parte di un miner, maggiori sono le probabilità che questo venga scelto come nodo validatore del blocco e ricevere la ricompensa di convalida. La Proof-of-Stake nasce per risolvere l'inefficienza congenita della PoW causata dal fatto che l'energia spesa nel tentativo computazionale dei moltissimi miners che non sono riusciti ad aggiudicarsi la validazione del blocco venga consumata inutilmente, impattando negativamente tanto sui costi energetici quanto sull'ambiente: l'unica utilità che potrebbe emergere soltanto indirettamente dall'energia spesa in questo modo sarebbe quella di garantire la sicurezza della rete, seppur in maniera particolarmente energivora.
Inoltre, il protocollo di validazione basato sullo *staking* sembra essere particolarmente utile nel risolvere il secondo problema congenito della PoW, ossia quello delle "barriere all'ingresso" dell'attività di mining che si traducono inevitabilmente in una maggiore centralizzazione della rete: con la Proof-of-Stake infatti, i miners acquistano criptovaluta con gli stessi soldi che altrimenti avrebbero speso nell'acquisizione di macchine da mining specializzate (come le ASIC) e l'ingresso in questa attività può risultare profittevole anche con una dimensione ridotta dell'investimento, lucrando al tempo stesso sull'eventuale *capital gain* dell'asset che si va ad acquistare. L'intuizione dietro al concetto di "staking" risiede nel fatto che la criptovaluta bloccata agisca da *collateral* sull'efficacia dell'attività di validazione: nel caso in cui il nodo assuma un atteggiamento

malevolo, esso rischia di perdere la criptovaluta messa in staking; allo stesso modo, se i validatori non mantengono la rete sufficientemente sicura, sono loro stessi a rischiare la criptovaluta che hanno bloccato. Inoltre, maggiore è la criptovaluta messa in *staking*, maggiore è la copertura dal fenomeno inflazionistico che inevitabilmente ne inficia il valore, soprattutto se non è previsto un tetto massimo alla *total supply* (come nel caso di Ethereum). Anche in questo caso quindi, il principio di validazione è da ricercare nel nome stesso dell'algoritmo di consenso impiegato: se nel caso della "Proof-of-Work" la validazione del blocco sarà riconosciuta al "maggior lavoro computazionale speso efficientemente", nel caso della "Proof-of-Stake" la validazione sarà riconosciuta al "maggior interesse riversato nella rete" in termini di *skin in the game*, poiché saranno gli stessi validatori a "puntare" sulla sicurezza della rete rischiando (in senso lato) le proprie risorse economiche.

In ogni caso, involuzioni di centralizzazione possono comunque verificarsi anche in questo protocollo, poiché se la PoW poteva prevedere un accentramento di macchine da mining, la PoS può prevedere un accentramento di criptovaluta nelle mani dei nodi validatori, un meccanismo che può essere combattuto soltanto con una maggiore diffusione della criptovaluta stessa, secondo un meccanismo che però è contrario alla dinamica di emissione.

In altre parole, anche il mining basato su PoS risulta *capital intensive* seppur in forma allegoricamente diversa rispetto a quello basato su PoW: un individuo che vorrà partecipare con capitale modesto alla validazione di una blockchain basata su Proof-of-Stake avrà remote possibilità di aggiudicarsi un blocco da validare, patendo una concorrenza non troppo lontana da quella che si osserva su un tavolo da poker tra giocatori aventi un numero di *fiches* significativamente diverso gli uni dagli altri.

È per questo motivo che anche nel caso della PoS si assiste al fenomeno delle *mining pools*, rappresentando l'alternativa più conveniente per nuovi entranti nel competere con gli *incumbents* del settore del mining, causando però al tempo stesso involuzioni in termini di centralizzazione, polarizzando con accelerazione crescente la distribuzione di criptovaluta tra i diversi nodi.

1.3 Bitcoin

1.3.1 Storia

La primissima criptovaluta che ha visto la luce è Bitcoin, ideata da uno sviluppatore che ancora oggi rimane nell'anonimato definito con lo pseudonimo di "Satoshi Nakamoto". Il 18 agosto 2008, in piena crisi finanziaria, avvenne la registrazione del dominio di "bitcoin.org", dando vita a quel sito web che ancora oggi risulta essere il principale polo informativo di questa criptovaluta per neofiti, appassionati ed investitori consapevoli. Successivamente, il 31 ottobre dello stesso anno, un utente anonimo inserisce all'interno una mailing list di crittografi[8] l'estratto di un documento PDF in cui si delineava un sistema di pagamento in grado

[8] https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

di eliminare l'onere fiduciario tra i contraenti di una stessa transazione mediante l'utilizzo della crittografia asimmetrica, rendendo superflua al tempo stesso la presenza di qualsiasi tipo di intermediazione a riguardo.

"*I've been working on a new electronic cash system that's fully*

peer-to-peer, with no trusted third party."

Nel testo del messaggio, l'autore mise un collegamento ipertestuale per permettere ai partecipanti della community di essere reindirizzati presso un percorso web del sito "bitcoin.org", avendo così la possibilità di scaricare un documento di 9 pagine intitolato "*Bitcoin: A Peer-to-Peer Electronic Cash System*"[9], ossia il whitepaper di Bitcoin. Come asserisce lo stesso autore nel documento, l'idea di questo sistema di pagamento prende spunto da un progetto avviato nel 1983 dal famoso crittografo David Chaum intitolato "*eCash*"[10] e pensato per la realizzazione di un'anonima moneta elettronica che, mediante un sistema di firme digitali, avrebbe permesso agli utenti di effettuare i pagamenti senza dover condividere le informazioni della propria carta di credito con i venditori, i quali avrebbero ricevuto sul loro computer, in forma digitale, il denaro firmato crittograficamente dalle banche degli acquirenti. Il progetto fu concretamente avviato nel 1990 con la realizzazione della società "DigiCash" e, nonostante un primissimo interesse da parte delle banche, il servizio non fu mai concretamente messo in pratica a causa dell'impopolarità riscontrata sia per l'indifferenza dei consumatori rispetto alla tematica della privacy nei pagamenti sia per il fatto che i venditori aberrassero un sistema di pagamento in cui si dovesse pagare una commissione per ricevere del denaro che, attraverso i mezzi tradizionali, si sarebbe ottenuto direttamente. Il progetto quindi si rivelò fallimentare portando al fallimento di DigiCash nel 1998.

L'ibridazione tra anonimia dei pagamenti e coinvolgimento di terze parti come "garanti" della transazione risultò un connubio fatale per "*eCash*" e di questo Satoshi Nakamoto ne sembrò consapevole evidenziando la necessità di un sistema di pagamento elettronico che sostituisse la fiducia con una "prova crittografica" della stessa: questo avrebbe permesso la realizzazione di un circuito, all'epoca inesistente, scevro in senso assoluto da qualsiasi intromissione di terze parti, dal momento che la convenienza di tale intromissione fosse sempre dipesa unicamente dall'impossibilità dei contraenti di instaurare tra loro un rapporto fiduciario altrimenti necessario.

"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."

Le transazioni sarebbero avvenute mediante crittografia asimmetrica come evidenziato nel capitolo precedente, e l'algoritmo di consenso impiegato per la validazione dell'insieme di transazioni sarebbe stato quello della Proof-of-Work. Chiunque avrebbe partecipato alla rete in qualità di nodo validatore avrebbe ricevuto come potenziale ricompensa della propria attività una speciale transazione che l'avrebbe reso titolare

[9] https://bitcoin.org/bitcoin.pdf
[10] https://www.investopedia.com/terms/e/ecash.asp

dei bitcoin estratti mediante la validazione delle transazioni, in modo tale da immettere liquidità all'interno del sistema creando al tempo stesso un incentivo reso necessario dall'assenza di un unico ente emittente diverso dalla rete stessa. Lo schema di emissione avrebbe seguito dinamiche deflazionistiche dimezzando ogni 4 anni il premio di validazione (detto anche *"coinbase reward"* o *"block reward"*), fino all'estrazione di 21 milioni di bitcoin complessivi in modo tale da immunizzare il sistema dall'inflazione, spostando poi gli incentivi dell'attività di mining sulle commissioni riscosse attraverso la validazione delle transazioni

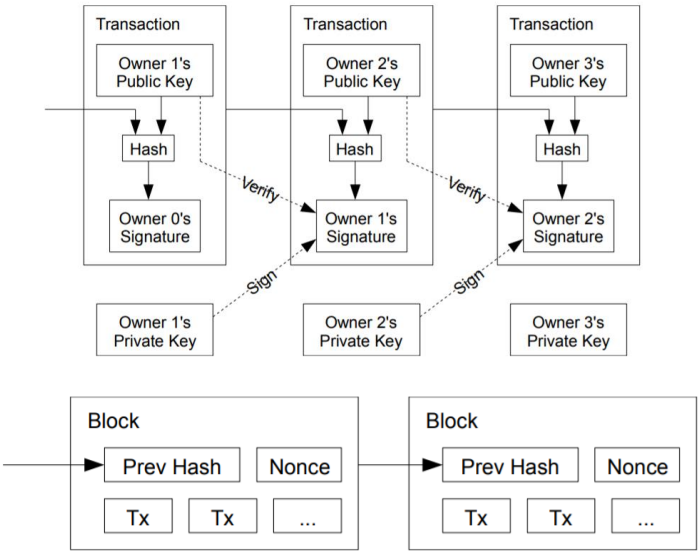


Figura 1: Meccanismo di validazione transazioni Bitcoin

Il meccanismo di Proof-of-Work avrebbe risolto alcune potenziali problematiche significative: *in primis*, avrebbe offerto un semplice algoritmo di consenso che avrebbe permesso ai nodi di decidere collettivamente rispetto agli sviluppi della rete; *in secundis*, avrebbe permesso la libera partecipazione alla rete risolvendo il problema politico del consenso sulle decisioni, prevenendo allo stesso tempo che la proliferazione di nodi in capo ad uno stesso soggetto permettesse allo stesso di maturare un qualche vantaggio nella determinazione del consenso, danneggiando in definitiva la democraticità della rete (il c.d. *Sybil Attack*). Questo perché il peso specifico del voto di ciascun nodo sarebbe dipeso esclusivamente dalla capacità computazionale prestata da esso. Quindi, pochi mesi più tardi dalla pubblicazione del whitepaper, il 3 gennaio 2009 venne validato il primo blocco della blockchain di Bitcoin, anche detto "genesis block"[11] attraverso cui furono accreditati 50 BTC come coinbase reward all'indirizzo "1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa", uno dei diversi indirizzi attribuiti a Satoshi Nakamoto (ad oggi l'indirizzo conta 68.38389718 BTC ed è stato coinvolto in 2834 transazioni malgrado in nessuna di esse sia mai stata alienata criptovaluta dall'indirizzo: si pensa infatti che la differenza positiva tra i Bitcoin accreditati ed i 50 Bitcoin riscossi come coinbase reward sia costituita da micro-donazioni effettuate deliberatamente dagli utenti della rete per ricompensarlo di questa invenzione).

[11] https://www.blockchain.com/btc/block/0

Il *genesis block* è costituito dall'unica transazione con cui veniva accreditato il coinbase reward all'indirizzo e nel "sigscript" della transazione fu riportato il seguente codice esadecimale:

04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e2062
72696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73

Che tradotto in forma testuale diventa

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

Riportando testualmente il titolo di prima pagina del quotidiano "The Times" del 3 Gennaio 2009 che, tradotto in italiano, corrisponde a "Il Cancelliere ipotizza un secondo salvataggio per banche". Nell'articolo, infatti, veniva spiegato come l'ex cancelliere dello scacchiere (ministro delle finanze inglese) Alistair Darling si trovasse a decidere in merito all'eventualità che il governo intervenisse nuovamente per salvare le banche dal tracollo finanziario attraverso la rimozione dei "titoli tossici", responsabili della crisi finanziaria di quegli anni, dai bilanci delle banche. Con questo "messaggio segreto" Satoshi Nakamoto ha inteso sottolineare la *verve* rivoluzionaria che segnava l'atto di nascita di Bitcoin, suggerendo la possibilità che dietro a tale pseudonimo si nasconda un esponente (o un gruppo di esponenti) del movimento libertario "Cypherpunk", nato alla fine degli anni '80, che promuove l'utilizzo della crittografia informatica come radice di possibili rivoluzioni sociali e politiche del contemporaneo (anche Julian Assange, leader del sito "Wikileaks", è esponente dell'attivismo Cypherpunk).


THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

Figura 2: Prima Pagina "The Times" 03/01/09

L'inserimento di questo messaggio infatti evidenziava l'inammissibilità di un sistema basato sull'intermediazione fiduciaria che, proprio per la discrezionalità e la ricerca al profitto di banche, società di rating, e società di revisione contabile, ossia di terze parti fiduciarie, sancisse una pericolosa precarietà del sistema a cui si cercava di porre rimedio attraverso provvedimenti che, in ultima istanza, avrebbero avuto ripercussione negative sui cittadini tanto sulla loro ricchezza corrente, quanto sul trasferimento del valore a livello intergenerazionale.

I successivi sviluppi di Bitcoin rimasero "argomenti di nicchia" almeno fino al 2016 e questa criptovaluta veniva tradizionalmente utilizzata da videogiocatori nella compravendita di componenti addizionali in ambito *gaming* ma anche e soprattutto come mezzo di pagamento per transazioni illegali all'interno del "Deep Web", ossia nella parte "oscura" dell'internet (perché non indicizzata dai motori di ricerca), tanto da essere

demonizzata mediaticamente ancora oggi come la "moneta dei criminali". Il discredito gettato su Bitcoin fu anche dovuto all'iniziale (ed in parte persistente) assenza di regolamentazione a riguardo, cosa che permise ad organizzazioni criminali di servirsene per il riciclaggio di denaro alienando materialmente valuta *fiat* ed ottenendo in cambio Bitcoin attraverso transazioni che, seppur visibili sulla rete, mantenevano un anonimato in assenza di una corrispondenza tra gli indirizzi dei wallet ed i nominativi anagrafici.

Successivamente, Bitcoin iniziò ad essere scambiato insieme alle primissime criptovalute nate dopo di lui presso nuovi intermediari non bancari (talvolta decentralizzati, come nel caso di Bitmex), definiti comunemente "*exchanges*", istituiti appositamente per la loro negoziazione contro valuta fiat. Questo permise l'ingresso di investitori retailers incrementando l'attenzione di questo asset anche per i "non addetti ai lavori", facendo crescere il mercato di Bitcoin e delle criptovalute in generale in termini di liquidità. Tuttavia, l'interesse nei confronti della novità si tradusse presto in euforia secondo un meccanismo autoindotto dettato in parte dalla crescita progressiva del prezzo ed in parte dalla totale assenza di consapevolezza in merito alla natura stessa dell'investimento.

1.3.2 Evoluzione del prezzo di BTC

Di seguito si andrà analizzare l'evoluzione del prezzo di Bitcoin nella coppia BTC/USDT (la coppia più liquida del mercato spot di Bitcoin, USDT è una stablecoin che ancora il suo valore nominale a quello del dollaro) sulla base dei dati forniti dall'exchange Binance.com.

L'apertura di Bitcoin al grande pubblico avvenne a patire dal 2016, con la crescita verticale del suo prezzo protratta fino al termine del 2017 con il raggiungimento del picco di $19798 il 17/12/2017, seguito quindi dal primo grande crollo del suo valore fino al raggiungimento di un minimo di $3156 (-84,06%) quasi un anno più tardi, il 15/12/2018

In questa fase di "crisi" della criptovaluta, che veniva additata per essersi rivelata una delle più grandi bolle finanziarie degli ultimi anni, gli exchanges furono sottoposti al primo vaglio di regolamentazione da parte delle autorità competenti, proprio per garantire il monitoraggio di tutti i movimenti che potessero riguardare un asset di cui, ancora oggi, gli stessi legislatori nazionali riscontrano difficoltà nell'assegnargli un preciso inquadramento giuridico. Quindi si verificò un progressivo irrigidimento di misure di controllo dei conti presso gli exchanges imponendo misure notevoli di KYC (*Know your customer*) soprattutto come contromisura di riciclaggio di denaro. Questo definì un terreno fertile per una progressiva regolamentazione, ancora oggi lacunosa, ma che fu servile all'accettazione di Bitcoin nella sua dignità di asset finanziario da parte della generalità degli investitori. Tutti questi elementi contribuirono alla ripartenza del prezzo di questo asset che, a circa 6 mesi di distanza dal raggiungimento del minimo assoluto, raggiunse il valore di mercato di $13970 (+342.61%) il 26/6/2019

Il raggiungimento di questo massimo locale fu quindi seguito da un periodo di ritracciamento del prezzo che sembrava ripetere in rima lo stesso movimento "*dead cat bounce*" che aveva caratterizzato il post-2017: un

generale *downtrend* inframezzato da fasi repentine di apparente recupero annullate, con superiore intensità, da prosecuzioni ribassiste. Il culmine del *bear market* si ebbe il 12 Marzo 2020 proprio nella fase in cui l'emergenza sanitaria del COVID-19 assumeva i connotati di una crisi pandemica a livello globale: in quell'unica giornata il prezzo di Bitcoin crollò del 44%. La fase ribassista, iniziata nella fine di giugno 2019, si concluse il giorno seguente, con una contrazione complessiva del prezzo del 72,93%

Dal 13 Marzo 2020 ad oggi, 19 Aprile 2021, si è assiste ad un generale trend rialzista caratterizzato da una crescita esponenziale del prezzo, passato da $3782 a $57526 (+1421,04%), avendo superato il massimo assoluto di fine 2017 in data 30 Novembre 2020 e trovando un *all time high* di $64854.

I moventi di questa crescita esplosiva del prezzo sono da ricercare in parte dall'interesse nutrito da investitori istituzionali nel ricercare alternative profittevoli di investimento in una fase caratterizzata dal forte sanguinamento dell'economia reale, accomodando al tempo stesso le esigenze della propria clientela in un'offerta di strumenti finanziaria che coinvolga anche il mercato delle criptovalute, in parte (soprattutto a partire dalla seconda gamba rialzista del movimento), dall'inedito fenomeno di *meme-investing* che sta caratterizzando in maniera sempre più marcata il segmento *retail* dell'attività di investimento: esso si basa sull'assidua imitazione di operazioni di *trading* di breve periodo tra traders appartenenti a communities trasversali sui social network (Reddit e Twitter in particolar modo), concentrando in un breve intervallo temporale operazioni di acquisto spesso attivate dall'endorsement da parte di celebrità particolarmente popolari alle comunità online, come Elon Musk, considerato altresì fautore del successo e della popolarità della criptovaluta "Dogecoin", nata da un fork della blockchain di Litecoin nel dicembre 2013 ma diventata mainstream soltanto a partire da Gennaio 2021, registrando fino ad ora un incremento del 7840% sul suo valore di mercato .

Ad oggi la capitalizzazione totale di Bitcoin è di $1,026,062,593,153, figurando leader indiscussa nel panorama della criptovalute con una *dominance* pari al 51,13% dell'intera capitalizzazione del mercato delle criptovalute.

Per quanto riguarda l'analisi dei rendimenti di Bitcoin, come per le altre criptovalute ci si è basati sulle informazioni di prezzo ricavate da CoinMarketCap.com, piattaforma di riferimento nell'acquisizione di metriche finanziarie in ambito criptovalute, e fornite da Kaggle.com, scaricabili in formato .csv.

1.3.3 Analisi dei rendimenti di BTC

I rendimenti di bitcoin sono stai computati analizzando le chiusure delle candele di prezzo generate con frequenza giornaliera all'interno dell'intervallo temporale compreso tra il 29 Aprile 2013 ed il 27 Febbraio 2021, in modo tal da considerare all'interno dell'osservazione ogni fase che ha caratterizzato significativamente la storia del prezzo di questo asset.

Data la numerosità dei dati che compongono il campionamento dei rendimenti giornalieri, la distribuzione dei rendimenti è approssimabile ad una distribuzione normale avente una Media pari a 0,29% ed una Mediana pari a 0,19%. La varianza dei rendimenti è pari a 0,00181 e la deviazione standard è pari a 0,04249. Il rendimento massimo che si è osservato all'interno di un'unica giornata è stato del 42,97% il 18/11/2013 mentre il rendimento giornaliero peggiore è stato di -37,17% nella giornata del 12/3/2020 (dato leggermente diverso da quello individuato precedentemente poiché fornito da un provider diverso).

Assumendo un rendimento risk-free dello 0% come stabilito dalle ultime rilevazioni presenti sul sito di Kenneth French[12], L'indice di Sharpe, inteso come il rendimento per ciascuna unità di rischio dell'investimento e, analiticamente, definito dal rapporto tra l'excess return dell'asset di riferimento (rispetto al tasso risk free) e la deviazione standard dei suoi rendimenti, è pari allo 0,069. Il grado di asimmetria è piuttosto contenuto, pari a 0,26, mentre l'indice di Curtosi assume un valore particolarmente elevato e pari a 10,82, suggerendo una bassa verosimiglianza ad ottenere rendimenti giornalieri che si collocano lungo le code della distribuzione. Il value-at-risk (VaR), inteso come il "miglior rendimento nello scenario peggiore", ossia il rendimento riscontrato al quinto percentile, è pari a -6,11%, un valore molto distante rispetto al rendimento peggiore che è stato registrato in questo intervallo temporale. Al contrario, il novantacinquesimo percentile, che potrebbe essere definito come il "rendimento peggiore nello scenario migliore", assume un valore pari a 6,74%, quasi speculare al VaR. Il terzo quartile (settantacinquesimo percentile) ed il primo quartile (venticinquesimo percentile), che definiscono gli estremi della "scatola" del box plot, sono pari rispettivamente ad 1,85% e a -1,24%, confermando la notevole concentrazione dei valori intorno alla media definita dall'alto valore dell'indice di curtosi.

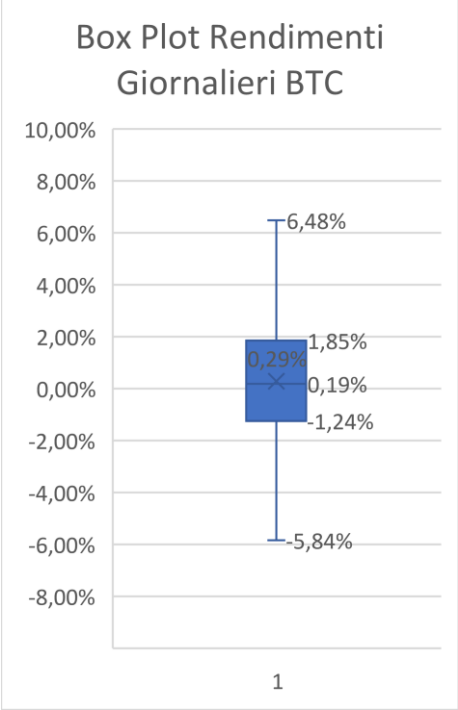


Figura 3: Box Plot Rendimenti Giornalieri BTC

[12] https://mba.tuck.dartmouth.edu/pages/faculty/ken.french/data_library.html

Per quanto riguarda i rendimenti settimanali invece, si riscontra una Media pari a 2.14% ed una Mediana pari a 0.73%. La varianza dei rendimenti è pari a 0.014823 e la deviazione standard è pari a 0.121751. Il rendimento massimo che si è osservato all'interno di un'unica settimana è stato del 105.43% nei giorni compresi tra l'11 ed il 18 Novembre 2013 mentre il rendimento settimanale peggiore è stato di -38.43% nella settimana compresa tra il 29 Gennaio 2018 ed il 5 Febbraio 2018 (proprio nel corso del primissimo grande "crollo" del prezzo). L'indice di Sharpe settimanale è pari allo 0,17. Il grado di asimmetria è suggerisce una coda destra più lunga della coda di sinsitra, con un valore pari a 1.83, mentre l'indice di Curtosi è particolarmente elevato come nel caso dei rendimenti giornalieri, assumendo un valore pari a 13.32. Il value-at-risk (VaR) è pari a -14.19%, mentre il novantacinquesimo percentile assume un valore pari a 23.14%. Il terzo quartile è pari a 6.82% mentre il primo quartile è pari a -4.42%

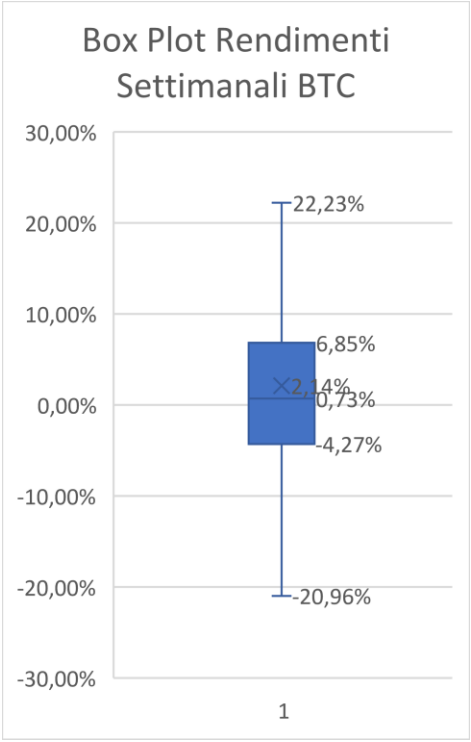


Figura 4: Box Plot Rendimenti Settimanali BTC

Infine, per quanto riguarda i rendimenti mensili, si riscontra una Media pari a 11.45% ed una Mediana pari a 5.27%. La varianza dei rendimenti è pari a 0.267164 e la deviazione standard è pari a 0.51687 . Il rendimento massimo che si è osservato all'interno di un unico mese è stato del 453.83% nei giorni compresi tra il 29 Ottobre 2013 ed il 29 Novembre 2013 mentre il rendimento mensile peggiore è stato di -34.36% nel mese compresa tra il 28 Ottobre 2018 ed il 28 Novembre 2018. L'indice di Sharpe mensile è pari allo 0,22. Il grado di asimmetria suggerisce una coda di destra molto più lunga della coda di sinistra, con un valore pari a 6.84, mentre l'indice di Curtosi è molto elevato assumendo un valore pari a 13.32, collocandosi a livelli particolarmente distanti rispetto ai rendimenti precedentemente analizzati. Il value-at-risk (VaR) è pari a -26.97%, mentre il novantacinquesimo percentile assume un valore pari a 54.13%. Il terzo quartile è pari a 22.01% mentre il primo quartile è pari a -4.42%

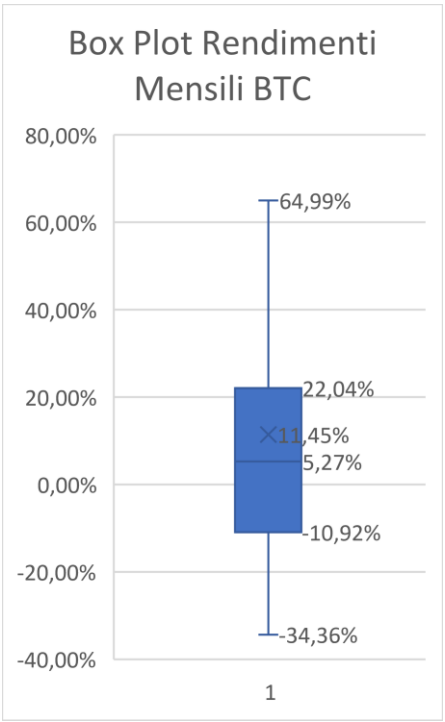
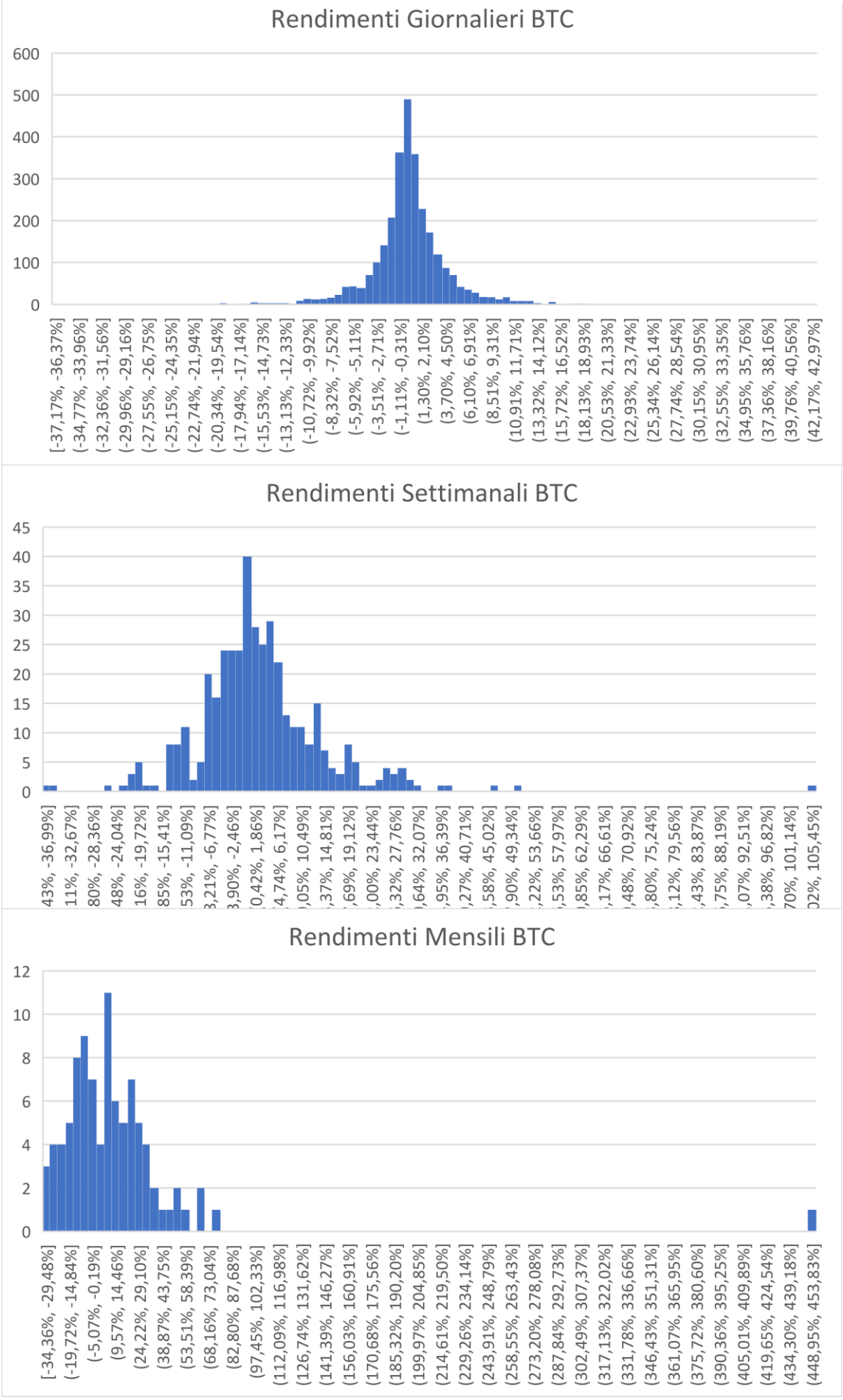


Figura 5: Box Plot Rendimenti Mensili BTC

Figura 6: Istogramma rendimenti BTC



1.4 Ether

1.4.1 Storia

Ethereum, dopo Bitcoin, è uno dei più storici progetti blockchain ancora in circolazione. Ad oggi, la capitalizzazione di mercato di un Ether (criptovaluta della blockchain "Ethereum") è pari a $262,058,745,496, seconda solo a Bitcoin, ricoprendo il 12.99% della capitalizzazione totale del mercato crypto. Ether viene considerata la principale criptovaluta di riferimento all'interno dello scenario delle "Altcoins" (indicando con esse l'insieme di criptovalute diverse da Bitcoin) essendo per altro la blockchain attualmente più utilizzata data la sua versatilità di impiego, seppur frenata da problemi di scalabilità di prossima risoluzione . La storia di Ethereum, diversamente da quella di Bitcoin, è particolarmente documentata in ragione della notorietà degli sviluppatori che hanno lavorato al progetto e per il fatto che la nascita di questa blockchain sia avvenuta a distanza di qualche anno dal rilascio del whitepaper di Bitcoin.

Nel 2013 il programmatore Vitalik Buterin, cofondatore della rivista "Bitcoin Magazine", realizza un documento, che diverrà il whitepaper di Ethereum[13], in cui, omaggiando l'idea avuta da Satoshi Nakamoto, dichiara che le possibilità di impiego della blockchain potessero andare ben aldilà di quelle di un semplice sistema di pagamento. Nel documento, Buterin ipotizzava che un'infrastruttura decentralizzata, scevra da qualsiasi rapporto fiduciario tra gli utenti che vi partecipavano, avrebbe permesso agli stessi di utilizzare asset digitali per la rappresentazione di valute e strumenti finanziari personalizzati, nonché della proprietà di dispositivi fisici sottostanti o di asset non fungibili (ad esempio i domini). L'utilità di tali "rappresentazioni" sarebbe emersa attraverso la programmazione nel linguaggio "Solidity" di applicazioni complesse su blockchain che, per mezzo di regole arbitrarie ma vincolanti (*smart contracts*), avrebbero definito la natura di questi *digital assets* e la loro circolazione.

