Università
Ca'Foscari
Venezia

Corso di Laurea magistrale

in

Economia e gestione delle aziende

Tesi di Laurea

Bitcoin e Litecoin: un'analisi dei dati

Relatore

Ch. Prof. Giovanni Fasano

Correlatrice

Ch. Prof.ssa Paola Ferretti

Laureando

Luca Storer

Matricola 988885

Anno Accademico

2019 / 2020

Indice

Introduzione

Il mio elaborato di tesi riguarda le criptovalute, in particolare Bitcoin e Litecoin, insieme all'analisi di dati.

L'obiettivo del lavoro è quello di fornire un'analisi delle caratteristiche principali delle criptovalute e analizzare alcuni dati numerici su di esse, riguardanti principalmente la quantità in circolazione, la quantità prodotta ogni anno e il valore di mercato.

La motivazione che mi ha spinto ad approfondire questo argomento è stato il mio interesse verso le tecnologie collegate all'economia in un ambito, quello delle criptovalute, che non avevo mai approfondito in passato.

Il primo capitolo introduce la moneta e le criptovalute, dando ad entrambe una definizione, per poi spiegare le rispettive caratteristiche principali. Inoltre si è cercato di capire se, dal punto di vista tecnico e legale, le criptovalute possano essere classificabili come una moneta.

Il secondo capitolo si focalizza sulla più famosa tra le criptovalute, cioè Bitcoin, con un approfondimento sulle sue caratteristiche tecniche e sulle tecnologie che ha adottato.

Il terzo capitolo è incentrato sullo Stock-to-Flow, indice che viene di solito utilizzato per valutare la scarsità (o l'abbondanza) di alcune risorse, come i metalli preziosi. Questo indice può essere utilizzato anche per le criptovalute, dato che alcune sono disponibili in quantità limitata, in quanto la loro creazione è predeterminata da un algoritmo. Verrà approfondito il modello Stock-to-Flow di Bitcoin, un modello che sostiene che l'aumento della scarsità di Bitcoin comporti l'aumento del valore di mercato della criptovaluta stessa.

Il quarto capitolo tratta delle criptovalute alternative create dopo la nascita di Bitcoin, le Altcoin. Infatti, dato che il codice sorgente di molte criptovalute è pubblico, è possibile scaricarlo e modificarlo a piacimento. Questo comporta che molti programmatori abbiano approfittato di ciò per creare nuove criptovalute con l'intento di crearne di migliori, aggiungendo o togliendo funzionalità, modificando i parametri, senza andare a modificare le funzionalità salienti delle criptovalute originali. In questo modo non si mette a rischio il valore della criptovaluta originaria e soprattutto non si mettono a rischio le persone che la possiedono.

Il quinto capitolo introduce la criptovaluta Litecoin con le sue caratteristiche e le differenze che presenta rispetto a Bitcoin, da cui ha preso gran parte del codice sorgente. È stato poi calcolato un modello simile al modello Stock-to-Flow su Bitcoin, per verificare se il valore di Litecoin è influenzato dalla sua scarsità.

Inoltre, siccome alcuni trader, cioè coloro che investono giocando sulle variazioni del tasso di cambio, sono convinti che le quotazioni di Litecoin anticipino quelle di Bitcoin, nel sesto capitolo è stata fatta un'analisi di dati con una rete neurale, cioè un modello matematico di intelligenza artificiale, per verificare se quest'ipotesi possa essere vera.

Capitolo 1

La moneta e le criptovalute

1.1 La moneta

La natura della moneta è cambiata nel tempo: originariamente si parlava di moneta merce, infatti la moneta era costituita da alcuni materiali, come l'oro e l'argento, che attribuivano un valore di mercato all'oggetto che fungeva da mezzo di scambio; poi fu introdotta la moneta rappresentativa, come le banconote, convertibili in oro o argento; oggi, nell'economia moderna si parla la moneta fiduciaria, la quale non ha valore intrinseco e non può essere convertita in oro o argento. La moneta fiduciaria è emessa da una banca centrale che si impegna a mantenere stabile il suo valore nel tempo e la comunità, sulla fiducia che verrà mantenuto questo impegno, accetta questa moneta come mezzo di scambio e riserva di valore, e assume valore legale: «la moneta legale è la moneta dotata del potere di estinguere le obbligazioni in denaro, riconosciuta come tale dall'ordinamento giuridico. L'unica forma di moneta legale è la moneta contante emessa da una banca centrale - per l'euro la Banca Centrale Europea (BCE) - in quanto la sua creazione si basa su rigorose procedure che garantiscono la fiducia generale nella moneta e la stabilità del suo valore nel tempo»[1]. La valuta è «il termine generico per indicare le monete in circolazione e i titoli fiduciari che le rappresentano»[2].

Oggi può essere considerata moneta anche se non ha carattere di fisicità, come quella nei depositi bancari. «La moneta digitale, o elettronica, costituisce valore monetario memorizzato, ad esempio, in una carta prepagata o uno smartphone. Gli addebiti diretti, i pagamenti in Internet e quelli con carta sono tutte forme di pagamento che non implicano l'uso di contante. (Tra gli sviluppi più recenti vi sono persino le valute digitali decentrate o i circuiti di moneta virtuale come Bitcoin, che funzionano senza un'istanza di controllo centralizzata quale una banca centrale. Da un punto di vista giuridico non sono considerati moneta»[3].

1.2 La crittografia e le criptovalute

La crittografia è «l'insieme delle teorie e delle tecniche (manuali, meccaniche o elettroniche) che permettono di cifrare un testo in chiaro, cioè di ottenerne un crittogramma, impiegando una chiave di cifratura, e di decifrare un crittogramma impiegando una chiave di decifratura»[4].

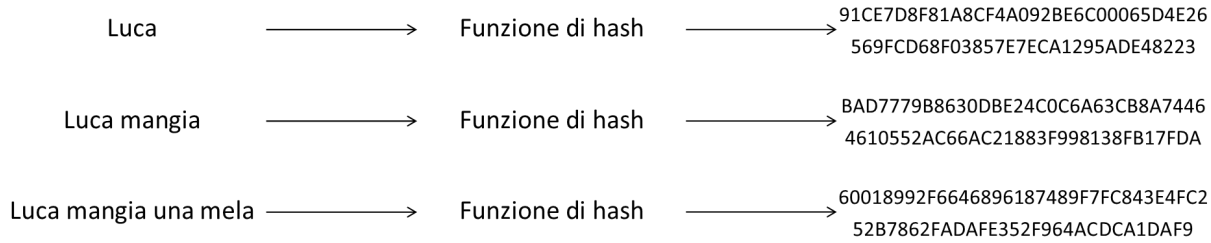
[1] https://economiapertutti.bancaditalia.it/informazioni-di-base/moneta-legale-scritturale/index.html
[2] http://www.treccani.it/vocabolario/valuta/
[3] https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.it.html
[4] http://www.treccani.it/vocabolario/crittografia/

Una criptovaluta (cripto = nascosto, coperto), o valuta virtuale, è «la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente»[5].
Le criptovalute sono basate sulla crittografia, la quale viene utilizzata per vari scopi, come ad esempio per firmare le transazioni, verificarle, controllare la creazione di moneta e garantire la privacy degli utenti.
Le criptovalute non esistono in forma fisica perché sono digitali. Sono detenute nei wallet, cioè dei portafogli digitali/elettronici, ed è possibile scambiarle via Internet tra utenti oppure comprare beni e servizi in alcune attività commerciali che le accettano come mezzo di pagamento.
Le criptovalute costituiscono un'attività per chi le detiene senza essere la passività per un altro ente. Il denaro che una persona detiene nel conto corrente è un'attività, cioè un credito del proprietario e nel contempo è una passività per la banca, perché è un debito che la banca si impegna a convertire in contanti nel caso venga richiesto. Da questo punto di vista, le criptovalute assomigliano all'oro.

1.2.1 La funzione di hash

Nella crittografia vengono utilizzate le funzioni di hash per trasformare i messaggi in messaggi criptati, in modo da non renderli leggibili a terzi.
L'hash è una funzione non invertibile che trasforma una stringa alfanumerica di qualsiasi lunghezza in una stringa, sempre alfanumerica, di lunghezza predefinita (in base al tipo di funzione di hash utilizzata), che prende il nome di ***digest***; Bitcoin usa la funzione di hash SHA-256, che era la più sicura funzione crittografica di hash disponibile al tempo, che trasforma i messaggi di input in un *digest* composto da 256 bit.

Figura 1.1: Esempio della stessa funzione di hash (SHA-256) che converte tre messaggi diversi



Come si può notare dalla Figura 1.1 i vari *digest* hanno lo stesso numero di caratteri e sono molto diversi tra loro, nonostante le frasi in input presentino piccole variazioni.

[5]D.lgs. 90/2017 (art. 1, comma 2, lett. qq). Recepimento della Direttiva UE 2018/843 del 30 maggio 2018, art. 1 (d), cfr. Parlamento Europeo (2018)

Siccome una funzione di hash è una funzione non invertibile che genera un risultato variabile e casuale, se si volesse ricavare il valore originario è necessario che un calcolatore provi il maggior numero di input casuali al secondo finché non viene trovato quello corretto. L'hashrate è un'unità di misura per valutare la potenza di calcolo di un dispositivo. Indica il numero di hash, e quindi il numero di calcoli al secondo, che un dispositivo è in grado di fare: maggiore è il suo valore, maggiore è la velocità del dispositivo nell'applicare funzioni di hash ad input casuali. Maggiore è l'hashrate, maggiore è la velocità nel trovare il valore originario.

1.2.2 La crittografia asimmetrica: chiave pubblica e privata

Le criptovalute fanno largo uso dei metodi crittografici per codificare in modo sicuro le informazioni. In particolare viene utilizzata la crittografica asimmetrica: un sistema crittografico che prevede l'associazione ad ogni persona coinvolta in una comunicazione di una coppia di chiavi per criptare e decriptare dei messaggi.
«Le due chiavi, chiamiamole A e B, possono essere usate alternativamente per cifrare o decifrare un messaggio, nel senso che il messaggio cifrato con A può essere decifrato con B e il messaggio cifrato con B può essere decifrato con A. Ogni persona coinvolta nello scambio di messaggi possiede dunque una coppia di chiavi che agiscono, di fatto, l'una come l'inverso dell'altra»[6].
Quando viene creata una coppia di chiavi, una viene resa pubblica, cioè è visibile da chiunque, può essere distribuita a più persone e prende il nome di chiave pubblica, mentre l'altra deve rimanere segreta e conservata in modo sicuro e prende il nome di chiave privata.

Esempio

A vuole mandare un messaggio a B.
A cripta il messaggio utilizzando la chiave pubblica di B e lo invia nella rete. Una volta arrivato a destinazione, B lo decripta utilizzando la sua chiave privata (si presume che solo B la conosca) e legge il messaggio.

Figura 1.2: Esempio: A invia un messaggio a B

Grazie a questo sistema i messaggi sono inviati in modo sicuro perché se un altro soggetto dovesse appropriarsi del messaggio, per leggerlo, dovrebbe possedere la chiave privata di

[6] http://www.programmiamo.altervista.org/File/critto/critto8.html

B, perché è l'unica chiave in grado di decifrarlo ed è per questo motivo che deve rimanere al sicuro.
È possibile utilizzare le coppie di chiavi in modo leggermente diverso, cioè per la firma digitale: il mittente cripta il messaggio con la sua chiave privata e poi lo cripta nuovamente utilizzando la chiave pubblica del destinatario. Quando il messaggio arriva al destinatario, lo decripta utilizzando la sua chiave privata e poi lo decripta un'altra volta utilizzando la chiave pubblica del mittente. Quest'ultimo passaggio permette al destinatario di verificare se il messaggio è stato inviato dal vero mittente, perché solo la chiave pubblica del mittente è in grado di decifrare il messaggio che dovrebbe essere stato cifrato con la chiave privata del mittente stesso.

Esempio

A vuole mandare un messaggio a B.
A cripta il messaggio utilizzando la sua chiave privata, poi cripta il risultato ottenuto utilizzando la chiave pubblica di B e lo invia nella rete. Una volta arrivato a destinazione, B lo decripta utilizzando la sua chiave privata e poi decripta con la chiave pubblica di A. Se riesce a leggere il messaggio significa che è stato effettivamente A ad inviarlo (si presume che solo A conosca la sua chiave privata), perché solo la chiave pubblica di A può decifrare un messaggio criptato con la chiave privata di A.

Figura 1.3: Esempio: A invia un messaggio a B

1.3 Le criptovalute sono una moneta?

Le criptovalute, come indicato nella definizione in sezione 1.2, attualmente non sono una moneta dal punto di vista giuridico perché non sono validamente riconosciute dalla legge per l'adempimento di obbligazioni di pagamento, nessun ente centrale le emette e non vi è l'obbligo di accettazione al momento dell'offerta.
Inoltre, perché possano essere considerate moneta, devono rispettare alcune caratteristiche. «La moneta, in qualsiasi sua forma, assolve tre diverse funzioni. È un mezzo di scambio, un mezzo di pagamento con un valore in cui tutti confidano. La moneta è anche unità di conto che permette di attribuire un prezzo a beni e servizi. Ed è anche riserva di valore»[7].

Mezzo di scambio Le criptovalute sono un mezzo di scambio ma solo nella dimensione immateriale, non hanno valore intrinseco e sono pochissime le persone che le accettano

[7]https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.it.html

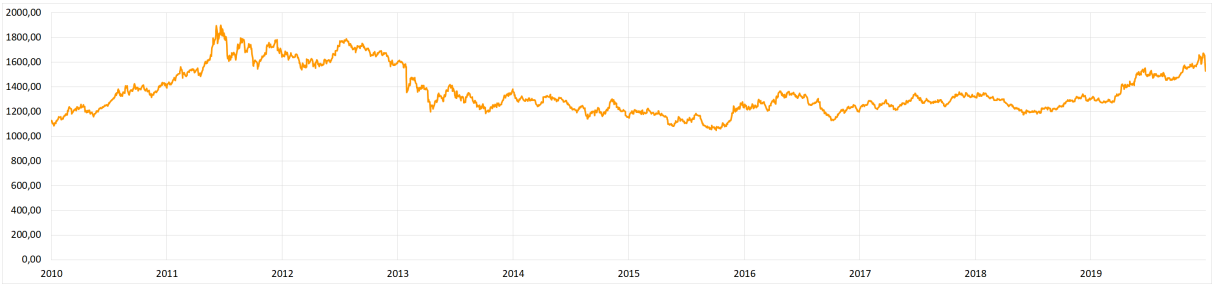
come mezzo di pagamento. Inoltre ottenere ad esempio dei bitcoin è possibile se si è un miner (colui che estrae criptovalute attraverso dei calcoli, vedi 2.3 a pagina 25), che possiede numerosi e potenti computer per produrli in autonomia, altrimenti si è costretti a comprarli online in siti specializzati che siano sicuri. Per le criptovalute non è prevista alcuna risoluzione delle controversie, per cui in caso di frode non è possibile effettuare un rimborso e questa situazione è aggravata dal fatto che gli utenti sono protetti dalla pseudonimia e dalla crittografia, che rendono gli utenti difficili da identificare. Inoltre, il tempo impiegato per effettuare una transazione è più alto rispetto all'acquisto di beni e servizi in un negozio fisico: una transazione in criptovalute richiede un tempo di conferma che, in base alla commissione inclusa, può variare da pochi secondi, a molte ore e a volte giorni. Una differenza considerevole rispetto al pagamento in contanti, o con carte di credito/debito, che dura pochi secondi.

Unità di conto Siccome le criptovalute hanno frequenti fluttuazioni del valore, (vedi Figura 1.5) che derivano da domanda e offerta, è difficile utilizzarle come unità di conto, cioè come unità numerica standard per misurare il valore di beni e servizi per paragonarli tra loro. Inoltre, dato che il valore di una singola criptovaluta è relativamente elevato[8] rispetto al valore di molte merci (come i generi alimentari o di prima necessità), per valutare la differenza di prezzo tra loro bisognerebbe usare molti decimali, rendendo più complicati i confronti.

Riserva di valore La funzione di riserva di valore in una moneta è data dal fatto che il proprietario detiene moneta, fisicamente in casa o in una banca, in un certo momento nel tempo, per scambiarla nel futuro con beni e servizi, presupponendo che la moneta mantenga il suo valore e il prezzo dei beni non subisca variazioni eccessive nel tempo. Le criptovalute hanno un'alta volatilità, il loro valore è instabile e cambia frequentemente nel corso del tempo rispetto alle valute ufficiali, oppure ad asset meno volatili come l'oro (vedi Figura 1.4) e ciò non le rende adatte al risparmio, ma sono verosimilmente più un bene speculativo su cui investire.

[8] Al 23 aprile 2020, un bitcoin (la criptovaluta più famosa) vale 7081,36$. Un litro di latte da 1,5$ varrebbe circa 0,00021 bitcoin, oppure 21.000 satoshi, sottomultiplo di bitcoin.

Figura 1.4: Prezzo dell'oro (oz) in dollari americani, dal 2010



Fonte dati: https://mercati.ilsole24ore.com/materie-prime/commodities/oro/GLD

Figura 1.5: Prezzo di un bitcoin in dollari americani, dal 2010

Fonte dati: https://coinmetrics.io/data-downloads-2/

Nella Figura 1.4 è possibile osservare l'andamento del prezzo di un'oncia di oro in un periodo di dieci anni mentre la Figura 1.5 mostra l'evoluzione nel tempo del prezzo in dollari di un bitcoin. Come si può notare, il prezzo dell'oro mostra un andamento abbastanza regolare con variazioni di prezzo lievi da un anno all'altro, mentre nel caso del prezzo dei bitcoin in Figura 1.5, soprattutto a partire dal 2017 cioè quando la criptovaluta ha iniziato a essere più conosciuta, si notano variazioni piuttosto marcate anche da un mese all'altro nel corso degli anni. L'oro è considerato un bene rifugio, cioè un bene che tende a non perdere valore nel tempo a causa di eventi nel mercato. Invece i bitcoin da alcuni vengono ancora visti come un investimento speculativo piuttosto che moneta e riserva di valore, dato che il loro prezzo è molto volatile.

«Le criptovalute rappresentano beni privati, poiché sono presenti in quantità scarsa per costruzione, accessibili ed utili. Infatti secondo la teoria economica, i beni sono qualunque mezzo (materiale o immateriale) o servizio, impiegabile per la soddisfazione di un bisogno umano oppure per la produzione di altro bene»[9].

Quindi la criptovaluta è comunque un bene, perché disponibile in quantità limitate, accessibile e utile per i bisogni umani, ma non soddisfa pienamente e contemporaneamente le funzioni della moneta tradizionale.

[9] A. Contaldo e F. Campara. *Blockchain, criptovalute, smart contract, industria 4.0. Registri digitali, accordi giuridici e nuove tecnologie*. Pisa: Pacini Giuridica, 2019, p. 173.

1.4 La legge italiana sulle criptovalute

Secondo la legge italiana, le criptovalute sono da considerare come redditi finanziari prodotti all'estero, per cui vanno indicate nel Modello Unico.
Secondo l'art. 4 del decreto legge n. 167/1990, convertito in legge n. 227/1990, nel primo comma:
«Le persone fisiche, gli enti non commerciali e le società semplici ed equiparate ai sensi dell'articolo 5 del testo unico delle imposte sui redditi, di cui al decreto del Presidente della Repubblica 22 dicembre 1986, n. 917, residenti in Italia che, nel periodo d'imposta, detengono investimenti all'estero ovvero attività estere di natura finanziaria, suscettibili di produrre redditi imponibili in Italia, devono indicarli nella dichiarazione annuale dei redditi».
I destinatari di questa norma devono riportare i redditi imponibili nel quadro RW del Modello Unico, precisamente nella colonna 3 inserendo il codice 14 (Altre attività estere di natura finanziaria) e, nel caso non vengano utilizzate criptovalute per investimenti, devono segnare la casella nella colonna 20, poiché non si è tenuti alla liquidazione della IVAFE (Imposta sul valore delle attività finanziarie detenute all'estero) ma solo al monitoraggio fiscale: il semplice possesso di criptovalute non è considerato investimento in depositi bancari e quindi non si è soggetti a questa imposta.
Il TAR del Lazio, con una sentenza pubblicata il 28 gennaio 2020, si è espresso in merito alla assoggettabilità a trattamento fiscale dell'utilizzo di moneta elettronica:
«Gli atti con i quali, nell'approvare le istruzioni per la compilazione del Modello Unico Persone Fisiche 2019, si indicano come da inserire nel quadro RW, tra i redditi finanziari di provenienza estera, anche le valute virtuali, non hanno natura costitutiva della corrispondente obbligazione tributaria, ma sono meramente ricognitivi di obblighi dichiarativi già esistenti, come definiti ai sensi degli artt. 1 e 4, d.l. n. 167 del 1990, convertito in l. n. 227 del 1990 (modificati dal d.lgs. n. 90 del 2017) e nei relativi limiti; come tali non sono lesivi (1). Nel quadro ordinamentale italiano vigente, l'impiego di moneta virtuale è rilevante ai fini dell'art. 67 del TUIR, ai sensi del quale è soggetto a tassazione laddove (e nella misura in cui) generi materia imponibile»[10].
Quindi non è il possesso di criptovalute che fa scattare il trattamento fiscale, diversamente dal loro investimento in operazioni finanziarie.

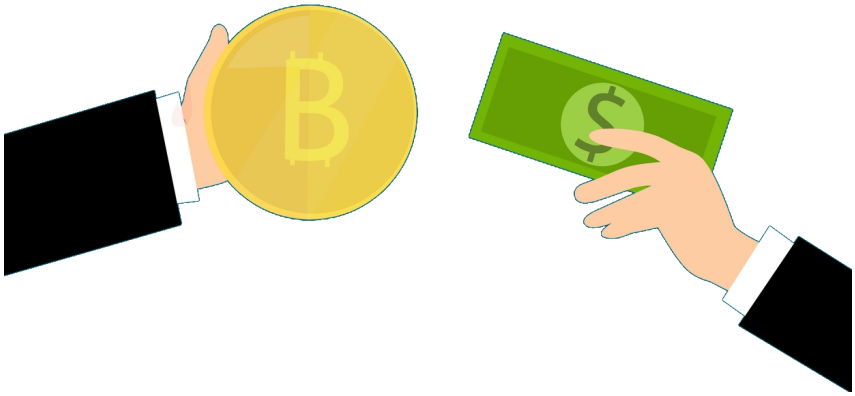
1.5 Currency exchange (Cambiavalute)

L'exchange è un sito che permette di scambiare criptovalute in cambio di moneta legale o di altre criptovalute, e viceversa.
Gli exchange funzionano principalmente come punto di incontro per compratori e venditori, infatti, ad esempio, una persona può decidere il prezzo e la valuta a cui vendere una certa

[10]https://www.giustizia-amministrativa.it/-/tassazione-della-moneta-elettronica-

quantità di criptovalute e il sito cercherà di trovare un compratore disposto a comprare a quel prezzo. L'exchange è una piattaforma che funziona come una borsa valori, infatti l'utente non sa da chi sta acquistando o a chi sta vendendo, perché l'exchange funge da intermediario e gli scambi sono fatti in modo automatico, in cambio di una commissione che va all'exchange. Ogni exchange vende e compra valuta ad un proprio prezzo e quindi possono esserci prezzi diversi tra gli exchange per la stessa valuta.
Queste piattaforme vengono utilizzate anche per il trading, cioè per scambiare valuta col fine di guadagnare sulle variazioni del tasso di cambio.

Figura 1.6: Bitcoin in cambio di dollari



Fonte: https://pxhere.com/en/photo/1444947

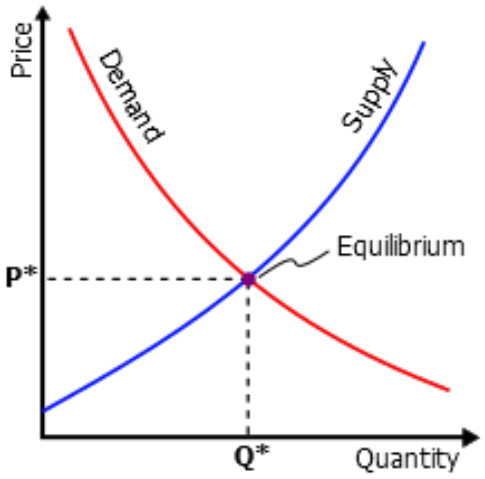
Gli exchange presentano alcune funzioni tipiche delle banche, perché si ha la possibilità di aprire un conto dove depositare valute (e criptovalute) tra quelle supportate dalla piattaforma; inoltre consentono di effettuare trasferimenti tra utenti.
La particolarità è che quando una transazione avviene tra due utenti dello stesso exchange, non viene registrata nel registro pubblico della criptovaluta (cioè la blockchain, vedi 2.2 a pagina 18) come transazione da un portafoglio all'altro, ma vengono solo registrati i movimenti di moneta, cioè una variazione nel saldo delle parti coinvolte. Gli exchange, come le banche, non hanno fisicamente tutta la moneta che dichiarano di avere, ma tengono una riserva giornaliera per poter garantire i prelievi di denaro da parte degli utenti. Infatti, l'exchange è come se detenesse un debito verso l'utente che ha depositato la valuta, e si impegna a ripagarlo, quando richiesto. Ad esempio, se detenessi 1 BTC nel mio conto e decidessi di venderlo, il saldo del conto diventerebbe di circa 8000$, all'attuale tasso di cambio. Non ci sono movimenti reali nell'economia, o presso conti bancari, e nemmeno nella blockchain, c'è solo un cambiamento del saldo del conto nell'exchange. Nel caso lo richiedessi, l'exchange si impegna a rendermelo, per esempio trasferendo i dollari in un conto corrente affiliato ad una banca.
Un vantaggio degli exchange è che rappresentano un collegamento tra l'economia delle valute legali e l'economia delle criptovalute, per trasferire valore da un'economia all'altra e

viceversa. Sono presenti anche alcuni svantaggi nell'utilizzo, come il rischio del fallimento dell'exchange, lo stesso rischio che corre un risparmiatore che tiene i propri risparmi in una banca. Un altro rischio è che i proprietari dell'exchange si approprino illegalmente dei fondi dei risparmiatori. Poi, considerando la portata e l'accesso online del sito, un ulteriore pericolo è che il sito venga hackerato e vengano rubati i dati che consentono l'accesso ai fondi degli utenti. Per evitare ciò, è meglio trasferire il denaro nel proprio conto corrente bancario e, nel caso si detengano criptovalute, è utile aprire un portafoglio privato (un wallet, vedi 2.2.1 a pagina 19) nel proprio computer, dove trasferire i fondi.
Alcuni exchange sono: Binance, Coinbase, Bittrex, Kraken, Bitstamp.

1.5.1 Formazione del prezzo delle criptovalute: domanda e offerta

Gli exchange sono i mercati dove la domanda e l'offerta di ogni criptovaluta si incontrano in un punto, nel quale si forma il prezzo di equilibrio.

Figura 1.7: Punto di incontro tra domanda e offerta



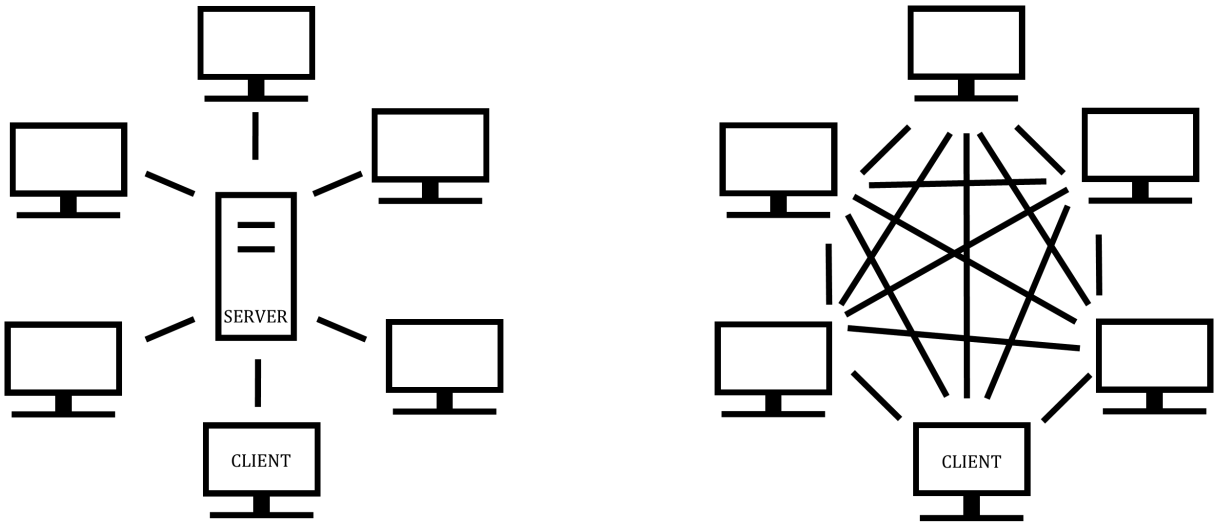
Fonte: https://commons.wikimedia.org/wiki/Image:Supply-demand-equilibrium.svg?uselang=it

L'offerta di criptovalute è pari al totale della moneta potenzialmente acquistabile in circolazione. Per alcune criptovalute, come per Bitcoin, si sa esattamente la quantità in circolo, perché la creazione di moneta è prefissata da un algoritmo, con un limite massimo di valuta creabile entro un arco di tempo predeterminato. Nell'offerta possono essere inclusi anche i depositi di criptovaluta negli exchange, tenendo conto che queste piattaforme detengono solo una parte di ciò che è stato depositato dagli utenti, come riserva, ma che può comunque essere speso o trasferito ad altri utenti.
La domanda è formata da coloro che desiderano acquistare criptovalute in cambio di una valuta legale, come l'euro o il dollaro, per utilizzarle come mezzo di pagamento; poi ci sono coloro che le acquistano a titolo di investimento finanziario, per detenerle e rivenderle ad un prezzo più alto nel futuro.

