



Dipartimento di Economia e Finanza
Cattedra di Econometria per la Finanza

PAIR TRADING:
“UNA STRATEGIA DI ARBITRAGGIO STATISTICO SUL
MERCATO DELLE CRIPTOVALUTE ”

RELATORE
Prof. Stefano Grassi

CORELATORE
Prof. Paolo Santucci De Magistris

CANDIDATO
Carmine Zeno
Matr. 704481

ANNO ACCADEMICO 2019/2020

Sommario

Introduzione.....	4
Capitolo 1	5
1.1 Elementi Introduttivi	5
1.2 Prima del Bitcoin	6
1.3 Il sistema crittografico.....	7
1.3.1 Crittografia e funzione Hash nel protocollo Bitcoin	11
1.3.2 La Blockchain	11
1.3.3 Network Bitcoin: una rete Peer to Peer	14
1.4 Una transazione: aspetti pratici e tecnici	15
1.5 Il processo di Mining	15
1.6 Attacchi al sistema Bitcoin.....	19
1.7 Gli Altcoins.....	19
Capitolo 2	22
2.1 Pair Trading: Storia.....	22
2.2 Definizione	22
2.3 Distance Method	23
2.4 Approccio di cointegrazione	25
2.5 Test di radici unitarie e stazionarietà.....	26
2.5.1 Test Dickey-Fuller e Augmented Dickey Fuller.....	26
2.5.2 Il Test Phillips-Perron	27
2.5.3 Test KPSS	28
2.6 Engle Granger Test Cointegrazione	28
2.7 Procedura di Johansen.....	30
Capitolo 3	32
3.1 Introduzione.....	32
3.2 Costruzione del set di dati	35
3.3 Test di Integrazione e Stazionarietà	36
3.4 Test Engle e Grenger.....	38
3.5 Regole di Trading	41
3.6 Fase di Backtesting	42
3.7 Test di Johansen.....	43
3.8 Bollinger Band.....	46
3.9 Relative Strenght Index.....	49

Conclusioni.....	52
Appendice: Codice Matlab	53
Cointegrazione Engle e Granger.....	53
Cointegrazione Procedura di Johansen	59
Bande di Bollinger	60
Strategia con RSI	63
Bibliografia.....	66

Introduzione

Lo scopo dell'elaborato è analizzare la possibilità di applicare in modo profittevole strategie di Pair Trading al mercato delle Criptovalute. Le motivazioni che mi hanno spinto ad approfondire tale tema hanno una duplice natura. In primo luogo l'interesse nel continuare, a due anni di distanza, l'analisi di questo nuovo strumento tecnologico e finanziario , che fin da subito mi ha appassionato. La tesi triennale analizzava infatti l'utilizzo delle criptovalute come strumento di diversificazione del portafoglio , mentre in questo elaborato analizzeremo una funzione speculativa delle criptovalute. In secondo luogo la possibilità di poter analizzare, a seguito di un percorso magistrale il cambiamento nelle modalità di analisi dello stesso strumento.

L'elaborato riparte proprio da una rielaborazione delle ricerche riguardanti il funzionamento del bitcoin e di altre criptovalute , con i dovuti aggiornamenti, svolte nell'elaborato di tesi triennale. In questo primo capitolo il mercato delle criptovalute è analizzato da un punto di vista storico, tecnologico e statistico.

Nel secondo capitolo si passa invece alle varie metodologie analizzate nella letteratura finanziaria , in particolare nei lavori di Gatev et al. e Vidamurthy. Si analizza il metodo della distanza e i diversi test di cointegrazione.

Nel parte finale dell'elaborato di analizzano due strategie di Pair Trading , entrambe basate sull'analisi della cointegrazione , ma svolta attraverso due differenti test: Engle e Granger e Johansen. Inoltre si analizzano due strategie di analisi tecnica , Bande di Bollinger e Relative Strenght Index, in modo da poter effettuare un confronto tra strategie di Analisi Tecnica e strategie di Arbitraggio statistico.

Capitolo 1

1.1 Elementi Introduttivi

Il XX secolo ha conosciuto una rivoluzione tecnologica, che ha cambiato in modo radicale il mondo intero. Negli ultimi anni, si è poi assistito ad uno sviluppo in continua crescita delle tecnologie crittografiche. Proprio le innovazioni in ambito crittografico, hanno reso possibile la creazione di nuovi strumenti di pagamento. L'innovazione più importante e rivoluzionaria, è di sicuro rappresentata dalle criptovalute. La prima criptovaluta "*il Bitcoin*" fu presentata per la prima volta nel novembre del 2008 da un autore o autori anonimi, sotto lo pseudonimo giapponese "Satoshi Nakamoto". Il 9 gennaio 2009 venne rilasciata la prima versione del software Bitcoin. Di norma, con il termine "Bitcoin" si indica la tecnologia e la rete alla base di questo sistema di pagamento, mentre, nella denominazione "*bitcoin*" si fa riferimento alla valuta utilizzata per gli scambi. Ciò che rende innovativo il bitcoin rispetto ai sistemi di pagamento di tipo tradizionale è la sua decentralizzazione. Il Bitcoin utilizza la tecnologia blockchain per tenere traccia delle transazioni, la crittografia per la gestione degli aspetti funzionali e il meccanismo di mining per la generazione di nuova moneta e la verifica delle transazioni. Nel sistema Bitcoin non è presente alcuna unità organizzativa, che controlli e gestisca l'emissione di nuova moneta, ma soprattutto non necessita di affidarsi ad alcuna istituzione finanziaria che ne funga da garante. Il bitcoin utilizza una rete peer-to-peer (P2P), ovvero una rete senza alcuna struttura gerarchica, tipica dei sistemi client/server, e nella quale ciascun nodo (detto *servent*) può operare come client o come server a seconda delle circostanze. Un nodo può essere rappresentato da un computer, da uno smartphone o da un qualsiasi altro dispositivo elettronico in grado di far funzionare il software. Per le monete digitali uno dei maggiori rischi è rappresentato dalla cosiddetta *double spending*, ovvero dalla possibilità che il denaro (essendo non fisico ma "virtuale") venga speso più di una volta. Per questo motivo ogni transazione va verificata e convalidata prima di essere conclusa. L'analisi delle transazioni viene affidata agli stessi utilizzatori della rete, che mettono a disposizione del network la potenza computazionale dei loro computer, in modo che possano essere convalidati i pagamenti. Gli user della rete che raccolgono le transazioni e le organizzano in blocchi, prendono il nome di "*miner*". Ogni volta che un miner convalida un blocco lo trasmette alla rete in modo che si possa aggiungere alla Blockchain. Quest'ultima, altro non è, che un registro unico e condiviso delle transazioni in modo che nella rete si possa garantire trasparenza, sicurezza e la non falsificabilità dei pagamenti. Qualsiasi minatore per la risoluzione di un nuovo

blocco viene ricompensato in bitcoin di nuova emissione, ed è il protocollo stesso a stabilire le ricompense. Attualmente, le ricompense sono di 6.25 bitcoin per blocco, da dividere tra tutti i partecipanti alla risoluzione del singolo blocco. L'emissione di ricompense è pianificata per dimezzarsi ogni quattro anni, fino ad arrivare ad un totale di bitcoin in circolazione di 21 milioni. Il meccanismo di ricompense è anche l'unico modo in cui nuova moneta viene immessa nel mercato. Allo scopo di garantire l'effettiva convalidazione dei blocchi, il sistema utilizza un protocollo crittografico noto come proof-of-work. Questo sistema costringe i miner a risolvere un complesso problema matematico, per dimostrare che la giusta potenza computazionale è stata spesa per la convalida del blocco. La proof-of-work rende la convalida dei blocchi come una lotteria, in cui le possibilità di vincita aumentano all'aumentare della potenza computazionale impiegata.

1.2 Prima del Bitcoin

Il protocollo Bitcoin è una tecnologia relativamente giovane, ma rappresenta la realizzazione di un intero movimento ideologico nato verso la fine degli anni 80, Cyberpunks. Questo gruppo di attivisti vedevano nelle tecnologie informatiche e nella crittografia uno strumento utile per liberare l'uomo, ormai schiavo delle istituzioni. Tra gli esponenti del movimento troviamo figure di rilievo come David Chaum e Wei Dai. Nel 1982 il crittografo americano David Chaum nell'articolo, intitolato "Blind signature for untraceable payments", introduce per la prima volta il concetto delle "firme cieche" (blind signature). Quest'ultime sono una sorta di firma digitale, che permettono di autenticare un messaggio e vedere se è stato manomesso durante la trasmissione. Le blind signature sono utilizzate nei protocolli in cui il firmatario e l'autore del messaggio sono differenti (ex. voto elettronico). Successivamente nel 1988, Chaum fonda Digicash Inc., società che nei primi anni novanta lancia il sistema di pagamento elettronico e-cash. Quest'ultimo permette di custodire denaro digitale nella memoria del proprio computer, effettuare acquisti anonimi e sicuri su internet, il tutto senza passare attraverso le istituzioni bancarie, che si limitavano a controllare l'effettiva presenza del denaro necessario all'operazione. Il mercato però, non era ancora pronto per questa rivoluzione e Digicash fallì nel 1998. Un altro tentativo di creare una valuta digitale scambiabile istantaneamente su internet, fu realizzata nel 1996, dalla società privata Gold e Silver Inc.. Questa valuta digitale prese il nome di e-gold, e detenerla significava detenere una certa quantità di metalli preziosi custoditi dalla G&SR come riserva. E-gold poteva essere usata sia per trasferire denaro tra privati sia per gli acquisti on-line, aprendo inoltre alla possibilità di effettuare micro pagamenti online. Nel 2007 e-gold venne accusato dal governo statunitense

di permettere il riciclaggio di denaro, nel 2009 furono poi bloccati gli account e la possibilità di effettuare transazioni. La svolta dal punto di vista concettuale avvenne nel 1998, anno in cui il programmatore Wei Dai e il crittografo Nick Szabo proposero, separatamente, due diversi sistemi di pagamento decentralizzati. Wei Dai chiamò la sua moneta b-money, il sistema permetteva, almeno teoricamente, il trasferimento di valore tra utenti attraverso la rete internet. Il sistema b-money presentava caratteristiche riscontrabili nell'attuale sistema Bitcoin. Secondo lo schema presentato da Wei Dai, la creazione di moneta, sarebbe dovuta avvenire tramite risoluzione di problemi matematici, che imponevano agli utenti l'utilizzo di una certa potenza di calcolo. Le transazioni avrebbero sfruttato il meccanismo della firma digitale per la convalidazione, e infine gli utenti registrati nel network sarebbero rimasti anonimi grazie all'utilizzo di uno pseudonimo. Nick Szabo ideò nello stesso periodo di Wei Dai (ma separatamente da quest'ultimo) una criptomoneta (bit-gold), la quale presentava caratteristiche ancora più vicine al Bitcoin. Anche nel caso di bit-gold la creazione di moneta avveniva grazie a calcoli effettuati da diversi processori proprio come previsto dall'idea di Wei Dai. Nello specifico i calcolatori dovevano trovare la cosiddetta "challenge string", ovvero una stringa di bit tramite un processo definito "proof-of-work". Ogni challenge string era unica e poteva essere individuata da un solo utente ,(il primo in ordine cronologico che riusciva a risolverla) e solo una volta terminata la ricerca della stringa precedente era possibile passare alla successiva. Proprio dall'analisi di questi precedenti progetti e dall'ideologia che accomunava gli appartenenti al Cyberpunks, è nato il Bitcoin.

1.3 Il sistema crittografico

Il termine crittografia deriva dalle parole greche " Kriptòs" e "Graphìa" , e significa "scrittura nascosta". Come suggerisce la stessa etimologia della parola , la crittografia è una scienza che fornisce metodi per la cifratura delle informazioni , in modo da renderle incomprensibili a soggetti non autorizzati. I sistemi di cifratura presentano due elementi fondamentali: l'algoritmo e la chiave . L'algoritmo rappresenta la funzione matematica che permette di cifrare il messaggio, mentre la chiave è il parametro che permette di decodificare il messaggio. Nei metodo di cifratura più elementari, la chiave e l'algoritmo coincidono, in crittografia un metodo con questa caratteristica prende il nome di "crittografia simmetrica" . L'introduzione nel XX secolo di sistemi informatizzati e di internet , richiedevano nuovi standard di sicurezza per la trasmissione delle informazioni. Questa nuova esigenza di sicurezza ha portato a nuove svolte in ambito crittografico. La vera rivoluzione è rappresentata dall'introduzione di un nuovo

metodo di cifratura dei messaggi, che prende il nome di “crittografia asimmetrica” . Il nuovo metodo, conosciuto anche come crittografia a coppie di chiavi, basa il suo funzionamento sull’utilizzo di due chiavi :

- ✓ una chiave pubblica: che può essere divulgata
- ✓ una chiave privata: che deve restare personale e segreta

In un sistema crittografico asimmetrico chiunque può cifrare un messaggio usando la chiave pubblica del destinatario , ma il messaggio è decodificabile solamente attraverso l’utilizzo della chiave privata. Volendo fare un esempio: il mittente “A” può utilizzare la chiave pubblica del destinatario “B” per cifrare il messaggio , in modo che quest’ultimo possa essere l’unico a decifrarlo con l’utilizzo della propria chiave privata . Questo metodo di cifratura risulta sicuramente più efficace e sicuro rispetto al “cifrario di Cesare”, ma presenta un punto debole. Durante la trasmissione il messaggio potrebbe essere intercettato e sostituito ; il destinatario del messaggio non avrebbe modo di verificare l’autenticità del messaggio . Per rendere la trasmissione delle informazioni autentica e insostituibile , bisogna fare un passo avanti e introdurre il concetto di funzione di Hash .

Gli algoritmi di hash sono particolari funzioni che permettono di dare al messaggio un impronta digitale tale da identificarlo univocamente . La funzione di hash trasforma un qualsiasi messaggio in una stringa alfanumerica di lunghezza prefissata , che prende il nome di *hash* , *digest* o impronta digitale . Dal punto di vista matematico , se ipotizziamo che :

- ✓ " Σ " Rappresenti l’insieme delle lettere dell’alfabeto ,
- ✓ " Σ^* " Rappresenti l’insieme delle stringhe di qualsiasi lunghezza , composte dalle lettere dell’alfabeto
- ✓ " Σ^n " Rappresenti l’insieme delle possibili stringhe di lunghezza n , ottenibili combinando le lettere dell’alfabeto .

Una qualsiasi funzione “ h ”, si definisce “ funzione di hash” se dato un qualsiasi input di valori appartenente all’insieme Σ , si ottiene applicando la funzione, un valore unico appartenete all’insieme di valori “ Σ^n ” . Dunque “ h ” è detta funzione hash se :

$$(1) \quad h : \Sigma^* \rightarrow \Sigma^n$$

$$(2) \quad x \rightarrow h(x)$$

La funzione crittografica di hash presenta le seguenti caratteristiche :

- ✓ semplicità: dato un valore di input di lunghezza qualsiasi , deve risultare agevole calcolare il codice hash di output.
- ✓ non invertibilità: deve risultare impossibile poter risalire al messaggio originale , partendo dal codice hash .
- ✓ univocità: deve essere quasi impossibile che informazioni diverse abbiano lo stesso hash .
- ✓ “effetto valanga”: data un’informazione di input e il relativo hash , anche una minima modifica dell’input deve generare un’alterazione radicale del relativo hash .

Il protocollo Bitcoin utilizza come funzione Hash l’algoritmo SHA-256 . Il “*Secure Hash Algorithm*” (SHA) fu sviluppato dalla NSA (National Security Agency) nel 1993 . Tale algoritmo è in grado di processare messaggi con dimensione inferiore a 264 bit e, restituire un codice alfanumerico di 64 caratteri con dimensione di 256 bit.

Esempio partico dell’applicazione della funzione hash SHA-256 ad un messaggio:

Messaggio 1 : compra bitcoin

Relativo hash : 7A65B3B5DA7707CE000D42C2AFF97305A7F1551E61EEDACF81D6BAC85FD410CE

Messaggio 2 : compro bitcoin

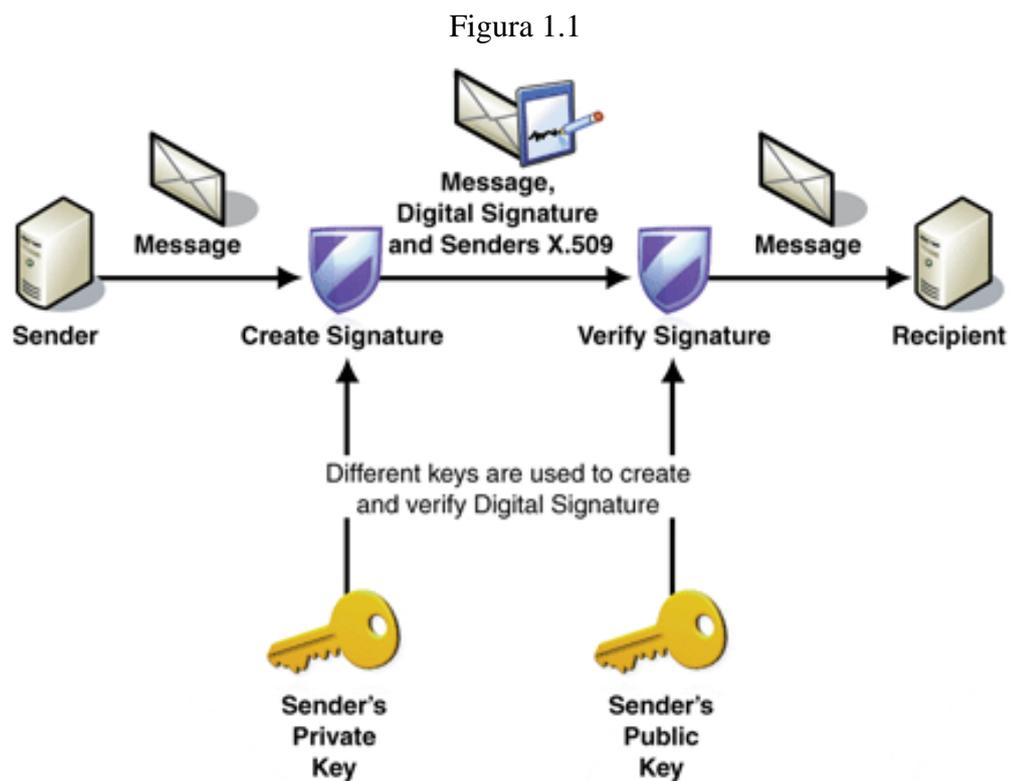
Relativo hash : 189717F0C15A8210F56C3805FA0202E7C3F4C89ECA93BD4F4DB01EFB0B942F91

Quest’esempio dimostra come cambiando anche una sola lettera del messaggio si ottiene un hash completamente differente , in accordo con quanto stabilisce il principio di “effetto valanga” (Fonte <http://www.hashemall.com/>).

L’utilizzo combinato della crittografia a chiave asimmetrica e della funzione di hash permette di firmare digitalmente i documenti, ma l’utilizzo di chiave privata e pubblica avviene in modo inverso rispetto all’utilizzo analizzato in precedenza. La chiave privata viene utilizzata dal mittente per cifrare la firma apposta sul documento , il destinatario utilizza la chiave pubblica del mittente per decifrare la firma e constatare l’identità del mittente . L’utente per firmare un documento per prima cosa utilizza un algoritmo di hash per produrre un’impronta digitale del documento stesso , utilizza poi la sua chiave privata per cifrare l’impronta del documento , producendo così una firma su quel documento. Il documento una volta inviato al destinatario , con in allegando la propria chiave pubblica, può decifrare la firma e verificare che l’Hash

risultante corrisponde all'impronta digitale di quel documento. In questo modo il destinatario può:

- verificare l'identità del mittente (ossia l'autenticità del documento);
- assicurarsi che il mittente non neghi di aver firmato quel documento (non riproducibilità);
- assicurarsi che il documento non sia stato modificato da terzi dopo l'apposizione della firma (integrità).



fonte: <https://www.firmadigitale.com/news/firma-elettronica-o-firma-digitale.html>

1.3.1 Crittografia e funzione Hash nel protocollo Bitcoin

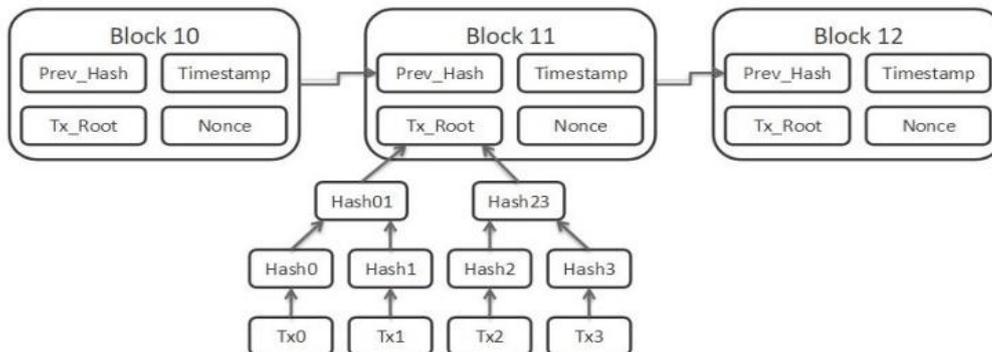
Al momento dell'apertura di un conto denominato in bitcoin, vengono assegnate all'utente tre codici: una chiave privata, una chiave pubblica e un indirizzo. Vediamo in che modo questi tre codici vengono utilizzati dal protocollo. La chiave privata assegnata dal protocollo è un codice casuale di 256 bit, con il quale vengono digitalmente firmate le operazioni in uscita che provengono dal relativo account. La chiave privata permette di spendere in bitcoin ha chi ne è in possesso, e può essere custodita in uno dei qualsiasi wallet bitcoin, di cui si è parlato nel capitolo precedente. La chiave pubblica viene invece generata a partire dalla chiave privata, sfruttando l'algoritmo crittografico ECDSA (Elliptic Curve Digital Signature Algorithm). Si presenta come un codice di 512 bit, e viene utilizzata per la verifica delle firme digitali apportate sulle transazioni. Infine attraverso l'utilizzo dell'algoritmo di Hash si genera l'indirizzo Bitcoin, un codice a 160 bit, utilizzata per individuare il destinatario e il mittente della transazione.