1.4.2 Paradigma del valore

Pur omaggiando il meccanismo della PoW, utilizzato da Bitcoin, Buterin puntualizzava sul fatto che la partecipazione alla relativa blockchain fosse "libera" formalmente ma non sostanzialmente, dal momento che l'assenza di formali requisiti di partecipazione fosse sostituita dalla presenza di barriere economiche quantificate dalla capacità computazionale prestata al sistema, poiché solo a partire da essa l'algoritmo di consenso avrebbe determinato la rilevanza di ciascun nodo: in sostanza, nonostante tutti potessero entrare a far parte della rete "accedendo" un nodo con un semplice dispositivo dotato di processore, soltanto i dispositivi con processori più evoluti (e pertanto più costosi) sarebbero stati concretamente rilevanti nella determinazione del consenso della rete, mentre i nodi "più piccoli" ne sarebbero estati completamente esclusi. Per questo motivo, Buterin suggerì un sistema basato sulla PoS poiché, pur non eliminando completamente il problema delle barriere economiche, essa avrebbe definito un sistema in cui le risorse economiche investite sarebbero

[13] https://ethereum.org/en/whitepaper/

state efficacemente impiegate all'interno della rete anziché consumate inutilmente in corrente elettrica che comunque, pur garantendo la sicurezza della rete, non ne avrebbero fatto variare le opportunità di impiego.
Infatti, la Proof-of-Stake avrebbe permesso la realizzazione di un sistema che avrebbe incentivato i nodi validatori ad accumulare Ether, definendo così una domanda strutturale per tale criptovaluta (poiché è sulla base di essa che la blockchain avrebbe continuato ad operare) permettendo alla rete di adottare una "strategia monetaria" autopoietica e non-limitata da un tetto massimo di emissione (diversamente da Bitcoin per cui, come si è detto, è previsto un tetto massimo di emissione pari a 21.000.000 BTC). Infatti, oltre al movente transattivo e speculativo (entrambi comuni anche a Bitcoin, tipici dell'equazione keynesiana della domanda di moneta), la domanda di Ether sarebbe stata definita anche a partire da una componente strutturale e questo avrebbe coperto l'handicap dovuto all'assenza di un tetto di emissione, cementificando la fiducia nel valore di tale criptovaluta da parte dei nodi accumulatori ed utilizzatori. Pertanto, le funzioni di domanda di Bitcoin ed Ether possono essere confrontate nel modo seguente:

$$D(BTC) = D(transazioni) + D(speculazioni)$$

$$D(ETH) = D(transazioni) + D(speculazioni) + D(strutturale)$$

In sintesi, la Proof-of-Stake avrebbe reso possibile un'emissione periodica ma illimitata di criptovaluta combattendone l'inflazione attraverso le logiche di *staking*, garantendo alla stessa le funzioni di riserva ed accumulazione di valore. La domanda strutturale di Ether ne avrebbe permesso l'apprezzamento al crescere delle dimensioni della blockchain. Si pensi ad un nodo che ambisca a diventare validatore: le probabilità che esso "vinca" la validazione di un blocco sono direttamente proporzionali alla criptovaluta accumulata e messa in staking ma non in termini assoluti, bensì in termini relativi, ossia rispetto a quanta criptovaluta sia stata messa in *staking* dagli altri nodi;
Ipotizzando una quantità complessiva di criptovaluta pari ad N ed un numero generico di nodi validatori pari a n, se la criptovaluta fosse equamente distribuita tra questi, essi avrebbero le stesse opportunità di vincere la validazione del blocco secondo una probabilità approssimabile a $1/n$, poiché ciascun nodo sarà in possesso di N/n ETH. Ora, poiché la validazione del blocco impone l'emissione in somma fissa di criptovaluta pari a ΔN, indicando con esso il *coinbase reward*, accadrà che le probabilità di vincita del nodo che ha appena validato il blocco saranno superiori rispetto a prima (poiché egli sarà in possesso di $\frac{N}{n} + \Delta N$ ETH) e che, di riflesso, le probabilità di vittoria da parte degli altri blocchi saranno inferiori, poiché la criptovaluta che ciascuno di essi avrà messo in *staking* sarà relativamente inferiore rispetto a quella destinata dal nodo validatore vincitore, e con essa sarà inferiore la loro probabilità di vittoria: per mantenere quantomeno impareggiata la probabilità di vincita, gli altri nodi saranno costretti a domandare criptovaluta al nodo vincitore patendo la concorrenza sul prezzo da parte degli altri nodi e la posizione monopolistica del nodo che ha vinto la validazione: il risultato è un incremento del valor di mercato di ETH proprio per la pressione esercitata a livello strutturale da parte della

domanda. Affinché tutti i nodi mantengano inalterate e pari a $1/n$ le opportunità di vincita, è necessario che si siano concluse transazioni che abbiano portato ciascun nodo ad avere un ammontare pari a $\frac{(N+\Delta N)}{n}$ ETH. Ammettendo che il numero di nodi rimanga lo stesso e che la validazione di un blocco avvenga con periodo t, i nodi che intenderanno mantenere impareggiate le proprie opportunità di vincita dovranno possedere una quantità di Ether pari a $\frac{(N+t*\Delta N)}{n}$ (ad esempio, pensando che la validazione del secondo blocco coincida con l'inizio del secondo periodo, i nodi avranno le stesse opportunità di vincere la validazione del terzo blocco solo se ciascuno di essi avrà $\frac{(N+2\Delta N)}{n}$ ETH). Pertanto, un utente che al tempo t decide di diventare nodo validatore potrà ambire ad una probabilità di vincita pari a $\frac{1}{n+1}$ domandando una quantità di Ether pari a $\frac{(N+t*\Delta N)}{n+1}$ (ammesso che nel frattempo la distribuzione di criptovaluta rimanga costante tra gli altri nodi): questo rende evidente come l'ingresso di nuovi nodi faccia aumentare il prezzo di vendita dell'asset in qualità di "attori" della domanda strutturale poiché questi, per rendersi competitivi, dovranno domandare un quantità di criptovaluta tanto maggiore quanto maggiore sarà la finestra temporale in cui la domanderanno, ossia il periodo t, assumendo che il tasso di crescita dei nodi validatori sia costante. I benefici della PoS sono riscontrabili anche in ambito di sicurezza blockchain: infatti, richiamando il concetto del 51% attack, ossia una situazione in cui un nodo malevolo arrivi a possedere il 51% dell'ammontare complessivo della variabile su cui si gioca la competizione del mining, il nodo malevolo in questo caso sarebbe chiamato a possedere sistematicamente il 51% dell'ammontare di Ether complessivamente in circolo, considerando anche l'Ether di nuova e periodica emissione. Per quanto questa situazione possa già ritenersi inverosimile, bisogna riflettere anche sul fatto che il nodo malevolo non possa essere certo del risultato del proprio operato, poiché pur possedendo più della metà della criptovaluta in circolo, la probabilità di "vincere" la validazione del blocco rimarrebbe comunque inferiore ad uno.

La PoS quindi, oltre a garantire la sicurezza della rete, si rende anche servile per garantire la funzione di riserva di valore del "carburante" con cui la blockchain Ethereum si evolve, una funzione che nel caso della PoW non viene garantita dall'algoritmo di consenso bensì dalla sola "limited supply" della criptovaluta che si avrà in futuro, compensando l'assenza di una componente strutturale nella domanda di Bitcoin. Infine, è evidente come la Proof-of-Stake minimizzi l'impronta carbonica dell'attività di mining, almeno rispetto al protocollo PoW.

In ogni caso, nonostante il whitepaper di Ethereum si basi sulla Proof-of-Stake, il progetto Ethereum è nato utilizzando la PoW come algoritmo di consenso, e persiste nel suo utilizzo, nonostante sia prevista in futuro la transizione al protocollo Proof-of-Stake.

In ragione dell'opportunità di impiego della blockchain Ethereum, di gran lunga superiori a quelle di Bitcoin, ad oggi è la blockchain maggiormente utilizzata in assoluto per la realizzazione di piattaforme di finanza decentralizzata (DeFi), *Non-Fungible-Tokens* (NFT) e applicazioni decentralizzate in generale (dApps) che si

servono della blockchain tanto nell'archiviazione quanto nel funzionamento, dando vita a vere architetture *server-less*.

Il successo di questa rete è segnato soprattutto dal fatto che qualsiasi programmatore, imparando il linguaggio "Solidity", possa realizzare un'applicazione decentralizzata definendone gli standard di funzionamento attraverso la scrittura, ed il successivo *deploy sulla rete*, del relativo *smart contract* scritto nel linguaggio sopracitato, regolando poi il funzionamento dell'applicazione stessa per mezzo di "*transactions*" che richiamano le funzioni (*methods*) dello smart contract e che vengono eseguite per mezzo della validazione del blocco di transazioni a cui appartengono.

La popolarità di questa rete ne sta causando il congestionamento per il numero di transazioni che, all'interno del periodo, richiedono di essere validate, causando rallentamenti della rete e facendo emergere un problema generale di scalabilità.

Questo ha portato i nodi a competere tra loro per portare le proprie transazioni in cima alla lista delle *transactions* in attesa di essere validate da parte dei miners. La competizione si è iniziata a basare sul pagamento di commissioni (*gas fees*) agli stessi miners affinché le proprie transazioni vantino una "prelazione", rispetto alle altre, per la validazione. L'ammontare della commissione è variabile a seconda del grado di congestionamento della rete all'interno di un determinato arco di tempo infragiornaliero.

Ad oggi è impossibile eseguire una transazione su Ethereum senza il pagamento di *gas fees* estremamente significative, poiché la rinuncia del loro pagamento implica l'ancoraggio della propria transazione in fondo alla lista d'attesa di validazione, poiché ci saranno sempre nodi disposti a pagare commissioni facendo passare avanti le proprie transazioni, rimuovendo così anche il carattere privilegiato della commissione. Questo problema, intensificatosi particolarmente a partire dalla metà del 2020, è prossimo ad una possibile risoluzione per mezzo dell'aggiornamento della rete definito "Ethereum 2.0" o "Serenity" attraverso il quale avverranno notevoli cambiamenti, primo tra tutti il perfezionamento del passaggio alla Proof-of-Stake. Allo stato attuale la rete è in grado di sostenere 30 transazioni al secondo, ma con la realizzazione di un secondo *layer* sulla blockchain si arriverà ad una frequenza di 100.000 transazioni al secondo. Inoltre, a partire dall'aggiornamento imminente "EIP-1559", programmato per il 14 Luglio, parte delle *gas fees* spese per la validazione della transazione verranno distrutte anziché essere trasferite ai miners, creando uno schema deflazionistico che ne aumenterà il valore reale in maniera direttamente proporzionale all'utilizzo della rete. In questo senso si capisce la convenienza per i miners a promuovere questo aggiornamento, proprio perché la rinuncia di n-esime *gas fees* si tradurrebbe in un apprezzamento dell'asset da loro messo in staking (e comunque riscosso validando le transazioni) in ragione del maggiore utilizzo della blockchain e del rallentamento nella crescita della *total supply*, permettendo in altre parole di beneficiare del "valore attuale delle opportunità di crescita" del progetto Ethereum.

1.4.3 Evoluzione del prezzo di ETH

Di seguito si andrà analizzare l'evoluzione del prezzo di Ether nella coppia ETH/USDT (la coppia più liquida del mercato spot di e Ether) sulla base dei dati forniti dall'exchange Binance.com.

Il listing di Ether sulla piattaforma Binance avvenne il 17 Agosto 2017, diversi anni più tardi rispetto a quello di Bitcoin, ad un prezzo di $298. Come qualsiasi criptovaluta di quegli anni, il suo prezzo fu profondamente e positivamente condizionato dal rally rialzista di Bitcoin, essendo la criptovaluta di maggiore rilevanza in termini di capitalizzazione, soprattutto in quegli anni. Questo ha portato il prezzo di Ether ad estendersi fino al prezzo di $1440 (+383.22%) il 10 Gennaio 2018, circa un mese dopo il raggiungimento del picco da parte di Bitcoin

Successivamente si avviò la fase di ritracciamento di cui si è avuto modo di discutere analizzando il grafico di Bitcoin, arrivando al minimo assoluto di $82 (-94.29%) il 14/12/2018, esattamente un giorno prima rispetto al raggiungimento del minimo anche da parte di Bitcoin.

Quindi avvenne la ripresa fino al raggiungimento del massimo locale di $366 (+346.23%) in data 26 Giugno 2019, l'esatto giorno in cui anche Bitcoin raggiunse il picco.

In seguito, prese piede un movimento ribassista protratto fino al 13 marzo 2020, riportando così il prezzo a $86 (-76.55%): soltanto nella giornata precedente (12 marzo 2020), il prezzo perse il 48.42%, confermando l'esposizione del mondo crypto ai "cigni neri" dei mercati tradizionali.

Quindi, toccato il bottom, analogamente a Bitcoin fu avviato un ciclo rialzista attivo ancora oggi indirizzato al raggiungimento dell'*all-time-high* di $2543 (+2857.52%) il 15 Aprile 2021, dopo aver battuto il precedente massimo assoluto (quello di Gennaio 2018) il 2 Febbraio 2021

1.4.4 Analisi dei rendimenti di ETH

I rendimenti di Ether sono stati computati analizzando le chiusure delle candele di prezzo generate con frequenza giornaliera all'interno dell'intervallo temporale compreso tra l'8 Agosto 2015 ed il 27 Febbraio 2021, in modo tal da considerare all'interno dell'osservazione ogni fase che ha caratterizzato significativamente la storia del prezzo di questo asset.

Data la numerosità dei dati che compongono il campionamento dei rendimenti giornalieri, anche nel caso di Ether la distribuzione dei rendimenti è approssimabile ad una distribuzione normale avente una Media pari a 0,57% ed una Mediana pari a 0,04%. La varianza dei rendimenti è pari a 0,003956 e la deviazione standard è pari a 0,062896: pertanto, sotto il profilo giornaliero, Ether si rivela essere un asset più volatile di Bitcoin, compensando tale volatilità con un maggior rendimento medio. Il rendimento massimo che si è osservato all'interno di un'unica giornata è stato del 50.73% l'11 Agosto 2015 mentre il rendimento giornaliero peggiore è stato di -42.35% nella giornata del 12 Marzo 2020 (quando anche Bitcoin subì il peggior crollo storico).

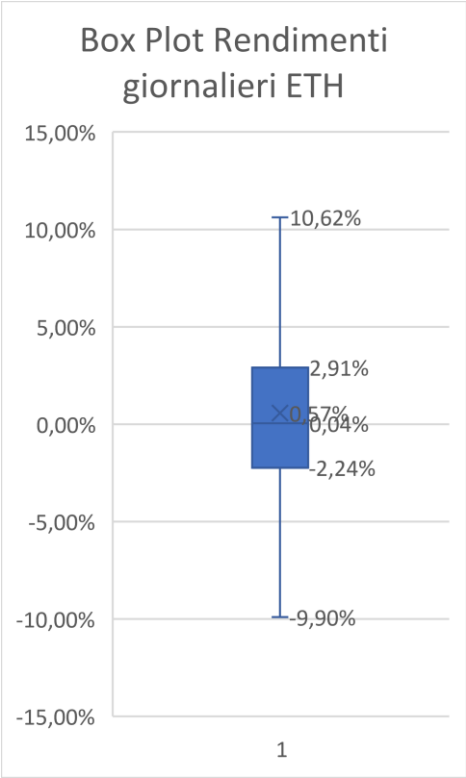


Figura 7: Box Plot Rendimenti Giornalieri ETH

Assumendo un rendimento risk-free dello 0% come stabilito dalle ultime rilevazioni presenti sul sito di Kenneth French, l'indice di Sharpe è pari allo 0.09, remunerando il rischio in maniera leggermente superiore rispetto a quanto fatto da Bitcoin. Il grado di asimmetria è leggermente più pronunciato rispetto a Bitcoin, assumendo un valore di 0.96, mentre l'indice di Curtosi assume un valore meno pronunciato rispetto all'altro asset e pari a 8.2, suggerendo comunque una bassa verosimiglianza ad ottenere rendimenti giornalieri che si collocano lungo le code della distribuzione.

Il value-at-risk (VaR) è pari a -8,17%. Al contrario, il novantacinquesimo percentile assume un valore pari a 10.84%, non esattamente speculare al VaR dato il valore positivo dell'asimmetria. Il terzo quartile ed il primo quartile sono pari rispettivamente a 2.91% e a -2.23%,.

Per quanto riguarda i rendimenti settimanali invece, si riscontra una Media pari a 4.24% (quasi il doppio rispetto a Bitcoin) ed una Mediana pari a 1.76%. La varianza dei rendimenti è pari a 0.03842 e la deviazione standard è pari a 0.196012. Il rendimento massimo che si è osservato all'interno di un'unica settimana è stato del 124.19% nei giorni compresi tra l'8 ed il 15 Agosto 2015 mentre il rendimento settimanale peggiore è stato di -48.16% nella settimana compresa tra il 7 Marzo 2020 ed il 14 Marzo 2020 (valore che risente molto del crollo avuto nella giornata del 12 Marzo). L'indice di Sharpe settimanale è pari allo 0,22. Il grado di asimmetria suggerisce una coda destra più lunga della coda di sinsitra, con un valore pari a 1.97, in maniera più pronunciata rispetto a quanto visto con la distribuzione dei rendimenti giornalieri. L'indice di curtosi assume un valore analogo a quello dei rendimenti giornalieri e paria 8.1559. Il value-at-risk (VaR) è pari a -19.24%, mentre il novantacinquesimo percentile assume un valore pari a 40.13%, molto superiore rispetto al valore assoluto del value at risk a causa dell'asimmetria positiva. Il terzo quartile è pari a 10.73% mentre il primo quartile è pari a -6.9%

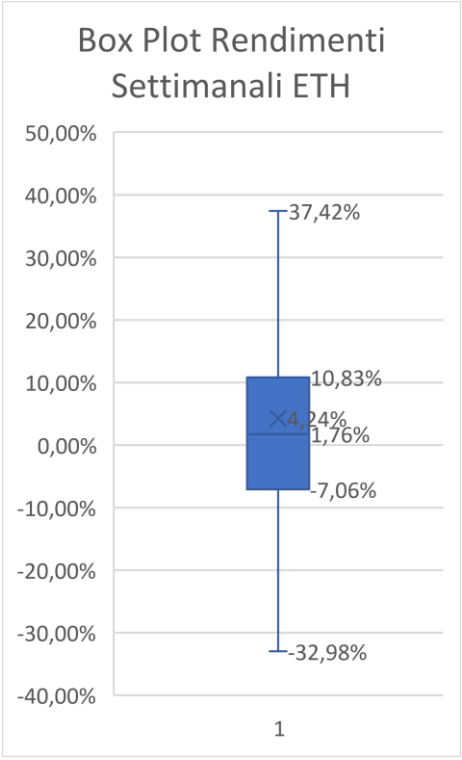


Figura 8: Box Plot Rendimenti Settimanali ETH

Infine, per quanto riguarda i rendimenti mensili, si riscontra una Media pari a 23.26% ed una Mediana pari a 2.55%. La varianza dei rendimenti è pari a 0.346865 e la deviazione standard è pari a 0.588952, confermando ancora una volta la natura più rischiosa, in termini di volatilità, di questo asset rispetto a Bitcoin. Il rendimento massimo che si è osservato all'interno di un unico mese è stato del 222.24% (valore inferiore rispetto al massimo rendimento mensile di Bitcoin, seppur riferiti ad un diverso orizzonte temporale) nei giorni compresi tra il 8 Gennaio 2016 e l'8 Febbraio 2016 mentre il rendimento mensile peggiore è stato di -56.58% nel mese compresa tra il 8 Novembre 2018 ed il 8 Dicembre 2018 (in maniera analoga a quanto accaduto a Bitcoin. L'indice di Sharpe mensile è pari allo 0,395.. Il grado di asimmetria è leggermente inferiore rispetto a quello dei rendimenti mensili assumendo un valore pari a 1.73, di gran lunga inferiore rispetto al valore ottenuto dall'analisi dei rendimenti in Bitcoin. Allo stesso modo, anche l'indice di Curtosi è significativamente inferiore rispetto ai rendimenti analizzati in precedenza, sia di questo asset che di Bitcoin, assumendo un valore pari a 2.99 e comunicando quindi una maggiore tendenza verso rendimenti

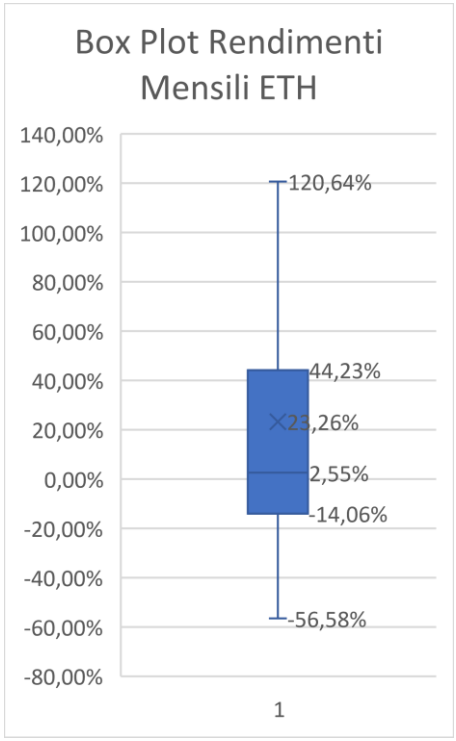
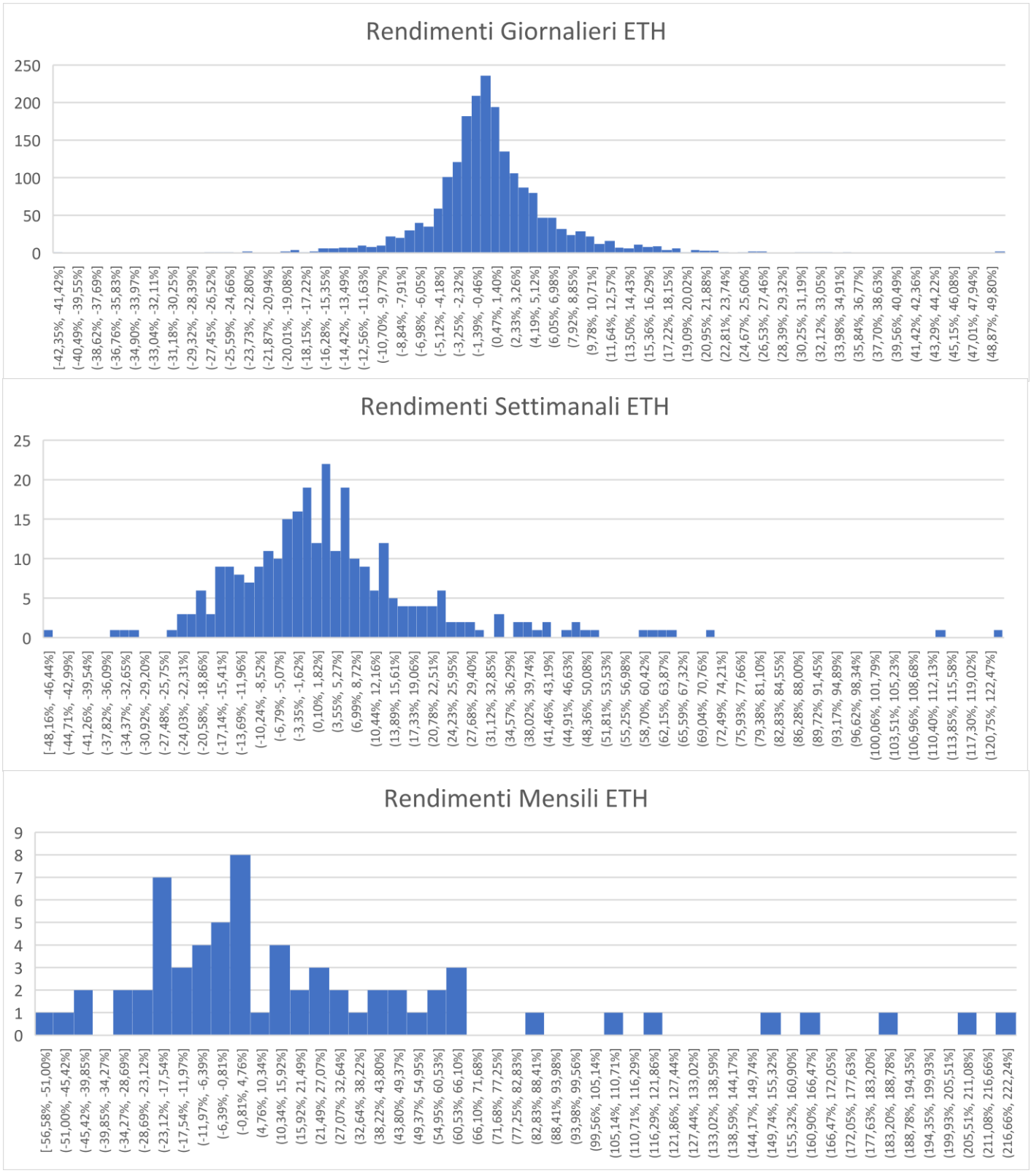


Figura 9: Box Plot Rendimenti Mensili ETH

disposti lungo le code della distribuzione. Il value-at-risk (VaR) è pari a -39.74%, mentre il novantacinquesimo percentile assume un valore pari a 162.53%. Il terzo quartile è pari a 43.48% mentre il primo quartile è pari a -13.94%

Figura 10: Istogramma rendimenti ETH



1.5 ChainLink

1.5.1 Funzioni di un "Oracolo"

ChainLink si colloca come uno dei progetti più recenti ma allo stesso tempo più promettenti in ambito blockchain. Il 4 settembre 2017 gli sviluppatori Steve Ellis, Ari Juels e Sergey Nazarov pubblicano il whitepaper di ChainLink[14], definendolo come una "rete di oracoli decentralizzata" (*decentralized oracle network*). L'idea nasce dalla consapevolezza di un problema strutturale: il fatto che, indipendentemente dal protocollo di consenso impiegato, le blockchains che supportano l'implementazione di *smart contracts* (come Ethereum) non siano nativamente idonee a leggere, interpretare e restituire dati da parte e verso sistemi esterni, come il mondo reale. Questa realtà sembrerebbe tradire in parte il potenziale applicativo della tecnologia blockchain, frenandone in maniera significativa le opportunità di impiego tanto nei settori tradizionali quanto nella vita di tutti i giorni. Si è detto infatti che le transazioni presenti sulla blockchains rispondano ad un insieme di "regole arbitrarie e vincolati" definite dallo *smart contract* a cui si riferiscono: tale "arbitrarietà", con cui ciascun sviluppatore realizza su blockchain il protocollo che preferisce, si espleta in un'esecuzione automatica delle transazioni, condizionata dal verificarsi o meno di determinati eventi previsti dal protocollo stesso.

Ad esempio, uno *smart contract* potrebbe regolare l'asta di un *digital collectible* (come un NFT) permettendo ad un nodo di firmare la transazione con cui possa "mettere in vendita" l'asset che preferisce, impedendogli momentaneamente di disporre dello stesso, raccogliendo quindi le proposte di acquisto avanzate dagli altri nodi entro un certo intervallo temporale: una volta scaduto il tempo, il miglior offerente firmerebbe digitalmente la transazione che, in maniera automatica, porterebbe contestualmente al trasferimento della somma a favore del venditore e dell'asset a favore del compratore. Si noti come in questo esempio l'esecuzione automatica della transazione di vendita risulterebbe condizionata dal verificarsi di tre condizioni chiave previste dallo smart contract a cui tale transazione si riferirebbe: 1) il termine del tempo previsto per la raccolta delle proposte di acquisto; 2) l'esistenza di almeno una proposta di acquisto superiore alle altre eventualmente avanzate; 3) la firma digitale dell'acquirente. È evidente come sia l'oggetto della transazione sia le condizioni che ne subordinano l'esecuzione siano necessariamente elementi nativi della rete: tuttavia, proprio per massimizzare l'arbitrarietà con cui si possa definire uno *smart contract*, si potrebbe desiderare che l'esecuzione di una transazione sia subordinata, ad esempio, al raggiungimento della parità tra dollaro ed euro, piuttosto che all'esito di una certa partita di calcio o di altro fenomeno qualitativamente rilevabile ed inconfutabilmente valutabile appartenente al mondo esterno.

La soluzione proposta dagli sviluppatori di ChainLink consiste nell'utilizzo di "*oracoli*", intendendo con essi qualsiasi entità che connette una rete deterministica, come la blockchain, a dati variabili provenienti da sistemi dinamici, come il mondo reale. Si tratta quindi di entità di confine, le Colonne d'Ercole che separano il mondo *on-chain* dal mondo *off-chain*, permettendo alla blockchain di connettersi con il mondo acquisendone i dati in

[14] https://link.smartcontract.com/whitepaper

un formato che possa interpretare ed è per questo motivo che un oracolo venga anche definito "*blockchain middleware*". Generalmente gli oracoli si servono di chiamate API per raccogliere i dati esterni da parte di *providers* che li forniscono, tuttavia è naturale avere perplessità in merito alla completezza e all'autenticità dei dati ottenuti in questo modo, soprattutto per il fatto che essi vengano impiegati in un ecosistema pensato proprio per azzerare la natura fiduciaria tanto dei rapporti quanto delle informazioni. I dati infatti provengono da fonti tipicamente centralizzate ed hanno bisogno di essere confermati e validati per poter essere impiegati in un mondo decentralizzato.

Questo problema è spesso definito "*oracle problem*"[15] e risolto da ChainLink attraverso un agile sistema di incentivi e di compliance reputazionale. Infatti, diversamente da semplici "porte" di ingresso delle informazioni all'interno della blockchain, ChainLink definisce una vera e propria "rete di confine", in cui ciascun nodo compete con gli altri per essere il miglior fornitore di informazioni. Chiunque può diventare un nodo "informatore" mettendo in *staking* una determinata quantità di token LINK (alla base della rete di ChainLink) dimostrando in questo modo la volontà di comunicare dati attendibili e completi, consapevole del fatto che, laddove venisse giudicato come un cattivo informatore da parte della rete, verrebbe escluso perdendo tutti i token messi in *staking* (fenomeno di *slashing*). Ogni volta che uno *smart contract* richiede l'accesso ad informazioni *off-chain*, è chiamato a pagare una piccola commissione in LINK che costituirà il premio per la fornitura di informazioni da parte dei nodi di confine. Quindi, l'algoritmo di consenso di ChainLink seleziona il nodo "informatore" facendo uno *screening* di tutti i nodi che offrono i dati richiesti dalla blockchain, scegliendo il nodo avente il maggiore "*score reputazionale*" determinato in base ai LINK messi in *staking* nonché sulla base della qualità delle informazioni storicamente trasmesse alla rete dal nodo in questione. Il nodo che vince la "competizione reputazionale" trasmette le informazioni allo smart contract che le richiede, ottenendo in cambio i LINK pagati come commissione. Nel caso in cui le informazioni trasmesse dovessero rivelarsi fallaci o incomplete, la rete diminuirebbe lo score reputazionale del nodo responsabile della loro trasmissione, estromettendolo dalla rete nel caso in cui tale punteggio si abbassi al di sotto di uno specifico valore soglia. Analogamente, la rimozione dei token LINK dallo *staking* porta ad un peggioramento dello *score reputazionale* facendone diminuire così le probabilità di "vincita della fornitura di informazioni", fino ad arrivare all'estromissione del nodo dalla rete nel caso in cui la quantità di token messi in staking sia inferiore al requisito minimo.

Per questo motivo, oltre che ad essere buoni informatori, ciascun nodo è incentivato ad accumulare LINK per fornire alla rete un *collateral* sulla qualità delle informazioni trasmesse, in modo tale da essere preferito nella selezione della loro fornitura e riscuotere in questo modo i token pagati in commissione. Come analizzato nel caso di Ethereum, il meccanismo di *staking* definisce una domanda strutturale per questo asset che ne costruisce il valore congiuntamente al movente transattivo e speculativo. Tuttavia, diversamente dai progetti analizzati in precedenza, LINK non è una criptovaluta nativa bensì un token presente sulla blockchain

[15] https://blog.chain.link/what-is-the-blockchain-oracle-problem/

Ethereum, basato sullo standard ERC-677. Il *listing* con denominazione in dollari di questo token presso Binance.com è particolarmente recente, avvenuto il 19 Gennaio 2019 ad un prezzo di $0.4586, ma l'evoluzione del suo prezzo è stata esponenziale in un trend costituito unicamente da minimi locali ascendenti, arrivando ad una quotazione attuale (22 Aprile 2021) di $40.9899 (+8838.72%)

1.5.2 Analisi dei rendimenti di LINK

I rendimenti di LINK sono stati computati analizzando le chiusure delle candele di prezzo generate con frequenza giornaliera all'interno dell'intervallo temporale compreso tra IL 21 Settembre 2017 ed il 27 Febbraio 2021.

Pur non godendo di un'elevata numerosità di rilevazioni, la distribuzione dei rendimenti giornalieri è comunque approssimabile ad una normale avente una Media pari a 0,71% ed una Mediana pari a -0,01%. La varianza dei rendimenti è pari a 0,006354 e la deviazione standard è pari a 0,079712. Il rendimento massimo che si è osservato all'interno di un'unica giornata è stato del 61.71% il 13 Giugno 2019 mentre il rendimento giornaliero peggiore è stato di -45.91% nella giornata del 12 Marzo 2020 (analogamente ad Ether e Bitcoin). Assumendo un rendimento risk-free dello 0% come stabilito dalle ultime rilevazioni presenti sul sito di Kenneth French, l'indice di Sharpe è pari allo 0.088842, remunerando il rischio in maniera leggermente inferiore rispetto ad Ethereum. Il grado di asimmetria è più pronunciato rispetto a Bitcoin ed Ethereum, assumendo un valore di 1.09, mentre l'indice di Curtosi assume un valore inferiore rispetto agli altri asset e pari a 7.294, suggerendo una discreta verosimiglianza ad ottenere rendimenti giornalieri che si collocano lungo le code della distribuzione.

