UNIVERSITÀ CA'FOSCARI VENEZIA

Corso di Laurea Magistrale
in Economia e Finanza

Tesi di laurea Magistrale

Utilizzo di indicatori tecnici per il trading su Criptovalute

Relatore
Prof. Marco Corazza

Laureando: Mircea Jignea
Matricola: 850062

Anno Accademico 2020/2021

INDICE

INTRODUZIONE

Con il presente elaborato, si propone una analisi del funzionamento e delle innovazioni apportate dalla tecnologia Blockchain e da alcune criptovalute in ambito finanziario.
L'elaborato si sviluppa seguendo due linee guida: la prima è puramente descrittiva in cui vengono spiegati aspetti tecnici alla base del funzionamento della Blockchain e delle criptovalute. Evidenziandone in primis gli aspetti caratteristici, si proseguirà poi fornendo un excursus maggiormente approfondito degli strumenti tecnico-matematici che permettono l'efficace funzionamento di tale tecnologia, la Blockchain, quali tra questi la crittografia e gli algoritmi di Hash. Procedendo in questo modo si fornisce uno strumento informativo che permetta allo stesso tempo di consentire una comprensione che sia più ampia possibile di un argomento che, ad oggi, in letteratura economica e nella cronaca giornalistica, risulta tanto dibattuto quanto presentato in maniera frammentaria e talvolta poco esaustiva.

La seconda linea guida prende in esame due articoli scientifici, pubblicati uno nel 2020 e l'altro nel 2019, i quali affrontato due diversi approcci per quanto riguarda gli investimenti in criptovalute: il primo di questi prende in esame l'utilizzo di indicatori tecnici per fare trading mentre il secondo è incentrato sull'acquisto e l'accumulo di criptovalute in determinati periodi. Quello di Shaker, Klaus e Sapkota[1] cerca di capire se utilizzando l'analisi delle Medie Mobili su dieci criptovalute (Dash, Bytecoin, DigitalNote, Monero, CloakCoin, Aeon, Stealth, Ptime-Xi, NavCoin, Verge) si riesce ad essere profittevoli, prendendo in esame un arco temporale di tre anni.
Per quanto riguarda invece il secondo articolo, scritto da PlanB, creatore anonimo del modello "Stock to Flow"[2], si darà una spiegazione in merito alla relazione tra il concetto di scarsità che determina le materie naturali, come oro e

[1] "Profitability of technical trading rules among cryptocurrencies with privacy function". Finance Research Letters, 2020.
[2] Verrà ampiamente descritto nel capitolo 3.

argento, applicandola a Bitcoin per determinarne il prezzo in base ai vari *halving* che lo caratterizzano.

Gli ultimi capitoli della tesi descrivono in modo dettagliato cinque criptovalute (Ethereum, Litecoin, Dash, Ripple e Iota) delle quali verranno utilizzati i prezzi giornalieri dal 2016 al 2020 per rappresentare gli indicatori tecnici del trading quali Media Mobile, MACD e RSI. Si tenterà, inoltre, di spiegare in maniera semplicistica come comportarsi quando si hanno davanti questi indicatori.

Infine, l'ultimo capitolo, tratterà le conclusioni sia in ambito della tecnologia che sostiene la Blockchain e le criptovalute, sia in ambito dell'analisi tecnica in modo da poter capire i risultati dei due articoli e quelli ottenuti dai grafici creati.

CAPITOLO 1: CRIPTOVALUTE E BITCOIN

1. CHE COSA SONO LE CRIPTOVALUTE?

Le criptovalute costituiscono nel mondo finanziario un approccio innovativo per l'utilizzo di una rappresentazione digitale di valore come mezzo o strumento di scambio che si basa su di un'importante applicazione della crittografia.
Il termine è composto da due parole: "cripto" e "valuta". Si tratta quindi di uno mezzo di pagamento o di scambio visibile e utilizzabile solo se si è a conoscenza di un determinato codice informativo, quello che viene definito "chiave di accesso".

Ciò che caratterizza tale strumento o bene è il suo essere esclusivamente virtuale in quanto viene generata e scambiata solo per via telematica. Il Bitcoin (BTC), che è la principale criptovaluta al momento, non si può reperire in formato cartaceo o metallico.
A livello normativo[3] le criptovalute vengono definite come valuta virtuale che costituisce una rappresentazione digitale di valore e che può essere usata come mezzo di scambio o utilizzata come investimento. Le criptovalute possono infatti essere trasferite, conservate o negoziate elettronicamente.

Nello stesso modo in cui esistono dei "portafogli" per le monete a corso legale, così se ne possono trovare anche per le monete virtuali. In questo caso parleremo di *e-wallet* o di *wallet* digitale/elettronico.
Inoltre, le criptovalute possono essere scambiate per l'acquisto di servizi e beni tramite la modalità definita "*peer-to-peer*" cioè uno scambio che avviene in modo immediato senza che vi sia la necessità di un intermediario.

[3] La regolamentazione delle criptovalute trova spazio in Italia nella normativa sul contrasto al riciclaggio di denaro e specificamente nel D.Lgs. 90/2017 introdotto in attuazione della IV Direttiva Antiriciclaggio dell'Unione Europea (Direttiva UE 2015/859).

Una classificazione attualmente in uso prevede che la criptovaluta venga suddivisa in “chiusa”, “unidirezionale” o “bidirezionale”. La differenza tra le tre suddivisioni sta nella possibilità o meno di poterla scambiare con moneta a corso legale e nella tipologia di beni/servizi che possono essere acquistati con essa.

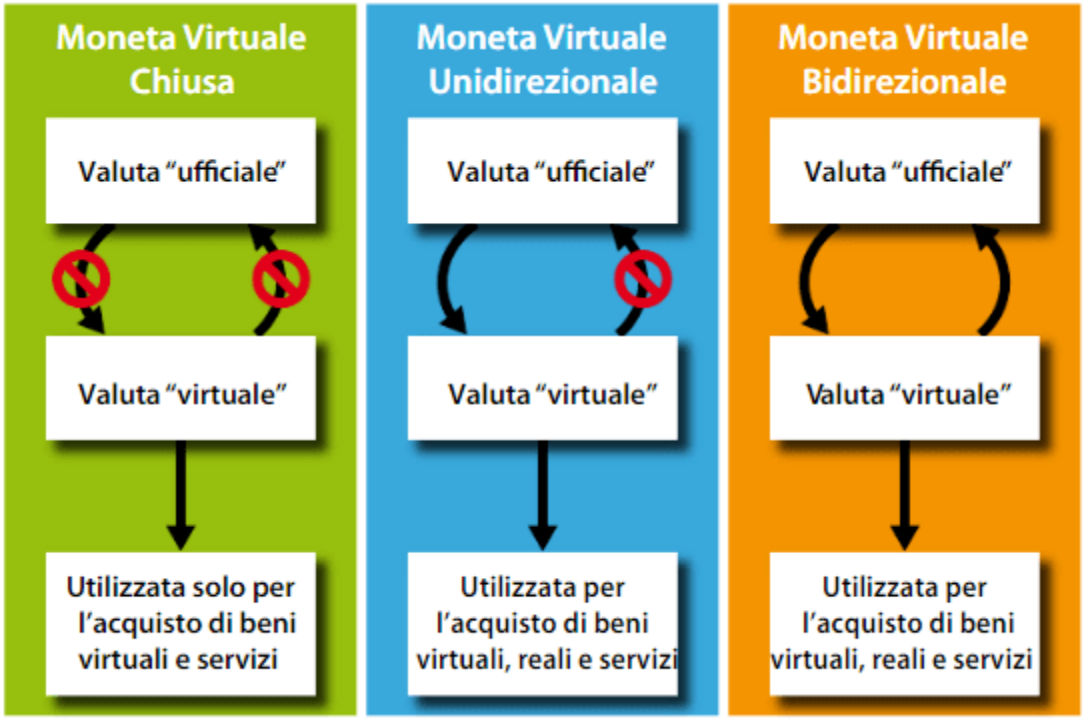

Fig.1. Differenza tra criptovaluta “chiusa”, “unidirezionale” e “bidirezionale”.

Fin da subito va sottolineato che una criptovaluta non ha corso legale in nessuno stato del pianeta e dunque la loro accettazione come modalità di pagamento è su base volontaria; inoltre non essendo regolate da enti centrali governativi, sono generalmente emesse e supervisionate dall’ente che le emette secondo regole proprie, a cui i membri della comunità di riferimento accettano di aderire.

Ci sono però degli stati, come ad esempio l’Uruguay con il suo e-peso, che hanno deciso di sperimentare, sotto il proprio controllo, l’uso della moneta virtuale. Altri stati invece ne hanno annunciato l’utilizzo senza però fornire ulteriori informazioni a riguardo, altri ancora hanno annunciato di stare preparando iniziative al riguardo, come ad esempio Venezuela con il Petro, o Estonia, Svezia e Russia.

Per capire bene in cosa le criptovalute si differenzino dalla moneta a corso legale, bisogna prima di tutto paragonare le une alle altre. Alle monete a corso legale vengono generalmente riconosciute le funzioni di "unità di conto", di "mezzo di pagamento", o ancora di "deposito di valore". La criptovaluta invece, data la sua elevata volatilità sui mercati finanziari, non permette un corretto svolgimento della funzione di "unità di conto": ogni giorno infatti il prezzo di ciascuna criptovaluta è soggetta a elevate variazioni e oscillazioni sui mercati e ciò porta ad una marcata variazione del loro valore. Per tale motivo risulta praticamente impossibile prezzare beni e servizi in unità di criptovalute.

Per quanto riguarda invece la funzione di "riserva di valore" bisogna considerare che, a causa della loro progettazione, più le criptovalute aumenteranno il loro valore più verranno utilizzate per il pagamento di beni e servizi.
La spiegazione di tale fenomeno la si può trovare nel fatto che c'è un limitato numero di unità[4] di criptovalute che possono essere prodotte e di conseguenza più aumentano le transizioni che sono regolate mediante criptovalute, più il valore di queste ultime aumenta.
Per finire, non possono essere considerate come un valore merce, cioè sono prive di funzione d'uso, come ad esempio l'oro. Potrebbero però in un futuro andare ad assolvere ad una funzione di scambio.
Se si fa una breve analisi dell'oro si può evidenziare come questo abbia le seguenti caratteristiche:

- È raro o comunque ne abbiamo una limitata quantità;
- È malleabile, quindi può essere fuso e suddiviso in unità più piccole;
- Il valore unitario non cambia quando si divide in pezzi più piccoli;
- È stabile e non degrada;
- È difficile da contraffare;

Bitcoin ha le stesse caratteristiche, anche se in versione digitale;

[4] La limitazione del numero di criptovalute create serve ad evitare problemi di inflazione; esse sono autoregolate dalla tecnologia stessa e quindi l'andamento del prezzo è dettato da regole di mercato, secondo il principio di domanda e offerta. Siccome il prezzo di mercato è il risultato dell'incontro tra domanda e offerta, niente ha valore intrinseco (interessi politici, macroeconomici).

- Disponibilità/offerta limitata;
- Suddivisibile in unità più piccole (un BTC è divisibile in cento milioni di unità, 1 BTC = 100.000.000 satoshi);
- Tecnologia e algoritmi che lo rendono stabile e impossibile da contraffare;
- A differenza dell'oro può essere trasferito in qualsiasi luogo in pochi minuti, senza avere vincoli di quantità;

Per questi motivi molti sostengono che oltre ad essere l'oro digitale dell'era moderna, Bitcoin è una più che valida alternativa all'oro che troviamo in natura. Bitcoin è un pagamento valido e la sua peculiarità è che tante più persone lo utilizzeranno per i pagamenti tanto più aumenterà il suo valore e sarà incentivo per lo sviluppo e la creazione di nuove tecnologie che faranno perno sulla Blockchain.

2. BITCOIN, LA PRINCIPALE CRIPTOVALUTA

Storicamente la "nascita" vera e propria del Bitcoin la si può far risalire al 2009, anno in cui venne presentata al mondo. L'inventore del Bitcoin viene chiamato Satoshi Nakamoto, nome di fantasia utilizzato per garantire l'anonimato alla persona (o alle persone) che l'ha creato. L'idea originaria di Nakamoto era quella di creare un nuovo sistema di valuta elettronico che potesse eliminare qualsiasi tipo di autorità centrale (conseguenza della crisi finanziaria del 2008, momento in cui le banche hanno perso molta credibilità). Tale scopo venne raggiunto in tempi relativamente brevi tant'è che nel 2010 Nakamoto sparì sfilandosi completamente dal sistema che egli stesso aveva creato.

Per aver chiaro cosa si intende quando si parla di Bitcoin, bisogna fare una premessa spiegando cosa si intende invece per valuta reale. Per valuta reale si intende la valuta che noi quotidianamente utilizziamo per l'acquisto di un qualsiasi bene o per qualsiasi transazione che preveda un intermediario; per intermediario si può prendere come esempio la BCE (Banca Centrale Europea) il cui compito è quello di emanare regole sulla politica monetaria, sulle operazioni

sui cambi, funzionamento dei sistemi di pagamento, stabilità finanziaria e vigilanza prudenziale.
Il valore che noi attribuiamo al denaro deriva però da una convenzione: una normale banconota, che sia da $1, $10, o da $100, rimane pur sempre un pezzo di carta e se è possibile utilizzarlo per ottenere in cambio beni più complessi è dovuto al fatto che vi è un accordo comune sul valore che viene riconosciuto e attribuito al quel pezzo di carta. Da notare però che una banconota da $100 non vale 10 volte di più di una da $10, ma per convenzione è stato deciso così e nel momento in cui si volesse cambiare tale valore di paragone, basterebbe decidere un nuovo valore convenzionale.

A differenza della valuta reale, i Bitcoin rappresentano una moneta in formato digitale che gli utenti possono conservare in appositi portafogli virtuali. I Bitcoin possono inoltre essere utilizzati, ad esempio, per pagamenti in negozi, per il trasferimento peer-to-peer tra i vari utenti, oppure si possono conservare nel tempo a scopo speculativo, nella speranza che in futuro il loro valore accresca e arrivino ad avere un valore maggiore a quello odierno.

Uno dei vantaggi che possono essere riconosciuti al Bitcoin è quello di poter risolvere una moltitudine di problemi che di norma si presentano nelle transazioni economiche online come ad esempio l'assenza di un'autorità centrale che vigila sul Bitcoin, l'assenza di società e organizzazioni che ne gestiscono i flussi e il relativo valore. Le valute reali invece richiedono la presenza di queste ultime per poter circolare da A a B, con le conseguenti commissioni a Visa, Mastercard o Western Union, e perciò hanno un maggior rischio di subire hackeraggi volti a sottrarre numeri e codici di carte di credito.

Ad oggi però il Bitcoin non è l'unica moneta virtuale presente, anzi chiunque potrebbe crearne una nuova. Nonostante tutto, il Bitcoin rimane la più forte, e siccome è la criptovaluta più conosciuta risulta essere anche la più sicura in circolazione.

Di seguito elenchiamo quelle che analizzeremo in base alla loro capitalizzazione sul mercato e in base al progetto tecnico che ci sta dietro:

- BTC: Bitcoin;
- ETH: Ethereum;
- LTC: Litecoin;
- XRP: Ripple;
- DASH: Dash;
- MIOTA: Iota;

2.1 COME FUNZIONANO LE TRANSAZIONI SU BITCOIN?

Come precedentemente detto, i Bitcoin funzionano sulla base di un protocollo peer-to-peer, somigliante ai sistemi che vengono utilizzati per scaricare e condividere file online, quei sistemi quindi in cui ogni computer diventa un nodo della rete alla pari con gli altri senza la presenza di un nodo centrale.
In questo modo ogni utente che utilizza Bitcoin viene collegato con tutti gli altri utenti e detiene una copia di una sorta di libro mastro, un documento cioè in cui sono contenuti tutti i conti di un sistema contabile, che viene chiamato *blockchain* (catena di blocchi) di cui parleremo più avanti. Nella blockchain si registrano tutte le transizioni effettuate da qualsiasi utente, da quando sono nati i Bitcoin.

Fig.2. Come funziona una transizione con il Bitcoin.

Il meccanismo della blockchain risolve il problema della verifica della regolarità delle transizioni economiche effettuale online. Così facendo si possono evitare gli interventi delle autorità centrali per il controllo dell'assenza di imbrogli da parte dei destinatari nei confronti dei mittenti, o che gli utenti non stiano pagando con soldi in realtà non in loro possesso. La blockchain, quindi, va ad assumere il ruolo di intermediario che potrebbe ad esempio ricoprire la banca: il compito è quello di rimuovere dal conto dell'utente che ha speso il denaro la quantità esatta di denaro e assicurarsi che non possa spendere più di quanto possiede realmente.

Durante questo processo qualunque utente ha la possibilità di controllare lo svolgimento di qualunque transizione. Nel momento in cui viene effettuata una transizione si aggiunge un nuovo "blocco" e tutti i dispositivi collegati al sistema Blockchain i quali devono acconsentire affinché questo venga confermato. Con l'aggiunta di un nuovo blocco, ogni nodo della catena aggiorna la propria copia, senza che ci sia più alcuna possibilità di modificare i dati una volta inseriti e validati. La transazione quindi viene inviata dal mittente, validata dalla Blockchain e ricevuta dal destinatario.

Si deve considerare che circa sei volte all'ora viene creato un nuovo "blocco" di transazioni che devono essere confermate, che si aggiunge poi alla blockchain generale. Una transazione con oggetto Bitcoin viene registrata in modo definitivo solo nel momento in cui è avvenuta realmente e tale ammontare viene "depositata" in un unico posto in cui si tiene il conto della quantità di Bitcoin esistenti e a chi appartengono. In tal modo si evita che i clienti spendano più volte gli stessi Bitcoin poiché i Bitcoin spesi sono stati registrati sulla blockchain in possesso di qualunque utente che faccia uso di tale metodo di pagamento. Così facendo risulta praticamente impossibile imbrogliare falsificando Bitcoin.

Tutte queste operazioni avvengono "all'oscuro" delle persone che stanno davanti al computer in quanto vengono generati input casuali dal protocollo e il programma effettua in modo del tutto autonomo il calcolo. I proprietari dei Bitcoin

mantengono l'anonimato in quanto la loro identificazione avviene esclusivamente mediante un codice.

Come detto sopra, si tratta di una valuta digitale visibile e utilizzabile solo se si è a conoscenza di un determinato codice, quello che viene definito "chiave di accesso".
Ci sono due tipologie di chiave, una "pubblica" e una "privata": la prima viene utilizzata per l'identificazione del ricevente e tutti i dispositivi se ne servono per controllare e verificare l'operazione, mentre la seconda viene utilizzata per l'autorizzazione della transazione da parte degli utenti che sono coinvolti direttamente.
Nel momento in cui viene persa la chiave privata, si perdono automaticamente e definitivamente i soldi. In tal modo risulta quindi impossibile falsificare Bitcoin, ma resta ancora aperto il problema riguardo la possibilità di rubare le monete virtuali, fatto già avvenuto in passato**.**

2.2 L'ESTRAZIONE

Vengono denominati *miners* coloro che si occupano di risolvere il problema crittografico (certificano le transazioni tramite la Proof of Work), cercando così di trovare quell'unico numero in grado di confermare la transazione per poi poterla aggiungere in modo sicuro alla blockchain. Chi per primo riesce a risolvere il problema invia la soluzione agli altri nodi della rete, che a quel punto ne possono dare conferma o meno e in caso di esito positivo ricevono una remunerazione in Bitcoin. Infatti, chi contribuisce attraverso l'uso dei suoi dispositivi ai calcoli necessari a confermare le varie transazioni, permettendo così alla valuta di rimanere attiva e sicura, riceve un compenso dal sistema Bitcoin attraverso la distribuzione di nuova criptovaluta.

Al momento della nascita di tale criptovaluta i computer che potevano essere utilizzati erano quelli di uso comune dato che la potenza richiesta per minare nuovi Bitcoin non era elevata. Ad oggi però, data la maggior importanza e i

maggiori volumi di criptovalute raggiunti da Bitcoin (la quantità massima totale dei Bitcoin è di 21 milioni di unità, presumibilmente raggiungibile non prima del 2030) ha fatto sì che il partecipare attivamente a operazioni di conferma delle transizioni richiedesse una grandissima potenza di calcolo, non più fornibile dai computer di uso comune. Con il passare del tempo si sono andati a formare centri specializzati costituiti da dei capannoni molto grandi in cui sono presenti migliaia di computer, raffreddati da imponenti impianti di ventilazione.
Questo meccanismo viene chiamato "estrazione", o *mining*, passato recentemente sotto i riflettori della critica ambientalista in quanto porta a un ingente utilizzo di energia: basti sapere che attualmente i processi di estrazione consumano in totale più energia di interi stati di piccole dimensioni, come l'Irlanda, e circa lo 0,8% dell'energia consumata negli Stati Uniti.

2.3 COME SI CALCOLA QUANTO VALGONO I BITCOIN

A differenza di quanto avviene per la valuta a corso reale, il valore di Bitcoin è determinato dalla domanda e dall'offerta presenti, in base cioè a quanto sono disposte le persone a spendere per averli. Il valore viene calcolato basandosi sul valore delle normali valute con cui viene scambiato: in pratica, un BTC ha un determinato valore solo perché gli utenti del sistema concordano sul fatto che abbia quel determinato valore.

Un particolare fatto connesso al Bitcoin è che, come già detto precedentemente, il numero totale di unità prodotte è stato prestabilito dalle autorità internazionali: ne saranno emesse fino a quando non si avvicineranno alla quantità totale di 21 milioni senza però mai raggiungere tale soglia[5]. Questo valore è stato scelto seguendo il seguente ragionamento: sapendo che un bitcoin è divisibile fino allo 0,00000001, l'equivalente di 1 Satoshi (la più piccola unità di Bitcoin) e sapendo che all'epoca i miners ricevevano un premio di 50 bitcoin per ogni blocco minato

[5] Ogni quattro anni il numero dei miners viene dimezzato dal sistema, rendendo le restanti monete BTC sempre più difficili da minare. Questo significa che col passare del tempo il numero dei miners diminuirà a tal punto da non avere più la potenza dei calcolatori per riuscire a minare le ultime frazioni di Bitcoin.

ovvero riguardante le transazioni citate in precedenza e/o azioni che il miner compie.

Data la forte crescita di miner all'epoca, dopo 4 anni si decise di diminuire il premio a 25 Bitcoin, e si impose che ogni 210.000 blocchi "minati" si sarebbe dimezzato il premio dei miners, da li fu un susseguirsi di dimezzamenti anche a causa dell'innalzamento del numero di questi ultimi soggetti nel mercato. Riscrivendo la funzione di produzione in algoritmo portandolo avanti fino al momento di scelta dei famosi 21 milioni arriviamo alla seguente funzione:

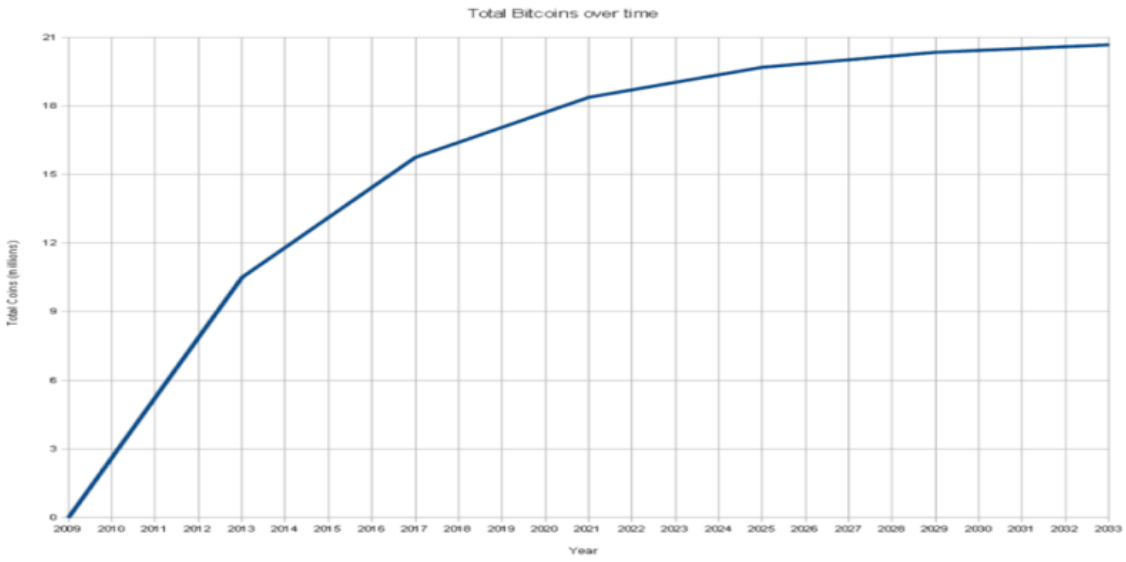

Fig.3. Grafico relativo alla quantità di Bitcoin nel tempo (in milioni).

50 Bitcoin * 210.000 blocchi + 25 Bitcoin * 210.000 blocchi + 12,5 Bitcoin * 210.000 blocchi + 12,5 /2 Bitcoin * 210.000 blocchi e così via raccogliamo 50 * 210.000 blocchi otteniamo 10.500.000 * (1 + ½ e così via) tra parentesi troviamo la scomposizione del premio associato al mining; la sommatoria all'interno della parentesi dà come valore finale 2 che moltiplicato a 10.500.000 dà 21.000.000 (21 milioni) scelti come limite di immissione nel mercato.

$$\sum_{n=0}^{\infty} \frac{210000 \times 50}{2^n} = 210000 \times 50 \times \frac{1}{1-\frac{1}{2}} = 21000000$$

Ogni quattro anni il numero di miners viene dimezzato così come la quantità di moneta distribuita a chi scopre nuovi blocchi da aggiungere alla blockchain. Dalla sua nascita nel 2009 al giorno odierno, Bitcoin ha già completato tre halving. In base ai dati storici, in seguito ad ogni dimezzamento il prezzo della criptovaluta è aumentato in maniera esponenziale.

A tal proposito si può citare uno studio effettuato dai ricercatori del *The TIE*[6] pubblicato sul sito *cointelegraph.com*, in cui sostengono una correlazione tra il valore di mercato di BTC e le altcoin[7], e il numero di volte che i media hanno menzionato l'imminente halving. Nel grafico si può notare come ci sia forte correlazione tra i due eventi, infatti nell'autunno 2019 una volta che i riferimenti all'halving erano diminuiti, anche il prezzo del BTC era calato, e quando si è tornato a parlare di nuovo di halving, anche il prezzo della criptovaluta è risalito.

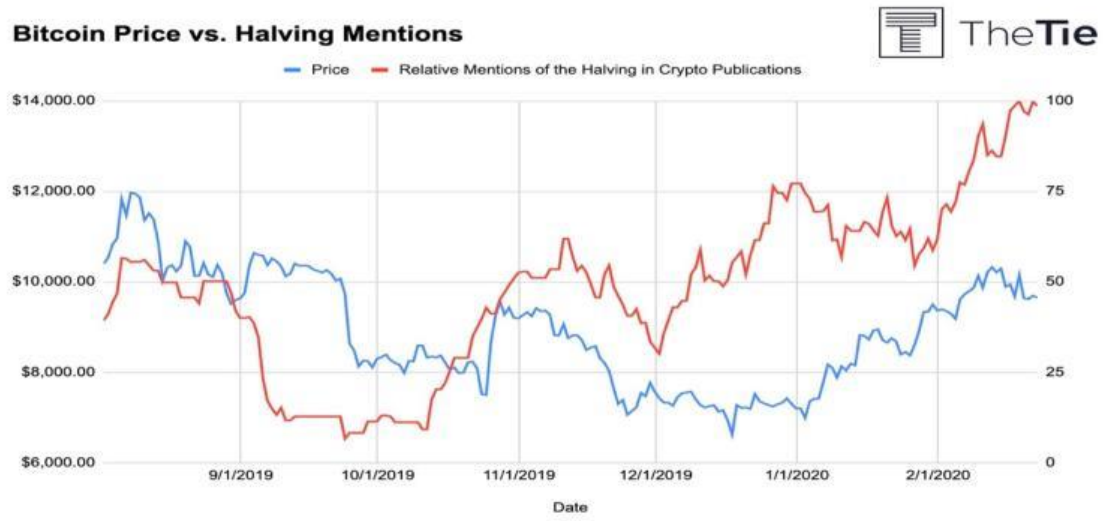

Fig.4. andamento del prezzo (blu) a confronto con le menzioni del bitcoin in concomitanza con l'halving (rosso).

