Università
Ca'Foscari
Venezia

Corso di Laurea
Magistrale

(*Ordinamento ex D.M*. 270/2004)

in Economia e
Finanza

Tesi di Laurea

Investimenti in criptovalute

Relatore
Ch. Prof. Marco Corazza

Correlatore
Ch. Prof.ssa. Diana Barro

Laureando
Giulio Righetto
Matricola 847768

Anno Accademico
2017/2018

Alla mia famiglia.

INDICE

INTRODUZIONE **2**

CAPITOLO 1 ..... **4**

CRIPTOVALUTE E BITCOIN **4**

1.1. COSA SONO LE CRIPTOVALUTE? 5
1.1.1 LE CRIPTOVALUTE IN BREVE *7*
1.2 IL CONCETTO DI CRIPTOVALUTA 8
1.3 IL BITCOIN, ATTORI PRINCIPALI E 9
DIFFERNEZE CON LA MONETA FIAT 9
1.4 SATOSHI NAKAMOTO, IL BITCOIN 11
1.5 PRINCIPALI CARATTERISTICHE DEL BITCOIN 14
1.6 LA BLOCKCHAIN 23
1.7 IL MINING E I MINATORS 27
1.8 I PORTAFOGLI (WALLET) 33
1.9. GLI EXCHANGE 37

CAPITOLO 2 ..... **44**

LE PRINCIPALI CRIPTOVALUTE **44**

2.1. CARATTERISTICHE DELLE CRIPTOVALUTE 51
2.1.1. CAPITALIZZAZIONE DI MERCATO *52*
2.1.2 VOLUME DEGLI SCAMBI *53*
2.1.3 CIRCULATING SUPPLY *55*
2.2. LE ALTCOIN 57
2.2.1 BITCOIN CASH *58*
2.2.2. LITECOIN *62*
2.2.3. MONERO *66*
2.2.4. DASH *71*
2.3 CRIPTOVALUTE INNOVATIVE RIPPLE E IOTA 77
2.3.1 RIPPLE *77*
2.3.2. IOTA *83*
2.4 LE CRIPTOVALUTE 2.0 91
2.4.1. ETHEREUM *91*
2.4.2. NEO *96*
2.4.3 ICO *100*

CAPITOLO 3 ..... **102**

INVESTIMENTI IN CRIPTOVALUTE **102**

3.1 PROBLEMATICHE DEL MERCATO CRYPTO 106
3.2 SELEZIONE DI PORTAFOGLIO ALLA MARKOWITZ 108
3.3 LA SELEZIONE DELLE CRIPTOVALUTE 116
3.4 PORTAFOGLI QUADRIMESTRALI 127
3.4.1 PRIMO PERIODO *127*
3.4.2 SECONDO PERIODO *131*
3.4.3 TERZO PERIODO *135*
3.4.4 QUARTO PERIODO *138*
3.4.5 QUINTO PERIODO *142*

3.4.6 SESTO PERIODO *145*
3.4.7 SETTIMO PERIODO *149*
3.4.8 OTTAVO PERIODO *153*
3.4.9 NONO PERIODO *156*
3.4.10 DECIMO PERIODO *160*
3.5 ANDAMENTO DEI PORTAFOGLI SELEZIONATI 164
APPENDICE A 177
CAPITOLO 4 ..... **179**
CONCLUSIONI **179**
UN PORTAFOGLIO PER IL FUTURO 186
BLIOGRAFIA **193**
SITOGRAFIA **194**

INTRODUZIONE

La nascita del Bitcoin nel 2009 e il successivo sviluppo delle altre criptovalute negli anni seguenti sono stati gli avvenimenti più importante di sempre nel mondo della finanza alternativa. Le criptovalute sono un fenomeno complesso, di rilevanza internazionale ed interdisciplinare, che tocca temi di carattere economico, matematico, giurisprudenziale, politico e sociale.

L'interesse per le criptovalute si è manifestato sia con riguardo alla tecnologia "blockchain" sia per la possibilità di effettuare pagamenti senza l'intermediazione di soggetti terzi (le banche ed in generale gli intermediari finanziari). L'evoluzione di questo mercato, tuttavia, va legata indissolubilmente ad un contesto di investimento finanziario. L'interesse per questo "mondo" è stato amplificato dalla situazione economica-finanziaria globale, caratterizzata da tassi di interesse particolarmente bassi, dovuti alle politiche monetarie espansive adottate dalle Banche Centrali in risposta alla crisi del 2007. Una situazione come questa ha portato gli investitori più esigenti a ricercare nella finanza alternativa situazioni in grado di soddisfare il loro desiderio di ritorno in termini di rendimento. Per questi motivi molti soggetti hanno visto nelle criptovalute un "prodotto finanziario", inteso con l'accezione più generica di opportunità di investimento, adeguato a soddisfare le proprie necessità. Dopo aver guardato al contesto storico e sistemico che ha consentito la nascita della prima criptovaluta, il Bitcoin, obiettivo di questa tesi è quello di analizzare le possibilità di investimento in questo mercato, in primo luogo attraverso uno studio teorico del funzionamento delle criptovalute, ed in un secondo momento in maniera pratica, attraverso un investimento vero e proprio con la creazione di un portafoglio.

Il primo capitolo della tesi tratta il fenomeno delle criptovalute, prima generalmente, poi soffermandosi in maniera particolare sulla tecnologica del Bitcoin. Il Bitcoin, in quanto prima criptovaluta, merita una considerazione particolare ed un'analisi più accurata e completa rispetto a quella che sarà riservata alle successive criptomonete.

Per questo motivo, nel capitolo, saranno toccate tutte le tematiche che riguardano il suo funzionamento: dallo scopo principale dell'ideatore di Bitcoin Satoshi Nakamoto, alla rivoluzionaria tecnologia della blockchain. Attenzione particolare verrà riservata anche ai soggetti che operano per il funzionamento del network Bitcoin, i cosiddetti "Minatori", e per coloro che permettono lo scambio dalle criptovalute in monete fiat e viceversa, i cosiddetti "exchange", fino a toccare i modi con i quali il Bitcoin viene detenuto nei vari tipi di portafogli (wallet).

Il secondo capitolo si occupa di introdurre e classificare le criptovalute che sono state sviluppate successivamente al Bitcoin. La classificazione viene effettuata sia tenendo conto dell'obiettivo perseguito dagli sviluppatori e ideatori delle "Coin", sia studiando le peculiarità della tecnologia sottostante le criptomonete. Per ogni criptovaluta sarà anche presentata un'analisi dell'andamento di mercato ed un confronto con il Bitcoin, in modo da individuarne le differenze. La scelta di Bitcoin come "Coin" di riferimento e confronto va senza dubbio legata al fatto che essa sia tuttora la criptomoneta più importante e conosciuta nonché quella che domina (in termine tecnico appunto la "dominance") il settore dal punto di vista della capitalizzazione di mercato.

Il terzo capitolo, nel quale viene svolta un'analisi empirica, analizza le possibilità di costruire un portafoglio diversificato di criptovalute, che possa garantire un rendimento proporzionato al rischio intrinseco del mercato. L'analisi verrà effettuata a periodi quadrimestrali a partire dal primo gennaio 2015, fino ad arrivare al 30 aprile 2018. Nell'analisi verranno considerate in totale 28 criptovalute, individuate tra quelle caratterizzate da una maggiore capitalizzazione di mercato nel periodo considerato.

Il quarto ed ultimo capitolo riguarda le conclusioni, che oltre al commento dei risultati ottenuti nelle analisi precedenti, conterrà alcune considerazioni personali su come sarebbe corretto investire in futuro in questo settore.

CAPITOLO 1

CRIPTOVALUTE E BITCOIN

Negli ultimi anni è emerso un sistema di pagamento legato strettamente alla tecnologia informatica ed alla rete web. Internet è stata l'innovazione più importante che ha coinvolto il XX secolo in un modo che ha influenzato tutti gli aspetti della realtà. È avvenuto un cambiamento sociale, economico, politico, giuridico ed in generale sulla vasta scala del quotidiano, con un'infiltrazione graduale e dirompente.

In questo contesto in continua evoluzione anche le banche hanno dovuto adeguarsi ai cambiamenti, aggiornando e a volte rivoluzionando i propri sistemi di pagamento, in modo da renderli più efficaci ed efficienti per permettere transazioni on-line rapide e sicure.

Il mondo dei sistemi di pagamento e della finanza si sta trasformando davanti i nostri occhi. Le risorse ed i canali digitalizzati, i nuovi strumenti e sistemi finanziari stanno creando nuove metodologie per le transazioni finanziarie e per gli investimenti del capitale.

In un tale processo di innovazione e adeguamento tecnologico si inseriscono le criptovalute[1], conosciute anche come monete virtuali.

[1] Il termine può essere scritto anche "Crittovalute", "Cryptovalute", "Criptomonete". Viene spesso utilizzata anche l'abbreviazione del termine inglese "Cryptocurrency" ovvero "Crypto".

1.1. COSA SONO LE CRIPTOVALUTE?

Il Bitcoin è stato utilizzato a partire dal gennaio del 2009, ed è stata la prima criptovaluta. La seconda criptovaluta, Namecoin[2], è emersa solo due anni dopo, nell'aprile del 2011. Da allora sono nate migliaia di monete virtuali e centinaia di esse possono essere scambiate negli exchange ed hanno un valore ed una capitalizzazione di mercato considerevoli[3]. La risposta alla domanda su cosa siano le criptovalute non è né semplice né banale; una criptovalute è un bene (asset, nel più vasto significato del termine) crittografico, nel senso che utilizza la crittografia per garantire la sicurezza delle proprie transazioni, di tipo digitale, che viene impiegato come bene di scambio tra soggetti che operano nella rete. Si dice che le criptovalute siano generici "asset" perché dalla regolamentazione attuale e dall'utilizzo che ne viene fatto non è ancora possibile stabilire specificatamente in che categoria di asset rientrino. Le criptovalute da un lato possono sembrare degli asset assimilabili a "monete", infatti vengono utilizzati per l'acquisto di altri beni, dall'altro invece, come verrà analizzato in seguito nella tesi, hanno caratteristiche ed utilizzi simili a quelle di asset finanziari, nel senso che vengono messe in circolazione da delle società, come mezzi per il finanziamento delle società[4] stesse (una funzione simile all'azione) senza però permettere a coloro che gli acquistano di poter diventare proprietari (azionisti) della società in questione.

---

[2] https://namecoin.org/ Namecoin (NMC) è la seconda cryptocurrency nata come "fork" del bitcoin il 18 aprile 2011. Il fork è definito in informatico come lo sviluppo di un progetto software nuovo che parte dal codice sorgente di uno già esistente. Namecoin in sostanza è nata da una "scissione" del bitcoin, per questo motivo si basa sulla stessa tecnologia e sullo stesso algoritmo poof-of-work.

[3] Nel sito https://coinmarketcap.com/ si possono vedere, in ogni istante, le capitalizzazioni di mercato ed i prezzi medi calcolati in base a quelli di tutti gli exchange che si occupano di acquistare/vendere cryptovalute.

[4] Le ICO (Initial Coin Offering) sono operazioni simili alle IPO (Initial Public Offering), utilizzate dalle società per raccogliere il capitale nel mercato, con la differenza che le società in questione non raccolgono il capitale con la vendita delle proprie azioni, ma con la concessione di quantità della propria criptovaluta. La logica di fondo tuttavia è la stessa, colui che investe nelle ICO, "scommette" sulla riuscita del progetto di business della società in questione e crede che il prezzo della criptovaluta della società aumenterà in futuro.

L'elemento comune di queste differenti monete virtuali è appunto la tecnologia blockchain, un "libro mastro" pubblico che permette agli utenti di partecipare alla rete e gestirla in assenza di un'autorità centrale. Le ampie potenzialità di applicazione della blockchain, in vari ambiti disciplinari[5], sono forse l'aspetto che più ha suscitato interesse nelle vicende che hanno portato alla ribalta le criptovalute.

Le monete virtuali sono digitali, paritarie[6] e decentralizzate, la decentralizzazione sta nel fatto che, al contrario di tutte le monete tradizionali, le criptovalute sono prive di un ente centrale che si occupi della loro emissione (emissione della "moneta"), non c'è una Banca Centrale che ne controlli il valore e non sono necessari intermediari per la convalida delle transazioni. Le criptovalute utilizzano i principi criptografici per la convalida delle operazioni e per la stessa creazione della moneta, in un processo di "espansione monetaria" di piccole dimensioni ma continuo nel tempo. Il processo congiunto di "creazione" della criptovaluta e convalida delle operazioni viene eseguito grazie all'operato dei "miner", il loro compito, come verrà analizzato, è quella di eseguire gli algoritmi che permettono il funzionamento sicuro dei network delle crypto, in cambio di un corrispettivo (pagato con le criptovalute stesse).

Vista la collocazione storica del loro avvento, si può affermare che le criptovalute siano una risposta sia alla crisi finanziaria ed economica iniziata nel 2007, sia alla necessità di un'unità di conto legata in maniera diretta al mondo interconnesso.

L'innovazione principale delle criptovalute riguarda il fatto di riuscire ad utilizzare i principi della criptografia[7] con una moneta digitale il cui ammontare sia limitato.

---

[5] Si possono pensare moltissime applicazioni che una tecnologia come questa potrebbe avere; per fare solo alcuni esempi in ambito catastale, sarebbe possibile delineare tutti i passaggi di proprietà di una casa senza che vi possano essere manomissioni o errori, o anche in ambiti come quello alimentare, applicando la blockchain per garantire l'origine di ogni prodotto (per risalire in ogni momento a tutti i passaggi che il prodotto stesso ha compiuto prima di arrivare al consumatore).

[6] Nel senso che è fondata sul criterio di parità ed uguaglianza, ogni soggetto che lo desidera può attivarsi per gestire in maniera condivisa la piattaforma che permette il funzionamento della criptovaluta. Da questo punto di vista le criptovalute vengono considerate paritarie.

[7] La Crittografia (o Criptografia) è una scienza che si occupa dello studio delle tecniche e metodologie per codificare un testo "in chiaro", al fine di produrre un testo cifrato,

Anche se il bitcoin ha iniziato ad operare solo all'inizio del 2009, il concetto di criptovaluta ha origini più lontane, e si è sviluppato nel tempo in maniera progressiva, sfruttando le nuove tecnologie e le esigenze nate a seguito dello sviluppo della rete e di internet.

Per prima cosa è opportuno individuare gli aspetti comuni che legano tutte le monete virtuali e ripercorrere la storia che ha portato alla nascita nel 2008 e all'utilizzo a partire dal 2009 della prima criptovaluta: il bitcoin.

1.1.1 LE CRIPTOVALUTE IN BREVE

Un primo equivoco linguistico che va chiarito è quello sulla differenza tra il concetto di moneta elettronica (attraverso la quale avviene un pagamento elettronico) e quello di criptovaluta (moneta digitale[8]). I due termini possono sembrare sinonimi ma in realtà non lo sono affatto; quando si parla di moneta/valuta elettronica o denaro elettronico ci si riferisce a quello che in inglese viene definito e-cash. Il termine concerne quella moneta che viene utilizzata sul web per effettuare pagamenti, che avvengono attraverso le valute di corso legale. Gli acquisti che avvengono nel web prevedono un pagamento elettronico, cioè un pagamento senza passaggio fisico di denaro. Il funzionamento delle transazioni è sostanzialmente simile per tutte le società che si occupano di questo tipo di pagamenti: viene aperto un conto deposito, versando somme di danaro fisico presso un intermediario. Attraverso il conto si possono effettuare pagamenti via internet in tutti i negozi presenti nel web. Ogni volta che viene effettuato un pagamento, la cifra spesa online viene scalata dal deposito e la società la trasferisce sul conto del destinatario. Utilizzare una moneta elettronica equivale in sostanza ad effettuare pagamenti attraverso l'utilizzo di moneta fiat[9] dematerializzata, senza la necessità di un effettivo passaggio fisico tra coloro che effettuano la transazione.

---

comprensibile ad un solo ricevente (quello legittimo), il è in possesso dell'informazione necessaria per decifrarlo (detta chiave), recuperando il testo in chiaro.

[8] La moneta digitale verrà analizzata durante la tesi.

[9] Dal termine inglese "Fiat Money", moneta legale o di corso legale, è quel mezzo di pagamento non coperto da riserve di altro materiale (per esempio le riserve auree) e quindi priva di valore

Le criptovalute (monete digitali) sono la prima forma di "contante digitale" esse uniscono in sé i vantaggi della moneta elettronica e del contante. Come un bonifico bancario, consentono pagamenti a distanza; ma allo stesso tempo, come un pagamento effettuato in contanti, garantiscono l'istantaneità dell'operazione e non comporta costi né per chi effettua il pagamento né per chi lo riceve.

Le criptovalute, come una banconota, sono anonime: non richiedono cioè che siano rese note le identità di coloro che effettuano la transazione né la causa del pagamento; ma, essendo digitali e divisibili pressoché illimitatamente consentono dei trasferimenti per qualsiasi importo, dal pagamento di pochi centesimi, al regolamento di traffici commerciali internazionali. Come una carta di pagamento permettono di pagare in tempo reale ed in maniera sicura un qualsiasi importo ed in qualunque parte del mondo; ma, in analogia con il contante consentono ai soggetti che effettuano l'operazione di rimanere in anonimato.

1.2 IL CONCETTO DI CRIPTOVALUTA

La prima persona a parlare di criptovalute fu David Lee Chaum[10] nel 1982 quando pubblicò un articolo intitolato "Blind Signatures for Untraceable Payments" nel quale introduceva il concetto di moneta virtuale. La pubblicazione non riscosse successo in un primo momento, probabilmente perché i tempi non erano ancora maturi, venendo per lungo tempo trascurata e accostata perlopiù al movimento dei chyperpunk[11].

intrinseco. La moneta legale ha un valore grazie al fatto che esiste un'autorità (lo Stato) che agisce come se avesse questo valore. Se un'organizzazione abbastanza grande (una collettività) emette, usa e accetta qualcosa come pagamento, automaticamente quel qualcosa acquisisce valore, dato che è riconosciuto come mezzo di scambio.

[10] David Lee Chaum è nato nel 1955 ed è un informatico e crittografo americano.

[11] Il Cypherpunk è un movimento, attivo negli Stati Uniti dalla fine degli anni 70, influenzato dalla cultura punk. Esso è formato da attivisti che sostengono l'uso della crittografia informatica per l'avviamento di un cambiamento politico e sociale, ad esempio violando archivi riservati con lo scopo di rendere pubbliche alcune verità scomode. Originariamente comunicavano attraverso una mailing list, in gruppi informali con l'intento di ottenere la privacy e la sicurezza informatica

Nel 1990 Chaum fondò ad Amsterdam nei Paesi Bassi, che furono scelti per la loro struttura legislativa vantaggiosa per questo tipo di attività, la società Digicash, una compagnia che ambiva ad integrare la crittografia con la moneta, perseguendo lo scopo di rendere anonime le transazioni. Nel 1994, grazie a Digicash fu effettuato il primo pagamento elettronico. Nonostante l'inizio positivo la società fu chiusa nel 1999 a causa di alcuni problemi economici. Pur essendo stato il primo ad introdurre il concetto di criptovaluta, Chaum con la sua società non ne sviluppò una, bensì si occupò di moneta elettronica.

1.3 IL BITCOIN, ATTORI PRINCIPALI E DIFFERNEZE CON LA MONETA FIAT

Il 18 agosto 2008 viene registrato il nome di dominio bitcoin.org[12] su anonymousspeech.com, mentre il 31 ottobre dello stesso anno appare un articolo in una mailing list intitolato "Bitcoin[13]: a peer-to-peer Electronic cash system" firmato da Satoshi Nakamoto[14].

degli account personali, attraverso l'uso della crittografia, contro governi e gruppi economici. Il più famoso esempio di attivismo cypherpunk è il sito di Wikileaks di Julian Assange.

[12] https://bitcoin.org/en/ è il sito di riferimento della comunità Bitcoin.

[13] È necessario precisare che, convenzionalmente, il termine Bitcoin (con la "B" maiuscola) si riferisce alla tecnologia ed alla rete di pagamento virtuale, mentre bitcoin (con la "b" minuscola) è la valuta scambiata nella rete network.

[14] Satoshi Nakamoto probabilmente è lo pseudonimo dell'inventore del bitcoin. Le teorie sulla sua vera identità sono molte, la maggior parte delle quali basate su illazioni o teorie prive di un vero e proprio fondamento. Attualmente non si è in grado di dire con certezza se dietro questo nome si celi un "lui", una "lei", oppure un gruppo di persone. Se si guarda all'etimologia del termine giapponese "Satoshi" significa "un pensiero chiaro, veloce e saggio". "Naka" può significare "medium, dentro o relazione". "Moto" può significare "origine" o "fondamento". Le ipotesi più accreditate affermano che in realtà il Bitcoin non sia stato ideato e rilasciato da una sola persona, ma da un team di soggetti che hanno sviluppato il progetto ed hanno deciso di rimanere nascosti dietro questo pseudonimo.

Per meglio capire il funzionamento del meccanismo blockchain e del funzionamento del Bitcoin ritengo sia necessario in primo luogo introdurre tutti i concetti chiave e gli attori principali, per poi approfondire ogni argomento successivamente nella tesi.

Che cos'è il Bitcoin? I Bitcoin è la prima valuta digitale decentralizzata. La novità di questa valuta non è tanto quella della digitalizzazione dei pagamenti, alla quale siamo ormai abituati nell'era di internet, quanto al fatto che sia decentralizzata. Contrariamente a tutte le monete tradizionali i bitcoin non sono assoggettati ad una qualsiasi autorità centrale. Della loro coniazione non si occupa la zecca dello Stato e non è presente una Banca Centrale che ne controlli il valore né un intermediario finanziario che ne convalidi le transazioni e gli spostamenti.

Bitcoin è nato con un obiettivo primario: quello di rendere le transazioni sulla rete internet più veloci senza far venir meno la sicurezza. Bitcoin è un sistema per le transazioni elettroniche che non è basato sulla fiducia in un'autorità terza, come avviene nelle transazioni effettuate tutti i giorni, ma al contrario è fondato sulla crittografia. I compiti e le funzioni svolte dalla Banca centrale vengono sostituiti dalla rete Bitcoin. La rete è strutturata come un network di tipo peer-to-peer[15](p2p) a cui possono partecipare tutti coloro che lo vogliano, a patto che installino nel proprio computer il software omonimo (Bitcoin), il quale è libero ed open-source[16]. I nodi del network, facendo "girare" il software all'interno dei propri dispositivi, contribuiscono in modo diffuso a convalidare e registrare le transazioni tra due utenti che desiderino scambiare tra di loro delle unità di questo tipo di valuta, garantendone inoltre l'anonimato grazie alla crittografia insita nel sistema.

L'attività attraverso la quale vengono validate e registrate le transazioni viene definita di "mining", minare in italiano", un termine che richiama in maniera metaforica l'attività

[15] Peer-to-peer(p2p) o rete paritetica: architettura di rete informatica in cui I nodi sono tra loro paritetici, potendosi comportare sia da client che da server.

[16] Open source: software di cui gli autori rendono pubblico il codice sorgente, permettendone lo sviluppo a chiunque.

di estrazione dell'oro da una miniera[17], e i nodi che la svolgono sono chiamati appunto "miners" (minatori). Tale attività sfrutta la potenza computazionale dei dispositivi dei minatori, ed e remunerata attraverso Bitcoin di nuova emissione, secondo un preciso sistema di ricompense.

1.4 SATOSHI NAKAMOTO, IL BITCOIN

L'articolo di Satoshi Nakamoto, richiamato al paragrafo precedente, parla di una moneta virtuale decentralizzata e puramente peer-to-peer (PTP o P2P[18]) che permette pagamenti on-line senza il passaggio attraverso un intermediario.

L'espressione PTP indica un modello di architettura logica di una rete informatica i cui nodi sono sistemati in ordine gerarchico, attraverso forme paritarie ("peer" in inglese), le quali possono fungere sia da servente che da cliente (client o server fissi) verso gli altri nodi terminali della rete. La cosa fondamentale che contraddistingue questa rete è che ogni nodo è in grado di avviare o completare una transazione.

La decentralizzazione sta nel fatto che nel bitcoin, a differenza delle altre valute tradizionali, non è presente un ente centrale che ne controlli e gestisca l'emissione e che regoli il funzionamento e l'operato di coloro che svolgono la funzione di intermediari. L'European Central Bank (ECB) è l'ente centrale che controlla l'euro attraverso la politica monetaria nei paesi dell'Euro Zona; in modo analogo la Federal Reserve (Fed) controlla il dollaro statunitense. Per il bitcoin, al contrario, manca un soggetto, sia questo un ente pubblico o un ente privato, che svolga questa funzione. Nonostante ciò affermare che la rete Bitcoin sia priva di controllo è profondamente sbagliato, infatti il controllo esiste. Esso è diffuso (nel senso che è ripartito tra i partecipanti al network) e distribuito nella

[17] Il Bitcoin è stato spesso paragonato all'oro per la sua caratteristica di essere diventato nel tempo una riserva di valore digitale.

[18] Peer-To-Peer in sigla PTP (tenendo solo le iniziali delle parole), ovvero P2P dall'assonanza di 2 (Two) con "To", con il "2" che viene sostituito quindi alla "T".

rete, garantito dall'adesione ad un protocollo comune. Il protocollo è formato da un insieme di regole che definiscono il funzionamento del sistema e che si applicano nel funzionamento del software Bitcoin. Tutti i dispositivi hardware nei quali opera il software Bitcoin (definiti tecnicamente come "nodi del network") possono comunicare attraverso la rete con gli altri dispositivi, in questo modo avviene la gestione attiva[19] della criptovaluta. Tanto più è grande il numero di nodi che aderiscono al network, tanto più la "decentralizzazione" diventa significativa ed effettiva.[20]

Poiché il software e il protocollo sono stati ideati e rilasciati dall'inventore del Bitcoin (Satoshi Nakamoto), alcuni scettici pensano che il "controllo" e la funzione di autorità centrale della valuta sia nelle mani dello stesso creatore. Questo tuttavia è smentito dai fatti; la natura del progetto Bitcoin è open-source, il software è "aperto" agli sviluppatori che vogliano apportarvi migliorie. Agli stessi sviluppatori tuttavia risulta impossibile forzare un cambiamento drastico del software, in quanto ogni nodo può scegliere con libertà quale versione del software utilizzare, a patto che essa sia conforme e compatibile con i software utilizzati dagli altri nodi. In sostanza è necessario il consenso tra utilizzatori e sviluppatori del sistema affinché esso possa funzionare correttamente. Fatte queste considerazioni è evidente che un tentativo di centralizzazione del sistema risulti quasi impossibile, perché dovrebbe coinvolgere la maggioranza degli utilizzatori e degli sviluppatori della piattaforma Bitcoin.

Per sopperire alla mancanza di un controllo centralizzato è utilizzato un network peer-to-peer; le transazioni di criptovalute avvengono attraverso una firma digitale. Il network P2P è utilizzato per effettuare "marcature temporali"[21] per la cui apposizione

[19] Per gestione attiva si intende la partecipazione al network bitcoin attraverso lo sviluppo del software per migliorarne le inefficienze, grazie alla struttura open-source del protocollo Bitcoin, ovvero la partecipazione alla risoluzione degli hash che garantisce la sicurezza (mining).

[20] È necessario chiarire che per effettuare operazioni con i bitcoin non è necessario essere uno dei nodi. I nodi sono indispensabili per il funzionamento del sistema, come verrà spiegato approfonditamente in seguito, ma coloro che vogliono effettuare delle semplici operazioni di acquisto/vendita on-line necessita solamente di un indirizzo Bitcoin.

[21] La marcatura temporale è un processo attraverso il quale viene generato e viene apposta una marca temporale su un documento di tipo informatico, digitale o anche elettronico. Il processo di marcatura temporale consiste nella generazione, da parte di una terza parte (in questo caso

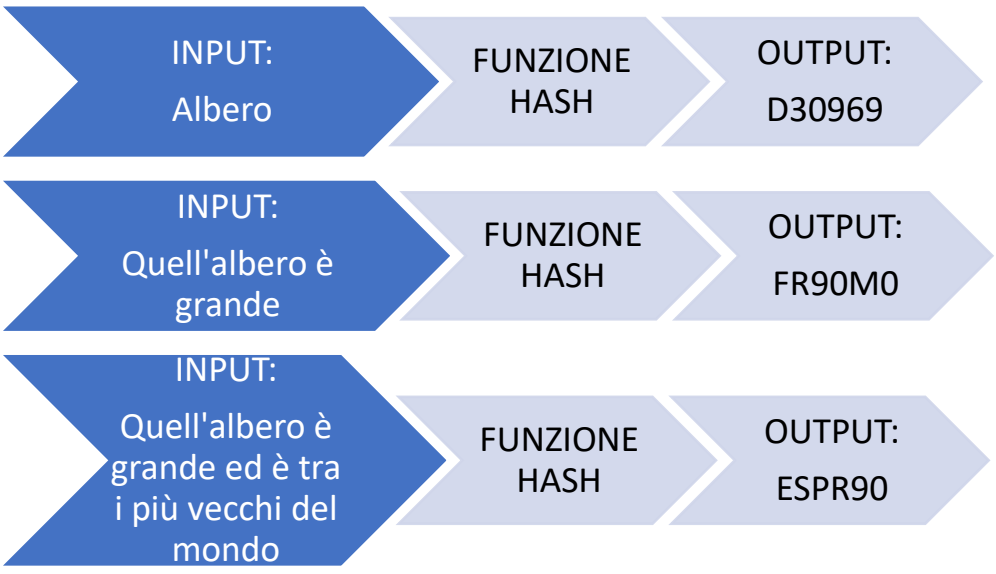
è necessaria l'applicazione di un algoritmo alfanumerico. Come premio al nodo che per primo riesce ad eseguire l'algoritmo è rilasciato un quantitativo di bitcoin, questo processo in termini informatici viene definito "hash", e consiste in sostanza nella trasformazione per il tramite di una funzione iniettiva (non invertibile) di una sequenza di caratteri di lunghezza arbitraria (detta messaggio) in una sequenza di lunghezza predefinita chiamata "valore di hash" o "message digest".

Per spiegare il funzionamento dell'hash ritengo sia necessario procedere con un esempio:

FIGURA 1.1: In figura 1.1 è riportato un banale esempio di hash. Come si può vedere, da un input di tipo arbitrario (quanto si voglia grande), tramite una funzione hash si giunge ad un output equivalente ad un "codice" alfanumerico di lunghezza predefinita.

Le funzioni sono unidirezionali, per questo motivo anche piccole modifiche dei dati in ingresso possono comportare notevoli cambiamenti di quelli in uscita.

FIGURA 1.1



un nodo), di una "firma digitale del documento" a cui viene associata l'informazione relativa ad una data e ad un orario certo.

Quella sopra descritta è una funzione hash generale, tuttavia le funzioni utilizzate per Bitcoin, sono classi specifiche di hash chiamate "funzioni criptografiche di hash". Queste particolari classi sono progettate per non essere invertibili (in termine tecnico definite "one- way[22]"). Una funzione di questo tipo deve possedere almeno due caratteristiche; deve identificare in maniera univoca il messaggio, nel senso che non deve essere possibile che due messaggi differenti abbiano come risultato una stessa sequenza alfanumerica, deve essere quasi impossibile genere un messaggio hash uguale a meno che non si provino tutte le combinazioni possibili.

La scelta di utilizzare un software open-source ha riscontri sia positivi che negativi. Se da un lato la natura open-source ha permesso lo sviluppo di altre valute cloni e concorrenti del bitcoin (le cosiddette "Altcoin[23]"), dall'altro ha fatto sì che fosse possibile una manutenzione ed un miglioramento di efficienza continuo del sistema, tramite il valore intellettuale apportato dagli interventi degli esperti e dei sviluppatori di tutto il mondo.

1.5 PRINCIPALI CARATTERISTICHE DEL BITCOIN

Ai sensi della direttiva della Banca Centrale Europea "Virtual currency schemes – A further analysis" del 2015, il bitcoin è definito come una moneta digitale non regolata utilizzata tra i membri di una comunità virtuale. Il bitcoin è una moneta virtuale che viene scambiata in ogni momento con le monete fiat sia in entrata che in uscita (può essere acquistato con monete fiat ed essere trasformato in monete fiat).

[22] Le funzioni sono unidirezionali, per questo motivo anche piccole modifiche dei dati in ingresso possono comportare notevoli cambiamenti di quelli in uscita.

[23] Con questo termine si fa riferimento alle Criptovalute cloni del Bitcoin, quelle cioè che sostanzialmente hanno una procedura simile e che non presentano alcuna caratteristica particolarmente innovativa.

FIGURA 1.2: Nella figura sono elencate le caratteristiche principali del Bitcoin che verranno analizzate nel seguente paragrafo.

FIGURA 1.2

Le principali caratteristiche sono:

1. DECENTRALIZZAZIONE:

Bitcoin non è stato istituito né controllato da alcuna autorità centrale. Il controllo sulle transazioni viene effettuato da tanti soggetti indipendenti (i nodi). In questo modo non è necessaria la presenza di intermediari per lo svolgimento dei trasferimenti della criptovaluta.

2. INDIPENDENZA E NON ASSOGGETTAZIONE A POLITICA MONETARIA:

L'assenza di un'autorità centrale fa sì che il circolante di moneta non possa essere aumentato o diminuito a piacimento come avviene nella politica monetaria delle banche centrali. L'offerta di moneta è stabilita a priori dal protocollo, essa aumenta in maniera

decrescente fino al raggiungimento della soglia massima di unità prestabilite di 21 milioni di bitcoin[24].

L'aumento del circolante avviene ogni qual volta venga eseguito un algoritmo, quindi attraverso il cosiddetto mining[25], che rende possibile il funzionamento del sistema. Ogni volta in cui viene eseguito un algoritmo come premio per ciò il "minatore" riceve in cambio una quantità X di bitcoin di nuova emissione prestabilita dal protocollo, alla quale quantità X vanno sommate tutte le commissioni che coloro che effettuano le transazioni in quell'arco di tempo decidono di lasciare ai minatori. Ad esempio un soggetto A che trasferisce 1 bitcoin (BTC in sigla) ad un soggetto B può decidere di lasciare una commissione di 0.0001 BTC ai minatori, la somma di tutte le commissioni lasciate viene attribuita al minatore che per primo esegue l'algoritmo. Per i primi quattro anni dalla creazione del bitcoin, la quantità X decisa come premio per la risoluzione dell'algoritmo era di 50 bitcoin. Ogni 4 anni la quantità di bitcoin emessa dopo ogni operazione si riduce del 50%, così dal 2013 fino al 2017 il premio per il mining è stato di 25 BTC. In questo momento e per i prossimi 2 anni verranno emessi 12,5 bitcoin per ogni esecuzione dell'algoritmo. L'esecuzione dell'algoritmo avviene ogni circa 10 minuti, questo periodo temporale è stabilito dal sistema, e viene mantenuto uguale in quanto ogni due settimane l'algoritmo viene calibrato in modo da garantire che sia rispettato questo periodo di tempo. Come conseguenza di questa scelta l'aumento del circolante cresce seguendo una serie geometrica che tende asintoticamente a 21 milioni. Come si può vedere dalla figura 1.3, nel 2013 il circolante di bitcoin ha raggiunto la metà dell'ammontare massimo stabilito e nel 2017 sono stati superati i due terzi del circolante finale.

[24] 21 milioni è il numero massimo di bitcoin che potrà essere raggiunto, questa cifra è stabilita a priori dal protocollo.

[25] Il mining è svolto dai "minatori" essi hanno il compito di garantire la sicurezza e l'autenticazione delle transazioni avvenute tramite Bitcoin ed allo stesso tempo sono coloro che permettono l'emissione di nuovi bitcoin. Questi temi verranno analizzati meglio al paragrafo 1.6 (Blockchain) e 1.7 (Mining).

FIGURA 1.3: Riportata da https://blockchain.info/it/charts/total-bitcoins?timespan=all, mostra l'ammontare del circolante della criptovaluta bitcoin. È la curva di emissione di bitcoin nel corso del tempo. La curva a differenza di quella teorica ha un andamento non regolare, questo perché l'emissione non avviene ad intervalli regolari di 10 minuti. Il numero di bitcoin generato decresce geometricamente, dimezzandosi ogni 4 anni. Il numero di bitcoin in circolazione non supererà mai i 21 milioni di unità. (Ultima data di consultazione 3/04/2018) All'ultima data di consultazione i BTC emessi hanno quasi raggiunto i 17 milioni di unità.

FIGURA 1.3

Secondo questo schema tutti i BTC saranno emessi entro 36,52 anni a partire dal 3 gennaio 2009 (giorno della prima generazione di BTC). In sostanza l'ultimo giorno di emissione, quando si raggiungeranno i 21 milioni di BTC, sarà il 12 luglio 2045.

Con un foglio Excel è stato possibile approssimare la funzione di emissione dei bitcoin tenendo conto degli anni bisestili ed ottenendo i seguenti risultati:

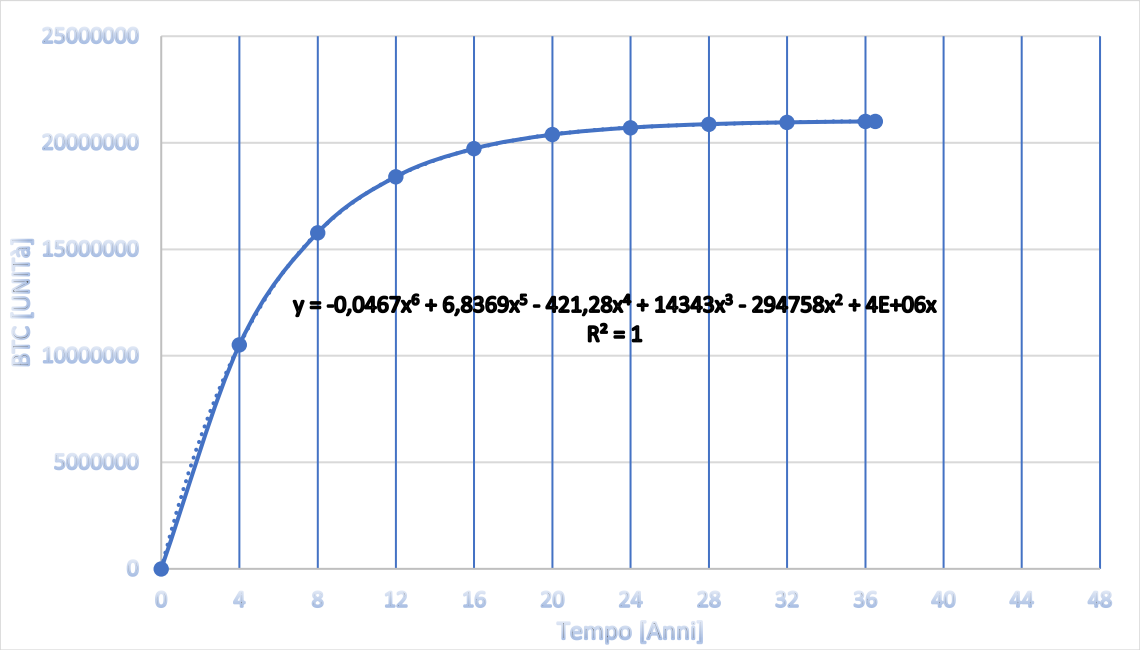
La seguente funzione, ottenuta tramite Excel, come verrà spiegato nella "Tabella 1.1", approssima l'emissione dei bitcoin ed è valida fino a che X (unità di tempo) non raggiunge i 36,52 anni, data alla quale verranno raggiunti i 21 milioni di BTC emessi:

$$y = -0{,}0467x^6 + 6{,}8369x^5 - 421{,}28x^4 + 14343x^3 - 294758x^2 4 * 10^6 x^{26}$$

In figura 1.4 è riporta una funzione che approssima l'andamento del circolante di bitcoin, effettuata attraverso Excel. Nel generarla è stato tenuto conto del fatto che venissero emessi 50 bitcoin ogni dieci minuti per i primi 4 anni. Dal quarto anno all'ottavo 50/2 bitcoin ogni dieci minuti e così via, dimezzando ogni quattro anni l'emissione, fino ad arrivare ad emettere 21 milioni di bitcoin (cifra predefinita dal sistema). Nella funzione sopra riportata basta sostituire a "X" il tempo nel quale sì vuole individuare il numero di BTC in circolazione. Come si può notare l'andamento reale dell'emissione dei BTC (in "figura 1.3") differisce dalla curva approssimata che è stata generata tramite Excel (in "figura 1.4"), questa differenza è dovuta al fatto che l'emissione dei BTC, come verrà spiegato in seguito, non avviene ad intervalli regolari di tempo. Il tempo dipende dal numero di "Minatori" e dalla potenza computazionale (potenza di calcolo dei computer utilizzati in quel momento per occuparsi del mining) che è utilizzata in quel momento. Il sistema fa sì che l'algoritmo diventi più o meno difficile da eseguite all'aumentare o al diminuire dei minatori per far modo che nell'arco di due settimane avvengano circa 2016 esecuzioni dell'algoritmo. Il numero di 2016 è stato predefinito dagli ideatori del sistema.

[26] Se alla seguente funzione si sostituisce alla X il tempo si riesce ad ottenere un'approssimazione del numero di BTC in circolazione.

FIGURA 1.4



In figura 1.4 sull'ascissa è stato riportato il tempo in anni, sull'ordinata il numero di bitcoin emessi. In questo modo è stato possibile ottenere i seguenti risultati.

La "tabella 1.1" è il foglio Excel utilizzato per il calcolo dei bitcoin emessi nel tempo e per la creazione del grafico in "Figura 1.4".

Sulla prima colonna è stato riportato l'incremento del numero di BTC per minuto; per effettuare i calcoli è stato supposto che l'emissione di bitcoin avvenga ogni 10 minuti esatti, senza tener conto delle possibili variazioni di velocità di svolgimento degli algoritmi che aumentano o diminuiscono in maniera temporanea a seconda della potenza computazionale che sta partecipando al network Bitcoin. La seconda colonna riporta i minuti che sono trascorsi per il conteggio dei 4 anni dopo i quali verrà dimezzata la quantità di BTC emessi. La terza colonna riporta il numero di bitcoin che verranno (o sono stati emessi nel caso in cui il periodo sia già trascorso) nello specifico periodo di 4 anni, tenendo conto del dimezzamento di emissione che avviene ogni 4 anni, la quarta colonna invece calcola le unità totali che sono state emesse alla fine di ogni intervallo di tempo considerato.

TABELLA 1.1

Incremento [Unità/minuto]	Minuti	Unità totali ogni 4 anni	Unità totali		Anni
0	0	0	0		0
5	2103840	10519200	10519200		4
2,5	4207680	5259600	15778800		8
1,25	6311520	2629800	18408600		12
0,625	8415360	1314900	19723500		16
0,3125	10519200	657450	20380950		20
0,15625	12623040	328725	20709675		24
0,078125	14726880	164362,5	20874037,5		28
0,0390625	16830720	82181,25	20956218,75		32
0,01953125	18934560	41090,625	20997309,38		36
0,009765625	21038400	20545,3125	21017854,69		40
		ANNI EFFETTIVI			
Numero massimo di BTC		36,52			
21000000					
Minuti effettivi 40 anni					
21038400					

3. ANONIMATO:

Le transazioni avvengono tra “indirizzi pubblici” a partire dai quali è impossibile risalire alla reale persona fisica che opera tramite quello pseudonimo. Gli indirizzi pubblici sono sostanzialmente punti di ricezione e invio dei BTC che possono essere assimilati ad una sorta di IBAN bancario. Nello specifico verranno analizzati al paragrafo 1.8.

4. TRASPARENZA:

Tutte le transazioni sono annotate in registri pubblici (consultabili da chiunque), le blockchain. Esplorando le blockchain è possibile sapere di quanti bitcoin dispone un indirizzo pubblico e sapere quale altro indirizzo glieli ha forniti. Sostanzialmente è come se ogni volta che avviene una transazione di un bitcoin tale transazione rimanesse per sempre registrata nel bitcoin stesso. Nonostante questa trasparenza, come verrà spiegato successivamente, non è possibile arrivare dalla chiave pubblica all’utente persona fisica.

5. BASSI COSTI DI TRANSAZIONE:

Il costo per ogni operazione effettuata in bitcoin è libero, ogni utente può decidere l'importo nel momento in cui effettua l'operazione. Nonostante questa libertà le commissioni si aggirano di solito attorno a 0,00001BTC. Effettuare le cosiddette "donazioni" al Minator di importi più bassi può essere rischioso per l'effettivo riuscire della transazione qualora vi siano molte operazioni nell'arco dei 10 minuti[27] nei quali si effettua la propria. I minatori nel momento in cui si occupano di autenticare le transazioni, possono scegliere quali transazioni inserire nel proprio blocco. Un blocco, come verrà spiegato nel paragrafo 1.6 dedicato alla Blockchain, rappresenta un "contenitore" all'interno del quale vengono inserite tutte le operazioni in bitcoin svolte nell'arco temporale considerato, ogni blocco può contenere un numero di transazioni limitate, il cui massimo valore è di 4200; per questo motivo transazioni con commissioni basse, possono essere lasciate per ultime, se nel periodo in cui vengono effettuate vi sono più di 4200 operazioni effettuate tramite BTC.

Costi molto più alti sono quelli di commissione che vengono posti dagli exchange che si occupano della trasformazione del Dollaro/Euro o a volte anche altre monete di corso legale in bitcoin e viceversa. Questi possono essere anche considerevoli, come analizzerò successivamente nella tesi, anche se c'è da notare che gli exchange si prendono dei rischi enormi trattando con le criptovalute, vista l'elevatissima volatilità che contraddistingue questo mercato e considerata anche la mancanza di una legislazione chiara.

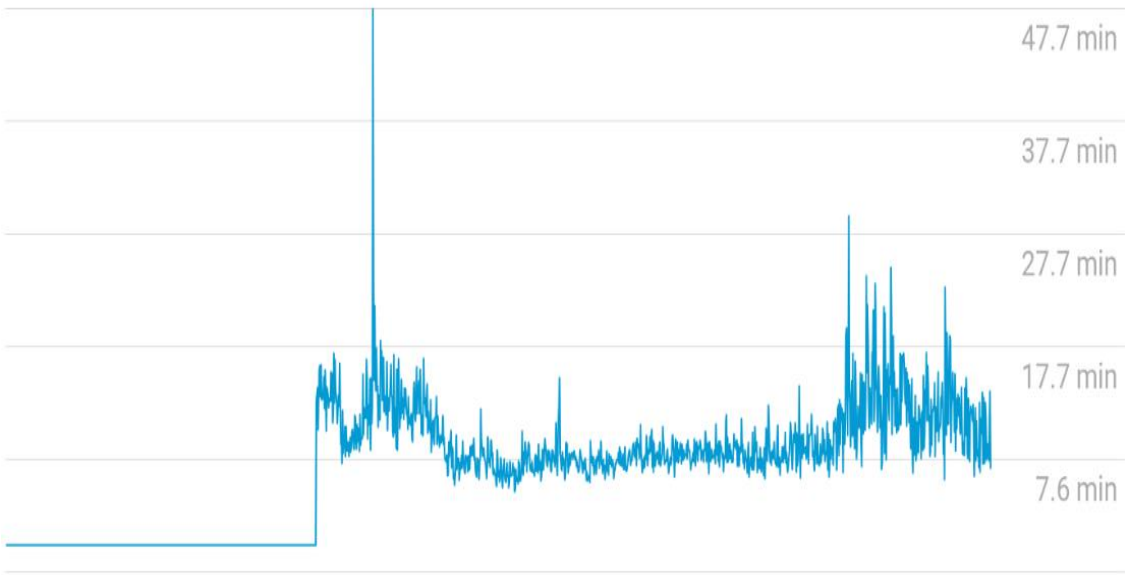
6. SICUREZZA E VELOCITA' DELLE TRANSAZIONI:

Ogni transazione bitcoin impiega mediamente 10 minuti per essere effettuata, queste transazioni sono irreversibili, impossibili da annullare.

[27] Il sistema prevede che siano autenticate le transazioni ogni circa 10 minuti, come verrà spiegato in seguito.

FIGURA 1.5: La Figura 1.5 mostra i tempi di convalida di un'operazione effettuata attraverso i bitcoin, i dati tratti da https://blockchain.info/it/charts/median-confirmation-time?timespan=all mostrano che fino al 2012 un'operazione impiegava meno di un minuto ad essere autenticata, in seguito con l'espansione e la notorietà che ha assunto il bitcoin, le tempistiche si sono stabilizzate attorno ai 10 minuti, fatta eccezione per alcuni momenti di manutenzione e miglioramento del network blockchain che hanno provocato un allungamento delle tempistiche (per esempio il 14 giugno 2012 la convalida delle operazioni ha necessitato un tempo di 48 minuti). Ad oggi ogni due settimane il sistema Bitcoin tara automaticamente il funzionamento con l'obiettivo di garantire l'autenticazione delle transazioni in un periodo di tempo di 10 minuti.

FIGURA 1.5



1.6 LA BLOCKCHAIN

La Blockchain è l'equivalente informatico di un libro mastro pubblico di tutte le transazioni in Bitcoin che sono state eseguite fino ad ora. Essa può essere pensata come una "catena" formata da un insieme di "blocchi", i quali a loro volta sono formati da un insieme di transazioni. La "catena" ha la caratteristica di registrare e archiviare[28] tutte le transazioni effettuate all'interno del network, senza la necessità di una terza parte che si occupi della gestione del sistema. Il "libro mastro" è in continua crescita con la registrazione al suo interno dei dati relativi a tutte le operazioni. I dati sono dotati di un meccanismo di difesa, basato sulla crittografia, dalle manomissioni o dalla possibilità di modifica. Le transazioni avvengono con frequenza continua nel network, mentre i blocchi sono "agganciati" alla catena mediamente ogni dieci minuti. In questo modo ogni blocco viene disposto sulla catena in sequenza cronologica a partire dal blocco originale, il cosiddetto "genesis block"[29]. Un blocco è la parte corrente della blockchain, esso può essere visto come un "contenitore" all'interno del quale sono stipate tutte le transazioni in attesa di autenticazione. Il numero di dati iscrivibili in ogni singolo blocco è definito e limitato, come già detto, ad un massimo di 4200 transazioni; una ogni sette secondi circa. Ogni blocco viene riempito di scritture contabili, coincidenti alle singole transazioni (per esempio A trasferisce a B X numero di bitcoin), le quali operano in maniera simile ad un IBAN bancario. Una volta completato ed autenticato, il blocco, viene legato alla blockchain e registrato in maniera definitiva nel database (la transazione non può essere in alcun modo annullata). La rete globale dei nodi effettua ogni circa 10 minuti il concatenamento, ovvero prima dell'autenticazione del nuovo blocco, verifica l'effettivo collegamento di tutti i blocchi della catena (tutti i blocchi dal genesis block fino all'ultimo blocco autenticato). Tramite il meccanismo appena

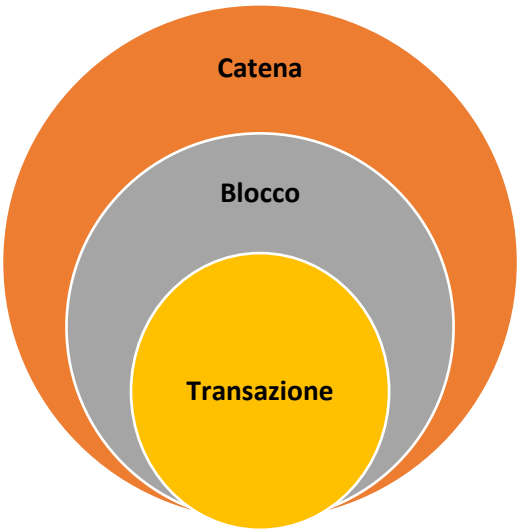
[28] La registrazione e archiviazione avviene nel web.

[29] Il "genesis block" bitcoin venne generato il 3 gennaio 2009 alle 18:15 orario di Greenwich, la prima convalida fu effettuata da Satoshi Nakamoto, e la soluzione del primo hash è la seguente: "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f". Come spiegato a pagina 12, la soluzione di un hash equivale alla riduzione di un "input" arbitrario in un output alfanumerico di un numero predefinito di caratteri.

descritto è possibile verificare in ogni momento che le transazioni siano avvenute correttamente, in modo che ogni bitcoin sia trasferito una sola volta, evitando la cosiddetta “doppia spesa”. In questo modo il funzionamento della blockchain evita che un soggetto invii uno stesso bitcoin a due individui diversi. Ogni nodo, ossia tutti i computer connessi alla rete Bitcoin, detiene una copia della blockchain, che viene scaricata automaticamente da ogni miner che si unisce alla rete Bitcoin. La struttura della catena si può quindi schematizzare come nella figura 1.6.

Le transazioni contenute all’interno dei blocchi hanno un funzionamento simile a quello della catena blockchain. La differenza sta nel fatto che le transazioni non sono collegate una all’altra secondo un ordine cronologico, ma sono legate alla precedente transazione che ha fornito al mittente i bitcoin con i quali effettua l’attuale trasferimento (l’utente che nella transazione precedente era il ricevente, nella transazione in atto diventa il mandante).

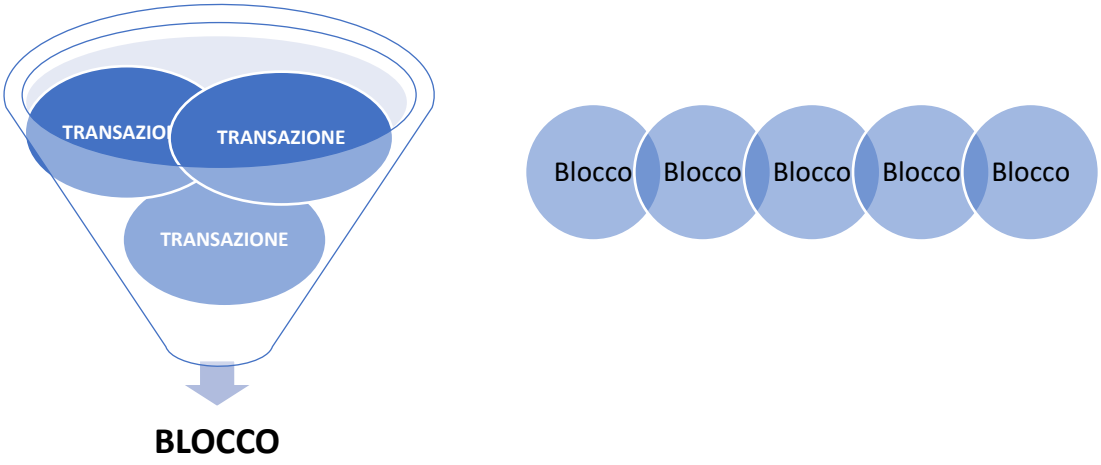
FIGURA 1.6



La Blockchain è un sistema la cui particella più piccola è la singola transazione, cioè la scrittura contabile base, l'insieme di più transazioni forma un blocco, l'insieme di tutti i blocchi la catena.

FIGURA 1.7: Come esemplificato dalla figura 1.7 tutte le transazioni avvenute nell'arco temporale predefinito formano un blocco. L'insieme dei blocchi su unisce in ordine temporale formando la catena.

FIGURA 1.7



Fino a pochi anni fa la blockchain era utilizzata solo per il funzionamento del network Bitcoin, nel senso che non si erano ancora individuati tutti i possibili ambiti applicativi a cui una simile tecnologia avrebbe potuto essere applicata. Negli ultimi anni invece, l'interesse per questa tecnologia è aumentato e numerose potrebbero essere le applicazioni future. In quest'ottica è da leggere la nascita di moltissime criptovalute, interessanti non tanto per le valute in sé, ma piuttosto per le tecnologie che sottostanno alle stesse crypto. Molto spesso infatti a "creare" la propria valuta sono società che si occupano di sviluppare una blockchain. Come verrà analizzato nel secondo capitolo, grande importanza nello sviluppo di nuove tecnologie blockchain stanno avendo le ICO (Initial Coin Offering) le quali hanno per le società che sviluppano una tecnologia

blockchain la stessa importanza e funzione che hanno le IPO[30] (Initial Public Offering) per le normali società: raccogliere capitale da reinvestire per lo sviluppo della società stessa. Per questa ragione la tecnologia blockchain ha riscontrato grande interesse dei colossi finanziari e molto spesso delle istituzioni, questo fa pensare che in futuro la "catena" possa essere applicata nella finanza (il cosiddetto FINTECH).
In un futuro non lontano quindi l'utilizzo della blockchain potrebbe essere fondamentale anche per la trasmissione di informazioni tra intermediari finanziari e le varie Autorità di vigilanza, portando da un lato una facilitazione delle procedure di controllo e conformità e dall'altro una maggiore efficienza e velocità della vigilanza.
Oltre alle applicazioni finanziarie, le applicazioni della blockchain possono essere molte altre e si muovono su un campo interdisciplinare. Grande importanza potrebbe avere un'applicazione nei contratti nel fenomeno conosciuto come REGTECH, contrazione di Regulation e Technology, cioè l'impiego di strumenti tecnologici a supporto delle procedure di adeguamento, conformità, rispetto di norme, regolamenti, leggi, reportistica.

Per meglio capire il funzionamento della blockchain è necessario introdurre il concetto di "mining" e la funzione svolta dai cosiddetti "minatori".

[30] L'IPO, letteralmente Initial Public Offering, è l'Offerta Pubblica Iniziale (al mercato) delle azioni di una società. Quando si parla di IPO si intende la prima offerta dei titoli di una società al pubblico generale degli investitori, attraverso una quotazione in borsa. Le IPO possono essere "primarie" se riguardano azioni di nuova emissione ovvero "secondarie" quando gli azionisti preesistenti decidono di monetizzare le proprie quote vendendole tutte o in parte sul mercato. Le IPO primarie sono finalizzate a raccogliere capitale per l'azienda, in modo da poter supportare gli investimenti necessari per lo sviluppo dell'azienda stessa, le IPO secondarie invece hanno lo scopo di liquidazione dei soci preesistenti, che mettono sul mercato le proprie partecipazioni.