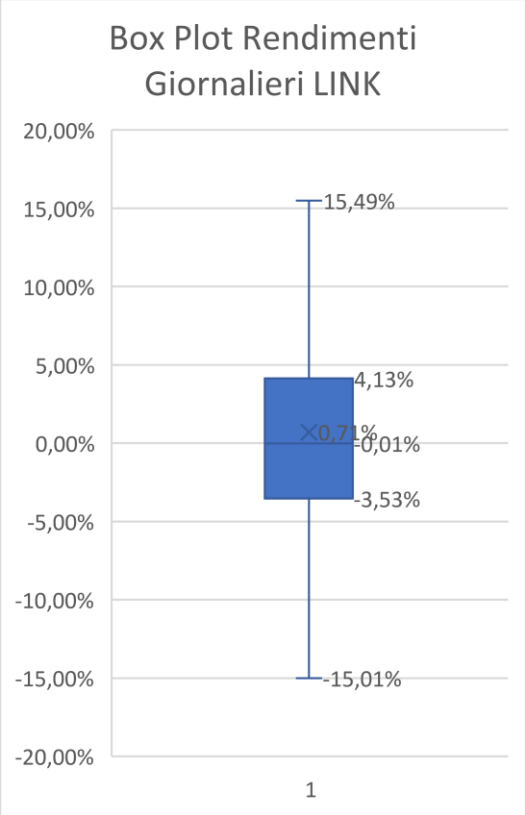


Figura 11: Box Plot Rendimenti Giornalieri LINK

Il value-at-risk (VaR) è pari a -10.33%. Al contrario, il novantacinquesimo percentile assume un valore pari a 13.74%, non esattamente speculare al VaR dato il valore positivo dell'asimmetria. Il terzo quartile ed il primo quartile sono pari rispettivamente a 4.12% e a -3.52%,

Per quanto riguarda i rendimenti settimanali invece, si riscontra una Media pari a 5.02% ed una Mediana pari a 2.18%. La varianza dei rendimenti è pari a 0.04819 e la deviazione standard è pari a 0.219522. Il rendimento massimo che si è osservato all'interno di un'unica settimana è stato del 94.27% nei giorni compresi tra il 28 Dicembre 2017 ed il 4 Gennaio 2018 (proprio quando Bitcoin iniziava il suo ciclo ribassista) mentre il rendimento settimanale peggiore è stato di -56.27% nella settimana compresa tra il 5 Marzo 2020 ed il 12 Marzo 2020 (valore che risente molto del crollo avuto nella giornata del 12 Marzo). L'indice di Sharpe settimanale è pari allo 0,22851. Il grado di asimmetria è pari a 0.862566. L'indice di curtosi assume un valore estremamente basso e pari a 1.771382, dovuto probabilmente alla povertà del numero di rilevazioni. Il value-at-risk (VaR) è pari a -24.51%, mentre il novantacinquesimo percentile assume un valore pari a 44.36%. Il terzo quartile è pari a 13.71% mentre il primo quartile è pari a -7.67%

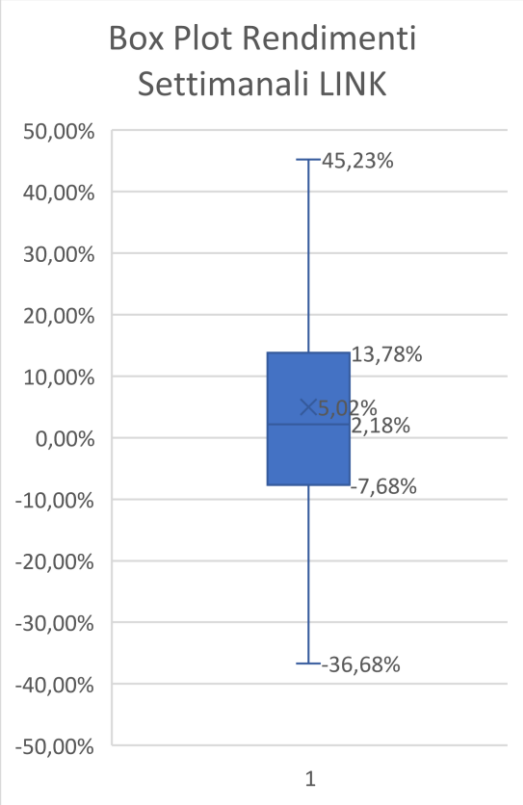


Figura 12: Box Plot Rendimenti Settimanali LINK

Infine, per quanto riguarda i rendimenti mensili, si riscontra una Media pari a 22.99% ed una Mediana pari a 10.31%. La varianza dei rendimenti è pari a 0.243343 e la deviazione standard è pari a 0.493298. Il rendimento massimo che si è osservato all'interno di un unico mese è stato del 173.78% nei giorni compresi tra il 21 Novembre ed il 21 Dicembre 2017 mentre il rendimento mensile peggiore è stato di -49.83% nel mese compreso tra il 21 Maggio 2018 ed il 21 Giugno 2018. L'indice di Sharpe mensile è pari allo 0.466. Il grado di asimmetria è pari a 0.95249. Anche in questo caso, l'indice di curtosi assume un valore particolarmente basso e pari a 1.006. Il value-at-risk (VaR) è pari a -38.67%, mentre il novantacinquesimo percentile assume un valore pari a 109.25%. Il terzo quartile è pari a 49.28% mentre il primo quartile è pari a -13.63%

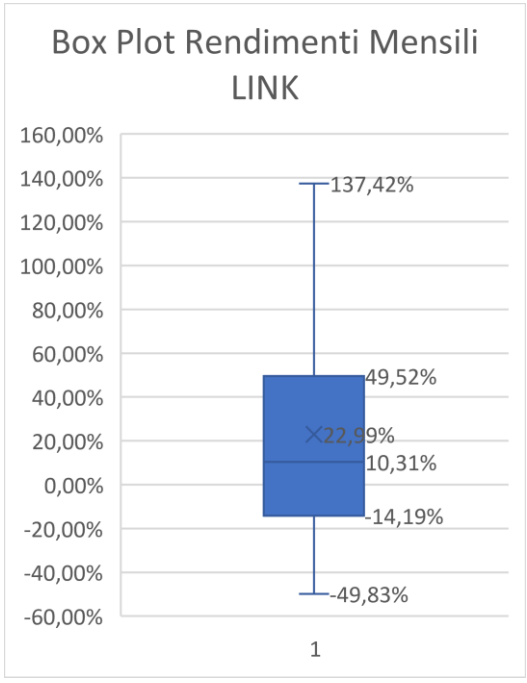
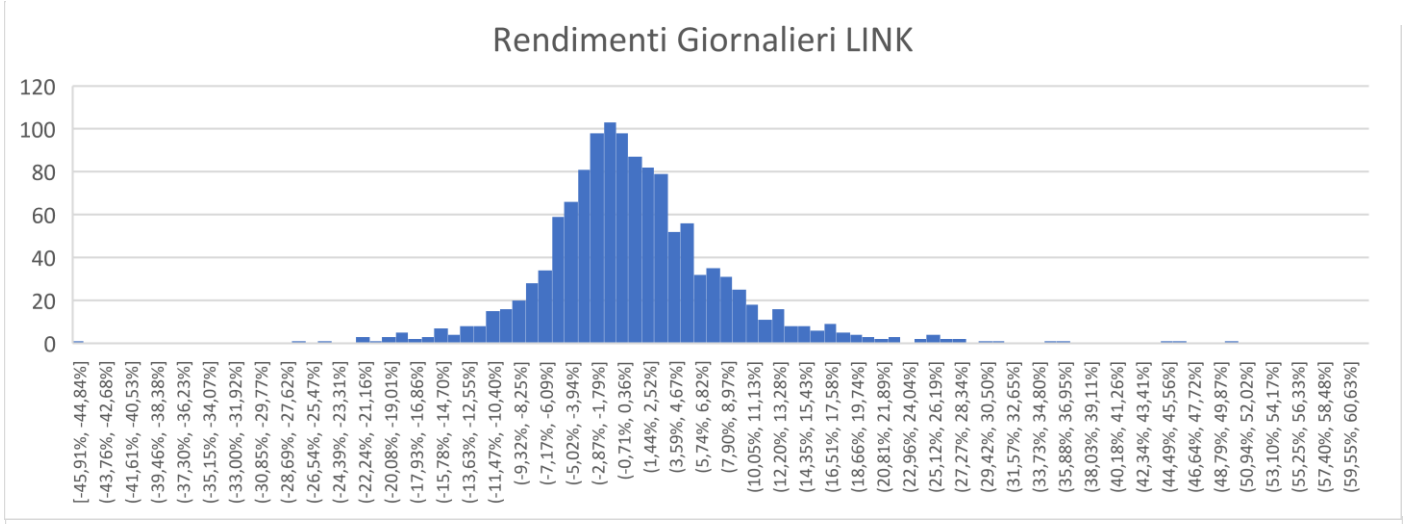
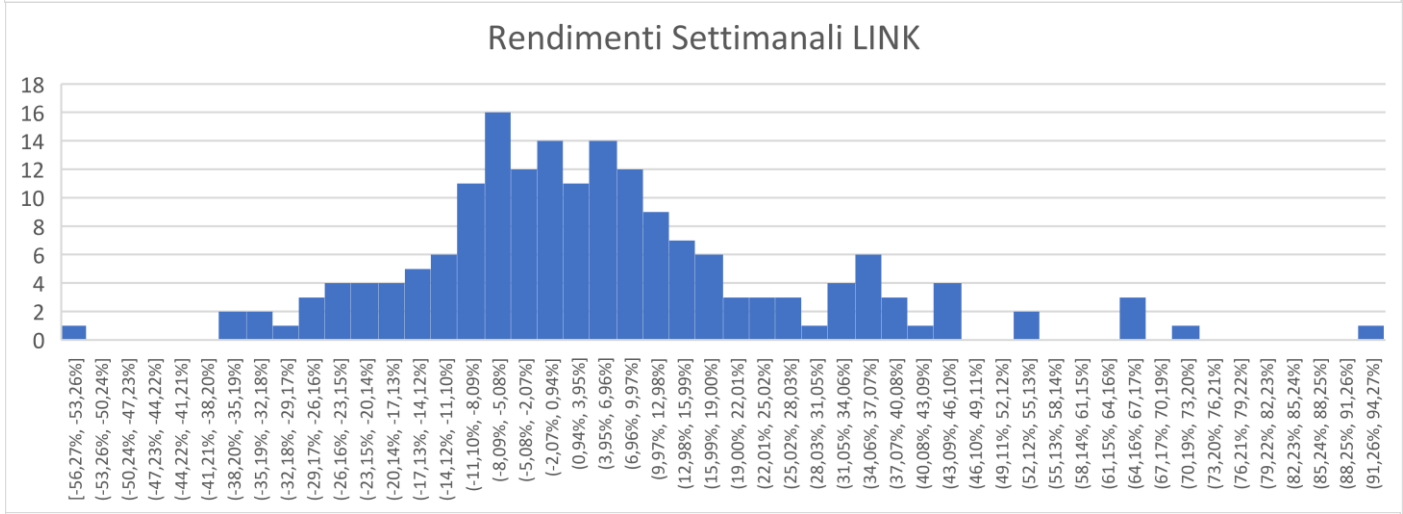
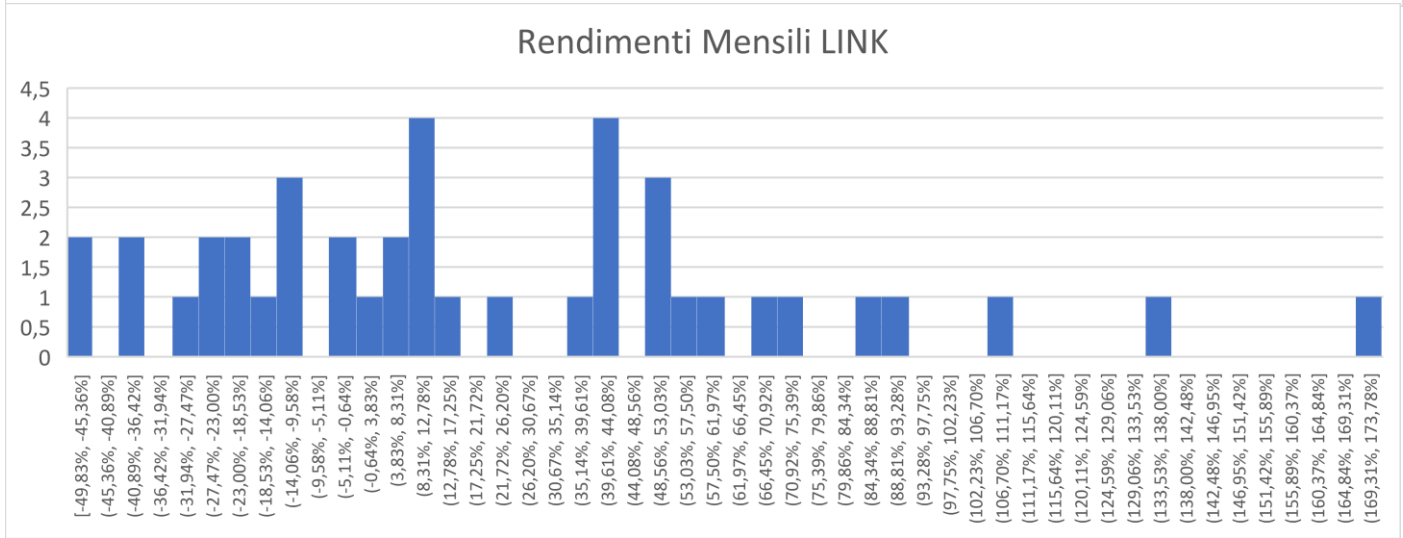


Figura 13: Box Plot Rendimenti Mensili LINK

Figura 14: Istogramma rendimenti LINK







1.6 Binance Coin

1.6.1 Storia

Anche Binance Coin è una criptovaluta relativamente più "giovane" rispetto a Bitcoin ed Ether, nata e sviluppatasi grazie all'endorsement di uno degli exchange attualmente più rilevanti nel mercato di negoziazione di questi strumenti: Binance.

Originariamente BNB nasce come un token ERC-20 presente sulla blockchain Ethereum ed emesso al pubblico per mezzo di una *Initial Coin Offering* (ICO) il 26 Giugno 2017, pochi giorni prima l'apertura dell'exchange. La quantità di token "coniata" inizialmente fu pari a 200.000.000, ma soltanto la metà fu offerta al pubblico permettendo ai sottoscriventi di scambiare 1 Ether per 2700 BNB o 1 Bitcoin per 20.000 BNB. Nonostante la divulgazione di questo asset sia avvenuta tramite ICO, BNB non rappresenta in alcun modo una *security* di Binance. Il protocollo di Binance Coin non prevede l'emissione di nuovi token ma, al contrario, Binance stessa si impegna ad acquistarli ed eliminarli periodicamente (destinandoli ad indirizzi cui sono state eliminate le chiavi private) attraverso eventi di "*burning*", in modo tale da aumentarne il valore nel tempo riducendone la "*total supply*" fino al raggiungimento di 100.000.000 di token (ad oggi il numero complessivo di BNB in circolo è di 153.432.897, quindi si attende una futura eliminazione del 33% dei token circolanti). Nell'Aprile del 2019 fu inaugurata la "Binance Chain" e con essa si verificò la migrazione dei token dal network Ethereum alla nuova Blockchain secondo uno *swap ratio* pari ad 1:1: pertanto la denominazione del protocollo di questo token passò dall'essere ERC-20 a BEP-2. La Binance Chain (BC), diversamente da quella di Ethereum e Bitcoin, è basata sull'algoritmo di consenso "Byzantine Fault Tolerance" (BFT) e l'attività di validazione delle transazioni sulla rete non prevede la remunerazione per mezzo di nuova criptovalute emessa, bensì la sola riscossione delle commissioni di transazione versate dai nodi. Successivamente, per superare limiti congeniti all'architettura della BC che ne avrebbero compromesso la scalabilità, fu inaugurata una blockchain parallela chiamata Binance Smart Chain (BSC)[16], attraverso la quale sarebbe stato possibile integrare *smart contracts* particolarmente complessi senza che ciò causasse congestionamenti della rete. Ad oggi, la BSC rappresenta un'alternativa particolarmente appetibile per gli sviluppatori di applicazioni decentralizzate, soprattutto a causa dell'attuale saturazione della blockchain Ethereum che persisterà almeno fino all'aggiornamento "Serenity".

I nodi hanno la possibilità di trasferire i token da una blockchain all'altra per mezzo di un servizio di *bridge* accessibile presso il dominio di *binance.org*. I token presenti sulla BSC presentano lo standard BEP-20 ed il protocollo di consenso impiegato è quello della Proof-of-Stake, permettendo a ciascun nodo di diventare validatore per mezzo dello *staking* di BNB. Le determinanti della domanda di BNB sono molteplici ed in parte associate all'attività dell'exchange Binance: indubbiamente vi è un movente transattivo legato all'utilizzo della BSC, in ragione del fatto che per realizzare una transazione su questa blockchain è necessario pagare una piccola *gas fee* in BNB essendo questo l'unico mezzo di remunerazione per i nodi validatori. Inoltre, come già

[16] https://academy.binance.com/it/articles/an-introduction-to-binance-smart-chain-bsc

analizzato con Ethereum e, in parte, con ChainLink, il meccanismo di staking definisce una componente strutturale per la domanda di questo asset. Infine, vi è sicuramente un movente speculativo dettato dall'evoluzione del suo prezzo e dal fatto che esso possa impiegato per beneficiare di vantaggi commerciali associati all'utilizzo dei servizi offerti da Binance, come ad esempio la scontistica del 25% sulle commissioni di negoziazione o il servizio di *cashback* utilizzando la "Binance Card" nei propri acquisti. La volontà di inserire il seguente token all'interno di questa argomentazione dipende indubbiamente dalla rilevanza che esso ha nell'ecosistema crypto, essendo terza per capitalizzazione ($75,993,332,612, pari al 4.27% della capitalizzazione totale), ma anche e soprattutto dal fatto che, pur non essendo una *security* propriamente detta, rimane comunque condizionata da dinamiche "aziendali" legate alla piattaforma privata Binance, poiché essa rientra inevitabilmente nel suo paradigma del valore (tanto per le scontistiche commerciali, quanto per l'attività di *burning* in cui assume indirettamente il ruolo di "garante" del suo valore).

Analogamente a ChainLink, la storia del prezzo di questo asset relativamente recente è caratterizzata minimi crescenti in un generale trend ascendente (+28860.44%), pur avendo presentato finestre ribassiste nel corso del 2018 e nella seconda metà del 2019. L'ultimo ciclo ribassista si è interrotto nell'Aprile del 2020, dopo il grande crollo di Marzo che ha caratterizzato il mondo crypto in generale, portando poi il valore ai massimi storici di $638 e alla quotazione odierna (23 Aprile 2021) di $505.87

1.6.2 Analisi dei rendimenti di BNB

I rendimenti di BNB sono stati computati analizzando le chiusure delle candele di prezzo generate con frequenza giornaliera all'interno dell'intervallo temporale compreso tra IL 26 Luglio 2017 ed il 27 Febbraio 2021.

Pur non godendo di un'elevata numerosità di rilevazioni, la distribuzione dei rendimenti giornalieri è comunque approssimabile ad una normale avente una Media pari a 0.87% ed una Mediana pari a 0.12%. La varianza dei rendimenti è pari a 0,006386 e la deviazione standard è pari a 0,079915. Il rendimento massimo che si è osservato all'interno di un'unica giornata è stato del 96.44% il 13 Agosto 2017 mentre il rendimento giornaliero peggiore è stato di -41.90% nella giornata del 12 Marzo 2020 (come nei casi precedentemente analizzati). Assumendo un rendimento risk-free dello 0% come stabilito dalle ultime rilevazioni presenti sul sito di Kenneth French, l'indice di Sharpe è pari allo 0.109246. Il grado di asimmetria assume un valore particolarmente elevato e pari a 3.011, mentre l'indice di Curtosi assume un valore estremamente alto e pari a 28.0233, suggerendo una bassissima verosimiglianza ad ottenere rendimenti giornalieri che si collocano lungo le code della distribuzione.

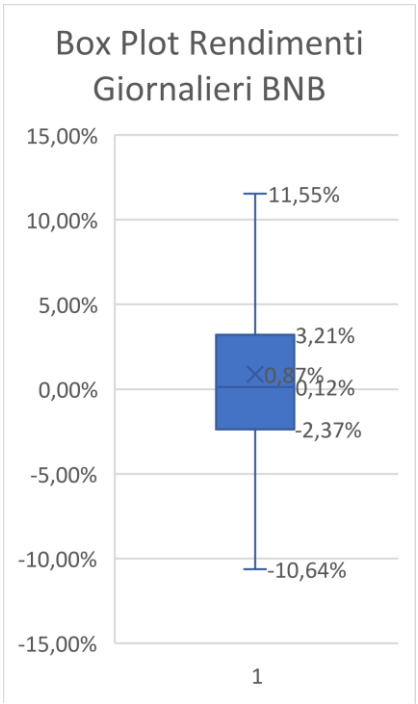


Figura 15: Box Plot Rendimenti Giornalieri BNB

Il value-at-risk (VaR) è pari a -8.18%. Al contrario, il novantacinquesimo percentile assume un valore pari a 11.9%. Il terzo quartile ed il primo quartile sono pari rispettivamente a 3.21% e a -2.36%.

Per quanto riguarda i rendimenti settimanali invece, si riscontra una Media pari a 8.10% ed una Mediana pari a 1.17%. La varianza dei rendimenti è pari a 0.185224 e la deviazione standard è pari a 0.430377. Il rendimento massimo che si è osservato all'interno di un'unica settimana è stato del 491.67% nei giorni compresi tra il 9 ed il 16 Gennaio 2017, mentre il rendimento settimanale peggiore è stato di -53.78% nella settimana compresa tra il 30 Agosto 2017 ed il 6 Settembre 2017. L'indice di Sharpe settimanale è pari allo 0,185224. Il grado di asimmetria è pari a 8.102. L'indice di curtosi assume un valore estremamente alto e pari a 85.97. Il value-at-risk (VaR) è pari a -18.25%, mentre il novantacinquesimo percentile assume un valore pari a 51.36%. Il terzo quartile è pari a 9.90% mentre il primo quartile è pari a -5.64%

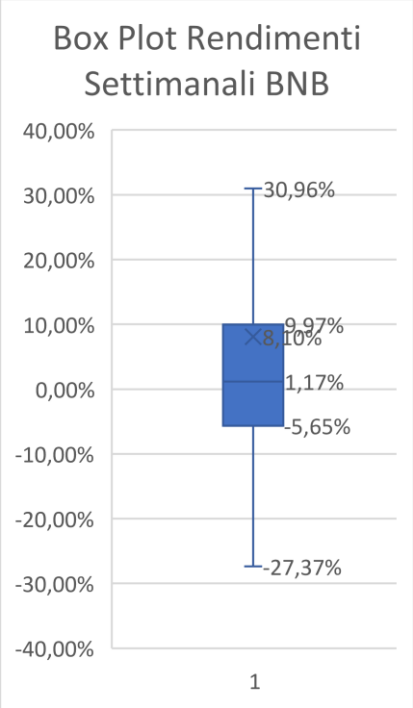


Figura 16: Box Plot Rendimenti Settimanali BNB

Infine, per quanto riguarda i rendimenti mensili, si riscontra una Media pari a 71.94% ed una Mediana pari a 15.97%. La varianza dei rendimenti è pari a 9.309 e la deviazione standard è pari a 3.0511. Il rendimento massimo che si è osservato all'interno di un unico mese è stato del 1963.35% nei giorni compresi tra il 26 Luglio ed il 26 Agosto 2017 mentre il rendimento mensile peggiore è stato di -60.32% nel mese compreso tra il 26 Agosto 2017 ed il 26 Settembre 2017. L'indice di Sharpe mensile è pari allo 0.2357. Il grado di asimmetria è pari a 5.79391. L'indice di curtosi assume un valore particolarmente alto e pari a 35.556. Il value-at-risk (VaR) è pari a -39.68%, mentre il novantacinquesimo percentile assume un valore pari a 355.68%. Il terzo quartile è pari a 28.29% mentre il primo quartile è pari a -9.69%

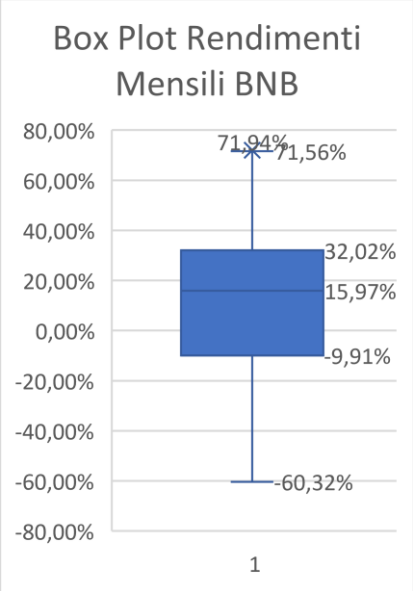
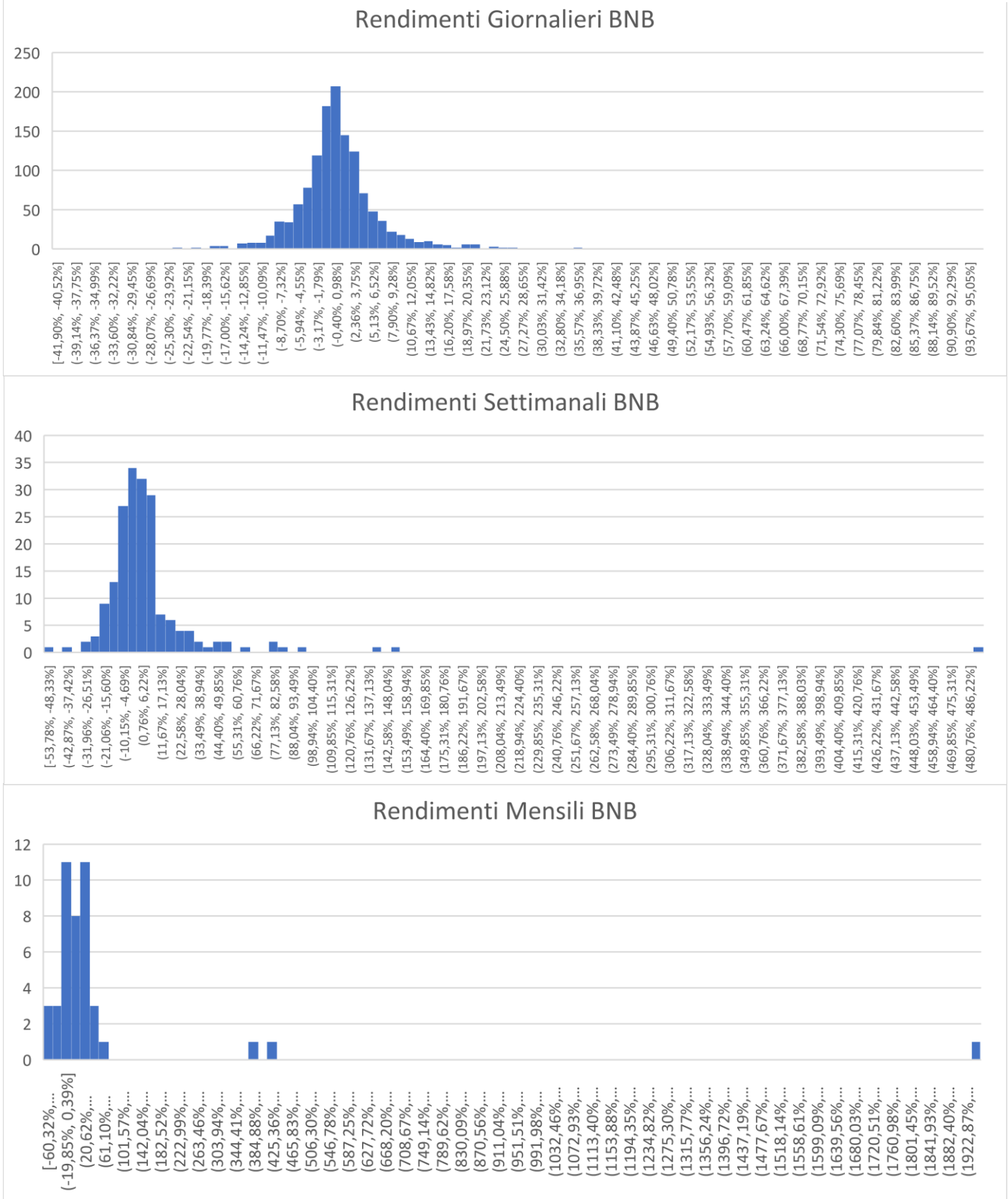


Figura 17: Box Plot Rendimenti Mensili BNB

Figura 18: Istogramma rendimenti BNB



1.7 Cardano

1.7.1 Principi

La quinta ed ultima criptovaluta analizzata in questa argomentazione è Cardano che, insieme a LINK e BNB, rappresenta un crypto-asset anagraficamente più giovane rispetto a ETH e BTC. La particolarità di Cardano è da ricercare nel modo in cui viene sviluppata secondo un approccio *"research-driven*", in base al quale informatici ed accademici collaborano arricchendone l'ecosistema mediante pubblicazioni scientifiche: per questo motivo non esiste un unico whitepaper di questo progetto, bensì un insieme di "*peer reviewed papers*" (i documenti presenti sul web che vengono presentanti come "whitepapers" non sono altro che fogli di sintesi dei testi sopracitati). Il progetto di questa criptovaluta nasce da un'idea di Charles Hoskinson, ex-collaboratore di Vitalik Buterin e co-fondatore di Ethereum. Dopo aver abbandonato lo sviluppo di Ethereum, Hoskinson fonda "IOHK", una società di *blockchain engineering* a scopo di lucro il cui business principale è lo sviluppo di Cardano, coadiuvata dalla società a scopo di lucro Emurgo e dall'ente no-profit Cardano Foundation. Queste tre persone giuridiche sono in possesso rispettivamente di 2.5 miliardi, 2.1 miliardi e 648 milioni della *total supply* di 45 miliardi di ADA. L'algoritmo di consenso di Cardano è la Proof-of-Stake e la sua blockchain si articola su due *layers*: uno riferito al sistema di pagamento (*Cardano Settlement Layer*) ed un altro riferito invece all'implementazione di *smart contracts* (*Cardano Computation Layer*). Sotto il punto di vista fondamentale e di potenzialità di impiego, la blockchain di Cardano non è eccessivamente lontana da quella di Ethereum, con la differenza che, allo stato attuale, essa sia molto più veloce nelle transazioni presentando bassissime *gas fees*. Tuttavia, quello che può sembrare un punto di forza, potrebbe essere inquadrato come un punto di debolezza strutturale a causa della bassa adozione di questa infrastruttura rispetto a quella di Ethereum, motivo per cui l'assenza di congestionamento sia in realtà interpretabile come carenza di utilizzo, almeno in termini relativi. Nonostante ciò, la popolarità di Cardano è dovuta soprattutto alle campagne promozionali avviate dai tre enti *endorser* del progetto, portando ad un potenziale accordo tra IOHK ed il governo etiope, che verrà delineato nei prossimi mesi, per l'implementazione della criptovaluta nell'economia del paese. Ad oggi Cardano figura come sesta criptovaluta per capitalzzazione ($36,163,715,750; par al 1.94% della capitalizzazione totale del mondo crypto.

La quotazione di Cardano avvenne ad un prezzo di $0.26546 Il 18 Aprile 2018 e fu da subito caratterizzato da una fase ribassista protratta nel complesso fino al 12 Marzo 2020, raggiungendo il minimo assoluto di $0.01771 (-93.33%). Successivamente però fu avviato quel ciclo rialzista che persiste ancora oggi, caratterizzato da una crescita parabolica che ha descritto l'andamento convesso del prezzo, portandolo ad una quotazione attuale di $1.11827 (+6235.78%), dopo aver superato il massimo storico precedente (vicino alla quotazione di partenza) il 3 Febbraio 2021.

1.7.2 Analisi dei rendimenti di ADA

I rendimenti di ADA sono stati computati analizzando le chiusure delle candele di prezzo generate con frequenza giornaliera all'interno dell'intervallo temporale compreso tra il 2 Ottobre 2017 ed il 27 Febbraio 2021.

La distribuzione dei rendimenti giornalieri è approssimabile ad una normale avente una Media pari a 0.62% ed una Mediana pari a 0.1%. La varianza dei rendimenti è pari a 0,007153 e la deviazione standard è pari a 0,084574. Il rendimento massimo che si è osservato all'interno di un'unica giornata è stato del 136.68% il 28 Novembre 2017 mentre il rendimento giornaliero peggiore è stato di -39.57% nella giornata del 12 Marzo 2020 (come nei casi precedentemente analizzati). Assumendo un rendimento risk-free dello 0% come stabilito dalle ultime rilevazioni presenti sul sito di Kenneth French, l'indice di Sharpe è pari allo 0.072785. Il grado di asimmetria assume un valore particolarmente elevato e pari a 5.27; anche l'indice di Curtosi assume un valore estremamente alto e pari a 70.2725, suggerendo una bassissima verosimiglianza ad ottenere rendimenti giornalieri che si collocano lungo le code della distribuzione. Il value-at-risk (VaR) è pari a -9.37%. Al contrario, il novantacinquesimo percentile assume un valore pari a 11.27%. Il terzo quartile ed il primo quartile sono pari rispettivamente a 3.25% e a -2.92%.

