Davide Capoti, Emanuele Colacchi, Matteo Maggioni

BITCOIN REVOLUTION

La moneta digitale alla conquista del mondo

HOEPLI

BITCOIN REVOLUTION

Davide Capoti Emanuele Colacchi Matteo Maggioni

BITCOIN REVOLUTION

LA MONETA DIGITALE ALLA CONQUISTA DEL MONDO

EDITORE ULRICO HOEPLI
MILANO

via Hoepli 5, 20121 Milano (Italy)
tel. +39 02 864871 – fax +39 02 8052886
e-mail hoepli@hoepli.it

www.hoepli.it

Seguici su Twitter: @Hoepli_1870

ISBN EBOOK 978-88-203-6986-6

Realizzazione editoriale: Maurizio Vedovati - Servizi editoriali (www.iltrio.it)

Copertina: Sara Taglialegne

Realizzazione digitale: Promedia, Torino

C’è chi guarda alle cose come sono e si chiede “perché?”.
Io penso a come potrebbero essere e mi chiedo “perché no?”

Robert F. Kennedy

SOMMARIO

Capitolo 1

Che cos'è il Bitcoin

Che cos'è il Bitcoin?

Il protocollo Bitcoin

Introduzione alla crittografia

Funzione Hash

Firme digitali

Blockchain

- Il concetto di Blocco
- Il blocco 0

Script

Wallet

Network

Transazioni

Moneta

Parte II

Il Mining

Capitolo 2

Che cos'è il mining?

Il problema del *double spending*
Incentivi per il minatore
Fee delle transazioni

Capitolo 3

L'algoritmo di mining

Target
Difficoltà
Tempo per cambio Difficoltà
Hash rate

Capitolo 4

Costo e Fair value del Bitcoin

Costo della generazione dei Bitcoin

- Spesa di capitale
- Spesa operativa
- Costo totale

Confronto Bitcoin, oro e valute

- Confronto costi economici
- Confronto costi ambientali

Fair value del Bitcoin

- Fair value come mezzo di scambio
- Fair value come riserva di valore
- Fair value finale

Costo e Fair value a confronto

Parte III

Il Trading

Capitolo 5
Mercati OTC e mercato Forex

I mercati OTC
Il mercato Forex

Capitolo 6
Analisi di prezzo del Bitcoin

Analisi grafica del trend
Analisi prezzo-Difficoltà
Analisi statistica

Capitolo 7
L'Analisi tecnica e il Bitcoin

Capitolo 8

Trading system per il Bitcoin

Trading system statistico

PREFAZIONE

È in atto un cambiamento epocale: la moneta digitale irrompe sulla scena mondiale e rivoluziona le tradizionali forme di pagamento.

Argomento attualissimo, attraente, complesso e in evoluzione che con il presente lavoro ci prefiggiamo di

rendere più comprensibile. Quindi, vi guideremo nel campo delle valute digitali, in particolare del Bitcoin, del quale illustreremo caratteristiche tecniche e strategie operative.

Il libro è articolato in tre macro-aree.

Nella prima parte presenteremo in dettaglio le caratteristiche del Bitcoin e il funzionamento del protocollo. Particolare attenzione è dedicata al concetto di Blockchain e di Blocco.

Proseguiremo con la spiegazione dettagliata dell'algoritmo di mining, cioè di quel processo che permette di confermare le transazioni in Bitcoin e coniarne di nuovi. Questo è un punto nevralgico. È una sezione prettamente

tecnica che permette di comprendere la dinamica del processo di creazione della moneta. Quindi merita tutta la nostra attenzione.

L'ultima parte del libro è dedicata all'analisi tecnica e al trading. Vedremo alcuni indicatori che possono essere applicati in modo profittevole sul mercato Bitcoin e concluderemo con la costruzione di alcuni *trading system*.

Se il lettore arriverà fino all'ultima pagina, vorrà dire che saremo riusciti nel nostro intento: suscitare curiosità e interesse. Noi ci siamo avvicinati al mondo delle valute digitali quasi per caso, leggendo alcune news sparse qua e là su Internet. Tutto è iniziato da lì. Nel

giro di poco tempo abbiamo acquistato tutte le componenti hardware per assemblare un PC, estremamente performante, per "minare" Bitcoin e altre valute digitali.

Ma la tecnologia invecchia in fretta, così le nostre macchine sono diventate obsolete e siamo necessariamente passati a macchine ASIC, progettate e costruite esclusivamente per l'attività di mining. Da qui il salto, da un contesto domestico a uno industriale. Nasce CloudMiningBiz, una delle prime startup italiane (www.cloudminingbiz.com) che svolge attività di mining in conto proprio e per terzi.

Oltre all'aspetto del mining, in generale il nostro obiettivo è divulgare

il know-how maturato in questo settore, convinti che la condivisione della conoscenza sia il motore dell'evoluzione umana. A tale scopo, il 23 maggio 2014 ne abbiamo parlato presso l'ITF di Rimini, uno dei principali appuntamenti di trading in Europa, organizzato da Traderlink; di fatto la prima conferenza italiana sul Bitcoin.

La pubblicazione di questo libro va nella stessa direzione. I nostri ringraziamenti a Hoepli, che ha sostenuto fin da subito il nostro progetto editoriale.

Non ci dilunghiamo oltre.

A tutti voi auguriamo buona lettura.

CRONISTORIA DEL BITCOIN

- 18 agosto 2008: viene registrato il dominio www.Bitcoin.org. Sembra sia stato registrato da Satoshi Nakamoto attraverso il sito

www.anonymousspeech.com, che permette registrazioni anonime di domini internet.

- 31 ottobre 2008: viene pubblicato il "Bitcoin design paper". Si aprono i battenti della storia alla rivoluzione.
- 9 novembre 2008: il progetto "Bitcoin" viene registrato sul sito www.sourceforge.net, che fornisce gli strumenti per sviluppare software in modo collaborativo.
- 3 gennaio 2009: nasce il "Genesis block" alle 18:15:05 GMT.
- 30 dicembre 2009: si verifica il primo cambio di Difficoltà (dal

valore 1 al valore 1,18289953).

- 17 agosto 2010: viene istituito "Mt. Gox" (Magic: "The Gathering Online Exchange"), cioè il primo exchange in cui negoziare i Bitcoin. Il sito (www.mtgox.com), creato da Jed McCaleb, è nato inizialmente come punto di scambio per carte da gioco online, e si è poi convertito allo scambio di Bitcoin. Nel primo giorno di contrattazione 1 Bitcoin è stato scambiato con $ 0,0769. Attualmente, McCaleb sta lavorando a una nuova valuta digitale chiamata "ripple", che

secondo alcuni potrebbe essere un potenziale concorrente del Bitcoin.

- 10 febbraio 2011: il Bitcoin ha superato la parità con il dollaro americano ($ 1,1 al prezzo di chiusura 18:15:05 - Mt. Gox).
- 1 marzo 2011: Mark Karpelès ha acquistato Mt. Gox dal fondatore Jed McCaleb.
- 24 giugno 2011: la Difficoltà supera il valore di 1.000.000 con il Blocco 133056.
- 2 aprile 2013: il Bitcoin ha superato i 100 dollari ($ 104,79261 al prezzo di chiusura delle 18:15:05 - Mt. Gox).
- 28 novembre 2013: il Bitcoin ha

superato i 1000 dollari ($ 1086,50818 al prezzo di chiusura delle 18:15:05 - Mt. Gox).

- 7 febbraio 2014: Mt. Gox comunica la sospensione dei *withdrawal*. Questo è l'inizio della fine per l'exchange più importante.
- 23 febbraio 2014: Mark Kerpelès si dimette dal consiglio della Bitcoin Foundation.
- 24 febbraio 2014: Mt. Gox sospende il trading sulla propria piattaforma e, poco dopo, mette offline il sito internet. Un documento ufficiale comunica che la società è in bancarotta e le

sono stati sottratti circa 744.408 Bitcoin.

- 11 marzo 2014: la U.S. Commodity Futures Trading Commission (CFTC) ha dichiarato di voler valutare la possibilità di regolamentare il mercato delle valute digitali.
- 11 aprile 2014: il Governatore della PBOC (People's Bank of China) ha dichiarato che la Cina non bannerà il Bitcoin e ha suggerito di classificarlo come una sorta di asset negoziabile e da collezione, come per esempio i francobolli, piuttosto che una moneta di pagamento.
- 30 luglio 2014: Wikimedia

Foundation apre alla possibilità di ricevere donazioni in Bitcoin (attraverso Coinbase).

- 23 settembre 2014: PayPal offre, per la prima volta, ai commercianti nordamericani la possibilità di scegliere se ricevere pagamenti in Bitcoin per beni digitali.

Qualunque sia la vostra opinione, i fatti elencati dimostrano che il Bitcoin è un evento che non è più possibile ignorare: una rivoluzione è in atto!

PARTE I

I fondamentali

Non pretendiamo che le cose

cambino
se continuiamo a farle nello
stesso modo.

Albert Einstein

CAPITOLO 1

Che cos'è il Bitcoin

CHE COS'È IL BITCOIN?

Per una moneta digitale, come lo è il Bitcoin, non possiamo non partire dalla definizione data da Wikipedia (http://en.wikipedia.org/wiki/Bitcoin):

> Bitcoin is a peer-to-peer payment system and digital currency introduced as open source software in 2009. It is a cryptocurrency, so-called because it uses cryptography to control the creation and transfer of money. Conventionally, the

capitalized word “Bitcoin” refers to the technology and network, whereas lowercase “Bitcoin” refers to the currency itself.

Bitcoin è un sistema di pagamento peer-to-peer e una moneta digitale, sviluppato nel 2009 come software open source. Si tratta di una crypto valuta, poiché utilizza la crittografia per controllare la creazione e il trasferimento della moneta. Convenzionalmente la parola “Bitcoin”, scritta in

maiuscola, si riferisce alla tecnologia e al network, mentre la parola “bitcoin” scritta in minuscolo, si riferisce alla valuta stessa.

Nelle prime due frasi di questa definizione troviamo la maggior parte dei concetti che andremo a esporre nei prossimi capitoli:

- Bitcoin è un sistema di pagamento peer-to-peer.
- Bitcoin è una moneta (digitale).
- Bitcoin utilizza la crittografia.
- Bitcoin si può creare e trasferire.

La parola Bitcoin raccoglie tre concetti

in uno:

- Bitcoin è un protocollo.
- Bitcoin è un progetto software open source.
- Bitcoin è un network.

Il Bitcoin è un protocollo, cioè un insieme di regole che servono a definire il funzionamento del software utilizzato da un network di computer collegati tra loro, con lo scopo di creare e gestire la valuta bitcoin.

Il punto di partenza si è avuto il 31 ottobre 2008, giorno in cui Satoshi Nakamoto ha pubblicato il "Bitcoin design paper", in cui spiega la struttura,

il funzionamento e le motivazioni che lo hanno spinto a svilupparlo. Qui vi riportiamo la traduzione del sommario:

> Una versione puramente peer-to-peer di denaro elettronico consentirebbe ai pagamenti online di essere inviati da una persona all'altra senza passare attraverso un'istituzione finanziaria. Le firme digitali forniscono parte della soluzione, ma i principali benefici si perdono se, per impedire la doppia spesa (*double-spending*), è ancora necessario un terzo

soggetto di fiducia. Noi proponiamo una soluzione al problema della doppia spesa usando un network peer-to-peer. Il network marca in maniera temporale le transazioni attraverso un codice Hash e le posiziona in una catena continua di prove di lavoro (*proof-of-work*) basate su funzioni Hash, formando un registro che non può essere modificato senza rifare la prova di lavoro stessa. La catena più lunga serve non soltanto come prova della sequenza di eventi di cui è testimone, ma anche come

evidenza che proviene dal più grande pool di potenza CPU. Fintanto che la maggior parte della potenza CPU è controllata dai nodi che non cooperano ad attaccare il network, questi genereranno la catena più lunga e distanzieranno eventuali aggressori. Lo stesso network richiede una struttura minima. I messaggi vengono trasmessi nel miglior modo possibile e i nodi possono sganciarsi e ricollegarsi al network a propria volontà, accettando la catena di lavoro più lunga

come prova di quanto successo, mentre erano assenti.

La traduzione integrale del documento la trovate sul sito internet: www.bitcoinrevolution.it

IL PROTOCOLLO BITCOIN

Comprendere il protocollo Bitcoin in tutti i suoi dettagli è un lavoro complesso, che richiede tempo e specifiche conoscenze di

programmazione e crittografia.

Non è nostra intenzione annoiarvi con tali argomenti, ma al tempo stesso riteniamo che sia fondamentale mostrare il funzionamento del sistema Bitcoin e lo faremo semplificando il più possibile i concetti, senza cadere in particolari tecnicismi.

L'esposizione verrà articolata nei seguenti punti:

- Introduzione alla crittografia.
- Funzione Hash.
- Firme digitali.
- Blockchain.
- Transazioni.

INTRODUZIONE ALLA CRITTOGRAFIA

La crittografia ci sarà utile per comprendere meglio alcuni aspetti legati al funzionamento e alla sicurezza del network Bitcoin.

Il termine crittografia deriva dall'unione di due parole di origine greca: "kryptós" che significa "nascosto" e "graphia" che significa "scrittura". Come è insito nell'etimologia della parola, lo scopo della crittografia è quello di nascondere il contenuto di un messaggio. In sostanza, la crittografia è un insieme di

tecniche che consentono di trasmettere un messaggio mantenendolo segreto a tutti, tranne alle persone che possiedono le chiavi per decifrarlo.

Immaginate ora di aver intercettato il seguente messaggio:

ZLHMOD ZBIQL VFQZLFI

La soluzione la trovate nei versi latini tratti dall'opera *Vita dei Cesari* dello scrittore romano Svetonio:

> "Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua

occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.”