1.7 IL MINING E I MINATORS

I "Minatori[31]" svolgono un ruolo cruciale in ogni sistema di funzionamento delle criptovalute. Essi sono i soggetti che permettono il funzionamento del network Bitcoin e, attraverso la loro partecipazione attiva, garantiscono la sicurezza del protocollo. I minatori sono responsabili del raggruppamento e dell'autenticazione delle transazioni che avvengono tramite bitcoin. La loro attività consiste nel risolvere gli "hash[32]" per l'autenticazione delle transazioni e operazioni, hanno quindi una funzione di "notai", nel senso che certificano la validità delle procedure di trasferimento dei bitcoin attraverso la creazione di nuovi blocchi da aggiungere al "libro mastro" (la blockchain). I minators forniscono la potenza di calcolo necessaria per proteggere la blockchain da possibili tentativi di sovvertimento e centralizzazione del suo funzionamento[33]. I nuovi blocchi vengono aggiunti a tempi costanti. Per garantire le tempistiche, il protocollo prevede che la difficoltà della soluzione degli hash dipenda dal numero di soggetti che si stanno occupando del mining. Indipendentemente da quante transazioni avvengono nel sistema, ogni due settimane, per previsione del protocollo Bitcoin, devono essere prodotti mediamente 2016 nuovi blocchi, circa 1 ogni 10 minuti, anche se nessuno effettuasse alcuna transazione. Ogni due settimane, se i nuovi blocchi prodotti si discostano dal numero obiettivo di 2016, la difficoltà di produzione di un nuovo blocco viene rivista verso il basso o verso l'alto, a seconda che l'output di nuovi blocchi sia stato inferiore o superiore a 2016. La difficoltà di produzione del blocco dipende dalla facilità con la quale è possibile eseguire la funzione hash.

Se il numero dei soggetti aumenta, la difficoltà della risoluzione dell'hash aumenta di conseguenza, perché aumentando la potenza computazione i minatori coinvolti nella risoluzione di un hash impiegheranno meno tempo a trovare la soluzione. Poiché il

[31] Minators, il cui nome fa riferimento all'estrazione di oro "gold mining".

[32] Come è stato spiegato precedentemente la risoluzione di un "hash" consiste nell'applicare una funzione che trasformi un "messaggio" di lunghezza arbitraria in una sequenza alfanumerica di lunghezza predefinita.

[33] Questo è possibile nel caso in cui la maggior parte della potenza di calcolo si organizzi congiuntamente, per ripercorrere tutta la blockchain e deviarla dal suo normale funzionamento.

funzionamento Bitcoin prevede che le soluzioni siano "trovate" ogni 10 minuti, è necessario che l'hash sia adeguato al numero di partecipanti alle operazioni di applicazione della funzione hash. La soluzione corretta per la continuazione della catena blockchain viene selezionata dal protocollo, e come premio per la sua generazione il "minatore" che l'ha risolta riceve un quantitativo X di bitcoin di nuova generazione più la somma di tutte le commissioni che sono state apposte nelle operazioni del blocco. Le commissioni, pur essendo libere, devono avere un importo adeguato; i minatori infatti possono decidere quali transazioni inserire nell'autenticazione, visto che da protocollo esiste un numero massimo di autenticazioni con una sola operazione di convalida (circa 4200 transazioni). Presumibilmente i minatori sceglieranno di autenticare per prime le operazioni con commissioni più generose. In questo modo una commissione inferiore a 0,00001 BTC rischia di richiedere un tempo più lungo per essere autenticata. Il pagamento di un "premio" riservato ai minatori che sostengono il network è stato pensato affinché in questo modo si disincentivano tentativi di centralizzazione del sistema, che sarebbero possibili solo con il consenso della maggioranza dei partecipanti alla piattaforma. Essendoci una ricompensa per il proprio operato, ai minatori risulta conveniente non sovvertire il sistema e continuare a lavorare per il suo mantenimento.
All'inizio, l'attività di mining poteva essere svolta con un normale computer. Tuttavia con l'aumentare dei partecipanti al network questa funzione può essere svolta solo con macchinari costosi e sofisticati, progettati e creati appositamente per svolgere questa funzione. Oggigiorno in realtà nemmeno questi tipi di apparecchi garantiscono l'efficienza nella risoluzione degli hash; il costo energetico per alimentare questo tipo di strumenti è considerevole, per questo motivo molto spesso i minators si uniscono per aumentare la probabilità di riuscire a risolvere gli hash e proseguire la blockchain. Dalla difficoltà sempre più alta di riuscire a "minare" in maniera efficiente è nato il cosiddetto "mining pool"[34].

[34] Il "mining pool" è il fenomeno attraverso il quale soggetti interessati a "minare" le criptovalute mettono in comune delle risorse per condividere il loro potere di elaborazione su una rete. Condividendo il potere computazionale essi suddividono equamente la ricompensa, in base alla quantità di lavoro che hanno apportato per la risoluzione del blocco. L'attività di "mining pool"

Secondo il sito https://blockchain.info/it/pools, il quale si occupa di raccogliere ed analizzare dati sul mondo delle criptovalute ed in particolare sui Bitcoin, il mining della più importante crypto è ormai quasi un'esclusiva di "colossi" del mining. Questi sono gruppi di minatori organizzati con l'obiettivo di dividere la capacità computazionale per riuscire ad eseguire con probabilità più alta i vari hash delle criptovalute. I gruppi si dividono il mercato in linea di massima secondo il grafico sotto riportato in "figura 1.8". Come si può vedere più di un blocco su quattro viene risolto dal gruppo conosciuto come BTC.com, altre "fette" considerevoli della torta di mining appartengono ad Antpool, BTC.TOP, Via.BTC e SlushPool. Visti i dati riportati dal sito (uno tra i più autorevoli nel mondo delle criptovalute) appare evidente che sia ormai pressoché impossibile per un singolo soggetto minare Bitcoin senza assoggettarsi ad un gruppo di riferimento con il quale condividere la potenza computazionale[35].

è iniziata nel momento in cui la difficoltà per il "mining" è aumentata al punto da richiedere anni affinché un minatore singolo potesse generare un blocco.

[35] Anche se la possibilità esiste ancora, essa può risultare poco conveniente dal punto di vista economico. Per effettuare operazioni di mining sono necessari apparecchi e schede apposite, molto potenti ed estremamente costose. Attrezzarsi per poter minare in maniera importante può venire a costare anche 50000 $ ed alle spese di attrezzatura vanno aggiunge anche quelle dell'elettricità; il computer (o i computer nel caso in cui ne siano usati più di uno) devono rimanere accesi ininterrottamente 24 ore su 24 per poter sperare di individuare un hash che venga inserito nella blockchain. Tutti questi costi ed i ricavi sempre aleatori fanno sì che le singole persone siano sempre meno interessate al mining di Bitcoin. Discorso diverso va fatto per altre criptovalute, per le quali è attualmente ancora possibile minare in maniera "artigianale" e poco onerosa.

FIGURA 1.8: Il grafico riportato da https://blockchain.info/it/pools evidenza la suddivisione della potenza computazionale all'interno del network bitcoin. Come si può notare più del 25% delle autenticazioni vengono eseguite da BTC.com che in questo senso può essere considerato un "colosso" del mining.

FIGURA 1.8

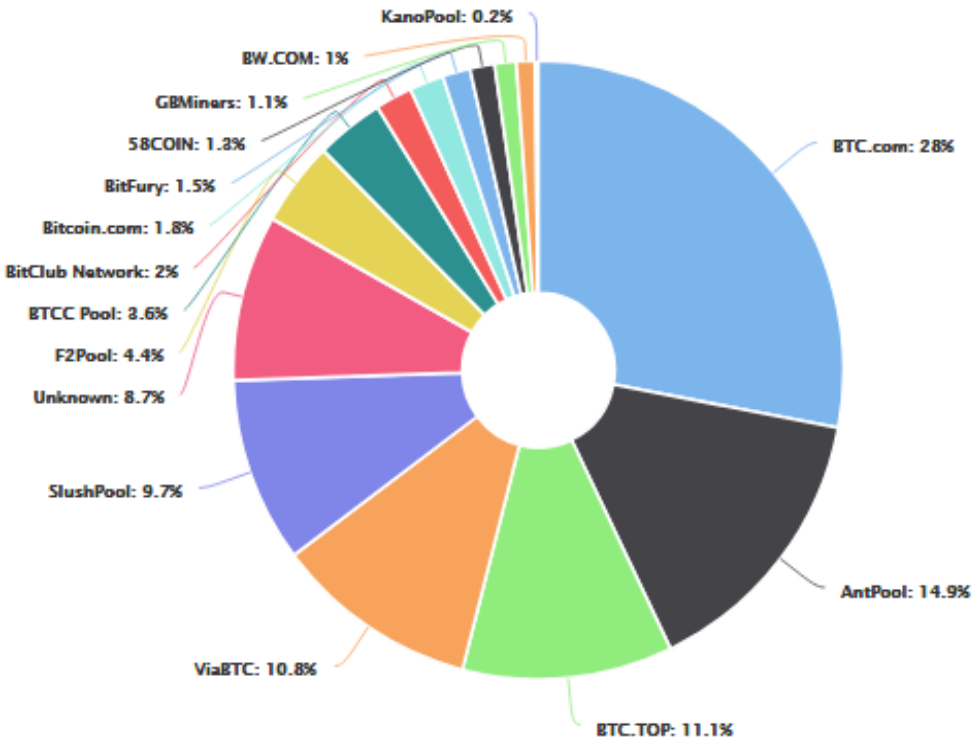
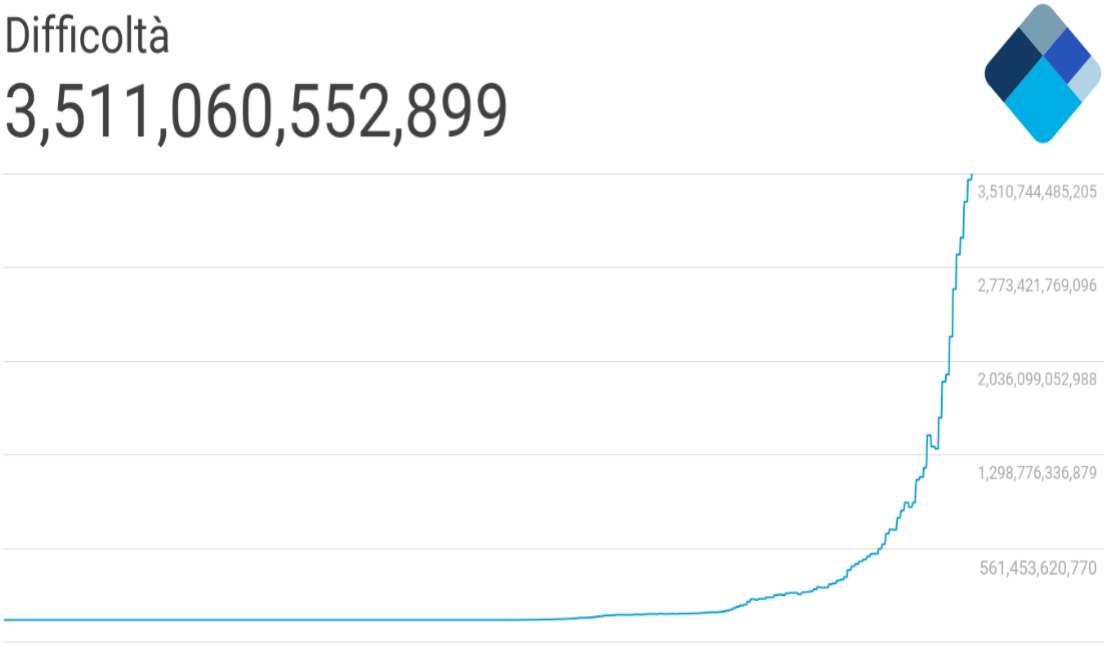


FIGURA 1.9: Riportato dal sito https://blockchain.info/it/charts, Il grafico mostra l'andamento in termini di difficoltà della risoluzione degli hash nel tempo. La difficoltà è misurata in "hashing power" il numero cioè di hash che è necessario generare per giungere a quello che risolve il problema computazionale necessario per il relativo blocco. Sostanzialmente un valore 1 di "hashing power" vuol dire che per giungere all'individuazione della combinazione hash adatta a risolvere il blocco è necessario un solo tentativo di risoluzione. Al 5/04/2018 (data di consultazione del grafico relativo alla difficoltà delle soluzioni degli hash) sono necessari 3.551.060.552.899 tentativi di combinazioni hash in media prima di giungere alla combinazione corretta per il proseguimento della catena. Questo vuol dire che attualmente la potenza computazionale che si occupa di risolvere gli hash Bitcoin in tutto il mondo genera circa 6 miliardi di combinazioni hash al secondo. Come si può notare la difficoltà e la necessità di hashing power necessaria per risolvere.

FIGURA 1.9



La difficoltà dell'algoritmo dei blocchi è aumentata in maniera che si può ricondurre ad un esponenziale, specialmente dell'ultimo periodo. La difficoltà degli algoritmi dipende dal numero di utenti che "minano" in quel momento. È presumibile pensare che quando il prezzo dei bitcoin sale molti più utenti siano interessati a minarli, visto che il costo computazionale potrà essere coperto più rapidamente.

Considerando un esempio si può presto capire quanti profitti possono essere ottenuti attraverso il mining. L'attuale premio per la risoluzione di un hash è di 12,5 BTC al quale vanno aggiunte tutte le commissioni che coloro che effettuano le operazioni in Bitcoin concedono. Se per esempio l'attuale prezzo di un bitcoin fosse 5000$, colui che risolve l'hash riceverebbe una cifra di circa 65000$, nel caso in cui un bitcoin valesse 7000$ il "minatore" che risolve l'hash riceverebbe circa 90000$. Nel momento in cui il BTC raggiunse il suo massimo storico di 20000$ per la risoluzione di un hash il minatore riusciva ad ottenere un corrispettivo fiat di 250000$.

1.8 I PORTAFOGLI (WALLET)

I portafogli (wallet) bitcoin sono simili ad un conto corrente. Essi forniscono informazioni in ogni momento riguardanti il "contenuto" del portafoglio e le operazioni di entrata e uscita avvenute nel wallet, come una sorta di estratto conto in tempo reale. Nonostante questa similitudine con i conti correnti, i bitcoin non sono realmente contenuti all'interno del portafoglio, ma sono memorizzati in un registro pubblico (la blockchain) sotto degli specifici indirizzi appartenenti ai diversi utenti. Gli indirizzi sono punti di ricezione e invio formati sostanzialmente da codici alfanumerici composti da 33 o 34 caratteri il cui primo è sempre un "1"[36].

Ogni codice non contiene alcuna informazione riguardante il cliente, ed essendo una combinazione casuale di numeri e lettere non può in alcun modo rimandare all'utente utilizzatore. Questa caratteristica fa sì che il Bitcoin sia un metodo di pagamento completamente anonimo, attraverso il quale gli utenti effettuano pagamenti con pseudonimi.

Le transazioni in bitcoin si basano sul meccanismo delle "transazioni asimmetriche", chiamato anche meccanismo chiave pubblica – chiave privata. Le due chiavi sono dei codici alfanumerici attraverso i quali è possibile eseguire le operazioni nella piattaforma Bitcoin. Ogni utente detiene una coppia di chiavi, una pubblica ed una privata. Gli indirizzi di cui si parlava prima derivano algoritmicamente dalle chiavi pubbliche, che a loro volta derivano attraverso una funzione non iniettiva dalle chiavi private. Sostanzialmente con questo meccanismo si può arrivare dalla chiave privata a quella pubblica, ma non viceversa. Dalla chiave pubblica è impossibile giungere a quella privata, in questo senso il meccanismo di transazione viene definito asimmetrico.

Attraverso il meccanismo appena descritto, partendo dall'indirizzo risulta impossibile giungere alle chiavi originali (sia alla chiave pubblica ovvero alla chiave privata) e di conseguenza all'utilizzatore del wallet.

[36] Un esempio di codice è il seguente: "*1F4TdCKjqJ6gdjghCVO7yTBy9uPHC5Klg*".

L'utente è autorizzato ad usufruire dei bitcoin presenti nel suo wallet solo nel momento in cui sia in possesso della propria chiave privata di riferimento. È quindi necessario che la chiave privata sia custodita con massimo riserbo e non sia smarrita[37]. Ogni volta che viene generato un nuovo wallet, vengono create cento (100) chiavi pubbliche che fanno riferimento ad un'unica chiave privata (kay-pool). In questo modo l'utente può usufruire di 100 indirizzi diversi collegati allo stesso wallet. La privacy viene garantita attraverso questo meccanismo perché, anche se qualcuno riuscisse ad associare un soggetto ad una chiave pubblica (cosa molto difficile) gli sarebbe impossibile risalire alle altre operazioni effettuate dallo stesso soggetto, in quanto ogni altro spostamento potrebbe essere effettuato con altre 99 chiavi pubbliche e conseguentemente con altri 99 indirizzi generati attraverso le chiavi pubbliche.

Per quanto questo tipo di operazioni possano sembrare complesse, in realtà esse sono svolte totalmente dal sistema. Il wallet infatti risulta abbastanza semplice ed intuitivo e non differisce molto da un'area riservata di un sito internet di una banca.

È possibile avere diversi tipi di wallet i quali dipendono sostanzialmente dal livello di praticità e sicurezza che l'utente desidera avere.

Il primo portafoglio, quello più comune, è il "desktop wallet". Esso consiste in un software da installare nel proprio computer. Questo tipo di portafoglio può essere rischioso, infatti se non si presta la dovuta attenzione attraverso l'inserimento di password modificate periodicamente e di antivirus sempre aggiornati, il proprio computer potrebbe essere hackerato. In questo modo sarebbe possibile recuperare la chiave privata e pertanto rubare i bitcoin detenuti nel wallet.

Il "mobile wallet" è simile al "desktop wallet", l'unica differenza è che viene installato come un'applicazione sul proprio smartphone. Lo stesso vale per il "tablet wallet" che come è evidente dal nome verrà istallato sul proprio tablet.

Il modo più rischioso da un lato, ma più pratico e veloce dall'altro, per tenere i propri bitcoin è quello del wallet on-line. Questo tipo di servizio è solitamente fornito dagli exchange, le piattaforme di compravendita on-line che si occupano di scambiare i

[37] Qualora la chiave privata venisse smarrita tutti i bitcoin presenti nel wallet verrebbero persi e sarebbero per sempre impossibili da recuperare.

bitcoin e le altre cryptocurrency con la moneta fiat. Poiché ci sono stati alcuni casi di attacchi ai server delle piattaforme degli exchange[38], detenere bitcoin on-line è fortemente sconsigliato.

L'ultima categoria di portafoglio è quello hardware; esso consiste in un dispositivo creato appositamente per custodire le chiavi private degli indirizzi bitcoin e delle altre crypto. Questo tipo di wallet si collegano al computer tramite USB (solitamente sono delle vere e proprie chiavette USB), ed interagiscono in questo modo con il software del wallet in totale sicurezza. Una volta finite le operazioni da svolgere, l'hardware wallet può essere estratto dal dispositivo computer. In questo modo non sarà possibile a nessun hacker entrare nel wallet, essendo un portafoglio scollegato dalla rete. Questo metodo di "conservazione" del portafoglio bitcoin, pur essendo meno pratico da utilizzare, è senza dubbio il più sicuro e dà la certezza all'utente che i propri bitcoin non siano rubati.

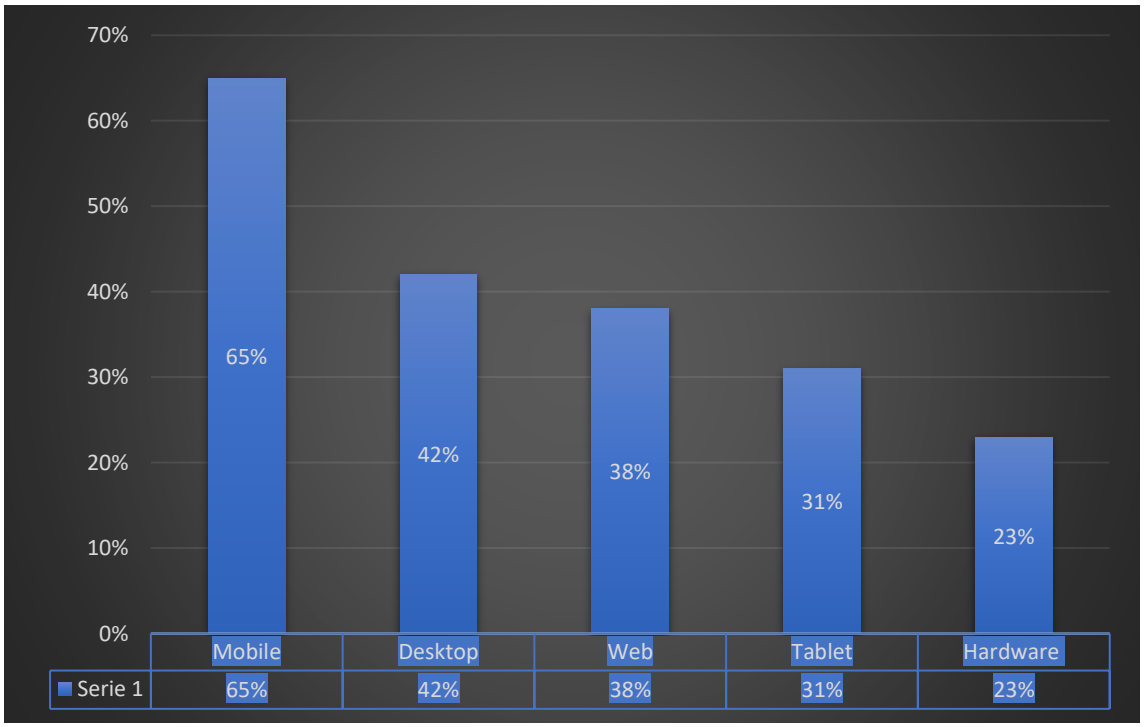
Secondo una ricerca condotta dall'Università di Cambridge per il dipartimento di "Alternative Finance" nel settembre dello scorso anno da Garrick Hilleman & Michel Rauchs l'utilizzo dei wallet sul proprio telefono è quello più frequente con il 65% degli utenti che detengono le proprie criptovalute in portafoglio di questo tipo, mentre solo il 23% utilizza hardware wallet (il metodo più sicuro per detenere cryptovalute).

MOBILE WALLET	65%
DESKTOP WALLET	42%
WEB WALLET	38%
TABLET WALLET	31%
HARDWARE WALLET	23%

[38] L'attacco più famoso è stato quello alla piattaforma Mt.Gox, con sede a Tokyo che tra il 2010 e il 2014 è stato il più grande exchange che si occupava di scambiare bitcoin e moneta fiat. Nel Aprile 2014 Mt.Gox fu costretta a chiudere a causa di un attacco hacker sul proprio server che portò alla scomparsa di più di 500000 BTC.

GRAFICO 1.1: riportato dal lavoro di Garrick Hilleman & Michel Rauchs “Global Cryptocurrency Banchmarking Study”. University Of Cambridge Centre for alternative finance 20017. Lo studio riporta le percentuali di utilizzo dei vari wallet.

GRAFICO 1.1



Pur potendo sembrare una statistica banale questa non lo è affatto. Un utilizzo così distribuito dei portafogli può indurre a pensare, come sottolineano anche i ricercatori di Cambridge, che l’interesse per le cryptovalute sia più che altro da inquadrare in operazioni di tipo speculativo ed investimento finanziario. Detenere le cripto in un “mobile wallet” infatti permette agli utenti di poter vendere ed acquistare le stesse più rapidamente rispetto ad altri sistemi, ritenuti però più sicuri. Come verrà analizzato in seguito nella tesi, l’utilizzo delle criptovalute ha preso una piega differente rispetto a quella che l’ideatore del Bitcoin aveva pensato, esse infatti sono ritenuta dagli utenti “prodotti finanziari”, nel senso più ampio del termine, ovvero vengono percepiti come opportunità di investimento.

1.9. GLI EXCHANGE

Per operare attraverso le criptovalute è quasi sempre necessario passare per i bitcoin, i quali sono riconosciuti da tutti come la crypto più importante e più liquida, nel senso che è la più facile da trasformare in moneta fiat. L'acquisto di bitcoin può avvenire in due modi: attraverso uno scambio diretto tra un soggetto che detiene bitcoin e vuole venderli ed un altro che li vuole acquistare, oppure attraverso l'intermediazione di un exchange.

Lo scambio diretto può essere organizzato anche attraverso siti come https://localbitcoins.com/, che possono di conseguenza essere considerati degli exchange, i quali si occupano di mettere in contatto i soggetti che sono interessati a vendere/acquistare bitcoin. Lo scambio può avvenire sia on-line, tramite pagamenti con bonifici bancari o PostePay oppure attraverso incontri e pagamenti elettronici in presenza fisica. Gli incontri avvengono ovviamente in luoghi provvisti di connessione internet e spesso organizzati dallo stesso sito. Per quanto riguarda il sito localbitcoins.com, esso è attivo in 15962 città in e 248 nazioni, tra le quali l'Italia, facendo così si che sia il sito leader del settore. I siti che si occupano degli scambi in presenza fisica tra soggetti in Italia hanno numerosi sedi, soprattutto al nord, dove sono presenti in quasi tutti gli ex capoluoghi di provincia. Le città con più sedi sono: Milano, Torino e Roma. Un altro modo per incontrare soggetti interessati allo scambio face-to-face di bitcoin è quello che può essere organizzato per il tramite dei social network come ad esempio bitcoin.meetup.com[39].

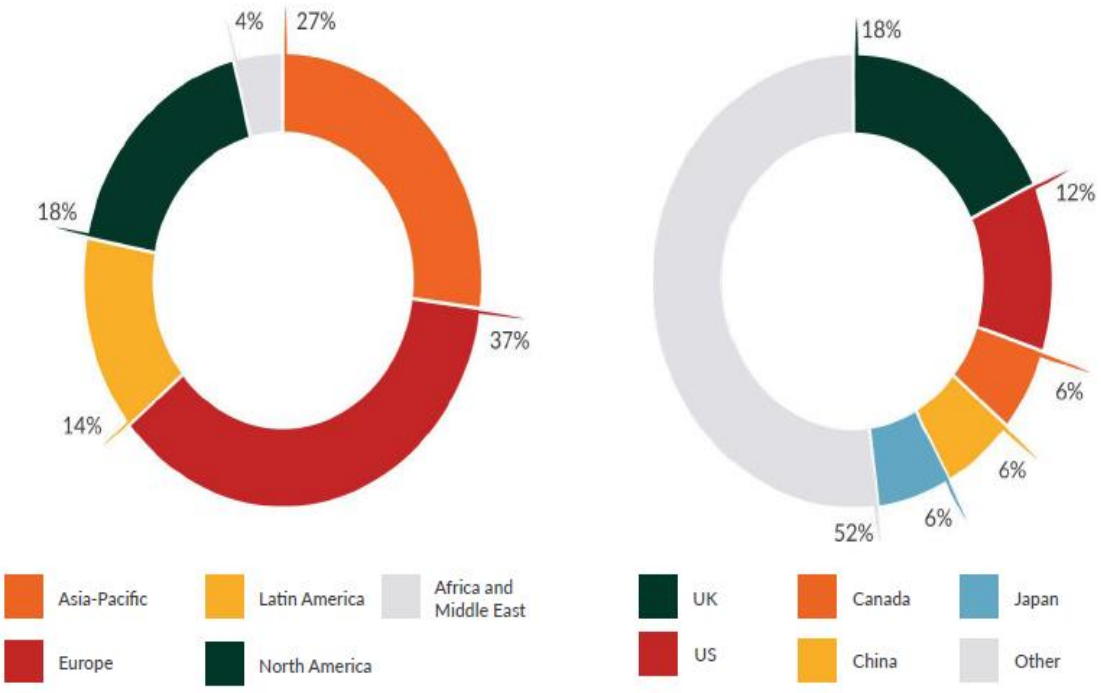
Il modo più comune per acquistare e vendere i propri bitcoin rimane in ogni caso quello di appoggiarsi ad un intermediario on-line, il vero e proprio exchange. Gli exchange forniscono servizi per la compravendita di criptovalute con valute di corso legale. Il ruolo degli exchange è fondamentale per il mercato delle monete virtuali perché essi garantiscono un mercato per il trading e la liquidità dello stesso e di conseguenza la possibilità di creare un prezzo per le varie crypto. Hanno in sostanza una funzione di

[39] https://www.meetup.com/it-IT/topics/bitcoin/.

Market Maker, cioè quella di un intermediario che “decide” quali debbano essere i prezzi di acquisto e di vendita di un determinato asset.

GRAFICO 1.2: Nel grafico a torta di sinistra è riportata la distribuzione degli exchange nelle aree geografiche di tutto il mondo, suddivise in Europa, Asia, Nord America, Sud America ed Africa e Medio Oriente. L’Europa è la prima area del mondo per numero di exchange, seguita dall’Asia. Nel grafico a torta di destra invece vengono considerati i singoli stati, il primato di numero di piattaforme di scambio di criptovalute è detenuto dal Regno Unito.

GRAFICO 1.2



Gli exchange sono stati il primo fenomeno che si è sviluppato a seguito della nascita del bitcoin. Il primo, “Bitcoin Market”, fu aperto il 6 febbraio del 2010, da allora ne sono nati a centinaia e il settore degli exchange è quello più importante in termini di volumi e di attività.

In base ai dati riportati dal sito https://bitcoinity.org/, l'Europa è il continente nel quale sono presenti il maggior numero di exchange, seguito dall'Asia e distanziando sorprendentemente di quasi 20 punti percentuali il Nord America (che considera sia USA che Canada). Per quanto riguarda i singoli stati, come mostrato nel grafico 1.2 il primato di numero di exchanges è detenuto dal Regno Unito (UK).

Secondo i dati riportati da bitcoinity.org, quelli riportati nel grafico 1.3 sono i principali exchanges in termini di volumi delle operazioni che scambiano i bitcoin e le altre criptovalute nell'ultimo anno (il 2017). Le più importanti piattaforme hanno sede in Asia (in particolar modo Giappone), Regno Unito e Malta. Nessuna delle più importanti piattaforme exchange del mondo ha la sede in Italia.

Gli exchange possono essere suddivisi in due gruppi: quelli che operano prevalentemente attraverso i bitcoin e quelli che permettono un rapido passaggio dalle varie criptovalute alle valute fiat. I primi permettono il cambio di bitcoin in tutte le altre criptovalute: il soggetto che intende operarvi quindi deve possedere bitcoin e versarli nel conto dell'exchange. Una volta depositati i bitcoin nel conto dell'exchange egli potrà acquistare tutte le criptovalute supportate dalla piattaforma per il tramite dei bitcoin. Facendo un esempio; se Luigi vuole acquistare X unità di Litecoin[40] in un'exchange che opera solo attraverso i Bitcoin, egli dovrà detenere un numero sufficiente di bitcoin nel suo conto dell'exchange per acquistare il Litecoin desiderati. Il cambio avviene quindi tra Bitcoin/Litecoin. Qualora Luigi volesse acquistare un'altra crypto con i suoi Litecoin, dovrebbe cambiare quei Litecoin i Bitcoin e poi con il tramite dei Bitcoin acquistare la criptovaluta desiderata. Anche nel caso in cui Luigi volesse cambiare i suoi Litecoin in moneta fiat (dollaro o euro) egli dovrebbe effettuare prima il passaggio per i Bitcoin. Nel momento in cui si effettua un cambio-criptovaluta nell'operazioni saranno ovviamente previste delle commissioni[41]. L'utilizzo come criptovaluta di passaggio dei Bitcoin è

[40] https://litecoin.com/it/ Il "Litecoin" è una delle principali Criptovalute, creata nel 2013, verrà trattata nel secondo capitolo.

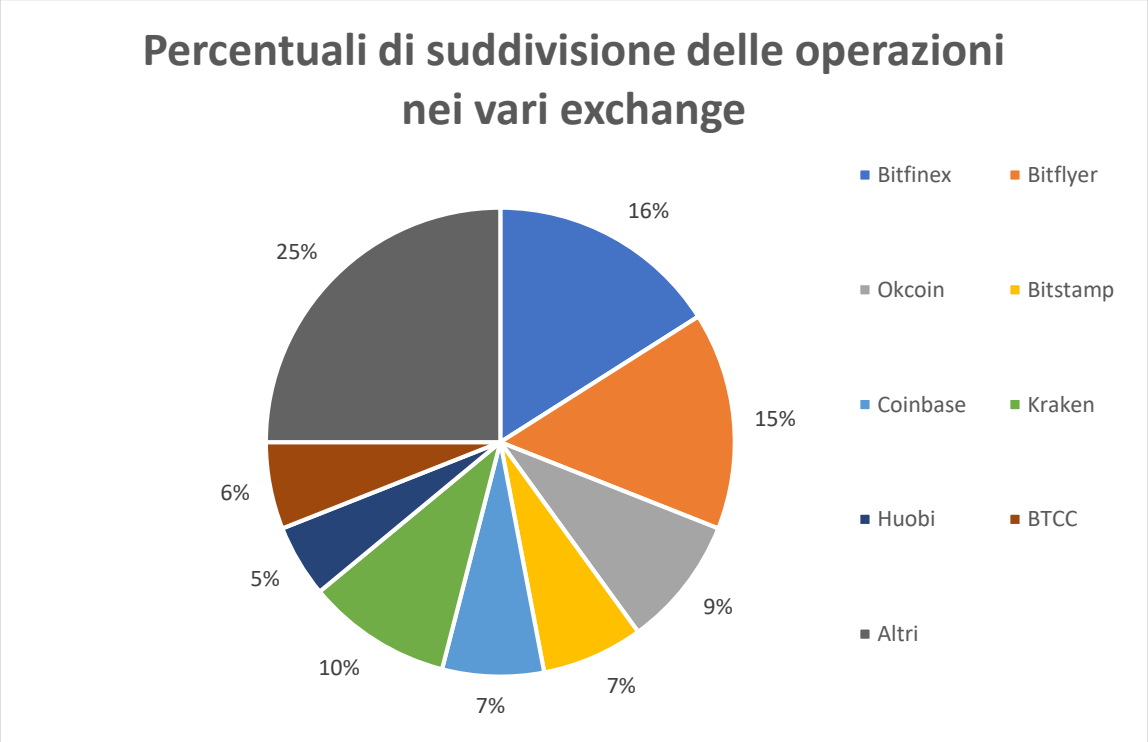
[41] In un'operazione di questo genere per l'acquisto di Litecoin a partire da dollari/euro sarebbe necessario in primo luogo scambiare la moneta fiat con i Bitcoin (in un exchange che permetta questo scambio oppure effettuando lo scambio con qualcuno che detenga Bitcoin), successivamente trasferire i Bitcoin acquistati nell'exchange e attraverso i Bitcoin acquistare il

ovviamente dovuto al fatto che il Bitcoin è la criptovaluta più conosciuta, con una capitalizzazione di mercato più alta e con una liquidità superiore. Gli exchange più famosi che operano in questo modo sono: Bitfinex (https://www.bitfinex.com/), Kraken (https://www.kraken.com/) e Bitflyer (https://bitflyer.com/en-us/).

In altri exchange è invece possibile passare direttamente dalla valuta fiat (dollaro più comunemente o in alcuni casi anche euro[42]) alla criptovaluta e viceversa. Queste piattaforme sono per esempio Coinbase[43]o Litebit.

GRAFICO 1.3: Dal grafico si può notare come Bitfinex sia l'exchange nel quale sono effettuate più transazioni, seguito da Bitflyer. Tra quelli non considerati nell'analisi va sicuramente nominato Bitterex, in ascesa nell'ultimo periodo. I dati fanno riferimento a tutto l'anno 2017.

GRAFICO 1.3



Litecoin desiderati. Nel momento in cui si volesse effettuare la stessa operazione al contrario il procedimento sarebbe il medesimo.

[42] Questo è il caso di https://www.litebit.eu/en uno dei pochi exchange che permette il passaggio immediato dalla criptovaluta desiderata all'Euro e viceversa.

[43] https://www.coinbase.com/

TABELLA 1.1

TIPO DI ATTIVITA’	DESCRIZIONE
Order-Book Exchange	Piattaforma che abbina gli ordini di acquisto e quelli di vendita degli utenti. Può anche favorire l’incontro fisico dei soggetti e lo scambio diretto delle criptovalute.
Brokerage Service	Servizio che consente agli utenti di acquisire e /o vendere le criptovalute ad un dato prezzo.
Trading Platform	Piattaforma che permette di acquistare criptovalute o ETF delle stesse, anche in leva. L’utente opera solo con la piattaforma, non vi sono operazioni tra utenti.

Nella tabella 1.1 sono riportati i tipi di exchange e quali siano le funzioni che essi svolgono. Alcune piattaforme di scambio criptovalute svolgono tutte e tre le mansioni elencate, altri invece solo una di esse. Il primo, l’”Order-Book Exchange”, ha la funzione di “Order” nel senso che funge semplicemente da intermediario. L’exchange non acquista in proprio criptovalute, ma abbina ordini di acquisto e di vendita, il loro guadagno deriva unicamente dalle commissioni; in sostanza l’exchange non si espone in prima persona nell’acquisto e nella vendita delle criptovalute, la transazione viene effettuata dai due soggetti in maniera diretta. L’’intermediario li fa unicamente “incontrare”. Questo tipo di funzione può essere anche finalizzata all’incontro fisico delle persone che vogliono scambiare criptovalute, nel modo che è stato spiegato prima. Il “Brokerage Service” è la vera e propria funzione di “Broker”. L’intermediario riceve un ordine di acquisto e vendita dall’utente e “va sul mercato” per eseguirlo. Anche in questo caso il rischio è minimo e il guadagno deriva da commissioni; la differenza con il primo exchange sta nel fatto che nel Brokerage Service l’exchange non unisce la domanda all’offerta ma si occupa in maniera diretta di acquistare/vendere per conto del

cliente. L'ultimo tipo di exchange è invece quello più rischioso, le "Trading Platform" detengono criptovalute nei loro portafogli ed effettuano l'acquisto/vendita come diretto venditore/acquirente del cliente. La piattaforma è uno dei due soggetti che effettuano l'operazione (o è il venditore o è il compratore). In questo ultimo caso di exchange, la piattaforma si assume un rischio molto elevato perché si espone alla possibilità che le criptovalute si svalutino o si rivalutino; il rischio è per di più accentuato dall'elevatissima volatilità che contraddistingue il mercato delle criptovalute. In quest'ottica vanno lette le considerevoli commissioni richieste in ogni operazione (nelle piattaforme più sicure e con un servizio efficiente come Coinbase[44] si aggirano attorno al 3,5% per ogni operazione, sia di acquisto che di vendita, oltre ad un prezzo di acquisto/vendita più alto, nel caso di acquisto, o più basso, nel caso di vendita, rispetto a quello che si trova in altri exchange).

Dopo aver individuato ed analizzato brevemente il mondo delle criptovalute; soffermandosi sui momenti cardine della loro nascita e sulle caratteristiche della prima criptovaluta, il Bitcoin, l'obiettivo del prossimo capitolo sarà quello di selezionare e spiegare i tratti distintivi delle principali criptovalute che sono scambiate nel mercato in questo momento. Su di esse è necessario concentrarsi per analizzare le innovazioni tecnologiche che hanno sviluppato rispetto al Bitcoin ed in particolare le innovazioni riguardanti la blockchain. Come sarà spiegato in seguito, sono nate altre tecnologie di blockchain che, pur partendo dagli stessi presupposti, si differenziano in maniera sostanziale dalla tecnologia che è alla base dei Bitcoin, ed hanno avuto un notevole interesse per i potenziali ambiti di applicazione alle quali possono essere adattate.
A mio avviso vanno sempre letti, almeno in parte, in quest'ottica (quella degli ambiti potenziali applicativi) il fervore e la dirompente salita e dei prezzi del mercato delle

[44]Coinbase è una società che si occupa dello scambio di criptovalute; la sede legale ed amministrativa è a San Francisco in California (Stati Uniti). La società è stata fondate nel giugno 2012 da Brian Armstrong e Fred Ehrsam. Opera scambio di Bitcoin (BTC), BitcoinCash (BCH), Ethereum (ETH), Litecoin (LTC) e altri beni digitali con valute di corso legale in 32 nazioni, e con transazioni bitcoin e di deposito in 190 nazioni.

criptovalute alla fine del 2017. Se è vero infatti che negli ultimi tempi c'è stata una notevole speculazione, è altrettanto vero che nonostante le cadute del prezzo il mercato delle criptovalute mantiene comunque livelli considerevoli; le capitalizzazioni di mercato rimangono alte e tali da non poter essere spiegate semplicemente con la speculazione.

CAPITOLO 2

Le principali criptovalute

La caratteristica principale del progetto Bitcoin è quella di essere open-source, cioè di permettere a chiunque partecipi al network di introdurre interventi migliorativi alla piattaforma. Se da un lato questa caratteristica è stata uno dei sui punti di forza, tramite il quale è stato possibile un continuo miglioramento ed efficientamento del network con il contributo degli sviluppatori da tutto il mondo, dall'altro lato si è rivelato come una debolezza perché ha fatto si che fosse possibile la nascita di nuove criptovalute concorrenti al BTC che, in maniera diversa, hanno sfruttato le informazioni pubbliche alla base della piattaforma Bitcoin.

Le criptovalute create successivamente al Bitcoin, si possono dividere in tre gruppi: le "Altcoin" (ovvero "Alternative Coin", alternative appunto al Bitcoin), le "Criptovalute Innovative" e le "Criptovalute piattaforme". Le prime vengono sviluppate o in maniera diretta dal Bitcoin con "fork[45]" del progetto, cioè come "espansione" di un progetto software nuovo che parte dal codice sorgente[46] di un altro già esistente (in questa circostanza da quello del Bitcoin), oppure vengono sviluppate dall'inizio, ripercorrendo o addirittura copiando, quasi interamente il protocollo dei BTC. Le Altcoin quindi

[45] Cosa sia un fork è già stato spiegato nel paragrafo 1.1.

[46] Il codice sorgente, detto anche semplicemente "codice" o "sorgente" è, in gergo informatico, il testo di un algoritmo di un programma scritto in linguaggio di programmazione da un programmatore.

possono essere descritte come criptovalute che non introducono innovazioni sostanziali o importanti né alla procedura Bitcoin né alla blockchain; sono in pratica delle copie di Bitcoin. Si possono trovare centinaia di esempi di Altcoin[47]. Per citarne alcuni si può ricordare: "Namecoin[48]" la seconda criptovaluta, nata da un fork di Bitcoin nell'aprile del 2011, "Dogecoin[49]", "Dash[50]" o la più recente "Bitcoin Cash[51]". Come già detto, le Altcoin non presentano migliorie sostanziali al Bitcoin, ma alcune di esse hanno l'obiettivo di superare dal punto di vista dell'efficienza alcune lacune della tecnologia Bitcoin. Solo per fare un esempio, i tempi necessari per un trasferimento di Bitcoin sono relativamente lunghi se si considerano quelli impiegate da criptovalute nate successivamente; per ovviare a questa problematica alcune crypto hanno ridotto i tempi previsti per l'autenticazione dei blocchi ad intervalli di tempo più ridotti (anche sotto il minuto).

[47] Come si può vedere nel sito https://coinmarketcap.com/all/views/all/, delle più di 1500 criptovalute esistenti, circa il 40% sono Altcoin, o fork diretti del Bitcoin, oppure Altcoin che vengono create da zero copiando quasi totalmente il protocollo Bitcoin, introducendo solo dei cambiamenti minimi.

[48] Namecoin, https://namecoin.org/, è una criptovaluta nata nell'aprile 2011, la prima "Altcoin" a venire alla luce, nonché seconda criptovaluta in assoluto. Nel sito ufficiale viene definita come "una tecnologia sperimentale open source che migliora il decentramento, la sicurezza, la resistenza alla censura, la privacy e la velocità di alcuni componenti dell'infrastruttura Internet come DNS e identità."

[49] Dogecoin, http://dogecoin.com, è una delle prime criptovaluta "Altcoin" nata nel gennaio 2014. Come si può notare dal sito essa non fornisce alcuna innovazione rispetto al Bitcoin e punta tutto su un marketing importante basata sull'immagine di un cane. Per coloro che operano nel mondo delle criptovalute è considerata una "criptospazzatura". Il suo prezzo è sempre stato inferiore al centesimo di dollaro, anche se nel periodo di massimo valore gli si è avvicinato fortemente.

[50] Dash, https://www.dash.org/, conosciuta precedentemente come "Darkcoin" è nata nel gennaio 2014 e varrà analizzata meglio in questo capitolo. Pur essendo un'Altcoin ha una capitalizzazione di mercato considerevole e viene spesso utilizzata per i pagamenti visto la velocità con la quale possono essere effettuate le transazioni (viene generato un blocco ogni minuto).

[51] Bitcoin Cash, https://www.bitcoincash.org/, è uno dei più recenti fork di Bitcoin, nato ad inizio del 2017. Nonostante sia stato generato da poco ha già accumulato una notevole capitalizzazione di mercato, è la quarta crypto in classifica per questo parametro.

Le "Criptovalute Innovative", al contrario della Altcoin, sono monete virtuali il cui funzionamento, pur partendo dai principi del Bitcoin è innovativo. L'innovazione può stare nel fatto che la blockchain sia concepita in maniera differente, come nel caso di "Iota[52]", ovvero possono differire in maniera sostanziale altre caratteristiche della criptovaluta; questo è il caso di "Ripple[53]" che, per esempio, è una criptovaluta "centralizzata", nel senso che è controllata da un soggetto centrale terzo.

Infine, le "Criptovalute piattaforme", quali per esempio "Ethereum[54]", come verrà spiegato in seguito, consentono la creazione di "contratti intelligenti" (smart contracts[55]). Ethereum è la seconda criptovaluta per capitalizzazione di mercato[56] dopo Bitcoin ed è considerata, per l'innovazione sostanziale che ha introdotto, una criptovaluta 2.0. L'innovazione sostanziale di Ethereum sta nel fatto che oltre ad essere

---

[52] Iota, https://iota.org/, "Next Generation Blockchain" è una criptovaluta innovativa. Il suo contenuto innovativo è nella blockchain. Come verrà meglio analizzato nel capitolo la sua blockchain è diversa da quella Bitcoin perché non è unica (non ne esiste una sola), ma esiste una blockchain per ogni possessore della crypto Iota.

[53] Ripple, https://ripple.com/, è considerata da alcuni una "non criptovaluta". La sua caratteristica di essere una crypto centralizzata la fa estraniare infatti dalle altre criptovalute. È stata recentemente accostata ad alcune tra le principali banche Europee, tra le quali anche Unicredit, perché sembra stia per essere sperimentata come criptovaluta utilizzabile dalle banche per le operazioni tra di esse. Utilizzando una criptovaluta come Ripple le operazioni quali per esempio i bonifici bancari che gli utenti effettuano tra due banche diverse, che attualmente possono richiedere alcuni giorni per essere eseguiti, potrebbero essere eseguiti in maniera quasi immediata o comunque impiegando pochi minuti.

[54] Ethereum, https://www.ethereum.org/, è la prima criptovaluta piattaforma (criptovaluta 2.0).

[55] Gli "smat contract" sono protocolli di tipo informatico atti a facilitare, verificare, o far rispettare la negoziazione o l'esecuzione (che può essere sia parziale che totale di un contratto). Sostanzialmente sono dei contratti che vengono eseguiti in maniera automatica da un sistema. Con dei contratti di questo tipo molti tipi di clausole contrattuali sono rese parzialmente o integralmente automatiche o auto-ottemperanti. Gli smart contract aspirano ad assicurare una sicurezza superiore alla contrattualistica esistente (quella standard) e a ridurre i costi di transazione associati alla contrattazione. Pur avendo molto potenziale, dal punto di vista applicativo i contratti intelligenti sono utilizzati in pochissimi ambiti. Il loro sviluppo ed utilizzo nel futuro, a mio parere, sarà sicuramente inevitabile.

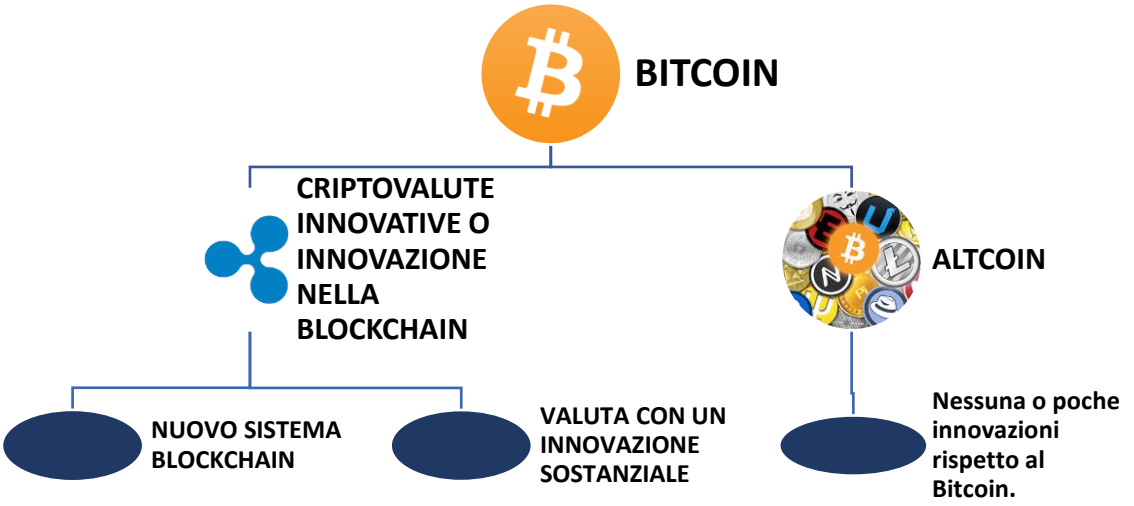
[56] La capitalizzazione di mercato della criptovalute viene calcolata moltiplicando il numero di criptovaluta in circolazione per il prezzo medio con il quale si può scambiare tale criptovaluta. Essa viene calcolata minuto per minuto, quindi vengono utilizzati i prezzi medi delle ultime 24 ore. Attualmente le prime tre posizioni sono occupate da Bitcoin, Ethereum e Ripple.

un criptomoneta è anche una piattaforma all'interno della quale possono essere sviluppate "applicazioni[57]" e posso girare altre criptovalute.

Tutte le criptovalute sono una piattaforma (anche Bitcoin lo è), ma tale piattaforma può essere utilizzata esclusivamente per le transazioni che avvengono per il tramite della criptovaluta che è nata in quella piattaforma specifica. Le "Criptovalute 2.0", invece, hanno una piattaforma programmata per essere condivisa con coloro che vogliano utilizzarla; essa è quindi utilizzata sia per le transazioni della criptovaluta principale della piattaforma, che come piattaforma adatta ad esercitare le funzioni sopra esposte. Il funzionamento della piattaforma Ethereum ed in generale delle piattaforme delle criptovalute 2.0 verrà in seguito spiegato in questo capitolo.

FIGURA 2.1: Come spiegato nel paragrafo precedente la figura illustra la classificazione delle criptovalute diverse dal Bitcoin. La differenza tra Altcoin, Criptovalute innovative e Criptovalute Piattaforma sta appunto nella portata innovativa che possiede la criptovaluta specifica.

FIGURA 2.1



[57] Intesi come applicazioni simili a quelle che è possibile installare negli smartphone o nei tablet. Esse sono sostanzialmente dei "programmi" che possono essere sviluppati all'interno della piattaforma Ethereum.

Oltre alla distinzione sopra fatta, va introdotta un'ulteriore differenziazione delle crypto, in base non più alla tecnologia sottostante, ma riguardante la piattaforma sulla quale operano. Da questo punto di vista esistono due tipi di criptovalute: le "Coin" e i "Token". Le "Coin" sono criptovalute indipendenti, il cui funzionamento non dipende da nessun'altra criptovaluta, possiedono una propria blockchain ed un proprio network. I "Token", al contrario, sono criptovalute che operano nella stessa piattaforma di una "Coin", e sostanzialmente dipendo direttamente da quella "Coin". I Token non hanno una propria blockchain ed una piattaforma propri, ma sono sviluppate all'interno della blockchain e della piattaforma di una Coin. Questo tipo di criptovalute può essere sviluppata solo all'interno di una piattaforma delle criptovalute 2.0, ovvero crypto come Ethereum o NEO[58].

Solo per fare un esempio, si consideri la criptovaluta NEO, che verrà tratta in seguito. A coloro che possiedono NEO è attribuito a periodi predefiniti di tempo un ammontare proporzionale di un'altra crypto, "Token" di NEO, il "GAS". Sostanzialmente, con meccanismi come questo, viene attribuito al possessore di una determinata crypto una sorta di "dividendo" sotto forma di un'altra criptovaluta "Token" di quella detenuta. Altri Token, pur girando all'interno della piattaforma di una Coin, possono essere sviluppati in maniera indipendente dalla Coin, quindi senza che siano generati e forniti come "dividendo[59]" ai possessori della Coin principale della piattaforma. Un esempio di questo può essere EOS[60], il Token più importante a livello di capitalizzazione di mercato, che è stato sviluppato nella piattaforma Ethereum, ma indipendentemente dalla Coin Ethereum. La piattaforma che sta avendo più successo per la sua operatività in Token è senza dubbio Ethereum. Se si visita il sito https://coinmarketcap.com/tokens/, otto dei

58 NEO, https://neo.org/ , viene descritto nel sito ufficiale come "An Open Network For Smart Economy" è la seconda piattaforma più importante dopo Ethereum ed è stata fondata da un team di sviluppo cinese nel febbraio 2014.

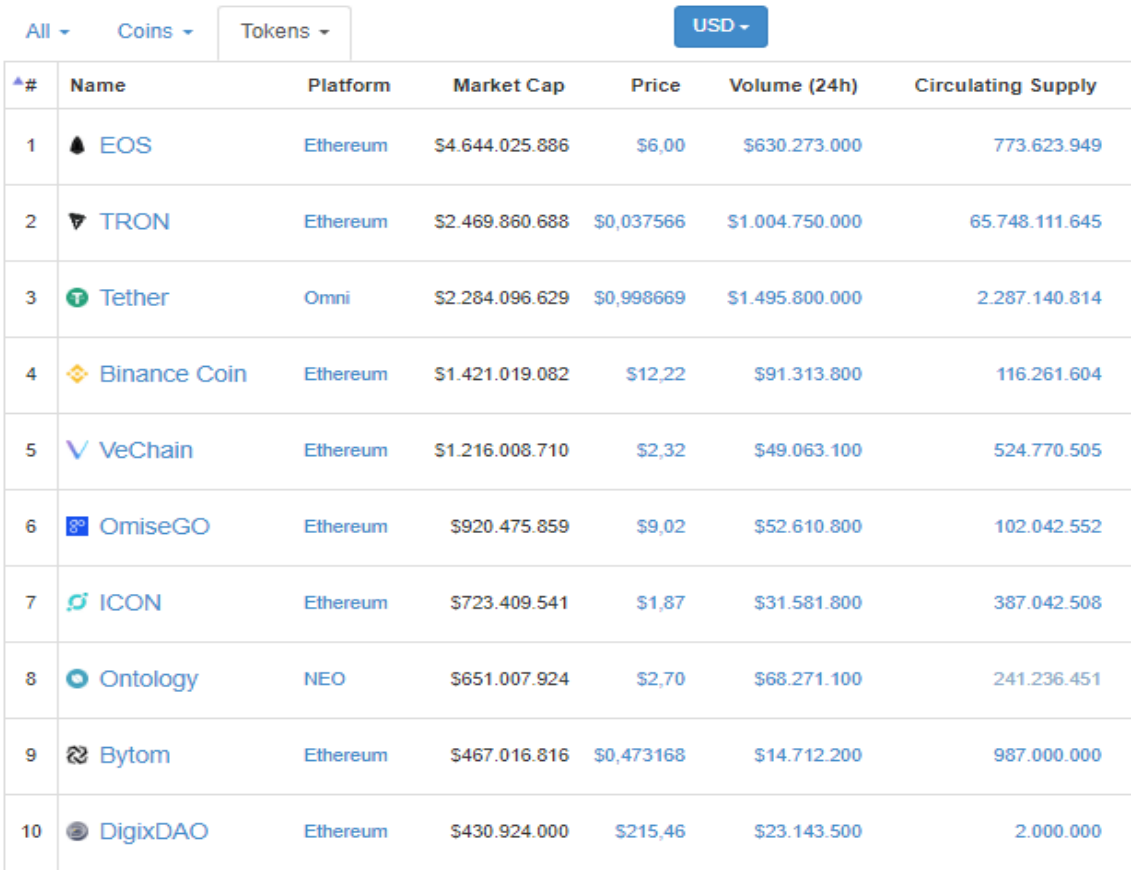
59 Il dividendo ha sostanzialmente la funzione di invogliare gli investitori a detenere la criptovaluta principale, con l'incentivo appunto di ottenere in cambio un "Token" che in alcune circostanze può avere un valore di mercato importante.

60 EOS https://eos.io/ è il più importante Token per quanto riguarda la capitalizzazione di mercato. È stato sviluppato nel 2017 a partire dalla piattaforma Ethereum.

primi dieci Token in base alla capitalizzazione di mercato “girano” sulla piattaforma Ethereum.

FIGURA 2.2: In “figura 2.2” è riportata la classifica ordinata per capitalizzazione di mercato dei primi 10 Token il 6/04/2018. Nella seconda riga è possibile individuare quali siano le piattaforme nelle quali “girino” i vari Token. Come già detto ben otto delle prime dieci funzionano per il tramite di Ethereum. Altre piattaforme utilizzate sono quella di “Omni” e di NEO.

FIGURA 2.2



#	Name	Platform	Market Cap	Price	Volume (24h)	Circulating Supply
1	EOS	Ethereum	$4.644.025.886	$6,00	$630.273.000	773.623.949
2	TRON	Ethereum	$2.469.860.688	$0,037566	$1.004.750.000	65.748.111.645
3	Tether	Omni	$2.284.096.629	$0,998669	$1.495.800.000	2.287.140.814
4	Binance Coin	Ethereum	$1.421.019.082	$12,22	$91.313.800	116.261.604
5	VeChain	Ethereum	$1.216.008.710	$2,32	$49.063.100	524.770.505
6	OmiseGO	Ethereum	$920.475.859	$9,02	$52.610.800	102.042.552
7	ICON	Ethereum	$723.409.541	$1,87	$31.581.800	387.042.508
8	Ontology	NEO	$651.007.924	$2,70	$68.271.100	241.236.451
9	Bytom	Ethereum	$467.016.816	$0,473168	$14.712.200	987.000.000
10	DigixDAO	Ethereum	$430.924.000	$215,46	$23.143.500	2.000.000

Riassumendo quanto detto fin ora, le criptovalute si differenziano per quanto riguarda la portata innovativa rispetto al Bitcoin in: “Altcoin”, “Criptovalute innovative” e “Criptovalute piattaforma”. A loro volta le “Criptovalute innovative” possono essere innovative per due aspetti: 1) per quanto riguarda il funzionamento della blockchain, come avviene per esempio Iota; 2) per quanto riguarda la caratteristica fondamentale della decentralizzazione, come il caso di Ripple che è una crypto centralizzata.