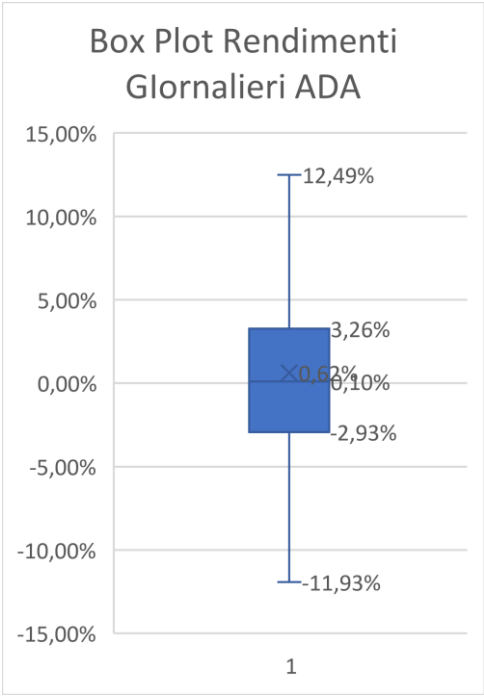


Figura 19: Box Plot Rendimenti Giornalieri ADA

Per quanto riguarda i rendimenti settimanali invece, si riscontra una Media pari a 5.17% ed una Mediana pari a -0.1%. La varianza dei rendimenti è pari a 0.109598 e la deviazione standard è pari a 0.331056. Il rendimento massimo che si è osservato all'interno di un'unica settimana è stato del 326.91% nei giorni compresi tra l'11 ed il 18 Dicembre 2018, mentre il rendimento settimanale peggiore è stato di -47.47% nella settimana compresa tra il 29 Gennaio 2018 ed il 5 Febbraio 2018. L'indice di Sharpe settimanale è pari allo 0,15614. Il grado di asimmetria è pari a 6.0217. L'indice di curtosi assume un valore estremamente alto e pari a 52.82. Il value-at-risk (VaR) è pari a -24.11%, mentre il novantacinquesimo percentile assume un valore pari a 36.94%. Il terzo quartile è pari a 12.29% mentre il primo quartile è pari a -8.89%

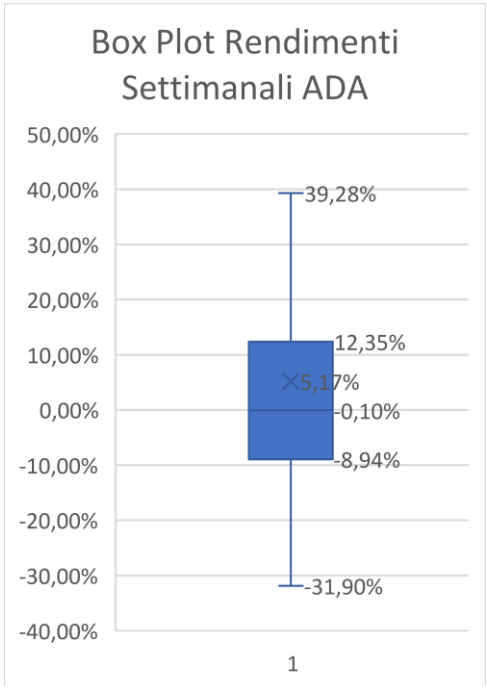


Figura 20: Box Plot Rendimenti Settimanali ADA

Infine, per quanto riguarda i rendimenti mensili, si riscontra una Media pari a 31.17% ed una Mediana pari a -12.63%. La varianza dei rendimenti è pari a 1.398 e la deviazione standard è pari a 1.182. Il rendimento massimo che si è osservato all'interno di un unico mese è stato del 521.19% nei giorni compresi tra il 2 Novembre ed il 2 Dicembre 2017 mentre il rendimento mensile peggiore è stato di -50.1% nel mese compreso tra il 2 Gennaio 2018 ed il 2 Febbraio 2018. L'indice di Sharpe mensile è pari allo 0.263577. Il grado di asimmetria è pari a 3.3259. L'indice di curtosi assume un valore pari a 11.74516. Il value-at-risk (VaR) è pari a -42.79%, mentre il novantacinquesimo percentile assume un valore pari a 157.8%. Il terzo quartile è pari a 41% mentre il primo quartile è pari a -20.88%

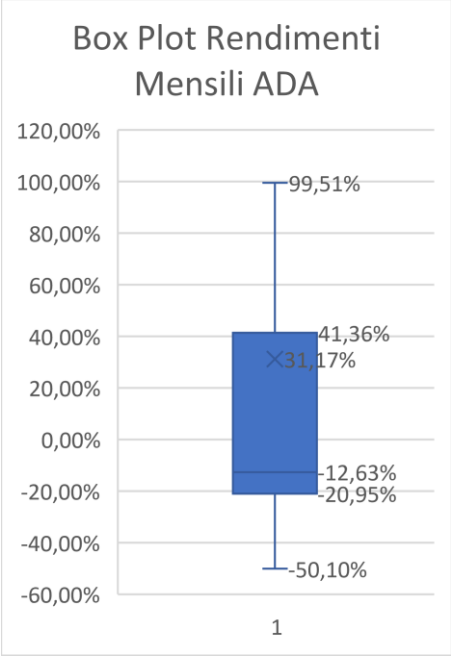
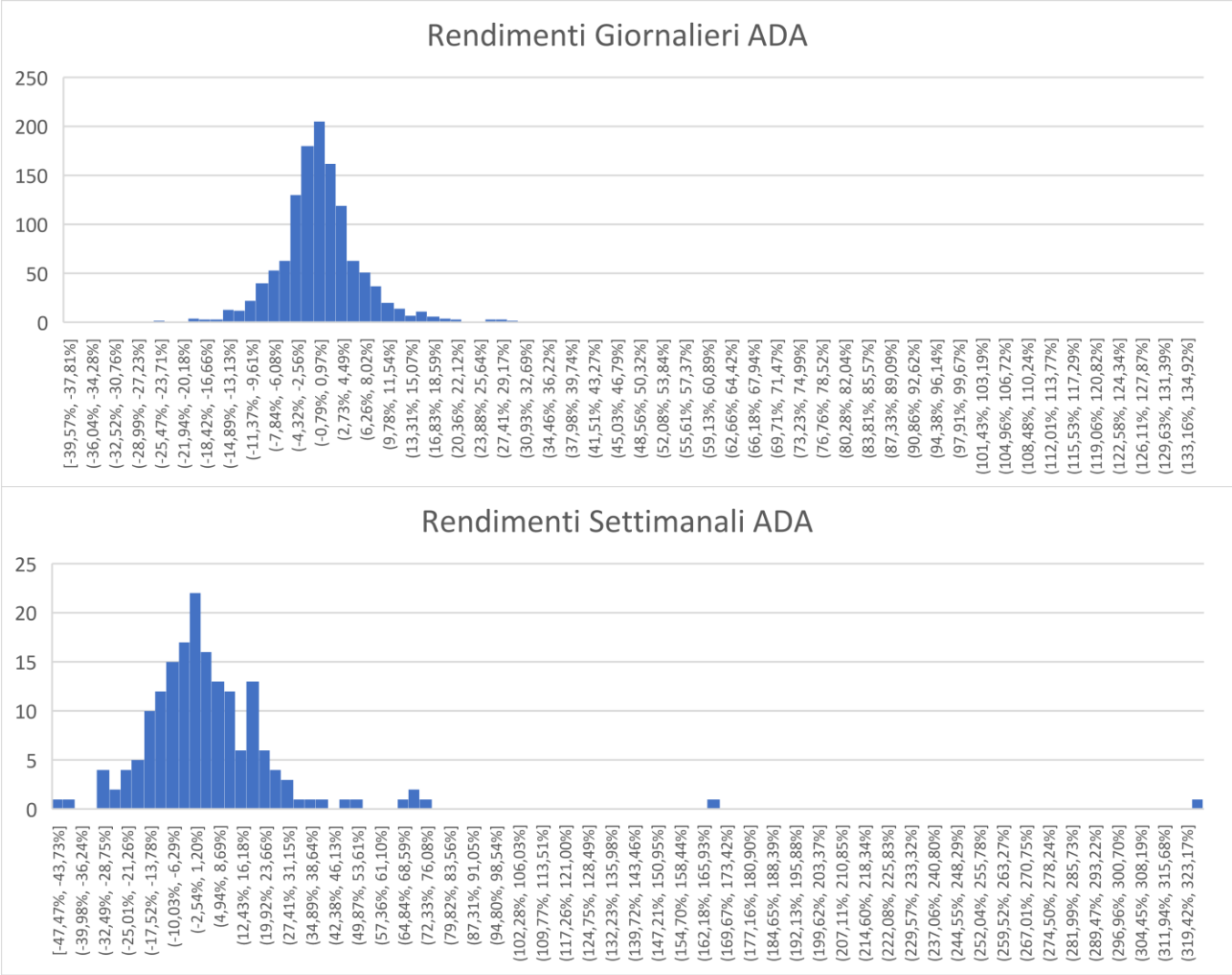


Figura 21: Box Plot Rendimenti Mensili ADA

Figura 22: Istogramma rendimenti ADA



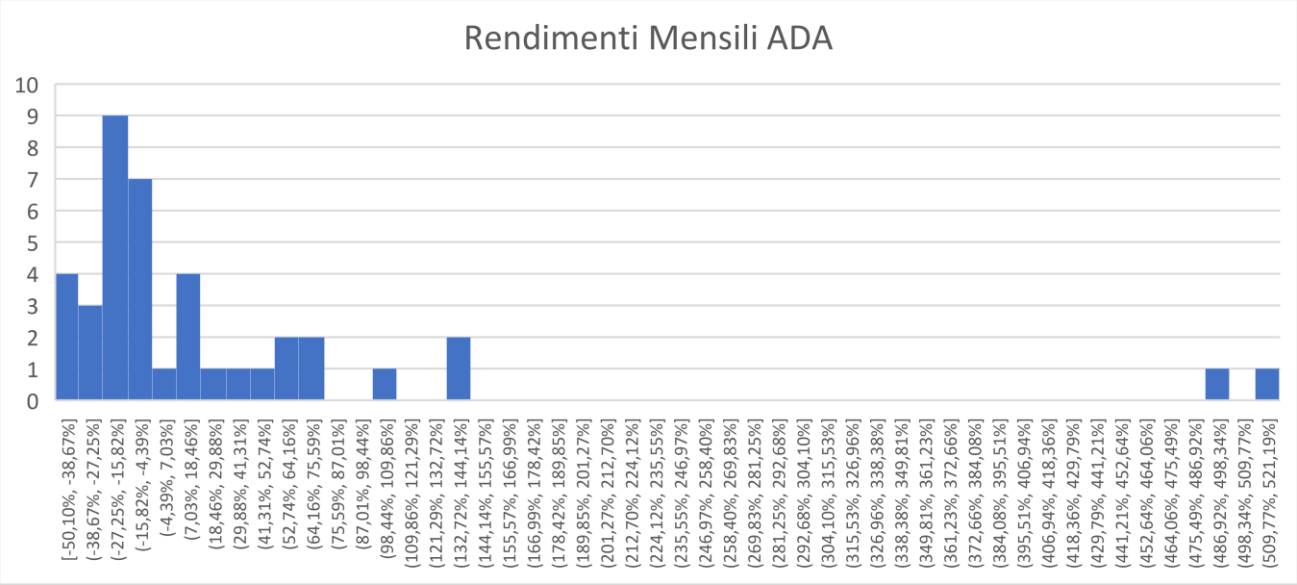


TABELLE DI SINTESI

RENDIMENTI GIORNALIERI					
	BTC	*ETH*	*ADA*	*BNB*	*LINK*
MEDIA	0,29%	0,57%	0,62%	0,87%	0,71%
R MAX	42,97%	50,73%	136,68%	96,44%	61,71%
R MIN	-37,17%	-42,35%	-39,57%	-41,90%	-45,91%
MEDIANA	0,19%	0,04%	0,10%	0,12%	-0,01%
DEV.ST	0,04249	0,06290	0,08457	0,07992	0,07971
VARIANZA	0,00181	0,00396	0,00715	0,00639	0,00635
SHARPE	6,88%	9,01%	7,28%	10,92%	8,88%
CURTOSI	10,82	8,20	70,27	28,02	7,29
ASIMMETRIA	0,26	0,93	5,28	3,01	1,09
VaR	-6,11%	-8,17%	-9,37%	-8,18%	-10,33%
95^ percentile	6,74%	10,84%	11,27%	11,90%	13,74%
Terzo Quartile	1,85%	2,91%	3,25%	3,21%	4,12%
Secondo Quartile	0,19%	0,04%	0,10%	0,12%	-0,01%
Primo Quartile	-1,24%	-2,23%	-2,92%	-2,36%	-3,52%
Primo Quintile	-1,78%	-2,97%	-3,72%	-3,17%	-4,45%
Secondo Quintile	-0,26%	-0,75%	-1,08%	-0,60%	-1,28%
Terzo Quintile	0,70%	0,89%	1,10%	1,18%	1,45%
Quarto Quintile	2,52%	3,94%	4,22%	3,91%	5,35%

Tabella 1: Analisi dei rendimenti giornalieri di BTC, ETH, ADA, BNB, LINK

RENDIMENTI SETTIMANALI					
	BTC	*ETH*	*ADA*	*BNB*	*LINK*
MEDIA	2,14%	4,24%	5,17%	8,10%	5,02%
R MAX	105,45%	124,19%	326,91%	491,67%	94,27%
R MIN	-38,43%	-48,16%	-47,47%	-53,78%	-56,27%
MEDIANA	0,73%	1,76%	-0,10%	1,17%	2,18%
DEV.ST	0,12175	0,19601	0,33106	0,43038	0,21952
VARIANZA	0,01482	0,03842	0,10960	0,18522	0,04819
SHARPE	17,54%	21,66%	15,61%	18,82%	22,85%
CURTOSI	13,32	8,16	52,82	85,98	1,77
ASIMMETRIA	1,83	1,97	6,02	8,10	0,86
VaR	-14,19%	-19,24%	-24,11%	-18,25%	-24,51%
95^ percentile	23,14%	40,13%	36,94%	51,36%	44,36%
Terzo Quartile	6,82%	10,73%	12,29%	9,90%	13,71%
Secondo Quartile	0,73%	1,76%	-0,10%	1,17%	2,18%
Primo Quartile	-4,24%	-6,90%	-8,89%	-5,64%	-7,67%
Primo Quintile	-5,67%	-9,50%	-11,39%	-8,10%	-10,82%
Secondo Quintile	-0,80%	-1,27%	-2,48%	-1,07%	-1,72%
Terzo Quintile	3,12%	4,53%	3,59%	4,54%	6,39%
Quarto Quintile	9,28%	13,23%	16,90%	11,62%	18,44%

Tabella 2: Analisi dei rendimenti settimanali di BTC, ETH, ADA, BNB, LINK

RENDIMENTI MENSILI					
	BTC	*ETH*	*ADA*	*BNB*	*LINK*
MEDIA	11,45%	23,26%	31,17%	71,94%	22,99%
R MAX	453,83%	222,24%	521,19%	1963,35%	173,78%
R MIN	-34,36%	-56,58%	-50,10%	-60,32%	-49,83%
MEDIANA	5,27%	2,55%	-12,63%	15,97%	10,31%
DEV.ST	0,51688	0,58895	1,18240	3,05114	0,49330
VARIANZA	0,26716	0,34686	1,39808	9,30944	0,24334
SHARPE	22,15%	39,50%	26,36%	23,58%	46,61%
CURTOSI	57,95	2,99	11,75	35,56	1,01
ASIMMETRIA	6,85	1,73	3,36	5,79	0,95
VaR	-26,97%	-39,74%	-42,79%	-39,68%	-38,67%
95^ percentile	54,13%	162,53%	157,80%	355,68%	109,25%
Terzo Quartile	22,01%	43,48%	41,00%	28,29%	49,28%
Secondo Quartile	5,27%	2,55%	-12,63%	15,97%	10,31%
Primo Quartile	-10,66%	-13,94%	-20,88%	-9,69%	-13,63%
Primo Quintile	-12,14%	-17,92%	-21,76%	-14,13%	-18,78%
Secondo Quintile	-1,98%	-1,30%	-14,78%	3,67%	4,75%
Terzo Quintile	10,91%	15,81%	2,70%	21,55%	39,31%
Quarto Quintile	25,46%	52,04%	54,93%	38,36%	53,03%

Tabella 3: Analisi dei rendimenti mensili di BTC, ETH, ADA, BNB, LINK

CAPITOLO 2

MODELLI FATTORIALI TRADIZIONALI

2.1 L'attenzione da parte degli istituzionali

Indipendentemente dai giudizi che si possono esprimere in merito all'inquadramento concettuale e regolatorio delle criptovalute, esse rappresentano a tutti gli effetti una categoria a sé stante di *asset finanziari*, rispetto ai quali, malgrado l'iniziale scetticismo, sta crescendo un notevole interesse da parte degli intermediari finanziari tradizionali, arricchendo lo spettro di attività accessibili alla negoziazione per la propria clientela. Morgan Stanley ad esempio, nel mese di Marzo 2021, è stata la prima grande banca di investimento ad abilitare la negoziazione di Bitcoin[17] ai clienti con almeno cinque milioni di dollari depositati da almeno sei mesi (concependo la criptovaluta come uno strumento adatto solo ad investitori caratterizzati da un'elevata tolleranza al rischio). Allo stesso modo, anche la banca di investimento JP. Morgan sta realizzando uno strumento finanziario finalizzato ad un investimento "indiretto" nel mercato delle criptovalute, accomodando in questo modo la domanda crescente della propria clientela istituzionale per avere un'esposizione all'interno di questo settore: lo strumento in questione prenderà il nome di "Cryptocurrency Exposure Basket"[18] e, sulla base del prospetto informativo inviato alla SEC, corrisponderà ad un titolo di debito il cui sottostante sarà costituito da azioni, presenti non nella stessa ponderazione, di undici società le cui attività economiche si riferiscono alla produzione di componenti hardware destinati al *mining* (Square, NVIDIA, Riot Blockchain, Advanced Micro Devices, Taiwan Semiconductor Manufacturing Complany Limited), piuttosto che operanti nell'ambito del sistema di pagamento (Paypal) oppure nell'offerta di servizi complementari in ambito finanziario e non (CME Group, Overstock.com, Intercontinental Exchange, Silvergate Capital Corporation, MicroStrategy). Infine, oltre alla possibilità di operare direttamente sul mercato delle criptovalute attraverso exchange centralizzati (come Binance, Huobi o FTX) o decentralizzati (come MDEX, Uniswap o Sushiswap), la clientela *retail* ha modo di investire in questo mercato servendosi dei tradizionali intermediari mobiliari negoziando strumenti finanziari ETC che riproducono passivamente l'andamento di una precisa criptovaluta (come BTCE[19] o ZETH[20], ancorati rispettivamente al prezzo di Bitcoin e di Ether).

Malgrado i segnali ancora prematuri e l'impossibilità di prevedere aprioristicamente l'orizzonte temporale entro cui si completerà, l'accettazione di Bitcoin e delle altre criptovalute in qualità di *asset classes* sembra essere un percorso inesorabilmente destinato alla loro ibridazione con gli strumenti finanziari tradizionali, verso la creazione di un unico ecosistema finanziario.

[17] https://www.cnbc.com/2021/03/17/bitcoin-morgan-stanley-is-the-first-big-us-bank-to-offer-wealthy-clients-access-to-bitcoin-funds.html

[18] https://www.sec.gov/Archives/edgar/data/0001665650/000121390021014247/s131027_424b2.html

[19] https://www.morningstar.it/it/etf/snapshot/snapshot.aspx?id=0P0001K5IC

[20] https://etc-group.com/it/products/ethetc/

In ragione di ciò, il pubblico degli investitori dovrebbe interrogarsi in merito all'adeguatezza dei tradizionali modelli di *pricing* impiegati nella stima di rendimenti delle criptovalute, oppure crearne nuovi nel caso in cui essi risultino insufficienti, il tutto al fine di trovarne un corretto collocamento nelle strategie di *asset allocation*.

2.2 Rischio sistematico e rischio idiosincratico

Tipicamente, tanto nella teoria di portafoglio quanto nei modelli fattoriali di *pricing*, ci si basa sul presupposto comune per cui la differenza di rendimento tra un qualsiasi asset ed il tasso privo di rischio (sia in termini di volatilità che di rischio emittente) costituisca la remunerazione aggiuntiva riconosciuta dal mercato soltanto in ragione di una componente di rischiosità indissolubilmente legata al sistema (o alla pluralità di sistemi) di cui il titolo stesso fa parte, un elemento che si rende ineliminabile anche in caso di strategie di investimento razionali. Questa componente è spesso definita come *rischio sistematico* (o rischio non diversificabile) ed è l'unica componente della rischiosità di un titolo che deve essere necessariamente patita dall'investitore. Al contrario, il complemento del rischio sistematico che, insieme ad esso, definisce la volatilità complessiva del titolo, prende il nome di *rischio idiosincratico* (spesso richiamato come rischio specifico o rischio diversificabile). Il rischio idiosincratico, diversamente da quello sistematico, si riferisce unicamente alla specificità del titolo in questione e può essere progressivamente eliminato inserendo il titolo all'interno di un portafoglio di altri asset, rispetto ai quali esso non è perfettamente correlato positivamente nei rendimenti. L'aggregazione di più titoli in un unico portafoglio ne definisce la composizione "genetica" di rendimento e rischio, poiché il rendimento sarà pari alla media ponderata dei rendimenti attesi dei titoli che lo comporranno, mentre il rischio godrà di questa proprietà lineare solo nel caso in cui i rendimenti di ciascun titolo siano perfettamente e positivamente correlati, ossia nel caso in cui il coefficiente di correlazione di ciascun titolo nei confronti degli altri sia costantemente pari a 1. Se invece, come è comune, la correlazione tra i rendimenti di più asset non è perfettamente positiva, la deviazione standard del portafoglio costituito da più titoli non perfettamente correlati risulterà inferiore rispetto alla media ponderata delle deviazioni standard di ciascun titolo. In tale differenza alberga *l'effetto diversificazione*, un fenomeno posto alla base del concetto di strategia razionale di investimento (postulando che tutti gli investitori abbiano funzioni di utilità avverse o neutrali al rischio), in ragione del fatto che la costruzione di portafogli diversificati permetta l'ottimizzazione del rapporto di rendimento e rischio (definita Sharpe Ratio), producendo maggiore utilità per gli investitori, soprattutto a causa del fatto che la mancata diversificazione implichi la sopportazione di una parte di rischio "inutile" poiché non remunerata dal mercato: la componente idiosincratica per l'appunto. In altre parole, un portafoglio efficacemente diversificato risulterà *più efficiente* di un portafoglio non-diversificato (o diversificato in maniera meno efficace a causa di una subottimale distribuzione delle ponderazioni dei titoli al suo interno) poiché riuscirà a produrre un maggiore rendimento a parità di volatilità, oppure perché riuscirà a produrre lo stesso rendimento con minore volatilità.

2.2.1 Derivazione dell'extra-rendimento di un generico titolo

L'equazione di extra-rendimento effettivo di un titolo (ossia il rendimento effettivo di un titolo che eccede il tasso privo di rischio) può essere descritta da tre componenti: una componente *epsilon*, il cui andamento è totalmente indipendente e approssimabile a quello di una variabile casuale con valore atteso nullo, e due componenti *alfa e beta*, entrambe riferite ai "sistemi" a cui lo stesso titolo appartiene: in altre parole, sia *alfa* che *beta* si riferiscono alla componente *sistematica* della natura del titolo, con la differenza che *beta* sia un coefficiente riferito all'andamento di una variabile benchmark x in grado di spiegare, seppur parzialmente, la natura sistematica del titolo, mentre *alfa* ne quantifica la componente che rimane ignota. Non a caso, infatti, si dice che *alfa* rappresenti l'*excess return* del titolo quando il fattore di rischio sistematico (tipicamente il mercato) è neutrale, ad esempio quando il premio al rischio di mercato è nullo e quindi il rendimento del mercato è esattamente pari al tasso privo di rischio

$$r_i - r_f = \alpha_i + \beta_i x + \varepsilon_i$$

Dopo aver costruito un dataset dei rendimenti effettivi del titolo, si potrà calcolare il suo rendimento atteso facendo il valore atteso dell'equazione di rendimento effettivo. Assumendo che i valori di beta e di alfa siano costanti, e ricordando che la componente epsilon abbia valore atteso nullo, si ottiene la seguente equazione

$$E[r_i - r_f] = \alpha_i + \beta_i E[x] + 0$$

La misura della varianza, metrica di statistica descrittiva che esprime la dispersione intorno alla media di un dataset, viene comunemente calcolata come il quadrato del valore atteso della distanza di ciascuna rilevazione dal valore atteso. Pertanto, la varianza degli extra-rendimenti di un titolo sarà pari al quadrato del valore atteso della differenza tra gli extra-rendimenti effettivi e l'extra-rendimento atteso

$$\sigma^2_{r_i - r_f} = E\left[r_i - r_f - E\left[r_i - r_f\right]\right]^2$$

$$\sigma^2_{r_i - r_f} = E[\alpha_i + \beta_i x + \varepsilon_i - (\alpha_i + \beta_i E[x] + 0)]^2$$

$$\sigma^2_{r_i - r_f} = E\left[\alpha_i + \beta_i x + \varepsilon_i - \alpha_i - \beta_i E[x]\right]^2$$

$$\sigma^2_{r_i - r_f} = E[\beta_i (x - E[x]) + \varepsilon_i]^2$$

$$\sigma^2_{r_i - r_f} = \beta_i^2 E\left[x - E[x]\right]^2 + E[\varepsilon_i]^2 + \left(2\beta_i E\left[x - E[x]\right] * E[\varepsilon_i]\right)$$

$$\sigma^2_{r_i - r_f} = \beta_i^2 E\left[x - E[x]\right]^2 + E[\varepsilon_i]^2 + 0$$

Ricordando che il valore atteso di epsilon sia nullo e che la varianza di una variabile possa essere espressa anche come la differenza tra il valore atteso del quadrato delle rilevazioni ed il quadrato del valore atteso

$$\sigma^2_{r_i - r_f} = \beta_i^2 E\left[x - E[x]\right]^2 + E\left[\varepsilon_i - E[\varepsilon_i]\right]^2$$

$$\boldsymbol{\sigma^2_{r_i - r_f} = \beta_i^2 \sigma_x^2 + \sigma_\varepsilon^2}$$

In questo modo si osserva come la variabilità degli extra-rendimenti di un titolo, ossia la volatilità misurata in termini di varianza, sia data dalla somma di due componenti: una componente sistematica, pari al prodotto tra il quadrato del coefficiente beta descritto nell'equazione di rendimento e la varianza della variabile benchmark descrittiva del sistema a cui il titolo si riferisce, ed una componente idiosincratica, pari alla varianza della variabile epsilon indipendente e tipica del titolo.

2.2.2 Derivazione dell'extra-rendimento di un portafoglio titoli

Estendendo il ragionamento alla dinamica di portafoglio, è possibile dimostrare il carattere eliminabile del rischio idiosincratico: nel caso in cui si realizzasse un portafoglio dato dall'aggregazione di *n* titoli, il suo extra-rendimento effettivo sarà pari alla media ponderata degli extra-rendimenti effettivi dei titoli che lo comporranno.

$$r_p - r_f = \frac{1}{n}\sum_{i=1}^{n} r_i - rf = \frac{1}{n}\sum_{i=1}^{n}[\alpha_i + \beta_i x + \varepsilon_i]$$

$$r_p - r_f = \frac{\sum \alpha_i}{n} + \frac{\sum \beta_i}{n}x + \frac{\sum \varepsilon_i}{n}$$

Indicando con $\bar{\alpha}$ e $\bar{\beta}$ rispettivamente i valori di alfa medio e beta medio (ottenuta dalla media ponderata dei rispettivi valori associati agli asset che compongono il portafoglio), si ottiene l'equazione di extra-rendimento effettivo del portafoglio

$$r_p - r_f = \bar{\alpha} + \bar{\beta}x + \frac{\sum \varepsilon_i}{n}$$

Quindi, il valore atteso dell'extra-rendimento di portafoglio sarà pari a

$$E\big[r_p - r_f\big] = E\left[\bar{\alpha} + \bar{\beta}x + \frac{\sum \varepsilon_i}{n}\right]$$

$$E\big[r_p - r_f\big] = \bar{\alpha} + \bar{\beta}E[x]$$

Pertanto, volendo misurare la varianza degli extra-rendimenti di portafoglio analogamente a quanto svolto per il calcolo della varianza degli extra-rendimenti del titolo:

$$\sigma^2_{r_p - r_f} = E\left[r_p - r_f - E\big[r_p - r_f\big]\right]^2$$

$$\sigma^2_{r_p - r_f} = E\left[\bar{\alpha} + \bar{\beta}x + \frac{\sum \varepsilon_i}{n} - \big(\bar{\alpha} + \bar{\beta}E[x]\big)\right]^2$$

$$\sigma^2_{r_p - r_f} = E\left[\bar{\alpha} + \bar{\beta}x + \frac{\sum \varepsilon_i}{n} - \bar{\alpha} - \bar{\beta}E[x]\right]^2$$

$$\sigma^2_{r_p - r_f} = E\left[\bar{\beta}(x - E[x]) + \frac{\sum \varepsilon_i}{n}\right]^2$$

$$\sigma^2_{r_p - r_f} = \bar{\beta}^2 E\big[x - E[x]\big]^2 + E\left[\frac{\sum \varepsilon_i}{n}\right]^2 + \left(2\bar{\beta}E\big[x - E[x]\big] * E\left[\frac{\sum \varepsilon_i}{n}\right]\right)$$

$$\sigma^2_{r_p-r_f} = \bar{\beta}^2 E\big[x - E[x]\big]^2 + E\left[\frac{\sum \varepsilon_i}{n}\right]^2 + 0$$

$$\sigma^2_{r_p-r_f} = \bar{\beta}^2 E\big[x - E[x]\big]^2 + \frac{1}{n^2} * E[\varepsilon_i + \varepsilon_{i+1} + \cdots + \varepsilon_n]^2$$

$$\sigma^2_{r_p-r_f} = \bar{\beta}^2 E\big[x - E[x]\big]^2 + \frac{1}{n^2} * E[n * \varepsilon_i]^2$$

$$\sigma^2_{r_p-r_f} = \bar{\beta}^2 E\big[x - E[x]\big]^2 + \frac{1}{n^2} * n * E[\varepsilon_i]^2$$

Ricordando ancora che il valore atteso di epsilon sia nullo

$$\sigma^2_{r_p-r_f} = \bar{\beta}^2 E\big[x - E[x]\big]^2 + \frac{1}{n} E\big[\varepsilon_i - E[\varepsilon_i]\big]^2$$

$$\boldsymbol{\sigma^2_{r_p-r_f} = \bar{\beta}^2 \sigma^2_x + \frac{\sigma^2_\varepsilon}{n}}$$

Si ottiene in definitiva l'equazione della varianza degli extra-rendimenti di portafoglio esplicitando, come nel caso del singolo titolo (ossia quando $n = 1$), sia la componente sistematica $\bar{\beta}^2\sigma^2_x$ che la componente idiosincratica $\frac{\sigma^2_\varepsilon}{n}$. Diversamente da quanto evidenziato dalla varianza del singolo titolo, la varianza di portafoglio rivela come essa sia marginalmente decrescente all'aumentare dei titoli inclusi nel portafoglio stesso, fino ad arrivare ad una situazione teorica per cui, costruendo un portafoglio di infiniti titoli, si verifichi la totale eliminazione del rischio idiosincratico, con la sopravvivenza del solo rischio sistematico che giustifichi interamente la volatilità degli extra-rendimenti di portafoglio

$$\lim_{n\to\infty} \sigma^2_{r_p-r_f} = \lim_{n\to\infty} \bar{\beta}^2\sigma^2_x + \frac{\sigma^2_\varepsilon}{n} = \boldsymbol{\bar{\beta}^2\sigma^2_x + 0}$$

2.3 CAPM

Tipicamente, con l'espressione "Portafoglio di Mercato" si fa riferimento a quel portafoglio inclusivo di tutti i titoli presenti sul mercato e caratterizzato quindi dalla massima diversificazione possibile. Pertanto, la componente idiosincratica del suo rischio è minimizzata e considerata nulla per ipotesi. In altre parole, la variabilità degli extra-rendimenti del portafoglio di mercato, espressa dalla sua varianza, è costituita unicamente dalla componente sistematica del rischio. Il portafoglio di mercato assume una rilevanza centrale nel Capital Asset Pricing Model (CAPM), un modello mono-fattoriale di *pricing* che inquadra gli extra-rendimenti del portafoglio di mercato come radice della natura sistematica del rischio di qualsiasi asset.

Il CAPM è solo uno dei diversi modelli fattoriali impiegati nella stima dei rendimenti degli asset e, di riflesso, del loro ipotetico *fair value*. L'esistenza di molteplici modelli ad n-fattori è giustificata dal fatto che gli investitori razionali considerino diverse composizioni *qualitative* e *quantitative* del rischio sistematico, composizioni che promettono di riflettere la complessità del sistema di riferimento. Questo giustifica l'inserimento, nelle equazioni di pricing, di un numero variabile di elementi eterogenei e potenzialmente epesegetici dell'aspetto sistematico degli asset analizzati.

Il CAPM, come anticipato, è un modello ad un unico fattore ideato da William Sharpe nel 1964. Esso è basato sul presupposto per cui la spiegazione del rischio sistematico di un qualsiasi asset si esaurisca attraverso l'osservazione degli extra-rendimenti del portafoglio di mercato. Il fondamento di tale modello può essere derivato analiticamente a partire dall'analisi della volatilità di un qualsiasi portafoglio, questa volta senza esplicitare l'equazione del rendimento effettivo ed atteso di ciascun titolo, ma solo del portafoglio.

2.3.1 Derivazione della varianza di un portafoglio titoli

Il rendimento effettivo di un portafoglio, come si è detto, è dato dalla media ponderata dei rendimenti effettivi di ciascun titolo di cui è composto; y_i rappresenta la quantità, in termini percentuali, dell'i-esimo titolo in portafoglio:

$$r_p = \sum_{i=1}^{n} y_i r_i$$

Analogamente, il valore atteso dei rendimenti del portafoglio sarà pari alla media ponderata dei rendimenti attesi di ciascun titolo

$$E[r_p] = \sum_{i=1}^{n} y_i E[r_i]$$

La varianza del portafoglio invece è pari a

$$\sigma_r^2 = E\left[r_p - E[r_p]\right]^2$$

$$\sigma_r^2 = E\left[\sum_{i=1}^{n} y_i r_i - \sum_{i=1}^{n} y_i E[r_i]\right]^2$$

$$\sigma_r^2 = E[y_i r_i + y_{i+1} r_{i+1} + \cdots + y_n r_n - y_i E[r_i] - y_{i+1} E[r_{i+1}] - \cdots - y_n E[r_n]]^2$$

Praticando il raccoglimento a fattor comune

$$\sigma_r^2 = E[y_i(r_i - E[r_i]) + y_{i+1}(r_{i+1} - E[r_{i+1}]) + \cdots + y_n(r_n - E[r_n])]^2$$

$$\sigma_r^2 = E[y_i(r_i - E[r_i]) + y_{i+1}(r_{i+1} - E[r_{i+1}]) + \cdots + y_n(r_n - E[r_n])] * E\left[r_p - E[r_p]\right]$$

Per mezzo della legge delle aspettative iterate, è possibile riunire i due valori attesi entro un unico valore atteso

$$\sigma_r^2 = E\left\{[y_i(r_i - E[r_i]) + y_{i+1}(r_{i+1} - E[r_{i+1}]) + \cdots + y_n(r_n - E[r_n])] * \left[r_p - E[r_p]\right]\right\}$$

$$\sigma_r^2 = E\left\{\left[\left(y_i(r_i - E[r_i])\left[r_p - E[r_p]\right]\right) + \left(y_{i+1}(r_{i+1} - E[r_{i+1}]) * \left[r_p - E[r_p]\right]\right) + \cdots + \left(y_n(r_n - E[r_n]) * \left[r_p - E[r_p]\right]\right)\right]\right\}$$

$$\sigma_r^2 = E\left[y_i(r_i - E[r_i]) * (r_p - E[r_p])\right] + E\left[y_{i+1}(r_{i+1} - E[r_{i+1}]) * (r_p - E[r_p])\right] + \cdots + E\left[y_n(r_n - E[r_n]) * (r_p - E[r_p])\right]$$

$$\sigma_r^2 = y_i * E\left[(r_i - E[r_i]) * (r_p - E[r_p])\right] + y_{i+1} E\left[(r_{i+1} - E[r_{i+1}]) * (r_p - E[r_p])\right] + \cdots + y_n E\left[(r_n - E[r_n]) * (r_p - E[r_p])\right]$$

Ma dal momento che il valore atteso del prodotto degli scarti tra due dataset è pari alla loro covarianza, si ottiene che la varianza di portafoglio sia data dalla media ponderata delle covarianza di ciascun asset con lo stesso

$$\boldsymbol{\sigma_r^2 = y_i \sigma_{i,r} + y_{i+1} \sigma_{i+1,r} + \cdots + y_n \sigma_{n,r}}$$

Pertanto, il 100% della volatilità di un portafoglio, sarà dato dalla somma delle quantità di ciascun titolo ponderata per il rapporto tra la covarianza dei rendimenti del titolo con il portafoglio e la varianza del portafoglio stesso. Questo è evidente normalizzando la funzione appena esplicitata.

$$1 = y_i \frac{\sigma_{i,r}}{\sigma_r^2} + y_{i+1} \frac{\sigma_{i+1,r}}{\sigma_r^2} + \cdots + y_n \frac{\sigma_{n,r}}{\sigma_r^2}$$

2.3.2 Il coefficiente beta e la security market line

Richiamando ancora una volta la definizione del portafoglio di mercato, si ottiene che la rischiosità di tale portafoglio sia data dalla somma della quantità relativa di ciascun titolo esistente ponderata per la covarianza dei suoi rendimenti con il portafoglio di mercato e rapportata alla varianza di quest'ultimo. In altre parole, $\frac{\sigma_{i,r}}{\sigma_r^2}$ rappresenta il contributo di rischio portato dall'i-esimo titolo presente sul mercato. Questo rapporto può essere definito "beta" intendendo per esso il coefficiente di sensibilità dei rendimenti dell'i-esimo titolo rispetto alle variazioni del rendimento del portafoglio di mercato

$$\boldsymbol{\beta_i = \frac{\sigma_{i,r}}{\sigma_r^2}}$$

In base ai valori assunti da beta, la reattività rispetto alle variazioni del rendimento del portafoglio di mercato sarà amplificata ($|\beta_i| > 1$), ridotta ($|\beta_i| < 1$) o nulla ($\beta_i = 0$) come nel caso del titolo risk-free. Ovviamente, il valore di beta può anche assumere valori negativi poiché tali valori possono essere assunti dalla covarianza (diversamente dalla varianza che è necessariamente positiva). Pertanto, in base al segno ed al valore assunto da beta, si potrà dedurre la natura e l'intensità della relazione tra un generico titolo ed il portafoglio di mercato, poiché il premio al rischio del rendimento atteso di quel titolo sarà necessariamente un coefficiente del premio al rischio del portafoglio di mercato

$$E[r_i] - r_f = \beta_i (E[r_r] - r_f)$$

Alla luce di questa equazione, è possibile ottenere un'equazione di *Pricing* di un qualsiasi asset in ragione della sua appartenenza teorica al portafoglio di mercato. L'equazione è derivabile da quella precedente semplicemente esplicitando il titolo risk free alla destra dell'equazione, ottenendo così la *security market line*. Pertanto, il sentiero rischio-rendimento del titolo (o, generalizzando, del portafoglio) sarà evidenziato da una retta avente inclinazione pari al premio al rischio del portafoglio di mercato, termine noto pari al tasso risk free, variabile indipendente pari a β_i attraverso il quale si potrà quantificare, almeno in termini relativi, la componente sistematica del rischio: laddove la relazione di rischio-rendimento venisse esplicitata ponendo sulle ascisse la deviazione standard anziché il beta, il rendimento osservato non risulterebbe quello autentico essendo condizionato dalla presenza della componente idiosincratica di rischio.

$$SML: E[r_i] = r_f + \beta_i(E[r_r] - r_f)$$

Ovviamente questa relazione è vera fintanto che la relazione tra l'andamento del titolo e del portafoglio di mercato sia esaustiva nel descrivere la semantica del rischio sistematico, e soprattutto fintanto che si collochi il titolo in un contesto di ottima diversificazione. Laddove non fosse così, allora vi sarebbe una componente del rischio sistematico che risulterebbe inspiegata e che verrebbe pertanto quantificata dal valore di alfa, mentre la componente idiosincratica del rischio del titolo in assenza di diversificazione verrebbe concretizzata dal valore di epsilon. Pertanto, l'equazione dell'extra-rendimento del generico titolo tornerebbe ad essere quella a partire dalla quale è stato dimostrato il discernimento tra rischio sistematico e rischio idiosincratico, con l'unica differenza che la variabile di benchmark x, impiegata nella spiegazione del sistema a cui il titolo appartiene, sarebbe costituita esattamente dal premio al rischio del portafoglio di mercato.

$$\boldsymbol{r_i - r_f = \alpha_i + \beta_i(r_r - r_f) + \varepsilon_i}$$

Mentre nella forma di extra-rendimento atteso, l'equazione sarà

$$\boldsymbol{E[r_f] - r_f = \alpha_i + \beta_i(E[r_r] - r_f)}$$

Pertanto, a livello grafico, l'equazione del premio al rischio del titolo corrisponderà alla retta di regressione avente α_i come termine noto (la parte del rischio sistematico che non viene spiegata dal modello fattoriale) e β_i come coefficiente angolare, trovando sulle ascisse il premio al rischio del portafoglio di mercato e sulle ordinate il premio al rischio del titolo.