Svetonio, *De Vita Caesarum*, §56

Ecco la traduzione:

“Restano quelle (le lettere) a Cicerone, così come quelle ai familiari sugli affari

> domestici, nelle quali, se doveva fare delle comunicazioni segrete, le scriveva in codice, cioè con l'ordine delle lettere così disposto che nessuna parola potesse essere ricostruita: se qualcuno avesse voluto capire il senso e decifrare, avrebbe dovuto cambiare la quarta lettera degli elementi, cioè D per A e così via per le rimanenti."
>
> Svetonio, *Vita dei Cesari*, §56

Svetonio racconta che Giulio Cesare, per le sue corrispondenze riservate,

utilizzava un codice di cifratura a sostituzione alfabetica, in cui ogni lettera dell'alfabeto era sostituita con quella relativa a 3 posizioni successive. In questo modo al posto della lettera A scriveva la lettera D, al posto della lettera B scriveva la lettera E ecc. (Tabella 1.1).

TABELLA 1.1 – La cifratura di Giulio Cesare.

Chiaro	A	B	C	D	...	U	V	Z
Cifrato	D	E	F	G	...	A	B	C

Ora anche voi dovreste essere riusciti a decifrare il messaggio che abbiamo intercettato:

COMPRA CENTO BITCOIN

Il cifrario di Giulio Cesare è sicuramente un metodo semplice e facilmente scardinabile, ma nella sua semplicità conteneva già i due elementi caratteristici di un codice di cifratura, cioè l'algoritmo e la chiave. L'algoritmo non è altro che la regola con cui si modifica il messaggio originale, rendendolo criptato (o cifrato), mentre la chiave è il parametro che permette di decodificare (o decifrare) il messaggio stesso. La distinzione tra algoritmo e chiave è fondamentale.

Nei sistemi crittografici più raffinati l'algoritmo può essere noto a tutti, mentre la sicurezza della cifratura risiede nella mancata divulgazione della

chiave.

Quello che abbiamo visto è un metodo di cifratura simmetrico, in cui la chiave per codificare e decodificare il messaggio è la stessa (Figura 1.1).

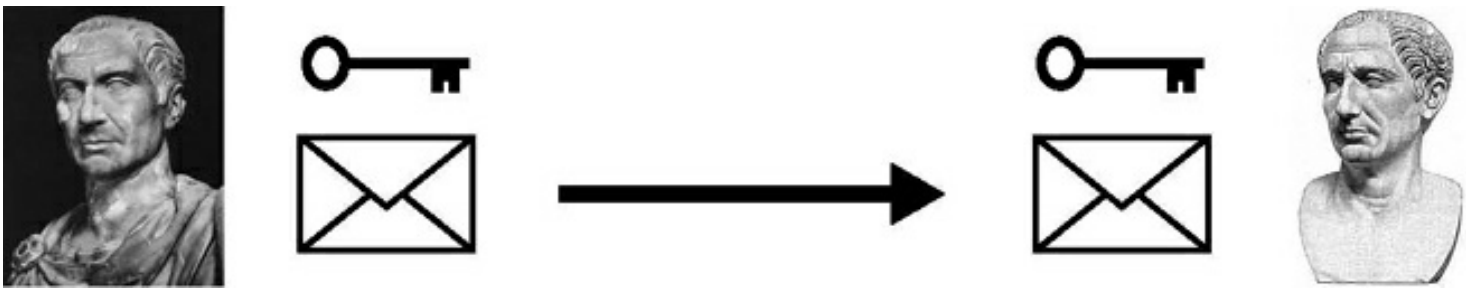


FIGURA 1.1 – Il metodo di cifratura di Giulio Cesare.

La vera evoluzione della crittografia si è però avuta solo nel XX secolo, sulla scia dell'arrivo di nuovi mezzi di trasmissione dell'informazione e della sempre più pressante richiesta di sistemi di sicurezza per lo scambio di

informazioni.

La novità si è avuta con l'introduzione di due chiavi:

- chiave pubblica (o chiave di cifratura);
- chiave privata (o chiave di decifratura).

La chiave pubblica è nota a tutti coloro che vogliono inviare un messaggio cifrato, mentre la chiave privata è nota solo al destinatario ed è indispensabile per decifrare quanto ricevuto. In questo modo è facile passare dal testo in chiaro a quello cifrato, ma non si è in grado di passare dal testo cifrato a quello in

chiaro. Decade una delle principali caratteristiche dei tradizionali sistemi di cifratura, la simmetria. Cifrare e decifrare non sono più la stessa cosa.

Siamo passati a un metodo di cifratura asimmetrico. Con un esempio capirete meglio il funzionamento della crittografia asimmetrica: il mittente (A) utilizza la chiave pubblica del destinatario (B) per cifrare il messaggio, dando la possibilità a quest'ultimo di essere l'unico a decifrarlo con la propria chiave privata. In questo modo è garantita la sicurezza e l'integrità (Figura 1.2).

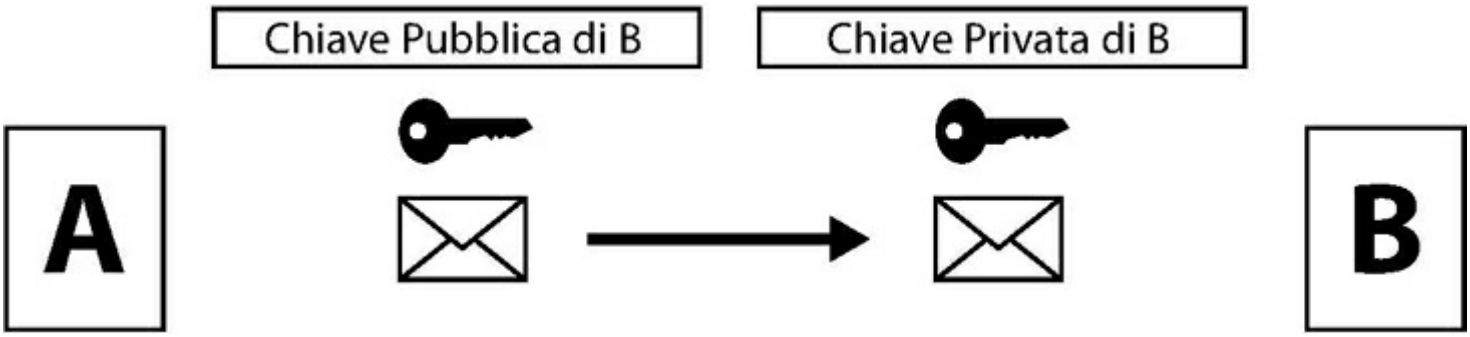


FIGURA 1.2 – Il primo metodo di cifratura.

I vantaggi rispetto alla crittografia simmetrica sono enormi. Ripensate al cifrario di Cesare: si usava la chiave 3 sia per criptare sia per decriptare il messaggio e inoltre, per concordare e scambiarsi la chiave, il destinatario e il mittente dovevano preventivamente essersi messi in contatto. Mentre con la crittografia asimmetrica tutto questo non è necessario ed è possibile comunicare in tutta segretezza, senza usare la stessa chiave e senza essersi mai incontrati in

precedenza.

Lo schema che abbiamo presentato ha però un punto debole. Durante la trasmissione del messaggio, questo potrebbe essere intercettato da un malintenzionato (C) e sostituito con un altro messaggio, sempre cifrato con la chiave pubblica del destinatario (B). Quando riceve il messaggio, il destinatario (B) non ha modo di sapere se il suo messaggio sia stato sostituito o se si tratta effettivamente di quello inviato dal mittente (A) (Figura 1.3).

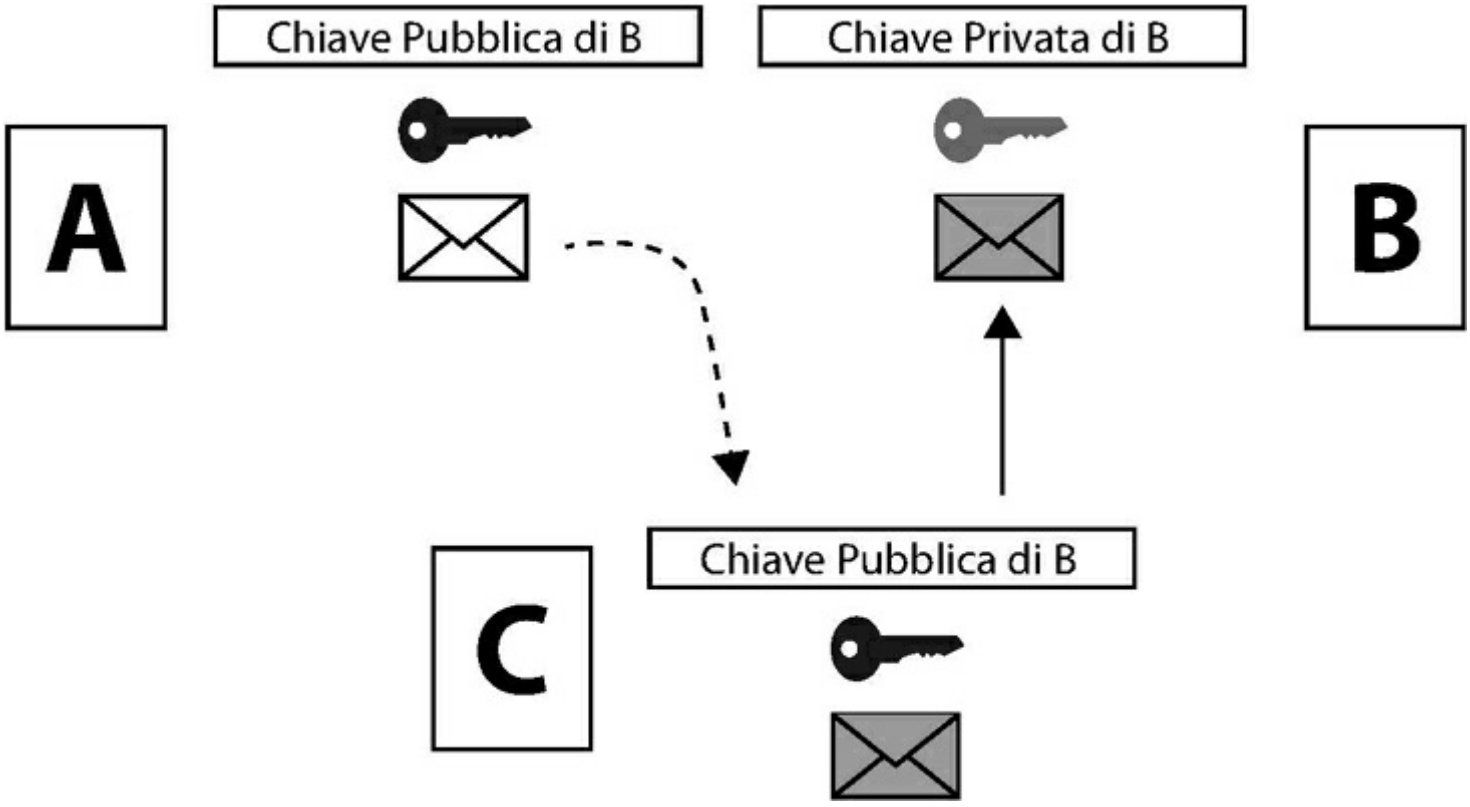


FIGURA 1.3 – Il punto debole del primo metodo di cifratura.

Abbiamo visto come il primo metodo sia in grado di garantire sicurezza e integrità. Ma per garantire autenticità e accettazione analizziamo un altro metodo: il mittente (A) utilizza la propria chiave privata per cifrare il messaggio e il destinatario (B) è in

grado di decifrarlo utilizzando la chiave pubblica del mittente (A) (Figura 1.4).

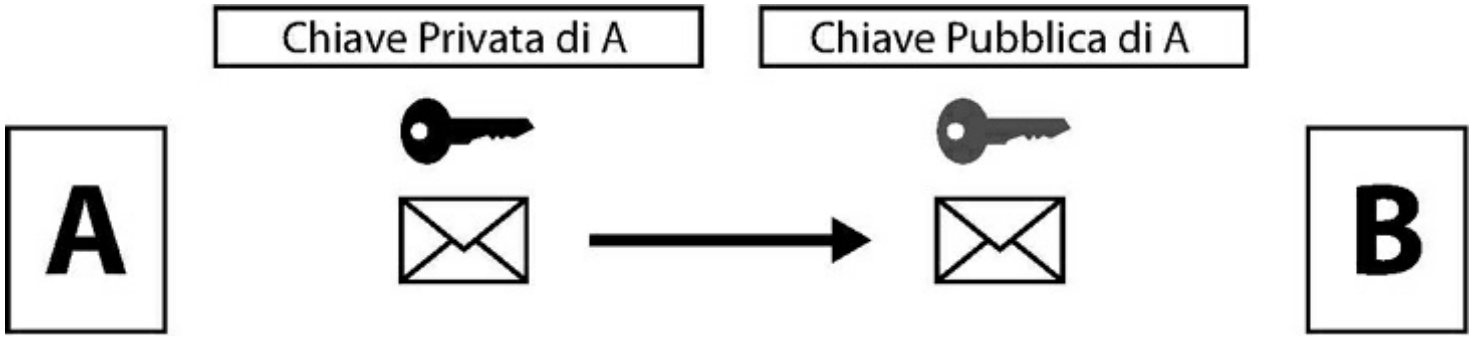


FIGURA 1.4 – Il secondo metodo di cifratura.

È evidente che questo metodo non è sicuro. Infatti, il messaggio può essere decifrato da tutti i possessori (i soggetti C, D ecc.) della chiave pubblica del mittente (A) (Figura 1.5).