1.3.2 La Blockchain

La Blockchain è un protocollo informatico che permette, attraverso la condivisione di risorse informatiche e di algoritmi crittografici, la gestione di un registro pubblico decentralizzato di transazioni. La Blockchain è formata da una serie di record, chiamati blocchi, contenenti le informazioni sulle transazioni convalidate dalla rete. Grazie al meccanismo della decentralizzazione i dati memorizzati in un blocco, una volta che quest'ultimo si è unito alla catena precedente, non possono essere modificati (alterazione retroattiva). Ogni blocco all'interno della catena, contiene un puntatore di Hash, che gli permette di essere identificato in modo univoco e, un timestamp³ per l'identificazione temporale del blocco e dati riguardanti le transazioni. La blockchain risulta quindi strutturata come un contenitore di blocchi, al cui interno sono presenti le transazioni.

Il blocco presenta dimensioni variabili, a seconda del numero di transazioni che la rete richiede di convalidare. Il blocco si presenta composto da due parti fondamentali: l'header e il body.

Figura 1.2



fonte: https://www.silicon.it/e-enterprise/block-chain-se-non-sara-bitcoin-poco-importa-il-sistema-funziona-95275?inf_by=5b7c2956671db8c22f8b46b8

Le transazioni sono racchiuse nel body del blocco, e nell'header sono presenti sette campi riportanti le informazioni del blocco stesso. I sette campi dell'header sono: versione, hash del blocco precedente, merkle root, timestamp, bits, nonce e numero di transazione.

- (1) *Versione*: indica la versione del software utilizzato dall'utente per immettere la transazione in rete.
- (2) *PrevHash* : è un hash di 256 bit identificato del blocco precedente; è proprio grazie alla presenza di questo codice che è possibile unire in modo cronologico tutti i blocchi convalidati.
- (3) *Merkle root* : hash che sintetizza tutte le transazioni ricomprese nel blocco. Tutti gli hash delle diverse transazioni vengono cifrati a coppia, fino a quando non si ottiene un unico codice alfanumerico.
- (4) *Timestamp*: indica la data e l'ora dell'ultima transazione. In informatica i marcatori temporali rappresentano un'unità di misura, che esprime la data e l'ora attraverso un codice numerico intero.
- (5) *Bits*: indica il target di riferimento per il blocco convalidato. Nel protocollo Bitcoin il target rappresenta la differenza percentuale tra il tempo effettivo e il tempo teorico necessario per minare il blocco. Il valore del target viene inserito nel codice come un numero a 256 bit.
- (6) *Nonce* : è un numero casuale utilizzato nel processo di hashing di un blocco. Un nonce viene utilizzato nei protocolli di autenticazione per assicurare che i dati scambiati nelle

vecchie comunicazioni non possano essere riutilizzati successivamente, permettendo l'attacco del sistema.

(7) *Numero di transazione*: identifica il numero del blocco. Tutti i blocchi vengono numerati in ordine cronologico a partire dallo zero (il genesis block).

Come detto le transazioni sono racchiuse nel body del blocco, che a loro volta contengono una serie di informazioni. Le informazioni contenute nelle transazioni possono essere catalogate in tre grandi categorie:

1 Header o carta di identità della transazione, presenta otto informazioni fondamentali:

a) Hash della transazione: codice alfanumerico generato per identificare in modo univo ogni singola transazione. Nel codice sono riassunte le informazioni principali sulla transazione attraverso l'utilizzo della funzione hash

b) Numero del blocco in cui la transazione è stata memorizzata;

c) Numero di inputs: numero delle diverse precedenti transazioni fornitrici complessivamente dell'ammontare di bitcoin impiegato nella transazione in oggetto;

d) Totale dei BTC riscattati: somma dei bitcoin risultanti dalle transazioni di cui illustrato al punto ;

e) Numero degli outputs: numero dei diversi indirizzi Bitcoin a cui sono inviati i BTC in uscita;

f) Totale dei BTC in uscita: somma dei bitcoin in uscita nella transazione in oggetto;

g) Size: le transazioni, così come i blocchi sono informazioni, che occupano una memoria all'interno della rete. Le dimensioni in termini informatici della transazione, vengono usate nel protocollo per il calcolo della commissione;

h) Commissione: ammontare di BTC attribuiti ai miners, che hanno contribuito alla risoluzione del blocco.

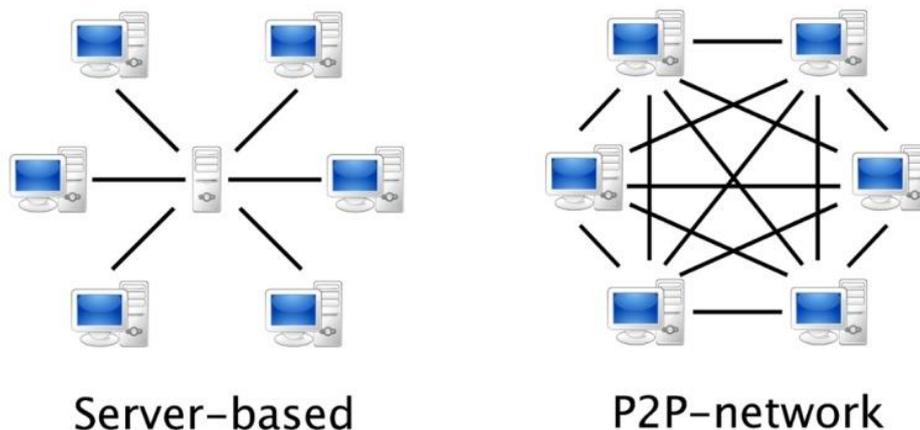
2 Dettaglio degli input: tabella in cui vengono elencate nel dettaglio le transazioni fornitrici dell'ammontare di bitcoin impiegato nella specifica transazione. In ogni riga della tabella viene indicato l'hash della transazione input, l'ammontare trasferito e l'indirizzo Bitcoin di colui che lo riceve. Per ogni input viene inoltre indicato lo Script Sig, questo codice serve ad identificare la firma digitale. Nel protocollo la firma digitale viene usata per controllare la reale appartenenza dell'indirizzo al richiedete della transazione.

3 Dettaglio degli output: tabella in cui vengono elencati gli indirizzi Bitcoin destinatari complessivamente dell'ammontare che si chiede di trasferire. Per ogni output viene indicato l'indirizzo del destinatario e la relativa somma trasferita. Viene inoltre indicato per ogni output la Script Public Key, che rappresenta la chiave pubblica, attraverso il quale il protocollo del sistema si assicura la presenza della somma che si richiede di trasferire.

1.3.3 Network Bitcoin: una rete Peer to Peer

Tutti i dati relativi della blockchain sono memorizzati e distribuiti su tutti i dispositivi che partecipano al network bitcoin. Il protocollo bitcoin utilizza per la trasmissione delle informazioni una rete di tipo peer to peer. La rete peer-to-peer è organizzata in modo da rendere i nodi del sistema tra loro equivalenti, ogni utente può svolgere funzioni sia il ruolo di client sia di server. Generalmente le reti informatiche sono di tipo client server, costruzione che prevede un sistema di archiviazione centralizzato. La funzione di server è svolta da un sistema centralizzato, il quale svolge una funzione passiva, accettando le richieste dei client e inviando la risposta richiesta.

Figura 1.3



fonte: <https://www.thinglink.com/scene/977515732151566338>

In una rete p2p il controllo sulle operazioni del network è affidato ad ogni singolo nodo, inoltre le informazioni sono distribuite e condivise in forma crittografata su ogni dispositivo della rete.

1.4 Una transazione: aspetti pratici e tecnici

Abbiamo detto che le transazioni altro non sono che informazioni salvate nel registro della Blockchain. Analizziamo ora in che modo un utente può effettuare una transazione, e cosa avviene nella network prima che questa sia definitivamente conclusa. Colui che deve ricevere il pagamento genera un indirizzo da inviare al mittente. Una volta inserito nel software l'indirizzo del ricevente, la quantità di bitcoin da trasferire e il fee (il fee rappresenta la quantità di bitcoin offerta per risolvere il blocco), il mittente inoltra la transazione alla rete. Il ricevente ottiene immediatamente sul suo software l'avviso che la transazione è avvenuta, ma prima di poter considerare il pagamento effettuato deve attendere che la transazione sia inserita nella blockchain. In un massimo di 10 minuti circa la transazione viene convalidata, diventando così irreversibile. Queste sono le operazioni che vengono messe in atto per effettuare una transazione nella rete Bitcoin, vediamo invece cosa succede da un punto di vista tecnico nella rete. Il ricevente crea una chiave privata, la quale viene convertita in chiave pubblica attraverso l'algoritmo della curva ellittica, a sua volta la chiave pubblica viene convertita in un hash e ridotta infine ad indirizzo. Queste quattro operazioni vengono eseguite all'interno del sistema in pochi attimi, senza l'intervento dell'utente. Una volta che l'indirizzo è stato inviato al pagante, quest'ultimo lo decodifica con la funzione hash. Subito dopo crea la transazione, specificando l'output e il "signature script"⁵ con l'hash della chiave pubblica del ricevente. Il mittente conferma la transazione inviando i bitcoin presenti in uno o più output e la firma con la chiave privata. La transazione viene trasmessa alla rete, in modo che i minatori possano convalidarla. Infine il ricevente firma il signature script con la propria chiave privata e pubblica, dimostrando di essere proprietario dell'output della transazione. Ovviamente questa serie di operazioni viene svolta in modo automatico dai software installati sui dispositivi degli utenti.

1.5 Il processo di Mining

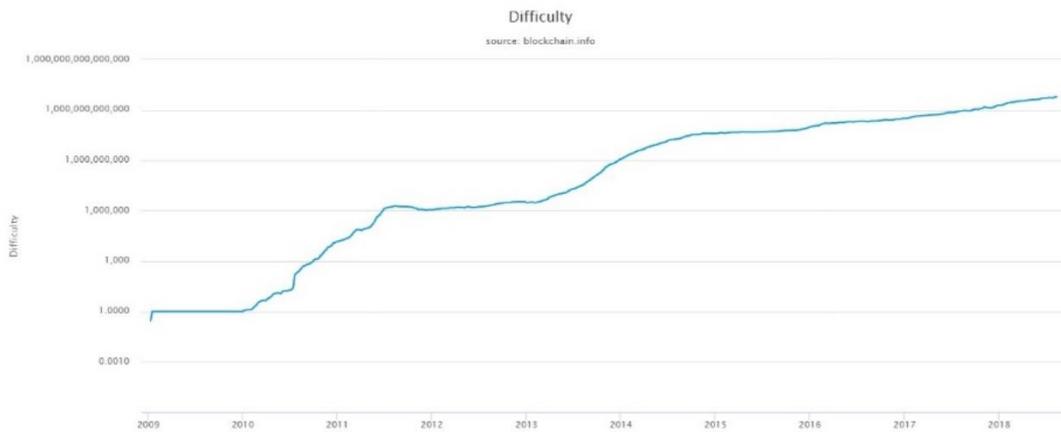
Il processo di mining previsto dal protocollo bitcoin ha il duplice scopo di validare le transazioni, unirle alla Blockchain e creare bitcoin di nuova emissione. In tal modo è possibile ovviare al problema della double spending, presente in ogni sistema di pagamento elettronico, e risolto fino alla creazione del bitcoin con l'utilizzo di intermediari. Il problema della double spending, in un sistema di pagamento elettronico, si presenta nel momento in cui un utente prova ad inviare la stessa quantità di bitcoin a due diversi indirizzi, in modo che le due operazioni entrino in contrasto fra loro. Con l'attività di mining i nodi attivi della rete mettono

a disposizione la potenza di calcolo dei propri dispositivi hardware, in modo da garantire la validazione e la registrazione delle operazioni. Ogni volta che un nuovo blocco viene prodotto, il protocollo crea una quantità stabilita di nuovi bitcoin, assegnati al minatore che per primo riesce a risolvere il blocco. Oltre ai bitcoin di nuova emissione, i minatori vengono ricompensati con una commissione, offerta in modo volontario dall'emittente della transazione. I partecipanti al processo di mining non sono obbligati a processare tutte le transazioni, per questo inserire una commissione più alta può rappresentare un incentivo. Attualmente molte transazioni vengono processate anche senza commissione, dato che la ricompensa in bitcoin di nuova emissione risulta sufficientemente remunerativa (soprattutto se si considerano i valori di cambio attualmente raggiunti dal bitcoin). Ogni volta che si effettua una transazione in bitcoin, gli altri nodi della rete ricevono una comunicazione di avviso, in cui è indicata la quantità che si intende spostare, l'indirizzo del mittente e quello del destinatario. Una volta ricevuta la richiesta, i nodi che decidono di accettarla, provvederanno:

- (1) a verificare la validità della richiesta; verificando la firma digitale apposta sulla richiesta di trasferimento
- (2) a verificare la disponibilità dei bitcoin da spostare nell'indirizzo del mittente; questo è possibile ripercorrendo lo storico della transazioni avvenute verso quell'indirizzo bitcoin
- (3) a includere la transazione nel blocco che si sta minando, in modo da poterla ritenere confermata.

Nel protocollo bitcoin la creazione di nuovi blocchi è prestabilita, e indipendente dal numero di transazioni che vengono effettuate nel sistema. Ogni due settimane il protocollo deve produrre in media 2016 blocchi, quindi circa ogni 10 minuti un nuovo blocco viene creato, anche se nessuno decidesse di effettuare operazioni. Inoltre ogni due settimane, il protocollo analizza il numero di blocchi creati, e di conseguenza modifica la difficoltà di estrazione. Se il numero di nuovi blocchi creati risulta essere maggiore del valore obiettivo, la difficoltà di estrazione viene innalzata; se invece risulta inferiori, la difficoltà di estrazione viene abbassata.

Figura 1.4



fonte: blockchain.com

Per ogni nuovo blocco, vengono creati, dei nuovi bitcoin. Anche la creazione di nuova moneta è prefissata. A partire da 50 bitcoin iniziali si dimezza in progressione geometrica, ogni 210 mila blocchi creati, raggiunti ogni quattro anni circa. Anche la soglia massima di bitcoin in circolazione è prestabilita dal protocollo a 21 milioni, tuttavia non si conoscono le motivazioni che hanno portato l'autore del sistema a scegliere tale soglia. Una volta che il sistema smetterà di produrre bitcoin, la remunerazione dei minatore sarà rappresentata esclusivamente dalle commissioni erogate dagli utenti. Quindi il futuro del bitcoin dipende dal numero di utenti che deciderà di usarlo come mezzo di pagamento. Nell'ipotesi che questo numero sia sufficientemente alto sarà possibile ripagare in modo adeguato i minatori. Riguardo l'attività di mining si è parlato più volte della risoluzione di problemi per la validazione dei blocchi, tale sistema prende il nome di proof of work, vediamo più nello specifico di cosa si tratta. Il protocollo Bitcoin impone la risoluzione di un algoritmo crittografico di tipo hashcash, un sistema utilizzato per rendere costoso in termini di tempo di elaborazione, ovvero di energia consumata, la validazione di un operazione. Minare un blocco contenente una sola transazione non rende il mining più veloce ed economico, per questo i minatori sono incentivati a includere più transazioni in un solo blocco, incassando le relative commissioni. Il processo di mining si basa sostanzialmente sulla così detta risoluzione per forza bruta, i minatori eseguono diversi tentativi fino a quando uno di loro non riesce a trovare una soluzione valida. I minatori per risolvere la proof of work applicano la funzione SHA-256 all'header del blocco, ottenendo così un codice a 64 caratteri. Viene poi aggiunto un valore finale, che prende il nome di Nonce, e utilizzando nuovamente la funzione SHA-256 si ottiene un nuovo codice hash. Quest'ultimo hash deve essere ricalcolato, modificando ogni volta il valore del Nonce, fino a quando non si ottiene un codice, che inizia per zero ed inferiore o uguale al valore target. Le soluzioni al

problema non sono univoche, e i miner per essere ricompensati devono essere più veloci dei competitor, utilizzando quindi una maggiore potenza computazionale. Le regole a cui i minatori devono sottostare per produrre un nuovo blocco sono necessarie affinché i tempi di risoluzione di un blocco rimangano costanti a 10 minuti. Dunque le operazioni di mining possono essere sostanzialmente scomposte nelle seguenti fasi:

- Le transazioni sono trasmesse ai nodi mediante la rete bitcoin, (una rete peer to peer)
- Ogni nodo seleziona le transazioni che intende risolvere, procede alla produzione di un nuovo blocco, elaborando il merkle root, e costruendo la tabella di input che andrà sottoposta ad hashing;
- L'hardware dei minatori è sottoposto alla prova di lavoro, che si considera risolta quando l'hash è inferiore o uguale al target. La soluzione viene comunicata agli altri nodi del sistema, che lavorano sullo stesso blocco;
- I nodi controllano che il nuovo blocco non comprenda transazioni inconsistenti, e convalidano il blocco utilizzandone l'hash del blocco seguente.

Per iniziare l'attività di mining, attualmente, è possibile scegliere tra tre principali alternative:

- ✓ *Solo-mining*: l'attività di mining è svolta in modo individuale, per far proprie la ricompensa e la somma delle commissioni delle transazioni incluse nel nuovo blocco. L'elevata competitività del mining richiede ingenti investimenti in energia elettrica e processori creati appositamente per l'attività di mining. Il solo-mining tuttavia non garantisce una remunerazione continua, ed è quindi un'alternativa molto rischiosa in termini economici.
- ✓ *Pool-mining*: Una mining pool può essere vista come un'organizzazione di persone che uniscono le forze computazionali dei propri dispositivi per minare bitcoin. In questo modo è possibile accrescere la probabilità di chiudere un blocco e quindi aumentare il guadagno. Per minare unirsi ad una "pool" è necessario creare un account personale e scaricare un particolare programma. Il programma di fatto consente di condividere parte della potenza di calcolo del pc col gruppo. Con il passare del tempo il mining diventa sempre più competitivo e al giorno d'oggi è molto difficile "trovare" o risolvere un blocco prima che ci riescano altri.
- ✓ *Cloud-mining*: è possibile partecipare all'attività di mining senza possedere hardware necessari, eliminando i problemi relativi alla manutenzione e alla collocazione fisica di tali apparecchiature. Attraverso il cloud-mining è possibile prendere a noleggio in un

determinato ammontare di potenza computazionale e farne propri i profitti in cambio di un canone di locazione.

✓

1.6 Attacchi al sistema Bitcoin

I protocolli crittografici utilizzati dal sistema bitcoin, attualmente, risultano essere i più sicuri del sistema informatico. Tuttavia, come per ogni software, esiste la possibilità di attacchi informatici, che comprometterebbero la funzionalità dell'intero sistema. La complessità nel mettere in atto un attacco al sistema spinge, piuttosto, i nodi disonesti della rete a concentrarsi su attacchi verso i servizi connessi al Bitcoin, come i wallet e gli exchange. Tuttavia, da un punto di vista teorico, esistono due tipologie di attacchi sferrabili alla rete Bitcoin: 51% attack e attacco a collisione.

- ✓ 51 % Attack: è una forma di attacco al protocollo Bitcoin , che consente, al possessore del 51% della forza computazionale della rete, di gestire le transazioni a proprio piacimento. Quest'attacco non risulta molto conveniente, poiché verrebbe individuato immediatamente dalla rete, portando ad una totale perdita di fiducia nel sistema.
- ✓ Attacco a collisione: il nodo disonesto dovrebbe tentare la creazione di un indirizzo hash uguale a quello di un altro utente. In questo modo potrebbe utilizzare i fondi dell'indirizzo attaccato. Tuttavia nella pratica non è realizzabile, poiché non esiste un computer con la forza computazionale necessaria a svolgere tutti i calcoli per l'attacco.

1.7 Gli Altcoins

Dopo il successo del progetto Bitcoin si è assistito alla proliferazione di numerose nuove criptovalute anche chiamate “alt-coin” (alterative coins), realizzate per i più svariati fini e operative in sempre più eterogenei settori. Nella maggior parte dei casi queste nuove criptovalute si allontanano poco dal progetto originale Bitcoin , più che altro tentano di modificare alcuni limiti reali o presunti del protocollo originale. La proliferazione di così tante criptovalute , ad oggi circa 6.643 (fonte:coinmarket.com) , è stata resa possibile grazie al rilascio del codice relativo alla rete Bitcoin in modalità open-source. Il motivo di tale scelta è dovuto alla visione degli ideatori , ispirata al pensiero Hayek , secondo cui la moneta (in questo caso le criptomonete) possa raggiungere la stabilità grazie a meccanismi concorrenziali. Elenchiamo ora di seguito le cinque criptomonete (sei considerando Bitcoin , ampiamente

trattato) scelta per la nostra analisi in base al livello di capitalizzazione e alla disponibilità dei dati.

Ethereum: Ethereum nasce nel 2013 per opera di Vitalik Buterin, uno sviluppatore di origini russe, cresciuto in Canada, che univa la competenza di programmatore a quelle di ricercatore nell'ambito delle cryptocurrency. Ethereum è diventato pubblico e accessibile online solo nel 2015. Oltre ad essere un sistema di pagamento Ethereum permette di eseguire i cosiddetti smart contract. Gli smart contract sono protocolli informatici che permettono di verificare e far rispettare l'esecuzione di un contratto.

Bitcoin Cash : Il Bitcoin Cash apparso il primo di agosto 2017, e deve quasi tutto il suo codice al progetto originario del Bitcoin. Si tratta infatti di un hard fork del Bitcoin. Gli hard fork in informatica avvengono quando il team di sviluppo di un software, essendo in disaccordo con il resto del gruppo, decide di creare in modo indipendente una nuova versione del codice. Si crea quindi un software derivato con specifiche proprietà distinte e separate. Lo scopo principale degli autori di bitcoin cash era quello di creare una moneta virtuale, che permettesse di velocizzare i tempi di validazione dei blocchi.

Litecoin: distribuito il 7 ottobre 2011 da Charles Lee, un ex-dipendente di Google. Le caratteristiche principali del Litecoin sono molto simili a quelle del protocollo Bitcoin. L'obiettivo principale di Litecoin è la diminuzione dei tempi di conferma delle transazioni, la difficoltà di mining è stata infatti abbassata in modo da rendere possibile la creazione di un nuovo blocco circa ogni due minuti. Inoltre il tetto massimo di monete generabili è più alto rispetto al Bitcoin, con una soglia di 84 milioni.