L'ultimo halving è avvenuto a maggio del 2020: l'evento prevede sempre lo stesso modus operandi; la riduzione della ricompensa per il mining di nuovi blocchi, esattamente la metà (da 12,5 a 6,25 BTC, in questo caso), diminuendo così il numero di criptovalute che entrano regolarmente nel mercato.

The Tie: fornitore di dati e grafici per assets digitali.
[7] *Altcoin (Alternative Coin):* una qualsiasi alternativa a Bitcoin.

Dopo aver preso in esame gli articoli di 22 portali d'informazione, fra i quali anche Cointelegraph, CoinDesk, Bitcoinist e The Block, The TIE ha individuato una correlazione "*moderatamente forte e positiva"* tra il numero di riferimenti all'halving e prezzo dell'asset

Seguendo tale logica, inoltre, risulta assente il pericolo di inflazione della valuta, cioè una sua perdita di valore, in quanto non sono previste iniezioni di liquidità da parte di un ente come la Banca centrale. Dall'altra parte però, più ci si avvicinerà alla soglia dei 21 milioni di Bitcoin minati, dovuto all'aumento della richiesta, più ci sarà il rischio di un processo esponenziale di deflazione a causa della sempre meno disponibilità della valuta.

2.4 VANTAGGI DI BITCOIN

Essendo una nuova tecnologia il bitcoin assieme alle altre criptovalute è studiato per l'apporto di numerose novità.

Sicurezza e controllo: chi utilizza Bitcoin ha il controllo totale delle proprie transizioni dal momento che per ogni transizione ci deve essere l'esplicito consenso del proprietario, nessun altro può ritirare denaro da un portafoglio. Con altri metodi di pagamento questo potrebbe invece accadere.

Maggior difficoltà di contraffazione: tra i metodi più utilizzati c'è quello denominato "doppia spesa", ovvero far spendere alla vittima la stessa quantità di denaro due volte. La prevenzione a questa frode è stata offerta da Bitcoin all'inizio del 2009 utilizzando un protocollo crittografico chiamato "proof-of-work" per evitare la necessità che una terza parte attendibile convalidi le transizioni. Tramite l'utilizzo della blockchain una transizione si considera valida quando vi è inclusa in questa, ed è proprio la blockchain a contenere la maggior quantità di lavoro computazionale. Tutto questo processo rende sempre più difficoltoso la truffa "doppia spesa" a mano a mano che aumentano le dimensioni della rete complessiva.

No *PCI (Payment Card Industry)*[8]*:* ovvero l'utilizzo di carte di credito, debito, prepagate, ATM e POS, e tutte le numerose aziende associate ad esse. Al suo interno si trovano organizzazioni che si occupano di elaborare, archiviare e trasmettere i dati degli utenti, e comprende tutte le più importanti compagnie di carte di credito del pianeta. La PCI impone una serie di regole e normative molto severe. Un complesso di norme unificato è conveniente per le grosse aziende, mentre non lo è per gli utenti. Al contrario, quando si utilizza il Bitcoin, non è necessario sottostare alle regole imposte dalla PCI. Gli utenti possono pagare quindi commissioni più economiche in conseguenza del fatto che vengono ridotte le spese amministrative e burocratiche degli istituti creditizi.

Commissioni stabilite dagli utenti: le commissioni sono totalmente volontarie in quanto è l'utente che decide come modellare costi/tempi di attesa per una transazione. Una commissione più alta implica una transazione codificata più veloce. Sono infatti le tariffe pagate dagli utenti a generare profitto per i miners al termine della generazione di un nuovo blocco, molto più profittevoli della ricompensa che ricevono in seguito al completamento di un blocco.

Alta portabilità: le criptovalute offrono agli utenti la libertà di inviare e ricevere denaro virtuale attraverso l'utilizzo dei codici QR, scansionabili con la fotocamera del telefono. Questo implica una notevole facilità nel loro trasporto e utilizzo. Poiché il Bitcoin esiste in forma digitale, somme di denaro digitale molto ingenti possono essere trasportate su una chiave USB oppure essere archiviate in rete. La transazione, come detto prima, può essere istantanea: basta essere collegati a una rete internet.

[8] Payment Card Industry Data Security Standard (PCI DSS): è un Sistema di sicurezza creato per aumentare i controlli sui dati dei titolari di carte per ridurre le frodi su carte di credito.

2.5 SVANTAGGI DI BITCOIN

Questioni legali: data la natura del Bitcoin, basata sul digitale e sull'anonimato, a livello giuridico la sua caratterizzazione varia molto se ci si sposta da un paese all'altro; in alcuni di questi l'utilizzo delle criptovalute viene incoraggiato, al contrario, in altri viene bandito e reso illegale. In passato, il suo utilizzo ha fatto sì che spopolasse sul Dark Web, luogo in cui si può acquistare e vendere illegalmente quasi tutto quello che si vuole, portando alla chiusura di Silk Road nel 2013, celebre mercato in rete dedicato alla vendita di merce illegale, per l'appunto.

Volatilità: il prezzo del Bitcoin ha un andamento molto oscillatorio, a tal punto che alcuni lo considerano una semplice bolla finanziaria o addirittura uno schema piramidale[9]. Il suo valore è imprevedibile e molti investitori imprudenti possono andare incontro ad ingenti danni economici.

Chiavi[10] perdute: ciascuna chiave è composta da un codice alfanumerico che permette al proprietario del portafoglio di accedervi. In passato ci sono stati casi molto eclatanti di possessori di portafogli contenenti un ingente numero di Bitcoin che hanno perso le chiavi e di conseguenza gran parte del loro patrimonio. Uno di questi è Gerard Cotten, fondatore di QuadrigaCX, una delle più importanti piattaforme di scambio di criptovalute canadese. Alla sua morte, non avendo lasciato a nessuno i dati di accesso al suo e-wallet, i suoi eredi hanno completamente perso circa $150.000.000,00.

[9] Schema piramidale (o schema Ponzi): è un particolare modello di commercio e di marketing non sostenibile, che implica lo scambio di denaro primariamente per arruolare nuovi soggetti nel modello, solitamente (ma non sempre) con lo scambio di beni o servizi. Man mano che vengono reclutate altri soggetti diventa sempre più complicato trovare nuove reclute fino a quando non diventa rapidamente impossibile e la maggior parte dei membri non è in grado di trarre alcun profitto; in quanto tali, gli schemi piramidali sono insostenibili e spesso illegali.

[10] Chiavi private: La chiave privata Bitcoin è un numero segreto generato per consentire alle persone di utilizzare i propri bitcoin tramite spese e transazioni. Quando agli utenti viene rilasciato un indirizzo bitcoin, viene rilasciata anche una chiave privata bitcoin. È un numero a 256 bit e poiché è il biglietto d'oro che consente a un individuo di spendere i propri bitcoin, deve essere tenuto al sicuro e protetto.

Sviluppo continuo: l'evoluzione delle criptovalute, dal punto di vista sia dell'incremento della sicurezza e sia per quanto riguarda la diffusione tra gli utilizzatori a livello globale, è continua; le banche e i governi cercano quindi di capirle e regolamentarle una norma alla volta. Questo potrebbe significare che divenendo sempre più popolare un giorno i governi decidano di imporvi il proprio controllo, andando contro però a uno dei principi fondanti del Bitcoin.

CAPITOLO 2: BLOCKCHAIN

1. BLOCKCHAIN: CREARE ASSET DIGITALI UNICI

Per asset digitale si intende un documento in formato word, un file .jpeg o pdf, o un audio mp3, per citarne alcuni. Sono file che vengono generati attraverso un computer e nel momento in cui vengono inviati si duplicano andando a perdere la loro originaria unicità. Tramite la blockchain ciò non accade in quanto il file iniziale non appena viene trasferito da un computer all'altro viene crittografato e chi lo invia ne perde la "proprietà", come avviene con il trasferimento di beni materiali nella realtà.

Si può quindi dire che la blockchain consente di "riacquistare" il concetto di scarsità dei beni proprio del mondo reale, cosa che invece non avviene nel mondo digitale a seguito dell'automatica duplicazione del documento durante il passaggio.
Tale concetto assume maggior importanza nel momento in cui non si tratta più di un semplice file word ma si entra nel mondo finanziario in cui la possibile duplicazione di asset, che rappresentano un valore monetario, esige una garanzia. Per questo motivo il mondo della finanza ha per primo compreso il valore della blockchain nel garantire l'unicità di un asset digitale.

Va inoltre chiarito ciò che lega la Blockchain e la Distributed Ledger Tecnology (archivi distribuiti).
Una DLT è un sistema distribuito che grazie a un meccanismo di consenso[11], coinvolge tutti i nodi del sistema (ovvero i partecipanti alla rete Blockchain, per esempio) con l'obbiettivo di garantire l'univocità, la persistenza e la condivisione dei dati presenti in un *repository* detto registro o ledger (libro mastro). Il registro che troviamo in ogni nodo di un sistema DLT, è un database che si distribuisce

[11] Meccanismo del consenso: caratteristica principale della DLT, prevede l'adozione di un algoritmo capace di garantire che su ogni nodo della rete sia sempre presente una copia identica dl registro, assicurando la coerenza tra i nodi. In particolare, tale algoritmo deve essere in grado di garantire sia una corretta esecuzione dello stesso meccanismo del consenso, coinvolgendo tutti i nodi della rete, sia salvare i dati nel ledger presente su di un nodo e la successiva replicazione della copia del ledger ai restanti nodi della rete.

su tutti i nodi della rete, in cui le informazioni sono organizzate in tabelle correlate che consentono ricerche e aggiornamenti incrociati.

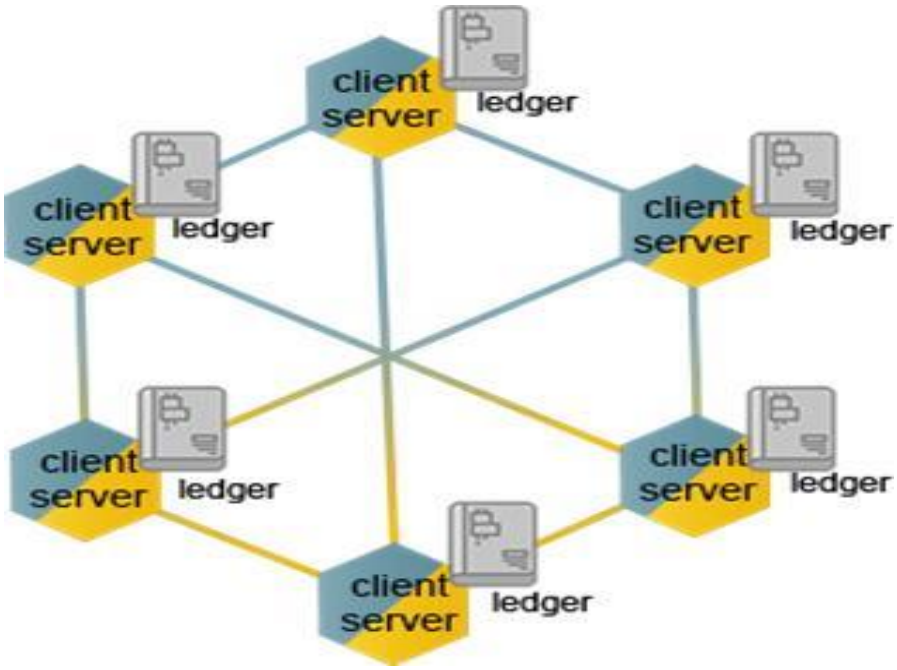

Fig.5. DLT, il ledger distribuito su ogni nodo del sistema Blockchain.

Qualunque transazione che avviene nella Blockchain, e di conseguenza anche i dati che descrivono tale transazione, vengono sottoposti ad un meccanismo di doppia chiave asimmetrica[12] che funziona con un meccanismo simile a quello usato per la firma digitale.

Le DTLs, per abilitare l'utente all'utilizzo del sistema, utilizzano degli algoritmi crittografati e così facendo mettono a disposizione dell'utente una chiave pubblica e una privata da usare per sottoscrivere transazioni o per l'attivazione degli *smart contract*[13] o altri servizi legati alla blockchain.

Le Blockchain si basa dunque sulla Distributed Ledger Technology caratterizzate da un registro impostato e strutturato che permette la gestione delle transizioni

[12] Chiave asimmetrica: è un tipo di crittografia dove, ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi:

- La chiave pubblica, che deve essere distribuita;
- La chiave privata, appunto personale e segreta;

evitando così qualunque problema connesso alla necessità di uno scambio in modo sicuro dell'unica chiave utile alla cifratura/decifratura presente invece nella crittografia simmetrica. Il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra.

[13] *smart contract*: contratti intelligenti e automatizzati garanti dell'impossibilità, per ciascuna delle parti coinvolte, di decisioni arbitrarie o di non rispettare pagamenti e/o condizioni prestabilite; Gli smart contract, di solito, hanno anche un'interfaccia utente e spesso simulano la logica delle clausole contrattuali.

all'interno di una Catena di Blocchi. Ciascun "blocco" viene aggiunto alla catena sulla base di un processo di consenso distribuito su tutti i nodi della rete, ovvero attraverso la partecipazione di ogni nodo che viene chiamato a contribuire alla validazione delle transazioni in ciascun blocco e alla loro "inclusione" nel registro.

1.1 CARATTERISTICHE ALLA BASE DELLA BLOCKCHAIN

Fatta questa piccola premessa possiamo andare ad analizzare più nel dettaglio le caratteristiche che compongono la Blockchain e come avvengono le transazioni contenenti criptovalute.

La Blockchain appartiene ad una sottocategoria di tecnologie digitali in cui è presente un registro strutturato come una catena di blocchi in cui sono riportate le transizioni, la cui validazione viene affidata ad un meccanismo che si basa sul consenso. Cosa significa questo? La Blockchain deve essere vista come una "catena di blocchi", cioè una struttura dati (registro, database) decentralizzata, condivisa e crittograficamente immutabile. Tale struttura funge da registro digitale di tutte le transazioni e/o informazioni inserite e suddivise appunto in "blocchi" di dati. L'aggiunta di ogni nuovo blocco alla catena deve passare attraverso un preciso protocollo che si basa sul consenso tra i computer (nodi) che costituiscono la rete Blockchain. Quando avviene l'aggiunta di un nuovo blocco, ogni nodo aggiorna la propria copia (questo implica che non è richiesto che i nodi coinvolti conoscano l'identità reciproca o si fidino l'uno dell'altro), senza che ci sia più alcuna possibilità di modificare i dati, una volta inseriti e validati, perché tramite un protocollo condiviso, ognuno di questi nodi aggiorna la propria copia privata. Per "blocco" si intende un file; in particolare, ciascun blocco si compone di due parti principali:

3 *Header*, nel quale sono conservati una serie di dati, tra cui:

a. Numero del blocco (numero crescente a partire dal blocco 0);
b. Codice *hash*[14] del blocco;
c. *Timestamp* (data e ora in cui il blocco è stato prodotto);

[14] Il codice hash: è un codice alfanumerico che coincide con il codice fiscale di una persona, solo che vale per un nodo della blockchain. Se la data di nascita viene falsificata su un documento, cambia anche il codice fiscale. La stessa cosa accade nella blockchain: se il contenuto di un blocco viene manipolato, cambia anche il suo codice hash.

d. Totale dei bitcoin movimentati nel blocco;
e. Dimensione del blocco (in *kilobyte*);

- *Body*, nel quale sono contenute tutte le transazioni registrare su quel blocco.

Ogni blocco ha al suo interno un certo numero di transazioni, quindi all'aumentare di queste, aumenta anche la dimensione media dei blocchi all'interno della blockchain. Il codice hash presente in ciascun blocco fa da tramite tra il blocco vecchio e quello nuovo, ecco perché viene comunemente chiamata "catena" di blocchi, perché ogni singolo blocco è incatenato a quello precedente e a quello successivo.

Facciamo un breve esempio: digitando sul sito https://www.blockchain.com[15] il numero del blocco 567890 otteniamo tutte le sue caratteristiche. Le informazioni che troviamo sono:

- Data in cui è stato prodotto: 2019-03-20 (riga tre);
- Al suo interno ci sono 695 transazioni (riga sei);
- Il totale dei bitcoin contenuti nel nodo è 20859,25287081 BTC (riga quattordici)
- La sua dimensione è di 401,637 bytes (riga dodici);
- Il suo codice hash è 00000000000000000002629ce3e8e71d7577f6b12b7598f77e5a61abfa8458894 (riga 1);
- Il codice hash del blocco precedente a cui è incatenato risulta essere 00000000000000000292aeafcff600480e7848c7396ed8f33a0e4a6865fb584;

[15] Blockchain.com: è un servizio di esplorazione di blocchi Bitcoin, nonché un portafoglio di criptovaluta e uno scambio di criptovaluta che supporta Bitcoin, Bitcoin Cash ed Ethereum. Inoltre, vengono forniti anche grafici, statistiche e aggiornamenti di mercato per quanto riguarda le criptovalute.

hash	000000000000000000002629ce3e8e71d7577f6b12b7598f77e5a61abfa8458894
conferme	74.593
timestamp	2019-03-20 00:00
Altezza	567890
Minatore	F2Pool
Numero di transazioni	695
Difficoltà	6.068.891.541.676,55
Radice di Merkle	d5b70ef3780a7ac3516280ca7df135063903d32b421c8ebd845eaa08068fd30a
Versione	0x3fffe000
bits	388.915.479
Peso	1.317.003 WU
Taglia	401.637 bytes
nonce	910.791.929
Volume delle transazioni	20859.25287081 BTC
Block Reward	12.50000000 BTC
Premio tariffa	0.05586195 BTC

Fig. 6. https://www.blockchain.com. Informazioni relative al blocco 567890.

Attuando lo stesso procedimento possiamo trovare il blocco 0, ovvero quello che è l'origine di tutto. È stato prodotto alle 18.15 del 03/01/2009, contiene un'unica transazione da 50 bitcoin ad una dimensione totale di 285 bytes, il codice hash è 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f, il numero della transizione in oggetto è 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b ed è stato inviato all'indirizzo 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa.

Per ogni transizione è previsto un input e un output che ci danno un'indicazione su dove provengono le criptovalute e a chi sono stati inviate.
Tenendo sempre come riferimento il blocco 0 si possono visualizzare informazioni diverse riguardanti sia l'input che l'output. Per esempio, si può notare che lo *ScriptSig*[16] che è contenuto nell'input è: 04ffff001d0104455468652054696d6573203033;

[16] *ScriptSig*: è la prima parte della firma crittografica per verificare l'autenticità dell'input ed è composto, oltre che dallo Script di Firma, dalla chiave pubblica.

mentre lo ScriptPubKey[17] dell'output è: 04678aefdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c38df7ba0b8578a4c702b6bf11d5f.
I due codici appena citati sono rispettivamente la prima e la seconda metà dello script.[18]

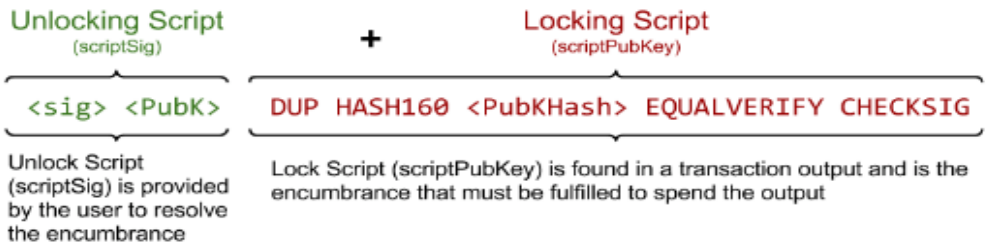

FIg.7. Illustrazione di come si compone il codice (input) e (output) in una transazione. Fonte: Mastering Bitcoin

Lo Script a sua volta è formato da due elementi:

- *PublicKey* ovvero la "chiave pubblica", cioè la chiave che appartiene a chi è destinato l'output della transizione e che permette quindi al destinatario di riscattare la criptovaluta che è specificata nell'output;
- *Signature* ovvero "firma dell'hash" che serve per dimostrare l'originalità della transazione e che tale transazione è stata eseguita in modo legittimo dal proprietario dell'indirizzo in oggetto.

Si può dire quindi che tale sistema consente di inviare una transazione ma attraverso l'utilizzo di uno script che può essere risolto solo con una specifica chiave privata, ovvero con quella chiave pubblica che è stata utilizzata per creare lo stesso script. Questo passaggio risulta importante in quanto garantisce sostegno all'intera tecnologia blockchain.
Attraverso quest'ultima si possono fare due cose fondamentali: registrare un qualsiasi tipo di evento e aver la sicurezza che tale registrazione rimanga permanente. Ciò risulta molto utile e vantaggioso in quelle situazioni in cui due individui devono accordarsi ma non si fidano l'uno dell'altro. Quindi la blockchain fa in modo che si possa portare a termine con successo un accordo o una

[17]ScriptPubKey: è uno script di blocco posizionato sull'output di una transazione Bitcoin che richiede che siano soddisfatte determinate condizioni affinché un destinatario possa spendere i propri bitcoin;

[18] Script: "*lo script non è altro che un particolare programma scritto in uno specifico linguaggio di programmazione che, accompagnando le transazioni, istruisce i nodi su cosa fare con i dati presenti nelle transizioni*" (Comandini, 2020).

transizione tra due o più individui senza la necessità che ci sia fiducia o garanzia. Ogni catena di blocchi arriva a pesare vari gigabyte e si può facilmente scaricare e visualizzare sul proprio computer.

Per di più, ciò che caratterizza le tecnologie blockchain è il fatto che il registro sia immutabile, trasparente, si basi sulla tracciabilità delle transazioni e sulla sicurezza grazie all'utilizzo di tecniche crittografiche. La Blockchain viene identificata sempre più frequentemente come *Intenet of People,* o più in generale *Internet of Things*[19] in quanto diventa sulla base di sette aspetti che la rendono unica:

- Decentralizzazione;
- Trasparenza;
- Sicurezza;
- Immutabilità;
- Consenso;
- Responsabilità;
- Programmabilità;

La blockchain può essere vista come una piattaforma che permette lo sviluppo e la concretizzazione di una innovativa forma di rapporto sociale che, basandosi e facendo affidamento sulla partecipazione di tutti, garantisce alla comunità intera la possibilità di controllare, verificare e disporre di una totale e completa trasparenza sugli atti e le decisioni, che sono a loro volta registrati in archivi che non possono essere alterati e modificati, risultando così immuni alla corruzione.

[19] Internet of Things (IoT): neologismo che viene utilizzato per dare un nome agli oggetti reali connessi a internet. Si comprendono un insieme di tecnologie che permettono di collegare a internet qualsiasi genere di apparato con l'obbiettivo di monitorare, controllare e trasferire informazioni per poi svolgere azioni conseguenti. P.e. la macchina del caffè che manda una notifica a un'applicazione del telefono quando ha finito i chicchi di caffè.

1.2 LA BLOCKCHAIN COME EVOLUZIONE DEL CONCETTO LEDGER

La blockchain può essere intesa come la realizzazione del Distribuited Ledger, una evoluzione del Centralized Ledger e del Decentralized Ledger. Esse si contraddistinguono in base alle seguenti caratteristiche:

- Centralized Ledger: alla base troviamo la logica di un rapporto rigorosamente centralizzato uno-a-tanti, dove la gestione di tutto fa riferimento a una struttura, autorità o sistema centralizzato. Nel CL viene riposta la fiducia nell'autorità, nell'autorevolezza del soggetto o sistema che rappresenta il "centro" dell'organizzazione.

- Decentralized Ledger: si trova una centralizzazione ma solo a livello "locale" con dei "satelliti" strutturati nella forma uno-a-tanti che interagiscono tra loro ripetendo la suddetta forma uno-a-tanti. Così facendo viene a mancare un unico "grande" soggetto centrale lasciando il posto a tanti "soggetti centrali". Anche in questo caso la fiducia viene riposta in un soggetto centrale che anche se più vicino ai nodi rimane comunque centralizzato.
Le organizzazioni che si basano su Decentralized Ledger individuano una Governance che si occupa di stabilire delle forme di coordinamento di tipo centralizzato.

- Distributed Ledger: rappresenta il vero cambiamento in cui non è più presente alcun centro e dove la logica di Governance è costruita attorno ad un nuovo concetto di fiducia tra i soggetti. Così facendo viene eliminata la possibilità di prevalere gli uni sugli altri e le decisioni passano attraverso un processo di costruzione del Consenso.

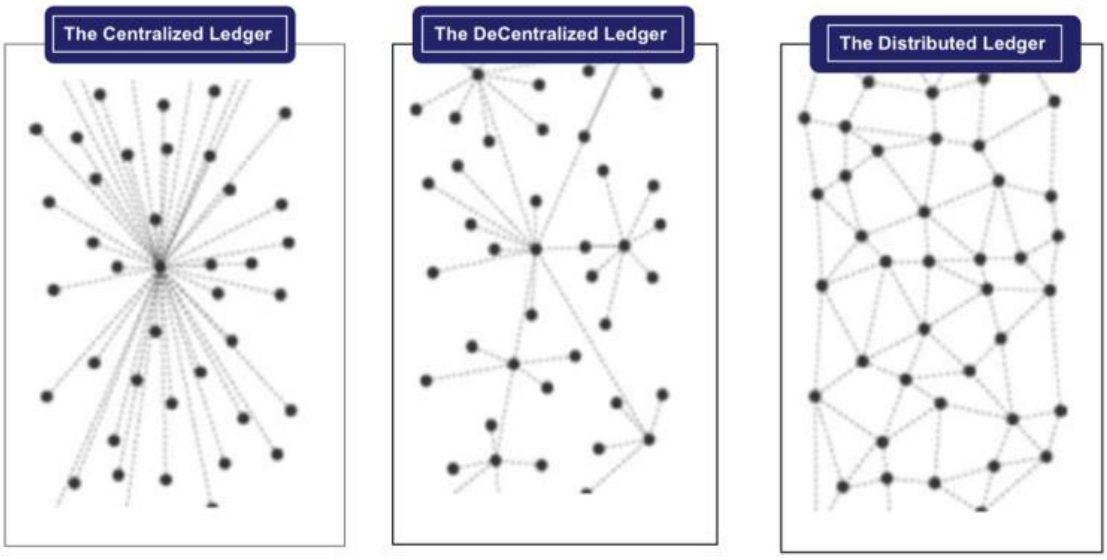

Fig.8. Centralized Ledger, Decentralized Ledger, Distributed Ledger.

1.3 LA BLOCKCHAIN COME REGISTRO PUBBLICO APERTO A TUTTI

Si può descrivere la blockchain come un database decentralizzato che archivia asset e transazioni su una rete di tipo peer-to-peer[20]. È un registro accessibile a tutti per la gestione dei dati collegati alle transazioni presenti nei blocchi e che vengono gestite tramite una crittografia da parte dei partecipanti alla rete che possono verificare, approvare e successivamente registrare ciascun blocco contenente i dati di ciascuna transazione sui nodi. In questo modo le medesime informazioni si ritrovano in ogni nodo e così diventa impossibile modificarla se non attraverso una operazione che necessita l'approvazione da parte della maggioranza dei nodi della rete.

La blockchain non va considerata come una applicazione, né un sistema, né una tecnologia, ma un nuovo modo di gestire le informazioni che garantisce

[20] Peer-to-peer: nella telecomunicazione indica un modello di architettura logica di rete informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di *client o server* fissi ma anche sotto forma di nodi equivalenti o 'paritari' (*peer*) potendo fungere al contempo da *client* o *server* verso gli altri nodi terminali (*host*) della rete. Mediante questa configurazione, qualsiasi nodo è in grado di avviare o completare una transazione. I nodi equivalenti possono differire nella configurazione locale, velocità di elaborazione, ampiezza di banda e quantità di dati memorizzati. Un tipico esempio di P2P è la rete per la condivisione di file (*file sharing*).

l'immutabilità dei dati poiché assicura e certifica la storia completa di ciascun dato e di tutte le operazioni connesse ad ogni transazione.

I tipi di transazioni che la blockchain può amministrare e appoggiare sono innumerevoli. Uno di questi può essere il *payment,* così come le transizioni collegate allo scambio di beni e servizi o la gestione di informazioni legate alla contrattualistica. La blockchain rappresenta quindi il Libro Mastro decentralizzato e crittograficamente sicuro per la gestione delle transizioni che avvengo su reti pee-to-peer. La blockchain rende possibile scambiarsi sia informazioni che documenti che denaro attraverso internet; queste ovviamente sono solo alcune, altre verranno create e modellate in base alle caratteristiche della blockchain.