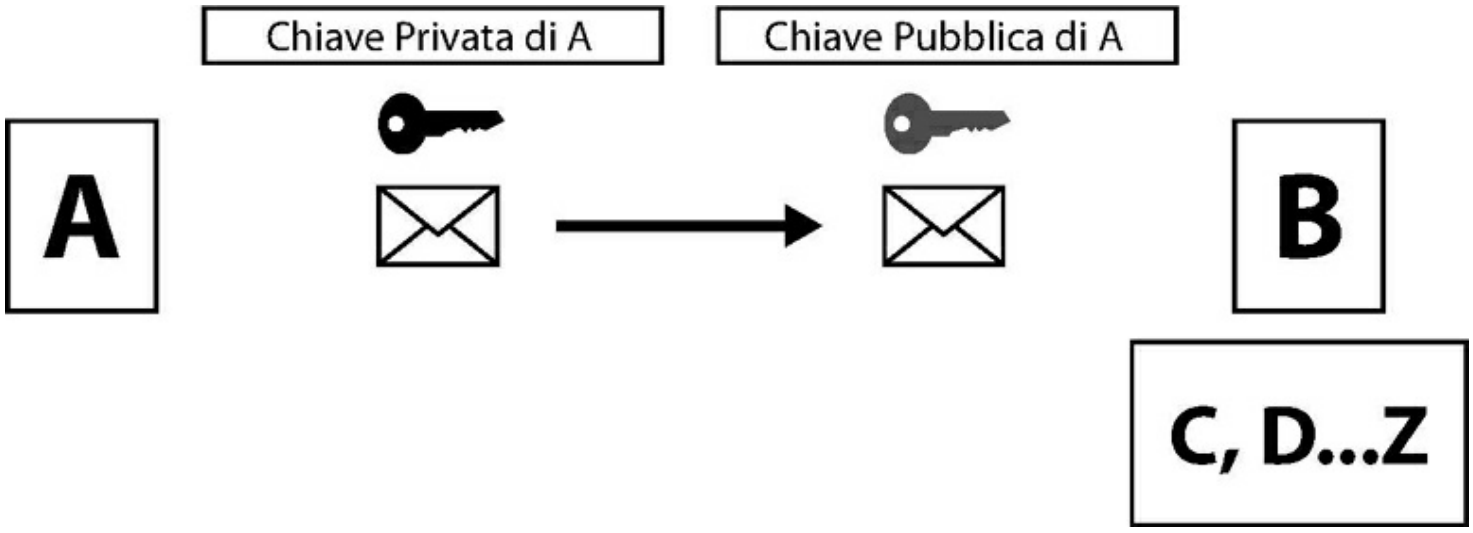


FIGURA 1.5 – Il punto debole del secondo metodo di cifratura.

È possibile però combinare i due metodi visti per costruirne un terzo in grado di conservare i punti di forza di entrambi. Il mittente (A) utilizza la chiave pubblica del destinatario (B) per cifrare il messaggio e lo autentica con la propria chiave privata. Avviene quindi una doppia cifratura. In sintesi, chiunque è in grado di verificare l'autenticità del

messaggio decifrando la prima cifratura con la chiave pubblica del mittente (A), ma solo il destinatario (B) ha la possibilità di decifrare la seconda cifratura con la propria chiave privata. In questo modo è garantita la sicurezza, l'integrità, l'autenticità e l'accettazione (Figura 1.6).

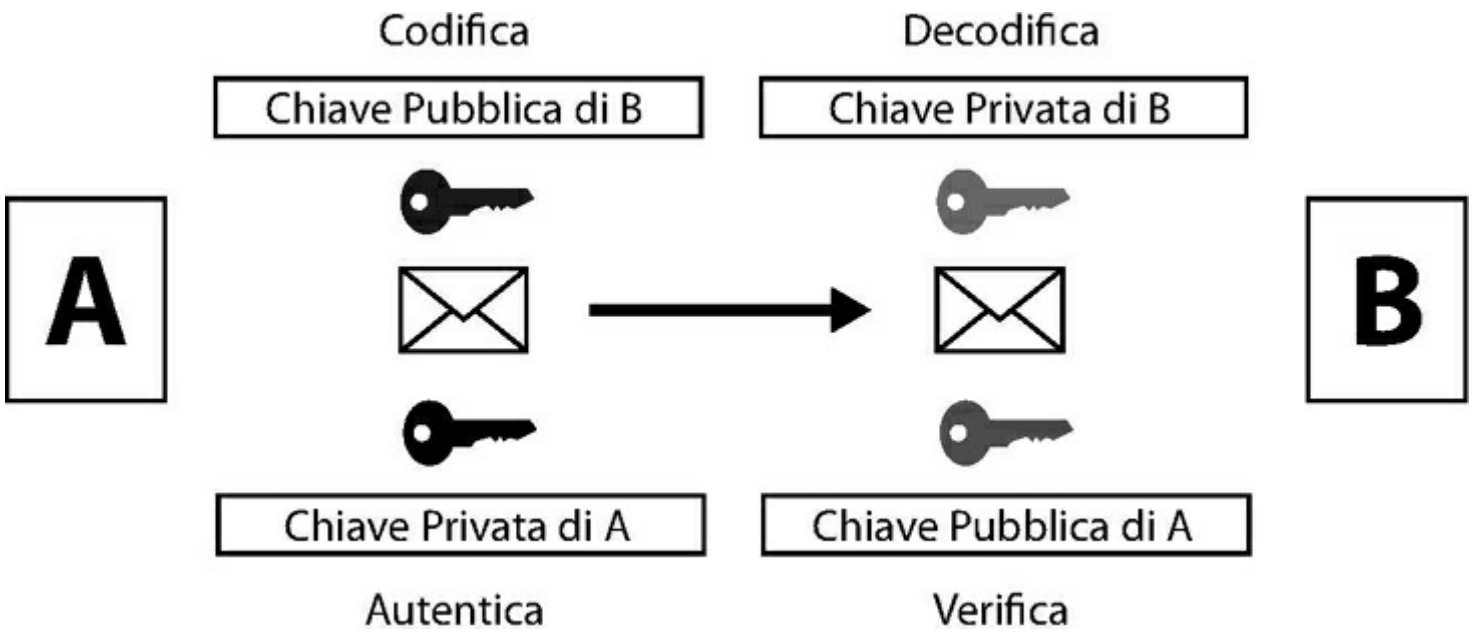


FIGURA 1.6 – Il terzo metodo di cifratura.

Non siamo però ancora contenti.

Facciamo un passo in avanti e aggiungiamo il concetto di funzione Hash, con lo scopo di aumentare il grado d'integrità e autenticità del messaggio.

FUNZIONE HASH

La funzione Hash è un sistema che trasforma un messaggio di lunghezza arbitraria in un codice alfanumerico di lunghezza prefissata, che prende il nome di Hash, Digest o impronta del messaggio (Figura 1.7).

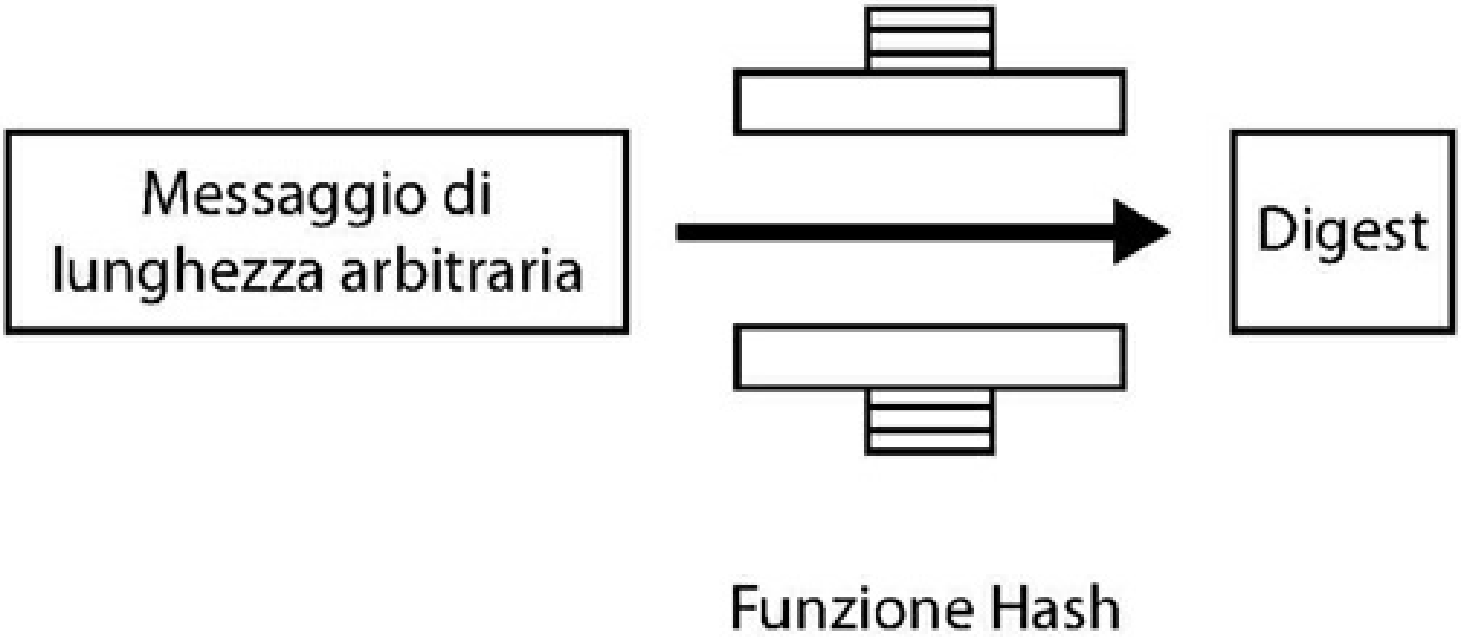


FIGURA 1.7 – Schema della funzione Hash.

In linguaggio matematico, se ipotizziamo che:

- Σ è un alfabeto.
- $\boldsymbol{\Sigma^*}$ è l'insieme delle stringhe di qualsiasi lunghezza composte dai simboli dell'alfabeto.
- Σ^n è l'insieme delle stringhe di lunghezza n.

h è detta funzione Hash se:

$$h: \Sigma^* \rightarrow \Sigma^n$$

$$x \rightarrow h_{(x)}$$

Questa funzione presenta le seguenti proprietà:

- Semplicità: deve essere agevole calcolare il codice Hash da qualunque tipo di messaggio di qualunque dimensione.
- Univocità: deve essere praticamente nulla la probabilità che due messaggi generino lo stesso codice Hash.

- Non invertibilità: deve essere praticamente impossibile poter risalire dal codice Hash al messaggio.
- "Effetto valanga": la minima modifica del messaggio deve generare un'alterazione radicale dell'Hash.

L'Hash è, dunque, una specie di impronta digitale, che identifica in modo univoco e irreversibile un certo messaggio, conferendogli integrità e autenticità.

Le funzioni Hash più utilizzate sono:

- MD4 (Message Digest 4);

- MD5 (Message Digest 5);
- SHA (Secure Hash Algoritm).

Quello che ci interessa è l'algoritmo SHA:

- L'algoritmo SHA è stato sviluppato dalla NSA (National Security Agency) e le specifiche sono state pubblicate dal NIST (National Institute of Standards and Technology) nel 1993. Questa versione è nota come SHA-0.
- Nel 1995 è stata pubblicata una nuova versione, nota come SHA-1.

- Nel 2001 sono state pubblicate quattro funzioni: SHA-224, SHA-256, SHA-384 e SHA-512. Queste funzioni sono spesso indicate come SHA-2.

Le principali proprietà degli algoritmi SHA sono riassunte nella Tabella 1.2.

TABELLA 1.2 – Proprietà degli algoritmi SHA.

Algoritmo	Messaggio	Blocco	Parola	Digest	Sicurezza
SHA-1	$<2^{64}$ bit	512 bit	32 bit	160 bit	80 bit
SHA-256	$<2^{64}$ bit	512 bit	32 bit	256 bit	128 bit
SHA-384	$<2^{64}$ bit	1024 bit	64 bit	384 bit	192 bit
SHA-512	$<2^{64}$ bit	1024 bit	64 bit	512 bit	256 bit

Nel sistema Bitcoin viene utilizzato l'algoritmo SHA-256, che è in grado di processare messaggi con dimensione inferiore a 264 bit, in blocchi da 512 bit,

ognuno formato da 16 parole da 32 bit. Questo algoritmo restituisce un Digest a 256 bit.

Di seguito analizziamo un esempio pratico che sicuramente vi chiarirà questi concetti. Se prendiamo il nostro messaggio (“compra cento bitcoin”) e applichiamo la funzione SHA-256 (dal sito www.hashemall.com) otteniamo il seguente codice Hash:

```
5335C303E0981E00317EC53582DE99D9
```

Si tratta di un codice alfanumerico di 64 caratteri, che identifica in modo univoco il messaggio. E infatti se sostituiamo solo una lettera (“compro cento bitcoin”) otteniamo un codice Hash completamente diverso, in accordo con

il principio di “Effetto valanga”:

AE6DBD264B706DDCF3E98052E65C417DI

FIRME DIGITALI

La crittografia e le funzioni Hash trovano applicazione nel campo delle firme digitali. Analizziamo quindi come funziona la firma digitale.

Il mittente (A) applica una funzione Hash sul messaggio da inviare, ottenendo un Digest che cifra usando la propria chiave privata. Si ottiene in questo modo la firma, che è in sostanza il Digest crittografato. Il documento e la

firma vengono inviati al destinatario (B) (Figura 1.8).