L’ultima categoria è quella delle “Criptovalute 2.0”, per esempio Ethereum e NEO; esse, come detto, non sono solamente delle crypto ma sono anche delle piattaforme all’interno delle quali è possibile operare e sviluppare, “contratti intelligenti”, applicazioni e altre criptovalute (i cosiddetti Token). Le criptovalute che operano all’interno di piattaforme di un’altra criptovaluta si differenziano dalle normali crypto. Si definiscono “Coin” le criptovalute tradizionali, quelle cioè che possiedono una propria blockchain ed una propria piattaforma all’interno della quale possono operare in maniera indipendente. Si definiscono “Token” invece, quelle crypto che funzionano per il tramite di una piattaforma altrui, quella delle criptovalute 2.0, e quindi risultano essere dipendenti da tale piattaforma.

Considerando il ginepraio che imperversa nel mondo crypto, ritengo sia necessario analizzare le categorie di criptovalute una alla volta, spiegandone le caratteristiche. Per ogni categoria crypto analizzata verranno inoltre studiate le principali criptovalute appartenenti a tale categoria.

2.1. CARATTERISTICHE DELLE CRIPTOVALUTE

Prima di procedere con la spiegazione delle categorie delle criptovalute, è utile introdurre alcuni concetti fondamentali che verranno utilizzati per analizzare le varie criptomonete. Prima di tutto va detto che di qui in avanti tutti i dati utilizzati e le informazioni riguardanti quotazioni di mercato, capitalizzazione di mercato, volume degli scambi, ecc… faranno riferimento a quanto riportato dal sito coinmarketcap.com/. La scelta del sito, il più autorevole e completo tra quelli che si occupano del mercato delle criptovalute, è stata quasi obbligatoria. Il sito infatti è l'unico che fornisca informazioni per tutte le circa 1500 criptovalute esistenti in questo momento. Anche la piattaforma Bloomberg[61], pur essendo stata consultata per alcuni confronti e ricerche, non fornisce con la stessa puntualità e completezza le informazioni sulle criptovalute considerate in questa tesi.

Il sito CoinMarketCap è comunque abbastanza completo ed affidabile, unisce le quotazioni giornaliere di tutti gli exchange, fornendo una media del prezzo della singola criptovaluta che può essere individuata come una buona approssimazione della valutazione di mercato.

[61] Bloomberg è stata consultata più volte, ma all'8 aprile 2018 possedeva quotazioni di mercato riguardanti solo 4 criptovalute (Bitcoin, Ripple, Litecoin ed Ethereum). Le informazioni relative a tali criptovalute riguardavano unicamente la quotazione di mercato (ripartita in "Bid" ed "Ask", e per Bitcoin e Ripple anche aggregata in un unico prezzo), senza far alcun riferimento alla capitalizzazione di mercato, ai volumi correnti degli scambi e conseguentemente senza fornire alcun dato relativo alla liquidità della criptovaluta considerata. Per tale motivo, oltre che per la scarsa disponibilità di criptovalute considerate (solo 4 su 1500), è stato deciso di non utilizzare Bloomberg come riferimento per i dati in seguito utilizzati nella tesi.

2.1.1. CAPITALIZZAZIONE DI MERCATO

Il primo concetto che verrà utilizzato per l'analisi delle criptovalute è quello di "Capitalizzazione di Mercato" (Market Cap in inglese).
La capitalizzazione di mercato della criptovaluta viene calcolata moltiplicando il numero di unità di criptovaluta in circolazione con il prezzo medio di mercato di tale crypto. Nel caso del sito CoinMarketCap il prezzo medio di mercato viene calcolato come media ponderata dei prezzi proposti su tutti gli exchange che detengono tale criptovaluta[62].

La capitalizzazione di mercato viene quindi calcolata come nella seguente formula:

$$\boldsymbol{CdM = NCE \times \ PMM}$$

CdM = Capitalizzazione di Mercato;

NCE = Numero di unità di criptovaluta emessa fino a quel momento;

PMM = Prezzo medio di mercato della criptovaluta in questione, calcolata tenendo conto dei prezzi degli exchange che scambiano tale cripto.

È possibile fare un parallelo in questo senso, con la capitalizzazione di mercato delle azioni negoziate nei mercati regolamentati. La capitalizzazione di mercato delle criptovalute viene calcolata in modo analogo; si tende in questo senso ad equiparare le criptovalute a strumenti finanziari utilizzati come azioni. Come sarà visto in seguito, in realtà, le criptovalute, non sono affatto azioni delle società che le emette. Coloro che

[62] Pur essendo molti, il numero degli exchange è comunque limitato. È quindi ancora possibile calcolare un prezzo di mercato tenendo in considerazione tutti gli exchange che scambiano la criptovaluta presa in considerazione. Nel sito CoinMarketCap è possibile vedere nel giorno considerato la percentuale degli scambi che stanno avvenendo in quel momento in ognuno degli exchange sulla criptovaluta presa in considerazione.

detengono una criptovaluta infatti non diventano proprietari di tale società, ma possiedono semplicemente un "asset" emesso dalla società stessa. Questo asset però è diverso da tutti gli asset conosciuti dal diritto. Non è né un'azione, né un'obbligazione né uno strumento finanziario ibrido.

2.1.2 VOLUME DEGLI SCAMBI

I volumi rappresentano l'insieme delle operazioni di compravendita effettuate su una criptovaluta in una determinata unità di tempo (nel caso del sito CoinMarketCap, i volumi vengono calcolati nelle ultime 24 ore). Con riferimento ai titoli negoziati nel mercato regolamentato, e conseguentemente anche alle criptovalute, i volumi possono essere interpretati come l'espressione dell'interesse che gli investitori ripongono in un determinato titolo o in un determinato mercato. I volumi sono inoltre un indicatore per quanto riguarda il dinamismo del mercato e danno anche un'informazione sulla relazione che esiste tra domanda ed offerta. Oltre a quanto appena detto, l'analisi del volume di mercato è interessante per lo studio delle criptovalute perché fornisce un'indicazione approssimativa della liquidità della moneta digitale considerata.

Secondo coloro che svolgono analisi tecniche[63] il volume è una misura dell'intensità o della pressione che sta alla base di una tendenza[64]. Maggiore è il volume più affidabile e duraturo sarà il trend in atto. Alcuni osservatori dei mercati finanziari attribuiscono a questi un comportamento "fisico", immaginando che le traiettorie seguite dai prezzi sul grafico siano governate da leggi simili a quelle che regolano il movimento di un corpo

[63] L'analisi tecnica (AT) consiste nello studio dell'andamento dei prezzi dei mercati finanziari, attraverso l'utilizzo di metodi grafici e statistici. L'analisi ha l'obiettivo di prevedere il comportamento futuro dei prezzi. Essa viene utilizzata, congiuntamente all'analisi fondamentale, per la definizione delle decisioni di operatività finanziaria. L'analisi fondamentale, differentemente da quella tecnica, ha l'obiettivo di stabilire il prezzo corretto di un titolo in base alle caratteristiche economico-finanziarie intrinseche della società o dell'emittente date titolo.

[64] La tendenza o trend indica l'andamento di un determinato titolo o di un determinato mercato in un periodo di tempo prestabilito. La tendenza può essere rialzista o ribassista.

nello spazio reale. Da qui la convinzione che i volumi, o meglio un loro aumento, sia di maggiore importanza nelle fasi iniziali di una tendenza rialzista piuttosto che di una ribassista. L'analisi dell'andamento dei volumi può quindi fornire una serie di importanti segnali di conferma o incertezza del trend.

FIGURA 2.3: Nella figura è possibile vedere la suddivisione dei volumi nell'apposita sezione di CoinMarketCap. Come detto precedentemente i volumi sono divisi per exchange e per cambio valuta-criptovaluta o criptovaluta-criptovaluta effettuato. Sfortunatamente non è possibile recuperare tutti i dati giorno per giorno, ma essi sono visibili sono nel giorno considerato. Con riferimento alla figura i dati sono del 11 aprile 2018. USDT è la criptovaluta che replica l'andamento del dollaro, in alcuni exchange infatti per acquistare le cripto è necessario cambiare i propri dollari in USDT con il cambio 1USDT=1USD.

FIGURA 2.3

Bitcoin Markets

USD -

#	Source	Pair	Volume (24h)	Price	Volume (%)	Updated
1	Bitfinex	BTC/USD	$398.963.000	$6.722,90	8,50%	Recently
2	OKEx	BTC/USDT	$262.072.000	$6.738,97	5,58%	Recently
3	Binance	BTC/USDT	$218.367.000	$6.730,96	4,65%	Recently
4	Binance	XVG/BTC	$165.560.000	$6.666,21	3,53%	Recently
5	Huobi	BTC/USDT	$122.039.000	$6.737,64	2,60%	Recently
6	bitFlyer	BTC/JPY	$117.215.000	$6.753,77	2,50%	Recently
7	Upbit	BTC/KRW	$105.913.000	$6.855,28	2,26%	Recently
8	Upbit	XVG/BTC	$99.859.900	$6.731,94	2,13%	Recently
9	Bittrex	XVG/BTC	$86.320.200	$6.704,40	1,84%	Recently
10	GDAX	BTC/USD	$82.899.700	$6.730,75	1,77%	Recently
11	BTCBOX	BTC/JPY	$79.605.500	$6.746,81	1,70%	Recently
12	Bithumb	BTC/KRW	$78.903.900	$6.859,97	1,68%	Recently
13	Bitstamp	BTC/USD	$66.542.000	$6.733,05	1,42%	Recently
14	Kraken	BTC/USD	$61.476.700	$6.726,30	1,31%	Recently
15	OKEx	TRX/BTC	$59.366.700	$6.687,85	1,26%	Recently
16	Binance	TRX/BTC	$56.839.100	$6.675,57	1,21%	Recently
17	Kraken	BTC/EUR	$56.501.600	$6.740,72	1,20%	Recently
18	Binance	ETH/BTC	$55.584.400	$6.745,89	1,18%	Recently
19	OKEx	ETH/BTC	$52.337.500	$6.737,72	1,12%	Recently
20	Binance	ONT/BTC	$46.691.500	$6.748,91	0,99%	Recently

Nella sezione apposita del sito CoinMarketCap è possibile vedere il volume degli scambi effettuati nelle ultime 24 ore suddivise per exchange e per tipo di scambio effettuato (ad esempio differenziando gli scambi di tale criptovaluta rispetto al dollaro o rispetto allo scambio diretto con altre monete fiat o a volte addirittura il cambio con altre criptovalute).

2.1.3 CIRCULATING SUPPLY[65]

L'ultima caratteristica che verrà considerata è il circolante. Esso indica il numero di criptovaluta in questione che è stato emesso[66]. La caratteristica più importante della maggior parte delle criptovalute è quella di avere un numero limitato di unità della stessa che può essere emesso. Per questo motivo è sicuramente importante tenere conto della quantità di valuta già emessa; tanto più si è vicini al numero massimo previsto per la criptovaluta, tanto più si può essere portati a pensare che il valore della criptovaluta possa aumentare (il bene è limitato). In modo analogo va analizzato anche il valore massimo di unità di criptovaluta raggiungibile; più tale numero è basso più è presumibile che il valore della criptovaluta possa essere alto (ovviamente il prezzo dipende soprattutto dalla validità e affidabilità del progetto della criptovaluta in questione e della fiducia che il mercato pone su tale progetto). Se si considerano criptovalute che hanno un elevatissimo circolante, il prezzo per singola criptovaluta tenderà ad essere più basso, al contrario quando una criptovaluta ha un basso numero di circolante il suo prezzo tenderà ad essere alto. Il circolante va valutato quindi con due accorgimenti; il primo è quello di valutarlo in valore assoluto (se sia un circolante

[65] Letteralmente la fornitura di circolante.

[66] Il numero fa riferimento non al numero di unità della criptovaluta presa in considerazione che viene scambiato, ma al numero totale della criptovaluta in circolazione, cioè tutte le unità di tale cripto che sono state emesse. Sarebbe più corretto per la determinazione del prezzo della criptovaluta in questione tenere conto solamente delle unità di tale criptovaluta che vengano scambiate in quel momento, tuttavia, tale dato non è disponibile in nessuna piattaforma.

“elevato” o “basso” rispetto a quello delle altre criptovalute concorrenti) ed in secondo luogo va valutato in proporzione rispetto al massimo circolante raggiungibile.
Per fare un esempio, se si considera il Bitcoin, l’attuale ammontare del circolante (aprile-maggio 2018) è di circa 17 milioni di unità, una quantità relativamente bassa se si considerano altre criptovalute. Per altro il numero massimo di Bitcoin che verrà emesso è quello di 21 milioni di unità; in questo momento sono già stati emessi 17/21 delle unità totali di Bitcoin previste, circa l’80% del totale.

Queste sono le tre caratteristiche fondamentali dal punto di vista numerico che possono essere analizzate in una criptovaluta. L’analisi può essere limitata solamente a questi tre aspetti, che comunque sono quelli più significativi, soprattutto per la difficoltà nel reperire altri dati attendibili e per un periodo di tempo adeguato.

2.2. LE ALTCOIN

Visto che l'obiettivo di questa tesi di analizzare le possibilità di investimento in criptovalute, è a mio avviso necessario individuare quale siano le principali "Altcoin", elencandone le caratteristiche principali, i punti di forza e le debolezze nonché gli eventuali possibili sviluppi futuri, che potrebbero farne mutare il prezzo o farne aderire il più diffuso utilizzo.

FIGURA 2.4: La figura è stata presa da CoinMarketCap e prende in considerazione le "COIN" considerandole in ordine di capitalizzazione di mercato. Le Coin in rosso sono le Altocoin. La figura è stata riportata il 10/04/2018. Pur cambiando minuto per minuto l'ordine delle criptovalute principali non varia molto frequentemente.

FIGURA 2.4

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	$114.866.556.636	$6.769,24	$4.126.460.000	16.968.900 BTC
2	Ethereum	$39.458.300.554	$399,64	$1.091.330.000	98.733.624 ETH
3	Ripple	$19.024.097.437	$0,486618	$156.894.000	39.094.520.623 XRP *
4	Bitcoin Cash	$10.898.670.191	$638,63	$210.485.000	17.065.650 BCH
5	Litecoin	$6.357.105.689	$113,48	$197.865.000	56.021.588 LTC
6	Cardano	$3.946.126.063	$0,152201	$54.416.000	25.927.070.538 ADA *
7	Stellar	$3.683.590.160	$0,198563	$27.094.600	18.551.241.469 XLM *
8	NEO	$3.310.892.000	$50,94	$105.497.000	65.000.000 NEO *
9	IOTA	$2.754.200.424	$0,990887	$20.523.900	2.779.530.283 MIOTA *
10	Monero	$2.620.577.012	$164,66	$22.059.400	15.914.886 XMR
11	Dash	$2.394.702.881	$299,26	$65.307.000	8.002.215 DASH

Per selezionare in un primo momento ed in maniera approssimativa le criptovalute più importanti, al fine di analizzarle, viene tenuto conto della loro capitalizzazione di mercato, dei volumi degli scambi e della loro presenza nei vari exchange che si occupano dello scambio delle criptovalute con le monete correnti. Facendo riferimento alla capitalizzazione di mercato, la più importante "Altcoin" è BITCOIN CASH, criptovaluta che occupa il quarto posto per quanto riguarda la classificazione secondo la capitalizzazione di mercato. Le altre Altcoin sono LITECOIN (al quinto posto della classifica della capitalizzazione di mercato), MONERO (al decimo posto) e DASH (all'undicesimo). Tutte le criptovalute "Altcoin" qui nominate verranno esaminate nei paragrafi seguenti in ordine di capitalizzazione di mercato.

2.2.1 BITCOIN CASH

FIGURA 2.5: In figura 2.5 è mostrato il logo ufficiale del Bitcoin Cash, riportato dal sito. Il logo è simile a quello del Bitcoin ma, come si può notare, l'inclinazione della "B" è invertita. Le due "linee" sopra e sotto la lettera richiamano alle linee che sono utilizzate nella simbologia di Dollaro($), Euro(€) e Sterlina(£).

FIGURA 2.5

Bitcoin Cash, https://www.bitcoincash.org/, nasce come "fork[67]" di Bitcoin il primo agosto 2017 (in realtà si parla di "hard fork" vista l'importanza del fork in questione), la criptovaluta ha l'obiettivo di continuare il progetto Bitcoin e di superarne alcune inefficienze. Gli sviluppatori hanno deciso di mettere a disposizione di tutti coloro che detenevano "Bitcoin" al momento del fork una quantità analoga di Bitcoin Cash. La criptovaluta dipende quindi, nel suo momento di nascita dal Bitcoin. La blockchain del

[67] Come già visto nella prima parte della tesi un "fork" in informatica è lo sviluppo di un progetto software nuovo che parte dal codice sorgente di un altro già esistente.

Bitcoin Cash si lega alla Blockchain del Bitcoin in partenza (nel senso che fino al 1 agosto 2017 la blockchain delle due criptovalute è la stessa), ma dal primo agosto 2017 inizia una blockchain indipendente e opera in maniera completamente slegata al Bitcoin.
Nonostante sia nata come fork del Bitcoin e sia presente sul mercato da un periodo limitato di tempo (meno di un anno), Bitcoin Cash è subito riuscita a raggiungere un prezzo considerevole e si è infatti rapidamente piazzata tra i primi posti delle criptovalute per quanto riguarda la capitalizzazione di mercato. Come la maggior parte delle criptovalute, il Bitcoin Cash (BTCC in sigla) è contraddistinto da una notevole volatilità di mercato, il prezzo è infatti passato in pochi mesi da 600$ a 4000$ per poi tornare nuovamente sulla soglia dei 600$.

GRAFICO 2.1: Il grafico preso da https://coinmarketcap.com/currencies/bitcoin-cash/, mostra l'andamento del Bitcoin Cash dal 1 agosto 2017 al 30 aprile 2018. Come si può vedere sin dal momento in cui è stato emesso ha avuto un valore di mercato considerevole

GRAFICO 2.1

Il grafico mostra oltre al prezzo di mercato in dollari anche il prezzo del Bitcoin Cash rispetto al Bitcoin, l'andamento della capitalizzazione di mercato ed i volumi giornalieri

relativi alla criptovaluta. Come si può vedere il massimo del valore in termini di prezzo in dollari (circa 3.900$), il volume di mercato (2.747.010.000 USD in 24 ore) e il Market Cap (65.603.515.837 USD) è stato raggiunto il 20 dicembre 2017. Il prezzo più alto invece in termini di Bitcoin è stato di 0,40802400 BTC ed è stato toccato il 12 novembre 2017. Il prezzo in termini di bitcoin può avere una rilevanza considerevole nel momento in cui sia necessario passare dalla criptovaluta creata da Satoshi Nakamoto per l'acquisto di un'altra criptovaluta[68].

Dopo aver visionato l'andamento di mercato della criptovaluta ritengo sia ora importante individuarne le caratteristiche fondamentali e le differenze rispetto al Bitcoin.

Bitcoin Cash è il risultato di un lunghissimo diverbio tra i programmatori e sviluppatori del network Bitcoin, per il superamento del cosiddetto "Bitcoin Scalability[69] Problem". Il problema fa riferimento alla quantità limitata di transazioni che è possibile effettuare all'interno del network Bitcoin. Come già visto nel primo capitolo, il problema della quantità limitata delle transazioni elaborabili dalla rete è legata al fatto che i blocchi nella blockchain Bitcoin hanno dimensioni e frequenza limitata, in particolare:

1) Il problema dimensionale riguarda il fatto che nella rete Bitcoin possono essere convalidate un numero limitato (4200) di transazioni per ogni blocco.
2) Il problema della frequenza è legato invece alla circostanza che il sistema Bitcoin prevede che venga convalidato un blocco ogni circa 10 minuti. Questa funzione non è modificabile, visto che è stata pensata dall'ideatore di Bitcoin per far sì che le unità di Bitcoin emessa fosse limitata. Con le tempistiche sopra indicate il massimo numero delle transazioni che possono essere convalidate ogni secondo è di 7. Questo può diventare un problema nel momento in cui avvengano più transazioni di quelle convalidabili, perché potrebbe far sì che alcune transazioni

[68] Come spiegato precedentemente, alcuni exchange prevedono che per l'acquisto di Altcoin sia necessario passare per il tramite del Bitcoin. Sostanzialmente tali criptovalute non possono essere acquistate direttamente con moneta fiat, ma è necessario un passaggio intermedio in BTC.

[69] Letteralmente, problema di scalabilità del Bitcoin.

impieghino molto tempo per essere convalidate, con la possibilità teorica che una transazione possa non esserlo mai[70].

Il Bitcoin Cash nasce sostanzialmente per risolvere questo problema. Come precedentemente detto, il primo agosto 2017 tutti coloro che erano in possesso di Bitcoin sono divenuti possessori anche dello stesso quantitativo di Bitcoin Cash.
Come avviene in tutti i fork, c'è stata una scissione della blockchain che ha portato quindi ad un'indipendenza completa (dalla data di scissione 1 agosto 2017) tra Bitcoin e Bitcoin Cash. La differenza sostanziale sta nel fatto che in BTCC ogni blocco ha una dimensione molto più grande, che permette di eseguire più transazioni all'interno dello stesso. Le transazioni eseguibili e convalidabili con la rete Bitcoin Cash sono otto volte superiori rispetto a quelle che possono essere eseguite e convalidate con Bitcoin (si passa da 7 al secondo a 56 al secondo).

TABELLA 2.1: La tabella mostra le differenze tra Bitcoin e Bitcoin Cash. Come si può notare l'unica differenza è presente nel numero di transazioni che possono essere inserite in un blocco.

TABELLA 2.1

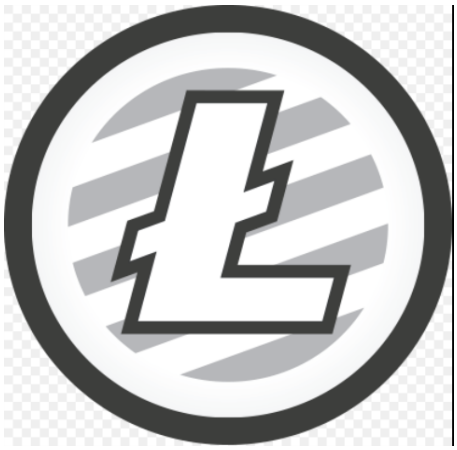
	BITCOIN	**BITCOIN CASH**
NUMERO DI UNITA' MASSIME	21 milioni di unità.	21 milioni di unità.
INTERVALLO BLOCCHI	Ogni 10 minuti.	Ogni 10 minuti.
GRANDEZZA BLOCCO	Blocco di 1 Megabyte (7 transazioni al secondo).	Blocco di 8 Megabyte (56 transazioni al secondo).
AGGIUSTAMENTO DIFFICOLA' HASH	Ogni 2 settimane.	Ogni 2 settimane.

[70] Nel caso in cui ogni secondo via siano sempre più di 7 transazioni, la transazione in eccesso potrebbe non essere mai convalidata, perché i blocchi potrebbero sempre essere riempiti senza considerare la transazione in questione. Questo potrebbe causare un problema enorme per l'affidabilità del Bitcoin.

Le altre caratteristiche del Bitcoin sono fatte salve nel Bitcoin Cash; il numero massimo di unità che possono essere emesse è di 21 milioni; il blocco viene convalidato ogni 10 minuti e la difficoltà dell'hash che deve essere risolto per la convalida del blocco viene aggiustato ogni due settimane in modo da permettere che le tempistiche dei blocchi siano rispettate.

2.2.2. LITECOIN

FIGURA 2.6[71]



La seconda Altcoin per capitalizzazione di mercato è Litecoin[72]. La criptovaluta è stata distribuita a partire dal 7 ottobre 2011 e come affermato anche dalla pagina principale del suo sito web è "Una valuta globale decentralizzata basata sulla tecnologia Bitcoin". Anche per quanto riguarda gli inventori di Litecoin, l'obiettivo del progetto è stato quello di migliorare la tecnologia del Bitcoin attraverso il superamento di alcune lacune di quest'ultimo. Il software Litecoin è stato distribuito per la prima volta nell'ottobre del 2011 nella piattaforma di hosting[73] per progetti software "GitHub[74]", da un ex dipendente di Google, Charles Lee. Le principali

[71] Il logo ufficiale di Litecoin.

[72] https://litecoin.com/it/.

[73] In informatica si definisce hosting (dal verbo inglese "to host", ospitare) un servizio che consiste nell'allocare su un server web le pagine web di un sito web o un'applicazione web, rendendolo così accessibile dalla rete Internet e ai suoi utenti.

[74] GitHub, https://github.com/, è un servizio hosting dedicato ai progetti software. Il sito è utilizzato prevalentemente dagli sviluppatori, che caricano i loro programmi all'interno di esso (caricano il codice sorgente dei loro programmi) e lo rendono utilizzabile e scaricabile a tutti gli utenti. Questi ultimi, visto che le informazioni sono open-source, possono interagire con gli sviluppatori dei programmi; in questo modo si permette di migliorare il codice, risolvendo bug o aggiungendo funzionalità. GitHub inoltre elabora moltissime pagine dettagliate che riassumono come gli sviluppatori lavorano sulle varie versioni dei loro programmi.

caratteristiche del Litecoin, che lo differenziano dal Bitcoin, sono il periodo di tempo inferiore necessario per la convalida di un blocco e l'aumento notevole del numero delle unità di criptovaluta prevista dal sistema.

Per quanto riguarda la prima innovazione del Litecoin, come è stato già detto nel paragrafo precedente con riguardo al Bitcoin Cash, essa è volta a risolvere il problema del numero di transazioni che possono essere convalidate in ogni blocco e della durata di convalida di un blocco. Riducendo i tempi di convalida dei blocchi, è possibile ottenere un efficientamento dei due problemi sopra esposti. Un discorso diverso va fatto per l'ammontare delle unità circolanti di Litecoin previste dal sistema. Quando il Bitcoin ha raggiunto un livello di prezzo, in termini di valute fiat, considerevole è risultato sempre più difficile il suo utilizzo come mezzo di pagamento. Questo problema è sorto non tanto per l'impossibilità di dividere il Bitcoin percentualmente (il Bitcoin è trasferibile fino alla minima unità di 0.000001), ma soprattutto per le sempre maggiori spese di commissione richieste dagli exchange per cambiare la valuta[75].

Prima di analizzare nel dettaglio le caratteristiche del Litecoin, ritengo sia necessario osservarne l'andamento dal momento della prima emissione nell'ottobre del 2011 fino ad oggi[76].

Tra la fine del 2011 e metà 2013 il prezzo della criptovaluta è sempre rimasto stabile (la stabilità viene intesa nel senso che il prezzo non ha avuto variazioni così importanti come avviene di solito nel mercato delle crypto), variando tra i 2 ed i 5 dollari. Tra settembre e novembre 2013 il prezzo dei Litecoin ha avuto un'impennata clamorosa, raggiungendo i 50 dollari il 28 novembre 2013. Questo valore è rimasto per lungo tempo il massimo del valore raggiunto dal Litecoin; nella stessa data inoltre, è stato raggiunto anche il massimo del valore del Litecoin in termini di Bitcoin (0,04829090 BTC). Dal momento di massimo prezzo a fine novembre 2013, il Litecoin ha subito una, prima improvvisa, e poi graduale caduta del prezzo, che lo ha portato a stabilizzarsi nuovamente attorno ad i 2

[75] Essendo le commissioni degli exchange molto spesso fisse (per esempio 0.0001BTC ad operazione), all'aumentare del valore della criptovaluta le commissioni si alzano notevolmente in termini di moneta fiat.

[76] È stato tenuto in considerazione un periodo tra l'ottobre 2011 e l'aprile 2018.

dollari. Il periodo di stabilità[77] è perdurato fino al marzo del 2017 quando il prezzo è cresciuto in maniera esponenziale, fino a raggiungere il suo massimo storico il 19 dicembre 2017. In questa data il prezzo del Litecoin si attestava attorno ai 370 USD, la capitalizzazione di mercato a 19.909.059.746 USD ed i volumi 2.379.250.000 USD.

GRAFICO 2.2: [1] Il grafico riportato da https://coinmarketcap.com/currencies/litecoin/, mostra l'andamento del Litecoin tra giugno 2013 e il 30 aprile 2018. Come detto si possono vedere il picco del cambio Litecoin/Bitcoin il 28 novembre 2013 ed il picco di prezzo in dollaro il 19 dicembre 2017. Il periodo precedente al 2013 non è stato inserito nel grafico perché il prezzo ha avuto variazioni poco significative che non vengono percepite a causa dell'unità di misura del grafico stesso.

GRAFICO 2.2

[77] Quando si utilizza il termine stabilità all'interno del mercato delle criptovalute va comunque tenuto conto che il mercato è molto volatile, soprattutto a causa della scarsa regolamentazione.

Dopo una breve osservazione dell'andamento di mercato del Litecoin si procede adesso con l'illustrazione delle sue caratteristiche.

Come si evince dal sito stesso del Litecoin, la criptovaluta è una "copia" del Bitcoin. Il sito infatti afferma pubblicamente che il funzionamento della criptovaluta è lo stesso. Litecoin, la cui sigla è LTC, quindi è una criptovaluta P2P (peer-to-peer)[78] che si basa su un sistema open source. Ad oggi Litecoin è la quinta valuta virtuale per capitalizzazione di mercato. Come tutte le criptovalute anche Litecoin non viene emesso da alcuna autorità centrale, ma "prende vita" grazie a delle procedure di mining. Tramite questa attività, i cosiddetti miner risolvono complessi problemi matematici in cambio di criptovalute. Questa è un'altra delle caratteristiche che accomuna Litecoin a Bitcoin e alle altre valute virtuali in circolazione. L'incentivo per i miner è di 50 Litecoin ogni blocco verificato con successo. La ricompensa in termini di Litecoin, come nel caso del BTC si dimezza ogni 4 anni. Ogni 2,5 minuti il network genera un cosiddetto blocco che si aggiunge agli altri e con essi va a comporre la blockchain, il registro pubblico di tutte le transazioni in Litecoin. Come nel caso del Bitcoin, il numero massimo di Litecoin è già stato stabilito a priori dal sistema ed è di 84 milioni.

Nel momento della nascita del Litecoin, il suo ideatore Charles Lee, fece un confronto tra Bitcoin e Litecoin, paragonando il Bitcoin all'oro ed il Litecoin all'argento. Questa volontà di paragone è evidente anche dalla scelta dei loghi delle due criptovalute, la prima color oro, la seconda caratterizzata dal grigio argentato. Il paragone con oro e argento è stato fatto soprattutto per giustificare l'esistenza di tutte e due le criptovalute; i due metalli preziosi hanno la stessa funzione di bene rifugio ed il loro differente prezzo è caratterizzato dalla loro diversa rarità (anche il Litecoin è stato fatto volontariamente meno raro del Bitcoin). Lee sostanzialmente ha voluto mandare un messaggio importante, cioè quello della possibilità di coesistenza di due criptovalute molto simili.

[78] Come spiegato nel primo capitolo.

Con l'aiuto della "Tabella 2.2" vengono riassunte tutte le differenze tra Bitcoin e Litecoin.

TABELLA 2.2[79]

	BITCOIN	**LITECOIN**
NUMERO DI UNITA' MASSIME	21 milioni di unità.	84 milioni di unità.
INTERVALLO BLOCCHI	Ogni 10 minuti.	Ogni 2,5 minuti.
GRANDEZZA BLOCCO	Blocco di 1 Megabyte (7 transazioni al secondo).	Blocco di 1 Megabyte (16,8 transazioni al secondo).
AGGIUSTAMENTO DIFFICOLA' HASH	Ogni 2 settimane.	Ogni 2 settimane.

2.2.3. MONERO[80]

FIGURA 2.7[81]

Litecoin è stata la prima Altcoin che ha riscontrare un grosso successo ed una ribalta a livello internazionale, tanto che, a partire dal 2013 è stata spesso protagonista di articoli da parte di importanti giornali come il "Wall Street Journal" e il "New Your Times", i quali lo individuavano come possibile alternativa al Bitcoin, se non addirittura in alcuni casi come suo successore. Dopo

[79] Il numero massimo di unità di Litecoin previste dal sistema è di 84 milioni. Ogni blocco viene autenticato ogni 2,5 minuti, questo fa sì che aumenti il numero di transazioni convalidabili dal sistema fino ad un massimo di 16,8 al secondo.

[80] "Monero" vuol dire "moneta" in lingua "Esperanta". La Lingua esperanta è una lingua "artificiale" creata tra il 1872 e il 1887, con lo scopo di mettere in comunicazione tra loro popoli diversi mediante un linguaggio che non appartenga a nessuno in particolare.

[81] Il simbolo ufficiale di "Monero" è una "M" bianca contornata da un cerchio arancio e nero.

l'interesse che si è sviluppato nel mondo delle "Alternative Coin", molti programmatori hanno cominciato a lavorare e sviluppato altri progetti crypto.

I programmatori delle criptovalute alternative hanno ritenuto fondamentale, per lo sviluppo delle stesse, contraddistinguere ognuna di esse di un tratto distintivo concettuale o programmatico, che potesse garantire una caratteristica di esclusività alla nuova crypto. Uno di questi progetti, conclusosi all'inizio del 2014, ha portato alla nascita di "Monero[82]", XMR in sigla. La criptovaluta è stata creata a partire dal 18 aprile 2014, gli sviluppatori più importanti sono gli spagnoli Riccardo Spagni e Fransisco Cabañas. In un primo momento la criptovaluta venne chiamata "BitMonero", solo in seguito il "Bit" iniziale è stato perso per lasciare posto al solo "Monero". Nel video introduttivo della criptovaluta[83] i programmatori di Monero insistono molto sull'importanza della "Financial Privacy" e sullo slogan della crypto "You are your own bank". Monero è una criptomoneta decentralizzata, digitale e sicura, basata sulla tecnologia criptografica operata da un network di utenti le cui transazioni sono confermate e registrata immutabilmente della blockchain della crypto. Le tre caratteristiche principali di Monero sono: la sicurezza, la privacy e la non tracciabilità. La privacy della criptovaluta è garantita dal fatto che il funzionamento della blockchain, pur essendo analogo a quello del Bitcoin, non è completamente pubblico, nel senso che viene offuscata l'origine, l'ammontare e la destinazione di tutte le transazioni effettuate. Sostanzialmente Monero fa sue tutte le caratteristiche del Bitcoin senza però far venir meno la privacy e l'anonimato delle transazioni[84]. Esiste in ogni caso la possibilità della

[82] https://getmonero.org/.

[83] Nel sito ufficiale di ogni criptovaluta è spesso presente un video introduttivo che riassume in 4/5 minuti tutte le caratteristiche principali della criptovaluta ed i suoi obiettivi.

[84] Come spiegato nel capitolo precedente dedicato al Bitcoin, anche le transazioni che avvengono in Bitcoin sono anonime, tuttavia, in alcune circostanze con una correlazione di informazioni (ad esempio indirizzo pubblico, chiave pubblica ecc..) potrebbe essere possibile individuare una transazione effettuate dallo stesso soggetto. Per fare un esempio, se il soggetto A effettua una transazione a favore del soggetto B, egli deve venire a conoscenza da parte del soggetto B di una delle sue chiavi pubbliche. In una circostanza molto remota, ma comunque possibile, il soggetto B potrebbe effettuare un'altra transazione con l'indirizzo pubblico utilizzato per l'operazione con il soggetto A. In questa circostanza, il soggetto A potrebbe individuare la transazione, Infatti le informazioni contenute nella Blockchain Bitcoin sono "aperte". Con

"Selectively Trasparent", ovvero può essere possibile decidere di rendere una, alcune o tutte le proprie transazioni visibili, e può anche essere scelto quali sono i soggetti che possono vedere tali transazioni. Per fare un esempio: Giacomo decide di trasferire a Marta 100 Monero; nel momento in cui effettua tale transazione Giacomo può decidere se tale transazione debba essere visibile oppure no. Sostanzialmente, può scegliere se tutti possono vedere tutte le informazioni di tale transazione (origine, ossia il suo indirizzo pubblico, ammontare, in questa circostanza 100 Monero e indirizzo al quale vengono spediti; per quanto riguarda quest'ultima informazione, essa potrà essere pubblica solo se congiuntamente anche Marta vorrà che tale informazione sia pubblica).
Dopo una breve sintesi riguardante le caratteristiche principali di Monero ritengo necessario effettuare una breve analisi riguardante il suo andamento di mercato.
Come prima cosa va sottolineato che Monero è tra la decima e la quindicesima criptovaluta per capitalizzazione di mercato[85] e la terza "Altcoin". Sin dal momento della sua creazione si è sempre affermata come una delle principali criptomonete.
Come il Litecoin, Monero si è caratterizzato in un primo momento per il mantenimento di un prezzo molto basso, attorno ad i 2 dollari. Con il passare del tempo, la cripto ha riscontrato sempre un maggiore interesse da parte degli investitori, ed il suo prezzo è aumentato in maniera graduale ma continua, portandolo dai 2 dollari di marzo 2016 fino ad i 40 dollari dell'agosto dell'anno successivo. Da lì in poi, seguendo il trand profondamente rialzista del mercato, Monero ha raggiunto tutti i suoi massimi, il primo il 29 agosto 2017, quando il suo valore in termini di BTC ha toccato 0,033BTC (valore quasi raggiunto nuovamente nei primi giorni di marzo 2018). Il 7 gennaio 2018 la criptomoneta ha raggiunto il suo massimo storico in termini di prezzo in dollari (circa 500 UDS), di volume delle transazioni (318.729.000 USD) e di capitalizzazione di mercato

Monero questo non può avvenire, perché appunto le informazioni riguardanti l'origine, l'ammontare e la destinazione delle transazioni, contenute nella Blockchain sono completamente offuscate.

[85] Il valore di Monero è molto simile a quelle di altri criptovalute quali "NEO", "IOTA" e quindi il suo posizionamento nella classifica di Market Cap, può cambiare giorno per giorno, stabilizzandosi comunque tra le prime 15 cripto.

(7.695.285.722 USD). A seguito della spinta ribassista dei primi mesi del 2018 il valore della criptomonata si è più che dimezzato avvicinandosi alla soglia di 200 dollari.

GRAFICO 2.3: Il grafico riportato da https://coinmarketcap.com mostra l'andamento di mercato del prezzo di Monero dalla prima osservazione disponibile il 21 maggio 2014 ad oggi. Nel presente grafico, come nei precedenti è riportato congiuntamente l'andamento della capitalizzazione di mercato, del prezzo del Monero in termini di Bitcoin, del cambio con l'USD e i volumi di mercato nelle 24 ore.

GRAFICO 2.3

Come per le precedenti Altcoin, si procede con un riassunto schematizzato delle caratteristiche che differenziano la criptomoneta dal Bitcoin.

TABELLA 2.3: La tabella riassume le caratteristiche fondamentali di Monero e le mette a confronto con quelle di Bitcoin.

TABELLA 2.3[86]

	BITCOIN	**MONERO**
NUMERO DI UNITA' MASSIME	21 milioni di unità.	18,4 milioni di unità.
INTERVALLO BLOCCHI	Ogni 10 minuti.	Ogni 2 minuti.
GRANDEZZA BLOCCO	Blocco di 1 Megabyte (7 transazioni al secondo).	Blocco di 1 Megabyte (35 transazioni al secondo).
PARTICOLARITA'	---	Aumento del Privacy nelle transazioni.
AGGIUSTAMENTO DIFFICOLA' HASH	Ogni 2 settimane.	Ogni 2 settimane.

[86] Il numero di unità che verranno emesse in totale è inferiore rispetto a quello di Bitcoin e si attesta circa a 18,4 milioni. Le unità verranno emesse in otto anni al partire dalla prima emissione di "Monero".

2.2.4. DASH

L'ultima "Altcoin" che verrà presa in considerazione in questa tesi è Dash. Come Bitcoin, Dash è un open-source peer-to-peer cryptocurrency. Il suo ideatore e attuale CEO è Ryan Taylor ex manager della società statunitense McKinsey & Company. La moneta digitale venne messa in circolazione a partire dal 18 gennaio 2014 con il nome di XCoin (XCO), il 28 dello stesso mese il nome fu cambiato in DarkCoin, solo nel marzo dello 2015 il nome fu definitivamente cambiato in Dash (dall'inglese Digital Cash). Pur avendo un funzionamento simile al Bitcoin, Dash ha introdotto una serie di migliorie per quanto riguarda il funzionamento e della velocità delle transazioni.

FIGURA 2.8[87]

Dal punto di vista "amministrativo" le funzionalità di Dash sono differenti da quelle del Bitcoin.

Nelle network Dash sono presenti due funzioni; quella di "Minatore[88]" e quella di "MasterNode". I primi svolgono la medesima funzione svolta per le altre criptovalute, ovvero quella di creare i blocchi e di convalidare le transazioni avvenute nel network. I "MasterNode" hanno un compito differente, essi sono coloro che si occupano direttamente di svolgere le "funzioni opzionali" di Dash. Le funzioni opzionali sono appunto dei servizi aggiuntivi che, a corrispettivo di una commissione, possono essere richiesti da coloro che effettuano transazioni per il tramite di Dash. Le funzioni opzionali sono due: il così detto "Private Send" e "l'Instant Send". La prima funzione riguarda appunto la possibilità

[87] Il simbolo ufficiale riportato dal sito di Dash, https://www.dash.org/.

[88] Il ruolo dei minatori è spiegato nel paragrafo apposito del capitolo 1.

da parte dei fruitori dei servizi di pagamento Dash di effettuare la propria transazione in completo anonimato. Questo servizio avviene "mescolando" più transazioni effettuate da soggetti che vogliano fruire di questo servizio. Il meccanismo si sostanzia in uscite ed entrate di Dash da un indirizzo pubblico[89] ad un altro. Attraverso questo meccanismo non sarà possibile rintracciare in alcun modo a chi siano fatte le singole transazioni, anche in considerazione del fatto che ogni utente possiede 100 indirizzi pubblici per ogni chiave pubblica ed un totale di 100 chiavi pubbliche. "L'Instant Send" consiste nella possibilità da parte di coloro che detengono un Wallet Dash di effettuare transazioni che vengano autenticate in maniera immediata (1,4 secondi medi). Queste due funzioni sono, come detto, garantite dai MasterNode; essi sono appunto "nodi" particolarmente importanti. I MasterNode devono essere attivi 24 ore al giorno e 7 giorni a settimana e per operare devono depositare almeno 1000 Dash coin nel sistema. I MasterNode, oltre alle funzioni sopra esposte, hanno un'altra funzione importante; essi infatti in virtù della grande quantità di Dash che detengono, hanno il diritto di partecipare attivamente alle decisioni di sviluppo del network Dash[90]. Lo sviluppo del network Dash funziona attraverso il finanziamento dei progetti proposti dagli utenti o dagli sviluppatori. Questi progetti, che possono essere presentati in una sezione apposita del sito, vengono analizzati ed infine messi alla votazione dei MasterNode. I progetti che vengono scelti dai MasterNode vengono finanziati dal network stesso e permettono in questa maniera di far migliorare il funzionamento della rete Dash. Il finanziamento è autofinanziamento nel senso che i progetti vengono retribuiti attraverso il pagamento di Dash ai programmatori. L'autofinanziamento avviene attraverso una sorta di "tassazione" del network al momento della creazione di un blocco. Quando viene creato un blocco dai minatori, il quantitativo di Dash generato da quel blocco viene distribuito in questa maniera: il 45% dei Dash generati vengono attribuiti al minatore che ha risolto l'hash corrispondente al blocco, un altro 45% dei proventi viene distribuito ai MasterNodes,

[89] Gli indirizzi pubblici di Dash sono simili ad IBAN bancari ed hanno lo stesso funzionamento degli indirizzi di Bitcoin.

[90] Le decisioni all'interno del network Dash vengono prese attraverso un sistema di "democrazia diretta". Coloro che partecipano al sistema nella qualità di MasterNode hanno il diritto di votare qualsiasi decisione di sviluppo che venga proposta all'interno del sistema.

come retribuzione per il compito svolto per garantire le funzioni opzionali, e l'ultimo 10% viene depositato nel "Treasury". Il "Treasury" è una sorta di "conto corrente" dello stesso network Dash, all'interno del quale appunto confluiscono il 10% dei Dash generati attraverso il meccanismo blockchain. I fondi contenuti nel "Treasury" vengono spesi per retribuire coloro che propongono e sviluppano dei progetti che aiutano a migliorare la rete Dash. Come sopra detto, i progetti vengono selezionati dai MasterNode attraverso un sistema di "democrazia diretta" secondo la quale ogni MasterNode vota ogni decisione che deve essere presa dal network.

La moneta digitale Dash è a mio avviso quella che più si avvicina al senso di "criptomoneta" introdotto dall'ideatore di Bitcoin. Dash è una piattaforma che si occupa in maniera esclusiva di sviluppare un sistema di pagamento veloce, sicuro e anonimo. Il progetto della società che ha emesso i Dash è tra i più strutturati e completi, ed il modo attraverso il quale vengono retribuiti gli sviluppatori permette al sistema di migliorare con velocità le inefficienze. Al progetto Dash sono stati spesso interessati soggetti che operano in stati nei quali vi sia un'altissima inflazione monetaria; come per esempio Cuba e Il Venezuela. Gli abitanti di questi paesi guardano a Dash come una possibilità di sottrarsi all'inflazione monetaria e allo stesso tempo come moneta utilizzabile per i pagamenti di tutti i giorni.

Dopo aver individuato le caratteristiche principali della criptomoneta è necessario studiarne l'andamento del prezzo dal momento del suo lancio nel mercato.

GRAFICO 2.4: Il grafico riportato da https://coinmarketcap.com/currencies/dash/, mostra l'andamento del prezzo di Dash da febbraio 2014 sino al 30 aprile 2018. È riportato l'andamento del prezzo di Dash in relazione al $ e al BTC e l'andamento del volume e della CDM.

GRAFICO 2.4

Dal momento del suo "lancio" sul mercato nell'febbraio 2014 sino all'inizio del 2017, Dash ha avuto una crescita costante e graduale del prezzo. Al suo esordio sul mercato, la criptomoneta valeva 1 dollaro ed ha raggiunto i 10 dollari ad inizio 2017. A partire da quest'anno, seguendo la tendenza di tutto il mercato delle criptovalute Dash ha avuto un aumento vigoroso del prezzo che lo ha portato a raggiungere tutti i massimi. Il 19 marzo 2017 Dash ha raggiunto il valore in termini di Bitcoin di 0,108336 BTC, massimo storico nel cambio con la principale criptovaluta. Il 21 dicembre dello stesso anno invece, sono stati raggiunti tutti gli altri massimi: il cambio con il dollaro ha toccato i 1500 USD

per Dash, la capitalizzazione di mercato ha raggiunto il valore di 11.643.487.099 USD e il volume delle transazioni nelle 24 ore è stato di 450.049.000 USD.

Per riassumere le caratteristiche della criptovaluta e le differenze con il Bitcoin viene proposta una tabella. La grandezza dei blocchi (2 Megabyte) e la loro frequenza ogni 60 secondi fa sì che le commissioni per effettuare un'operazione con Dash, siano pressoché nulle. Il gran numero di transazioni convalidabili in un secondo (140 transazioni al secondo), permette di convalidare tutte le operazioni all'interno di un medesimo blocco. Il costo di ogni transazione effettuata per il tramite di Dash è quindi il minimo esigibile, ovvero 1 centesimo di dollaro per transazione.

TABELLA 2.4: In tabella sono riportate le principali caratteristiche di Dash ed il confronto con il Bitcoin.

TABELLA 2.4

	BITCOIN	**DASH**
NUMERO DI UNITA' MASSIME	21 milioni di unità.	18,9 milioni di unità.
INTERVALLO BLOCCHI	Ogni 10 minuti.	1 minuto.
GRANDEZZA BLOCCO	Blocco di 1 Megabyte (7 transazioni al secondo).	Blocco di 2 Megabyte (140 transazioni al secondo).
DISTRIBUZIONE MONETA	100% a coloro che risolvono l'hash del Blocco (Minatori).	45% Minatori 45% MasterNote 10% Treasury.

PARTICOLARITA'	---	Funzioni opzionali: "Private Send" e l'"Instant Send". "Democrazia diretta" che può essere svolta dai MasterNode.
AGGIUSTAMENTO DIFFICOLA' HASH	Ogni 2 settimane.	Ogni 2 settimane.

2.3 CRIPTOVALUTE INNOVATIVE RIPPLE E IOTA

Dopo aver analizzato il panorama delle Alternative Coin ora ci si affaccia alle criptovalute innovative, quelle cioè che hanno nel loro funzionamento un tratto caratteristico sostanzialmente nuovo rispetto al Bitcoin. Tra di esse si possono individuare due criptovalute più importanti; la prima è Ripple e la seconda è IOTA.

Tutte e due sono delle criptovalute atipiche, nel senso che le loro caratteristiche fondamentali sono insolite e profondamente differenti rispetto a quelle delle normali crypto. Ripple si contraddistingue, come verrà analizzato nel paragrafo 2.3.1, per essere una criptomoneta centralizzata, nel senso che il funzionamento, la sicurezza e l'autenticazione delle transazioni viene gestita da una società. IOTA invece è profondamente innovativa perché non utilizza la blockchain, ma funzione per il tramite del "Tangle".

2.3.1 RIPPLE

FIGURA 2.9[91]

Ripple è una società, fondata nel 2012 da Ryan Fugger, con sede in California che si occupa di trasferire asset (intesi come moneta fiat, oro e altre materie prime), attraverso la propria piattaforma. La creazione e lo sviluppo della piattaforma Ripple è oggetto sociale della società in questione ed è perseguita dal così detto "Ripple Lab" a San Francisco. Altra cosa è invece la criptomoneta Ripple (XRP), la quale opera nella piattaforma, ma è completamente slegata allo sviluppo della stessa. La società Ripple è stata creata con l'obiettivo di

[91] In figura è riportato il logo ufficiale di Ripple. Solitamente il logo è seguito dalla scritta Ripple sulla destra.

sviluppare una tecnologia che potesse permettere un nuovo sistema di pagamento in tempo reale, la cui funzione principale fosse quella di consentire il trasferimento dei fondi tra banche o società finanziarie. La società collabora con un gran numero di banche[92], in particolare europee, ed ha sviluppato una piattaforma che è stata pensata come concorrente a SWIFT (Society For Wordwile Interbanck Financial Telecomunication) dalla quale in gergo tecnico è utilizzato il termine "Bonifico SWIFT[93]" per intendere un pagamento interbancario ed interstatale.

FIGURA 2.10[94]

[92] Tra le collaborazioni riportate nel sito di Ripple, https://ripple.com/solutions/, spiccano quella con la banca spagnola "Santander", il gruppo svizzero UBS, Unicredit, American Express, Credit Agricole,

[93] Il Bonifico SWIFT è il bonifico internazionale più utilizzato in questo momento. Esso è l'unico che garantisce il trasferimento di fondi da un paese ad un altro. Pur funzionando in maniera adeguata possiede una serie di aspetti negativi; prima di tutto è lento, nel senso che impiega 2 o più giorni lavorativi per essere eseguito, ed il secondo è che è costoso. In un mondo globalizzato come quello di oggi questi due aspetti possono rappresentare un problema non indifferente.

[94] In figura sono riportate dal sito di Ripple le principali collaborazioni della società con gli operatori del sistema finanziario internazionale.

Pur essendo solo alla fase iniziale, le collaborazioni con gli intermediari finanziari sono numerose e stanno portando ad uno studio di fattibilità per quanto riguarda l'utilizzo di Ripple come una nuova piattaforma per effettuare le transazioni interbancarie.

Altra cosa è invece la criptovaluta XRP, comunemente conosciuta come Ripple. Come prima cosa va detto che Ripple è una moneta digitale atipica, che molti esperti del mondo crypto non considerano nemmeno una criptovaluta. Questa preclusione nei confronti di XRP è legata principalmente al fatto che la moneta digitale non sia decentralizzata. Essa, pur essendo basata sulla struttura blockchain, è controllata dalla società Ripple che si occupa di sviluppare e garantire le transazioni che avvengono all'interno della propria piattaforma. Un'altra peculiarità di Ripple, che la allontana dal mondo delle criptovalute, è proprio lo stesso obiettivo con il quale è stata creata: al contrario della maggior parte delle criptovalute, XRP non è stata pensata come "moneta" di uso comune, la sua funzione infatti è quella di "moneta" utilizzabile tra intermediari finanziari, per permettere il superamento ed efficientamento di vecchie tecnologie come quella SWIFT. Quest'ultima caratteristica di Ripple è forse quella che più allontana la moneta digitale dal mondo "crypto" e più la avvicina al mondo della finanza convenzionale. Da questo punto di vista si può affermare che XRP sia il primo punto di congiunzione tra la finanza e il mondo delle criptovalute.

In un contesto nel quale molto spesso le banche e le istituzioni finanziarie guardano alle criptovalute come una minaccia e come una pericolosa fonte di bolle speculative, Ripple, per prima tra le criptovalute, è riuscita a riscontrare un interesse concreto[95] da parte degli intermediari finanziari.

XRP è stato rilasciato a partire dal 2012 dalla stessa società Ripple. Una delle caratteristiche fondamentali della criptomoneta è che tutte le unità di XRP previste dal sistema sono state emesse subito; l'importo previsto di 100 miliardi di unità di XRP è stato "minato" al momento della nascita della criptovaluta. La grossa quantità di Ripple estratti (se si mette in relazione per esempio con il limite massimo di Bitcoin di 21

[95] Basti pensare che ad una delle conferenze della società Ripple nell'ottobre del 2017 ha partecipato ed è intervenuto l'ex presidente della Federal Reserve Ben Bernanke, il quale ha espresso un parere molto positivo sulla tecnologia Ripple ed ha individuato nello sviluppo della Blockchain in società come questa il futuro della finanza mondiale.

milioni) è stata scelta proprio per questioni di funzionalità. Il valore dei Ripple non può essere così tanto elevato come quello di Bitcoin, perché gli ideatori non volevano che XRP diventasse una riserva di valore virtuali (oro virtuale) come è diventato il Bitcoin, ma potesse essere utilizzata in maniera pratica dalle Banche per l'esecuzione delle operazioni interbancarie. Se l'obiettivo della società di sostituire la tecnologia SWIFT fosse raggiunta, tutte le banche vorrebbero detenere quantità considerevoli di XRP sufficienti a poter garantire le operazioni che esse vogliano svolgere[96].

Pur essendo state "estratte" tutte, le unità di Ripple non sono state immesse subito nel mercato, esse infatti sono distribuite in maniera graduale dalla società Ripple, che attualmente ne ha immesse sul mercato poco più di 40 miliardi. La politica di rilascio dei Ripple, secondo quanto affermato dal CEO della società Brad Garlighouse in diverse interviste con alcune importanti emittenti televisive americane (come per esempio CNBC[97]), è finalizzata a garantire un giusto equilibrio nel rapporto tra XRP nel mercato e valuta fiat[98].

Poiché, come detto, tutti i Ripple sono già stati generati, il funzionamento di XRP non si basa sull'operato dei "miners", ma la società stessa si occupa del funzionamento della blockchain, eseguendo gli hash per garantirne la sicurezza.

Nel momento della sua immissione sul mercato nel 2012, Ripple aveva un valore inferiore al millesimo di dollaro, tuttavia i dati disponibili nella piattaforma CoinMarketCap partono da metà del 2013, quando il valore del XRP in termini di dollari si aggirava attorno agli 0,005$. Il valore così basso dell'XRP è appunto giustificabile dal fatto che siano state "estratte" subito tutte le unità di XRP previste dal protocollo. Il

[96] Se le unità di Ripple fossero inferiori risulterebbe difficile effettuare le operazioni tra le banche, anche perché Ripple è divisibile solo fino alla sesta cifra dopo la virgola (0,000001 XRP). Le operazioni tra banche devono in ogni caso essere effettuate per il tramite di XRP per garantire la velocità delle operazioni. Se fossero svolte per il tramite di moneta fiat, la loro immediatezza non sarebbe garantita.

[97] https://www.youtube.com/watch?v=vnGNycbhJlE.

[98] Il rilascio graduale, anche se il CEO della società non lo afferma pubblicamente, è evidentemente anche legato al prezzo di mercato di Ripple. I vertici aziendali non vogliono immettere tutti gli XRP prima che non abbiano raggiunto un valore considerevole.

valore della criptovaluta è sempre rimasto piuttosto basso. Purtuttavia nella classifica della capitalizzazione di mercato Ripple ha sempre occupato i primi cinque posti, raggiungendo ad inizio del 2018 il secondo posto, per un piccolo periodo di tempo, spodestando Ethereum e raggiungendo una capitalizzazione di mercato complessiva superiore ai 100 miliardi di dollari.

Il grafico 2.5 sottostante, riportato da https://coinmarketcap.com/currencies/ripple/, mostra l'andamento del prezzo di mercato della criptomoneta dal 4 agosto 2013 fino Al 30 aprile 2018. Il grafico fa riferimento all'andamento di mercato rispetto al dollaro, rispetto al Bitcoin e mostra i volumi giornalieri e la capitalizzazione di mercato.

GRAFICO 2.5

Il prezzo di Ripple è oscillato dal settembre 2013 al marzo 2015 tra gli 0,005 e gli 0,01 USD. Da quel momento in poi è avvenuta una graduale crescita fino al marzo 2017 quando il prezzo di XRP si assestò per qualche periodo attorno ai 7 centesimi di dollaro.

Da qui in poi, seguendo il periodo Bull del mercato delle criptovalute, Ripple ha avuto una crescita esponenziale che ha portato il suo prezzo a raggiungere il 5 gennaio 2018 il suo massimo storico di 3,56 dollari. Nella stessa data si è registrato anche il più alto valore in termini di Bitcoin (0,00023342 BTC) e di capitalizzazione di mercato (128.715.070.060 USD) e di volumi nelle 24 ore (8.130.050.000 USD).
Per riassumere le caratteristiche di Ripple e individuare le differenze rispetto al Bitcoin viene proposta una tabella.