2.3.3 Limiti del CAPM

I presupposti del CAPM, ossia quell'insieme di assunzioni che descrivono la legittimità e l'applicabilità del modello, si riferiscono ad elementi connotativi del mercato e degli investitori che vi operano. Sul versante del mercato, si suppongono diversi tratti tipici della concorrenza perfetta, ad esempio il fatto che il processo di determinazione dei prezzi abbia carattere esogeno, scevro dal condizionamento di taluni investitori caratterizzati da un maggiore "potere di mercato" (pertanto, si afferma che gli investitori siano "*price-takers*"), che il bagaglio informativo utile per l'analisi degli strumenti finanziari sia completo, veritiero, disponibile a tutti i decisori economici e che non esistano costi di transazione nelle negoziazioni né che i rendimenti degli investimenti vengano tassati. Sul versante egli investitori invece, si prevede che essi abbiano lo stesso orizzonte uniperiodale di investimento, che le aspettative siano omogenee, che essi si indebitino e prestino al tasso privo di rischio e che guidino la razionalità delle loro scelte di investimento secondo l'approccio media-varianza, cercando di ottimizzarne il rapporto.

Gli assunti teorici del CAPM rivelano quindi solo una parziale congruità del modello con le dinamiche concrete dei mercati finanziari, soprattutto a causa delle frizioni informative, transattive e fiscali tipiche del mondo finanziario, nonché dell'eterogeneità degli investitori sia in termini di dimensioni economiche, di

razionalità delle scelte e di orizzonti temporali di interesse. A questi elementi si aggiunge un'ulteriore criticità strutturale del CAPM, ossia il fatto che non esista un portafoglio di mercato propriamente detto, essendo questo approssimabile soltanto da indici che, per quanto diversificati, non possono tecnicamente raggiungere la massima diversificazione prevista per il portafoglio di mercato a causa dell'inevitabile esclusione di asset appartenenti alla vastità dei mercati finanziari: pertanto, malgrado la somiglianza, gli *index models* basati sull'utilizzo di un indice come *proxy* del portafoglio di mercato appaiono come semplici imitazioni del CAPM, non riuscendone a concretizzare i principi rigorosi.

Laddove gli assunti del CAPM fossero tutti verificati, non esisterebbero opportunità di investimento razionalmente appetibili diverse da quelle offerte dal portafoglio di mercato. Pertanto, in questo scenario, tutta l'attività di investimento convoglierebbe nell'unico portafoglio di mercato, e le strategie di investimento baserebbero la loro eterogeneità soltanto sulle diverse permutazioni di titolo privo di rischio e portafoglio di mercato, al fine di risultare coerenti con le avversioni al rischio degli investitori, ossia sulla loro diversa tolleranza alla volatilità sopportata nel corso dell'*holding period*. Questo renderebbe ingiustificate strategie attive di investimento a causa dell'impossibilità, attraverso queste, di produrre risultati più efficienti rispetto a quelli dalla ottenuti replicazione passiva del portafoglio di mercato. In sintesi, l'universo dei portafogli di investimento si svilupperebbe lungo la *capital market line*, ossia quella retta che, esplicitando rischio e rendimento in forma cartesiana, risulterebbe tangente alla curva del portafoglio di mercato e avrebbe come intercetta verticale il tasso privo di rischio: gli investitori caratterizzati da una maggiore avversione al rischio ricercherebbero combinazioni di investimento a sinistra del portafoglio ottimo (costituito dall'universalità di titoli rischiosi), costruendo così un portafoglio con beta inferiore a uno e caratterizzato dalla combinazione di portafoglio di mercato e prestiti erogati al tasso privo di rischio (in misura direttamente proporzionale alla riluttanza alla volatilità, al fine di minimizzare la deviazione standard del portafoglio); al contrario, investitori più propensi al rischio ricercherebbero portafogli alla destra del portafoglio ottimo di mercato, indebitandosi al tasso privo di rischio ed ottenendo così un quantitativo superiore del portafoglio di mercato, accettando così una maggiore volatilità remunerata in maniera lineare da un maggior rendimento. In estrema sintesi, pur accettando i limiti applicativi del modello, le intuizioni che esso suggerisce rimangono corrette: un approccio basato sulla diversificazione di investimento è sicuramente razionale e, alla luce di ciò, i modelli di *asset pricing* impiegati in mercati efficienti dovrebbero basarsi primariamente sull'esplicitazione delle determinanti del rischio sistematico.

2.4 Modelli multifattoriali

Sulla falsa riga del CAPM, come accennato in precedenza, si sono sviluppati modelli multifattoriali di rendimento che, per quanto eterogenei tra loro, partono dal presupposto comune per cui le performance di rendimento di qualsiasi asset siano funzione di numerosi fattori sistematici. Si potrebbe riassumere l'equazione generica di un modello ad n-fattori, in termini di rendimento effettivo e rendimento atteso, in questo modo

$$r_i = \alpha_i + \sum_{w=1}^{n} \beta_{xw} x_w + \varepsilon_i \qquad\qquad E[r_i] = \alpha_i + \sum_{w=1}^{n} \beta_{xw} x_w$$

In cui x_w rappresenta l'n-esimo fattore sistematico e β_{xw} il coefficiente che misura la reattività del rendimento studiato rispetto alla variazione unitaria dell'n-esimo fattore.

2.4.1 Il modello Fama-French a tre fattori

Il modello Fama-French a tre fattori[21] si propone come il modello multifattoriale più autorevole su questo argomento. Ideato negli anni '90 dai professori Eugene Fama e Kenneth French della "*University of Chicago Booth School of Business*", questo modello si propone come un estensione del CAPM e nasce dalla ricerca di una giustificazione "strutturale" dei rendimenti anomali riscontrati nel prezzo delle azioni a bassa capitalizzazione e delle *value stocks,* azioni caratterizzate da un alto valore contabile rispetto al valore di mercato. Il primo fenomeno, noto come "*small firm effect*", viene spesso citato dagli esponenti della tesi contraria all'ipotesi di mercato efficiente. In questo modello, diversamente dal CAPM, il rischio sistematico viene scomposto in tre fattori strutturali anziché in uno solo. Al *market risk factor,* presente anche nella migliore approssimazione del CAPM (ossia l'*index model*), si aggiungono il *size risk factor* ed il *value risk factor* al fine di trovare una spiegazione alle *outperformances* rispettivamente delle *small-cap stocks* contro le *large-cap stocks* e delle *value stocks* contro le *growth stocks*.

Il *size risk factor* viene richiamato attraverso la dicitura SMB, acronimo di "*Small Minus Big*", indicando che la variabile di rischio consista nella differenza tra il rendimento di un portafoglio di azioni a bassa capitalizzazione ed un portafoglio di azioni ad alta capitalizzazione; al contrario, il *value risk factor* viene identificato con HML, acronimo di "*High Minus Low*", indicando con esso la differenza di rendimento tra un portafoglio di *value stocks* (caratterizzate da un elevato valore del *book to market ratio*) ed un portafoglio di *growth stocks*. Pertanto, l'equazione di rendimento descritta dal modello Fama-French è funzione positiva di tre extra-rendimenti: il premio per il rischio di mercato, l'*excess return* delle azioni a bassa capitalizzazione (rispetto a quelle ad alta capitalizzazione) e l'*excess return* delle *value stocks* (rispetto alle *growth stocks*). In definitiva, il modello a tre fattori di Fama-French viene descritto, in termini di rendimento effettivo

$$r_i = r_f + \alpha_i + \beta_{MRKT} MRKT + \beta_{SMB} SMB + \beta_{HML} HML + \varepsilon_i$$

Quindi, in termini di rendimento atteso:

$$E[r_i] = r_f + \alpha_i + \beta_{MRKT} MRKT + \beta_{SMB} SMB + \beta_{HML} HML$$

I tre fattori di rischio sono calcolati periodicamente e pubblicati presso il sito web di Kenneth French, indicando con essi anche il tasso *risk free* del periodo considerato. È possibile quindi scaricare i dati storici

[21] https://en.wikipedia.org/wiki/Fama%E2%80%93French_three-factor_model

dei tre fattori e calcolarne i rispettivi beta eseguendo una regressione multipla con il dataset dei rendimenti dell'asset che si sta analizzando.

Il successo del modello a tre fattori rispetto all'*index model* appare evidente per diversi aspetti come, ad esempio, il migliore grado di spiegazione della volatilità dei rendimenti generalmente studiati, la percentuale inferiore di volatilità residua ed il valore inferiore di alfa. Questi elementi concorrono nel dimostrare come i fattori di rischio impiegati siano effettivamente epesegetici di parte del rischio sistematico che, nel caso del modello ad un unico fattore, rimaneva inspiegato.

2.4.2 Il modello Fama-French a cinque fattori

A partire dal 2015, il modello a tre fattori di Fama-French è stato ufficialmente esteso in un modello a cinque fattori, includendo due nuove componenti di rischio sistematico: il *profitability factor* e l'*investment factor*. Anche questi due fattori, analogamente agli altri, rappresentano degli extra-rendimenti: nel caso del *profitability factor*, indicato con RMW ("*Robust Minus Weak*"), esso corrisponde alla differenza di rendimento tra un portafoglio di azioni di società caratterizzate da una notevole profittabilità ed un portafoglio di azioni di società aventi una minore profittabilità; invece, per quanto riguarda l'*investment factor*, esso viene indicato con l'acrononimo CMA ("*Conservative Minus Aggressive*") e misura l'extra-rendimento delle azioni di società caratterizzate da politiche di investimento conservative rispetto ai rendimenti delle azioni di società caratterizzate da politiche di investimento particolarmente aggressive (in termini di allocazione delle risorse). Pertanto, l'equazione di rendimento effettivo del modello a cinque fattori di Fama-French è la seguente:

$$r_i = r_f + \alpha_i + \beta_{MRKT} MRKT + \beta_{SMB} SMB + \beta_{HML} HML + \beta_{RMW} RMW + \beta_{CMA} CMA + \varepsilon_i$$

Per il rendimento atteso, invece:

$$E[r_i] = r_f + \alpha_i + \beta_{MRKT} MRKT + \beta_{SMB} SMB + \beta_{HML} HML + \beta_{RMW} RMW + \beta_{CMA} CMA$$

Un ulteriore espansione del modello prevede l'ingresso di un sesto fattore di rischio associato alla presunta ricorsività (positiva o negativa) dei rendimenti di alcune azioni. Questo fattore di rischio, presente nel modello di Carhart a quattro fattori (nato a sua volta da un'espansione di quello a tre fattori di Fama-French), corrisponde al *momentum risk factor* e viene indicato con l'acronimo MOM: esso corrisponde alla differenza tra la media di rendimenti delle azioni meno performanti e la media dei rendimenti delle azioni più performanti, rallentata di un periodo. Questo modello ha incontrato diverse critiche per il carattere scarsamente significativo a livello generale di questo ulteriore elemento di rischio. In sintesi le equazioni di rendimento effettivo e atteso del modello a sei fattori di Fama-French sono:

$$r_i = r_f + \alpha_i + \beta_{MRKT} MRKT + \beta_{SMB} SMB + \beta_{HML} HML + \beta_{RMW} RMW + \beta_{CMA} CMA + \beta_{MOM} MOM + \varepsilon_i$$

$$E[r_i] = r_f + \alpha_i + \beta_{MRKT} MRKT + \beta_{SMB} SMB + \beta_{HML} HML + \beta_{RMW} RMW + \beta_{CMA} CMA + \beta_{MOM} MOM$$

CAPITOLO 3

MODELLI DI ASSET PRICING PER LE CRIPTOVALUTE

3.1 Metriche guida nella valutazione dei modelli fattoriali

I modelli multifattoriali evidenziati sinora appartengono all'analisi di *asset pricing* svolta per gli asset tradizionali. La definizione di un modello ad n-fattori dipende dallo svolgimento di un'analisi di regressione lineare (semplice o multipla a seconda del numero di fattori) in cui la variabile dipendente coincide con la successione dei rendimenti dell'asset su cui si intende applicare il modello, mentre le variabili indipendenti coincidono con le successioni di valori associate ai fattori considerati epesegetici del rischio sistematico.

3.1.1 R^2

Il modo migliore per stimare l'applicabilità di un modello ad n-fattori è quello di osservare la misura dell'R^2ed il grado di significatività statistica delle sue componenti: Infatti il valore di R^2 suggerirà la percentuale con cui il modello utilizzato sarà in grado di "spiegare" la variabilità dei rendimenti osservati, essendo questo il quadrato del coefficiente di correlazione (quest'ultimo detto anche "R multiplo") tra i rendimenti osservati e la successione di valori derivante dall'equazione di regressione. Alternativamente, assumendo una regressione lineare semplice, il valore di R^2 può essere ottenuto a partire dal rapporto tra la varianza descritta dal modello (pari appunto al prodotto tra la varianza della variabile indipendente ed il rispettivo quadrato del beta) e la varianza totale dei rendimenti dell'i-esimo asset considerato

$$R^2 = \frac{\beta_x^2 \sigma_x^2}{\sigma_i^2}$$

Il modello ad n-fattori si rende tanto più utile quanto maggiore è il valore assunto da R^2, poiché maggiore sarà la sua utilità nello spiegare la variabilità dei rendimenti considerati. I valori assunti da R^2 sono compresi nell'intervallo $[0,1]$: un valore nullo implica una totale decorrelazione tra i rendimenti e l'equazione di regressione, pertanto il modello sarà insufficiente nel suo scopo; al contrario, un valore pari a uno evidenzia la piena capacità del modello nel descrivere perfettamente la variabilità dei rendimenti analizzati (infatti questa situazione limite si verifica in presenza di perfetta correlazione, positiva o negativa che sia, quindi in presenza di un valore del coefficiente di correlazione pari a $\rho = 1$ e $\rho = -1$).

3.1.2 Test di ipotesi

Tuttavia, affinché un modello fattoriale si renda applicabile, è necessario anche che l'analisi di regressione produca risultati statisticamente consistenti ed apprezzabili. Per questo motivo, è necessario anche che l'*errore standard* dei coefficienti derivanti dall'analisi di regressioni siano ridotti, poiché soltanto in questo caso si potrà avere la ragionevole certezza che i rispettivi valori, ottenuti da un campione di dati, siano

sufficientemente vicini al loro valore atteso. A tal proposito, è necessario interrogarsi anche sul valore del *p-value* associato a ciascun coefficiente. In un test di ipotesi, fissando come ipotesi nulla H_0 l'assenza di correlazione tra i rendimenti analizzati e la successione di valori una certa variabile indipendente impiegata nella regressione, il *p-value* (p-valore) corrisponde all'evidenza a favore dell'ipotesi nulla. In altre parole, l'ipotesi nulla suppone sempre che ciascun coefficiente *beta* sia pari a zero ed il *p-value* rappresenta la probabilità di osservare il valore di beta, ottenuto dall'analisi di regressione, ammettendo che l'ipotesi nulla sia vera (ossia che effettivamente il beta sia nullo). Se questa probabilità è particolarmente remota, proprio perché il *p-value* assume un valore estremamente ridotto, allora è ragionevole pensare che l'ipotesi nulla sia falsa, poiché altrimenti l'osservazione del valore ottenuto dovrebbe rappresentare un caso particolarmente eccezionale. Quindi, fissata una certa probabilità associata al rischio di respingere l'ipotesi nulla quando essa in realtà è vera (commettendo così un errore statistico) e chiamando questa probabilità "livello di significatività" del test di ipotesi, se il *p-value* è inferiore al livello di significatività, ossia se la probabilità di osservare il beta ottenuto dalla regressione, assumendo che in realtà il beta sia pari a zero, è inferiore alla probabilità associata al rischio di sbagliare affermando che il beta sia in realtà diverso da zero, allora bisognerà rigettare l'ipotesi nulla ed affermare che il beta ottenuto dalla regressione sia statisticamente significativo per quel livello di significatività. Pertanto, il testi di ipotesi in questo caso assume natura bilaterale e dipendendo da un campionamento sarà di tipo t-test. Il test di ipotesi può essere schematizzato come segue

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

Assumendo che non si conosca la varianza dell'intera distribuzione, che σ sia la deviazione standard dello stimatore β_x e che n sia il numero di rilevazioni, si ottiene la formula dell'errore standard

$$SE(\beta_x) = \sigma/\sqrt{n}$$

Per calcolare la Statistica T è necessario fare la differenza tra lo stimatore β_x (ottenuto attraverso la regressione lineare) ed il valore ipotizzato dall'ipotesi nulla per poi fare il rapporto tra questo risultato e l'errore standard

$$T = \frac{\beta_x - \mu_{\beta_x}}{SE(\beta_x)}$$

Rapporto che può essere esplicitato come

$$T = \frac{\beta_x - \mu_{\beta_x}}{\sigma/\sqrt{n}}$$

Ma poiché il valore ipotizzato dall'ipotesi nulla è pari a zero, allora si ottiene

$$T = \frac{\beta_x}{\sigma/\sqrt{n}}$$

La Statistica T si distribuisce come una Student con $n-1$ gradi di libertà. Assumendo che la distribuzione sia centrata in zero, ossia accogliendo l'ipotesi nulla come vera, quanto maggiore è la distanza della Statistica T da zero, tanto maggiore è la debolezza dell'assunzione che l'ipotesi nulla sia vera, poiché altrettanto minore dovrebbe essere la probabilità (ossia il *p-value*) di osservare almeno quel valore (in termini assoluti). Pertanto, fissato un certo valore (genericamente 0.05) per il livello di significatività α, si rigetterà l'ipotesi nulla ammettendo la significatività statistica dello stimatore calcolato se il *p-value* sarà inferiore di α

$$p_{value} = 2 * \min\{\Pr(t \leq T|H_0), \Pr(t \geq T|H_0)\}$$
$$p_{value} < \alpha \rightarrow H_0\ rifiutata; \beta_x\ significativo$$

L'individuazione e l'analisi di modelli fattoriali impiegati nella spiegazione dei rendimenti delle cinque criptovalute precedentemente introdotte ha previsto l'utilizzo del software "Excel" e della componente aggiuntiva "Analisi Dati" al fine di ottenere fogli riassuntivi delle regressioni lineari che sono state effettuate. Oltre ai valori di cui si è scritto finora, questo strumento ha permesso di calcolare altre metriche riferite alla generalità del modello di regressione: l'errore standard sintetico ed il valore di significatività F. L'errore standard sintetico corrisponde alla distanza media dei valori rispetto all'equazione di regressione; il valore di significatività F, invece è assimilabile ad un *p-valore* coinvolto in un F-test, ammettendo come ipotesi nulla quella per cui un'ipotetica equazione di regressione costituita dal solo valore dell'intercetta (quindi costituita da soli coefficienti nulli) sia parimenti efficace, rispetto all'equazione di regressione ottenuta, nel descrivere i rendimenti osservati. Ovviamente, fissato un certo livello di significatività, è auspicabile ottenere un valore di significatività F inferiore al livello fissato, poiché quanto è inferiore tale valore, tanto maggiore è l'evidenza contraria all'ipotesi nulla, portando ad accogliere l'ipotesi alternativa per cui l'equazione ottenuta dall'analisi di regressione sia sufficientemente più idonea nella descrizione dei rendimenti studiati rispetto a quanto fatto da un'equazione costituita dal solo valore dell'intercetta verticale.

3.2 Applicazione dei modelli tradizionali

Di seguito, si andranno a presentare i risultati ottenuti dall'applicazione dei modelli fattoriali tradizionali (CAPM, Fama-French 3 fattori, Fama-French 5 fattori) e di modelli tradizionali costruiti appositamente per questa trattazione basandosi su relazioni e fattori tipici del mondo delle criptovalute. I dati riferiti ai modelli tradizionali sono stati ottenuti dal sito ufficiale di Kenneth R. French. Le misure di R^2 sono riferite a R^2 normale nel caso delle regressioni lineari semplici (modelli ad un unico fattore) mentre sono riferite a R^2 corretto nel caso di regressioni lineari multiple (modelli ad n-fattori). I valori aventi all'apice *, **, ***, sono associati rispettivamente a livelli di significatività del 10%, del 5% e dell'1%. Il valore di significatività riferito all'intero modello dipende dal valore di significatività F restituito dall'analisi di regressione. L'applicazione dei modelli tradizionali si rivela piuttosto insufficiente nello studio dei rendimenti di tutte le cinque criptovalute analizzate, caratterizzandosi per valori di R^2 estremamente contenuti e scarsa significatività statistica dei fattori di rischio diversi da quello di mercato.

3.2.1 Sintesi dei risultati su Bitcoin

Osservando i rendimenti di Bitcoin, i valori di alfa rimangono statisticamente significativi all'1% fino all'orizzonte settimanale, diventando significativi al 10% nell'orizzonte mensile. I modelli tradizionali si rivelano statisticamente significativi nell'orizzonte giornaliero e settimanale, mentre il valore di significatività F diventa maggiore del 10% nell'orizzonte mensile. Nei tre orizzonti temporali i rendimenti di questo asset mantengono una persistente relazione positiva con i fattori $MRKT$, HML ed una persistente relazione negativa con il fattore CMA. Questo suggerisce che Bitcoin si muova nella stessa direzione del mercato tradizionale e delle *value stocks* (rispetto alle *growth stocks*), seppur la ridotta significatività statistica della rilevazione; al contrario, in ragione del sistematico segno negativo del beta riferito al fattore CMA, si potrebbe ipotizzare cautamente (in ragione della scarsa significatività statistica) che i rendimenti di questo asset si muovano nella stessa direzione delle *high investment firms* (rispetto alle *low investment firms*)

I valori assoluti dei coefficienti beta crescono in valore assoluto all'aumentare del periodo considerato, pur non raggiungendo mai valori particolarmente elevati (diversamente da quanto accade per le altcoins): rispetto alle rilevazioni di Yukun Liu e Aleh Tsyvinski (2018)[22] sembrerebbe che i rendimenti di Bitcoin abbiano raggiunto un'apparente "maturità" in termini di co-movimento con i tradizionali fattori di rischio, diversamente dal passato in cui i valori assoluti dei coefficienti potevano arrivare anche a 6 unità. Inoltre, aldilà della ridotta sensibilità alle variazioni dei fattori di rischio, sembrerebbe che si sia modificata anche la natura delle loro relazioni: per quanto riguarda i fattori di HML e CMA, i segni dei coefficienti beta sono diventati rispettivamente positivi e negativi, almeno rispetto all'orizzonte mensile. In sintesi, i modelli tradizionali sono insufficienti nel descrivere i rendimenti di Bitcoin, assumendo un R^2 massimo di 0.031 (inferiore rispetto al 2018) soltanto nel caso del modello a 5 fattori applicato all'orizzonte mensile; la significatività statistica dei coefficienti beta è minima fatta eccezione per quello del fattore mercato.

	BTC: Giornaliero				BTC: Settimanale				BTC: Mensile		
	CAPM	3-Fac	5-Fac		CAPM	3-Fac	5-Fac		CAPM	3-Fac	5-Fac
α_i	**0,395*** **	**0,401*** **	**0,4*** **		**2,018*** **	**2,023*** **	**2,036*** **		**9,19***	**9,116***	**9,167***
	[3,417]	[3,464]	[3,453]		[3,387]	[3,386]	[3,397]		[1,941]	[1,851]	[1,842]
β_{MRKT}	**0,472*** **	**0,445*** **	**0,421*** **		**0,616** **	**0,506***	**0,404**		**1,622**	**1,813**	**1,49**
	[4,506]	[4,197]	[3,789]		[2,396]	[1,892]	[1,43]		[1,485]	[1,531]	[1,144]
β_{SMB}		**0,218**	**0,2**			**0,821***	**0,766**			**-0,916**	**-0,21**
		[1,085]	[0,977]			[1,655]	[1,492]			[-0,483]	[-0,095]
β_{HML}		**0,149**	**0,176**			**0,033**	**0,097**			**0,046**	**0,445**
		[0,98]	[0,903]			[0,095]	[0,212]			[0,028]	[0,211]
β_{RMW}			**-0,197**				**-0,273**				**1,835**
			[-0,608]				[-0,352]				[0,535]
β_{CMA}			**-0,169**				**-0,745**				**-1,615**
			[-0,417]				[-0,782]				[-0,441]
R^2	**0,010**	**0,011**	**0,012**		**0,014**	**0,021**	**0,023**		**0,024**	**0,026**	**0,031**
Significatività	***	***	***		**	**	*				

Tabella 4: Applicazione dei modelli fattoriali tradizionali su BTC

[22] Yukun Liu, Aleh Tsyvinski, Risks and returns of cryptocurrency, National Bureau of Economic Research, Agosto 2018

3.2.2 Sintesi dei risultati su Ether

Osservando i rendimenti di Ether, i valori di alfa rimangono statisticamente significativi all'1% fino all'orizzonte settimanale, mantenendo una persistenza nel grado di significatività anche nell'orizzonte mensile. Analogamente a BTC, i modelli tradizionali mantengono significatività statistica apprezzabile soltanto fino all'orizzonte settimanale, anche se in corrispondenza di tale periodo il modello a 5 fattori perde di significatività. Nei tre orizzonti temporali i rendimenti di Ether mantengono una persistente relazione positiva soltanto nel caso del fattore mercato: nel caso degli altri fattori di rischio, la relazione cambia di segno al variare dell'orizzonte temporale considerato. Rispetto a Bitcoin, i valori dei coefficienti beta risultano essere particolarmente elevati, soprattutto nel caso dell'orizzonte mensile e del fattore RMW, per il quale si rileva un'apprezzabile significatività statistica ad un livello di confidenza del 5%. Rispetto alla rilevazione del 2018, il valore di questo beta persiste ad un livello estremamente alto (10.195), mentre tutti gli altri coefficienti sembrano essersi ridotti particolarmente. La persistenza e la significatività del coefficiente β_{RMW} suggerirebbe una notevole relazione positiva tra i rendimenti delle *high profit stocks* (rispetto alle *low profit*). Il contributo marginale degli ennesimi fattori di rischio risulta essere minimo nell'orizzonte giornaliero e settimanale (la variazione di R^2 non supera 0.001) mentre diventa sostanziale nel passaggio dal modello a 3 a 6 fattori nell'orizzonte mensile, portando R^2 al valore di 0.103

	ETH: Giornaliero				ETH: Settimanale				ETH: Mensile		
	CAPM	3-Fac	5-Fac		CAPM	3-Fac	5-Fac		CAPM	3-Fac	5-Fac
α_i	**0,798*** **	**0,799*** **	**0,8*** **		**3,556*** **	**3,547*** **	**3,514*** **		**20,035*** **	**18,789** **	**17,419** **
	[3,78]	[3,784]	[3,783]		[3,059]	[3,035]	[2,993]		[2,751]	[2,457]	[2,324]
β_{MRKT}	**0,803*** **	**0,803*** **	**0,8*** **		**1,203*** **	**1,05** **	**1,031** **		**0,939**	**1,444**	**1,019**
	[4,655]	[4,588]	[4,357]		[2,666]	[2,213]	[2,039]		[0,613]	[0,851]	[0,545]
β_{SMB}		**-0,069**	**-0,077**			**1,059**	**1,263**			**-1,339**	**2,033**
		[-0,199]	[-0,219]			[1,158]	[1,338]			[-0,46]	[0,624]
β_{HML}		**0,046**	**0,079**			**0,06**	**-0,364**			**-1,234**	**-4,018**
		[0,188]	[0,249]			[0,1]	[-0,445]			[-0,527]	[-1,401]
β_{RMW}			**-0,079**				**0,868**				**10,195** **
			[-0,145]				[0,609]				[2,027]
β_{CMA}			**-0,033**				**0,022**				**6,337**
			[-0,051]				[0,013]				[1,291]
R^2	**0,015**	**0,015**	**0,015**		**0,024**	**0,029**	**0,030**		**0,006**	**0,016**	**0,103**
Significatività	***	***	***		***	**					

Tabella 5: Applicazione dei modelli fattoriali tradizionali su ETH

3.2.3 Sintesi dei risultati su ChainLink

Il comportamento dei rendimenti di questo asset è del tutto analogo rispetto a quello di Bitcoin, sia in termini di significatività statistica dell'alfa, del beta di mercato e di significatività generale dei modelli fattoriali. Diversamente da Bitcoin però, il segno del coefficiente β_{CMA} è sistematicamente positiva in tutti i modelli e in tutti gli orizzonti temporali, suggerendo pertanto una possibile correlazione positiva con le *low investment stock* (rispetto alle *high investment*), soprattutto nell'orizzonte mensile, dove si osserva il coefficiente di beta più alto in assoluto e statisticamente significativo al 10%. Il contributo marginale degli n-esimi fattori di rischio si rende cautamente apprezzabile già a partire dall'orizzonte settimanale e, analogamente ad ETH, si evidenzia in maniera rilevante nell'orizzonte mensile passando al modello a 5 fattori, portando il valore di R^2 al valore massimo di 0.131. Analogamente ad Ether, i valori di alfa rimangono particolarmente elevati pur perdendo di significatività nell'orizzonte mensile. Diversamente dai due asset analizzati in precedenza, β_{MRKT} non assume mai un valore inferiore ad uno in nessuno dei modelli fattoriali e orizzonti temporali, ad indicare che gli extra-rendimenti di ChainLink siano sistematicamente più che proporzionali rispetto agli extra-rendimenti del portafoglio di mercato.

	LINK: Giornaliero				LINK: Settimanale				LINK: Mensile		
	CAPM	3-Fac	5-Fac		CAPM	3-Fac	5-Fac		CAPM	3-Fac	5-Fac
α_i	**0,903*** **	**0,899*** **	**0,898*** **		**4,583*** **	**4,643*** **	**4,754*** **		**23,999***	**27,437***	**22,967**
	[2,94]	[2,923]	[2,922]		[2,797]	[2,821]	[2,879]		[1,93]	[1,963]	[1,656]
β_{MRKT}	**1,253*** **	**1,213*** **	**1,304*** **		**1,661*** **	**1,357** **	**1,548** **		**2,166**	**2,319**	**3,092**
	[5,745]	[5,493]	[5,615]		[3,018]	[2,379]	[2,553]		[0,968]	[0,913]	[1,061]
β_{SMB}		**0,74**	**0,74**			**2,089***	**1,752**			**-2,695**	**0,11**
		[1,576]	[1,545]			[1,738]	[1,385]			[-0,564]	[0,019]
β_{HML}		**0,077**	**-0,262**			**0,541**	**0,097**			**2,356**	**-2,483**
		[0,251]	[-0,628]			[0,726]	[0,089]			[0,593]	[-0,49]
β_{RMW}			**-0,694**				**-1,987**				**7,549**
			[-0,916]				[-1,027]				[0,764]
β_{CMA}			**1,333**				**2,898**				**15,165***
			[1,456]				[1,296]				[1,845]
R^2	**0,037**	**0,040**	**0,043**		**0,049**	**0,071**	**0,082**		**0,024**	**0,039**	**0,131**
Significatività	***	***	***		***	***	**				

Tabella 6: Applicazione dei modelli fattoriali tradizionali su LINK

3.2.4 Sintesi dei risultati su Binance Coin

I rendimenti di BNB risultano essere quelli meno spiegabili dal CAPM, mantenendo un valore di R^2 mai superiore a 0.017 (inferiore a 0.001 peraltro nell'orizzonte mensile). I modelli fattoriali tradizionali si rivelano statisticamente significativi soltanto nell'orizzonte giornaliero, assumendo invece valori di significatività F superiore a 0.1 dall'orizzonte settimanale in poi. Nell'orizzonte mensile i valori assoluti dei coefficienti beta e soprattutto degli alfa arrivano a livelli del tutto inediti in termini di grandezza rispetto agli altri asset. Diversamente da quanto accade con le altre criptovalute, il segno di β_{MKT} non rimane sistematicamente positivo, passando da negativo a positivo dal CAPM al modello a 3 fattori nell'orizzonte mensile. L'unico coefficiente per il quale si osserva una persistenza di segno è β_{RMW}, assumendo segno negativo nel modello a 5 fattori dei tre orizzonti temporali: questo lascerebbe intendere una relazione positiva tra i rendimenti di BNB e quelli delle *low profit stocks* (almeno rispetto alle *high profit stocks*), malgrado il fatto che in nessun caso il valore assume un grado apprezzabile di significatività statistica. Il massimo valore raggiunto da R^2 è 0.048 con il modello a 6 fattori applicato all'orizzonte mensile.

