Un possibile uso della costante di Lipschitz per crypto-assets

Università Ca' Foscari

Dipartimento di Scienze Ambientali, Informatica e Statistica

Corso Informatica

Autore: Tamai Edoardo

Relatore: Prof. Fasano Giovanni

Anno Accademico 2018-2019

Indice

Capitolo 1

Introduzione

Al giorno d'oggi si stanno sempre più diffondendo nuove monete virtuali. La moneta fondatrice di tutto questo sistema di cripto-asset è proprio Bitcoin.

Bitcoin è una delle prime monete virtuali creata nel 2009 da uno sviluppatore noto con lo pseudonimo di Satoshi Nakamoto. Essa si basa su due concetti chiave che sono il peer-to-peer (P2P) e l'open source. Per P2P si fa riferimento a un modello di architettura logica di rete in cui i nodi possono essere visti come client-server (come nel modello classico di rete informatica) oppure come nodi paritari, cioè un nodo può essere allo stesso tempo client e server [20]. Invece con il termine open source si indica un tipo di software in cui la licenza è "open", ciò significa che il software può essere modificato a piacimento [12].

Uno dei problemi che presenta questa moneta virtuale è la comprensione dei meccanismi che consentono di investire in essa. Essendo una criptovaluta non è regolamentata da nessun ente principale (come per esempio l'Euro), il suo andamento può essere molto volatile e indurre l'investitore alle volte a una consistente perdita di capitale.

L'obiettivo di questa tesi è quello di trovare, tramite l'utilizzo di alcune definizioni matematiche, un modello per prevedere il movimento di questa moneta nel breve e medio termine. Si potrà vedere, dopo numerosi test con dati storici del Bitcoin, come la costante di Lipschitz può aiutare l'investitore a definire qualche indicazione per ridurre quindi il rischio di investimento, cercando di aumentare il profitto. Altri strumenti utilizzati sono il polinomio approssimante e il calcolo della media mobile semplice (SMA), quest'ultimo già adottato nella letteratura associata alla criptovaluta. Abbinando l'uso della SMA alla costante di Lipschitz, si possono ricavare ulteriori informazioni che possono essere d'ausilio per l'investitore.

Capitolo 2

Bitcoin

In questo capitolo andremo a vedere come funziona il Bitcoin andandolo a descrivere per capire il suo funzionamento e cosa c'è alla base.

2.1 Cenni Storici

Il Bitcoin è stato ideato nel Gennaio del 2009 da Satoshi Nakamoto, pseudonimo utilizzato dal suo inventore che ancora ad oggi non ha svelato il suo vero nome. Proprio in quel periodo viene rilasciata la prima versione mettendo in pratica il concetto già conosciuto di "criptovaluta", descritto poco tempo prima da Wei Dai [5]. Molti esperti sostengono che la nascita di questa criptovaluta sia avvenuta in un periodo di grande crisi economico-finanziaria, apertasi negli Stati Uniti, per cercare di approfittare del momento di difficoltà delle banche e attirare quella parte di clientela delusa.

Nell'estate del 2010, un grave errore di sicurezza venne trovato nel protocollo della moneta dove le transazioni non venivano verificate correttamente prima di essere messe nella blockchain (si veda in seguito). Questa falla poteva consentire a malintenzionati di generare una quantità arbitraria di BTC, cosa che successe nei giorni successivi alla scoperta di questa falla che subito dopo venne chiusa per stabilizzare la situazione.

Negli anni a seguire il valore del BTC iniziò a crescere in maniera decisa passando da pochi euro agli attuali circa 9400€. Nel 2011 alcune associazioni iniziarono ad accettare il BTC per ricevere donazioni oppure utilizzarlo per aggirare blocchi finanziari. Negli anni successivi l'impiego del BTC ha preso piede e si è cominciato ad usare in ambito commerciale grazie a Coinbase, piattaforma digitale con sede in California dove venditori e consumatori possono scambiarsi criptovalute [2] e che permette ai siti internet di accettare pagamenti in BTC e convertirli nella valuta desiderata [6].

Qui di seguito possiamo vedere un grafico che riassume tutti i prezzi del BTC da fine 2015/inizio 2016 fino ad oggi.

Figura 2.1: Grafico dello storico BTC/EUR

2.2 Crittografia

Il Bitcoin fa un enorme utilizzo della crittografia e per capire i meccanismi che stanno alla base di questa criptovaluta è necessario introdurre alcuni concetti di crittografia.

Uno strumento alla base della comprensione del BTC è la *funzione hash*. Essa è una funzione che trasforma dati di lunghezza arbitraria in una stringa con dimensione fissa chiamata digest. Un punto fondamentale della funzione hash è che essa è unidirezionale, cioè non invertibile. Per esempio, se la funzione hash è: $h(k)=k \ mod \ n$, dove k è la chiave da cifrare e n numero arbitrario, si può vedere che per tornare al valore originario di k, conoscendo $h(k)$, è impossibile. Unico modo per passare da digest, cioè il valore dove è stata applicata la funzione hash alla stringa iniziale è utilizzare una ricerca di forza bruta o cercare di recuperare la funzione hash [18].

Altro strumento crittografico utilizzato nel BTC è la ***crittografia simmetrica*** conosciuta anche come *crittografia a chiave privata*. Essa prevede che per criptare un messaggio si utilizzi una chiave e, per leggerlo, il destinatario deve essere in possesso di tale chiave. Un problema di questo strumento è il fatto che mittente e destinatario devono essere sicuri di essere in possesso della stessa chiave e devono conservarla segretamente. Un esempio di crittografia a chiave simmetrica è il "Cifrario di Cesare". In questo metodo la chiave è un numero che va ad indicare di quante posizioni andare avanti e criptarla con quella lettere. Ad esempio, se si deve cifrare la parola "BITCOIN", prendendo come chiave il numero 5, la lettera "B" che, nell' nell'alfabeto classico, è nella seconda posizione si somma a 2 la nostra chiave (2+5=7) e andare a prendere la settima lettera dell'alfabeto che nel nostro caso corrisponde alla lettera "G". Proseguendo con questo metodo otterremmo la parola cifrata che sarà "GNYHTNS" [17].

Oltre alla crittografia a chiave simmetrica esiste la crittografia a ***chiave asimmetrica***, che consente di risolvere il problema della chiave nella crittografia simmetrica, cioè che la chiave per criptare e decriptare il messaggio deve essere in possesso sia al mittente e sia al destinatario ed essa può essere rubata durante lo scambio. In questo metodo, invece, si creano una coppia di chiavi dove una è detta privata e una pubblica. La chiave privata, generata in maniera casuale, viene utilizzata per decifrare il messaggio, invece la chiave pubblica, generata attraverso la chiave privata, grazie ad una funzione, viene utilizzata per cifrare il messaggio. Per utilizzare

questa crittografia, bisogna essere in possesso di un algoritmo per generare la chiave pubblica e privata. Un tipico algoritmo utilizzato è l'RSA che è molto efficace e si basa sulla fattorizzazione dei numeri primi, i cui passaggi sono:

1. *Scegliere due numeri p e q abbastanza grandi.*
2. *Calcolare n che non è altro che il prodotto tra p e q.*
3. *Scegliere un numero 'e' che deve avere due caratteristiche: deve essere più piccolo e coprimo con n.*
4. *Calcolare un numero d tale che il prodotto tra e*d sia congruo modulo 1.*

Una volta effettuati i passaggi possiamo andare a comporre la chiave pubblica e privata. La chiave pubblica sarà formata dalla coppia *(n,e)*, invece quella privata dalla coppia *(n,d)*. Per cifrare il messaggio utilizzeremo la chiave privata e quindi ci basterà elevare il messaggio (tradotto in decimale) al numero *e*. Poi al risultato dell'elevamento a potenza fare la divisione modulo n e quest'ultimo risultato sarà il messaggio criptato. Per decifrare il messaggio basterà prendere quello criptato, elevarlo a esponente d (che fa parte della chiave pubblica) e al risultato applicare modulo n. Il risultato finale sarà il messaggio iniziale. [16] [14]

2.3 Come funziona Bitcoin

Per effettuare transazioni, cioè scambi di BTC, si utilizzano software che forniscono portafogli digitali (wallet) dove poi risiederanno i BTC. A questi portafogli sono associate due chiavi: una pubblica e una privata. La chiave pubblica è una sequenza alfanumerica e va ad indicare l'indirizzo del portafoglio e sarà inoltre contenuta nella transazione insieme alla quantità di denaro da trasferire. La chiave privata servirà per firmare la transazione in maniera tale che il destinatario possa avere la prova che il denaro ricevuto arrivi proprio dalla persona desiderata.