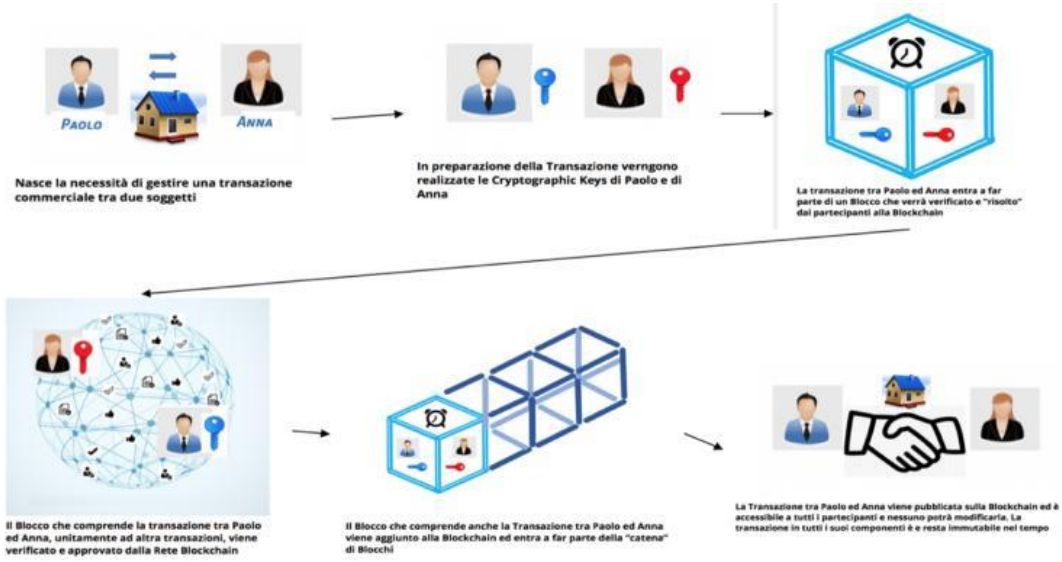

Fig.9. Flusso completo: dalla transazione al blocco alla blockchain.

2. COSA SI INTENDE PER FORK

Le criptovalute, come qualsiasi altra nuova tecnologia, hanno bisogno di continue modifiche e aggiornamenti. In modo specifico, molte volte si deve aggiornare il codice originario (e di conseguenza il software) di un protocollo, come può essere il protocollo del Bitcoin o di Ethereum. Nel momento in cui una proposta di modifica va a buon fine, e quindi viene eseguita, si crea un fork.

Uno dei fork più famosi è stato quello di Bitcoin, avvenuto nel 2017, da cui è nato Bitcoin Cash. Nonostante sia la criptovaluta più preziosa, più conosciuta e con la più alta capitalizzazione di mercato ha un grave problema ovvero quello della scalabilità. Quest'ultima infatti risente della limitata grandezza dei blocchi (1MB) per cui impiega tempi molto lunghi nel processo dell'elaborazione delle transizioni rispetto ad altri protocolli; il tutto fa si che il numero di transizioni che la rete riesce a gestire sia basso (4/7 transizioni al secondo). Un simile problema nella pratica significa aspettare anche diversi giorni per pagare una somma irrisoria come una bottiglietta d'acqua, cosa realmente accaduta nel 2017. La *community* che ruota attorno al mondo Bitcoin, dopo svariate proposte risolutive, optò per un protocollo in cui si portava la grandezza dei blocchi da 1MB a 2MB. Il protocollo, nel quale si elencavano anche altre migliorie, prese il nome di SegWit2x, e così come accade per la proposta di qualsiasi miglioria, messa ai voti, riscosse il 95% dei voti favorevoli da parte dei miner. Successivamente, tramite ulteriori ampliamenti che portarono la dimensione dei blocchi da 2MB a 8MB, si è arrivati a quello che oggi è Bitcoin Cash. Ma una modifica così drastica ha inevitabilmente portato ad una separazione dalla rete originale di Bitcoin, ciò si traduce nell'utilizzo di un hard fork[21].

La differenza tra hard fork e soft fork si basa sul concetto di retrocompatibilità. Per aggiornare Bitcoin, per esempio, c'è stata una divisione totale dei due diversi codici sorgenti e dei loro dati. Quando invece abbiamo retrocompatibilità con la blockchain precedente, e i nodi non aggiornati sono ancora in grado di eseguire transizioni e aggiungere blocchi, allora si definisce soft fork. Quando avviene il fork, chiunque sia in possesso di "pezzi" di criptovaluta in oggetto, avrà lo stesso ammontare di unità della nuova criptovaluta "forkata", come incentivo per non averla venduta. Quando ci si avvicina ad un aggiornamento di una criptovaluta, ovvero quando sta per avvenire un hard fork, c'è molto interesse da parte degli speculatori sul mercato. Per esempio, se nell'agosto del 2017 avessimo avuto 5 BTC (pari a circa a 4000$ ciascuno, in quel mese) ci saremmo ritrovati in seguito al fork con 5 BCH gratuitamente (pari a 295$ ciascuno, in quel mese).

[21] Hard Fork e Soft Fork: Binance.vision

L’interesse speculativo prima e dopo un fork porta inevitabilmente a grandi variazioni del prezzo della criptovaluta oggetto di analisi, poiché vengono acquistate in grande numero per ricevere il premio, evento che alza il prezzo; successivamente al fork le nuove criptovalute ricevute gratuitamente vengono vendute, fatto che fa crollare il prezzo sul mercato.
Ciononostante, un evento come quello relativo ad un hard fork viene visto da molti negativamente, in particolar modo dai “puristi”, coloro che credono più nella filosofia delle criptovalute che nelle sue naturali utilità monetarie e finanziarie, in quanto si va a distruggere uno dei principi cardini: l’immutabilità.

3. ATTACCHI ALLA RETE

Nonostante possa sembrare sicura e inespugnabile più di una volta si sono verificati attacchi da parte degli hacker nei confronti della blockchain. La maggior parte delle volte però, questi fanno leva sull’inesperienza degli utenti utilizzatori che non tengono nascoste le chiavi oppure eseguono in modo errato le transizioni. Più nello specifico troviamo due grandi esempi di hackeraggio:

3.1 51% ATTACK

È uno degli attacchi hacker più noti e può essere valido su blockchain o criptovalute che si basano su un metodo di consenso Proof to Work, come Bitcoin. L’obbiettivo è quello di prendere il possesso del 50% + 1 dei nodi di una rete (la maggioranza del consenso) per far approvare i blocchi da lui creati e. sfruttare la *double spending* o “doppia spesa” descritta nel capitolo precedente.
“questa metodologia implica l’invio di transazioni alla catena, la ricezione del bene o del servizio per cui la transizione viene pagata e successivamente l’hashpower di maggioranza per imporre la blockchain in un punto precedente alla transazione, così da cancellare velocemente quella transazione dalla cronologia della catena di blocchi e consentire al truffatore di effettuare altre transazioni con le stesse monete per una seconda volta. Colui che viene

“danneggiato” in questa circostanza non è tanto chi possiede bitcoin ma colui a cui la somma era destinata tramite l’invio. Significa prendere il possesso del quorum dei nodi per usarlo a proprio vantaggio, cosa non molto facile nel caso del bitcoin in quanto si necessita di una potenza computazionale molto alta rispetto al profitto che se ne ricaverebbe. Viene molto spesso utilizzata per altre criptovalute con una capitalizzazione e una potenza computazionale decisamente inferiore al BTC.

3.2 DDOS

Il DDoS (Distributed Denial of Service) si basa sul “bombardamento” tramite un elevato volume di traffico con l’obbiettivo di paralizzare il nodo di una blockchain. È un attacco molto comune volto per lo più a paralizzare temporaneamente la rete allungando i tempi di transizione, che rubare criptovalute e anche in questo caso le reti delle criptovalute principali sono rigorosamente strutturate per sopperire a simili attacchi. Nello specifico vengono inviate tante piccole transazioni o non valide col solo obbiettivo di impedire l’elaborazione delle transazioni reali.

CAPITOLO 3: ALCUNI SISTEMI DI INVESTIMENTI IN CRIPTOVALUTE NELLA LETTERATURA

Con la nascita e lo sviluppo delle criptovalute si è avuto modo di approfondire e studiare questa nuova tecnologia. Ci sono molti articoli che trattano dell'aspetto informatico, ingegneristico o finanziario alla base delle criptovalute, ma in questa tesi si è deciso di prendere in considerazione due lavori: il primo esamina i risultati di alcuni indicatori tecnici applicati su dieci altcoins, mentre il secondo articolo illustra lo "stock to flow model"[22]. Di seguito si presenteranno i risultati dei due articoli.

1. UTILIZZO DI INDICATORI TECNICI SULLE CRIPTOVALUTE

Nell'articolo *"Profitability of technical rules among cryptocurrencies with privacy function[23]"* sono state applicate delle semplici strategie di trading basate sulla media mobile, prendendo in considerazione come dati i prezzi giornalieri di dieci criptovalute. Lo studio effettuato in questo articolo si basa su criptovalute caratterizzate dalla "*privacy function*", cioè dalla possibilità per chi le possiede di mantenere un certo grado di anonimità sia per quanto riguarda le transazioni o l'account del saldo personale. La criptovaluta Dash è un esempio, in tal senso, in quanto permette agli utenti di utilizzare la funzione "invio transizione in anonimo" in modo da mantenere un certo grado di anonimità pagando delle commissioni in più[24].

I prezzi giornalieri presi in esame vanno dall' 1/01/2016 al 31/12/2018 e si ipotizza che se il mercato delle criptovalute fosse stato efficiente, non sarebbe stato possibile generare dei profitti utilizzando informazioni sui prezzi passati, cioè relativi al periodo appena menzionato. Le criptovalute scelte per l'esperimento

[22] "*Stock to flow model*": è un modello che determina il prezzo di Bitcoin nel lungo periodo. Viene descritto nel prossimo paragrafo.
[23] Shaker Ahmed, Klaus Grobys, Niranjan Sapkota, 2020. *Profitability of technical rules among cryptocurrencies with privacy function.*
[24] Esempio di *Privacy function* utilizzando la criptovaluta Dash:
https://docs.dash.org/en/stable/wallets/dashcore/privatesend-instantsend.html

sono: Dash (DASH), Bytecoin (BCN), DigitalNote (XDN), Monero (XMR), CloakCoin (CLOAK), Aeon (AEON), Stealth (XST), Ptime-Xi (PXI), NavCoin (NAV), Verge (XVG).

Lo studio presentato in questo elaborato è utile per più motivi:

- Porta avanti l'argomento che prende in considerazione l'analisi tecnica e lo applica alle criptovalute;
- Si prendono in considerazione criptovalute aventi la "*privacy function"*, cosa che non era mai stata fatta;
- Si contribuisce alla letteratura scientifica perché si cerca di capire l'efficienza del mercato delle criptovalute; gli studi precedenti a questo riguardo (Urquhart, 2016; Khuntia and Pattanayak, 2018; Tiwari et al., 2018; Bariviera, 2017; Sensoy, 2019; Kristoufek, 2018) prendevano in considerazione solo Bitcoin e la sua capitalizzazione di mercato, mentre in questo caso si cerca di affrontar il tema da un punto di vista più ampio ovvero considerando più criptovalute simultaneamente.

1.1 RISULTATI OTTENUTI

Nella tabella 1 si osservano i rendimenti medi e le corrispondenti t-statistiche delle differenti strategie di trading, utilizzando la media mobile esponenziale.

Payoffs of MA trading strategies using price data.

Strategy	Tests on individual coin's MA returns										Joint Test of MA returns		
	DASH	BCN	XDN	XMR	CLOAK	AEON	XST	PXI	NAV	XVG	*3 coins*	*7 coins*	*10 coins*
(1, 20)	0.0018***	0.0005	0.0015	0.0022***	0.0001	−0.0003	−0.0004	−0.0042**	0.0007	−0.0019			
	2.75	0.35	1.25	2.7	0.08	−0.21	−0.27	−2.14	0.46	−1.16	11.22**	13.15*	23.37***
(1,50)	0.0016**	0.0006	0.0012	0.0018**	0.0002	0.001	0.0005	−0.0031	0.0009	−0.0014			
	2.46	0.39	1	2.13	0.16	0.76	0.32	−1.56	0.58	−0.85	7.83**	8.17	14.44
(1, 100)	0.0018***	0.0001	0.0012	0.0015*	−0.0001	0.0015	0.0002	−0.0035*	0.0006	−0.0019			
	2.63	0.05	0.93	1.77	−0.04	1.17	0.13	−1.79	0.35	−1.15	7.46*	8.25	16.87*
(1, 150)	0.0018**	0.0007	0.0013	0.0024**	0.0007	0.0017	0.0009	−0.0014	0.002	−0.0014			
	2.47	0.39	0.98	2.53	0.44	1.16	0.6	−0.69	1.12	−0.79	8.8**	9.21	14.18
(1, 200)	0.0018**	0.0008	0.0008	0.0022**	0.0016	0.0024	0.0007	−0.002	0.0022	0.0004			
**	2.28	0.43	0.56	2.25	0.91	1.59	0.45	−0.92	1.63	0.22	7.19*	8.41	11.02

Tabella 1: questa tabella contiene gli stessi calcoli della tabella 1, ma vengono usati come dati i prezzi delle criptovalute selezionate, e non il logaritmo dei prezzi.

Le varie strategie vengono definite come (*short period MA, long period MA)*, in cui con

i termini "*short period"* e "*long period"* si intendono rispettivamente il numero di giorni totali trascorsi in posizioni short o long, analizzati con la media mobile.

Payoffs of MA trading strategies using the log of price data.

Strategy	Tests on individual coin's MA returns										Joint Test		
	DASH	BCN	XDN	XMR	CLOAK	AEON	XST	PXI	NAV	XVG	*3 coins*	*7 coins*	*10 coins*
(1, 20)	0.0018***	0.0006	0.0015	0.0022***	0.0002	0	−0.0004	−0.0042**	0.0007	−0.0016			
	2.79	0.4	1.24	2.76	0.13	−0.03	−0.28	−2.15	0.45	−0.94	11.61***	13.15*	22.43**
(1,50)	0.0017***	0.0004	0.0011	0.0017**	0.0002	0.001	0.0005	−0.003	0.001	−0.0016			
	2.59	0.29	0.94	2.08	0.13	0.79	0.36	−1.52	0.59	−0.98	8.20**	8.52	15.12
(1, 100)	0.0018**	0.0005	0.0009	0.0017*	0	0.0016	0.0005	−0.0028	0.0006	−0.002			
	2.49	0.32	0.74	1.92	0.02	1.18	0.36	−1.41	0.34	−1.18	7.22*	7.76	14.95
(1, 150)	0.0017**	0.0007	0.0014	0.0025***	0.0006	0.002	0.0007	−0.0013	0.0022	−0.0012			
	2.29	0.42	1	2.63	0.37	1.38	0.44	−0.63	1.17	−0.66	8.57**	9.12	13.30
(1, 200)	0.0018**	0.0007	0.0014	0.0021**	0.0017	0.0023	0.0008	−0.0021	0.002	0.0002			
	2.28	0.4	0.94	2.17	0.95	1.53	0.49	−0.97	1.46	0.12	6.89*	7.70	10.89

Nota: la tabella 2 presenta la media dei rendimenti delle strategie di trading della media mobile di acquisto e il loro significato statistico sia di ciascuna criptovaluta analizzata, sia a livello congiunto prendendo in considerazione tre, sette o dieci criptovalute. Il campione chiamato *"10 coins"* contiene dieci criptovalute *privacy*: Dash (DASH), Bytecoin (BCN), DigitalNote (XDN), Monero (XMR), CloackCoin (CLOAK), Aeon (AEON), Stealth (XST), Prime-Xi (XPI), NavCoin (NAV), Verge (XVG). Il campione chiamato *"3 coins"* contiene le criptovalute *privacy* con la capitalizzazione di mercato maggiore: Dash, Bytecoin e Monero. Il campione chiamato *"7 coins"* contiene tutte le criptovalute *privacy* eccetto le tre aventi la più bassa capitalizzazione di mercato, cioè Stealth, Prime-Xi e Verge.

*** p < 0.01,

** p < 0.05,

* p < 0.10.

I risultati proposti nella tabella 2, in concomitanza con quelli della tabella 3, mostrano che la strategia di trading utilizzata per la criptovaluta Dash (1, 20)[25], per esempio, ha creato un rendimento medio annuo pari a 18.25%[26].

[25] Media Mobile a 20 periodi.

[26] (0.0018 – 0.0013) * 365 = 0.1825

Descriptive statistics.

Currency	Mean	Median	Max	Min	Std. Dev.	Skew	Kurt	Obs.
DASH	0.0013	−0.0005	0.1901	−0.1056	0.0272	0.8476	8.7271	1095
BCN	0.0012	0.0000	0.6939	−0.3953	0.0561	3.5782	46.3122	1095
XDN	0.0012	−0.0012	0.4394	−0.2229	0.0483	2.1572	18.3847	1095
XMR	0.0018	−0.0001	0.2539	−0.1273	0.0317	1.0620	10.1287	1095
CLOAK	0.0013	−0.0006	0.5724	−0.4470	0.0617	1.5343	21.6904	1095
AEON	0.0012	−0.0018	0.4453	−0.2178	0.0517	1.1308	10.9023	1095
XST	0.0012	−0.0014	0.5194	−0.4077	0.0588	1.0123	15.6361	1095
PXI	−0.0009	−0.0025	0.7282	−0.5947	0.0840	0.9249	17.2251	1095
NAV	0.0018	−0.0018	0.8914	−0.6569	0.0585	2.6581	69.0285	1095
XVG	0.0024	0.0000	0.4227	−0.3010	0.0701	0.7374	8.6747	1095

Tabella 3: la tabella presenta la statistica descrittiva (Media, Mediana, Massimo, Minimo, Deviazione Standard, Skewness, Curtosi e numero delle osservazioni) utilizzando il logaritmo dei rendimenti giornalieri delle seguenti criptovalute: Dash (DASH), Bytecoin (BCN), DigitalNote (XDN), Monero (XMR), CloackCoin (CLOAK), Aeon (AEON), Stealth (XST), Prime-Xi (XPI), NavCoin (NAV), Verge (XVG).

Per quanto riguarda, invece, l'analisi congiunta di dieci criptovalute, la tabella 1 ci mostra come i rendimenti medi siano significativi solo per la strategia di trading (1, 20) ad un livello del 5% (vedasi colonna "*10 coins*" nella tabella 1). Applicando, invece, orizzonte temporali maggiori ai 20 giorni per calcolare la media mobile *long period* aumentano mediamente i rendimenti che si ottengono a supporto della strategia di trading applicata; tuttavia, il test di significatività non è statisticamente accettabile ($p < 0.01$, $p < 0.05$, $p < 0.10$). Nessuna di queste

strategie di trading riesce a performare meglio di quella basata sul "*buy-and-hold*[27]" (vedasi colonna *"10 coins"* nella tabella 1).
Osservando i rendimenti medi delle singole criptovalute si nota che solo Dash e Monero generano rendimenti statisticamente significativi per ciascuna strategia basata sulla media mobile. Per quanto riguarda Dash, i rendimenti sono mediamente compresi tra 62.05% e 65.7% all'anno e corrispondono mediamente a +14.6% e +18.25% all'anno in più rispetto alla strategia *"buy-and-hold"* relativa alla stessa Dash. Per quanto riguarda Monero invece, i rendimenti sono statisticamente significativi con un $p < 0.05$ in tutti i casi tranne per la media mobile (1, 100) per la quale abbiamo un $p < 0.10$.

Per quanto riguarda invece i rendimenti a livello aggregato di portafoglio equipesato, come si può osservare nella tabella 4 panel B, i rendimenti medi del portafoglio contenenti tutte e dieci le criptovalute è pari a 2.92% all'anno, se si utilizza la strategia delle medie mobili. Parimenti, utilizzando la strategia del *buy-and-hold* abbiamo un rendimento medio annuo pari al 45.63%; ciò significa che la media mobile esponenziale utilizzata sul portafoglio contenete queste criptovalute non riesce a generare extra rendimenti rispetto a quest'ultima.

Nell'analisi delle medie mobili sono state calcolate utilizzando i rendimenti logaritmici; utilizzando però la serie dei prezzi, come si può osservare nella tabella A.3, i risultati non cambiano e le conclusioni restano le stesse.

[27] *Buy-and-hold*: chiamata anche *position trading*, è una strategia finanziaria in cui si acquistano criptovalute con l'obbiettivo di mantenerle per l'intero periodo di investimento.

Average return in annualized percentage rate.

Strategy	DASH	BCN	XDN	XMR	CLOAK	AEON	XST	PXI	NAV	XVG	*3 Coins*	*7 Coins*	*10 coins*
Buy and Hold	47.45	43.80	43.80	65.70	47.45	43.80	43.80	−32.85	65.70	87.60	52.32	51.10	45.63

Panel B: Log of price

Strategy	**DASH**	**BCN**	**XDN**	**XMR**	**CLOAK**	**AEON**	**XST**	**PXI**	**NAV**	**XVG**	***3 Coins***	***7 Coins***	***10 coins***
(1, 20)	65.70	21.90	54.75	80.30	7.30	0.00	−14.60	−153.30	25.55	−58.40	55.97	36.50	2.92
(1,50)	62.05	14.60	40.15	62.05	7.30	36.50	18.25	−109.50	36.50	−58.40	46.23	37.02	10.95
(1, 100)	65.70	18.25	32.85	62.05	0.00	58.40	18.25	−102.20	21.90	−73.00	48.67	37.02	10.22
(1, 150)	62.05	25.55	51.10	91.25	21.90	73.00	25.55	−47.45	80.30	−43.80	59.62	57.88	33.95
(1, 200)	65.70	25.55	51.10	76.65	62.05	83.95	29.20	−76.65	73.00	7.30	55.97	62.57	39.79

Panel C: Price

Strategy	**DASH**	**BCN**	**XDN**	**XMR**	**CLOAK**	**AEON**	**XST**	**PXI**	**NAV**	**XVG**	***3 Coins***	***7 Coins***	***10 coins***
(1, 20)	65.70	18.25	54.75	80.30	3.65	−10.95	−14.60	−153.30	25.55	−69.35	54.75	33.89	0.00
(1,50)	58.40	21.90	43.80	65.70	7.30	36.50	18.25	−113.15	32.85	−51.10	48.67	38.06	12.05
(1, 100)	65.70	3.65	43.80	54.75	−3.65	54.75	7.30	−127.75	21.90	−69.35	41.37	34.41	5.11
(1, 150)	65.70	25.55	47.45	87.60	25.55	62.05	32.85	−51.10	73.00	−51.10	59.62	55.27	31.76
(1, 200)	65.70	29.20	29.20	80.30	58.40	87.60	25.55	−73.00	80.30	14.60	58.40	61.53	39.79

Tabella 4: questa tabella riporta i rendimenti medi del tasso percentuale annualizzato utilizzando la convenzione di 365 giorni in un anno poiché il mercato delle criptovalute opera ogni giorno durante un anno. Il campione chiamato *"10 coins"* contiene dieci criptovalute *privacy*: Dash (DASH), Bytecoin (BCN), DigitalNote (XDN), Monero (XMR), CloackCoin (CLOAK), Aeon (AEON), Stealth (XST), Prime-Xi (XPI), NavCoin (NAV), Verge (XVG). Il campione chiamato *"3 coins"* contiene le criptovalute *privacy* con la capitalizzazione di mercato maggiore: Dash, Bytecoin e Monero. Il campione chiamato *"7 coins"* contiene tutte le criptovalute *privacy* eccetto le tre aventi la più bassa capitalizzazione di mercato, cioè Stealth, Prime-Xi e Verge.

1.2 Conclusione

Lo studio effettuato in questo articolo analizza la redditività di indicatori tecnici che si basano sulla media mobile ((1, 20), (1, 50), (1, 100), (1, 200)) applicati su un set di dieci criptovalute che utilizzando la *"privacy function"*: indicatori che normalmente sono utilizzati nei mercati azionari. I risultati mostrano che la strategia basata sulla media mobile esponenziale ha successo solo nel caso della criptovaluta Dash (a livello singolo) e genera rendimenti annuali pari a circa 14.6% - 18.25% in più rispetto alla strategia *buy-and-hold*. Dall'altra parte però,

considerando le dieci criptovalute a livello aggregato, non si riscontra alcun rendimento positivo significativo a livello di portafoglio se comparato a uno uguale che utilizza la strategia *buy-and-hold.*

Lo studio, quindi, indica che, a livello di portafoglio, le criptovalute che si basano sulla *"privacy function"* sono fondamentalmente differenti da quelle che non lo fanno per quanto riguarda i loro *payoff*. Gli investitori dovrebbero prendere in seria considerazione questo aspetto quando devono applicare differenti strategie di trading nel mercato delle criptovalute.

2. MODELLO *STOCK TO FLOW*

Il modello *Stock to Flow* (SF o S2F) è un modo per misurare l'abbondanza di una particolare risorsa. Il rapporto *Stock to Flow* è la quantità di risorsa presente nelle riserve divisa per la quantità che viene prodotta all'anno.

Questo modello è generalmente utilizzato in ambito delle risorse naturali. Prendendo in esame l'oro, per esempio, sappiamo che secondo il *World Council*[28] sono state estratte circa 190.000 tonnellate di oro nella storia fino ad oggi. Questa quantità (fornitura totale) è quello che si può anche chiamare *stock*. Si stima, inoltre, che circa 2.500 – 3.000 tonnellate di oro vengono minate/estratte ogni anno; quindi, tale quantità si può anche chiamare il *flow*.

Il rapporto tra queste due quantità è un valore che ci viene fornito da quante nuove unità di una data risorsa entrano nel mercato ogni anno, in relazione alla fornitura totale. Maggiore è il rapporto Stock to Flow, meno sarà la nuova fornitura che entra nel mercato in relazione al totale. Un asset con un rapporto S2F più alto dovrebbe, in teoria, mantenere il suo valore in modo efficace nel lungo termine.

Al contrario, i beni di consumo e i prodotti industriali hanno generalmente un rapporto Stock to Flow basso; dato che il loro valore deriva tipicamente dalla loro distruzione o consumo, le scorte (lo *stock*) sono sufficienti solo a coprire la domanda. Queste risorse generalmente non hanno un alto valore come proprietà, quindi hanno la tendenza a non risultare buoni asset di investimento. Salvo casi eccezionali (il prezzo potrebbe aumentare rapidamente se si dovesse prevedere una mancanza nel futuro) la produzione di questi beni normalmente rimane al passo con la domanda.

Si premette che la scarsità da sola non implica che una risorsa sia preziosa (l'oro non è così raro dato che ne abbiamo già 190.000 tonnellate); un bene è prezioso perché la produzione annuale rispetto alla fornitura esistente è relativamente esigua e costante, stando al rapporto Stock to Flow.

[28] *World Council of Credit Unions:* è la principale associazione commerciale internazionale e agenzia di sviluppo per le unioni di credito e le istituzioni finanziaria cooperative.

2.1 Rapporto Stock to Flow dell'oro

Storicamente, l'oro ha avuto il rapporto Stock to Flow maggiore tra tutti i metalli preziosi. Ma qual è la cifra esatta? Se si riprendono i dati sull'oro citati nel paragrafo precedente e dividiamo la fornitura totale di 190.000 tonnellate per 3.500 otteniamo un rapporto Stock to Flow circa di ~54. Tale dato indica che ci vorranno circa 54 anni per minar 190.000 tonnellate di oro, al tasso di produzione attuale. Se si diminuisse la produzione annua (il *flow*) a 3.200 il rapporto S2F scenderebbe a circa 59.
Il valore totale di tutto l'oro estratto nella storia (questo concetto può essere paragonato alla capitalizzazione di mercato delle criptovalute) ad un prezzo di circa $1500 per ogni oncia di oro è di circa $9 trilioni.

	Stock (tn)	Flow (tn)	SF	supply growth	Price $/unit	Market Value
gold	190,000	3,500	54	1.8%	$ 1,425	$ 9,476,250,000,000
diamonds	2,812	150	19	5.3%	$ 533	$ 1,500,000,000,000
silver	71,000	25,000	3	35.2%	$ 16	$ 39,760,000,000
palladium	244	215	1	88.1%	$ 1,488	$ 12,707,520,000
platinum	86	229	0.4	266.7%	$ 844	$ 2,532,000,000

Fig.10. dati relativi al valore totale (stock) e alla produzione annua (flow) dell'Oro, Diamanti, Argento, Palladio e Platino.

L'oro ha lo SF pari a 54, ci vogliono quindi 54 anni di produzione attuale, per terminare l'intero ammontare presente sulla Terra (chiaramente l'oro non finirà tra 54 anni in quanto, molto probabilmente, il prezzo aumenterà in modo da eguagliare domanda e offerta). Il diamante è il secondo con un SF pari a 19. L'argento e il palladio hanno SF appena superiore a 1, mentre il platino è pari a 0.4. Le scorte esistenti di solito sono uguali o inferiori alla produzione annuale, rendendo la produzione un fattore molto importante. È quasi impossibile per le materie prime ottenere uno SF più alto, perché non appena qualcuno le accumula, i prezzi aumentano, la produzione aumenta e il prezzo scende di nuovo.