TABELLA 2.5

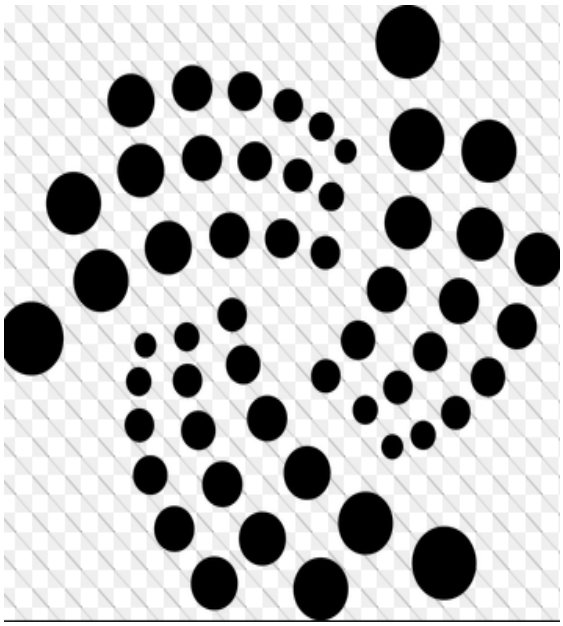
	BITCOIN	**RIPPLE**
NUMERO DI UNITA' MASSIME	21 milioni di unità.	100 miliardi di unità.
INTERVALLO BLOCCHI	Ogni 10 minuti.	Il blocco viene generato sulla singola transazione. La transazione impiega in media meno di 10 secondi per giungere dal mandante al destinatario.
DISTRIBUZIONE MONETA	100% a coloro che risolvono l'hash del Blocco (Minatori).	Non è previsto il Mining. Tutte le unità previste sono state generate al momento della nascita del sistema Ripple.
PARTICOLARITA'	---	Ripple è pensato per essere utilizzato tra intermediari finanziari per lo svolgimento di operazioni tra di essi.

2.3.2. IOTA

IOTA[99] è un progetto di criptovaluta open-source, non minabile[100], sviluppata e lanciata tra il 2015 e il 2016 da un gruppo di sviluppatori tedeschi[101]. A sostegno del progetto è stata fondata la "IOTA fondation[102]" con l'apporto di fondi donati dagli utenti.
IOTA è una criptovaluta innovativa nata con un obiettivo preciso; quello di superare la gravosità e la pesantezza della tecnologia blockchain. Come dichiarato anche nel sito ufficiale di IOTA, gli sviluppatori hanno voluto operare nella direzione di una criptovaluta "lightweight", ovvero "leggera".

In figura è stato riportato il logo ufficiale di IOTA.

FIGURA 2.11



Gli inventori dell'idea IOTA sono partiti da un presupposto molto importante, quello cioè che nella prossima decade si stima che ci saranno più di 50 miliardi di dispositivi connessi a Internet. Tali dispositivi saranno connessi in tutto il mondo, anche in paesi nelle quali le strutture bancarie ed in generale dei servizi finanziari sono pressoché assenti. Oltre al problema dello scarso sviluppo dell'economia finanziaria, questi nuovi paesi che si affacciano al mondo interconnesso, sono caratterizzati da istituzioni statali molto spesso inadeguate, che non riescono ad imporre con forza la moneta statale e che spesso la sottopongono

[99] IOTA, https://www.iotaitalia.com/about. Con IOTA tutto maiuscolo si intente il network, con Iota con solo la prima lettere maiuscola l'unità più piccola di criptovaluta IOTA.
[100] Nel senso che non prevede l'emissione di criptovaluta per il tramite del "mining".
[101] Fondato nel 2015 da David Sønstebø, Sergey Ivancheglo, Dominik Schiener e Serguei Popov.
[102] Il team di sviluppo ha sede a Berlino.

a forti svalutazioni. Monete così deboli e sottoposte ad alta svalutazione impediscono a coloro che la usano di svolgere i pagamenti di tutti i giorni. IOTA ha l'obiettivo di permettere di gestire i "micropagamenti[103]", garantendone la sicurezza e dei costi pressoché nulli. I dispositivi interconnessi dovranno essere in grado di scambiare tra loro minuscole quantità di denaro, in modo immediato. Proprio per questo scopo è stato concepito IOTA, che tuttavia rimane adatto anche a qualsiasi altro scenario in cui vi sia la necessità di gestire un qualsiasi tipo di transazione, anche di grosse dimensioni.

Per il raggiungimento di questo ambizioso obiettivo, al momento della progettazione di IOTA si è scelto di prendere le distanze dalle crittovalute basate su blockchain. Pur mantenendo la visione legata a un consenso distribuito[104], è risultato necessario un approccio diverso per rendere il network scalabile[105] nell'ambito dell'ecosistema IOTA, in cui saranno presenti decine di miliardi di dispositivi connessi. Nell'ottica di IOTA infatti si vuole favorire l'utilizzo delle criptovalute per le operazioni di tutti i giorni; così facendo sarebbe necessario convalidare migliaia di transazioni ogni secondo. Come è stato visto in precedenza per altre criptovalute, anche attraverso l'ampliamento dei blocchi della blockchain e la riduzione dei tempi di convalida, nessuna criptovaluta fin ora riesce a convalidare più di 200 operazioni al secondo. Cercando di risolvere questo problema è nata la principale innovazione di IOTA, il Tangle.

IOTA usa il Tangle, che è un protocollo software basato su grafi aciclici diretti e profondamente diverso dal protocollo blockchain.

Prima di procedere con la spiegazione dell'innovazione sostanziale del "Tangle" è necessario soffermarsi sul concetto di "grafo aciclico diretto". In informatica e talvolta anche in matematica si intende per grafo aciclico diretto, detto anche "grafo aciclico

[103] I pagamenti che avvengono per le operazioni di tutti i giorni; quali per esempio gli acquisti al supermercato.

[104] Le transazioni che avvengono attraverso la blockchain sono legate al consenso distribuito, perché devono essere convalidate dai minatori che effettuano la transazione.

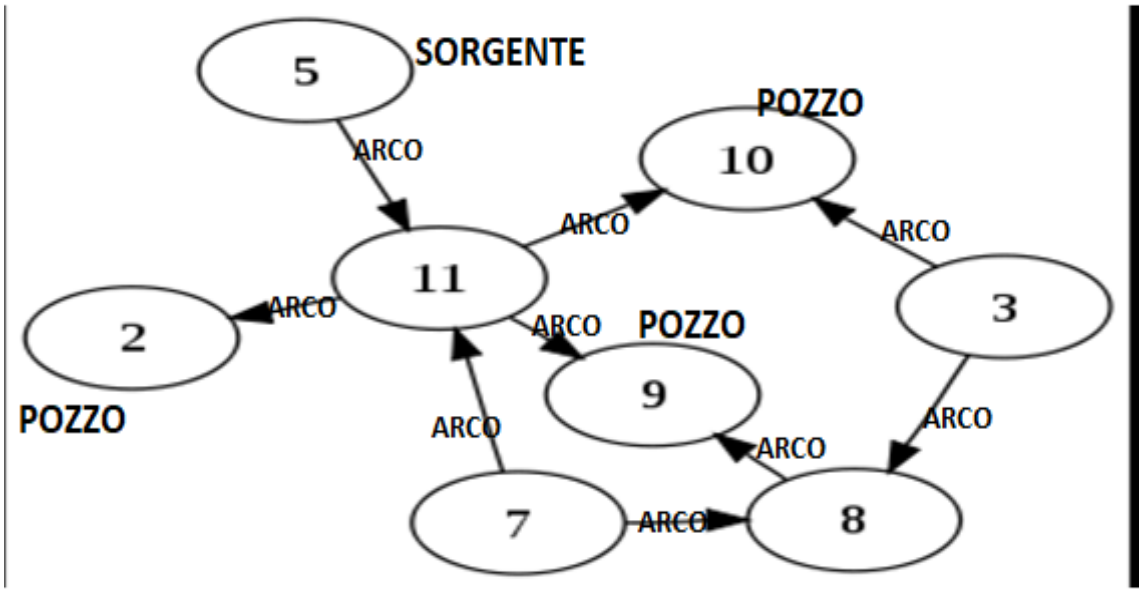
[105] La scalabilità è legata alla capacità della criptovaluta di poter convalidare tutte le operazioni che vengano effettuate in un determinato intervallo temporale. Come già detto questo è uno dei principali problemi del Bitcoin, i cui blocchi sono di grandezza di un solo megabyte. In questo modo possono essere effettuate solo 7 transazioni al secondo.

orientato" (dall'inglese "Directed Acyclic Graph, DAG), una particolare categoria di grafo diretto o digrafo.

Il digrafo è la struttura più generale di un semplice grafico ad albero. In un grafico ad albero vi è una sorgente comune ed un insieme di nodi, posizionati in più livelli. Il digrafo, al contrario del grafico ad albero, non ha una struttura così organizzata, ma ad ogni "sorgente", corrispondono dei nodi non ordinati in maniera regolare

Per esemplificare cosa sia un digrafo se ne riporta uno nella figura 2.12.

FIGURA 2.12[106]



[106] Nella figura i numeri cerchiati rappresentano i nodi, le frecce invece gli "archi" che collegano i vari nodi. Come si può notare, per esempio, è possibile passare dal "5" all'"11", ma non viceversa. Questo tipo di strutture sono alla base del Tangle di IOTA. In un DAG vengono identificati le "sorgenti" ed i "pozzi": i primi sono tutti i nodi che si trovano alla fine di un "arco" e non ne rappresentano l'inizio di un altro, i secondi invece sono tutti i nodi che sono inizio di almeno un "arco", ma non rappresentano la fine di nessun arco.

All'interno del digrafo sono appunto presenti dei "nodi", ovvero le "caselle" del grafico, e degli "archi" ovvero il percorso necessario per giungere da un nodo ad un altro. Il digrafo si può rappresentare mediante una struttura matriciale i cui valori sono ottenuti dalle combinazioni tra i nodi e le traiettorie. La struttura può essere riassunta nella seguente equazione:

$$D = (Q, U)$$

"D" è appunto il Digrafo, "Q" è l'insieme finito dei nodi nel grafo e "U" (con U $\subseteq$[107] Q×Q) come insieme degli "archi" di "D". Gli archi sono tutti i collegamenti tra nodi possibili che esistono all'interno del digrafo. Un digrafo diretto è un particolare tipo di digrafo che non ha cicli, nel senso che da qualunque nodo si parta non è possibile tornare a quello stesso nodo percorrendo gli archi del grafo.

In un DAG si definiscono "pozzi" tutti i nodi che sono alla fine di un "arco", ma non ne rappresentano l'inizio di un altro; sostanzialmente essi sono gli ultimi nodi raggiunti da una transazione. Si definiscono invece "sorgenti" tutti i nodi che sono inizio di almeno un "arco", ma non rappresentano la fine di nessun arco.

L'innovazione del Tangle sta nel fatto che le transazioni vengono processate in parallelo, perché ogni transazione segue l'arco desiderato, nel senso che è singolarmente autenticata, non viene inserita in un blocco. In IOTA non esiste il mining e i blocchi, quindi le transazioni del Tangle vengono confermate in maniera asincrona[108].

Quando un utente vuole effettuare una transazione per il tramite di IOTA, il sistema preveda che egli debba prima di tutto autenticarne altre due transazioni[109]. Gli utenti che effettuano transazioni quindi diventano direttamente dei nodi del network. Per autenticare le transazioni, come avviene nella blockchain, il nodo deve prestare la sua

[107] Indicando con il simbolo l'inclusione dell'insieme U in quello formato da Q x Q.

[108] In informatica il termine fa riferimento a modalità di trasmissione dati che non dipendono dal compiersi di altri processi. Le transazioni vengono confermate una ad una.

[109] Questo sistema è stato pensato per permettere alla comunità IOTA di migliorare la propria efficienza all'aumentare degli utenti. Obbligando gli utenti ad autenticare due transazioni prima di veder autenticata la propria fa sì che essi siano costretti a partecipare al network.

potenza computazionale per la risoluzione di un hash. In questo modo il network IOTA può scalare in maniera direttamente proporzionale alla crescita del network. Più utenti effettueranno transazioni con IOTA più il sistema si velocizzerà. Nell'autenticazione di un'operazione il nodo verifica che le unità di IOTA trasferiti giungano da una sorgente, questo avviene ripercorrendo all'indietro la traiettoria dell'unità IOTA considerata. Se la verifica non incappa in irregolarità, la transazione viene confermata.

CARATTERISTICHE DI IOTA:

1) Nessun costo di transazione: per l'invio di una transazione di IOTA, il dispositivo del mittente deve verificare due transazioni precedenti nel Tangle, effettuando un'operazione di "Proof of Work[110]". In IOTA manca la differenziazione tra "utente" e "miner". Tutti i soggetti che partecipano al network sono nodi della rete IOTA e devono obbligatoriamente "lavorare" per potervi partecipare.

2) **Infinitamente scalabile:** visto che per inviare una transazione occorre prima confermarne altre due, all'aumentare degli utenti aumenta anche l'efficienza della rete. Viene in questo modo superato il problema di altre criptovalute che consentono un numero limitato di operazioni al secondo. Più cresce il network più IOTA velocizza le proprie transazioni. Il sistema si adegua alle proprie dimensioni.

3) **Transazioni rapide**: i tempi di esecuzione delle transazioni sono inversamente proporzionali al numero di transazioni nel Tangle. Quando IOTA raggiungerà un'adozione di massa, le transazioni saranno praticamente istantanee.

[110] Con il termine si intende che il servizio di transazione viene ripagato dal lavoro dell'utente che deve appunto convalidare altre due transazioni per veder convalidata la propria. Il sistema in questo senso è "autogestito" dagli aderenti.

4) **Offerta di moneta fissa:** tutte le unità esistenti sono stati creati nel "genesis block", e tale quantità non varierà mai. La quantità totale corrisponde a 2.779.530.283.277.761 iota.

Prima di procedere con l'osservazione dell'andamento del prezzo di IOTA nel mercato è necessario effettuare una precisazione riguardante la nomenclatura.

Iota	= 1 Iota	= 1i	= 1i
KiloIota	= 1 Kiota	= 1Ki	= 1.000i
MegaIota	= 1 Miota	= 1Mi	= 1.000.000i
GigaIota	= 1 Giota	= 1Gi	= 1.000.000.000i
TeraIota	= 1 Tiota	= 1Ti	= 1.000.000.000.000i
PetaIota	= 1 Piota	= 1Pi	= 1.000.000.000.000.000i

La classificazione sopra fatta è importante perché i dati relativi al prezzo di IOTA vengono fatti tenendo come unità di riferimento il "Miota" e non, come ci si potrebbe aspettare, "Iota".

Per quanto riguarda l'andamento di mercato di IOTA, non è stato possibile recuperare i dati relativi al periodo tra il 2015 e il giugno 2017. I dati a disposizione partono dal 13 giugno 2017, quando il "Miota" si trovava circa al valore di 0,5 dollari.
Il prezzo di Miota ha oscillato tra i 10 centesimi di dollaro ed i 60 centesimi di dollaro nel periodo tra metà giugno 2017 ed inizio agosto. Il 17 agosto la criptovaluta ha raggiunto per la prima volta il valore di un dollaro. A seguito del trend rialzista del mercato delle criptovalute a partire dal novembre 2017 è cominciata un'impennata del prezzo che ha portato Miota a raggiungere il massimo di tutti i suoi valori; prima il 6 dicembre 2017

quando ha raggiunto il suo picco nel cambio con il BTC (0,00044531) e poi il 19 dicembre dello stesso anno quando ha toccato il valore di 5,37 USD, 1.117.890.000 come volume di transazioni nelle 24 ore ed una capitalizzazione di mercato poco inferiore ai 12 miliardi di dollari.

Il grafico seguente riportato da https://coinmarketcap.com mostra l'andamento del prezzo del Miota a partire dal giugno 2017. Oltre al prezzo relativo in USD, nel grafico è riportato il prezzo in BTC, il volume delle transazioni nelle 24 ore e la capitalizzazione di mercato.

GRAFICO 2.6

Per meglio individuare le differenze tra IOTA e la criptovaluta più importante, il Bitcoin, viene proposta una tabella di confronto.

TABELLA 2.6[111]

	BITCOIN	**IOTA**
NUMERO DI UNITA' MASSIME	21 milioni di unità	2.779.530.283.277.761 unità.
TECNOLOGIA UTILIZZATA PER LA CONVALIDA DELLE TRANSAZIONI	Blockchain.	Tangle.
INTERVALLO BLOCCHI	Ogni 10 minuti	Non esistono, viene generato sulla singola transazione.
OPERAZIONI CONVALIDABILI	7 al secondo	Le transazioni aumentano all'aumentare del network, visto che per la convalida della sua transazione un utente deve convalidarne altre due.
DISTRIBUZIONE MONETA	100% a coloro che risolvono l'hash del Blocco (Minatori)	Non è previsto il Mining. Tutte le unità previste sono state generate al momento della nascita del sistema IOTA.

[111] La tabella confronta le principali caratteristiche di Bitcoin e IOTA.

2.4 LE CRIPTOVALUTE 2.0

Le criptovalute 2.0, dette anche criptovalute "piattaforme", sono nate da un'idea di Vitalik Buterim[112], tra il 2013 ed il 2015. Buterim è l'inventore di Ethereum; l'idea del programmatore canadese è stata quella di sfruttare la tecnologia blockchain a 360 gradi, non limitando l'utilizzo della stessa all'applicazione nel mondo delle criptovalute. Quasi parallelamente all'idea di Buterim si è sviluppata un'altra piattaforma di funzionamento simile, quella di NEO.

Le piattaforme sono uno sviluppo del web 3.0 nel senso che hanno l'obiettivo di permettere l'amplia diffusione della "Smart Economy" per il tramite dello sviluppo di larga scala delle applicazioni, dei software condivisi e dei contratti intelligenti. Lo sviluppo della Smart Economy in queste piattaforme è favorito dalla struttura open-source ed in generale dalla possibilità di condivisione delle informazioni tra tutti gli utenti. Ogni applicazione e software sono scaricabili gratuitamente dagli utenti e i loro script sono "aperti" ad ogni soggetto che voglia consultarli.

2.4.1. ETHEREUM

Ethereum, a differenza di Bitcoin, non è solo una criptomoneta: esso è una piattaforma decentralizzata per la gestione di contratti intelligenti. Mentre Bitcoin ha lo scopo di fungere da mezzo di scambio virtuale, il fondatore di Ethereum, Vitalik Burerim, non ha voluto limitare solo a questa funzione il suo progetto. Il concetto di piattaforma è molto più ampio rispetto a quello di criptovaluta. La piattaforma Ethereum è anche una criptomoneta, la coin che gira nel network Ethereum è appunto l'Ether (ETH in sigla), ma la sua caratteristica principale è quella di essere una piattaforma all'interno della quale è possibile sviluppare applicazioni, software e "Smart Contract". Il funzionamento di

[112] È un programmatore canadese, di origini russe. È l'Inventore di Ethereum, che è stata progettata nel 2013 quando il ragazzo aveva appena 20 anni.

questi contratti si sostanzia nella programmazione di applicazioni che eseguono in maniera autonoma esattamente quanto è stato programmato al momento dell'accordo tra le parti. In questo modo non vi è alcuna possibilità di tempi di fermo, censura, frode o interferenza da parte di terzi. L'idea di Buterim, nel momento in cui ha iniziato a sviluppare Ethereum nel 2013 è stata quella di sfruttare al massimo tutte le potenzialità della blockchain; egli infatti riteneva che un utilizzo della tecnologia come semplice "libro mastro" degli scambi di una criptovaluta fosse limitante.

FIGURA 2.13[113]

Lo sviluppo di Ethereum è iniziato nel 2013 e la prima versione del software è divenuta disponibile a partire dal febbraio 2014. Da allora sono state rese pubbliche una serie di versioni del software che hanno introdotto e sviluppato tre nuovi linguaggi di programmazione[114] per la scrittura di Smart Contract.

Per il finanziamento dello sviluppo della piattaforma è stata lanciata per la prima volta un'offerta pubblica di pre-vendita di Ether, in una forma simile a quella delle IPO (initial pubblic offering), che ha permesso di raccogliere circa 19 milioni di dollari in BTC.

In estrema semplicità Ethereum potrebbe essere presentato come il più grande computer condiviso che è in grado di erogare una enorme potenza disponibile ovunque e per sempre. Ethereum è in altre parole una piattaforma di tipo computazionale che viene "remunerata" attraverso scambi che vengono effettuati per il tramite di Ether. È

[113] In figura è riportato il logo di Ethereum.

[114] Nello specifico i linguaggi di programmazione sono: il Serpent (ispirato al linguaggio Python), il Mutan (ispirato al linguaggio Go) e LLL (ispirato al linguaggio di programmazione Lisp).

una piattaforma che può essere adottata da tutti coloro che desiderano entrare a far parte della Rete e che in questo modo avranno a disposizione una soluzione che consente a tutti i partecipanti di disporre di un archivio condiviso ed immutabile. Il progetto Ethereum è flessibile e adatto all'utilizzo in diversi ambiti applicativi, si può definire come una "Programmable Blockchain" che non si limita a permettere di svolgere "operazioni" predefinite e standardizzate, ma permette agli utenti di creare le proprie personali "operazioni".

Alla base del funzionamento di tutto il network Ethereum vi è la criptovaluta coin della piattaforma, l'Ether. Esso è utilizzato per l'effettuazione di tutte le transazioni e le operazioni all'interno della piattaforma. Ad esempio un utente che voglia "far girare" un proprio contratto all'interno di Ethereum deve pagare tale servizio al sistema in Ether. In modo analogo, uno sviluppatore di un'applicazione o di un software per il tramite della piattaforma deve "pagare" il servizio offerto da Ethereum. Il pagamento può avere o attraverso esborsi di Ether detenuti dal soggetto, ovvero attraverso il "lavoro" del soggetto; cioè attraverso la concessione della propria potenza computazionale per garantire il sistema Ethereum[115].

Per quanto riguarda il funzionamento della blockchain di Ethereum essa ha le stesse caratteristiche di quella Bitcoin: funzione fondamentale è quella svolta dai "minatori" che creano i blocchi e convalidano le transazioni. Un blocco viene generato in media ogni 15 secondi e come ricompensa per il lavoro svolto i minatori ricevono 15 Ether a Blocco. Non è stato previsto dal sistema un numero massimo di Ether che possano essere emessi, per tale motivo attualmente sono in circolazione circa 100 milioni di Ether. Il numero di Ether, secondo quando previsto attualmente dal sistema, continuerà ad aumentare costantemente secondo lo schema prestabilito. Non è però da escludere che possa essere proposta dai programmatori una modifica alla crescita illimitata del

[115] Il lavoro consiste sostanzialmente nel generare i blocchi. Per tale servizio il minatore viene remunerato, come in Bitcoin, con la criptomoneta Ether.

numero di Ether che, se accettata dal network, potrebbe portare ad una riduzione graduale della loro emissione, come avviene per esempio con Bitcoin.

SMART CONTRACT

La caratteristica distintiva di Ethereum, nonché la sua innovazione più importante, è l'introduzione degli "Smart Contract". I contratti intelligenti sono protocolli informatici che facilitano, verificano, o fanno rispettare, la negoziazione o l'esecuzione parziale o totale di un contratto[116]. Sostanzialmente sono dei contratti che vengono eseguiti in maniera automatica da un sistema. Con dei contratti di questo tipo molti tipi di clausole contrattuali possono essere rese parzialmente o integralmente automatizzate, auto-ottemperanti, o entrambe le cose. Gli smart contract aspirano ad assicurare una sicurezza superiore alla contrattualistica esistente e a ridurre i costi di transazione associati alla contrattazione.
A garanzia dei contratti intelligenti è posta la piattaforma Ethereum stessa[117], la quale si occupa di autorizzare, convalidare ed autenticare i contratti.

Dopo una rapida visione dell'universo Ethereum è necessario osservare l'andamento della criptomoneta sul mercato.

Dall'agosto 2015, primi dati a disposizione per quanto riguarda Ether, fino al febbraio 2016, il prezzo della criptovaluta si è aggirato tra uno e due dollari. La prima salita drastica del prezzo lo ha portato a raggiungere i 15 dollari nel marzo 2016. Da qui ad un anno il prezzo è rimasto stabile in questo livello, per poi salire, seguendo il trend di tutto

[116] Per fare un esempio uno "smart contract" potrebbe essere stipulato e programmato per garantire che al verificarsi di un determinato evento una delle due parti debba pagare una predeterminata cifra. Qualora tale evento si dovesse verificare lo smart contract procederebbe automaticamente al pagamento della cifra a colui che ha diretto di riceverla.
[117] La piattaforma funziona per il tramite dell'operato dei minatori, che concedono la potenza computazionale per garantire la sicurezza e l'efficienza della piattaforma, attraverso la creazione dei blocchi e l'autenticazione degli stessi.

il mercato delle crypto, fino a raggiungere dai 15 dollari di marzo i 380 dollari del 20 giugno 2017. In questa data l'Ether ha raggiunto il suo livello massimo di cambio con il Bitcoin (0,1506BTC). Dopo qualche mese di flessione, Ether ha ripreso a salire in maniera esponenziale, ed ha raggiunto il massimo storico in termini di cambio con il dollaro (1400 USD), di capitalizzazione di mercato (134.728.863.762) e di volumi nelle 24 ore (4.940.690.000 USD) il 15 gennaio 2018.

Il grafico 2.7 riportato da https://coinmarketcap.com, mostra l'andamento di Ether tra agosto 2015 e 30 aprile 2018.

GRAFICO 2.7

Di seguito viene proposta una tabella che mette a confronto la tecnologia Bitcoin con quelle Ethereum. La tabella mette in evidenza le caratteristiche più importanti delle due criptovalute e le loro principali differenze.

TABELLA 2.7

	BITCOIN	**ETHEREUM**
NUMERO DI UNITA' MASSIME	21 milioni di unità.	Ammontare illimitato, viene generato circa un Ether al secondo.
TECNOLOGIA UTILIZZATA PER LA CONVALIDA DELLE TRANSAZIONI	Blockchain.	Blockchain.
INTERVALLO BLOCCHI	Ogni 10 minuti.	Ogni 15 secondi.
OPERAZIONI CONVALIDABILI	7 al secondo.	Circa 40 transazioni al secondo.
PARTICOLARITA'	---	Possibilità di generare contratti intelligenti.

2.4.2. NEO

NEO[118] è la seconda più importante piattaforma blockchain dopo Ethereum; esso è un progetto di sviluppatori cinesi, lanciato poco dopo Ethereum nel febbraio 2014, che mira a competere con la prima piattaforma. L'obiettivo ambizioso di NEO è quello di aiutare il cambiamento economico attraverso lo sviluppo della "Smart Economy". Il progetto NEO gestisce nella propria piattaforma contratti intelligenti e sviluppo di software per il tramite di un pagamento con la coin della piattaforma, ovvero il NEO. La piattaforma funziona per il tramite di un blockchain i cui blocchi sono generati ad intervalli di 15 secondi l'uno. Il funzionamento del network è sempre garantito dai minatori, i quali creano ed autenticano in blocchi e vengono per questo ricompensati del loro lavoro con

[118] Il nome deriva dal greco e vuol dire "novità", https://neo.org/.

un ammontare di criptomoneta. I programmatori di NEO, pur ammettendo la similitudine del proprio progetto rispetto a quello Ethereum, individuano un vantaggio in termini di scalabilità, ovvero di numero di operazioni autenticabili dalla propria blockchain ogni secondo. Differenza importante rispetto ad Ethereum è quella che NEO supporta diversi linguaggi informatici di uso comune, come per esempio Microsoft.net e Java; Ethereum al contrario richiede una conoscenza specifica dei propri linguaggi di programmazione. Un'altra difformità tra il progetto NEO e quello Ethereum sta nella quantità di unità di NEO che possono essere emesse, il limite è fissato a 100 milioni di unità.

FIGURA 2.14[119]

Le unità di NEO non sono divisibili, infatti non è possibile acquistare per esempio 0,5 NEO. Il numero di NEO detenibili deve essere sempre un numero intero. Per questo motivo per le operazioni all'interno del network vengono utilizzati come criptovaluta di scambio il "GAS" una criptomoneta subordinata a NEO, ma funzionante nello stesso network[120]. Tutti coloro che detengono per un determinato periodo di tempo dei NEO

[119] In figura è riportato il logo di NEO.

[120] I cosiddetti Token analizzati nella prima parte di questo capitolo.

nel proprio portafoglio ricevono una quantità di GAS[121] proporzionale all'ammontare di NEO detenuti, come se fosse una specie di "dividendo". In questo modo i detentori di NEO sono incentivati a detenere a lungo la criptomoneta.

In un primo momento, l'interesse per NEO non fu così importante, tanto che il prezzo della criptovaluta è rimasto dal momento della sua quotazione sul mercato nel 2014 fino alla metà del 2017 tra i 0,50 dollari e un dollaro. A metà 2017 seguendo il trend di tutto il mercato il prezzo della criptovaluta è cresciuto in maniera esponenziale, fino a raggiungere i suoi massimi i termini di cambio con il dollaro (160 USD), di cambio con il Bitcoin (0,014772 BTC), di capitalizzazione di mercato (10.537.150.000 USD) e di volumi di mercato nelle 24 ore (633.048.000 USD) il 30 gennaio 2018.

GRAFICO 2.8[122]

[121] Vengono generati 0.00000008 GAS per NEO posseduto, ogni volta che viene eseguito un blocco.

[122] Il grafico riportato da https://coinmarketcap.com/currencies/neo/, mostra l'andamento del prezzo del NEO dal settembre 2016 al 30 aprile 2018.

Nella tabella sotto riportata è fatto un confronto tra le principali caratteristiche di NEO e quelle di Bitcoin ed Ethereum. In questo caso il confronto anche con Ethereum è d'obbligo, essendo NEO dichiaratamente un suo concorrente.

TABELLA 2.8

	BITCOIN	**ETHEREUM**	**NEO**
NUMERO DI UNITA' MASSIME	21 milioni di unità.	Ammontare illimitato.	100 milioni di unità.
TECNOLOGIA UTILIZZATA CONVALIDA	Blockchain.	Blockchain.	Blockchain.
INTERVALLO BLOCCHI	Ogni 10 minuti.	Ogni 15 secondi.	Ogni 15 secondi.
OPERAZIONI CONVALIDABILI	7 al secondo.	Circa 40 transazioni al secondo.	Circa 50 transazioni al secondo.
PARTICOLARITA'	---	Possibilità di generare contratti intelligenti. Linguaggio di programmazione specifico per Ethereum.	Possibilità di generare contratti intelligenti. Conformità a più linguaggi di programmazione, anche utilizzati in altri ambiti, quali ad esempio Java e Microsoft.net

2.4.3 ICO

L'ICO (Initial Coin Offering), è una raccolta fondi per il tramite della quale viene offerto un "Token" o una "Coin" attraverso una piattaforma blockchain in cambio di denaro valuta fiat o di un'altra criptovaluta (come per esempio Ether, NEO o Bitcoin). Le ICO avvengono all'interno delle piattaforme come Ethereum e NEO e sono implementate attraverso uno Smart Contract. Sostanzialmente viene generato uno Smart Contract studiato in modo che le due controparti siano: la società o il soggetto che vuole immettere nel mercato il Token o il Coin; il soggetto che intende sottoscrivere l'ICO. Attraverso questo contratto, il sottoscrittore riceverà la criptovaluta immessa nel mercato alla scadenza prestabilita dal contratto. I proventi raccolti attraverso l'ICO sono impiegati per finanziare l'impresa o il progetto di coloro che hanno lanciato l'offerta.
Il meccanismo di finanziamento per il tramite delle ICO ricorda quello effettuato dalle società che vogliono quotarsi in borsa attraverso l'IPO[123] (Initial Pubblic Offering). Anche se simile nello scopo, l'ICO è profondamente differente rispetto all'offerta pubblica iniziale. In primo luogo le criptovalute sono asset digitali, ma non rientrano in maniera specifica in uno strumento finanziario regolato in maniera chiara dai legislatori. I soggetti che si mettono in lista per partecipare ad un IPO sono tutelati dalla normativa ed hanno diritto di non acquista le azioni di nuova emissione fino al giorno di effettiva quotazione dell'azione. L'aspetto più importante da sottolineare è che coloro che partecipano ad un IPO acquistano le azioni di una società; essi diventano azionisti della stessa. I soggetti che comprano una criptovaluta non diventano azionisti della società che propone l'ICO, anche se dal punto di vista della società emittente il risultato, cioè quello di raccogliere fondi per finanziare la crescita ed i propri progetti, è lo stesso.

[123]Le IPO (Initial Public Offering) sono utilizzate dalle società per raccogliere il capitale nel mercato, con la differenza che le società in questione non raccolgono il capitale con la vendita delle proprie azioni. Le IPO sono sottoscritte solitamente con un Banca d'investimento, con una Società d'Intermediazione Mobiliare (SIM) o con gruppi di Intermediari Finanziari, i quali si occupano di promuovere l'IPO e di garantire la sottoscrizione di una soglia minima di azioni. I soggetti in questione sottoscrivono in prima persona le azioni e poi le vendono agli investitori, quindi si assumono il rischio che tali azioni possano non essere vendute.

I token o i coin oggetto delle ICO possono essere scambiati ed utilizzati come una normale criptovaluta, ma il loro funzionamento e l'autenticazione delle loro transazioni avviene nella stessa blockchain della piattaforma nella quale sono lanciati.

I soggetti che "lanciano" l'ICO, definiti "sponsor", di solito forniscono l'accesso ad un "white paper[124]" che descrive il progetto, i membri chiave del team, e i termini chiave dell'ICO (ad esempio, i termini economici, i dettagli del contratto e le tempistiche).

Nel processo di sottoscrizione, il partecipante in genere è tenuto a trasferire criptovaluta o una moneta fiat ad uno o più indirizzi designati o ai portafogli online dello "sponsor" ICO. Le iscrizioni possono essere completate in pochi minuti. Un soggetto può anche essere ricompensato con token dell'ICO anche svolgendo alcuni compiti per la società emittente, come ad esempio, il marketing sui forum di criptovaluta. Una volta completato l'ICO, i token ICO vengono distribuiti agli indirizzi designati o ai portafogli online dei partecipanti.

[124]Con il termine "White Paper" (libro bianco), si indica una relazione pubblicata da un governo nazionale o da una società su un determinato argomento o settore di attività. I "libri bianchi" sono utilizzati prevalentemente come strumento di promozione di una tecnologia o di un prodotto, sottolineandone le caratteristiche principali, i possibili utilizzi e i punti di forza.

CAPITOLO 3

INVESTIMENTI IN CRIPTOVALUTE

Questo capitolo conclusivo della tesi ha come obiettivo quello di analizzare le possibilità di creazione di un portafoglio di criptovalute che possa sfruttare al meglio le opportunità di investimento in un'ottica di massimizzazione del rendimento o di minimizzazione del rischio. Oggetto di particolare attenzione è la correlazione tra i rendimenti delle varie criptovalute considerate, in particolare quella riguardante le categorie crypto individuate nel capitolo 2.

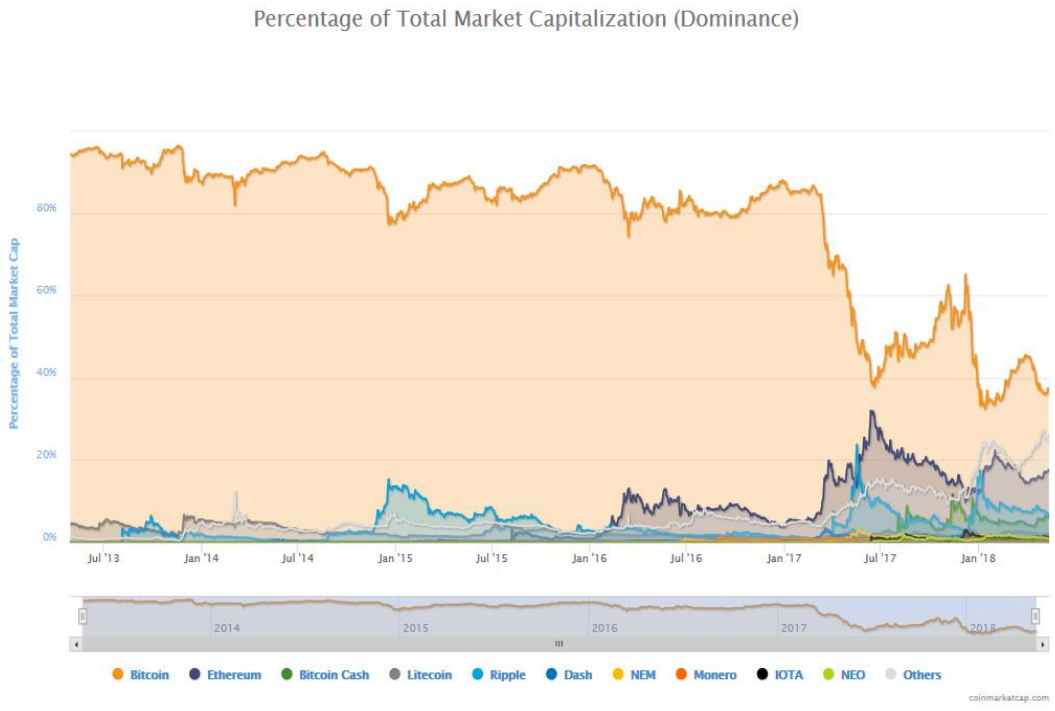
Fino a pochi anni fa parlare di creazione di un portafoglio di criptovalute poteva sembrare inappropriato; la maggior parte della capitalizzazione di mercato di questo "settore" era infatti quasi totalmente coperta dal Bitcoin. In un contesto così, la liquidità delle criptovalute meno importanti rispetto al Bitcoin non era tale da poter permettere di effettuare investimenti sicuri dal punto di vista del cambio della criptovaluta in moneta fiat.

Come si può notare dalla figura che segue, negli ultimi anni si è notevolmente ridotto il peso del Bitcoin nel mercato totale delle criptovalute. Nel giugno 2013, quando parte l'analisi di del sito CoinMarketCap dal quale è ripotato il grafico 3.1, la capitalizzazione di mercato del Bitcoin era il 95% di quella totale del settore delle criptovalute. Negli anni successivi, con l'entrata in gioco delle nuove criptovalute, l'incidenza della capitalizzazione di mercato del BTC su quella totale del settore si è ridotta in maniera graduale ma costante fino al gennaio 2017. Di li in poi la discesa è stata più rapida,

causata dal sempre maggiore interesse nel mondo delle criptovalute e dall'investimento effettuato da molti soggetti anche sulle criptovalute alternative a quella creata da Satoshi Nakamoto. Nel giugno 2017 si è raggiunta una sostanziale tripartizione della capitalizzazione di mercato del settore. Il BTC è sempre rimasto al primo posto, ma con una percentuale del 37%, a seguirlo Ethereum con il 32% e Ripple con il 10%. La rimanente parte era distribuita tra le altre principali crypto che si attestavano di poco sopra o attorno l'1%. I dati alla fine di aprile 2018 sono rimasti più o meno uguali per quanto riguarda il rapporto capitalizzazione di mercato del BTC su capitalizzazione totale (attorno al 36%), si sono invece ridotte le percentuali di Ethereum (16%) e di Ripple (8%), vedendo però aumentata l'incidenza di altre criptovalute come ad esempio il BitcoinCash (6%).

Il grafico 3.1 mostra il rapporto tra la capitalizzazione di mercato delle singole criptovalute e la capitalizzazione di mercato totale del mercato crypto.

GRAFICO 3.1



Attualmente, pur non essendo un mercato del tutto liquido, il grande numero di exchange che hanno "adottato" un elevato numero di criptovalute permette di operare in questo settore con più tranquillità; inoltre, l'importante interesse generato anche a livello mediatico ha portato ad una crescita della capitalizzazione di mercato di settore molto importante, che ha superato, nel suo momento di massimo, gli 800 miliardi di dollari. Un mercato come quello delle criptovalute, pur essendo per molti versi atipico, alternativo e non regolamentato[125], ha raggiunto un livello di capitalizzazione e di volumi che non possono più essere ignorati.

Il grafico in figura 3.2, mostra l'andamento della capitalizzazione di mercato di tutto il mercato delle criptovalute. Questo mercato, dopo avere raggiunto i suoi massimi a gennaio 2018 ha subito un pesante crollo che tuttavia è durato solamente per due mesi, da marzo 2018 la capitalizzazione totale ha ripreso a salire sfiorando nuovamente i 500 miliardi di dollari.

Il grafico 3.2 è tratto da https://coinmarketcap.com/charts/.

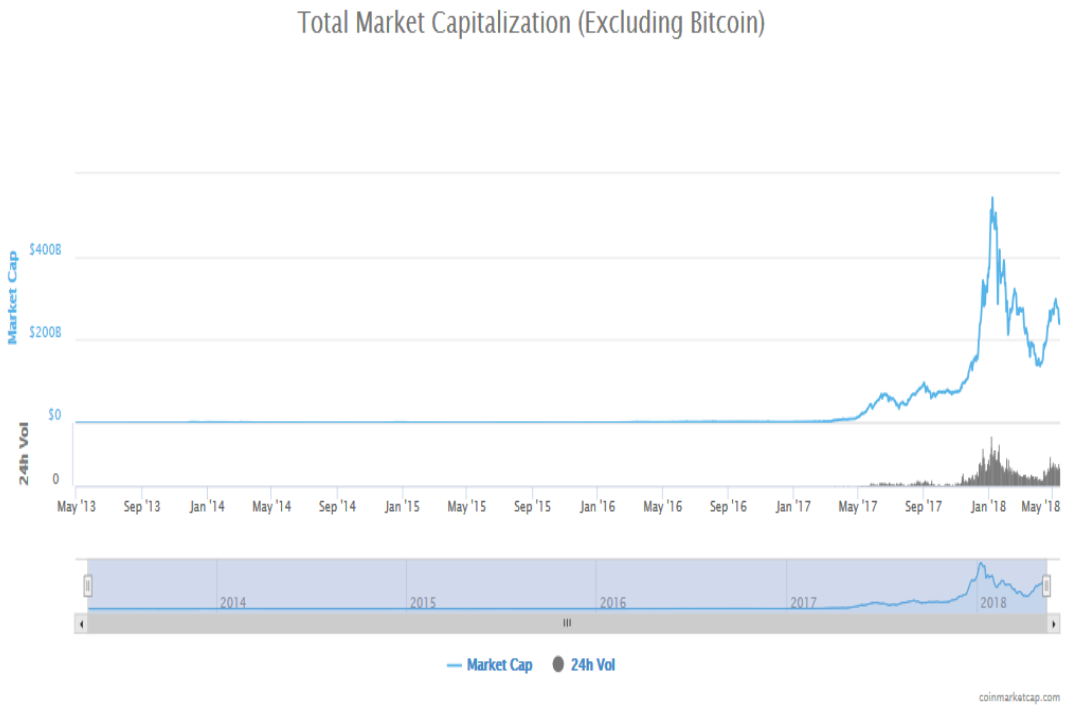
GRAFICO 3.2

[125]La non regolamentazione del mercato se da un certo punto di vista lo svantaggia d'altro, a mio avviso è uno dei fattori principali per i quali è possibile ottenere rendimenti così importanti in questo mercato.

A testimonianza di quanto detto sin ora si può osservare il grafico della capitalizzazione di mercato delle criptovalute senza considerare il Bitcoin. Come riportato dalla figura sottostante si può vedere che il mercato crypto ha raggiunto livelli considerevoli di "Market Capitalization" anche senza considerare Bitcoin.

Il grafico 3.3, riportato da https://coinmarketcap.com/charts/, fa riferimento alla somma della capitalizzazione di mercato di tutte le criptovalute escludendo quella del Bitcoin.

GRAFICO 3.3



3.1 PROBLEMATICHE DEL MERCATO CRYPTO

Nonostante tutte le considerazioni fatte nel paragrafo precedente, le possibilità di creare un portafoglio diversificato di criptovalute risulta molto difficile per tutta una serie di aspetti. Il settore di riferimento infatti, come verrà sottolineato successivamente con l'ausilio concreto dei calcoli, è profondamente correlato in maniera positiva e la scarsa presenza di dati ed informazioni non permette di effettuare analisi di mercato approfondite. Non è per esempio possibile considerare degli indici settoriali o dei Beta di mercato dei singoli settori di criptovalute, introdotti nel capitolo precedente. Per tale motivo, effettuare una preselezione ed una diversificazione pur potendo risultare ragionevole dal punto di vista operativo, non potrebbe avere il supporto più importante dei dati. Partendo da queste difficoltà l'idea è quella di costruire inizialmente un portafoglio alla Markowitz[126], con un solo accorgimento, cioè quello di selezionare le criptovalute con capitalizzazione di mercato maggiore.

Al fine di selezionare un portafoglio, sono state prese in considerazione le prime 21 criptovalute per capitalizzazione di mercato nel momento nel quale viene iniziata l'analisi il 1 gennaio 2015. Il portafoglio alla Markowitz è stato creato quadrimestralmente, permettendo via via di inserire le nuove criptovalute affacciatesi nel mercato[127]. Dopo la creazione dei portafogli è stato effettuato un primo confronto tra i portafogli creati alla Markowitz in maniera statica. In questa analisi viene verificato il rendimento che il portafoglio avrebbe ottenuto nei 4 mesi successivi e nel periodo tra la sua creazione e il 30 aprile 2018 giorno dell'ultima osservazione considerata in questa tesi.

[126]Per completezza della tesi nel paragrafo 3.2 verrà riassunta brevemente la selezione del portafoglio alla Markowitz.

[127]L'analisi iniziale parte dal 1 gennaio 2015, nei quadrimestri successivi verranno aggiunte le criptovalute che si affacciano nel mercato crypto con volumi e capitalizzazioni di mercato considerevoli.

Nel corso dell'analisi quadrimestrale sono state fatte alcune considerazioni con riferimento ai volumi di mercato giornalieri fatti registrare dalle varie criptovalute. Come verrà spiegato in seguito, in taluni casi è stato ritenuto necessario eliminare delle criptovalute dall'analisi. Queste situazioni sono state determinate da un problema di liquidità creato dai bassissimi volumi di alcune criptovalute, che in alcuni giorni ha impedito la formazione di un prezzo di mercato. Essendo in questa analisi le osservazioni giornaliere, la mancanza di più dati giornalieri avrebbe impedito di effettuare le analisi media-varianza necessarie per la creazione del portafoglio.

Per i singoli periodi è stato fatto riferimento alla frontiera dei portafogli alla Markowitz e alla correlazione dei rendimenti delle varie criptovalute. Oggetto di particolare attenzione è stato il variare delle correlazioni da periodo a periodo, come verrà analizzato nel paragrafo 3.3. Le correlazioni dei rendimenti sono molto alte (spesso superiori all'80%) nei periodi "Bear" del mercato crypto, essi invece diventano più tenui, pur rimanendo comunque positivi, nei momenti "Bull". Questa considerazione, che può sembrare banale assume, una certa importanza soprattutto nei momenti in cui il mercato della criptovalute decresce, perché in tali momenti ottenere una diversificazione risulta estremamente importante per ridurre le perdite.

3.2 SELEZIONE DI PORTAFOGLIO ALLA MARKOWITZ

Nel mondo della finanza è piuttosto frequente osservare come gli investitori tendano a non concentrare la propria ricchezza in un solo titolo, preferendo al contrario detenere una ricchezza distribuita su più titoli. Un comportamento simile risponde ad una prescrizione di buon senso, secondo la quale non è opportuno tenere "tutte le uova in uno stesso cestino". Il comportamento degli investitori fa riferimento alle possibilità di considerare l'analisi rischio-rendimento associata ad ogni portafoglio finanziario.

I precetti teorici di questi comportamenti derivano dagli studi di Harry Markowitz, che per la prima volta, nell'articolo "Portfolio Selection" pubblicato nel 1952 sul "Journal of Finance" scrive della selezione di un portafoglio tenendo conto sia del rendimento atteso che del rischio. Per tale pubblicazione ed i suoi studi successive, Markowitz ricevette nel 1990 il premio Nobel per l'economia.

Prima di Markowitz l'unico indicatore utilizzato per la scelta di un titolo rispetto ad un altro era quello della "media". Attraverso il criterio della media si sceglieva il titolo in base alla media dei rendimenti passati. Sostanzialmente il "criterio della media" considera la massimizzazione della media, che viene quindi utilizzata come misura di performance di attività rischiose.

Questo criterio tuttavia non tiene conto in alcun modo del rischio. Un soggetto che scelga in base a questo criterio dovrebbe essere completamente indifferente al rischio. Per soddisfare le esigenze della maggior parte degli investitori, i quali sono avversi al rischio, è necessario tener conto nella scelta di investimento anche di una misura che quantifichi il rischio stesso.

L'intuizione di Markowitz è stata quella di utilizzare la varianza, indicatore statistico di variabilità, come misura di rischio delle attività finanziarie. Più elevata è la varianza di un titolo, più tale titolo è rischioso e viceversa.

Il metodo di creazione di un portafoglio alla Markowitz si fonda sulle seguenti ipotesi:

1) Gli investitori formano il portafoglio sulla base del rendimento medio atteso e del rischio atteso.
2) L'orizzonte temporale è uniperiodale.
3) Gli investitori sono avversi al rischio[128]
4) I costi di transazione e le imposte sono nulli, le attività sono perfettamente divisibili
5) Il mercato è perfettamente concorrenziale
6) Gli investitori sono price-taker

Dalla prima e dalla terza ipotesi elencate è implicito il principio della "Media-Varianza". Tale principio sancisce che tra due strategie di investimento sia preferibile quella che presenta maggior rendimento atteso e minor deviazione standard[129].
Dati due portafogli X e Y, il portafoglio X domina quello Y se:

$$E(r_x) \geq E(r_y) \quad \text{e} \quad \sigma_x \geq \sigma_y$$

con almeno una disuguaglianza forte. Con *E(-)* si indica il valore atteso del rendimento di X e Y, con σ invece, viene indicata la deviazione standard di X e Y.

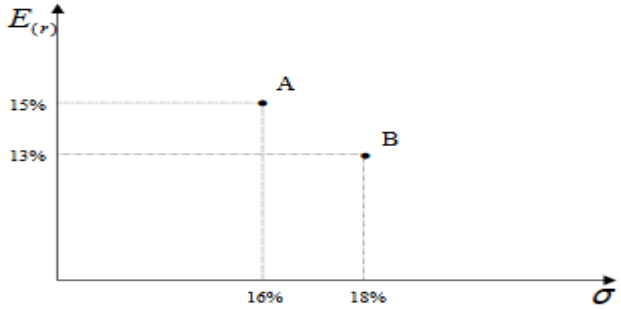
[128] L'avversione al rischio è la preferenza di un agente economico per un ammontare certo più che per uno aleatorio. Più precisamente, l'agente preferisce ricevere il valore atteso di una variabile aleatoria (ad esempio una lotteria) rispetto al valore che la variabile può assumere.
[129] Il principio è conosciuto come quello di "media-varianza" perché nel suo articolo, Markowitz fece riferimento alla varianza e non alla standard deviation.

Per esemplificare il funzionamento del metodo “media-varianza” si procede con alcuni esempi:

Esempio 1

Portafoglio A: $E(r_A) = 15\%$ $\sigma_A = 16\%$

Portafoglio B: $E(r_B) = 13\%$ $\sigma_B = 18\%$



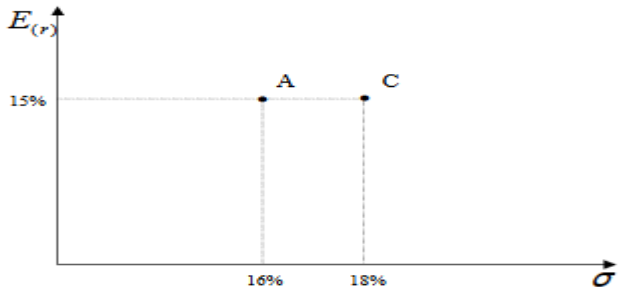
Nel grafico dell’esempio 1 nell’asse delle ascisse viene indicata la deviazione standard in quello delle ordinate invece il rendimento.

Il portafoglio A ha un rendimento maggiore ed una varianza inferiore rispetto al portafoglio B (formato dal solo titolo B). Il portafoglio A quindi domina il portafoglio B secondo il criterio “Media-Varianza”.

Esempio 2

Portafoglio A: $E(r_A) = 15\%$ $\sigma_A = 16\%$

Portafoglio C: $E(r_C) = 15\%$ $\sigma_C = 18\%$

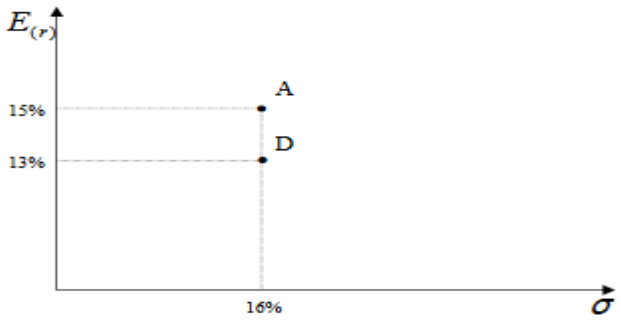


Nell'esempio 2 il portafoglio A ha lo stesso valore atteso del portafoglio C, ma ha una deviazione standard inferiore. Anche in questo caso A domina C secondo il criterio "Media-Varianza".

Esempio 3

Portafoglio A: $E(r_A) = 15\%$ $\sigma_A = 16\%$

Portafoglio D: $E(r_D) = 13\%$ $\sigma_D = 16\%$



Nell'esempio 3 i portafogli A e D hanno la stessa deviazione standard, ma A presenta un valore atteso superiore di D. Anche in questa circostanza, secondo il criterio "media-varianza" A domina D.

Il criterio "media-varianza" non offre soluzioni nelle situazioni nelle quali vi sia un titolo che abbia nei confronti di un altro un valore atteso e una deviazione standard superiori o inferiori. In situazioni come queste la scelta su quale dei due investire dipenderà quindi dalla propensione al rischio dell'investitore.

Un ragionamento analogo a quello appena fatto può essere sviluppato in una situazione nella quale venga considerato un portafoglio formato da più titoli anziché da solo uno.

Passiamo ora all'analisi di un portafoglio. Il suo valore atteso è dato dalla somma dei valori attesi dei singoli titoli moltiplicata per la percentuale di portafoglio investita in tale

titolo. Sostanzialmente è sufficiente calcolare media ponderata dei rendimenti dei singoli titoli:

$$E(r_p) = \sum_{i=1}^{n} [X_i \times E(r_i)]$$ [130]

Discorso diverso va invece fatto per la stima del rischio di portafoglio. Esso non può essere calcolato sommando la deviazione standard dei singoli titoli moltiplicata per la ponderazione del titolo nel portafoglio. Calcolando il rischio in questo modo non si terrebbe conto dell'effetto diversificazione.

Per il calcolo della volatilità di un portafoglio è necessario richiamare all'indicatore statistico noto come coefficiente di correlazione lineare (**ρ**). Attraverso la correlazione è possibile capire in che modo varia il rendimento di un'attività finanziaria al variare del rendimento di un'altra.

Se si prende a riferimento il caso particolare di un portafoglio a due titoli, la varianza e la standard deviation sono rispettivamente definite dalle seguenti formule:

$$\sigma_P^2 = (X_1 \times \sigma_1)^2 + (X_2 \times \sigma_2)^2 + 2 \times X_1 \times X_2 \times \sigma_1 \times \sigma_2 \times \rho_{1,2}$$

$$\sigma_P = \sqrt{(X_1 \times \sigma_1)^2 + (X_2 \times \sigma_2)^2 + 2 \times X_1 \times X_2 \times \sigma_1 \times \sigma_2 \times \rho_{1,2}}$$ [131]

La correlazione lineare (**ρ**) viene calcolata come:

$$\rho_{1,2} = \frac{Cov_{1,2}}{\sigma_1 \times \sigma_2}$$ [132]

[130] Dove Xt è il peso del singolo titolo nel portafoglio.

[131] La varianza e la deviazione standard possono essere scritte come nelle formule.

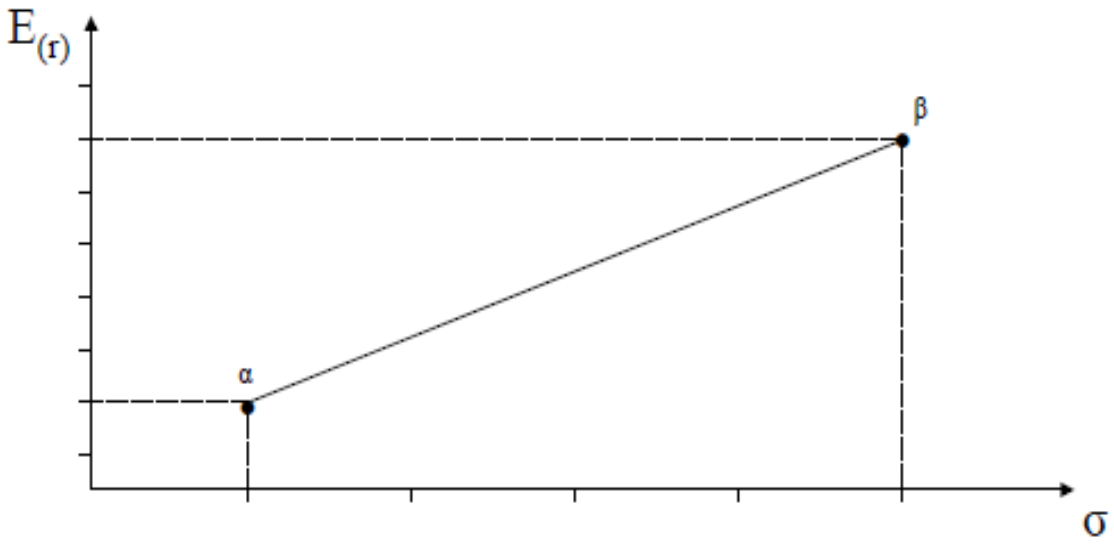
[132] La correlazione è data dal rapporto tra covarianza dei due titoli/portafogli considerati e il prodotto delle due deviazioni standard.

La correlazione è un valore compreso tra -1 e +1. Qualora il valore della correlazione sia +1 vuol dire che i due asset sono perfettamente correlati tra di loro. In questa situazione non vi è alcun beneficio di diversificazione nell'avere di asset così correlato. Se il valore della correlazione è compreso tra 0 e +1 i due asset sono correlati positivamente; il beneficio di diversificazione cresce al decrescere del coefficiente di correlazione. Nel caso in cui ρ sia uguale a -1 i due asset sono perfettamente correlati negativamente; in questa circostanza vi è la massima espressione di diversificazione. Analogamente in situazioni nelle quali il coefficiente di correlazione sia compreso tra -1 e 0 vi è una correlazione negativa sempre più marcata al diminuire del valore di ρ.