Quando il destinatario riceve il messaggio, lo separa in documento originale e firma digitale. Essendo in possesso della chiave pubblica del mittente è in grado di decifrare la firma digitale ottenendo il Digest, applica poi al documento originale la medesima funzione Hash, utilizzata dal mittente, e se questa produce un Digest uguale a quello che ha appena decifrato allora ha la garanzia che il messaggio è integro e autentico (Figura 1.9).

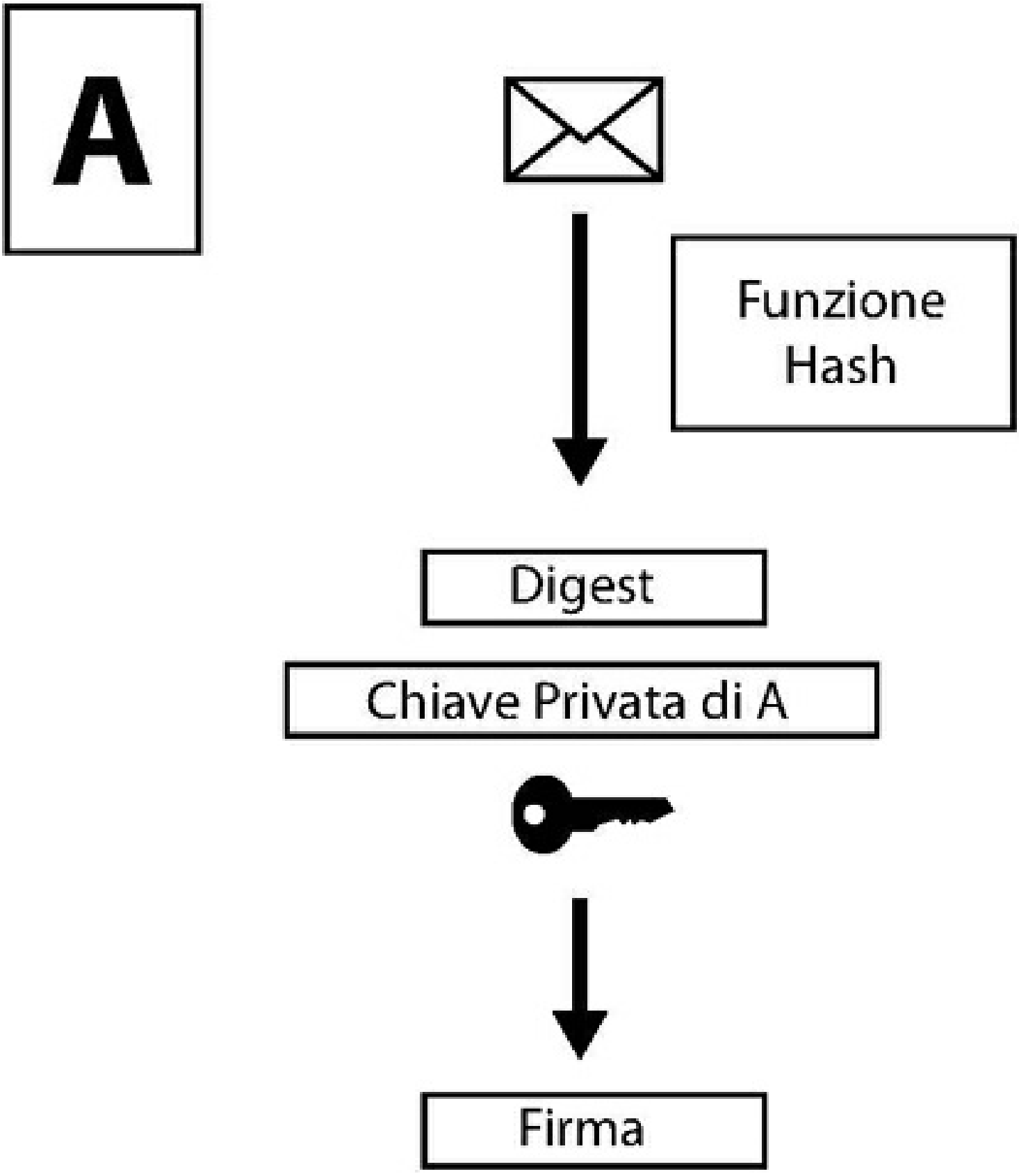


FIGURA 1.8 – Funzione Hash e chiave privata.

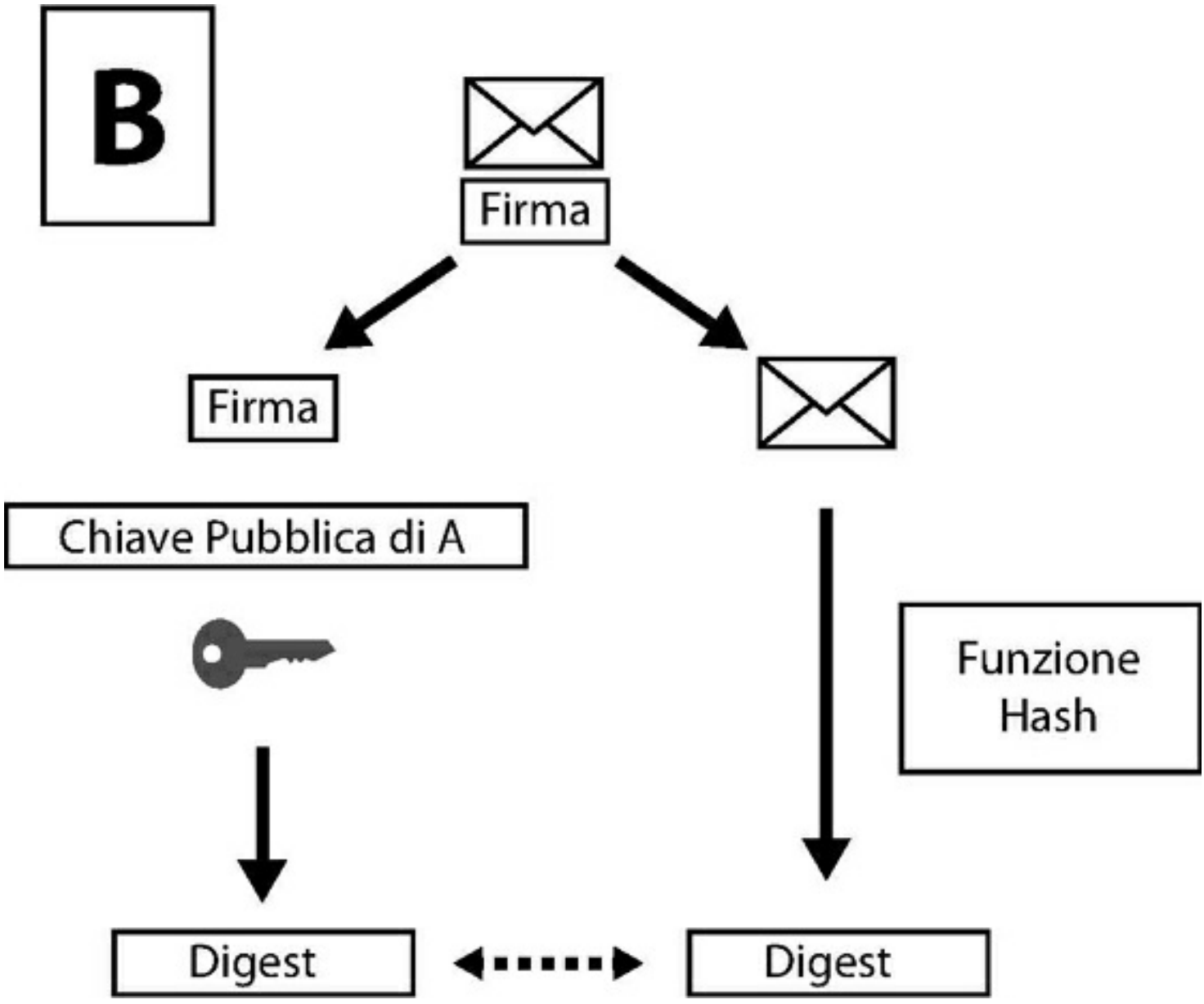


FIGURA 1.9 – Schema di funzionamento firme digitali.

Perché abbiamo parlato di crittografia, funzioni Hash e firma digitale? Proseguendo nel corso della lettura ne

capirete il motivo e tutto vi sarà più chiaro.

BLOCKCHAIN

Per comprendere la struttura e il funzionamento del sistema Bitcoin, dobbiamo introdurre il concetto di Blockchain. Questo non è altro che un registro pubblico di tutte le transazioni in Bitcoin e queste sono contenute in blocchi ordinati cronologicamente. La traduzione di Blockchain è, infatti, "catena di blocchi", questo perché ogni blocco che la compone è, per costruzione, collegato con il precedente.

È chiaro che se ogni blocco ha un legame con quello precedente, di conseguenza è possibile svolgere un percorso a ritroso. Partendo dall'ultimo blocco generato, si può risalire la catena fino ad arrivare al numero 0, cioè il "Genesis Block", nato alle ore 18:15:05 del 3 gennaio 2009 (Figura 1.10).

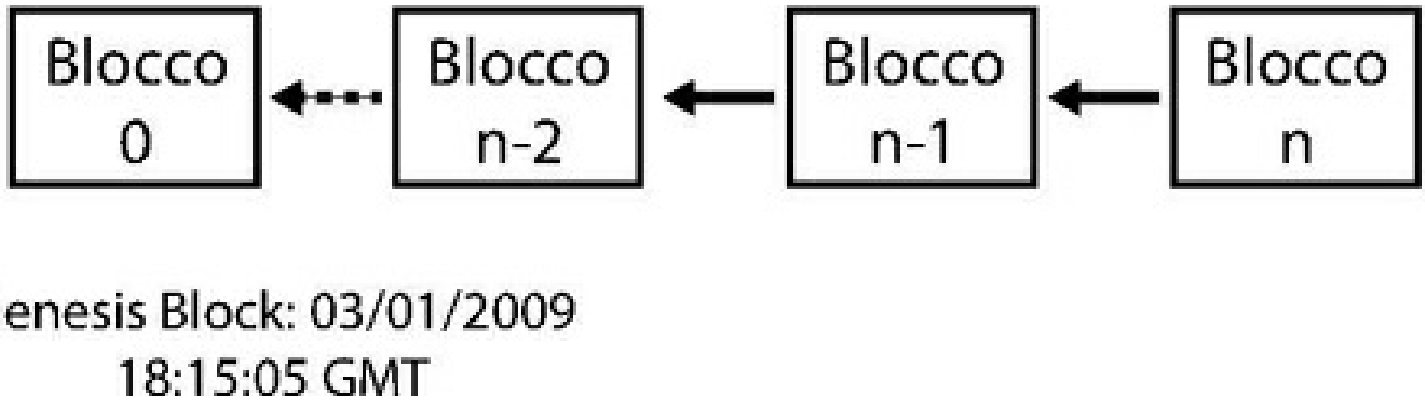


FIGURA 1.10 – Genesis Block.

Da un punto di vista informatico, il Blockchain si definisce come un database memorizzato e distribuito su

ogni macchina che fa parte del network Bitcoin. La sua dimensione, espressa in MB, è in continua crescita, come mostra la Figura 1.11.

Logicamente il Blockchain comprende i vari blocchi e tutte le transazioni, come mostrato nello schema logico della Figura 1.12:

Procediamo analizzando le sottocomponenti del Blockchain.

Il concetto di Blocco

A questo punto nasce immediatamente una domanda: che cos'è esattamente un blocco? Non è altro che un file in cui sono contenute una serie di informazioni,

di cui le più importanti sono:

- numero del blocco: i blocchi sono numerati in modo crescente, a partire dallo 0;
- codice Hash: ogni blocco è identificato in maniera univoca da un certo codice alfanumerico;

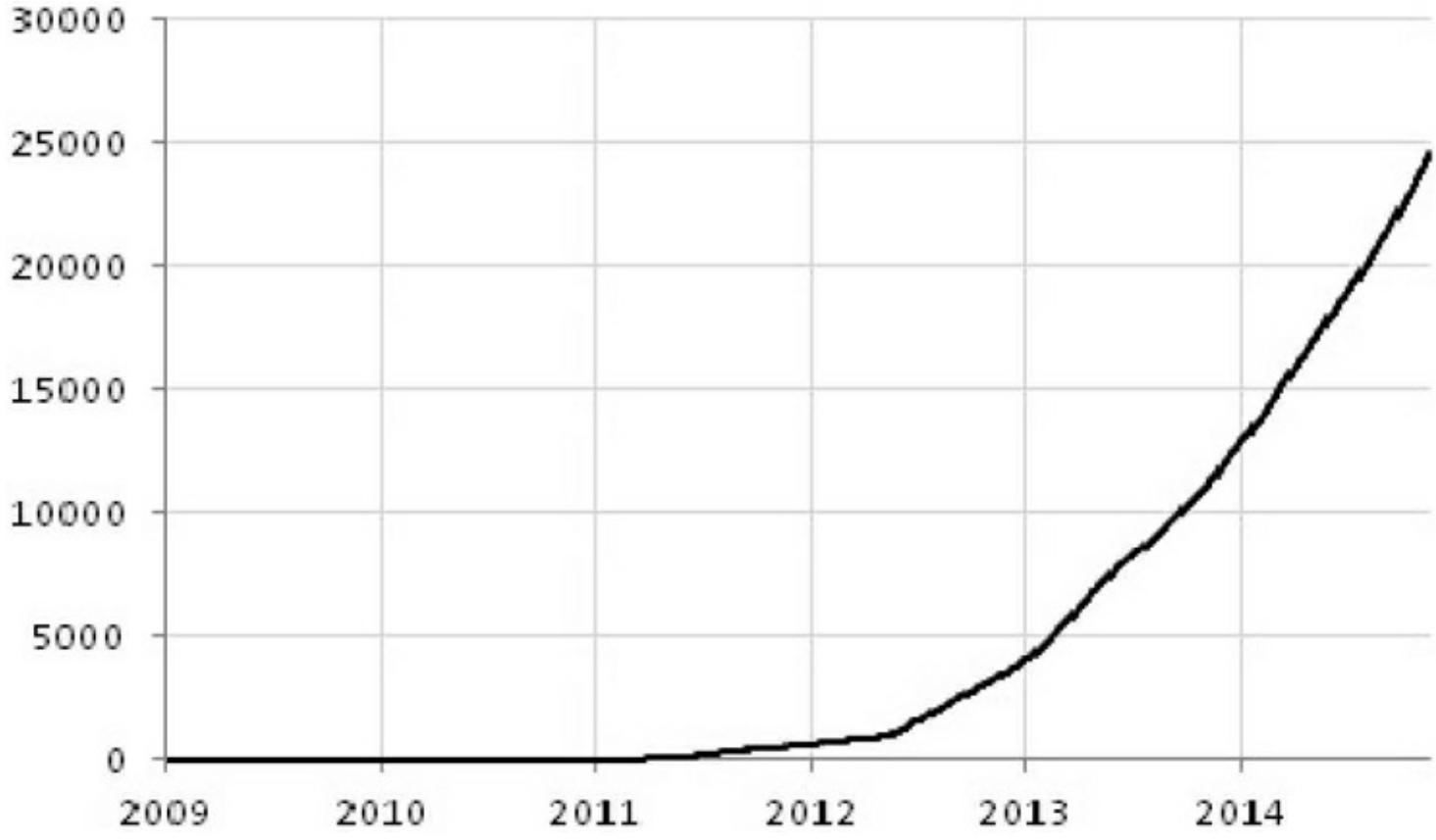


FIGURA 1.11 – Dimensione Blockchain in MB.