	BNB: Giornaliero				BNB: Settimanale				BNB: Mensile		
	CAPM	3-Fac	5-Fac		CAPM	3-Fac	5-Fac		CAPM	3-Fac	5-Fac
α_i	**1,314*** **	**1,3*** **	**1,301*** **		**8,39** **	**8,564** **	**8,794** **		**70,943**	**68,779**	**79,953**
	[3,257]	[3,219]	[3,22]		[2,434]	[2,448]	[2,51]		[1,244]	[1,079]	[1,23]
β_{MRKT}	**1,152*** **	**1,1*** **	**1,088*** **		**0,428**	**0,413**	**-0,212**		**-1,481**	**1,836**	**-1,495**
	[3,943]	[3,72]	[3,496]		[0,362]	[0,333]	[-0,162]		[-0,141]	[0,154]	[-0,106]
β_{SMB}		**1,27** **	**1,172***			**-0,702**	**-1,522**			**-13,907**	**-17,271**
		[2,029]	[1,835]			[-0,271]	[-0,561]			[-0,635]	[-0,625]
β_{HML}		**-0,04**	**-0,224**			**0,513**	**2,677**			**-1,754**	**15,641**
		[-0,099]	[-0,403]			[0,319]	[1,151]			[-0,095]	[0,645]
β_{RMW}			**-0,53**				**-3,631**				**-14,116**
			[-0,526]				[-0,875]				[-0,296]
β_{CMA}			**0,092**				**-6,434**				**-46,869**
			[0,075]				[-1,349]				[-1,212]
R^2	**0,017**	**0,022**	**0,022**		**0,001**	**0,002**	**0,015**		**0,000**	**0,012**	**0,048**
Significatività	***	***	***								

Tabella 7: Applicazione dei modelli fattoriali tradizionali su BNB

3.2.5 Sintesi dei risultati su Cardano

Analizzando i rendimenti di Cardano, si osserva che analogamente a Binance Coin i modelli fattoriali mantengono apprezzabile significatività statistica soltanto nell'orizzonte giornaliero, fatto salvo il CAPM che mantiene significatività a livello di 5% anche nell'orizzonte settimanale. Analogamente a ChainLink, il segno del coefficiente β_{CMA} è sistematicamente positivo e, pur non essendo mai statisticamente significativo, questo suggerirebbe un co-movimento positivo con i rendimenti delle *low investment stocks*. Sempre come LINK, il valore di β_{MRKT} non è mai inferiore ad 1. I valori di alfa diventano piuttosto larghi nell'orizzonte mesnile, pur non essendo statisticamente significativi.

La capacità esplicativa dei modelli tradizionali è del tutto analoga a quanto si osserva con ETH e LINK, arrivando ad un R^2 massimo di 0.119 nel caso del modello a 6 fattori applicato alla dimensione mensile.

	ADA: Giornaliero				ADA: Settimanale				ADA: Mensile		
	CAPM	3-Fac	5-Fac		CAPM	3-Fac	5-Fac		CAPM	3-Fac	5-Fac
α_i	**0,855****	**0,864****	**0,862****		**4,884***	**5,305****	**5,34****		**26,388**	**31,654**	**23,058**
	[2,276]	[2,296]	[2,29]		[1,902]	[2,045]	[2,048]		[1,436]	[1,523]	[1,097]
β_{MRKT}	**1,188*****	**1,13*****	**1,166*****		**1,768****	**1,466**	**1,806***		**2,548**	**2,489**	**2,092**
	[4,471]	[4,2]	[4,114]		[2,06]	[1,639]	[1,895]		[0,779]	[0,667]	[0,489]
β_{SMB}		**0,751**	**0,754**			**0,491**	**0,525**			**-2,529**	**5,459**
		[1,307]	[1,286]			[0,259]	[0,263]			[-0,356]	[0,627]
β_{HML}		**0,253**	**0,001**			**1,481**	**0,93**			**3,412**	**-5,259**
		[0,675]	[0,002]			[1,266]	[0,542]			[0,584]	[-0,673]
β_{RMW}			**-0,305**				**-1,354**				**18,904**
			[-0,329]				[-0,445]				[1,299]
β_{CMA}			**0,631**				**4,484**				**20,909**
			[0,563]				[1,275]				[1,598]
R^2	**0,023**	**0,026**	**0,026**		**0,024**	**0,034**	**0,044**		**0,016**	**0,027**	**0,119**
Significatività	***	***	***		**						

Tabella 8: Applicazione dei modelli fattoriali tradizionali su ADA

3.3 Valutazione di fattori di rischio *crypto-market based*

Malgrado le deboli assunzioni in merito ai potenziali co-movimenti delle criptovalute rispetto agli asset tradizionali, i valori estremamente contenuti delle metriche di interesse evidenziano la necessità di definire nuovi modelli fattoriali pur mantenendo lo stesso approccio metodologico nella loro applicazione. Di seguito si andranno ad evidenziare i risultati di modelli che provano a sopperire a questa mancanza. Il ragionamento di fondo è quello per cui, riflettendo la distanza significativa del mondo *on-chain* rispetto a quello *off-chain*, anche il mercato delle criptovalute sembra muoversi in maniera totalmente autonoma ed indipendente rispetto al mercato tradizionale, e questa situazione appare evidente sottolineando l'inapplicabilità dei modelli tradizionali di *asset pricing* come già dimostrato da Liu, Tsyvinski e Wu nel 2019[23]. Pertanto, la trattazione seguente cercherà di ricostruire il rischio sistematico associato all'unico mercato delle criptovalute a partire da suoi sottoinsiemi come Bitcoin e *clusters* di criptovalute definiti sulla base della capitalizzazione e di altre variabili di raggruppamento. La volontà di escludere dall'analisi fattori associati all'attenzione da parte degli investitori (trend di ricerca su Google, trend di condivisioni su Twitter etc.), al rendimento delle azioni di società coinvolte nel settore del mining (come Nvidia e AMD, entrambe presenti nello strumento "Cryptocurrency Exposure Basket" di JP Morgan) e ad altri elementi che, pur riferendosi tipicamente alle criptovalute, non si riferiscono in senso stretto al *mercato* delle criptovalute, dipende dai risultati a cui sono pervenuti Liu e Tsyvinski nel 2018, i quali hanno evidenziato come modelli fattoriali costruiti a partire da questi benchmark producessero valori di alfa piuttosto alti e statisticamente significativi, valori di beta scarsamente significativi e valori di R^2 vicini allo zero.

[23] Yukun Liu, Aleh Tsyvinski, Xi Wu, Common risk factors in cryptocurrency, Maggio 2019

3.3.1 Fattore BTC

In primis, pur ammettendo la sostanziale differenza rispetto ad un portafoglio benchmark diversificato, ci si è chiesto quale potesse essere il contributo esplicativo dei rendimenti di questi asset da parte della criptovaluta principale: Bitcoin. Aldilà del fatto che essa sia stata la prima ad entrare in circolazione, nonché *brand* stesso, per certi versi, del mondo *cryptocurrency*, l'importanza di Bitcoin nell'analisi dei rendimenti è che il peso della sua capitalizzazione su quella totale delle criptovalute è sempre stata al di sopra del 50%, fatta eccezione per un intervallo compreso tra Giugno 2017 e Giugno 2018 nonché una finestra temporale ancora aperta nata ad aprile 2021.

L'analisi è stata condotta attraverso una regressione lineare confrontando i rendimenti di Bitcoin con quelli di ciascun asset in questione. I modelli di regressione così studiati hanno tutti riportato un valore di significatività F tale da considerarsi statisticamente rilevanti ad un livello di confidenza dell'1% (fatta eccezione per il modello applicato ai rendimenti mensili di BNB, in cui il livello di significatività è del 5%). Questo semplice modello, basato su un unico fattore, è in grado di offrire valori di R^2 sistematicamente superiori rispetto ai modelli fattoriali tradizionali, indicando pertanto una scarsa adeguatezza da parte di questi nel descrivere efficacemente i rendimenti delle criptovalute. Pur mantenendosi superiori, tuttavia i valori di R^2 non sempre raggiungono livelli apprezzabili. Ether si rivela la criptovaluta maggiormente spiegata dal modello, mantenendo un R^2 mai inferiore al 43% ed un'intercetta scarsamente significativa a livello statistico, mentre il coefficiente beta mantiene un'elevata significatività statistica su tutti gli orizzonti temporali (le Statistiche-T sono sistematicamente superiori rispetto alle altre criptovalute) assumendo valori mai superiori a 1 (seppur vicini ad esso).

LINK viene spiegato dal modello con minor efficacia rispetto a quanto fatto con Ether, mantenendo valori di R^2 compresi tra 0.1877 e 0.1764 nei tre orizzonti temporali considerati. Il beta rimane sempre statisticamente significativo mentre l'alfa perde di significatività a partire dall'orizzonte mensile. Nell'orizzonte mensile, peraltro, il valore di beta diventa maggiore di 1.

Per quanto riguarda BNB, la capacità epesegetica del modello decresce all'aumentare dell'orizzonte temporale considerato: l'R^2 giornaliero è secondo soltanto a quello di ETH, mentre l'R^2 mensile è ultimo in termini di grandezza. I coefficienti alfa si mantengono statisticamente significativi fino all'orizzonte settimanale, mentre il valore di beta persiste nella sua significatività statistica in tutti i periodi. Soltanto nell'orizzonte mensile la significatività statistica di beta è associata ad un livello del 5%, rappresentando un *unicum* dal momento che i beta delle altre criptovalute persistono ad un livello di significatività dell'1% su tutti gli orizzonti temporali. Infine, analizzando Cardano, il modello si rivela sempre statisticamente significativo per quanto riguarda i beta e mai per quanto riguarda gli alfa, rivelandosi in questo molto simile ad ETH. Tuttavia, la capacità epesegetica del modello è ridotta ad un R^2 compreso tra lo 0.1901 e lo 0.2417. Nel caso di Cardano, si ha la

particolarità di osservare che già a partire dall'orizzonte settimanale il coefficiente beta assuma un valore maggiore di 1 e che esso diventi persino maggiore di 2 nell'orizzonte mensile.

	GIORNALIERO				SETTIMANALE				MENSILE			
	α_i	β_{BTC}	R^2	Significatività	α_i	β_{BTC}	R^2	Significatività	α_i	β_{BTC}	R^2	Significatività
ETH	0,00013	0,89264***	0,5312	***	0,00173	0,91505***	0,5299	***	0,02206	0,92073***	0,4371	***
	[0,1383]	[37,51157]			[0,22123]	[14,04609]			[0,46545]	[5,43191]		
LINK	0,00413**	0,80609***	0,1877	***	0,03177**	0,79663***	0,1764	***	0,15765	1,0786***	0,1865	***
	[2,08379]	[16,943]			[2,02804]	[6,12237]			[1,54279]	[2,95135]		
BNB	0,00337**	0,8997***	0,3224	***	0,02757**	0,81979***	0,2277	***	0,09608	0,7498**	0,1265	**
	[2,18341]	[24,30773]			[2,00618]	[7,18257]			[1,07489]	[2,34549]		
ADA	0,00342	0,98444***	0,2352	***	0,02579	1,218***	0,1901	***	0,12317	2,1855***	0,2417	***
	[1,63066]	[19,54482]			[1,12733]	[6,41003]			[0,70146]	[3,48027]		

Tabella 9: Applicazione del modello basato sul fattore BTC

3.3.2 Fattore CRIX

Al fine di definire modelli autorevoli nell'analisi dei rendimenti delle criptovalute, si è pensato di studiarne gli extrra-rendimenti, assumendo un tasso *risk free* nullo (analogamente a quanto fatto nelle rilevazioni presenti sul sito di Kenneth Fama), rispetto a quelli di portafogli diversificati e costruiti sulla base di diversi criteri, spesso riferiti all'imputabilità di ciascuna criptovaluta a particolari categorie di appartenenza. Il primo portafoglio a cui si fa riferimento è quello $CRIX$[24], un indice costruito in maniera analoga all'indice di Laspeyres, e basato quindi sulla misurazione delle variazioni di volumi o di prezzi di ciascuna criptovaluta considerata. Definendo con 0 l'anno base, con t il periodo corrente (in cui viene eseguita la rilevazione), con n il numero di elementi compresi nell'aggregato, si ottiene la formula dell'indice di Laspeyres

$$Indice_{Laspeyres} = \frac{\sum_{i=1}^{n} P_{it} Q_{i0}}{\sum_{i=1}^{n} P_{i0} Q_{i0}}$$

La formula impiegata nel calcolo dell'indice CRIX rapporta la capitalizzazione corrente di ciascuna criptovaluta (facendone il prodotto tra prezzo e quantità correnti) rispetto ad un divisore che viene aggiustato rispetto alle variazioni della quantità in circolo di ciascuna criptovaluta considerata, in modo tale che le variazioni del valore dell'indice riflettano unicamente le variazioni di prezzo.

$$\begin{cases} MV_{it} = capitalizzazione\ corrente\ dell'i-esima\ crypto \\ MV_{i0} = capitalizzazione\ dell'i-esima\ crypto\ al\ tempo\ base \end{cases}$$

$$Divisor = \frac{\sum_{i=1}^{n} MV_{i0}}{1000}$$

$$Indice_{CRIX} = \frac{\sum_{i=1}^{n} MV_{it}}{Divisor} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{MV_{it}} * \frac{\boldsymbol{1000}}{\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{MV_{i0}}}$$

Pertanto, assumendo il periodo corrente come il tempo base, è chiaro stabilire che il valore di partenza dell'indice CRIX sia esattamente 1000, dal momento che, se $t = 0$ allora $\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{MV_{it}} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{MV_{i0}}$

[24] https://thecrix.de/

Le coppie considerato nell'aggregato sono 10 e sono tutte appartenenti alle prime due generazioni di criptovalute: BTC, ETH, BNB, ADA, USDT, XRP, DOGE, DOT, LTC, LINK (l'indice non può considerare anche quelle della terza essendo nato nel luglio 2014, riferendosi ad esso come tempo base).

Procedendo secondo la stessa metodologia applicata nella definizione del modello basato sul fattore BTC, si è analizzata l'idoneità dell'indice CRIX ad essere utilizzato in un modello di *pricing*, al fine di dare un'approssimazione del portafoglio di mercato (alla base del CAPM e dei modelli multifattoriali tradizionali) malgrado il numero estremamente ridotto di coppie considerate nell'indice. L'efficacia del modello appare evidente nell'orizzonte mensile, con una capacità di spiegare i rendimenti di ciascun asset analizzato in maniera proporzionale al suo peso nell'indice (e quindi, indefinitiva, alla sua capitalizzazione): i valori di beta sono tutti statisticamente significativi ad un livello dell'1% mentre i valori di alfa non lo sono. Al contrario, il modello si rivela particolarmente inidoneo nello spiegare i rendimenti giornalieri, portando a valori di R^2 addirittura peggiori rispetto a quelli osservati nell'applicazione dei modelli tradizionali. Analizzando l'orizzonte mensile, Cardano si conferma la criptovaluta più reattiva alle variazioni del benchmark, seguita da ChainLink, Binance Coin, Ether e Bitcoin.

	GIORNALIERO				SETTIMANALE				MENSILE			
	α_i	β_{CRX}	R^2	Significatività	α_i	β_{CRX}	R^2	Significatività	α_i	β_{CRX}	R^2	Significatività
BTC	0,00248**	0,1001***	0,0101	***	0,00289	0,83969***	0,6787	***	0,01409	0,76032***	0,7799	***
	[2,10655]	[3,55376]			[0,56042]	[19,22807]			[0,66545]	[11,60463]		
ETH	0,0025*	0,03663	0,0009		-0,00047	0,99073***	0,5980	***	0,00764	0,98873***	0,6800	***
	[1,72652]	[1,05689]			[-0,06582]	[16,13443]			[0,21487]	[8,98605]		
LINK	0,00639***	-0,00637	0,0000		0,02758*	0,96601***	0,2497	***	0,12609	1,31281***	0,3727	***
	[2,89851]	[-0,12109]			[1,84169]	[7,63147]			[1,41215]	[4,75153]		
BNB	0,00568***	0,06326	0,0016		0,02361*	0,97797***	0,3119	***	0,05151	1,15104***	0,4021	***
	[3,03026]	[1,41114]			[1,81734]	[8,90643]			[0,70006]	[5,0549]		
ADA	0,00571**	0,154***	0,0058	***	0,01795	1,54219***	0,2934	***	0,04882	2,76972***	0,5237	***
	[2,38359]	[2,68762]			[0,83905]	[8,52525]			[0,35255]	[6,4642]		

Tabella 10: Applicazione del modello basato sul fattore CRIX

3.3.3 Fattori FTX

Di seguito si andranno ad analizzare altri indici al fine di definire modelli multifattoriali che scompongano il *market risk factor* in una pluralità di declinazioni, sopperendo così all'insufficienza del CRIX in termini di numerosità degli asset considerati. Tutti gli indici che seguiranno corrispondono a portafogli equiponderati di criptovalute appartenenti a medesime categorie[25]. I portafogli vengono ribilanciati in maniera irregolare (l'ultimo ribilanciamento è avvenuto il 27 Marzo 2020, quello precedente il 25 Ottobre 2020) modificando la quantità di ciascuna criptovaluta considerata al fine di ripristinarne il peso relativo (che inevitabilmente si modifica nel tempo a causa delle variazioni di prezzo).

I valori storici degli indici che seguiranno sono stati collezionati in formato JSON (JavaScript Object Notation) utilizzando chiamate API rivolte direttamente al sito di FTX, exchange che li ha realizzati.

[25] https://help.ftx.com/hc/en-us/articles/360027668812-Index-Calculation

3.3.3.1 Fattore ALT

L'indice ALT corrisponde ad un portafoglio costituito dalle 10 principali criptovalute diverse da Bitcoin, appartenenti alle prime due generazioni. Le quantità presenti di ciascuna sono evidenziate nella tabella a fianco. Molte delle coppie sono presenti anche nell'indice CRIX, con la differenza che in questo caso Bitcoin (BTC), Dogecoin (DOGE) e Tether (USDT) vengano sostituite da Bitcoin Cash (BCH), EOS (EOS) e Tron (TRX). Pertanto, nonostante il fatto che 7 coppie su 10 siano le stesse, l'equiponderazione del portafoglio, l'assenza di Bitcoin e della stablecoin USDT permettono a questo indice di avere un'autonoma identificabilità rispetto al CRIX.

Ticker	Quantity
BCH	0.325
BNB	2.565
EOS	16.508
ETH	0.268
LTC	1.154
XRP	431.691
TRX	1250.901
DOT	16.283
LINK	6.785
ADA	543.475

Il modello fattoriale costruito a partire da questo indice, come accade anche per gli altri indici realizzati da FTX, risulta essere particolarmente significativo ed epesegetico su ogni orizzonte temporale considerato. I beta si rivelano sempre statisticamente significativi ad un livello dell'1% mentre gli alfa appaiono moderatamente significativi soltanto nell'orizzonte giornaliero e settimanale di Cardano, nonché nell'orizzonte mensile di Ether. Peraltro, il fattore "Altcoin" sembrerebbe spiegare in maniera particolarmente rilevante i rendimenti di Ether, registrando valori di R^2 compresi tra 0.7546 e 0.8485, mentre non risulterebbe parimenti efficace nel descrivere i rendimenti mensili di Bitcoin (assente nell'indice considerato), malgrado il fatto che i suoi valori di R^2, assunti negli orizzonti temporali inferiori, siano particolarmente più alti rispetto a quelli registrati ChainLink e Binance Coin (entrambi presenti nell'indice ALT). Ancora una volta, Cardano si conferma la criptovaluta più reattiva rispetto alle variazioni del benchmark, mentre Bitcoin quella meno reattiva non assumendo mai un valore di beta maggiore di 0.66031. Al contrario, Ether e ChainLink risultano piuttosto allineate rispetto al benchmark, così anche Binance Coin fatta eccezione per i rendimenti mensili, in cui il valore di beta si riduce in maniera rilevante.

	GIORNALIERO				SETTIMANALE				MENSILE			
	α_i	β_{ALT}	R^2	Significatività	α_i	β_{ALT}	R^2	Significatività	α_i	β_{ALT}	R^2	Significatività
BTC	0,00096	0,62058***	0,6498	***	0,00757	0,66031***	0,6094	***	0,05111	0,47864***	0,3792	***
	[1,02719]	[33,27909]			[1,05616]	[11,3104]			[1,0622]	[3,12632]		
ETH	0,001	0,889***	0,8264	***	0,0094	0,91184***	0,7546	***	0,06964*	1,04558***	0,8485	***
	[1,20089]	[53,30225]			[1,33268]	[15,8809]			[2,0065]	[9,46727]		
LINK	0,00284	0,86229***	0,4658	***	0,02213	0,80633***	0,3660	***	0,11442	1,08306***	0,6242	***
	[1,50229]	[22,81478]			[1,53738]	[6,88034]			[1,73282]	[5,1552]		
BNB	0,00216	0,85844***	0,5198	***	0,01247	1,12756***	0,5267	***	0,00661	0,61605***	0,6266	***
	[1,27502]	[25,41912]			[0,8603]	[9,55317]			[0,177]	[5,18128]		
ADA	0,00353**	0,92397***	0,6086	***	0,01842*	1,14531***	0,6967	***	0,07672	1,24995***	0,7290	***
	[2,32518]	[30,46755]			[1,79701]	[13,72331]			[1,2812]	[6,56056]		

Tabella 11: Applicazione del modello basato sul fattore ALT

3.3.3.2 Fattore MID

L'indice MID corrisponde ad un portafoglio equiponderato costituito da 30 criptovalute caratterizzate da una media capitalizzazione di mercato. Le quantità presenti di ciascuna sono evidenziate nella tabella a fianco. Insieme all'indice SHIT, esso è un indice costituito da un numero particolarmente elevato di asset, almeno rispetto agli indici precedentemente analizzati, includendo trasversalmente criptovalute al mondo della finanza decentralizzata (DeFi), dei sistemi di pagamento e delle transazioni confidenziali. Anche in questo caso il modello si rende particolarmente efficace e significativo nel descrivere i rendimenti delle coppie analizzate, producendo risultati sistematicamente migliori nell'analisi di Cardano, Binance Coin e ChainLink. Il modello infatti è sempre statisticamente significativo ad un livello dell'1%, fatta eccezione per Bitcoin nell'orizzonte mensile in cui il livello di significatività passa al 5% (al pari del beta). Tuttavia, osservando i valori di R^2, questo modello appare peggiorativo rispetto a prima nel descrivere i rendimenti di Bitcoin ed Ether, entrambi assenti in questo indice.

I beta sono sempre statisticamente significativi al livello dell'1% (fatta eccezione per il beta mensile di bitcoin) e gli alfa non lo sono mai tranne che per l'orizzonte giornaliero e settimanale di Cardano nonché per quello mensile di ChainLink. La reattività rispetto alle variazioni del benchmark è leggermente maggiore in termini di intensità rispetto al modello precedente, ma la gerarchia dei beta tra le diverse coppie rimane pressocché la stessa. Il beta più alto si rinviene in quello settimanale di Binance Coin, malgrado il fatto che nell'orizzonte mensile esso sia penultimo in termini di grandezza

Ticker	Quantity
ALGO	24.933
ATOM	7.468
BAT	46.44
CRO	656.601
DASH	0.307
DCR	0.379
DOGE	3962.982
HT	7.276
IOTA	88.489
LEO	30.357
NEO	2.232
OKB	8.582
ONT	19.975
QTUM	3.248
VET	2073.785
XEM	280.944
XLM	656.262
XMR	0.56
XTZ	22.713
ZEC	0.327
ZRX	22.509
OMG	4.427
COMP	0.118
BSV	0.495
FTT	2.899
YFI	0.001
UNI	6.311
SNX	3.994
MKR	0.028
AAVE	0.333

	GIORNALIERO				SETTIMANALE				MENSILE			
	α_i	β_{MID}	R^2	Significatività	α_i	β_{MID}	R^2	Significatività	α_i	β_{MID}	R^2	Significatività
BTC	0,00117	0,65393***	0,5954	***	0,00861	0,69825***	0,5808	***	0,05405	0,42629**	0,3189	**
	[1,17854]	[29,43884]			[1,14844]	[10,59357]			[1,07108]	[2,73717]		
ETH	0,00138	0,91697***	0,7218	***	0,01285	0,87085***	0,5861	***	0,0723	0,97168***	0,7770	***
	[1,31345]	[39,08987]			[1,38929]	[10,70985]			[1,71459]	[7,46583]		
LINK	0,00245	1,06519***	0,5803	***	0,02155	0,96092***	0,4451	***	0,10888*	1,09573***	0,6774	***
	[1,46377]	[28,53778]			[1,58906]	[8,0601]			[1,77751]	[5,79622]		
BNB	0,00216	0,91226***	0,4693	***	0,01264	1,17571***	0,4851	***	0,00422	0,61512***	0,6623	***
	[1,20712]	[22,82201]			[0,8259]	[8,73653]			[0,1186]	[5,6019]		
ADA	0,00351**	1,0627***	0,6515	***	0,0168*	1,31328***	0,7764	***	0,07088	1,25858***	0,7836	***
	[2,44728]	[33,1827]			[1,88545]	[16,77244]			[1,32318]	[7,61255]		

Tabella 12: Applicazione del modello basato sul fattore MID

3.3.3.3 Fattore SHT

L'indice SHIT corrisponde ad un portafoglio equiponderato costituito da 50 criptovalute caratterizzate da una bassa capitalizzazione di mercato (definite "shitcoins" dalle communities dei cultori delle criptovalute). Le quantità presenti di ciascuna sono evidenziate nella tabella a fianco. Di tutti gli inidici analizzati questo è il più numeroso in termini di coppie che lo compongono, pur non presentando nessuna delle 5 coppie su cui si basa la seguente trattazione (essendo queste caratterizzate da capitalizzazioni medio-alte). Malgrado ciò, il modello appare comunque adeguatamente idoneo nello studio dei rendimenti analizzati, presentando valori di R^2 compresi tra lo 0.3496 e lo 0.7437. Come nel caso delle altre rilevazioni, il modello non si presta particolarmente nello studio dei rendimenti di Bitcoin, per il quale i valori di R^2 decrescono all'aumentare dell'orizzonte temporale considerato, e non rivela un'oggettiva maggiore efficacia nel descrivere quelli delle altre coppie considerate. Malgrado ciò, il modello appare sempre statisticamente significativo al livello dell'1%, cosi come per i beta. Gli alfa non sono mai statisticamente significativi tranne nel caso dell'orizzonte giornaliero e settimanale di Binance Coin, nonché in quello mensile di ChainLink, esattamente come accade nel modello basato sul fattore MID. La gerarchia dei beta rimane pressoché la stessa dei modeli precedenti

Ticker	Quantity
AE	90.7
AION	109.577
ARDR	289.037
ARPA	1409.004
BCD	23.404
BEAM	26.024
BTG	1.423
BTM	199.291
BTS	630.948
BTT	43049.882
CHZ	1271.805
CKB	2213.181
DGB	2679.856
ELF	167.133
ENJ	147.2
GNT	292.22
GRIN	16.363
GT	28.196
HBAR	297.911
HC	9.537
ICX	43.877
IOST	2938.887
KMD	25.77
KNC	21.036
LAMB	571.357
LRC	350.963
LSK	11.672
MANA	344.492
MATIC	658.699
MCO	3.155
NANO	20.295
NULS	60.502
OMG	17.647
POWR	156.025
PUNDIX	88.703
REN	244.799
REP	1.311
RVN	594.201
SC	7385.085
SNT	1035.665
STEEM	74.739
THETA	122.358
TOMO	30.848
VSYS	342.519
WAVES	12.183
XVG	4263.355
XZC	2.991
ZEN	1.633
ZIL	2405.968
ZRX	59.559

	GIORNALIERO				SETTIMANALE				MENSILE			
	α_i	β_{SHT}	R^2	Significatività	α_i	β_{SHT}	R^2	Significatività	α_i	β_{SHT}	R^2	Significatività
BTC	0,00122	0,6136***	0,5806	***	0,01172	0,57789***	0,4507	***	0,05087	0,52272***	0,3496	***
	[1,20233]	[28,40809]			[1,35708]	[8,10218]			[1,02886]	[2,93277]		
ETH	0,00154	0,84527***	0,6730	***	0,0153	0,74399***	0,4798	***	0,07146	1,11331***	0,7437	***
	[1,34837]	[34,64003]			[1,45868]	[8,59004]			[1,5764]	[6,81286]		
LINK	0,00284	0,92919***	0,4859	***	0,02317*	0,90717***	0,4492	***	0,10281*	1,31788***	0,7144	***
	[1,52842]	[23,4721]			[1,70345]	[8,0774]			[1,7793]	[6,32695]		
BNB	0,00203	0,89005***	0,4890	***	0,01423	1,10362***	0,4819	***	0,00516	0,68673***	0,6019	***
	[1,14599]	[23,61887]			[0,9183]	[8,62656]			[0,13326]	[4,91804]		
ADA	0,00391**	0,92274***	0,5388	***	0,02066*	1,08619***	0,5942	***	0,07721	1,35138***	0,6587	***
	[2,35577]	[26,10024]			[1,6996]	[10,82401]			[1,14451]	[5,55701]		

Tabella 13: Applicazione del modello basato sul fattore SHT

3.3.3.4 Fattore EX

Ticker	Quantity
BNB	9.05
HT	60.992
OKB	57.541
LEO	222.129
FTT	71.615

L'indice EXCH corrisponde ad un portafoglio equiponderato costituito da sole 5 criptovalute, ciascuna riferita direttamente o indirettamente ad un exchange operante sul mercato (Binance, Huobi, OKEx, Bitfinex, Ftx). Le quantità presenti di ciascuna sono evidenziate nella tabella a fianco. Un grande assente che emerge dalla lista di coin che compongono questo portafoglio è CRO, criptovaluta della blockchain di Crypto.com che, adottando un business model per certi versi molto simile a quello di Binance, sta acquisendo sempre maggiore popolarità nel pubblico degli investitori. La clusterizzazione di criptovalute sulla base della loro associazione a determinati exchange è potenzialmente in grado di produrre risultati interessanti poiché potrebbe mettere in luce l'influenza di dinamiche tipicamente aziendali, riferite agli exchange, sul prezzo delle criptovalute a cui si riferiscono e, di riflesso, sul mercato in generale. Per BTC, ETH, LINK e ADA, i risultati proposti dalla regressione lineare nono sono particolarmente brillanti in termini di R^2, evidenziando come questo modello sia quello meno efficace rispetto agli altri basati sugli indici di FTX nel descrivere i rendimenti di queste criptovalute. Al contrario, questo modello si rende particolarmente efficace osservando i valori di R^2 di BNB nell'orizzonte giornaliero e settimanale, dal momento che il portafoglio benchmark è composto da questa criptovaluta per il 20%. Malgrado la scarsa capacità nel descrivere i rendimenti, che rimane modesta nel caso di ETH, il modello presenta sistematicamente una significatività statistica a livello dell'1%, che passa al 5% soltanto con Cardano e Bitcoin nell'orizzonte mensile (come accade per i beta). Per quanto riguarda gli alfa, essi non sono mai statisticamente significativi fatto salvo il caso di Cardano nell'orizzonte giornaliero e di Cardano, Ether e ChainLink nell'orizzonte settimanale

	GIORNALIERO				SETTIMANALE				MENSILE			
	α_i	β_{EX}	R^2	Significatività	α_i	β_{EX}	R^2	Significatività	α_i	β_{EX}	R^2	Significatività
BTC	0,00106	0,55217***	0,4081	***	0,0121	0,42646***	0,3449	***	0,05373	0,74154**	0,3107	**
	[0,83793]	[19,31364]			[1,22328]	[6,24132]			[0,9233]	[2,51195]		
ETH	0,00218	0,67841***	0,3704	***	0,02274*	0,45732***	0,2454	***	0,07012	1,41872***	0,5167	***
	[1,29093]	[17,83928]			[1,68527]	[4,90605]			[0,96988]	[3,8686]		
LINK	0,00384	0,71732***	0,2466	***	0,03873**	0,37352***	0,1043	***	0,10703	1,59356***	0,4475	***
	[1,60637]	[13,308]			[2,10245]	[2,93552]			[1,14731]	[3,36762]		
BNB	0,00052	1,26124***	0,8288	***	0,00263	1,28756***	0,8740	***	0,01246	1,00152***	0,6483	***
	[0,47641]	[51,18384]			[0,31986]	[22,65808]			[0,32068]	[5,0797]		
ADA	0,00496**	0,69276***	0,2597	***	0,02918*	0,74467***	0,3741	***	0,119	1,3069**	0,2662	**
	[2,21885]	[13,77647]			[1,8]	[6,64985]			[1,04091]	[2,25372]		

Tabella 14: Applicazione del modello basato sul fattore EX

3.4 Applicazione dei modelli fattoriali *crypto-market based*

Di seguito si andranno a definire modelli multifattoriali (da 1 a 5 fattori) basati sull'aggregazione dei fattori rischio di rischio costruiti a partire dei cinque portafogli precedentemente analizzati. La realizzazione di tali modelli è avvenuta attuando regressioni lineari multiple mediante l'utilizzo di Microsoft Excel.