Ripple (XRP): ideata da Chris Larsen e Jed McCaleb, fondatori di OpenCoin (ora rinominata Ripple Labs), una start-up di San Francisco. Il simbolo della criptovaluta è XRP, Ripple è il nome della piattaforma che ospita la valuta. Il Ripple non può essere creato attraverso mining, secondo le regole stabilite dal protocollo, di XRP dovranno essercene in circolazione 100 miliardi. L'intera scorta è stata emessa nel 2012, ma oltre la metà è ancora nelle mani di OpenCoin, che intende rilasciarla sul mercato in modo graduale. Non prevedendo il processo di mining dispendioso dal punto di vista energetico, XRP rappresenta la versione ecologica del bitcoin.

EOS: ideata dal noto ingegnere Dan Larimer a metà del 2017. Inizialmente tale sistema nasce con lo scopo di fornire servizi personalizzabili di autenticazione, di cloud storage e di server hosting. Per prima cosa bisogna specificare che EOS è il nome della criptovalute, mentre il software open source su cui gira la criptovalute prende il nome di Eos.io. Nelle prime fasi di sviluppo EOS non possedeva alcuna blockchain , ma si appoggiava alla blockchain di Ethereum. Tra i punti di forza di tale criptovaluta, gli sviluppatori elogiano la sua scalabilità, flessibilità e usabilità. La scalabilità indica la quantità di transazioni che la piattaforma riesce a supportare contemporaneamente. La flessibilità fa riferimento alla possibilità di poter bloccare l'operazione nel caso di errori (errore di indirizzo, digitazione errata della quantità da inviare, ecc....) . L'usabilità è la sua capacità di essere usata anche da coloro che non possiedono particolari capacità informatiche.

Capitolo 2

2.1 Pair Trading: Storia

La prima forma di Pair Trading come strategia di investimento è attribuita all'investitore e trader americano Jesse Livermore. Egli intorno al 1920 concepì una strategia di investimento che prese il nome di "sister stock". La strategia consisteva nell'identificazione di coppie di titoli i cui prezzi tendevano a muoversi insieme. Ogni volta che si presentavano anomalie nel rapporto tra le coppie di titoli, i due titoli venivano scambiati contemporaneamente, con l'idea che l'anomalia si sarebbe corretta nel futuro. La strategia di Livermore è probabilmente uno dei primi esperimenti per le strategie di Pair Trading, la cui teorizzazione è avvenuta solo una decade dopo. Tale teorizzazione è attribuita al quant di Wall Street Nunzio Tartaglia, Trader alla Morgan Stanley a metà degli anni '80. Al tempo Tartaglia, riunì un gruppo di matematici, fisici e esperti di computer; la loro missione era quella di sviluppare strategie di arbitraggio quantitativo utilizzando tecniche statistiche all'avanguardia. Le strategie sviluppate dal gruppo erano completamente automatizzate, tecniche che risultavano assolutamente all'avanguardia per quel periodo. Una delle tecniche utilizzate per la negoziazione era proprio una strategia di trading di coppie. Questa strategia è poi diventata particolarmente utilizzata e ha preso il nome di "*Pair Trading*". Tartaglia e il suo gruppo grazie alle strategie di Pair Trading fecero un profitto di circa 50 milioni di dollari nel 1987. Il gruppo non riuscì a ottenere le stesse performance l'anno seguente e si sciolse definitivamente nel 1989. Da allora le strategie di Pair Trading hanno assunto sempre maggior rilievo all'interno di hedge fund e presso investitori istituzionali.

2.2 Definizione

L'idea alla base delle strategie di Pair Trading è quella di vendere i titoli sopravvalutati e acquistare i titoli sottovalutati. Per individuare una sopravvalutazione o una sottovalutazione, occorre conoscere il valore dei titoli in termini assoluti. Spesso risulta però difficile l'individuazione di tale valore. Le strategie di Pair Trading tentano di risolvere tale problema, utilizzando il concetto di valore relativo. L'idea alla base è che se due titoli presentano caratteristiche simili, devono avere un prezzo che è più o meno lo stesso. In questa strategia il prezzo di uno specifico titolo non è importante, perché può essere sbagliato, ciò che importa è che i due prezzi siano simili. Se i prezzi si discostano, significa che uno dei due titoli è

sopravvalutato o sottovalutato, o magari questa differenza è data dalla combinazione di entrambi gli elementi. Le strategie di Pair Trading da un punto di vista operativo prevedono l'acquisto del titolo con il prezzo più basso e la vendita del titolo con il prezzo più alto, con l'idea che la discrepanza tra i due prezzi si corregga da sola nel futuro. Di fondamentale importanza nelle strategie di Pair Trading è l'identificazione dei titoli che presentano un equilibrio di lungo periodo, e l'individuazione del temporaneo disallineamento dall'equilibrio di lungo periodo. Per la selezione dei titoli è possibile dividere le strategie in due grandi macro aree: analisi fondamentale e analisi econometrica.

L'analisi fondamentale si concentra sull'acquisizione di dati finanziari ed economici di una società, con lo scopo di determinare se il prezzo del titolo emesso sia correttamente valutato dal mercato. Attraverso la valutazione di tutte le informazioni disponibili sul mercato, come le previsioni di ricavi, costi dell'andamento del settore e dell'economia, si cerca di individuare il valore intrinseco del titolo. Secondo la teoria economica, nel lungo periodo il prezzo tende a muoversi verso il valore intrinseco, se questo si trova al di sopra del valore corrente del prezzo, si apre una posizione lunga sul suddetto titolo. Contrariamente, nel caso in cui il valore intrinseco si trova al di sotto del prezzo corrente del titolo, questo viene venduto allo scoperto.

La pair selection basata su modelli statistico-econometrici ha lo scopo di individuare la distanza media dei prezzi delle coppie di titoli e come questi si muovono nel tempo. Mentre l'analisi dei fondamentali teoricamente permette di selezionare trasversalmente le coppie tra società che hanno un core business simile, con un metodo statistico vi sono regole per la selezione più stringenti. Tra le strategie basate su modelli econometrici quelle più note sono: distance method e il cointegration approce .

2.3 Distance Method

Il metodo della distanza è stato introdotto per la prima volta in un paper del 1999 di Gatev e all.: *“Pairs Trading: Performance of a Relative Value Arbitrage Rule”*. Nel lavoro di Gatev per l'identificazione delle coppie di asset che presentano co-movimento si utilizza una sorta di funzione distanza. Gli autori introducono il concetto di Tracking Variance , una misura della distanza tra i prezzi normalizzati di due asset. Data una serie storica dei prezzi di due asset “A,B”; $\{P_1^A; P_2^A; \dots \dots \dots; P_t^A; \dots \dots \dots; P_T^A\}$ e $\{P_1^B; P_2^B; \dots \dots \dots; P_t^B; \dots \dots \dots; P_T^B\}$, la Tracking Variance è calcolata come :

$$TV = \frac{1}{T} \sum_{t=1}^T (Q_t^A - Q_t^B)^2$$

Con $Q_t^A = \frac{P_t^A}{P_1^A}$ e $Q_t^B = \frac{P_t^B}{P_1^B}$ sono i prezzi normalizzati dei due asset A e B ; inoltre la differenza tra i due asset prende il nome di spread e si indica con $\delta = Q_t^A - Q_t^B$.

Una volta ottenuta la Tracking Variance è possibile utilizzare i criteri di minimizzazione per ottenere le coppie di asset compatibili e che presentano quindi livelli di co-movimento sufficiente a poter applicare una strategia di Pair Trading. Il secondo step consiste nell'individuazione del momento di apertura delle operazioni. Per capire quando aprire un'operazione bisogna osservare lo spread. Ogni qual volta lo spread si allontana da una certa soglia prestabilita le due operazioni ,long e short ,vengono aperte, per poi aspettare che il valore si ristabilisca. Nello studio di Gatev e all. si utilizza come valore soglia il doppio del valore della deviazione standard. Il valore della deviazione standard viene così calcolato :

$$SD = \frac{1}{T-1} \sum_{t=1}^T [(Q_t^A - Q_t^B)^2 - TV]^{1/2}$$

Ogni volta che $\delta > 2SD$ si apre un operazione lunga sul titolo B e un'operazione corta sul titolo A, allo stesso modo, quando $\delta < -2SD$ si apre un operazione corta sul titolo B e un operazione lunga sul titolo A. Le posizione vengono tenute aperte finche lo spread non rientra nel valore soglia oppure quando le perdite superano un valore prestabilito (stop loss). Nello studio effettuato da Gatev sul mercato americano è stato preso un periodo di osservazione considerevolmente lungo (1962-2002). Durante questo periodo, per ogni anno, sono stati creati dei portafogli in base alle coppie con minor Tracking Variance. Su tali portafogli è stato calcolato il rendimento nei sei mesi successivi all'anno di stima. Questo processo è stato reiterato per tutti i 40 anni del periodo di osservazione, ed in seguito è stata effettuata una media dei rendimenti ottenuti dai portafogli. Tra i vari portafogli (top 5, top 20 e top 100), la miglior performance è stata ottenuta dal portafoglio in cui erano presenti le 20 coppie con minor Tracking Variance. Il rendimento medio mensile, ottenuto nel periodo dei sei mesi (trading period) successivi ad ogni anno di stima è stato corrispondente a 1,44%, ossia circa il 18% su base annua.

Tabella 2.1

Portfolio	top 5	top 20	20 after top 100	All
Panel A: Excess Return Distribution (No Waiting)				
Mean (Committed capital)	0.0598	0.0601	0.0451	0.0410
Standard error (Newey-West)	0.0065	0.0055	0.0038	0.0038
t-statistic	9.1363	10.8866	11.8900	10.7022
Excess return distribution				
Median	0.0549	0.0543	0.0457	0.0325
Standard deviation	0.0704	0.0526	0.0482	0.0354
Kurtosis	0.7323	2.5906	0.2319	1.5074
Skewness	0.4352	0.9781	0.1500	1.1730
Minimum	-0.1423	-0.0792	-0.0793	-0.0248
Maximum	0.2972	0.3124	0.1946	0.1756
Observations with excess return < 0	16%	9%	16%	7%
Mean excess return on employed capital	0.0601	0.0606	0.0456	0.0423

Fonte: Gatev, et al. “*Pairs trading: Performance of a relative value arbitrage rule*”

Questo risultato ha così dimostrato l’evidenza empirica della profittabilità del pair trading basato sulla tracking variance. Il lavoro di Gatev è stato estremamente oneroso a causa della vastità dei titoli presi in considerazione ed del periodo sotto osservazione.

2.4 Approccio di cointegrazione

L’utilizzo dell’approccio di cointegrazione applicato a strategie di Pair Trading è stato introdotto per la prima volta da Vidyamurthy nel suo libro del 2004: “*Pairs Trading: Quantitative Methods and Analysis*”. Il test di cointegrazione viene utilizzato nelle strategie di Pair Trading per individuare movimenti di lungo periodo tra coppie di asset. Diversi sono i test statistici elaborati per analizzare la cointegrazione di due serie storiche non stazionarie. Vidyamurthy approfondisce in particolare due test: la procedura a due fasi di Engle e Granger (1987) e il Metodo di Johansen per l’analisi multivariata. Il concetto di cointegrazione fu introdotto per la prima volta dagli econometrici Engle e Granger, idea che gli valse il premio Nobel per l’economia nel 2003. Engle e Granger osservando il comportamento di serie storiche non stazionarie e si resero conto che in alcuni casi attraverso una specifica combinazione lineare era possibile ottenere una nuova serie, e quest’ultima risultava essere stazionaria. Da

un punto di vista formale , date due serie storiche integrate di ordine uno $\{X_t; Y_t\}$, se esiste qualche coefficiente θ , tale che la relazione $Y_t - \theta X_t$ risulta integrata di ordine zero ; allora $\{X_t; Y_t\}$ sono dette cointegrate. Il termine $Y_t - \theta X_t$ è detto termine a correzione d'errore , tale differenza permette di eliminare il trend stocastico comune. Nella definizione di cointegrazione si è parlato di serie storiche integrate di ordine uno, dunque prima di passare ad un'ulteriore approfondimento sul test di cointegrazione , occorre definire quando una serie storica è integrata di ordine uno.

2.5 Test di radici unitarie e stazionarietà

Un processo stocastico y_t si definisce stazionario se il suo momento primo e il suo momento secondo sono costanti nel tempo. In altre parole un processo stocastico y_t è stazionario se :

- $E(y_t) = \mu_y \quad \forall t \in T$
- $[(y_t - \mu_y)((y_{t-h} - \mu_y))] = \gamma_h \quad \forall t \in T$

La prima condizione ci dice che una serie storica generata da un processo stocastico stazionario deve fluttuare intorno a un valore medio costante e non deve avere un trend . La seconda condizione invece ci dice che la varianza di un processo stocastico stazionario deve restare costante nel tempo ; inoltre le covarianze non dipendono dal tempo “t” ma semplicemente dalla distanza tra le osservazioni, ovvero dall' ordine del ritardo. Se il processo stocastico che si sta analizzando non è stazionario , ma è stazionaria la sua differenza prima , allora si dice che il processo stocastico è integrato di ordine uno , $I(1)$. In generale si definisce come processo $I(d)$, ovvero integrato di ordine d , un processo la cui differenza d -esima è stazionaria. dunque solo dopo aver analizzato che le serie storiche che si sta analizzando sono integrate di ordine uno , è possibile passare al test di cointegrazione. nel corso degli anni sono stati individuati diversi test statistici in grado di verificare la stazionarietà di una serie storica e il grado di integrazione . Tra questi i più utilizzati sono :

- Test Augmented Dickey Fuller (ADF)
- Test Phillips-Perron (PP)
- Test KPSS

2.5.1 Test Dickey-Fuller e Augmented Dickey Fuller

Il test di Dickey-Fuller fu teorizzato nel 1979 per testare la stazionarietà di un processo , analizzando la presenza di radici unitarie nel polinomio autoregressivo. In primo momento il test era quindi stato pensato soltanto per modelli $AR(1)$. In seguito nel 1984 Said e Dickey

riuscirono ad estendere la procedura a modelli autoregressivi di ordine superiore al primo , creando il cosiddetto Augmented Dickey_Fuller test. Nel test ADF si ipotizza che il processo stocastico y_t sia caratterizzato da una forma AR(p):

$$y_t = a_0 + a_1 t + \sum_{j=1}^p p_j y_{t-j} + u_t \quad \text{con } u_t \sim WN$$

Da tale processo attraverso una riformulazione del modello , ottenuta sottraendo y_{t-1} da entrambi i lati:

$$\Delta y_t = a_0 + a_1 t + \beta y_{t-1} + \sum_{j=1}^{p-1} \gamma_j y_{t-j} + u_t \quad \text{con } u_t \sim WN$$

Le ipotesi del test sono dunque:

$$H_0: \beta = 0; H_1: \beta < 0$$

La statistica test è data da $\frac{\hat{\beta}}{\sigma_{\hat{\beta}}}$, tale statistica test non si distribuisce né come una t-student né come una normale. Si ricorre invece alla distribuzione Dickey-Fuller , scoperta dagli autori del test.

Il test Dickey-Fuller come già accennato risulta essere un caso particolare del test ADF, dove l'ordine p del modello autoregressivo è pari a uno.

2.5.2 Il Test Phillips-Perron

Il test PP, acronimo di Phillips-Perron , teorizzato nel 1988 è un tipo di test di radice unitaria che parte dalla seguente relazione:

$$y_t = \beta c_t + \varphi y_{t-1} + u_t$$

dove u_t è un processo integrato di ordine zero I(0) , che può essere eteroschedastico. Dunque il test Phillips-Perron, rispetto al test ADF, prevede delle statistiche test non parametriche per lo studio dell'ipotesi nulla della radice unitaria . Infatti, esso suppone che la componente erratica del processo possa essere dipendente, ossia correlata ed eteroschedastica. L'attenzione si fonda sulla modalità differente dall'ADF nella trattazione della correlazione seriale nelle regressioni usate: il primo sfrutta una struttura parametrica autoregressiva; invece il test di PP non tiene conto di alcuna forma di correlazione nel processo usato per la verifica dell'ipotesi.

2.5.3 Test KPSS

In statistica ed in econometria, il test KPSS (dal nome degli autori Kwiatkowski, Phillips, Schmidt e Shin) è un test di verifica d'ipotesi che si utilizza quando si vuole confrontare l'ipotesi nulla di stazionarietà di una serie storica autoregressiva con l'ipotesi alternativa che la serie abbia una o più radici unitarie. Questa statistica si basa sul seguente modello autoregressivo:

$$x(t) = v(t) + \theta v(t - 1)$$
$$y(t) = \xi + \beta y(t - 1) + x(t)$$

Il test si sviluppa sulle seguenti ipotesi:

- H0: i dati derivano da un processo stazionario o da processi stazionari con tendenza in media (trend)
- H1: i dati derivano da un processo non stazionario

La statistica del test è calcolata tramite i moltiplicatori di Lagrange:

$$S = \frac{(T^{-2} \sum_{t=1}^T \hat{S}_t^2)}{\sigma_\varepsilon^2}$$

- ✓ T è la dimensione del campione
- ✓ σ_ε^2 è la varianza di long-run
- ✓ $\sum_{t=1}^T \hat{S}_t^2$ è la somma parziale degli errori dalla regressione $y(t)$

2.6 Engle Granger Test Cointegrazione

Il metodo proposto da Engle e Granger nel 1987 per verificare la presenza di cointegrazione e stimare la relazione di lungo periodo è costituito essenzialmente da due step:

- ➔ Il primo step: Stima di un modello di regressione lineare tra le variabili non stazionarie in gioco semplicemente mediante il metodo OLS.
- ➔ Secondo step: Test per la presenza di radici unitarie nei residui del modello.

Espresso in maniera formale, date due serie storiche non stazionarie y_t e x_t , se esiste un certo valore λ , per cui $y_t - \lambda x_t$ è una nuova serie storica stazionaria, allora le due serie di partenza si dicono cointegrate. Nelle serie storiche non stazionarie i momenti primi variano nel tempo: media, varianza e covarianza sono valori non costanti nel tempo.

$$E(y_t) = \mu_t$$

$$Var(y_t) = kf(\mu_t)$$

$$Cov(y_t, y_{t-h}) = \gamma_t(h)$$

Dove k è una costante e $f(\cdot)$ è una funzione nota. Un esempio di serie storica non stazionaria è la serie storica generata a partire da un processo AR(1) con un coefficiente di regressione pari a 1 ($\phi = 1$), tale processo prende il nome di random walk. Generalmente dalla combinazione lineare di due serie storiche non stazionarie si ottiene una nuova serie storica non stazionaria; esistono però alcuni casi in cui la nuova serie storica risulta stazionaria e in qual caso si dice che le serie storiche di partenza sono cointegrate. In termini matematici, se esiste un vettore β tale che la combinazione lineare :

$$\epsilon_t = Y_t - \beta X_t \sim I(0)$$

è stazionaria le due serie storiche $X_t, Y_t \sim I(1)$ si dice che sono cointegrate. Per questo la cointegrazione esprime l'equilibrio di lungo periodo tra due variabili stocastiche, equilibrio che può divergere nel breve periodo, ma che tende poi a ristabilirsi. Di fondamentale importanza non confondere il concetto di cointegrazione con il concetto di correlazione, mentre il primo esprime la relazione di lungo periodo, il secondo esprime la relazione nel breve periodo, relazione instabile che varia in modo significativo nel tempo. Avere cointegrazione non vuol dire che le due serie storiche si muovono nella stessa direzione, ma che nel lungo periodo il rapporto tra le differenze prime tende ad essere costante. Inoltre è possibile osservare serie storiche che presentano cointegrazione ma non correlazione.

2.7 Procedura di Johansen

Il test di Johansen è un'ulteriore metodo per verificare la presenza o meno di cointegrazione tra due o più serie storiche. A differenza del test di Engle e Granger, che basa la propria analisi di cointegrazione su un modello autoregressivo, il test di Johansen utilizza l'ipotesi di processi stocastici modellati attraverso un modello autoregressivo vettoriale (VAR).

Definizione: VAR (Stock e Watson Introduzione all'Econometria)

Un' modello autoregressivo vettoriale (VAR) è un insieme di k regressori temporali, in cui i regressori sono i valori ritardati delle k variabili dipendenti. Il Var generalizza l'autoregressione univariata a un insieme, o vettore, di serie temporali. Quando il numero dei ritardi è lo stesso in ogni equazione ed è pari a p , allora il sistema di equazioni è detto VAR(p). Nel caso di due variabili, $Y_t; X_t$, il Var(p) consiste in due equazioni:

$$Y_t = \beta_{10} + \beta_{11}Y_{t-1} + \dots + \beta_{1p}Y_{t-p} + \gamma_{1p}X_{t-p} + u_{1t}$$

$$X_t = \beta_{20} + \beta_{21}Y_{t-1} + \dots + \beta_{2p}Y_{t-p} + \gamma_{2p}X_{t-p} + u_{2t}$$

dove i β, γ sono i coefficienti ignoti e u_{1t}, u_{2t} sono i termini di errore.

Per il test di Johansen consideriamo il modello autoregressivo vettoriale generale, VAR(p):

$$X_t = \mu + \Lambda_1 X_{t-1} + \dots + \Lambda_p X_{t-p} + w_t$$

Dove μ rappresenta la media a valori vettoriali delle serie, Λ_1 sono le matrici dei coefficienti per ogni ritardo (lag) e w_t è un termine di rumore gaussiano multivariato con media zero.

Passando al modello di correzione degli errori vettoriali (VECM), ottenuto differenziando la serie:

$$\Delta X_t = \mu + \Lambda_1 X_{t-1} + \Gamma_1 \Delta X_{t-1} + \dots + \Gamma_p \Delta X_{t-p} + w_t$$

Dove $\Delta X_t = X_t - X_{t-1}$ è l'operatore di differenziazione, Λ_1 è la matrice dei coefficienti per il primo ritardo e Γ_i sono le matrici per ogni ritardo differenziato.

Nel test di Johansen la situazione di non cointegrazione si verifica quando la matrice Λ_1 è uguale a zero. Se invece $\Lambda_1 \neq 0$, possiamo continuare il test, e a questo punto bisogna considerare il rango (r) della matrice Λ_1 . Il numero di coppie indipendenti che si possono formare attraverso la combinazione delle serie storiche cointegrate è pari al rango di Λ_1 . Nel test Johansen è possibile calcolare il rango (r) attraverso due modi distinti, entrambi basati sulla decomposizione spettrale di Λ_1 . Nel test di Johansen si verifica in modo sequenziale se il

rango della matrice Λ_1 è uguale a zero, uguale a uno, fino ad arrivare a $r = n - 1$, dove n è il numero di serie temporali in esame. L'ipotesi nulla di $r = 0$ significa che non c'è affatto cointegrazione, mentre un rango $r > 0$ implica una relazione di cointegrazione tra due o forse più serie temporali. Gli autovettori associati all'insieme di autovalori costituiscono i coefficienti di combinazione lineare, dalla quale è possibile ottenere la nuova serie storica stazionaria.