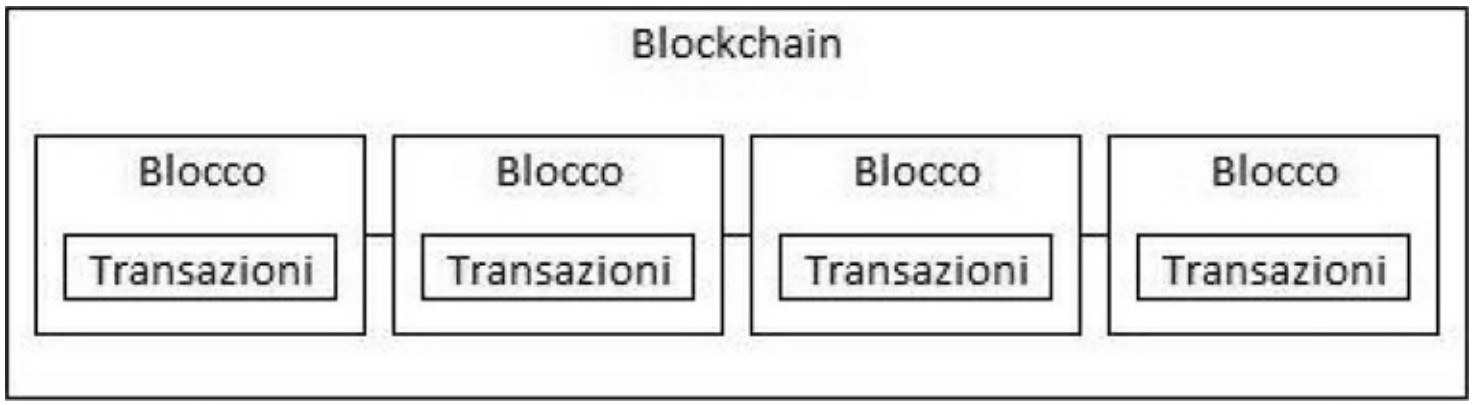


FIGURA 1.12 – Schema logico Blockchain.

- data e ora in cui il blocco è stato prodotto;
- tutte le transazioni confermate nel blocco;
- totale dei bitcoin movimentati all'interno del blocco;
- dimensione (in kiloByte) del blocco.

Il grafico della Figura 1.13 mostra la dimensione media dei blocchi espressa in MB.

Come sappiamo, un blocco è un contenitore di un certo numero di transazioni. Di conseguenza un aumento della dimensione media dei blocchi significa, indirettamente, che sono in aumento le transazioni contenute al loro

interno, come in effetti ci conferma la Figura 1.14.

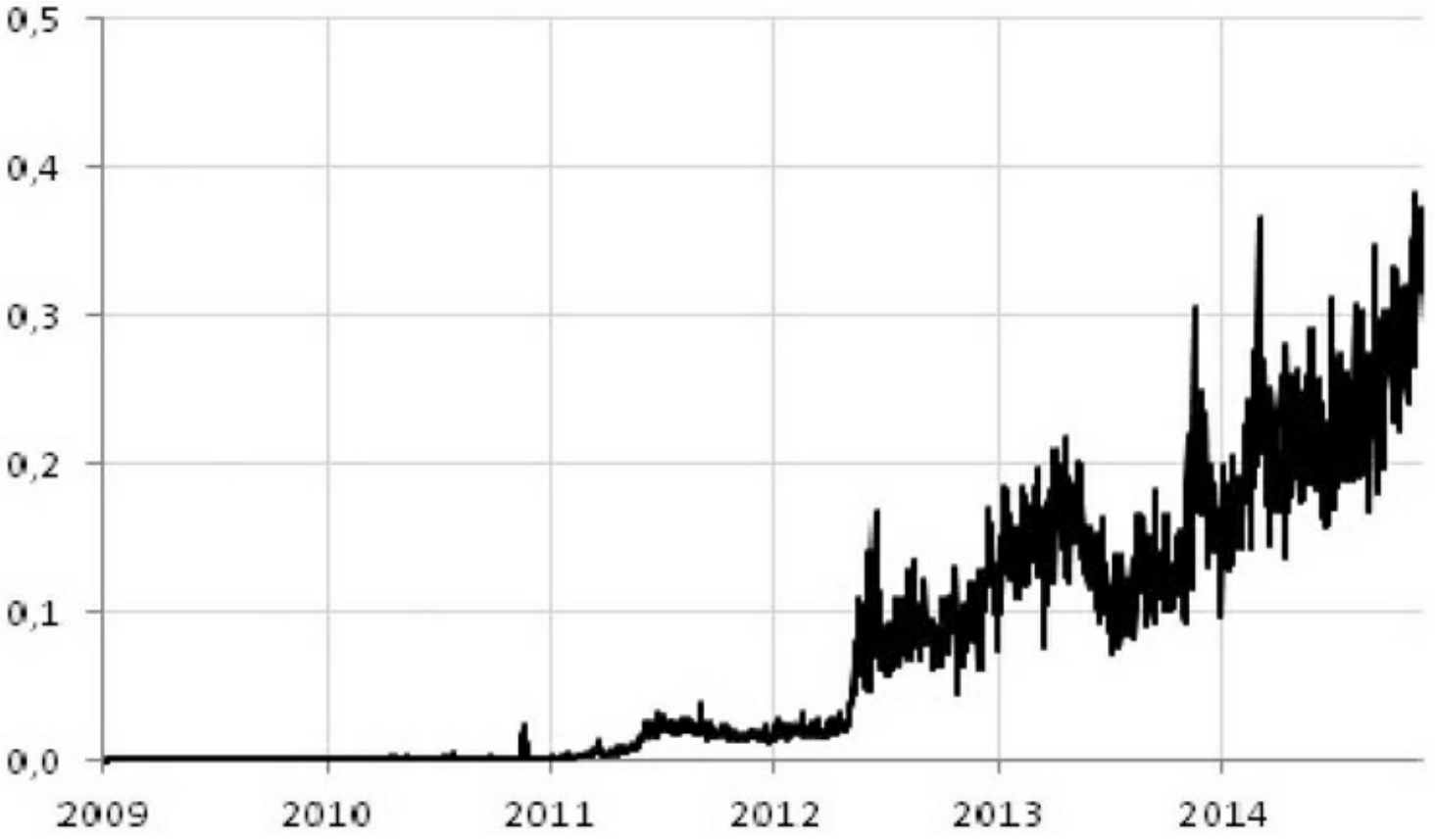


FIGURA 1.13 – Dimensione media di un blocco.

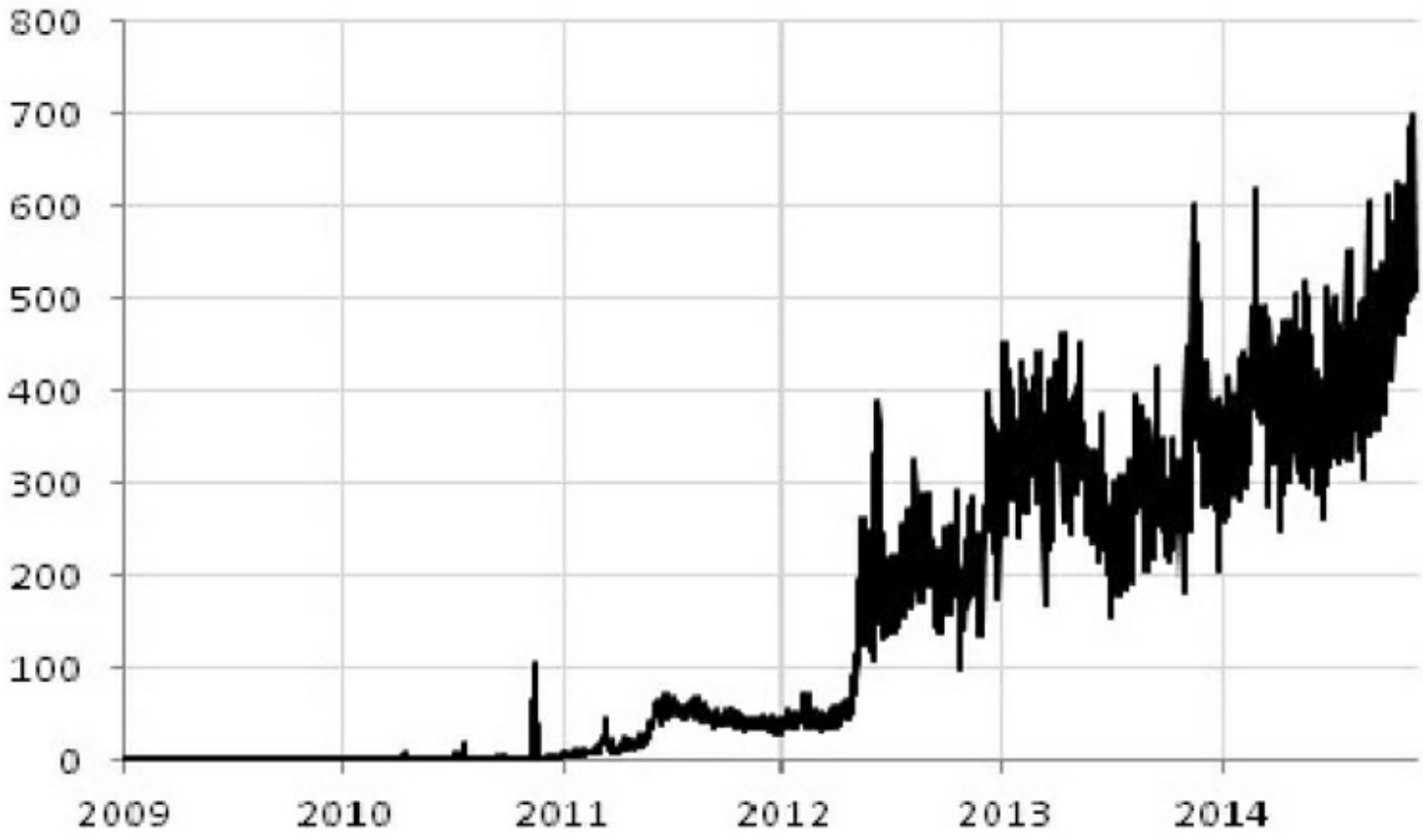


FIGURA 1.14 – Numero transazioni in un blocco.

Il blocco 0

Cercheremo ora di fornirvi tutte le informazioni per comprendere come è costruito un blocco.

A titolo di esempio, alla data del 30 giugno 2014 è stato prodotto il blocco numero 308671 alle ore 23:40:28, contenente 216 transazioni per un totale di 246,84692826 bitcoin.

Come già detto, ogni blocco è collegato al precedente e dunque dal blocco 308671 possiamo risalire al blocco 308670, quindi al blocco 308669… fino ad arrivare al blocco 0.

Studiare il blocco 0 ci fornirà tutti gli elementi per poter poi analizzare qualunque altro blocco a cui potessimo essere interessati.

Vediamo dunque il DNA del blocco 0, consultabile all'indirizzo internet: http://blockexplorer.com/block/0

```
Hash:
000000000019d6689c085ae165831e93
Next                                block:
00000000839a8e6886ab5951d76f4114
Time: 2009-01-03 18:15:05
Transactions: 1
Total BTC: 50
Size: 285 bytes
Merkle                               root:
4a5e1e4baab89f3a32518a88c31bc87f
Nonce: 2083236893
```

Nel DNA del blocco sono contenute tutte le informazioni genetiche che lo caratterizzano. Nello specifico, il blocco 0 è nato alle ore 18:15:05 del 3 gennaio 2009, ha un certo codice Hash composto da numeri e lettere, ha una dimensione di 285 bytes e contiene una sola transazione per un totale di 50

Bitcoin.

A loro volta ogni transazione è composta da una serie di informazioni, tra cui:

- ora dell'invio;
- importo in bitcoin (BTC);
- indirizzo di provenienza;
- indirizzo di destinazione;
- dati della transazione precedente.