2.2 Stock to Flow e Bitcoin

Questo modello tratta I bitcoin come se fossero risorse naturali, come l'oro e l'argento. Questi ultimi due vengono spesso definiti come risorse che fungono da riserva di valore e quindi, in teoria, dovrebbero mantenere il loro valore a lungo termine per via della scarsità relativa e del *flow* basso. Per di più, risulta difficile aumentare in modo significativo la fornitura in un breve periodo di tempo, a causa del processo di ricerca.

Se si paragona bitcoin all'oro troviamo delle somiglianze:

- È scarso;
- Relativamente costoso da produrre;
- Fornitura massima limitata a 21 milioni di unità;

per di più la fornitura di bitcoin è definita a livello del protocollo, cosa che rende il *flow* completamente prevedibile (gli *halving* di bitcoin, cioè la fornitura che entra nel sistema viene dimezzata ogni 210.000 blocchi circa ogni quattro anni).

La combinazione di queste proprietà crea una risorsa digitale scarsa con caratteristiche profondamente valide per mantenere valore a lungo termine.

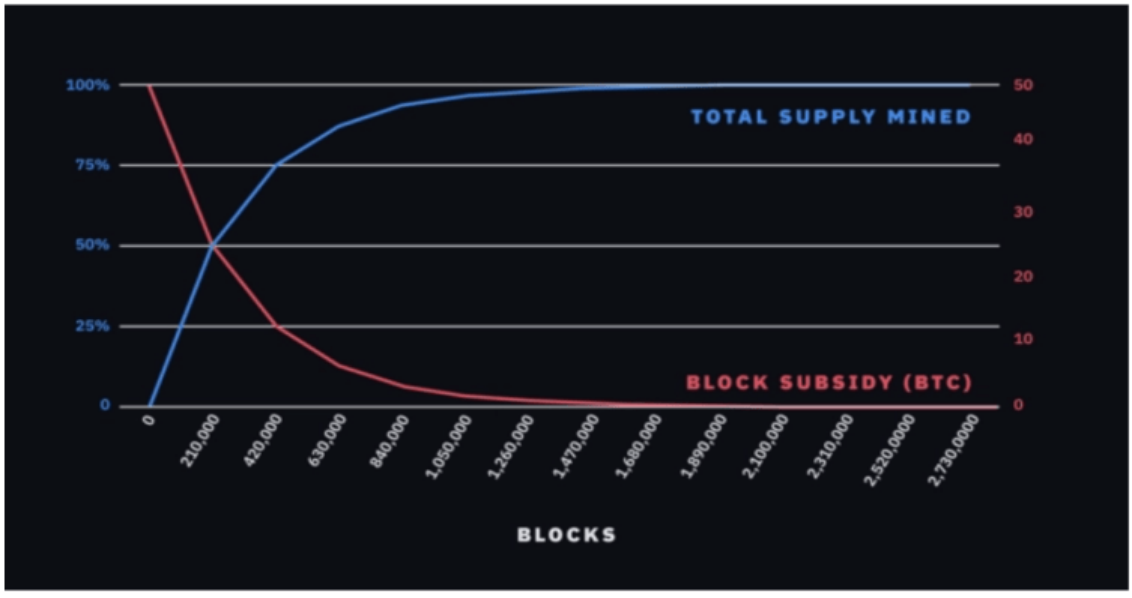

Fig. 11. Fornitura totale minata BTC(%) e Block Subsidy(BTC)[29]

In base al modello, il prezzo di bitcoin dovrebbe aumentare notevolmente nel tempo a causa del suo rapporto Stock to Flow costantemente ridotto.

[29] *Block subsidy*: ammontare di nuovi bitcoin minati in ciascuno blocco.

2.3 Dati

La formula dello Stock to Flow applicata a Bitcoin è su base mensile e il valore va da dicembre 2009 a febbraio 2019. Il numero di blocchi mensili può essere richiesto dalla blockchain Bitcoin tramite Python/Rpc/bitcoind[30]. Il numero effettivo di blocchi minati è differente dal numero teorico dato che i blocchi non vengono prodotti esattamente ogni 10 minuti (nel 2009 si avevano meno blocchi del previsto a causa della poca conoscenza della tecnologia delle criptovalute). Dato il numero di blocchi minati al mese ed essendo nota la *block subsidy*, si riescono a calcolare sia lo *stock* che il *flow* di Bitcoin. C'è però un accorgimento che deve essere aggiunto alla formula del modello finale. Si stima infatti che durante il primo anno di vita di bitcoin (2009), Satoshi Nakamoto abbia minato circa 1 milione di bitcoin e, ad oggi, questi non sono mai stati spostati su un altro *wallet*. Non si sa se questi siano stati persi oppure semplicemente Satoshi stia ancora aspettando peer venderli, ma la cosa certa è che non sono ancora mai stati spostati. Si dovrà togliere quindi 1 milione di unità dalle 21 totali.

Per quanto riguarda i dati sui prezzi di bitcoin, questi sono disponibili da luglio 2010. Sono stati aggiunti i primi prezzi noti di bitcoin (1$ per 1309 BTC a ottobre 2009, la prima quotazione a 0,003 per BTC su BitcoinMarket a marzo 2010) e sono stati interpolati.

2.4 Modello

Nel modello sono stati usati valori e assi logaritmici per la capitalizzazione di mercato, perché questa si estende su 8 ordini di grandezza (da 10.000 a 100 miliardi di dollari). Con l'utilizzo di valori logaritmici o dell'asse anche per SF mostra una sorprendente relazione lineare tra *ln*(SF) e *ln*(capitalizzazione di mercato). Va precisato, inoltre, che viene utilizzato il logaritmo naturale (*ln* con base *e*) con il logaritmo *ln* (base 10), si avrebbe avuti risultati simili.

[30] Python/Rpc/bitcoind: programmi utili per scaricare le stringhe di file che danno informazioni sui blocchi di Bitcoin, a partire da quanto è stato creato.

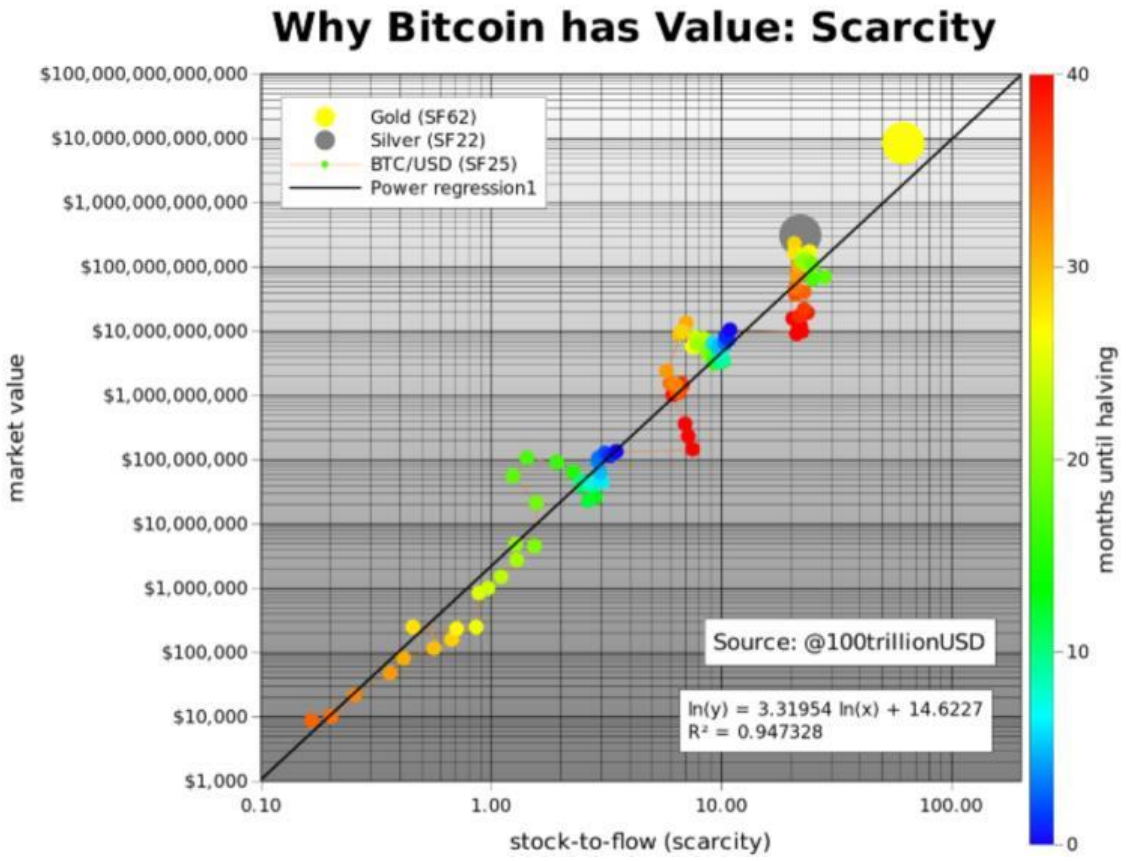

Fig. 12. La capitalizzazione di mercato dell'oro, dell'argento di Bitcoin stanno tutti sulla stessa retta, stando al modello SF. I punti precedenti all'*halving* (blu) e quelli immediatamente successivi (rossi) sono separati da un improvviso cambio di regime dello SF cui segue un altrettanto rapido riaggiustamento del prezzo.

Nella Fig.12 possiamo osservare che il *fit*[31] di una regressione lineare applicata ai dati dà conferma a quello che si può vedere a occhio nudo: abbiamo una relazione lineare statisticamente significativa tra SF e il valore di mercato ($R^2 = 95\%$, livello di significatività di $F = 2.3E-17$, $p - value = 2.3E-17$). La probabilità che la relazione tra SF e il valore di mercato sia data da un caso è vicina allo zero. Ci sono comunque fattori esterni quali regolamentazioni, *hack* e altre notizie che possono influire sul modello, per questo motivo abbiamo un $R^2 = 95\%$ e non superiore. Tuttavia, il fattore dominante risulta essere la scarsità, ovvero il rapporto SF.

[31] *Fit*: espressione gergale che indica genericamente l'adeguamento dei dati al risultato della variabile endogena.

Una conferma di validità del modello è che l'oro e l'argento, che hanno mercati totalmente diversi, sono allineati (punti grigio e oro nella Fig.12) con i valori di bitcoin stimati col modello SF.

Nella figura che segue è stato tracciato il prezzo di bitcoin secondo il modello SF (nero)ed il prezzo reale di bitcoin nel tempo, con il numero di blocchi come sovrapposizione di colore.

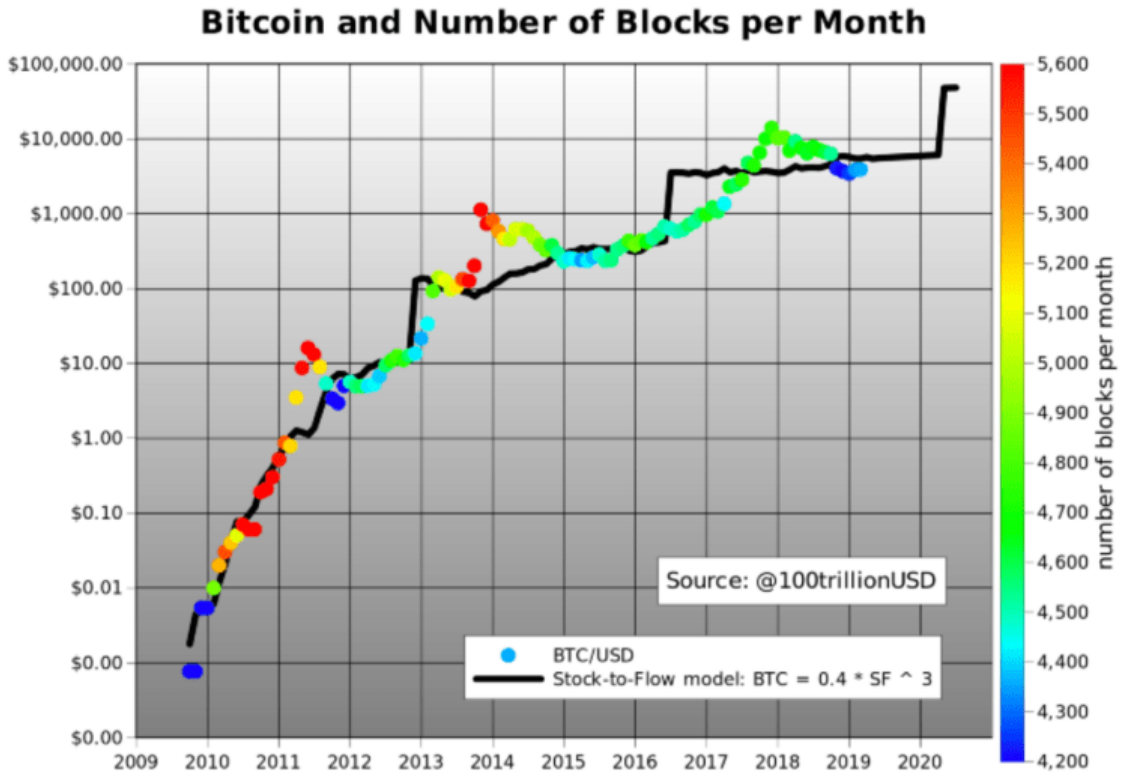

Fig. 13. Il prezzo del bitcoin secondo il modello SF (linea nera) ed i prezzi realizzati (colorati a seconda del numero di blocchi minati nel corrispondente mese).

Nella fig. 13 si nota la bontà del *fit*, in particolar modo l'adeguamento del prezzo quasi immediato dopo essere avvenuto l'*halving* di novembre 2012. Per quanto riguarda l'adeguamento dopo l'*halving* di giugno 2016 è stato più lento, probabilmente a causa della concorrenza della criptovaluta Ethereum, e della vicenda di DAO, che portò ad un *hackeraggio* del sistema Ethereum pari a circa 50 milioni di dollari. Per quanto riguarda il numero dei blocchi, come detto anche prima, nel 2009 ne venivano creati pochi e questo lo possiamo riscontrare anche sul grafico (punti blu); questo vale anche per gli adeguamenti al ribasso della difficoltà di fine 2011, metà 2015 e fine 2018.

2.4 Rapporto Stock to Flow di Bitcoin

L'attuale fornitura in circolazione di Bitcoin è pari circa a 18 milioni di unità, mentre la nuova fornitura è pari a circa 0,7 milioni per anno. Al momento della scrittura, il rapporto S2F di bitcoin si aggira attorno a 44.7 (https://stats.buybitcoinworldwide.com/stock-to-flow/).

Così come è stata utilizzata la formula del modello Stock to Flow per l'oro, proviamo ad applicarla anche per bitcoin.

$$SF = \frac{stock}{flow} = \frac{18.000.000}{657.000}[32] = \sim 27$$

Se per l'oro lo S2F ci dava come risultato circa ~59, nel caso di bitcoin abbiamo circa ~27[33] anni di produzione per terminare lo stock, cioè l'ammontare totale (se si continuasse a generare 657.000 bitcoin all'anno). Questo numero sarebbe decisamente minore rispetto a quello dell'oro ma bitcoin è caratterizzato dagli *halving* e infatti, a maggio del 2020, quando è avvenuto effettivamente l'*halving*, lo S2F è salito a ~44.7, molto più vicino all'oro. Il prossimo *halving*, nel 2024, alzerà il numero a 113 anni poiché nuovamente verrà dimezzata la potenza di calcolo. Di seguito utilizziamo i dati fino a qui spiegati per determinare il prezzo di bitcoin in USD:

$$model\ price\ (USD) = exp(-1{,}84) * SF\ \hat{}\ 3{,}36[34]$$

se mettiamo il valore SF = 44.7 otteniamo il prezzo giornaliero di Bitcoin in dollari, secondo il modello.

$$exp(-1{,}84) * 44.7\ \hat{}\ 3{,}36 = \$55709.77[35]$$

[32] 1800 (bitcoin generati ogni giorno) * 365= 657000.
[33] Questo calcolo è stato fatto a Marzo 2019, ci è utile per controllare s effettivamente il calcolo è corretto e se si sta aggiornando in maniera efficiente.
[34] Il parametro riporta la "dimensione frattale". Per maggiori informazioni sui frattali, si può consultare: http://progettomatematica.dm.unibo.it/Infinito/pag2/2p1.html
[35] Calcolo eseguito il 20/05/2021

2.5 Conclusioni

Bitcoin risulta essere il primo bene digitale scarso che il mondo abbia mai conosciuto; è scarso come l'oro e l'argento ma può essere inviato attraverso Internet, satellite ecc.
Questa scarsità di bitcoin ha un valore e in questo articolo si è proposto un modello che potesse quantificarla: il modello *stock to flow*.
Esiste una relazione statisticamente significativa tra *stock to flow* e la capitalizzazione di mercato. La probabilità che la relazione tra valore di mercato di bitcoin e modello S2F sia casuale è vicina allo zero.

I seguenti fatti aggiungono fiducia al modello:

- Argento e oro, che hanno mercati totalmente diversi, sono in linea con il valore di bitcoin secondo il modello SF.
- Vi è la possibilità dell'esistenza di una relazione di potenza.

"Il modello prevede una capitalizzazione di mercato di bitcoin di 1000 miliardi di dollari dopo l'halving a maggio 2020, che si traduce in un prezzo di bitcoin pari a circa $55000".[36]
Effettivamente, a febbraio 2021 il prezzo di Bitcoin è arrivato ad avere un prezzo pari a $55000 e una capitalizzazione di mercato di 1000 miliardi.

[36]Articolo pubblicato il 22/03/2019 da Plan B, autore del modello Stock to Flow: https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25

CAPITOLO 4: DESCRIZIONE DELLE CRIPTOVALUTE SCELTE

1. SCELTA DELLE CRIPTOVALUTE E METODO DI DECISIONE

Molti tendono a confondere e ad indentificare Bitcoin con Blockchain dal momento che Bitcoin è la più importante forma di Blockchain.
Le esperienze e i vari progetti orbitanti attorno alla Blockchain si sono moltiplicate negli ultimi anni, anche e non solo nell'ambito delle *Criptocurrency*. Certi casi hanno dato alla luce progetti che non nascevano espressamente come nuove "monete virtuali", ma come progetti di Distributed Ledger Tecnology di tipo *Open Source* con diverse possibilità di sviluppo e utilizzo. Sorge spontaneo chiedersi però, come mai abbiano iniziato a svilupparsi tanti progetti che utilizzano una tecnologia simile a quella di Satoshi Nakamoto, cioè al Bitcoin. Un primo motivo è sicuramente legato alla totale innovazione e rivoluzione tecnologica apportata dal mondo delle criptovalute rispetto agli strumenti di pagamento tradizionali con annessi pregi e difetti. Sono stati proprio questi ultimi, infatti, a far nascere successivamente alla data del 18 agosto 2008[37] le centinaia di *Altcoin*[38], molte basate sulla tecnologia blockchain ma aventi obbiettivi differenti.

Tra le prime altcoin troviamo Namecoin (2011) nata con l'obbiettivo di creare un sistema di registrazione di domini decentralizzati[39]; in seguito sono nate GeistGeld[40] e Tenebrix[41], il cui obbiettivo è stato quello di modificare il tempo di uscita dei blocchi e hanno modificato l'algoritmo del mining. Non sempre rilasciare blocchi più velocemente implica un miglioramento della sicurezza del

[37] 18 agosto 2008: data in cui è stato notificato il Bitcoin per la prima volta all'atto di registrazione di bitcoin.org su *anonymousspeech.com*
[38] *Altcoin*: ovvero *alternative coin*, termine utilizzato per definire le criptovalute diverse dal Bitcoin.
[39] Domini decentralizzati: Il sistema dei nomi dei domini con i quali identifichiamo i siti web è molto vulnerabile alla censura e agli attacchi informatici. Namecoin è stato uno dei primi progetti open-source che ha avuto l'idea di decentralizzare il sistema di denominazione di internet**,** creandone alternativi che nessuno riesca a controllare. In questo modo gli attacchi che sfruttano le vulnerabilità dns (*domain name service*) e i governi che agiscono sui nomi di dominio per limitare la libertà di espressione, sono impossibilitati a portare a termine i loro raid.
[40] GeistGeld: https://bitcointalk.org/index.php?topic=42417.0
[41] Tenebrix: https://bitcointalk.org/index.php?topic=45667.0

sistema in quanto si potrebbe andare ad intaccare la decentralizzazione del sistema, e ciò avvantaggerebbe i miner di maggiori dimensioni.
Da questo punto di vista le altcoin sono definite anche come *bitcoin alternative*, perché la maggior parte di esse è volta a sostituire o migliorare almeno una caratteristica di Bitcoin.

Di seguito verranno descritte dettagliatamente 5 criptovalute: Ethereum, Ripple, Iota, Litecoin e Dash. La scelta di queste *altcoin* verte su un duplice motivo;

- da una parte sono quelle che hanno una maggior capitalizzazione sul mercato, infatti sono tutte nelle prime dieci posizioni su tutti gli Exchange[42] cripto-valutari. Questo significa che non c'è alcun pericolo di scalabilità all'interno della criptovaluta oppure di eventuali schemi piramidali;
- l'altro motivo per cui sono state scelte verte sul fatto che i progetti e gli obbiettivi a cui ciascuna di queste criptovalute ambisce sono tutti molto interessanti e ognuna apporta una forte ventata di innovazione in ambito finanziario e socioeconomico.

Dal punto di vista socioeconomico si avrebbe un miglioramento in termini di trasparenza da parte delle istituzioni bancarie nei confronti dei clienti e viceversa. Come viene sottolineato nell'articolo
"L'era delle valute virtuali: banche centrali, moneta e innovazione tecnologica" sul sito dell'IRPA (Istituto di ricerca sulla Pubblica Amministrazione):
"Le specifiche tecniche e giuridiche ne determinerebbero, poi, l'effettiva capacità di sostituire in maniera piena il denaro contante: mentre una valuta digitale concepita per una diffusione limitata potrebbe avere un uso circoscritto al regolamento delle transazioni all'ingrosso di determinate tipologie di asset finanziari tra gli operatori di mercato, una CBDC ad accesso pubblico generalizzato – all'estremo opposto – consentirebbe anche ai singoli cittadini di farne pieno uso attraverso wallet digitali, di fatto sostituendo (o integrando) la circolazione del denaro contante. In quest'ultimo caso, le implicazioni per la

[42] In questo caso si è tenuto conto dell'Exchange Binance https://www.binance.com/it, piattaforma tecnologica che permette uno scambio di criptovalute, o uno scambio di valute digitali con altre risorse, come il denaro *fiat* convenzionale o altre valute digitali.

politica monetaria e per il sistema bancario sarebbero estremamente significative, creandosi un rapporto sempre più diretto tra privati e istituti di emissione, con una ridotta esigenza di forme di intermediazione attraverso il circuito bancario-finanziario tradizionale."

Per quanto riguarda il versante finanziario Francesco Piras, uno dei massimi esperti di criptovalute e tecnologia blockchain sostiene che *"Ce ne sono diversi. La prima innovazione che mi viene in mente è la cosiddetta tokenizzazione dell'economia. I token in generale sono rappresentazioni digitali di valore. Le stesse criptovalute sono una particolare tipologia di token. Un'altra famiglia è quella dei security token che consentono, senza intermediari e con i margini di sicurezza descritti prima, di creare diritti di proprietà scambiali di qualsiasi bene. Quindi non solo quote azionarie o immobiliari ma anche, per esempio, quote di una singola opera d'arte. La disintermediazione può trovare però applicazione in tantissimi ambiti finanziari e per questo motivo si comincia già a parlare di finanza decentralizzata (DeFi[43]). Un caso rilevante è sicuramente quello dei prestiti. In questo caso attraverso la creazione dei cosiddetti smartcontracts (contratti intelligenti) al verificarsi di determinate condizioni vengono erogati prestiti tra privati (in questo caso sulla blockchain di Ethereum) senza la presenza di intermediari che possono bloccare o sottrarre le somme"*

[43] DeFi (Decentralized Finance): La Finanza Decentralizzata è una forma sperimentale di sistema finanziario che non si basa su intermediari finanziari centrali come broker, Exchange o banche e utilizza invece smart contract sulla blockchain.

2. ETHEREUM

Fig. 14. Logo https://ethereum.org/en/

Ethereum nasce nel 2013, grazie a Vitalik Buterin, sviluppatore e ingegnere informatico di origini russe, il quale ha saputo unire la competenza del programmatore a quelle tipiche del ricercatore nell'ambito delle *criptocurrency*. Grazie ad un'operazione di *crowdfunding* l'anno seguente riuscì a completare il programma alla base di Ethereum e lo rese pubblico e accessibile online.
Buterin è a tutti gli effetti il fondatore di Ethereum e nel 2014 si è meritato il premio World Technology Award, 'premio Oscar della tecnologia', per tale co-creazione (durante lo sviluppo del progetto è stato affiancato da un team composto da Mihai Alisie, Anthony Di Iorio, Charles Hoskinson, Joe Lubin e Gavin Wood) e invenzione.

2.1 COME FUNZIONA ETHEREUM?

Quando si parla di Ethereum la si può paragonare al più grande computer condiviso in grado di disporre di una grande potenza che si occupa di utilizzare la blockchain per sostituire le terze parti di Intenet; quelle che si occupano della

memorizzazione dei dati. Con Ethereum, inoltre, si passa dal concetto di *Distributed Database*[44] a *Distributed Computing*[45]*.*

È una piattaforma di tipo computazionale "remunerata" grazie a degli scambi che si basano su una *criptocurrency* calcolata in Ether. Alla base troviamo lo stesso principio sociale della condivisione, tant'è che grazie a questa piattaforma si può entrare e far parte della Rete permettendo così una soluzione che consente a tutti i partecipanti di disporre di un archivio di dati immutabile e condiviso comprendente tutte le operazioni attuate nel corso del tempo con la peculiarità che queste non potranno mai essere fermate, bloccate o censurate.

Ethereum è una "Programmable Blockchain"[46], progettata per essere flessibile e adattabile e allo stesso tempo per inventare in modo immediato e semplice nuove applicazioni; non si limita però a disposizione *operations* predefinite e standardizzate, ma permette ai suoi utenti di creare le proprie *operations*.

Si può quindi dire che è una Blockchain *Platform* che permette di dare vita a diverse applicazioni di Blockchain decentralizzate non necessariamente limitate alle sole *cryptocurrencies*.

2.2 COSA SONO I CONTRATTI ETHEREUM?

Si tratta di Smart Contracts che permettono la gestione di servizi contrattuali in modo sicuro e pubblico, grazie alla remunerazione che si calcola in Ether. Tra i servizi troviamo quelli legati alla registrazione di domini, servizi di *crowdfunding*, sistemi per gestione di copyright nell'ambito dei media. Di fatto chi partecipa al protocollo Ethereum dispone del *Ethereum Virtual Machine (EVM)*[47] in grado di

[44] *Distributed Database:* in informatica il database distribuito è un databse che si trova sotto il controllo di un database management system nel quale gli archivi di dati non sono memorizzati sullo stesso computer bensì su più elaboratori o nodi.

[45] *Distributed Computing:* si intende un "sistema distribuito" o "algoritmo distribuito" riferendosi a processi autonomi che sono eseguiti sullo stesso computer fisico ed interagiscono tra loro tramite il passaggio di messaggi. Non c'è una singola definizione di sistema distribuito quindi si usano le seguenti proprietà che sono da minimo comune denominatore:

- Esistono molte entità computazionali autonome, ciascuna delle quali ha una propria memoria locale;
- Tali entità "comunicano" tra loro con il passaggio di messaggi;

[46] *Programmable Blockchain:* piattaforma che non si limita allo sviluppo di operazioni predefinite ma consente agli utenti di attivare delle proprie operazioni: gli smart contracts

[47] Ethereum Virtual Machine (EVM): Ethereum è un sistema "*Turing* complete" che permette agli sviluppatori di creare applicazioni che girano sulla EVM utilizzando linguaggi di programmazione che fanno a loro volta riferimento a piattaforme tradizionali come JavaScript e Python. EVM opera in modo sicuro e protetto in modo completamente separato dalla Rete.

eseguire algoritmi su una rete globale basata sui nodi di tutti i partecipanti. Ciascun nodo (partecipante) compensa o è compensato con Ether.