3.4.1 Sintesi dei risultati su Bitcoin

Osservando la relazione sussistente tra i rendimenti di Bitcoin e le evoluzioni percentuali degli altri fattori di rischio, si evince come gli extra-rendimenti di questo asset siano soltanto una proporzione ridotta rispetto agli extra-rendimenti degli indici analizzati, fatto salvo il caso dell'indice $CRIX$ in cui si riscontra un beta vicino ad 1 nei modelli multifattoriali calcolati su base mensile. A livello giornaliero, il contributo epesegetico degli n-esimi fattori di rischio è sostanziale rispetto al solo fattore $CRIX$: passando al modello a due fattori, il valore di R^2 passa da 0.01 a 0.65, il beta del fattore $CRIX$ perde di significatività che invece viene assunta dal fattore ALT fino all'orizzonte settimanale. In sintesi, a livello giornaliero la relazione tra i rendimenti di Bitcoin e quelli dell'indice $CRIX$ sembra essere assente e, in ogni caso, scarsamente significativa, mentre la relazione con l'indice ALT e con l'indice SHT è statisticamente significativa nel passaggio tra i diversi modelli, suggerendo la possibilità che i movimenti di Bitcoin risultino condizionati (magari anche in senso reciproco, alla luce dei risultati condotti dall'analisi del fattore BTC), seppur con modestissima reattività, sia da quelli delle criptovalute principali diverse da sé che da quelli delle criptovalute a bassa capitalizzazione. Invece, la relazione con gli indici MID ed EX appare statisticamente significativa soltanto in corrispondenza dei modelli che li aggiungono come n-esimi fattori, evidenziando comunque una reattività prossima allo zero. Ampliando l'orizzonte temporale invece, si evince come la relazione statisticamente significativa persista solo con l'indice $CRIX$ e, seppur nella sola dimensione settimanale, con il fattore ALT nel modello a due fattori e con il fattore MID: passando all'orizzonte mensile infatti, il coefficiente della retta di regressione tra i rendimenti di Bitcoin e quelli del $CRIX$ diventa particolarmente vicina ad uno e statisticamente significativa, mentre lo stesso coefficiente calcolato sulla base degli indici ALT e MID diventa prossimo allo zero. In altre parole, si potrebbe affermare che nel breve periodo i rendimenti di Bitcoin siano parzialmente condizionati da quelli delle altre criptovalute, in particolar modo da parte di quelle principali e a ridottissima capitalizzazione, ma che questa influenza, pur sopravvivendo in parte nella dimensione settimanale con le criptovalute a media capitalizzazione, si minimizza ampliando il focus dell'analisi a vantaggio di una sintonia quasi perfetta (i valori di alfa infatti sono tutti prossimi allo zero e scarsamente significativi) con l'indice $CRIX$

	BTC: Giornaliero					BTC: Settimanale					BTC: Mensile				
	CRIX	2-Fac	3-Fac	4-Fac	5-Fac	CRIX	2-Fac	3-Fac	4-Fac	5-Fac	CRIX	2-Fac	3-Fac	4-Fac	5-Fac
α_i	**0,00248****	**0,00082**	**0,00081**	**0,00079**	**0,00037**	**0,00289**	**0,00096**	**0,00143**	**0,00167**	**-0,00001**	**0,01409**	**-0,00435**	**-0,0035**	**-0,00352**	**-0,00677**
	[2,106]	[0,877]	[0,872]	[0,861]	[0,396]	[0,56]	[0,154]	[0,231]	[0,267]	[-0,002]	[0,665]	[-0,184]	[-0,144]	[-0,141]	[-0,234]
β_{CRX}	**0,1*****	**0,03757**	**0,046***	**0,04531***	**0,03493**	**0,839*****	**0,49373**	**0,482*****	**0,4946*****	**0,47849*****	**0,76*****	**1,01285**	**1,012*****	**0,99089*****	**0,97004*****
	[3,553]	[1,532]	[1,889]	[1,861]	[1,403]	[19,228]	[5,524]	[5,473]	[5,508]	[5,242]	[11,604]	[7,625]	[7,46]	[6,803]	[6,465]
β_{ALT}		**0,624*****	**0,44*****	**0,41278*****	**0,36649*****		**0,365*****	**0,189**	**0,19741**	**0,16519**		**-0,108**	**0,023**	**0,06519**	**0,00809**
		[33,257]	[9,874]	[9,279]	[7,933]		[5,004]	[1,576]	[1,631]	[1,296]		[-1,033]	[0,097]	[0,247]	[0,028]
β_{MID}			**0,216*****	**0,026**	**0,03449**			**0,219***	**0,335****	**0,34061****			**-0,135**	**-0,247**	**-0,16661**
			[4,394]	[0,43]	[0,546]			[1,795]	[2,156]	[2,197]			[-0,605]	[-0,779]	[-0,489]
β_{SHT}				**0,221*****	**0,20803*****				**-0,139**	**-0,10198**				**0,11**	**-0,03599**
				[4,65]	[4,232]				[-1,234]	[-0,885]				[0,512]	[-0,136]
β_{EX}					**0,07542****					**0,00369**					**0,24478**
					[2,431]					[0,057]					[1,136]
R^2	**0,010**	**0,650**	**0,652**	**0,662**	**0,673**	**0,679**	**0,709**	**0,721**	**0,720**	**0,730**	**0,780**	**0,856**	**0,849**	**0,841**	**0,837**
Significativ	***	***	***	***	***	***	***	***	***	***	***	***	***	***	***

Tabella 15: Applicazione dei modelli crypto-market based su BTC

3.4.2 Sintesi dei risultati su Ether

Analizzando il caso di Ether invece, si ottengono risultati diversi rispetto a quelli precedentemente analizzati: infatti, malgrado il fatto che, confrontando i valori di R^2 la capacità epesegetica dei modelli sia pressocché la stessa rispetto a Bitcoin negli orizzonti settimanali e mensili, i modelli multifattoriali danno un contributo notevole nel giustificare i rendimenti di ETH anche nella dimensione giornaliera, arrivando a valori di R^2 maggiori di 0.8 (rispetto a Bitcoin in cui non si superava il valore di 0.673). Analogamente a quanto accade con gli altri asset analizzati, i valori di alfa dei modelli studiati si mantengono estremamente piccoli e poco significativi. Tuttavia, la relazione tra Ether e l'indice $CRIX$ appare sensibilmente diversa rispetto al caso di Bitcoin. Infatti, nell'orizzonte settimanale e mensile essa è molto vicina ad 1 ed estremamente significativa soltanto finché si analizza il modello ad un unico fattore: poi, aumentando i fattori di rischio, il valore di R^2 aumenta notevolmente ed il coefficiente β_{CRIX} diminuisce sia nel valore che nella significatività. Al contrario, un ruolo centrale viene assunto dall'indice ALT rispetto al quale il coefficiente beta tende ad assumere valori sempre più vicini ad uno man a mano che si allarga l'orizzonte temporale considerato, evidenziando una prevedibile congruenza tra i movimenti di Ether e quelli delle principali criptovalute diverse da Bitcoin. Questa relazione, infatti, persiste generalmente con la stessa intensità e con la stessa significatività statistica nel corso dei diversi modelli fattoriali e degli orizzonti temporali analizzati. È curioso osservare anche che vi sia una debole relazione negativa, seppur statisticamente significativa, tra i rendimenti di Ether analizzati nella dimensione giornaliera e settimanale con quelli delle criptovalute collegate ai principali exchanges operanti sul mercato, forse in ragione del fatto che ETH e BNB possano farsi concorrenza in termini di potenzialità di utilizzo delle rispettive blockchains, sia per quanto riguarda la "messa a rendita" della criptovaluta mediante lo staking che per la realizzazione di applicazioni decentralizzate. Invece, contrariamente a quanto si potrebbe pensare, la relazione tra ETH e i rendimenti delle criptovalute a media capitalizzazione è generalmente modesta e statisticamente significativa soltanto nel modello a tre fattori analizzato su base giornaliera. Per quanto riguarda le criptovalute a bassa capitalizzazione invece, la relazione rimane contenuta e statisticamente significativa nella dimensione giornaliera, perdendo poi di significatività nei diversi orizzonti temporali fatto salvo quello mensile nel caso del modello a 4 fattori.

	ETH: Giornaliero					ETH: Settimanale					ETH: Mensile				
	CRIX	2-Fac	3-Fac	4-Fac	5-Fac	CRIX	2-Fac	3-Fac	4-Fac	5-Fac	CRIX	2-Fac	3-Fac	4-Fac	5-Fac
α_i	**0,0025***	**0,00083**	**0,00089**	**0,00091**	**0,00109**	**-0,00047**	**0,00802**	**0,00904**	**0,0089**	**0,01222**	**0,00764**	**0,05668**	**0,05611**	**0,056**	**0,03938**
	[1,726]	[0,996]	[1,067]	[1,088]	[1,231]	[-0,065]	[1,116]	[1,25]	[1,203]	[1,629]	[0,214]	[1,571]	[1,504]	[1,686]	[0,956]
β_{CRX}	**0,036**	**0,0465**	**0,046****	**0,04936****	**0,05482****	**0,99*****	**0,10274**	**0,114**	**0,12097**	**0,17076**	**0,988*****	**0,23678**	**0,237**	**0,11552**	**0,13878**
	[1,056]	[2,124]	[2,098]	[2,221]	[2,361]	[16,134]	[1,002]	[1,106]	[1,142]	[1,608]	[8,986]	[1,168]	[1,133]	[0,594]	[0,65]
β_{ALT}		**0,893*****	**0,751*****	**0,72771*****	**0,76145*****		**0,85*****	**0,935*****	**0,93536*****	**1,09832*****		**0,908*****	**0,82****	**1,05419****	**0,95653****
		[53,324]	[18,656]	[17,922]	[17,67]		[10,143]	[6,656]	[6,551]	[7,415]		[5,663]	[2,184]	[3]	[2,373]
β_{MID}			**0,166*****	**0,039**	**0,05221**			**-0,111**	**-0,068**	**-0,15815**			**0,089**	**-0,543**	**-0,45889**
			[3,739]	[0,693]	[0,887]			[-0,78]	[-0,373]	[-0,877]			[0,259]	[-1,281]	[-0,947]
β_{SHT}				**0,158*****	**0,18811*****				**-0,049**	**0,04364**				**0,624****	**0,57985**
				[3,651]	[4,103]				[-0,371]	[0,325]				[2,162]	[1,541]
β_{EX}					**-0,11582*****					**-0,24833*****					**0,13885**
					[-4,003]					[-3,32]					[0,453]
R^2	**0,001**	**0,827**	**0,825**	**0,828**	**0,829**	**0,598**	**0,752**	**0,753**	**0,749**	**0,774**	**0,680**	**0,843**	**0,832**	**0,867**	**0,850**
Significativ		***	***	***	***	***	***	***	***	***	***	***	***	***	***

Tabella 16: Applicazione dei modelli crypto-market based su ETH

3.4.3 Sintesi dei risultati su ChainLink

Per quanto riguarda l'applicazione dei modelli sui rendimenti di ChainLink invece, non è possibile formulare relazioni sistematicamente osservabili come in precedenza con Bitcoin rispetto al $CRIX$ esoprattutto con Ether rispetto all'indice ALT. Infatti, nell'orizzonte giornaliero gli extra-rendimenti di LINK appaiono leggermente sovra-reattivi rispetto a quelli dell'indice MID, osservando peraltro valori particolarmente più significativi rispetto a quelli di β_{ALT}, indice del quale fa parte. Nell'orizzonte settimanale invece, ogni n-esimo fattore di rischio che viene aggiunto si rivela essere quello più statisticamente significativo del modello analizzato, fatta eccezione per il modello a cinque fattori in cui β_{SHT} sopravvive ad un livello di significatività statistica dell'1% rispetto al 5% di β_{EX}. Infine, nell'orizzonte mensile, l'apparente significatività statistica delle relazioni con $CRIX$ e ALT viene tradita dal passaggio a modelli fattoriali successivi, probabilmente a causa della scarsità del numero di rilevazioni di questo orizzonte temporale. Analogamente ad Ether, anche ChainLink sembra presentare una debole relazione negativa rispetto ai rendimenti delle criptovalute degli exchange, ed il comportamento analogo potrebbe ricercarsi nel fatto che LINK sia un token ERC-20 della blockchain di ETH, e che pertanto sia inevitabilmente condizionato dal discreto antagonismo con la blockchain di BNB. Per quanto riguarda la relazione di LINK con le criptovalute a bassa capitalizzazione invece, i coefficienti crescono tendendo al valore unitario man a mano che si aumenta l'orizzonte temporale, anche se la significatività statistica dei valori ottenuti si rende apprezzabile solo nella dimensione settimanale. Inoltre, analogamente a quanto si osserva con Cardano, i valori di R^2 non sono elevatissimi registrando un massimo di 0.637 soltanto nella prospettiva mensile con il modello a 5 fattori, un valore piuttosto distante rispetto a quelli che si ottengono nei casi di BTC, ETH e BNB.

	LINK: Giornaliero					LINK: Settimanale					LINK: Mensile				
	CRIX	2-Fac	3-Fac	4-Fac	5-Fac	CRIX	2-Fac	3-Fac	4-Fac	5-Fac	CRIX	2-Fac	3-Fac	4-Fac	5-Fac
α_i	**0,00639*** **	**0,00288**	**0,0025**	**0,00255**	**0,00279**	**0,02758***	**0,02369**	**0,02365***	**0,02484***	**0,02747***	**0,12609**	**0,12209**	**0,11597**	**0,11577***	**0,09067**
	[2,898]	[1,515]	[1,484]	[1,505]	[1,549]	[1,841]	[1,608]	[1,7]	[1,805]	[1,949]	[1,412]	[1,71]	[1,694]	[1,867]	[1,172]
β_{CRX}	**-0,006**	**-0,01127**	**0**	**0,00198**	**-0,00005**	**0,966*** **	**-0,11669**	**-0,172**	**-0,2456**	**-0,23693**	**1,312*** **	**-0,14018**	**-0,137**	**-0,34883**	**-0,30748**
	[-0,121]	[-0,226]	[-0,018]	[0,044]	[-0,001]	[7,631]	[-0,555]	[-0,871]	[-1,247]	[-1,188]	[4,751]	[-0,349]	[-0,357]	[-0,96]	[-0,766]
β_{ALT}		**0,861*** **	**-0,12**	**-0,12886**	**-0,10743**		**0,875*** **	**0,132**	**0,12474**	**0,29235**		**1,164*** **	**0,211**	**0,6178**	**0,45034**
		[22,602]	[-1,484]	[-1,564]	[-1,225]		[5,095]	[0,489]	[0,469]	[1,05]		[3,668]	[0,307]	[0,941]	[0,594]
β_{MID}			**1,185*** **	**1,143*** **	**1,15469*** **			**0,936*** **	**0,452**	**0,36244**			**0,973**	**-0,127**	**0,0224**
			[13,281]	[9,947]	[9,649]			[3,403]	[1,326]	[1,07]			[1,539]	[-0,161]	[0,024]
β_{SHT}				**0,053**	**0,07285**				**0,557** **	**0,74685*** **				**1,086***	**1,00066**
				[0,602]	[0,781]				[2,253]	[2,966]				[2,016]	[1,415]
β_{EX}					**-0,07388**					**-0,32823** **					**0,224**
					[-1,255]					[-2,335]					[0,388]
R^2	**0,000**	**0,464**	**0,580**	**0,577**	**0,579**	**0,250**	**0,353**	**0,430**	**0,454**	**0,493**	**0,373**	**0,578**	**0,613**	**0,682**	**0,637**
Significativ		***	***	***	***	***	***	***	***	***	***	***	***	***	***

Tabella 17: Applicazione dei modelli crypto-market based su LINK

3.4.4 Sintesi dei risultati su Binance Coin

I rendimenti di Binance Coin evidenziano come nell'orizzonte giornaliero e mensile esista, seppur discreta, una relazione statisticamente significativa rispetto al fattore $CRIX$. Ciò che sorprende, e che sembrerebbe apparentemente tradire i ragionamenti fatti con ETH e LINK, è la relazione positiva e statisticamente significativa tra i rendimenti di questo asset e quelli dell'indice ALT, soprattutto nella dimensione giornaliera e settimanale, anche se l'intensità del relativo coefficiente diminuisce nel passaggio a modelli fattoriali successivi (diventando negativa nel caso dell'orizzonte mensile). La situazione potrebbe spiegarsi affermando che, se è vero che ETH in questa fase possa subire la concorrenza di BNB, non è necessariamente vero il contrario, in ragione del fatto che ad oggi, prima dell'aggiornamento di Ethereum, la Binance Smart Chain offra transazioni più rapide e a minor costo rispetto al suo competitor, pur non godendo del grado di decentralizzazione di Ethereum. In altre parole, si potrebbe dire che la BSC risolvi il "trilemma" tra decentralizzazione, scalabilità e sicurezza della rete sacrificando la prima a vantaggio delle altre due. Inoltre, il peso di BNB all'interno dell'indice EX è superiore rispetto a quello di ETH nel rispettivo indice ALT, poiché in entrambi casi gli indici sono equiponderati e la numerosità del secondo è superiore rispetto a quella del primo. Il contributo epesegetico del fattore EX è ovviamente evidente osservando la variazione del valore di R^2 passando dai 4 ai 5 fattori, indipendentemente dall'orizzonte temporale considerato. Il coefficiente β_{EX} infatti è il più significativo a livello statistico rispetto a ciascun coefficiente appartenente al medesimo orizzonte temporale. I rendimenti di BNB sembrano particolarmente sincronizzati con quelli dell'indice di cui ne fa parte, fatto salvo l'orizzonte mensile in cui sembrano leggermente meno reattivi.

	BNB: Giornaliero					BNB: Settimanale					BNB: Mensile				
	CRIX	2-Fac	3-Fac	4-Fac	5-Fac	CRIX	2-Fac	3-Fac	4-Fac	5-Fac	CRIX	2-Fac	3-Fac	4-Fac	5-Fac
α_i	**0,00568*** **	**0,00177**	**0,00144**	**0,00127**	**0,00009**	**0,02361***	**0,00909**	**0,00784**	**0,00832**	**-0,00043**	**0,05151**	**-0,01557**	**-0,01857**	**-0,01858**	**-0,01464**
	[3,03]	[1,047]	[0,845]	[0,756]	[0,091]	[1,817]	[0,617]	[0,527]	[0,559]	[-0,053]	[0,7]	[-0,432]	[-0,535]	[-0,516]	[-0,505]
β_{CRX}	**0,063**	**0,10509**	**0,111****	**0,11179****	**0,05993****	**0,977*****	**0,25217**	**0,225**	**0,16782**	**-0,01528**	**1,151*****	**0,40512**	**0,406***	**0,39459***	**0,34614****
	[1,411]	[2,373]	[2,465]	[2,502]	[2,163]	[8,906]	[1,199]	[1,064]	[0,787]	[-0,133]	[5,054]	[2,002]	[2,088]	[1,872]	[2,306]
β_{ALT}		**0,868*****	**0,665*****	**0,59653*****	**0,19697*****		**0,977*****	**0,701****	**0,68887****	**-0,07339**		**0,381****	**-0,085**	**-0,06266**	**-0,28798**
		[25,617]	[8,117]	[7,308]	[3,832]		[5,683]	[2,433]	[2,399]	[-0,457]		[2,379]	[-0,244]	[-0,164]	[-1,016]
β_{MID}			**0,254*****	**-0,122**	**-0,18936*****			**0,353**	**-0,066**	**0,32056**			**0,477**	**0,414**	**0,74313***
			[2,808]	[-1,071]	[-2,698]			[1,202]	[-0,181]	[1,642]			[1,487]	[0,903]	[2,182]
β_{SHT}				**0,467*****	**0,18557*****				**0,49***	**0,01967**				**0,061**	**-0,49267***
				[5,335]	[3,393]				[1,832]	[0,135]				[0,196]	[-1,862]
β_{EX}					**1,09965*****					**1,16158*****					**0,76008*****
					[31,866]					[14,346]					[3,527]
R^2	**0,002**	**0,523**	**0,524**	**0,544**	**0,843**	**0,312**	**0,524**	**0,527**	**0,537**	**0,881**	**0,402**	**0,666**	**0,691**	**0,668**	**0,814**
Significativ		***	***	***	***	***	***	***	***	***	***	***	***	***	***

Tabella 18: Applicazione dei modelli crypto-market based su BNB

3.4.5 Sintesi dei risultati su Cardano

Come anticipato, Cardano è insieme a ChainLink la criptovaluta i cui rendimenti trovano minor grado di spiegazione da parte dei seguenti modelli. Infatti, i valori degli R^2, seppur sempre maggiori di 0.5, sono generalmente quelli più bassi rispetto ai casi precedentemente analizzati, mentre gli alfa sono relativamente alti e statisticamente significativi, soprattutto nell'orizzonte giornaliero. In ogni caso, la relazione tra i rendimenti di questo asset e quelli dell'indice MID è statisticamente significativa fino all'orizzonte settimanale, quando assume i valori più alti. Questa evidenza appare particolarmente importante confrontando la relazione che l'asset ha con il suo indice di appartenenza, ALT: il coefficiente β_{ALT} diminuisce all'aumentare dei fattori di rischio considerati nel modello, ed il livello di significatività statistica nell'orizzonte settimanale arriva fino al 10%, mentre la significatività statistica ed il valore del coefficiente β_{MID} (indice di cui l'asset non fa parte) persistono sugli stessi livelli.

	ADA: Giornaliero					ADA: Settimanale					ADA: Mensile				
	CRIX	2-Fac	3-Fac	4-Fac	5-Fac	CRIX	2-Fac	3-Fac	4-Fac	5-Fac	CRIX	2-Fac	3-Fac	4-Fac	5-Fac
α_i	**0,00571****	**0,00351****	**0,00336****	**0,00345****	**0,00381****	**0,01795**	**0,01935***	**0,01784****	**0,01653***	**0,01655***	**0,04882**	**0,07779**	**0,07109**	**0,07106**	**0,07985**
	[2,383]	[2,294]	[2,354]	[2,397]	[2,512]	[0,839]	[1,843]	[2]	[1,828]	[1,708]	[0,352]	[1,197]	[1,186]	[1,146]	[1,011]
β_{CRX}	**0,154*****	**0,00746****	**0,01**	**0,00988**	**0,02125**	**1,542*****	**-0,06936***	**-0,138**	**-0,1105**	**-0,10052**	**2,769*****	**-0,01961**	**-0,016**	**-0,04693**	**-0,04005**
	[2,687]	[0,186]	[0,283]	[0,258]	[0,534]	[8,525]	[-0,463]	[-1,086]	[-0,853]	[-0,732]	[6,464]	[-0,053]	[-0,049]	[-0,129]	[-0,097]
β_{ALT}		**0,924*****	**0,279*****	**0,2861*****	**0,36037*****		**1,186*****	**0,371****	**0,36172****	**0,3383***		**1,261*****	**0,218**	**0,27742**	**0,4191**
		[30,242]	[4,074]	[4,097]	[4,885]		[9,688]	[2,147]	[2,073]	[1,767]		[4,365]	[0,362]	[0,422]	[0,542]
β_{MID}			**0,783*****	**0,833*****	**0,83049*****			**1,033*****	**1,146*****	**1,17626*****			**1,065***	**0,907**	**0,73402**
			[10,351]	[8,545]	[8,246]			[5,857]	[5,112]	[5,05]			[1,924]	[1,146]	[0,79]
β_{SHT}				**-0,057**	**-0,00522**				**-0,117**	**-0,17362**				**0,156**	**0,39444**
				[-0,764]	[-0,066]				[-0,725]	[-1,002]				[0,29]	[0,546]
β_{EX}					**-0,18744*****					**0,05847**					**-0,37934**
					[-3,785]					[0,605]					[-0,645]
R^2	**0,006**	**0,607**	**0,659**	**0,658**	**0,663**	**0,293**	**0,690**	**0,781**	**0,782**	**0,783**	**0,524**	**0,693**	**0,740**	**0,722**	**0,666**
Significativ	***	***	***	***	***	***	***	***	***	***	***	***	***	***	***

Tabella 19: Applicazione dei modelli crypto-market based su ADA

CAPITOLO 4

LA MODERN PORTFOLIO THEORY NEL MERCATO DELLE CRIPTOVALUTE

4.1 La convenienza dell'approccio Media-Varianza

La Teoria Moderna del Portafoglio, nata a partire dagli studi di Harry Markowitz, parte dal presupposto per cui le generiche funzioni di utilità degli investitori descrivano uno stato di avversione al rischio nelle scelte dell'investimento. Intendendo per "rischio" la variabilità dei risultati alternativi dell'investimento a seconda dei diversi stati del mondo, gli investitori sceglierebbero sicuramente una strategia in grado di pronosticare un certo rendimento atteso con quanta minore volatilità possibile, poiché soltanto in caso di minore volatilità vi sarà maggiore verosimiglianza a conseguire il rendimento stimato. In altre parole, "l'attendibilità" del rendimento atteso è inversamente proporzionale alla varianza, poiché in presenza di un'alta volatilità sarà maggiore la probabilità di ottenere *ex-post* un rendimento distante da quello pronosticato, il quale corrisponderà alla media (aritmetica o ponderata a seconda della distribuzione di probabilità dei diversi stati del mondo) dei rendimenti pronosticabili. Ovviamente, a livello statistico, questo si spiega a seconda della "larghezza" della curva dei rendimenti che si potranno ottenere. La distribuzione dei rendimenti, in forza del teorema del limite centrale, tenderà ad approssimare una distribuzione gaussiana all'aumentare dei potenziali rendimenti conseguibili dall'investimento. In uno stato di razionalità limitata, come quello in cui si trova il generico investitore, i diversi rendimenti potenziali di uno strumento finanziario possono essere determinati soltanto sulla base dell'analisi storica dei suoi rendimenti, assumendo che la loro distribuzione rimanga la stessa anche in futuro e che quindi, in termini di volatilità dei ritorni economici conseguibili, lo strumento "continui a comportarsi come si è sempre comportato". Per questo motivo, nell'impossibilità di stabilire un'efficace relazione causale tra i diversi stati del mondo ed i rendimenti conseguibili che ne deriverebbero, la distribuzione dei rendimenti studiata dall'investitore è quella costruita a partire dalla loro analisi storica. In ragione di ciò, dopo aver collezionato un certo numero di rendimenti storici, il rendimento atteso di un certo asset non potrà che essere la loro media aritmetica, assumendo un'omogenea distribuzione di probabilità tra i diversi stati del mondo. Per questo motivo, confrontando due strumenti che, storicamente, hanno sempre offerto lo stesso rendimento medio, l'investitore razionale sceglierà lo strumento che in passato ha presentato quel rendimento con minore volatilità, poiché a questa scelta sarà associato un livello di utilità superiore. Per questo motivo, la funzione di utilità del generico investitore sarà positiva rispetto al rendimento e negativa rispetto alla volatilità, ottenendo la seguente schematizzazione:

$$U(E[r_i]; \sigma_i^2) \begin{cases} \dfrac{\partial U}{\partial E[r]} > 0 \\ \dfrac{\partial U}{\partial \sigma_i} < 0 \end{cases}$$

Con approccio microeconomico, la funzione di utilità può essere impiegata nel descrivere la curva di indifferenza dell'investitore, ossia quell'insieme di opportunità di investimento le cui combinazioni di rendimento-rischio producono lo stesso livello di utilità e che, pertanto, risultano interscambiabili per l'investitore stesso. Per questo motivo, un'opportunità di investimento caratterizzata da un'unità di rischio aggiuntiva rispetto ad un'alternativa di investimento giacerà lungo la sua stessa curva di indifferenza soltanto se presenterà un rendimento superiore in misura variabile a seconda del grado di avversione al rischio dell'investitore stesso. In altre parole, quanto maggiore sarà l'avversione al rischio, altrettanto maggiore sarà il rendimento che si richiederà dall'investimento all'aumentare del suo rischio. A livello grafico, ponendo sulle ascisse la volatilità dell'investimento e sulle ordinate il suo rendimento atteso, questa situazione si spiega attraverso una curva di indifferenza che avrà pendenza positiva e convessità tanto maggiore quanto maggiore sarà l'avversione al rischio avvertita dall'investitore. Pertanto, assumendo che l'avversione al rischio sia tale da richiedere un incremento più che proporzionale del rendimento rispetto all'incremento marginale del rischio, si ottiene che la derivata seconda di questa curva di indifferenza sia positiva, e tanto più positiva quanto più l'investitore sarà avverso al rischio

$$\frac{\partial^2 E[r_i]}{\partial \sigma_i^2} > 0$$

Per questo motivo, gli investitori razionali cercheranno di massimizzare la propria utilità cercando opportunità di investimento che, a parità di rischio, permettano di massimizzare il rendimento. Il dominio di questa funzione di utilità corrisponde all'insieme di tutte le combinazioni di investimento possibili che, anche nel caso in cui non sono direttamente osservabili sul mercato, possono scaturire dalle diverse aggregazioni dei singoli prodotti finanziari. Ovviamente l'investitore è libero di allocare il suo capitale presso un unico prodotto finanziario, ma questa scelta appare necessariamente subottimale se, alla luce delle considerazioni fatte in merito al rischio idiosincratico nel capitolo 2, viene confrontata con l'opportunità di combinare quell'asset insieme ad altri prodotti finanziari al fine di ottenere una formula di investimento che, pur promettendo lo stesso rendimento, promette altresì minore volatilità nel conseguirlo. In altre parole, la scelta di fare *all-in* presso un unico strumento finanziario, sperando che esso ottenga una performance di rendimento superiore rispetto a quelle delle altre opportunità di investimento, impone il costo-opportunità di rinunciare ai benefici tipici della diversificazione. Pertanto, a meno che non si vantino poteri divinatori o informazioni private di cui disporre, la scelta di investimento razionale, che non si abbandona alla semplice "fortuna" delle conseguenze, dovrebbe vertere verso l'opportunità di diversificare. In ogni caso, assumendo che esistano n-titoli, la rappresentazione grafica di ciascuno di essi sarebbe quella di un punto sul grafico rischio-rendimento e pertanto, l'universo finanziario apparirebbe come una "nuvola" di punti, caratterizzato dall'esistenza di opportunità di investimento più efficienti di altre perché in grado di promettere un maggior rendimento al massimo allo stesso rischio. Tuttavia, come discusso, la scelta dell'investitore non dovrebbe ricadere su quei singoli asset, poiché parte della loro rischiosità risulterà caratterizzata da una parte idiosincratica eliminabile

per mezzo della diversificazione. Infatti, la rappresentazione grafica di un'efficace diversificazione corrisponde ad una curva in grado di perimetrare superiormente la nuvola di punti appena descritta, offrendo così strategie di investimento (nella forma di portafogli di investimento) sistematicamente più efficienti rispetto a qualsiasi opportunità presente sul mercato, almeno fintanto che non si ammette l'opportunità di indebitarsi e prestare il capitale al tasso privo di rischio. Questa curva, non a caso, prende il nome di *frontiera efficiente*, e agisce come vincolo di bilancio nel problema di massimizzazione vincolata dell'utilità dell'investitore. Infatti, lo stesso investitore che aveva deciso di investire tutto il suo capitale in un unico prodotto finanziario, si renderà conto dell'esistenza di un'opportunità di investimento più efficiente associata allo stesso livello di rischio che aveva sopportato fino a quel momento: pertanto, la scelta di investire nel portafoglio presente lungo la frontiera efficiente, in corrispondenza di quel livello di volatilità, permetterà all'investitore di muovere verticalmente la propria curva di indifferenza, sbloccando in questo modo valori di utilità superiori. In definitiva, la scelta razionale di quell'investitore giacerà in corrispondenza del punto di tangenza tra la sua curva di indifferenza e la *frontiera efficiente*. Ammettendo la possibilità di indebitarsi e prestare capitale al tasso privo di rischio però, si rende subottimale anche la scelta di acquistare un portafoglio presente lungo la frontiera efficiente, a meno che non si tratti di un certo portafoglio presente su essa. Infatti, con la "tecnologia" del prestito e dell'indebitamento al tasso privo di rischio, l'investitore potrà costruirsi opportunità di investimento date dalla combinazione del titolo privo di rischio e di portafogli efficienti ma rischiosi. Infatti, scegliendo di combinare un portafoglio efficiente e meno rischioso, rispetto a quello scelta in precedenza, con il tasso privo di rischio, si potrà ottenere un portafoglio più efficiente rispetto a quello precedentemente scelto e presente lungo la frontiera. Infatti, l'insieme di combinazioni del titolo privo di rischio ed un certo portafoglio rischioso efficiente è rappresentabile attraverso una retta avente come intercetta verticale il tasso *risk free* e come equazione quella che scaturisce dall'interpolazione lineare tra i due punti. Ricordando che la deviazione standard del titolo risk free sia nulla, si ottiene il sentiero rischio-rendimento di queste nuove opportunità di investimento

$$E[r_p] = r_f + \frac{E[r_i] - r_f}{\sigma_i}\sigma_p$$

Ovviamente, a seconda dei portafogli efficienti e rischiosi che vengono scelti, si ottengono rette più o meno inclinate, poiché diversa sarà l'interpolazione lineare che verrà eseguita. Per questo motivo, tutte le combinazioni di un certo portafoglio rischioso efficiente ed il titolo privo di rischio potranno risultare sistematicamente inefficienti se esiste una retta caratterizzata da una maggiore pendenza descrivente combinazioni di titolo *risk free* ed un altro portafoglio. Quindi, in presenza della "tecnologia" del debito e del prestito al tasso risk-free, l'investitore è chiamato a risolvere il problema di massimizzazione del coefficiente angolare di questa retta sotto il vincolo di dover compiere l'interpolazione lineare necessariamente con un punto presente lungo la frontiera efficiente. Quello che si ottiene è una retta che massimizza il proprio coefficiente angolare risultando tangente alla frontiera efficiente. Questa retta, fintanto che si analizza

l'universo dei prodotti finanziari, è detta *capital market line* mentre, se l'analisi si limita ad un sottoinsieme dell'intero mercato, viene definita *capital allocation line*.

La frontiera efficiente, in corrispondenza del punto di tangenza con la *capital allocation line*, presenta lo stesso coefficiente angolare della retta, ossia il coefficiente angolare massimizzato. Per questo motivo, il portafoglio associato al punto di tangenza tra le due curve (detto appunto "*tangency portfolio*") sarà il portafoglio di titoli rischiosi caratterizzato dal massimo valore possibile del coefficiente angolare della CAL, ossia sarà il portafoglio in corrispondenza del quale il valore di $\frac{E[r_i]-r_f}{\sigma_i}$ risulterà massimizzato. In altre parole, il "*tangency portfolio*" è quel portafoglio che massimizza lo Sharpe ratio ed è definito per questo motivo "portafoglio ottimo". L'assunzione della Modern Portfolio Theory è che gli investitori razionali, pur non avendo la possibilità di indebitarsi o prestare al tasso privo di rischio, scelgano il portafoglio che risolve questo ipotetico problema di massimizzazione vincolata del coefficiente angolare della CAL, ossia il portafoglio ottimo.