Le transazioni sono mappate e identificate da un codice alfanumerico e quella relativa al blocco 0 è consultabile all'indirizzo internet: http://blockexplorer.com/tx/4a5e1

Riportiamo per completezza tutti i dati della transazione contenuta nel

blocco 0:

```
Transaction:
4a5e1e4baab89f3a32518a88c31bc87f
Appeared in Block 0 (2009-01-03
18:15:05)
Fee: 0
Sice (kB): 0,204
From (amount): Generation: 50 +
0 total fees
To                          (amount):
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfN
50
```

Inoltre, la transazione ha un input e un output, i quali rispettivamente ci dicono da dove arrivano i bitcoin e verso dove sono diretti. Di seguito sono elencate le caratteristiche degli input e degli output della transazione che stiamo

analizzando:

Input:

```
Previous output (index): N/A
Amount: 50 + fee
From address: N/A
Type: generation
ScriptSig:
04ffff001d0104455468652054696d65
```

Output:

```
Index: 0
Redeemed at input: Not yet
redeemed
Amount: 50
To address:
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfN
Type: Pubkey
ScriptPubKey:
04678afdb0fe5548271967f1a67130b7
b649f6bc3f4ce
```

f38c4f35504e51ec112de5c384df7ba0b

Sappiamo che, dopo aver generato i primi 50 bitcoin, Satoshi Nakamoto li ha trasferiti all'indirizzo 1A1zP1eP5QGefi2DMPTfTL5SLmv7Div che identifica in modo univoco un certo portafoglio (wallet).[1] Questa è nota come transazione di generazione (o *Coinbase Transaction*) ed è la prima operazione che compare in ogni blocco. Si tratta della ricompensa ottenuta dai minatori per aver risolto il problema matematico contenuto nel blocco stesso.

La quantità assegnata in ogni blocco è 50 bitcoin, ma si dimezza ogni 210.000 blocchi. Quindi, nel blocco attuale (numero 308671)[2] vengono

assegnati 25 bitcoin. Le informazioni di questo blocco si possono consultare al seguente indirizzo: http://blockexplorer.com/block/0(

Eccole qui riportate:

```
Hash:
000000000000003fd81437deee6d94(
Previousblock:000000000000000304
Next block:
000000000000003cd0095dd3f8ab067
07651c13bc9d
Time: 2014-06-30 23:40:28
Difficulty: 16 818 461
371,161111 (“Bits”: 18415fd1)
Transactions: 216
Total BTC: 246,84692826
Size: 109.538 kiloBytes
Merkle root:
d70057cffbee21d66e24d933f8107fb64
Nonce: 1256580202
```

SCRIPT

Procediamo prendendo in esame lo ScriptSig e lo ScriptPubKey. Dal codice che abbiamo esposto in precedenza, si evince come ScriptSig e ScriptPubKey siano rispettivamente degli elementi identificativi dell'input e dell'output. Sono infatti codici alfanumerici e, nello specifico, il primo è la prima metà dello script mentre il secondo è la seconda metà dello script.

La domanda ora è: cos'è lo script? In estrema sintesi, si tratta di un linguaggio che accompagna le transazioni in modo da istruire i nodi su che cosa fare dei pacchetti per

realizzare operazioni più complesse del semplice trasferimento.

Lo Script si compone di due elementi:

- signature (Firma digitale),
- public key (Chiave pubblica);

La chiave pubblica appartiene al beneficiario dell'output della transazione, così da permettergli di riscattare il valore di moneta contenuto nell'output.

L'altra componente è la firma dell'Hash. Questa, combinata con la chiave pubblica, dimostra che la transazione è stata eseguita dal legittimo

proprietario dell'indirizzo in oggetto.

In sintesi, il sistema Bitcoin prevede di inviare una transazione con uno script che può essere risolto esclusivamente con una specifica chiave privata, cioè attraverso l'uso della chiave pubblica usata per creare lo script.

WALLET

Tradizionalmente quando pensiamo a un *wallet* siamo portati a pensare a un posto dove sia possibile tenere o conservare moneta. Tuttavia, data la natura del Bitcoin, organizzato con un sistema di Blockchain, è impossibile

pensare a questa valuta come un'entità separata dalla catena di transazioni che lo hanno generato. Quindi, la definizione migliore di wallet è: "Un portafoglio elettronico che memorizza tutte le credenziali digitali per accedere, spendere e trasferire i bitcoin." Sappiamo bene che tutto l'universo Bitcoin si appoggia sulle due fondamentali chiavi di accesso, quella pubblica e quella privata; quindi, il wallet è il luogo elettronico dove tali chiavi vengono conservate.

Esistono anche altre tre tipologie di wallet:

- desktop wallet: è un client che si

installa sul proprio computer;

- smartphone wallet: è un'app che permette di effettuare e ricevere pagamenti in mobilità;
- web wallet: è un account che permette di accedere al wallet dal proprio browser.

Tutte queste tipologie ovviamente hanno un rischio legato sia alla sicurezza del mezzo fisico (furto dello smartphone o del PC) sia a quella informatica. Per completezza di informazioni, presentiamo il più sicuro di tutti i wallet. Con il termine *Cold Storage* si definisce una riserva di bitcoin presenti su un wallet creato e mantenuto offline, come per esempio su una penna USB o

su un foglio di carta. Questo rappresenta il sistema di protezione più efficiente nell'ambiente delle cryptovalute: per esempio, qualora il PC di un utente fosse soggetto a un attacco hacker, tale intrusione non produrrebbe risultati significativi a favore del "ladro" in quanto le chiavi private di accesso al wallet dell'utente non sarebbero più presenti su quel dispositivo o sul server, ma sarebbero al sicuro *offline*.

Mediante il *Cold Storage* i rischi si riducono a quelli impliciti nella conservazione di ogni bene fisico di valore, per esempio dove collocare le chiavette USB e come assicurarsi che nessuno, tranne i proprietari, ne abbia accesso.

NETWORK

Tutti i dati relativi ai blocchi e al Blockchain sono memorizzati e distribuiti sulle macchine che partecipano al network Bitcoin. Tuttavia, se non si è un attore attivo nei nodi del network Bitcoin, è comunque possibile consultare le informazioni contenute nel Blockchain al sito http://blockexplorer.com. Le macchine che ne fanno parte sono organizzate in nodi secondo una rete distribuita, decentralizzata e paritaria (P2P = peer-

to-peer). Con questo tipo di configurazione, ogni nodo è in grado di comunicare direttamente con gli altri senza dover passare da un server centrale.

L'architettura peer-to-peer si distingue da quella Client/Server, usata per esempio per i servizi di posta elettronica o dei domini internet. La Figura 1.15 chiarisce meglio le differenze tra queste due strutture.

Nel Client/Server è chiaro come l'architettura preveda l'esistenza di due soggetti:

- client: usufruisce del servizio offerto dal server;

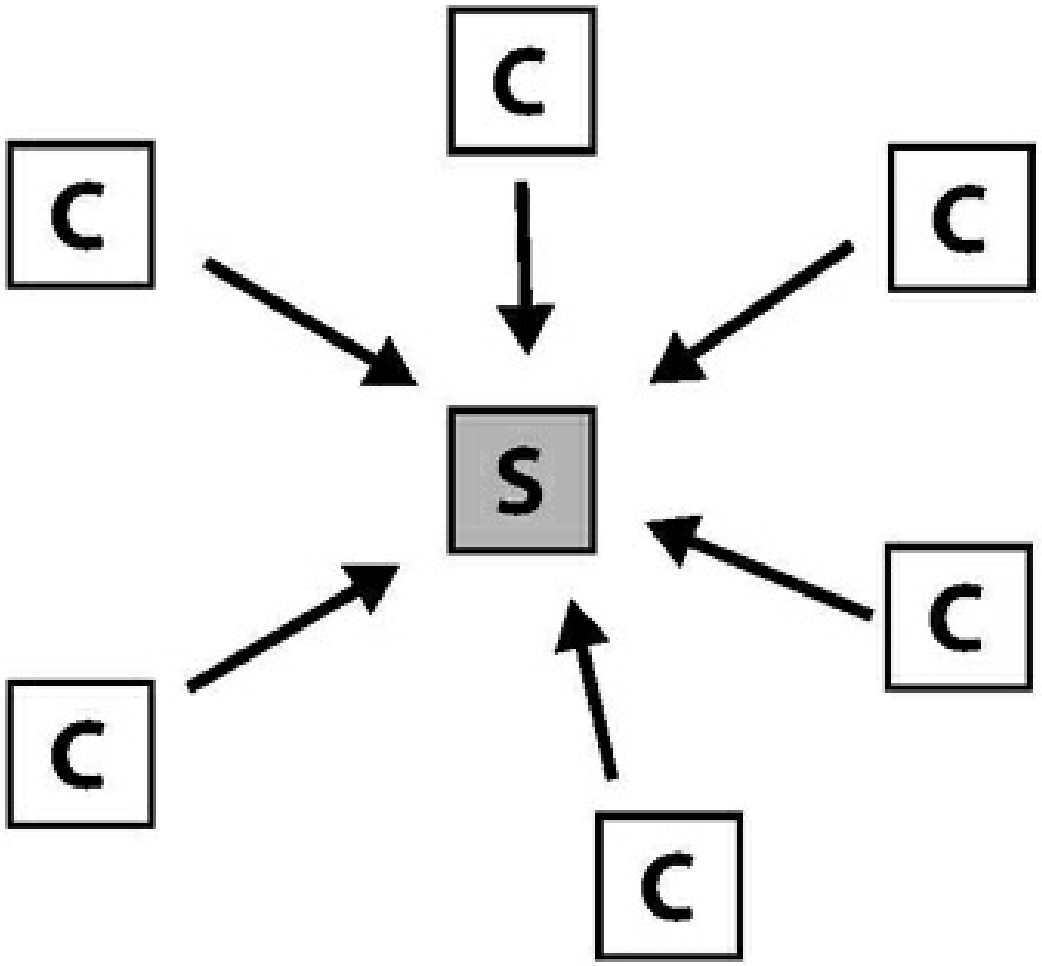
- server: mette a disposizione un servizio con lo scopo di soddisfare le richieste del client.

Si tratta di un sistema centralizzato, che è in netto contrasto con la natura distribuita di un sistema peer-to-peer, in cui tutti i soggetti che lo compongono sono paritari, cioè funzionano sia come client che come server. La decentralizzazione conferisce al modello P2P alcune importanti proprietà:

- scalabilità;
- condivisione e riduzione dei costi;
- disponibilità del servizio;

- autonomia;
- anonimato.

Tuttavia, il principale svantaggio è legato alla sicurezza del network stesso e si tratta di un fatto non irrilevante, che deve essere sempre tenuto in debita considerazione.


C
C
C
S
C
C
C

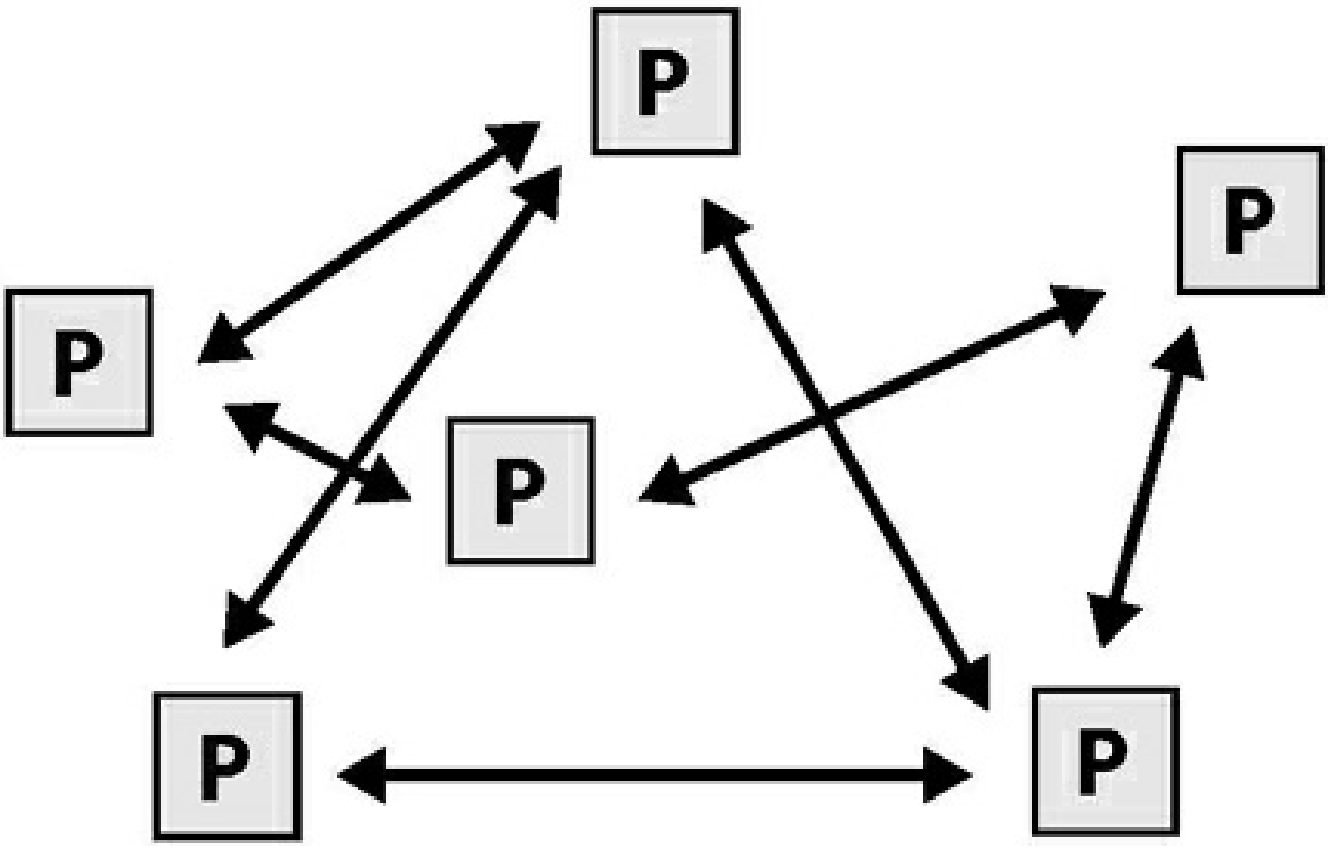

P
P
P
P
P
P
P

FIGURA 1.15 – Confronto rete Client/Server (sopra) e P2P (sotto).