2.3 CHE COSA SI INTENDE PER SMART CONTRACTS[48] IN ETHEREUM?

Grazie alla Blockchain Ethereum non serve un organismo centrale che autorizza le attività (smart contracts) poiché si possono vincolare le decisioni prese consensualmente nel network. L'obbiettivo di questi smart contracts è semplificare la burocrazia tutelando allo stesso tempo le parti coinvolte garantendo quindi l'integrità dei dati e delle informazioni. Uno smart contract si basa infatti su condizioni e clausole: esso si attiva nel momento in cui la realtà della situazione corrisponde alle clausole e alle condizioni predefinite nel contratto. Il contratto funzione in modo automatico, senza quindi coinvolgere intermediari fisici; i vantaggi che ne derivano sono molteplici:

- Indipendenza: non c'è bisogno di intermediazione;
- Risparmio: risparmio sui costi;
- Sicurezza: immunità ad attacchi data la protezione crittografica;
- Precisione: abbassamento del numero di errori;

I contratti intelligenti eseguono porzioni di codice che vengono interessate da una transazione; questi esercitano un controllo diretto sul proprio conto di valuta Ether e sul relativo valore il cui obiettivo è conservare traccia delle variabili in gioco, al fine di rendere garantita la tracciabilità e la trasparenza. Per transazione in questo caso ci si riferisce a un pacchetto di dati che contengono un messaggio diretto e un account esterno; grazie ai contratti intelligenti in Ethereum utilizzando un linguaggio di programmazione (linguaggio di programmazione "Solidity[49]" per gli smart contract su Ethereum) molto simile ai più comuni linguaggi (*Python,*

[48] Smart contracts in Ethereum (o contratti intelligenti); si chiamano contratti ma non devono essere redatti come quelli abitualmente utilizzati.
[49] Solidity: linguaggio di programmazione utilizzabile per scrivere linguaggi intelligenti; il suo utilizzo implementa contratti intelligenti su varie piattaforme Blockchain, tra cui Ethereum. Questo linguaggio permette altresì la scrittura codificata per la creazione di *token*, *ICO* e giochi sulla Blockchain.

C++, GO, R, Matlab, ecc.)[50] è possibile accedere alla EVM che li esegue mantenuta dalla rete stessa. La rete "fotografa" lo stato nel tempo sulla Blockchain di Ethereum, in questo modo risulta possibile tenere costantemente sotto controllo la corretta esecuzione del contratto fra le parti.
All'interno di una transazione tipo troviamo presenti:

- La firma del mittente;
- Il nominativo del destinatario del messaggio;
- La quantità Ether che è l'oggetto della transazione;
- Il valore pari alla commissione che il mittente paga per lo step computazionale;
- Il valore rappresentante il numero massimo di passaggi eseguibili nella transizione;

All'interno della rete, la valuta Ether serve per pagare lo stesso network per poter usufruire della potenza computazionale: in questo modo si assolve ad una duplice funzione, ovvero Ether come blockchain ma anche come criptovaluta necessaria per poter effettuare transazioni, cioè ricevere e inviare denaro per permettere agli smart contracts di poter circolare nel sistema.
Per quanto riguarda le caratteristiche del contratto queste sono differenti da quelle di un accordo scritto. Le parti in causa infatti sono vincolate senza alcuna possibilità di modificare il contratto, tuttavia è difficile scrivere sotto forma di codice tutti i possibili aspetti di una relazione contrattuale: per esempio, la logica del linguaggio di programmazione potrebbe non essere in grado di definire ed incorporare tutti i concetti legali astratti coperti da "forza maggiore" o dal "buon senso". Per di più quando si contratta con i clienti per via elettronica, le informazioni devono essere rese disponibili in maniera chiara, includendo il linguaggio o i linguaggi in cui l'accordo deve essere disponibile; a questi ultimi non è richiesto di capire il linguaggio dei *software*. Per questo motivo esistono due diverse tipologie di modello *smart contracts*:

[50] *Python, C++, GO, R, Matlab:* linguaggi di programmazione.

- Modello “esterno” in cui il codice non costituisce per intero l’accordo legale delle parti, ma automatizza l’esecuzione di alcuni suoi termini.
- Modello “interno” in cui il codice avrebbe l’obbiettivo di costituire solo una. Parte integrale di un contratto legalmente vincolante (piuttosto che la totalità del contratto) e sostituirebbe qualsiasi altra clausola scritta in linguaggio naturale.

Dal punto di vista della legge bisogna sottolineare che in Europa, dove le parti di uno smart contract legale sono localizzate in diversi Paesi, ma non hanno fatto una specifica scelta di legge, il Regolamento UE “Roma I” po' essere d’aiuto a una corte nel determinare la norma applicabile per questa nuova forma di contratto: i seguenti principi generali sono fissati nel *Regolamento Roma I*:

– *“Un contratto per la prestazione dei servizi deve essere regolata dalla legge del Paese dove il fornitore del servizio ha la sua residenza permanente.”*
– *“In caso di strumenti finanziari negoziati in un sistema multilaterale di negoziazione, “un contratto concluso all’interno di questo sistema multilaterale che mette insieme o facilita l’avvicinamento di interessi multipli di acquisto e di vendita negli strumenti finanziari, in accordo con regole non discrezionali e regolate da una singola legge, deve essere regolato da quella legge.”*
– *“Questi principi potrebbero essere applicabili per analogia ad altre aree. Per esempio, i diritti in rem (registrazione dei titoli o immobili) sono tipicamente connessi alla legge del Paese dove la proprietà è registrata o localizzata.”*
– *“La legge del Paese dove la parte che è tenuta “alla prestazione più caratteristica” ha la residenza permanente, si applicherà in casi residuali dove lo smart contract non è coperto da nessuno degli altri criteri, o dove si potrebbe applicare più di uno.”*
– *“I contratti eseguiti elettronicamente con i consumatori sono eseguiti dove il consumatore ha il suo indirizzo permanente.”*
– *“Dove non può essere determinato altrimenti, la legge del Paese più collegato allo smart contract potrà essere anche applicato.”*

Resta evidente il fatto che data la complessità tecnica degli smart contracts, la progettazione della Blockchain, l'interesse commerciale, il numero dei partecipanti e la portata giurisdizionale c'è bisogno di una rapida quanto chiara e completa regolamentazione a tutela di tutte le parti coinvolte.

2.4 COSA SONO GLI ETHER?

Utilizzando le risorse computazionali della rete i partecipanti a Ethereum sviluppano e gestiscono contratti lavorando su una rete peer-to-peer. L'uso di queste risorse viene remunerato con una speciale "moneta virtuale" denominata Ether, la quale ha due ruoli fondamentali: da un lato è essa stessa la potenza elaborativa necessaria per produrre i contratti e dall'altra parte rappresenta la criptovaluta che permette di "pagare" per la realizzazione dei contratti. In concreto Ether è rappresenta un *token* che vien trattato come *cryptocurrency exchanges* con il *ticker symbol* di ETC.
Ethereum conta poi su un *International Transaction Pricing Mechanism* denominato Gas che ha lo scopo di ottimizzare le risorse della rete, di prevenire lo spam e di allocare le risorse in modo proporzionato e corretto in funzione delle richieste.

3. LITECOIN

Fig. 15. Logo https://litecoin.org

Litecoin è una valuta di tipo cripto peer-to-peer che consente pagamenti istantanei a costi pari quasi a zero, a chiunque nel mondo. Litecoin è una rete di pagamento globale, open source, completamente decentralizzata senza alcuna autorità centrale. Litecoin offre tempi di conferma delle transazioni più rapidi e una migliore efficienza di archiviazione rispetto alla valuta a cui si ispira, Bitcoin. Viene creata nell'ottobre 2011 da un ex dipendente di Google, Charlie Lee che intuisce fin da subito il potenziale innovativo apportato dalle criptovalute e dalla loro peculiarità che si basa su un sistema totalmente decentralizzato.
Litecoin ha caratteristiche molto simili al Bitcoin, non a caso se la seconda è sempre più associata all'oro digitale questa è la sua controparte digitale, ovvero l'argento. Lo stesso Lee, infatti ha definito Bitcoin come una *brilliant invention* ma, nonostante ciò, ci sono diversi aspetti che rendono le due criptovalute differenti:

- Litecoin riesce a generare nuovi blocchi ad una velocità maggiore rispetto Bitcoin; un blocco viene creato ogni 2,5 minuti, 7,5 in meno rispetto a Bitcoin. Ciò implica che i tempi di mining sono quattro volte inferiori a quest'ultimo;

- La funzione dell'algoritmo di Proof of Work che utilizza Litecoin necessita di una minor memoria RAM rispetto a Bitcoin, questo permette ai miners di utilizzare anche computer di uso comune piuttosto che grandi calcolatori che solo società con grandi capitali possono permettersi. Come conseguenza Litecoin ha una potenza di hashing maggiore rispetto alla sua controparte BTC;
- Litecoin fa perno su tempi e costi di transazione nettamente inferiori; il tempo per una transazione tramite questa criptovaluta sono 20 volte più rapidi rispetto a Bitcoin;
- La crittografia del wallet di Litecoin permette di proteggere il wallet di ogni cliente in modo tale da poter visualizzare le transazioni e il saldo del conto, tramite inserimento della propria password necessaria per spendere Litecoin al fine di proteggere l'account da attacchi virus e *trojan*[51].

3.1 LIGHTNING NETWORK

Viene definite come protocollo che darà nuovo interesse e slancio a Bitcoin e alle altcoins rendendole più comode come mezzo di pagamento destinato alla massa. Bitcoin ha ancora notevoli problemi derivanti in particolar modo dalle capacità limitate della propria blockchain che non gli permettono di essere un valido e comodo mezzo per i micro-pagamenti.

Come primo aspetto c'è il problema del numero di transizioni, pari a circa 7 secondi per bitcoin. Come secondo aspetto abbiamo il problema delle fees; infatti, durante periodi di congestioni (periodi in cui c'è bassa frequenza di utilizzo di una certa criptovaluta), come accaduto nel dicembre del 2017, le fees da pagare ai miner per la conferma aumentano in maniera non indifferente. In quel periodo infatti se si pagava un caffè tramite Bitcoin la commissione arrivava a

[51] *Trojan* o *horse Trojan* ("cavallo di Troia", in italiano): è un tipo di *malware* (virus) in ambito informatico. Questo virus viene nascosto solitamente in un programma che apparentemente sembra essere normale e funzionante; per questo motivo non desta alcun sospetto nell'utente, eseguendolo o installandolo però si dà il permesso al virus di infettare un programma, un documento ecc.

costare anche 20€, diventando un sistema di pagamento più obsoleto e inutile che innovativo quale si presta ad essere.

Per questo motivo si è sviluppano negli anni un *layer* aggiuntivo da affiancare alla blockchain di Bitcoin, in modo da poter aumentarne scalabilità, usabilità, velocità e diminuire le spese di commissione. Litecoin è diventata fin da subito importante e innovativa in quanto Charlie Lee aveva intuito questo problema con Bitcoin e da subito aveva lavorato per inserire il Lightning Network all'interno della sua criptovaluta.

Una soluzione ai problemi sopracitati viene previsto da Lightning Network tramite l'utilizzo di alcune transazioni *off-chain*[52], quindi non trasmesse nella blockchain di Bitcoin. Questo significa che le transazioni che vengono ad eseguirsi sul canale dedicato avvengono istantaneamente, senza nessuna trasmissione alla Blockchain. A quest'ultima verrà inviata solo la transazione di apertura e di chiusura. Per di più con Lightning Network si ha una riduzione delle fees, che con Bitcoin, in periodi di bassa frequenza, diventano, come visto, molto ingombranti e dispendiose.

Il protocollo Bitcoin si costituisce in essenza da transizioni legate a transazioni precedenti e future. Ogni transazione ha degli ingressi che si riferiscono agli indirizzi da cui vengono inviati i Bitcoin, e le uscite, che si riferiscono agli indirizzi a cui vengono indirizzati. In aggiunta a questo passaggio, gli input devono includere i requisiti per inviare i Bitcoin, cioè le firme che dimostrano la proprietà degli indirizzi di input. Nel frattempo, gli output, stabiliscono i nuovi requisiti che devono a loro volta essere inclusi nell'input di una transazione successiva.

Una delle caratteristiche principali di Lightning Network consiste nel fatto che è costituita da transazioni Bitcoin più o meno regolari. Queste transazioni di solito non vengono trasmesse attraverso la rete Bitcoin. Infatti, esse vengono

[52] *Off-chain:* transazione di una criptovaluta che avviene al di fuori della Blockchain. Stanno diventano sempre più popolari a causa del fatto che garantiscono fees basse, se non pari a zero. Il vantaggio che propongono è che non implicano sempre l'*agreement* della maggior parte dei partecipanti alla Blockchain per effettuare una transazione, basta anche l'accordo e lo scambio dei dati personali dei due interessati al trasferimento.

memorizzate localmente nei nodi degli utenti, ma possono poi essere trasmessi in qualsiasi momenti attraverso la rete.

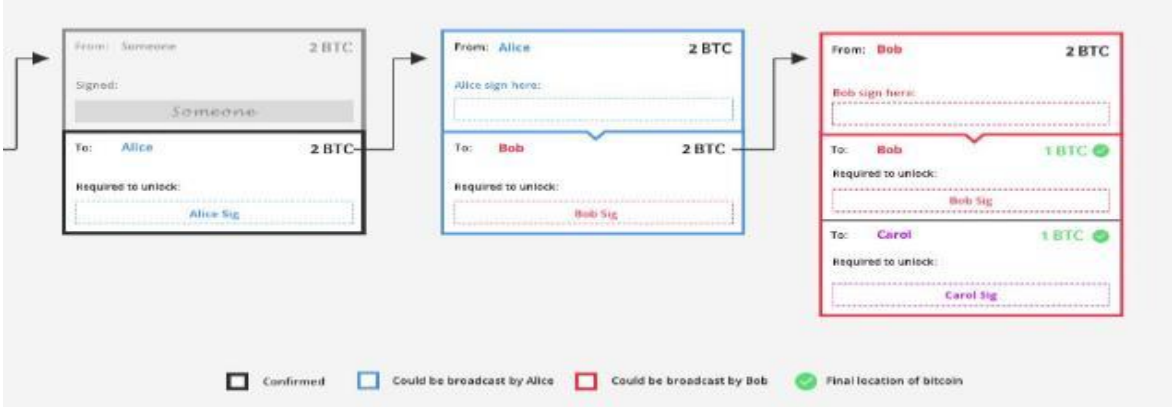

Fig.16. Esempio di transazione Off-chain

Nell'esempio che vediamo in figura, si nota come Alice possa firmare ed effettuare il *broadcast* delle transazioni non confermate, così da inviare due Bitcoin a Bob. Ma solo dopo che Alice avrà effettuato il *broadcasting* che Bob potrà mandare uno dei due Bitcoin ricevuti da Alice a Carol.

4. DASH

Fig.17. Logo https://www.dash.org

I fondatori di Dash sono Evan Duffield e Ryan Taylor, esperto di programmazione e intelligenza artificiale. Nel 2010 avevano intuito che i problemi quali velocità, privacy e velocità di transizione alla base di Bitcoin potevano essere affrontati. Così, dopo vari esperimenti, crearono la loro criptovaluta. Inizialmente chiamata Xcoin, successivamente Darkcoin, durante i periodi dei vari esperimenti, il 18 gennaio 2014 nasce ufficialmente Digital Cash o la meglio conosciuta Dash.
Dash è una criptovaluta decentralizzata che permette di effettuare transazioni sicure e private; sono tutte caratteristiche che fanno da pilastri per questa criptovaluta, gli stessi che furono criticati a Bitcoin nel 2010 da Duffield.

Un altro aspetto che caratterizza Dash è l'offerta di elevati standard di affidabilità e sicurezza. Caratteristiche quali commissioni medie pari a 0,0002 Dash su qualsiasi ammontare della transazione, e velocità di transazione mediamente pari a 2,5 minuti cadauna rendono questa criptovaluta molto *user-friendly* sia tra i consumatori ordinari che la utilizzano come metodo di pagamento o di scambio di denaro, sia tra i trader come oggetto di speculazione o investimento.

La fornitura totale di monete Dash progettate risale a 18 milioni; ad oggi, momento della stesura di questa tesi, l'ammontare è arrivato a circa 7,5 milioni[53]. Alla base del funzionamento di questa criptovaluta c'è un modello auto-finanziato, ovvero un modello che permette agli individui e alle imprese che apportano valore al network di essere "monetizzati", cioè essere pagati. Questa caratteristica si sviluppa su due livelli:

- Livello 1: processo di mining per la creazione di nuovi blocchi in cui i miner confermano direttamente le transazioni riportate sulla blockchain;
- Livello 2: processo che viene gestito dai *masternodes*, il cui compito è quello di occuparsi delle funzioni più sviluppate della criptovaluta, come la distribuzione dei pagamenti. I *masternodes* sono dei server che svolgono attività utili per facilitare le operazioni su questa blockchain.

4.1 COSA SONO I MASTERNODES?

Per masternodes si intende un server privato messo a disposizione di una criptovaluta, cioè offrire la garanzia di una fonte computazionale per minare o per approvare le transazioni di tale criptovaluta. La contropartita prevede un profitto per chi si impegna in questo "contratto" che solitamente si traduce con monete, in questo caso, per esempio, saranno monete Dash.
In poche parole, un masternode è un server con una copia completa della blockchain di Dash, che garantisce un certo livello minimo di prestazioni e funzionalità per eseguire determinate attività relative alla convalida dei blocchi, nonché PrivateSend e InstantSend, ovvero le funzionalità di privacy e transazione istantanea in Dash. I masternode vengono pagati per questo servizio, utilizzando un concetto noto come Proof of Service. I masternode possono anche votare su proposte di *governance* e finanziamento.

Chiunque può mettere a disposizione un masternode. L'obiettivo è avere una decentralizzazione sufficiente per garantire che nessuna singola persona

[53] https://www.blockchain4innovation.it

controlli una frazione significativa dei masternodes. Tuttavia, per evitare di “gonfiare” la rete con masternodes non necessari, c'è una condizione che deve essere soddisfatta: la prova della proprietà di almeno 1000 monete Dash. Non è necessario che le monete siano nel masternode, ma devono essere conservate in modo che sia trasparente per l'intera rete, bisogna darne prova dell’effettivo possesso. Se il proprietario sposta o spende quelle monete, il masternode smette di funzionare e il pagamento cessa.

Il mantenimento di un masternode genera rendimenti per ogni masternode-*owner*, tale che la ricompensa viene tripartita come di seguito:

- Il 45% della ricompensa del blocco viene pagato ai masternodes;
- Il 45% della ricompensa ai miner;
- Il 10% viene assegnato al sistema di bilancio del network in vista di sviluppi futuri;

Avere tanti server che contengono una copia completa della blockchain e che lavorano per la moneta può essere estremamente utile. Grazie al sistema di ricompensa, non c'è il rischio di non avere abbastanza masternode e gli sviluppatori possono fare affidamento su di loro implementando rapidamente qualsiasi nuova funzionalità decentralizzata che desiderano implementare. Dash è un sistema incentivato da migliaia di server distribuiti che lavorano 24 ore su 24, 7 giorni su 7. Ciò significa che Dash può scalare in modo più efficiente e distribuire i servizi più rapidamente. Più masternode, migliore e più sicura è la rete Dash.

In questo modo Duffield ha sviluppato la prima piattaforma di criptovaluta decentralizzata autosufficiente, organizzata come una Decentralized Autonomous Organization (DAO).

5. RIPPLE

Fig.18. Logo https://ripple.com

La criptovaluta Ripple (XRP) nasce nel 2013 all'interno di Ripple Labs, Inc. (società tecnologica americana, operante a San Francisco) ad opera di Chris Larsen e Jed McCaleb con l'esigenza di ovviare ad alcuni problemi riscontrati in Bitcoin tra i quali ma non solo: velocità di transazione e utilizzo limitato all'acquisto di beni e servizi. Al contrario di Bitcoin, Ripple è caratterizzato da natura bancaria e finanziaria e si pone l'obbiettivo di porre rimedio alle esigenze degli istituti bancari in quanto finanziari. Tant'è che le banche che si appoggiano sulla tecnologia di questo protocollo hanno un incremento della velocità nelle operazioni di transazione riuscendo a garantire la tracciabilità della criptovaluta stessa: garantisce transazioni efficienti ed economiche in tempo reale a chi ne usufruisce, in tutto il mondo. Tra le 15 banche più grandi che lavorano con Ripple possiamo nominare PNC Bank, una tra le prime dieci banche più importanti negli Stati Uniti.

Il funzionamento di Ripple ha una struttura "ternaria", ovvero si costituisce in:

- Un network di pagamento;
- Una criptovaluta, chiamata XRP;

Oltre questi tre elementi caratterizzanti la criptovaluta, bisogna sottolineare l'algoritmo su cui poggia l'intera rete e che disciplina gli scambi monetari; il *Ripple Consensus*, e il database su cui sono registrate e archiviate le informazioni: il *Ripple Consensus Ledger* (RCL). Grazie al RCL sia ha garanzia dell'immutabilità delle transazioni e vi è la capacità di tenere sempre sotto controllo gli scambi per poter concludere le transazioni nel più breve tempo possibile senza la necessità di alcuna presenza centrale.
Oltre a questo, con Ripple è possibile il trasferimento di denaro "senza continuità di forma" nel senso che si possono scambiare euro a un soggetto che potrà riceverli sotto forma di altra valuta, il tutto svolto nella rete RippleNet[54], (dollaro, sterlina, yen, etc.).

5.1 COME FUNZIONANO LE TRANSAZIONI?

Come si è accennato, le transazioni sono istantanee, irreversibili, caratterizzate da costi molto bassi e con una crittografia end-to-end[55]; ma di fatto come si articola una transazione utilizzando il protocollo Ripple?
Alla base troviamo una ferrea logica di fiducia che è garantita dai crediti *I Owe You* (IOU), cioè "sono in debito con te". La peculiarità di questi crediti è che sono la rappresentazione delle valute reali e sono inviati per poi essere ricevuti con l'obiettivo di essere successivamente convertiti in valute fiat all'interno del *gateway* Ripple. Il denaro non viene trasferito in modo fisico ma tramite il passaggio per il registro delle transazioni (Ledger) tracciando quindi gli spostamenti e verificando la somma promessasi vicendevolmente. Coloro che si occupano di accettare i depositi da parte di vari nodi della rete, gli utenti, definiscono anche il saldo dei debiti e dei crediti, e quindi raccolgono eventuali commissioni nel momento in cui si ha il riscatto di una moneta.

[54] RippleNet: "spina dorsale" per tutti i servizi e prodotti offerti da Ripple agli istituti di credito che vi si appoggiano.
[55] Crittografia end-to-end (E2EE): (letteralmente da un estremo all'altro) si basa su un sistema di comunicazione cifrata all'interno del quale solo le persone che stanno comunicando possono leggere i messaggi. In questo modo si evita che terzi parti, tra cui gli stessi *Internet Service Provider* e i gestori delle reti di telecomunicazione, possano leggere o provare ad alterare i messaggi che due soggetti si scambiano.

Relativamente a questo aspetto, i *gateway* hanno il compito di creare un quadro completo dei clienti con cui entrano in contatto rispettando le leggi antiriciclaggio vigenti in tale materia.

Ripple, spesso sotto la definizione "la cryptocurrency delle banche" rende semplice l'attività bancaria riuscendo a trasferire di grandi somme di denaro senza che questo siano spostate fisicamente con l'alternativa di. poter effettuar scambi con valute fiat senza il pagamento di commissioni. Detto questo però c'è da dire che XRP è l'unica valuta a poter circolare nella rete Ripple e anche l'unità di misura alla base dello scambio dei crediti IOU. È necessario quindi che al momento dello scambio, il destinatario della transizione acquisti i crediti IOU dell'emittente per una data quota di Ripple, nel caso in cui si stessero scambiando sterline ma si avessero a disposizione solo euro. In seguito, il destinatario avrà la possibilità di vendere quei crediti per un'altra valuta reale al fine di poter ottenere altri Ripple. A garanzia di tutti i passaggi e transazioni c'è il Ledger.

5.2 MARKET MAKER

All'interno del sistema Ripple i market maker hanno il compito di garantire che sulla rete ci sia presente una quota minima di liquidità di token XRP[56] in modo da permettere lo scambio della quantità desiderata, che abbia bassi livelli dei costi di commissione e che sia indipendente dalla coppia di valute considerate. Più precisamente una valuta (euro, dollaro, yen, sterlina, ecc.) di input viene scambiata per il token XRP prima di. una transazione e trasmessa sulla rete. Quando arriva al destinatario, viene scambiato con la valuta originale (euro, dollaro, yen, sterlina, ecc.).
I market maker sono tipicamente delle aziende garanti della fluidità dei mercati finanziari tramite la vendita o l'acquisto di grandi volumi in asset. Quindi, i market

[56] Token XRP: vengono utilizzati come elemento regolatore della valuta e per pagare le commissioni di transazione. Ogni transazione ha una commissione pari a circa 0,00001 XRP, per evitare spam nella rete Ripple. È stato emesso un totale di 100 miliardi di XRP proprio per garantire liquidità durante le transazioni. Il token XRP è indipendente dall'organizzazione Ripple Labs, quindi anche in caso di chiusura o fallimento di quest'ultima i token XRP continueranno a svolgere le proprie funzioni.

maker detengono un certo numero di asset tramite cui possono fare trading, in particolar modo nel mercato azionario. Per di più hanno il compito di stabilire sia il prezzo di acquisto che quello di vendita, cioè possono “fare mercato”, cercando di assicurare il. Funzionamento del mercato in modo che si creino dei flussi di cassa disponibile per gli investitori che operano in esso.
Il margine di profitto che i market maker hanno è determinato dallo *spread* tra il *bid price* e l’*ask price*[57]*.* Questo stesso criterio che vale sia per i tradizionali mercati azionari vale anche all’interno della reta Ripple.

Per quanta riguarda la quantità di monete XRP, ce ne sono in circolazione 100 miliardi che sono distribuiti da OpenCoin[58] e non come avviene per il BTC, tramite il *mining*. Quindi, non essendoci il tramite dei *miner,* si ottiene questa valuta tramite il conferimento al *server* Ripple di potenza computazionale dei computer. Le monete appartengono ai Laboratori Ripple e infatti la tecnologia utilizzata si basa sulla blockchain in maniera decentralizzata. Si elencano di seguito le sue peculiarità che la rendono tra le prime cinque criptovalute più importanti in base alla capitalizzazione di mercato:

- Assenza di un ente centrale, quindi transizioni dirette tra i nodi;
- Elevata distribuzione;
- Tracciabilità delle transizioni;
- Riconciliazione automatica: sistema garante che l’ammontare uscito da un e-wallet corrisponda ai soldi reali spesi dal conto in oggetto.

Essendo una valuta scalabile, con Ripple possiamo avere fino a 150 transazioni al secondo. Detto ciò, con nessuna criptovaluta, se non con Ripple, esistono delle divergenze tanto grandi da Bitcoin, in particolar modo:

- Bitcoin è alternativo il sistema bancario, mentre Ripple ha natura finanziaria;

[57] *Bid-ask spread:* si tratta della differenza tra il prezzo che il venditore vuole per un titolo (*ask*) e quello che l’acquirente è disposto a pagare per tale titolo (*bid*). Viene spesso usato come misura della liquidità del mercato.
[58] OpenCoin: Il progetto OpenCoin è relativo al "denaro digitale". Tramite OpenCoin si sviluppa un protocollo per utilizzare il contante elettronico nella vita quotidiana. Per questo è stato sviluppato anche un sistema composto da software di conio, software per wallet e tutto ciò che è necessario per avere un sistema per transazioni elettroniche anonime.

- Ripple impiega dai 2 ai 5 secondi per una transazione mentre Bitcoin impiega anche 10 minuti;
- Bitcoin ha una quota massima di coin fissata a 21 milioni, mentre Ripple a 100 miliardi;
- Con il sistema BTC si riescono a tracciare solo i movimenti Bitcoin, mentre con Ripple è possibile tracciare qualsiasi asset;
- Bitcoin gestisce globalmente un massimo di 7 transazioni al secondo, mentre con Ripple si arriva ad effettuarne fino a 1500 nello stesso arco temporale;
- Elevata velocità nelle transizioni di Ripple significa costi più bassi nello scambio delle stesse, a differenza di Bitcoin;
- Bitcoin è un sistema decentralizzato mentre Ripple si presta al servizio di istituti bancari in quanto, sfrutta la tecnologia blockchain, e propone una rapida e sicura soluzione agli scambi interbancari. Anche se è nato come sistema centralizzato è riuscito nella decentralizzazione grazi alla diversità del nodo validatore Ripple Consensus Ledger (RCL);
- Se per Bitcoin il *mining* è fondamentale, ciò non vale per Ripple poiché è stato alimentato con 100 miliardi di XRP;

Se Bitcoin si rivolge ad un utilizzo più “quotidiano” nella nostra vita, Ripple cerca di dare un valido appoggio finanziario a tutto il sistema bancario tramite l’utilizzo della blockchain technology.