1.6 Rete peer-to-peer

Molte criptovalute utilizzano un particolare tipo di rete: la rete peer-to-peer.
I dispositivi connessi ad una rete si distinguono in server e client. Il server è un elaboratore potente che mette a disposizione le proprie risorse hardware e software ai client, dispositivi che si connettono al server per utilizzarne le risorse. Di solito in una rete sono presenti uno o più server centrali insieme ai vari client che accedono alle risorse messe a disposizione. Una rete peer-to-peer è un tipo di rete decentralizzata, in cui non sono presenti un server centrale e vari client, ma tutti gli utenti sono dei nodi (chiamati peer) direttamente collegati tra loro. A differenza di una rete normale, nella rete peer-to-peer ogni nodo copre le funzioni sia di server che di client contemporaneamente e il carico di lavoro è distribuito tra tutti i nodi. In questo tipo di rete non è presente una gerarchia: tutti gli utenti nella rete hanno eguali poteri e privilegi.

Figura 1.8: Architettura client-server e architettura peer-to-peer



Capitolo 2

Introduzione a Bitcoin

Bitcoin è una moneta digitale decentralizzata utilizzabile come valuta per i pagamenti a distanza tramite Internet. La parola "bitcoin" assume significato diverso a seconda di come viene scritta: con la lettera maiuscola si riferisce alla tecnologia e alla rete, mentre con la minuscola si riferisce alla moneta, cioè l'unità virtuale scambiabile tra gli utenti, identificata con la sigla BTC o XBT. Un bitcoin è frazionabile in satoshi, come un euro o un dollaro frazionabili in centesimi. Un bitcoin equivale a 100.000.000 satoshi.

Figura 2.1: Logo di Bitcoin

Il software utilizzato è open-source (sorgente aperta), ciò significa che il codice è accessibile e modificabile da tutti: «la sua progettazione è pubblica, nessuno possiede o controlla Bitcoin e ognuno può prendere parte al progetto»[11], in questo modo può essere sviluppato e migliorato dalla comunità.

Per poter partecipare alla rete è necessario aprire un portafoglio (wallet), per cui non è richiesto alcun costo di attivazione e non è necessario fornire alcun dato personale, l'utente deve però farsi carico della sicurezza dei suoi fondi mettendo al sicuro il suo portafoglio, i cui dati di accesso non sono recuperabili una volta persi.

Una volta creato il proprio portafoglio digitale è possibile inviare e ricevere i propri bitcoin tramite la rete, direttamente da un utente all'altro, senza passare attraverso un intermediario, come ad esempio una banca, perché gli utenti fanno parte di una rete peer-to-peer.

2.1 Storia

Prima di Bitcoin, David Chaum «ha fondato una società nel 1989 chiamata DigiCash, probabilmente la prima azienda che ha cercato di risolvere il problema dei pagamenti online. Il denaro effettivo nel sistema di Digicash era chiamato Ecash [...]. Ci sono state banche che l'hanno effettivamente implementato - alcune negli Stati Uniti e almeno una in Finlandia»[12]. Era un sistema di pagamento elettronico che utilizzava la crittografia, per evitare che una somma di denaro venisse spesa due volte e per garantire la privacy degli utenti. Prevedeva il prelievo di fondi da una banca, affiliata a questo sistema di pagamento, per poi effettuare transazioni utilizzando la crittografia, in modo che i pagamenti non fossero tracciabili da terzi.

[11] https://bitcoin.org/it/

[12] Tradotto da: Arvind Narayanan et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton e Oxford: Princeton University Press, 2016, p. XVI

Successivamente, all'inizio degli anni 2000, iniziarono a diffondersi nuove forme di moneta elettronica come e-Gold, sistema di micropagamenti online che introdusse nuove tecniche per l'e-commerce, come i pagamenti effettuati su connessioni SSL (Secure Sockets Layer), con la possibilità per i siti web di costruirsi i propri servizi di pagamento usando questa tecnologia. «Un sistema diverso, utilizzato da e-Gold, era quello di mettere una riserva d'oro in un caveau e di emettere denaro digitale solo fino al valore dell'oro»[13].
Con la crisi finanziaria del 2008 crebbe l'interesse per le criptovalute, dato che potevano essere una soluzione ai problemi della moneta legale e Hal Finney sviluppò Hashcash, il primo sistema Proof-of-Work riutilizzabile, cioè un algoritmo utilizzato poi da Bitcoin per sviluppare il suo sistema di conferma delle transazioni tra gli utenti nella rete, chiamato mining.
Il dominio bitcoin.org venne registrato il 18 agosto 2008 da Satoshi Nakamoto (pseudonimo dell'inventore del protocollo). Venne rilasciata la prima versione del software Bitcoin con incluso il sistema di generazione dei bitcoin che fissa un limite massimo di 21 milioni di bitcoin creabili entro l'anno 2140. Il 3 gennaio 2009 fu creato il primo blocco della blockchain, cioè una serie di blocchi concatenati fra loro in ordine cronologico contenenti le transazioni, la quale funge da registro contabile distribuito tra gli utenti.
Il 12 gennaio 2009 avvenne la prima transazione in bitcoin da Satoshi a Hal Finney e, a partire dal 2010, nacquero i primi cambiavalute online, come Bitcoin Market e Mt.Gox, in cui è possibile detenere un proprio wallet, depositare e ritirare denaro nelle valute supportate del sito ed effettuare trasferimenti ad altri utenti. Il 6 novembre 2010 il tasso di cambio raggiunse la quotazione di mezzo dollaro e l'economia dei bitcoin superò il milione di dollari.
A gennaio del 2011 un quarto del massimo numero possibile (21 milioni) di bitcoin era già stato generato, il 9 febbraio il bitcoin raggiunse il valore di un dollaro per poi salire a dieci dollari il 2 giugno dello stesso anno e vari cambiavalute nacquero in diverse nazioni. A settembre 2012 nacque la Bitcoin Foundation e sempre più esercizi commerciali iniziarono ad accettare questa criptovaluta come mezzo di pagamento. Nel 2013 la FinCEN (Financial Crimes Enforcement Network), ufficio del dipartimento del Tesoro degli Stati Uniti, stabilì delle linee guide di regolamentazione per monete digitali decentralizzate, classificando coloro che convertono bitcoin in denaro come suscettibili di registrazione e di altre obbligazioni legali; nel frattempo la capitalizzazione di mercato di Bitcoin raggiunse il miliardo di dollari, con un tasso di cambio pari a cento dollari. Per la prima volta l'agenzia federale antidroga degli Stati Uniti inserì alcuni bitcoin come merce sequestrata.
«Martedì 1 ottobre 2013 le autorità statunitensi hanno chiuso Silk Road, il più conosciuto tra i siti illegali di e-commerce, nascosto e difficilmente raggiungibile, e hanno arrestato

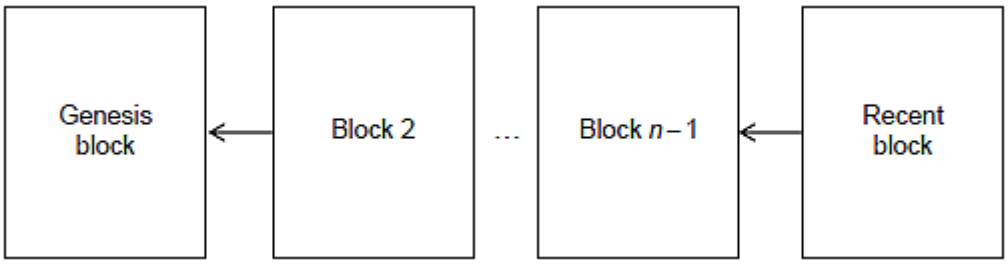
[13]Tradotto da: Arvind Narayanan et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton e Oxford: Princeton University Press, 2016, p. XVIII - XIX

il fondatore e proprietario del sito in una biblioteca di San Francisco: si chiama Ross William Ulbricht»[14].
Era un sito specializzato nella vendita di droghe e altri prodotti illegali che si posizionava in una parte della rete Internet non indicizzata dai classici motori di ricerca e utilizzava come metodo di pagamento i bitcoin per permettere di acquistare in anonimato.
La chiusura di questa piattaforma diede popolarità al bitcoin che il 27 novembre 2013 raggiunse i mille dollari di valore e venne persino creato il primo ATM a Vancouver in Canada per permettere ai clienti di acquistare al bar del centro città con bitcoin. Anche Baidu (il motore di ricerca cinese) permise ai clienti di pagare con bitcoin; l'Università di Nicosia annunciò che avrebbe accettato bitcoin per il pagamento delle tasse, chiamandolo l'oro del domani. Nel mese di dicembre la banca popolare cinese proibì alle istituzioni finanziarie l'uso di bitcoin e da quel momento il suo valore da poco più di mille dollari incominciò a scendere, conseguentemente Baidu smise di accettare bitcoin per alcuni servizi e poco dopo la Cina vietò completamente la criptovaluta nel paese con la chiusura di alcuni cambiavalute.
Con l'aumento della popolarità di Bitcoin molti cambiavalute diventarono obiettivo di hacker e alcuni dovettero sospendere la loro attività, come Mt.Gox, mentre alcune aziende iniziavano ad accettare bitcoin come il giornale Sun-Times, oltre a Dell e Microsoft.
Il Giappone riconobbe che le criptovalute presentavano funzionalità simili alle reali monete, approvandole come mezzo di pagamento legale nel 2017. Nel frattempo continuarono ad aprire nuovi cambiavalute in diverse nazioni, altre aziende iniziarono ad accettare bitcoin e si verificarono altri attacchi hacker. La popolarità della criptovaluta crebbe anche a livello accademico, a tal punto che il simbolo grafico del Bitcoin fu inserito nella categoria delle valute nel sistema di codifica Unicode.
Nel 2017 il prezzo di Bitcoin, che valeva 3.000 dollari a giugno, superò i 10.000 dollari il 29 novembre e arrivò a valere quasi 20.000 dollari il 17 dicembre, per poi decrescere a causa dell'annuncio da parte della Corea del Sud dell'adozione di misure addizionali per regolare il commercio di bitcoin. Inoltre, nel 2018, diverse compagnie vietarono l'uso di questa criptovaluta, il cui prezzo rimase abbastanza basso per poi ricrescere molto velocemente a partire dal 2019.
Al 14/02/2020 sono 15.955 i locali che nel mondo accettano bitcoin come mezzo di pagamento secondo il sito Coinmap.org.

[14]https://www.ilpost.it/2013/10/04/arresto-ross-ulbricht-silk-road/

2.2 Blockchain

Figura 2.2: La blockchain: la catena dei blocchi



Fonte: David Lee Kuo Chuen. *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data.* Amsterdam [etc.]: Academic Press - Elsevier, 2015, p. 49

La blockchain è un registro pubblico, distribuito e condiviso nei dispositivi facenti parte della rete peer-to-peer di Bitcoin, ed è composta da una catena di blocchi ordinati cronologicamente. Un blocco è paragonabile ad una pagina di un libro contabile ed è un file contenente i dati di una serie di transazioni. Tutte le transazioni sono raggruppate nei blocchi che compongono la blockchain e le nuove transazioni vengono inserite in un nuovo blocco che viene sottoposto alla verifica e all'approvazione da parte dei partecipanti alla blockchain. Una volta approvato, il blocco si unisce alla catena, in modo permanente. I blocchi formano una catena perché ogni blocco, oltre a contenere le transazioni e altri dati, ha un riferimento del blocco precedente, per cui tutti i blocchi, fin dal primo, sono legati fra loro ed è quasi impossibile che un blocco venga modificato (tranne nel caso dell'*attacco del 51%*, a pagina 32), soprattutto all'inizio della catena, visto che la modifica di un blocco comporterebbe la modifica di tutti i blocchi successivi.

La blockchain è un **distributed ledger** (libro contabile distribuito), nel senso che tale registro non è memorizzato in un punto centrale ma è presente contemporaneamente su tutti i dispositivi connessi alla rete, ognuno dei quali perfettamente sincronizzato sui medesimi documenti: quindi ogni utente ne possiede una copia ed è possibile visualizzarlo anche online, in alcuni siti, senza scaricare software.
I vantaggi di questo sistema sono numerosi, infatti il potere è distribuito tra gli utenti della rete perché per approvare i blocchi è necessaria partecipazione, come vedremo in seguito. Non è necessario avere un'autorità centrale che gestisce l'offerta di moneta, in quanto la sua creazione è legata ad un algoritmo, basato su un sistema di crittografia per garantire la sicurezza delle transazioni e la privacy. Inoltre, dato che non è presente un'entità centrale, i costi per effettuare le transazioni sono ridotti e il rischio dell'accentramento del potere in un unico individuo è un evento poco realizzabile nella pratica (vedi 2.4.2 a pagina 32).
C'è fiducia nel network, infatti l'affidabilità e la sicurezza del sistema si basano sul consenso di tutti gli utenti, la cui privacy è garantita grazie alla pseudonimia e contemporaneamente

godono di trasparenza e tracciabilità, perché ciascun utente può visualizzare tutte le transazioni registrate e quelle in corso di validazione.
È un sistema solido, grazie alla crittografia e alla irrevocabilità delle transazioni, che incentiva gli utenti a partecipare alla conferma delle transazioni e alla validazione dei blocchi, perché si viene ricompensati con bitcoin di nuovo conio insieme alle commissioni incluse nelle transazioni.

2.2.1 Portafogli Bitcoin

Per poter utilizzare i bitcoin è necessario usare un software, il portafoglio bitcoin (Bitcoin Wallet) che permette di effettuare i trasferimenti tra utenti ed esercizi commerciali (anche e-commerce online) che accettano bitcoin e tiene conto dei trasferimenti effettuati.
Una volta creato un proprio portafoglio, il software genera attraverso un algoritmo una o più coppie di chiavi crittografiche digitali asimmetriche, la privata e la pubblica e genera anche l'indirizzo del portafoglio.
La chiave pubblica è visibile da chiunque, mentre la privata deve rimanere segreta, perché tramite essa è possibile accedere al proprio indirizzo e inviare bitcoin da qualsiasi dispositivo che consente di installare un software portafoglio.
Quindi possedere dei bitcoin e poterli trasferire equivale a immagazzinare e gestire le proprie chiavi, la cui perdita causa l'incapacità di accedere ai propri fondi. È opportuno ad esempio stamparle su carta per poi metterle al sicuro e recuperarle in caso di smarrimento del dispositivo (esempio: cellulare o portatile) o incapacità di accedervi (file corrotti, disco inutilizzabile, etc).
Ci sono diversi tipi di portafoglio, in base alla piattaforma utilizzata, siano essi fisici o digitali, siano essi online oppure offline:

- Mobile: è un'app installabile su un dispositivo mobile come lo smartphone. È portatile e si può utilizzare facilmente il codice QR per trasferire i fondi, infatti le applicazioni, oltre a riportare in caratteri il proprio indirizzo dove ricevere bitcoin, lo converte anche in un codice a barre, cioè il codice QR. Il codice QR facilita i trasferimenti, perché non è necessario scrivere a mano gli indirizzi dei wallet: per esempio se dovessimo inviare dei bitcoin ad un utente, è sufficiente fotografare con il nostro smartphone il codice QR dell'indirizzo del ricevente, per poi inviargli i fondi.

Figura 2.3: Lettura di un codice QR stampato su carta

Fonte: https://pixabay.com/it/illustrations/codice-qr-mobile-scansione-4425886/

Siccome il portafoglio è sempre a portata di mano, con la perdita del dispositivo si perde tutto, a parte nei casi di alcune applicazioni che consentono l'accesso online. Esempi: Bitcoin Wallet, Plutus Wallet, CoinCorner, MyceliumWallet.

- Desktop: software che si scarica e si installa nei PC, portatili oppure desktop. Ce ne sono diversi, progettati da vari sviluppatori e la maggior parte di essi dispongono di diverse versioni dello stesso programma compatibile con i sistemi operativi PC/Desktop maggiormente utilizzati, cioè Windows, MacOS e Linux, in modo che l'utente possa scegliere in base al sistema operativo installato. Troviamo due categorie di portafogli: *thick wallet* e *thin wallet*. I primi occupano molto spazio nel computer perché scaricano l'intera blockchain e generalmente richiedono più tempo per l'installazione, in base alla velocità della connessione alla rete Internet. Permettono la gestione indipendente dei fondi ed effettuano il controllo dell'autenticità dei blocchi. Esempi: Bitcoin-Qt e Armory.
  I secondi sono più leggeri poiché non scaricano la blockchain, presentano un'installazione semplificata e sono presenti terze parti che effettuano controlli sulle operazioni. Esempi di desktop wallet: Multibit, Electrum.

  In entrambi i casi è possibile utilizzare il codice QR, ma è necessario avere a disposizione una webcam per scannerizzare il codice della persona a cui vogliamo inviare i fondi, oppure averne già un'immagine nel computer. In questi tipi di wallet c'è la possibilità di subire un attacco da parte di virus, spyware e malware.

- Web: applicazione online a cui è possibile accedere da qualsiasi browser web (Chrome, Firefox, Safari, Internet Explorer, etc). In questo caso è impossibile perdere i fondi per la perdita del dispositivo, ma vi è il rischio di perderli a causa di interruzione del servizio o hackeraggio. Esempi di Web wallet: BTC.com, Coin.

- Hardware: dispositivo hardware (es. chiavetta USB) in cui è possibile conservare la chiave privata. Tipologia tra le più sicure, dato che i dispositivi fisici sono offline ed è

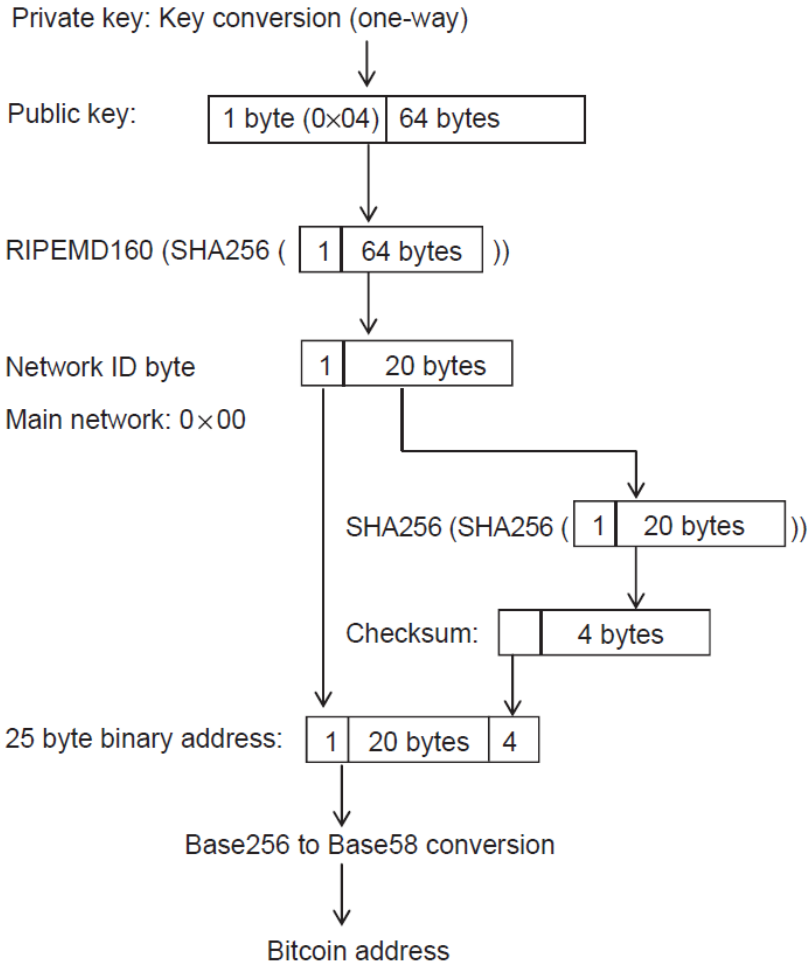
adatta per grandi quantità di bitcoin. Non permette l'uso del codice QR e perdendo il dispositivo, senza aver fatto un backup, rende irrecuperabili i fondi. Esempi di hardware wallet: Denarium, Ledger.

- Paper: è un documento cartaceo contenente la chiave pubblica e quella privata. Per creare il wallet è necessario utilizzare un software che genera una coppia di chiavi crittografiche, per poi stamparle e conservare i documenti in un luogo sicuro. Può essere una soluzione quando si vuole ricevere solamente bitcoin senza installare software, controllando di volta in volta il saldo su siti che visualizzano la blockchain inserendo il proprio indirizzo e, nel caso si volesse inviare bitcoin, è sufficiente installare un software in cui inserire la chiave privata. Un esempio è bitaddress.org che è in grado di generare una coppia di chiavi crittografiche.

2.2.2 La creazione di un indirizzo Bitcoin

Una volta creato un portafoglio, il software ricava l'indirizzo per inviare e ricevere transazioni Bitcoin. Il software genera una chiave privata a cui si applica prima la funzione irreversibile ECDSA-512 per ottenere la chiave pubblica. Una funzione di hash SHA256 viene applicata alla chiave pubblica; al risultato viene ulteriormente applicata una funzione di hash RIPEMD-160 che genera un risultato a 160 bit. A ciò viene applicata una funzione di hash SHA256 due volte. Del risultato viene eseguita la checksum, la quale viene poi aggiunta al risultato precedente a 160 bit e l'insieme viene convertito attraverso il sistema di codifica Base58Check nell'indirizzo Bitcoin.

Figura 2.4: Processo di generazione di un indirizzo Bitcoin



Fonte: David Lee Kuo Chuen. *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data.* Amsterdam [etc.]: Academic Press - Elsevier, 2015, p. 52

2.2.3 Come avviene una transazione

La chiave pubblica cifra i messaggi in uscita e decifra la propria firma, mentre la chiave privata decifra i messaggi in entrata e appone la firma ai messaggi in uscita, in modo che il destinatario sia sicuro della provenienza del messaggio e che non sia stato modificato. Per ricevere serve soltanto la chiave pubblica, mentre per inviare servono entrambe le chiavi. Esempio: A vuole effettuare una transazione a B.

1. A crea la transazione (contenente informazioni sullo scambio, prezzo, disponibilità economica) e applica una funzione di hash alla stessa, creandone così il *digest*;
2. A firma il *digest* con la propria chiave privata, e aggiunge la chiave pubblica di B;
3. A invia la transazione agli altri nodi della rete per la verifica della disponibilità di A dell'ammontare di criptovaluta da inviare attraverso l'analisi dello storico dei trasferimenti già effettuati;

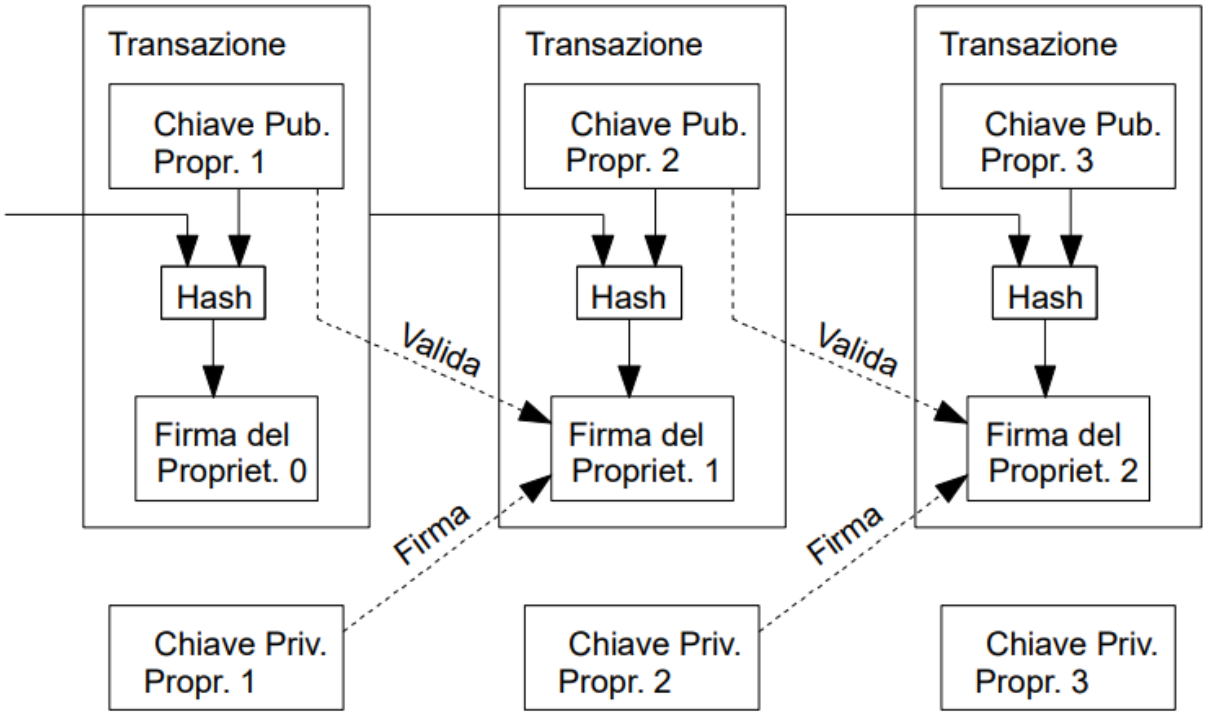
4. I nodi iniziano la costruzione di un blocco, in cui viene registrata la transazione e altre successive, il quale verrà poi sottoposto al mining, cioè alla sua validazione. Una volta validato il blocco, viene aggiunto alla blockchain;

5. B riceve la transazione, con la chiave pubblica di A ne decifra la firma digitale e acquisisce così il *digest*;

6. siccome la chiave pubblica di B è ora inserita nella transazione, solo B attraverso la sua chiave privata può sbloccare la disponibilità e avviare nuove transazioni ripetendo l'iter.

Trasferendo la proprietà delle criptovalute, con la firma digitale della transazione precedente e aggiungendo di volta in volta la chiave pubblica del nuovo destinatario, si crea una catena di possesso: questa modalità annulla la possibilità da parte di un utente di spendere due volte uno stesso ammontare di bitcoin.

Figura 2.5: Transazioni tra utenti della rete Bitcoin



Fonte: https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf

2.2.4 Pubblicità della blockchain e pseudonimia

Ogni transazione viene registrata nella blockchain, visibile online da chiunque e resa disponibile anche da alcuni siti web specializzati, ed è possibile visualizzare anche gli indirizzi degli utenti che inviano e ricevono bitcoin.

L'indirizzo è pubblico in quanto esposto nella rete Internet ed è visibile e raggiungibile da chiunque, a differenza di un indirizzo privato che non è visibile su Internet e non è raggiungibile da chiunque, ma solo da alcuni utenti.
Gli indirizzi degli utenti sono anonimi perché sono sequenze alfanumeriche di caratteri casuali che non riportano dati personali e quindi non permettono di identificare l'utente. Quindi, l'utente rimane anonimo perché può effettuare transazioni senza rivelare la propria identità ma, siccome le transazioni sono pubbliche e sono tracciabili, è più corretto dire che è pseudonimo, perché rimane identificabile solo mediante l'indirizzo.
Grazie alla pseudonimia, similmente al denaro contante che può essere utilizzato per attività legittime e non, questa criptovaluta è utilizzabile anche per condurre attività criminali, infatti si sono sviluppati nel tempo mercati di beni e servizi illegali nel Deep Web, come è avvenuto con Silk Road.

2.2.5 Tipi di nodi nella rete Bitcoin

I nodi della rete Bitcoin non sono tutti uguali, sono presenti più tipologie, ognuna delle quali ha un ruolo differente nella rete e fa in modo che essa funzioni correttamente:

- nodo **full**: sono pienamente sincronizzati con la rete, perché scaricano nella memoria del computer una copia dell'intera blockchain dalla sua creazione. Per essere un nodo full è necessario scaricare un software, come Bitcoin Core, e avere uno spazio di archiviazione molto elevato, perché attualmente servono almeno 294 GB per contenere una copia della blockchain e, siccome la sua dimensione aumenterà sempre di più nel tempo, servirà molto più spazio di archiviazione nel dispositivo.

  Un nodo full partecipa al processo di verifica e validazione dei blocchi e delle transazioni da altri nodi, per far sì che siano conformi alle regole. Se viene violata una regola da un blocco o da una transazione e un nodo rifiuta il blocco o la transazione, il rifiuto avviene da parte dell'intera rete automaticamente.

  Ogni utente, scaricandosi una copia della blockchain, detiene lo storico di tutte le transazioni avvenute dalla creazione di Bitcoin fino ad oggi. Con la rete peer-to-peer, ogni nodo full ha le stesse informazioni e non è possibile modificarle senza che siano modificate in un altro nodo, rendendo più sicura la rete da manomissioni.
  Questo tipo di nodo è il più sicuro.

- nodo **listening** (super nodo) è un nodo che opera come punto di ridistribuzione altamente connesso, cioè come se fosse un ripetitore. È un nodo pubblico a cui chiunque può collegarsi per ottenere informazioni sulle transazioni e per ottenere la blockchain. Questi nodi di solito sono sempre attivi e richiedono più potenza e una connessione migliore, dato che il carico di lavoro è più elevato e ci sono molte richieste di informazioni da parte degli utenti.