Le transazioni avvengono in Internet e in base al protocollo P2P si può inviare/-ricevere denaro direttamente senza ricorrere a exchange andando a diminuire il costo delle commissioni. Gli exchange sono piattaforme online dove si possono depositare criptovalute e anche convertirle in valuta a corso legale oppure in altre criptovalute. Queste transazioni, prima di essere messe nella blockchain, vengono controllate andando a verificare due cose fondamentali: l'integrità e l'autenticazione. (vedere figura paragrafo "Cenni sulla Blockchain").

L'insieme di tutte le transazioni vanno a formare una moneta digitale. Questa catena viene allungata ogni volta che viene effettuata una transazione.

Uno dei problemi che affliggeva questa moneta era quello della tracciabilità della transazione, in quanto l'utente non aveva informazioni. Per risolvere questo problema, si utilizza un server di timestamp, che permette di mettere in ordine cronologico le varie transazioni. Esso calcola l'hash della transazione che vuole datare e lo pubblica su un database distribuito. Inoltre va a provare che la suddetta transazione esisteva già prima di calcolare l'hash e si riesce anche ad andare a ricavare datazioni anteriori. Inoltre, l'ordine di tutti i timestamp non può essere modificato a

piacimento, a meno che non si vada a ricostruire tutta la catena e questo comporta di avere una potenza di calcolo come quella del server di timestamp per cercare di ricostruire la catena con annessi calcoli di valore di hash.

Ogni timestamp contiene un numero variabile di transazioni, e la catena formata da tutti i timestamp viene chiamata blockchain. Essa è un database distribuito dove è contenuta tutta la cronologia delle transazioni di BTC in rete. Una transazione, una volta entrata nella blockchain, non può essere più annullata e quindi l'unico modo per ritornare in possesso della moneta e farsela ritornare mediante una nuova transazione. Essendo la blockchain un database distribuito, si possono verificare in ogni momento tutte le transazioni in tempo reale.

Un modo ulteriore di interagire con la blockchain, oltre a quello dello scambio di BTC già esistenti, è quello di minare (mining), cioè aggiungere blocchi alla blockchain. Questa attività è svolta da nodi speciali, detti minatori, i quali svolgono un duplice ruolo: verifica delle transazioni ed emissioni di BTC. Ovviamente, tutto questo lavoro, per i minatori, comporta l'utilizzo di un importante consumo di risorse di calcolo e di energia elettrica e per questo essi vengono premiati mediante l'emissione di nuovi BTC nel sistema.

Nonostante sembri conveniente essere dei minatori, se si ha la disponibilità dei mezzi, con l'andare degli anni per colpa del fenomeno chiamato "Bitcoin halving", che in italiano si traduce con "Dimezzamento Bitcoin", ha visto sempre di più diminuire il reward nei confronti dei minatori, cioè il premio in BTC dato ai minatori dopo aver aggiunto dei blocchi alla blockchain. Questo dimezzamento va a combattere l'inflazione che si va a creare, andando a diminuire il reward ad ogni dimezzamento, che si tiene circa ogni 4 anni [7].

I dati dicono che all'inizio si è partiti da un reward di circa 50 BTC nel 2012 e quattro anni dopo si è passati direttamente a 12,5 BTC di reward. Gli esperti affermano che, dopo il prossimo dimezzamento che avverà circa nel Maggio del 2020, il reward di BTC passerà addirittura a 6,25 andando a raggiungere poi con i prossimi dimezzamenti, la soglia dello zero [1].

In questo periodo, però, il numero di BTC disponibile nel sistema si sta piano piano esaurendo in quanto serve una potenza di calcolo sempre maggiore per gestire le transazioni (ruolo dei minatori) e con l'andare del tempo, e con l'aumento delle transazioni, i minatori stanno scomparendo portando a una diminuzione di BTC. Nel mondo del BTC restano molti dubbi sul valore esatto dei BTC esistenti. Infatti, molti articoli, affermano che esistono dei depositi (cioè wallet digitali) in cui risiedono BTC e in essi non sono mai state svolte delle operazioni. Per adesso si può dire che nel sistema ci sono ancora da estrarre circa il 14,70% di BTC e in circolazione ce ne sono 17.896.250,0. [4]

2.4 Cenni sulla Blockchain

La Blockchain gestisce tutte le transazioni che avvengono nel mondo dei BTC. Essa non è altro che un registro digitale aperto e distribuito dove vengono registrate tutte le transazioni (ragruppandole in blocchi) in maniera sicura, verificabile e permanente. Una volta che il blocco è stato scritto sulla blockchain non può essere eliminato

né modificato. La blockchain aumenterà la dimensione sempre di più, formando una lista sicura (grazie all'utilizzo della crittografia) di blocchi.

La struttura di un blocco è composta da un numero variabile di transazioni e la sua dimensione varia in base alla grandezza di queste transazioni. L'header di un blocco, che sono dei metadati che contengono un riassunto di tutto quello che è contenuto nel blocco, è formato dalle seguenti informazioni:

- **Versione**: si intende quella del software utilizzato.
- **Hash del blocco precedente**: è l'hash che fa riferimento al blocco precedete, andando così a collegare tutti i blocchi.
- **Timestamp**: indica la datazione dell'ultima transazione effettuata che è dentro al blocco.
- **Bits**: è il valore corrente target.
- **Nonce**: valore che serve per far sì che l'output della funzione hash sia minore o al massimo uguale al valore target.
- **Numero di transazione**: è l'id della transazione.

Ogni volta che un blocco viene validato (che è il processo di mining) viene inserito nella blockchain.

Nella immagine sottostante si può vedere come nella blockchain presa in considerazione, suddivisa in 2 blocchi di transazioni ("Blocco 1" e "Blocco 2"), è stata compiuta ed è in corso di validazione una transazione TR8.

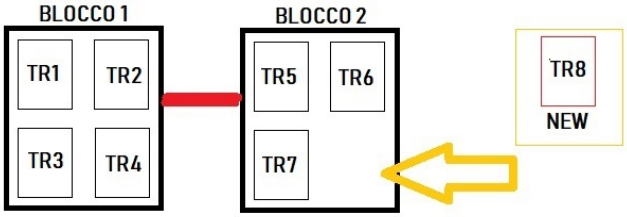

Figura 2.2: Blockchain prima della validazione della transazione

Successivamente alla sua validazione, TR8 verrà inserita nel Blocco2 e quest'ultimo verrà aggiunto nella Blockchain. La Blockchain si presenterà nel seguente modo, pronta ad accettare ulteriori blocchi di transazioni validate [15].

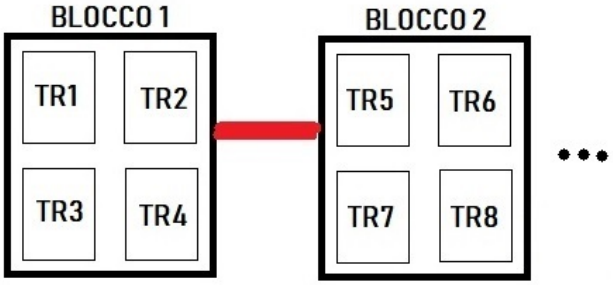

Figura 2.3: Blockchain dopo la validazione della transazione

Uno degli attacchi più famosi che si può effettuare sulla Blockchain viene chiamato “Attacco del 51%”. Questo attacco serve per inserire nella Blockchain blocchi (e quindi transazioni) falsi all’interno della rete. Per effettuare l’attacco bisogna che almeno il 51% della rete della Blockchain debba essere sotto il controllo del medesimo gruppo di minatori. Successivamente, essi possono inserire nella Blockchain blocchi falsi contenenti operazioni fraudolente. Questo attacco è stato effettuato pochissime volte, infatti fonti storiche dicono che, per quanto riguarda la Blockchain del BTC, c’è stato solo un attacco del 51% avvenuto circa nel 2014 [3].

Capitolo 3

Elementi di teoria dell'approssimazione: il polinomio approssimante

In questo capitolo verrà introdotto il concetto di approssimazione polinomiale, come trovarlo mediante formule e utilizzando il software MATLAB.

3.1 Definizione

Il polinomio approssimante è un polinomio che approssima i punti dati con un errore minimo. Quindi, non si cerca un polinomio che passi esattamente per quei punti, bensì uno che passi in maniera approssimativa per quei punti.

Il teorema che ci viene in aiuto qundo si parla di polinomio approssimante è quello di Taylor, il quale afferma che alcune funzioni sotto opportune ipotesi possono essere approssimate a un polinomio, andando a diminuire sempre di più l'errore fino ad arricare a 0 [10].

3.2 Metodi per calcolarlo

Esiste principalmente un metodo semplice per calcolare il polinomio approssimante che utilizza il *polinomio di Lagrange*.