Capitolo 3

3.1 Introduzione

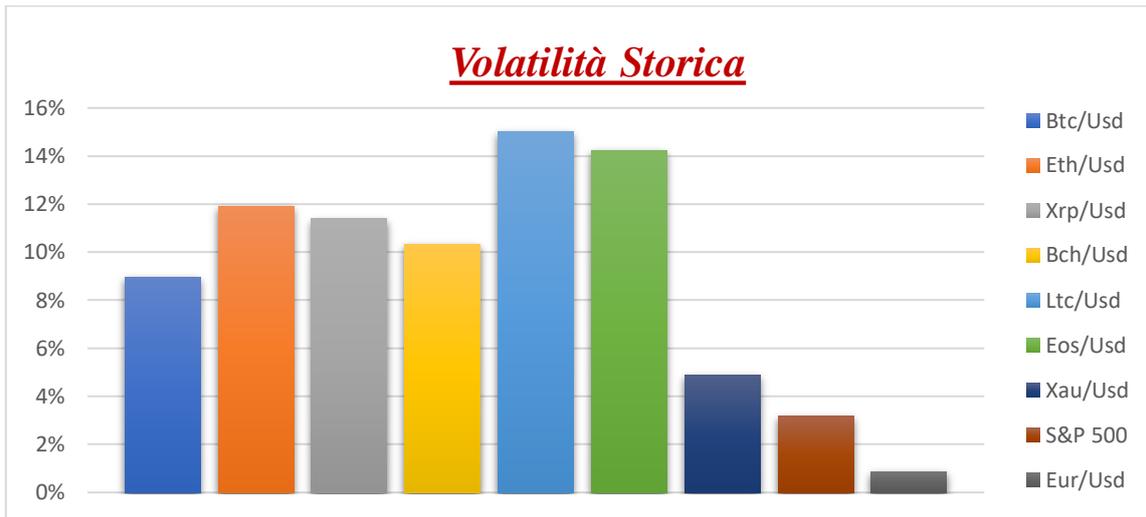
Lo scopo della ricerca è capire se è possibile applicare in modo profittevole una strategia di Pair Trading al mercato delle criptovalute. Ciò che spinge ad analizzare proprio il mercato delle criptovalute per testare la profittabilità di una strategia di Pair Trading è:

- la presenza di elevati livelli di volatilità
- la presenza di elevati livelli di correlazione tra le diverse criptovalute

Per l'analisi si utilizzeranno le serie storiche di sei criptovalute scelte tra quelle con maggior capitalizzazione e in base alla disponibilità dei dati. Le sei criptovalute sono: Bitcoin, Ethereum, XRP, Bitcoin Cash, Litecoin e Eos. I dati storici delle sei criptovalute sono stati raccolti tramite estensione Api per Excel dal sito CoinMarket per il periodo 9 aprile 2019 – 23 Luglio 2020. I prezzi di tutte le criptovalute sono espressi in dollari e rappresentano in valore di chiusura giornaliera. La volatilità degli asset finanziari esprime il livello di rischio collegato alla detenzione dello strumento finanziario. Il termine rischio non è utilizzato come connotazione negativa, ma semplicemente come caratteristica statistica delle serie storiche che tendono a discostarsi dal valore medio con maggiore ampiezza. Alti livelli di volatilità possono essere interpretati proprio come sintomo di un' instabilità del mercato; instabilità che può essere appunto sfruttata attraverso strategie di arbitraggio. Confrontiamo ora i livelli di volatilità delle sei criptovalute che stiamo analizzando rispetto ad asset tradizionali, in particolare l'oro, l'indice S&P 500 e il cambio Eur/Usd. Come indicatore di volatilità utilizzeremo la deviazione standard. Data un serie storica di dati $\{X_1, \dots, \dots, X_n\}$, di media campionaria μ , la deviazione standard campionaria o scarto quadratico medio campionario si calcola come:

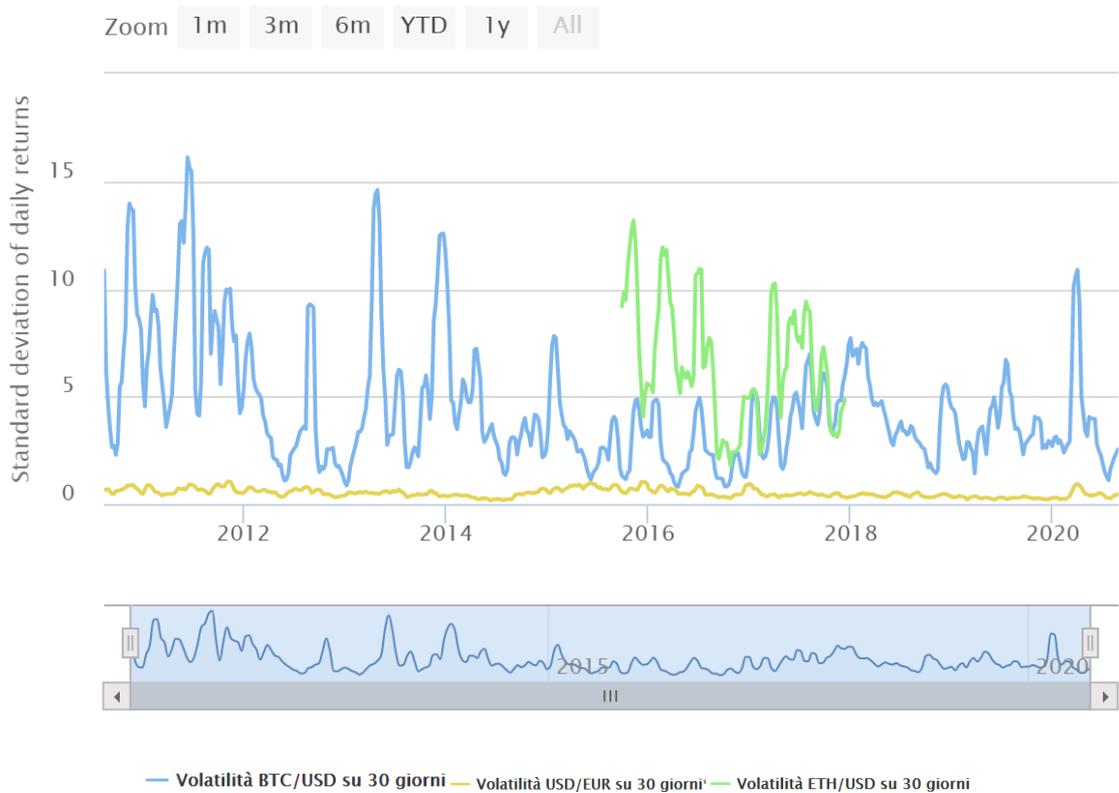
$$\sigma = \sqrt{\frac{(x_1 - \mu)^2 + \dots + (x_n - \mu)^2}{n-1}}$$

Figura 3.1



Fonte: Elaborazione Propria

Figura 3.2



fonte: <https://www.buybitcoinworldwide.com/it/indice-di-volatilita/>

Com'è possibile osservare dall' istogramma nonostante i recenti avvenimenti (Covid-19) abbiano portato grandi instabilità sui mercati finanziari, e di conseguenza l'aumentato temporaneo dei livelli di volatilità, gli asset tradizionali non hanno ancora raggiunto i livelli

del Bitcoin. Questo indica un mercato non ancora maturo in cui appunto è possibile sfruttare disallineamenti. Proprio per la caratteristica di persistenza di alti livelli di volatilità presente sul mercato delle criptovalute si è deciso di utilizzare i prezzi di chiusura giornalieri. Altro elemento di cui si parlato gli alti livelli di correlazione presenti sul mercato delle criptovalute. La correlazione indica la tendenza che hanno due variabili (X e Y) a variare insieme, ovvero, a covariare. La covarianza si calcola come media dei prodotti degli scarti dalle rispettive medie:

$$Cov(X, Y) = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{n}.$$

Analizziamo la matrice delle correlazione , la quale può risultare un buon indicatore approssimativo per identificare la relazione tra asset finanziari.

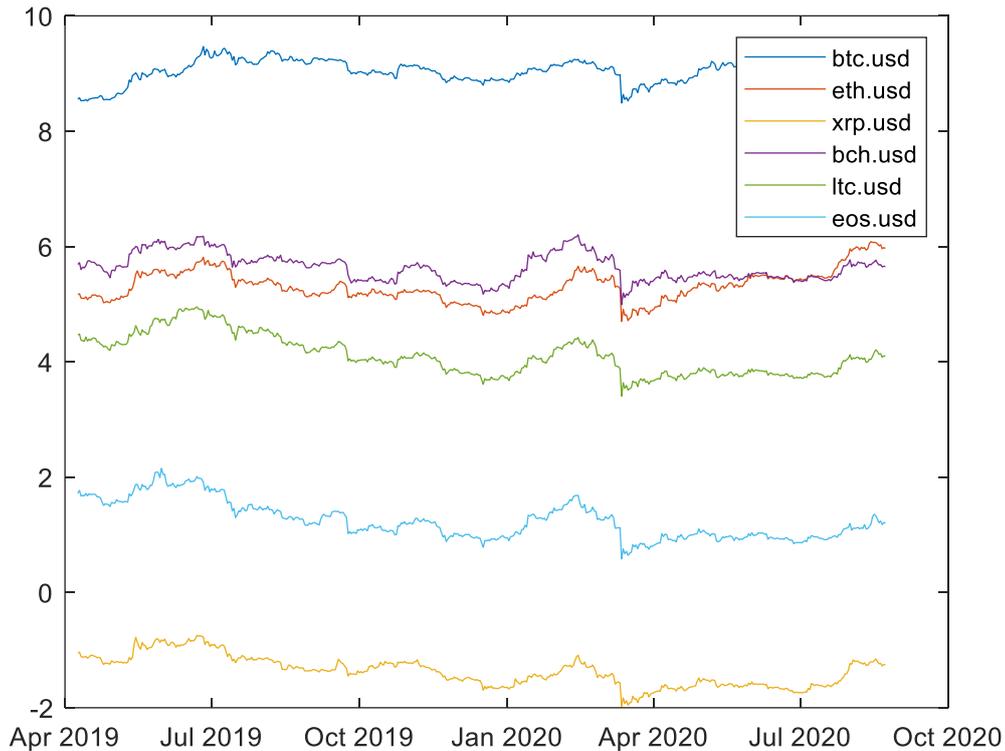
Tabella 3.1

	<i>Btc</i>	<i>Eth</i>	<i>Xrp</i>	<i>Bch</i>	<i>Ltc</i>	<i>Eos</i>
<i>Btc</i>	1					
<i>Eth</i>	0.718378	1				
<i>Xrp</i>	0.27317	0.45644	1			
<i>Bch</i>	0.430302	0.493208	0.802413	1		
<i>Ltc</i>	0.314557	0.40042	0.93627	0.84524	1	
<i>Eos</i>	0.122982	0.344572	0.929294	0.868048	0.931922	1

Fonte: Elaborazione propria

Come è osservabile dalla matrice di correlazione, la maggior parte delle criptovalute presenta valori superiore a 0.6. Quindi è possibile affermare che almeno nel breve periodo esiste una relazione di equilibrio. Relazione che si evince anche dall'osservazione del grafico delle serie storiche dei logaritmi dei prezzi.

Figura 3.3



Fonte: Elaborazione propria

Partendo proprio da tali considerazioni passiamo all'analisi di cointegrazione per individuare l'equilibrio di lungo periodo.

3.2 Costruzione del set di dati

Nella creazione di una strategia di Pair Trading automatico risulta fondamentale la fase di backtesting . Tale metodologia consiste nell'analisi dei dati storici per valutare la profittabilità della nostra strategia di Trading. E necessario suddividere la serie storica in due diversi set per le diverse due fasi del processo di analisi. Il primo set, definito training set, utilizzato uno per la stima delle diverse tipologie di modelli . Il secondo set, detto testing set, di cui fanno parte i restanti dati viene utilizzato per la valutazione delle prestazioni della strategia di Pair Trading. Per quanto riguarda la suddivisione della serie storica da analizzare non esiste una regola precisa. Nel suo lavoro "*Quantitative Trading: How to Build Your Own Algorithmic Trading Business* ,(John Wiley & Sons, 2009)", Ernie Chan consiglia la suddivisione del campione in due parti uguali. Nel caso il campione non risulti sufficientemente grande è possibile assegnare i due terzi del campione totale al training set e il restante un terzo al testing set. Seguendo tale linea per la costruzione e la validazione della nostra strategia di Pair Trading si è diviso il campione in tal modo :

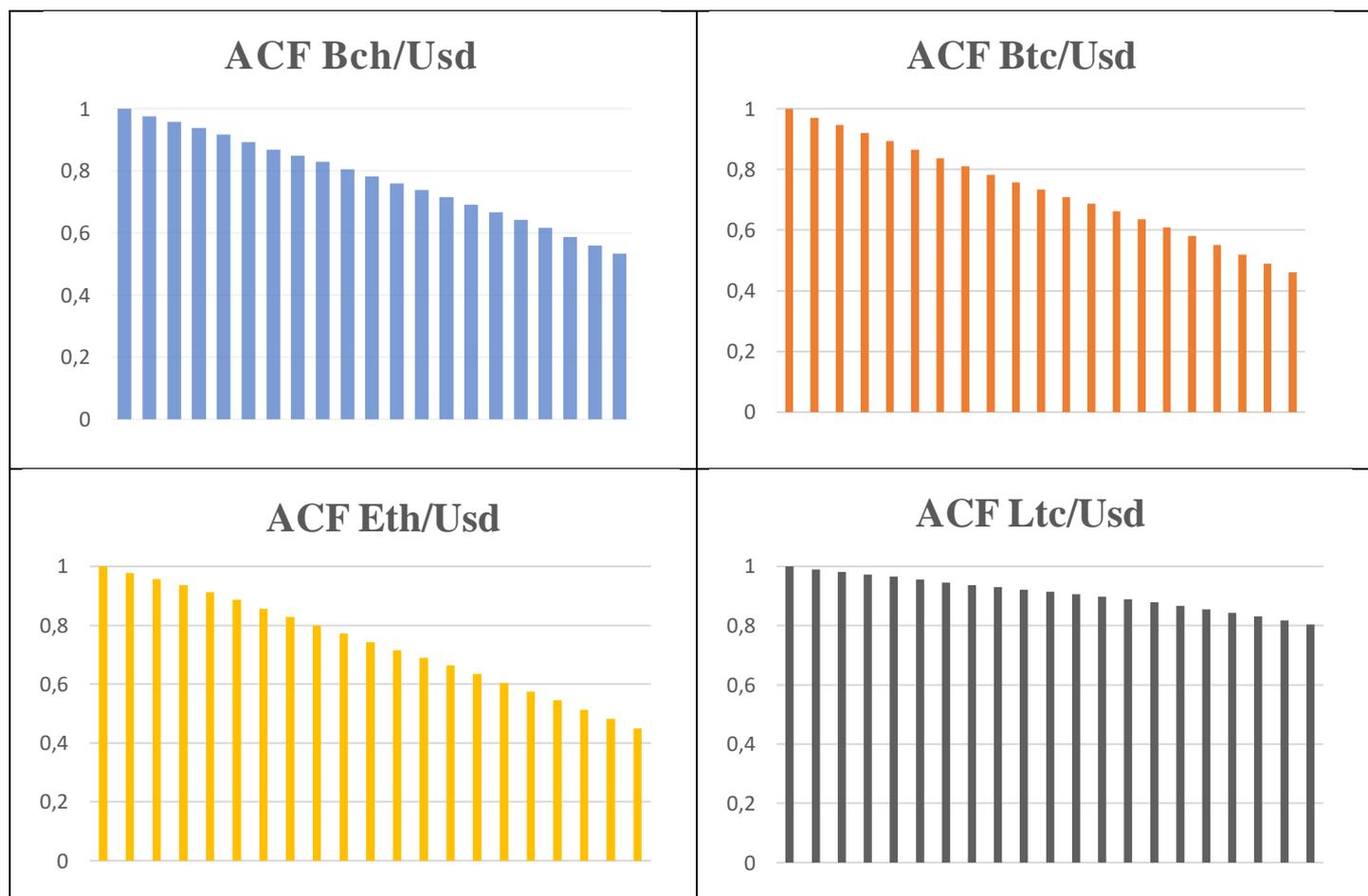
- 1) 316 osservazioni nel Training set
- 2) 157 osservazioni nel Testing set

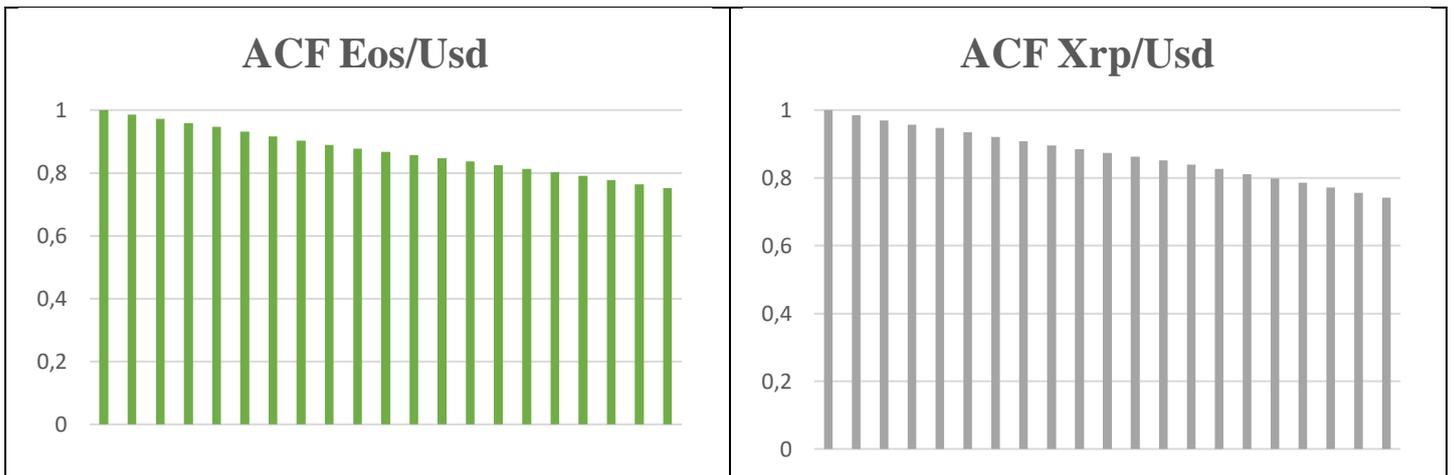
Alla fine della costruzione della strategia le performance dei due set vengono confrontati, in modo che l'algoritmo non degradi le proprie performance nell'immediato futuro rispetto le performance ottenute sul Training set utilizzato per la stima dei parametri.

3.3 Test di Integrazione e Stazionarietà

Come già detto nei capitoli precedenti una condizione necessaria per effettuare un test di cointegrazione, è che le serie stazionarie che si stanno analizzando siano integrate di ordine 1. Una prima metodologia, meno robusta, per individuare se una serie storica è stazionaria o non stazionaria è l'analisi della funzione di autocorrelazione (ACF). L'autocorrelazione è una funzione che misura la correlazione tra i valori della serie corrente e quelli delle serie passate, in questo modo definisce quali sono i valori delle serie passate più utili per prevedere i valori futuri. Analizziamo ora il correlogramma delle serie storiche delle sei criptovalute.

Tabella 3.2





Fonte: Elaborazione propria

Come è possibile osservare dai correlogrammi di tutte e sei le serie storiche delle criptovalute, il valore dell'autocorrelazione è sempre positivo e decresce lentamente all'aumentare dei ritardi. Tale comportamento del correlogramma indica che i valori della serie storica sono fortemente correlati a quelli della serie ritardata di un periodo, poi un po' meno per quella ritardata di due periodi e così via, ovvero che il presente è influenzato dal passato recente, questo dal passato più remoto e, in generale, che la serie presenta una componente di trend. Tale componente tendenziale potrebbe risultare eliminabile prendendo le differenze prime delle serie storiche.

Passiamo ora ad un'analisi più puntuale utilizzando due test statistici per l'individuazione di radici unitarie: ADF e KPSS. I due test sono stati applicati ai prezzi assoluti del training set delle sei criptovalute. La versione di Matlab del test ADF restituisce un valore che ci dà l'esito di decisione di rigetto dell'ipotesi nulla e il p-value associato. Se il test dà esito $h=1$ si sta indicando il rigetto dell'ipotesi di presenza di radici unitarie in favore dell'ipotesi alternativa di stazionarietà. La situazione opposta si presenta per il test KPSS; un esito di $h=1$ indica il rifiuto dell'ipotesi di stazionarietà, mentre un esito $h=0$ indica l'accettazione dell'ipotesi nulla di serie storiche stazionarie. L'ipotesi nulla in entrambi i test viene rigettata ad un livello di confidenza del 95%, ovvero quando il p-value è più piccolo del livello di significatività $\alpha = 0.05$. I risultati dei test sono presentati nelle tabelle seguenti:

Tabella 3.3

	BTC	ETH	XRP	BCH	LTC	EOS
ADF	0.116	0.345	0.461	0.297	0.615	0.435
KPSS	0.001	0.001	0.001	0.001	0.001	0.001

	Δ BTC	Δ ETH	Δ XRP	Δ BCH	Δ LTC	Δ EOS
ADF	0.010	0.010	0.010	0.010	0.010	0.010
KPSS	0.100	0.100	0.100	0.100	0.100	0.100

Fonte: Elaborazione propria

I risultati del test ADF mostrano che l'ipotesi nulla di presenza di radici unitarie nelle serie storiche dei prezzi è accettata, dunque come già si poteva intuire dall'analisi della funzione di autocorrelazione le serie storiche dei prezzi delle criptovalute non sono stazionarie. Invece i risultati del test ADF applicato alle differenze prime dei prezzi, mostrano l'accettazione della tesi di stazionarietà. Il test KPSS conferma l'ipotesi che i prezzi delle serie storiche non sono stazionarie, mentre lo sono le differenze prime. Possiamo quindi affermare che le serie storiche dei prezzi delle sei criptovalute sono processi storici integrati di ordine uno, $I(1)$.