- nodo **light**: sono più leggeri rispetto agli altri tipi di nodi perché non scaricano l'intera catena di blocchi, ma solamente gli header dei blocchi (vedi 2.3.1) e validano l'autenticità delle transazioni con un metodo semplificato chiamato Simplified Payment Verification (SPV). Non sono indipendenti come i nodi full e per questo sono più vulnerabili ad attacchi, perché non sono perfettamente sincronizzati con la blockchain. Inoltre, la maggior parte dei software per partecipare come nodo light sono progettati da terze parti, che ricevono i nostri dati riguardanti il wallet.

- nodo **miner**: coloro che partecipano al mining, cioè alla validazione dei blocchi della catena, utilizzano programmi specifici, atti a questo scopo.

2.3 Mining

Affinché le transazioni vengano eseguite, è previsto un processo di validazione chiamato mining che prevede la verifica e l'approvazione dei blocchi della catena da parte degli utenti (chiamati miner, cioè minatori) che, con le loro risorse computazionali, risolvono un problema matematico (o un puzzle crittografico) di difficoltà elevata. Il problema da risolvere consiste nel risalire, attraverso tentativi, al contenuto originale che è stato crittografato attraverso una funzione di hash. Tale processo rappresenta la Proof-of-Work alla base del sistema Bitcoin, cioè il meccanismo del consenso distribuito.

2.3.1 Struttura di un blocco

Un blocco è composto dall'header e dal body. L'header è composto principalmente da:

- versione, numero che indica quale set di regole è stato adottato per convalidare il blocco. La versione si aggiorna con i cambiamenti del protocollo e del software utilizzato;

- hash del blocco precedente, cioè la serie di caratteri alfanumerici che fa da riferimento al blocco precedente;

- radice di *merkle*, cioè l'hash di tutti gli hash di tutte le transazioni nel blocco;

- una marca temporale (*timestamp*), che indica quando il miner ha iniziato a minare il blocco (secondo il miner);

- campo bits, cioè una versione codificata del target soglia, rispetto al quale l'hash che identifica il blocco deve essere minore o uguale;

- *nonce*, un numero unico che viene aggiunto al blocco criptato dall'hash. In crittografia il termine *nonce* (number only used once) è usato in riferimento ad un valore casuale che può essere utilizzato una sola volta in una comunicazione crittografica.

Il body invece contiene i dati delle transazioni.

Figura 2.6: Blocco della blockchain: header e body

Versione
Hash blocco precedente
Radice di Merkle
Timestamp
Bits
Nonce
Contatore di transazioni
Transazioni

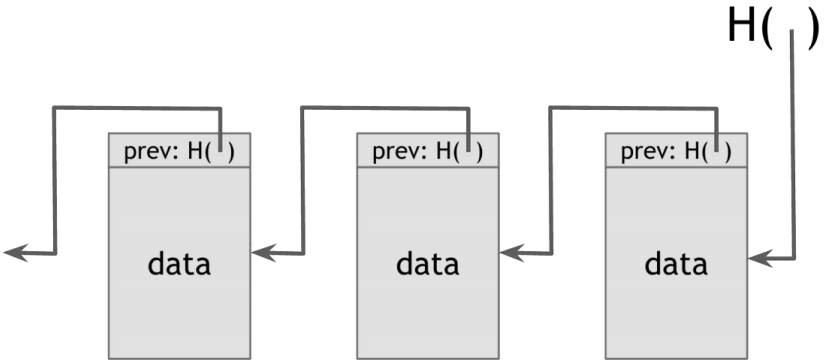
2.3.2 Il processo di mining

Una volta connesso alla rete, il miner può iniziare il processo di mining. Il miner, dopo aver richiesto lo storico della blockchain, raccoglie alcune transazioni in attesa di conferma e si assicura che siano valide controllando le firme digitali e che gli utenti non abbiano già speso i bitcoin. Una volta compiuta questa operazione, il miner può iniziare a costruire un proprio blocco, candidato al network come successivo nella catena. Per costruirlo, raggruppa e poi aggiunge alcune transazioni che aveva verificato, nei limiti dimensionali del blocco. Una volta costruito, deve risolverlo, perché deve calcolare l'ultimo mattone del blocco, cioè deve trovare un nonce che lo renda valido.
Il problema da risolvere è trovare il valore del *nonce* tale per cui quando si applica la funzione di hash all'header del blocco, l'output della funzione deve essere un numero che è minore o uguale rispetto ad un valore target (*target value*), che cambia nel tempo in base alla difficoltà corrente.

$$[f\text{-}hash(header)] \leq targetvalue$$

Si inserisce nella funzione un ipotetico valore del *nonce*, che viene incrementato di uno finché si raggiunge la condizione per cui l'output della funzione è minore o uguale al target. Se questa condizione è vera, il blocco è valido e il valore dell'hash identifica in maniera univoca e sicura ciascun blocco come se fosse un'impronta digitale, senza possibilità di risalire al contenuto generato. Inoltre, il fatto che ogni blocco contiene il riferimento all'hash del blocco precedente crea la struttura dei dati a catena (vedi Figura 2.7) e ci permette di verificare che il suo valore, che rimane ignoto, non abbia subìto variazioni.

Figura 2.7: La catena di blocchi



Fonte: Arvind Narayanan et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton e Oxford: Princeton University Press, 2016, p. 11

Esempio

Ad esempio in un'ipotetica situazione in cui:

- header = (versione||hash blocco preced||radice di merkle||etc..) = "Hello, world!"
- *nonce* = incognita
- *target value* = 000d4fg5t698...
- funzione di hash utilizzata: SHA-256

I miners conoscono già gli altri elementi dell'header del blocco, a parte il *nonce*. Lo scopo è trovare un valore del *nonce* tale per cui:

$$SHA\text{-}256(\text{Hello, world!}\boldsymbol{nonce}) \leq \text{000d4fg5t698...}$$

Ogni elemento all'interno dell'header del blocco corrisponde ad una stringa. «La stringa in informatica è una sequenza finita di caratteri alfanumerici registrata in memoria o in un altro supporto (nastro, disco, ecc.), che rappresenta dati in forma codificata»[15].
Come si può notare nei dati dell'header, all'interno delle parentesi tonde, le stringhe sono concatenate fra loro con la doppia barra verticale || (usate in alcuni linguaggi di programmazione come simbolo di concatenazione di stringhe). Per cui si collegano fra loro e diventano un'unica stringa.
Per trovare il *nonce* i miners spendono molto tempo di calcolo: inseriscono nella funzione una serie di valori al posto del *nonce* e calcolano la funzione di hash ogni volta.
La serie di valori da inserire al posto del *nonce* parte dal numero 0, viene calcolata la funzione di hash e se il risultato della funzione è minore o uguale al target, significa che il valore del *nonce* è corretto e la soluzione è stata trovata. In caso contrario il valore al