Il ***polinomio di Lagrange*** è una particolare approssimazione polinomiale. Essa afferma che data una funzione *f(x)* e *n+1* punti, per cui sono noti i valori $\mathbf{f_1}$, $\mathbf{f_2}$,...,$\mathbf{f_n}$, si definisce polinomio approssimante della funzione f il polinomio

$$P(x) = \sum_{i=0}^{n} f(a_i) \prod_{j!=i}^{n} \frac{x - a_j}{a_i - a_j} \tag{3.1}$$

[19]

3.3 Come trovarlo con Matlab

Per andare a calcolare il polinomio approssimante si può utilizzare un software, MATLAB, dedicato al calcolo numerico scritto in linguaggio C. Esso consente di manipolare per lo più matrici e vettori, visualizzare funzioni, implementare algoritmi e fare calcoli che per altri software sarebbero troppo laboriosi. Mediante i moltissimi comandi per la gestione dei polinomi forniti da questo software ci sono quelli per trovare il polinomio approssimante. Per individuarlo si possono usare i seguenti 2 comandi:

- **Polyfit(X,Y,n)**: con questo comando si va a determinare il polinomio di ordine n che "fitta", cioè collega, meglio le coppie di punti contenute nei vettori X e Y. n è il grado del polinomio che si vuole ottenere. Come output da un vettore con i coefficienti del polinomio.
- **Polyval(p,X)**: con questo comando si va a valutare il polinomio p calcolato in precedenza nei punti del vettore X. p sarà un vettore di $n+1$ punti dove questi punti sono saranno altro che i coefficienti del polinomio calcolato precedentemente. Come output darà una matrice con tutti i punti che serviranno poi a disegnare il grafico.

Un esempio di utilizzo dei due comandi è il seguente:

```
X = [valori del vettore X];
Y = [valori del vettore Y];

p=polyfit(X,Y,6);

pol=polyval(p,X);

plot(X,pol);
```

Come possiamo vedere, nell'algoritmo qui sopra abbiamo due vettori X ed Y in cui sono presenti rispettivamente i giorni (cioè l'asse delle ascisse) e i valori giornalieri di chiusura del BTC (cioè l'asse delle ordinate). Questi due vettori vengono passati in input alle funzioni *polyfit* aggiungendo anche il grado del polinomio risultante. Il risultato viene dato in input alla funzione *polyval* insieme al vettore dei giorni. Il risultato della funzione viene poi passato in input al comando *plot*, che vuole come parametri di input il vettore X dei giorni e il risultato calcolato precedentemente, che ci permette di plottare il grafico a video. Questo è il modo più veloce per trovare il polinomio approssimante. Esistono altri metodi da poter utilizzare con MATLAB, basterà implementare un algoritmo apposito.

Capitolo 4

Costante di Lipschitz

In questo capitolo affrontiamo in maniera teorica, la costante di Lipschitz ed inoltre verrà vista l'applicazione che può avere nel mondo delle criptovalute, e in particolare nel Bitcoin. Più che la costante di Lipschitz si analizzerà cos'è una funzione Lipschitziana e la sua costante.

4.1 Definizione

Secondo la matematica una funzione a variabile reale si può definire Lipshitziana quando essa ha una crescita limitata, cioè il rapporto tra variazione di ordinata e ascissa non supererà mai un valore fissato chiamato **costante di Lipschitz**.

Un uso molto importante della lipschitzianità viene fatto nella risoluzione dei problemi di Cauchy in merito alle equazioni differenziali.

La condizione di Lipshitzianità è la seguente:

$$|f(x'') - f(x') \leq L \cdot |x'' - x'| \tag{4.1}$$

I punti *x"* e *x'* sono scelti nel dominio della funzione presa in considerazione. [13]

Il concetto di lipschitzianità risulta molto più forte del concetto di continuità, infatti si può affermare che se una funzione è lipschitziana, essa sarà anche continua. Ma il concetto di lipschitzianità è meno forte della derivabilità. Quindi è una condizione che si trova a metà tra continuità e derivabilità. Una cosa è sicura: la costante di Lipschitz non è in stretta correlazione con la derivabilità di secondo grado. [8]

4.2 Significato geometrico

Per capire la funzionalità che può avere l'utilizzo della costante di Lipschitz nel Bitcoin è bene comprendere come può essere interpretata graficamente per intuirne poi l'efficacia. Il seguente grafico riporta in blu la funzione *sin(x)*cos(4x)* e in rosso le rette *1.5x* e *-1.5x*.

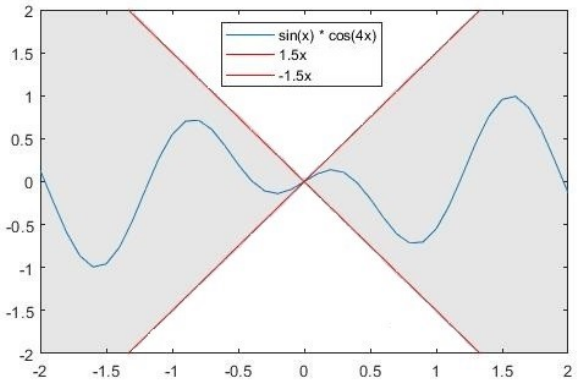

Figura 4.1: Costante di Lipschitz

Prendendo in considerazione la funzione *sin(x)*cos(4x)* e applicando la definizione di Lipschitz vista in precedenza, si ottiene come costate di Lipschitz *K=1.5*. Questo significa che prendendo un qualsiasi punto della funzione, e andando a disegnare le rette passanti per quel punto con coefficiente angolare 1.5 e -1.5, la funzione *sin(x)*cos(4x)* starà dentro alla zona che si è creata, che nel grafico è in grigio chiaro.

La costante di Lipschitz non verrà calcolata ogni giorno per vedere dove si posizionerà il grafico del BTC rispetto ad essa, ma verrà definita settimanalmente e successivamente si andrà a determinare la spezzata passante per tutte le costanti trovate in tutta la settimana. Si rinvia tutta la spiegazione di tutto il procedimento ai capitoli successivi.

4.3 Uso della costante di Lipschitz per la previsione del prezzo del Bitcoin

Come già detto nel paragrafo 4.2, in questo studio non si usa completamente l'interpretazione geometrica classica della costante di Lipschitz. Verrà calcolata sulla base dei dati in possesso in quell'istante di tempo, il valore settimana per settimana, della costante con riferimento al valore di chiusura del BTC. Una volta trovati i punti, si troverà la spezzata passante per quei punti. Calcolata la spezzata, la si confronterà con il grafico del BTC in quel momento e si proverà a fare delle previsioni in base alla pendenza di tale spezzata oppure in base alla posizione del grafico del BTC rispetto alla spezzata. In seguito verrà riportata l'analisi dei vari modelli trovati.

Per calcolare la costante di Lipschitz e quindi della sua spezzata, si sono create delle piccole funzioni in MatLab che ci permettono in primo luogo di calcolare tutto il necessario con facilità e in maniera parametrica.

Per calcolare la costante di Lipschitz, la funzione implementata (che chiameremo *searchLip*) è la seguente:

```
function [costante]=searchLip(x,xx,vettY)
    ris=abs(vettY(xx)-vettY(x));
    costante= ris / abs(xx-x);
end
```

Alla funzione *searchLip* vengono passati 3 parametri: *x'*, *x"* e il vettore da considerare per applicare la *fromula*. Essa restituirà alla fine il valore della costante di Lipschitz e per trovarla si è usata la formula classica vista in precedenza.

Trovato tutte le costanti di Lipschitz settimana per settimana, si andrà a trovare in primo luogo la retta passante per ogni punto trovato e successivamente la spezzata unendo tutte le rette precedentemente trovate. La funzione che permette di trovare le varie rette è la seguente:

```
function [eq]=searchRetta(xp,yp,vettx,m)
    eq=m*vettx+((m*-xp)+yp);
end
```

Alla funzione vengono date in input le coordinate del punto *(xp,yp)*, il vettore di tutti i punti della settimana ed infine il coefficiente angolare, che in questo caso sarà, la costante di Lipschitz appena trovata. Quest'ultima verrà passata con segno positivo quando il valore del Bitcoin cresce, oppure con segno negativo quando il valore del Bitcoin nella settimana decresce, cioè la differenza tra primo giorno della settimana e l'ultimo è positiva e negativa nel secondo caso.

Trovata la spezzata, questa viene messa a confronto con il grafico della funzione del BTC ed analizzare i due grafici per capire le informazioni e dedurre un nostro modello. Tutto questo verrà approfondito nel prossimo capitolo, dove si entrerà nel dettaglio dei modelli trovati.