3.4 Test Engle e Grenger

Ora che si è verificato che le serie storiche che stiamo analizzando sono processi stocastici integrati di ordine uno, possiamo passare al test di cointegrazione, per individuare le coppie di criptovalute da usare nella strategia di Pair Trading. Per testare l'ipotesi di cointegrazione utilizzeremo il test a due stadi di Engle e Granger. Il primo stadio del test consiste nella stima dei parametri della coppia di criptovalute tramite regressione lineare. Come metodo risolutivo per la regressione lineare è stato utilizzato il metodo degli OLS (metodo dei minimi quadrati). Date le serie storiche di due criptovalute X_t, Y_t il metodo dei minimi quadrati permette di stimare i parametri $\beta = [\beta_0; \beta_1]$ della relazione:

$$Y_t = \beta_0 + \beta_1 X_t + \epsilon_t$$

, $[\beta_0; \beta_1]$ rappresentano rispettivamente l'intercetta e il coefficiente di relazione. Il parametro β_1 rappresenta anche il cosiddetto, Hedge Ratio, ovvero il coefficiente che misura il grado di ritorno alla media dello spread tra le due criptovalute. A seconda di quale criptovaluta si decide di utilizzare come variabile indipendente il risultato del test di cointegrazione cambia. Riportiamo nella tabella 3.4 i risultati dei coefficienti di regressione per le dodici coppie di criptovalute:

Tabella 3.4

COPPIA	β_0	β_1	R^2
ETH/BTC	4381.4000	21.9440	0.3600
BTC/ETH	53.7360	0.0160	0.3600
XRP/BTC	6860.6000	6211.1000	0.0615
BTC/XRP	0.2092	0.0000	0.0615
ETH/XRP	0.0445	0.0012	0.7640
XRP/ETH	19.6750	599.0000	0.7640
XRP/EOS	-1.3529	18.8560	0.8550
EOS/XRP	0.1041	0.0454	0.8550
EOS/BTC	8041.7000	154.9300	0.0159
BTC/EOS	3.3225	0.0001	0.0159
EOS/ETH	82.8550	26.9740	0.6440
ETH/EOS	-0.4802	0.0239	0.6440
LTC/EOS	0.5310	0.0491	0.8120
EOS/LTC	5.2953	16.5270	0.8120
LTC/ETH	73.3023	1.6443	0.8050
ETH/LTC	-21.2850	0.4897	0.8050

Fonte: Elaborazione propria

Tabella 3.5

COPPIA	β_0	β_1	R^2
BTC/LTC	22.439	0.0060411	0.164
LTC/BTC	6663.3	27.099	0.164
LTC/XRP	0.10963	0.0024768	0.858
XRP/LTC	-27.292	346.27	0.858
XRP/BCH	54.09	863.63	0.583
BCH/XRP	0.08679	0.00067454	0.583
BCH/BTC	5391.7	10.685	0.233
BTC/BCH	119.45	0.021815	0.233
EOS/BCH	110.98	47.004	0.717
BCH/EOS	-0.50294	0.015264	0.717
BCH/LTC	-8.2527	0.2692	0.664
LTC/BCH	124.31	2.4654	0.664
ETH/BCH	29.447	1.4228	0.742
BCH/ETH	-82527	0.2692	0.664

Fonte: Elaborazione propria

Il secondo step della procedura di Engle e Granger consiste in un test di radici unitarie (ADF) sui residui della regressione precedentemente stimata. Se i residui risultano stazionari, allora le

due coppie di criptovalute sono cointegrate. Nella tabella seguente sono ripostati i p-value per il test ADF sui residui di tutte le coppie di criptovalute analizzate:

Tabella 3.6

COPPIA	P-VALUE	H=
ETH/BTC	0.0203	1
BTC/ETH	0.2823	0
XRP/BTC	0.0179	1
BTC/XRP	0.0687	0
ETH/XRP	0.0783	0
XRP/ETH	0.1698	0
XRP/EOS	0.0052	1
EOS/XRP	0.0045	1
EOS/BTC	0.0193	1
BTC/EOS	0.0873	0
EOS/ETH	0.1485	0
ETH/EOS	0.0681	0
LTC/EOS	0.0124	1
EOS/LTC	0.0169	1
LTC/ETH	0.0300	1

Fonte: Elaborazione propria

Tabella 3.7

COPPIA	P-VALUE	H=
ETH/LTC	0.2190	0
BTC/LTC	0.200	0
LTC/BTC	0.0138	1
LTC/XRP	0.0017	1
XRP/LTC	0.0036	1
XRP/BCH	0.0959	0
BCH/XRP	0.0679	0
BCH/BTC	0.0189	1
BTC/BCH	0.1348	0
EOS/BCH	0.0335	1
BCH/EOS	0.0279	1
BCH/LTC	0.1231	0
LTC/BCH	0.0738	0
ETH/BCH	0.0220	1
BCH/ETH	0.1231	0

Fonte: Elaborazione propria

Le coppie di criptovalute che risultano cointegrate presentano un valore dell' R^2 più alto, ovvero la variabile indipendente riesce a spiegare meglio la variabile dipendente. In assenza di cointegrazione abbiamo infatti stimatori di regressione che risultano distorti.

A questo punto occorre definire le regole della strategia di Pair Trading e applicarle alle ventuno coppie di criptovalute che hanno superato il test di cointegrazione.

3.5 Regole di Trading

Prendiamo ora in considerazione una delle coppie che risulta cointegrate, ad esempio Btc/Eth. I residui rappresentano lo spread della coppia, essendo quest'ultimi stazionari è possibile strutturare una strategia che preveda l'acquisto simultaneo, e di posizioni opposte. Lo spread può essere definito come:

$$\delta_t = BTC_t - \beta_1 ETH_t \text{ con } \beta_1 = 0.0168$$

Aprire una posizione lunga sullo spread significa aprire una posizione di 1 unità sul Bitcoin e una posizione corta di 0.0168 unità sull'Ethereum; per una posizione corta si fa l'opposto. Per prima cosa bisogna standardizzare lo spread in modo da normalizzare i segnali di entrata e di uscita. Calcoliamo la media (μ_t) e la deviazione standard (σ_t) dello spread utilizzando come campione il training set. Definiamo ora lo Z-score (Spread normalizzato) :

$$Z_t = \frac{\delta_t - \mu_t}{\sigma_t}$$

In una strategia di Pair Trading di questo tipo le operazioni sullo spread vengono aperte quando il valore dello Zscore diverge più di "n" deviazioni standard dalla media. Quando nel mercato in cui si sta operando i costi di transazione risultano alti, come nel caso delle criptovalute in cui le transazioni sono di circa lo 0.10-0.30%, si preferisce aumentare l'ampiezza della divergenza "n". Nel nostro caso si è impostato come segnale di entrata e di uscita:

Entrata Lunga	Zscore < -2
Uscita Lunga	Zscore > 0
Entrata Corta	Zscore > 2
Uscita Corta	Zscore < 0

3.6 Fase di Backtesting

Una volta identifica le regole per la strategia di trading , utilizzando la parte del campione definita training set, si passa alla fase di test della strategia. Per la valutazione della strategia , oltre a calcolare i ritorni cumulati, è stato utilizzando un' indicatore molto noto in Finanza "Sharpe Ratio". Per la valutazione della strategia è stato utilizzato una versione modificata di tale indice, versione proposta da Ernie Chan. Analizziamo le performance sulle coppie di criptovalute cointegrate:

Tabella 3.8

COPPIA	SHARPE RATIO	SHARPE RATIO	RITONI CUMULATI	RITORNI
	TRAIN	TEST	TRAIN %	CUMULATI TEST %
ETH/BTC	1.479	1.516	46.563	31.091
XRP/BTC	1.140	2.328	53.952	161.220
XRP/EOS	1.725	0.465	53.293	5.189
EOS/XRP	2.404	0.280	86.668	3.090
EOS/BTC	2.382	0.485	234.678	10.571
LTC/EOS	1.591	0.184	47.403	1.581
EOS/LTC	1.141	0.979	25.042	3.238
LTC/ETH	1.382	0.309	31.967	13.333
LTC/BTC	1.759	1.534	73.651	56.123
LTC/XRP	2.547	0.536	69.390	7.514
XRP/LTC	2.347	1.092	60.791	11.395
BCH/BTC	1.741	1.424	56.608	34.890
EOS/BCH	2.198	2.327	74.160	60.333
BCH/EOS	0.438	1.428	7.465	21.264
ETH/BCH	2.620	1.258	68.195	14.155

Fonte: Elaborazione propria

La strategia presenta valori positivi per tutte le coppie di criptovalute considerate. Si registrano valori di rendimento superiore sul training set, dato che i parametri sono stati stimati sul medesimo campione. Inoltre va considerato che non sono compresi i costi di transazione, i quali influiscono in modo decisivo sulla profittabilità della strategia. In letteratura si è stimato che in media su ogni operazione i costi di transazione incidono di circa il 0.2%. Implementando ora la stima di tali costi, otteniamo i rendimenti elencati nella tabella seguente:

Tabella 3.9

COPPIA	SHARPE RATIO TRAIN	SHARPE RATIO TEST	RITONI CUMULATI TRAIN %	RITorni CUMULATI TEST %
ETH/BTC	1.479	1.516	23.789	10.345
XRP/BTC	1.140	2.328	42.620	97.643
XRP/EOS	1.725	0.465	22.273	1.283
EOS/XRP	2.404	0.280	66.648	2.581
EOS/BTC	2.382	0.485	115.563	4.651
LTC/EOS	1.591	0.184	23.312	- 1.200
EOS/LTC	1.141	0.979	15.022	-0.700
LTC/ETH	1.382	0.309	21.967	3.433
LTC/BTC	1.759	1.534	53.051	36.143
LTC/XRP	2.547	0.536	46.590	1.354
XRP/LTC	2.347	1.092	35.561	8.355
BCH/BTC	1.741	1.424	34.519	21.760
EOS/BCH	2.198	2.327	54.153	30.343
BCH/EOS	0.438	1.428	2.565	11.354
ETH/BCH	2.620	1.258	56.185	1.174

Fonte: Elaborazione propria

Se si considerano anche i costi di transazione i rendimenti della strategia diminuiscono in modo sostanzioso, in alcuni casi si toccano addirittura rendimenti negativi. Nonostante ciò si può affermare che la strategia risulta profittevole. La strategia presenta ampi margini di profitto sia nel training set che nel testing set, e anche aggiungendo i costi di transazione, la strategia risulta profittevole. Proviamo ora a migliorare tale strategia utilizzando una diversa procedura per l'individuazione della relazione di cointegrazione.

3.7 Test di Johansen

Si è parlato nel precedente capitolo di un altro test per la verifica di una relazione di cointegrazione, il test di Johansen. Tale modello per la stima dei coefficienti di cointegrazione utilizza la funzione di massima verosimiglianza, portando dunque stime diverse rispetto al test di Engle e Granger. In questo paragrafo analizzeremo proprio i risultati di una strategia di Pair Trading con gli stessi parametri e dati utilizzati nel caso precedente, ma come unica differenza utilizzeremo il test di cointegrazione di Johansen. Avendo già effettuato su tutte e sei le criptovalute il test di radice unitarie ADF e KPSS, dove si è riscontrato che tutte e sei le serie storiche sono processi stocastici integrati di ordine uno; passiamo direttamente al test di cointegrazione. I risultati per le sei coppie di criptovalute sono riportati nella seguente tabella:

Tabella 3.10

COPPIA	P-VALUE	H=
ETH/BTC	0.4638	0
BTC/ETH	0.3188	0
XRP/BTC	0.1673	0
BTC/XRP	0.0402	1
ETH/XRP	0.5991	0
XRP/ETH	0.1225	0
XRP/EOS	0.1299	0
EOS/XRP	0.0540	0
EOS/BTC	0.0528	0
BTC/EOS	0.0182	1
EOS/ETH	0.0098	1
ETH/EOS	0.0094	1
LTC/EOS	0.1822	0
EOS/LTC	0.0716	0
LTC/ETH	0.4821	0

Fonte: Elaborazione propria

Tabella 3.11

COPPIA	P-VALUE	H=
ETH/LTC	0.1154	0
BTC/LTC	0.1453	0
LTC/BTC	0.0406	1
LTC/XRP	0.3367	0
XRP/LTC	0.2073	0
XRP/BCH	0.5723	0
BCH/XRP	0.0890	0
BCH/BTC	0.1028	0
BTC/BCH	0.0258	1
EOS/BCH	0.5367	0
BCH/EOS	0.1228	0
BCH/LTC	0.4969	0
LTC/BCH	0.1475	0
ETH/BCH	0.0027	1
BCH/ETH	0.0047	1

Fonte: Elaborazione propria

In Matlab un valore del parametro “h” uguale a zero indica l’accettazione dell’ipotesi nulla di cointegrazione ; mentre un valore pari a uno indica il rifiuto dell’ipotesi nulla a favore dell’ipotesi alternativa di non cointegrazione. Come è possibile osservare confrontando le due tabelle, il tesi di Johansen risulta meno stringente rispetto il test di Engle e Granger. Sono 22 le coppie di criptovalute che risultano cointegrate con il test di johansen, rispetto alle solo 15 coppie trovate con il test di Engle e Granger. Sia le modalità di calcolo dello Zscore, sia i segnali di entrata e di uscita restano gli stessi utilizzati per la strategia con il test di Engle e Grenger. I ritorni cumulati e il valore dello sharpe ratio con la strategia di Johansen sono riportati nella tabella che segue (in questo caso la stima dei costi di transazione del 0.2% è già stata inclusi nel calcolo):

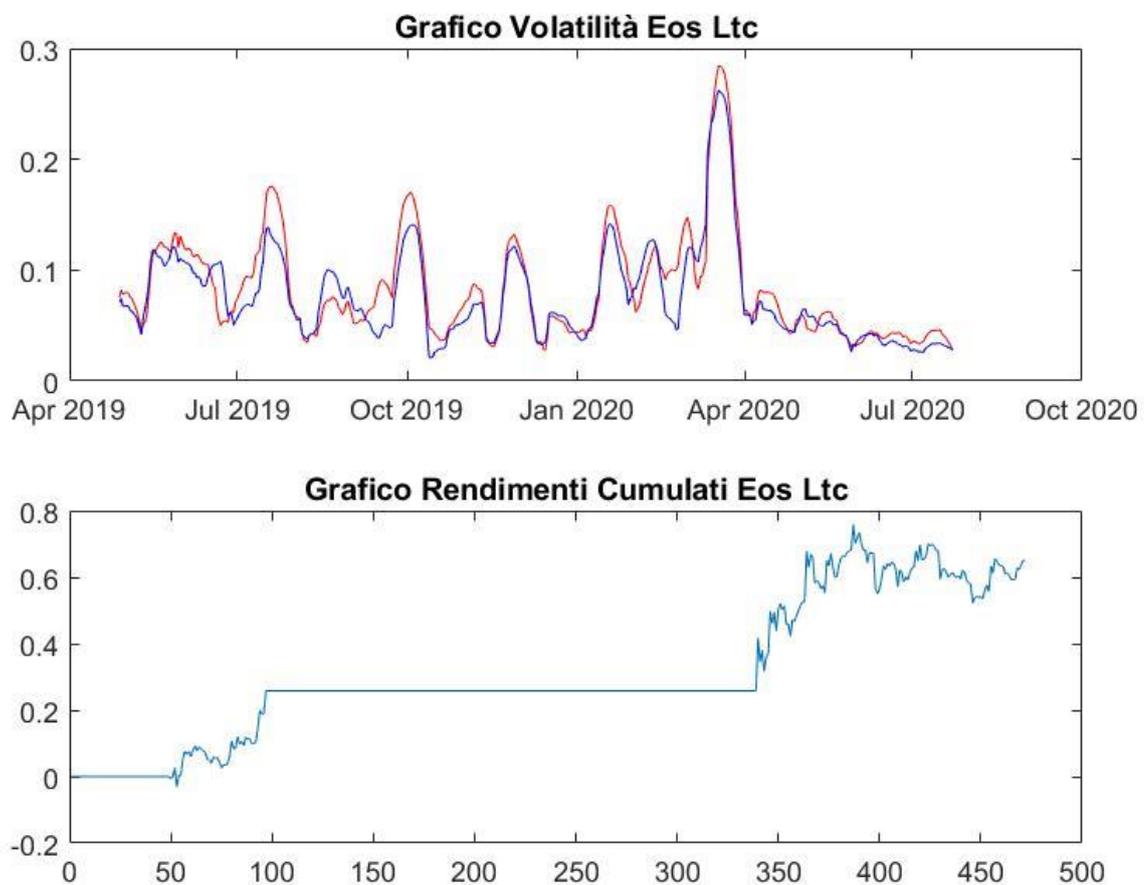
Tabella 3.12

COPPIA	SHARPE RATIO		RITONI CUMULATI	
	TRAIN	TEST	TRAIN %	RITONI CUMULATI TEST %
ETH/BTC	1.516	1.233	6.930	7.420
BTC/ETH	2.0973	1.789	4.450	2.340
XRP/BTC	1.5766	0.637	15.640	5.120
ETH/XRP	1.2130	1.253	7.350	9.690
XRP/ETH	1.3363	0.276	15.040	5.530
XRP/EOS	1.407	0.847	44.82	15.890
EOS/XRP	1.704	1.0715	44.470	46.860
EOS/BTC	1.758	0	8.960	0
LTC/EOS	1.592	0.894	13.370	10.180
EOS/LTC	1.601	1.062	25.830	31.090
LTC/ETH	1.671	0.767	13.050	7.560
ETH/LTC	1.139	1.508	5.050	1.480
BTC/LTC	1.126	1.602	6.070	9.460
LTC/XRP	1.657	0.875	15.060	10.290
XRP/LTC	1.456	0.869	3.642	1.379
XRP/BCH	1.525	0.844	26.280	10.310
BCH/XRP	2.164	1.530	14.410	14.720
BCH/BTC	1.854	0.854	8.650	4.970
EOS/BCH	1.641	1.064	35.566	37.490
BCH/EOS	2.111	1.571	13.440	14.890
BCH/LTC	0.668	1.568	1.150	12.430
LTC/BCH	1.699	0.861	12.820	8.310

Fonte: Elaborazione propria

I rendimenti risultano tutti positivi fatta eccezione per la coppia EOS/BTC. Rispetto ad i rendimenti della strategia con il test di Engle e Granger i rendimenti risultano nettamente inferiori, troviamo però una maggiore aderenza tra i risultati ottenuti nel training set e nel test set. Una maggiore vicinanza tra i rendimenti dei due set, indica una maggiore robustezza della strategia.

Figura 3.4



Fonte: Elaborazione propria

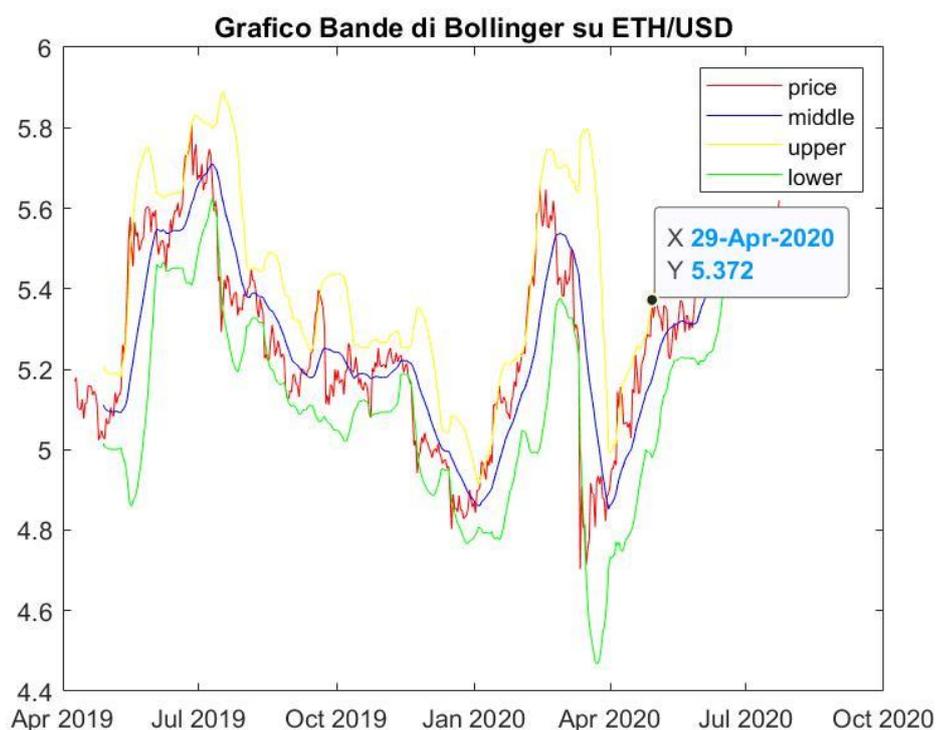
Come è possibile osservare dal grafico i profitti maggiori si sono ottenuti nei periodi successivi ad elevati livelli di volatilità. Infatti nei periodi di elevata volatilità i prezzi delle criptovalute si allontanano dal loro equilibrio di lungo periodo, per poi ristabilirsi solo in un secondo momento.

3.8 Bollinger Band

Sviluppiamo ora una strategia basata su un indicatore tecnico, in modo da poter confrontare i risultati ottenuti per la strategia di Pair Trading. In particolare utilizzeremo come strumento di analisi tecnica le così dette Bande di Bollinger. Le bande di Bollinger prendono il nome dal

loro ideatore John Bollinger, un analista tecnico americano , che le ha formalizzate nel libro del 2002 “Bollinger on Bollinger Bands”. Il lavoro di Bollinger si ispira alla teoria di John Hurst. Le bande di Bollinger appartengono alla categoria di indicatori tecnici di volatilità del mercato. Queste vengono utilizzate per individuare le fasi del titolo di ipercomprato e ipervenduto e per capire il range di oscillazione dei prezzi. Le Bande di Bollinger da un punto di vista grafico si presentano come tra linee tracciate all’interno e intorno alla serie storica dei prezzi , linee che formano delle “Buste di negoziazione – envelopes” , che possono guidare l’investitore nelle sue scelte di investimento.