[15]http://www.treccani.it/vocabolario/stringa2/

posto del *nonce* viene incrementato di uno, calcolando poi la funzione di hash e così via, finché non viene trovato un valore corretto.

```
SHA256(Hello, world!0)=
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

SHA256(Hello, world!1)=
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
....
SHA256(Hello, world!4250)=
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Quindi il calcolatore ha incrementato il valore del *nonce* 4250 volte per raggiungere l'obiettivo: il *digest* trovato con il *nonce* 4250 inizia con quattro zeri ed è perciò minore del *target value*, perché quest'ultimo inizia con solo tre zeri.

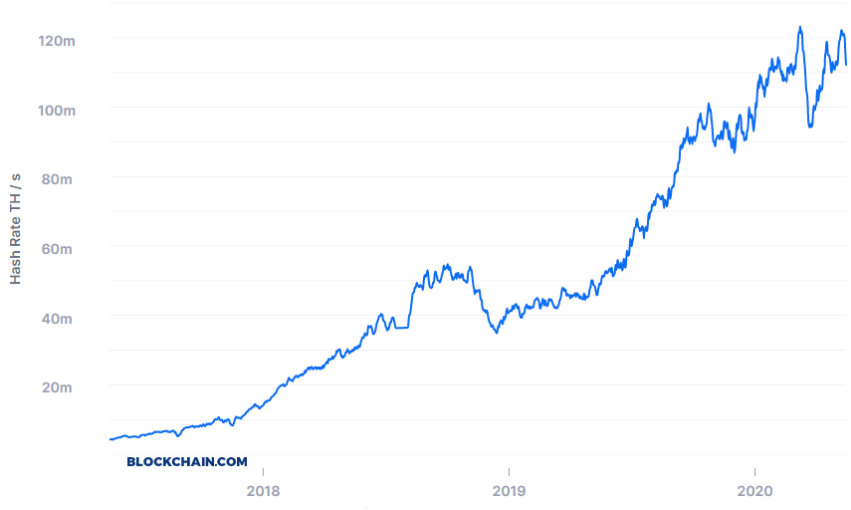
Il *nonce* viene poi trasmesso agli altri nodi network che ne verificano la correttezza: se l'esito è negativo il blocco viene rifiutato, se invece è positivo il blocco viene aggiunto alla catena che si aggiorna in tutti i dispositivi.
Il miner che per primo ha fornito la soluzione al problema, e che ha quindi validato il blocco, riceve una ricompensa pari a 6,25 bitcoin (da maggio 2020) ed inoltre, se le transazioni del blocco contengono commissioni, il miner ha diritto a riceverle come premio aggiuntivo.
Nel caso in cui più nodi validino un blocco allo stesso istante si crea un *fork* (biforcazione) nella blockchain che viene risolta dai miners che lavorano per estendere la biforcazione più lunga tra le due.

2.3.3 La difficoltà nel mining

La difficoltà viene misurata con un valore che indica il numero di tentativi di calcolo che hanno la probabilità di generare un numero minore del target. Indica quindi una stima del numero di hash da calcolare per risolvere un blocco alla difficoltà corrente.
Gli zeri all'inizio del *target value* (vedi 2.3.2 nella pagina precedente) sono un indicatore della difficoltà per risolvere un blocco: un numero maggiore di zeri significa che la difficoltà è maggiore, perché il valore del nonce da calcolare sarà molto piccolo, per cui è necessario svolgere più calcoli.
La difficoltà è la stessa per tutti i miners ed è il valore che indica quanto è difficile trovare un hash minore o uguale rispetto al valore target e regola il tempo che i miners impiegano per minare il blocco successivo. Per bilanciare l'aumento della capacità di calcolo da parte della rete, la difficoltà aumenta del 10-20% ogni 2016 blocchi, cioè ogni circa due settimane, in modo che la validazione dei blocchi impieghi sempre circa dieci minuti in media. La difficoltà aumenta con l'aumentare della dimensione della blockchain in relazione

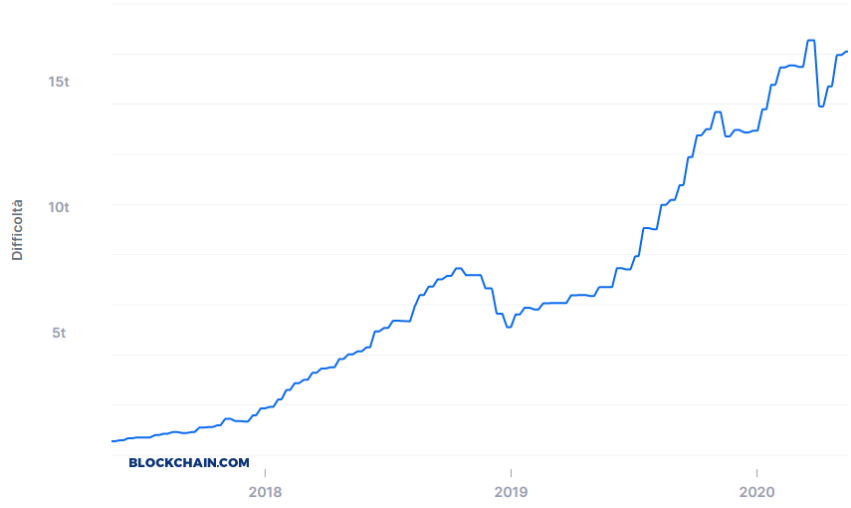
all'attività nel mercato, per esempio in relazione al numero di nuovi miners, oppure in relazione all'hardware più efficiente che permette di risolvere blocchi più velocemente. All'interno di ogni blocco vi è memorizzata una rappresentazione compressa (per risparmiare spazio all'interno del block header) del target alla creazione del blocco considerato, che corrisponde al campo Bits.

Figura 2.8: Hashrate totale (TH/s) negli ultimi tre anni



Fonte: https://www.blockchain.com/charts/hash-rate

Figura 2.9: Difficoltà negli ultimi tre anni



Fonte: https://www.blockchain.com/charts/difficulty

Nella Figura 2.8 è indicato l'hashrate totale globale negli ultimi tre anni, cioè la potenza di calcolo della rete Bitcoin. La Figura 2.9 indica invece il livello di difficoltà per minare i blocchi negli ultimi tre anni. Le due Figure presentano un andamento praticamente identico nel tempo, in quanto se aumenta l'hashrate globale, la difficoltà globale aumenta

di conseguenza e, se la difficoltà aumenta, i miners dovranno aumentare la potenza di calcolo per poter minare i blocchi.

2.3.4 Costi del mining

Fare mining, dal punto di vista economico, è molto costoso. I costi che un miner deve sostenere sono molti: il costo dell'hardware, che deve essere sempre aggiornato; il costo dell'energia elettrica per fare i calcoli; i costi operativi, come ad esempio il costo per avere un luogo dove tenere i computer; il sistema di raffreddamento delle macchine, la manutenzione, i costi di ricerca, etc. L'hardware è un costo fisso, l'elettricità è un costo variabile che dipende anche dal luogo in cui ci si trova, infatti può essere conveniente stabilirsi dove l'energia elettrica costa meno e posizionare i computer in luoghi freddi, in modo che il calore generato sia dissipato meglio.
Il ricavo è dato dalla ricompensa, attualmente di 6,25 bitcoin per blocco, insieme alle commissioni che gli utenti aggiungono al blocco, sempre in bitcoin. Il ricavo che un miner ottiene dipende dal rateo di risoluzione dei blocchi che dipende non solo dall'hashrate, ma anche dal rapporto dell'hashrate del miner rispetto all'hashrate globale. Infatti, l'aumento dell'hashrate globale porta ad un aumento della difficoltà globale e quindi il costo per le macchine aumenta, dato che è necessaria maggior potenza di calcolo per risolvere i blocchi. La condizione per fare un profitto è che la ricompensa sia maggiore dei costi. I costi sono espressi nella valuta del paese in cui ci si trova, mentre la ricompensa viene sempre data in bitcoin, che non hanno sempre lo stesso valore nel corso del tempo. Siccome la maggior parte delle criptovalute cambiano valore spesso e velocemente, bisogna tenere conto del tasso di cambio rispetto alla valuta in cui si intende convertire i bitcoin, dato che potrebbe influire pesantemente nel profitto del miner.

Figura 2.10: Esempi di mining farm

(a) *Una mining farm di dimensioni ridotte*

(b) *Una mining farm di grandi dimensioni*

Fonte: https://pixabay.com/it/photos/azienda-agricola-mining-2852024/
https://commons.wikimedia.org/wiki/File:Cryptocurrency_Mining_Farm.jpg

Le Figure in 2.10 mostrano due esempi di mining farm (letteralmente: fattoria mineraria), cioè strutture composte da apparecchiature e macchine per estrarre criptovaluta attraverso

il mining. Nella 2.10a è rappresentata una mining farm di dimensioni ridotte, collocabile anche in casa, mentre la 2.10b mostra una mining farm di grandi dimensioni che richiede ingenti investimenti.

2.4 Mining come sistema del consenso distribuito: Proof-of-Work

I calcoli del mining richiedono una notevole quantità di lavoro per essere risolti ed è necessario sostenere diverse tipologie di costi.
È un sistema che incentiva gli utenti a partecipare, infatti i miners sono in competizione fra loro per la soluzione del problema, perché il primo che fornisce la soluzione ai calcoli viene ricompensato con dei bitcoin di nuova creazione. È definito come un sistema **Proof-of-Work (PoW)** (prova di lavoro), chiamato così perché per aggiungere un blocco alla catena è necessaria una grande quantità di lavoro (il mining), la quale produce dati specifici (la prova, cioè la soluzione al problema crittografico) che permettono di verificare che è stata eseguita una notevole quantità di lavoro.
La Proof-of-Work di Bitcoin è un **algoritmo di consenso distribuito**, perché con questo sistema viene raggiunto un accordo decentralizzato tra i nodi per l'aggiunta dei nuovi blocchi, senza avere la necessità di un ente centrale che fa da controllore.

I vantaggi della PoW sono che la quantità di moneta posseduta non influenza il processo di mining e inoltre questo sistema garantisce una protezione dagli attacchi Ddos, attacco informatico che ha come scopo quello di esaurire le risorse di un sistema informatico, come un sito web aziendale, in modo che non riesca più a fornire servizi ai client.

Gli svantaggi sono che la PoW è costosa perché richiede elevate risorse computazionali, tempo, energia elettrica e, inoltre, i calcolatori adottati devono essere aggiornati nel tempo per compensare l'aumento nella difficoltà del mining.

2.4.1 Consumi di energia

Per via dei consumi di energia, dal punto di vista ecologico la PoW non ha un impatto positivo. Purtroppo non è possibile sapere esattamente quanto consuma Bitcoin in energia elettrica, perché ogni miner ha il proprio equipaggiamento, il quale può essere più o meno efficiente, in base ai macchinari che si è deciso di acquistare per il mining e non solo, ma anche ad esempio in base al sistema di raffreddamento, il quale consuma energia.
Secondo Digiconomist, Bitcoin ha consumato circa 73,121 Terawattora[16] di energia elettrica nel 2019. È un numero che varia nel tempo in base all'hashrate totale globale ed attualmente è pari quasi al consumo di energia elettrica in un anno della Colombia[17]. Secondo l'Università di Cambridge, invece, il consumo dei Bitcoin nel 2019 ammonterebbe a circa

[16] 1 TeraWatt = 1000 GigaWatt = 1.000.000.000 KiloWatt
[17] Dati presi da https://digiconomist.net/bitcoin-energy-consumption

53,03 Terawattora. Blockchainanalytics.pro, invece, ha previsto il consumo della rete Bitcoin nel 2019 pari a 43 TWh[18], cioè poco più del consumo annuale della Nuova Zelanda. Molti sollevano la questione che Bitcoin sia molto dispendioso dal punto di vista del consumo di energia elettrica, facendo confronti con interi paesi abitati del mondo, invece potrebbe essere un'alternativa spostare il confronto ad esempio sulle banche.
Il gruppo bancario Crédit Agricole Italia, con 1043 punti vendita, dal bilancio di fine esercizio del 2019[19], in un anno ha consumato 53,90 GWh solo di energia elettrica, pari a 0,0539 TWh[20]. Oltre all'energia elettrica, ci sono altri costi di diversa natura come il gasolio per riscaldamento, il gasolio per autotrazione, benzina, GPL. Poi è da considerare anche il materiale utilizzato: carta, contenitori in plastica, cancelleria, materiale informatico, rifiuti, etc.
Quindi, tenendo conto del numero di banche nel mondo, Bitcoin probabilmente ha consumi inferiori, dato che non ha infrastrutture come quelle bancarie e tenendo conto che il numero di utenti è inferiore. È chiaro che, con l'aumento della difficoltà, sarà necessaria più potenza computazionale per risolvere i blocchi e quindi sarà necessaria più energia elettrica sia per far funzionare i macchinari, che per il raffreddamento e altri servizi. Ma principalmente si parla di energia elettrica, che può essere recuperata con l'energia rinnovabile, infatti in questi studi è presente solo una stima dei consumi di energia elettrica e non vi sono riferimenti a come l'energia viene prodotta. Bitcoin e le altre criptovalute sicuramente richiedono molta energia, ma è importante ampliare il confronto guardando la questione da più punti di vista, considerando ad esempio tutti quei servizi online e non, utili e meno utili, che vengono utilizzati dagli utenti ogni giorno e che consumano anch'essi molta energia. Poi, non è solamente importante quanta energia viene consumata, ma quanto di questa è stata prodotta con processi che non impattano sull'ambiente.
Se in un futuro ipotetico verranno utilizzati solo strumenti digitali, sicuramente ci saranno meno infrastrutture, meno rifiuti, e principalmente solo costi di energia elettrica, che può essere recuperata con le energie rinnovabili.

2.4.2 Attacco del 51%

Il rischio in questo sistema è, il così denominato, **attacco del 51%**, cioè una situazione in cui uno o più utenti abbiano accumulato una maggiore potenza di calcolo, espressa in hashrate (vedi 1.2.1 a pagina 7), pari ad almeno il 51% della potenza rispetto agli altri membri presenti nella rete di Bitcoin. In questo caso l'attaccante, avendo la maggioranza della potenza di calcolo, avrebbe il controllo sulla blockchain e potrebbe escludere intenzionalmente delle transazioni impedendone la conferma o modificandone l'ordine:

[18]https://www.blockchainanalytics.pro/btc/electricity-consumption/
[19]https://static.credit-agricole.it/credit-agricole-it/system/rich/rich_files/rich_files/000/002/096/original/relazione-20e-20bilancio-202019.pdf
[20]Il dato esclude i consumi relativi ai condomini del Gruppo e riguarda pertanto il 40% degli immobili del Gruppo.

ad esempio potrebbe invertire alcune transazioni personali effettuate, realizzando così situazioni in cui potenzialmente sarebbe possibile spendere due volte gli stessi bitcoin (double spending). Quindi, potrebbe costruire i blocchi a suo piacimento, monopolizzando il mining e ricevendo le ricompense.
È comunque una situazione difficile da mettere in pratica, poiché modificare dei blocchi confermati in precedenza diventa sempre più difficile all'aumentare della dimensione della blockchain, perché i blocchi sono collegati fra loro e solo gli ultimi blocchi sarebbero modificabili. Inoltre, più il network è esteso, più è protetto da questo tipo di attacco, grazie al numero elevato di miner che competono fra loro per risolvere i blocchi. Sarebbe comunque molto costoso, dal punto di vista delle risorse hardware, avere a disposizione una tale potenza di calcolo in un network così ampiamente esteso a livello globale.

2.4.3 Un sistema alternativo: la Proof-of-Stake

La **Proof-of-Stake (PoS)** (Prova di interesse) è un'alternativa alla PoW e spesso viene utilizzata come complementare ad essa in alcune criptovalute. Nel caso della PoS, l'algoritmo del consenso distribuito prende il nome di *forging* (o *minting*), infatti il blocco viene forgiato invece di essere minato e colui che valida le transazioni e forgia nuovi blocchi è chiamato *forger* (o *validator*, cioè validatore).
A differenza della Proof-of-Work, in cui la probabilità di risolvere un blocco dipende dalla quantità di lavoro svolto, nella Proof-of-Stake invece dipende dalla quantità di moneta detenuta da un utente: ad esempio, se un utente detiene il 10% del totale della moneta nel network ha la probabilità del 10% di essere scelto da un algoritmo, che sceglie tra i validatori in modo casuale, per forgiare un nuovo blocco. Il validatore scelto ha il compito di verificare che le transazioni siano valide, firmare il blocco e aggiungerlo alla catena, per poi ricevere le commissioni associate ad ogni transazione contenuta nel blocco come ricompensa.
Quindi, nel caso della PoS non è importante la potenza computazionale, ma è rilevante il quantitativo della moneta posseduta dal validatore. Per questo motivo richiede meno elettricità ed è quindi più ecologica rispetto alla PoW.
Uno svantaggio di questo sistema è che i partecipanti alla rete più ricchi diventano sempre più ricchi perché, essendo facilitati nel mining, risolvono un maggior numero di blocchi e ricevono più ricompense. Questo problema comunque viene risolto dal fatto che gli algoritmi PoS delle criptovalute hanno meccanismi di selezione casuale tra i validatori che non considerano solo la moneta posseduta, ma anche la combinazione di altri fattori. Ad esempio la selezione basata sull'anzianità combina la selezione casuale con il concetto di anzianità delle monete possedute; infatti, se non vengono spese negli ultimi trenta giorni, assumono più valore nel meccanismo di scelta: le quantità di monete più anziane e più grandi hanno una maggiore probabilità di firmare il blocco successivo.
Anche nel caso della PoS è possibile un attacco al sistema del 51%, cioè una situazione in

cui un validatore possegga almeno il 51% della criptovaluta considerata e possa prendere il controllo sulla blockchain, ad esempio autorizzando transazioni fraudolente. Tuttavia, la probabilità di un attacco del genere al sistema è bassa perché per attuarlo è necessario avere almeno il 51% della criptovaluta in circolazione e, se ha un'alta capitalizzazione di mercato, per esempio 100 miliardi, diventa difficile appropriarsene.

Tabella 2.1: Principali differenze tra Proof-of-Work e Proof-of-Stake

Sistema	**Proof-of-Work**	**Proof-of-Stake**
Denominazione	Minatore	Validatore
Chi può esserlo	Chiunque	Validatori selezionati
Probabilità di..	minare blocchi -> quantità di lavoro	validare blocchi -> moneta posseduta
Ricompensa	numero fisso + commissioni	commissioni
Consumo	molta energia	poca energia
Costi	hardware ed energia elettrica	quantità di moneta posseduta

2.4.4 Possibilità di mining

Ci sono tre possibilità per fare mining e cercare di ottenere la ricompensa in bitcoin che differiscono in base alla quantità di persone che effettuano i calcoli, in base ai contratti stipulati tra le persone coinvolte, alla proprietà delle macchine utilizzate e ad altri fattori.

Solo mining

Il miner effettua i calcoli individualmente per risolvere un blocco e ricevere la ricompensa; se ben equipaggiato impiegherà circa tre mesi con un'efficienza che si riduce con l'aumento della difficoltà.
Possono essere utilizzati software speciali per connettersi alla blockchain, minare i blocchi e ritrasmettere indietro le informazioni. Alcuni software dedicati sono CGMiner, Bitminer, BFGMiner, EasyMine.
Il solo mining implica sostenere i costi dell'equipaggiamento che è necessario rinnovare, in quanto non è possibile mantenere nel tempo lo stesso hashrate, perché la difficoltà determina il processo di estrazione. Anche i costi di elettricità sono rilevanti e quindi è preferibile adottare hardware efficiente a minor consumo e che emette meno calore (spesso i miners hanno la possibilità eseguire i processi di estrazione in paesi nei quali i costi per l'elettricità sono più convenienti).

Mining contracts o cloud mining

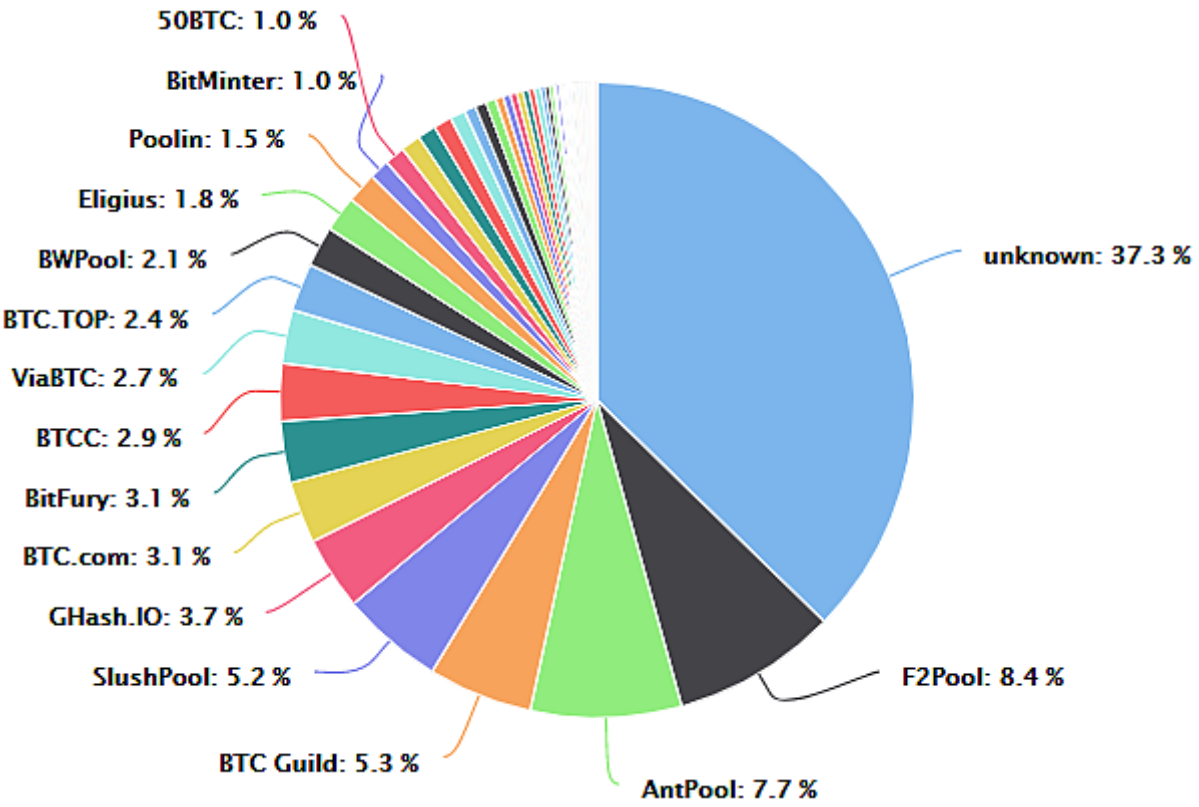
Sono contratti che forniscono servizi di mining, con specifiche performance per un certo periodo e sono adatti a coloro che vogliono investire in bitcoin senza gestire hardware e software, infatti attraverso il computer di casa è possibile usufruire della potenza condivisa da parte di centri dati distanti dall'utente.

Sono presenti più categorie: l'hosted mining, in cui un utente affitta una macchina di proprietà altrui per poter minare; il virtual hosted mining, in cui un utente crea un server privato virtuale per minare e il leased hashing power, in cui un utente può dare in prestito un quantitativo di potenza per risolvere problemi di hashing.
Tra i vantaggi di questo sistema troviamo l'assenza di costi di elettricità, equipaggiamento (e problemi correlati), costruzione del sistema e sua configurazione. Gli svantaggi sono i minori profitti, la mancanza di controllo, flessibilità e decremento dell'hashrate dovuto all'aumento della difficoltà.

Mining pools

Sono gruppi formati da molti minatori che minano collettivamente usando tutte le loro risorse e tale unione genera una maggiore potenza di hashing, aumentando la probabilità di risolvere i blocchi. La ricompensa è divisa tra i partecipanti in base al contributo che naturalmente è minore, dato anche dal fatto che è al netto delle commissioni per ricompensare i minatori e di una parte che va all'operatore del mining pool. Esistono molteplici mining pools, ognuna delle quali differisce per dimensione, potenza di hash, tipo di ricompensa data, etc.

Figura 2.11: Distribuzione delle mining pools per nr. blocchi dalla creazione di Bitcoin al 25/02/2020



Fonte: https://btc.com/stats/pool?pool_mode=all

2.5 Commissioni

È possibile inviare e ricevere Bitcoin da un paese all'altro in tutto il mondo, in un tempo molto breve, senza limiti e con commissioni molto basse.

Le transazioni in bitcoin non sono gratuite, infatti il mittente deve farsi carico di una commissione, di cui può deciderne l'ammontare da aggiungere alla transazione: più la commissione è alta, più veloce è la convalida della transazione stessa da parte dei miners.

Nel momento in cui una transazione viene inviata nella rete, viene verificata e poi collocata all'interno di una allocazione di memoria presente in ogni nodo, la **mempool**, dove vengono memorizzate le transazioni in attesa di convalida da parte dei miners. Dalla mempool, i miners scelgono le transazioni con cui riempire il blocco e tralasciano quelle meno appetibili.

I miners saranno più incentivati a considerare per prima le transazioni con commissioni più elevate da inserire nel blocco perché se sarà aggiunto alla catena, oltre a ricevere la ricompensa per aver minato il blocco, riceveranno anche le commissioni relative alle transazioni del blocco.

Ogni nodo di Bitcoin ha una differente capacità di mempool e, quando essa è sovraccarica, il nodo inizia a dare una priorità alle transazioni impostando una commissione minima per transazione: solo quelle che rispettano il requisito della commissione potranno avere accesso alla mempool.

Le commissioni sono calcolate in satoshi per byte della transazione: la dimensione in byte della transazione viene moltiplicata per la tariffa media di commissione. Per esempio con una transazione di 100 byte e una tariffa media di 400 satoshi/byte, la commissione sarà pari a 40.000 satoshi.

In alcuni casi, se le commissioni incluse sono troppo basse, è possibile che la transazione venga lasciata nella mempool per molto tempo, perché nessun miner ha intenzione di includerla nel blocco, allungando il tempo di validazione della stessa e quindi il pagamento.

Figura 2.12: Commissioni di una transazione che vanno al miner

Fonte: https://en.bitcoinwiki.org/index.php?curid=271868

2.6 Annullamento di una transazione

Le transazioni in bitcoin, una volta eseguite, sono irreversibili. Non è possibile annullare una transazione se i bitcoin sono già stati accreditati nel wallet del beneficiario e l'unico modo per

riottenere indietro i bitcoin è chiederne la restituzione alla persona a cui sono stati inviati, se la si conosce. Non è possibile nemmeno cancellare la transazione in rete una volta inviata per essere verificata, tuttavia ci sono due modi che permettono di recuperare i bitcoin, ma soltanto se la transazione non ha ancora nessuna conferma.

Figura 2.13: Pulsante di opzione per attivare il RBF