Capitolo 5

Analisi modello di previsione a breve/medio termine

In questo capitolo si entrerà nel dettaglio dei tre modelli di previsione per il BTC trovati utilizzando la costante di Lipschitz (nello specifico la spezzata di Lipschitz), il polinomio approssimante e la SMA.

5.1 Primo modello: utilizzo spezzata di Lipschitz

Il primo modello di previsione analizzato riguarderà il confronto fra la spezzata di Lipschitz e il grafico delle quotazione giornaliere del BTC.

Per calcolare la spezzata di Lipschitz, verrà utilizzato il metodo visto nel precedente capitolo, basato sul calcolo della costante di Lipschitz settimanalmente e sull'individuazione della spezzata passante per tutti i punti. Per quanto riguarda la funzione del BTC, verranno presi i valori del BTC giornalieri e rappresentati graficamente.

Per effettuare un confronto su questi due grafici, si effettuano delle prove e delle previsioni su dati storici del BTC. In particolare sono stati presi in considerazione come mesi di riferimento Febbraio, Marzo, Aprile, Maggio, Giugno, Luglio, Agosto dell'anno 2019. Per ogni mese sono stati presi i dati del valore in chiusura del BTC e calcolato, per ciascun mese, la spezzata di Lipschitz. Nel seguente grafico verrà analizzato nello specifico il mese di Febbraio 2019.

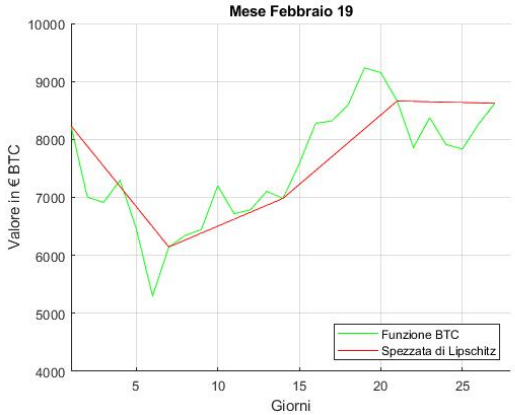

Figura 5.1: Grafico Febbraio 2019 con BTC e spezzata di Lipschitz

Nell'asse delle ascisse sono stati riportati i giorni e nell'asse delle ordinate è stato riportato il valore nella valuta Euro del prezzo del BTC. Tutti i valori storici in Euro del BTC sono stati trovati nel sito https://it.investing.com/crypto/bitcoin/btc-eur-historical-data. Con il colore rosso viene rappresentata la spezzata di Lipschitz e con il colore verde la funzione del BTC. Si può vedere che in alcuni momenti, la spezzata di Lipschitz, varia la sua pendenza passando da una pendenza positiva ad una pendenza negativa. Questa pendenza varia, ovviamente, ogni fine settimana visto che essa è calcolata settimanalmente.

Una prima previsione basata sul medio temine (base settimanale) è quella di valutare la pendenza della retta. Si può dire che se la pendenza della spezzata, alla fine della settimana presa in considerazione, ha valore positivo allora il mercato per la settimana successiva sarà *rialzista*, cioè il valore del BTC tenderà a salire. Se invece la pendenza della retta è negativa, allora il mercato per la settimana che sta per iniziare è *ribassista*. Come si può vedere in questo grafico nell'ultima settimana, la spezzata di Lipschitz non dà indicazioni sulla pendenza, quindi sarebbe molto difficile individuare una previsione. Per risolvere il problema entrerà in gioco il polinomio approssimante che, insieme alla spezzata, ci può offrire un modello più preciso.

Prendendo la seconda settimana (dal 7 al 14) del grafico di Febbraio 2019 sopra riportato, si può vedere come, alla fine della settimana, la spezzata ha pendenza positiva. Questo significa che per la terza settimana di Febbraio (14-21) il mercato, con molta probabilità ma senza avere la totale certezza, sarà rialzista. La previsione, quindi, potrà rivelarsi veritiera.

Utilizzando la spezzata di Lipschitz, si può ricavare un'altra previsione, però questa a breve termine e cioè su base giornaliera. Questo significa che ogni giorno essa può essere fatta per il giorno successivo. Non si prenderà in considerazione la pendenza della spezzata, bensì il posto in cui si trova la spezzata rispetto alla quotazione del BTC. Come mostrato nei grafici riportati sopra, nel momento in cui la spezzata è al di sopra del grafico del BTC, il mercato il giorno successivo sarà in fase rialzista. Al contrario, quando invece la spezzata sta al di sotto del grafico del BTC allora il mercato sarà ribassista. Prendendo in considerazione la prima settimana del mese di Marzo 2019, si può vedere come la spezzata di Lipschitz ogni giorno è al di sotto del grafico del BTC. Questo dice che, prendendo un giorno di quella settimana, il mercato del giorno successivo molto probabilmente sarà ribassista.

Di seguito si riportano i grafici dei mesi di Marzo, Aprile, Maggio, Giugno, Luglio e Agosto in cui si può verificare la correttezza del primo modello.

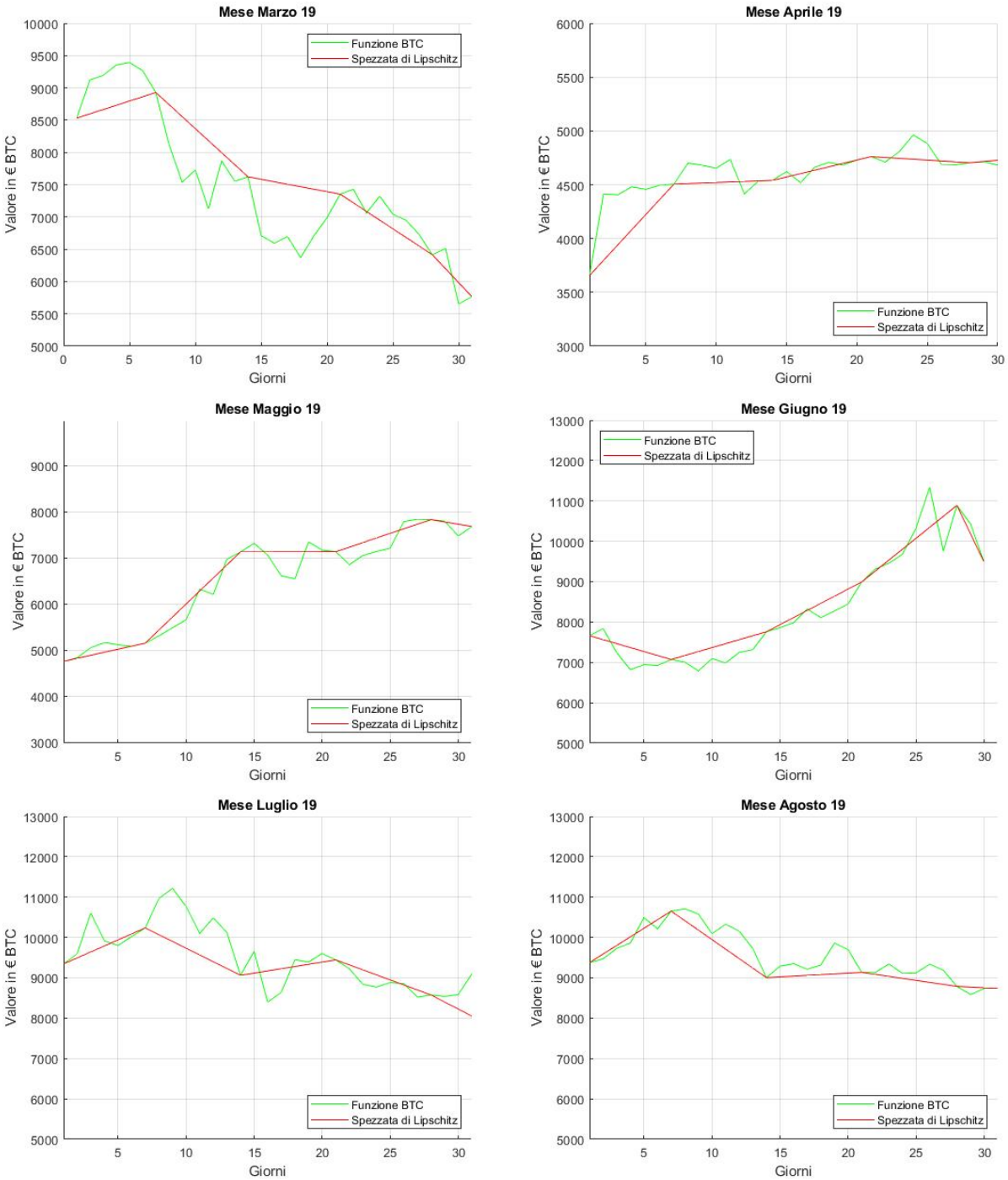

Figura 5.2: Grafici Marzo,Aprile,Maggio,Giugno,Luglio,Agosto

5.2 Secondo modello:utilizzo polinomio approssimante

Oltre alla spezzata di Lipschitz, è possibile costruire un modello di previsione a medio termine, utilizzando il polinomio approssimante. Nel capitolo 3 si spiega, dal punto di vista matematico cos' è un polinomio approssimante e si dice che esso permette di approssimare il grafico del BTC nei punti noti. Per arrivare al modello finale di previsioni sono stati fatti degli studi per individuare un grado del polinomio che permettesse di rappresentare al meglio il polinomio approssimante, perché più il grado del polinomio è alto, il suo grafico si avvicina al grafico vero e proprio del BTC andando a perdere l'utilità di approssimare un polinomio. Di seguito riportiamo i grafici di ogni mese con i rispettivi polinomi approssimanti di grado 6,8,10,12,20 e vediamo quali polinomio tenere in considerazione.