Si procede con alcuni esempi:

Sono dati due titoli α e β con correlazione tra di loro uguale ad 1, $\rho_{\alpha,\beta}$=1. I due titoli non si dominano l'un l'altro secondo il criterio media-varianza. La situazione descritta viene rappresentata dal seguente grafico. Nell'asse delle ascisse è riportata la deviazione standard di un titolo, in quella delle ordinate invece si riporta il valore atteso del rendimento.

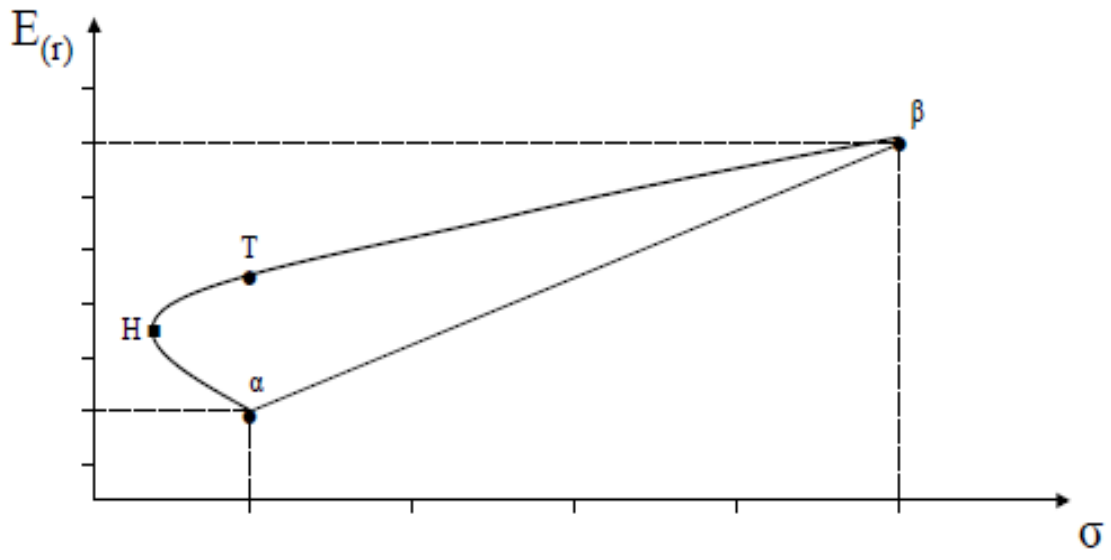
GRAFICO 3.4



I punti tra α e β rappresentano invece i portafogli formati da una combinazione lineare di investimento nel titolo α ed in quello β. Nel caso esaminato, in cui sono vietate le vendite allo scoperto, essendo la correlazione tra i due titoli uguale ad 1, nessuno dei portafogli possibili domina o è dominato da un altro portafoglio secondo il criterio media-varianza. In sostanza tutti i portafogli sono efficienti. L'insieme dei portafogli fattibili e quello dei portafogli efficienti coincidono.

Si procede ora con l'analisi della situazione nella quale i due titoli α e β abbiano una correlazione $\rho_{\alpha,\beta}$<1.

GRAFICO 3.5

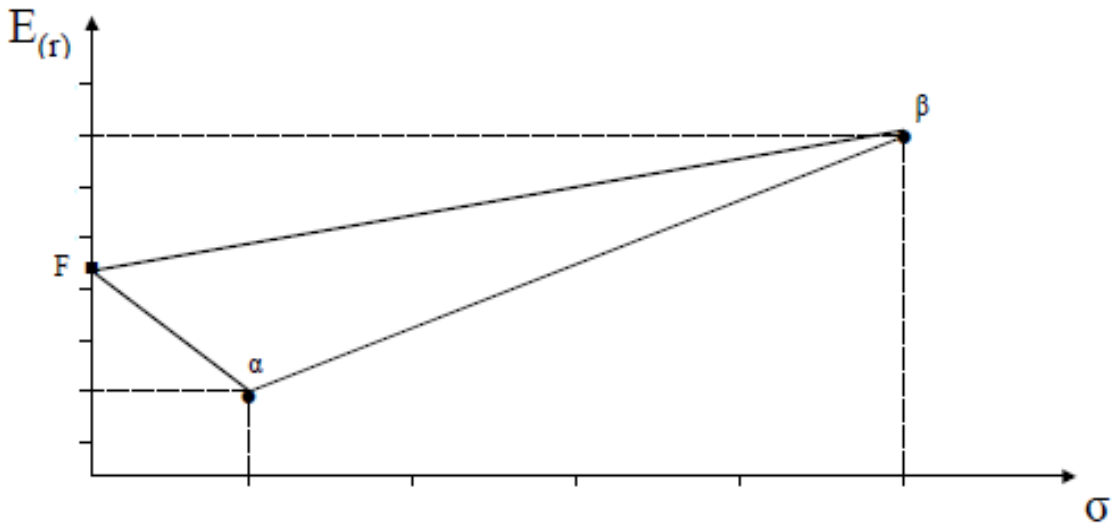


In questa circostanza le combinazioni rischio-rendimento assumono la seguente configurazione. Quando il coefficiente di correlazione è minore di 1 le combinazioni dei portafogli α e β assumono una forma curvilinea ad iperbole. A differenza del caso precedente non tutti i portafogli possibili sono anche portafogli efficienti. Il tratto $\widehat{\alpha\beta}$ rappresenta l'insieme dei portafogli possibili, $\widehat{\alpha H}$ l'insieme dei portafogli dominati mentre il tratto curvo $\widehat{H\beta}$ rappresenta l'insieme dei portafogli efficienti, la cosiddetta "frontiera efficiente". In una situazione del genere iniziano ad osservarsi i primi effetti

benevoli della diversificazione. Come si può vedere dal grafico, in una situazione come questa vi è una contrazione del rischio.

L'ultima situazione, che viene rappresentata nel grafico 3.6, è quella nella quale vi sia una correlazione tra i due titoli di -1.

GRAFICO 3.6



Nel caso di correlazione -1 i benefici ottenuti dalla diversificazione sono massimi. Come caso estremo si ottiene la situazione nella quale vi è un portafoglio F a rischio nullo. $\overline{F\beta}$ rappresenta la frontiera efficiente.

Il portafoglio ottimo per un investitore è quel portafoglio, appartenente alla frontiera efficiente, per il quale l'investitore ottimizza la propria utilità attesa.

3.3 LA SELEZIONE DELLE CRIPTOVALUTE

La situazione del mercato delle criptovalute il primo gennaio 2015 vedeva la presenza nella top 30 della capitalizzazione di mercato di alcune importanti criptovalute che hanno mantenuto la propria posizione fino ad oggi: queste sono senza dubbio il Bitcoin, Ripple, Litecoin, Dash, Monero e Stellar[133]. Ad esse si aggiungevano una serie di criptovalute che allora avevano un potenziale simile a quella delle crypto appena elencate, ma che successivamente si sono rivelate progetti non all'altezza di quelle più importanti. Nonostante non abbiano rispettato le attese queste altre criptovalute, per la maggior parte dei casi, continuano ad esistere ed hanno ottenuto dei rendimenti considerevoli, pur essendo scese gradualmente dalla classifica della capitalizzazione di mercato. Altre criptovalute, al contrario, non solo non hanno fornito i rendimenti sperati, ma addirittura sono quasi scomparse dalla circolazione e hanno raggiunto volumi di scambio talmente bassi che in alcuni giorni non è nemmeno possibile calcolarne il prezzo di mercato; si fa riferimento per esempio a FuelCoin, PayCoin e SuperNET[134].

L'analisi di questo paragrafo si concentra sulla selezione di un portafoglio di criptovalute partendo da una base di 21. Le criptovalute sono state selezionate considerando la loro capitalizzazione di mercato all'1 gennaio 2015. Obiettivo di questo paragrafo è quello di studiare i legami esistenti tra i rendimenti delle criptovalute considerate.

Nel gennaio 2015 la maggior parte delle criptovalute era formata da "Altcoin"; solo Ripple, Stellar ed Ethereum si erano già imposte come criptovalute innovative. Per quanto riguarda Ethereum, i dati riguardanti il suo prezzo e i volumi dei suoi scambi sono presenti solo a partire dall'agosto 2015, per tale motivo esso verrà inserito nell'analisi sono in un secondo momento.

[133] Le criptovalute nominate, tranne Stellar, sono state tutte analizzate nel capitolo 2. Esse verranno comunque richiamate nella tabella 1 alle pagine seguenti.

[134] Queste criptovaluta verranno brevemente analizzate nella tabella successiva.

Lo stesso discorso fatto con Ethereum va fatto anche per NEM, NEO, Z-Cash, IOTA e BitcoinCash; queste criptovalute sono state considerate dal momento nel quale è stato possibile ottenere la loro quotazione di mercato.

Nella tabella seguente sono state richiamate le caratteristiche fondamentali delle criptovalute considerate in questa analisi. La tabella seguente individua la tipologia di criptovaluta, le caratteristiche principali e il massimo numero di unità che possono essere raggiunte.

TABELLA 3.1[135]

NOME	TIPOLOGIA	CARATTERISTICHE PRINCIPALI	UNITA' MASSIME
BITCOIN (BTC)	--	--	21.000.000
BITCOINDARK (BTCD)	Altcoin.	Il nome rimanda al fatto che la criptovalute ha la caratteristica di essere più anonima del BTC.	1.288.862
BITSHARES (BTS)	Altcoin.	Criptovaluta della piattaforma di exchange Bitshares.	3.600.570.502
BLACKCOIN (BLK)	Altcoin.	Il "Bitcoin Australiano". Non presenta alcuna caratteristica particolare.	76.832.665
COUNTERPARTY (XCP)	Piattaforma.	Counterparty è una società che ha iniziato ad	2.616.436

[135] Il limite massimo di unità che possono essere emesse, può essere un indicatore approssimativo del valore che può raggiungere la criptovalute. A parità di progetto è più probabile che una criptovalute con un gran numero di unità abbia un prezzo unitario inferiore rispetto a quella che ha un numero inferiore di unità emesse.

		operare come Exchange. Dopo aver creato la propria criptovaluta Altcoin omonima ha ampliato le proprie funzioni diventando una piattaforma all'interno della quale vengono sviluppati Smart Contract. La piattaforma si concentra soprattutto in contratti di "Betting" (scommesse sportive) e contratti "Derivati".	
DASH (DASH)	Altcoin.	È stata analizzato dettagliatamente nel secondo capitolo. Pur essendo un Altcoin presenta delle caratteristiche innovative importanti ed una possibilità di rapido sviluppo grazie al sistema Poof-Of-Service.	18.900.000
DOGECOIN (DOGE)	Altcoin.	Nessuna particolare caratteristica. Punta molto sul Marketing grazie alla figura di un cane; il "Doge" abbastanza diffuso nei Social Network.	Nessun limite previsto.

FUELCOIN (FC2)	Altcoin.	Nessuna caratteristica particolare. Verrà abbandonata nel corso dell'analisi perché raggiunge livelli troppo bassi di volumi di scambio.	101.691.332
LITECOIN (LTC)	Altcoin.	Una delle prime Altcoin. Presenta intervalli dei Blocchi più brevi rispetto al Bitcoin. Se il Bitcoin è considerato "oro virtuale" Litecoin viene considerato "argento virtuale".	84.000.000
MAIDSAFECOIN (MAID)	Altcoin.	Nessuna particolare caratteristica.	Nessun limite previsto.
MONERO (XMR)	Altcoin.	La criptovaluta è stata trattata nel secondo capitolo.	18.400.000
NAMECOIN (NMC)	Altcoin.	La seconda criptovaluta. È sostanzialmente la copia di Bitcoin.	21.000.000
NXT (NXT)	Altcoin.	Nessuna caratteristica particolare.	1.000.000.000
OMNI (OMNI)	Piattaforma.	È la quarta piattaforma per importanza dopo Ethereum, NEO e NEM.	Nessun limite previsto.
PAYCOIN (XPY)	Altcoin.	Nessuna caratteristica particolare.	Nessun limite previsto.

PEERCOIN (PPC)	Altcoin.	È la criptovaluta creata dall'exchange "peercoin". Non presenta alcuna caratteristica particolare.	Nessun limite previsto.
REDDCOIN (RDD)	Altcoin.	È una criptovaluta che punta ad essere utilizzata per i pagamenti che avvengono nei social network. È utilizzata per i pagamenti delle "sponsorizzazioni" che avvengono su Facebook, Twitter, Instagram e YouTube.	56.000.000.000
RIPPLE (XRP)	Criptovaluta innovativa.	Già analizzata nel secondo capitolo, è una società che lavora per le banche e punta a garantire i pagamenti interbancari per il tramite della propria Criptovaluta XRP.	100.000.000.000
STELLAR (XLM)	Criptovaluta innovativa.	Stellar, come Ripple, si occupa di trasferimenti interbancari. A differenza di Ripple, Stellar è pensata come criptovaluta utilizzabile sia dagli intermediari finanziari che per uso comune come metodo di pagamento.	103.926.681.379

SUPERNET (UNITY)	Altcoin.	Ha la caratteristica di avere un numero di unità circolanti molto basso.	777.777
VERTCOIN (VTC)	Altcoin.	Nessuna caratteristica particolare.	84.000.000

Come già detto la maggior parte delle criptovalute inserite in questa analisi sono Altcoin. A partire dal terzo periodo[136] verranno inserite nell'analisi anche Ethereum e NEM. Dal primo gennaio 2017 NEO e Z-cash e solo da settembre 2017 IOTA e BitcoinCash.

ETHEREUM (ETH)	Piattaforma.	È la prima piattaforma di criptovalute. È la seconda criptovaluta per capitalizzazione di mercato. È stata trattata nella parte conclusiva del capitolo due.	Nessun limite previsto.
NEM (NEM)	Piattaforma.	Piattaforma blockchain sviluppata totalmente con il linguaggio Java. È la terza piattaforma per capitalizzazione di mercato.	Nessun limite previsto.
NEO (NEO)	Piattaforma.	Seconda piattaforma per capitalizzazione di	100.000.000

[136] Nella tabella 3.2 presente nelle pagine successive sono indicati con precisione i periodi e le criptovalute inserite nell'analisi.

		mercato è stata trattata nel secondo capitolo. A differenza di Ethereum supporta linguaggi di programmazioni già esistenti come Java e Microsoft.	
Z-CASH (ZEC)	Altcoin.	È una criptovaluta che ha come punto di forza la sicurezza e l'anonimato delle transazioni.	Nessun limite previsto.
IOTA (IOTA)	Criptovaluta innovativa.	Criptovaluta innovativa che sostituisce alla BlockChain il Tangle. È stata descritta al capitolo 2.	2.779.530.283
BITCOINCASH (BTCC)	Altcoin.	Occupa la quarta posizione per capitalizzazione di mercato. Fork di Bitcoin, ha come obiettivo quello di superare il problema di scalabilità del BTC attraverso l'ampliamento della dimensione di blocchi. È stato trattato nel capitolo 2.	21.000.000

La tabella 3.2 mostra con precisione i periodi considerati nell'analisi e le criptovalute utilizzate per la selezione nel periodo indicato.

TABELLA 3.2

PERIODO (GIORNI CONSIDERATI)	**CRIPTOVALUTE CONSIDETATE**
1° PERIODO (dal 1 gennaio 2015 al 30 aprile 2015)	1) Bitcoin 2) BitcoinDark 3) Bitshares 4) BlackCoin 5) CounterParty 6) Dash 7) Dogecoin 8) FuelCoin 9) Litecoin 10) MaidSaveCoin 11) Monero 12) Namecoin 13) NXT 14) Omni 15) Paycoin 16) Peercoin 17) Reddcoin 18) Ripple 19) Stellar 20) Supernet 21) Vertcoin
2° PERIODO (dal 1 maggio 2015 al 31 agosto 2015)	1) Bitcoin 2) BitcoinDark 3) Bitshares 4) BlackCoin 5) CounterParty 6) Dash 7) Dogecoin 8) FuelCoin 9) Litecoin 10) MaidSaveCoin 11) Monero 12) Namecoin 13) NXT 14) Omni 15) Paycoin 16) Peercoin 17) Reddcoin 18) Ripple 19) Stellar 20) Supernet 21) Vertcoin
TERZO PERIODO (dal 1 settembre 2015 al 31 dicembre 2015)	1) Bitcoin 2) BitcoinDark 3) Bitshares 4) BlackCoin 5) CounterParty 6) Dash

	7) Dogecoin 8) FuelCoin 9) Litecoin 10) MaidSaveCoin 11) Monero 12) Namecoin 13) NXT 14) Omni 15) Paycoin 16) Peercoin 17) Reddcoin 18) Ripple 19) Stellar 20) Supernet 21) Vertcoin 22) Ethereum 23) NEM
QUARTO PERIODO (dal 1 gennaio 2016 al 30 aprile 2016)	1) Bitcoin 2) BitcoinDark 3) Bitshares 4) BlackCoin 5) CounterParty 6) Dash 7) Dogecoin 8) FuelCoin 9) Litecoin 10) MaidSaveCoin 11) Monero 12) Namecoin 13) NXT 14) Omni 15) Paycoin 16) Peercoin 17) Reddcoin 18) Ripple 19) Stellar 20) Supernet 21) Vertcoin 22) Ethereum 23) NEM
QUINTO PERIODO (dal 1 maggio 2016 al 31 agosto 2016)	1) Bitcoin 2) BitcoinDark 3) Bitshares 4) BlackCoin 5) CounterParty 6) Dash 7) Dogecoin 8) FuelCoin 9) Litecoin 10) MaidSaveCoin 11) Monero 12) Namecoin 13) NXT 14) Omni 15) Paycoin 16) Peercoin 17) Reddcoin 18) Ripple 19) Stellar 20) Supernet

	21) Vertcoin 22) Ethereum 23) NEM
SESTO PERIODO (dal 1 settembre 2016 al 31 dicembre 2016)	1) Bitcoin 2) BitcoinDark 3) Bitshares 4) BlackCoin 5) CounterParty 6) Dash 7) Dogecoin 8) FuelCoin 9) Litecoin 10) MaidSaveCoin 11) Monero 12) Namecoin 13) NXT 14) Omni 15) Paycoin 16) Peercoin 17) Reddcoin 18) Ripple 19) Stellar 20) Supernet 21) Vertcoin 22) Ethereum 23) NEM
SETTIMO PERIODO (dal 1 gennaio 2017 al 30 aprile 2017)	1) Bitcoin 2) BitcoinDark 3) Bitshares 4) BlackCoin 5) CounterParty 6) Dash 7) Dogecoin 8) Litecoin 9) MaidSaveCoin 10) Monero 11) Namecoin 12) NXT 13) Omni 14) Peercoin 15) Reddcoin 16) Ripple 17) Stellar 18) Supernet 19) Vertcoin 20) Ethereum 21) NEM 22) NEO 23) Z-Cash
OTTAVO PERIODO (dal 1 maggio 2017 al 31 aprile 2017)	1) Bitcoin 2) BitcoinDark 3) Bitshares 4) BlackCoin 5) CounterParty 6) Dash 7) Dogecoin 8) Litecoin 9) MaidSaveCoin 10) Monero 11) Namecoin

	12) NXT 13) Omni 14) Peercoin 15) Reddcoin 16) Ripple 17) Stellar 18) Vertcoin 19) Ethereum 20) NEM 21) NEO 22) Z-Cash
NONO PERIODO (dal 1 settembre 2017 al 31 dicembre 2017)	1) Bitcoin 2) BitcoinDark 3) Bitshares 4) BlackCoin 5) CounterParty 6) Dash 7) Dogecoin 8) Litecoin 9) MaidSaveCoin 10) Monero 11) Namecoin 12) NXT 13) Omni 14) Peercoin 15) Reddcoin 16) Ripple 17) Stellar 18) Vertcoin 19) Ethereum 20) NEM 21) NEO 22) Z-Cash 23) IOTA 24) BitcoinCash
DECIMO PERIODO (dal 1 gennaio 2018 al 30 aprile 2018)	1) Bitcoin 2) BitcoinDark 3) Bitshares 4) BlackCoin 5) CounterParty 6) Dash 7) Dogecoin 8) Litecoin 9) MaidSaveCoin 10) Monero 11) Namecoin 12) NXT 13) Omni 14) Peercoin 15) Reddcoin 16) Ripple 17) Stellar 18) Vertcoin 19) Ethereum 20) NEM 21) NEO 22) Z-Cash 23) IOTA 24) BitcoinCash

3.4 PORTAFOGLI QUADRIMESTRALI

Attraverso “Matlab” sono stati calcolati i portafogli possibili alla Markowitz con il codice riportato in “appendice A” successivamente.

I soggetti che investono in criptovalute lo fanno perché sono attratti dalle possibilità di ottenere i rendimenti elevatissimi che contraddistinguono la cosiddetta finanza alternativa. A livello indicativo, nell’arco temporale di un anno un soggetto è interessato ad avere un rendimento di almeno il 100% del proprio investimento. Per tale motivo, per ogni periodo, verrà proposto il portafoglio alla Markowitz studiato per permettere di ottenere un tale rendimento. L’analisi è stata sviluppata in periodi di 4 mesi[137], considerando che il mercato delle criptovalute è attivo sette giorni su sette senza alcuna pausa le osservazioni annuali sono 365. Poiché il mercato è attivo 24 ore su 24 non avrebbe senso parlare di prezzo di “apertura” o di “chiusura” è stato scelto di prendere come riferimento il prezzo delle 00:00 di ogni giorno.

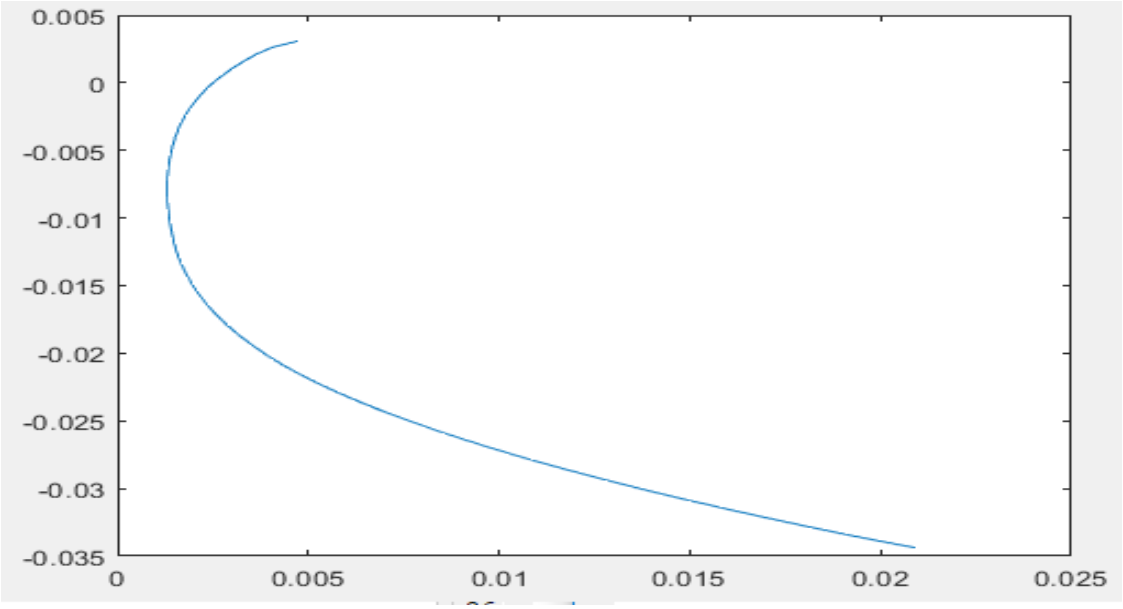
3.4.1 PRIMO PERIODO

1 gennaio 2015 - 30 aprile 2015

Il grafico 3.7 raffigura la frontiera dei portafogli ammissibili alla Markowitz considerando l’intervallo 1 gennaio 2015 30 aprile 2015. Come si può notare la frontiera efficiente è estremamente limitata. Il periodo considerato è stato caratterizzato da una discesa del prezzo di alcune criptovalute.

[137] Come si può vedere dalla tabella 3.2 l’analisi è divisa in tre periodi all’anno: dall’1 gennaio al 30 aprile, dal 1 maggio al 31 agosto e dal 1 settembre al 31 dicembre.

GRAFICO 3.7[138]



La maggior parte dei portafogli individuati presentano un rendimento negativo.

Aspetto più interessante da valutare è quello della correlazione tra i rendimenti delle 21 criptovalute considerate. Come prevedibile, l'andamento della maggior parte delle correlazioni delle crypto è fortemente positivo; alcune sono correlate in maniera elevatissima con percentuali di correlazioni anche superiori all'85%. Nonostante ciò sono state individuate delle correlazioni negative importanti, anche inferiori al -10%.
Nella tabella riportata di seguito è mostrata la correlazione tra tutte le criptovalute considerate nell'analisi. In rosso è indicata la correlazione fortemente positiva (superiore all'80%), in arancio la correlazione positiva superiore al 50% ed inferiore al 80%, In verde sono state indicate le correlazioni positive che sono vicine a 0 (tra 0 e +20%). In blu infine sono state indicate tutte le correlazioni negative. Le criptovalute sulle righe seguono l'ordine della tabella 3.1.

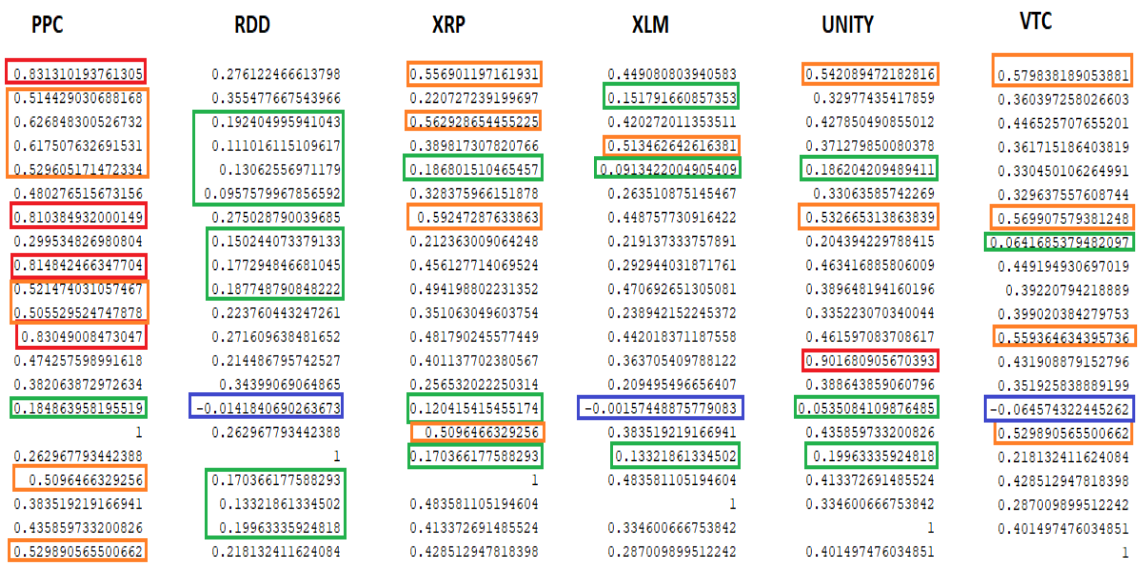
[138] I rendimenti e le varianze sono giornalieri.

FIGURA 3.1

BTC	BTCD	BTS	BLK	XCP
1	0.618979371322242	0.704348387243606	0.633456289960494	0.571038672874759
0.618979371322242	1	0.461280545477527	0.472580745369683	0.295081988624644
0.704348387243606	0.461280545477527	1	0.427840700048667	0.346704081347505
0.633456289960494	0.472580745369683	0.427840700048667	1	0.279122121431166
0.571038672874759	0.295081988624644	0.346704081347505	0.279122121431165	1
0.546222528390439	0.408172706983093	0.393236367756864	0.392976739787687	0.20186302113644
0.891453122951735	0.577184752165128	0.710836309665286	0.618901123345472	0.421793838057117
0.348244799083002	0.128095492937532	0.144401845870248	0.358507380107614	0.268055228527995
0.741666558245211	0.435823753015321	0.503824180529575	0.545589675399369	0.479940527786511
0.640626153776629	0.36938336030497	0.519820501630475	0.44024842002491	0.373625955629588
0.632542749958137	0.476362128936395	0.422803422476695	0.400652988739097	0.364322708816717
0.802867575152355	0.489759093247113	0.579113611723785	0.582560398292562	0.431806969077935
0.574241652537669	0.358742037120526	0.429958949379786	0.402021542849285	0.171753887833745
0.416482171568595	0.318492237378103	0.368948932955414	0.291694567992081	0.152722823667641
0.0987643658834503	-0.111562101009255	0.168975513452512	0.0588285886847788	0.0580324878863476
0.831310193761305	0.514429030688168	0.626848300526732	0.617507632691531	0.529605171472334
0.276122466613798	0.355477667543966	0.192404995941043	0.111016115109617	0.13062556971179
0.556901197161931	0.220727239199697	0.562928654455225	0.389817307820766	0.186801510465457
0.449080803940583	0.151791660857353	0.420272011353511	0.513462642616381	0.0913422004905409
0.542089472182816	0.32977435417859	0.427850490855012	0.371279850080378	0.186204209489411
0.579838189053881	0.360397258026603	0.446525707655201	0.361715186403819	0.330450106264991

DASH	DOGE	FC2	LTC	MAID
0.546222528390439	0.891453122951735	0.348244799083002	0.741666558245211	0.640626153776628
0.408172706983093	0.577184752165128	0.128095492937532	0.435823753015321	0.36938336030497
0.393236367756864	0.710836309665286	0.144401845870248	0.503824180529574	0.519820501630475
0.392976739787687	0.618901123345472	0.358507380107614	0.545589675399369	0.44024842002491
0.20186302113644	0.421793838057117	0.268055228527995	0.479940527786511	0.373625955629588
1	0.525896188502079	0.231175505656095	0.396028726426085	0.332777924943011
0.525896188502079	1	0.278069490111484	0.720758845475021	0.547603160652954
0.231175505656095	0.278069490111484	1	0.236116349581886	0.253285018648627
0.396028726426085	0.720758845475021	0.236116349581886	1	0.45480177760137
0.332777924943011	0.547603160652954	0.253285018648627	0.45480177760137	1
0.242583177864649	0.576311396209545	0.22893679930941	0.476181594041975	0.39842137872249
0.439210981071948	0.760525288214336	0.321050230096908	0.74669790014486	0.495273824833428
0.300254086830161	0.557117727639303	0.192881352195215	0.500459322406371	0.357894145327189
0.255933291187814	0.481128682223887	0.271900570272802	0.286194781328159	0.284575401111787
-0.0386783650892564	0.128381790815596	0.0254970607350934	0.182269204861979	-0.0831307541826343
0.480276515673156	0.810384932000149	0.299534826980804	0.814842466347704	0.521474031057467
0.0957579967856592	0.275028790039685	0.150244073379133	0.177294846681045	0.187748790848222
0.328375966151878	0.59247287633863	0.212363009064248	0.456127714069524	0.494198802231352
0.263510875145467	0.448757730916422	0.219137333757891	0.292944031871761	0.470692651305081
0.33063585742269	0.532665313863839	0.204394229788415	0.463416885806009	0.389648194160196
0.329637557608744	0.569907579381248	0.0641685379482097	0.449194930697019	0.39220794218889

XRM	NMC	NXT	OMNI	XPY
0.632542749958137	0.802867575152355	0.574241652537669	0.416482171568595	0.0987643658834503
0.476362128936395	0.489759093247113	0.358742037120526	0.318492237378103	-0.111562101009255
0.422803422476695	0.579113611723785	0.429958949379786	0.368948932955414	0.168975513452512
0.400652988739097	0.582560398292562	0.402021542849285	0.291694567992081	0.0588285886847788
0.364322708816717	0.431806969077935	0.171753887833745	0.152722823667641	0.0580324878863476
0.242583177864649	0.439210981071948	0.300254086830161	0.255933291187814	-0.0386783650892564
0.576311396209545	0.760525288214336	0.557117727639303	0.481128682223887	0.128381790815596
0.22893679930941	0.321050230096908	0.192881352195215	0.271900570272802	0.0254970607350934
0.476181594041975	0.74669790014486	0.50045932240637	0.286194781328159	0.182269204861979
0.39842137872249	0.495273824833428	0.357894145327189	0.284575401111787	-0.0831307541826343
1	0.492633495980443	0.352340701886583	0.202869943678136	0.0567283668177798
0.492633495980443	1	0.487128624218535	0.320469883052327	0.183634416876748
0.352340701886583	0.487128624218535	1	0.362351414506009	0.0302704043768883
0.202869943678136	0.320469883052327	0.362351414506009	1	0.0113232385424266
0.0567283668177798	0.183634416876748	0.0302704043768883	0.0113232385424266	1
0.505529524747878	0.83049008473047	0.474257598991618	0.382063872972634	0.184863958195519
0.223760443247261	0.271609638481652	0.214486795742527	0.34399069064865	-0.0141840690263673
0.351063049603754	0.481790245577449	0.401137702380567	0.256532022250314	0.120415415455174
0.238942152245372	0.442018371187558	0.363705409788122	0.209495496656407	-0.00157448875779083
0.335223070340044	0.461597083708617	0.901680905670393	0.388643859060796	0.0535084109876485
0.399020384279753	0.559364634395736	0.431908879152796	0.351925838889199	-0.064574322445262



PPC	RDD	XRP	XLM	UNITY	VTC
0.831310193761305	0.276122466613798	0.556901197161931	0.449080803940583	0.542089472182816	0.579838189053881
0.514429030688168	0.355477667543966	0.220727239199697	0.151791660857353	0.32977435417859	0.360397258026603
0.626848300526732	0.192404995941043	0.562928654455225	0.420272011353511	0.427850490855012	0.446525707655201
0.617507632691531	0.111016115109617	0.389817307820766	0.513462642616381	0.371279850080378	0.361715186403819
0.529605171472334	0.13062556971179	0.186801510465457	0.0913422004905409	0.186204209489411	0.330450106264991
0.480276515673156	0.0957579967856592	0.328375966151878	0.263510875145467	0.33063585742269	0.329637557608744
0.810384932000149	0.275028790039685	0.59247287633863	0.448757730916422	0.532665313863839	0.569907579381248
0.299534826980804	0.150244073379133	0.212363009064248	0.219137333757891	0.204394229788415	0.0641685379482097
0.814842466347704	0.177294846681045	0.456127714069524	0.292944031871761	0.463416885806009	0.449194930697019
0.521474031057467	0.187748790848222	0.494198802231352	0.470692651305081	0.389648194160196	0.39220794218889
0.505529524747878	0.223760443247261	0.351063049603754	0.238942152245372	0.335223070340044	0.399020384279753
0.83049008473047	0.271609638481652	0.481790245577449	0.442018371187558	0.461597083708617	0.559364634395736
0.474257598991618	0.214486795742527	0.401137702380567	0.363705409788122	0.901680905670393	0.431908879152796
0.382063872972634	0.343990690648651	0.256532022250314	0.209495496656407	0.388643859060796	0.351925838889199
0.184863958195519	-0.0141840690263673	0.120415415455174	-0.00157448875779083	0.053508410987648 5	-0.064574322445262
1	0.262967793442388	0.50964663292 56	0.383519219166941	0.435859733200826	0.529890565500662
0.262967793442388	1	0.170366177588293	0.13321861334502	0.19963335924818	0.218132411624084
0.5096466329256	0.170366177588293	1	0.483581105194604	0.413372691485524	0.428512947818398
0.383519219166941	0.13321861334502	0.483581105194604	1	0.334600666753842	0.287009899512242
0.435859733200826	0.19963335924818	0.413372691485524	0.334600666753842	1	0.401497476034851
0.529890565500662	0.218132411624084	0.428512947818398	0.287009899512242	0.401497476034851	1

Le criptovalute che risultano maggiormente correlate con le altre secondo questa prima analisi sono Bitcoin e Dogecoin. I rendimenti di 15 criptovalute su 21 sono correlati in maniera importante con il BTC (correlazione superiore al 50%) e nessuna delle criptovalute considerate presenta una correlazione negativa con esso. Come era lecito aspettarsi, quasi tutte le Altcoin avevano una forte correlazione con BTC. La criptovaluta che aveva una correlazione dei redimenti maggiormente negativa rispetto a tutte le altre è XPY (PayCoin).

Nel periodo considerato il rendimento massimo di portafoglio alla Markowitz si sarebbe potuto ottenere attraverso l'investimento del 100% del capitale nella crypto DASH, il rendimento garantito dalla crypto è stato di circa 0.00357877293898632 giornaliero che corrisponde ad un rendimento del 368.37% annuo. Il prezzo della criptovaluta è passato da 1,94$ a 2,97$ con un rendimento del 53,1% in 4 mesi.

Come obiettivo di portafoglio si è deciso di scegliere un rendimento del 100% annuo. Per tale motivo il rendimento giornaliero medio deve essere di 0.001900838.

Il portafoglio calcolato con questi parametri prevede l'acquisto di 4 criptovalute:

PORTAFOGLIO 1

BITCOIN	14%
DASH	57%
MONERO	27%
STELLAR	2%

L'andamento del portafoglio 1 e dei portafogli successivamente individuati è stato analizzato nel paragrafo 3.5.

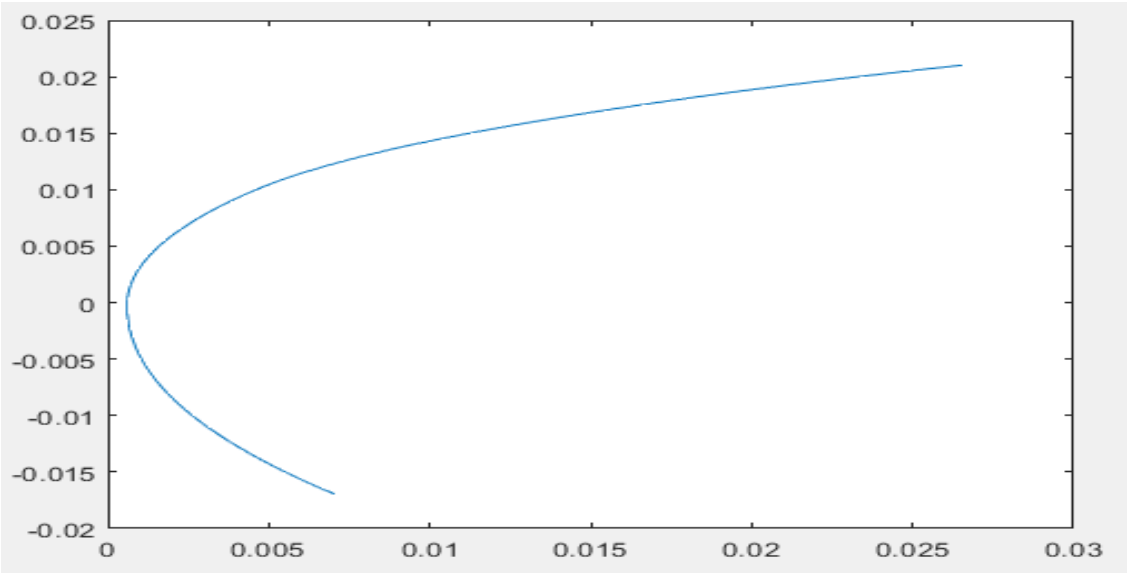
Considerando le criptovalute inserite nell'analisi quella che ha portato ad il peggior rendimento è PayCoin, passata dai 7,78$ iniziali agli 0,13$ al 30 aprile. La caduta così dirompente del prezzo di PayCoin spiega anche per quale motivo i rendimenti di essa siano correlati più marcatamente in maniera negativa rispetto alle altre criptovalute.

3.4.2 SECONDO PERIODO

1 maggio 2015 – 31 agosto 2015

L'analisi che segue riguarda il periodo tra l'1 maggio 2015 e il 31 agosto delle stesso anno. Oggetto dell'analisi sono sempre le 21 criptovalute considerate in precedenza.

GRAFICO 3.8 [139]

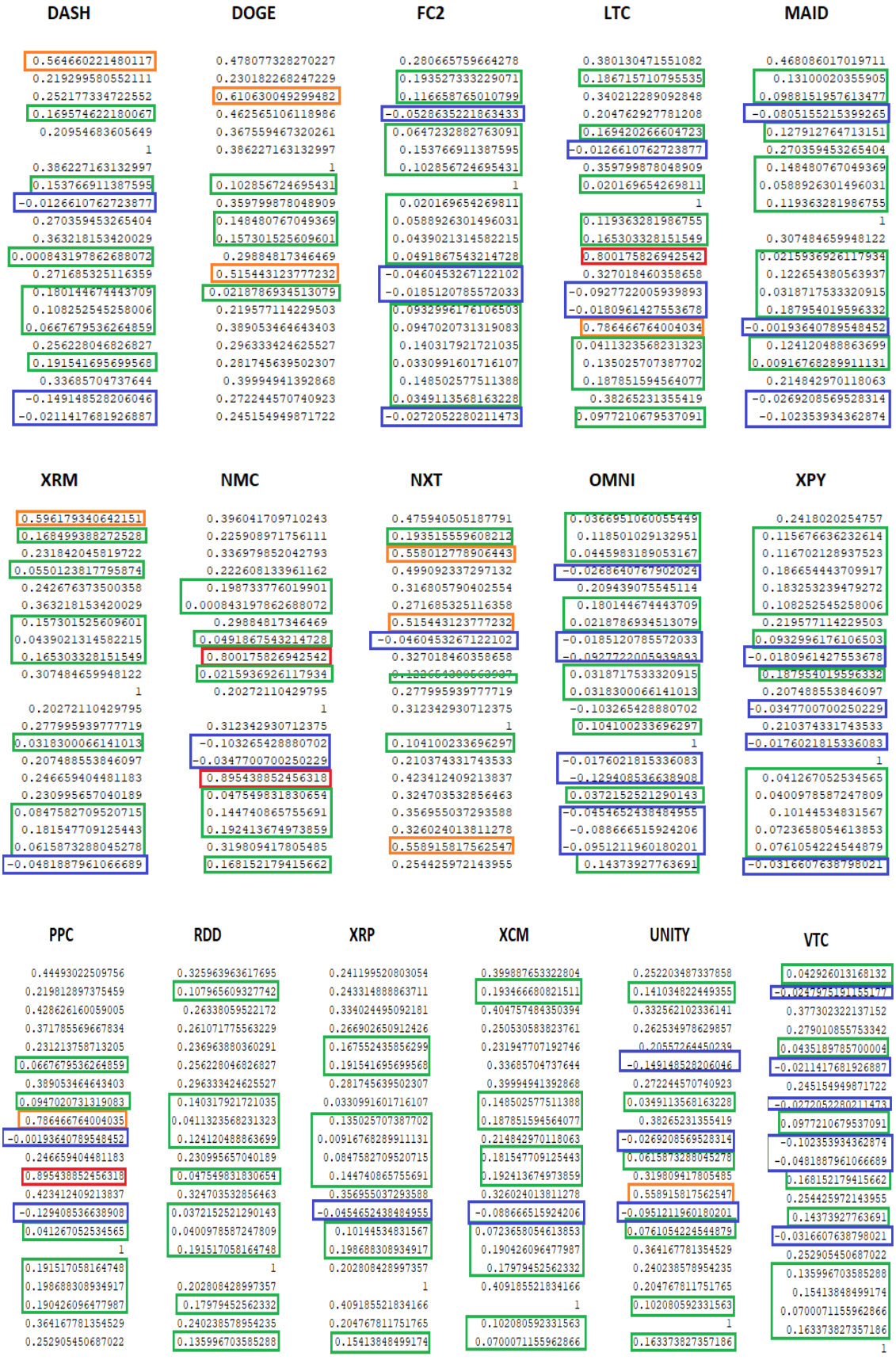


La frontiera efficiente individuata in questo intervallo di tempo è variata parecchio rispetto a quella del primo periodo. Nella figura 3.2 sono mostrate le correlazioni dei rendimenti tra le 21 criptovalute considerate.

FIGURA 3.2

BTC	BTCD	BTS	BLK	XCP
1	0.388338740719314	0.433843794731911	0.222665647558314	0.447287995869957
0.388338740719314	1	0.228639616910181	0.197026779172022	0.115198085559296
0.433843794731911	0.228639616910181	1	0.399875167212405	0.2044928525027
0.222665647558314	0.197026779172023	0.399875167212405	1	0.164871484230307
0.447287995869957	0.115198085559296	0.2044928525027	0.164871484230307	1
0.564660221480117	0.219299580552111	0.252177334722552	0.169574622180067	0.20954683605649
0.478077328270227	0.230182268247229	0.610630049299482	0.462565106118986	0.367559467320261
0.280665759664278	0.193527333229071	0.116658765010799	-0.0528635221863433	0.0647232882763091
0.380130471551082	0.186715710795535	0.340212289092848	0.204762927781208	0.169420266604723
0.468086017019711	0.13100020355905	0.0988151957613477	-0.0805155215399265	0.127912764713151
0.596179340642151	0.168499388272528	0.231842045819722	0.0550123817795874	0.242676373500358
0.396041709710243	0.225908971756111	0.336979852042793	0.222608133961162	0.198733776019901
0.475940505187791	0.193515559608212	0.558012778906443	0.499092337297132	0.316805790402554
0.0366951060055449	0.118501029132951	0.0445983189053167	-0.0268640767902024	0.209439075545114
0.2418020254757	0.115676636232614	0.116702128937523	0.186654443709917	0.183253239479272
0.44493022509756	0.219812897375459	0.428626160059005	0.371785569667834	0.231213758713205
0.325963963617695	0.107965609327742	0.26338059522172	0.261071775563229	0.236963880360291
0.241199520803054	0.243314888863711	0.334024495092181	0.266902650912426	0.167552435856299
0.399887653322804	0.193466680821511	0.404757484350394	0.250530583823761	0.231947707192746
0.252203487337858	0.141034822449355	0.332562102336141	0.262534978629857	0.20557264450239
0.042926013168132	-0.0247975191155177	0.377302322137152	0.279010855753342	0.0435189785700004

[139] Sull'asse delle "X" è riportata la deviazione standard su quella delle "Y" il rendimento atteso.


DASH
DOGE
FC2
LTC
MAID
XRM
NMC
NXT
OMNI
XPY
PPC
RDD
XRP
XCM
UNITY
VTC

Il periodo considerato è caratterizzato da una sostanziale crescita di tutto il mercato delle criptovalute. in una situazione del genere le correlazioni tra i rendimenti delle varie criptovalute si sono abbassate notevolmente, rientrando per la gran parte nel livello indicato con il colore verde (quindi compresa tra 0 e 20%).

Massimo rendimento quotidiano nel periodo è registrato introno al 0.0212308213775395 giornaliero, corrispondete al 2139% annuale, ed è stato ottenuto da VertCoin. Ancora una volta la peggior performance appartiene a PayCoin.

Il portafoglio costruito con l'obiettivo di conseguire un rendimento del 100% annuo cambia notevolmente rispetto a quello del periodo precedente. Viene aumentata la percentuale di Bitcoin al 36% del portafoglio e viene considerata anche Ripple (26%).

PORTAFOGLIO 2

BITCOIN	36%
BITCOINDARK	2,5%
DASH	13%
FUELCOIN	2%
LITECOIN	7%
MAIDSAVECOIN	5%
OMNI	2%
RIPPLE	26%
VERTCOIN	6,5%

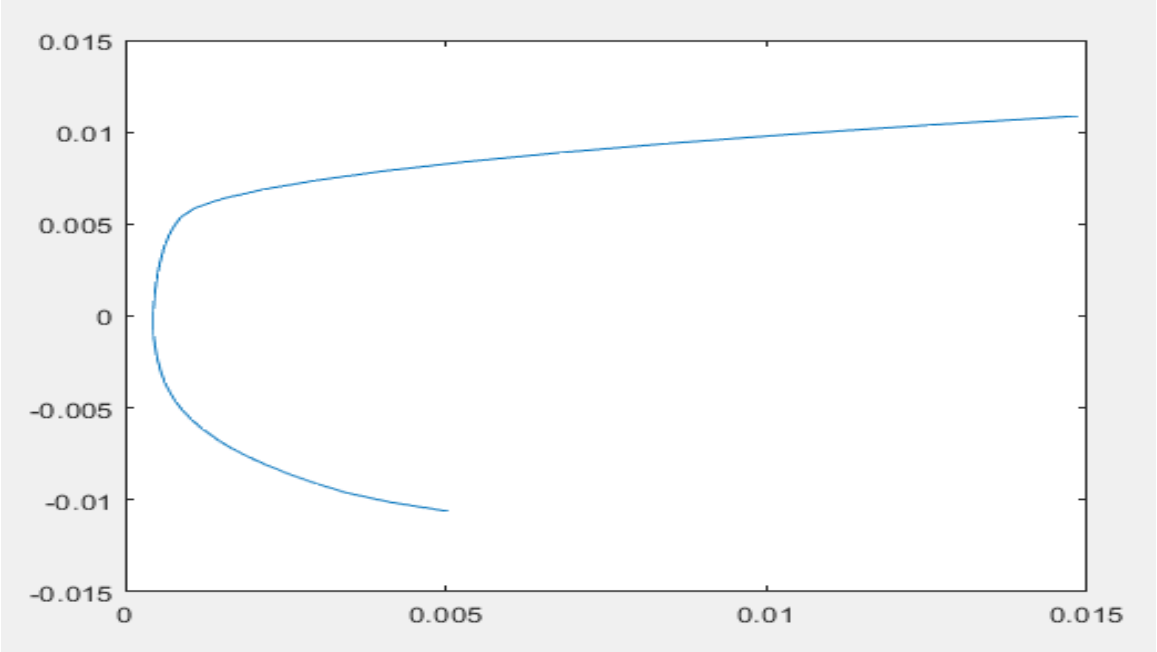
3.4.3 TERZO PERIODO

1 settembre 2015 – 31 dicembre 2015

Nel periodo considerato vengono inserite due nuove criptovalute; Ethereum e NEM.

Nel grafico sottostante è riportata la frazione dei portafogli possibili secondo Markowitz.

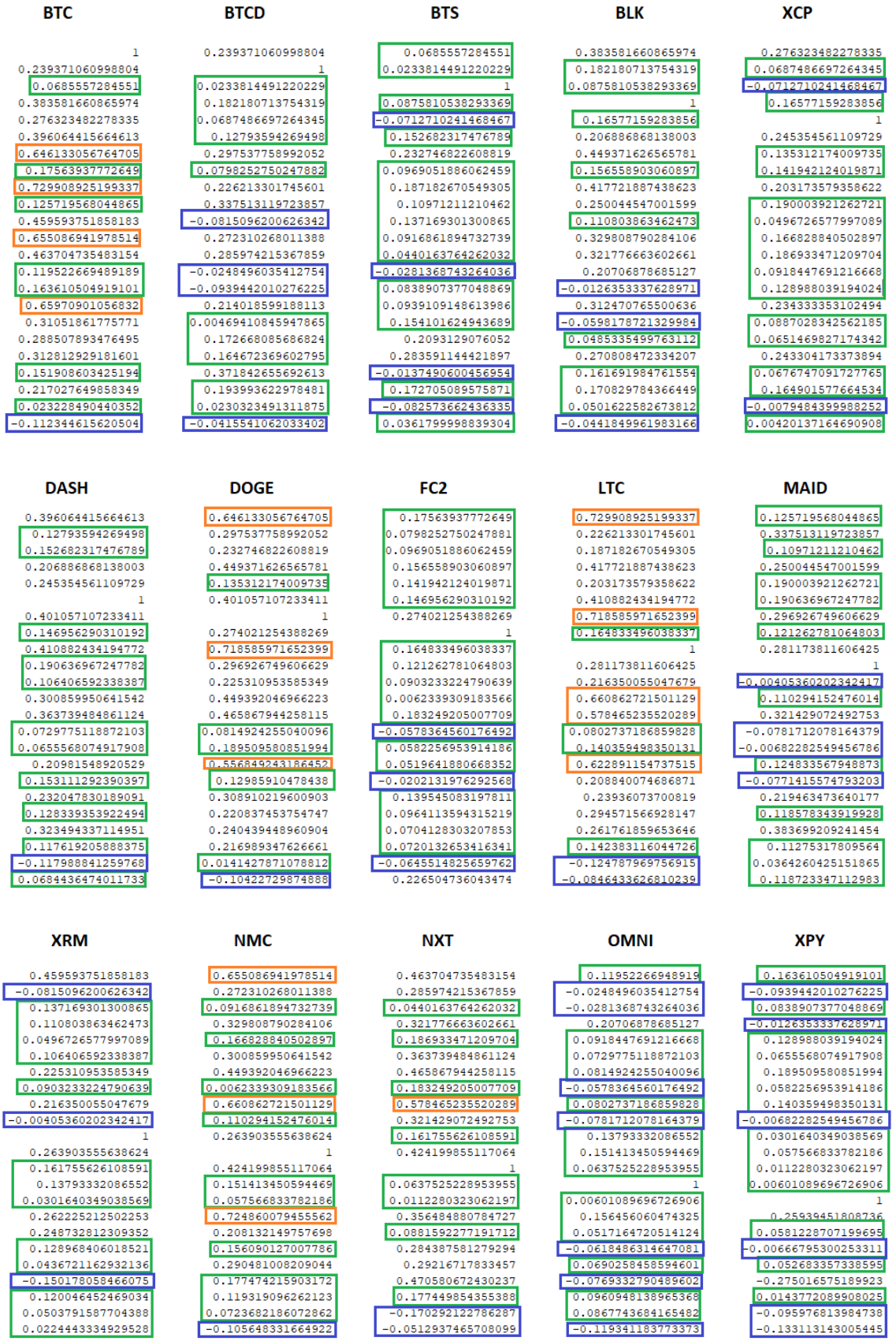
GRAFICO 3.9

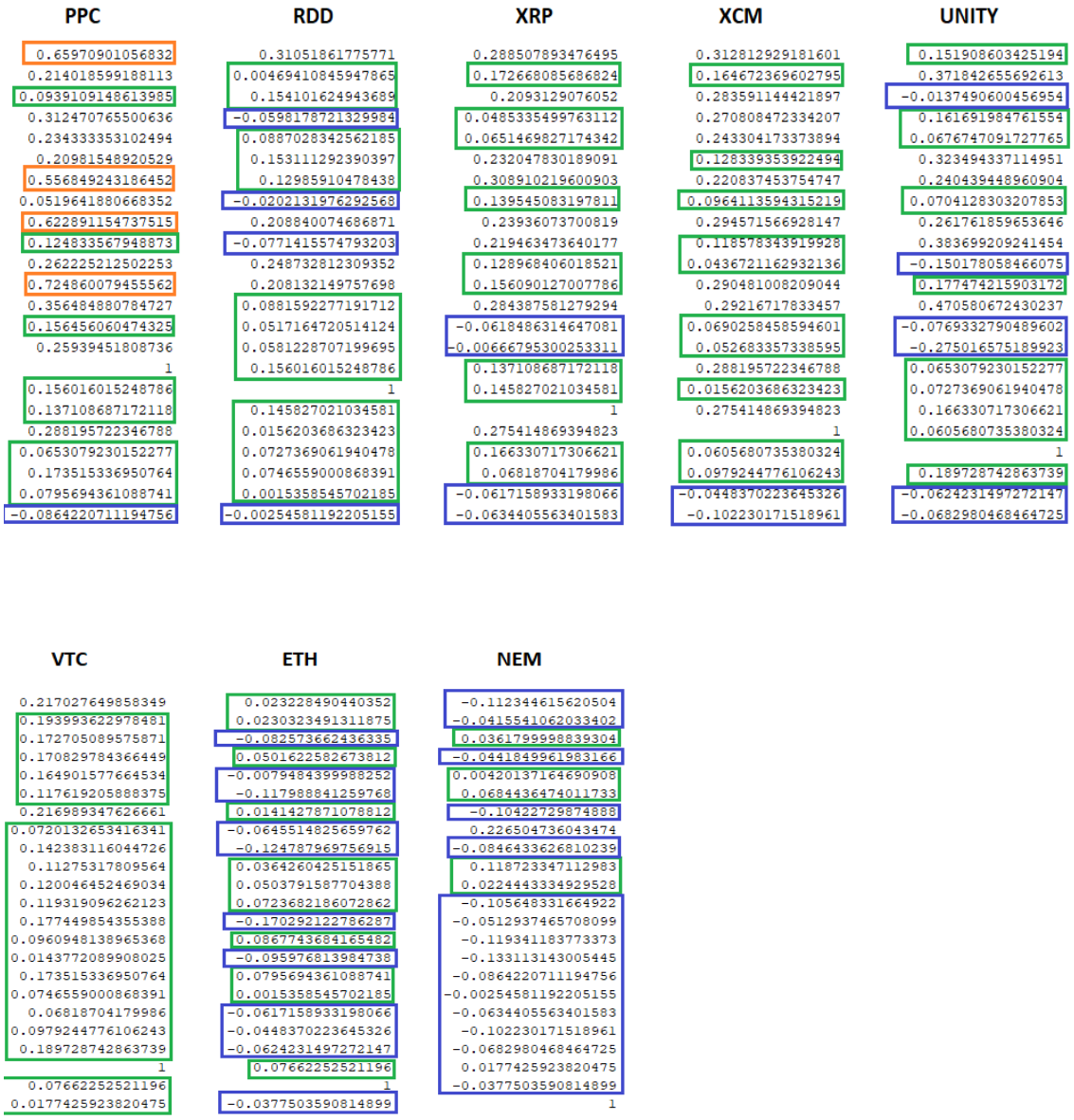


Anche se meno rispetto ai due periodi precedenti, la frontiera varia ancora, e aumenta notevolmente la frontiera nella quale sono presenti rendimenti positivi.

Come nei periodi precedenti sono state considerate le correlazioni dei rendimenti di tutte le criptovalute, con i risultati riportati nella figura seguente.