Le scelte razionali di investimento pertanto, secondo la MPT, consisterebbero nella costruzione del portafoglio ottimo a partire da un insieme di opportunità di investimento disponibili. Ammettendo un portafoglio costituito da soli due titoli, la varianza di tale portafoglio sarà pari a

$$\sigma_r^2 = y_i^2\sigma_i^2 + y_j^2\sigma_j^2 + 2y_i y_j \sigma_{i,j}$$

Ricordando che la varianza di un dataset sia pari alla covarianza che ha con sé stesso, questa formula può essere generalizzata al fine di ottenere la costruzione di un portafoglio costituito da n titoli

$$\sigma_r^2 = \sum_{i=1}^{n}\sum_{j=1}^{n} y_i y_j \sigma_{i,j}$$

Invece, come già evidenziato nel capitolo 2.3.1, per la determinazione del rendimento atteso di un portafoglio potrà essere sfruttata la linearità al fine ed utilizzare quindi la media ponderata dei rendimenti attesi

$$E[r_r] = \sum_{i=1}^{n} y_i E[r_i]$$

Alternativamente, rendimento atteso e varianza di un portafoglio titolo possono essere determinati attraverso prodotti tra matrici. Nel caso del rendimento atteso, sarà sufficiente fare il prodotto tra il vettore riga dei pesi ed il vettore colonna dei rendimenti attesi. Nel caso della varianza invece, bisognerà moltiplicare il vettore riga dei pesi per la matrice delle covarianze e moltiplicare nuovamente per il vettore colonna dei pesi. Assumendo che si stiano considerando n titoli, la matrice delle covarianze è di dimensioni $n \times n$ ed ha la particolarità di essere una matrice simmetrica, pertanto i valori che si collocano lungo un'i-esima riga sono gli stessi che si collocano la j-esima colonna dello stesso indice. La diagonale di questa matrice simmetrica è costituita dalle varianze dei titoli considerati, poiché i valori restituiti sono pari alle covarianze dei titoli con sé stessi. Il vettore colonna dei pesi ed il vettore colonna dei rendimenti attesi hanno entrambi dimensioni

$n \times 1$, mentre il vettore riga dei pesi ha dimensioni $1 \times n$. Sia per il rendimento atteso che per la varianza, il risultato finale è una matrice 1×1 e pertanto un unico valore, in ragione del fatto che le matrici risultanti dal prodotto hanno come numero di righe quello del primo fattore, e come numero di colonne quello del secondo.

$$E[r_r] = [y_1, y_2, \dots, y_i] * \begin{bmatrix} E[r_1], \\ E[r_2], \\ \dots, \\ E[r_i] \end{bmatrix} = \left[\sum_{i=1}^{n} y_i E[r_i]\right]$$

$$\sigma_r^2 = [y_1, y_2, \dots, y_i] * \begin{bmatrix} \sigma_{1,1}, \sigma_{1,2}, \dots, \sigma_{1,j} \\ \sigma_{2,1}, \sigma_{2,2}, \dots, \sigma_{2,j} \\ \dots \quad \dots \quad \dots \quad \dots \\ \sigma_{i,1}, \sigma_{i,2}, \dots, \sigma_{i,j} \end{bmatrix} * \begin{bmatrix} y_1, \\ y_2, \\ \dots, \\ y_j \end{bmatrix}$$

$$\sigma_r^2 = \left[\sum_{i=1}^{n} y_i \sigma_{i,1}, \sum_{i=1}^{n} y_i \sigma_{i,2}, \dots, \sum_{i=1}^{n} y_i \sigma_{i,j}\right] * \begin{bmatrix} y_1, \\ y_2, \\ \dots, \\ y_j \end{bmatrix} = \left[\sum_{i=1}^{n} y_i y_1 \sigma_{i,1} + \sum_{i=1}^{n} y_i y_2 \sigma_{i,2} + \cdots \sum_{i=1}^{n} y_i y_j \sigma_{i,j}\right]$$

$$\sigma_r^2 = \left[\sum_{i=1}^{n} \sum_{j=1}^{n} y_i y_j \sigma_{i,j}\right]$$

Pertanto, ricordando che la caratteristica tipica del portafoglio ottimo sia quella di avere il massimo Sharpe ratio, sarà possibile individuare la distribuzione dei pesi dei titoli rischiosi che lo comporranno impostando un problema di massimizzazione vincolata. La funzione da massimizzare sarà appunto quella dello Sharpe Ratio mentre il vincolo da rispettare sarà quello per cui la distribuzione dei titoli esaurisca la totalità del portafoglio: in altre parole, la somma dei pesi dovrà essere pari a uno. Inoltre, ammettendo l'impossibilità di indebitarsi al tasso risk free o di vendere allo scoperto determinati titoli al fine di ottenere il capitale per acquistarne di altri, è anche necessario che ciascun peso sia maggiore o uguale a zero. In sintesi, il problema di massimizzazione vincolata viene schematizzato come segue:

$$\begin{cases} \sigma_r^2 = \sum_{i=1}^{n} \sum_{j=1}^{n} y_i y_j \sigma_{i,j} \\ E[r_r] = \sum_{i=1}^{n} y_i E[r_i] \\ Sharpe = \dfrac{E[r_r]}{\sigma_r} = \dfrac{\sum_{i=1}^{n} y_i E[r_i]}{\sqrt{\sum_{i=1}^{n} \sum_{j=1}^{n} y_i y_j \sigma_{i,j}}} \end{cases}$$

$$\max \frac{\sum_{i=1}^{n} y_i E[r_i]}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} y_i y_j \sigma_{i,j}}}$$

sub:

$$1) \sum_{i=1}^{n} y_i = 1$$

$$2) \ 0 \leq y_i \leq 1$$

Il risultato di questo problema di massimizzazione è un vettore di dimensioni $1 \times n$ contenente i pesi di ciascun titolo che devono essere presenti al fine di ottenere la combinazione associata al portafoglio ottimo (e pertanto il portafoglio con maggior Sharpe Ratio possibile)

$$Y^* = [y_1^*, y_2^*, \dots, y_n^*]$$

All'atto pratico, l'individuazione del portafoglio ottimo è possibile mediante calcolatori come Excel, utilizzando il componente aggiuntivo "Risolutore" che, una volta impostato il problema di massimizzazione vincolata, individuerà il vettore dei pesi ottimi attraverso il motore di ottimizzazione "GRG non lineare".

Di seguito si andranno a studiare le caratteristiche dei portafogli ottimi delle criptovalute sulla base dei valori di mercato giornalieri, settimanali e mensili. Lo studio è stato condotto utilizzando un programma[26] in JavaScript realizzato appositamente per questa trattazione e reso open-source su GitHub sotto licenza General Public License 3.0. Si è preferito seguire questo approccio poiché lo scaricamento manuale dei dati di prezzo riferiti al maggior numero di criptovalute possibili, nonché i calcoli richiesti per l'impostazione e la risoluzione del problema di massimizzazione vincolata necessari per la determinazione dello Sharpe Ratio, sarebbe risultato eccessivamente dispendioso in termini di tempo e capacità computazionale.

Il programma, utilizzando chiamate API, permette di scaricare tutte le candele di prezzo di tutte le criptovalute listate sull'exchange Binance.com, riferite ad un certo *timeframe* e ad un certo *quote asset* (ossia l'asset in base al quale se ne esprime il valore). Quindi, dopo aver specificato un numero minimo di candele di prezzo che devono essere presenti per ciascuna coppia (così da filtrare le criptovalute che sono state aggiunte troppo recentemente sull'exchange) il numero di candele di ciascuna coppia viene tagliato per il numero minimo di candele presenti tra le coppie filtrate, al fine di ottenere un dataset omogeneo sia in termini temporali che di numerosità di rilevazioni. Pertanto, ottenuto il dataset, vengono calcolate misure di statistica descrittiva per ciascuna coppia, tra cui rendimento medio e deviazione standard. Successivamente, viene calcolata la successione storica dei rendimenti di ciascuna criptovaluta e, una volta aggregati i risultati, il programma calcola la matrice delle covarianze avvalendosi della *library* "portfolio-allocation"[27] pubblicata in forma *open-source* dal programmatore francese Roman Rubsamen ("lequant40" su GitHub). Quindi, richiamando ancora una volta le funzioni di questa *library*, si procede al calcolo della frontiere efficiente, del portafoglio ottimo e

[26] https://github.com/fedemagnani/Binance_Watcher.js
[27] https://github.com/lequant40/portfolio_allocation_js

del *minimum variance portfolio*, ottenendone i rispettivi vettori dei pesi. Il calcolo del portafoglio ottimo assume un tasso risk-free nullo, così come evidenziato dalle rilevazioni presenti sul sito di Kenneth French. Il portafoglio MVP (*minimum variance portfolio*) è il portafoglio collocato sulla frontiera efficiente a cui è associato il minor rischio possibile e quindi, per definizione, anche il minor rendimento. Il portafoglio MVP coincide con il portafoglio ottimo soltanto nel caso in cui ad esso sia associata una deviazione standard nulla (e pertanto lo Sharpe Ratio risulta sicuramente massimizzato), una situazione limite che si verifica soltanto nel caso in cui, in ragione di una perfetta correlazione negativa tra gli asset considerati, la rappresentazione grafica della frontiera efficiente assume la forma di una retta avente un'intercetta verticale: in questo caso, il punto associato all'intercetta verticale della frontiera efficiente è esattamente il portafoglio MVP (nonché il portafoglio ottimo), ossia quel portafoglio che riesce a sintetizzare il titolo privo di rischio a partire dall'aggregazione di titoli rischiosi, proprio in ragione di una loro perfetta correlazione negativa. Tuttavia, a causa della difficoltà di trovare una persistente e perfetta correlazione negativa tra i rendimenti di diversi asset, il portafoglio MVP e quello ottimo sono tipicamente separati ed al primo è associato un rendimento inferiore del secondo (e questo ovviamente vale anche per la deviazione standard).

I pesi del portafoglio MVP sono la soluzione del problema di minimizzazione vincolata della varianza di portafoglio. Richiamando le formule viste in precedenza per il portafoglio ottimo, il problema di minimizzazione vincolata può essere impostato nel modo seguente

$$\min \sum_{i=1}^{n}\sum_{j=1}^{n} y_i y_j \sigma_{i,j}$$

$$sub:$$

$$1) \sum_{i=1}^{n} y_i = 1$$

$$2)\ 0 \leq y_i \leq 1$$

Quindi, una volta calcolati i vettori dei pesi, si procede al calcolo di rendimento atteso e deviazione standard di ciascun portafoglio attraverso i prodotti tra matrici come descritto in precedenza. Queste metriche sono confrontabili con rendimento atteso e deviazione standard delle criptovalute di cui si è parlato inizialmente, poiché vengono calcolate a partire dai loro stessi dataset. Infine, utilizzando la *library* "*Chart.js*"[28] implementata su un'applicazione *Electron*, tutte le criptovalute filtrate ed i portafogli efficienti calcolati a partire da esse vengono rappresentati attraverso un grafico a dispersione utilizzando deviazione standard e rendimento atteso come coordinate cartesiane.

Si è scelto di utilizzare un numero minimo di 500, 72 e di 17 candele rispettivamente per l'analisi giornaliera, settimanale e mensile al fine di ottenere un dataset inclusivo al tempo stesso delle prime criptovalute di terza generazione, spesso trascurate dalla letteratura accademica. In oro, grigio, celeste, giallo e blu sono

[28] https://github.com/chartjs/Chart.js

rappresentati graficamente Bitcoin, Ether, ChainLink, Binance Coin e Cardano. In verde è rappresentato il portafoglio ottimo mentre in rosa il portafoglio MVP.

4.2 Studio del portafoglio ottimo basato su USDT

L'analisi è stata condotta su 77 criptovalute. Effettuando un'analisi multi-timeframe si evince che Cardano abbia prodotto risultati più efficienti rispetto a Binane Coin nell'orizzonte giornaliero e settimanale, offrendo un rendimento medio superiore con minore volatilità. La maggiore efficienza di Cardano emerge anche dal confronto con ChainLInk nell'orizzonte giornaliero. Nell'orizzonte mensile invece, non c'è una criptovaluta più efficiente delle altre, dal momento che esse sembrano distribuirsi lungo un medesimo sentiero rendimento-rischio, offrendo un maggiore rendimento in presenza di maggiore volatilità. Bitcoin si rivela la criptovaluta sistematicamente meno volatile su tutti i timeframe considerati; tuttavia, perseguendo un approccio basato sulla minimizzazione della volatilità dell'investimento, si dovrebbe valutare l'opzione offerta dal portafoglio MVP che, sfruttando i benefici della diversificazione, promette risultati più efficienti rispetto a quelli di Bitcoin, offrendo un maggior rendimento a minor rischio. Studiando il portafoglio ottimo, il beneficio apportato dall'effetto diversificazione è apprezzabile soltanto in termini relativi: infatti, la grande distanza tra lo Sharpe Ratio del portafoglio PFT e quelli delle singole criptovalute evidenzia una notevole eliminazione del rischio idiosincratico, ma dal momento che lo Sharpe Ratio si mantiene generalmente basso si evince la notevole difficoltà nel formulare strategie di investimento che siano desiderabilmente remunerative del proprio rischio. Questo potrebbe dipendere da una forte presenza della componente sistematica di rischio per cui, pur verificandosi una significativa eliminazione della componente idiosincratica, la rischiosità resultante rimane particolarmente alta. Il tutto si riassume in un'unica conclusione: il mercato delle criptovalute è rischioso.
Di seguito le rappresentazioni grafiche delle strategie di investimento, evidenziando a fianco il vettore dei pesi associato al portafoglio ottimo (di ciascuna criptovaluta ne viene evidenziata la coppia, quindi nella dicitura viene richiamato anche "USDT", ossia il *quote asset*).

DAILY	*PFT*	*MVP*	*BTC*	*ETH*	*LINK*	*BNB*	*ADA*
E[r]	1,27%	0,47%	0,39%	0,72%	0,72%	0,82%	0,96%
σ	6,23%	4,17%	4,24%	5,67%	7,28%	7,07%	6,89%
Sharpe	0,203789	0,111652	0,092745	0,126218	0,098733	0,116452	0,139121
WEEKLY							
E[r]	7,98%	3,16%	2,67%	4,89%	5,08%	6,32%	6,89%
σ	15,49%	10,47%	10,92%	14,33%	19,78%	23,59%	19,88%
Sharpe	0,515193	0,301603	0,24491	0,341356	0,25685	0,268128	0,346503
MONTHLY							
E[r]	28,99%	16,67%	15,83%	25,02%	28,58%	41,97%	39,71%
σ	24,53%	17,43%	20,57%	29,44%	41,69%	90,65%	73,33%
Sharpe	1,181772	0,956511	0,769402	0,850072	0,685521	0,462993	0,541581

Tabella 20: Sintesi delle performance di portafoglio

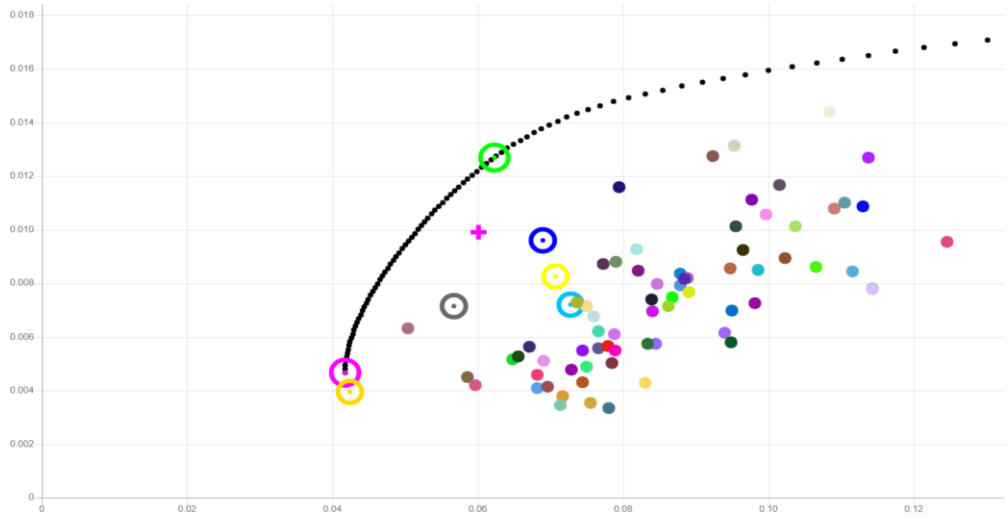


Grafico 3: Sintesi performance giornaliere e composizione del portafoglio ottimo

ADAUSDT	16,90%
ANKRUSDT	14,24%
BANDUSDT	5,53%
CVCUSDT	0,50%
DENTUSDT	1,43%
DOGEUSDT	9,29%
HBARUSDT	2,80%
MATICUSDT	12,85%
MTLUSDT	2,01%
NKNUSDT	8,16%
ONEUSDT	0,00%
TFUELUSDT	18,39%
THETAUSDT	7,89%

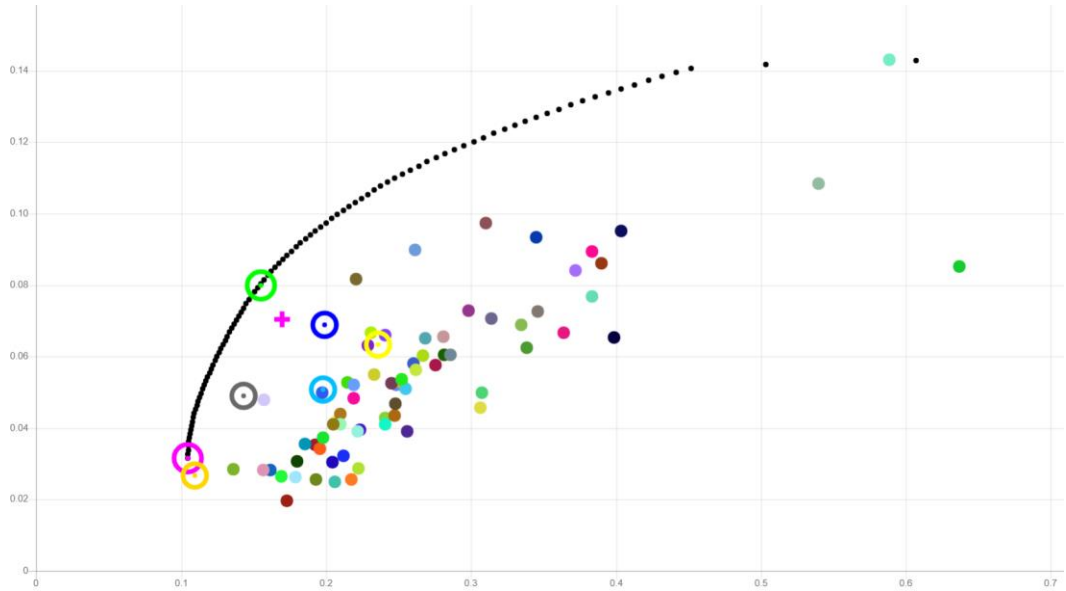


Grafico 2: Sintesi performance settimanali e composizione del portafoglio ottimo

ADAUSDT	21,67%
ANKRUSDT	4,58%
BANDUSDT	3,90%
CVCUSDT	1,53%
DOGEUSDT	9,49%
ENJUSDT	1,50%
ETHUSDT	0,72%
FTMUSDT	0,54%
HBARUSDT	3,62%
MATICUSDT	5,52%
MTLUSDT	6,33%
NKNUSDT	1,17%
ONGUSDT	3,76%
TFUELUSDT	2,48%
THETAUSDT	23,47%
WAVESUSDT	9,71%

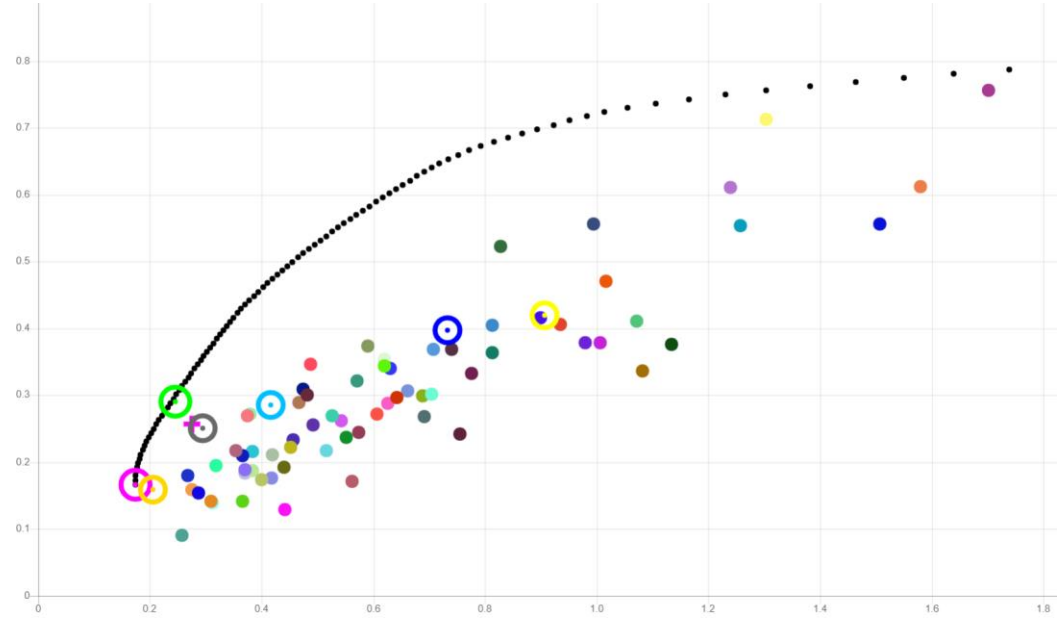


Grafico 1: Sintesi performance mensili e composizione del portafoglio ottimo

ADAUSDT	1,43%
BANDUSDT	2,62%
DOGEUSDT	0,42%
FUNUSDT	6,74%
HBARUSDT	4,22%
RENUSDT	0,51%
THETAUSDT	9,42%
TOMOUSDT	0,65%
WAVESUSDT	28,38%
XMRUSDT	35,08%
ZILUSDT	10,52%

4.3 I risultati di uno studio empirico

I risultati di questa analisi sembrano confermare empiricamente gli studi di Brauneis e Mestel (2018) portando alla conclusione che l'approccio media-varianza, fulcro della *Modern Portfolio Theory*, non sia una strategia di investimento efficace nelle criptovalute, almeno non quanto ci si aspetterebbe. I due studiosi, infatti, collezionando le informazioni giornaliere di prezzo di 20 criptovalute tra il 01/01/2015 e il 31/12/2017 ed escludendo dalla rilevazione le c.d. *stablecoins* (ossia criptovalute ancorate al valore nominale di valute fiat, tipicamente del dollaro), hanno costruito di diversi portafogli su base giornaliera effettuandone il ribilanciamento con lo stesso periodo del loro ricalcolo. In altre parole, il distaccamento tra il peso effettivo di ciascuna criptovaluta (quantità*prezzo/valore totale del portafoglio) ed il relativo peso teorico (appartenente al vettore dei pesi di quello specifico portafoglio), causato inevitabilmente dall'autonomo andamento dei prezzi, veniva annullato soltanto in corrispondenza del ricalcolo del vettore dei pesi teorici per quello specifico portafoglio. I portafogli costruiti dagli studiosi sono il *minimum variance portfolio* (MVP), il portafoglio ottimo (PFT), il portafoglio efficiente che massimizza il rendimento atteso ($maxR$) (ossia posto all'estremo destro della frontiera efficiente), tre generici portafogli efficienti ($PF1, PF2, PF3$), il portafoglio efficiente associato alla deviazione standard di Bitcoin ($BTC_{\mu_{opt}}$) ed il portafoglio equi-ponderato ($1/N$) (*naively diversified portfolio*). La rappresentazione grafica della frontiera efficiente e delle strategie di portafoglio è la seguente:

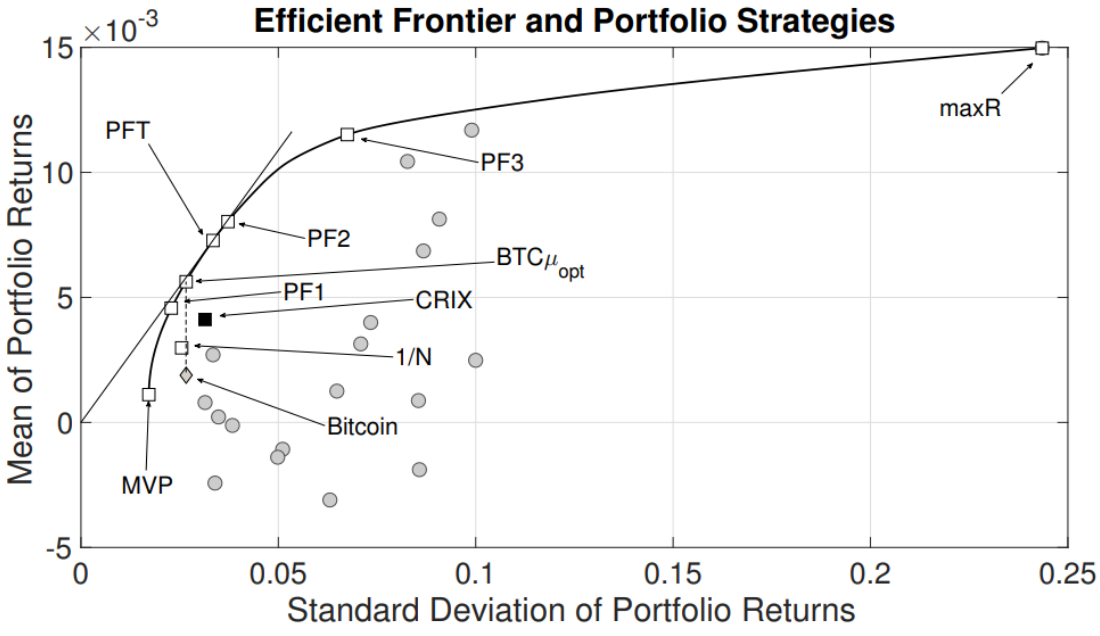


Grafico 4: Frontiera efficiente (Brauneis e Mestel)

Fatta eccezione per il *naively diversified portfolio* ed uno dei tre portafogli efficienti generici¸ un incremento dell'intervallo temporale compreso tra un ribilanciamento e l'altro (nonché del ricalcolo) provoca una riduzione sia del rendimento che della deviazione standard. L'informazione più rilevante che emerge dalla sintesi dei risultati di questo studio è l'inefficienza della performance del portafoglio ottimo comparata con

quelle degli altri portafogli. Infatti, osservando il caso di ribilanciamento (e ricalcolo) giornaliero, si osserva come il *tangency portfolio* abbia prodotto, con maggiore volatilità, un rendimento medio inferiore rispetto a quelli del *naively diversified portfolio*, del *minimum variance portfolio*, del portafoglio efficiente associato alla volatilità di Bitcoin e al primo dei tre generici portafogli efficienti. La performance invece è stata più efficiente rispetto a quelle del secondo e terzo portafoglio generico, nonché del portafoglio massimizzante il rendimento atteso (l'unico peraltro a conseguire un rendimento medio negativo, come si osserva nell'orizzonte mensile di ribilanciamento). Di seguito la tabella sintetica di media e varianza (valori in percentuale):

mean(r)	$1/N$	$BTC\mu_{opt}$	PFT	MVP	$PF1$	$PF2$	$PF3$	$maxR$
$h = 1$	0.6858	0.6085	0.6055	0.6064	0.6087	0.5844	0.5613	0.3023
$h = 7$	0.6816	0.5598	0.5268	0.6067	0.5767	0.5481	0.5764	0.2538
$h = 30$	0.6861	0.4920	0.4160	0.6000	0.5432	0.4499	0.3619	-0.5317
std(r)								
$h = 1$	4.40	4.38	5.09	3.48	3.96	5.41	7.64	12.83
$h = 7$	4.38	4.15	4.83	3.74	3.79	4.95	7.16	12.48
$h = 30$	4.35	4.07	4.57	3.85	3.99	4.71	6.07	9.04

Tabella 21: Sintesi delle performance di portafoglio (Braunesi e Mestel)

Graficamente, includendo tutte le coppie e tutti i portafogli associati ai tre intervalli di ribilanciamento, si ottiene una rappresentazione grafica estremamente diversa da quella predittiva vista in precedenza

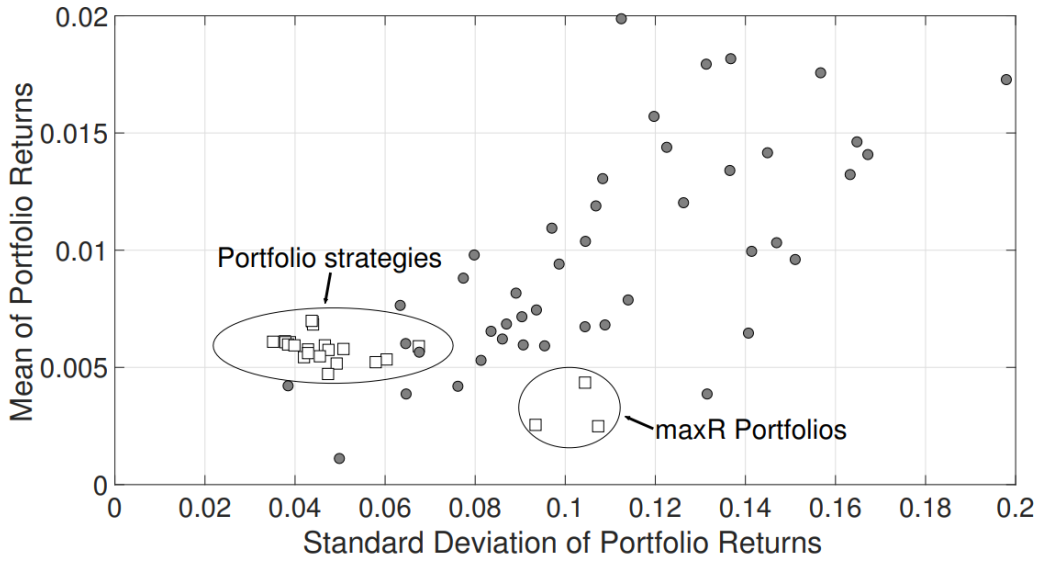


Grafico 5: Risultati ex-post delle strategie di portafoglio (Brauneis e Mestel)

In sintesi, sembrerebbe che il portafoglio ottimo tradisca la promessa di essere il portafoglio massimizzante lo Sharpe Ratio, proprio perché produce risultati relativamente inefficienti in termini di capacità remunerativa del rischio. Uno dei possibili motivi legati all'inefficienza del portafoglio ottimo potrebbe dipendere dalla mancata persistenza nella correlazione e nel comportamento remunerativo (rapportato al rischio) da parte delle criptovalute: in altre parole, il portafoglio ottimo potrebbe non considerare gli effetti dei brevi cicli di "boom and bust" dei prezzi delle criptovalute, riscontrabili proporzionalmente anche su intervalli temporali ridotti.

Questo porterebbe alla costruzione di un vettore di pesi "prociclico" caratterizzato da una maggiore presenza di criptovalute iperestese nel rapporto rendimento/rischio, cercando di sfruttare il beneficio della diversificazione seguendo uno schema di correlazione tra i rendimenti che potrebbe non persistere successivamente. In ogni caso, seppur contenuti, i benefici della diversificazione esistono dal momento che i risultati dei portafogli appaiono più efficienti rispetto a quelli delle singole criptovalute.

Tuttavia, come si è visto, il beneficio della diversificazione non appare massimizzato in corrispondenza del *tangency portfolio*, in quanto la semplice distribuzione equi-ponderata dei pesi o l'investimento nel minimum variance portfolio sembra produrre effetti preferibili a quelli del portafoglio ottimo.

Rapportando la media dei rendimenti giornalieri con la volatilità giornaliera, emergono Sharpe Ratio estremamente insoddisfacenti, che mai si spingono aldilà del valore di 0.2. Come confermato anche dall'analisi condotta in questa sede, malgrado la stragrande maggioranza delle criptovalute sia caratterizzata da crescite paraboliche nel prezzo, intervallate con periodo irregolare da crolli importanti, emerge una generale inadeguatezza da parte di questi asset nel remunerare correttamente il loro rischio. Una possibile causa di ciò potrebbe essere legata alla notevole correlazione positiva tra le diverse criptovalute che minimizzerebbe gli effetti di diversificazione derivanti dalle strategie di portafoglio. Un'altra possibilità è che, malgrado situazione sporadiche di correlazione negativa, e non necessariamente persistente, il beneficio derivante dall'eliminazione del rischio idiosincratico non sia sufficientemente apprezzabile rispetto alla consistenza della componente sistematica di rischio, associata alla totalità del mercato delle criptovalute. In altre parole, il beneficio della diversificazione non genererebbe effetti evidenti proprio a causa della volatilità tipica di questa categoria di asset

Conclusione

Le criptovalute sono espressione di un cambiamento in atto i cui effetti saranno tanto più evidenti quanto maggiore sarà l'adozione della tecnologia blockchain nel prossimo futuro. Tuttavia, nell'attesa del perfezionamento del passaggio da "invenzione" ad "innovazione", le criptovalute rappresentano una novità che, in quanto tale, non viene ancora compresa a pieno nel suo significato, soprattutto economico, poiché esso può scaturire soltanto da un'analisi approfondita del loro contenuto tipicamente tecnico e complesso.

Questa situazione potrebbe tradursi in scelte di investimento inconsapevoli veicolate ora dalla paura ora dall'euforia degli investitori, dettando una volatilità particolarmente marcata per questa tipologia di asset. Il comportamento riscontrato nel prezzo delle criptovalute nel periodo di Marzo 2020, agli albori dell'emergenza Covid-19, potrebbe denotare un'esposizione comune agli asset tradizionali per i "*black swan*" del mercato classico.

Nonostante ciò, questo nuovo mercato sembra crescere su un binario separato rispetto a quello dei mercati tradizionali come evidenziato dall'inadeguatezza dei modelli fattoriali tradizionali nel giustificare i rendimenti delle criptovalute. Al contrario, la costruzione di modelli fattoriali che ricompongono il rischio sistematico di questo mercato, utilizzando indici di riferimento come sue declinazioni, sembra essere particolarmente efficace nel descrivere i rendimenti delle criptovalute, minimizzando la significatività dei rendimenti anomali ed offrendo valori di R^2 apprezzabili.

Infine, pur presentando rendimenti medi particolarmente elevati, la volatilità intrinseca di questo mercato non sembrerebbe proporre le criptovalute come l'investimento ideale per soggetti avversi al rischio. Indubbiamente, confrontando gli Indici di Sharpe dei portafogli efficienti e quelli delle singole criptovalute, si evince un'eliminazione notevole della rischiosità idiosincratica dell'investimento, denunciando così uno stato di imperfetta correlazione positiva tra questi asset. Tuttavia, i benefici apportati dalla diversificazione non sono sufficienti per generare apprezzabili riduzioni del rischio a livello aggregato: infatti la variabilità dei rendimenti, anche nel caso dei portafogli efficienti, spesso si rivela troppo più alta rispetto ai rendimenti medi, determinando Indici di Sharpe generalmente inferiori ad uno. Inoltre, contrariamente a quanto augurato dalla *Modern Portfolio Theory*, l'investimento nel portafoglio ottimo sembrerebbe produrre effetti ben lontani da quelli pronosticabili, registrando risultati spesso meno efficienti rispetto a quelli conseguiti dal portafoglio di varianza minima o dal portafoglio equi-ponderato, frutto di una diversificazione *naïve*.

Bibliografia e Sitografia

Brauneis, Alexander. Mestel, Roland. *Cryptocurrency-portfolios in a mean-variance framework*. 2018;

Comandini, Gianluca. *Da Zero alla Luna. La Blockchain: quando, come, perché sta cambiando il mondo*. Flaccovio, 2020;

Ellis, Steve. Juels, Ari. Nazarov, Segey. *ChainLink. A Decentralized Oracle Network*. Link.smartcontract.org, 2017;

Liu, Yukun. Tsyvinski, Aleh. Wu, Xi. *Common risk factors in cryptocurrency*. National Bureau of Economic Research, 2019;

Liu, Yukun. Tsyvinski, Aleh. *Risks and returns of cryptocurrency*. National Bureau of Economic Research, 2018;

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org, 2008;

Udienze della Commissione speciale della Camera dei Deputati costituita per esaminare il Sistema d'organizzazione industriale del Taylor ed altri sistemi, in seguito della risoluzione 90 della Camera. (Vol. III);

99Bitcoins.com. *Bitcoin obituaries*;

10Bitcoin.it. *Firma di una transazione in Bitcoin*;

Binance.com. *An introduction to Binance Smart Chain*;

Binance.com. *What is BNB*;

Blockchain.com. *Genesis Block*;

Chain.Link. *What is the Blockchain Oracle Problem*, 2020;

CNBC.com. *Morgan Stanley becomes the first big U.S. bank to offer its wealthy clients access to bitcoin funds*, 2021;

Crix.de. *Crix Index*;

Cryptonomist.ch. *Dentro Bitcoin: chiavi e indirizzi*, 2019;

Etc-group.com. ZETH;

Ethereum.org. *Ethereum Whitepaper*;

Ftx.com: *FTX indexes calculation*;

GitHub.com. *Binance_Watcher.js*;

GitHub.com. *Chart.js*;

GitHub.com. *portfolio-allocation*;

Investopedia.com: *Bitcoin Minting*;

Investopedia.com. *eCash*;

Kenneth French. *Data Library for Fama-French factor models*;

Morningstar.it. BTCE;

Nakamoto, Satoshi. *Bitcoin P2P e-cash paper*, 2008;

Sec.gov; *Insight Notes Linked to the J.P. Morgan Basket of Companies with Exposure to Cryptocurrency*;