6. IOTA

Fig. 19. Logo https://www.iota.org

Iota è un token crittografico[59] creato da David Sonstebo, Sergey Ivancheglo, Dominik Schiener e Dr. Serguei Popov nel 2015, la cui Fondazione senza scopo di lucro ha sede a Berlino, in Germania.

Al contrario delle altre criptovalute, Iota nasce con l'obbiettivo di essere "*lightweight"* (caratteristica che la contraddistingue da altre criptovalute, basate tutte su blockchain gravose e complesse) ed essere utilizzata per il mondo IoT (*Internet of Things*) quindi per poter effettuare micro-transazioni tra *smart device*[60] per lo scambio dei dati.

Tramite una ICO, avvenuta nel 2015, che ha portato a una raccolta fondi di 1337 Bitcoin (circa $400.000,00, in base alla media prezzo BTC di quell'anno) il team IOTA ha iniziato a lavorare con l'obbiettivo di trovare una soluzione al problema del regolamento transattivo per l'IoT, date le mancanti soluzioni ad oggi disponibili.

[59] Token crittografico: si tratta di un generatore di codici numerici pseudocasuali a intervalli regolari (uno a distanza di pochi secondi dall'altro) in base ad un algoritmo che tiene conto sia dei codici da generare sia del tempo da intervallare (grazie ad un orologio interno). Altri fattori che. Influenzano l'algoritmo possono essere il numero di serie dei token o altri elementi associati al possessore all'atto della consegna del token.

[60] *Smart device:* dispositivo elettronico che può essere collegato ad altri dispositivi tramiti diversi protocolli quali Bluetooth, Zigbee, NFC, Wi-Fi, LiFi, 3G, etc.

Il funzionamento di questa criptovaluta non si appoggia alla blockchain, bensì su un protocollo software basato su Directed Acyclic Graph (DAG)[61], che è parallelo ma diverso dal sistema a blocchi della blockchain. È un approccio innovativo e prende il nome di Tangle, cioè "groviglio". Ci sono aspetti molto comuni a quello già osservato relativamente alla blockchain, mentre altri sono totalmente differenti.

Per quanto riguarda le somiglianze abbiamo che entrambi:

- Hanno database distribuiti;
- Vengono retti da una rete P2P;
- Si strutturano sul consenso e su un meccanismo di validazione delle transazioni;

Per quanto riguarda invece i punti di divergenza, questi sono:

- Tangle non possiede alcun blocco, miner o catena;
- Le transazioni vengono processate in parallelo e non in serie come avviene per la blockchain;

Fig.20. Differenza di protocollo software tra Tangle (IOTA, in cui si ha il "groviglio", ovvero transazioni processate in parallelo) e blockchain (in questo esempio utilizzato per Ethereum, in cui abbiamo l'aggiunta dei blocchi in sequenza)

Non essendoci il processo che si basa sul mining, spetta ad ogni utente che fa parte del *network* verificare la veridicità delle due transazioni precedenti alla sua e solo in seguito può inoltrare la sua nel circuito. Tale "referenziazione" della

[61] Directed Acyclic Graph (DAG): struttura dati non avente cicli diretti, ovvero utilizzando qualsiasi vertice del grafo non è possibile ritornarci percorrendo gli archi del grafo.

transizione assume il ruolo di attestazione in quanto con la transazione si attesta direttamente che le due transazioni precedenti sono validate. Il consenso con IOTA, quindi, diventa una parte intrinseca al processo transattivo ed è anche questa peculiarità a permettere l'abbattimento dei costi delle *fees*.
La riduzione di *fees* è dovuta al fatto che si utilizza il sistema *Proof of Work*[62] (*PoW*) tramite la quale si verifica la propria transizione e quella delle altre precedenti all'interno del network.
Questo comporta che all'aumento degli utenti su Tangle e al numero delle transazioni aumenta anche la *Proof of Work* eseguita da questi ultimi per la verifica delle transazioni, senza quindi dover ricorrere ai minatori.
Il meccanismo di validazione delle transazioni si può delineare nel seguente modo:

- Firma delle transazioni attraverso chiave privata;
- Attraverso l'uso di un metodo casuale si trovano in modo casuale due transazioni non ancora confermate che saranno poi referenziate dalla transazione;
- Tramite la *Proof of Work* la transazione verrà accettata dalla rete e trasmessa dal network.

IOTA, come altre criptovalute (Bitcoin, Ethereum, Litecoin etc.), è scalabile, e dal momento che non si divide in intervalli sequenziali come la Blockchain, la rete riesce a crescere e scalare in modo dinamico al pari del numero delle transazioni al proprio interno: più sono gli utenti a fare uso della tecnologia IOTA, più la rete è rapida, solida ed efficiente. Allo stesso tempo anche The Tangle è decentralizzato: bisogna avere l'approvazione di più nodi per poter validare una transazione, e lo storico di quest'ultimo deve essere condiviso.

[62] *Proof of Work (PoW):* è una misura poco costosa per scoraggiare attacchi *denial of service* e altri abusi del servizio, come lo spam sulla rete, che si traduce in "lavoro" da parte del richiedente del servizio, ovvero del tempo di elaborazione di un computer.

6.1 L'IMPORTANZA DEL COO IN IOTA

Questa figura è presente per evitare problemi quali il *double spending* nell'utilizzo della rete IOTA fino al momento in cui non avrà abbastanza potenza di *hashing* per essere considerata sicura e per poter definitivamente allontanare l'ombra del *34% attack*. Stefano della Valle, parte del team IOTA Evangelist Network, definisce il Coordinatore (COO): "Il Coordinatore non ha potere di firmare le transazioni altrui, quindi non può commettere frodi; le chiavi private non sono gestite o gestibili dal coordinatore; il COO non ha alcuna funzione di controllo dei nodi e non conferma le transazioni modificando in qualche modo lo stato del *ledger*[63]. Il COO ha funzione di convalida: se le transazioni sono approvate da questo nodo, esse sono necessariamente uniche e valide. Quindi il Coordinatore non minaccia la decentralizzazione del network sia perché, successivamente, sarà disattivato o la sincronizzazione sarà facoltativa sia perché il suo operato è controllato e approvato da tutti i nodi della rete."[64]

[63] Ledger: libro mastro delle criptovalute
[64] Intervista a Stefano delle Valle: https://cryptonomist.ch

CAPITOLO 5: INDICATORI TECNICI

1. CHE COSA SI INTENDE PER MEDIA MOBILE?

La media mobile è un indicatore che viene utilizzato per analizzare le serie storiche. Essa è utile nell'analisi tecnica in quanto mostra il valore medio di un prezzo in un certo intervallo di tempo.

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

- m_1 il numero dei periodi precedenti a t;
- m_2 il numero dei periodi successivi a t;
- θ_1 Il peso da attribuire all'i-esimo valore osservato

Si definisce media mobile al tempo t il valore:

$$mm_t = \sum_{i=-m_1}^{m_2} \theta_i \, \varphi_{t+1},$$

dove $m_1 + m_2 + 1 = k$ è il periodo, o l'ordine della media mobile.
Una media mobile si classifica in:

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

Considerando dunque una media mobile a 20 periodi, con il termine "mobile" ci si riferisce al fatto che ogni volta che si aggiungerà un nuovo prezzo, il più vecchio non verrà più considerato. Per quanto riguarda il grafico, la media mobile è utile perché mette in rilievo la direzione del trend attenuando le fluttuazioni del prezzo che possono confondere nell'interpretazione del grafico stesso. Il calcolo della

media mobile funziona in modo semplice: dato un tempo t il numero delle osservazioni rimane costante in tale tempo, mentre il valore della media viene aggiornato attraverso un algoritmo che procede eliminando di volta in volta il valore più vecchio (utilizzato per il calcolo relativo al tempo $t - 1$) e introducendo quello più recente.

I tipi di media mobile più utilizzati sono la media mobile semplice, la media ponderata e la media esponenziale. Differiscono tra loro in base alla formula del calcolo che può risultare più o meno sensibile alla variazione di prezzo. Di seguito si farà la descrizione di ciascuno.

1.1 MEDIA MOBILE SEMPLICE

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

$$SMA = \frac{i}{N}\sum_{i=1}^{N} C_i$$

Dal punto di vista grafico questa corrisponde a una curva che attraversa le candele del grafico[65] e ne indica il trend corrente. Questa indica la direzione del grafico (*uptrend, downtrend* ecc.).
Un altro utilizzo della media mobile semplice è quello dell'"incrocio": infatti basta prendere in considerazione due SMA differenti, una di breve periodo (solitamente quelle a 25 o 50 periodi) e una di lungo periodo (solitamente quella di 200 periodi) e si va ad analizzare cosa succede una volta che avviene un loro incrocio. Se

[65] Candela giapponese (candlestick): viene utilizzata per visualizzare dati sui grafici, prevalentemente in ambito finanziario. Per costruire un grafico a candele sono necessari i valori di apertura, massimo, minimo e chiusura (*Open, High, Low, Close*) di un titolo o di un bene negoziato su un mercato.

l'incrocio tra la curva della SMA(200) e la SMA(50) volge verso l'alto, si tratta di un'indicazione che il trend del prezzo del titolo o della criptovaluta sottostante è in salita ed è quindi consigliato aprire posizioni l*ong* (*buy)*. In caso contrario se l'incrocio tra le due SMA appena citate volge verso il basso, c'è da aspettarsi un *downtrend* ed è quindi utile considerare posizioni *short* (*sell*). Il grafico seguente chiarisce quanto appena descritto: possiamo osservare che quando la Media Mobile(20) in verde "taglia" la Media Mobile(100) in rosso, il prezzo della criptovaluta Bitcoin diminuisce (in questo caso il suo valore è diminuito da 8.000$ a 4.000$ circa); al contrario, quando la Media Mobile(20) in verde "taglia" verso l'alto la Media Mobile(100) in rosso, il valore di Bitcoin aumenta da poco più di 8.000$ a circa 10.000$.

Fig.21. Incrocio al ribasso e al rialzo con l'utilizzo di media mobile semplice a 20 periodi (verde) e a 100 periodi (rosso).
Fonte: https://demo-deal.ig.com/wtp/#/workspace/NWY3MDczMmQwZTcxNTRiOTY0NGNiYzky

1.2 MEDIA MOBILE PONDERATA

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

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

$$WMA = \frac{C_1*1+C_2*2+\ldots+C_n*n}{1+2+\ldots+n};$$

nella Fig.18 possiamo osservare il confronto tra media mobile ponderata a 20 periodi in viola e la media mobile semplice a 20 periodi in verde. La WMA(20) risulta seguire la curva dei prezzi con maggior accuratezza rispetto alla SMA(20), cioè quando il prezzo di Bitcoin aumenta o diminuisce è molto più rapida a seguirne il trend;

Fig.22. Incrocio al ribasso e al rialzo con l'utilizzo della media mobile ponderata a 20 periodi (viola) e a 100 periodi (blu).
Fonte: https://demo-deal.ig.com/wtp/#/workspace/NWY3MDczMmQwZTcxNTRiOTY0NGNiYzky

1.3 MEDIA MOBILE ESPONENZIALE

Anche la *Exponential Moving Average*, EMA, viene utilizzata per superare le imperfezioni della media mobile semplice. Il vantaggio delle Medie Mobili Esponenziali si basa sull'adozione di una serie storica che contiene un range di dati maggiore rispetto alle altre Medie Mobili spiegati fino a qui, attribuendo ai dati più recenti meno peso, ma prendendo comunque in considerazione quelli più lontani nel tempo. Rispetto alla Media Mobile Ponderata, è necessario definire un parametro (detto fattore decadimento), compreso tra 0 e 1, il quale consente di attribuire, in modo esponenziale e non più lineare, un peso maggiore ai valori più recenti, senza però annullare del tutto il peso dei valori meno recenti. Il coefficiente è calcolato nel seguente modo:

$$coeff = \frac{2}{n + 1}$$

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

$$EMA = (prezzo\ Close - EMAprecedente) * coeff + EMAprecedente$$

Se si fa un confronto tra Media Mobile Semplice e Media Mobile Esponenziale si può dire che quest'ultima reagisce in maniera più rapida alle variazioni della tendenza del prezzo. Dal grafico possiamo inoltre notare un'altra differenza: oltre al fatto che l'EMA segue con più accuratezza i prezzi, si vede anche che essa cambia pendenza più rapidamente. Nella Fig. 19 abbiamo raggruppate tutte e tre le Medie Mobili fino a qui descritte, sia per l'intervallo temporale a 20 periodi che per quello a 100: si nota che la media esponenziale EMA20 (colore verde chiaro, e l'EMA100 (colore marrone) sono quelle che seguono meglio l'andamento dei prezzi, ovvero si sanno adeguare più velocemente quando avviene un inversione del trend.

Fig. 23. Incrocio al ribasso e al rialzo con l'utilizzo della media mobile esponenziale a 20 periodi (verde acqua) e a 100 periodi (marrone). Fonte: https://demo-deal.ig.com/wtp/#/workspace/NWY3MDczMmQwZTcxNTRiOTY0NGNiYzky

2. CHE COSA SI INTENDE PER MACD?

Con l'acronimo MACD (*Moving Average Convergence/Divergence,* ovvero convergenza e divergenza di medie mobili*)* si intende un oscillatore di analisi tecnica[66] utilizzato per studiare l'andamento dei prezzi dei mercati finanziari nel tempo con l'obbiettivo di prevederne le tendenze future.

Questo oscillatore è stato studiato e sviluppato da Gerard Appeal alla fine del 1970 e si basa su medie mobili esponenziali. Successivamente, nel 1986, Thomas Aspray ideò un'implementazione di tale oscillatore, ovvero il MACD istogramma di cui parleremo in seguito.

Per costruire questo indicatore sono necessarie tre medie mobili esponenziali, sul grafico però verranno visualizzate solo due linee dato che una coppia delle tre appena citate è utilizzata unicamente per calcolare la loro differenza. La prima

[66] Oscillatore in analisi tecnica: strumento utile per individuare condizioni estreme sui mercati finanziari. Aiuta, inoltre, ad individuare le fasi di mercato caratterizzate da una perdita di forza (*momentum*), fattore non ancora individuabile sui grafici tradizionali.

media mobile, quella più veloce viene calcolata a 12 periodi, mentre quella più lenta è a 26 periodi. Queste due medie vengono sottratte tra loro per calcolarne la differenza che sarà quindi rappresentata graficamente da una sola linea. Per la generazione di segnali si è introdotto una terza linea, cioè una media mobile esponenziale, solitamente a 9 periodi della precedente differenza.
Abbiamo quindi:

$$MACD = EMA12 - EMA26$$

dove EMA sta per media mobile esponenziale

$$SignalLine^{67} = EMA9[MACD]$$

cioè una media mobile esponenziale della linea di MACD.

Il MACD permette l'individuazione di differenti tipi di segnali: il più importante tra questi è quello che sei genera in seguito all'incrocio della linea della MACD e la *Signal Line*. Un incrocio rialzista (dal basso verso l'alto) tra queste due linee sarà un segnale di acquisto, al contrario, un incrocio ribassista (dall'alto verso il basso) indicherà un segnale di vendita.
Per quanto riguarda invece lo sviluppo da parte di Aspray del MACD istogramma, risolve il problema del ritardo dei segnali che il MACD genera rispetto al movimento dei prezzi, in particolar modo se si prende in considerazione un *timeframe* di lungo periodo come quello settimanale o mensile. L'istogramma del MACD rappresenta la differenza tra il MACD e la *Signal Line* del MACD. Tale differenza viene presentata come un istogramma, rendendo le divergenze identificabili in maniera più semplice. Se c'è un *crossover*[68] della linea media, in tal caso si crea l'istogramma. Se il valore del MACD sarà positivo al valore dell'EMA a 9 giorni, allora il valore dell'istogramma MACD sarà positivo; in caso contrario, il valore dell'istogramma sarà negativo.

[67] *SignalLine* (linea di segnale): ci permette di capire se acquistare o vendere durante i vari movimenti del grafico riferito all'andamento del prezzo.
[68] *Crossover:* è un incrocio su un grafico di trading; può essere formato dal prezzo e da una linea di indicatori tecnici o da due indicatori. Questi segnali vengono utilizzati per prevedere futuri cambiamenti di tendenza come segnali di ingresso, di uscita e di inversione.

Fig. 24. Esempio di utilizzo dell'indice MACD con incroci al rialzo e al ribasso (linea blu = MACD; linea rossa *Signal Line*).

Ulteriori aumenti o diminuzioni del divario tra il MACD e la sua linea di mediana si rifletteranno nell'istogramma del MACD. Nel caso in cui ci siano dei forti aumenti del valore dell'istogramma del MACD, allora questi indicano che il MACD è in crescita più velocemente rispetto all'andamento della media a 9 giorni dell'EMA, quindi il trend rialzista si sta rafforzando (opportunità di acquisto di una o più criptovalute). Se, invece, c'è un forte calo del valore dell'istogramma del MACD, questo indica che il MACD è in calo più velocemente del valore a 9 giorni dell'EMA, dunque l'andamento del trend ribassista è in aumento (vendita di una o più criptovalute).
Solitamente, l'indice MACD si accompagna con quello RSI, che si presenta nella sezione che segue.

6. CHE COSA SI INTENDE PER RSI?

Il *Relative Strength Index* (RSI), o Indice di Forza Relativa, è un oscillatore molto popolare utilizzato nell'analisi tecnica. Fu ideato da John Welles Wilder, che lo presentò nel suo libro "New Concepts in Techinal Trading System" nel 1978.
Questo indicatore presenta una banda d'oscillazione costante, da 0 a 100, che permette una comparazione dei valori con alcuni livelli costanti prestabiliti.

La costruzione matematica di questo oscillatore necessita di un solo parametro, cioè il numero di periodi che si vuole considerare. La formula è la seguente:

$$RSI = 100 * \frac{U}{(U + D)}$$

dove:
U = media delle differenze dei prezzi di chiusura al rialzo di X giorni;
D = media del valore assoluto delle differenze dei prezzi di chiusura al ribasso[69] di X giorni;

la media del valore rialzista si trova sommando il totale delle differenze alla chiusura dei giorni di rialzo e dividendo per i periodi considerati, mentre la media dei valori ribassista si trova sommando il numero totale dei valori assoluti delle differenze di chiusura durante i giorni di ribasso e dividere sempre per il numero di periodi considerati. Così come avviene per tutti gli oscillatori, più i periodi utilizzati sono brevi più si otterrà un oscillatore sensibile con un'ampiezza maggiore, generando d'altra parte un maggior numero di falsi segnali.
Data la creazione di una banda d'escursione costante, da 0 a 100, è possibile individuare zone fisse in cui l'oscillatore si trovi in situazione di estremo; avremo quindi zone di "ipercomprato" quando l'oscillatore segnerà valori superiori a 70, e zone di "ipervenduto" qualora ci saranno valori inferiori a 30 (valori consigliati da Wilder). Anche la linea mediana del 50 va considerata ma pur sempre in subordine rispetto ai valori 30 e 70.
Molto importanti e interessanti sono anche le divergenze rialziste o ribassiste in relazione al corso dei prezzi sul grafico. Tali segnali devono essere monitorati molto attentamente in quanto possono essere catalogati come situazioni assai pregnanti. Si ricordi inoltre che un forte mercato può generare prematuramente segnali di "ipercomprato" o "ipervenduto" e tale situazione può portare a precipitose uscite da un trend ancora potenzialmente valido; infatti, in certe fasi di "ipercomprato", durante i quali un mercato è rialzista, possono dilungarsi per

[69] Chiusura in rialzo/ribasso: sono i prezzi dei prodotti finanziari a fine giornata. Abbiamo i prezzi di apertura degli strumenti finanziari quando aprono le borse e quelli di chiusura quando queste chiudono a fine giornata. In rialzo o in ribasso è riferito al prezzo di apertura.

molto tempo, così come può avvenire con quello di “ipervenduto” durante un mercato ribassista.

Nella Fig.35 oltre all’oscillatore MACD è stato inserito anche l’RSI seguendo l’andamento del prezzo di Bitcoin, con un “timeframe” giornaliero. Si può facilmente osservare che in corrispondenza dell’incrocio tra la linea MACD e quella della *Signal Line* ci troviamo anche in zona “ipercomprato” sul grafico RSI, segnali che appunto consigliano di abbandonare posizioni di *BUY and Hold,* e di posizionarsi in *Short*.

Fig. 25. Esempio di utilizzo dell’indice MACD e Oscillatore RSI (in basso).

3. SELEZIONE DATI

I dati sono stati scaricati dal sito coinmarketcap.com utilizzando un *timeframe* giornaliero che va dal periodo 1Gennaio 2016 al 31 Dicembre 2020, fatta eccezione per Miota, per la quale i dati vengono resi disponibili solo dal 17 Agosto 2017; sono stati utilizzati i dati delle criptovalute descritte nel capitolo precedente di questa tesi. Il basket di criptovalute selezionate è composto quindi da: Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), Miota (IOTA), Litecoin (LTC), Dash (DASH). Inoltre sono stati utilizzati anche i dati giornalieri del fondo Bitwise20, il quale contiene 20 criptovalute tra cui anche quelle analizzate qui. L'utilizzo di questi ultimi dati è stato utili per essere messo a confronto con l'andamento dei prezzi di ciascuna criptovaluta in modo da capire meglio performance (basata su vari indici che verranno spiegati successivamente) e volatilità durante tutto l'arco temporale selezionato.

3. TRADING RULE E METODOLOGIA

La tecnica di trading che si utilizzerà in questa tesi è una delle più adottate quando si parla di investimenti (CFD[70], Forex, azioni, Bond, ecc.), ovvero la Media Mobile Ponderata (WMA) la quale genera segnali trading di breve e di lungo periodo rispetto al livello dell'indice della criptovaluta selezionata.
Per calcolare la media mobile di breve e lungo periodo si utilizzano le seguenti formule:

$$Long\ MA_n = \frac{1}{n} \sum_{t=0}^{t=(n-1)} log^{71}(P_t)$$

$$Short\ MA_{\boldsymbol{n}} = \log(P_t)$$

[70] CFD (Contratti per Differenza): si prevede che un investitore, nel voler andare *long* o *short* su un sottostante si impegna in un contratto con un *broker* di CFD anziché acquistare direttamente tale sottostante.
[71] Trasformazione logaritmica: il vantaggio dell'utilizzo di una scala logaritmica (si basa sulla trasformazione logaritmica dei prezzi di una serie storica) rispetto a quella lineare (si basa sui prezzi di una serie storica) è più utili quando si hanno attività finanziarie che presentano escursioni molto ampie nel tempo (elevata volatilità).

in cui, $Long\ MA_n$ ($Short\ MA_{\boldsymbol{n}}$**)** è la media mobile di lungo (breve) periodo, P_t è il prezzo della criptovaluta che stiamo esaminando al giorno *t* e *n* rappresenta il numero dei giorni utilizzati per calcolare la media mobile di lungo periodo. Ogni *n* indica una strategia diversa seguendo le regole di trading dettate WMA. Si utilizzerà quindi *n* = 20, 50, 100, 150, 200.

Va precisato che nel mercato criptovalutario, ad oggi, non è possibile prendere *short positions* utilizzate in un mercato finanziario tradizionale (compravendita di strumenti finanziari) quindi ci si concentrerà sui *payoff*[72] delle posizioni *buy.* Utilizzando le medie mobili a breve e lungo periodo spezziamo in due le decisioni su che investimento fare. Come prima illustrato, avremo *buy signals*[73] quando la media mobile a breve periodo incrocia al rialzo quella a lungo periodo (dal basso verso l'alto). L'idea alla base del calcolo della media mobile è quella di identificare il trend rialzista/ribassista del prezzo della criptovaluta in considerazione, cosicché ogni qualvolta la media mobile di breve periodo incrocia quella di lungo periodo inizierà un nuovo trend, a sua volta rialzista/ribassista.

$$Buy\ Signal_t = \begin{Bmatrix} 1, se\ Short\ MA_t - Long\ MA_t > 0 \\ 0,\ Altrimenti \end{Bmatrix}$$

Come seconda cosa, una posizione *long* viene aperta sulla criptovaluta sottostante quando prende avvio un segnale *buy* (in base agli indicatori tecnici che sono stati decritti precedentemente) e tenuta fino a quando non si genererà un segnale *sell*, momento in cui si venderà la criptovaluta acquistata.

[72] *Payoff:* associato al trading questo termina indica il rendimento/perdita derivante dall'acquisto/vendita di un'azione, bond o uno strumento finanziario.
[73] *Buy signals:* segnale che ci dà la conferma per poter effettuare l'acquisto di una criptovaluta, o di una parte di essa.

4. CONFRONTO TRA CRIPTOVALUTE E MEDIA MOBILE

4.1 BITCOIN

Procediamo quindi con la visualizzazione dei grafici risultanti dall'applicazione della Media Mobile (25-50-100 periodi) e successivamente a quelle con intervalli temporali (10-20-40 periodi).

Fig. 26. Grafico relativo all'andamento del prezzo del Bitcoin a confronto con le medie mobili MA(25) in colore rosso, MA(50) in colore viola e MA(100) in colore arancione.

In questo grafico possiamo notare l'andamento del prezzo di Bitcoin messo a confronto con le sue Medie Mobili. Chiaramente, più aumentano le lunghezze dei periodi presi in considerazione più sarà lento il movimento della curva *Moving Average*. Come possiamo notare nel grafico della Fig.20, la curva arancione, ovvero la MA(100), segue molto "in ritardo" l'andamento del prezzo della criptovaluta presa in considerazione, a differenza della curva rossa, MA(25), che è più reattiva. Sono stati calcolati anche gli scarti quadratici medi[74] per ciascuna Media Mobile per capire quanta volatilità c'è stata ad ogni intervallo di tempo preso in considerazione. Per quanto riguarda la MA(25) abbiamo uno sqm pari a 28533%, per la MA(50) è risultata una volatilità pari a 68618%, mentre, per quanto riguarda la MA(100) abbiamo uno sqm uguale a 150119% (per fare un confronto, quella dell'oro si aggira attorno al 13%-15% annualmente[75]).

[74] Nota: per Scarto Quadratico Medio si intende un indice di dispersione statistico, ovvero una stima di una popolazione di dati o di una variabile casuale. È un metodo per esprimere la dispersione dei dati intorno ad un indice di posizione la quale potrebbe essere, per esempio, la media aritmetica oppure una sua stima.
[75] Fonte: https://it.cointelegraph.com/news

Fig. 27. Grafico relativo all'andamento del prezzo del Bitcoin a confronto con le medie mobili MA(10) in colore rosso, MA(20) in colore viola e MA(40) in colore arancione.

Per quanto riguarda la Fig. 27 questa rappresenta il prezzo di BTC messo a confronto con le rispettive MA a 10, 20, 40 periodi. In questo caso si è voluto sperimentare il movimento delle medie mobili prendendo in considerazione intervalli temporali più brevi per capire che differenze troviamo. In effetti, osservando l'andamento dei prezzi sul grafico, si nota una maggior reattività delle Medie Mobili nei confronti del prezzo di Bitcoin; questo implicherà, di conseguenza, movimenti di "*buy and sell"* più frequenti se si vorrà seguire la strategia spiegata precedentemente. Per quanto riguarda gli scarti quadratici medi si può osservare che essi sono rispettivamente pari a 52882% per la MA(10), 74679% per la MA(20) e 110688% per la MA(40). Queste ultime sono più alte rispetto a quelle rispettivamente a 25-50-100 periodi, il che significa che il prezzo di Bitcoin è molto più volatile quando si prende in considerazione la Media Mobile MA(10), MA(20) e MA(100). La varianza, per quanto riguarda queste Medie Mobili, è inferiore a quelle riscontrate con intervalli temporali maggiori, come nella Fig. 26.

La Fig. 28 ci è utile perché è stata "zoomata" per inquadrare meglio l'intreccio di grafici tra il prezzo di BTC e le sue Medie Mobili a 10, 20, 40 periodi durante l'ultimo *bull run market*[76] risalente al 2017.

[76] *Bull run market:* detta anche *"bull market"*, si intende una fase prolungata in cui il mercato, in questo caso delle criptovalute, è fortemente in rialzo.