Il primo è supportato soltanto da alcuni wallet ed è il protocollo Replace by Fee (RBF). È necessario prima attivare questo protocollo nelle impostazioni del wallet, cliccando sul pulsante di opzione. Il protocollo RBF dà la possibilità di rimpiazzare la transazione con una nuova, che include una commissione più alta. Se il proprio wallet non consente il protocollo RBF è possibile provare un secondo modo, cioè creare una seconda transazione con lo stesso importo della prima e inviarla a se stessi, però con una commissione più alta rispetto alla prima. In questo modo la rete individua un caso di doppia spesa degli stessi bitcoin e i miners prenderanno in considerazione la seconda transazione con la commissione più alta, scartando la prima.

2.7 Confronto tra transazione bancaria e transazione in bitcoin

Bitcoin può essere un'alternativa come metodo di pagamento per le aziende, rispetto ai pagamenti internazionali o ai micropagamenti, senza aver bisogno di un intermediario come la banca, perché i trasferimenti avvengono direttamente tra gli utenti.

Limiti massimo di denaro inviabile Uno dei mezzi di pagamento più veloci, introdotto dal 2017, è il bonifico istantaneo (o SEPA Instant Credit Transfer). Può essere effettuato in ogni momento, il pagamento avviene entro dieci secondi, prevede un massimo di 100.000 euro ad operazione e, una volta effettuato, è irrevocabile. Non c'è invece un limite massimo di bitcoin inviabili.

Costi delle operazioni Il costo di un bonifico dipende dalla banca e dalle condizioni contrattuali, dal tipo di bonifico (se nazionale, o verso beneficiario all'estero), dall'urgenza (bonifico standard o istantaneo) dalla cifra, dalle modalità (online, sportello), dalla banca del destinatario, etc. Un bonifico online nazionale va dall'essere gratuito ai 2,50 euro circa, a carico dell'ordinante. Per fare un bonifico estero è necessario avere, oltre al nome del beneficiario e al suo numero di conto, anche il codice SWIFT. SWIFT (Society of Worldwide Interbank Financial Telecommunication) è una rete tra istituti bancari che consente di effettuare bonifici a livello internazionale. Il bonifico SWIFT ha costi più elevati rispetto ad un bonifico nazionale che variano da banca a banca, ma solitamente vengono applicate una commissione fissa (tra i 10 ed i 20 euro), una commissione variabile in percentuale all'importo da trasferire e una maggiorazione sul tasso di cambio, cioè una tariffa per la conversione di valuta. Invece, per inviare bitcoin si ha una commissione

media pari (secondo blockchain.com, al 07/07/2020) a 1,08 dollari statunitensi. Non ci sono maggiorazioni di costo per i pagamenti internazionali.

Tempi di accreditamento Il bonifico ha tempi di accreditamento del denaro che dipendono dall'operazione: di solito sono 2-3 giorni lavorativi dall'ordine (se bonifico estero all'incirca 3-5 giorni), a meno che non sia un bonifico istantaneo, disponibile solo in alcune banche, con un tempo di accreditamento sul conto del beneficiario in dieci secondi. Il tempo di accreditamento di una transazione in bitcoin varia in base al tempo di conferma della transazione e suo inserimento nella blockchain. Il tempo di conferma è, in media, pari a dieci minuti e varia in base alle commissioni pagate: può essere di pochi minuti, oppure ore e a volte anche alcuni giorni o di più, nel caso di commissioni troppo basse.

Annullamento e reversibilità Si può annullare un bonifico bancario, solo se il denaro non è stato accreditato sul conto corrente del beneficiario; per Bitcoin ci sono dei modi per annullare le transazioni se non è già stato accreditato l'importo, spiegati nella sezione 2.6 a pagina 36.
L'irreversibilità delle transazioni in bitcoin può essere un vantaggio per un esercizio commerciale nel caso in cui l'utente paghi e poi decida di annullare il pagamento per commettere una truffa, ma è anche uno svantaggio per l'utente nel caso subisca una frode, perché non c'è nessuna garanzia e nessun ente terzo che possa intervenire.

Assistenza e garanzie Le banche forniscono assistenza ai loro clienti in caso di furto dei dati del conto online, mentre per Bitcoin non ci sono tutele o garanzie: con un furto di dati è possibile appropriarsi dell'intero portafoglio, a meno che non ci si rivolga a compagnie che offrono un'assicurazione.

2.8 Bitcoin Halving

Nel sistema di Bitcoin non c'è nessuna banca centrale, come la BCE o la FED, che regola la base monetaria. Al momento della nascita di Bitcoin è stato impostato un algoritmo che regola la base monetaria, quindi che già definisce in anticipo quanta moneta verrà creata, con che modalità e a quale tasso.
Il numero massimo di bitcoin è pari a 21 milioni, creabili entro il 2140 e la creazione di nuova criptovaluta avviene quando un miner aggiunge un nuovo blocco alla catena e riceve la ricompensa.
La ricompensa per i minatori si riduce della metà ogni 210.000 blocchi, cioè ogni quattro anni circa. Inizialmente la ricompensa era di 50 bitcoin per blocco minato, per arrivare oggi a 6,25 bitcoin per blocco, infatti l'11 maggio 2020 è avvenuto l'halving.
Questo algoritmo di offerta decrescente dei bitcoin è stato scelto perché simile al tasso per cui le commodity come l'oro vengono minate.

Tabella 2.2: Dati sui dimezzamenti dei bitcoin

Date reached	Reward Era	BTC/block	Year (estimate)	Start BTC	BTC Added	End BTC	End BTC % of Limit
2009-01-03	1	50,00	2009	0	2.625.000	2.625.000	12,500%
2010-04-22	1	50,00	2010	2.625.000	2.625.000	5.250.000	25,000%
2011-01-28	1	50,00	2011	5.250.000	2.625.000	7.875.000	37,500%
2011-12-14	1	50,00	2012	7.875.000	2.625.000	10.500.000	50,000%
2012-11-28	2	25,00	2013	10.500.000	1.312.500	11.812.500	56,250%
2013-10-09	2	25,00	2014	11.812.500	1.312.500	13.125.000	62,500%
2014-08-11	2	25,00	2015	13.125.000	1.312.500	14.437.500	68,750%
2015-07-29	2	25,00	2016	14.437.500	1.312.500	15.750.000	75,000%
2016-07-09	3	12,50	2016	15.750.000	656.250	16.406.250	78,125%
2017-06-23	3	12,50	2018	16.406.250	656.250	17.062.500	81,250%
2018-05-29	3	12,50	2019	17.062.500	656.250	17.718.750	84,375%
2019-05-24	3	12,50	2020	17.718.750	656.250	18.375.000	87,500%
2020-05-11	4	6,25	2021	18.375.000	328.125	18.703.125	89,063%
	4	6,25	2022	18.703.125	328.125	19.031.250	90,625%
	4	6,25	2023	19.031.250	328.125	19.359.375	92,188%
	4	6,25	2024	19.359.375	328.125	19.687.500	93,750%

Fonte: https://en.bitcoin.it/wiki/Controlled_supply

La Tabella 2.2 mostra cosa è accaduto finora nel sistema Bitcoin riguardo ai dimezzamenti e al numero dei bitcoin. Per ogni data sono indicati il numero dei bitcoin dati come ricompensa ai miners, il numero dei bitcoin totali, il numero dei bitcoin aggiunti e la percentuale di bitcoin creati rispetto ai 21 milioni. Sono evidenziate in giallo le righe della tabella che indicano i momenti in cui sono avvenuti gli halving, dove si può notare il dimezzamento della ricompensa nella colonna BTC/block.
Dove non sono presenti date è indicata la situazione nel futuro prossimo, cioè il numero dei bitcoin che esisteranno e la ricompensa futura per i miners. Gli anni in cui avverranno i prossimi halving sono una stima, perché i quattro anni che separano un halving dall'altro sono un intervallo teorico.

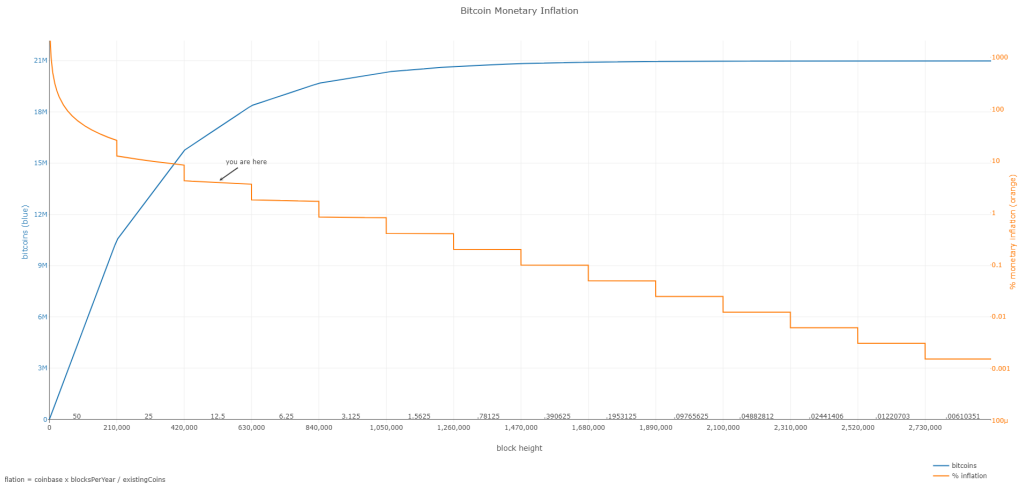
2.8.1 L'inflazione e la deflazione di Bitcoin

L'inflazione è «l'aumento progressivo del livello medio generale dei prezzi, o anche diminuzione progressiva del potere di acquisto (cioè del valore) della moneta»[21].
Le banche centrali possono controllare l'inflazione mantenendola stabile perché hanno la libertà di gestire la moneta in circolazione e la quantità di moneta creabile non ha limiti: per esempio se vogliono aumentare l'inflazione stampano moneta così si svaluta, quindi il suo valore diminuisce perché perde potere di acquisto e si genera inflazione, perché se la moneta si svaluta occorreranno più unità di moneta per acquistare uno stesso bene. Possono anche generare deflazione diminuendo l'offerta di moneta, o assorbire moneta

[21] http://www.treccani.it/enciclopedia/inflazione/

attraverso i tassi di interesse, in base alla situazione economica e al risultato che vogliono ottenere.
Mentre le banche centrali possono creare quanta moneta vogliono, teoricamente potrebbero generare inflazione all'infinito; Bitcoin invece non ha una banca centrale che gestisce la creazione di nuova moneta perché la quantità massima totale, la modalità e il rateo di creazione di moneta sono fissati a priori.
Siccome vengono prodotti nuovi bitcoin, è presente il fenomeno dell'inflazione, perché l'emissione di nuova moneta fa svalutare i bitcoin stessi. Però, via via che ne vengono prodotti di nuovi, ci si avvicina sempre più al limite massimo e si prevede che, se questa criptovaluta continuerà ad essere utilizzata e avrà domanda di mercato, l'inflazione si abbasserà col trascorrere del tempo per tendere a zero, perché diventa un bene sempre più scarso ed è ragionevole pensare che aumenti di valore. Nei momenti degli halving, in cui il tasso di estrazione dimezza e vengono prodotti la metà dei bitcoin rispetto al passato, il tasso di inflazione si dimezza. Quando non sarà più possibile produrli, l'inflazione cesserà e bitcoin diventerà una moneta deflazionistica: ciò significa che una volta smesso di essere estratto non ci potrà essere svalutazione e in teoria aumenterà di valore, anche per via del fatto che molti bitcoin diventeranno sempre meno accessibili per la perdita da parte dei proprietari delle proprie chiavi private. Una volta minati tutti i possibili bitcoin, l'unico premio e incentivo per continuare a fare mining saranno le commissioni, perché quando sarà minato l'ultimo bitcoin, non se ne potranno più produrre. Quindi bitcoin è una moneta inflazionistica finché raggiungerà il limite massimo di 21 milioni, da quel momento in poi l'inflazione cesserà e diventerà deflazionistica.

Figura 2.14: Totale dei bitcoin e inflazione



Fonte: https://plotly.com/ BashCo/5.embed?share_key=ljQVkaTiHXjX2W41UiqzCn

Nella Figura 2.14 sono rappresentati in blu il totale dei bitcoin che sono già stati prodotti e che verranno prodotti in futuro: il totale di nuovi bitcoin dipende dall'aumento del

numero di blocchi e dalla ricompensa data ai miners. Ha un andamento crescente, con un incremento marginale decrescente, perché la ricompensa ai miners si riduce della metà ogni quattro anni circa; l'andamento rimarrà tale fino al raggiungimento dei 21 milioni, dopodiché la crescita sarà pari a zero.
In arancione invece è evidenziata l'inflazione: si può notare l'andamento decrescente dell'inflazione a gradini, con un decremento marginale decrescente e il dimezzamento della stessa quando accadono gli halving. Manterrà questo andamento fino al limite massimo di bitcoin creabili, in cui l'inflazione sarà pari a zero e da quel momento in poi diventerà un fenomeno deflazionistico.
Il tasso di inflazione annuo viene calcolato con questa formula:

$$inflation = \frac{Coinbase \times blocksPerYear}{existingCoins}$$

Coinbase si riferisce al numero di bitcoin in ricompensa ai minatori.
BlocksPerYear sono i blocchi aggiunti all'anno.
ExistingCoins è il totale di bitcoin esistenti.

L'inflazione annua al 10/05/2020, cioè il giorno prima dell'halving, è pari a:

$$\frac{12,5 \times 52.500}{18.365.000} = 3,5733732\%$$

L'inflazione annua al 11/05/2020, cioè il giorno dell'halving, è pari a:

$$\frac{6,25 \times 52.500}{18.375.000} = 1,7857142\%$$

Capitolo 3

Stock-to-Flow e Modello Stock-to-Flow

3.1 Stock-to-Flow

«Il rapporto Stock to Flow è la quantità di una merce detenuta in scorte, divisa per la quantità prodotta annualmente»[22].
È un indice utilizzato per valutare la scarsità o l'abbondanza di un bene perché indica il tempo, all'attuale tasso di estrazione o produzione (*flow*), richiesto per raggiungere lo stock corrente. Mette in correlazione lo *stock*, cioè la giacenza totale della risorsa estratta fino ad oggi e il *flow*, cioè il flusso estratto in una specifica unità di tempo (anno, mese, giorno).

$$\text{Stock-to-Flow} = \frac{stock}{flow}$$

È usato di solito per valutare la scarsità dei metalli preziosi e viene oggi utilizzato anche per le criptovalute, in quanto possono essere paragonate a queste risorse per via delle modalità con cui vengono create.
Il valore dipende dalla grandezza della giacenza (*stock*) rapportata rispetto a ciò che viene estratto ogni anno, mese o giorno (*flow*): maggiore il valore dell'indice, maggiore è la scarsità del bene considerato.
Questo indice può essere utile ad un investitore quando vuole valutare un bene che possiede o su cui decide di investire. Infatti, più una risorsa è scarsa, perché i tempi di estrazione sono lunghi, più il suo prezzo è alto sul mercato. Questo fenomeno, però, ha un certo effetto quando la risorsa considerata ha un'alta domanda sul mercato, perché in caso di bassa domanda la scarsità non influirebbe, dato che nessuno compra il bene.

Di converso, *flow/stock*, indica invece il tasso di crescita dell'offerta.

3.1.1 Stock-to-Flow di Bitcoin

Lo Stock-to-Flow di Bitcoin è calcolato dividendo il numero di bitcoin complessivamente estratti finora, per il numero di bitcoin emessi in una specifica unità di tempo (giorno, mese, anno) e indica quanto tempo è richiesto per raggiungere lo *stock* corrente di bitcoin.

[22] Tradotto da: https://monetary-metals.com/gold-economics/lexicon/?mmdesc=stock-to-flow-ratio#stock-to-flow-ratio

Stock-to-Flow (*flow* annuo) prima dell'halving, il 10 maggio 2020 =

$$\frac{18.374.999}{656.250} = \textbf{27,99999847619048 anni}$$

Stock-to-Flow (*flow* annuo) l'11 maggio 2020 =

$$\frac{18.375.000}{328.125} = \textbf{56 anni}$$

$$27,99999847619048(1+x) = 56$$

$$\textbf{(1+x) = 2,00000014455784}$$

I calcoli riguardano un'ipotetica situazione in cui il numeratore dell'indice è stato aumentato di uno nel momento in cui il *flow* si è dimezzato, col fine di valutare l'effetto che ha una piccola variazione di bitcoin in circolazione sull'indice, mentre avviene l'halving.
Il 10 maggio 2020, con 18.374.999 bitcoin già creati e con una produzione annua di 656.250 bitcoin, sono necessari circa 28 anni al ritmo di produzione attuale per raggiungere il numero di bitcoin creati. Siccome la ricompensa dei bitcoin si riduce della metà ogni quattro anni, anche il flusso di nuovi bitcoin per anno diminuirà, mentre lo *stock* sale e quindi l'indice più che raddoppia, arrivando a 56 anni per raggiungere lo *stock* corrente.
Come si può notare dai calcoli, quando è avvenuto l'halving l'indice non ha avuto un raddoppio secco, infatti il coefficiente moltiplicativo $(1 + x)$ è maggiore di due, perché nel tempo il denominatore si dimezza, sebbene resterà fisso per circa quattro anni, ma il numeratore continua ad aumentare nel tempo.
Siccome quest'anno, l'11 maggio 2020, è avvenuto l'halving e l'indice è più che raddoppiato, significa che, da un giorno all'altro, i bitcoin sono diventati maggiormente scarsi, più del doppio rispetto a prima.

3.2 Modello Stock-to-Flow di PlanB

Il modello Stock-to-Flow è stato pubblicato a Marzo 2019 da PlanB[23], che è lo pseudonimo dell'autore. È un modello che mette in relazione il valore dell'indice con il prezzo di Bitcoin. «L'ipotesi in questo studio è che la scarsità, misurata dal rapporto SF, guidi direttamente il valore»[24]. Il modello prevede che, con gli halving e con l'aumento della scarsità, e quindi con l'aumento dell'indice, il prezzo dei bitcoin aumenti.
Di solito per i metalli lo Stock-to-Flow è costante in quanto il tempo di estrazione per la medesima quantità di metallo è circa costante nel corso del tempo; per i bitcoin invece non è costante perché, ogni quattro anni, aumenta più del doppio rispetto a prima.

[23] https://twitter.com/100trillionusd
[24] https://medium.com/@carloclerici/il-concetto-di-scarsita-nella-determinazione-del-valore-di-bitcoin-c716c0ad3fff

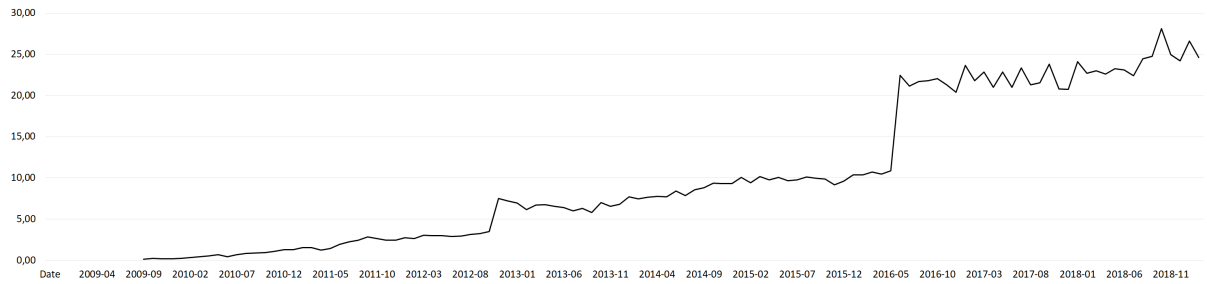
La scarsità digitale ha un valore quantificabile con lo Stock-to-Flow e il modello basato sullo Stock-to-Flow potrebbe essere utilizzato per prevedere il valore dei bitcoin nel futuro.

3.2.1 La costruzione del modello

L'autore, per ricavare i dati su cui costruire il modello, ha eseguito una query[25] della blockchain di Bitcoin: ha scaricato il numero di blocchi costruiti al mese, da dicembre 2009 a febbraio 2019, li ha moltiplicati per la ricompensa che veniva data in quel momento ai miners e così ha calcolato il valore dello *stock* per ogni mese, però senza considerare il primo milione di bitcoin, cioè quelli di Satoshi Nakamoto, minati e mai trasferiti. Poi, facendo la differenza tra uno *stock* mensile e il suo precedente, ha calcolato il *flow* mensile, che ha moltiplicato per 12 per ricavare il flow annuo.
Avendo a disposizione lo *stock* e il *flow* annuo, ha calcolato lo Stock-to-Flow annuo, per ogni mese.

$$\mathbf{SF} = \frac{stockmese - 1.018.750}{(stockmese - stockmeseprecedente) \times 12}$$

Figura 3.1: Stock-to-Flow dei bitcoin, valore annuo per ogni mese



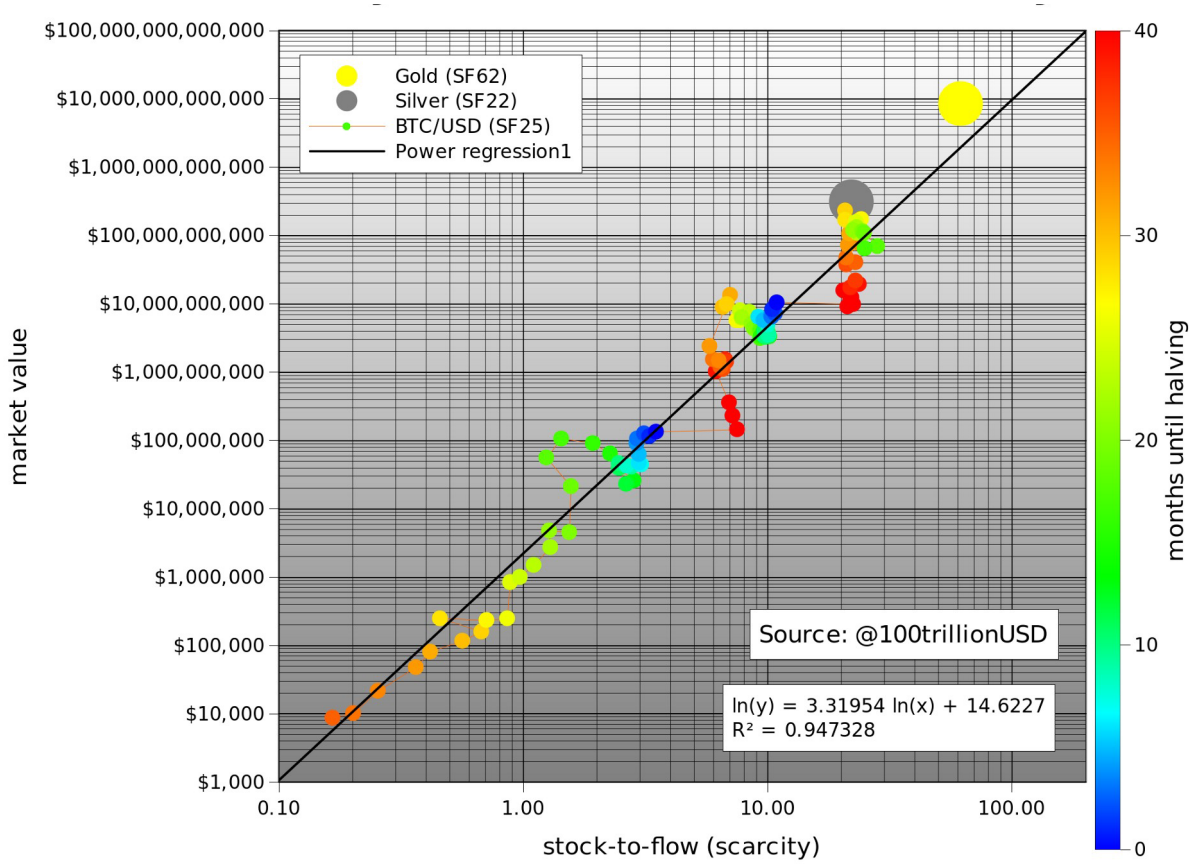
Fonte dati: https://github.com/100trillionUSD/bitcoin

Il grafico nella Figura 3.1 rappresenta l'andamento dello Stock-to-Flow: l'asse orizzontale indica il tempo, mentre l'asse verticale il valore dello SF in anni. Il grafico mostra un andamento crescente nel tempo e si evidenziano dei rialzi "a gradini" nei giorni in cui è avvenuto l'halving, infatti in quel momento l'estrazione dei bitcoin si dimezza, lo Stock-to-Flow più che raddoppia e i bitcoin diventano un bene più scarso.
Poi, l'autore ha aggiunto ai dati i prezzi noti di Bitcoin che partono da luglio 2010. Con i dati a disposizione è stato possibile creare un primo grafico di dispersione che mette in relazione lo SF e il valore di mercato dei bitcoin: nell'asse delle ascisse c'è lo Stock-to-Flow, mentre nell'asse delle ordinate c'è il valore o capitalizzazione di mercato (*stock* dei bitcoin in circolazione moltiplicato per il prezzo in dollari americani). Dato che gli halving hanno un peso rilevante sullo SF, i punti del grafico hanno un colore diverso in base ai mesi che

[25]Termine che indica l'interrogazione di un database da parte di un utente

separano dall'halving successivo: il colore passa da tonalità calde a tonalità più fredde (rosso, giallo, verde e infine blu) all'avvicinarsi dell'evento. Sono stati aggiunti, per avere un riferimento, lo Stock-to-Flow annuo dell'oro (62) e dell'argento (22), con i rispettivi valori di mercato: 8,5 trilioni di dollari e 308 miliardi di dollari. Il modello si basa sull'assunzione che vi sia domanda sufficiente di bitcoin per arrivare al valore di mercato indicato in Figura 3.2.

Figura 3.2: Grafico di dispersione



Fonte: https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25

L'autore ha elaborato un modello di regressione lineare, calcolando una funzione matematica corrispondente all'equazione di una retta, che descrive la dipendenza di una variabile rispetto ad un'altra, in questo caso che il valore di mercato dei bitcoin dipenda dallo Stock-to-Flow. Per calcolare la regressione, i valori di entrambe le variabili sono stati espressi attraverso una scala logaritmica con base naturale (cioè calcolando il logaritmo naturale di entrambe), perché i valori della capitalizzazione di mercato sono molto elevati, fino ai 100 miliardi di dollari.
Il modello ha una funzione di regressione lineare pari a:

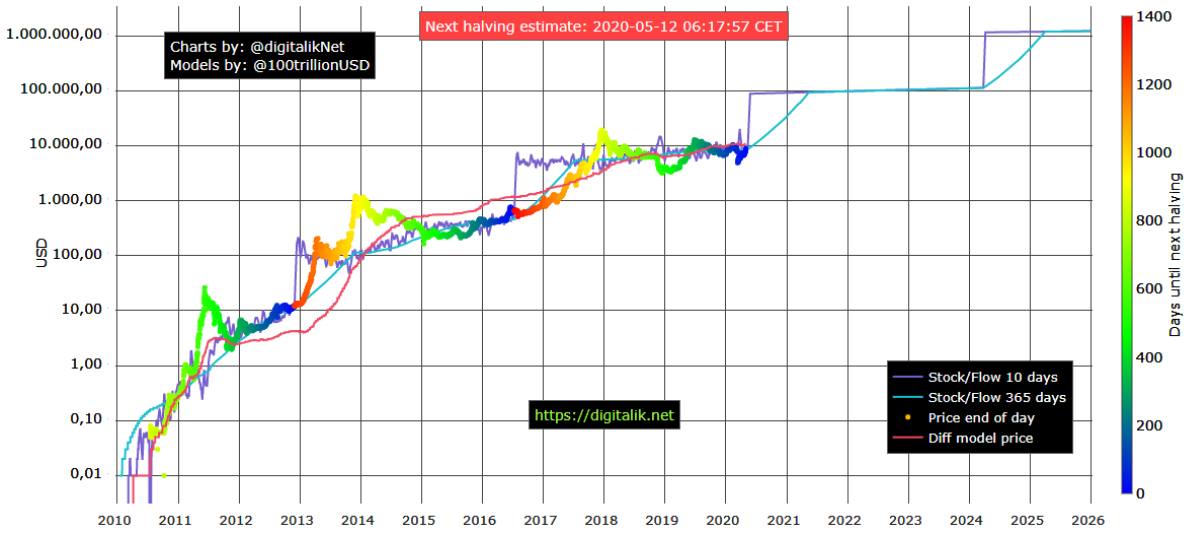
$$\ln(capmercato) = 3,31954 \ln(SF) + 14,6227$$

Può essere scritta anche come:

$$capmercato = SF^{3,31954} \times e^{14,6227}$$

I risultati forniti dalla regressione mostrano una relazione tra Stock-to-Flow e il valore di mercato con un indice di determinazione r^2, indice che misura la bontà dell'approssimazione della retta ai punti osservati, pari al 0,947328. Non è al 100% perché, secondo l'autore, il prezzo non dipende solo dallo SF ma anche da altri fattori, come regolamentazioni varie, notizie, eventi, hackeraggio, etc.
L'autore poi ha messo a confronto il valore di mercato dei bitcoin e lo Stock-to-Flow. Siccome la produzione dei bitcoin è già stata predeterminata, nell'ipotesi che la domanda di bitcoin sia sempre alta, si può tracciare una linea che prevede lo SF futuro.

Figura 3.3: Stock-to-Flow e capitalizzazione di mercato in dollari americani



Fonte: https://digitalik.net/btc/

Nel grafico in Figura 3.3, sono presenti quattro linee che corrispondono a quattro serie di valori.
La linea più spessa e multicolore rappresenta il prezzo a fine giornata dei bitcoin, e si colora diversamente in base al tempo che rimane al successivo halving.
Lo Stock-to-Flow invece è stato calcolato in due modi diversi in base alla finestra temporale a cui il flow fa riferimento.
La linea viola è lo "Stock-to-Flow 10 giorni", perché il flow viene calcolato in questo modo: prende la produzione di bitcoin di dieci giorni, la divide per dieci e moltiplica il risultato per 365.
La linea azzurra invece è lo "Stock-to-Flow 365 giorni", perché il flow viene calcolato prendendo in considerazione la produzione di 365 giorni, precedenti rispetto al valore del

giorno osservato sul grafico. In entrambi i casi lo stock è sempre quello corrente, aggiornato giorno per giorno e l'indice viene sempre calcolato con la formula vista a pagina 42.
La linea rossa invece mostra il valore di mercato di Bitcoin, ma attraverso un diverso modello del prezzo calcolato utilizzando il parametro della difficoltà giornaliera nel mining. Dal grafico in Figura 3.3 è possibile vedere che le linee crescono quasi contemporaneamente, c'è una correlazione positiva tra SF e la capitalizzazione di mercato e si nota anche dal rialzo del prezzo circa un anno dopo il dimezzamento, data dal fatto probabilmente che è necessario un periodo di tempo in cui gli utenti si rendano consapevoli del dimezzamento del tasso di estrazione della criptovaluta e il relativo aumento del valore.