FIGURA 3.3


BTC
1
0.239371060998804
0.0685557284551
0.383581660865974
0.276323482278335
0.396064415664613
0.646133056764705
0.17563937772649
0.729908925199337
0.125719568044865
0.459593751858183
0.655086941978514
0.463704735483154
0.119522669489189
0.163610504919101
0.65970901056832
0.31051861775771
0.288507893476495
0.312812929181601
0.151908603425194
0.217027649858349
0.023228490440352
-0.112344615620504
BTCD
0.239371060998804
1
0.0233814491220229
0.182180713754319
0.0687486697264345
0.12793594269498
0.297537758992052
0.0798252750247882
0.226213301745601
0.337513119723857
-0.0815096200626342
0.272310268011388
0.285974215367859
-0.0248496035412754
-0.0939442010276225
0.214018599188113
0.00469410845947865
0.172668085686824
0.164672369602795
0.371842655692613
0.193993622978481
0.0230323491311875
-0.0415541062033402
BTS
0.0685557284551
0.0233814491220229
1
0.0875810538293369
-0.0712710241468467
0.152682317476789
0.232746822608819
0.0969051886062459
0.187182670549305
0.10971211210462
0.137169301300865
0.0916861894732739
0.0440163764262032
-0.0281368743264036
0.0838907377048869
0.0939109148613986
0.154101624943689
0.2093129076052
0.283591144421897
-0.0137490600456954
0.172705089575871
-0.082573662436335
0.0361799998839304
BLK
0.383581660865974
0.182180713754319
0.0875810538293369
1
0.16577159283856
0.206886868138003
0.449371626565781
0.156558903060897
0.417721887438623
0.250044547001599
0.110803863462473
0.329808790284106
0.321776663602661
0.20706878685127
-0.0126353337628971
0.312470765500636
-0.0598178721329984
0.0485335499763112
0.270808472334207
0.161691984761554
0.170829784366449
0.0501622582673812
-0.0441849961983166
XCP
0.276323482278335
0.0687486697264345
-0.0712710241468467
0.16577159283856
1
0.245354561109729
0.135312174009735
0.141942124019871
0.203173579358622
0.190003921262721
0.0496726577997089
0.166828840502897
0.186933471209704
0.0918447691216668
0.128988039194024
0.234333353102494
0.0887028342562185
0.0651469827174342
0.243304173373894
0.0676747091727765
0.164901577664534
-0.0079484399988252
0.00420137164690908
DASH
0.396064415664613
0.12793594269498
0.152682317476789
0.206886868138003
0.245354561109729
1
0.401057107233411
0.146956290310192
0.410882434194772
0.190636967247782
0.106406592338387
0.300859950641542
0.363739484861124
0.0729775118872103
0.0655568074917908
0.20981548920529
0.153111292390397
0.232047830189091
0.128339353922494
0.323494337114951
0.117619205888375
-0.117988841259768
0.0684436474011733
DOGE
0.646133056764705
0.297537758992052
0.232746822608819
0.449371626565781
0.135312174009735
0.401057107233411
1
0.274021254388269
0.718585971652399
0.296926749606629
0.225310953585349
0.449392046966223
0.465867944258115
0.0814924255040096
0.189509580851994
0.556849243186452
0.12985910478438
0.308910219600903
0.220837453754747
0.240439448960904
0.216989347626661
0.0141427871078812
-0.10422729874888
FC2
0.17563937772649
0.0798252750247881
0.0969051886062459
0.156558903060897
0.141942124019871
0.146956290310192
0.274021254388269
1
0.164833496038337
0.121262781064803
0.0903233224790639
0.0062339309183566
0.183249205007709
-0.0578364560176492
0.0582256953914186
0.0519641880668352
-0.0202131976292568
0.139545083197811
0.0964113594315219
0.0704128303207853
0.0720132653416341
-0.0645514825659762
0.226504736043474
LTC
0.729908925199337
0.226213301745601
0.187182670549305
0.417721887438623
0.203173579358622
0.410882434194772
0.718585971652399
0.164833496038337
1
0.281173811606425
0.216350055047679
0.660862721501129
0.578465235520289
0.0802737186859828
0.140359498350131
0.622891154737515
0.208840074686871
0.23936073700819
0.294571566928147
0.261761859653646
0.142383116044726
-0.124787969756915
-0.0846433626810239
MAID
0.125719568044865
0.337513119723857
0.10971211210462
0.250044547001599
0.190003921262721
0.190636967247782
0.296926749606629
0.121262781064803
0.281173811606425
1
-0.00405360202342417
0.110294152476014
0.321429072492753
-0.0781712078164379
-0.00682282549456786
0.124833567948873
-0.0771415574793203
0.219463473640177
0.118578343919928
0.383699209241454
0.11275317809564
0.0364260425151865
0.118723347112983
XRM
0.459593751858183
-0.0815096200626342
0.137169301300865
0.110803863462473
0.0496726577997089
0.106406592338387
0.225310953585349
0.0903233224790639
0.216350055047679
-0.00405360202342417
1
0.263903555638624
0.161755626108591
0.13793332086552
0.0301640349038569
0.262225212502253
0.248732812309352
0.128968406018521
0.0436721162932136
-0.150178058466075
0.120046452469034
0.0503791587704388
0.0224443334929528
NMC
0.655086941978514
0.272310268011388
0.0916861894732739
0.329808790284106
0.166828840502897
0.300859950641542
0.449392046966223
0.00623393091835666
0.660862721501129
0.110294152476014
0.263903555638624
1
0.424199855117064
0.151413450594469
0.057566833782186
0.724860079455562
0.208132149757698
0.156090127007786
0.290481008209044
0.177474215903172
0.119319096262123
0.0723682186072862
-0.105648331664922
NXT
0.463704735483154
0.285974215367859
0.0440163764262032
0.321776663602661
0.186933471209704
0.363739484861124
0.465867944258115
0.183249205007709
0.578465235520289
0.321429072492753
0.161755626108591
0.424199855117064
1
0.0637525228953955
0.0112280323062197
0.356484880784727
0.0881592277191712
0.284387581279294
0.29216717833457
0.470580672430237
0.177449854355388
-0.170292122786287
-0.0512937465708099
OMNI
0.119522669489191
-0.0248496035412754
-0.0281368743264036
0.20706878685127
0.0918447691216668
0.0729775118872103
0.0814924255040096
-0.0578364560176492
0.0802737186859828
-0.0781712078164379
0.13793332086552
0.151413450594469
0.0637525228953955
1
0.00601089696726906
0.156456060474325
0.0517164720514124
-0.0618486314647081
0.0690258458594601
-0.0769332790489602
0.0960948138965368
0.0867743684165482
-0.119341183773373
XPY
0.163610504919101
-0.0939442010276225
0.0838907377048869
-0.0126353337628971
0.128988039194024
0.0655568074917908
0.189509580851994
0.0582256953914186
0.140359498350131
-0.00682282549456786
0.0301640349038569
0.0575668337821866
0.0112280323062197
0.00601089696726906
1
0.259394518087366
0.0581228707199695
-0.00666795300253311
0.0526833573385955
-0.0275016575189923
0.0143772089908025
-0.0959768139847388
-0.133113143005445



Il periodo considerato vede l'entrata nell'analisi di due piattaforme, Ethereum e NEM. Esse, in questo primo periodo, sembrano avere, per quanto riguarda i rendimenti, una correlazione negativa o molto debole rispetto a tutte le altre. Come nella situazione precedente sono presenti poche correlazioni molto positive (superiori al 50%) ed in ogni caso tutte con il Bitcoin. Per quanto riguarda i rendimenti quotidiani, il migliore è stato registrato da Paycoin: 0.0110317331466221 giornaliero, che corrisponde al a circa il 550% annuo.

Il portafoglio selezionato per raggiungere un rendimento del 100% annuale è il seguente:

PORTAFOGLIO 3

BITCOIN	32%
BITSHARES	5%
DASH	9%
DOGECOIN	6%
MONERO	6%
NXT	6%
PAYCOIN	4%
RIPPLE	6%
STELLAR	8%
ETHEREUM	10%
NEM	8%

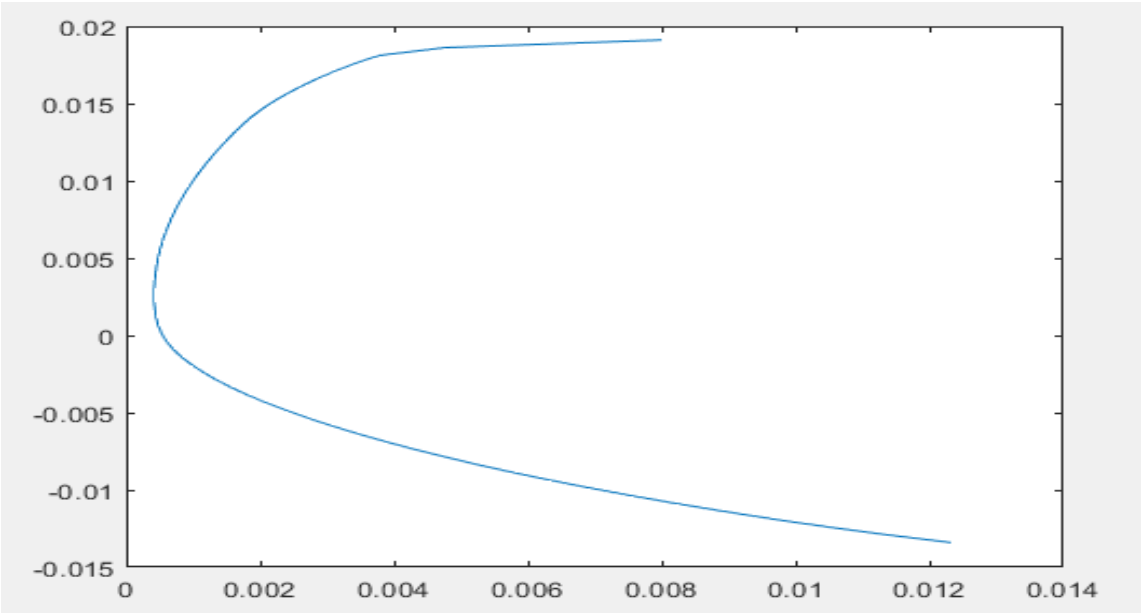
La peggior performance del periodo viene fatta registrare da Vertcoin.

3.4.4 QUARTO PERIODO

1 gennaio 2016 – 30 aprile 2016

Il grafico sottostante mostra la frontiera dei portafogli possibili creati con il metodo media-varianza nel periodo 1 gennaio 2016 30 aprile 2016.

GRAFICO 3.10



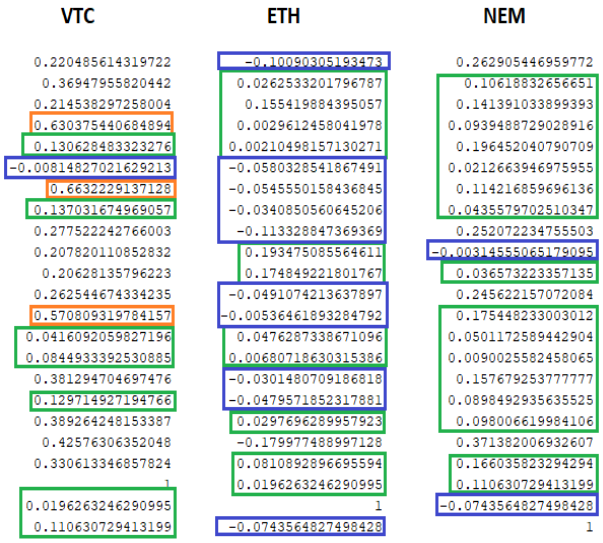
Come si può notare dal grafico, il periodo è stato caratterizzato da elevati rendimenti, vicini al 2% giornaliero, ma allo stesso tempo da perdite importanti superiori al -1% giornaliero.

Nella figura 3.4 sono mostrate le correlazioni dei rendimenti delle 23 criptovalute considerate.

FIGURA 3.4

BTC	BTCD	BTS	BLK	XCP
1	0.513546157960876	0.0126323044904368	0.3317343532729	0.185915630538977
0.513546157960876	1	0.182214820221117	0.353959836900538	0.295415743579131
0.0126323044904368	0.182214820221117	1	0.318592054036472	0.13392203452201
0.3317343532729	0.353959836900538	0.318592054036472	1	5.97517532997404e-05
0.185915630538977	0.295415743579131	0.13392203452201	5.97517532997404e-05	1
0.177841496852564	0.0575792048231127	0.130144841171308	0.181890544852499	0.0780193208081732
0.259295104609406	0.32306721924051	0.267320484911815	0.557209124351637	0.123059701265403
0.140056280288502	0.00603265713826954	0.04107094495458 73	0.151525224155285	-0.0201063575399161
0.865095983978646	0.502536636654803	0.0208402786926759	0.406019547502793	0.132304380530984
0.103354566292423	0.117105021577134	0.249451827645943	0.216650658459644	-0.0197636848033333
0.170398254821959	0.192989542260603	0.184054627522525	0.226378074708638	0.169940463757293
0.655922400457843	0.436829765437429	-0.0510911971499526	0.285309880319189	0.112205859425062
0.250212727352072	0.444381369328596	0.348079853794553	0.618727628752456	0.120706687207636
0.140742233267074	0.0761030588897972	0.0387699695522068	-0.0500005053216513	0.102675918629059
0.411038428147526	0.223265821492366	0.0784237492665719	0.206400427017503	0.074154321671408
0.696404888531987	0.461835109436044	0.0791230422855592	0.514427889430475	0.0963799026547762
0.0685326033228962	0.109417348970233	0.0650649212105397	0.213949412038247	0.0308216273309878
0.250629363398731	0.325474473842782	0.181440811698515	0.428757384008936	0.168976636776877
0.22623779462779	0.249809438511125	0.412820660296405	0.49610943037927	0.141241146592737
0.192976587359656	0.348895067313727	0.194970077275337	0.36325969395806	0.243882322244579
0.220485614319722	0.36947955820442	0.214538297258004	0.630375440684894	0.130628483323276
-0.100903051934 73	0.0262533201796787	0.155419884395057	0.00296124580419779	0.00210498157130271
0.262905446959772	0.10618832656651	0.141391033899393	0.0939488729028916	0.196452040790709


DASH
0.177841496852564
0.0575792048231127
0.1301448411713308
0.181890544852499
0.0780193208081732
1
0.08162200440113118
0.214550271146765
0.09106161918165220
0.010947687896433
0.04185081855681660
0.110149460290676
0.05212506017275570
-0.01238607573183770
0.146021194024478
0.253221142989552
-0.05924355036490130
0.04222290201892140
-0.02245069766083
-0.03919856381014040
-0.00814827021629213
-0.05803285418674910
0.02126639469759550
DOGE
0.259295104609406
0.32306721924051
0.267320484911815
0.557209124351637
0.123059701265403
0.08162200440113180
1
0.08631672574009850
0.35225458967294
0.159779304111652
0.06816602506922250
0.263824951042417
0.50909017552902
0.07910221206277940
0.177853074076877
0.424950204150297
0.115195617791525
0.333450081856303
0.437169130568431
0.35987783877021300
0.66322291371280
-0.05455501584368450
0.11421685969613600
FC2
0.140056280288502
0.00603265713826954
0.04107094495458730
0.151525224155285
-0.02010635753991610
0.214550271146765
0.08631672574009850
1
0.11468114113873500
0.09534237309869030
-0.04244282801561930
0.13723344617368900
-6.706000503148998e-05
0.00300237932666149
-0.09172733603547040
0.16527015060535200
0.01065511744211860
0.15094720475389500
0.08050324161740180
0.08217449348882160
0.13703167496905700
-0.03408505606452060
0.04355797025103470
LTC
0.8650959839786460
0.5025366366548030
0.02084027869265590
0.40601954750279300
0.13230438053098400
0.09106161918165220
0.35225458967294
0.11468114113873500
1
0.00481656203370472
0.08310828300836630
0.63164210016812700
0.33178566881112800
0.08818370375714730
0.37409261742843
0.70476191847167100
0.07535465646935400
0.28494448483323930
0.25935151572282800
0.29398639988221400
0.27752224276600300
-0.11332884736936900
0.25207223475550300
MAID
0.1033545662924230
0.1171050215771340
0.24945182764594300
0.21665065845964400
-0.01976368480333300
0.01094768789643300
0.15977930411165200
0.09534237309869030
0.00481656203370472
1
0.18340035766701300
0.06153941884962200
0.19854225703955100
0.07579230919209880
0.15948511633146500
0.10065671368478100
0.04355552498718060
0.12179099764716600
0.14353468474634000
0.22426288664380200
0.20782011085283200
0.19347508556461100
-0.00314555065179095
XRM
0.170398254821959
0.192989542260603
0.184054627522525
0.22637807470863900
0.16994046375729300
0.04185081855681660
0.06816602506922250
-0.04244282801561930
0.08310828300836630
0.18340035766701300
1
0.11876929254706900
0.24304773342814300
-0.08707029431068660
0.17621793585185300
0.28585066905762000
0.12091616692322300
0.13497174781114400
0.24508239000526500
0.23664035971249300
0.20628135796223000
0.17484922180176700
0.03657322335713500
NMC
0.65592240045784300
0.43682976543742900
-0.05109119714995260
0.28530988031918900
0.11220585942506200
0.11014946029067600
0.26382495104241700
0.13723344617368900
0.63164210016812700
0.06153941884962200
0.11876929254706900
1
0.31777021404358500
0.13481943710600
0.23088237009977700
0.75687596838297600
0.08129795205400900
0.19893442396500500
0.29153217021695800
0.22443336761734700
0.26254467433423500
-0.04910742136378970
0.24562215707208400
NXT
0.25021272735207200
0.44438136932859600
0.34807985379455300
0.61872762875245600
0.12070668720763600
0.05212506017275570
0.50909017552902
-6.706005031489980e-05
0.33178566881112800
0.19854225703955100
0.24304773342814300
0.31777021404358500
1
0.06360823027786210
0.18472468734990600
0.50191383987593400
0.09912832032600330
0.46747222276876800
0.51928244668766500
0.56038477035167400
0.57080931978415700
-0.00536461893284792
0.17544823300301200
0.14074223326707400
0.07610305889079720
0.03872699655220680
-0.05000050532165130
0.10267591862905900
-0.01238607573183770
0.07910221206277940
0.00300237932666149
0.08818370375714730
0.07579230919209880
-0.08707029431068660
0.13484194371060600
0.06360823027786210
1
0.13555807738291400
0.09385711125893240
0.05316267349077490
0.02713541940143780
0.16647192359108300
0.03146332514192330
0.04160920598271960
0.04762873386710960
0.05011725894429040
OMNI
0.14074223326707400
0.07610305889079720
0.03872699655220680
-0.05000050532165130
0.10267591862905900
-0.01238607573183770
0.07910221206277940
0.00300237932666149
0.08818370375714730
0.07579230919209880
-0.08707029431068660
0.13484194371060600
0.06360823027786210
1
0.13555807738291400
0.09385711125893240
0.05316267349077490
0.02713541940143780
0.16647192359108300
0.03146332514192330
0.04160920598271960
0.04762873386710960
0.05011725894429040
XPY
0.411038428147526
0.223265821492366
0.07842374926657200
0.20640042701750300
0.07415432167140800
0.14602119402447800
0.17785307407687700
-0.09172733603547050
0.37409261742843000
0.15948511633146500
0.17621793585185300
0.23088237009977700
0.18472468734990600
0.13555807738291400
1
0.35746157152137000
-0.04913189096555260
0.14981825336935500
0.03731191943487990
0.13331158096109100
0.08449333925308850
0.00680718630315386
0.00900255824580650
PPC
0.6964048885319870
0.4618351094360440
0.07912304228555920
0.5144278894304750
0.09637990265477620
0.25322114298955200
0.42495020415029700
0.16527015060535200
0.70476191847167100
0.10065671368478100
0.28585066905762000
0.75687596838297600
0.50191383987593400
0.09383571112589324
0.35746157152137000
1
0.02925164717244820
0.40436941522602100
0.35223794298626100
0.31843443781729900
0.38129470469747600
-0.03014807091868180
0.15767925377777700
RDD
0.06853260332289620
0.10941734897023300
0.06506492121053970
0.21394941203824700
0.03082162733098780
-0.05924355036490130
0.11519561779152500
0.01065511744211860
0.07535465646935400
0.04355552498718060
0.12091616692322300
0.08129795205400900
0.09912832032600330
0.05316267340977490
-0.04913189096555260
0.02925164717244820
1
0.09172992120478370
0.15969772800297900
0.24087341118640700
0.12971492719476600
-0.04795718523178810
0.08984929356355250
XRP
0.25062936339873100
0.32547447384278200
0.18144081169851500
0.42875738400893600
0.16897663767768700
0.04222290201892140
0.33345008185630300
0.15094720475389500
0.28494448483323930
0.12179099764716600
0.13497174781114400
0.19893442396500500
0.46747222276876800
0.02713541940143780
0.14981825336935500
0.40436941522602100
0.09172992120478370
1
0.34910972951251300
0.34643539512695800
0.38926424815338700
0.02976962899579230
0.09800661998410600
XCM
0.22623779462779000
0.24980943851112500
0.41282066029640500
0.49610943037927000
0.14124114659273700
-0.02245069766083000
0.43716913056843100
0.08050324161740180
0.25935151572282800
0.14353468474634000
0.24508239000526500
0.29153217021695800
0.51928244668766500
0.16647192359108300
0.03731191943487990
0.35223794298626100
0.15969772800297900
0.34910972951251300
1
0.34640758669888700
0.42576306352048000
-0.17997748899712800
0.37138200693260700
UNITY
0.19297658735965600
0.34889506731372700
0.19497007727533700
0.36325969395806000
0.24388232224457900
-0.03919856381014040
0.35987783877021300
0.08217449348882160
0.29398639988221400
0.22426288664380200
0.23664035971249300
0.22443336761734700
0.56038477035167400
0.03146332514192330
0.13331158096109100
0.31843443781729900
0.24087341118640700
0.34643539512695800
0.34640758669888700
1
0.33061334685782400
0.08108928966955940
0.16603582329429400



Come nel periodo precedente, le piattaforme Ethereum e NEM registrano una correlazione dei rendimenti negativa o comunque bassa rispetto alle altre criptovalute. In generale i rendimenti sono correlati con percentuali quasi mai superiori al 50%. Il miglior rendimento quotidiano è stato registrato da NEM 0.0192817481555053, di poco superiore al 10634% annuo.

Il portafoglio che ha come obiettivo quello di garantire un rendimento del 100% annuo è il seguente:

PORTAFOGLIO 4

BITCOIN	30%
BITSHARES	3%
DASH	6,5%
LITECOIN	28,5%
OMNI	2%
REDDCOIN	1%
RIPPLE	22%
STELLAR	2%
ETHEREUM	5%

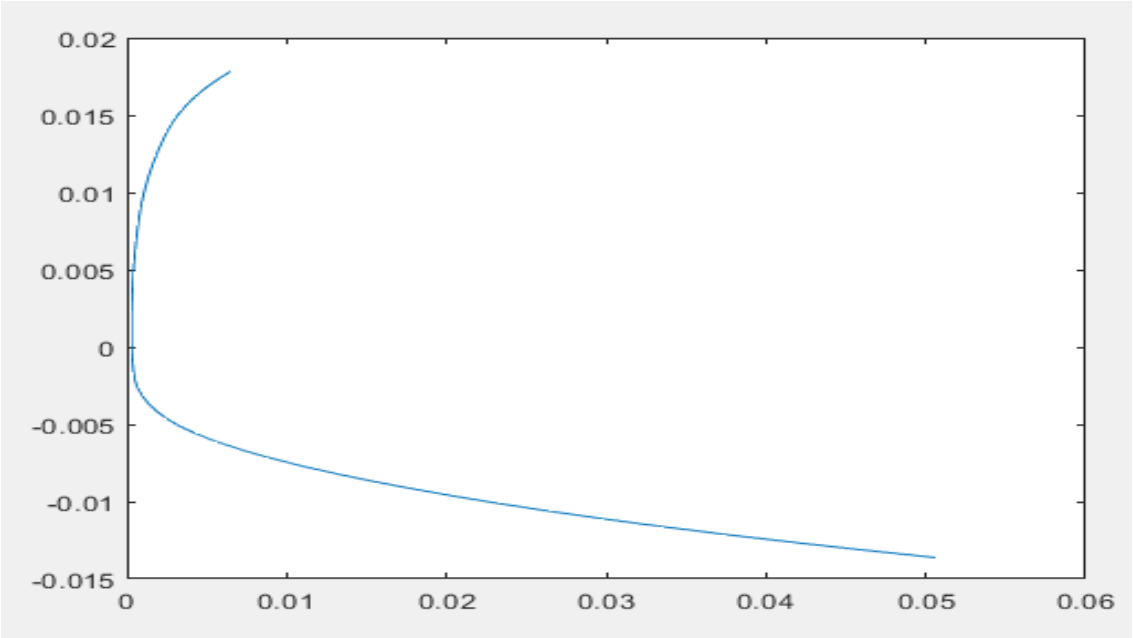
Il peggiore rendimento è stato registrato da PayCoin con un -0.0133871606767986 giornaliero, pari ad una perdita di quasi il 100% del capitale.

3.4.5 QUINTO PERIODO

1 maggio 2016 – 31 agosto 2016

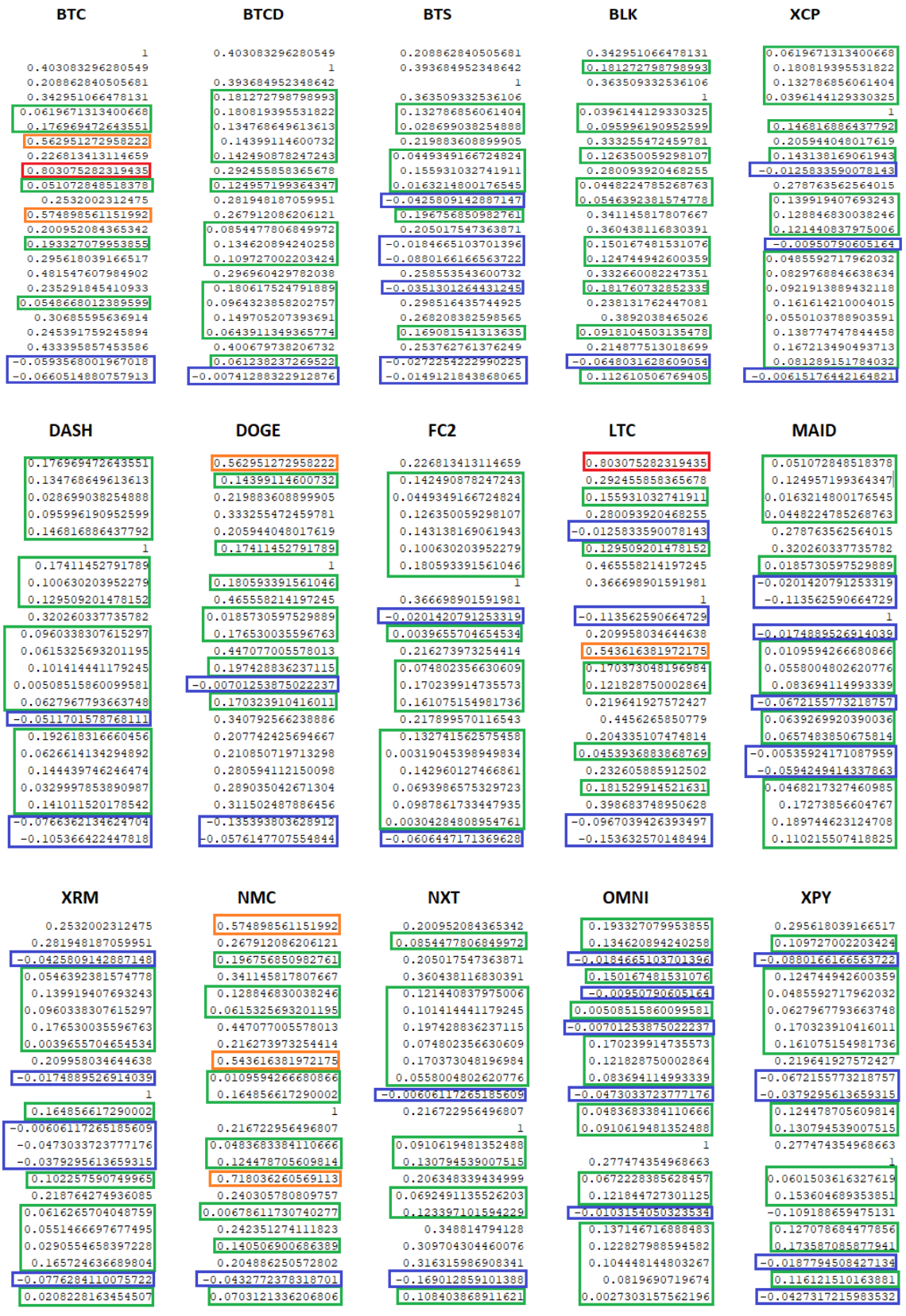
Il grafico sottostante mostra la frontiera dei portafogli possibili. Come si può notare, in questo periodo sono presenti alcuni portafogli che garantiscono un rendimento importante ed una varianza molto bassa.

GRAFICO 3.11



Nella figura 3.5 sono riportate le correlazioni dei rendimenti delle 23 criptovalute considerate.

FIGURA 3.5


BTC
1
0.403083296280549
0.208862840505681
0.342951066478131
0.0619671313400668
0.176969472643551
0.562951272958222
0.226813413114659
0.803075282319435
0.051072848518378
0.2532002312475
0.574898561151992
0.200952084365342
0.193327079953855
0.295618039166517
0.481547607984902
0.235291845410933
0.0548668012389599
0.30685595636914
0.245391759245894
0.433395857453586
-0.0593568001967018
-0.0660514880757913
BTCD
0.403083296280549
1
0.393684952348642
0.181272798798993
0.180819395531822
0.134768649613613
0.14399114600732
0.142490878247243
0.292455858365678
0.124957199364347
0.281948187059951
0.267912086206121
0.0854477806849972
0.134620894240258
0.109727002203424
0.296960429782038
0.180617524791889
0.0964323858202757
0.149705207393691
0.0643911349365774
0.400679738206732
0.061238237269522
-0.00741288322912876
BTS
0.208862840505681
0.393684952348642
1
0.363509332536106
0.132786856061404
0.028699038254888
0.219883608899905
0.0449349166724824
0.155931032741911
0.0163214800176545
-0.0425809142887147
0.196756850982761
0.205017547363871
-0.0184665103701396
-0.0880166166563722
0.258553543600732
-0.0351301264431245
0.298516435744925
0.268208382598565
0.169081541313635
0.253762761376249
-0.0272254222990225
-0.0149121843868065
BLK
0.342951066478131
0.181272798798993
0.363509332536106
1
0.0396144129330325
0.095996190952599
0.333255472459781
0.126350059298107
0.280093920468255
0.0448224785268763
0.0546392381574778
0.341145817807667
0.360438116830391
0.150167481531076
0.124744942600359
0.332660082247351
0.181760732852335
0.238131762447081
0.3892038465026
0.0918104503135478
0.214877513018699
-0.0648031628609054
0.112610506769405
XCP
0.0619671313400668
0.180819395531822
0.132786856061404
0.0396144129330325
1
0.146816886437792
0.205944048017619
0.143138169061943
-0.0125833590078143
0.278763562564015
0.139919407693243
0.128846830038246
0.121440837975006
-0.00950790605164
0.0485592717962032
0.0829768846638634
0.092191388932118
0.161614210004015
0.0550103788903591
0.138774747844458
0.167213490493713
0.081289151784032
-0.00615176442164821
DASH
0.176969472643551
0.134768649613613
0.028699038254888
0.095996190952599
0.146816886437792
1
0.17411452791789
0.100630203952279
0.129509201478152
0.320260337735782
0.0960338307615297
0.0615325693201195
0.101414441179245
0.00508515860099581
0.0627967793663748
-0.0511701578768111
0.192618316660456
0.0626614134294892
0.144439746246474
0.0329997853890987
0.141011520178542
-0.0766362134624704
-0.105366422447818
DOGE
0.562951272958222
0.14399114600732
0.219883608899905
0.333255472459781
0.205944048017619
0.17411452791789
1
0.180593391561046
0.465558214197245
0.0185730597529889
0.176530035596763
0.447077005578013
0.197428836237115
-0.00701253875022237
0.170323910416011
0.340792566238886
0.207742425694667
0.210850719713298
0.280594112150098
0.289035042671304
0.311502487886456
-0.135393803628912
-0.0576147707554844
FC2
0.226813413114659
0.142490878247243
0.0449349166724824
0.126350059298107
0.143138169061943
0.100630203952279
0.180593391561046
1
0.366698901591981
-0.0201420791253319
0.00396557046545434
0.216273973254414
0.074802356630609
0.170239914735573
0.161075154981736
0.217899570116543
0.132741562575458
0.00319045398949834
0.142960127466861
0.0693986575329723
0.0987861733447935
0.00304284808954761
-0.0606447171369628
LTC
0.803075282319435
0.292455858365678
0.155931032741911
0.280093920468255
-0.0125833590078143
0.129509201478152
0.465558214197245
0.366698901591981
1
-0.113562590664729
0.209958034644638
0.543616381972175
0.170373048196984
0.121828750002864
0.219641927572427
0.4456265850779
0.204335107474814
0.0453936883868769
0.232605885912502
0.181529914521631
0.398683748950628
-0.0967039426393497
-0.153632570148494
MAID
0.051072848518378
0.124957199364347
0.0163214800176545
0.0448224785268763
0.278763562564015
0.320260337735782
0.0185730597529889
-0.0201420791253319
-0.113562590664729
1
-0.0174889526914039
0.0109594266680866
0.0558004802620776
0.083694114993339
-0.0672155773218757
0.0639269920390036
0.0657483850675814
-0.00535924171087959
-0.0594249414337863
0.0468217327460985
0.172738566047674
0.189744623124708
0.110215507418825
XRM
0.2532002312475
0.281948187059951
-0.0425809142887148
0.0546392381574778
0.139919407693243
0.0960338307615297
0.176530035596763
0.0039655704654534
0.209958034644638
-0.0174889526914039
1
0.164856617290002
-0.00606117265185609
-0.0473033723777176
-0.0379295613659315
0.102257590749965
0.218764274936085
0.0616265704048759
0.0551466697677495
0.0290554658397228
0.165724636689804
-0.0776284110075722
0.0208228163454507
NMC
0.574898561151992
0.267912086206121
0.196756850982761
0.341145817807667
0.128846830038246
0.0615325693201195
0.447077005578013
0.216273973254414
0.543616381972175
0.0109594266680866
0.164856617290002
1
0.216722956496807
0.0483683384110666
0.124478705609814
0.718036260569113
0.240305780809757
0.00678611730740277
0.242351274111823
0.140506900686389
0.204886250572802
-0.0432772378318701
0.0703121336206806
NXT
0.200952084365342
0.0854477806849972
0.205017547363871
0.360438116830391
0.121440837975006
0.101414441179245
0.197428836237115
0.074802356630609
0.170373048196984
0.0558004802620776
-0.00606117265185609
0.216722956496807
1
0.0910619481352488
0.130794539007515
0.206348339434999
0.0692491135526203
0.123397101594229
0.348814794128
0.309704304460076
0.316315986908341
-0.169012859101388
0.108403868911621
OMNI
0.193327079953855
0.134620894240258
-0.0184665103701396
0.150167481531076
-0.00950790605164
0.00508515860099581
-0.00701253875022237
0.170239914735573
0.121828750002864
0.083694114993339
-0.0473033723777176
0.0483683384110666
0.0910619481352488
1
0.277474354968663
0.0672228385628457
0.121844727301125
-0.0103154050323534
0.137146716888483
0.122827988594582
0.104448144803267
0.0819690719674
0.0027303157562196
XPY
0.295618039166517
0.109727002203424
-0.0880166166563722
0.124744942600359
0.0485592717962032
0.0627967793663748
0.170323910416011
0.161075154981736
0.219641927572427
-0.0672155773218757
-0.0379295613659315
0.124478705609814
0.130794539007515
0.277474354968663
1
0.0601503616327619
0.153604689353851
-0.109188659475131
0.127078684477856
0.173587085877941
-0.0187794508427134
0.116121510163881
-0.0427317215983532

La correlazione dei rendimenti è spesso lievemente negativa per alcune criptovalute, come ad esempio Ethereum e NEM nei confronti delle altre. Sono presenti ancora correlazioni importanti tra Bitcoin e Litecoin.

Il miglior rendimento è stato registrato da NameCoin con uno 0.0182462446054424 giornaliero, corrispondente al 7339% annuo. Non a caso i rendimenti della criptovaluta in questione sono molto correlati con quelli del Bitcoin in questo periodo. Il minor rendimento è stato quello di Fuelcoin con un - 0.0136189697561832 giornaliero.

Il portafoglio 5 è quello costruito per garantire un rendimento del 100% annuo.

PORTAFOGLIO 5

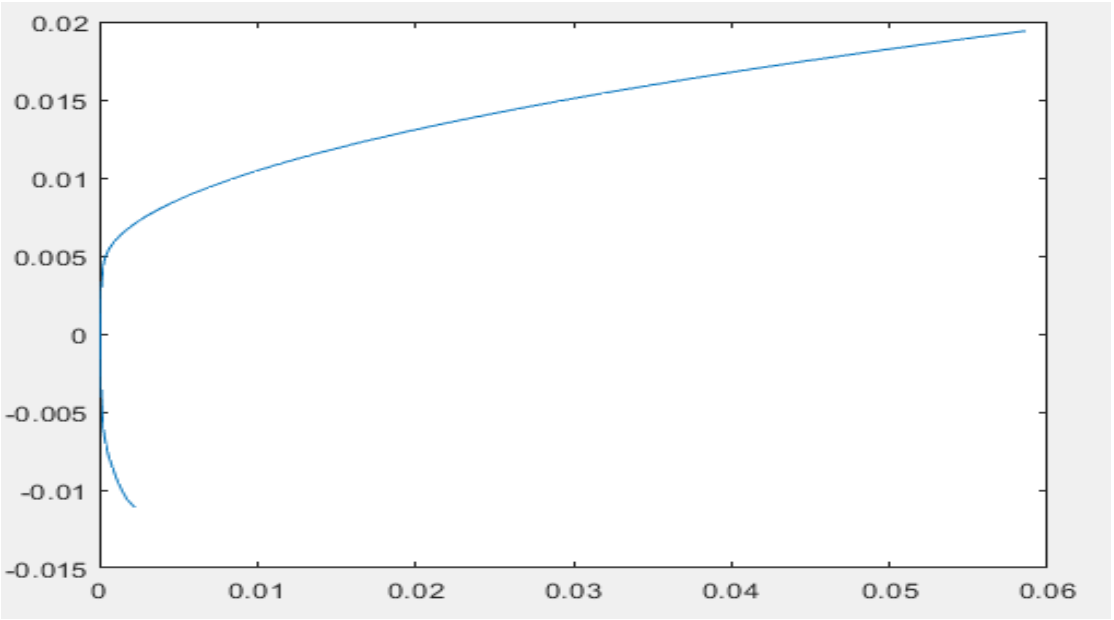
BITCOIN	6%
BITSHARES	1,5%
DASH	21%
DOGECOIN	3%
LITECOIN	10%
MONERO	4,5%
PEERCOIN	9%
RIPPLE	32%
STELLAR	2%
ETHEREUM	8%
NEM	3%

3.4.6 SESTO PERIODO

1 settembre 2016 – 31 dicembre 2016

Il grafico sottostante mostra la frontiera dei portafogli possibili alla Markowitz nel periodo 1 settembre 2016 - 31 dicembre 2016. In questo periodo, secondo il grafico sono presenti portafogli a rischio molto basso che garantiscono un rendimento positivo.

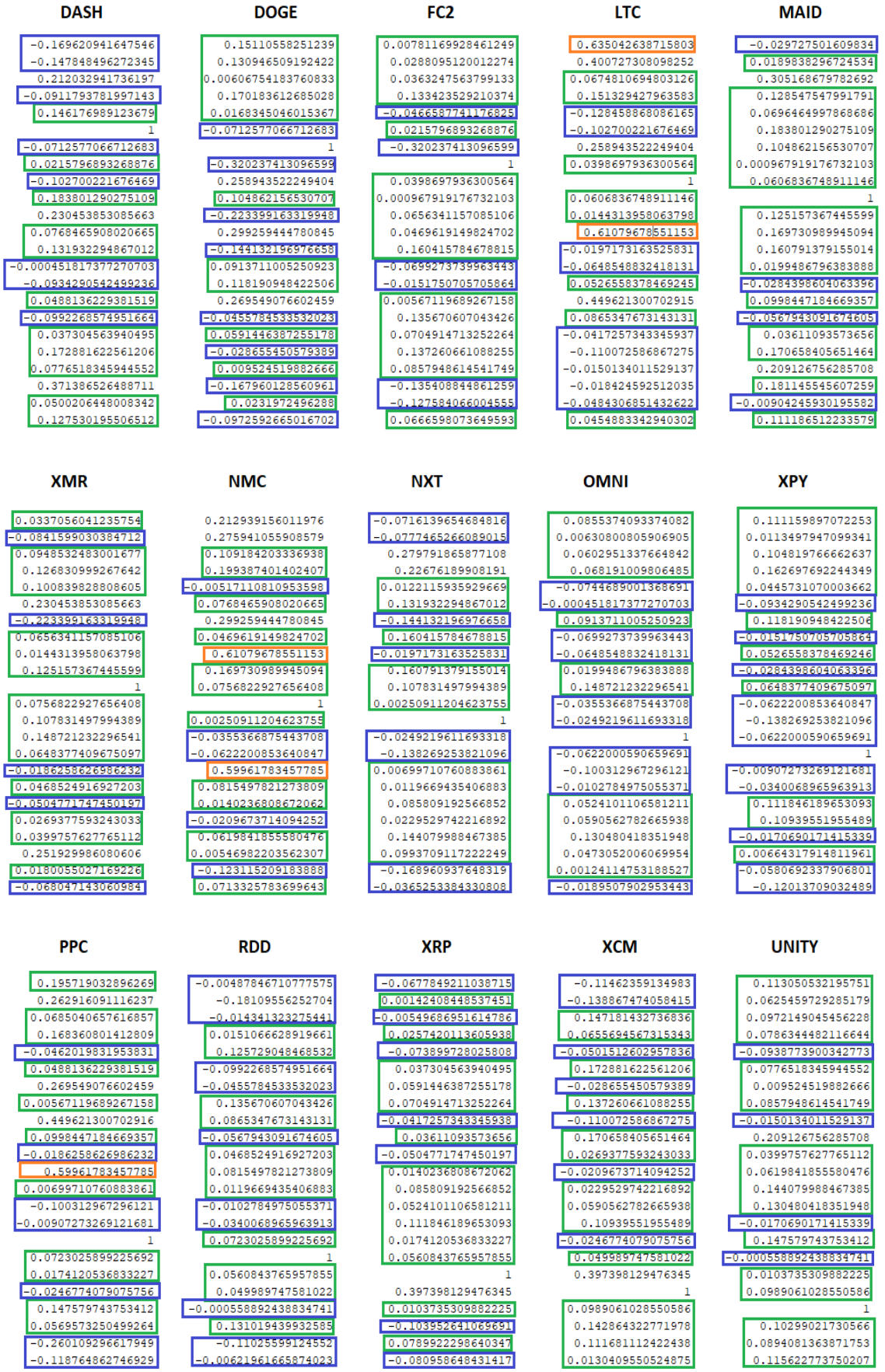
GRAFICO 3.12

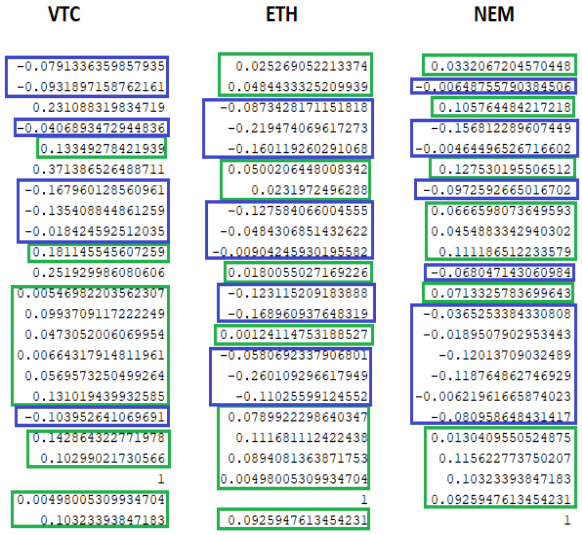


Nella figura 3.6 sono segnalate tutte le correlazioni tra le 23 criptovalute. A giustificare la presenza di un portafoglio a rischio estremamente basso vi sono le molte correlazioni negative dei rendimenti registrate in questo periodo.

FIGURA 3.6

BTC	BTCD	BTS	BLK	XCP
1	0.315747570837479	0.0186593727409593	0.0872478113806629	-0.183363368584524
0.315747570837479	1	-0.0680125390891558	0.14162999371957	-0.156348360200317
0.0186593727409593	-0.0680125390891558	1	0.112441167650447	0.124473221422112
0.0872478113806629	0.14162999371957	0.112441167650447	1	0.094202956802926
-0.183363368584524	-0.156348360200317	0.124473221422112	0.094202956802926	1
-0.169620941647546	-0.147848496272345	0.212032941736197	-0.0911793781997143	0.146176989123679
0.151105582512391	0.130946509192422	0.00606754183760833	0.170183612685028	0.0168345046015367
0.00781169928461249	0.0288095120012274	0.0363247563799133	0.133423529210374	-0.0466587741176825
0.635042638715803	0.400727308098252	0.0674810694803126	0.151329427963583	-0.128458868086165
-0.029727501609834	0.0189838296724534	0.305168679782692	0.128547547991791	0.0696464997868686
0.0337056041235754	-0.0841599030384712	0.0948532483001677	0.126830999267642	0.100839828808605
0.212939156011976	0.275941055908579	0.109184203336938	0.199387401402407	-0.0051711081095359
-0.0716139654684816	-0.0777465266089015	0.279791865877108	0.22676189908191	0.0122115935929669
0.0855374093374082	0.00630800805906905	0.0602951337664842	0.068191009806485	-0.0744689001368691
0.111159897072253	0.0113497947099341	0.104819766662637	0.162697692244349	0.0445731070003662
0.195719032896269	0.262916091116237	0.0685040657616857	0.168360801412809	-0.0462019831953831
-0.00487846710777575	-0.181095562527041	-0.0143413232754411	0.0151066628919661	0.125729048468532
-0.0677849211038715	0.00142408448537451	-0.00549686951614786	0.0257420113605938	-0.0738997280258081
-0.11462359134983	-0.138867474058415	0.147181432736836	0.0655694567315343	-0.0501512602957836
0.113050532195751	0.0625459729285179	0.0972149045456228	0.0786344482116644	-0.0938773900342773
-0.0791336359857935	-0.0931897158762161	0.231088319834719	-0.0406893472944836	0.13349278421939
0.025269052213374	0.0484433325209939	-0.0873428171151818	-0.219474069617273	-0.160119260291068
0.0332067204570448	-0.00648755790384506	0.105764484217218	-0.156812289607449	-0.00464496526716602


DASH
-0.169620941647546
-0.147848496272345
0.212032941736197
-0.0911793781997143
0.146176989123679
1
-0.0712577066712683
0.0215796893268876
-0.102700221676469
0.183801290275109
0.230453853085663
0.0768465908020665
0.131932294867012
-0.0004518173772707O3
-0.0934290542499236
0.0488136229381519
-0.0992268574951664
0.037304563940495
0.172881622561206
0.0776518345944552
0.371386526488711
0.0500206448008342
0.127530195506512
DOGE
0.15110558251239
0.130946509192422
0.00606754183760833
0.170183612685028
0.0168345046015367
-0.0712577066712683
1
-0.320237413096599
0.258943522249404
0.104862156530707
-0.223399163319948
0.299259444780845
-0.144132196976658
0.0913711005250923
0.118190948422506
0.269549076602459
-0.0455784533532023
0.0591446387255178
-0.028655450579389
0.009524519882666
-0.167960128560961
0.0231972496288
-0.0972592665016702
FC2
0.00781169928461249
0.0288095120012274
0.0363247563799133
0.133423529210374
-0.0466587741176825
0.0215796893268876
-0.320237413096599
1
0.0398697936300564
0.000967919176732103
0.0656341157085106
0.0469619149824702
0.160415784678815
-0.0699273739963443
-0.0151750705705864
0.00567119689267158
0.135670607043426
0.0704914713252264
0.137260661088255
0.0857948614541749
-0.135408844861259
-0.127584066004555
0.0666598073649593
LTC
0.6350426387158O3
0.400727308098252
0.0674810694803126
0.151329427963583
-0.128458868086165
-0.102700221676469
0.258943522249404
0.0398697936300564
1
0.0606836748911146
0.0144313958063798
0.610796785511S3
-0.0197173163525831
-0.0648548832418131
0.0526558378469245
0.449621300702915
0.0865347673143131
-0.0417257343345937
-0.110072586867275
-0.0150134011529137
-0.0184245925120S5
-0.0484306851432622
0.0454883342940302
MAID
-0.029727501609834
0.0189838296724534
0.305168679782692
0.128547547991791
0.0696464997868686
0.183801290275109
0.104862156530707
0.000967919176732103
0.0606836748911146
1
0.125157367445599
0.169730989945094
0.160791379155014
0.0199486796383888
-0.0284398604063396
0.0998447184669357
-0.0567943091674605
0.036110935736S6
0.170658405651464
0.209126756285708
0.181145545607259
-0.00904245930195582
0.111186512233579
XMR
0.0337056041235754
-0.0841599030384712
0.0948532483001677
0.126830999267642
0.100839828808605
0.230453853085663
-0.223399163319948
0.0656341157085106
0.0144313958063798
0.125157367445599
1
0.0756822927656408
0.107831497994389
0.148721232296541
0.0648377409675097
-0.0186258626986232
0.0468524916927203
-0.0504771747450197
0.0269377593243033
0.0399757627765112
0.251929986080606
0.0180055027169226
-0.0680471430609S4
NMC
0.212939156011976
0.275941055908579
0.109184203336938
0.199387401402407
-0.00517110810953598
0.0768465908020665
0.299259444780845
0.0469619149824702
0.610796785511S3
0.169730989945094
0.0756822927656408
1
0.00250911204623755
-0.0355366875443708
-0.0622200853640847
0.599611783457785
0.0815497821273809
0.0140236808672062
-0.0209673714094252
0.0619841855580476
0.00546982203562307
-0.123115209183888
0.0713325783699643
NXT
-0.0716139654684816
-0.0777465266089015
0.279791865877108
0.22676189908191
0.0122115935929669
0.131932294867012
-0.144132196976658
0.160415784678815
-0.0197173163525831
0.160791379155014
0.107831497994389
0.00250911204623755
1
-0.0249219611693318
-0.138269253821096
0.00699710760883861
0.0119669435406883
0.085809192566852
0.0229529742216892
0.144079988467385
0.0993709117222249
-0.168960937648319
-0.0365253384330808
OMNI
0.0855374093374082
0.00630800805906905
0.0602951337664842
0.0681910098064S5
-0.0744689001368691
-0.000451817377270703
0.0913711005250923
-0.0699273739963443
-0.0648548832418131
0.0199486796383888
0.148721232296541
-0.0355366875443708
-0.0249219611693318
1
-0.0622000590659691
-0.100312967296121
-0.0102784975055371
0.0524101106581211
0.0590562782665938
0.130480418351948
0.0473052006069954
0.00124114753188527
-0.0189507902953443
XPY
0.111159897072253
0.0113497947099341
0.104819766662637
0.162697692244349
0.0445731070003662
-0.0934290542499236
0.118190948422506
-0.0151750705705864
0.0526558378469246
-0.0284398604063396
0.0648377409675097
-0.0622200853640847
-0.138269253821096
-0.0622000590659691
1
-0.00907273269121681
-0.0340068965963913
0.111846189653093
0.109395551955489
-0.0170690171415339
0.00664317914811961
-0.0580692337906801
-0.120137090324S9
PPC
0.195719032896269
0.262916091116237
0.0685040657616857
0.168360801412809
-0.0462019831953831
0.0488136229381519
0.269549076602459
0.0056711968926715S
0.449621300702916
0.0998447184669357
-0.0186258626986232
0.599611783457785
0.00699710760883861
-0.100312967296121
-0.00907273269121681
1
0.0723025899225692
0.0174120536833227
-0.0246774079075756
0.147579743753412
0.0569573250499264
-0.260109296617949
-0.118764862746929
RDD
-0.00487846710777575
-0.181095562527O4
-0.0143413232754A1
0.0151066628919661
0.125729048468532
-0.0992268574951664
-0.0455784533532023
0.135670607043426
0.0865347673143131
-0.0567943091674605
0.0468524916927203
0.0815497821273809
0.0119669435406883
-0.0102784975055371
-0.0340068965963913
0.0723025899225692
1
0.0560843765957855
0.049989747581022
-0.000558892438834741
0.131019439932585
-0.11025599124552
-0.00621961665874023
XRP
-0.0677849211038715
0.00142408448537451
-0.00549686951614786
0.0257420113605938
-0.073899728025808
0.037304563940495
0.0591446387255178
0.0704914713252264
-0.0417257343345938
0.03611093573656
-0.0504771747450197
0.0140236808672062
0.085809192566852
0.0524101106581211
0.111846189653093
0.0174120536833227
0.056084376595785S
1
0.397398129476345
0.0103735309882225
-0.103952641069691
0.078992229864034S
-0.080958648431417
XCM
-0.114623591349S3
-0.138867474058415
0.147181432736836
0.0655694567315343
-0.0501512602957836
0.172881622561206
-0.028655450579389
0.137260661088255
-0.110072586867275
0.170658405651464
0.0269377593243033
-0.0209673714094252
0.0229529742216892
0.0590562782665938
0.109395519554S9
-0.0246774079075756
0.049989747581022
0.397398129476345
1
0.0989061028550586
0.142864322771978
0.111681112422438
0.0130409550524875
UNITY
0.113050532195751
0.0625459729285179
0.0972149045456228
0.0786344482116644
-0.0938773900342773
0.0776518345944552
0.009524519882666
0.0857948614541749
-0.0150134011529137
0.209126756285708
0.0399757627765112
0.0619841855580476
0.144079988467385
0.130480418351948
-0.0170690171415339
0.147579743753412
-0.000558892438834741
0.0103735309882225
0.0989061028550586
1
0.102990217305S6
0.0894081363871753
0.115622773750207



Il portafoglio 6 mostra il portafoglio alla Markowitz che nel periodo avrebbe garantito un rendimento del 100%.

PORTAFOGLIO 6

BITCOIN	47,5%
BITCOINDARK	1,5%
DASH	10%
DOGECOIN	22%
FUELCOIN	1%
MONERO	3%
RIPPLE	6%
VERTCOIN	3%
ETHEREUM	4%
NEM	2%

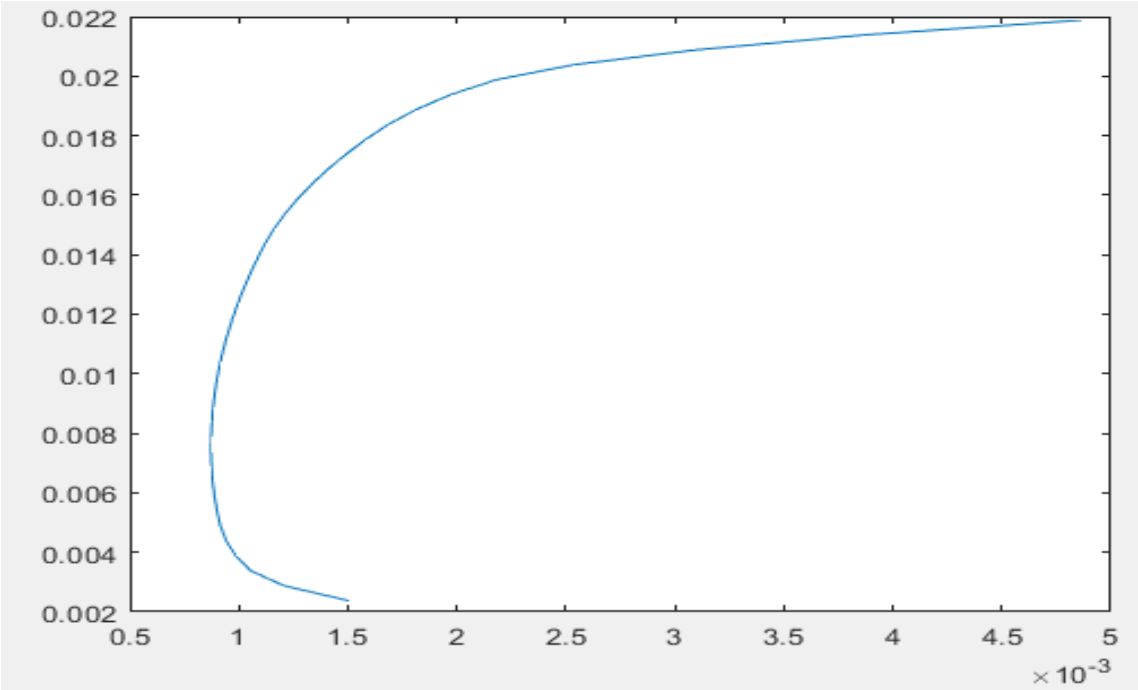
Il massimo rendimento nel periodo è stato registrato da FuelCoin con un +0.0198629597113799 giornaliero, corrispondente a più del 128126% annuo. La criptovaluta nel periodo precedente era stata la peggiore tra quelle considerate. Il minor rendimento lo ha avuto NXT con un - 0.0110859481340132 giornaliero.

3.4.7 SETTIMO PERIODO

1 gennaio 2017 – 30 aprile 2017

Nel grafico sottostante è riportata la frontiera dei portafogli possibili alla Markowitz del periodo 1 gennaio 2017 30 aprile 2017. Il periodo è caratterizzato da un andamento fortemente positivo del mercato, infatti la valutazione di tutte le criptovalute considerate sono aumentate.

GRAFICO 3.13



Nella figura 3.7 sottostante sono riportate le correlazioni dei rendimenti nel periodo considerato. Nel periodo considerato sono state aggiunte le criptovalute NEO e Z-Cash. FuelCoin e PayCoin non sono più state considerate nell'analisi perché la loro liquidità è stata talmente bassa da non poter garantire la formazione di un prezzo di mercato tutti i giorni.