TRANSAZIONI

Satoshi Nakamoto ha proposto un sistema di pagamento elettronico basato su prove di crittografia, invece che di fiducia, permettendo alle parti di negoziare direttamente tra loro senza bisogno di un soggetto terzo. Questo è un punto di rottura significativo rispetto all'architettura dei tradizionali sistemi di pagamento.

Ogni volta che effettuiamo un acquisto, utilizzando per esempio la

nostra carta di credito, abbiamo bisogno di una terza parte fidata, cioè un intermediario che si interpone tra noi e il venditore. L'intermediario svolge un lavoro di garanzia e di mediazione in caso di eventuali controversie tra compratore e venditore. Vale la pena di ricordare che il costo della mediazione è oneroso e intrinseco nel prezzo di ogni singola transazione. Di conseguenza, dal punto di vista economico, risulta essere un ostacolo per le transazioni, soprattutto per quelle di piccolo importo.

Facciamo un esempio: PayPal è tra gli strumenti di pagamento più utilizzati su Internet, ma per questo motivo è vantaggioso ed economico? Non

proprio. La tariffa standard per la ricezione di pagamenti per beni e servizi è pari al 3,4% dell'importo, questa tende poi a decrescere in caso di aumento dell'importo della transazione, ma la percentuale resta comunque elevata. L'utilizzo dei bitcoin tende a ridurre drasticamente i costi delle transazioni,[3] con ovvi benefici per l'economia di scambio.

Bisogna prendere in considerazione vari aspetti, uno su tutti: le transazioni sono irreversibili. A tal proposito, va distinta la posizione del mittente (compratore di beni o servizi) dal destinatario (venditore di beni o servizi):

- Il mittente deve accertarsi che l'indirizzo (*address*) presso cui si desidera inviare bitcoin sia corretto. In caso di errore, la transazione non può essere richiamata, e quindi l'unico modo per vedersi riaccreditare le somme trasferite è tramite una nuova transazione da parte del destinatario.
- Il destinatario deve avere la garanzia che i soldi non siano stati già spesi (*double-spending*).[4]

In quest'ultimo caso, una soluzione comune al fine di tutelare il destinatario

è quella di introdurre un'autorità centrale, come per esempio una Zecca, che controlli ogni transazione ed eviti così il *double-spending*. Con una siffatta struttura, dopo ogni transazione, la moneta deve essere restituita a questo istituto in modo che esso possa emettere nuova moneta. Solo le nuove emissioni danno la garanzia che le monete non siano state già spese. Questa soluzione, però, presenta un fattore di criticità: il destino dell'intero sistema monetario dipende dalla società che gestisce la Zecca, che nei sistemi economici moderni è lo Stato. Ma con il Bitcoin si vuole proprio scardinare questo sistema.

L'unico modo per confermare l'inesistenza di una transazione è quello

di essere a conoscenza di tutte le transazioni. Nel modello che abbiamo appena esposto, la Zecca è a conoscenza di tutte le transazioni e di quale le sia stata consegnata per prima. La prima transazione consegnata con una determinata moneta è ovviamente garantita dalla Zecca come prima transazione con quella specifica moneta. Di conseguenza, eventuali altre transazioni eseguite con la stessa moneta non sono accettate.

Nel mondo Bitcoin si vuole evitare la presenza di una terza parte di fiducia e al tempo stesso garantire la doppia spesa. Per poter raggiungere questo obiettivo le transazioni devono essere

annunciate pubblicamente, c'è quindi bisogno di un network di partecipanti al fine di confermare l'ordine delle varie transazioni. In sostanza il network, che abbiamo presentato nel paragrafo precedente, deve confermare al beneficiario della transazione che, al momento in cui la stessa è avvenuta, la maggioranza dei nodi è concorde nel confermare che si tratti del primo ricevente.

Cerchiamo ora di analizzare i passaggi necessari al fine di poter effettuare una transazione. Ipotizziamo di voler acquistare un certo bene e che il venditore sia disposto ad accettare i bitcoin come forma di pagamento. Quello che dobbiamo fare è inviare una

transazione verso l'indirizzo che identifica il portafoglio di proprietà del beneficiario. All'interno dei wallet è contenuta una chiave privata che serve per firmare le transazioni e fornire una prova crittografica della loro provenienza. Ogni proprietario di bitcoin che intenda trasferire le sue monete ad altro proprietario non fa altro che firmare, con firma digitale, l'Hash della precedente transazione e aggiungere la chiave pubblica del nuovo proprietario. Successivamente, la transazione passa nel network Bitcoin e, attraverso la rete peer-to-peer, il resto dei nodi valida le firme crittografiche.

La transazione così svolta è:

- irreversibile. Una volta che la transazione è stata effettuata non è più possibile annullarla;
- pubblica. La transazione viene processata dal network Bitcoin e, se confermata, entra di diritto nel Blockchain, diventando consultabile da chiunque;
- anonima per le parti che l'hanno eseguita. Le parti possono anche non conoscersi e non essersi mai incontrate. Quello che è noto è solo l'indirizzo di partenza e di arrivo della transazione.

Vediamo un esempio reale di transazione eseguibile con uno dei molti

wallet virtuali disponibili.[5]

Partiamo con la transazione in uscita che potete vedere in Figura 1.16.

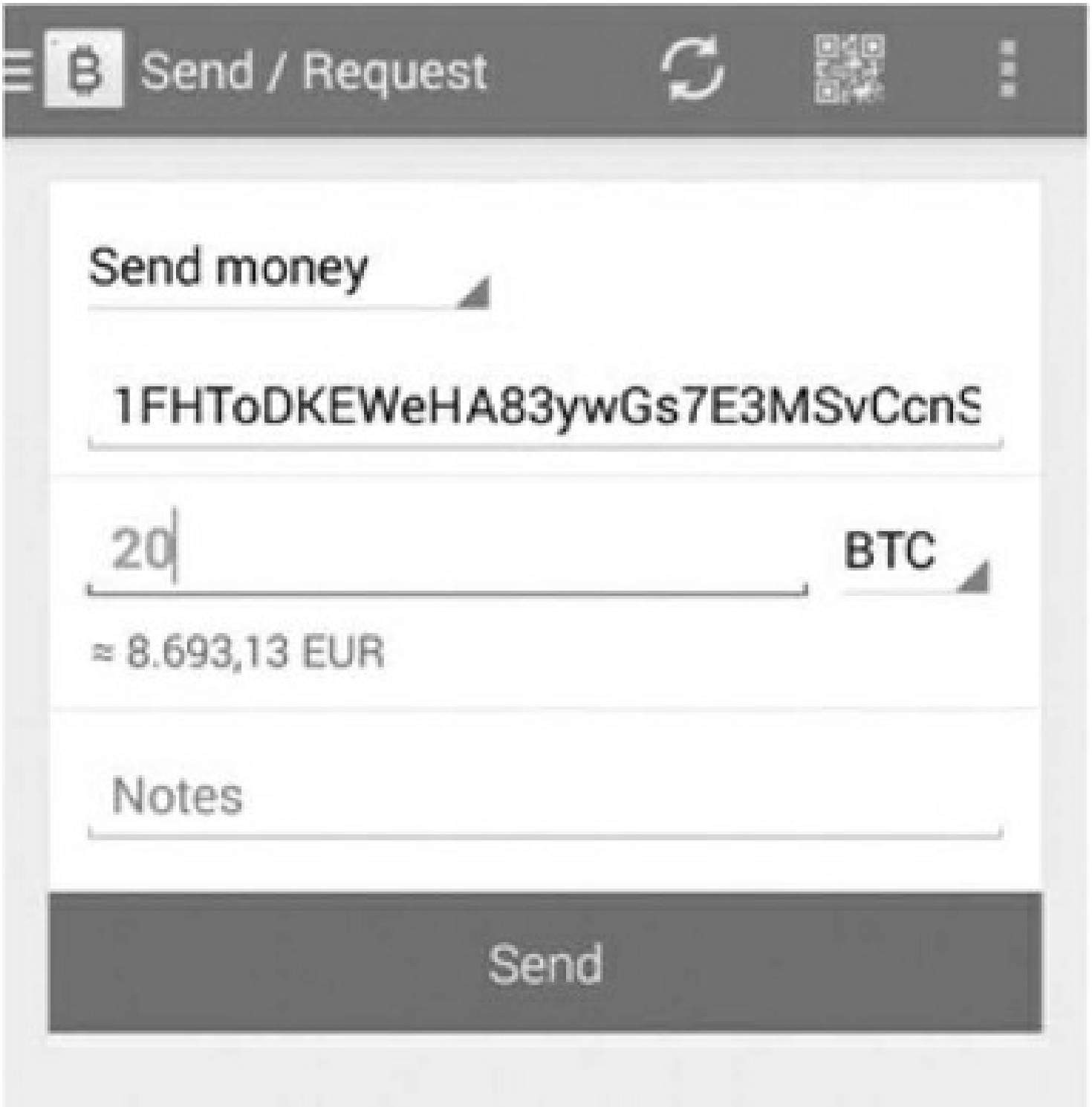


FIGURA 1.16 – Transazione in uscita.

È necessario inserire l'indirizzo (address) del destinatario che si compone di un codice alfanumerico,[6] l'importo da versare (20 BTC dell'esempio), che viene anche visualizzato nella "valuta *fiat*"[7] preferita (euro), e poi, premendo semplicemente il tasto "Send", la transazione viene effettuata. Da questo momento il network si prenderà cura di validare la transazione attraverso il processo di mining.[8]

Vediamo ora la transazione in entrata della Figura 1.17.

Dovunque vi troviate è sufficiente

avere con sé lo smartphone per poter ricevere un qualsiasi pagamento. Si seleziona l'importo da ricevere (15,25869 BTC dell'esempio), la tecnologia di scambio[9] e, dopo aver ricevuto l'autorizzazione del cliente, in pochi minuti si vedrà accreditato l'importo richiesto sul proprio wallet.

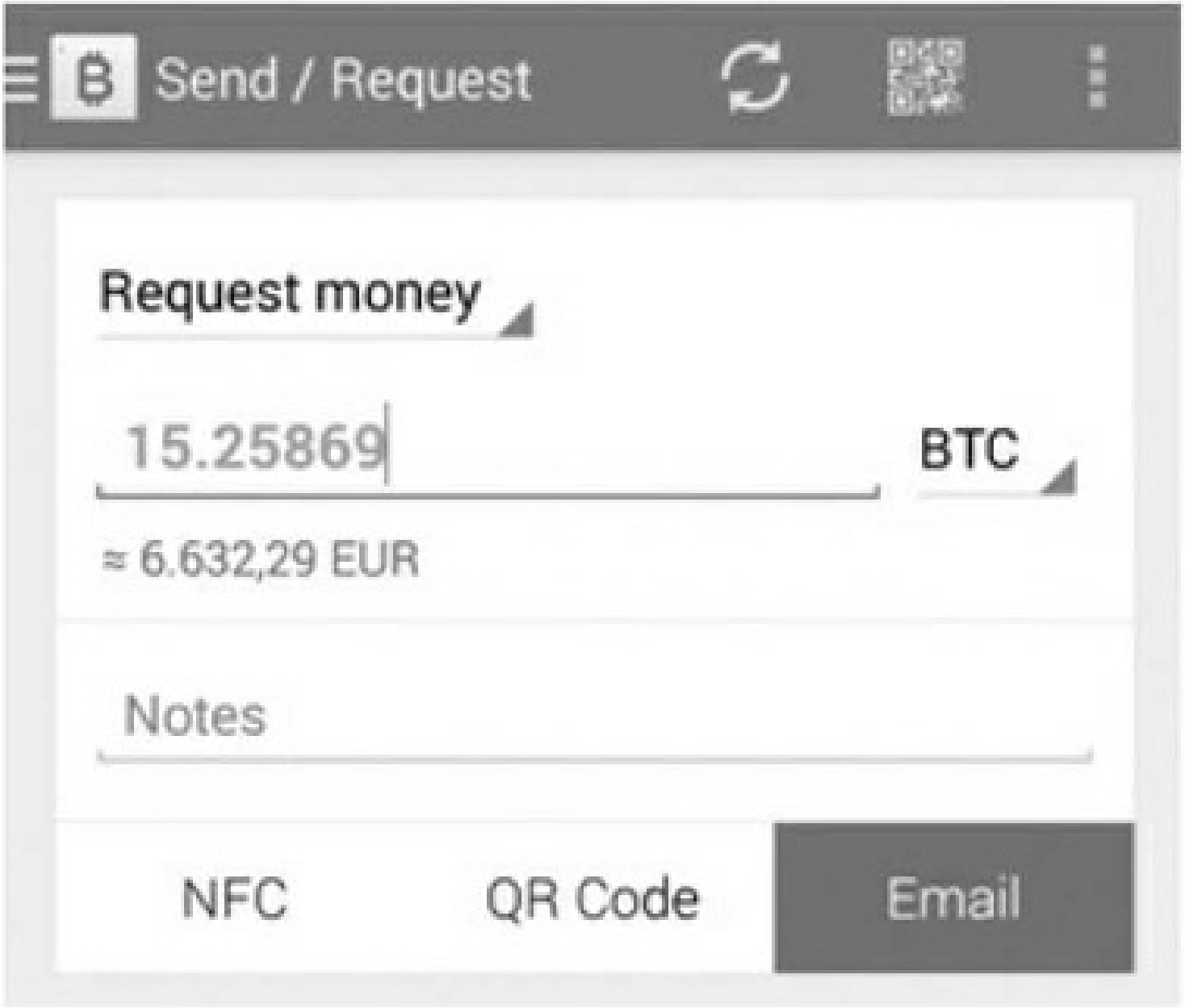


FIGURA 1.17 – Transazione in entrata.