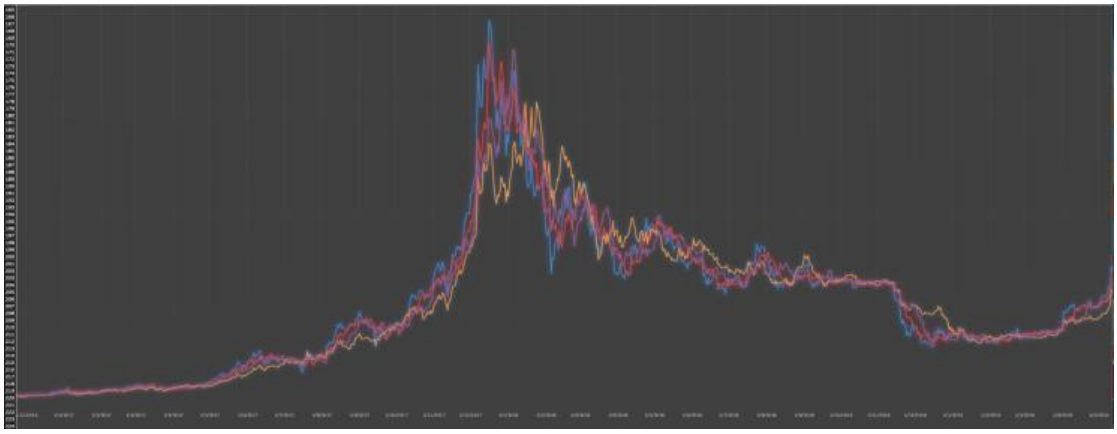

Fig. 28. Zoom effettuato sulla Fig. 27 per poter osservare meglio l'incrocio a rialzo e al ribasso tra il prezzo della criptovaluta Bitcoin e le tre Medie Mobili.

4.2 ETHEREUM

Fig. 29. Grafico relativo all'andamento del prezzo di Ethereum a confronto con le Medie Mobili MA(25) in colore rosso, MA(50) in colore. Viola e MA(100) in colore verde.

Come possiamo osservare nel grafico in Fig.29 abbiamo un andamento dei prezzi molto simile a quelli ritrovati nel grafico del prezzo di Bitcoin; questo perché le criptovalute sono correlate tra di loro quindi quando saremo in fase *bull run* oppure in fase *bearish*[77] il loro prezzo tendenzialmente salirà e scenderà insieme. Per quanto riguarda gli scarti quadratici medi, essi sono pari a 1030% per la MA(25), 2225% per la MA(50) e 10130% per la MA(100). La varianza, in questo

[77] *Bearish market:* si intende una fase prolungata del mercato fortemente discendente. Questo vale sia per il mercato delle criptovalute ma ci si può riferire anche a quello dei metalli preziosi oppure a quello azionario.

caso, è decisamente inferiore rispetto a quella degli stessi intervalli temporali messi a confronto con il prezzo di BTC.

Fig. 30. Grafico relativo all'andamento del prezzo di Ethereum a confronto con le medie mobili MA(10) in colore rosso, MA(20) in colore viola e MA(40) in colore arancione.

Quello che c'è da notare nella Fig. 30 è che anche in questo caso abbiamo che Medie Mobili che prendono in analisi archi temporali maggiori, MA(100) per esempio, seguono con più lentezza l'andamento del prezzo della criptovaluta a cui ci riferiamo rispetto ad archi temporali minori, MA(10) per esempio. In questa tesi si è deciso di utilizzare dati giornalieri ma se si accorcia il *timeframe* si può calcolare con la stessa metodologia anche Medie Mobili che vanno ad orientarsi su intervalli temporali di ore e minuti (in quest'ultimo caso entriamo nella sfera di competenza del trading intra-day).

4.3 LITECOIN

Di seguito sono stati creati anche i grafici delle altre criptovalute descritte nel capitolo 3. Una caratteristica che accumuna tutte le altcoins tra le quali anche Litecoin, Ripple, Iota e Dash è che presentono tutte la classica "montagna" nel rispettivo grafico in coincidenza con Dicembre 2017, ovvero durante l'ultimo halving[78]. I prezzi infatti sono saliti in maniera vertiginosa per poi ritornare circa

[78] *Halving:* si tratta di una caratteristica del protocollo di Bitcoin, poiché portando al dimezzamento del numero dei bitcoin coniati si va ad influenzare il tasso di emissione e la quantità di moneta circolante, riducendo in questo modo la quantità di moneta circolante. Il primo halving è avvenuto nel 2012, si è passati da 50 a 25 bitcoin minati per blocco. Nel 2020 è avvenuto il terzo halving, quindi si è passati da 12.5 a 6.25 bitcoin per blocco. Durante questi periodi il prezzo di Bitcoin aumenta in quanto deve in base al concetto che un bene prodotto in quantità sempre più scarse tende ad apprezzarsi.

ai loro livelli pre-halving. Qui di seguito verranno aggiunti i grafici prima di Litecoin, poi Dash, Ripple e come ultima Iota.

Fig. 31. Grafico relativo all'andamento del prezzo di Litecoin a confronto con le medie mobili MA(25) in colore rosso, MA(50) in colore viola e MA(100) in colore verde.

Nella Fig.31 si osserva, come visto per le precedenti criptovalute, le Medie Mobili a confronto con il prezzo di Litecoin. Per quanto riguarda gli sqm, pari a 1791% per la MA(25), 2075% per la MA(50) e 2698% per la MA(100), essi sono nettamente inferiori sia a quelli di BTC che ETH.

Fig. 32. Grafico relativo all'andamento del prezzo di Litecoin a confronto con le medie mobili MA(10) in colore rosso, MA(20) in colore viola e MA(40) in colore arancione.

Nella Fig.32 abbiamo invece le Medie Mobili a 10, 20, 40 periodi a confronto con il prezzo della criptovaluta Litecoin. Gli scarti quadratici medi sono pari a 976% per la MA(10), 1399% per la MA(20) e 1926% per la MA(40).

4.4 DASH

Fig. 33. Grafico relativo all'andamento del prezzo di Dash a confronto con le medie mobili MA(25) in colore rosso, MA(50) in colore viola e MA(100) in colore verde.

Si nota che lo scarto quadratico medio MA(25) è pari 5231%, quello dell' MA(50) è uguale a 7328% mentre lo sqm dell' MA(100) è pari a 9622%. La volatilità del prezzo della criptovaluta Dash è di circa un decimo rispetto a quella riscontrata nel prezzo di Bitcoin. Ciò significa fluttuazioni del prezzo di Dash 1/10 più moderate rispetto BTC.

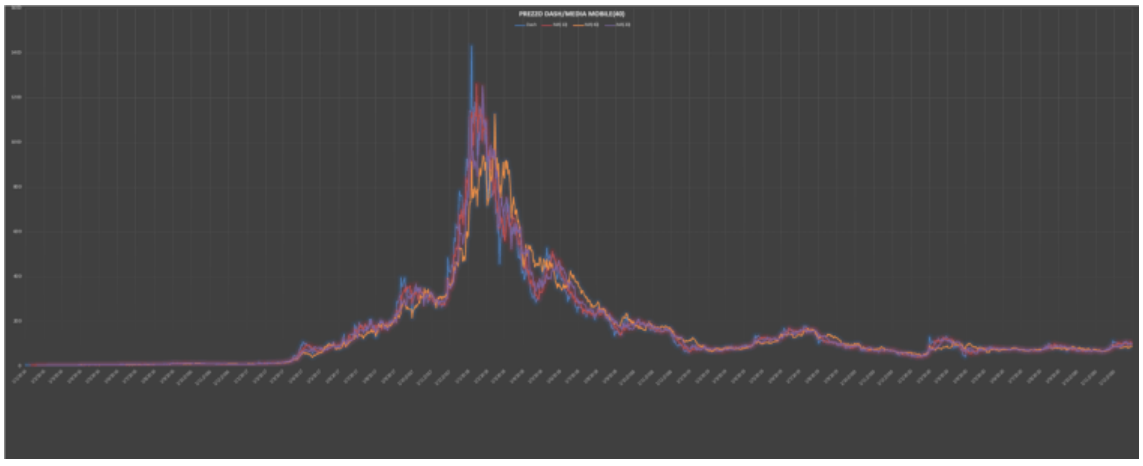

Fig. 34. Grafico relativo all'andamento del prezzo di Dash a confronto con le medie mobili MA(10) in colore rosso, MA(20) in colore viola e MA(40) in colore arancione.

In questo caso abbiamo gli scarti quadratici medi delle Medie Mobili MA(10) pari a 2684%, MA(20) pari a 4041% e lo sqm della MA(40) pari a 6486%. La volatilità dei prezzi di Bitcoin rispetto a quelli di Dash sale a 18 volte; più si abbassano i

periodi della Media Mobile più la volatilità dei prezzi di Dash si attenuano rispetto a quelli di Bitcoin.

4.5 RIPPLE

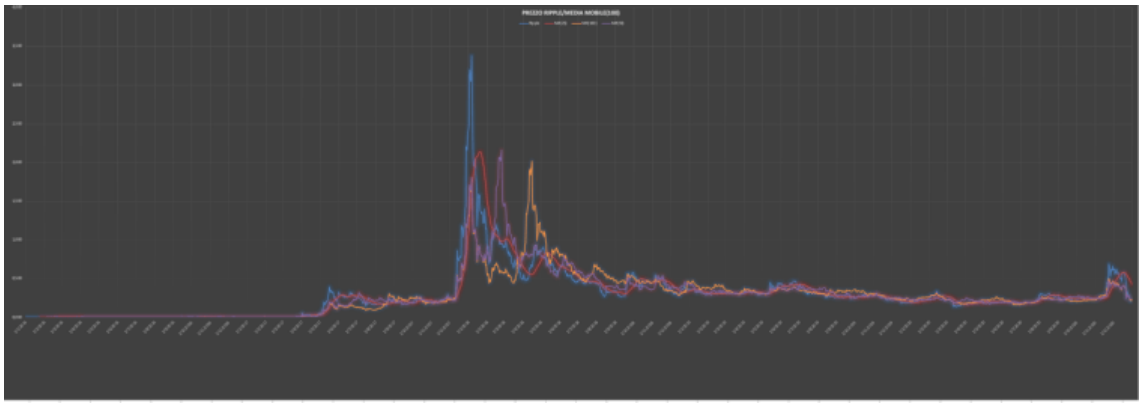

Fig. 35. Grafico relativo all'andamento del prezzo di XRP a confronto con le medie mobili MA(25) in colore rosso, MA(50) in colore viola e MA(100) in colore arancione.

Differentemente dalle altre criptovalute, il grafico di XRP mostra delle differenze. Come prima cosa, osservando la Fig. 35. si può notare un "ritardo" delle Medie Mobili a 50 e 100 periodi (in viola e arancione) rispetto al prezzo; infatti, a Dicembre 2017, il prezzo di questa criptovaluta è aumentato e poi diminuito in un lasso di tempo relativamente breve (20 giorni circa). Per quanto riguarda invece gli scarti quadratici medi rispettivamente delle MA(25), MA(50) e MA(100) sono pari a 15,60%, 16,34% e 18,79%. Essi sono inferiori a quelli delle altre criptovalute, questo a sottolineare un andamento del prezzo sul mercato molto più stabile rispetto alle variazioni di prezzo di Bitcoin o le altcoins.

Per quanto riguarda invece la Fig. 36 si osserva che riducendo la lunghezza degli intervalli presi in considerazione, rispettivamente MA(10), MA(20) e MA(40), questi riescono a seguire in maniera più accurata il prezzo di XRP. Per quanto riguarda invece gli scarti quadratici medi sono decisamente bassi rispetto a Bitcoin e le altcoins: pari a 8% per la MA(10), 12% per la MA(20) e 16% per quanto riguarda la MA(40).

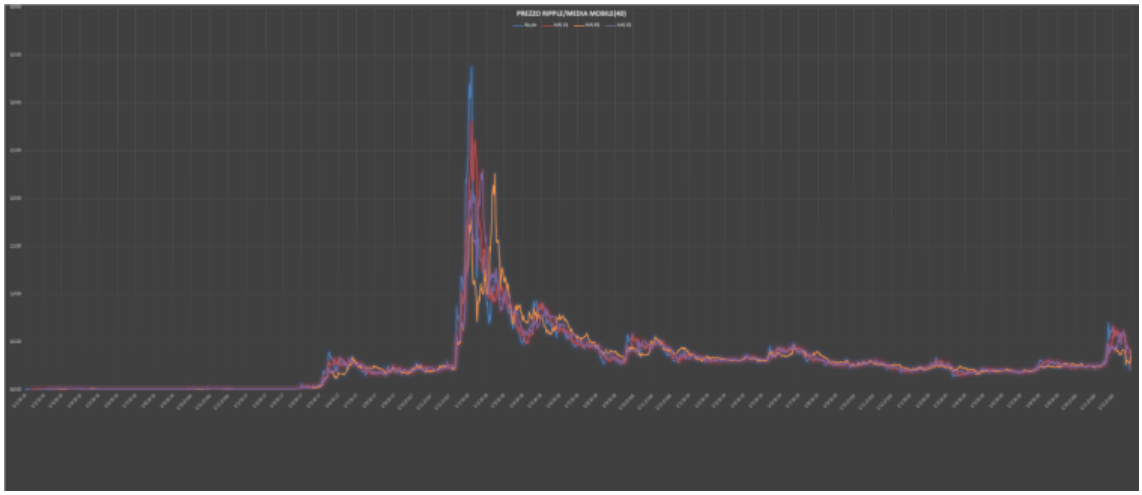

Fig. 36. Grafico relativo all'andamento del prezzo di XRP a confronto con le medie mobili MA(10) in colore rosso, MA(20) in colore viola e MA(40) in colore arancione.

4.6 MiOTA

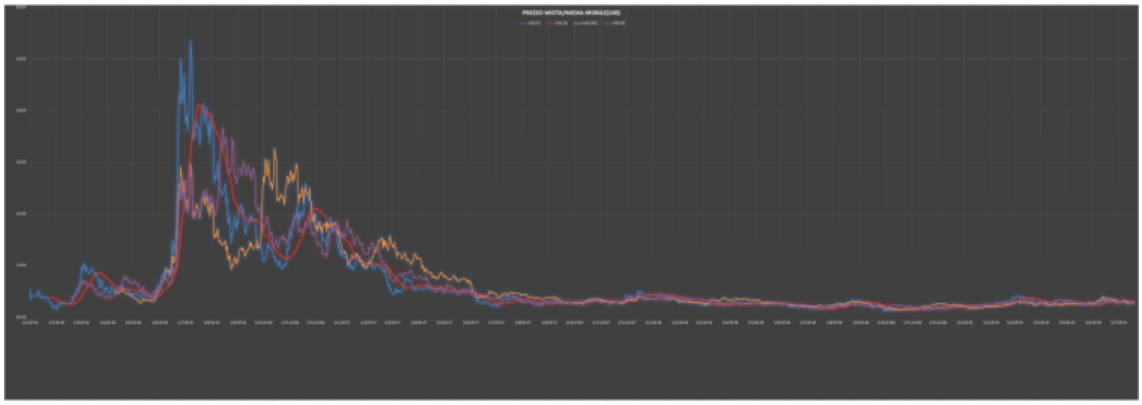

Fig. 37. Grafico relativo all'andamento del prezzo di MiOTA a confronto con le medie mobili MA(25) in colore rosso, MA(50) in colore viola e MA(100) in colore arancione.

Così come osservato per il grafico di XRP, anche in quello di MiOTA notiamo un deciso ritardo da parte delle medie mobili a 50 e 100 periodi in prossimità della *bull run* coincidente con i mesi Dicembre-Gennaio 2017. Se si guardano gli scarti quadratici medi, si nota che sono mediamente bassi se paragonati con quelli di Bitcoin; abbiamo un 32% per la MA(25), 41% per la MA(50) e 47% per la MA(100).

Fig. 38. Grafico relativo all'andamento del prezzo di MiOTA a confronto con le medie mobili MA(10) in colore rosso, MA(20) in colore viola e MA(40) in colore arancione.

Accorciando i *timeframe*s, rispettivamente utilizzando le MA(10), MA(20) e MA(40) si nota, nella Fig. 38, che questi seguono in maniera più accurata il prezzo della criptovaluta MiOTA. Per quanto riguarda gli scarti quadratici medi abbiamo 17% per la MA(10), 25% per la MA(20) e 37% per la MA(40): relativamente più stabili rispetto alla criptovaluta di confronto Bitcoin.

	Sqm MA(10)	**Sqm MA(20)**	**Sqm MA(40)**	**Sqm MA(25)**	**Sqm MA(50)**	**Sqm MA(100)**
Bitcoin	52882%	74679%	110688%	28533%	68618%	150119%
Ethereum	3145%	4505%	6912%	1030%	2225%	10130%
Litecoin	976%	1399%	1926%	1791%	2075%	2698%
Dash	5231%	7328%	9622%	2684%	4041%	6486%
Ripple	8%	12%	16%	15,60%	16,34%	18,79%
Miota	17%	25%	37%	32%	41%	47%

Tabella 5: sono state inseriti gli scarti quadratici medi ottenuti per ciascuna media mobile e ciascuna criptovaluta.

In base alla Tabella 5 possiamo osservare quanta fluttuazione media ci sia nel mercato delle criptovalute, in particolar modo per Bitcoin. Questo è dovuto perché è una tecnologia ancora molto giovane (vale per tutte le cripto) e quindi

c’è la presenza di molti investitori che vogliono solo sfruttare il momento per speculare. Per quanto riguarda Bitcoin, oltre alla speculazione in sé, c’è anche l’aspetto che ne caratterizza il protocollo ovvero i vari *halving* dovuti alla sua limitatezza. Di conseguenza si può affermare che questo volatilità offre occasioni buone per i trader di essere profittevoli sui mercati o, al contrario, perdere ingenti somme in poco tempo.

7. BITCOIN CON GLI INDICI TECNICI MACD E RSI

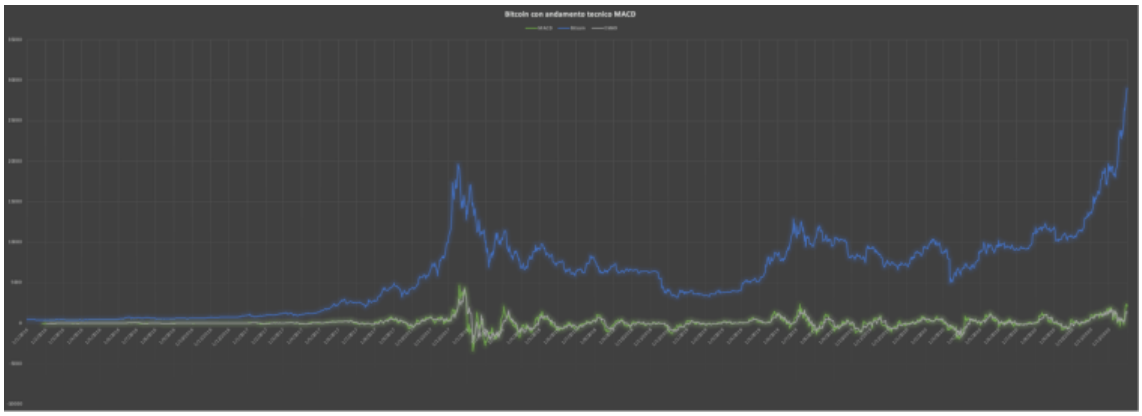

Fig. 39. In blu grafico del prezzo di BTC, in verde e bianco rispettivamente le linee MACD e EMA a 9 periodi.

Sono stati svolti i calcoli relativi alla creazione dell’indice MACD. In questo caso si può evidenziare come gli incroci al rialzo e al ribasso delle linee MACD e EMA9 coincidano con movimenti rialzisti e ribassisti del prezzo della criptovaluta in esame.

Come si è spiegato nella definizione dell’indicatore MACD, non si riesce a capire dove si troveranno i massimi e i minimi che il prezzo raggiungerà ma è molto utile per capire la direzione che il trend prenderà. Questo è validato dal fatto che quando ci sono stati movimenti rialzisti o ribassisti del prezzo di Bitcoin (in particolare nel periodo dicembre-gennaio 2017) anche l’indicatore MACD è stato molto ampio nei suoi movimenti. È importante sottolineare che questo indicatore deve essere affiancato ad altri per poter operare sui mercati, utilizzare unicamente questo significherebbe avere una parziale informazione sui futuri movimenti dei prezzi.

Fig. 40. Nel grafico superiore abbiamo il prezzo di BTC insieme alle Medie Mobili a 25, 50, 100 periodi. Nel grafico inferiore abbiamo l'oscillatore RSI con *timeframe* giornaliero che segue l'andamento del prezzo di Bitcoin.

Per quanto riguarda l'indicatore RSI sono stati affiancati due grafici; quello sopra è quello del prezzo di Bitcoin e le rispettive Medie Mobili a 25, 50, 100 periodi, mentre quello sotto è appunto quello relativo all'indice *Relative Strength Index*. In corrispondenza di massimi e minimi del prezzo di Bitcoin ci troveremo nelle rispettive zone di ipercomprato e ipervenduto sul grafico RSI. Come detto per l'indice tecnico MACD anche in questo caso si sottolinea che l'indice RSI è utile se affiancato ad altri per capire meglio la direzione che potrebbe prendere il trend.

8. ETHEREUM CON GLI INDICI TECNICI MACD E RSI

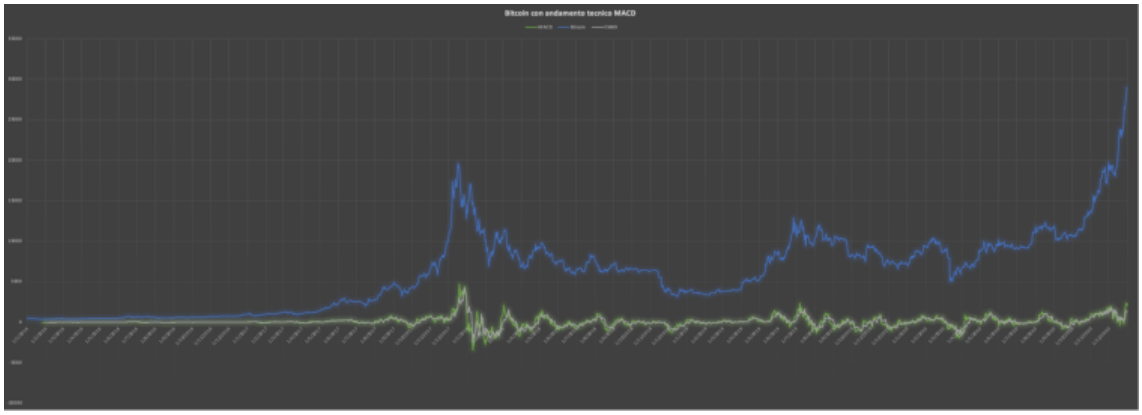

Fig. 41. In blu grafico del prezzo di ETH, in verde e bianco rispettivamente le linee MACD e EMA a 9 periodi.

Quanto detto per la criptovaluta Bitcoin vale anche per Ethereum. Anche in questo caso abbiamo movimenti più ampi dell'indice MACD in prossimità del periodo dicembre-gennaio 2017 come si può notare nella Fig41.

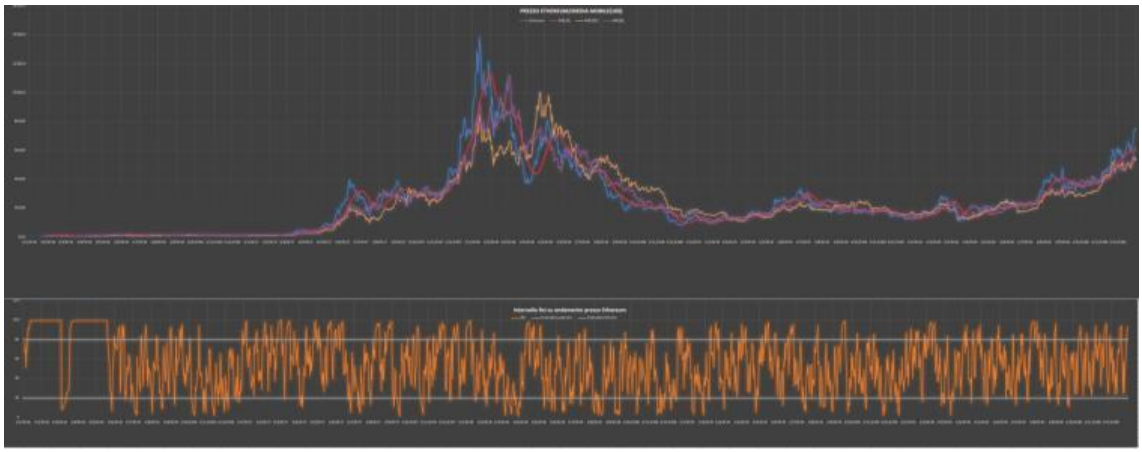

Fig. 42. Nel grafico superiore abbiamo il prezzo di ETH insieme alle Medie Mobili a 25, 50, 100 periodi. Nel grafico inferiore abbiamo l'oscillatore RSI con *timeframe* giornaliero che segue l'andamento del prezzo di Ethereum.

Nella Fig.42 si può vedere il grafico del prezzo di Ethereum con le Medie Mobili a 25, 50, 100 periodi a confronto con il grafico dell'indicatore RSI. Come si può notare nel grafico RSI dal 12 gennaio 2016 al 27 maggio 2016 è risultato un periodo prolungato in cui il prezzo di ETH è stato ipercomprato. Dall'analisi dei dati risulta infatti che in data 12/01/2016 ci sia stato, in un solo giorno, un profitto sul prezzo ETH del +408%. In data 4/03/2016 poi c'è stato un rendimento giornaliero di -85%, succeduto da un repentino rialzo del prezzo in pochi giorni. L'indice ha impiegato quindi del tempo per potersi adeguare a simili movimenti molto ampi.

Nella tabella 6 si mette in relazione la linea MACD e quella dell'EMA9 che ci permettere di capire quando compiere un'operazione di acquisto o vendita; il segnale "trade" nelle varie caselle coincide con i vari incroci MACD e EMA9, si dal basso verso l'alto che viceversa. L'input utilizzato è il seguente:

- "=SE(G60>0;SE(G59<0;" trade ";" ");" ")" per Bitcoin;
- "=SE(G77>0;SE(G76<0;" trade ";" ");" ")" per Ethereum.