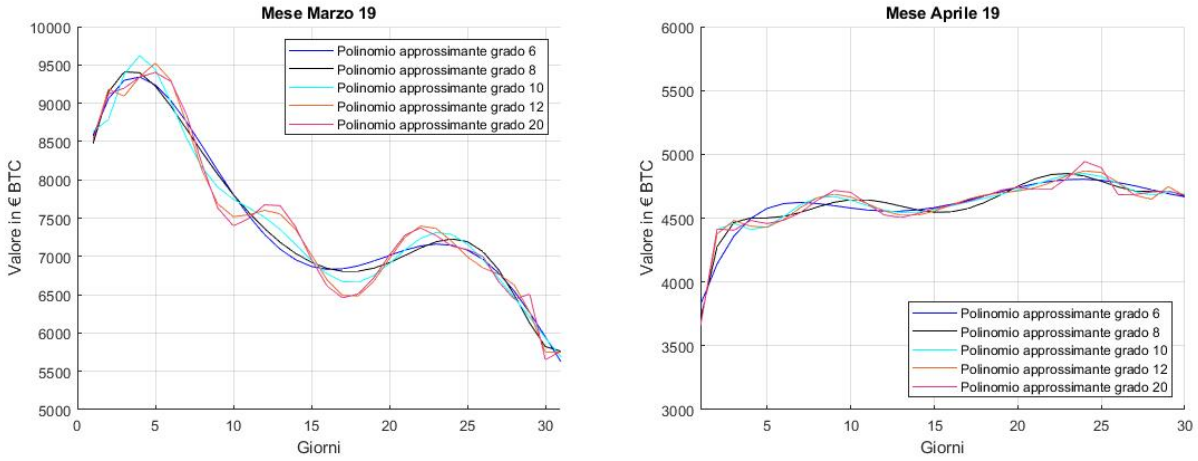

Figura 5.3: Grafici Marzo,Aprile

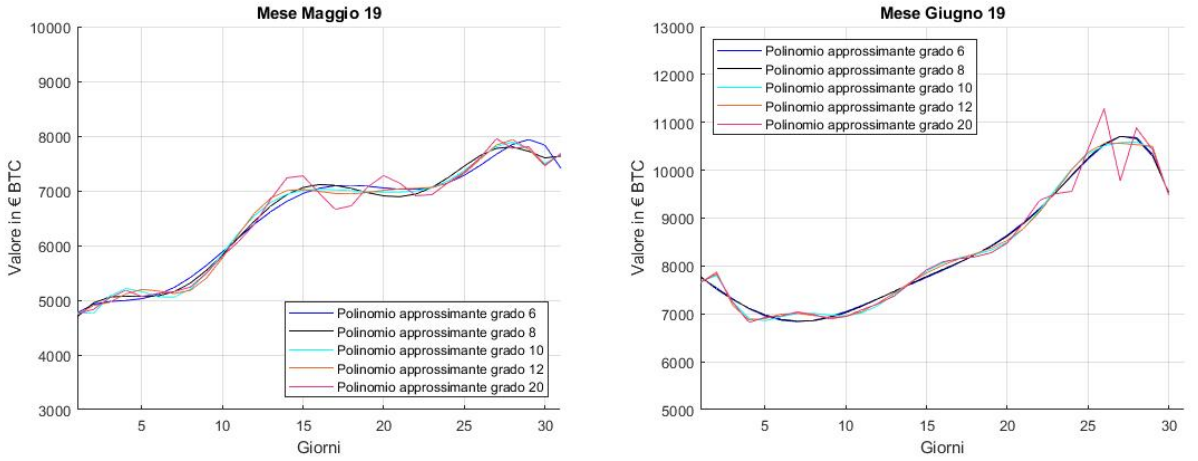

Figura 5.4: Grafici Maggio,Giugno

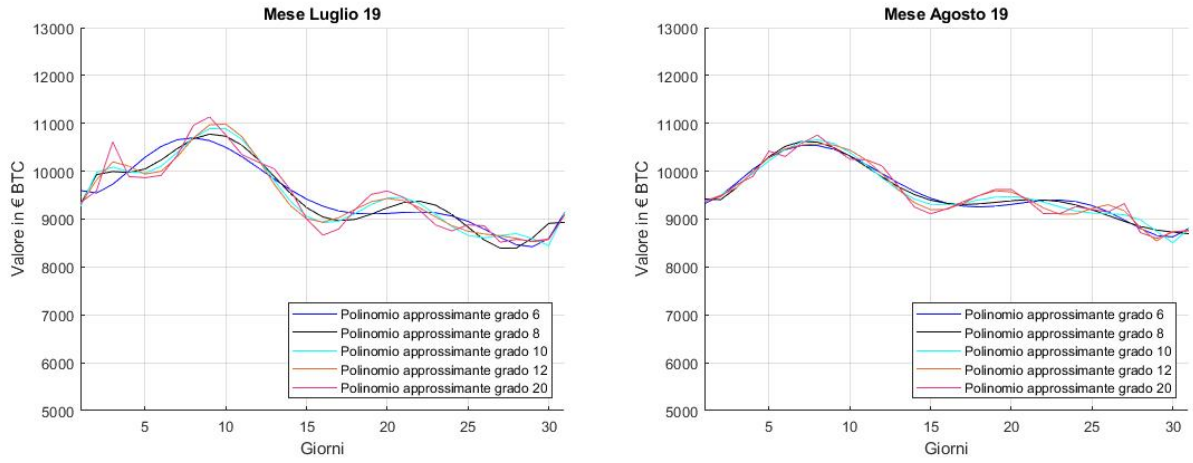

Figura 5.5: Grafici Luglio,Agosto

Possiamo vedere che il polinomio di grado 20 (di colore rosa) risulta molte oscillazioni, cioè ha molti punti di picco, proprio come sarebbe fatto un grafico del BTC. Per questo, scegliere un polinomio di grado 20 da confrontare con il grafico del BTC risulta poco utile in quanto l'approssimazione non dà informazioni utili. Per quanto riguarda gli altri gradi, si può vedere come svolgano meglio il lavoro di approssimatori.

Un confronto interessante tra polinomi approssimanti e grafico del BTC lo si può vedere nei seguenti grafici.