FIGURA 3.7

BTC	BTCD	BTS	BLK	XCP
1	0.267858798022062	0.262486661967912	0.390359178527943	0.346829318906568
0.267858798022062	1	0.0436017164864727	0.0416333309256844	0.169322947902156
0.262486661967912	0.0436017164864727	1	0.49803116367242	0.310500877624801
0.390359178527943	0.0416333309256844	0.498031163672419	1	0.275658987940948
0.346829318906568	0.169322947902156	0.310500877624801	0.275658987940948	1
0.332182105669735	-0.00997023428019838	-4.63113045656347e-05	0.0562097963105037	0.0180139290797048
0.219917644849343	-0.0967045772768392	0.533841308758149	0.421406415705359	0.275291690250306
0.210133419220477	0.0984866737724472	0.273054977963494	0.185380384702239	0.0591780485863861
0.603293331624708	0.214662301838271	0.212182074849492	0.404682605805632	0.350325537046331
0.509921646533823	0.0578900807622406	0.101417487998269	0.237322682401004	0.233450315415099
0.412896928733802	0.0719292977099698	0.38465362821933	0.428766684297514	0.348124285399604
0.333911138149164	-0.00973737854066257	0.450986988878111	0.46452887292364	0.240512223458976
0.445107678190098	0.462686038504668	0.250774037050879	0.285826756476158	0.132847372023361
0.395444993615775	0.0371392493033089	0.526966547855093	0.440966965455427	0.258524490296718
0.00374673548740408	0.0630819699749376	0.0608580397552654	0.13594014043837	0.0499579159922604
0.00896993303979089	-0.00102782514668756	0.547358384124631	0.240705734509724	0.167232879780336
0.195551931561858	-0.0244088897327387	0.673892094207039	0.406535459673543	0.221840811914918
0.339497646289078	0.313322526638011	0.136583905009802	0.0790913490074393	0.145558346351668
0.195899221873037	0.00758700712092719	0.173496691928327	0.183290057653155	0.15047133158122
0.289759727261661	-0.00672010966502237	0.142951153775813	0.366145111005445	0.285621401512031
0.286196039978739	-0.0144014040764792	0.0912724976650133	0.199239962599416	0.168444933064876
0.119939734936927	0.169423440112999	0.0673531307468392	0.0651239048819632	-0.042525445320633
0.178408706245809	-0.160137429224672	0.106487548136233	0.204237794961957	0.0708235462189057

DASH	DOGE	LTC	MAID	XRM
0.332182105669735	0.219917644849343	0.210133419220477	0.603293331624708	0.509921646533823
-0.00997023428019838	-0.0967045772768392	0.0984866737724472	0.214662301838271	0.0578900807622406
-4.63113045656347e-05	0.533841308758149	0.273054977963494	0.212182074849492	0.101417487998269
0.0562097963105037	0.421406415705359	0.185380384702239	0.404682605805632	0.237322682401004
0.0180139290797048	0.275291690250306	0.0591780485863861	0.350325537046331	0.233450315415099
1	-0.0445134021113171	0.119880218043486	0.18204932822763	0.388712816281007
-0.0445134021113171	1	0.411926613933212	0.137751541692471	0.15347699340674
0.119880218043486	0.411926613933212	1	0.193779738496121	0.145180471448841
0.18204932822763	0.137751541692471	0.193779738496121	1	0.451368279258907
0.388712816281007	0.15347699340674	0.145180471448841	0.451368279258907	1
-0.0406183622517076	0.423198469116295	0.350625460295229	0.35484298215625	0.360888002891279
0.026161958097144	0.469249230196034	0.168454592718092	0.223607152340849	0.0692687492576011
0.188648222176728	0.11324983921743	0.239696955506055	0.426093221963865	0.227681820620021
-0.0267489208071348	0.434458148767931	0.356472627021037	0.373235584353002	0.316060396249016
0.0368760598695089	-0.0214121095173903	-0.0942625058799522	0.238789573721556	0.0646122621036302
-0.18497542248942	0.620269977652143	0.214974007802222	-0.0690130706909875	-0.0312859746506638
-0.0425636703684152	0.668104063720552	0.399487089268594	0.144105148177306	0.14165084352667
0.0532198369983377	0.0808021160305239	0.215817954268389	0.323894900814173	0.194551017947396
0.0422733281745103	0.0217959488243236	-0.00175688532722341	0.245327042374984	0.202036082136764
0.242175864861903	0.219845161271573	0.116027718011493	0.326114512019369	0.647182866130245
0.167295828769749	-0.122952973104604	-0.0470534017828579	0.370955942149396	0.257152464984348
0.250391556312825	0.11375193659702	0.0527561689420305	0.130504589660088	0.0778492065699143
0.437651777942018	0.254402959376302	0.172314551592834	0.204731134045239	0.325716300654532


NMC
0.412896928733802
0.0719292977099698
0.38465362821933
0.428766684297514
0.348124285399604
-0.0406183622517076
0.423198469116295
0.350625460295229
0.35484298215625
0.360888002891279
1
0.329096516230542
0.271580623523978
0.823355169211668
0.00191551437882749
0.250239127152787
0.401040106202051
0.252289608129894
0.138039277407117
0.430801177237226
0.194520830189014
-0.0633551987352744
0.164552501584698
NXT
0.333911138149164
-0.00973737854066257
0.450986988878111
0.46452887292364
0.240512223458976
0.026161958097144
0.469249230196034
0.168454592718092
0.223607152340849
0.0692687492576011
0.329096516230542
1
0.253940826230219
0.399041148808112
0.0807510376982325
0.280508311464912
0.424833509948795
0.0857977992649637
0.145020804409775
0.0914583224877597
0.0434619542772372
-0.0565703852109909
0.0817905653585869
OMNI
0.445107678190098
0.462686038504668
0.250774037050879
0.285826756476158
0.132847372023361
0.188648222176728
0.11324983921743
0.239696955506055
0.426093221963865
0.227681820620021
0.271580623523978
0.253940826230219
1
0.373644689974263
0.109587908440049
-0.0334467053948232
0.0749845329772753
0.418073389989434
0.159957074423516
0.137092596627474
0.13586071550653
0.114645171345495
0.149306668466111
PPC
0.395444993615775
0.0371392493033089
0.526966547855093
0.440966965455427
0.258524490296718
-0.0267489208071348
0.434458148767931
0.356472627021037
0.373235584353002
0.316060396249016
0.823355169211668
0.399041148808112
0.373644689974263
1
0.0271688598486851
0.289136519428337
0.443715147114037
0.259001922776262
0.25817865674903
0.380735042995083
0.150232088921641
-0.0326134578818229
0.126388086822
RDD
0.00374673548740408
0.0630819699749376
0.0608580397552654
0.13594014043837
0.0499579159922604
0.0368760598695089
-0.0214121095173903
-0.0942625058799522
0.238789573721556
0.0646122621036302
0.00191551437882749
0.0807510376982325
0.109587908440049
0.0271688598486851
1
0.0423601728350131
-0.00948239254581527
0.030704920831345
0.112917519023821
-0.0395470819111174
0.146321265146882
0.0174818820717374
0.0659680956937255
XRP
0.00896993303979089
-0.00102782514668756
0.547358384124631
0.240705734509724
0.167232879780336
-0.184975422488442
0.620269977652143
0.214974007802222
-0.0690130706909875
-0.0312859746506338
0.250239127152787
0.280508311464912
-0.0334467053948232
0.289136519428337
0.0423601728350131
1
0.737382311425857
0.026388197555252
-0.00397522299353331
0.0126164776638699
-0.186035558363504
0.0336084664493155
0.106588517991756
XCM
0.195551931561858
-0.0244088897327387
0.673892094207039
0.406535459673543
0.221840811914918
-0.0425636703684152
0.668104063720552
0.399487089268594
0.144105148177306
0.14165084352667
0.401040106202051
0.424833509948795
0.0749845329772753
0.443715147114037
-0.00948239254581527
0.737382311425857
1
0.194738551900745
0.0295372186576309
0.180609750398597
-0.0343547398167695
0.132043888189059
0.1804579764716
UNITY
0.339497646289078
0.313322526638011
0.136583905009802
0.0790913490074393
0.145558346351668
0.0532198369983376
0.0808021160305239
0.215817954268389
0.323894900814172
0.194551017947396
0.252289608129894
0.0857977992649637
0.418073389989434
0.259001922776262
0.030704920831345
0.026388197555252
0.194738551900745
1
0.105562476725309
0.189638194538284
0.138443061534547
0.0520820852278537
0.0161373482781008
VTC
0.195899221873037
0.00758700712092719
0.173496691928327
0.183290057653155
0.15047133158122
0.0422733281745103
0.0217959488243236
-0.00175688532722341
0.245327042374984
0.202036082136764
0.138039277407117
0.145020804409775
0.159957074423516
0.25817865674903
0.112917519023821
-0.00397522299353331
0.0295372186576309
0.105562476725309
1
0.143542610293881
0.235299032773061
0.0268711251744687
0.0631343518734257
ETH
0.289759727261661
-0.00672010966502237
0.142951153775813
0.366145111005445
0.285621401512031
0.242175864861903
0.219845161271573
0.116027718011493
0.326114512019369
0.647182866130245
0.430801177237226
0.0914583224877597
0.137092596627474
0.380735042995083
-0.0395470819111174
0.0126164776638699
0.180609750398597
0.189638194538284
0.143542610293881
1
0.172678141618786
-0.0102343558408116
0.181089797847188
NEM
0.286196039978739
-0.0144014040764792
0.0912724976650133
0.199239962599416
0.168444933064876
0.167295828769749
-0.122952973104604
-0.0470534017828579
0.370955942149396
0.257152464984348
0.194520830189014
0.0434619542772372
0.13586071550653
0.150232088921641
0.146321265146882
-0.186035558363504
-0.0343547398167695
0.138443061534547
0.235299032773061
0.172678141618786
1
0.079214749090505
0.181097837984018
NEO
0.119939734936927
0.169423440112999
0.0673531307468392
0.0651239048819632
-0.042525445320633
0.250391556312825
0.11375193659702
0.0527561689420305
0.130504589660088
0.0778492065699143
-0.0633551987352744
-0.0565703852109909
0.114645171345495
-0.0326134578818229
0.0174818820717374
0.0336084664493155
0.132043888189059
0.0520820852278537
0.0268711251744687
-0.0102343558408116
0.079214749090505
1
0.380774446793294
ZEC
0.178408706245809
-0.160137429224672
0.106487548136233
0.204237794961957
0.0708235462189057
0.437651777942018
0.254402959376302
0.172314551592834
0.204731134045239
0.325716300654532
0.164552501584698
0.0817905653585869
0.149306668466111
0.126388086822
0.0659680956937255
0.106588517991756
0.1804579764716
0.0161373482781008
0.0631343518734257
0.181089797847188
0.181097837984018
0.380774446793294
1

Nel periodo considerato i rendimenti delle criptovalute sono generalmente correlati in maniera inferiore rispetto ai periodi precedenti. Il maggior rendimento è garantito da NEM con uno 0.0223435738103656 giornaliero, corrispondente al 317809% annuo. Il rendimento minore invece è stato ottenuto da BTC con uno 0.00237845995414379 giornaliero, circa il 200% annuo. Visto la tendenza fortemente positiva del periodo considerato, un rendimento inferiore allo 0.008 giornaliero non risulta nella frontiera efficiente in questo periodo. Infatti per i portafogli che garantiscono un rendimento inferiore esiste un portafoglio che lo domina secondo il criterio media-varianza. Per tale motivo il portafoglio considerato ha come obiettivo quello di garantire un rendimento di 0.008 giornaliero (1732% anno), il minor rendimento presente nella frontiera efficiente nel periodo.

PORTAFOGLIO 7

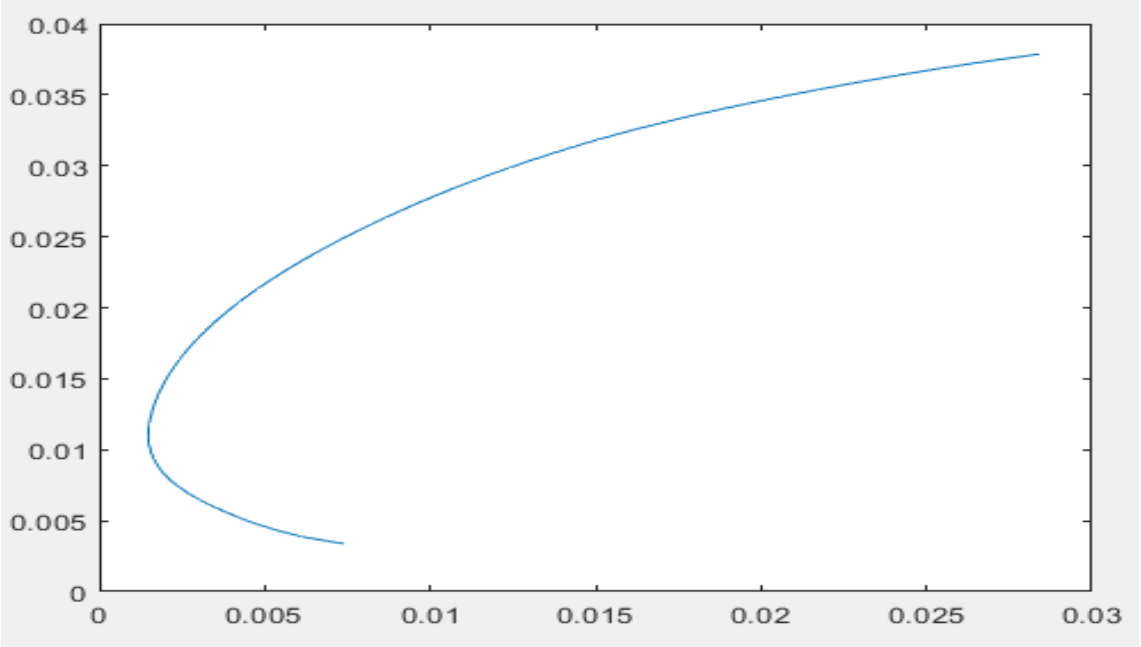
BITCOIN	35%
DOGECOIN	10%
LITECOIN	8%
NXT	4%
REDDCOIN	1,5%
RIPPLE	1,4%
VERTCOIN	2%
ETHEREUM	7%
NEM	7%
NEO	21%
Z-CASH	3,1%

3.4.8 OTTAVO PERIODO

1 maggio 2017 – 31 agosto 2017

Anche in questo periodo, come nel precedente, tutte le criptovalute hanno ottenuto un rendimento fortemente positivo, come si può vedere anche dal grafico sottostante.

GRAFICO 3.14



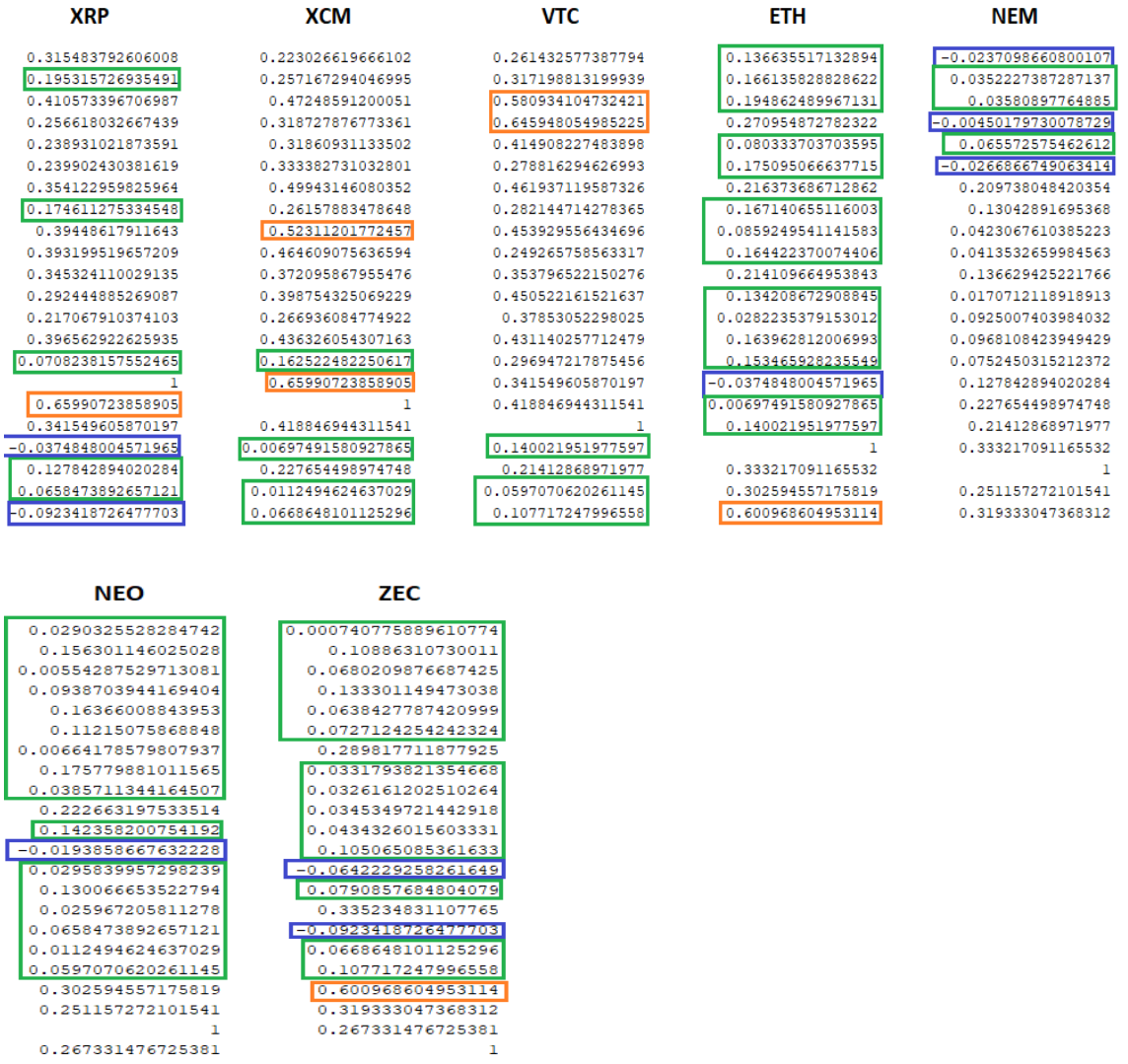
Nella figura 3.8 sottostante sono riportate tutte le correlazioni dei rendimenti delle criptovalute nel periodo considerato. Nel periodo considerato non è più stata considerata la criptovalute “Unity” che ha avuto degli scambi troppo bassi che non hanno più potuto garantire un prezzo giornaliero.

FIGURA 3.8

BTC	BTCD	BTS	BLK	XCP
1	0.417314127304557	0.417391315158585	0.37920144423237	0.35019162156087
0.417314127304557	1	0.341554826233852	0.405492323338354	0.383476956878976
0.417391315158586	0.341554826233852	1	0.634281355277595	0.44900217407225
0.37920144423237	0.405492323338354	0.634281355277595	1	0.487967077425564
0.35019162156087	0.383476956878976	0.44900217407225	0.487967077425564	1
0.530071000982263	0.331862931846929	0.357669351082423	0.41280409849471	0.491941510340877
0.44793602757819	0.311932758938504	0.59370497336533	0.503816619810052	0.458284681577877
0.454315987367115	0.261607967407746	0.321911439033351	0.368924253953028	0.193715184714246
0.548559730158555	0.42681304673672	0.474647391534378	0.481855560471368	0.578487802085687
0.42310862215951	0.280268270868446	0.333511065294664	0.317285542706967	0.305696643119484
0.454464689418534	0.37868776223566	0.353296455926745	0.375435848613144	0.351018660381404
0.346825153787644	0.31537186963323	0.574928835762215	0.704405724289454	0.426722725826958
0.353972027837346	0.276346276081363	0.400759891783954	0.434965736506389	0.443300611774352
0.502464909338388	0.422668638647442	0.466870608751018	0.471626337502183	0.407429184727581
0.273860604890326	0.309676833994558	0.313832387869391	0.217134421423151	0.332052242343888
0.315483792606008	0.195315726935491	0.410573396706987	0.256618032667439	0.238931021873591
0.223026619666102	0.257167294046995	0.47248591200051	0.318727876773361	0.31860931133502
0.261432577387794	0.317198813199939	0.580934104732421	0.645948054985225	0.414908227483898
0.136635517132894	0.166135828828622	0.194862489967131	0.270954872782322	0.080333703703595
-0.0237098660800107	0.0352227387287137	0.03580897764885	-0.00450179730078729	0.065572575462612
0.0290325528284742	0.156301146025028	0.00554287529713081	0.0938703944169404	0.16366008843953
0.00074077588961077 4	0.10886310730011	0.0680209876687425	0.133301149473038	0.0638427787420999

DASH	DOGE	LTC	MAID	XRM
0.530071000982263	0.44793602757819	0.454315987367116	0.548559730158555	0.42310862215951
0.331862931846929	0.311932758938504	0.261607967407746	0.42681304673672	0.280268270868446
0.357669351082423	0.59370497336533	0.321911439033351	0.474647391534378	0.333511065294664
0.41280409849471	0.503816619810052	0.368924253953028	0.481855560471368	0.317285542706967
0.491941510340877	0.458284681577877	0.193715184714246	0.578487802085687	0.305696643119484
1	0.414629234353004	0.352770087350992	0.60758121184066	0.610528593766122
0.414629234353004	1	0.391362730001283	0.522782533291589	0.372909417309065
0.352770087350992	0.391362730001283	1	0.380804552236952	0.427501647369689
0.60758121184066	0.522782533291589	0.380804552236952	1	0.553161339093172
0.610528593766122	0.372909417309065	0.427501647369689	0.553161339093172	1
0.451556091245052	0.381135005005238	0.54300864357942	0.483390722977628	0.506405371652793
0.441576485277388	0.485284804652824	0.344626845523625	0.521932527644175	0.348547287654674
0.434823082977883	0.335255137579444	0.17935168177353	0.458432136513845	0.357692388899097
0.50144965212932	0.44927201385215	0.580992474068939	0.550096641205978	0.547451569364917
0.29968544335907	0.558185981327588	0.179287063007011	0.33657050879192	0.245300897533592
0.239902430381619	0.354122959825964	0.174611275334548	0.39448617911643	0.393199519657209
0.333382731032801	0.49943146080352	0.26157883478648	0.52311201772457	0.464609075636594
0.278816294626993	0.461937119587326	0.282144714278365	0.453929556434696	0.249265758563317
0.175095066637715	0.216373686712862	0.167140655116003	0.0859249541141583	0.164422370074406
-0.0266866749063414	0.209738048420354	0.13042891695368	0.0423067610385223	0.0413532659984563
0.112150758688 48	0.00664178579807937	0.175779881011565	0.0385711344164507	0.222663197533514
0.0727124254242324	0.289817711877925	0.0331793821354668	0.0326161202510264	0.0345349721442918

NMC	NXT	OMNI	PCC	RDD
0.454464689418534	0.346825153787644	0.353972027837346	0.502464909338388	0.273860604890326
0.37868776223566	0.31537186963323	0.276346276081363	0.422668638647443	0.309676833994558
0.353296455926745	0.574928835762215	0.400759891783954	0.466870608751018	0.313832387869391
0.375435848613144	0.704405724289454	0.434965736506389	0.471626337502183	0.217134421423151
0.351018660381404	0.426722725826958	0.443300611774352	0.407429184727581	0.332052242343888
0.451556091245052	0.441576485277388	0.434823082977883	0.50144965212932	0.29968544335907
0.381135005005238	0.485284804652824	0.335255137579444	0.44927201385215	0.558185981327588
0.54300864357942	0.344626845523625	0.17935168177353	0.580992474068939	0.179287063007011
0.483390722977628	0.521932527644175	0.458432136513845	0.550096641205978	0.33657050879192
0.506405371652793	0.348547287654674	0.357692388899097	0.547451569364917	0.245300897533592
1	0.359521410466683	0.258401069885944	0.872402950095359	0.335531825262224
0.359521410466683	1	0.332629550190983	0.449628806048682	0.260125692384071
0.258401069885944	0.332629550190983	1	0.304959391368665	0.127908679364767
0.872402950095359	0.449628806048682	0.304959391368665	1	0.331725202396837
0.335531825262224	0.260125692384071	0.127908679364767	0.331725202396837	1
0.345324110029135	0.292444885269087	0.217067910374103	0.396562922625935	0.0708238157552465
0.372095867955476	0.398754325069229	0.266936084774922	0.436326054307163	0.162522482250617
0.353796522150276	0.450522161521637	0.37853052298025	0.431140257712479	0.296947217875456
0.214109664953843	0.134208672908845	0.0282235379153012	0.163962812006993	0.153465928235549
0.136629425221766	0.0170712118918913	0.0925007403984032	0.0968108423949429	0.0752450315212372
0.142358200754192	-0.0193858667632228	0.0295839957298239	0.130066653522794	0.0259672058112779
0.0434326015603331	0.105065085361633	-0.0642229258261649	0.0790857684804079	0.335234831107765



Le correlazioni dei rendimenti del periodo sono maggiori rispetto a quelle dei periodi precedenti, in particolare le Altcoin registrano correlazioni tra di loro superiori al 50%.

In questo periodo, come nel precedente, il minimo rendimento ottenuto è superiore al 100% annuale. Visto l'andamento fortemente positivo del settore in questo periodo e la crescita elevata di tutti gli asset considerati nell'analisi, un rendimento inferiore al 1% giornaliero (3700% annuo) sarebbe al di sotto della frontiera efficiente di Markowitz. Per rendimenti inferiori a questo, esiste un portafoglio con uguale rischio, ma con un rendimento atteso superiore. Per tale motivo il portafoglio 8 è stato ottenuto ponendo come obiettivo un rendimento dell'1% giornaliero.

PORTAFOGLIO 8

BITCOIN	58%
DASH	3,5%
LITECOIN	3%
RIPPLE	5,5%
ETHEREUM	7%
NEM	9%
ZCASH	14%

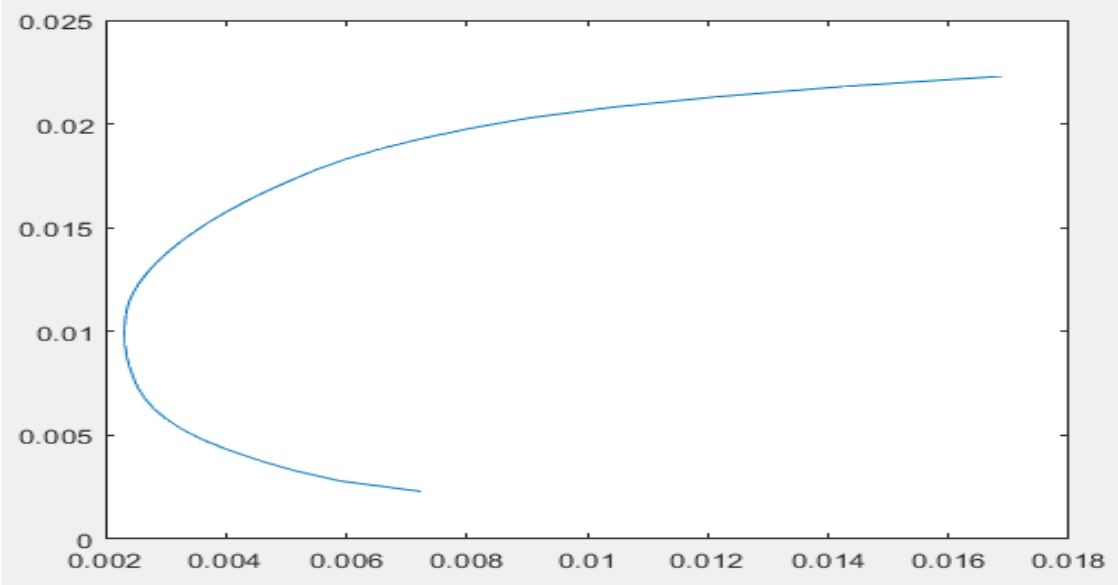
Il minimo rendimento del periodo è registrato da Peercoin 0.00336743484630779 giornaliero, mentre il più alto è stato garantito da NEO con quasi il 4% (0.0380689874790808) giornaliero, un rendimento del 83405772% annuo.

3.4.9 NONO PERIODO

1 settembre 2017 – 31 dicembre 2017

Anche nel periodo tra settembre e fine dicembre 2017 i rendimenti registrati da tutte le criptovalute considerate sono fortemente positivi.

GRAFICO 3.15



Nessun portafoglio alla Markowitz tra le criptovalute considerate ha registrato un rendimento negativo in questo periodo.

Il terzo periodo considerato nel 2017 vede l'inserimento di due nuove criptovalute nella scelta: IOTA e BitcoinCash. Nella figura 3.9 sono riportate le correlazioni dei rendimenti delle 24 criptovalute inserite nell'analisi.

FIGURA 3.9

BTC	BTCD	BTS	BLK	XCP
1	0.226823988628222	0.325489716127201	0.384042541227529	0.32084178932456
0.226823988628222	1	0.321319089495664	0.348838107619842	0.228267366877571
0.325489716127201	0.321319089495664	1	0.518025407725853	0.403339037965386
0.384042541227529	0.348838107619842	0.518025407725853	1	0.388958657463128
0.32084178932456	0.228267366877571	0.403339037965386	0.388958657463128	1
0.208790345343447	0.134391798061223	0.369086045524595	0.263631845211128	0.222960700655591
0.552645988597931	0.297183440528479	0.602138537892335	0.505757763851731	0.443984865199705
0.50372127931904	0.16851247976461	0.429802808755412	0.49374984850232	0.396096798783676
0.330754341702892	0.305732318716817	0.518999322923826	0.542981942857392	0.552381064904854
0.460022288652432	0.293432200383867	0.533421990008825	0.409021784972482	0.498553523508145
0.515602254740166	0.19459374078658	0.458365206938757	0.528184371845984	0.499439756970209
0.49807946811869	0.374807820309525	0.433057433540444	0.321749131859023	0.290134333579045
0.384128290626468	0.183904167343136	0.421881195465911	0.428709264780121	0.394495358502199
0.44792762778897	0.18886988957617	0.500015392060225	0.465069427396531	0.37410202854122
0.260437493207844	0.368413229628797	0.421559137448058	0.238174192992259	0.212181215297889
0.123073532677756	0.0896305713525136	0.432897035600375	0.270078140571243	0.360652258543194
0.332529088008821	0.163447765405916	0.514640537940999	0.336531973437708	0.446122515782696
0.263846874377366	0.114345827221128	0.286289639918826	0.379412853408118	0.441315917277437
0.459925788412754	0.273757335725012	0.565154344762059	0.617408351431963	0.519096117412447
0.197115667218828	0.0190384747278788	0.397601714294939	0.417403837235019	0.327929076701098
0.274842884747831	0.313126355384063	0.444984219198785	0.397879865518205	0.387714352416571
0.364276335756646	0.23923557691728	0.592326340564085	0.47385187511381	0.430027375247666
0.353730208905481	0.177590059005162	0.485589216483851	0.467710765865849	0.415686000606488
0.127201981454466	0.179460099959087	0.441948832258258	0.333015547197417	0.312556932024491

DASH	DOGE	LTC	MAID	XRM
0.208790345343447	0.552645988597931	0.50372127931904	0.330754341702892	0.460022288652432
0.134391798061223	0.297183440528479	0.16851247976461	0.305732318716817	0.293432200383867
0.369086045524595	0.602138537892335	0.429802808755412	0.518999322923826	0.533421990008825
0.263631845211128	0.505757763851731	0.49374984850232	0.542981942857392	0.409021784972482
0.222960700655591	0.443984865199705	0.396096798783676	0.552381064904854	0.498553523508145
1	0.355203586069046	0.419062663036317	0.455511086848281	0.579785557701073
0.355203586069046	1	0.551999312074245	0.545601020755996	0.581399578248271
0.419062663036317	0.551999312074245	1	0.578014625990568	0.518566612517288
0.455511086848281	0.545601020755996	0.578014625990568	1	0.704256791053215
0.579785557701073	0.581399578248271	0.518566612517288	0.704256791053215	1
0.398125414394533	0.591376691025318	0.519212199055624	0.582244099053755	0.578607281143625
0.276496869569344	0.425699545812349	0.403495601101842	0.469964066998665	0.476818729161964
0.0784356846020083	0.455172283417166	0.398856285682461	0.340396728021831	0.316566650099306
0.415053520761131	0.623217623498958	0.484676210975301	0.443815771165733	0.435005789740632
0.330712435313036	0.573178929840817	0.182899651335195	0.327517609248376	0.400874368068357
0.177871814472162	0.367423275430091	0.335941580960937	0.415807546757631	0.314390241078136
0.174398656157416	0.490939483493831	0.369955026930941	0.462549947445555	0.489418505441889
0.239417490474192	0.325344921039824	0.387187682549275	0.492562521306053	0.398550923754888
0.513064438703794	0.588826126208219	0.708921255877991	0.708921255877991	0.649785686651394
0.292481456232487	0.443140551979701	0.520444656827894	0.489978939732578	0.398243557992933
0.353986031770256	0.454595080211489	0.410357607680079	0.583076891226983	0.486375471064297
0.604546611005605	0.53002169217454	0.552700027164295	0.621900629193203	0.692263813339132
0.300614445967017	0.42500786652215	0.471304679325309	0.527789831452655	0.589095453547794
0.44921094144659	0.283023534360548	0.275264525940139	0.36049468507815	0.426227185724771

NMC	NXT	OMNI	PCC	RDD
0.515602254740166	0.49807946811869	0.384128290626468	0.44792762778897	0.260437493207844
0.19459374078658	0.374807820309525	0.183904167343136	0.18886988957617	0.368413229628797
0.458365206938757	0.433057433540444	0.421881195465911	0.500015392060225	0.421559137448058
0.528184371845984	0.321749131859023	0.428709264780121	0.465069427396531	0.238174192992259
0.499439756970209	0.290134333579045	0.394495358502199	0.37410202854122	0.212181215297889
0.398125414394533	0.276496869569345	0.0784356846020083	0.415053520761131	0.330712435313036
0.591376691025318	0.425699545812349	0.455172283417166	0.623217623498958	0.573178929840816
0.519212199055624	0.403495601101842	0.398856285682461	0.484676210975301	0.182899651335195
0.582244099053755	0.469964066998665	0.340396728021831	0.443815771165733	0.327517609248376
0.578607281143625	0.476818729161964	0.316566650099306	0.435005789740632	0.400874368068357
1	0.364163984014851	0.433373708200551	0.744290905963944	0.24170471381012
0.364163984014851	1	0.21836895244578	0.274857484972229	0.396474466408532
0.433373708200551	0.21836895244578	1	0.343414534114923	0.25801458877399
0.744290905963944	0.274857484972229	0.343414534114923	1	0.275456387102532
0.24170471381012	0.396474466408532	0.25801458877399	0.275456387102532	1
0.311160507560236	0.0840221136874645	0.263754281602676	0.233061804415818	0.0899905204941255
0.373872668999109	0.313728854198367	0.266847421262584	0.336125827646603	0.218644408021963
0.39434306600973	0.292787234294627	0.231222421442892	0.33803289753573	0.205411561304902
0.645769625618613	0.434421368732569	0.452395645432946	0.520504759098163	0.301839838227912
0.397031666025542	0.240143400824393	0.268380247883425	0.381368008244736	0.179301782907894
0.511050785167427	0.327220828302248	0.319207777779221	0.433568916222372	0.300244813293293
0.498591014722479	0.398939483144403	0.296599350642388	0.456601672136991	0.324304250667379
0.389393963147063	0.317186542820814	0.304210258080658	0.315069457940694	0.215844795985121
0.302860086072903	0.269245208752858	0.126481592506921	0.227625290744215	0.303803679982744

XRP	XCM	VTC	ETH	NEM
0.123073532677560	0.332529088008821	0.263846874377366	0.459925788412754	0.197115667218828
0.0896305713525136	0.163447765405916	0.114345827221128	0.273757335725012	0.0190384747278788
0.432897035600375	0.514640537940999	0.286289639918826	0.565154344762059	0.397601714294939
0.270078140571243	0.336531973437708	0.379412853408118	0.617408351431963	0.417403837235019
0.360652258543194	0.446122515782696	0.441315917277437	0.519096117412447	0.327929076701098
0.177871814472162	0.174398656157416	0.239417490474192	0.513064438703794	0.292481456232487
0.367423275430091	0.490939483493831	0.325344921039824	0.588826126208219	0.443140551979701
0.335941580960937	0.369955026930941	0.387187682549275	0.782415444044188	0.520444656827894
0.415807546757631	0.462549947445555	0.492562521306053	0.708921255877991	0.489978939732578
0.314390241078136	0.489418505441889	0.398550923754888	0.649785686651394	0.398243557992933
0.311160507560236	0.373872668999109	0.39434306600973	0.645769625618613	0.397031666025542
0.0840221136874645	0.313728854198367	0.292787234294627	0.434421368732569	0.240143400824393
0.263754281602676	0.266847421262584	0.231222421442892	0.452395645432946	0.268380247883425
0.233061804415818	0.336125827646603	0.33803289753573	0.520504759098163	0.381368008244736
0.0899905204941255	0.218644408021963	0.205411561304902	0.301839838227912	0.179301782907894
1	0.383553754908182	0.166018501649304	0.447129498228471	0.386582162658452
0.383553754908182	1	0.402261040733444	0.42194792457843	0.385244860341181
0.166018501649304	0.402261040733444	1	0.460859519891998	0.397214491315523
0.447129498228471	0.42194792457843	0.460859519891998	1	0.508781478675223
0.386582162658452	0.385244860341181	0.397214491315523	0.508781478675223	1
0.315257718577932	0.415971906112475	0.329948627486843	0.569995275104596	0.355903580512618
0.52979827259522	0.491499026593692	0.348640401866194	0.716193674000821	0.482454364790665
0.195961877456046	0.492045978089366	0.327962049757937	0.499375376283956	0.47983581798542
0.201344349150845	0.175341410240822	0.173334122954126	0.44490357849483	0.294308974077647

NEO	ZEC	IOTA	BTCC
0.274842884747831	0.364276335756646	0.353730208905481	0.127201981454466
0.313126355384063	0.23923557691728	0.177590059005162	0.179460099959087
0.444984219198785	0.592326340564085	0.485589216483851	0.441948832258258
0.397879865518204	0.47385187511381	0.467710765865849	0.333015547197417
0.387714352416571	0.430027375247666	0.415686000606488	0.312556932024491
0.353986031770256	0.604546611005605	0.300614445967017	0.44921094144659
0.454595080211489	0.53002169217454	0.42500786652215	0.283023534360548
0.410357607680079	0.552700027164295	0.471304679325309	0.275264525940139
0.583076891226983	0.621900629193203	0.527789831452655	0.36049468507815
0.486375471064297	0.692263813339132	0.589095453547794	0.426227185724771
0.511050785167427	0.498591014722479	0.389393963147063	0.302860086072903
0.327220828302248	0.398939483144403	0.317186542820814	0.269245208752858
0.319207777779221	0.296599350642388	0.304210258080658	0.126481592506921
0.433568916222372	0.456601672136991	0.315069457940694	0.227625290744215
0.300244813293293	0.324304250667379	0.215844795985121	0.303803679982744
0.315257718577932	0.52979827259522	0.195961877456046	0.201344349150845
0.415971906112475	0.491499026593692	0.492045978089366	0.175341410240822
0.329948627486843	0.348640401866194	0.327962049757937	0.173334122954126
0.569995275104596	0.716193674000821	0.499375376283956	0.44490357849483
0.355903580512618	0.482454364790665	0.47983581798542	0.294308974077647
1	0.577834073989885	0.32096162097752	0.388200101745693
0.577834073989885	1	0.512911515103465	0.479725714974144
0.32096162097752	0.512911515103465	1	0.269404756306748
0.388200101745693	0.479725714974144	0.269404756306748	1

Rispetto al periodo precedente, le correlazioni tra i rendimenti delle varie criptovalute, in particolar modo delle Altcoin, è più importante. Per la prima volta nei periodi considerati in questa tesi non è presente nessuna correlazione dei rendimenti negativa. Il portafoglio 9 è il portafoglio presente nella frontiera efficiente delle osservazioni del periodo secondo Markovitz che presenta la varianza inferiore.

PORTAFOGLIO 9

BITCOIN	45%
BITCOINDARK	10%
DASH	18,5%
OMNI	1%
RIPPLE	11%
VERTCOIN	1%
ETHEREUM	9,5%
BITCOINCASH	4%

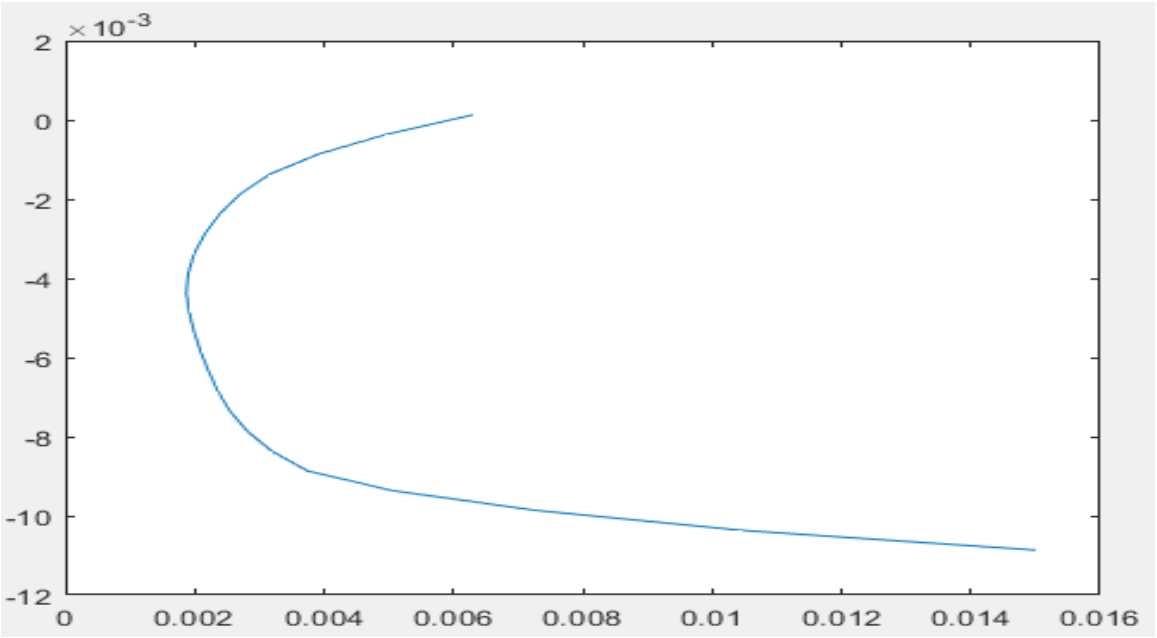
Nel periodo considerato il maggior rendimento è stato garantito da Stellar con uno 0.0224137727686528 giornaliero (325854% annuo), il minore invece lo ha fatto registrare MaidSaveCoin con un +0.00230152178279566 MaidSaveCoin, il 126% annuale.

3.4.10 DECIMO PERIODO

1 gennaio 2018 – 30 aprile 2018

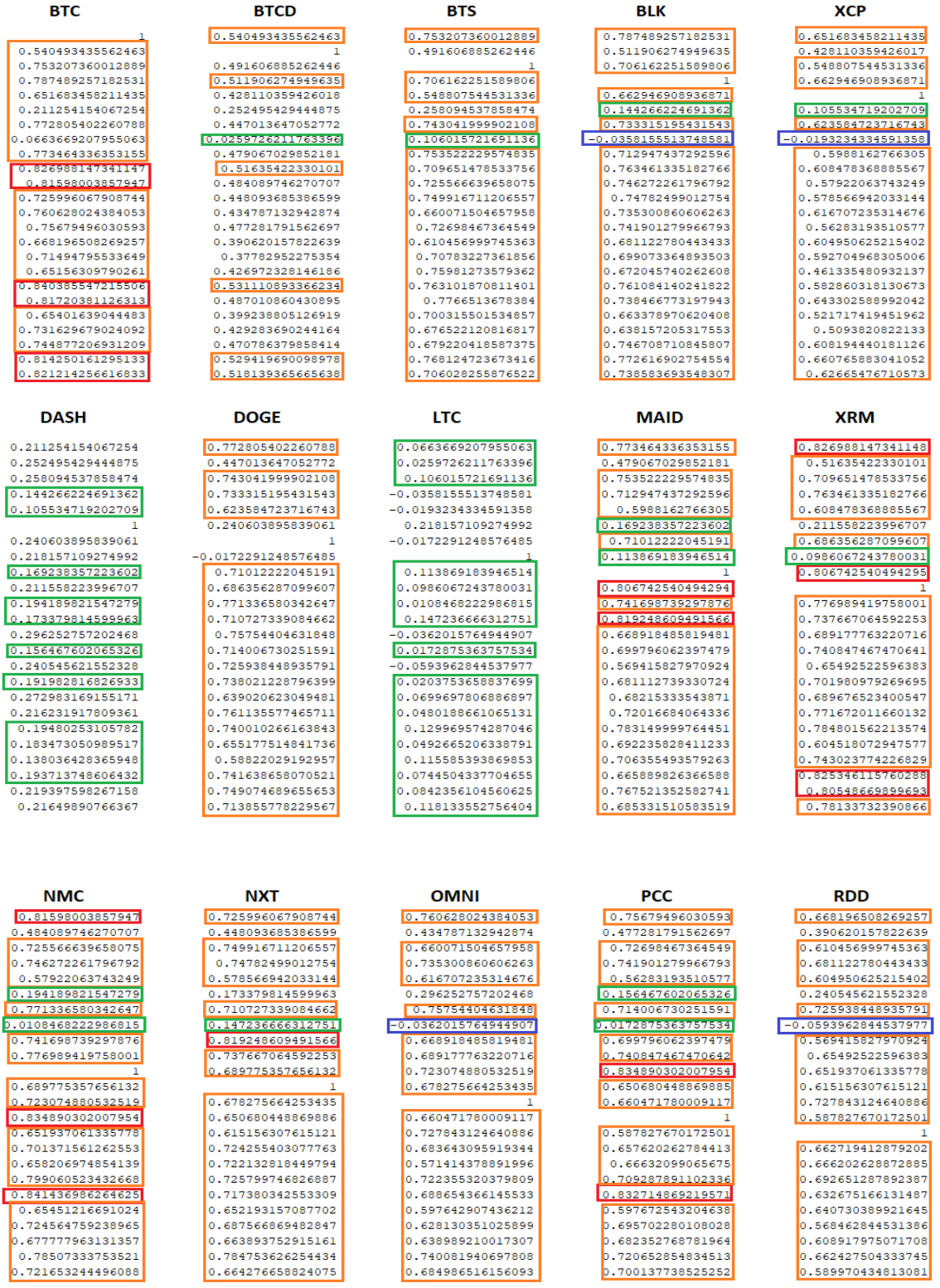
Il periodo in questione è quello che ha registrato l'andamento più negativo del mercato crypto di sempre. Solo una criptovaluta (NEO) tra quelle considerate è riuscita ad ottenere un rendimento positivo. Come sottolineato dal grafico seguente la maggior parte dei portafogli della frontiera ottenuti alla Markowitz hanno ottenuto un rendimento negativo.

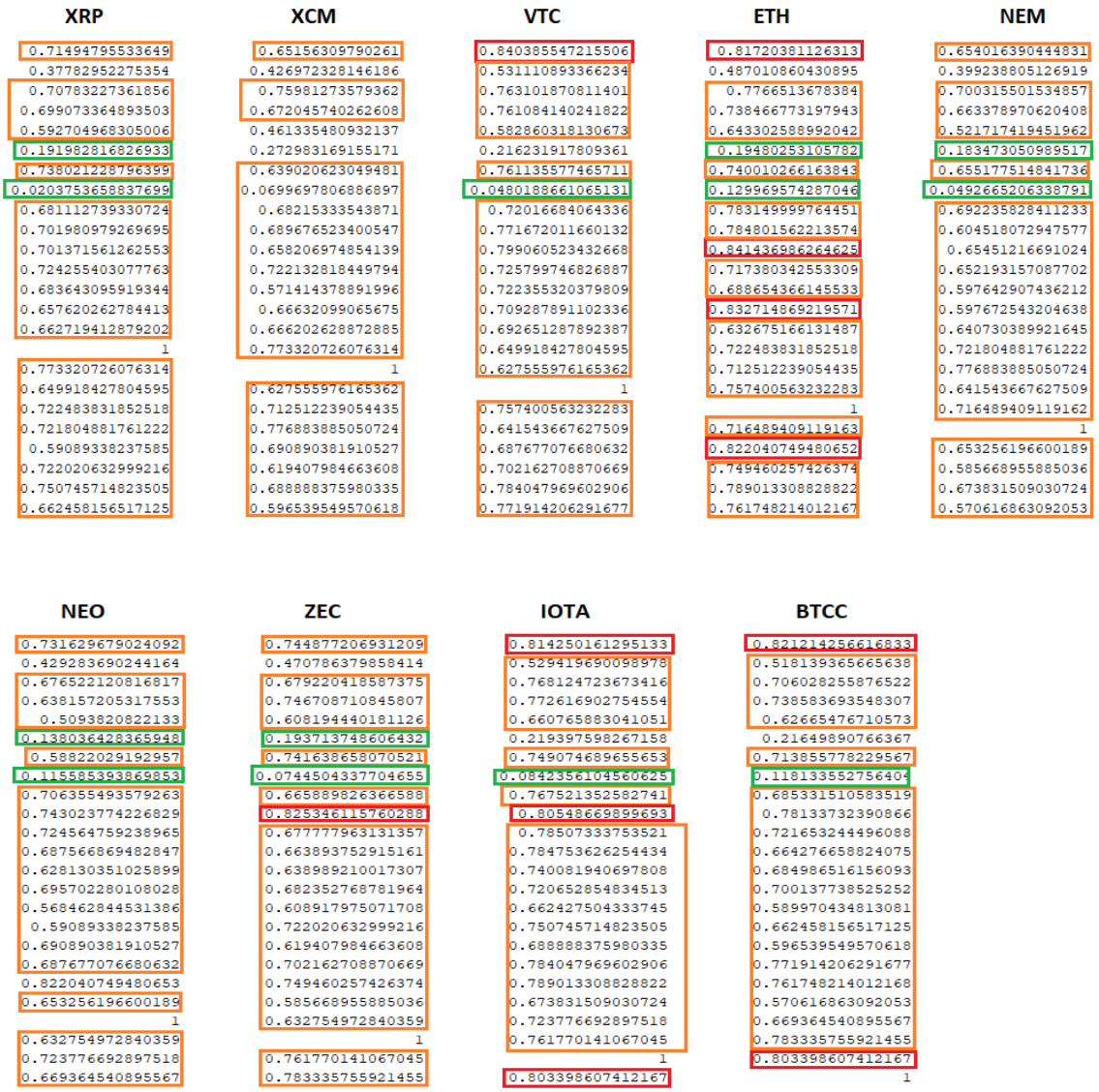
GRAFICO 3.16



Nella figura 3.10 sottostante sono riportate le correlazioni dei rendimenti delle 24 criptovalute considerate.

FIGURA 3.10





In un periodo di così forte decrescita del mercato delle criptovalute si è potuto osservare come la correlazione dei rendimenti del mercato in un momento “Orso” sia fortemente positiva. Quasi tutti i rendimenti delle criptovalute sono caratterizzati da una forte correlazione (o rossa o arancione quindi almeno superiore al 50%). Sono registrate alcune correlazioni negative tra criptovalute di seconda fascia come OMNI, ReddCoin, CounterParty e BlackCoin.

Il portafoglio 10 è stato tarato per ottenere un rendimento del 100% annuo. Visto il periodo fortemente negativo si nota come l’approccio alla Markowitz selezioni molte più criptovalute rispetto ai portafogli precedenti.

PORTAFOGLIO 10

BITCOIN	2%
BITSHARES	5,5%
BLACKCOIN	3,5%
COUNTERPARTY	4,2%
DASH	4%
DOGECOIN	5,8%
LITECOIN	2%
MAIDSAVECOIN	2%
MONERO	2%
NAMECOIN	5%
NXT	2%
OMNI	3%
REDDCOIN	8%
RIPPLE	3%
VERTCOIN	4%
ETHEREUM	30%
NEM	4%
ZCASH	4%
IOTA	4%
BITCOINCASH	2%

3.5 ANDAMENTO DEI PORTAFOGLI SELEZIONATI

Dopo aver selezionato i portafogli quadrimestre per quadrimestre, viene ora verificato quali siano state le loro performance nel periodo successivo a quello selezionato, supponendo prima un investimento di quattro mesi, e poi un investimento dal momento della selezione fino all'ultimo giorno di analisi il 30 aprile 2018.

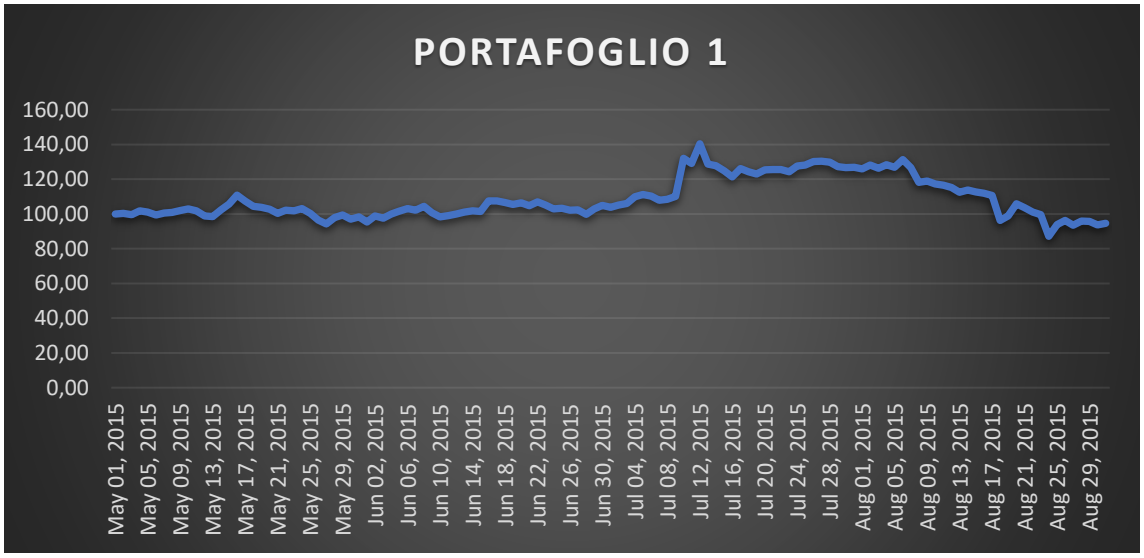
PORTAFOGLIO 1

Il portafoglio 1, selezionato nel periodo 1 gennaio 30 aprile 2015 viene analizzato nel periodo 1 maggio 31 agosto 2015. Il portafoglio è formato da Bitcoin per il 14%, Dash 57%, Monero 27% e Stellar 2%.

Il grafico sottostante mostra l'andamento del portafoglio 1 nei primi quattro mesi di selezione.

Nell'analisi si è considerata la partenza da un valore iniziale di 100 ad inizio periodo. Tale investimento viene tenuto costante sia nei primi 4 mesi successivi alla selezione, sia fino alla fine dell'analisi il 30 aprile 2018.Per tale motivo saranno riportati due grafici per ogni portafoglio, relativi ai due periodi considerati.

GRAFICO 3.17



Alla fine del periodo considerato il rendimento del portafoglio è stato negativo, registrando una perdita del 5.35%[140] nei quattro mesi. L'obiettivo del 100% annuo non è stato raggiunto considerando il periodo in questione.

Un rendimento diverso è invece quello fatto registrare dal portafoglio se si considerasse una gestione passiva dello stesso fino al 30 aprile 2018, come viene mostrato dal grafico sottostante.

GRAFICO 3.18

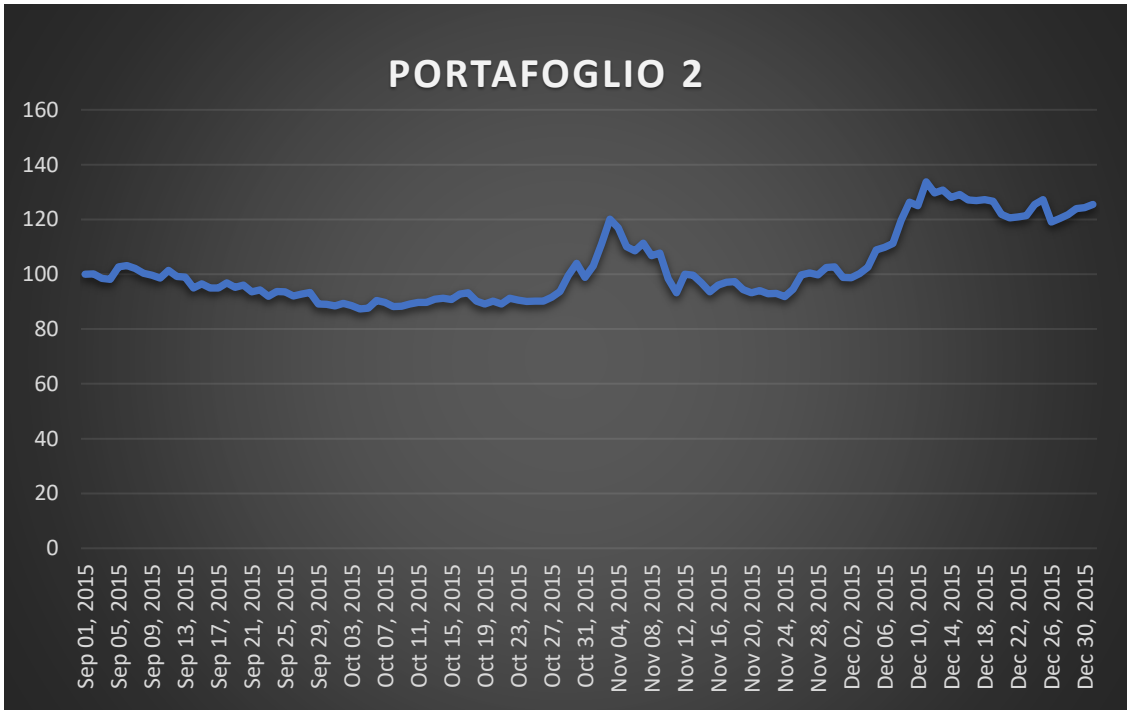
Il rendimento ottenuto in questo periodo sarebbe del 23806.66% nell'arco di 3 anni, quindi annualmente un rendimento superiore al 5000%

[140] Il Rendimento è stato considerato nel periodo, non trasformato in percentuale annua.