Bitcoin

Data	Prezzo	12 EMA	26 EMA	MACD	9 EMA	Istogramma	Trade Entry
1/1/2016	435,66						
2/1/2016	435,40						
3/1/2016	431,91						
4/1/2016	433,85						
5/1/2016	433,34						
6/1/2016	430,87						
7/1/2016	459,07						
8/1/2016	454,44						
9/1/2016	450,38						
10/1/2016	449,99						
11/1/2016	449,19						
12/1/2016	434,01	434,84					
13/1/2016	432,77	434,09					
14/1/2016	430,03	430,97					
15/1/2016	357,53	395,69					
16/1/2016	388,70	411,02					
17/1/2016	378,46	404,67					
18/1/2016	384,89	421,98					
19/1/2016	375,27	414,86					
20/1/2016	418,54	434,46					
21/1/2016	409,38	429,69					
22/1/2016	382,90	416,05					
23/1/2016	387,50	410,76					
24/1/2016	403,05	417,91					
25/1/2016	391,40	410,72					
26/1/2016	391,54	374,54	413,60	-39,07			
27/1/2016	394,79	391,75	415,10	-23,35			
28/1/2016	379,61	379,04	405,76	-26,73			
29/1/2016	378,68	381,79	406,27	-24,48			
30/1/2016	378,46	376,87	405,90	-29,04			
31/1/2016	367,95	393,25	399,41	-6,16			
1/2/2016	371,33	390,36	415,20	-24,85			
2/2/2016	372,93	377,92	413,69	-35,77			
3/2/2016	368,87	378,19	409,63	-31,44	-35,25	3,81	
4/2/2016	387,99	395,52	418,99	-23,47	-23,41	-0,06	
5/2/2016	384,50	387,95	416,85	-28,90	-27,81	-1,09	
6/2/2016	375,44	383,49	404,73	-21,24	-22,86	1,62	
7/2/2016	377,49	386,14	405,13	-18,99	-24,01	5,02	
8/2/2016	371,14	375,38	400,59	-25,21	-15,69	-9,52	
9/2/2016	372,68	375,68	365,11	10,58	-7,13	17,71	trade
10/2/2016	378,44	378,45	383,57	-5,12	-20,45	15,33	
11/2/2016	378,23	373,09	378,35	-5,26	-18,35	13,09	
12/2/2016	382,05	376,69	383,47	-6,78	-15,13	8,35	
13/2/2016	391,00	381,97	383,14	-1,17	-15,03	13,86	
14/2/2016	406,59	387,73	412,57	-24,84	-23,04	-1,80	
15/2/2016	398,95	393,47	404,17	-10,69	-14,84	4,15	
16/2/2016	407,42	395,96	395,16	0,80	-12,21	13,01	
17/2/2016	415,20	395,32	401,35	-6,03	2,27	-8,30	
18/2/2016	421,19	399,34	412,12	-12,78	-8,95	-3,83	
19/2/2016	420,72	395,93	406,06	-10,13	-7,69	-2,44	
20/2/2016	437,46	405,07	414,50	-9,43	-8,11	-1,32	
21/2/2016	438,56	408,50	416,68	-8,18	-4,67	-3,50	
22/2/2016	437,55	407,89	408,58	-0,69	-12,76	12,07	
23/2/2016	419,97	401,01	399,33	1,68	-4,51	6,19	
24/2/2016	423,94	407,47	401,20	6,27	3,54	2,73	trade
25/2/2016	423,54	415,07	395,75	19,32	6,64	12,68	
26/2/2016	430,85	414,90	401,09	13,81	0,51	13,30	
27/2/2016	433,12	420,27	403,03	17,25	3,56	13,69	
28/2/2016	433,73	424,47	401,30	23,17	6,87	16,30	
29/2/2016	436,44	428,82	412,22	16,60	4,21	12,39	
1/3/2016	431,08	426,90	408,79	18,11	8,71	9,40	
2/3/2016	420,39	428,93	397,92	31,01	16,35	14,66	
3/3/2016	418,80	428,68	398,15	30,54	18,40	12,13	
4/3/2016	407,35	422,45	389,25	33,21	26,26	6,94	
5/3/2016	396,08	408,03	384,38	23,65	18,73	4,92	
6/3/2016	403,24	413,59	390,84	22,75	20,00	2,75	
7/3/2016	412,21	417,88	395,22	22,66	22,91	-0,26	
8/3/2016	411,18	421,02	396,62	24,40	20,50	3,90	
9/3/2016	412,80	422,96	401,90	21,06	19,59	1,48	
10/3/2016	415,98	424,86	411,29	13,57	22,29	-8,72	
11/3/2016	419,39	427,92	409,17	18,75	24,64	-5,90	trade
12/3/2016	410,58	421,83	409,00	12,83	23,02	-10,19	
13/3/2016	412,52	416,46	413,86	2,59	13,12	-10,53	
14/3/2016	415,02	416,91	418,11	-1,20	10,78	-11,97	
15/3/2016	415,41	411,38	418,07	-6,69	7,98	-14,67	
16/3/2016	416,07	406,08	426,77	-20,69	1,85	-22,55	
17/3/2016	418,41	410,83	428,49	-17,66	1,70	-19,36	
18/3/2016	409,65	410,93	423,60	-12,67	0,45	-13,12	
19/3/2016	410,20	410,69	415,09	-4,40	7,17	-11,57	
20/3/2016	411,27	412,04	417,61	-5,57	3,63	-9,20	
21/3/2016	412,00	413,99	417,77	-3,78	-0,59	-3,19	
22/3/2016	416,66	418,03	423,76	-5,73	-3,46	-2,27	
23/3/2016	417,53	414,06	425,33	-11,27	-8,98	-2,29	
24/3/2016	412,95	412,74	423,34	-10,61	-15,65	5,04	trade

ETHEREUM

Data	Prezzo	12 EMA	26 EMA	MACD	9 EMA	Istogramma	Trade Entry
1/1/2016	0,92						
2/1/2016	0,92						
3/1/2016	0,93						
4/1/2016	0,94						
5/1/2016	0,95						
6/1/2016	0,94						
7/1/2016	0,95						
8/1/2016	0,95						
9/1/2016	0,97						
10/1/2016	0,98						
11/1/2016	0,98						
12/1/2016	0,99	0,96					
13/1/2016	1,06	0,99					
14/1/2016	1,13	1,03					
15/1/2016	1,14	1,04					
16/1/2016	1,19	1,07					
17/1/2016	1,21	1,08					
18/1/2016	1,22	1,09					
19/1/2016	1,33	1,14					
20/1/2016	1,37	1,17					
21/1/2016	1,43	1,21					
22/1/2016	1,50	1,24					
23/1/2016	1,53	1,26					
24/1/2016	1,55	1,31					
25/1/2016	1,97	1,55					
26/1/2016	10,00	5,57	5,46	0,11			
27/1/2016	10,06	5,63	5,49	0,14			
28/1/2016	10,07	5,64	5,50	0,14			
29/1/2016	10,16	5,69	5,55	0,14			
30/1/2016	10,24	5,79	5,60	0,19			
31/1/2016	10,32	5,85	5,63	0,22			
1/2/2016	10,41	5,92	5,68	0,24			
2/2/2016	10,42	5,96	5,69	0,28			
3/2/2016	10,44	5,99	5,71	0,28	0,20	0,08	
4/2/2016	10,51	6,03	5,75	0,29	0,21	0,08	
5/2/2016	10,53	6,25	5,76	0,50	0,32	0,18	
6/2/2016	10,69	10,35	5,84	4,51	2,32	2,18	
7/2/2016	10,74	10,40	5,90	4,50	2,35	2,16	
8/2/2016	10,97	10,52	6,05	4,47	2,34	2,13	
9/2/2016	11,00	10,58	6,07	4,51	2,38	2,14	
10/2/2016	11,00	10,62	6,10	4,53	2,40	2,13	
11/2/2016	11,08	10,70	6,15	4,56	2,42	2,14	
12/2/2016	11,08	10,75	6,15	4,60	2,44	2,16	
13/2/2016	11,16	10,79	6,25	4,55	2,52	2,03	
14/2/2016	11,17	10,81	6,27	4,54	4,52	0,02	
15/2/2016	11,23	10,87	6,33	4,54	4,52	0,02	
16/2/2016	11,27	10,90	6,39	4,52	4,49	0,02	
17/2/2016	11,31	11,00	6,42	4,58	4,55	0,04	
18/2/2016	11,38	11,06	6,47	4,60	4,56	0,03	
19/2/2016	11,40	11,19	6,69	4,50	4,53	-0,03	
20/2/2016	11,60	11,30	10,80	0,50	2,55	-2,05	
21/2/2016	11,62	11,31	10,84	0,47	2,51	-2,04	
22/2/2016	11,66	11,37	10,87	0,51	2,52	-2,02	
23/2/2016	11,66	11,37	10,91	0,46	2,50	-2,04	
24/2/2016	11,67	11,42	10,96	0,46	2,49	-2,03	
25/2/2016	11,86	11,52	11,09	0,43	2,50	-2,08	
26/2/2016	11,90	11,57	11,16	0,41	2,50	-2,09	trade
27/2/2016	11,95	11,61	11,19	0,43	2,46	-2,04	
28/2/2016	12,42	11,87	11,43	0,44	0,47	-0,03	
29/2/2016	12,45	11,92	11,48	0,43	0,45	-0,02	
1/3/2016	12,52	11,96	11,53	0,44	0,47	-0,03	
2/3/2016	13,01	12,31	11,85	0,46	0,46	0,00	
3/3/2016	13,53	12,58	12,14	0,44	0,45	-0,01	
4/3/2016	14,48	13,07	12,73	0,34	0,39	-0,04	
5/3/2016	2,14	6,90	6,57	0,33	0,37	-0,04	
6/3/2016	2,21	6,94	6,61	0,33	0,38	-0,05	
7/3/2016	2,28	7,07	6,68	0,39	0,41	-0,02	
8/3/2016	2,31	7,11	6,70	0,41	0,42	-0,01	
9/3/2016	2,39	7,17	6,78	0,40	0,42	-0,02	
10/3/2016	2,44	7,43	6,81	0,63	0,54	0,09	
11/3/2016	2,45	7,45	6,84	0,61	0,52	0,09	
12/3/2016	2,49	7,51	6,88	0,63	0,48	0,14	
13/3/2016	2,50	7,76	6,91	0,85	0,59	0,26	
14/3/2016	2,53	8,03	6,96	1,08	0,70	0,37	
15/3/2016	2,53	8,51	6,97	1,54	0,97	0,58	
16/3/2016	2,53	2,34	7,07	-4,73	-2,16	-2,57	
17/3/2016	2,54	2,38	7,08	-4,71	-2,16	-2,55	trade
18/3/2016	2,58	2,43	7,12	-4,69	-2,03	-2,66	
19/3/2016	2,96	2,64	7,31	-4,68	-2,03	-2,64	
20/3/2016	3,18	2,79	7,43	-4,64	-2,01	-2,63	
21/3/2016	3,76	3,10	7,81	-4,71	-1,93	-2,78	
22/3/2016	4,04	3,25	7,97	-4,73	-1,83	-2,90	
23/3/2016	4,32	3,41	8,14	-4,73	-1,60	-3,14	
24/3/2016	4,34	3,42	8,38	-4,96	-4,85	-0,12	

Tabella 6: si può osservare la voce “trade” in relazione a ciascun giorno. In presenza di questa voce la linea MACD ha intersecato quella dell’EMA9: se l’ha fatto dal basso verso l’alto vuol dire che abbiamo l’inizio di un trend rialzista, viceversa abbiamo l’inizio di un trend ribassista. Le tabelle sono relative a Bitcoin (a sinistra) ed Ethereum (a destra). Si consiglia l’affiancamento di un grafico avente l’andamento del prezzo di Bitcoin e Ethereum.

9. Esempio di Utilizzo degli indicatori MM-RSI-MADC

BTC	*Prezzo Apertura*	*Prezzo Chiusura*	*Media Mobile (25,50)*	*RSI*	*MACD*	*Profitto/ Perdita*
21/07/2020	$9161	$9139	SI	NO	NO	-0.24%
21/07/2020	$9139	$118021	SI	SI	SI	+29.35%
31/08/2020	$11802	$11563	SI	NO	NO	-2.02%
31/08/2020	$11563	$11617	SI	NO	SI	+0.46%
03/09/2020	$11617	$10456	SI	NO	SI	-9.99%
22/09/2020	$10456	$10755	SI	NO	NO	+2.86%
08/11/2020	$10666	$17955	SI	NO	SI	+68.33%
29/11/2020	$17955	$17806	SI	NO	NO	-0.83%
09/12/2020	$17806	$18867	SI	NO	SI	+5.95%
13/12/2020	$18867	$18625	SI	SI	SI	-1.28%
20/01/2021	$18625	$36224	SI	NO	SI	+94.5%

Tabella 7: nella tabella sono stati riassunti i prezzi di entrata e i prezzi di uscita da undici operazioni (posizioni long o short) sulla criptovaluta Bitcoin in diversi momenti durante il 2020 e 2021. Il broker utilizzato è IGMarkets, utilizzato per gli strumenti tecnici Media Mobile, RSI e MACD.

Dopo aver descritto e analizzato gli indicatori tecnici (Media Mobile, RSI e MACD) si è tentato di capire quali possano essere i risultati nell'utilizzarli, cercando quindi di fare trading. Nella tabella 4 si osserva che tutte le operazioni sono state svolte seguendo sempre l'andamento delle Medie Mobili (25, 50) per poi controllare anche gli indicatori RSI e MACD. I risultati mostrano che solo in due operazioni su undici gli indicatori hanno dato la stessa indicazione (tre "SI"). Per quanto riguarda l'indicatore MACD questo ha fornito lo stesso segnale della Media Mobile sette volte su undici osservazioni, mentre per quanto riguarda l'RSI, solo due volte su undici. L'indicatore RSI è spesso risultato contrastante con l'andamento del prezzo della criptovaluta e spesso, quando gli altri indicatori davano l'indicazione di aprire una posizione *long* o *short*, esso indicava il contrario. Probabilmente nel caso della criptovaluta Bitcoin potrebbe non essere un indicatore utile da utilizzare quanto gli altri due, a causa di movimenti oscillatori troppo rapidi.

CAPITOLO 6: DISCUSSIONE E CONCLUSIONI

Affrontare argomenti come la tecnologia alla base della Blockchain e delle criptovalute, che seppur nati recentemente hanno avuto sviluppi esponenziali, comporta attenzione, precisione e anche un pizzico di passione. Nonostante ciò, si deve cercare di documentare in maniera chiara ed efficace tutto il materiale che accompagna i temi trattati in questo documentario senza rischiare di sfociare in giudizi netti o arrivare a delle conclusioni certe, in quanto la materia è costantemente in aggiornamento sia dal punto di vista tecnologico sia per quanto riguarda l'aspetto puramente normativo[79]. Per questo motivo, con l'intento di rendere il processo il meno ambiguo possibile si cercherà di rendere la stesura delle conclusioni sul lavoro svolto nella tesi in modo parallelo a come è stato iniziato e poi svolto, cioè giustificando il binomio evoluzione tecnologica della Blockchain e delle criptovalute e l'aspetto più prettamente speculativo del settore cripto.

Per quanto riguarda il primo aspetto affrontato nel primo capitolo, si può sostenere che la Blockchain sia una delle più importanti innovazioni dell'ultimo secolo, in particolar modo se osservata dal punto di vista finanziario. Questa tecnologia, che permette di fornire un "certificato crittografato" univoco ed immodificabile a garanzia dell'esecuzione di una transazione, senza la necessità di un intermediario che prenda la parte di "validatore", è sicuramente un aspetto quantomeno rivoluzionario che ha margine di sviluppo e di espansione in tanti ambiti lavorativi (finanziario, giudiziario, societario, ecc.) potrà portare benefici in futuro in termini di costi e di rapidità dei processi.
Per quanto riguarda la scelta e la descrizione delle criptovalute (Bitcoin, Ethereum, Litecoin, Ripple, Dash e Iota) bisogna premettere che esse fanno parte di mare magnum di altcoins aventi progetti innovativi, tuttavia si è deciso di descrivere queste in quanto sono state tra le prime a nascere con l'obbiettivo di apportare una ventata innovativa in ambito economico-sociale capace sia di

[79] R. Razzante (a cura di), *Bitcoin e criptovalute. Profili fiscali, giuridici e finanziari*, Maggioli Editore, 2018

appoggiarsi alla Blockchain sia di seguire e migliorare la filosofia tecnologica con cui Satoshi Nakamoto ha creato Bitcoin.
Non vi è alcun dubbio che le criptovalute siano innovative su più punti; sul fronte sicurezza e controllo si permette all'utilizzatore il controllo totale delle transazioni grazie al consenso del proprietario, mentre per quanto riguarda la contraffazione, in particolare la "doppia spesa", si è visto come l'utilizzo delle criptovalute tramite il protocollo "proof-of-work" che si appoggia alla Blockchain renda sempre più difficoltoso tali truffe a mano a mano che aumentano le dimensioni della rete complessiva (Blockchain). Dal punto di vista commissionale si è visto come questo sia a discrezione dell'utente in quanto vige la regola che a una transazione più veloce corrisponda una commissione maggiore e viceversa, senza quindi l'intermediazione di terze parti (no PCI). Inoltre, si offre agli utenti la libertà di utilizzare i codici QR, già utilizzati in altri ambiti da anni, implicando quindi facilità nell'utilizzo e nel trasporto. Le transazioni, come si è visto con Ripple, nonostante un ingente ammontare, impiegano comunque pochi secondi per essere trasferite da un capo all'altro del mondo.

Fin dalla nascita della Blockchain e delle criptovalute, l'attenzione attorno ad esse è spesso stata di criticità e di diffidenza poiché poggiante su due grandi "pilastri" quali l'utilizzo illecito (riciclaggio) nel Dark Web[80] in quanto le transazioni non possono essere rintracciabili, e la volatilità sui mercati.
Anche se Bitcoin e le altcoin possono essere utili per l'introduzione e la stratificazione[81] nel processo del riciclaggio si può affermare che solo l'1,1% del volume totale delle criptovalute è ritenuto illecito.
Preconcetti che si basano sull' anonimato e l'identità si sono mostrati privi di fondamento in quanto le identità sulla blockchain di Bitcoin, per esempio, non sono anonime ma pseudo-anonime. Ciascuna identità, infatti, è associata a una

[80] Dark Web (web oscuro o rete oscura): terminologia che si usa per indicare i contenuti del World Wide Web nelle *darknet* (reti oscure) che si raggiungono via Internet attraverso specifici *software*, configurazioni e accessi autorizzativi.
[81] Le fasi del riciclaggio sono notoriamente stratificate in tre parti:

- introduzione: si immette in circolazione il denaro all'interno del sistema monetario esistente tramite particolari intermediari quali istituzioni finanziario, casinò, negozi o cambi di valuta;
- stratificazione: l'obbiettivo è quello di rendere difficile la provenienza dell'attività di riciclaggio, quindi si converte il denaro in strumenti monetari. Comprando asset con fondi illeciti per rivenderli;
- integrazione: è la fase finale del riciclaggio di denaro in cui quest'ultimo deve essere immesso nell'economia attraverso il sistema bancario, di conseguenza è ritenuto "pulito". I metodi usati in questa fase comprendono compravendite immobiliari, società di facciata, banche straniere e. fatture false.

stringa alfanumerica, chiamata chiave privata e nonostante sia possibile ammetter che Bitcoin offra un certo livello di protezione sull'identità dei suoi utenti, le transazioni sono in realtà pubbliche. A causa delle sue caratteristiche intrinseche, tutte le transazioni di una blockchain sono condivise tra i partecipanti, il cui consenso è necessario per convalidare la cronologia. A tal proposito, Dave Weisberger, CEO di CoinRoutes, ha spiegato: "L'obiettivo del riciclaggio di denaro è creare una catena di transazioni che non può essere rintracciata, e dato che la blockchain di Bitcoin è progettata per avere un registro pubblico indelebile di tutte le transazioni, il 'riciclaggio' diventa molto più difficile."

Quindi, a causa delle identità pseudo-anonime, delle transazioni pubbliche e della complessità del sistema necessarie per usare Bitcoin, l'alternativa di utilizzare le criptovalute per riciclare denaro non è attualmente né più efficiente né, tanto mento, più efficace delle valute fiat.

Per quanto riguarda la volatilità sui mercati è normale in quanto si tratta di una realtà finanziaria molto giovane ma con grandi potenziali. In questa prima fase (tempo necessario affinché l'argomento cripto venga conosciuto, capito e prenda confidenza con le persone) in cui non ci sono ancora investitori istituzionali (anche se tra il 2020 e il 2021 abbiamo visto interessarsi realtà come Paypal, Visa, JP Morgan, Tesla, per citarne alcune) e soprattutto mancano ancora gli investitori *retail* che sono un importante bacino di clienti, le criptovalute vengono detenute in grandi quantità dalle *Whale*[82]. Questi ultimi, in base a determinate strutture di mercato, indici e indicatori, acquistano e vendono sui mercati delle criptovalute ne innescando ampie oscillazioni.

C'è bisogno di tempo per una maggior familiarizzazione con tante novità sia concettuali che tecnologiche che avvolgono la blockchain e le criptovalute; soprattutto, però, c'è necessità di continue regolamentazioni da parte degli enti che hanno come obbiettivo la tutela dei mercati, la trasparenza e l'efficienza

[82] Il termine "whale" si riferisce ad un investitore con un ingente disponibilità di capitali che può "scuotere" il mercato comprando o vendendo in grandi volumi. Data la capitalizzazione di mercato relativamente modesta delle criptovalute rispetto ad altri settori, i movimenti delle whale possono fornire importanti segnali di prezzo a trader e investitori.

affinché la materia venga resa sicura, facilmente intuibile e di comodo utilizzo sia per le grandi istituzioni sia per la clientela *retail*.

Si sono introdotti nella tesi due articoli scientifici con l'obbiettivo di analizzare se sia più opportuno investire in criptovalute tramite il trading oppure acquistando con l'obbiettivo di un accumulo di critpo. Il primo articolo prende in esame dieci *altcoins* caratterizzate dalla *privacy function.* Utilizzando gli strumenti tecnici quali le Media Mobili, risulta che solo Dash dia dei rendimenti positivi nel tempo (rendimenti annuali pari a circa 14.6% - 18.25% in più rispetto alla strategia *buy-and-hold*). Allo stesso modo, considerando le dieci criptovalute a livello aggregato, non si riscontra alcun rendimento positivo significativo a livello di portafoglio se comparato a uno uguale che utilizzi la strategia *buy-and-hold.* Lo studio, quindi, indica che, a livello di portafoglio, criptovalute che si basano sulla *"privacy function"* e quelle che non lo fanno, sono fondamentalmente differenti per quanto riguarda i loro *payoff*.
Il secondo articolo non prende in esame le strategie di trading convenzionali, cioè quelle che si basano sull'utilizzo di indicatori tecnici, ma spiega piuttosto in maniera indiretta, tramite il concetto di scarsità di Bitcoin, che una strategia vincente potrebbe essere il semplice *buy-and-hold* in prossimità di ogni halving. Osservando il grafico, creato da PlanB[83], relativo al prezzo di Bitcoin si può osservare che, in seguito a ciascun *halving,* il prezzo ha poi segnato nuovi massimi:

- durante l'*halving* del 2012 il prezzo di BTC era pari a $5.33 mentre dodici mesi dopo aveva raggiunto il prezzo di $1148.00;
- durante l'*halving* del 2016 il prezzo di BTC era pari a $634.00 per poi arrivare ad un prezzo pari a $19065.71;
- durante l'*halving* del 2019 il prezzo di BTC era pari a $7724.16 e ad ora deve il nuovo massimo è $64742.3.

[83] https://stats.buybitcoinworldwide.com/stock-to-flow/

La traiettoria storica del prezzo di Bitcoin rimane fortemente sbilanciata verso l'alto. La criptovaluta tocca un minimo dopo ogni ciclo "rialzista-ribassista" e si riprende di nuovo verso nuovi massimi storici.

Fig. 43. Prezzo di Bitcoin con *timeframe* settimanale.

il grafico settimanale in Fig. mostra massimi crescenti consecutivi separati da anni: $500 a novembre 2015, $768 a giugno 2016, $2998 a giugno 2017, $19891 a dicembre 2017, $41986 a gennaio 2021e $64899 ad aprile 2021.

Utilizzare una strategia "*buy-and-hold*" potrebbe quindi essere buona nel momento in cui si decida di acquistare criptovalute ogni volta che il prezzo rintraccia, ovvero scende rispetto al suo massimo. In questo modo si attua un investimento con l'idea di mantenere le criptovalute nel proprio *e-wallet* per anni per anni prima di rivenderle completamente o solo una parte di esse.

La seconda parte della tesi è stata dedicata all'utilizzo dei prezzi giornalieri dal 1gennaio 2016 al 31dicembre 2020 delle criptovalute Bitcoin, Ethereum, Litecoin, Dash, Ripple, Iota, per capire se si possono loro applicare alcuni indicatori tecnici utilizzati dai *traders* e alcuni indici di performance utilizzati nella gestione di portafogli di investimenti. Per quanto riguarda gli indicatori tecnici sono stati utilizzati la Media Mobile, il MACD e l'RSI. Bisogna premettere che ogni *trader*

ha i suoi metodi per operare sui mercati che si basano sia su precisi intervalli temporali, sia s che indicatori utilizzare e, soprattutto, su che tipo di titoli finanziari operare. Detto ciò, è comune osservare come si comportano quattro o cinque indicatori e decidere in base alle indicazioni (che devono coincidere) di almeno tre o quattro di questi.

Peer quanto riguarda, invece, la volatilità, bisogna ammettere che, almeno per quanto riguarda, Bitcoin, Ethereum e Litecoin, risulta decisamente elevata e questa aumenta ancora di più se si utilizzano Medie Mobili a intervalli temporali maggiori.

Per esempio, per la criptovaluta BTC, lo scarto quadratico medio per la Media Mobile a 10 periodi è pari a 74679% mentre per quella a 100 periodi arriva a 150119%, pari al doppio. La stessa cosa si può osservare con Ethereum per il quale abbiamo uno sqm pari a 3145% per la MA(10) e uno pari a 10103% per la MA(100), pari a più del doppio. Se si osserva invece Iota (MiOTA) notiamo come i rispettivi scarti relativi alle stesse Medie Mobile siano decisamente inferiori, ovvero 25% per la MA(10) e 47% per la MA(100). Da un lato abbiamo quindi le criptovalute Bitcoin, Ethereum e Litecoin che hanno una volatilità molto elevata, dall'altra invece abbiamo Dash, Ripple e Iota che ne hanno una decisamente inferiore. Ci sono due motivi per cui si riscontra questa differenza:

- Sicuramente per quanto riguarda BTC, ETH e LTC si riscontra tanta volatilità perché c'è molto interesse intorno alla tecnologia e al numero limitato (in particolare peer Bitcoin), fattori strettamente collegati alle performance finanziarie passate e presenti[84]; cosa che invece ha toccato meno le criptovalute Dash, Ripple e Iota le quali, come si è osservato, hanno avuto volatilità decisamente più moderate.
- I progetti per cui sono state create Bitcoin, Ethereum e Litecoin sono più ampi dato che spaziano da riserve di valore, agli smart contract, oltre che metodi di pagamento e di transazione; Ripple, Dash e Iota si concentrano su progetti molto più specifici, anche se ugualmente molto interessanti ed importanti.

[84] In riferimento ai periodi strettamente successivi ai vari halving del 2012, 2016 e 2020.

Questi aspetti però, portano con sé anche ampie possibilità di speculazione e grandi profitti per chi sa operare sui mercati finanziari.

BIBLIOGRAFIA

BARRDEAR, J. e KUMHOF M., 2016. *The macroeconomics of central bank issued digital currencies*. Bank of England, London.

BOHME R., CHRISTIN N., EDELMAN B., MOORE T., *Bitcoin: Economics, Technology, and Governance*, Journal of Economic Perspectives, 20 Luglio 2015.

BOUOIYOUR, J. e SELMI, R., 2017. *The Bitcoin price formation: Beyond the fundamental sources.*

BOURI E., FANG L., GUPTA R., ROUBAUD D., *Does global economic uncertainty matter for the volatility and hedging effectiveness of Bitcoin?,* International Review of Financial Analysis, www.elsevier.com, 2018.

BUTTERIN, V. 2014. *A Next-Generation Smart Contract and Decentralized Application Platform,* White Paper.

COMANDINI, G. L., 2020. *Da zero alla luna.* Dario Floccovio Editore.

CHAPMAN, S., (2011). *"Bitcoin: a guide to the Future Currency",* ZDNet.

CHUEN, DAVID LEE KUO. Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data. Amsterdam [etc.]: Academic Press - Elsevier, 2015.

CONTALDO, A. e F. CAMPARA. Blockchain, criptovalute, smart contract, industria 4.0. Registri digitali, accordi giuridici e nuove tecnologie. Pisa: Pacini Giuridica, 2019.

FREE EXCHANGE. 2014. *Bitcoin's Deflation Problem*. The Economist.

GRAY, J., 1981. *The Transaction Concept: Virtues and Limitations*. Seventh International Conference on Very Large Databases.

GREENBERG, A. 2011. *Crypto Currency-Money You Can't Trace*. Forbes, 40.

HARRISON, R., (2007). *SecondLife: Revolutionary Virtual Market or Ponzi scheme?*. Capitalism 2.0.

LEMME G. e PELUSO S., Criptomoneta e distacco dalla moneta legale: il caso Bitcoin, in Riv. dir. banc., dirittobancario.it, 43, 2016.

LEORATO S., Dizionario di Economia e Finanza, Treccani.

MEGGIATO, R., (2014). *Il lato oscuro della rete: alla scoperta del Deep Web e dei Bitcoin,* Apogeo.

NAKAMOTO, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*.

NATARAJAN, H., KRAUSE, S. e GRADSTEIN, H., 2017. *Distributed Ledger Technology (DLT) and Blockchain*. World Bank, Washington DC.

SCHIROLI, I.W., 2012. *Dark web & Bitcoin*, Lantana Editore, Cerbara.

SEANG, S. e TORRE, D., 2018. *Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies*. Université Côte d'Azur.

YERMACK, D., 2013. *Is Bitcoin a Real Currency? An economic appraisal*. National Bureau of Economic Research, Massachusetts.

SITOGRAFIA

https://bitcoin.org/bitcoin.pdf

https://cryptorivista.com/insight/tech/

https://www.investopedia.com

https://www.ecb.europa.eu

https://www.forbes.com

https://www.irpa.eu

https://www.pandslegal.it/tecnologie-ict/smart-contracts/

https://cryptonomist.ch

https://www.consob.it/web/investor-education/criptovalute

https://www.bancaditalia.it/compiti/vigilanza

https://bitcoin.org/it/

https://ethereum.org/en/

https://www.dash.org

https://ripple.com

https://iotaitalia.com

https://litecoin.org

https://it.cointelegraph.com/search

https://cryptorivista.com/insight/tech

https://www.internet4things.it

https://cryptonomist.ch/2019/06/09/lightning-network

https://www.investopedia.com/terms/o/offchain-transactions

https://wordpress.com

https://ideas.repec.org

https://innovazione.tiscali.it

https://www.tradingonline.it/investire

https://www.sciencedirect.com