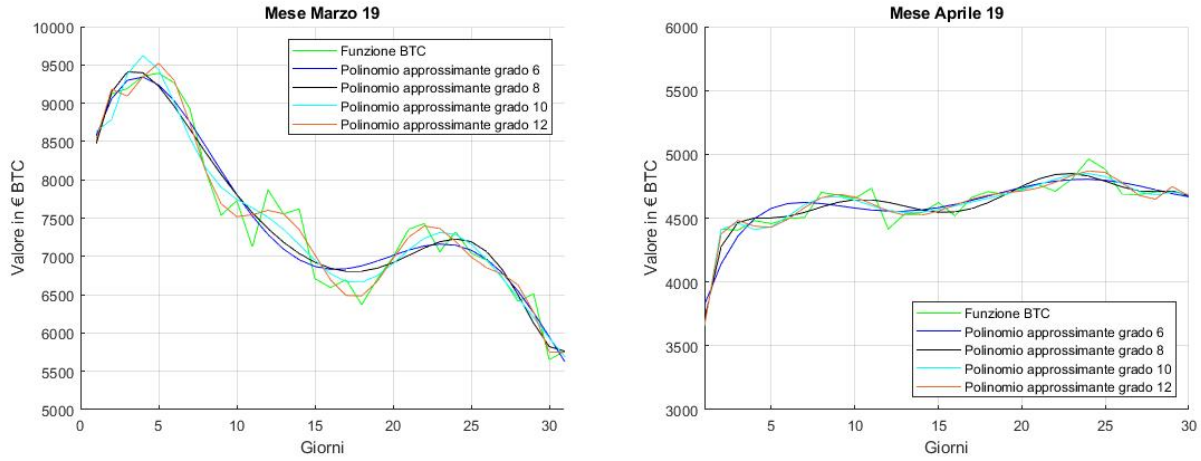

Figura 5.6: Grafici Marzo,Aprile

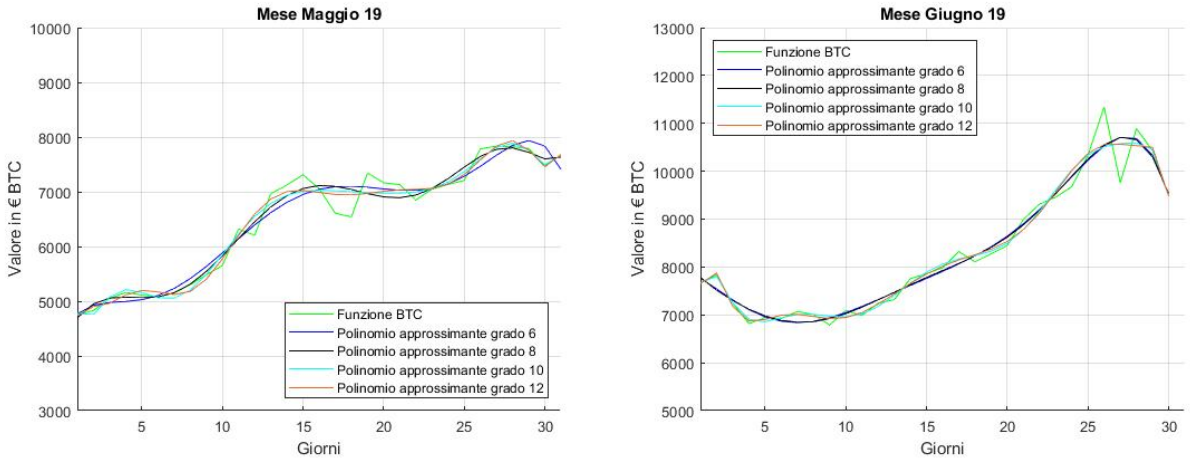

Figura 5.7: Grafici Maggio,Giugno

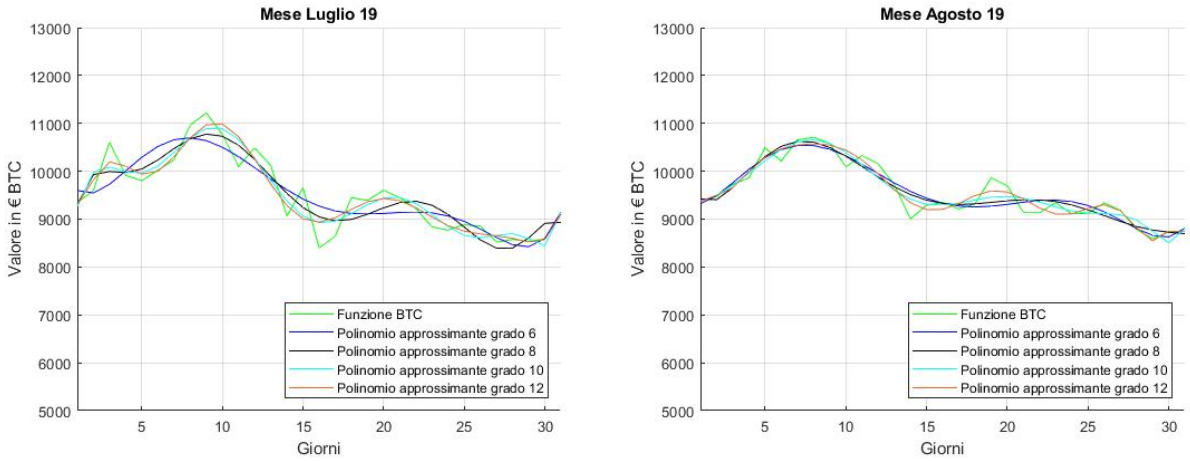

Figura 5.8: Grafici Luglio,Agosto

In questi grafici, vengono messi a confronto tutti i polinomi approssimanti, che sono stati trovati, escludendo quindi il polinomio di grado 20, con la funzione BTC. Si può osservare che il polinomio di grado 12, in alcuni punti va addirittura a sovrapporsi con il grafico del BTC. Quindi difficilmente da informazioni in più. Anche il polinomio di grado 10 risulta poco approssimante. Dei buoni polinomi approssimanti sono quelli di grado 8 e di grado 6 che si prenderanno in considerazione per il nostro nuovo modello.

Il nuovo modello che si può delineare utilizzando il polinomio approssimante, valuta la concavità e convessità del polinomio approssimante. Prima di analizzare i grafici e il modello, verranno date indicazioni relativamente alla convessità e concavità di una funzione. Una funzione si dice convessa quando, dati due punti qualsiasi del grafico, il segmento che li unisce giace sopra la funzione oppure coincide con una parte di essa. Invece, una funzione si dice concava se, sempre presi due punti qualsiasi del grafico il segmento che li unisce giace al di sotto della funzione stessa oppure coincide con una parte di essa [9].

Per quanto riguarda il nuovo modello, esso va a guardare la relazione di convessità e concavità con il grafico del BTC. Se il polinomio approssimante è concavo

allora il mercato a medio termine (quindi su base settimanale) sarà ribassista. Al contrario, il mercato (a medio termine) sarà rialzista. Come accennato nel paragrafo precedente, non sempre la costante di Lipschitz può darci delle indicazioni sul mercato del BTC. Un esempio di quando non dà nessuna informazione è quando la spezzata del BTC non ha né pendenza negativa né pendenza positiva (come si può vedere nella figura (FEB19) in cui nell'ultima settimana la spezzata non dà indicazioni di pendenze particolari). Qui di seguito vengono riportati i grafici per ogni mese mettendo insieme grafico del BTC e spezzata di Lipschitz.