PORTAFOGLIO 2

Il portafoglio 2 è stato selezionato nel periodo 1 maggio 31 agosto 2015. L'analisi parte dal quadrimestre successivo all'1 settembre. Il portafoglio è formato come segue: Bitcoin 36%, BitcoinDark al 2,5%, Dash al 13%, Fuelcoin 2%, Litecoin 7%, MaidSaveCoin 5%, Omni 2%, Ripple 26% e Vertcoin 6,5%. Come nella situazione precedente il portafoglio è stato selezionato con l'obiettivo di garantire un rendimento del 100% annuale. Il grafico sottostante ne mostra l'andamento nei primi quattro mesi.

GRAFICO 3.19



Nel quadrimestre successivo alla sua selezione il portafoglio 2 ha garantito un rendimento di circa il 25%. Questo è in linea con l'obiettivo del portafoglio.

Nel grafico seguente è mostrato l'andamento del portafoglio 2 dal momento della selezione fino all'aprile 2018. Il portafoglio ha lo stesso andamento della capitalizzazione di mercato dell'intero settore crypto che si può osservare nel paragrafo 3.1.

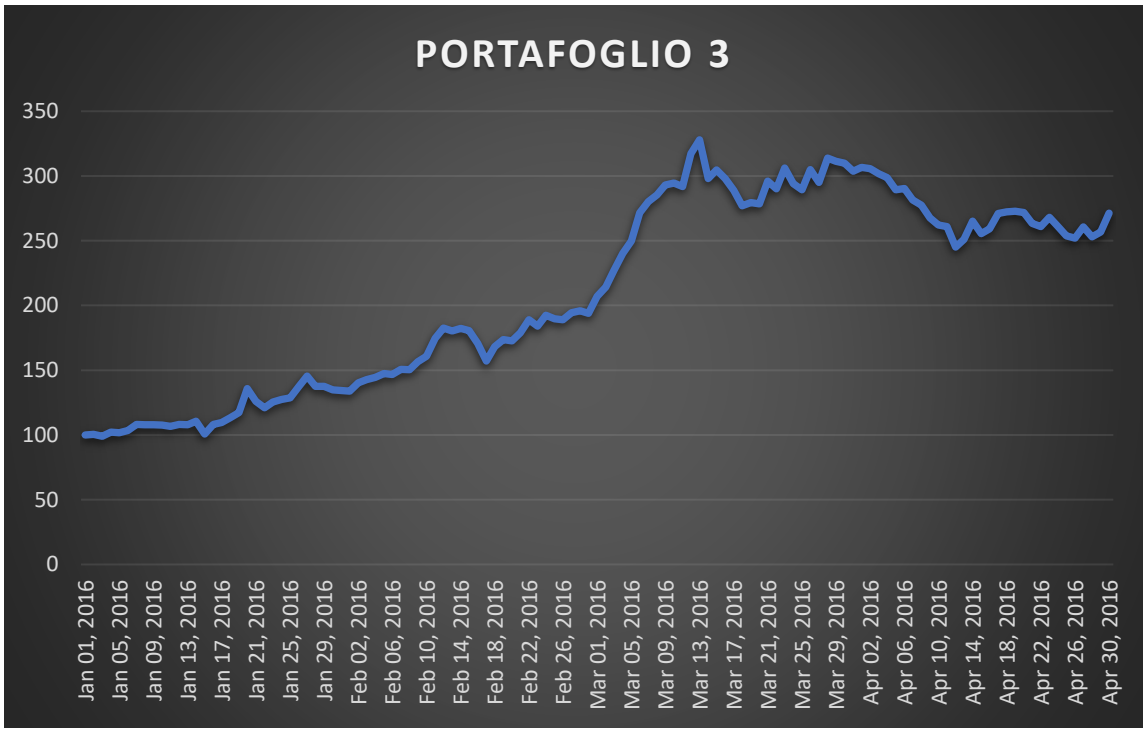
GRAFICO 3.20

Nel periodo tra l'1-settembre 2015 ed il 30-aprile 2018 il portafoglio 2 ha ottenuto un rendimento 7557.185%.

PORTAFOGLIO 3

Il portafoglio 3 è stato selezionato nel periodo 1-settembre 31-dicembre 2015. L'analisi sullo stesso parte dal quadrimestre successivo. Il portafoglio è formato per il 32% da Bitcoin, 5% Bitshares, 9% Dash, 6% Dogecoin, 6% Monero, 6% Nxt, 4% PayCoin, 6% Ripple, 8% Stellar, 10% Eth, 8% Nem. Il grafico seguente mostra l'andamento del portafoglio nei primi 4 mesi.

GRAFICO 3.21



Nel primo quadrimestre il portafoglio ha ottenuto un rendimento del 170%, corrispondente ad un 2700% annuo. Superando di molto l'obiettivo annuale del 100% già nel primo quadrimestre.

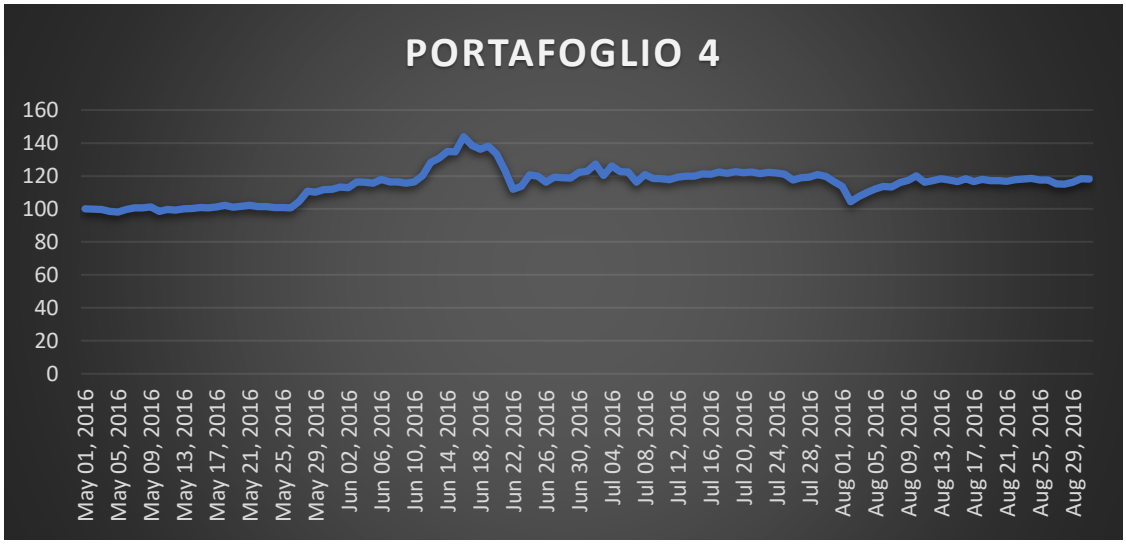
Nell'intero periodo dell'analisi, tra il 1-settembre 2015 ed il 30 aprile 2018, il portafoglio ha ottenuto invece un rendimento del 26743.45 %. Nel periodo di più alta quotazione di mercato il portafoglio era arrivato ad ottenere un rendimento del 122054.4%. La performance del titolo in questo intervallo è mostrata dal grafico sottostante.

GRAFICO 3.22

PORTAFOGLIO 4

Il portafoglio 4 è stato selezionato nel periodo 1-gennaio 30-aprile 2016, è formato per il 30% da Bitcoin, 3% da Bitshares, 6,5% Dash, 28,5% Litecoin, 2% Omni, 1% Reddcoin, 22% Ripple, 2% Stellar, 5% Eth. Il portafoglio nei primi 4 mesi ha garantito un rendimento del 18%, abbastanza in linea con l'obiettivo del 100% annuale. Il grafico sottostante mostra l'andamento del portafoglio nei primi 4 mesi.

GRAFICO 3.23



Nell'intero periodo il portafoglio ha avuto un rendimento inferiore rispetto ad altri, ma comunque ha garantito, come si può vedere dal grafico sottostante, una performance elevatissima del 6259.265% in 2 anni.

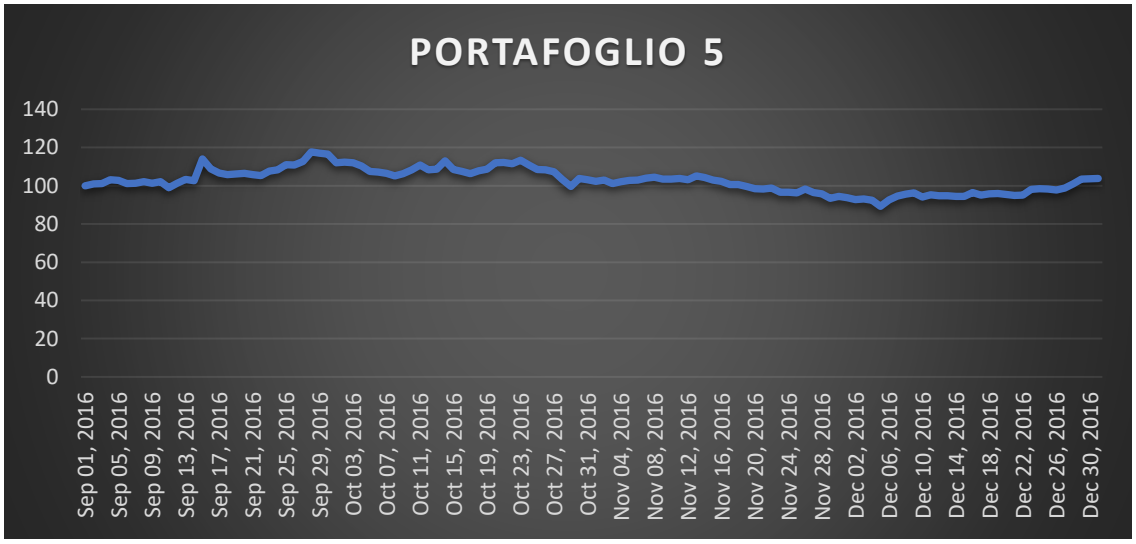
GRAFICO 3.24

PORTAFOGLIO 5

Il portafoglio 5 vede la selezione delle criptovalute tra il primo maggio 2016 ed il 31 agosto dello stesso anno. Il suo obiettivo, come per i portafogli precedenti, è quello di garantire un rendimento del 100% in un anno. Il portafoglio è formato dal 6% di Bitcoin, 21% Dash, 3% Dogecoin, 10% Litecoin, 4,5% Monero, 9% Peercoin, 32% Ripple, 2% Stellar, 8% Eth e 3% Nem.

Il grafico seguente mostra l'andamento del portafoglio nei primi quattro mesi.

GRAFICO 3.25



Il portafoglio in questione, non coadiuvato da un periodo di grande crescita del mercato, ha ottenuto nei primi quattro mesi un rendimento di solo il 4%, corrispondente ad un 12,5%. Un rendimento decisamente migliore è stato quello ottenuto nell'intero periodo di analisi fino al 30 aprile 2018 nel quale, come mostrato dal grafico seguente, il portafoglio ha avuto una performance del 7208.691%

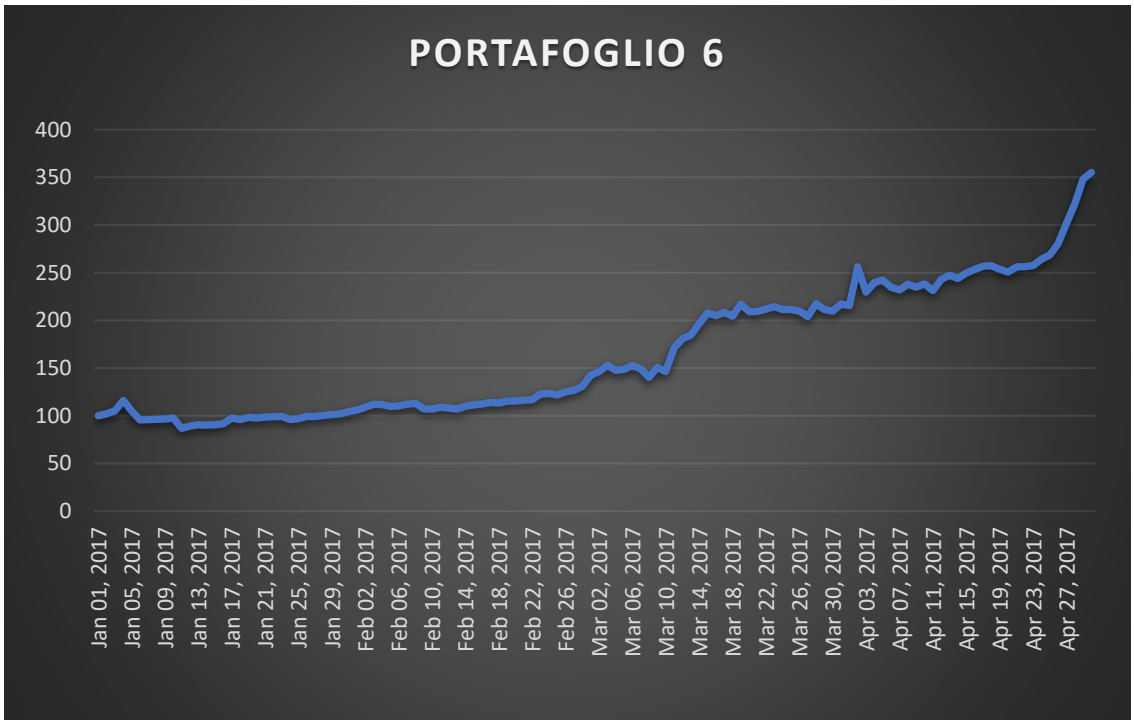
GRAFICO 3.26

PORTAFOGLIO 6

Il portafoglio 6 è stato selezionato nel periodo dal 1-settembre al 31-dicembre 2016 con l'obiettivo di garantire un rendimento del 100% annuale. Esso è formato da Bitcoin per il 47,5%, dal BitcoinDark per 1,5%, Dash per il 10%, Dogecoin 22%, FuelCoin 1%, Monero 3%, Ripple 6%, Vertcoin 3%, Eth 4% e Nem 2%.

Nei primi quattro mesi, come si può vedere dal grafico sottostante, ha ottenuto un rendimento del 250%, più che raddoppiando il rendimento obiettivo annuale.

GRAFICO 3.27



Nell'intero periodo la performance del portafoglio, per quando importante, è risultata più bassa di quella dei portafogli precedenti (2944.3%).

Il grafico seguente mostra l'andamento del portafoglio fino al 30 aprile 2018.

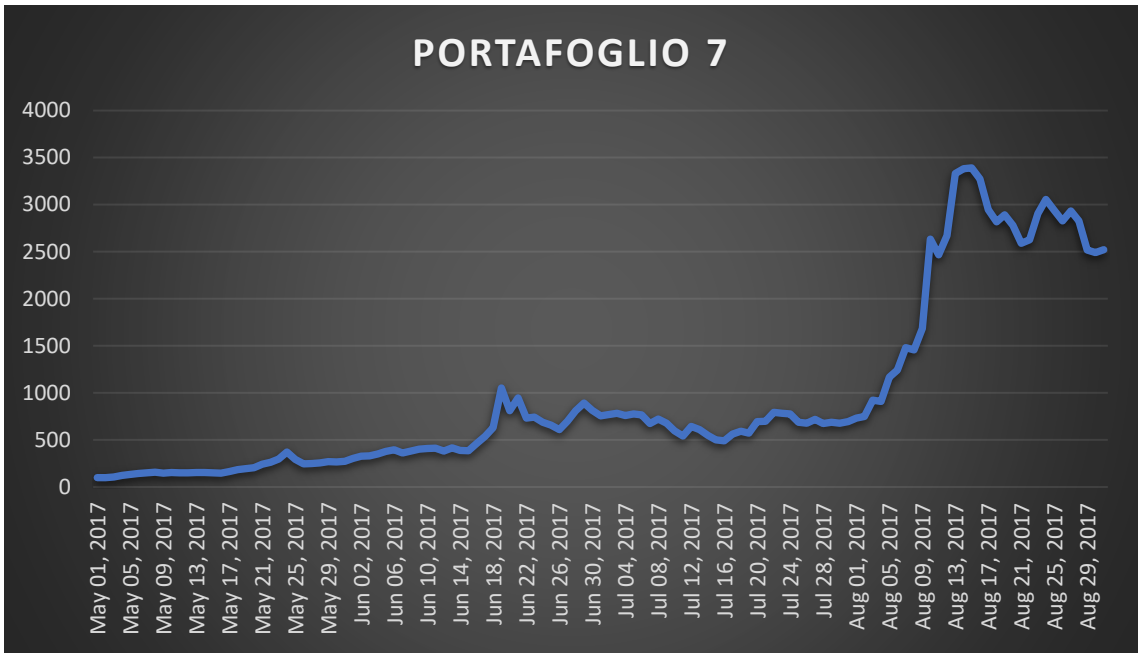
GRAFICO 3.28

PORTAFOGLIO 7

Il portafoglio 7, selezionato nel periodo dal primo gennaio al 30 aprile 2017, vede il Bitcoin come valuta principale con il 35% del capitale del portafoglio, Dogecoin il con10%, Litecoin 8%, Nxt 4%, Reddcoin 1,5%, Ripple 1,4%, Vertcoin 2%, Eth 7%, Nem 7%, 21% NEO, Z-cash 3,1%.

Nei quattro mesi iniziali, come mostrato dal grafico sottostante, ha avuto una performance incredibile del 2200%.

GRAFICO 3.29



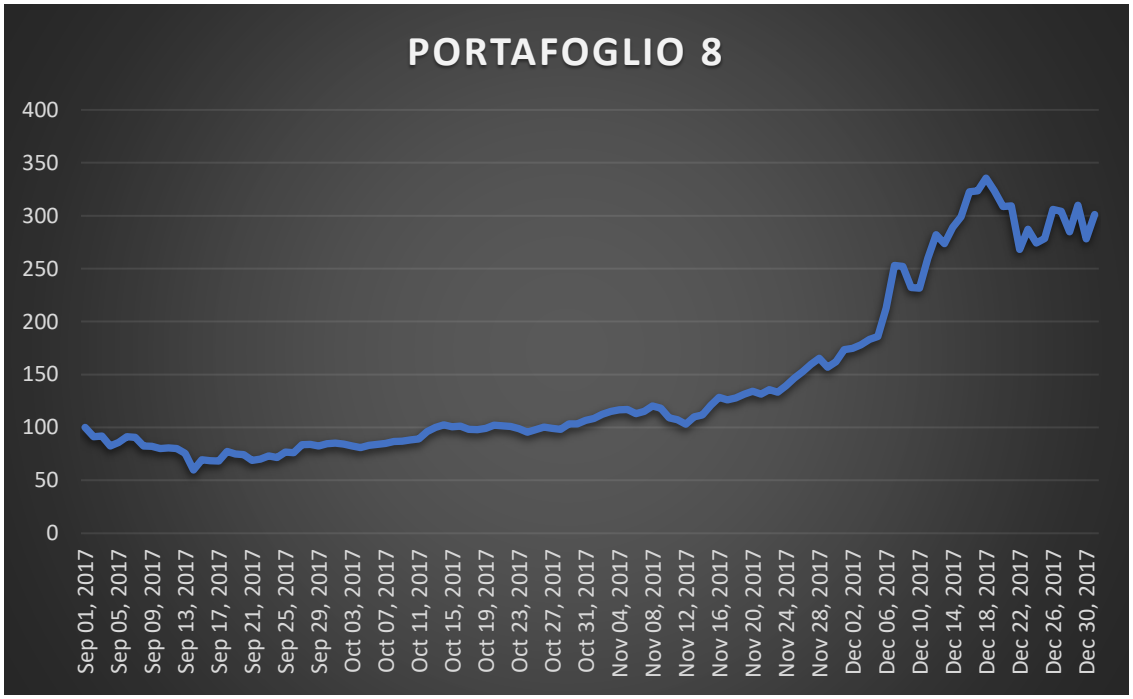
Nell'intero periodo, come si può vedere dal grafico sottostante, il rendimento è stato del 6297.391%.

GRAFICO 3.30

PORTAFOGLIO 8

Il portafoglio in questione è stato selezionato tra il 1-maggio e 31-agosto 2017. La presenza più importante è quella del Bitcoin con il 58% del capitale, 3,5% in Dash, 3% Litecoin, 5,5% Ripple, 7% Eth, 9% Nem e 14% Z-Cash. Il portafoglio, come si vede dal grafico seguente, ha garantito un rendimento del 200% nel primo quadrimestre.

GRAFICO 3.31



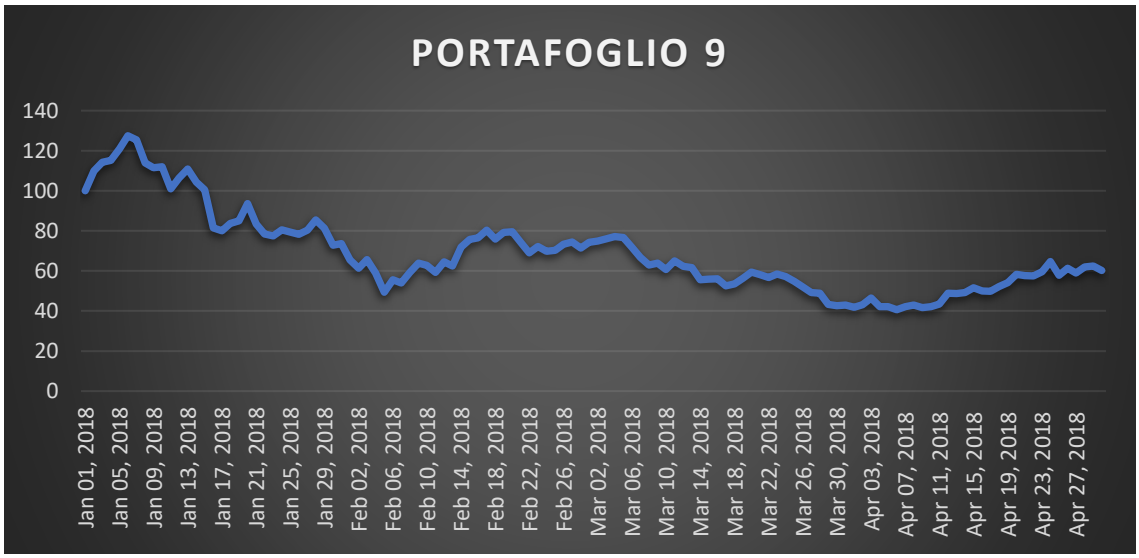
Nel periodo completo fino al 30 aprile 2018 il portafoglio ha ottenuto un rendimento del 70% annuo, cioè perdendo gran parte del valore acquisito nel periodo precedente a causa della caduta improvvisa del mercato crypto nel periodo da gennaio ad aprile 2018. Il grafico sottostante mostra il portafoglio fino al 30 aprile 2018.

GRAFICO 3.32

PORTAFOGLIO 9

Il portafoglio 9 vede la selezione dell'ultimo portafoglio con i dati del 2017. A causa della discesa del mercato nel 2018, esso ha ottenuto un rendimento profondamente negativo che ha portato ad una perdita nei quattro mesi del 40% del valore del portafoglio.

GRAFICO 3.33



APPENDICE A

SCRIPT

```
format long g

step0 = 1/2000;   → Step di 1/2000

% prezzi = dlmread('File.txt');
prezzi = xlsread('File.xlsx');

[rig,col] = size(prezzi);
rend = log(prezzi(2:end,:)./prezzi(1:end-1,:)); % rendimenti
logaritmici
[rig,col] = size(rend); % rig: numero di rendimenti; col: numero
di titoli
rig0 = rig;

r = mean(rend); % vettore dei rendimenti probabilistici;
v = cov(rend); % matrice di covarianza probabilistica;

%pg0 = min(r);
%pg1 = max(r);
 pg0= 0.01 → Rendimento richiesto
 pg1=pg0
    pg = pg0; % inizializzazione del contatore per il grafico
    while pg <= pg1;

        H = v; % per la funzione obiettivo
        A = zeros(col,col); % per il sistema dei vincoli
        b = zeros(col,1); % per il sistema dei vincoli
        e = ones(col,1);
        Aeq = [r;e']; % per il sistema dei vincoli
        beq = [pg;1]; % per il sistema dei vincoli
        lb = zeros(col,1); % per il sistema dei vincoli

        x = quadprog(H,[],[],[],Aeq,beq,lb,[],[]); %calcolo del
portafoglio

rp = r*x; % rendimento atteso del portafoglio
vp = x'*v*x; % varianza del rendimento del portafogli
sdp = sqrt(vp); % deviazione standard del rendimento del
portafoglio
        if pg == pg0
            xport_pro = x;
            rplot_pro = rp;
            vplot_pro = vp;
        else
            xport_pro = horzcat(xport_pro, x);
            rplot_pro = horzcat(rplot_pro, rp);
            vplot_pro = horzcat(vplot_pro, vp);
```

```
        end
        pg = pg + step0;
    end

    figure;
    plot(vplot_pro,rplot_pro)
    min(vplot_pro)
    for i=1:22  → Numero di criptovalute considerate nel
portafoglio
        v(i,i)
 end
```

CAPITOLO 4

CONCLUSIONI

L'obiettivo di questa tesi è stato quello di verificare le possibilità di investimento in un mercato complesso, poco maturo ed in continua evoluzione come quello delle criptovalute. L'analisi del mercato e degli "asset" che lo compongono è avvenuta osservando due linee guida. La prima è stata quella di individuare da un punto di vista teorico le caratteristiche rilevanti e quelle distintive delle criptovalute. Ciò è stato perseguito tramite lo studio delle differenze tra le criptovalute più importanti e la catalogazione delle stesse. Un'attenzione particolare è stata riservata sia alla funzionalità presente delle varie criptovalute, sia per quanto riguarda i possibili sviluppi futuri. La funzionalità ha avuto come oggetto di studio le caratteristiche intrinseche delle varie criptovalute e gli obiettivi generali inseriti nei "White Paper"[141] al momento della prima fase di emissione e di lancio dei vari progetti crypto. Per quanto riguarda invece gli sviluppi futuri si è fatto riferimento in particolare alle collaborazioni fatte registrate tra gli sviluppatori della criptovalute (o in taluni casi le società sviluppatrici della blockchain o della criptovaluta) e importanti intermediari finanziarie e società operanti

[141] Come già detto i "White Paper" sono i rapporti iniziali con i quali vengono promosse le criptovalute di nuova emissione.

in questo settore. In quest'ottica è stata data notevole importanza alle possibilità di sviluppo interno della criptovalute ed alle funzionalità ed organizzazione del Network[142]; La seconda linea guida seguita è stata quella di verificare, attraverso l'ausilio dei numeri, la percezione del mercato relativamente alle varie criptovalute. Per questo motivo è stata studiata la correlazione dei rendimenti, effettuando la selezione di alcuni portafogli secondo il criterio media-varianza. La selezione dei portafogli ha avuto luogo a partire dal 1 gennaio 2015 al 30 aprile 2018 con cadenza quadrimestrale, per un totale di 10 periodi considerati.

Il mercato delle criptovalute, come era lecito aspettarsi, si è rivelato fortemente correlato, in particolar modo nei momenti nei quali si è di fronte ad un trend ribassista. La correlazione molto positiva (a volte superiore all'80%) in questi periodi impedisce di raggiungere un livello di diversificazione sufficiente, il mercato infatti segue tendenzialmente in maniera compatta lo stesso andamento. Questa caratteristica rende in un certo senso poco sensata la selezione di un portafoglio secondo il criterio media-varianza puro, senza imporre delle limitazioni o delle preclusioni iniziali. È evidente che le correlazioni variano di periodo in periodo in maniera molto veloce, per tale motivo la selezione delle criptovalute non può basarsi solo sui risultati numerici, ma deve essere coadiuvata da osservazioni che possano essere valide in un periodo più lungo di tempo. A supportare i risultati numerici, da questo punto di vista, vi è una considerazione tangibile che va messa in evidenza: il mercato delle criptovalute è per molti aspetti atipico e non convenzionale. L'atipicità e la non convenzionalità in primo luogo sono legate al fatto che il mercato oggetto di studio non sia del tutto regolato. Per supportare questa affermazione basti solo pensare alla definizione stessa di criptovaluta. Già in fase

[142] Solo per fare un esempio; una criptovalute come Dash ha un'organizzazione interna tale che lo sviluppo della Blockchain e delle funzionalità della criptovaluta possa risultare molto più facile rispetto ad altre crypto. Come spiegato nel secondo capitolo il sistema di "remunerazione" per gli sviluppatori "Poof-Of-Service" garantisce infatti per questi ultimi un guadagno sicuro a corrispettivo del proprio operato. Questo incentiva i migliori sviluppatori a lavorare per la piattaforma e garantisce a quest'ultima la possibilità di progredire con poche difficoltà. Un sistema di questo tipo permetterà anche nel futuro di garantire a Dash uno sviluppo interno continuo, che possa permettere al sistema di pagamento e alla criptovaluta di rimanere sempre al passo con i tempi e con le eventuali innovazioni tecnologiche del mondo crypto.

di definizione la regolamentazione attuale non permette di delineare cosa sia o meno una criptovaluta: alcuni ritengono che le criptovalute siano "moneta", un semplice mezzo di scambio tra soggetti operanti nel web; altri invece le identificano come strumenti finanziari ibridi. Senza dubbio le criptovalute non sono azioni, perché non garantiscono al possessore alcun diritto di proprietà sulla società sviluppatrice delle stesse, e non sono nemmeno obbligazioni, non è infatti garantita la restituzione del capitale investito. Allo stesso tempo però le criptovalute vengono utilizzate da alcune società come strumenti attraverso i quali finanziarsi e svilupparsi (per il tramite delle ICO). La confusione regolamentare non permette di considerare "non vera" nessuna delle ipotesi elencate in precedenza. Questa incertezza ha creato in diversi momenti tensioni, che si sono concretamente riversate sull'andamento dei prezzi delle criptovalute ed hanno notevolmente influenzato la loro variabilità. La difficoltà di definizione e la carenza normativa non è questione di lana caprina, essa infatti ha un'importante ripercussione fiscale, basti pensare alle tasse sulle plusvalenze che dovrebbero essere pagate nel caso in cui una criptovaluta fosse considerata un investimento finanziario. In aggiunta va ricordato che se le criptovalute fossero investimenti finanziari per esse dovrebbe essere garantita anche una notevole informativa ed una più ampia trasparenza, che in questo momento non viene per niente assicurata[143].

Oltre alle considerazioni di carattere fiscale, va tenuto conto del fatto che il mercato delle criptovalute e delle "Blockchain" in generale, è molto giovane. Come mostrato nella parte iniziale del capitolo 3, il mercato non solo è giovane ma è stato fino a poco tempo fa "dominato" in termini di capitalizzazione di mercato da un solo "asset": il Bitcoin. Fino ad inizio 2015 in sostanza il mercato delle criptovalute non poteva essere considerato del tutto tale. Nell'ultimo periodo, come già spiegato, il settore si sta amalgamando, vedendo la crescita in termini di incisività (dominance[144]) nel rapporto

[143] Una normativa in questo senso andrebbe concordata a livello non solo Europeo, ma mondiale. È possibile acquistare una criptovaluta tramite il web in qualsiasi parte del mondo.

[144] La "Dominance" di un asset-criptovaluta nel mercato è definita come il rapporto percentuale della capitalizzazione di mercato della criptovaluta stessa e la capitalizzazione di mercato totale del settore.

totale di capitalizzazione di mercato di molte differenti criptomonete. Questa "spartizione" della capitalizzazione di mercato del settore in più soggetti è senza dubbio un segnale di "sviluppo" e di "crescita" del settore stesso. Purtuttavia, nonostante i notevoli passi avanti, si può senza dubbio affermare che questa fase di sviluppo non sia ancora del tutto completata.

Ad aggiungersi a queste problematiche va anche considerata la forte incidenza che gli exchange hanno sul prezzo delle crypto, che si sostanzia nella richiesta di forti corrispettivi per le commissioni. Questa elevata incidenza delle commissioni è conseguenza del rischio al quale sono esposti gli operatori che si offrono di intermediare negli scambi tra monete fiat e criptovalute. Un mercato così volatile e così poco regolamentato costringe infatti gli intermediari a tutelarsi e a richiedere un guadagno proporzionale al rischio assunto per il servizio svolto. La situazione appena delineata è sintomo di una non totale liquidità del mercato. Oltre a ciò va fatto presente che il numero degli exchange, pur essendo di gran lunga aumentato nell'ultimo periodo, rimane comunque poco elevato. Il numero esiguo non favorisce la concorrenza, che se fosse più ferrea porterebbe senza dubbio ad una riduzione delle commissioni. Anche questi aspetti appena elencati rendono il mercato delle criptovalute atipico.

Ultima considerazione, ma sicuramente non la meno importante, è quella legata ai soggetti investitori in criptovalute. La maggior parte di coloro che investono in questo settore non sono unicamente spinti dalla ricerca del rendimento, questi soggetti infatti sono perlopiù affascinati dall'obiettivo che Satoshi Nakamoto aveva identificato nel White Paper con il quale presentò Bitcoin a fine 2008. I primi investitori nel mondo delle criptovalute sono i soggetti maggiormente legati all'idea di Nakamoto di istituire un sistema di pagamento che possa scavalcare l'operato di intermediari finanziari terzi nelle operazioni che avvengono nel web. Questi soggetti, anche se sono sicuramente in minoranza rispetto al totale degli investitori, sono coloro che detengono il maggior numero di criptovalute[145]. I primi investitori in Bitcoin infatti sono quelli che sono riusciti

[145] Basti pensare che i primi soggetti che comprarono i Bitcoin poterono farlo ad un prezzo di pochi centesimi di dollaro. Un soggetto che per esempio avesse voluto investire 100 dollari in Bitcoin avrebbe potuto acquistare 5000 Bitcoin. Oggi con la stessa cifra si possono acquistare circa 0,01BTC.

ad accumulare una quantità più importante di criptovaluta e molto spesso essi sono stati anche i primi a comprare le criptovalute che via via sono state sviluppate.
Tutti questi aspetti fanno desumere che il mercato delle criptovalute non possa essere considerato ancora del tutto efficiente, per tale motivo una selezione dei portafogli basata unicamente sul criterio media-varianza non risulta adatta alla costruzione di un portafoglio diversificato per i prossimi anni.

Per risolvere l'inefficienza di mercato ritengo che sia necessario investire in futuro con una logica che, per il momento, non è ancora supportata dai numeri. A mio avviso il mercato delle criptovalute va diviso in quattro categorie:

1) Bitcoin ed Altcoin;
2) Criptovalute innovative del tipo IOTA;
3) Criptovalute innovative del tipo Ripple;
4) Criptovalute piattaforma;

Un comportamento ragionevole potrebbe essere quello di comporre un portafoglio con almeno una criptovaluta per ognuna delle quattro categorie sopra elencate. Operando in questo modo si terrebbe conto di tutti i possibili sviluppi dell'attuale applicazione della tecnologia blockchain. Anche se non sono azioni, il prezzo delle criptovalute rispecchia senza dubbio la fiducia che i mercati e gli investitori riversano nella tecnologia sottostante.
Per tale motivo ritengo possa essere corretto procedere con la selezione di due criptovalute per ogni categoria sopra elencata. Questo modo di agire, almeno logicamente, rimane congruente con un obiettivo di diversificazione. Dopo avere individuato gli otto "asset" verrà costruito un portafoglio attraverso il criterio media-varianza.

La tabella 4.1 riassume gli asset presi in considerazione per quest'ultima analisi.

TABELLA 4.1

BITCOIN	---
DASH	Altcoin
ETHEREUM	Piattaforma
NEO	Piattaforma
IOTA	Criptovaluta innovativa che utilizza il Tangle.
NANO	Criptovaluta innovativa concorrente di IOTA. Utilizza il Tangle per la convalida delle transazioni.
RIPPLE	Criptovaluta innovativa. La società creatrice lavora con gli intermediari finanziari.
STELLAR	Criptovaluta innovativa. La società creatrice lavora con gli intermediari finanziari.

Le 8 criptovalute (2 per categoria) sono state selezionate perché vengono ritenute le più promettenti all'interno delle loro categorie di appartenenza. Bitcoin non può mancare nella selezione. Oltre ad essere la prima criptovaluta per capitalizzazione di mercato, la sua presenza è giustificata dal fatto che nei 10 portafogli formati nel capitolo 3 è l'unica criptomoneta sempre presente. L'Altcoin Dash è stata scelta per la sua struttura organizzativa. Come spiegato nel capitolo 2, Dash ha una struttura molto complessa, basata sul concetto di Poof-Of-Service. Un'organizzazione di questo genere è ritenuta, a mio avviso, la migliore per permettere alla criptomoneta di rimanere sempre efficiente e sviluppata nel tempo, con essa infatti viene garantito agli sviluppatori una retribuzione in "denaro" Dash, che li incentiva notevolmente, rispetto ad altre realtà, a partecipare

al network. La retribuzione per i servizi svolti e la "democrazia diretta" dei MasterNode, permettono a Dash di crescere e adattarsi ai cambiamenti in maniera rapida ed efficace. Ethereum è stato selezionato perché è la prima Piattaforma e la seconda criptovaluta per capitalizzazione di mercato. Dal momento in cui è stata inserite nell'analisi svolta nel terzo capitolo (a partire da settembre 2015) è risultata sempre presente nei portafogli selezionati. La scelta della piattaforma NEO invece è legata al fatto che in essa possano essere sviluppati Smart-Contract con linguaggi di programmazione utilizzati comunemente come ad esempio Java e Microsoft.net.

Per quanto concerne IOTA, la criptovaluta è stata ritenuta la più interessante per l'applicazione del "Tangle" che, come spiegato nel capitolo 2, consiste in uno sviluppo della tecnologia Blockchain. Tale tecnologia permette di superare ogni problema di scalabilità dei blocchi, poiché ogni unità di criptovaluta "costruisce" la sua personale "catena". Questa peculiarità rende, almeno in maniera teorica, le transazioni pressoché istantanee. NANO è stata scelta perché risulta essere l'unica alternativa con un'importante capitalizzazione di mercato a IOTA, dal punto di vista del funzionamento essa è sostanzialmente basata sulla stessa struttura di IOTA.

L'ultima categoria considerata è quella di Ripple e Stellar. Queste due criptovalute oltre ad occupare un'importante posizione per quanto riguarda la capitalizzazione di mercato (Ripple è la terza criptomoneta, mentre Stellar occupa la settima posizione), sono quelle che hanno ricevuto un maggior interesse dal mondo della finanza "tradizionale". Come si può osservare dai siti delle due crypto esse contano considerevoli collaborazioni con importanti banche ed in intermediari finanziari. L'applicazione della blockchain al mondo della finanza "tradizionale" è sicuramente lo sviluppo più sicuro e probabile, tra quelli possibili. In virtù di questa considerazione, per quanto concerne questi due asset, è lecito aspettarsi un comportamento degli investitori più legato a quello tradizionale. Gli investitori in Ripple e Stellar si allontanano dai soggetti individuati nel paragrafo precedente come principali detentori delle criptovalute, i soggetti cioè legati all'idea di Satoshi Nakamoto. Questo allontanamento è evidente, proprio per la struttura e la funzione delle due criptomonete. In questi asset, in misura maggiore rispetto ad altri, è

più probabile aspettarsi in futuro un'entrata in "gioco" della finanza tradizionale, con investimenti in essi da parte di banche ed in generale di intermediari finanziari.

UN PORTAFOGLIO PER IL FUTURO

Nell'analisi sotto riportata è stato deciso di utilizzare come riferimenti gli ultimi due periodi a disposizione; tra l'1 settembre ed il 31 dicembre 2017 e tra l'1 gennaio ad il 30 aprile 2018. La scelta di utilizzare questi intervalli temporali è dovuta principalmente a due ragioni: la prima è il fatto che va data più importanza alle ultime osservazioni di mercato rispetto a quelle passate; la seconda ragione invece è più pratica. In questi ultimi due periodi si sono verificate due situazioni estremamente differenti, nel primo periodo si è vissuto un momento di trend fortemente positivo del settore delle criptovalute, nel secondo al contrario una tendenza profondamente negativa. Questi due momenti sono stati rispettivamente quelli nel quale il mercato delle criptovalute ha avuto il suo andamento maggiormente positivo e negativo della propria storia. Per tali motivi è stato ritenuto interessante procedere allo studio di un portafoglio in questi periodi, perché in questa maniera è possibile "vaccinare" la selezione degli asset poiché sono stati considerati i due scenari più estremi che hanno colpito questo settore.
Per tali ragioni nelle pagine successive verrà proposto un portafoglio di criptovalute costruito per il tramite dell'analisi media-varianza in questi ultimi due periodi. Come nella fase precedente, si porrà come obiettivo quello di raggiungere un rendimento annuale circa uguale al 100%. Il portafoglio verrà costruito prima tenendo in considerazione i due periodi separatamente (due periodi da quattro mesi ciascuno), ed infine considerandoli tutti e due congiuntamente (un unico periodo da 8 mesi), in totale quindi verranno proposti tre distinti portafogli.

Il primo periodo considerato è quello che va dall'1 settembre 2017 al 31 dicembre 2017. In questo periodo, attraverso lo studio delle correlazioni dei rendimenti, sono stati ottenuti i risultati riportati in figura 4.1

FIGURA 4.1

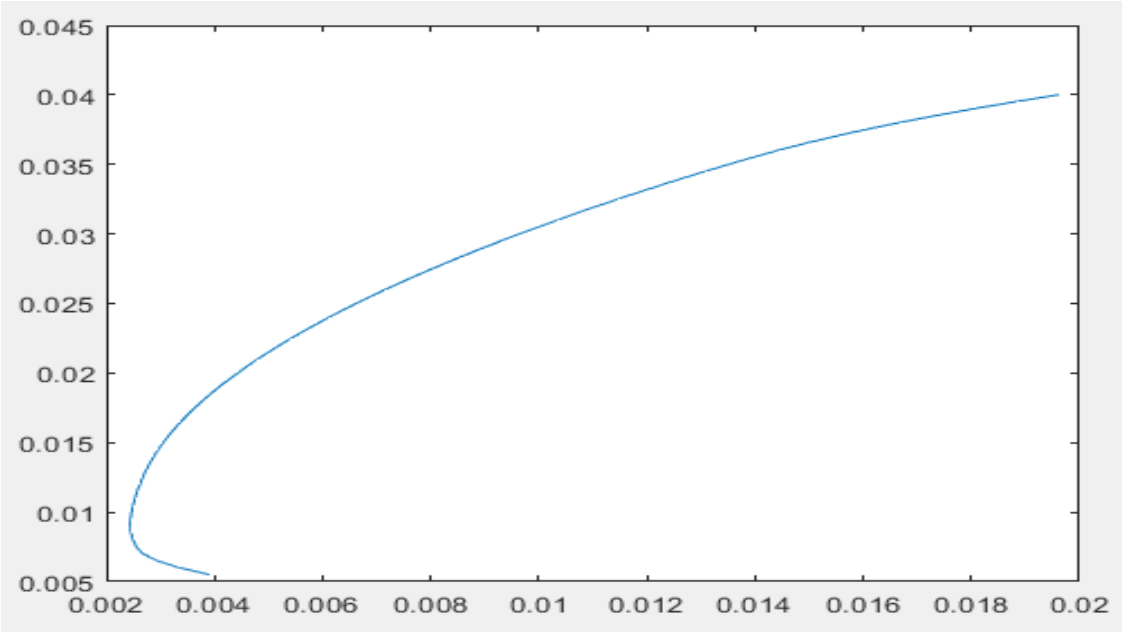
BITCOIN	DASH	ETHEREUM	NEO
1	0.208790345343447	0.459925788412754	0.274842884747831
0.208790345343447	1	0.513064438703795	0.353986031770256
0.459925788412754	0.513064438703795	1	0.569995275104596
0.274842884747831	0.353986031770256	0.569995275104596	1
0.353730208905481	0.300614445967017	0.499375376283956	0.32096162097752
0.298305714472415	0.154627206657175	0.395160964575679	0.192378854088751
0.12307353267756	0.177871814472162	0.447129498228471	0.315257718577932
0.33252908800882	0.174398656157416	0.42194792457843	0.415971906112475

IOTA	NANO	RIPPLE	STELLAR
0.353730208905481	0.298305714472415	0.12307353267756	0.33252908800882
0.300614445967017	0.154627206657175	0.177871814472162	0.174398656157416
0.499375376283956	0.395160964575679	0.447129498228471	0.42194792457843
0.32096162097752	0.192378854088751	0.315257718577932	0.415971906112475
1	0.35887975158328	0.195961877456046	0.492045978089365
0.35887975158328	1	0.43927118841149	0.27412037050081
0.195961877456046	0.43927118841149	1	0.383553754908182
0.492045978089365	0.27412037050081	0.383553754908182	1

Pur non essendo presente alcuna correlazione negativa, le correlazioni non sono risultate particolarmente importanti. Le uniche criptovalute i cui rendimenti hanno correlazione superiore al 50% sono Dash-Ethereum ed Ethereum-NEO. Tutte le altre criptovalute hanno fatto registrare correlazioni inferiori al 20%.

Nel grafico 4.1 è stata riportata la frontiera dei portafogli possibili nel periodo secondo Markowitz.

GRAFICO 4.1



Visti i rendimenti particolarmente alti fatti registrare in questo periodo, un rendimento obiettivo del 100% annuale non risulterebbe efficiente. Se si osserva il grafico 4.1 si può notare che un rendimento annuale del 100% (in termini di rendimento giornaliero circa uguale allo 0.0019, considerando che le criptovalute operano 365 giorni su 365) non è nemmeno presente nella frontiera. Per tale motivo ritengo che sia corretto imporre come rendimento obiettivo il rendimento presente nella frontiera che abbia la minor varianza. Questo valore è stato individuato come lo 0.95% giornaliero.

Il portafoglio così individuato è quello che segue:

PORTAFOGLIO 1

BITCOIN	51%
DASH	21%
ETHEREUM	11%
NANO	3%
RIPPLE	14%

Il secondo periodo considerato va dal 1° gennaio 2018 al 30 aprile 2018. Il trend fortemente ribassista del settore ha influenzato le correlazioni dei rendimenti, che hanno superato valori dell'80%, per esempio tra Bitcoin ed Ethereum o tra lo stesso Ethereum e Dash. Bitcoin ha registrato una forte correlazione dei rendimenti anche con IOTA. La criptovaluta che meno è risultata correlata con le altre è stata Dash, per la quale le correlazioni con i rendimenti delle altre crypto si sono assestate intorno al 20%.

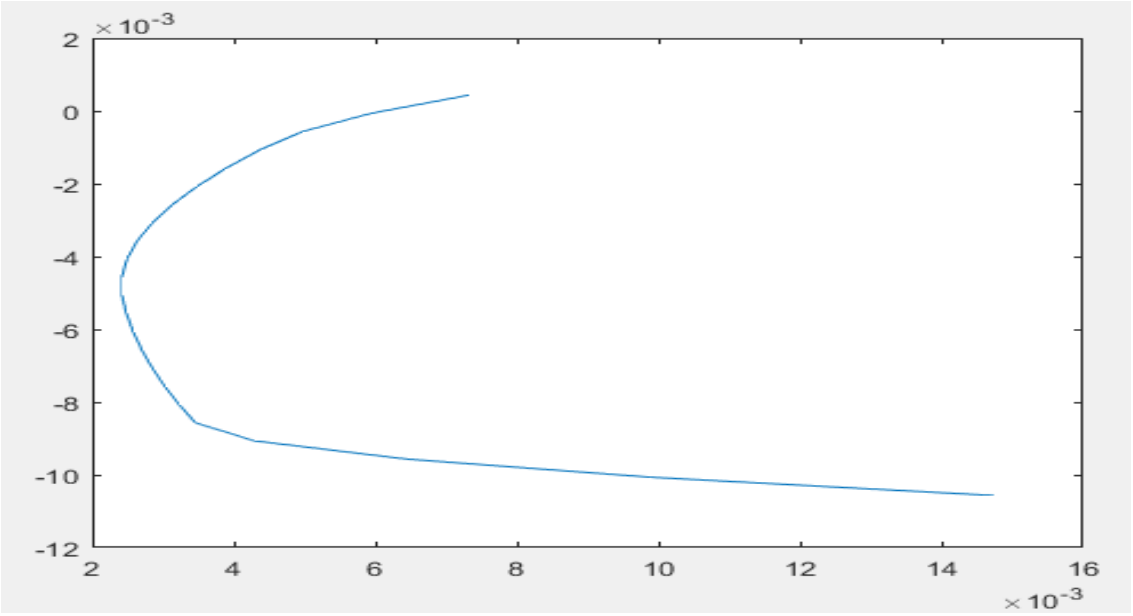
FIGURA 4.2

BITCOIN	DASH	ETHEREUM	NEO
1	0.211254154067254	0.81720381126313	0.731629679024092
0.211254154067254	1	0.19480253105782	0.138036428365948
0.81720381126313	0.19480253105782	1	0.822040749480652
0.731629679024092	0.138036428365948	0.822040749480652	1
0.814250161295134	0.219397598267158	0.789013308828822	0.723776692897518
0.62450356988361	0.0800045119836292	0.619191180009593	0.562963651960853
0.71494795533649	0.191982816826933	0.722483831852518	0.59089338237585
0.65156309790261	0.272983169155171	0.712512239054435	0.690890381910527

IOTA	NANO	RIPPLE	STELLAR
0.814250161295133	0.62450356988361	0.71494795533649	0.65156309790261
0.219397598267158	0.0800045119836292	0.191982816826933	0.272983169155171
0.789013308828822	0.619191180009593	0.722483831852518	0.712512239054435
0.723776692897518	0.562963651960853	0.59089338237585	0.690890381910527
1	0.617438259524514	0.750745714823505	0.688888375980335
0.617438259524514	1	0.433964578740003	0.361491777144204
0.750745714823505	0.433964578740003	1	0.773320726076314
0.688888375980335	0.361491777144204	0.773320726076314	1

Nel grafico sottostante è stata riportata la frontiera dei portafogli alla Markowitz. Il periodo è stato fortemente negativo, tant'è che sono NEO nell'arco dei 4 mesi è riuscita ad ottenere un buon rendimento. Tutte le altre criptovalute hanno registrato forti ridimensionamenti del valore.

GRAFICO 4.2



PORTAFOGLIO 2

NEO	100%

Per meglio percepire i due momenti del mercato ed ottenere un portafoglio meglio assortito ritengo sia corretto procedere con la selezione di un ultimo portafoglio considerando entrambi i periodi congiuntamente. Per tale motivo verrà effettuata una selezione tra il 1° settembre 2017 ed il 30 aprile 2018.

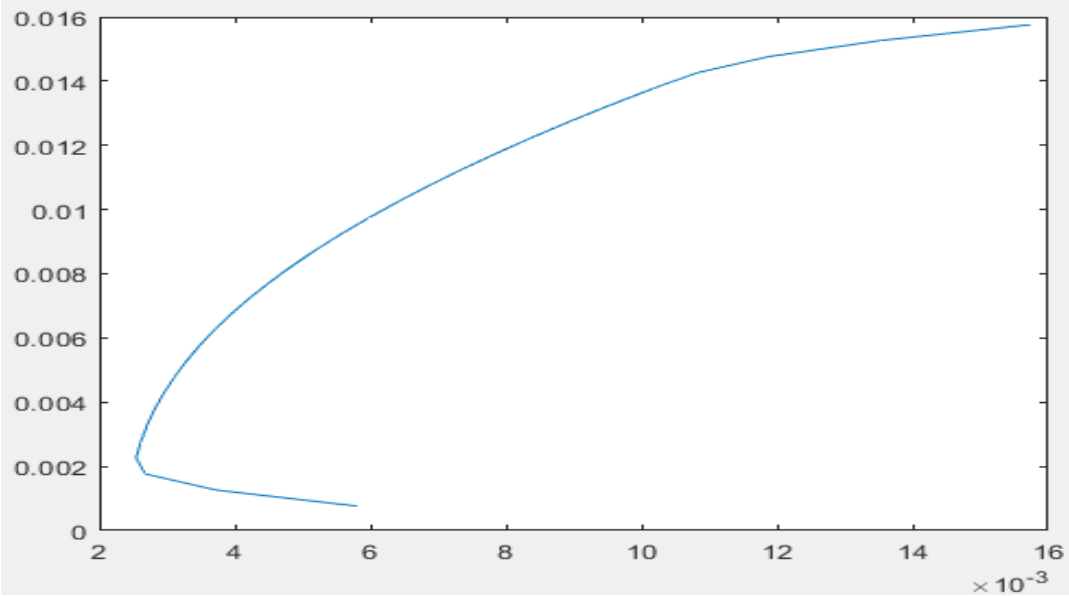
FIGURA 4.3

BITCOIN	DASH	ETHEREUM	NEO
1	0.211263532169896	0.636617260146539	0.476676981994769
0.211263532169896	1	0.361436346990708	0.26419279767934
0.636617260146539	0.361436346990708	1	0.68522993454597
0.476676981994769	0.26419279767934	0.68522993454597	1
0.525907953766193	0.280965945653614	0.606406762092922	0.466102558996005
0.44195323882956	0.154828063492844	0.49639948090158	0.347863143465664
0.391338625436865	0.197082235506686	0.573392713271822	0.430325741948736
0.449828843242584	0.234261503693786	0.534397080634417	0.515213073670778

IOTA	NANO	RIPPLE	STELLAR
0.525907953766193	0.44195323882956	0.391338625436865	0.449828843242584
0.280965945653614	0.154828063492844	0.197082235506686	0.234261503693786
0.606406762092922	0.49639948090158	0.573392713271822	0.534397080634417
0.466102558996005	0.347863143465664	0.430325741948736	0.515213073670778
1	0.462246937384901	0.402210579551459	0.562636426063766
0.462246937384901	1	0.449970595959129	0.332716374777148
0.402210579551459	0.449970595959129	1	0.530777298001641
0.562636426063766	0.332716374777148	0.530777298001641	1

Nel grafico 4.3 è riportata la frontiera dei portafogli possibili.

GRAFICO 4.3



PORTAFOGLIO 3

BITCOIN	40%
DASH	15%
ETHEREUM	20%
NEO	15%
RIPPLE	10%

Il portafoglio ottenuto attraverso la selezione nell'arco degli ultimi due periodi di questa analisi, si caratterizza per la presenza importante di Bitcoin (con il 40% del capitale). Le altre categorie sono rappresentate per ¾. Infatti risulta presente oltre all'Altcoin Dash, per le criptovalute piattaforme Ethereum (con il 20%) e NEO (15%), e con il 10% la criptovaluta innovativa Ripple. È invece assente la categoria di criptovalute innovative di tipo IOTA. A mio avviso per implementare ulteriormente il portafoglio, sarebbe necessario imporre un quantitativo minimo di IOTA o di NANO al fine di avere una copertura totale dei possibili sviluppi della tecnologia "blockchain".

BLIOGRAFIA

Garrick Hilleman & Michel Rauchs. Global Cryptocurrency Banchmarking Study. University Of Cambridge Centre for alternative finance 2017.

Stefano Capaccioli. Criptovalute e bitcoin: un'analisi giuridica. Giuffrè, Milano 2015.

Stefano Tonelli. Dal Bitcoin all'oro, conoscere il denaro per capire la crisi. Youcanprint, 2014.

Stefano Tonelli. Dall'oro al Bitcoin. Youcanprint, 2017.

David Lee Cham. "Blind signatures for untraceable payments". 1983. URL: http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF (ultima data consultazione 5 maggio 2018).

J. Bohr, M. Bashir. "Who Uses Bitcoin? An exploration of the Bitcoin community". Institute of Electrical and Electronics Engineers Inc. Toronto 2014.

Wei Dai. "b-money, an anonymous, distributed electronic cash system", 1998. URL: http://www.weidai.com/bmoney.txt/ (ultima data consultazione 5 maggio 2018).

Satoshi Nakamoto. "Bitcoin: a peer-to-peer Electronic cash system". 2008.URL: https://bitcoin.org/bitcoin.pdf (ultima data consultazione 5 maggio 2018)

European Central Bank "Virtual currency schemes – a further analysis", ECB. 2015. URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (ultima data consultazione 10 maggio 2018).

SITOGRAFIA

https://www.ecb.europa.eu/home/html/index.en.html (data ultima consultazione 15 aprile 2018).

https://en.wikipedia.org/wiki/Blind_signature (data ultima consultazione 30 aprile 2018).

https://bitcoin.org/it/ (data ultima consultazione 30 aprile 2018).

https://www.federalreserve.gov/aboutthefed/federal-reserve-system.htm (data ultima consultazione 15 aprile 2018).

https://en.wikipedia.org/wiki/Bitcoin (data ultima consultazione 14 giugno 2018).

https://namecoin.org/ (data ultima consultazione 3 aprile 2018).

https://en.wikipedia.org/wiki/Namecoin (data ultima consultazione 30 aprile 2018).

https://en.wikipedia.org/wiki/Fork_(software_development) (data ultima consultazione 20 aprile 2018).

https://en.wikipedia.org/wiki/Cryptography (data ultima consultazione 4 aprile 2018).

https://en.wikipedia.org/wiki/David_Chaum (ultima data consultazione 5 aprile 2018).

https://blockchain.info/it/charts/median-confirmation-time?timespan=all (data ultima consultazione 30 aprile 2018).

https://www.forbes.com/sites/bernardmarr/2018/02/28/what-is-the-difference-between-bitcoin-and-ripple/#e51b23c66118 (Ultima data di consultazione 20 aprile 2018) (data ultima consultazione 30 aprile 2018).

https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/ (data ultima consultazione 30 aprile 2018).

https://blockchain.info/it/pools (ultima data consultazione 20 aprile 2018).

https://coinmarketcap.com/ (data ultima consultazione 15 giugno 2018).

https://blockchain.info/it/charts (data ultima consultazione 18 aprile 2018).

https://bitcoinity.org/ (data ultima consultazione 20 aprile 2018).

http://dogecoin.com (data ultima consultazione 30 aprile 2018).

https://iota.org/ (data ultima consultazione 2 giugno 2018).

https://ripple.com/ (data ultima consultazione 3 giugno 2018).

https://www.ethereum.org/ (data ultima consultazione 4 giugno 2018).

https://www.dash.org/ (data ultima consultazione 4 giugno 2018).

https://www.bitcoincash.org/ (data ultima consultazione 4 giugno 2018).

https://neo.org/ (data ultima consultazione 4 giugno 2018).

https://eos.io/ (data ultima consultazione 4 giugno 2018).

https://litecoin.com/it/ (data ultima consultazione 5 giugno 2018).

https://github.com/ (data ultima consultazione 5 aprile 2018).