«Notate la bontà del fit, in particolare l'adeguamento del prezzo quasi immediato dopo l'halving del novembre 2012. L'adeguamento dopo l'halving di giugno 2016 è stato molto più lento, probabilmente a causa della concorrenza di Ethereum e della vicenda di DAO, che portò ad una perdita di 50 milioni di dollari»[26].
«La capitalizzazione di mercato prevista per bitcoin dopo l'halving del maggio 2020 è di 1000 miliardi di dollari, che si traduce in un prezzo bitcoin di $ 55.000. È abbastanza spettacolare. [...] sapremo se la previsione è vera probabilmente uno o due anni dopo l'halving, nel 2020 o nel 2021. Questo sarà un ottimo test fuori campione di questa ipotesi e modello»[27].

3.2.2 Coefficiente di correlazione lineare di Bravais

Per verificare se lo Stock-to-Flow e il valore di mercato abbiano una correlazione nelle loro rispettive variazioni nel corso del tempo, sono stati scaricati i dati del modello originale di PlanB così da avere a disposizione i dati dello Stock-to-Flow e del valore di mercato in dollari americani dei bitcoin nel tempo, in scala logaritmica. Entrambi fanno parte di una distribuzione doppia disaggregata, cioè un'elencazione delle coppie di modalità relative a due caratteri, così come si presentano nei dati.
Con i dati a disposizione è stato calcolato il coefficiente di correlazione lineare di Bravais, indice utilizzato in una distribuzione doppia disaggregata che varia dall'intervallo [-1,1]. Questo indice è pari ad 1 quando tutti i punti $(x_i; y_i)$ si trovano su una retta con coefficiente angolare[28] positivo, mentre è uguale a -1 quando tali punti si trovano su una retta con coefficiente angolare negativo. Tra i due caratteri, vi è correlazione positiva quando essi tendono a crescere (o decrescere) insieme, a differenza di una correlazione negativa quando al crescere di uno dei due l'altro tende a decrescere (o viceversa).

$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2 \sum_{i=1}^{n}(y_i - \overline{y})^2}}$$

[26] https://medium.com/@carloclerici/il-concetto-di-scarsita-nella-determinazione-del-valore-di-bitcoin-c716c0ad3fff
[27] Ibidem
[28] È un coefficiente numerico che indica la pendenza di una retta. Nell'equazione $y = mx + q$, m è il coefficiente della retta.

Impostando x e y rispettivamente come il logaritmo naturale dello Stock-to-Flow e il logaritmo naturale del prezzo in dollari di un bitcoin, il risultato ottenuto è 0,97519248. Siccome è un valore che si avvicina ad 1, significa che tra i valori delle due variabili, entrambi in scala logaritmica, c'è una relazione lineare: i punti $(x_i; y_i)$ si trovano su una retta con coefficiente angolare positivo e quindi all'aumentare di uno, l'altro generalmente aumenta.
r assume valori nell'intervallo [-1,1] perché è la radice quadrata dell'indice di determinazione r^2, relativo alla retta di regressione calcolata precedentemente con il modello di PlanB, che stima il valore di mercato in base al valore dello Stock-to-Flow.

3.2.3 Limiti del modello

Questo modello è basato sui dati passati e non tiene in considerazione gli eventi che possono accadere, come per esempio l'ingresso di una criptovaluta migliore, nuove norme, costi aggiuntivi, etc, che possono influenzare il valore di mercato di Bitcoin nel breve o nel lungo periodo. Un esempio è rappresentato dalla caduta del 50% del valore di un bitcoin in due giorni, a causa dell'emergenza Covid19 quando, l'11 marzo 2020, l'epidemia è stata dichiarata pandemia. Infatti i mercati hanno cercato di fuggire dal rischio, vendendo gli asset più rischiosi (come le criptovalute) per aumentare la liquidità e, siccome la domanda di questi beni è diminuita, c'è stato un ribasso nel loro prezzo. Nonostante ciò, il modello Stock-to-Flow ha continuato ad essere valido, anche immediatamente dopo la caduta dei mercati.
Inoltre, questo modello assume che l'aumento della scarsità implichi un aumento di prezzo, ma non tiene conto della domanda, che entra in gioco prima della scarsità del bene, perché in assenza di domanda nessuno comprerebbe bitcoin, indipendentemente dalla quantità disponibile. Poi non è possibile sapere con precisione i bitcoin realmente in circolazione, cioè senza i bitcoin persi (circa 3,7 milioni) a causa della perdita dei dati di accesso al wallet, che andrebbero a diminuire l'indice.
Vitalik Buterin, cofondatore della criptovaluta Ethereum, afferma che il modello Stock-to-Flow non sia utile per prevedere il futuro valore dei bitcoin e sostiene che questo modello sia «una cavolata razionalizzata a posteriori»[29].

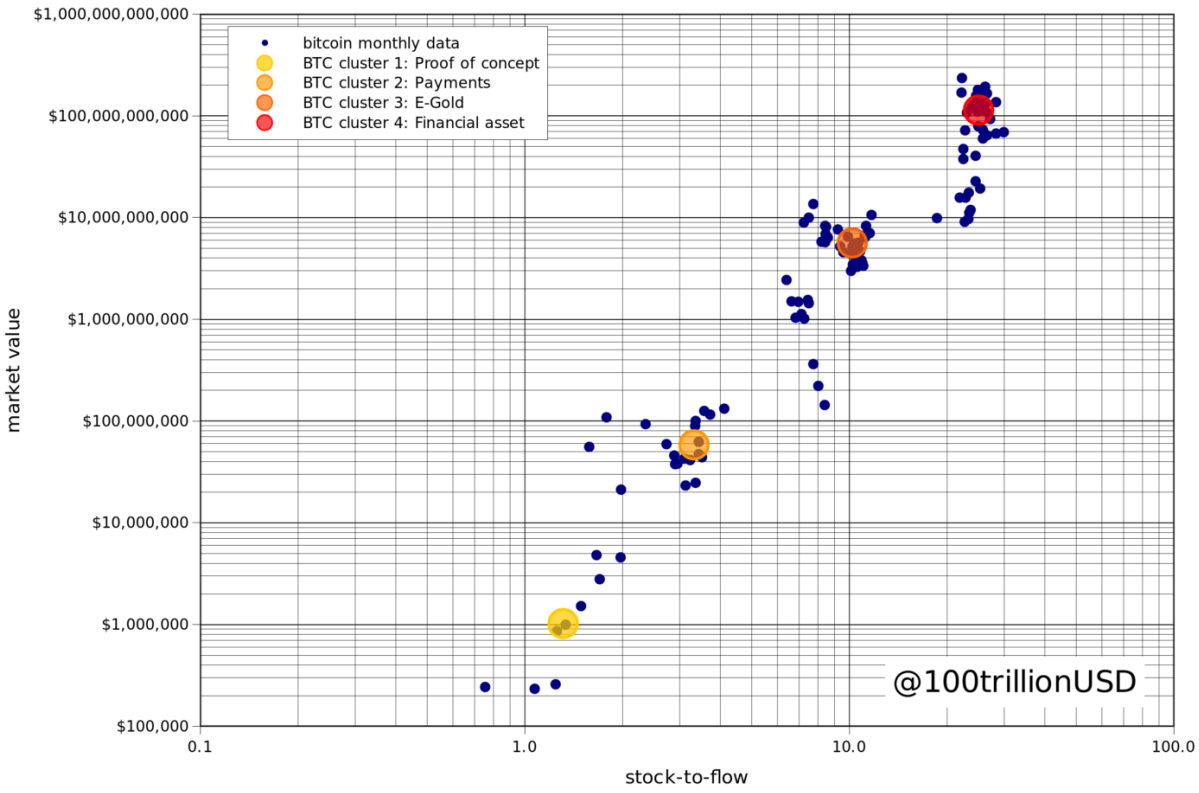
3.3 Modello Stock-to-Flow Bitcoin con asset incrociati (S2FX)

Il 27 aprile 2020 è stata pubblicata una nuova versione[30] del modello da parte di PlanB. Il modello originale presenta una serie di dati, riguardanti lo Stock-to-Flow e il valore di mercato di Bitcoin, ordinata cronologicamente nel tempo. In questo nuovo modello,

[29] https://it.cointelegraph.com/news/rationalized-bullst-vitalik-buterin-pans-bitcoin-price-forecasts
[30] https://medium.com/@100trillionUSD/bitcoin-stock-to-flow-cross-asset-model-50d260feed12

l'autore rimuove il tempo e, oltre ad introdurre due nuovi asset, cioè l'oro e l'argento, introduce il concetto delle transizioni tra fasi.
In una transizione tra fasi un elemento assume diverse proprietà, come il ghiaccio che diventa acqua e poi vapore. Queste transizioni sono presenti anche in finanza, come ad esempio il dollaro che ha avuto diverse transizioni nel corso del tempo: è passato da essere una moneta d'oro, ad una banconota senza valore coperta da una riserva d'oro in una banca, fino ad oggi con le banconote a corso legale.
Anche Bitcoin ha attraversato varie fasi. All'inizio era una **Proof of Concept** (letteralmente: Prova di concetto), cioè un progetto in fase di prova per verificare se l'idea di Bitcoin come moneta elettronica era fattibile. Poi è passato da essere un **mezzo di pagamento**, quando un bitcoin equivaleva ad un dollaro americano, a **oro digitale**, quando un bitcoin equivaleva ad un'oncia di oro. L'ultima fase vede Bitcoin come un **asset finanziario** su cui investire. Secondo l'autore, Bitcoin possiede differenti proprietà in base alla fase che sta attraversando.

Figura 3.4: Le quattro fasi, in quattro cluster



Fonte: https://medium.com/@100trillionUSD/bitcoin-stock-to-flow-cross-asset-model-50d260feed12

La Figura 3.4, mostra i valori relativi allo Stock-to-Flow e al valore di mercato del modello originale, rappresentati attraverso i punti in blu. È possibile individuare quattro cluster[31],

[31]Termine che indica un gruppo di oggetti vicini tra loro.

formati da più insiemi di punti in blu vicini fra loro. Ogni cluster corrisponde ad una fase, ognuna delle quali ha una differente combinazione di SF e valore di mercato:

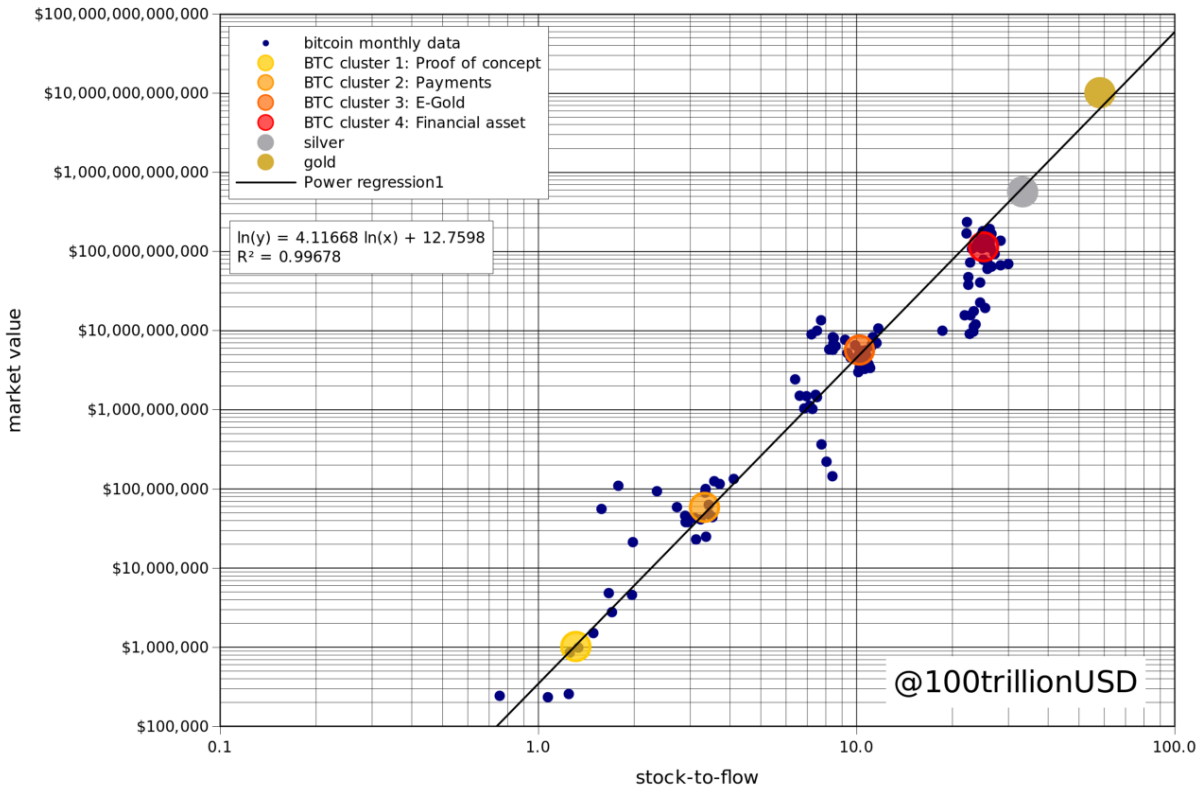
Tabella 3.1: Fasi, Stock-to-Flow e valori di mercato di Bitcoin

Fase	**Stock-to-Flow** (in anni)	**Valore di mercato**
Proof of Concept	1,3	1 milione di $
Mezzo di pagamento	3,3	58 milioni di $
Oro digitale	10,2	5,6 miliardi di $
Asset Finanziario	25,1	114 miliardi di $

Fonte: https://medium.com/@100trillionUSD/bitcoin-stock-to-flow-cross-asset-model-50d260feed12

Una volta identificate le quattro fasi, l'autore ha aggiunto nel grafico l'oro e l'argento in base al loro SF e alla loro capitalizzazione di mercato: l'**argento** presenta uno SF pari a 33,3 anni e un valore di mercato pari a 561 miliardi di dollari, mentre l'**oro** presenta uno SF pari a 58,3 anni e un valore di mercato pari a 10.088 miliardi di dollari.

Figura 3.5: Modello Stock-to-Flow Bitcoin con asset incrociati



Fonte: https://medium.com/@100trillionUSD/bitcoin-stock-to-flow-cross-asset-model-50d260feed12

Come si può notare nella Figura 3.5, i sei cluster si posizionano su una linea retta e l'autore ha calcolato una regressione lineare su questo modello. Rispetto al modello originario,

in questo caso l'autore ha calcolato la regressione non solo con i dati di Bitcoin, ma includendo anche i dati dell'oro e dell'argento.
Tra i risultati della regressione figura r^2, indice di bontà dell'adattamento della retta ai punti osservati, pari a 0,99678, vicinissimo al 100% e più alto rispetto a quello del modello precedente; ciò significa che i dati si adattano meglio a questo modello. Il coefficiente di correlazione lineare di Bravais, calcolato facendo la radice quadrata di r^2, è pari a 0,9984, perciò i valori presentano una correlazione lineare positiva, cioè tendono a crescere o a decrescere insieme.
L'equazione della retta è pari a:

$$\ln(capmercato) = 4,11668 \ln(SF) + 12,7598$$

la quale può essere scritta anche come:

$$capmercato = SF^{4,11668} \times e^{12,7598}$$

Con la nuova versione del modello è possibile stimare il valore di mercato di Bitcoin nella prossima fase/cluster. Il modello «stima un valore di mercato della prossima fase di BTC/cluster (BTC S2F sarà 56 nel 2020–2024) di 5,5 trilioni di $. Questo si traduce in un prezzo BTC (dato 19 milioni BTC nel 2020–2024) di 288.000$»[32], un valore molto più alto rispetto ai 55.000$ previsti dal modello originale.

3.3.1 Limiti e opportunità del modello

La regressione lineare è stata calcolata solamente con sei osservazioni, corrispondenti ai dati delle quattro fasi di Bitcoin e ai dati dell'oro e dell'argento. Inoltre, siccome è un modello pubblicato di recente, non è stato ancora confutato o verificato da altre persone. Questo modello permette di vedere da una prospettiva diversa, cioè la transizione tra fasi, riguardo alla crescita del valore di mercato insieme all'aumento della scarsità dei bitcoin e può essere utile per ampliare il confronto con altri asset simili, o come base per creare altri modelli.

[32]https://medium.com/@walterrizzo91/modello-di-stock-to-flow-cross-asset-di-bitcoin-81dca7e7e74a

Capitolo 4

Altcoin

Dato che il codice sorgente di Bitcoin è pubblico e scaricabile liberamente, molti programmatori nel mondo, oltre a contribuire al miglioramento di questa criptovaluta, hanno lanciato una serie di criptovalute alternative chiamate altcoin (alternative coin = moneta alternativa). Una altcoin è una qualsiasi criptovaluta creata dopo la nascita di Bitcoin. Ad oggi ci sono più di 5000 tra criptovalute e token al mondo, con una capitalizzazione di mercato in totale pari a circa 245 miliardi di dollari, secondo Coinmarketcap.com. Il supporto della comunità di una criptovaluta è essenziale per valutare la sua forza, comunità che può essere misurata ad esempio in base agli iscritti su varie piattaforme come reddit, social network che raggruppa alcune comunità di persone in base ad un loro interesse e che rappresentano un punto di incontro per sviluppatori per collaborare sulla moneta.
Creare una nuova altcoin è un modo per testare nuove idee, senza intaccare criptovalute con grande capitalizzazione come Bitcoin e non mettere a rischio gli utenti. Quindi, ad esempio, è possibile copiare il codice di una criptovaluta open-source (vedi 2 a pagina 15) e aggiungere nuove funzionalità, oppure modificare o aggiungere parametri per creare una criptovaluta migliore dell'originale. Molte altcoin sono costruite con un sistema decentralizzato come quello di Bitcoin e sono copie del codice sorgente con lievi modifiche su alcuni parametri, come l'offerta totale di moneta creabile, il tempo di conferma delle transazioni, l'algoritmo di hashing per il mining, la sostituzione del sistema proof-of-work, la gestione dell'anonimato, etc.

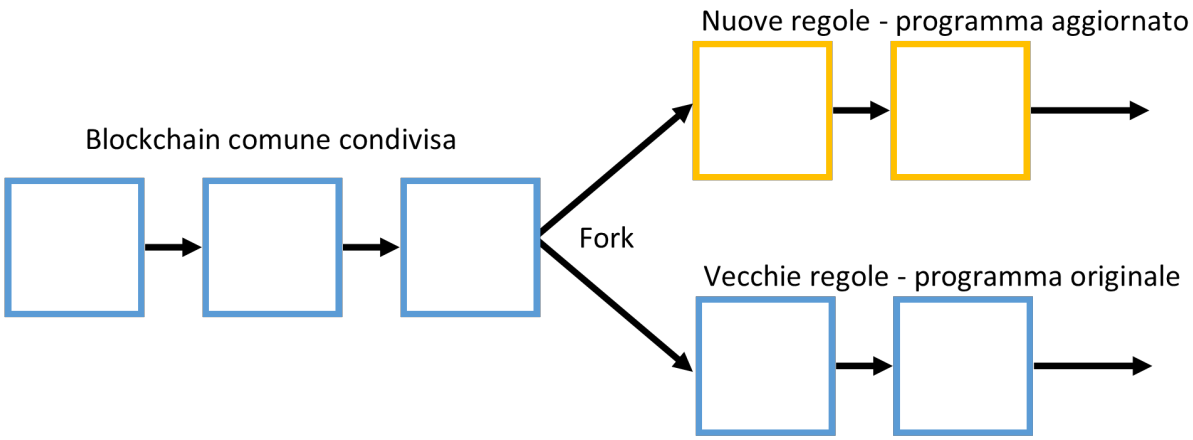
4.1 La creazione di una nuova altcoin

La creazione di una altcoin nasce attraverso un ***fork*** (biforcazione, bivio), termine informatico che indica lo sviluppo di un nuovo programma dal codice sorgente di uno già esistente.
Ogni programma informatico richiede aggiornamenti per riparare gli errori o per migliorare le prestazioni. Nel caso delle criptovalute, che si basano su un sistema decentralizzato, ogni nodo deve seguire le stesse regole, perciò se un nodo vuole continuare a partecipare alla rete deve aggiornarsi all'ultima versione.

Ci sono due tipi di *fork*: l'*hard fork* e il *soft fork*.
L'***hard fork*** si verifica quando vengono introdotte nuove funzionalità in una criptovaluta. I nodi che non hanno effettuato l'aggiornamento continuano sulla vecchia versione, e non potranno effettuare nuove transazioni e minare nuovi blocchi, fino a quando non aggiornano alla nuova versione. C'è la possibilità che alcuni nodi non siano d'accordo

sull'aggiornamento programmato e volontariamente decidano di continuare sulla vecchia versione, così si verifica una biforcazione della blockchain: da una parte la criptovaluta originaria e dall'altra la nuova altcoin con la sua comunità, le sue regole e i suoi aggiornamenti. Siccome la blockchain della nuova altcoin si basa su quella della criptovaluta d'origine, tutte le transazioni vecchie vengono copiate nella nuova blockchain. Ad esempio, se possiedo 100 bitcoin e tramite un *hard fork* viene creata una nuova altcoin di nome Newcoin, oltre ai 100 bitcoin, avrò anche 100 newcoin.
Il ***soft fork*** è una modifica di un programma con la caratteristica di essere retro-compatibile con le vecchie versioni del programma stesso. Infatti, in questo caso, i nodi non aggiornati sono ancora in grado di creare nuove transazioni e aggiungere blocchi, però rispettando le nuove regole. Ad esempio: se la dimensione massima di un blocco passasse da 2 MB a 1 MB, i nodi possono costruire nuovi blocchi anche senza aggiornare immediatamente il programma però, purché siano validi, devono costruirli seguendo la nuova regola introdotta.

Figura 4.1: Fork della blockchain



Fonte: https://medium.com/digitalassetresearch/blockchain-forks-explained-8ccf304b97c8

Una volta creata l'altcoin è importante il supporto della comunità, senza la quale la nuova criptovaluta non ha valore di mercato ed è meno sicura, in quanto non ci sono miners. È importante, perché venga conosciuta e adottata, che la propria altcoin sia accessibile negli exchanges e, per attirare nuovi miners ad usare la criptovaluta, una buona strategia potrebbe essere quella di offrire una maggiore ricompensa alla nascita della criptovaluta stessa.

4.2 Principali altcoin

Le principali altcoin per capitalizzazione in dollari americani dopo Bitcoin sono: Ether, XRP, Tether, Bitcoin Cash, Bitcoin SV, Litecoin.[33]

[33]Le immagini delle altcoin sotto riportate sono state prese da: https://coinmarketcap.com/

Ether (simbolo: ETH), nata nel 2013, è la criptovaluta utilizzata su Ethereum, una piattaforma decentralizzata basata su una blockchain che permette di implementare smart contract.

Gli smart contract sono protocolli informatici «impiegati per formalizzare gli aspetti di un rapporto - normalmente di scambio - e che sono capaci di dare autonoma esecuzione ai termini programmati qualora vengano soddisfatte certe condizioni definite ex ante»[34]. Dal punto di vista giuridico «costituisce un contratto avente alcuni elementi attivabili in maniera automatica, sia a livello informatico, poiché consta di linee di codice che si autoeseguono al verificarsi di una condizione prefissata»[35]. Un esempio di smart contract è la possibilità di utilizzare un servizio in streaming che smette di funzionare se non viene pagata una rata dell'abbonamento.

La peculiarità di Ethereum è il fatto che la sua blockchain è programmabile, perché gli sviluppatori possono utilizzarla per creare applicazioni, chiamate dApps che utilizzano la criptovaluta Ether. Tali applicazioni, una volta caricate su Ethereum, vengono eseguite sempre allo stesso modo secondo le istruzioni preimpostate e non necessitano di intermediari.

Ripple è un protocollo nato nel 2013 ed è anche la criptovaluta (XRP) utilizzata su RippleNet, rete globale per il trasferimento di fondi. Ripple è rivolto principalmente ad istituzioni finanziarie come banche e sistemi di pagamento, come ad esempio Mastercard. Secondo il loro sito ufficiale, più di 300 istituzioni finanziarie in più di 40 paesi in tutto il mondo sono dentro la rete di Ripple, perché possono effettuare transazioni finanziarie a livello globale più velocemente, a basso costo e in tempo reale.

Tether (USDT, EURT, CNHT, XAUT) è una criptovaluta che ha un valore stabile rispetto alle altre, perché il suo valore è ancorato al valore di una valuta reale con un rapporto 1:1. Per esempio, un tether vale un dollaro e viceversa e questo rapporto viene mantenuto nel tempo: ciò è reso possibile dal fatto che una singola unità di questa criptovaluta viene emessa soltanto se è coperta da un'unità della valuta corrispondente (dollaro, euro, etc.) nelle riserve della società Tether Limited. È definita come uno stablecoin, per via della sua stabilità e il progetto include altre monete Tether, legate rispettivamente al prezzo dell'euro, al prezzo dello yuan cinese (solo la quotazione offshore, valida per transazioni esterne al paese) e al prezzo dell'oro.

Bitcoin Cash (BCH) è nata nel 2017 a seguito di un fork di Bitcoin, perché alcuni utenti desideravano aumentare la velocità di elaborazione delle transazioni. Ciò è stato reso possibile incrementando la dimensione dei blocchi della catena fino a 8

[34] A. Contaldo e F. Campara. *Blockchain, criptovalute, smart contract, industria 4.0. Registri digitali, accordi giuridici e nuove tecnologie.* Pisa: Pacini Giuridica, 2019, p. 34

[35] A. Contaldo e F. Campara, cit., p.34

MB, superando il limite di 1 MB dei blocchi di Bitcoin.

Bitcoin Satoshi's Vision (BSV), o semplicemente Bitcoin SV, è nata nel 2018 da un fork di Bitcoin Cash da parte di Craig Wright, che propose di cambiare il modo di immagazzinare informazioni nella blockchain introducendo la scalabilità della dimensione dei blocchi. Bitcoin SV infatti prevede che la dimensione dei blocchi sia pari a 64 MB e che in sei mesi aumenti fino a 512 MB per arrivare a 2 GB entro un anno.

Capitolo 5

Introduzione a Litecoin

Figura 5.1: Logo di Litecoin

Litecoin (LTC) è un'altcoin creata nel 2011 da Charlie Lee (ex dipendente Google) a seguito di un *fork* della blockchain di Bitcoin, cioè un cambiamento del protocollo del network Bitcoin. «È una valuta digitale peer-to-peer che permette pagamenti istantanei quasi a zero costo a favore di un destinatario, ovunque esso si trovi. Litecoin è una rete di pagamenti globali, open source, pienamente decentralizzata e senza autorità centrale»[36]. È al settimo posto per capitalizzazione tra tutte le criptovalute ed è considerato l'argento digitale. Lo sviluppo di questa criptovaluta ha seguito Bitcoin, per cui le correzioni e i miglioramenti che sono stati fatti alla criptovaluta originaria sono stati adottati anche da Litecoin.

5.1 Caratteristiche

Totale di litecoin creabili Il numero di litecoin creabili sono 86 milioni, quattro volte il numero totale di bitcoin. La blockchain di Litecoin è progettata per sostenere un maggior numero di transazioni rispetto a Bitcoin, dato che ha una più frequente creazione di moneta e di blocchi, e il software è già predisposto senza bisogno di modifiche in futuro.

Tempo di conferma Il tempo di conferma dipende sempre dalla commissione aggiunta dal mittente, però si ha una maggiore velocità di conferma delle transazioni, perché è previsto un tempo inferiore per la generazione di un blocco pari a 2,5 minuti in media, un quarto del tempo impiegato da Bitcoin. Questo è sicuramente un vantaggio per tutti, soprattutto per i commercianti, che si vedono ridotto il tempo di accredito.

Difficoltà nel mining Siccome i blocchi vengono generati quattro volte più velocemente, la difficoltà del mining viene aumentata ogni 3,5 giorni, invece di due settimane come per Bitcoin, sempre ogni 2016 blocchi.

Creazione dei litecoin e ricompensa La ricompensa per il mining di un blocco inizialmente era di 50 litecoin e anche in questa criptovaluta è presente il fenomeno dell'halving: i litecoin subiscono un dimezzamento nella loro creazione, cioè della ricompensa data ai minatori, ogni 840.000 blocchi, un numero di blocchi quattro volte maggiore rispetto a Bitcoin.

[36] https://litecoin.org/it/

Inflazione Anche Litecoin è caratterizzato dal fenomeno dell'inflazione, con un andamento decrescente a gradini a causa degli halving per poi, una volta raggiunto il limite massimo di 86 milioni, diventare un fenomeno deflazionistico. Siccome l'offerta di litecoin è quattro volte maggiore rispetto a quella dei bitcoin l'inflazione è più alta e, in teoria, la capitalizzazione di mercato di questa criptovaluta, e quindi il suo potere di acquisto, sarà più alta nel futuro rispetto a Bitcoin.

5.2 L'algoritmo di hash scrypt

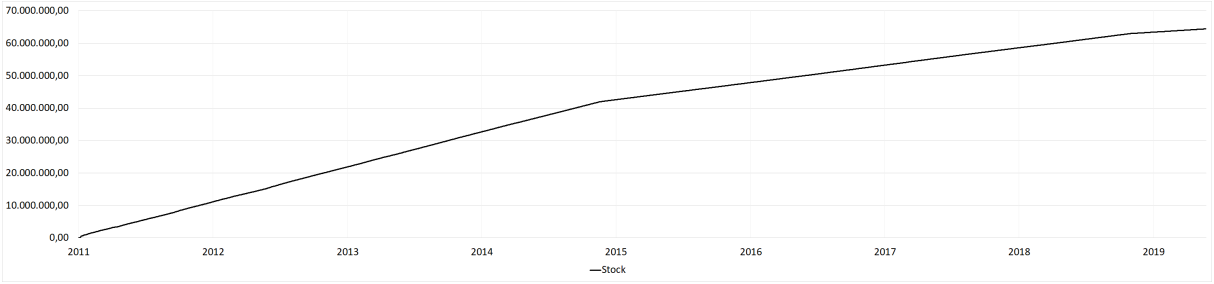
Litecoin usa l'algoritmo di hash "scrypt" (ess crypt) come Proof-of-Work per il mining, una funzione di hash che, quando viene calcolata, richiede un grande quantitativo di memoria e ne richiede altrettanta per essere verificata, in misura maggiore rispetto allo SHA-256 di Bitcoin. Ciò rende la creazione di Litecoin più difficile e costosa. L'algoritmo Scrypt riempie di rumore, cioè inserisce numeri generati casualmente all'interno del messaggio.

Il mining All'inizio svolgere i calcoli per il mining di qualsiasi criptovaluta che adottava questo sistema era possibile anche da computer generici, perché la difficoltà era molto bassa, utilizzando la CPU (Central Processing Unit) cioè il processore del computer, l'unità centrale di elaborazione del calcolatore. Al livello corrente di difficoltà del mining, il processo tramite la CPU non è sufficiente. Così, si è iniziato a usare le GPU, cioè le unità di elaborazione grafica, come il coprocessore della CPU oppure le schede grafiche dedicate. Le GPU vengono utilizzate in parallelo con la CPU e ciò permette di aumentare l'hashrate e quindi risolvere i blocchi più velocemente.