Figura 3.5



Fonte: Elaborazione propria

Come già accennato le bande di Bollinger consistono di tre linee: una linea centrale (CL), una linea inferiore (LI) e una linea superiore (LS). Da un punto di vista matematico è possibile calcolare questi tre valori:

$$CL_t = \frac{1}{n} \sum_{i=0}^{n-1} P_{t-i}$$

$$LI_t = CL_t + \frac{m}{n} \sqrt{\sum_{i=0}^{n-1} (P_{t-i} - CL_t)^2}$$

$$LS_t = CL_t - \frac{m}{n} \sqrt{\sum_{i=0}^{n-1} (P_{t-i} - CL_t)^2}$$

Dove “n” indica il valore dei periodi e il numero di dati utilizzati per calcolare la deviazione standard. Le due bande , superiore e inferiore, funzionano da supporto e resistenza dinamica . Nel momento in cui il prezzo supera la fascia superiore si aprirà un'operazione di vendita, la quale verrà chiusa solo quando il prezzo sarà più basso o uguale alla fascia inferiore. Nel caso contrario , si apre l'operazione di acquisto quando il prezzo supera la fascia inferiore e si chiude quando è uguale o superiore alla fascia superiore. Nella tabella che segue , sono riportati i rendimenti su ogni singola criptovaluta:

Tabella 3.13

COPPIA	SHARPE RATIO	SHARPE RATIO	RITONI CUMULATI	RITORNI
	TRAIN	TEST	TRAIN %	CUMULATI TEST %
ETH	-0.443	1.360	-6.700	2.290
BTC	-0.7311	-0.0520	-5.420	-0.069
XRP	-0.4282	0.3849	-3.718	6.980
EOS	1.2780	1.039	6.529	5.861
LTC	1.349	0.247	22.250	9.293
BCH	0.4107	0.4613	5.300	6.030

Fonte: Elaborazione propria

Come si evince dalla tabella precedente tale strategia risulta poco profittevole ed è inoltre particolarmente esposta a situazioni di instabilità. Spesso uno dei principali problemi delle bande di Bollinger riguarda le fasi di trend del mercato. In tali fasi del mercato può succedere che i prezzi corrano lungo tutta la banda , così che l'investitore chiuda l'operazione di vendita in modo prematuro e apra troppo presto l'operazione di acquisto.

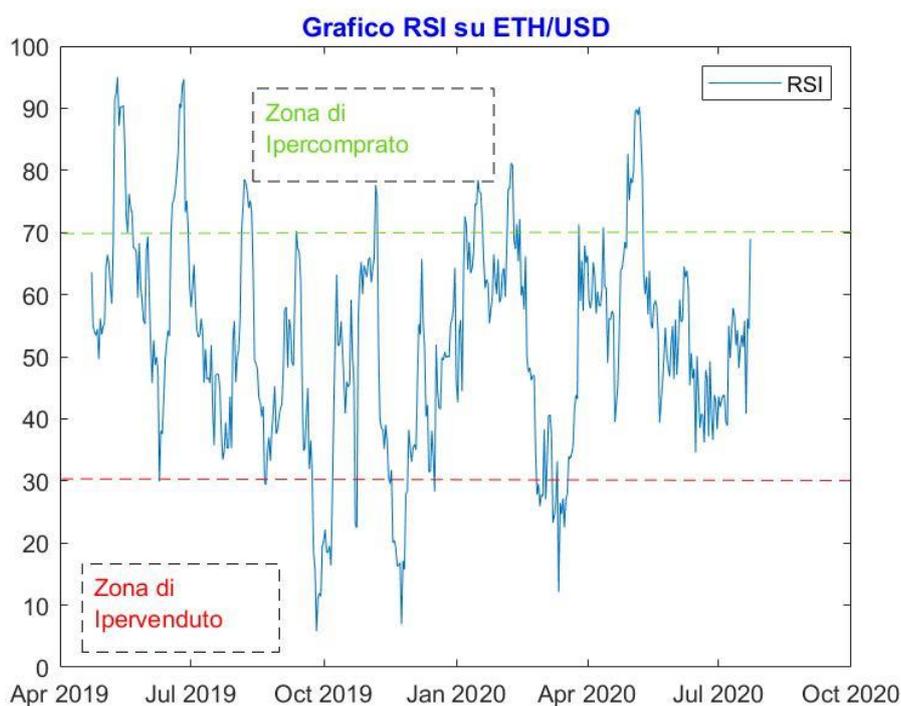
3.9 Relative Strength Index

Un altro indicatore molto utilizzato in Analisi Tecnica è il Relative Strength Index. Si tratta di un indicatore di forza relativa, sviluppato dall'ingegnere meccanico John Welles Wilder e pubblicato nel suo libro " *New Concepts in Technical Trading System*" del 1978. Tale indicatore è utilizzato per identificare la forza interna di un asset finanziario in un intervallo di tempo in modo tale da evidenziare zone di ipercomprato e ipervenduto. Il relative Strength Index è calcolato come:

$$RSI = \left[\frac{100}{1 + RS} \right]$$

dove RS è il rapporto tra la media delle variazioni positive al numeratore, e al denominatore la media delle variazioni negative fatte segnare dal prezzo del titolo nel periodo "n". La scelta del numero di periodi "n" da considerare risulta di fondamentale importanza, dato che all'aumentare del numero di periodi diminuisce il numero di falsi segnali, ma si ha anche una minore reattività. Nel suo libro Wilder consiglia l'utilizzo di un valore di n periodi uguale a 14. Il Relative Strength Index assume valori in un intervallo tra zero e cento; se l'indicatore va al di sopra dei settanta si è in una zona di ipercomprato, mentre al di sotto dei trenta si è in una zona di ipervenduto.

Figura 3.6



Fonte: Elaborazione propria

Tabella 3.14

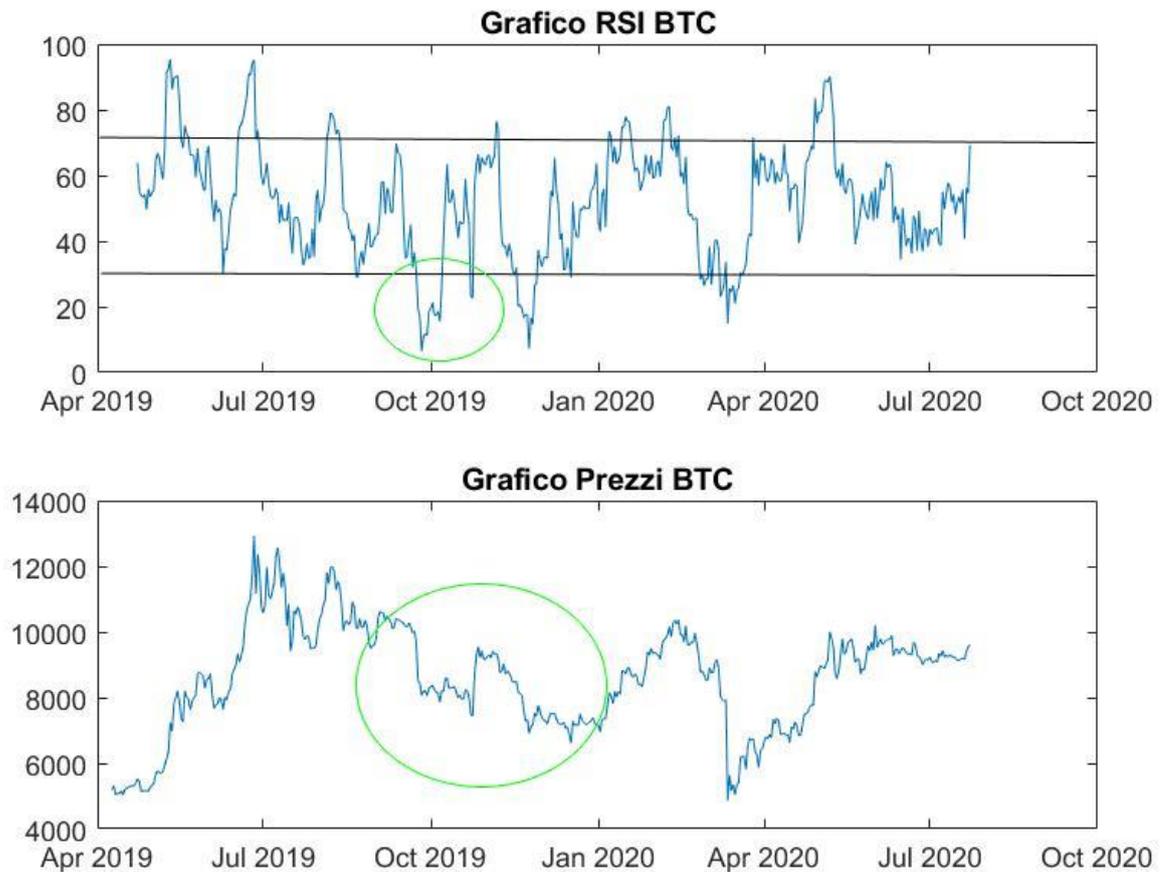
COPPIA	SHARPE RATIO	SHARPE RATIO	RITONI CUMULATI	RITORNI
	TRAIN	TEST	TRAIN %	CUMULATI TEST %
BTC	-0.018	-0.6643	-0.400	-5.240
ETH	-1.077	-0.551	-1.457	-9.740
XRP	0.1704	0.0841	7.457	9.675
EOS	0.5607	1.7852	12.220	179.40
LTC	0.2417	0.6186	-1.049	1.874
BCH	0.9727	0.0780	5.933	-2.332

Fonte: Elaborazione propria

Ogni volta che l'indicatore supera la fascia dei 70 , arrivando così nella zona di ipercomprato, si apre un'operazione di acquisto che verrà chiusa soltanto quando l'indicatore raggiunge la zona di ipervenduto. Al contrario un'operazione di vendita sul titolo si apre nel momento in cui RSI raggiunge un valore inferiore a trenta , ovvero nella fascia di ipervenduto, e si chiude nel momento in cui l'indicatore ritorna nella fascia di ipercomprato. Considerano gli stessi periodi analizzati per le strategie precedenti , la tabella seguente mostra i rendimenti ottenuti da tale strategia sulle sei criptovalute:

I rendimenti risultano bassi o addirittura negativi , tranne nel caso dell'EOS in cui si raggiunge addirittura il 179%.

Figura 3.7



Fonte: Elaborazione propria

Come è possibile osservare dal grafico il problema principale di tale indicatore è costituito dai segnali di falsa entrata ; per tutto il mese di ottobre continua la discesa del prezzo , nonostante l'indicatore segnalasse l'entrata di ipervenduto già dal 24 settembre 2019.

Conclusioni

L'elaborato esamina la possibilità di applicare una strategia di pair trading al mercato delle criptovalute in modo profittevole. Quindi per prima cosa ci siamo soffermati sulla domanda:

“Esistono coppie di criptovalute che risultano cointegrate ?”

Per rispondere a tale domanda sono stati applicati due differenti tipi di test di cointegrazione alle sei criptovalute con maggiore capitalizzazione. Entrambi i metodi hanno riscontrato la presenza di diverse coppie di criptovalute che risultano cointegrate. Nel caso del test a due stadi di Engle e Granger sono state individuate ben 15 coppie; mentre applicando la procedura di Johansen sono state individuate 22 coppie di criptovalute che risultano cointegrate. L'utilizzo degli autovettori, calcolati attraverso la procedura di Johansen, come stima dell'Hedge Ratio della strategia di Pair Trading ha mostrato maggiore stabilità tra i rendimenti ottenuti nel training set e nel test set. Risulta quindi più efficiente una strategia di Pair Trading che applichi la procedura di Johansen per l'identificazione delle coppie cointegrate e per la stima dei coefficienti. La seconda domanda che ci siamo posti è:

“Tra una strategia basata sull'analisi tecnica e una strategia di Pair Trading sulla cointegrazione, quale risulta maggiormente profittevole ?”

Per effettuare un confronto tra analisi tecnica e arbitraggio statistico sono state utilizzate due strategie basate su: Bande di Bollinger e Relative Strength Index. La strategia con le bande di Bollinger su alcune criptovalute ha mostrato rendimenti superiori, mentre su altre perdite consistenti. Un risultato di questo tipo dipende proprio dalla caratteristica intrinseca nel mercato delle criptovalute di elevati livelli di volatilità. Risultati ancor meno soddisfacenti sono stati ottenuti dal RSI. Nella strategia di Pair Trading grazie all'apertura in contemporanea di operazioni di segno opposto è stato possibile eliminare il rischio legato alle scosse dell'intero mercato delle criptovalute. La strategia basata sulle bande di Bollinger risulta maggiormente esposta al rischio di mercato. In conclusione è possibile affermare che le strategie di Pair Trading risultano profittevoli sul mercato delle criptovalute. Ulteriori ricerche sull'argomento dovrebbero esplorare la presenza di coppie cointegrate all'interno dell'intero mercato delle criptovalute, estendendo il set di dati ad intervalli temporali differenti. Inoltre l'utilizzo di algoritmi di neural network potrebbero migliorare i segnali di entrata e di uscita in modo da ottenere maggiori profitti.

Appendice: Codice Matlab

Cointegrazione Engle e Granger

```
%% Caricamento dei prezzi delle Criptovalute e conversione dei dati in logaritmi
data = readtable("C:\Users\zenoc\Desktop\DatiCriptovalute.xlsx");
S=size(data,1);
dates=data(1:S,1);
dates=dates{:,1};
assetNames = data.Properties.VariableNames(2:end);
assetPrice = data(:,assetNames).Variables;
btc_usd1=(assetPrice(1:S,1));
eth_usd1=(assetPrice(1:S,2));
xrp_usd1 = (assetPrice(1:S,3));
bch_usd1= (assetPrice(1:S,4));
ltc_usd1= (assetPrice(1:S,5));
eos_usd1 = (assetPrice(1:S,6));
btc_usd=log(assetPrice(1:S,1));
eth_usd= log(assetPrice(1:S,2));
xrp_usd = log(assetPrice(1:S,3));
bch_usd= log(assetPrice(1:S,4));
ltc_usd= log(assetPrice(1:S,5));
eos_usd = log(assetPrice(1:S,6));

%% Grafico dei logaritmi delle serie storiche
plot(dates,btc_usd,dates,eth_usd,dates,xrp_usd,dates,bch_usd,dates,ltc_usd,dates,eos_usd
)
legend('btc.usd','eth.usd','xrp.usd','bch.usd','ltc.usd','eos.usd')

%% Bisogna dividere i dati in due sottocampioni, un sottocampione servirà per l'analisi di
cointegrazione ed il calcolo degli spread, il secondo campione servirà in fase di backtest
trainset=1:316;
testset=trainset(end)+1:S;
```

%% ACF Funzione di autocorrelazione per una prima idea sulla stazionarietà delle serie storiche

```
acf_btc=autocorr(btc_usd1);
bar(acf_btc)
acf_eth=autocorr(eth_usd1);
bar(acf_eth)
acf_xrp=autocorr(xrp_usd1);
bar(acf_xrp)
acf_bch=autocorr(bch_usd1);
bar(acf_bch)
acf_ltc=autocorr(ltc_usd1);
bar(acf_ltc)
acf_eos=autocorr(eos_usd1);
bar(acf_eos)
acf_btc1=autocorr(diff(btc_usd1));
bar(acf_btc1)
acf_eth1=autocorr(diff(eth_usd1));
bar(acf_eth1)
acf_xrp1=autocorr(diff(xrp_usd1));
bar(acf_xrp1)
acf_bch1=autocorr(diff(bch_usd1));
bar(acf_bch1)
acf_ltc1=autocorr(diff(ltc_usd1));
bar(acf_ltc1)
acf_eos1=autocorr(diff(eos_usd1));
bar(acf_eos1)
```

%% Test Radici Unitarie ADF , KPSS

```
[h1,pVal1] = adftest(btc_usd1(trainset),'model','ARD');
[h1D,pVal1D] = adftest(diff(btc_usd1(trainset)),'model','ARD');

[h2,pVal2] = adftest(eth_usd1(trainset),'model','ARD');
[h2D,pVal2D] = adftest(diff(eth_usd1(trainset)),'model','ARD')
```

```

[h3,pVal3] = adftest(xrp_usd1(trainset),'model','ARD')
[h3D,pVal3D] = adftest(diff(xrp_usd1(trainset)),'model','ARD')

[h4,pVal4] = adftest(bch_usd1(trainset),'model','ARD')
[h4D,pVal4D] = adftest(diff(bch_usd1(trainset)),'model','ARD')

[h5,pVal5] = adftest(ltc_usd1(trainset),'model','ARD')
[h5D,pVal5D] = adftest(diff(ltc_usd1(trainset)),'model','ARD')

[h6,pVal6] = adftest(eos_usd1(trainset),'model','ARD')
[h6D,pVal6D] = adftest(diff(eos_usd1(trainset)),'model','ARD')

[h_kpss,pValue_kpss] = kpsstest(btc_usd1(trainset))
[h_kpssd,pValue_kpssd] = kpsstest(diff(btc_usd1(trainset)))

[h_kpss1,pValue_kpss1] = kpsstest(eth_usd1(trainset))
[h_kpssd1,pValue_kpssd1] = kpsstest(diff(eth_usd1(trainset)))

[h_kpss2,pValue_kpss2] = kpsstest(xrp_usd1(trainset))
[h_kpssd2,pValue_kpssd2] = kpsstest(diff(xrp_usd1(trainset)))

[h_kpss3,pValue_kpss3] = kpsstest(bch_usd1(trainset))
[h_kpssd3,pValue_kpssd3] = kpsstest(diff(bch_usd1(trainset)))

[h_kpss4,pValue_kpss4] = kpsstest(ltc_usd1(trainset))
[h_kpssd4,pValue_kpssd4] = kpsstest(diff(ltc_usd1(trainset)))

[h_kpss5,pValue_kpss5] = kpsstest(eos_usd1(trainset))
[h_kpssd5,pValue_kpssd5] = kpsstest(diff(eos_usd1(trainset)))
ADF.h=[h1 h2 h3 h4 h5 h6 ]
ADF.p=[ pVal1 pVal2 pVal3 pVal4 pVal5 pVal6];

```

```
ADF.hd=[ h1D h2D h3D h4D h5D h6D ]
```

```
ADF.pd=[ pVal1D pVal2D pVal3D pVal4D pVal5D pVal6D ]
```

```
KPSS.h=[ h_kpss h_kpss1 h_kpss2 h_kpss3 h_kpss4 h_kpss5]
```

```
KPSS.p=[ pValue_kpss pValue_kpss1 pValue_kpss2 pValue_kpss3 pValue_kpss4  
pValue_kpss5 ]
```

```
KPSS.hd=[ h_kpssd h_kpssd1 h_kpssd2 h_kpssd3 h_kpssd4 h_kpssd5 ]
```

```
KPSS.pd=[ pValue_kpssd pValue_kpssd1 pValue_kpssd2 pValue_kpssd3 pValue_kpssd4  
pValue_kpssd5]
```

```
%% Engle e Grenger primo step regressione
```

```
%Bitcoin/Etherum
```

```
Y=eth_usd1
```

```
X=ltc_usd1
```

```
Y_train=Y(trainset);
```

```
T=size(Y_train,1);
```

```
X0_train=ones(T,1);
```

```
X1_train=X(trainset);
```

```
X_train=[X0_train,X1_train];
```

```
[beta,sigma,E]=mvregress(X_train,Y_train);
```

```
hedgeRatio=beta(2)
```

```
errors=[E]
```

```
mdl=fitlm(X1_train,Y_train)
```

```
%% Engle e Grenger secondo step test adf dei residui
```

```
[h1a,pVal1a] = adftest(errors,'model','AR')
```

```
%% Calcolo dello Z-score
```

```
spread=Y-hedgeRatio*X;
```

```

spreadMean=mean(spread(trainset));
spreadStd=std(spread(trainset));
zScore=(spread-spreadMean)./spreadStd;

%% Regole di apertura, chiusura operazioni
entryZscore=1;
exitZscore=0;

longsEntry=zScore < -entryZscore;
longsExit=zScore > exitZscore;

shortsEntry=zScore > entryZscore;
shortsExit=zScore < -exitZscore;

numUnitsLong=NaN(length(spread), 1);
numUnitsShort=NaN(length(spread), 1);
numUnitsLong(1)=0;
numUnitsLong(longsEntry)=1;
numUnitsLong(longsExit)=0;
numUnitsLong=fillMissingData(numUnitsLong);

numUnitsShort(1)=0;
numUnitsShort(shortsEntry)=-1;
numUnitsShort(shortsExit)=0;
numUnitsShort=fillMissingData(numUnitsShort);
numUnits=numUnitsLong+numUnitsShort;
cl=[X Y];
positions= repmat(numUnits, [1 size(cl, 2)]).*[-hedgeRatio ...
ones(size(hedgeRatio))].*cl;
pnl=sum(lag(positions).*(cl-lag(cl))./lag(cl), 2);
ret=(pnl./sum(abs(lag(positions)), 2));
ret(isnan(ret))=0;

```

```
CumRet_trainset=cumprod(1+ret(trainset))-1;
CumRet_trainset=CumRet_trainset(end);
CumRet_testset=cumprod(1+ret(testset))-1;
CumRet_testset=CumRet_testset(end);

%Sharpe ratio
Sh_train=sqrt(size(trainset,2))*mean(ret(trainset))/std(ret(trainset));
Sh_test=sqrt(size(testset,2))*mean(ret(testset))/std(ret(testset));

Risultati= [ Sh_train Sh_test CumRet_trainset CumRet_testset]
```

Cointegrazione Procedura di Johansen

```
% Caricamento dati resta lo stesso del test Engle e Granger
% Test ADF uguale ..... così come la divisione del campione
%% johansen test
X=eos_usd
Y=btc_usd
y2=[X(trainset), Y(trainset)];
[h,pValue,stat,cValue,mles] = jcitest(y2)
coefficienti=mles.r0(1).eigVec
hedgeRatio=coefficienti(2,1)

%% Calcolo dello Z-score
spread=Y-hedgeRatio*X;
spreadMean=mean(spread(trainset));
spreadStd=std(spread(trainset));
zScore=(spread-spreadMean)./spreadStd;

% Caricamento dati resta lo stesso del test Engle e Granger
% Test ADF uguale ..... così come la divisione del campione
% Anche i segnali di entrata e uscita restano gli stessi della strategia precedente
```

Bande di Bollinger

%% Caricamento dei prezzi delle Criptovalute e conversione dei dati in logartmi

```
data = readtable("C:\Users\zenoc\Desktop\DatiCriptovalute .xlsx");
```

```
S=size(data,1);
```

```
dates=data(1:S,1);
```

```
dates=dates{:,1};
```

```
assetNames = data.Properties.VariableNames(2:end);
```

```
assetPrice = data(:,assetNames).Variables;
```

```
btc_usd1=(assetPrice(1:S,1));
```

```
eth_usd1=(assetPrice(1:S,2));
```

```
xrp_usd1 = (assetPrice(1:S,3));
```

```
bch_usd1= (assetPrice(1:S,4));
```

```
ltc_usd1= (assetPrice(1:S,5));
```

```
eos_usd1 = (assetPrice(1:S,6));
```

```
btc_usd=log(assetPrice(1:S,1));
```

```
eth_usd= log(assetPrice(1:S,2));
```

```
xrp_usd = log(assetPrice(1:S,3));
```

```
bch_usd= log(assetPrice(1:S,4));
```

```
ltc_usd= log(assetPrice(1:S,5));
```

```
eos_usd = log(assetPrice(1:S,6));
```