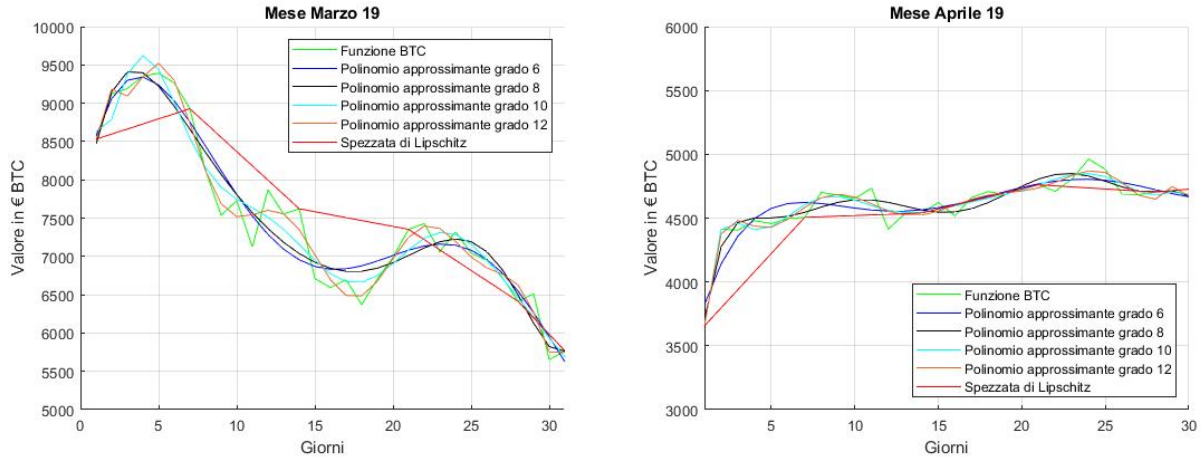

Figura 5.9: Grafici Marzo,Aprile

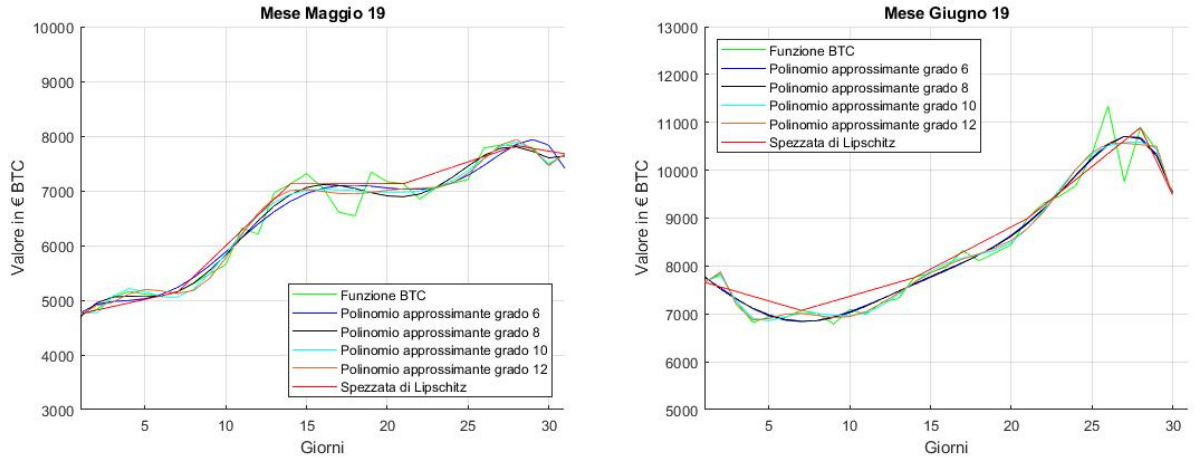

Figura 5.10: Grafici Maggio,Giugno

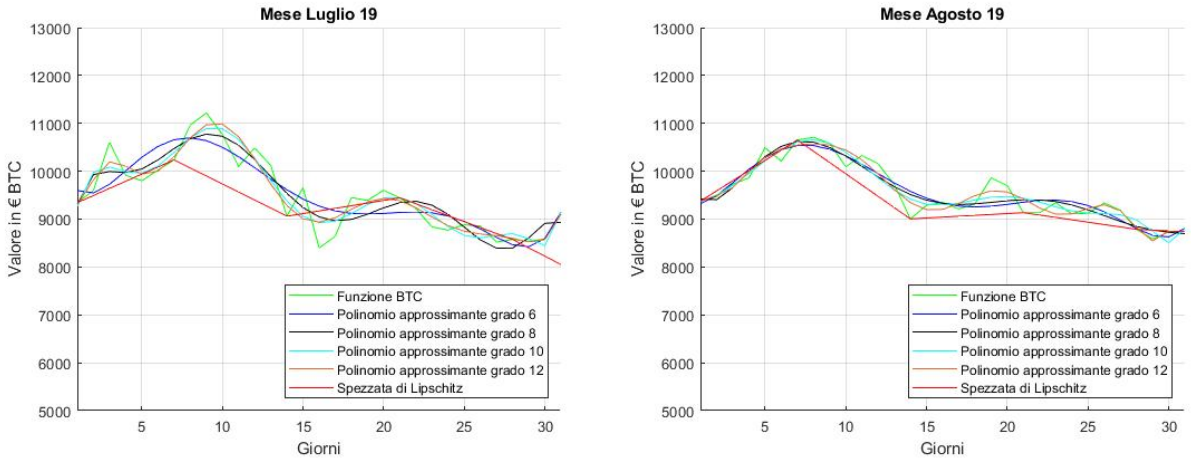

Figura 5.11: Grafici Luglio,Agosto

Dal momento in cui la spezzata di Lipschitz non dà informazioni precise, si possono utilizzare la concavità e convessità del polinomio approssimante per arrivare alla conclusione dando una previsione sempre a medio termine.

5.3 Terzo modello: utilizzo SMA

In questo ultimo modello di previsione, utilizziamo un nuovo indicatore che viene già usato negli indici di borsa e nelle criptovalute che applica il concetto di media mobile. Questo indice si chiama Media Mobile Semplice (SMA). Le medie mobili sono molto utili perché attraverso delle formule è possibile ricavare l'andamento del prezzo di un qualche indice di borsa, di valuta o, in questo caso, di criptovaluta. In questo tipologie di medie, il numero di elementi (i prezzi) è fisso, e la cosa che varia avanzando è la finestra temporale. Entrando nel particolare della media, la SMA consiste in una classica media aritmetica, che va a sommare tutti i prezzi del BTC di N periodi e, alla fine, va a dividere tutto per N. La formula è la seguente:

$$SMA = \frac{1}{N}\sum_{i=1}^{N} C_i \tag{5.1}$$

Di seguito viene presentato l'algoritmo che permette di calcolare la SMA:

```
function [media]= SMA(n,vettY,valInizio)
  media = 0;
  volte = n;
  while volte > 0
    media = media + vettY(valInizio);
    valInizio = valInizio +1;
    volte = volte - 1;
  end
  media = media / n;
end.
```

All'algoritmo viene passato in ingresso n che sarebbero il numero del valore su cui calcolare la media mobile (in questo caso calcolandola settimanalmente è pari a 7), il vettore *vettY*, che contiene i valori del BTC ed infine *valInizio*, che sta ad

indicare il valore di partenza (posizione del vettore, utile per l'algortimo). All'interno della funzione creata c'è un *ciclo while* che effettua le operazioni come nella formula sopra riportata. Alla fine, la funzione restituirà il valore della media per la settimana presa in considerazione e verranno svolti i seguenti calcoli per poi *plottare* tramite il comando plot il grafico:

```
n=7;
valInizio = 1;
media=zeros(1,25);
i=1;
while valInizio+n <= length(yM)+1
  media(i) = SMA(n,yM,valInizio);
  valInizio = valInizio + 1;
  i = i+1;
end
Xmedia = 7:31;
plot(Xmedia,media,'m');
```

Nel ciclo while si va a scorrere tutto il vettore dei giorni, richiamando la nostra funzione SMA sopra analizzata. Infine, dopo aver calcolato tutto il necessario, si va a creare un vettore di giorni, in quanto la media la si calcola di settimana in settimana, e a plottare i risultati passando al comando *plot* il vettore *Xmedia,media* dove, in quest'ultimo, saranno contenuti tutti i valori calcolati dalla funzione SMA.

Si può vedere come questo metodo è molto semplice dal punto di vista del calcolo, ma presenta dei difetti in quanto ogni prezzo ha la stessa rilevanza. Ciò significa che l'ultimo prezzo alla fine ha lo stesso peso dell'ultimo e via dicendo. Per correggere questo problema esiste una nuova formula che in questo caso non verrà affrontata in quanto la SMA risulta più che sufficiente per l'implementazione del nostro modello [11].

Dopo questa breve spiegazione, si entrerà nel dettaglio del nuovo modello di previsione, in cui si andrà a mettere a confronto la SMA e la spezzata di Lipschitz, come si può vedere nei seguenti grafici sotto riportati:

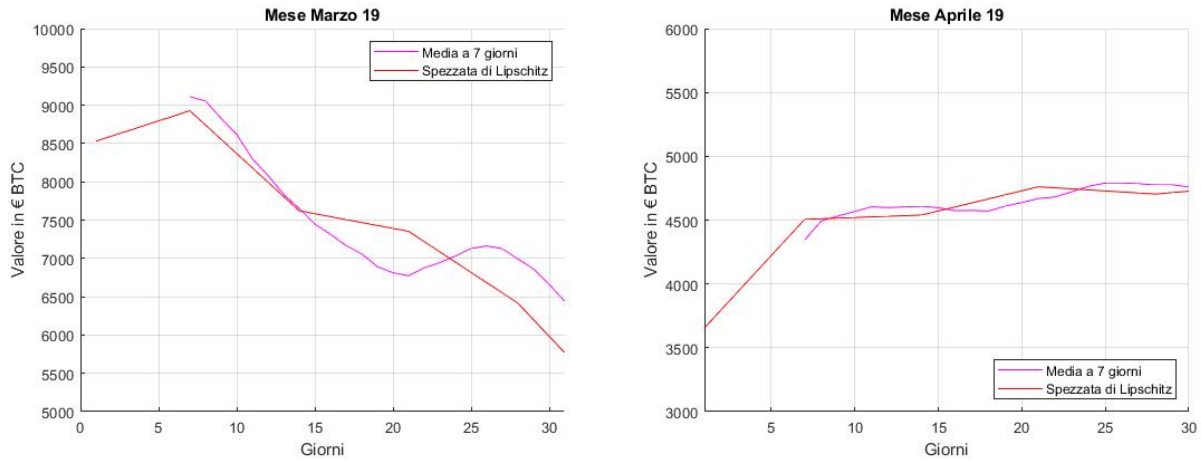

Figura 5.12: Grafici Marzo,Aprile

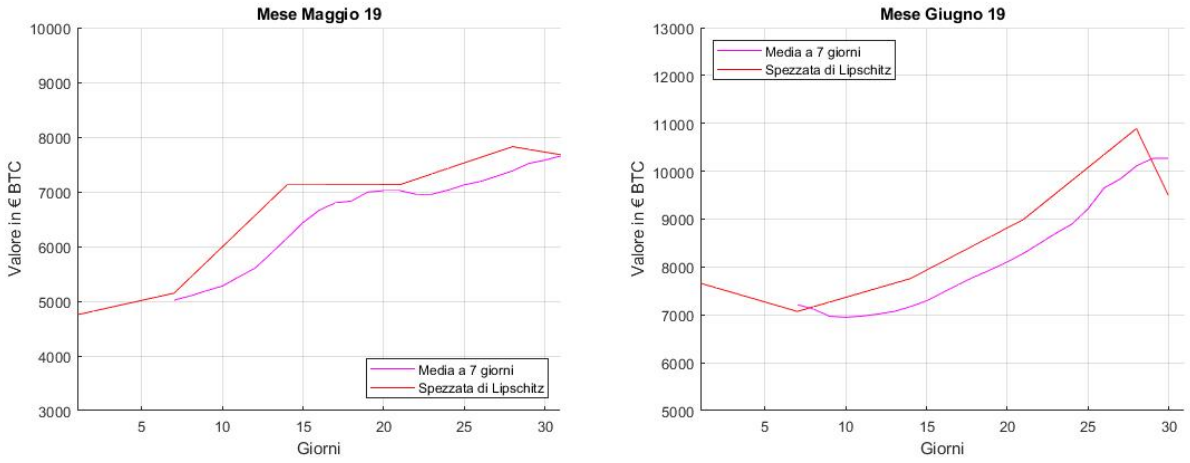

Figura 5.13: Grafici Maggio,Giugno

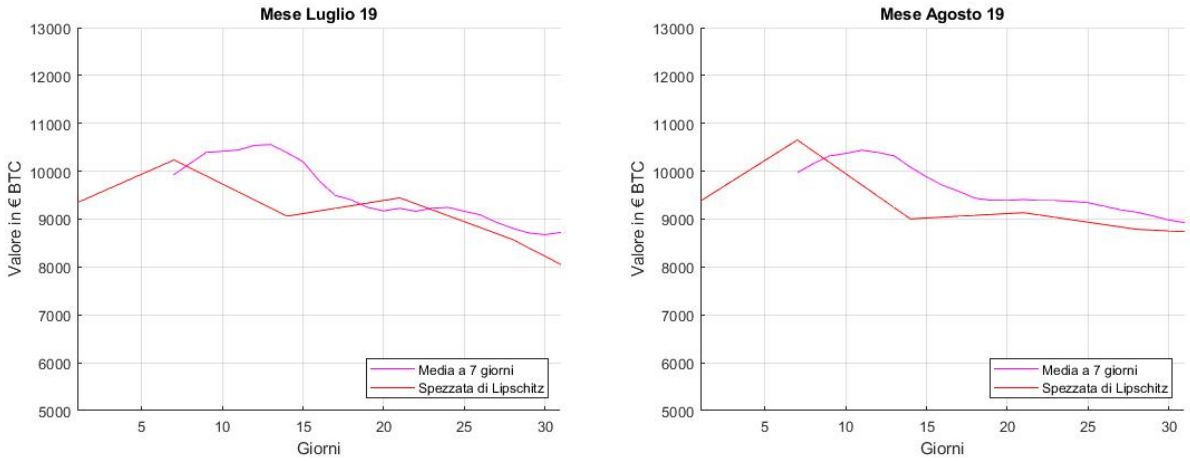

Figura 5.14: Grafici Luglio,Agosto

Nel caso in cui la SMA è al di sotto della spezzata di Lipschitz alla chiusura della settimana, allora si può dire che nel medio termine (su base settimanale) il mercato è rialzista. Altrimenti, se a fine settimana il grafico della SMA è al di sopra della spezzata, quasi sicuramente il mercato a inizio della settimana successiva sarà ribassisita.

Come tutti i modelli precedenti, questa previsione non sarà sempre vera, ma ci darà una buona base per un futuro investimento.

Capitolo 6

Conclusioni

Questo studio ha cercato di trovare dei possibili modelli di previsione per cercare di aiutare l'investitore a massimizzare il guadagno cercando di limitare le possibili perdite che possono creare le criptovalute, essendo molto fluttuanti. Al giorno d'oggi gli unici metodi di previsione che si possono avere online, sono delle analisi fatte da economisti utilizzando indici e trend del mercato, ma senza usare la costante di Lipschitz e polinomi approssimanti.

I modelli trovati, come spiegato durante il capitolo dove si sono analizzati i vari modelli, non sono validi sempre per tutte le previsioni, ma c'è una probabilità di 8/10 che la previsione effettuata si avveri. Sempre riguardo ai modelli trovati, essi vanno sempre ad effettuare previsioni a breve/medio termine e mai a lungo termine, questo perché il valore BTC varia molto durante la giornata e quindi risulta difficile fare una considerazione di questo tipo. Tutte le considerazioni però, vanno a porre delle basi per cercare in un futuro di trovare un modello che, mettendo insieme le previsioni a medio termine, porti a una previsione più o meno precisa a lungo termine. Questo darebbe la possibilità all'investitore di avere una certa libertà e sapere che non deve effettuare compravendita di criptovalute ogni giorno/settimana.

Nell'analisi è stato sempre preso in considerazione il BTC come criptovaluta, ma questi modelli trovati possono essere utilizzati anche con altre criptovalute come Etherum, Litecoin e molte altre. Tutti i grafici descritti e riportati nei capitoli precedenti sono tutti riproducibili mediante gli algoritmi sopra descritti e utilizzando il software MATLAB.

Bibliografia

[1] Giuliano Balestreri. *Bitcoin sugli scudi: ecco perché il prezzo potrebbe continuare a salire fino all'anno prossimo*. URL: https://it.businessinsider.com/bitcoin-sugli-scudi-ecco-perche-il-prezzo-potrebbe-continuare-a-salire-fino-allanno-prossimo/?refresh_ce.

[2] Coinbase. *Coinbase*. URL: https://www.coinbase.com/.

[3] Cryptonomist. *Attacco 51*. URL: https://cryptonomist.ch/2019/09/14/attacco-51-hashrate-blockchain/.

[4] Cryptonomist. *Quanti bitcoin ci sono*. URL: https://https://cryptonomist.ch/2018/09/19/bitcoin-in-circolazione.

[5] Wei Dai. *Wei Dai*. URL: http://weidai.com/bmoney.txt.

[6] Oksana Kimrnytska. *Bitcoin:limiti e soluzioni tecniche della scalabilità*.

[7] Andrea Lagni. *Bitcoin [BTC]: il dimezzamento del 2020 porterà ad un aumento dei prezzi già nel 2019*. URL: https://www.criptovalute24.com/bitcoin-btc-il-dimezzamento-del-2020-portera-ad-un-aumento-dei-prezzi-gia-nel-2019/#Bitcoin_Halving_che_cose_e_come_funziona.

[8] You Math. *Funzione lipschitziane*. URL: https://www.youmath.it/lezioni/analisi-due/equazioni-differenziali/622-funzioni-lipschitziane.html.

[9] You Math. *Funzioni concave e convesse*. URL: https://www.youmath.it/lezioni/analisi-matematica/le-funzioni-da-r-a-r-in-generale/3476-funzione-concava-funzione-convessa.html.

[10] R.Bevilaqua D. Bini M.Capovani O. Menchi. *Appunti di Calcolo Numerico*. URL: http://pages.di.unipi.it/bevilacq.

[11] Money. *Le medie mobili cosa sono e come si calcolano*. URL: https://www.money.it/Le-medie-mobili-cosa-sono-come-si#cos'%5C%C3%5C%A8.

[12] OpenSource.org. *The Open Source Definition*. URL: https://opensource.org/osd.

[13] Matematica e scuola. *Funzione lipschitziane*. URL: http://www.matematicaescuola.it/materiale/analisi/funzioni_continue/20140924_funzioni_lipschitziane_Teoria_esercizi.pdf.

[14] Wikibooks. *Crittografia/RSA*. URL: https://it.wikibooks.org/wiki/Crittografia/RSA.

[15] Wikipedia. *Blockchain*. URL: https://it.wikipedia.org/wiki/Blockchain.

[16] Wikipedia. *Crittografia asimmetrica*. URL: https://it.wikipedia.org/wiki/Crittografia_asimmetrica.

[17] Wikipedia. *Crittografia simmetrica*. URL: https://it.wikipedia.org/wiki/Funzione_crittografica_di_hash.

[18] Wikipedia. *Funzione crittografica di hash*. URL: https://it.wikipedia.org/wiki/Funzione_crittografica_di_hash.

[19] Wikipedia. *Interpolazione di Lagrange*. URL: https://it.wikipedia.org/wiki/Interpolazione_di_Lagrange.

[20] Wikipedia. *Peer-to-Peer*. URL: https://it.wikipedia.org/wiki/Peer-to-peer.