Fu scelto scrypt perché il mining di bitcoin era basato sulla GPU, perché usare solo la CPU era ormai inutile e l'intenzione era quella di permettere di minare ancora tramite la CPU su Litecoin. Purtroppo non si è riusciti nell'intento, per via del puzzle crittografico più difficile da implementare nell'hardware o semplicemente perché il tasso di cambio era troppo basso per incentivare gli utenti a partecipare. Questo portò ad un fallimento dell'obiettivo originario di avere un sistema più decentralizzato di miners che usavano la CPU.

5.3 Stock-to-Flow

Anche nel caso di Litecoin è previsto un dimezzamento della ricompensa data ai minatori, e quindi anche delle monete prodotte.

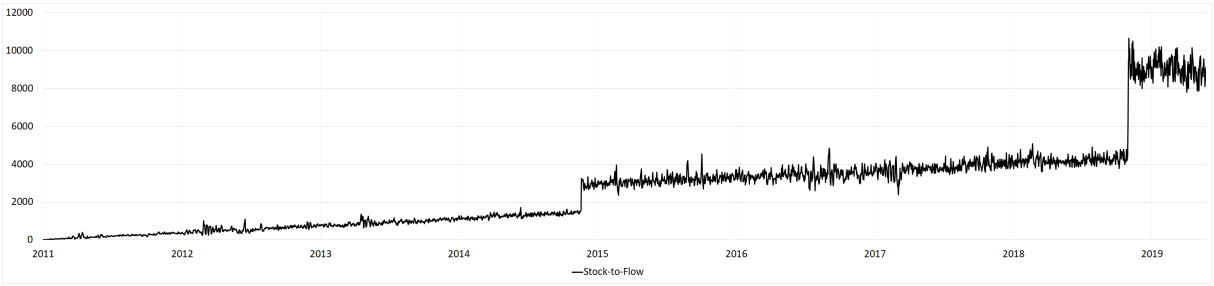
Figura 5.2: Totale litecoin prodotti



Fonte dati: https://coinmetrics.io/data-downloads-2/

In Figura 5.2 è rappresentato il totale dei litecoin prodotti. Ha un andamento crescente, con un incremento marginale decrescente, visibile dal fatto che ogni quattro anni circa si verifica l'halving in cui la ricompensa per i miners, perciò la creazione di nuova moneta, si dimezza.

Figura 5.3: Stock-to-Flow dei litecoin, con *flow* giornaliero



Fonte dati: https://coinmetrics.io/data-downloads-2/

In Figura 5.3 è rappresentato lo Stock-to-Flow di Litecoin, calcolato con la formula vista a pagina 42. Il *flow* è stato calcolato facendo la differenza tra lo stock giornaliero e il suo valore nel giorno precedente.
All'8 maggio 2020, dopo aver calcolato il *flow* prodotto durante l'ultimo anno, lo Stock-to-Flow annuo è pari a:

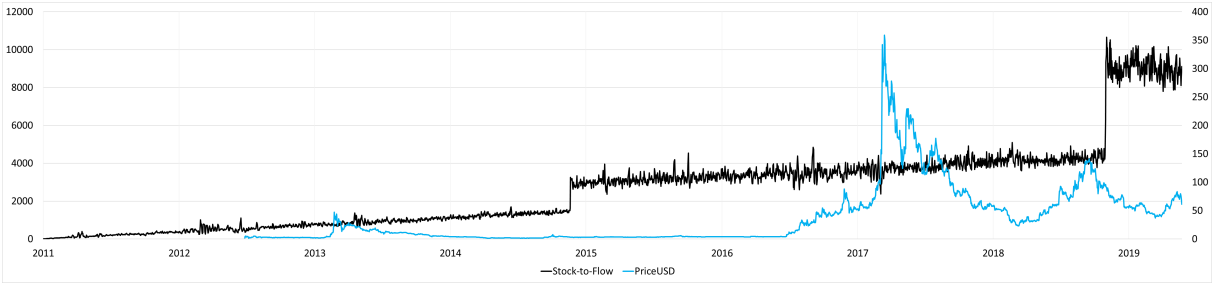
$$\frac{64.970.645}{3.275.174} = 19,83731093 \text{ anni}$$

L'8 maggio 2020, con 64.970.645 litecoin già creati e con una produzione annua di 3.275.174 litecoin, sono necessari circa 20 anni, al ritmo di produzione attuale, per raggiungere il numero di litecoin creati finora. Siccome la ricompensa dei litecoin si riduce della metà ogni circa quattro anni anche il flusso di nuovi litecoin per anno diminuirà, mentre lo *stock* sale e quindi l'indice aumenta più del doppio, come nel caso dei bitcoin.

5.3.1 Modello di regressione lineare

L'idea è quella di creare un modello Stock-to-Flow applicato a Litecoin ipotizzando che, anche nel caso di questa criptovaluta, la scarsità guidi il valore e quindi calcolare una retta di regressione lineare che preveda l'andamento del prezzo di Litecoin in base allo Stock-to-Flow.
Da Coinmetrics.io sono stati scaricati i dati giornalieri dal 07/10/2011 all'08/05/2020 riguardanti il totale dei litecoin prodotti, il loro prezzo e la loro capitalizzazione di mercato in dollari americani. Dopo aver calcolato il flow giornaliero facendo la differenza giornaliera tra i valori dello stock, è stato calcolato l'indice Stock-to-Flow su base giornaliera.

Figura 5.4: Stock-to-Flow e prezzo in dollari americani di Litecoin



Fonte dati: https://coinmetrics.io/data-downloads-2/

In Figura 5.4 è possibile vedere nello stesso grafico lo Stock-to-Flow e il prezzo di Litecoin. Si può notare che, due anni dopo il primo halving, il prezzo è aumentato per poi diminuire seguendo l'andamento del prezzo di Bitcoin ed è accaduto anche prima del secondo halving in misura però minore, infatti il prezzo non è aumentato di molto.

Per calcolare la regressione, sia lo Stock-to-Flow che la capitalizzazione di mercato sono stati trasformati mediante logaritmo naturale e i dati sono stati considerati a partire dall'01/04/2013, corrispondente alla prima data in cui si è formato il prezzo di un litecoin. Usando Excel per calcolare la regressione, si è ottenuto il seguente risultato:

Tabella 5.1: Dati della regressione sullo SF di Litecoin e il suo valore di mercato

Statistica della regressione	
R multiplo	0,70792437
R al quadrato	0,501156914
R al quadrato corretto	0,500964533
Errore standard	1,238250572
Osservazioni	2595

ANALISI VARIANZA			
	Regressione	Residuo	Totale
gdl	1	2593	2594
SQ	3994,195887	3975,754792	7969,950679
MQ	3994,195887	1,533264478	
F	2605,027341		
Significatività F	0		

	Intercetta	Variabile X 1
Coefficienti	7,578113212	1,609937009
Errore standard	0,248484891	0,031542981
Stat t	30,49727967	51,03946847
Valore di significatività	7,8166E-175	0
Inferiore 95%	7,090864338	1,54808503
Superiore 95%	8,065362086	1,671788988
Inferiore 95,0%	7,090864338	1,54808503
Superiore 95,0%	8,065362086	1,671788988

I risultati forniti dalla regressione mostrano un indice di determinazione r^2, che misura la bontà dell'adattamento della retta ai punti osservati, pari al 50,12%. Non c'è una relazione forte tra Stock-to-Flow e il valore di mercato come quella del modello originale applicato a Bitcoin.

Il modello consta di una funzione di regressione lineare pari a:

$$\ln(capmercato) = 1,609937009 \ln(SF) + 7,578113212$$

che può essere scritta anche come:

$$capmercato = SF^{1,609937009} \times e^{7,578113212}$$

Figura 5.5: Retta di regressione e punti osservati, in un grafico a dispersione, in scala logaritmica

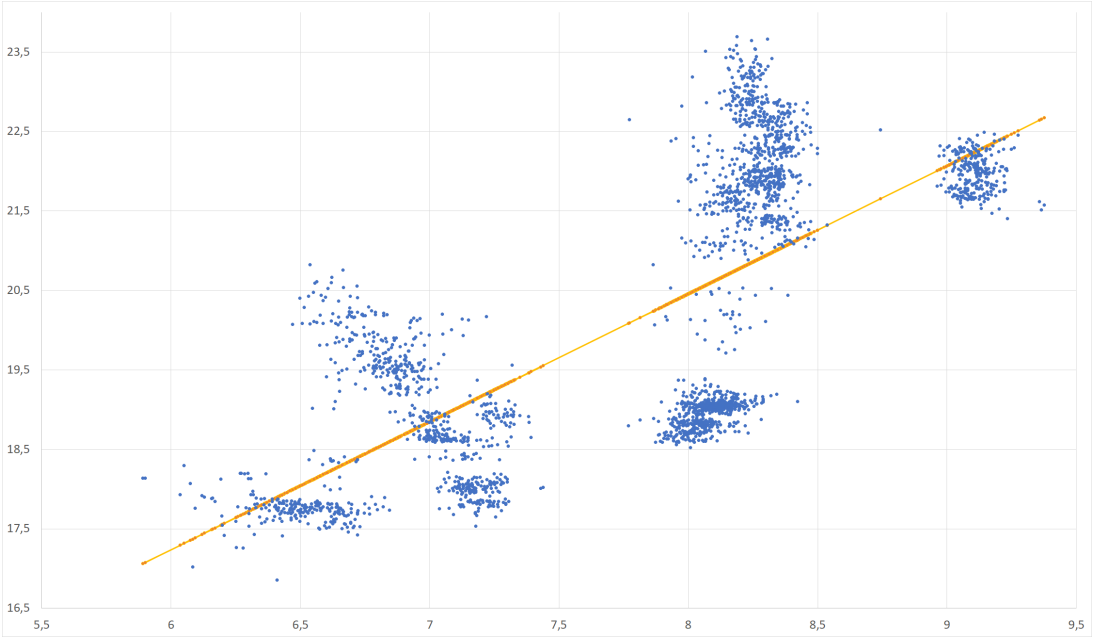
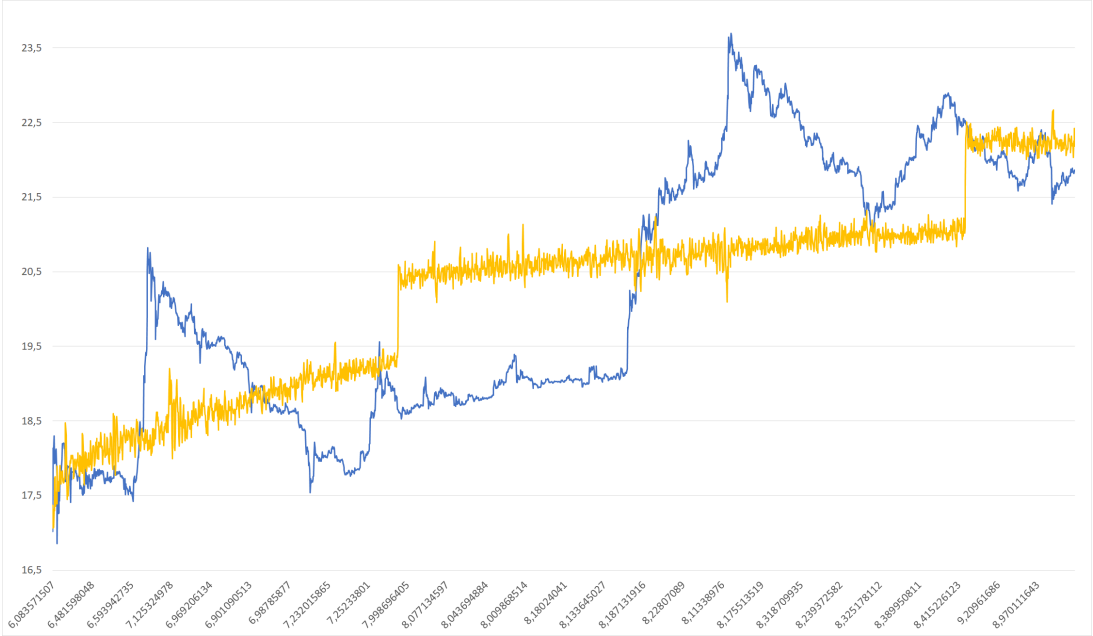


Figura 5.6: Retta di regressione e punti osservati, in un grafico a linee, in scala logaritmica



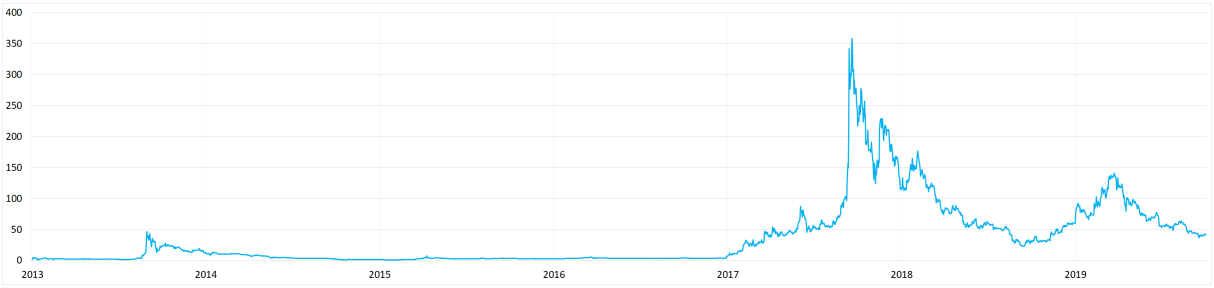
Nelle Figure 5.5 e 5.6, l'asse delle ascisse corrisponde ai valori dello Stock-to-Flow mentre l'asse delle ordinate alla capitalizzazione di mercato di Litecoin in dollari americani. In entrambi i grafici tutti i valori sono in scala logaritmica. Nella Figura 5.5 è possibile osservare la retta di regressione, in giallo, che corrisponde al valore di mercato stimato di Litecoin in dollari americani, per ogni valore dello Stock-to-Flow di Litecoin. Intorno alla retta, i punti in blu invece corrispondono alle osservazioni reali del valore di mercato. Nella Figura 5.6 i dati previsti e quelli osservati sono invece rappresentati in un grafico a linee.

5.3.2 Coefficiente di correlazione lineare di Bravais

Anche nel caso di Litecoin è stato calcolato il coefficiente di correlazione lineare di Bravais per capire se le variabili Stock-to-Flow e valore di mercato in dollari americani dei litecoin, entrambi espressi in scala logaritmica, abbiano una correlazione tra di loro. r è risultato pari a 70,79%.
L'indice si avvicina al 100% e quindi le due variabili sono positivamente correlate. L'indice di correlazione è minore rispetto al coefficiente di correlazione di Bitcoin, quindi il prezzo di Litecoin sembra essere meno influenzato dalla scarsità di moneta, rispetto a quanto si era visto con Bitcoin.

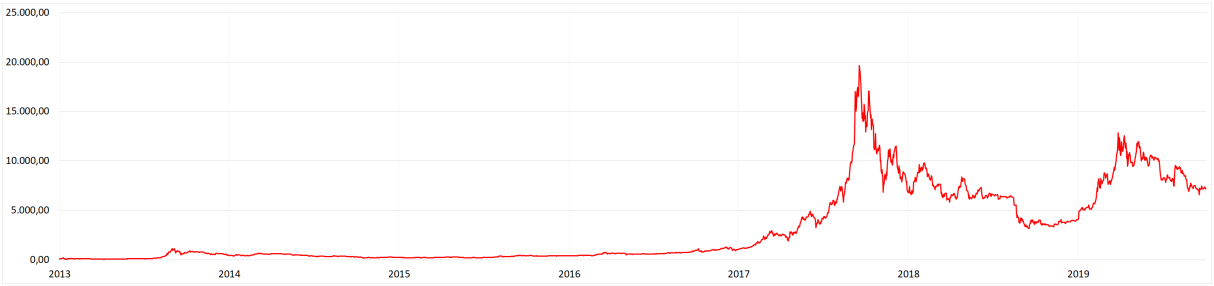
5.4 Relazione con il prezzo di Bitcoin?

Figura 5.7: Prezzo di un litecoin in dollari americani, dal 2013



Fonte dati: https://coinmetrics.io/data-downloads-2/

Figura 5.8: Prezzo di un bitcoin in dollari americani, dal 2013



Fonte dati: https://coinmetrics.io/data-downloads-2/

In Figura 5.7 è rappresentato il prezzo in dollari americani dei litecoin dal 2013, mentre in Figura 5.8 è rappresentato il prezzo in dollari americani dei bitcoin dal 2013.
È possibile notare, confrontando le due Figure, che i prezzi in dollari delle due criptovalute variano contemporaneamente nella stessa direzione pur avendo valori molto diversi. Siccome i prezzi si muovono insieme, l'idea è che ci sia una relazione tra i due prezzi, cioè che il prezzo di Litecoin dipenda da quello di Bitcoin.

5.4.1 Coefficiente di correlazione lineare di Bravais

Per verificare se ci sia una correlazione è stato calcolato il coefficiente di correlazione lineare di Bravais per capire se i prezzi dei litecoin e dei bitcoin, entrambi espressi in scala logaritmica con base naturale, abbiano una correlazione tra di loro. r è risultato pari a 94,09% la qual cosa indica una evidente correlazione tra i prezzi delle due criptovalute.

5.4.2 Regressione lineare

Alla luce di questa relazione tra i due prezzi è stato elaborato un modello di regressione lineare che descrive la dipendenza dei prezzi, con lo scopo di prevedere il prezzo dei litecoin nel futuro prossimo, sulla base del prezzo dei bitcoin.
Da Coinmetrics.io sono stati scaricati i dati giornalieri del prezzo in dollari americani di Bitcoin a partire dal 03/01/2009 e di Litecoin dal 07/10/2011, entrambi fino all'08/05/2020. Per calcolare la regressione, i valori dei prezzi di entrambe le criptovalute sono stati trasformati usando il logaritmo naturale e i dati sono stati considerati a partire dall'01/04/2013, perché è la prima data in cui si è formato un prezzo di un litecoin, pari a 1,52 dollari americani circa, mentre il prezzo dei bitcoin si era già formato prima.
Usando Excel per calcolare la regressione, si è ottenuto il seguente risultato:

Tabella 5.2: Dati della regressione sui prezzi di Bitcoin e Litecoin

Statistica della regressione	
R multiplo	0,940898039
R al quadrato	0,88528912
R al quadrato corretto	0,885244881
Errore standard	0,511038506
Osservazioni	2595

ANALISI VARIANZA			
	Regressione	Residuo	Totale
gdl	1	2593	2594
SQ	5226,251221	677,1888002	5903,440021
MQ	5226,251221	0,261160355	
F	20011,65615		
Significatività F	0		

	Intercetta	Variabile X 1
Coefficienti	-4,083362695	0,937835083
Errore standard	0,048406201	0,006629564
Stat t	-84,35619035	141,4625609
Valore di significatività	0	0
Inferiore 95%	-4,178281412	0,924835309
Superiore 95%	-3,988443979	0,950834858
Inferiore 95,0%	-4,178281412	0,924835309
Superiore 95,0%	-3,988443979	0,950834858

Come si può notare dai dati della regressione nella Tabella 5.2, r^2 è pari all'88,52%, indice del fatto che il modello è abbastanza rappresentativo dei dati.
Il modello consta di una funzione di regressione lineare pari a:

$$\ln(LTC) = 0,937609919 \ln(BTC) - 4,082009059$$

che può essere scritta anche come:

$$LTC = BTC^{0,937609919} \times e^{-4,082009059}$$

Figura 5.9: Retta di regressione e punti osservati, in un grafico a dispersione, in scala logaritmica

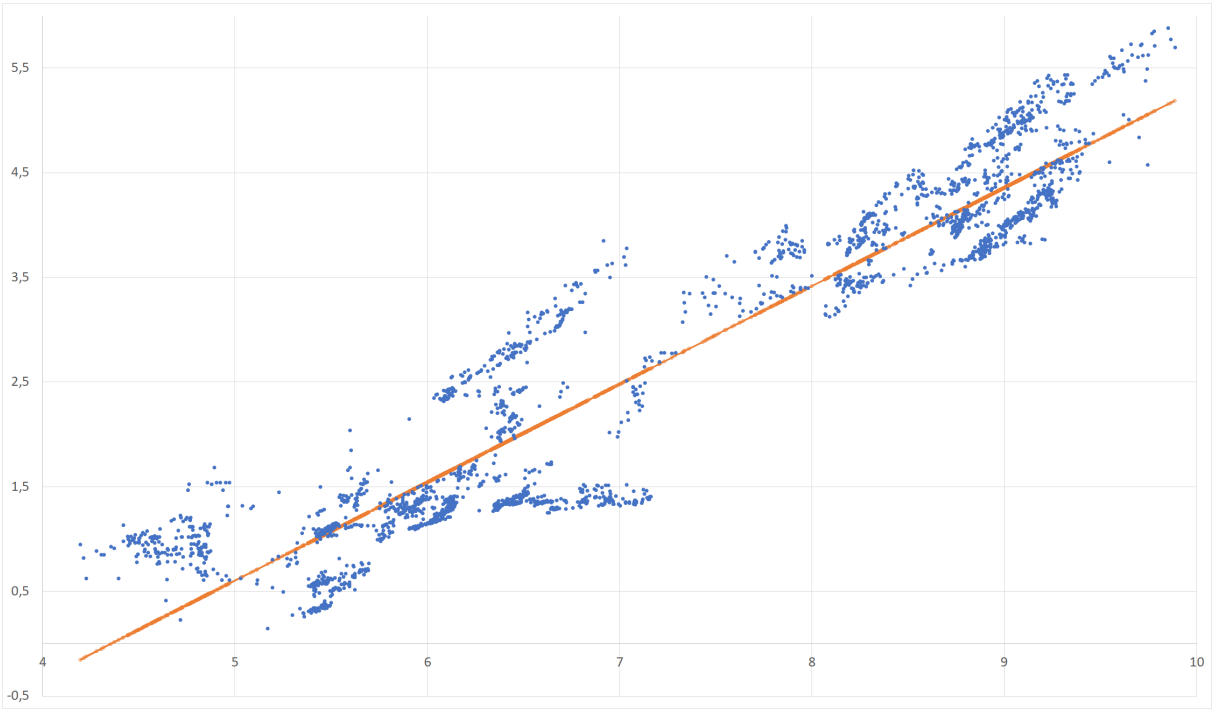


Figura 5.10: Retta di regressione e punti osservati, in un grafico a linee, in scala logaritmica

Nelle Figure 5.9 e 5.10 l'asse delle ascisse corrisponde al prezzo di Bitcoin mentre l'asse delle ordinate al prezzo di Litecoin. In entrambi i grafici tutti i valori sono in scala logaritmica. Nella Figura 5.9 è possibile osservare la retta di regressione, in arancione, che corrisponde al prezzo stimato di Litecoin in dollari americani per ogni valore del prezzo di Bitcoin. Intorno alla retta, i punti in blu invece corrispondono alle osservazioni reali del prezzo di Litecoin. Nella Figura 5.10 i dati previsti e quelli osservati sono invece rappresentati in un grafico a linee.
Dai risultati dell'analisi dei dati sembra che il prezzo di Bitcoin preveda il prezzo di Litecoin, dato che sono positivamente correlati fra loro. Quindi, nonostante i prezzi di Litecoin siano notevolmente inferiori rispetto a quelli di Bitcoin, se il prezzo di Bitcoin varia, il prezzo di Litecoin ne seguirà in modo simile l'andamento.

Capitolo 6

Confronto mediante Rete Neurale

Tra alcuni trader c'è la convinzione che l'andamento di Litecoin anticipi l'andamento di Bitcoin. Per verificare se ciò possa essere vero è stata calcolata una rete neurale, cioè una tecnica di machine learning, «branca dell'Intelligenza Artificiale che si occupa dello sviluppo di algoritmi e tecniche finalizzate all'apprendimento automatico mediante la statistica computazionale e l'ottimizzazione matematica»[37]. Una rete neurale è un modello di previsione che riproduce artificialmente un sistema ispirandosi al cervello umano e al suo funzionamento. La rete neurale è solitamente composta da una serie di nodi di elaborazione che costituiscono i neuroni collegati tra loro da relazioni, cioè le sinapsi. Sono modelli che operano in modo più flessibile rispetto agli algoritmi, che invece sono più rigidi, e sono in grado di adattarsi più efficacemente ad esempio per descrivere serie di dati che presentano grande varietà e volatilità.

6.1 Fasi nella creazione di una rete neurale supervisionata

La prima fase nella creazione di una rete neurale supervisionata consiste nella fase di **apprendimento**, in cui la rete neurale viene addestrata. La creazione parte dall'analizzare una serie di input e output già noti a priori e impostare i neuroni, assegnandogli dei numeri, cioè dei pesi (chiamati synaptic weight, cioè peso sinaptico). La rete, a partire dagli input e attraverso i neuroni, prova a generare un output e verifica poi quanto il risultato finale sia distante rispetto a quello reale. Mano a mano che fa questa verifica, corregge i pesi assegnati ai neuroni, minimizzando l'errore, finché non trova dei valori che permettono di ottenere risultati più fedeli agli originali, a partire dagli input. È il cosiddetto algoritmo di retropropagazione (**backpropagation**) dell'errore che consente alla rete di modificare i pesi in base all'errore ottenuto per avere un risultato più fedele a quello reale, così da ridurre al minimo l'errore stesso. La seconda fase è la **verifica** che consiste nel testare la rete neurale con alcuni dati nuovi in input per verificarne l'accuratezza nel predire l'output. L'ultima fase consiste nell'**implementazione** della rete neurale in un sistema esistente, per esempio in un'applicazione di uno smartphone.

6.2 Rete neurale per Litecoin e Bitcoin

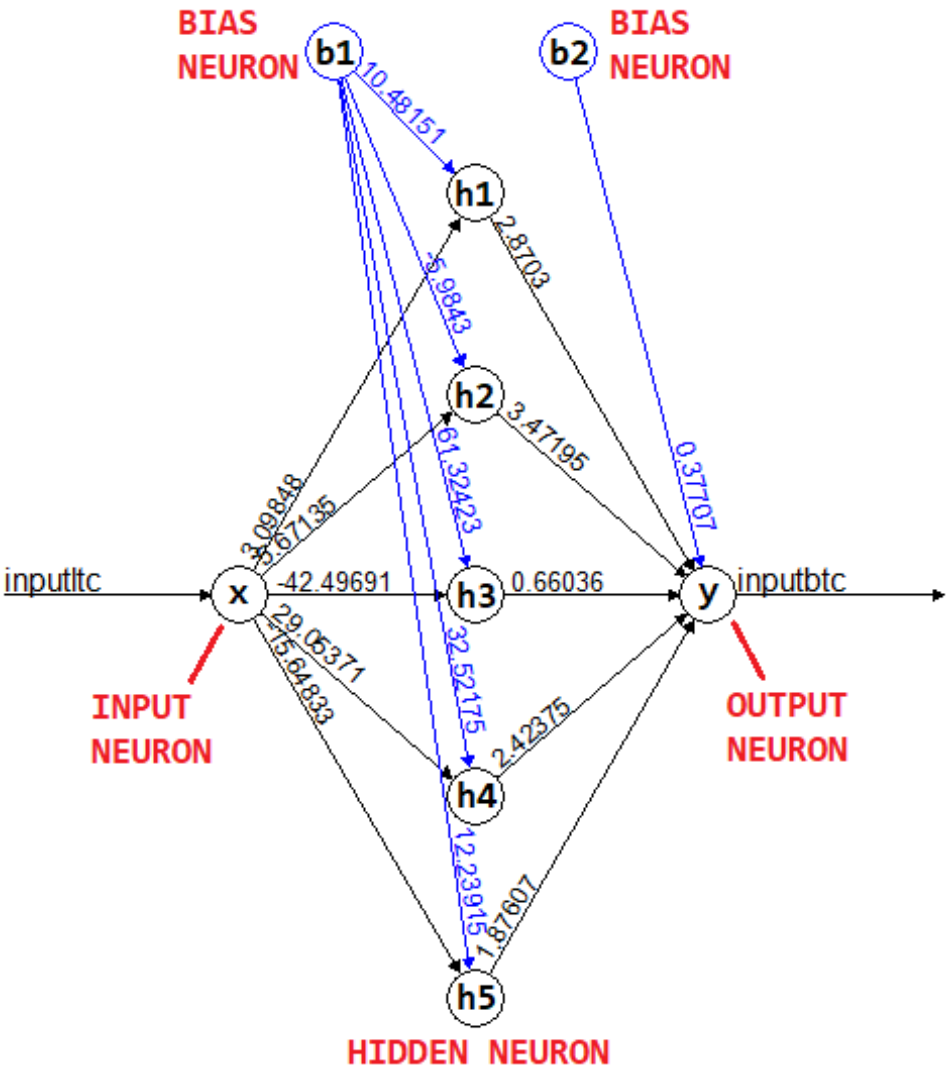
La rete neurale è stata creata con il software R, con la libreria R "neuralnet".
Da Coinmetrics.io sono stati scaricati i dati dei prezzi di Bitcoin e Litecoin in scala logaritmica dall'01/04/2013 al 04/06/2020. Per la fase di apprendimento sono stati utilizzati, in dollari americani e in scala logaritmica, il prezzo di Litecoin dal'01/04/2013

[37] http://www.treccani.it/vocabolario/machine-learning_%28Neologismi%29/

al 14/05/2020 e il prezzo di Bitcoin dall'08/04/2013 al 21/05/2020. I dati di Bitcoin sono stati fatti partire una settimana dopo quelli di Litecoin. Lo scopo è verificare se, attraverso la rete neurale, si possa prevedere il prezzo di Bitcoin a partire dai prezzi di Litecoin di una settimana prima. È stata creata una rete neurale **multistrato** di tipo **feed-forward** (flusso in avanti), una rete neurale in cui i neuroni sono organizzati in tre strati: strato di ingresso (input), strato nascosto (hidden) e strato d'uscita (output). La rete neurale feed-forward è caratterizzata dal fatto che le connessioni tra i neuroni non formano un ciclo ricorrente, perché le informazioni si muovono tra i neuroni dei vari strati in una sola direzione, rispetto allo strato di ingresso della rete.
L'algoritmo utilizzato per istruire la rete neurale è il "resilient back propagation with weight backtracking"[38], un algoritmo di apprendimento adattivo per reti multi-strato feed-forward inventato nel 1992 da Martin Riedmiller e Heinrich Brau.
La rete utilizza la tecnica della retropropagazione (backpropagation) dell'errore e per la creazione della rete è stato impostato un valore minimo di errore accettabile (threshold) pari a 0,01.

[38]Riedmiller M. e Braun H. *A direct adaptive method for faster backpropagation learning: the RPROP algorithm. IEEE International Conference on Neural Networks, San Francisco, CA, USA*. vol. 1, pp. 586-591. 1993.

Figura 6.1: Rappresentazione della rete neurale (settimana successiva)



Nella Figura 6.1 è possibile vedere la rappresentazione della rete neurale appena calcolata. Sono presenti in tutto sette neuroni: un neurone nello strato di ingresso (input), cinque neuroni nello strato nascosto (hidden), un neurone nello strato di uscita (output) e due neuroni bias.

Il segnale in input passa attraverso il neurone di input e viene moltiplicato per ogni coefficiente (indicato sopra ogni retta nera che parte dall'input neuron) e viene aggiunta una costante, rappresentata da ogni numero in blu sopra ogni retta dal primo bias neuron (il primo nodo blu da sinistra).

Ogni risultato passa ad ognuno dei cinque hidden neuron (neuroni nello strato nascosto), dove in ognuno di essi gli viene applicata la funzione di attivazione.

Ogni risultato ottenuto dalla funzione di attivazione per ogni neurone dello strato intermedio viene moltiplicato per ciascun coefficiente (cioè ogni numero indicato sopra le rette che partono dagli hidden neuron). Tutti gli output dei neuroni vengono sommati fra loro e il risultato viene sommato ad una costante, rappresentata dal numero in blu che proviene

dal secondo nodo bias (il secondo nodo blu da sinistra). Il risultato finale passa attraverso l'output neuron da cui fuoriesce l'output finale.

6.2.1 Esempio dei calcoli svolti dalla rete neurale

L'obiettivo è trovare il valore del prezzo di Bitcoin in scala logaritmica partendo dal prezzo di Litecoin in scala logaritmica, sulla base dell'apprendimento fatto dalla rete in precedenza. Il valore del prezzo di Litecoin in scala logaritmica inserito nella rete è pari a: $x = 3,754778$.

wi = pesi dal neurone di input, wj = pesi dai neuroni hidden (dello strato nascosto)
b1i = valore del primo neurone bias per ogni neurone hidden i, b2 = valore del secondo neurone bias

Prima di tutto, il valore in x viene moltiplicato per ciascun coefficiente wi ed ogni risultato viene sommato/sottratto ad ogni costante proveniente dal primo nodo bias da sinistra. Ogni risultato è il valore di input per ogni neurone hidden.

$hi = x \times wi - b1i$
$h1 = 3,754778 \times 3,09848 - 10,48151$
$h2 = 3,754778 \times 5,67135 - 5,98431$
$h3 = 3,754778 \times (-42,49691) + 61,32423$
etc...

I risultati dei calcoli svolti in precedenza vengono inseriti nella funzione di attivazione per ricavare l'output per ogni neurone hidden.

$$\text{Funzione di attivazione } = \frac{1}{1 + e^{-hi}}$$

$$outhi = \frac{1}{1 + e^{-hi}}$$

Poi, l'output di ciascun neurone viene moltiplicato per ciascun coefficiente wj e tutti i risultati vengono sommati fra loro. Alla somma viene aggiunto/sottratto il valore del secondo nodo bias giungendo così ad y, cioè il risultato finale.

$y = outh1 \times 2,87030 + outh2 \times 3,47195 + outh3 \times 0,66036 + outh4 \times 2,42375 + outh5 \times 1,87607 + 0,37707 = 8,45415$

Tabella 6.1: Esempio dei calcoli a partire da un valore x con la rete neurale

x	wi	x*wi	b1i	hi		outhi	wj	outhi*wj
3,75478	3,09848	11,63412	-10,48151	1,15261		0,75999	2,87030	2,18139
	5,67135	21,29466	-5,98431	15,31036	funzione di attivazione	1,00000	3,47195	3,47195
	-42,49691	-159,56646	61,32423	-98,24223		2,16E-43	0,66036	1,42E-43
	29,05371	109,09023	32,52175	141,61198		1,00000	2,42375	2,42375
	-15,64833	-58,75601	12,23915	-46,51686		6,28E-21	1,87607	1,18E-20
								8,07708

Σ(outhi*wj)	b2	y
8,07708	0,37707	8,45415

i=1,2,3,4,5 j=1,2,3,4,5

Nelle reti neurali i contributi degli output di ciascun neurone vengono sommati ed inviati alla "funzione di attivazione" di ogni neurone nello strato successivo.

Nota per le reti neurali con più di un neurone nello strato di input

Nel caso di 6.3 a pagina 75, il calcolo per trovare il valore in input per il primo hidden neuron (da sopra), che dopo verrà sottoposto alla funzione di attivazione, è il seguente:

$h1 = inputltc \times 12,42624 + lnSF \times 26,81496 - 192.1342$

6.3 Previsione dei prezzi di Bitcoin della settimana successiva

La fase di testing consiste nell'applicare la rete neurale sul prezzo di Litecoin in scala logaritmica dal 21/05/2020 al 28/05/2020 per provare a prevedere i prezzi di Bitcoin dal 28/05/2020 al 04/06/2020. È stato ottenuto il seguente risultato:

Tabella 6.2: Risultati della rete neurale (settimana successiva)

	Data Input	Input-ln(ltc)	Data output	Output rete neurale	ln(btc) reale
1	21/05/2020	3,7548	28/05/2020	8,4542	9,1662
2	22/05/2020	3,7884	29/05/2020	8,5072	9,1519
3	23/05/2020	3,7827	30/05/2020	8,4984	9,1790
4	24/05/2020	3,7479	31/05/2020	8,4429	9,1521
5	25/05/2020	3,7609	01/06/2020	8,4640	9,2301
6	26/05/2020	3,7441	02/06/2020	8,4367	9,1603
7	27/05/2020	3,7776	03/06/2020	8,4906	9,1739
8	28/05/2020	3,8006	04/06/2020	8,5257	9,1915

Nella Tabella 6.2 sono indicati rispettivamente per ogni colonna:

- un numero progressivo;
- la data dei valori in input;
- i valori in input (i prezzi di Litecoin dal 21/05/2020 al 28/05/2020 in dollari americani e in scala logaritmica);
- la data dei valori in output;
- l'output della rete neurale (cioè la previsione dei prezzi di Bitcoin dal 28/05/2020 al 04/06/2020 in dollari americani e in scala logaritmica);
- l'output reale, cioè i prezzi di Bitcoin (in dollari americani e in scala logaritmica) realmente registrati in quelle date.

I valori dei prezzi di Bitcoin calcolati dalla rete neurale si sono avvicinati ai valori reali di Bitcoin: in media, la differenza tra il prezzo reale e l'output della rete neurale, entrambi in scala logaritmica, è pari a 0,6982.
A parte i valori dal 28 al 30 maggio, dal 30 maggio al 04 giugno la rete ha previsto correttamente le variazioni in aumento e diminuzione del prezzo di Bitcoin, sulla base del prezzo di Litecoin osservato la settimana precedente. Comunque sembra che non ci siano abbastanza elementi per dire che si possa prevedere il prezzo di Bitcoin da quello di Litecoin, richiedendo l'analisi un'estensione ad una finestra temporale più ampia.

6.4 Previsione dei prezzi di Bitcoin del giorno successivo

Si è voluto addestrare la rete neurale per verificare se sia possibile prevedere il prezzo di Bitcoin, conoscendo il prezzo di Litecoin del giorno prima.
Per la fase di apprendimento sono stati utilizzati, in dollari americani e in scala logaritmica, il prezzo di Litecoin dall'01/04/2013 al 20/05/2020 e il prezzo di Bitcoin dal 02/04/2013 al 21/05/2020. Quindi, i dati di Bitcoin sono stati fatti partire un giorno dopo rispetto a quelli di Litecoin.