%% Bisogna dividere i dati in due sottocampioni, un sottocampione servirà per l'analisi di cointegrazione ed il calcolo degli spreadn, il second campione servirà in fase di backtest

```
trainset=1:316;
```

```
testset=trainset(end)+1:S;
```

Bande di Bollinger

```
X=bch_usd
```

```
[middle,upper,lower] = bollinger(X)
```

```
entryZscore=upper;
```

```
exitZscore=lower;
```

```
entryZscore1=lower;
```

```
exitZscore1=upper;
```

```

longsEntry=X < entryZscore1;
longsExit=X > exitZscore1;

shortsEntry=X > entryZscore;
shortsExit=X < exitZscore;

numUnitsLong=NaN(length(X), 1);
numUnitsShort=NaN(length(X), 1);
numUnitsLong(1)=0;
numUnitsLong(longsEntry)=1;
numUnitsLong(longsExit)=0;
numUnitsLong=fillMissingData(numUnitsLong);

numUnitsShort(1)=0;
numUnitsShort(shortsEntry)=-1;
numUnitsShort(shortsExit)=0;
numUnitsShort=fillMissingData(numUnitsShort);

numUnits=numUnitsLong+numUnitsShort;
cl=[X];
positions= repmat(numUnits, [1 size(cl, 1)]).*[ ...
ones(size(X))].*cl;
pnl=sum(lag(positions).*(cl-lag(cl))./lag(cl), 2);
ret=(pnl./sum(abs(lag(positions)), 2));
ret(isnan(ret))=0;

CumRet_trainset=cumprod(1+ret(trainset))-1;
CumRet_trainset=CumRet_trainset(end);
CumRet_testset=cumprod(1+ret(testset))-1;
CumRet_testset=CumRet_testset(end);

plot(cumprod(1+ret)-1); %

```

```
%Sharpe ratio
Sh_train=sqrt(size(trainset,2))*mean(ret(trainset))/std(ret(trainset));
Sh_test=sqrt(size(testset,2))*mean(ret(testset))/std(ret(testset));

Risultati= [ Sh_train Sh_test CumRet_trainset CumRet_testset]

plot(dates,X,'r',dates,middle,'b',dates,upper,'y',dates,lower,'g')
title('Grafico Bande di Bollinger su ETH/USD')
legend('price','middle','upper','lower')
```

Strategia con RSI

```
%% Caricamento dei prezzi delle Criptovalute e conversione dei dati in logartmi
data = readtable("C:\Users\zenoc\Desktop\DatiCriptovalute .xlsx");
S=size(data,1);
dates=data(1:S,1);
dates=dates{:,1};
assetNames = data.Properties.VariableNames(2:end);
assetPrice = data(:,assetNames).Variables;
btc_usd1=(assetPrice(1:S,1));
eth_usd1=(assetPrice(1:S,2));
xrp_usd1 = (assetPrice(1:S,3));
bch_usd1= (assetPrice(1:S,4));
ltc_usd1= (assetPrice(1:S,5));
eos_usd1 = (assetPrice(1:S,6));
btc_usd=log(assetPrice(1:S,1));
eth_usd= log(assetPrice(1:S,2));
xrp_usd = log(assetPrice(1:S,3));
bch_usd= log(assetPrice(1:S,4));
ltc_usd= log(assetPrice(1:S,5));
eos_usd = log(assetPrice(1:S,6));
%% Bisogna dividere i dati in due sottocampioni, un sottocampione servirà per l'analisi di
cointegrazione ed il calcolo degli spreadn, il second campione servirà in fase di backtest
trainset=1:316;
testset=trainset(end)+1:S;
%% johansen test
X=btc_usd1
index = rsindex(X)

Ipervenduto=20;
Ipercomprato=70;
```

```

longsEntry=index < lpervenduto;
longsExit=index > lpercomprato;

shortsEntry=index > lpercomprato;
shortsExit=index < lpervenduto;

numUnitsLong=NaN(length(X), 1);
numUnitsShort=NaN(length(X), 1);
numUnitsLong(1)=0;
numUnitsLong(longsEntry)=1;
numUnitsLong(longsExit)=0;
numUnitsLong=fillMissingData(numUnitsLong);

numUnitsShort(1)=0;
numUnitsShort(shortsEntry)=-1;
numUnitsShort(shortsExit)=0;
numUnitsShort=fillMissingData(numUnitsShort);

numUnits=numUnitsLong+numUnitsShort;
cl=[X];
positions= repmat(numUnits, [1 size(cl, 1)]).*[ ...
ones(size(X))].*cl;
pnl=sum(lag(positions).*(cl-lag(cl))./lag(cl), 2);
ret=(pnl./sum(abs(lag(positions)), 2));
ret(isnan(ret))=0;

CumRet_trainset=cumprod(1+ret(trainset))-1;
CumRet_trainset=CumRet_trainset(end);
CumRet_testset=cumprod(1+ret(testset))-1;
CumRet_testset=CumRet_testset(end);

```

```
plot(cumprod(1+ret)-1)
%Sharpe ratio
Sh_train=sqrt(size(trainset,2))*mean(ret(trainset))/std(ret(trainset));
Sh_test=sqrt(size(testset,2))*mean(ret(testset))/std(ret(testset));

Risultati= [ Sh_train Sh_test CumRet_trainset CumRet_testset]
subplot(2,1,1),plot(dates,index)
title('Grafico RSI BTC')
subplot(2,1,2), plot(dates,X)
title ('Grafico Prezzi BTC')
```

Bibliografia

Amato M. , Fantacci L. ; (2016) ; Per un pugno di Bitcoin: rischi e opportunità delle monete virtuali ; Università Bocconi Editore ; Prima edizione

Ammous S. ; (2016) ; Can cryptocurrencies fulfil the functions of money ? ; Center on Capitalism and Society ; Working Paper No. 92

Baur, D., Dimpfl, T. ; (2018) ; Excess Volatility as an Impediment for a Digital Currency ; University of Western Australia

Baur, D., Lee, A., Hong, K. ; (2015) Bitcoin: Currency or Investment? ; SWIFT Institute

Bollinger , J.. Using Bollinger Bands. *Stock & Commodities*(10:2), 47-51

Borri, N. (2018). Conditional Tail-Risk in Cryptocurrency Markets. *Journal of Empirical Finance*, 50:1-19.

Borri, N. and Shakhnov, K. (2018). Cryptomarket Discounts. *SSRN Electronic Journal*.

Bouoiyour, J., Selmi, R. (2017). Are Trump and Bitcoin Good Partners ; University of Tunis; University of Pau

Brock, W., Lakonishok , J., & LeBaro, B. (1992). Simple Technical Trading Rules and the Stochastic Properties of Stock Returns. *The Journal of Finance*, 47(5), 1731 - 1764.

Caparrelli F. ; (2004) ; Economia del mercato mobiliare ; McGraw-Hill ; pag. 201- 256

Capoti D. , Colacchi E. , Maggioni M. ; (2015) ; Bitcoin revolution: la moneta digitale alla conquista del mondo ; Hoelpy ; pag. 3-72

Chan, E. (2009). *Quantitative Trading: How to Build Your Own Algorithmic Trading Business*. John Wiley & Sons.

Chan, E. (2013). *Algorithmic Trading: Winning Strategies and Their Rationale*. John Wiley & Sons.

Chan, S., Chu, J., Nadarajah, S., Osterrieder, J. (2017). A Statistical Analysis of Cryptocurrencies.

Ciaian P., Rajcaniova M., Kancs. D. ; (2015); The Digital Agenda of Virtual Currencies, Can BitCoin Become a Global currency? ; JRC technical report ; Report EUR 27397 EN

D. Edwards e J. Magee, Technical Analysis of Stock Trends, U.S.A., CRC Press (11 edition) (1958)

De Cillibus M. F. , Mauro R. ; (2016) ; Hacking finance: la rivoluzione del Bitcoin e della Blockchain; Agenzia X ; pag. 37-81

Dyhrberg, A. ; (2015) ; Hedging Capabilities of bitcoin. Is it the Virtual Gold? ; University College Dublin, School of Economics; WP2015/21

Eisl, A., Gasser, S., Weinmayer, K. ; (2015) ; Caveat emptor: Does Bitcoin improve portfolio diversification? ; Vienna University of Economics and Business

Evans D. S. ; (2014) ; Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms ; Coase-Sandor institute for law and economics ; working paper no. 685 (2D SERIES)

Gatev, E., Goetzmann, W. N., and Rouwenhorst, K. (1999). Pairs trading: Performance of a relative value arbitrage rule. Working paper, Yale School of Management's International Center for Finance.

Gatev, E., Goetzmann, W. N., and Rouwenhorst, K. (2006). Pairs trading: Performance of a relative value arbitrage rule. Review of Financial Studies, 19(3):797{827.

Grise, C., Nitschka, T. ; (2013); On financial risk and the safe haven characteristics of Swiss franc exchange rates ; Swiss National Bank Working Papers

Hamilton, J. D. (1994). Time Series Analysis. Princeton university press.

Johansen, S. (1988). Statistical analysis of cointegration vectors. Journal of Economic Dynamics and Control, 12(2-3):231{254.

Journal of Risk and Financial Management, 10(2):1-23.

Krauss, C. (2015). Statistical arbitrage pairs trading strategies: Review and outlook. Journal of Economic Surveys, 31(2).

Molnár, P., Vagstad, K., Valstad, O. ; (2015); A bit risky? A comparison between Bitcoin and other assets using an intraday value at risk approach

Nakamoto S. (2008); Bitcoin: A Peer-to-Peer Electronic Cash System

Ozturk E. O. , Sheng S.X. ; (2017) ; Measuring Global and Country-Specific Uncertainty ; IMF ; WP/17/219

Panfili F. , Daini F. , Potente F. , Reale G.; (2015) ; L'oro come "safe haven asset"? Evidenze empiriche basate su un confronto fra diverse attività finanziarie ; Questioni di economia e finanza ; N. 277

Pieters G. C. ; (2016) ; Does Bitcoin Reveal New Information About Exchange Rates and Financial Integration? ; Federal Reserve Bank of Dallas Globalization and Monetary Policy Institute Working Paper No. 292

Sauer B. ; (2015) ; Central Bank Behaviour Concerning the Level of Bitcoin Regulation as a Policy Variable; Athens Journal of Business and Economics ; Vol. 1, No. 4

Stock, J.H. and M.W. Watson, 2015, Introduction to Econometrics, Pearson

Vidyamurthy, G. (2004). Pairs trading: Quantitative methods and analysis. John Wiley & Sons and N.J. Hoboken.

W. Schabacker, Technical Analysis and Stock Market Profits, U.S.A., Harriman House (1932)

Yermack, D. ; (2013) ; Is Bitcoin a real currency? An economic appraisal ; NBER Working Paper No. w19747



Dipartimento di Economia e Finanza
Cattedra di Econometria per la Finanza

PAIR TRADING:
**“UNA STRATEGIA DI ARBITRAGGIO STATISTICO SUL
MERCATO DELLE CRIPTOVALUTE ”**

RELATORE
Prof. Stefano Grassi

CORELATORE
Prof. Paolo Santucci De Magistris

CANDIDATO
Carmine Zeno
Matr. 704481

ANNO ACCADEMICO 2019/2020

Introduzione

Lo scopo dell'elaborato è analizzare la possibilità di applicare in modo profittevole strategie di Pair Trading al mercato delle Criptovalute.

Nel primo capitolo il mercato delle criptovalute è analizzato da un punto di vista storico, tecnologico e statistico. Si approfondisce il funzionamento della Blockchain e ogni aspetto delle transazioni in bitcoin.

Nel secondo capitolo si passa invece alle varie metodologie analizzate nella letteratura finanziaria , in particolare nei lavori di Gatev et al. e Vidamurthy. Si analizza il metodo della distanza e i diversi test di cointegrazione.

Nel parte finale dell'elaborato di analizzano due strategie di Pair Trading , entrambe basate sull'analisi della cointegrazione , ma svolta attraverso due differenti test: Engle e Granger e Johansen. Inoltre si analizzano due strategie di analisi tecnica , Bande di Bollinger e Relative Strenght Index, in modo da poter effettuare un confronto tra strategie di Analisi Tecnica e strategie di Arbitraggio statistico.

Il Mercato Delle Criptovalute

Il XX secolo ha conosciuto una rivoluzione tecnologica, che ha cambiato in modo radicale il mondo intero. Negli ultimi anni, si è poi assistito ad uno sviluppo in continua crescita delle tecnologie crittografiche. Proprio le innovazioni in ambito crittografico, hanno reso possibile la creazione di nuovi strumenti di pagamento. L'innovazione più importante e rivoluzionaria, è di sicuro rappresentata dalle criptovalute. La prima criptovaluta "*il Bitcoin*" fu presentata per la prima volta nel novembre del 2008 da un autore o autori anonimi, sotto lo pseudonimo giapponese "Satoshi Nakamoto". Il 9 gennaio 2009 venne rilasciata la prima versione del software Bitcoin. Di norma, con il termine "Bitcoin" si indica la tecnologia e la rete alla base di questo sistema di pagamento, mentre, nella denominazione "*bitcoin*" si fa riferimento alla valuta utilizzata per gli scambi. Ciò che rende innovativo il bitcoin rispetto ai sistemi di pagamento di tipo tradizionale è la sua decentralizzazione. Il Bitcoin utilizza la tecnologia blockchain per tenere traccia delle transazioni, la crittografia per la gestione degli aspetti funzionali e il meccanismo di mining per la generazione di nuova moneta e la verifica delle transazioni. Nel sistema Bitcoin non è presente alcuna unità organizzativa, che controlli e gestisca l'emissione di nuova moneta, ma soprattutto non necessita di affidarsi ad alcuna istituzione finanziaria che ne funga da garante. Il bitcoin utilizza una rete peer-to-peer (P2P), ovvero una rete senza alcuna struttura gerarchica, tipica dei sistemi client/server, e nella quale ciascun nodo (detto server) può operare come client o come server a seconda delle circostanze. Un nodo può essere rappresentato da un computer, da uno smartphone o da un qualsiasi altro dispositivo elettronico in grado di far funzionare il software. Per le monete digitali uno dei maggiori rischi è rappresentato dalla cosiddetta double spending, ovvero dalla possibilità che il denaro (essendo non fisico ma "virtuale") venga speso più di una volta. Per questo motivo ogni transazione va verificata e convalidata prima di essere conclusa. L'analisi delle transazioni viene affidata agli stessi utilizzatori della rete, che mettono a disposizione del network la potenza computazionale dei loro computer, in modo che possano essere convalidati i pagamenti. Gli user della rete che raccolgono le transazioni e le organizzano in blocchi, prendono il nome di "*miner*". Ogni volta che un miner convalida un blocco lo trasmette alla rete in modo che si possa aggiungere alla Blockchain. Quest'ultima, altro non è, che un registro unico e condiviso delle transazioni in modo che nella rete si possa garantire trasparenza, sicurezza e la non falsificabilità dei pagamenti. Qualsiasi minatore per la risoluzione di un nuovo blocco viene ricompensato in bitcoin di nuova emissione, ed è il protocollo stesso a stabilire le ricompense. Attualmente, le ricompense sono di 6.25 bitcoin per blocco, da dividere tra tutti

i partecipanti alla risoluzione del singolo blocco. L'emissione di ricompense è pianificata per dimezzarsi ogni quattro anni, fino ad arrivare ad un totale di bitcoin in circolazione di 21 milioni. Il meccanismo di ricompense è anche l'unico modo in cui nuova moneta viene immessa nel mercato. Allo scopo di garantire l'effettiva convalidazione dei blocchi, il sistema utilizza un protocollo crittografico noto come proof-of-work. Questo sistema costringe i miner a risolvere un complesso problema matematico, per dimostrare che la giusta potenza computazionale è stata spesa per la convalida del blocco. La proof-of-work rende la convalida dei blocchi come una lotteria, in cui le possibilità di vincita aumentano all'aumentare della potenza computazionale impiegata.

Dopo il successo del progetto Bitcoin si è assistito alla proliferazione di numerose nuove criptovalute anche chiamate "alt-coin" (alternative coins), realizzate per i più svariati fini e operative in sempre più eterogenei settori. Elenchiamo ora di seguito le cinque criptomonete (sei considerando Bitcoin, ampiamente trattato) scelta per la nostra analisi in base al livello di capitalizzazione e alla disponibilità dei dati.

- **Ethereum**: Ethereum nasce nel 2013 per opera di Vitalik Buterin, uno sviluppatore di origini russe, cresciuto in Canada, che univa la competenza di programmatore a quelle di ricercatore nell'ambito delle cryptocurrency. Ethereum è diventato pubblico e accessibile online solo nel 2015. Oltre ad essere un sistema di pagamento Ethereum permette di eseguire i cosiddetti smart contract. Gli smart contract sono protocolli informatici che permettono di verificare e far rispettare l'esecuzione di un contratto.
- **Bitcoin Cash**: Il Bitcoin Cash apparso il primo di agosto 2017, e deve quasi tutto il suo codice al progetto originario del Bitcoin. Si tratta infatti di un hard fork del Bitcoin. Gli hard fork in informatica avvengono quando il team di sviluppo di un software, essendo in disaccordo con il resto del gruppo, decide di creare in modo indipendente una nuova versione del codice. Si crea quindi un software derivato con specifiche proprietà distinte e separate. Lo scopo principale degli autori di bitcoin cash era quello di creare una moneta virtuale, che permettesse di velocizzare i tempi di validazione dei blocchi.
- **Litecoin**: distribuito il 7 ottobre 2011 da Charles Lee, un ex-dipendente di Google. Le caratteristiche principali del Litecoin sono molto simili a quelle del protocollo Bitcoin. L'obiettivo principale di Litecoin è la diminuzione dei tempi di conferma delle transazioni, la difficoltà di mining è stata infatti abbassata in modo da rendere possibile la creazione di un nuovo blocco circa ogni due minuti. Inoltre il tetto massimo di monete generabili è più alto rispetto al Bitcoin, con una soglia di 84 milioni.

- **Ripple (XRP)**: ideata da Chris Larsen e Jed McCaleb, fondatori di OpenCoin (ora rinominata Ripple Labs), una start-up di San Francisco. Il simbolo della criptovaluta è XRP, Ripple è il nome della piattaforma che ospita la valuta . Il Ripple non può essere creato attraverso mining , secondo le regole stabilite dal protocollo, di XRP dovranno essercene in circolazione 100 miliardi. L'intera scorta è stata emessa nel 2012, ma oltre la metà è ancora nelle mani di OpenCoin, che intende rilasciarla sul mercato in modo graduale. Non prevedendo il processo di mining dispendioso dal punto di vista energetico, XRP rappresenta la versione ecologica del bitcoin.
- **EOS**: ideata dal noto ingegnere Dan Larimer a metà del 2017. Inizialmente tale sistema nasce con lo scopo di fornire servizi personalizzabili di autenticazione, di cloud storage e di server hosting. Per prima cosa bisogna specificare che EOS è il nome della criptovalute, mentre il software open source su cui gira la criptovalute prende il nome di Eos.io. Tra i punti di forza di tale criptovaluta, gli sviluppatori elogiano la sua scalabilità, flessibilità e usabilità.

Pair Trading

La prima forma di Pair Trading come strategia di investimento è attribuita all'investitore e trader americano Jesse Livermore. Egli intorno al 1920 concepì una strategia di investimento che prese il nome di "sister stock". La strategia consisteva nell'identificazione di coppie di titoli i cui prezzi tendevano a muoversi insieme. Ogni volta che si presentavano anomalie nel rapporto tra le coppie di titoli, i due titoli venivano scambiati contemporaneamente, con l'idea che l'anomalia si sarebbe corretta nel futuro. La strategia di Livermore è probabilmente uno dei primi esperimenti per le strategie di Pair Trading, la cui teorizzazione è avvenuta solo una decade dopo. Tale teorizzazione è attribuita al quant di Wall Street Nunzio Tartaglia, Trader alla Morgan Stanley a metà degli anni '80. Da allora le strategie di Pair Trading hanno assunto sempre maggior rilievo all'interno di hedge fund e presso investitori istituzionali. L'idea alla base delle strategie di Pair Trading è quella di vendere i titoli sopravvalutati e acquistare i titoli sottovalutati. Per individuare una sopravvalutazione o una sottovalutazione, occorre conoscere il valore dei titoli in termini assoluti. Spesso risulta però difficile l'individuazione di tale valore. Le strategie di Pair Trading tentano di risolvere tale problema, utilizzando il concetto di valore relativo. L'idea alla base è che se due titoli presentano caratteristiche simili, devono avere un prezzo che è più o meno lo stesso. In questa strategia il prezzo di uno specifico titolo non è importante, perché può essere sbagliato, ciò che importa è che i due prezzi siano simili. Se i prezzi si discostano, significa che uno dei due titoli è sopravvalutato o sottovalutato, o magari questa differenza è data dalla combinazione di entrambi gli elementi. Le strategie di Pair Trading da un punto di vista operativo prevedono l'acquisto del titolo con il prezzo più basso e la vendita del titolo con il prezzo più alto, con l'idea che la discrepanza tra i due prezzi si corregga da sola nel futuro. Di fondamentale importanza nelle strategie di Pair Trading è l'identificazione dei titoli che presentano un equilibrio di lungo periodo, e l'individuazione del temporaneo disallineamento dall'equilibrio di lungo periodo. Per la selezione dei titoli è possibile dividere le strategie in due grandi macro aree: analisi fondamentale e analisi econometrica. La pair selection basata su modelli statistico-econometrici ha lo scopo di individuare la distanza media dei prezzi delle coppie di titoli e come questi si muovono nel tempo. Mentre l'analisi dei fondamentali teoricamente permette di selezionare trasversalmente le coppie tra società che hanno un core business simile, con un metodo statistico vi sono regole per la selezione più stringenti. Tra le strategie basate su modelli econometrici quelle più note sono: distance method e il cointegration approach.