Nella Figura 6.2 è possibile vedere la rappresentazione della rete neurale appena calcolata. Come nella rete neurale precedente, sono presenti in tutto sette neuroni: un neurone nello strato di ingresso (input), cinque neuroni nello strato nascosto (hidden), un neurone nello strato di uscita (output) e due neuroni bias.
La fase di testing consiste nell'applicare la rete neurale sul prezzo di Litecoin in scala logaritmica dal 21/05/2020 al 17/06/2020 per provare a prevedere i prezzi di Bitcoin dal 22/05/2020 al 18/06/2020. È stato ottenuto il risultato nella Tabella 6.3.

Dai risultati in Tabella 6.3 i valori dei prezzi di Bitcoin calcolati dalla rete neurale, anche in questo caso, si sono avvicinati ai valori reali di Bitcoin: in media, la differenza tra il prezzo reale e l'output della rete neurale, entrambi in scala logaritmica, è pari a 0,5883.

Analizzando le variazioni dell'output della rete neurale da un giorno all'altro, la rete neurale ha previsto correttamente una variazione in aumento e in diminuzione in 6 casi su 27 (è stata esclusa la prima data) ed è un risultato non sufficiente a provare che il prezzo di Litecoin possa prevedere il prezzo di Bitcoin del giorno successivo.

Figura 6.2: Rappresentazione della rete neurale (giorno successivo)

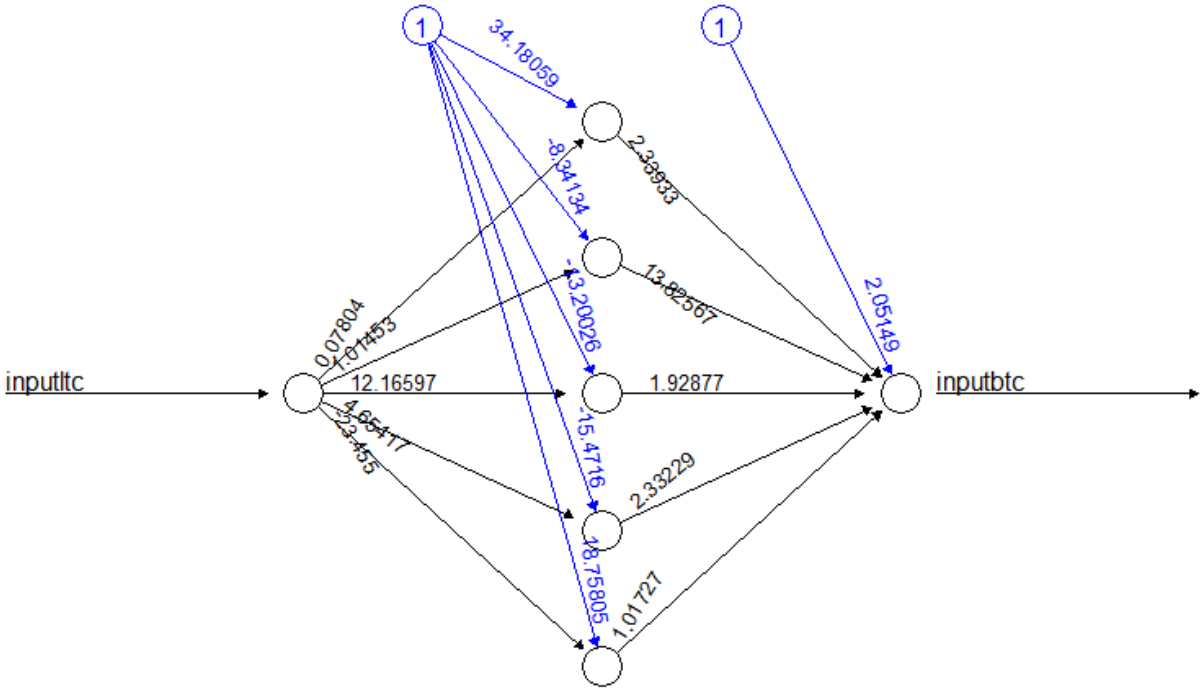


Tabella 6.3: Risultati della rete neurale (giorno successivo)

	Data Input	Input-ln(ltc)	Data output	Output rete neurale	ln(btc) reale
1	21/05/2020	3,7548	22/05/2020	8,5219	9,1662
2	22/05/2020	3,7884	23/05/2020	8,5630	9,1519
3	23/05/2020	3,7827	24/05/2020	8,5563	9,1790
4	24/05/2020	3,7479	25/05/2020	8,5130	9,1521
5	25/05/2020	3,7609	26/05/2020	8,5297	9,2301
6	26/05/2020	3,7441	27/05/2020	8,5080	9,1603
7	27/05/2020	3,7776	28/05/2020	8,5503	9,1739
8	28/05/2020	3,8006	29/05/2020	8,5768	9,1519
9	29/05/2020	3,7957	30/05/2020	8,5714	9,1790
10	30/05/2020	3,8642	31/05/2020	8,6413	9,1521
11	31/05/2020	3,8186	01/06/2020	8,5965	9,2301
12	01/06/2020	3,8797	02/06/2020	8,6552	9,1603
13	02/06/2020	3,8268	03/06/2020	8,6049	9,1739
14	03/06/2020	3,8520	04/06/2020	8,6299	9,1915
15	04/06/2020	3,8606	05/06/2020	8,6380	9,1739
16	05/06/2020	3,8484	06/06/2020	8,6264	9,1766
17	06/06/2020	3,8452	07/06/2020	8,6233	9,1848
18	07/06/2020	3,8420	08/06/2020	8,6203	9,1870
19	08/06/2020	3,8373	09/06/2020	8,6156	9,1880
20	09/06/2020	3,8278	10/06/2020	8,6060	9,1991
21	10/06/2020	3,8432	11/06/2020	8,6214	9,1353
22	11/06/2020	3,7674	12/06/2020	8,5378	9,1544
23	12/06/2020	3,7985	13/06/2020	8,5745	9,1550
24	13/06/2020	3,8081	14/06/2020	8,5851	9,1424
25	14/06/2020	3,7856	15/06/2020	8,5598	9,1529
26	15/06/2020	3,7803	16/06/2020	8,5534	9,1612
27	16/06/2020	3,7804	17/06/2020	8,5536	9,1536
28	17/06/2020	3,7841	18/06/2020	8,5580	9,1474

6.4.1 Aggiunta del parametro Stock-to-Flow

Per cercare di migliorare i risultati ottenuti, si è voluto addestrare la rete neurale per verificare se sia possibile prevedere il prezzo di Bitcoin conoscendo, oltre al prezzo di Litecoin, anche il valore dello Stock-to-Flow giornaliero di Litecoin.

Per la fase di apprendimento sono stati utilizzati gli stessi dati usati precedentemente

con, in aggiunta, il valore dello Stock-to-Flow giornaliero di Litecoin in scala logaritmica dall'01/04/2020 al 20/05/2020.

Dai risultati in Tabella 6.4, è possibile notare che, grazie all'aggiunta dello Stock-to-Flow, il risultato in output della rete neurale è più vicino a quello reale rispetto alla rete neurale addestrata in precedenza. Infatti, in media, la differenza tra il prezzo reale e l'output della rete neurale, entrambi in scala logaritmica, è pari a 0,2554, cioè quasi la metà rispetto alla stessa rete calcolata senza lo Stock-to-Flow. Quindi, l'aggiunta di questo nuovo parametro ha migliorato la precisione della rete nel prevedere il valore in output.
Analizzando invece le variazioni dell'output della rete neurale da un giorno all'altro, la rete neurale ha previsto correttamente una variazione in aumento e in diminuzione in 13 casi su 27 (è stata esclusa la prima data), un risultato migliore rispetto a quello di prima.

Figura 6.3: Rappresentazione della rete neurale con Stock-to-Flow (giorno successivo)

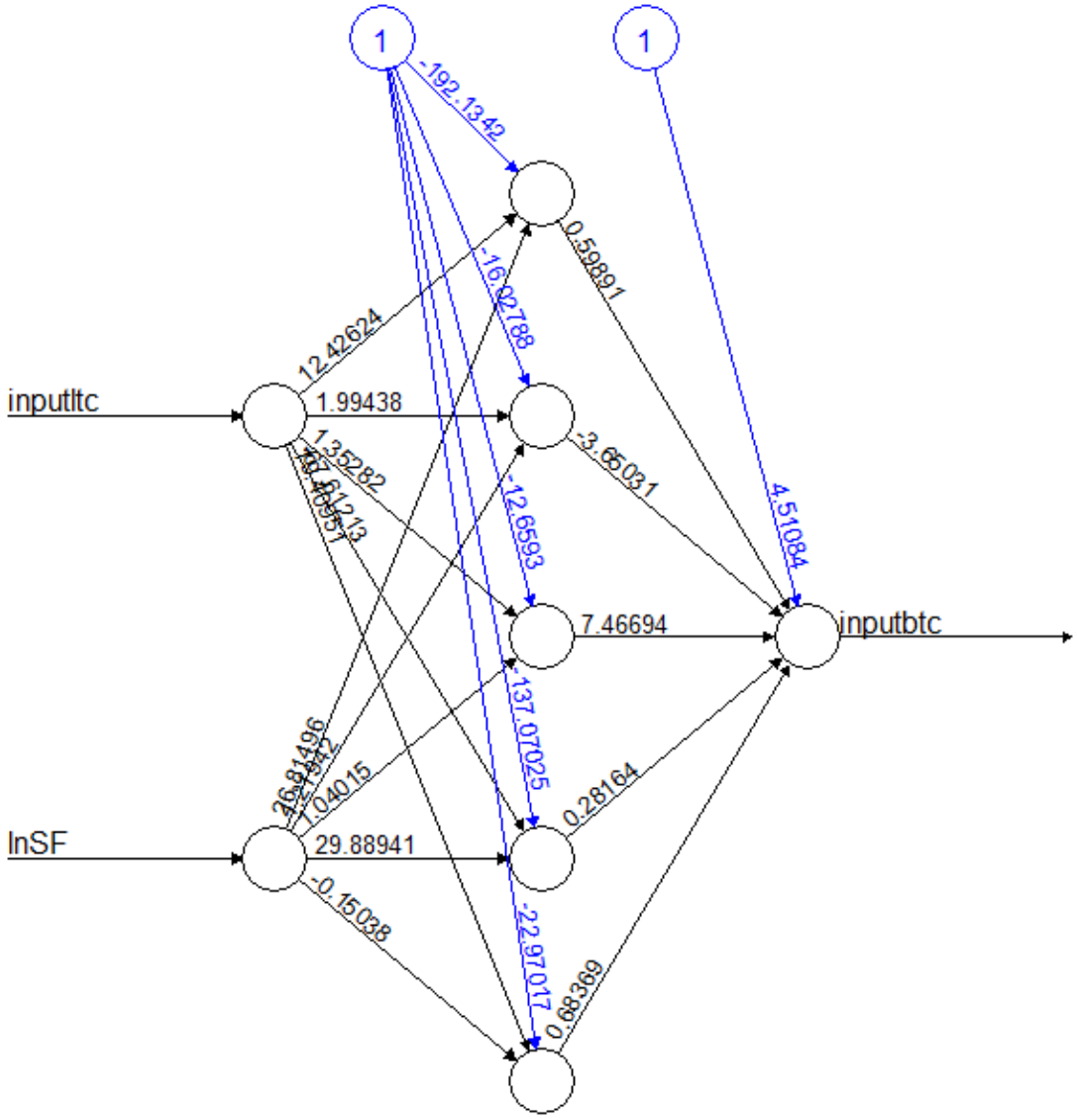


Tabella 6.4: Risultati della rete neurale, con Stock-to-Flow (giorno successivo)

	Data Input	Input-ln(ltc)	Input-ln(SF)	Data output	Output rete neurale	ln(btc) reale
1	21/05/2020	3,7548	9,0616	22/05/2020	8,8659	9,1662
2	22/05/2020	3,7884	8,9929	23/05/2020	8,8472	9,1519
3	23/05/2020	3,7827	8,9931	24/05/2020	8,8432	9,1790
4	24/05/2020	3,7479	9,0246	25/05/2020	8,8384	9,1521
5	25/05/2020	3,7609	9,0440	26/05/2020	8,8594	9,2301
6	26/05/2020	3,7441	8,9950	27/05/2020	8,8172	9,1603
7	27/05/2020	3,7776	9,0107	28/05/2020	8,8506	9,1739
8	28/05/2020	3,8006	8,9890	29/05/2020	8,8533	9,1519
9	29/05/2020	3,7957	9,0332	30/05/2020	8,8768	9,1790
10	30/05/2020	3,8642	9,0253	31/05/2020	8,9181	9,1521
11	31/05/2020	3,8186	9,0694	01/06/2020	8,9135	9,2301
12	01/06/2020	3,8797	9,0335	02/06/2020	8,9330	9,1603
13	02/06/2020	3,8268	9,1245	03/06/2020	8,9499	9,1739
14	03/06/2020	3,8520	9,1299	04/06/2020	8,9688	9,1915
15	04/06/2020	3,8606	9,1642	05/06/2020	8,9924	9,1739
16	05/06/2020	3,8484	9,2869	06/06/2020	9,0475	9,1766
17	06/06/2020	3,8452	9,0389	07/06/2020	8,9134	9,1848
18	07/06/2020	3,8420	9,0819	08/06/2020	8,9359	9,1870
19	08/06/2020	3,8373	9,1059	09/06/2020	8,9463	9,1880
20	09/06/2020	3,8278	9,0906	10/06/2020	8,9316	9,1991
21	10/06/2020	3,8432	9,1908	11/06/2020	8,9959	9,1353
22	11/06/2020	3,7674	9,1686	12/06/2020	8,9367	9,1544
23	12/06/2020	3,7985	9,1835	13/06/2020	8,9645	9,1550
24	13/06/2020	3,8081	9,1345	14/06/2020	8,9436	9,1424
25	14/06/2020	3,7856	9,1031	15/06/2020	8,9112	9,1529
26	15/06/2020	3,7803	9,0811	16/06/2020	8,8948	9,1612
27	16/06/2020	3,7804	9,1068	17/06/2020	8,9099	9,1536
28	17/06/2020	3,7841	9,1822	18/06/2020	8,9548	9,1474

6.5 Previsione dei prezzi di Bitcoin del mese successivo

Si è voluto addestrare la rete neurale per verificare se sia possibile prevedere il prezzo di Bitcoin, conoscendo il prezzo di Litecoin del mese prima.
Per la fase di apprendimento sono stati utilizzati, in dollari americani e in scala logaritmica, il prezzo di Litecoin dal'01/04/2013 al 21/04/2020, e il prezzo di Bitcoin dall'01/05/2013 al 21/05/2020. Quindi, i dati di Bitcoin sono stati fatti partire un mese dopo rispetto a quelli di Litecoin.
La fase di testing consiste nell'applicare la rete neurale sul prezzo di Litecoin in scala logaritmica dal 18/04/2020 al 18/05/2020 per provare a prevedere i prezzi di Bitcoin dal 18/05/2020 al 17/06/2020. È stato ottenuto il risultato in Tabella 6.5.

In questo caso, in media, la differenza tra il prezzo reale e l'output della rete neurale, entrambi in scala logaritmica, è pari a 0,5945. Analizzando le variazioni dell'output della rete neurale da un giorno all'altro, la rete neurale ha previsto correttamente una variazione in aumento, o in diminuzione, in 14 casi su 30 (è stata esclusa la prima data).

Figura 6.4: Rappresentazione della rete neurale (mese successivo)

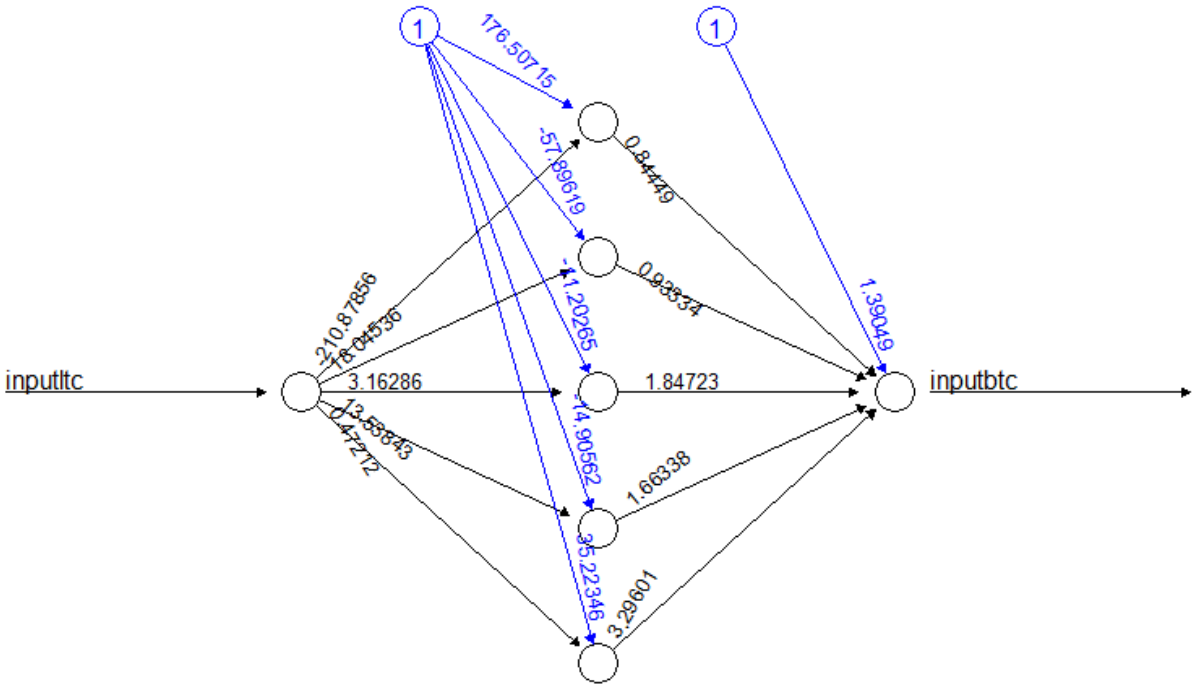


Tabella 6.5: Risultati della rete neurale (mese successivo)

	Data Input	Input-ln(ltc)	Data output	Output rete neurale	ln(btc) reale
1	18/04/2020	3,7882	18/05/2020	8,5493	9,1826
2	19/04/2020	3,7497	19/05/2020	8,4998	9,1855
3	20/04/2020	3,6995	20/05/2020	8,4322	9,1607
4	21/04/2020	3,7074	21/05/2020	8,4431	9,1126
5	22/04/2020	3,7340	22/05/2020	8,4789	9,1228
6	23/04/2020	3,7614	23/05/2020	8,5151	9,1252
7	24/04/2020	3,7957	24/05/2020	8,5588	9,0832
8	25/04/2020	3,7916	25/05/2020	8,5536	9,0948
9	26/04/2020	3,7972	26/05/2020	8,5607	9,0865
10	27/04/2020	3,7957	27/05/2020	8,5587	9,1236
11	28/04/2020	3,8248	28/05/2020	8,5945	9,1662
12	29/04/2020	3,8854	29/05/2020	8,6644	9,1519
13	30/04/2020	3,8387	30/05/2020	8,6110	9,1790
14	01/05/2020	3,8532	31/05/2020	8,6280	9,1521
15	02/05/2020	3,8968	01/06/2020	8,6768	9,2301
16	03/05/2020	3,8725	02/06/2020	8,6500	9,1603
17	04/05/2020	3,8501	03/06/2020	8,6244	9,1739
18	05/05/2020	3,8385	04/06/2020	8,6108	9,1915
19	06/05/2020	3,8256	05/06/2020	8,5954	9,1739
20	07/05/2020	3,8613	06/06/2020	8,6373	9,1766
21	08/05/2020	3,8704	07/06/2020	8,6476	9,1848
22	09/05/2020	3,8522	08/06/2020	8,6268	9,1870
23	10/05/2020	3,7380	09/06/2020	8,4844	9,1880
24	11/05/2020	3,7271	10/06/2020	8,4697	9,1991
25	12/05/2020	3,7426	11/06/2020	8,4904	9,1353
26	13/05/2020	3,7678	12/06/2020	8,5234	9,1544
27	14/05/2020	3,7849	13/06/2020	8,5452	9,1550
28	15/05/2020	3,7569	14/06/2020	8,5092	9,1424
29	16/05/2020	3,7682	15/06/2020	8,5239	9,1529
30	17/05/2020	3,7766	16/06/2020	8,5346	9,1612
31	18/05/2020	3,8135	17/06/2020	8,5808	9,1536

6.5.1 Aggiunta del parametro Stock-to-Flow

Anche in questo caso, per cercare di migliorare i risultati ottenuti, si è deciso di addestrare la rete neurale per verificare se sia possibile prevedere il prezzo di Bitcoin conoscendo, oltre al prezzo di Litecoin, anche il valore dello Stock-to-Flow di Litecoin del mese precedente. Per la fase di apprendimento sono stati utilizzati, gli stessi dati usati precedentemente con in aggiunta il valore dello Stock-to-Flow giornaliero di Litecoin in scala logaritmica dal 01/04/2013 al 21/04/2020.

Dai risultati in Tabella 6.6 è possibile notare che, grazie all'aggiunta dello Stock-to-Flow, il risultato in output della rete neurale è più vicino a quello reale, rispetto alle reti neurali addestrate in precedenza. Infatti, in media, la differenza tra il prezzo reale e l'output della rete neurale, entrambi in scala logaritmica, è pari a 0,19, molto più basso rispetto alla rete calcolata usando solamente il prezzo di Litecoin del mese precedente.
Analizzando le variazioni da un giorno all'altro dell'output della rete neurale, la rete ha previsto correttamente una variazione in aumento e in diminuzione in 14 casi su 30 (è stata esclusa la prima data), lo stesso risultato della rete calcolata in precedenza.

Figura 6.5: Rappresentazione della rete neurale con Stock-to-Flow (mese successivo)

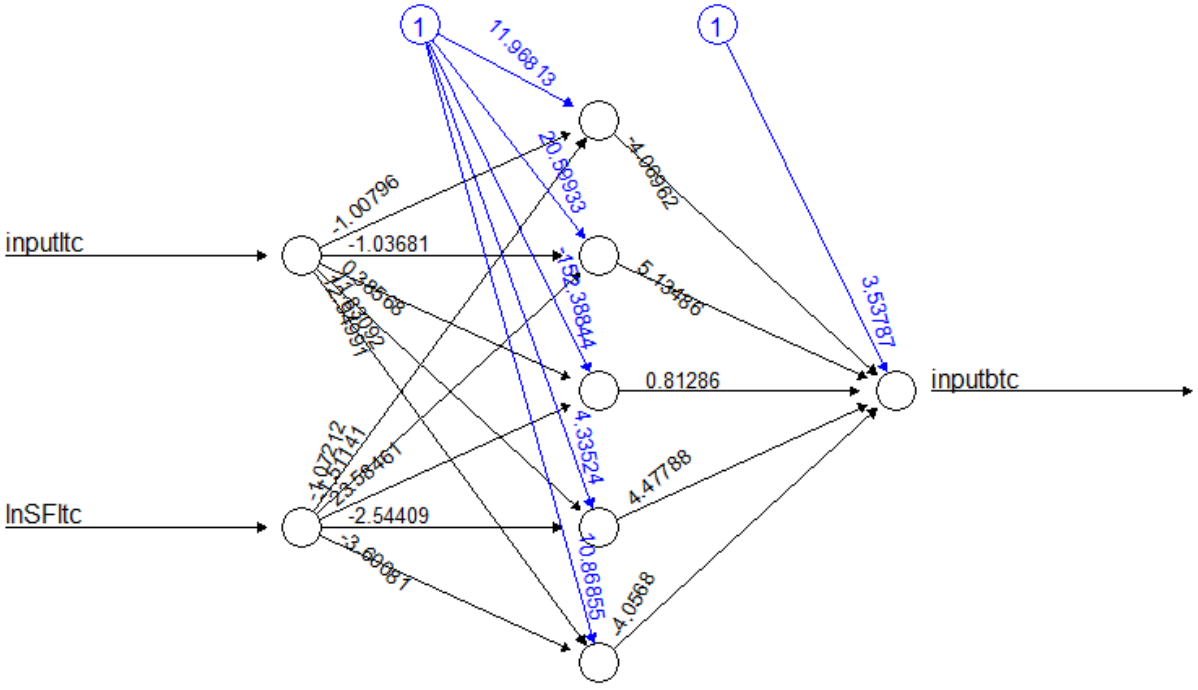


Tabella 6.6: Risultati della rete neurale, con Stock-to-Flow (mese successivo)

	Data Input	Input-ln(ltc)	Input-ln(SF)	Data output	Output rete neurale	ln(btc) reale
1	18/04/2020	3,7882	9,0189	18/05/2020	8,9418	9,1826
2	19/04/2020	3,7497	9,0531	19/05/2020	8,9378	9,1855
3	20/04/2020	3,6995	9,0417	20/05/2020	8,9146	9,1607
4	21/04/2020	3,7074	9,0616	21/05/2020	8,9244	9,1126
5	22/04/2020	3,7340	9,0955	22/05/2020	8,9444	9,1228
6	23/04/2020	3,7614	9,1705	23/05/2020	8,9701	9,1252
7	24/04/2020	3,7957	9,1148	24/05/2020	8,9690	9,0832
8	25/04/2020	3,7916	9,1361	25/05/2020	8,9721	9,0948
9	26/04/2020	3,7972	9,1132	26/05/2020	8,9691	9,0865
10	27/04/2020	3,7957	9,0706	27/05/2020	8,9588	9,1236
11	28/04/2020	3,8248	9,0169	28/05/2020	8,9544	9,1662
12	29/04/2020	3,8854	9,0792	29/05/2020	8,9874	9,1519
13	30/04/2020	3,8387	9,1547	30/05/2020	8,9874	9,1790
14	01/05/2020	3,8532	9,0744	31/05/2020	8,9775	9,1521
15	02/05/2020	3,8968	9,0880	01/06/2020	8,9918	9,2301
16	03/05/2020	3,8725	9,0813	02/06/2020	8,9843	9,1603
17	04/05/2020	3,8501	9,0968	03/06/2020	8,9810	9,1739
18	05/05/2020	3,8385	8,9772	04/06/2020	8,9478	9,1915
19	06/05/2020	3,8256	9,1144	05/06/2020	8,9775	9,1739
20	07/05/2020	3,8613	9,0700	06/06/2020	8,9789	9,1766
21	08/05/2020	3,8704	9,2215	07/06/2020	8,9999	9,1848
22	09/05/2020	3,8522	9,0636	08/06/2020	8,9749	9,1870
23	10/05/2020	3,7380	9,1166	09/06/2020	8,9513	9,1880
24	11/05/2020	3,7271	9,1397	10/06/2020	8,9534	9,1991
25	12/05/2020	3,7426	9,1327	11/06/2020	8,9567	9,1353
26	13/05/2020	3,7678	9,1435	12/06/2020	8,9667	9,1544
27	14/05/2020	3,7849	9,0331	13/06/2020	8,9448	9,1550
28	15/05/2020	3,7569	9,0726	14/06/2020	8,9461	9,1424
29	16/05/2020	3,7682	9,0430	15/06/2020	8,9416	9,1529
30	17/05/2020	3,7766	9,0111	16/06/2020	8,9349	9,1612
31	18/05/2020	3,8135	9,1513	17/06/2020	8,9807	9,1536

6.6 Previsione della capitalizzazione di mercato di Bitcoin del mese successivo

Per migliorare ancora di più i risultati si è voluto creare una nuova rete neurale, cambiando alcuni dati in input e aggiungendone di nuovi, ma questa volta per cercare di prevedere la capitalizzazione di mercato di Bitcoin del mese successivo.
Gli input, dall'01/04/2013 fino al 21/04/2020 e in scala logaritmica, sono:

- Capitalizzazione di mercato di Litecoin, in dollari americani;
- Stock-to-Flow di Litecoin;
- Capitalizzazione di mercato di Bitcoin, in dollari americani;
- Stock-to-Flow di Bitcoin.

Sempre per l'addestramento, per il valore a cui la rete fa riferimento per il futuro output che produrrà, c'è la capitalizzazione di mercato di Bitcoin dall'01/05/2013 fino al 21/05/2020, in scala logaritmica e in dollari americani.

Dai risultati in Tabella 6.7, il risultato in output della rete neurale è il più vicino a quello reale, rispetto alle reti neurali addestrate in precedenza. In media, la differenza tra il valore reale e l'output della rete neurale, entrambi in scala logaritmica, è pari a 0,1176.
Analizzando le variazioni dell'output della rete neurale da un giorno all'altro, la rete neurale ha previsto correttamente una variazione in aumento o in diminuzione in 16 casi su 30 (è stata esclusa la prima data).
Quindi, nonostante sia più precisa delle precedenti, non è ancora in grado di prevedere correttamente un numero sufficiente di variazioni in aumento o diminuzione da un giorno all'altro del mese dopo, per poter affermare che la rete sia efficace.

Figura 6.6: Rappresentazione della rete neurale con Stock-to-Flow e capitalizzazione di mercato (mese successivo)

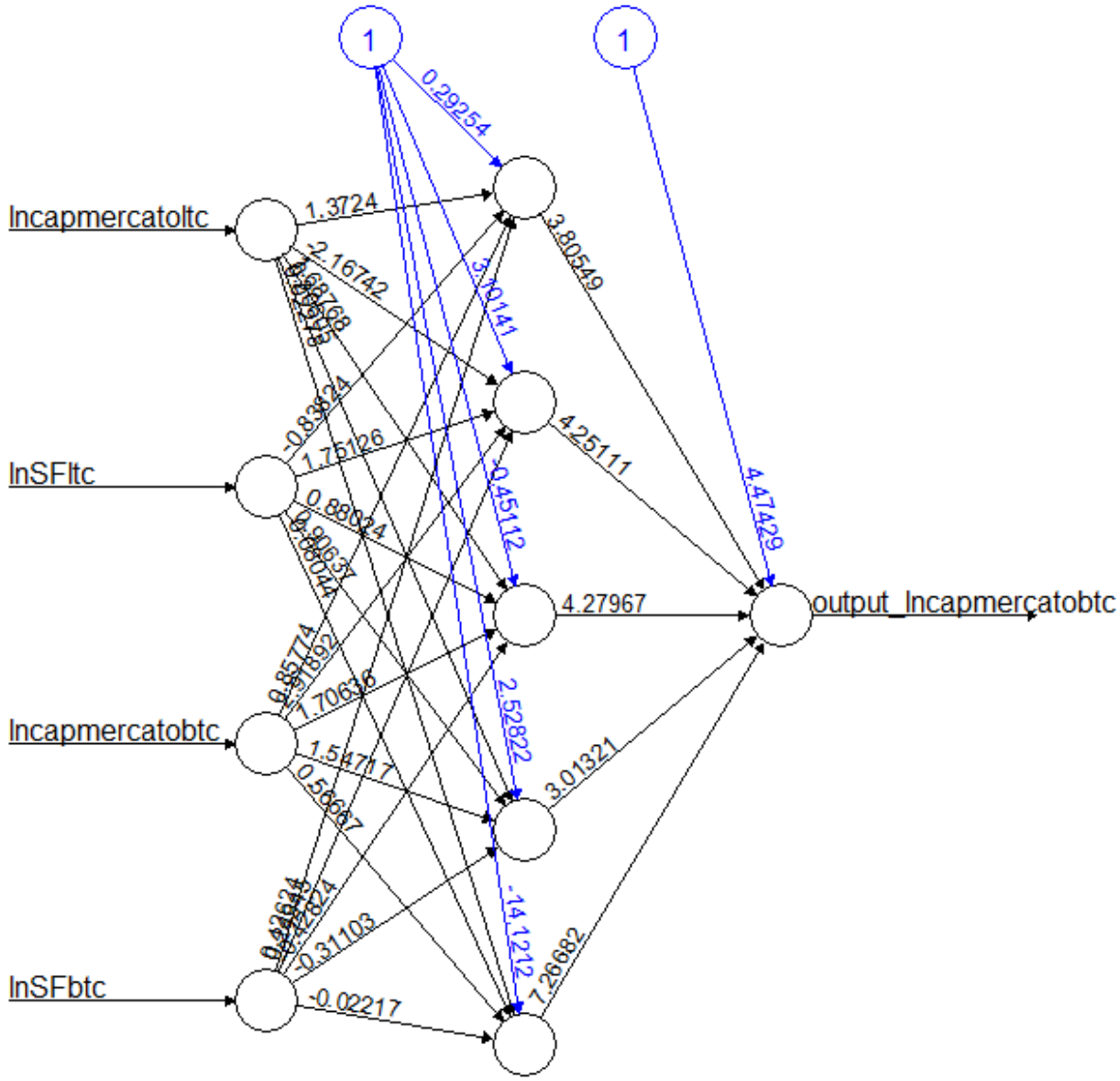


Tabella 6.7: Risultati della rete neurale, con Stock-to-Flow e capitalizzazione di mercato (mese successivo)

	Data Input	Input-ln(ltc_capmercato)	Input-ln(SF_ltc)	Input-ln(btc_capmercato)	Input-ln(SF_btc)	Data output	Output rete neurale	ln(btc_capmercato) reale
1	18/04/2020	21,7753	9,0189	25,6147	9,1359	18/05/2020	25,6679	25,9094
2	19/04/2020	21,7370	9,0531	25,5992	9,1747	19/05/2020	25,6590	25,9123
3	20/04/2020	21,6870	9,0417	25,5569	9,1173	20/05/2020	25,6303	25,8876
4	21/04/2020	21,6950	9,0616	25,5595	9,1948	21/05/2020	25,6321	25,8395
5	22/04/2020	21,7216	9,0955	25,5958	9,3237	22/05/2020	25,6565	25,8498
6	23/04/2020	21,7492	9,1705	25,6458	9,2431	23/05/2020	25,6984	25,8522
7	24/04/2020	21,7836	9,1148	25,6483	9,2293	24/05/2020	25,6962	25,8102
8	25/04/2020	21,7796	9,1361	25,6526	9,2865	25/05/2020	25,6993	25,8219
9	26/04/2020	21,7853	9,1132	25,6719	9,2793	26/05/2020	25,7098	25,8136
10	27/04/2020	21,7839	9,0706	25,6841	9,2506	27/05/2020	25,7144	25,8508
11	28/04/2020	21,8132	9,0169	25,6832	9,1625	28/05/2020	25,7119	25,8934
12	29/04/2020	21,8739	9,0792	25,8034	9,2228	29/05/2020	25,7919	25,8792
13	30/04/2020	21,8272	9,1547	25,7910	9,2944	30/05/2020	25,7880	25,9063
14	01/05/2020	21,8418	9,0744	25,8143	9,2510	31/05/2020	25,7965	25,8794
15	02/05/2020	21,8856	9,0880	25,8280	9,2026	01/06/2020	25,8082	25,9575
16	03/05/2020	21,8614	9,0813	25,8191	9,0760	02/06/2020	25,8046	25,8878
17	04/05/2020	21,8391	9,0968	25,8176	9,1375	03/06/2020	25,8030	25,9014
18	05/05/2020	21,8276	8,9772	25,8293	9,1376	04/06/2020	25,7996	25,9190
19	06/05/2020	21,8148	9,1144	25,8602	9,1633	05/06/2020	25,8287	25,9015
20	07/05/2020	21,8506	9,0700	25,9358	9,2099	06/06/2020	25,8690	25,9043
21	08/05/2020	21,8598	9,2215	25,9224	9,2805	07/06/2020	25,8722	25,9125
22	09/05/2020	21,8418	9,0636	25,8934	9,2879	08/06/2020	25,8418	25,9148
23	10/05/2020	21,7277	9,1166	25,7992	9,0649	09/06/2020	25,7927	25,9159
24	11/05/2020	21,7169	9,1397	25,7850	9,2414	10/06/2020	25,7816	25,9270
25	12/05/2020	21,7325	9,1327	25,8110	9,9104	11/06/2020	25,7813	25,8633
26	13/05/2020	21,7578	9,1435	25,8668	10,1149	12/06/2020	25,8117	25,8824
27	14/05/2020	21,7750	9,0331	25,9169	10,1579	13/06/2020	25,8315	25,8830
28	15/05/2020	21,7471	9,0726	25,8673	10,0658	14/06/2020	25,8068	25,8705
29	16/05/2020	21,7586	9,0430	25,8747	10,0579	15/06/2020	25,8092	25,8810
30	17/05/2020	21,7671	9,0111	25,9048	10,2692	16/06/2020	25,8197	25,8894
31	18/05/2020	21,8041	9,1513	25,9094	10,0422	17/06/2020	25,8403	25,8819

6.7 Riepilogo

Tabella 6.8: Riepilogo reti neurali

Rete	Media differenze tra output previsto e reale	Variazioni in aumento o diminuzione previste correttamente	
Settimana	0,6982	5/7	71,43%
Giorno	0,5883	6/27	22,22%
Giorno (con SF)	0,2554	13/27	48,15%
Mese	0,5945	14/30	46,67%
Mese (con SF)	0,1944	14/30	46,67%
Mese sul valore di mercato (con SF di Ltc e Btc, e valore di mercato di Ltc e Btc del mese precedente)	0,1176	16/30	53,33%

La rete meno precisa nel prevedere i valori è quella del prezzo di Bitcoin della settimana dopo, ma è anche la rete che ha previsto un numero maggiore di variazioni del valore da un giorno all'altro. È necessario però considerare che, in questo caso, il campione preso in esame è composto da solamente otto giorni.
Le reti addestrate successivamente, cioè quella che tenta di prevedere il prezzo di Bitcoin del giorno e del mese dopo, sono solo leggermente più precise nel prevedere il prezzo rispetto alla rete della settimana. La rete del mese ha riportato un numero leggermente più elevato di variazioni previste correttamente del prezzo di Bitcoin da un giorno all'altro. Grazie all'aggiunta di un input, cioè il valore dello Stock-to-Flow di Litecoin, è aumentata la precisione delle reti neurali, rendendole più accurate nel prevedere i valori e migliorando anche i risultati sulle variazioni da un giorno all'altro.
La rete neurale con i risultati migliori è quella col maggior numero di input, infatti la rete della capitalizzazione di mercato è più accurata rispetto alle precedenti nel prevedere i valori e ha avuto anche un miglioramento in termini di previsione dell'aumento o della diminuzione del prezzo da un giorno all'altro, anche se di poco e non ancora abbastanza alto per poter affermare che la rete sia efficace.

Conclusioni

L'obiettivo prefissato della mia tesi di fornire un approfondimento sul funzionamento delle criptovalute, insieme all'analisi di dati riguardante il modello Stock-to-Flow di Bitcoin e di Litecoin, spero sia stato raggiunto.

Il risultato del mio lavoro mi ha portato a capire che le criptovalute sono un argomento molto complesso che richiede conoscenze in numerosi ambiti, come la matematica, l'informatica e l'economia, per capirle a pieno. Le criptovalute sono un'idea innovativa di moneta elettronica grazie alla fusione delle tecnologie già esistenti come le tecniche crittografiche e l'introduzione della tecnologia della Blockchain, che permette ai sistemi basati su di essa di non aver bisogno di un'autorità centrale per funzionare.

È un ambito che richiede continui aggiornamenti non solo dal punto di vista tecnico, visto che la tecnologia cambia in fretta, ma anche dal punto di vista economico. In tal senso, il mercato delle criptovalute ha già una capitalizzazione di mercato rilevante e, anche da questo punto di vista, cambia molto velocemente nel tempo in base a domanda e offerta nel mercato.

Le criptovalute, a causa della volatilità nel loro prezzo, non sembrano ancora adatte a sostituire le monete e non vengono utilizzate da molte persone. Tuttavia, siccome il codice sorgente della maggior parte delle criptovalute è pubblico, è possibile partire da esso per creare sistemi sempre migliori e applicarli in altri ambiti. Le criptovalute possono essere un buon punto di partenza per creare un unico strumento digitale, il quale integri tutti i mezzi di pagamento e sia utilizzabile in diversi contesti della vita reale.

Elenco delle figure

Elenco delle tabelle

Bibliografia

Caponera, A. e C. Gola. *Aspetti economici e regolamentari delle «cripto-attività»*. 2019. URL: https://www.bancaditalia.it/pubblicazioni/qef/2019-0484/QEF_484_19.pdf.

Chuen, David Lee Kuo. *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. Amsterdam [etc.]: Academic Press - Elsevier, 2015.

Clerici, Carlo. *Il concetto di scarsità nella determinazione del valore di Bitcoin, traduzione in italiano dell'articolo originale di PlanB*. 2019. URL: https://medium.com/@carloclerici/il-concetto-di-scarsita-nella-determinazione-del-valore-di-bitcoin-c716c0ad3fff.

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

M., Riedmiller e Braun H. *A direct adaptive method for faster backpropagation learning: the RPROP algorithm. IEEE International Conference on Neural Networks, San Francisco, CA, USA*. Vol. 1, pp. 586-591. 1993.

Narayanan, Arvind et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton e Oxford: Princeton University Press, 2016.

PlanB. *Bitcoin Stock-to-Flow Cross Asset Model*. 2020. URL: https://medium.com/@100trillionUSD/bitcoin-stock-to-flow-cross-asset-model-50d260feed12.

– *Modeling Bitcoin's Value with Scarcity*. 2019. URL: https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25.

Rizzo, Walter. *Modello di Stock-to-Flow Cross Asset di Bitcoin*. 2020. URL: https://medium.com/@walterrizzo91/modello-di-stock-to-flow-cross-asset-di-bitcoin-81dca7e7e74a.

Sitografia

https://economiapertutti.bancaditalia.it/
https://www.ecb.europa.eu/
http://www.consob.it/
https://www.bancaditalia.it/pubblicazioni/qef/2019-0484/QEF_484_19.pdf
https://www.giustizia-amministrativa.it/-/tassazione-della-moneta-elettronica-/
https://www.gazzettaufficiale.it/eli/gu/2017/06/19/140/so/28/sg/pdf
https://www.blockchain.com/
https://bitcoin.org/it/
https://bitcoin.org/bitcoin.pdf
https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf
https://en.bitcoinwiki.org/wiki/
https://en.bitcoin.it/wiki/
https://cryptonomist.ch/
https://it.cointelegraph.com/
https://digitalik.net/btc/
https://github.com/100trillionUSD/bitcoin/
https://digitalik.net/btc/
https://coinmetrics.io/
https://coinmarketcap.com/
https://litecoin.org/it/
https://litecoin.info/
http://www.neuro.nigmatec.ru/materials/themeid_17/riedmiller93direct.pdf
http://www.inf.fu-berlin.de/lehre/WS06/Mustererkennung/Paper/rprop.pdf