Analisi Empirica

Lo scopo della ricerca è capire se è possibile applicare in modo profittevole una strategia di Pair Trading al mercato delle criptovalute. Ciò che spinge ad analizzare proprio il mercato delle criptovalute per testare la profittabilità di una strategia di Pair Trading è:

- la presenza di elevati livelli di volatilità
- la presenza di elevati livelli di correlazione tra le diverse criptovalute

Per l'analisi si utilizzeranno le serie storiche di sei criptovalute scelte tra quelle con maggior capitalizzazione e in base alla disponibilità dei dati. Le sei criptovalute sono: Bitcoin, Ethereum, XRP, Bitcoin Cash, Litecoin e Eos. I dati storici delle sei criptovalute sono stati raccolti tramite estensione Api per Excel dal sito CoinMarket per il periodo 9 aprile 2019 – 23 Luglio 2020. I prezzi di tutte le criptovalute sono espressi in dollari e rappresentano in valore di chiusura giornaliera.

E' necessario suddividere la serie storica in due diversi set per le diverse due fasi del processo di analisi. Il primo set, definito training set, utilizzato uno per la stima delle diverse tipologie di modelli . Il secondo set, detto testing set, di cui fanno parte i restanti dati viene utilizzato per la valutazione delle prestazioni della strategia di Pair Trading. Si è diviso il campione in tal modo :

- 1) 316 osservazioni nel Training set
- 2) 157 osservazioni nel Testing set

Alla fine della costruzione della strategia le performance dei due set vengono confrontati, in modo che l'algoritmo non degradi le proprie performance nell'immediato futuro rispetto le performance ottenute sul Training set utilizzato per la stima dei parametri.

Passiamo ora all' analisi di due test statistici per l'individuazione di radici unitarie: ADF e KPSS. I due test sono stati applicati ai prezzi assoluti del training set delle sei criptovalute. La versione di Matlab del test ADF restituisce un valore che ci dà l'esito di decisione di rigetto dell'ipotesi nulla e il p-value associato. Se il test dà esito $h=1$ si sta indicando il rigetto dell'ipotesi di presenza di radici unitarie in favore dell'ipotesi alternativa di stazionarietà . La situazione opposta si presenta per il test KPSS ; un esito di $h=1$ indica il rifiuto dell'ipotesi di stazionarietà , mentre un esito $h=0$ indica l'accettazione dell'ipotesi nulla di serie storiche stazionarie. L'ipotesi nulla in entrambi i test viene rigettata ad un livello di confidenza del 95%,

ovvero quando il p-value è più piccolo del livello di significatività $\alpha = 0.05$. I risultati dei test sono presentati nelle tabelle seguenti:

	BTC	ETH	XRP	BCH	LTC	EOS
ADF	0.116	0.345	0.461	0.297	0.615	0.435
KPSS	0.001	0.001	0.001	0.001	0.001	0.001

	Δ BTC	Δ ETH	Δ XRP	Δ BCH	Δ LTC	Δ EOS
ADF	0.010	0.010	0.010	0.010	0.010	0.010
KPSS	0.100	0.100	0.100	0.100	0.100	0.100

I risultati del test ADF mostrano che l'ipotesi nulla di presenza di radici unitarie nelle serie storiche dei prezzi è accettata. Invece i risultati del test ADF applicato alle differenze prime dei prezzi, mostrano l'accettazione della tesi di stazionarietà. Il test KPSS conferma l'ipotesi che i prezzi delle serie storiche non sono stazionarie, mentre lo sono le differenze prime. Possiamo quindi affermare che le serie storiche dei prezzi delle sei criptovalute sono processi storici integrati di ordine uno, $I(1)$.

Ora che si è verificato che le serie storiche che stiamo analizzando sono processi stocastici integrati di ordine uno, possiamo passare al test di cointegrazione, per individuare le coppie di criptovalute da usare nella strategia di Pair Trading. Per testare l'ipotesi di cointegrazione utilizzeremo il test a due stadi di Engle e Granger. Il primo stadio del test consiste nella stima dei parametri della coppia di criptovalute tramite regressione lineare. Come metodo risolutivo per la regressione lineare è stato utilizzato il metodo degli OLS (metodo dei minimi quadrati). Date le serie storiche di due criptovalute X_t, Y_t il metodo dei minimi quadrati permette di stimare i parametri $\beta = [\beta_0; \beta_1]$ della relazione:

$$Y_t = \beta_0 + \beta_1 X_t + \epsilon_t$$

, $[\beta_0; \beta_1]$ rappresentano rispettivamente l'intercetta e il coefficiente di relazione. Il parametro β_1 rappresenta anche il cosiddetto, Hedge Ratio, ovvero il coefficiente che misura il grado di ritorno alla media dello spread tra le due criptovalute. A seconda di quale criptovaluta si decide di utilizzare come variabile indipendente il risultato del test di cointegrazione cambia. Riportiamo nella tabella i risultati dei coefficienti di regressione per le dodici coppie di criptovalute:

COPPIA	β_0	β_1	R^2	COPPIA	β_0	β_1	R^2
ETH/BTC	4381.4000	21.9440	0.3600	BTC/LTC	22.439	0.0060411	0.164
BTC/ETH	53.7360	0.0160	0.3600	LTC/BTC	6663.3	27.099	0.164
XRP/BTC	6860.6000	6211.1000	0.0615	LTC/XRP	0.10963	0.0024768	0.858
BTC/XRP	0.2092	0.0000	0.0615	XRP/LTC	-27.292	346.27	0.858
ETH/XRP	0.0445	0.0012	0.7640	XRP/BCH	54.09	863.63	0.583
XRP/ETH	19.6750	599.0000	0.7640	BCH/XRP	0.08679	0.00067454	0.583
XRP/EOS	-1.3529	18.8560	0.8550	BCH/BTC	5391.7	10.685	0.233
EOS/XRP	0.1041	0.0454	0.8550	BTC/BCH	119.45	0.021815	0.233
EOS/BTC	8041.7000	154.9300	0.0159	EOS/BCH	110.98	47.004	0.717
BTC/EOS	3.3225	0.0001	0.0159	BCH/EOS	-0.50294	0.015264	0.717
EOS/ETH	82.8550	26.9740	0.6440	BCH/LTC	-8.2527	0.2692	0.664
ETH/EOS	-0.4802	0.0239	0.6440	LTC/BCH	124.31	2.4654	0.664
LTC/EOS	0.5310	0.0491	0.8120	ETH/BCH	29.447	1.4228	0.742
EOS/LTC	5.2953	16.5270	0.8120	BCH/ETH	-82527	0.2692	0.664
LTC/ETH	73.3023	1.6443	0.8050				
ETH/LTC	-21.2850	0.4897	0.8050				

Il secondo step della procedura di Engle e Granger consiste in un test di radici unitarie (ADF) sui residui della regressione precedentemente stimata. Se i residui risultano stazionari, allora le due coppie di criptovalute sono cointegrate. Nella tabella seguente sono riportati i p-value per il test ADF sui residui di tutte le coppie di criptovalute analizzate:

COPPIA	P-VALUE	H=	COPPIA	P-VALUE	H=
ETH/BTC	0.0203	1	ETH/LTC	0.2190	0
BTC/ETH	0.2823	0	BTC/LTC	0.200	0
XRP/BTC	0.0179	1	LTC/BTC	0.0138	1
BTC/XRP	0.0687	0	LTC/XRP	0.0017	1
ETH/XRP	0.0783	0	XRP/LTC	0.0036	1
XRP/ETH	0.1698	0	XRP/BCH	0.0959	0
XRP/EOS	0.0052	1	BCH/XRP	0.0679	0
EOS/XRP	0.0045	1	BCH/BTC	0.0189	1
EOS/BTC	0.0193	1	BTC/BCH	0.1348	0
BTC/EOS	0.0873	0	EOS/BCH	0.0335	1
EOS/ETH	0.1485	0	BCH/EOS	0.0279	1
ETH/EOS	0.0681	0	BCH/LTC	0.1231	0
LTC/EOS	0.0124	1	LTC/BCH	0.0738	0
EOS/LTC	0.0169	1	ETH/BCH	0.0220	1
LTC/ETH	0.0300	1	BCH/ETH	0.1231	0

A questo punto occorre definire le regole della strategia di Pair Trading e applicarle alle ventuno coppie di criptovalute che hanno superato il test di cointegrazione.

Prendiamo ora in considerazione una delle coppie che risulta cointegrate, ad esempio Btc/Eth. I residui rappresentano lo spread della coppia, essendo quest'ultimi stazionari è possibile strutturare una strategia che preveda l'acquisto simultaneo, e di posizioni opposte. Lo spread può essere definito come:

$$\delta_t = BTC_t - \beta_1 ETH_t \text{ con } \beta_1 = 0.0168$$

Aprire una posizione lunga sullo spread significa aprire una posizione di 1 unità sul Bitcoin e una posizione corta di 0.0168 unità sull' Ethereum; per una posizione corta si fa l'opposto. Per prima cosa bisogna standardizzare lo spread in modo da normalizzare i segnali di entrata e di uscita. Calcoliamo la media (μ_t) e la deviazione standard (σ_t) dello spread utilizzando come campione il training set. Definiamo ora lo Z-score (Spread normalizzato) :

$$Z_t = \frac{\delta_t - \mu_t}{\sigma_t}$$

In una strategia di Pair Trading di questo tipo le operazioni sullo spread vengono aperte quando il valore dello Zscore diverge più di "n" deviazioni standard dalla media. Quando nel mercato in cui si sta operando i costi di transazione risultano alti, come nel caso delle criptovalute in cui le transazioni sono di circa lo 0.10-0.30%, si preferisce aumentare l'ampiezza della divergenza "n". Nel nostro caso si è impostato come segnale di entrata e di uscita:

Entrata Lunga	Zscore < -2
Uscita Lunga	Zscore > 0
Entrata Corta	Zscore > 2
Uscita Corta	Zscore < 0

Una volta identificate le regole per la strategia di trading, utilizzando la parte del campione definita training set, si passa alla fase di test della strategia. Per la valutazione della strategia, oltre a calcolare i ritorni cumulati, è stato utilizzato un indicatore molto noto in Finanza "Sharpe Ratio". Per la valutazione della strategia è stato utilizzato una versione modificata di tale indice, versione proposta da Ernie Chan. Analizziamo le performance sulle coppie di criptovalute cointegrate:

COPPIA	SHARPE RATIO	SHARPE RATIO	RITONI CUMULATI	RITONI CUMULATI
	TRAIN	TEST	TRAIN %	TEST %
ETH/BTC	1.479	1.516	23.789	10.345
XRP/BTC	1.140	2.328	42.620	97.643
XRP/EOS	1.725	0.465	22.273	1.283
EOS/XRP	2.404	0.280	66.648	2.581
EOS/BTC	2.382	0.485	115.563	4.651
LTC/EOS	1.591	0.184	23.312	- 1.200
EOS/LTC	1.141	0.979	15.022	-0.700
LTC/ETH	1.382	0.309	21.967	3.433
LTC/BTC	1.759	1.534	53.051	36.143
LTC/XRP	2.547	0.536	46.590	1.354
XRP/LTC	2.347	1.092	35.561	8.355
BCH/BTC	1.741	1.424	34.519	21.760
EOS/BCH	2.198	2.327	54.153	30.343
BCH/EOS	0.438	1.428	2.565	11.354
ETH/BCH	2.620	1.258	56.185	1.174

La strategia presenta valori positivi per tutte le coppie di criptovalute considerate. Si registrano valori di rendimento superiore sul training set, dato che i parametri sono stati stimati sul medesimo campione. Inoltre va considerato che non sono compresi i costi di transazione, i quali influiscono in modo decisivo sulla profittabilità della strategia. In letteratura si è stimato che in media su ogni operazione i costi di transazione incidono di circa il 0.2% (tali costi sono stati implementati nella valutazione).

Un ulteriore test per la verifica di una relazione di cointegrazione, il test di Johansen. Tale modello per la stima dei coefficienti di cointegrazione utilizza la funzione di massima verosimiglianza, portando dunque stipe diverse rispetto il test di Engle e Granger. In questo paragrafo analizzeremo proprio i risultati di una strategia di Pair Trading con gli stessi parametri e dati utilizzanti nel caso precedente, ma come unica differenza utilizzeremo il test di cointegrazione di Johansen. Avendo già effettuato su tutte e sei le criptovalute il test di radice unitarie ADF e KPSS, dove si è riscontrato che tutte e sei le serie storiche sono processi stocastici integrati di ordine uno; passiamo direttamente al test di cointegrazione. I risultati per le sei coppie di criptovalute sono riportati nella seguente tabella:

COPPIA	P-VALUE	H=	COPPIA	P-VALUE	H=
ETH/BTC	0.4638	0	ETH/LTC	0.1154	0
BTC/ETH	0.3188	0	BTC/LTC	0.1453	0
XRP/BTC	0.1673	0	LTC/BTC	0.0406	1
BTC/XRP	0.0402	1	LTC/XRP	0.3367	0
ETH/XRP	0.5991	0	XRP/LTC	0.2073	0
XRP/ETH	0.1225	0	XRP/BCH	0.5723	0
XRP/EOS	0.1299	0	BCH/XRP	0.0890	0
EOS/XRP	0.0540	0	BCH/BTC	0.1028	0
EOS/BTC	0.0528	0	BTC/BCH	0.0258	1
BTC/EOS	0.0182	1	EOS/BCH	0.5367	0
EOS/ETH	0.0098	1	BCH/EOS	0.1228	0
ETH/EOS	0.0094	1	BCH/LTC	0.4969	0
LTC/EOS	0.1822	0	LTC/BCH	0.1475	0
EOS/LTC	0.0716	0	ETH/BCH	0.0027	1
LTC/ETH	0.4821	0	BCH/ETH	0.0047	1

In Matlab un valore del parametro “h” uguale a zero indica l’accettazione dell’ipotesi nulla di cointegrazione ; mentre un valore pari a uno indica il rifiuto dell’ipotesi nulla a favore dell’ipotesi alternativa di non cointegrazione. Come è possibile osservare confrontando le due tabelle, il test di Johansen risulta meno stringente rispetto al test di Engle e Granger. Sono 22 le coppie di criptovalute che risultano cointegrate con il test di Johansen, rispetto alle sole 15 coppie trovate con il test di Engle e Granger. Sia le modalità di calcolo dello Zscore, sia i segnali di entrata e di uscita restano gli stessi utilizzati per la strategia con il test di Engle e Granger. I ritorni cumulati e il valore dello sharpe ratio con la strategia di Johansen sono riportati nella tabella che segue (in questo caso la stima dei costi di transazione del 0.2% è già stata inclusa nel calcolo):

COPPIA	SHARPE RATIO	SHARPE RATIO	RITONI CUMULATI	RITONI CUMULATI
	TRAIN	TEST	TRAIN %	TEST %
ETH/BTC	1.516	1.233	6.930	7.420
BTC/ETH	2.0973	1.789	4.450	2.340
XRP/BTC	1.5766	0.637	15.640	5.120
ETH/XRP	1.2130	1.253	7.350	9.690
XRP/ETH	1.3363	0.276	15.040	5.530
XRP/EOS	1.407	0.847	44.82	15.890
EOS/XRP	1.704	1.0715	44.470	46.860
EOS/BTC	1.758	0	8.960	0
LTC/EOS	1.592	0.894	13.370	10.180
EOS/LTC	1.601	1.062	25.830	31.090
LTC/ETH	1.671	0.767	13.050	7.560
ETH/LTC	1.139	1.508	5.050	1.480
BTC/LTC	1.126	1.602	6.070	9.460
LTC/XRP	1.657	0.875	15.060	10.290
XRP/LTC	1.456	0.869	3.642	1.379
XRP/BCH	1.525	0.844	26.280	10.310
BCH/XRP	2.164	1.530	14.410	14.720
BCH/BTC	1.854	0.854	8.650	4.970
EOS/BCH	1.641	1.064	35.566	37.490
BCH/EOS	2.111	1.571	13.440	14.890
BCH/LTC	0.668	1.568	1.150	12.430
LTC/BCH	1.699	0.861	12.820	8.310

I rendimenti risultano tutti positivi fatta eccezione per la coppia EOS/BTC. Rispetto ad i rendimenti della strategia con il test di Engle e Granger i rendimenti risultano nettamente inferiori, troviamo però una maggiore aderenza tra i risultati ottenuti nel training set e nel test set.

Sviluppiamo ora una strategia basata su un indicatore tecnico, in modo da poter confrontare i risultati ottenuti per la strategia di Pair Trading. In particolare utilizzeremo come strumento di analisi tecnica le così dette Bande di Bollinger. Le bande di Bollinger appartengono alla categoria di indicatori tecnici di volatilità del mercato. Queste vengono utilizzate per individuare le fasi del titolo di ipercomprato e ipervenduto e per capire il range di oscillazione dei prezzi. Le bande di Bollinger consistono di tre linee: una linea centrale (CL), una linea inferiore (LI) e una linea superiore (LS). Da un punto di vista matematico è possibile calcolare questi tre valori:

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

Dove “n” indica il valore dei periodi e il numero di dati utilizzati per calcolare la deviazione standard. Le due bande , superiore e inferiore, funzionano da supporto e resistenza dinamica .

Nel momento in cui il prezzo supera la fascia superiore si aprirà un'operazione di vendita, la quale verrà chiusa solo quando il prezzo sarà più basso o uguale alla fascia inferiore. Nel caso contrario, si apre l'operazione di acquisto quando il prezzo supera la fascia inferiore e si chiude quando è uguale o superiore alla fascia superiore. Nella tabella che segue, sono riportati i rendimenti su ogni singola criptovaluta:

COPPIA	SHARPE RATIO	SHARPE RATIO	RITorni CUMULATI	RITorni CUMULATI
	TRAIN	TEST	TRAIN %	TEST %
ETH	-0.443	1.360	-6.700	2.290
BTC	-0.7311	-0.0520	-5.420	-0.069
XRP	-0.4282	0.3849	-3.718	6.980
EOS	1.2780	1.039	6.529	5.861
LTC	1.349	0.247	22.250	9.293
BCH	0.4107	0.4613	5.300	6.030

Come si evince dalla tabella precedente tale strategia risulta poco profittevole ed è inoltre particolarmente esposta a situazioni di instabilità. Spesso uno dei principali problemi delle bande di Bollinger riguarda le fasi di trend del mercato. In tali fasi del mercato può succedere che i prezzi corrano lungo tutta la banda, così che l'investitore chiuda l'operazione di vendita in modo prematuro e apra troppo presto l'operazione di acquisto.

Un altro indicatore molto utilizzato in Analisi Tecnica è il Relative Strength Index. Si tratta di un indicatore di forza relativa, sviluppato dall'ingegnere meccanico John Welles Wilder nel 1978. Tale indicatore è utilizzato per identificare la forza interna di un asset finanziario in un intervallo di tempo in modo tale da evidenziare zone di ipercomprato e ipervenduto. Il Relative Strength Index è calcolato come:

$$RSI = \left[\frac{100}{1 + RS} \right]$$

dove RS è il rapporto tra la media delle variazioni positive al numeratore, e al denominatore la media delle variazioni negative fatte segnare dal prezzo del titolo nel periodo "n". Il Relative Strength Index assume valori in un intervallo tra zero e cento; se l'indicatore va al di sopra dei settanta si è in una zona di ipercomprato, mentre al di sotto dei trenta si è in una zona di ipervenduto.

Considerando gli stessi periodi analizzati per le strategie precedenti, la tabella seguente mostra i rendimenti ottenuti da tale strategia sulle sei criptovalute:

COPPIA	SHARPE RATIO	SHARPE RATIO	RITONI CUMULATI	RITORNI
	TRAIN	TEST	TRAIN %	CUMULATI TEST %
BTC	-0.018	-0.6643	-0.400	-5.240
ETH	-1.077	-0.551	-1.457	-9.740
XRP	0.1704	0.0841	7.457	9.675
EOS	0.5607	1.7852	12.220	179.40
LTC	0.2417	0.6186	-1.049	1.874
BCH	0.9727	0.0780	5.933	-2.332

I rendimenti risultano bassi o addirittura negativi , tranne nel caso dell'EOS in cui si raggiunge addirittura il 179%.

Conclusioni

L'elaborato esamina la possibilità di applicare una strategia di pair trading al mercato delle criptovalute in modo profittevole. Quindi per prima cosa ci siamo soffermati sulla domanda:

“Esistono coppie di criptovalute che risultano cointegrate ?”

Per rispondere a tale domanda sono stati applicati due differenti tipi di test di cointegrazione alle sei criptovalute con maggiore capitalizzazione. Entrambi i metodi hanno riscontrato la presenza di diverse coppie di criptovalute che risultano cointegrate. Nel caso del test a due stadi di Engle e Granger sono state individuate ben 15 coppie; mentre applicando la procedura di Johansen sono state individuate 22 coppie di criptovalute che risultano cointegrate. L'utilizzo degli autovettori, calcolati attraverso la procedura di Johansen, come stima dell'Hedge Ratio della strategia di Pair Trading ha mostrato maggiore stabilità tra i rendimenti ottenuti nel training set e nel test set. Risulta quindi più efficiente una strategia di Pair Trading che applichi la procedura di Johansen per l'identificazione delle coppie cointegrate e per la stima dei coefficienti. La seconda domanda che ci siamo posti è:

“Tra una strategia basata sull'analisi tecnica e una strategia di Pair Trading sulla cointegrazione, quale risulta maggiormente profittevole ?”

Per effettuare un confronto tra analisi tecnica e arbitraggio statistico sono state utilizzate due strategie basate su: Bande di Bollinger e Relative Strength Index. La strategia con le bande di Bollinger su alcune criptovalute ha mostrato rendimenti superiori, mentre su altre perdite consistenti. Un risultato di questo tipo dipende proprio dalla caratteristica intrinseca nel mercato delle criptovalute di elevati livelli di volatilità. Risultati ancor meno soddisfacenti sono stati ottenuti dal RSI. Nella strategia di Pair Trading grazie all'apertura in contemporanea di operazioni di segno opposto è stato possibile eliminare il rischio legato alle scosse dell'intero mercato delle criptovalute. La strategia basata sulle bande di Bollinger risulta maggiormente esposta al rischio di mercato. In conclusione è possibile affermare che le strategie di Pair Trading risultano profittevoli sul mercato delle criptovalute. Ulteriori ricerche sull'argomento dovrebbero esplorare la presenza di coppie cointegrate all'interno dell'intero mercato delle criptovalute, estendendo il set di dati ad intervalli temporali differenti. Inoltre l'utilizzo di algoritmi di neural network potrebbero migliorare i segnali di entrata e di uscita in modo da ottenere maggiori profitti.