MONETA

Le transazioni che abbiamo appena mostrato hanno come oggetto di scambio il bitcoin, ma a questo punto è importante fermarsi un secondo ponendosi una domanda critica: *fino a ora abbiamo parlato sempre di bitcoin come se fosse una moneta, ma è vero*? Cerchiamo in questa sezione del libro di comprendere meglio il concetto di moneta e di valutare se il bitcoin ne presenta le caratteristiche.

In economia con il termine moneta si definisce l'insieme dei valori che vengono utilizzati in modo regolare dagli individui per acquistare beni e servizi. All'interno del sistema economico, la moneta svolge tre

funzioni:

- mezzo di scambio;
- unità di conto;
- riserva di valore.

La moneta, intesa come mezzo di scambio, è quanto il compratore dà al venditore nel momento in cui acquista un bene o un servizio. Come unità di conto è il parametro con cui si misurano e confrontano valori economici. Come riserva di valore permette agli individui di trasferire potere di acquisto dal presente al futuro.

La moneta può essere di due tipi:

- moneta merce;
- moneta a corso legale.

La prima è una forma materiale di moneta, rappresentata da un bene dotato di un proprio valore intrinseco. Un esempio è l'oro, il quale presenta un proprio valore intrinseco a prescindere dal fatto che possa essere utilizzato in questa funzione.

Quella priva di valore intrinseco è detta invece moneta a corso legale (o "moneta *fiat*") ed è considerata moneta per decreto del legislatore. Il valore di questa è fissato da un'autorità, cioè lo Stato, che ne garantisce stabilità e riconoscimento come mezzo di pagamento.

Come si pone il bitcoin in questa distinzione? Sulla base di quanto abbiamo scritto, il bitcoin non è una moneta merce, poiché è privo di un proprio valore intrinseco, e al tempo stesso non è una moneta a corso legale, poiché non è stata imposta e non è controllata da un'autorità centrale.

Quindi possiamo sentenziare che il bitcoin non è una moneta? Esatto. Secondo i canoni tradizionali dell'economia, il bitcoin difficilmente potrà essere considerato una moneta. Tuttavia, la definizione di moneta offre maggiori sfaccettature. In questo senso, se il bitcoin venisse utilizzato in modo regolare nelle transazioni per acquistare

beni e servizi, allora avrebbe tutti i carismi di una moneta. Considerando anche il fatto che già ora il bitcoin svolge le tre funzioni essenziali di una moneta:

- mezzo di scambio;
- unità di conto;
- riserva di valore.

In economia, per indicare l'insieme delle concezioni riguardanti la genesi e la determinazione del valore si parla della cosiddetta "teoria del valore": il valore è una proprietà delle merci distinta e logicamente antecedente rispetto al prezzo, che invece ne

costituisce in tale ottica la manifestazione fenomenica. Da tempo l'economia si interroga da dove derivi il valore e ancora non si è arrivati a una risposta univoca: si va dalla scarsità dei beni disponibili alla loro utilità, alla necessità di remunerare i fattori produttivi, includendovi il capitale e considerando la sua remunerazione e così via.

La scuola di pensiero che più di tutte ha analizzato la teoria del valore è quella austriaca, il cui punto di partenza è l'individuo: soggetto pensante, dotato di conoscenze, che agisce in vista di un fine. L'azione umana, secondo tale scuola, è un comportamento dotato di senso, comprensibile in quanto avente

uno scopo, ed è il mattone fondamentale dell'intera realtà sociale. La generalità di questo approccio è tale da consentire l'applicazione del metodo austriaco a qualunque sfera delle relazioni sociali, anche al di fuori dell'economia.

Ma cosa dà valore a un oggetto? Il suo essere in grado di realizzare un fine o la convinzione, di un individuo, che l'oggetto sia utile al suo perseguimento. Una banconota ha valore perché può essere impiegata per comprare merci: in un'isola deserta non avrebbe alcun valore, perché non potrebbe avere alcuna funzione. L'acqua ha molto valore nel deserto, ma molto meno in una città servita da numerosi acquedotti.

Il valore è frutto di una valutazione soggettiva dell'adeguatezza del mezzo alla luce del fine perseguito. La moneta ha valore solo se esiste un mercato, una sigaretta ha valore solo per chi fuma e solo per chi ha un accendino, un'auto ha più valore se si abita in un luogo isolato e se non si hanno altri mezzi di trasporto. Tutti questi esempi mostrano che il valore è un qualcosa di attribuito agli "oggetti" visti come mezzi, cioè una valutazione soggettiva.

L'architettura del Bitcoin si sposa bene con la scuola austriaca, sia per questa concezione di valore sia per gli effetti che avrebbe sul sistema economico. Vediamo insieme il perché.

La teoria austriaca del ciclo

economico afferma che le banche centrali creano artificiosamente cicli economici attraverso l'utilizzo di politiche monetarie espansive e restrittive. Quando perseguono una politica espansiva generano un costante aumento dell'offerta di moneta (inflazione monetaria).

È possibile perseguire tale politica grazie al sistema monetario, detto *Fiat Currency*, cioè la moneta fiduciaria. Tale politica monetaria si caratterizza per la presenza di tassi di interesse tenuti artificiosamente bassi, che come conseguenza diretta producono una maggiore richiesta di investimenti, che in una situazione normale non sarebbero

stati effettuati e di conseguenza a una loro collocazione deficitaria e falsificata. Quando tale situazione diventa insostenibile, e si rende quindi necessaria una ricollocazione ottimale delle risorse, le banche centrali attuano una politica restrittiva, che va a diminuire artificiosamente l'offerta di moneta, porta a un aumento dei tassi di interesse e ha generalmente un effetto recessivo.

La risposta del bitcoin è legata al fatto stesso che l'offerta è limitata a 21 milioni e questo pone un argine immediato rendendo impossibile perseguire tali politiche e potrebbe quindi fornire una soluzione all'inflazione monetaria.

È singolare notare come il caso bitcoin presenti delle forti analogie con quanto avvenuto nel passato nell'isola di Yap. Il racconto è istruttivo e interessante per varie ragioni. Lo Stato di Yap è uno dei quattro Stati Federati di Micronesia, situato nell'Oceano Pacifico occidentale, che comprende numerose isole dell'arcipelago delle Caroline posizionate fra la Repubblica di Palau, Guam e Chuuk.

I suoi quasi 12.000 abitanti hanno scelto di utilizzare come moneta le pietre Rai, grandi dischi circolari scavati nel calcare. La dimensione delle pietre è molto variabile, le più grandi hanno un diametro di 3 metri, sono

spesse 0,5 metri e pesano 4 tonnellate.

Il valore estrinseco (percepito) di una specifica pietra si basa non solo sulla sua dimensione e sulle modalità di produzione, ma anche sulla sua storia. Per esempio, se sono morte molte persone durante il suo trasporto, allora il suo valore è elevato.

Le pietre Rai sono state utilizzate nelle transazioni sociali, come matrimoni, eredità, affari politici, alleanze, riscatto dei morti in battaglia o solo per uno scambio di cibo.

Molte si trovano di fronte a locali di riunione o su percorsi specifici. Anche se la proprietà di una particolare pietra cambia, la pietra stessa è spostata raramente. I nomi dei precedenti

proprietari sono tramandati a quello nuovo. L'aspetto interessante è che l'isola di Yap non si è mai trovata isolata rispetto alle valute straniere: in un primo tempo è entrato in circolazione il denaro spagnolo; poi venne quello tedesco, che lo sostituì rendendo inutile il primo; fu quindi la volta del denaro giapponese ed anche la moneta tedesca perse il suo valore... La "ruota" di Yap ha, invece, conservato il suo valore ed è, a oggi, ancora utilizzata come mezzo di scambio.

---

1. Il concetto wallet verrà analizzato più avanti nello stesso capitolo.
2. Al giugno 2014.

3. I costi di transazione li tratteremo nel paragrafo "Fee delle transazioni", più avanti.
4. Il *double spending* lo tratteremo nel paragrafo "Il problema del *double spending*".
5. In questo esempio abbiamo utilizzato l'app "Bitcoin Wallet".
6. Nel nostro esempio è 1FHToDKEWeHA83ywGs7E3MSvCcnS5sLgzl
7. Autorità, cioè moneta che deriva il suo valore essenzialmente da un'autorità e dalla fiducia della gente. È un valore fiduciario, cioè non determinato dal valore intrinseco di un materiale, quale per esempio l'oro e l'argento.
8. Il processo di mining è spiegato dettagliatamente nella parte 2 del libro.
9. NFC, scansione codice QR o semplice email.

PARTE II

Il Mining

L'attuale creazione di denaro

dal nulla, operata dal sistema bancario,
è identica alla creazione di moneta da parte dei falsari.
La sola differenza è che sono diversi coloro che ne traggono profitto.

Maurice Allais

CAPITOLO 2

Che cos’è il mining?

Intorno alla rete Bitcoin c'è molta diffidenza e incertezza. Infatti, questa affascinante tecnologia di generazione di moneta è criticata da più parti con affermazioni che la attaccano asserendone la sua insostenibilità da un punto di vista sociale, economico e ambientale. Tutte critiche che vedremo essere infondate. Ci proponiamo, infatti, di dimostrare la non veridicità di questo tipo di affermazioni andando a presentare un confronto per ordini di grandezza nei costi sostenuti per la produzione di Bitcoin rispetto alla produzione dell'oro, o al processo di stampa/coniazione di moneta fisica.

L'evidenza dei dati dimostrerà che

l'impatto sociale, ambientale ed economico nella produzione di Bitcoin è una frazione minima, se confrontati con le tradizionali tecnologie di creazione di moneta che tutti conosciamo.

Come avremo modo di approfondire anche in seguito, il mining di Bitcoin è alla base del network Bitcoin e ne rappresenta l'aspetto fondamentale che sorregge la struttura complessiva. Il processo di mining non solo verifica e registra tutte le transazioni, ma è anche l'attività capace di creare nuovi Bitcoin. Infatti, se l'attività di generazione di nuovi Bitcoin viene definita con la parola "mining", in analogia con il gold mining cioè l'estrazione dell'oro, questa spiegazione è solo in parte esaustiva.

Il mining svolge un ruolo essenziale per il funzionamento del network:

- permette la verifica delle transazioni e la convalida dei blocchi;
- previene il *double spending*;
- raccoglie le fee delle transazioni.

In assenza di queste tre attività non esisterebbe il network Bitcoin.

La panoramica generale dell'industria legata all'attività di mining ci presenta una realtà dinamica e in continua evoluzione, che ha subito profondi cambiamenti a partire dalla sua nascita. È un mercato in gran parte

ancora vicino alla concorrenza perfetta e chiunque vi si può unire, anche se con il passare del tempo e l'aumento della Difficoltà iniziano a sorgere le prime significative barriere all'ingresso. Inoltre, è molto probabile che tutto l'equipaggiamento e la tecnologia per la generazione di bitcoin proseguirà per almeno un'altra decade, seguendo la legge di Moore,[10] per quanto riguarda l'efficienza nei processi, e le legge di Koomey,[11] per quanto riguarda l'efficienza nel consumo elettrico per i prossimi 30 anni.

IL PROBLEMA DEL

DOUBLE SPENDING

Il problema del *double spending* si verifica quando i Bitcoin vengono spesi più di una volta. Questo è uno dei problemi più gravi delle valute virtuali in generale. A differenza delle monete fisiche, infatti, esiste la possibilità che le valute digitali possano essere clonate e spese più volte. Il bitcoin non è esente da questo problema e la mancanza di un'entità centrale terza che verifichi e supervisioni il *double spending* rende più complessa la soluzione per evitarlo.

Per comprendere il senso di tale affermazione è importante specificare ancora una volta che nel network Bitcoin

non esiste né un “saldo” né un “conto”, ma esistono solo transazioni. Il loro susseguirsi nel corso del tempo determina la quantità di bitcoin presente su un certo wallet, cioè la quantità di bitcoin che il proprietario di quest’ultimo è in grado di spendere.

Il mining, come abbiamo iniziato a vedere, è un sistema distribuito di consensi sulle avvenute transazioni e il Blockchain è il libro contabile che ne contiene l’ordine cronologico. Ogni qualvolta vogliamo effettuare una transazione, comunichiamo agli altri *peer* del network la volontà di spostare *n* bitcoin da un determinato wallet, di cui siamo in grado di provare la paternità (tramite firma digitale), a un

altro. I *peer*, una volta ricevuta la richiesta, provvederanno a:

- verificare la validità della richiesta: questo è possibile grazie alla firma digitale con cui si certifica la paternità del wallet;
- verificare che il wallet contenga davvero *n* bitcoin: questo è possibile ripercorrendo la storia delle transazioni avvenute verso quel wallet nel Blockchain;
- includere la transazione nel prossimo blocco che mineranno, dandogli quindi conferma.

Tuttavia questa propagazione non è istantanea a tutti i *peer* della Rete. Di conseguenza, dopo x secondi dalla nostra "dichiarazione di transazione", ci saranno dei nodi del network che ne saranno a conoscenza e altri no: i primi includeranno la nostra transazione nel prossimo blocco da minare al fine di confermarla, i secondi no. Ma quando entrambi troveranno la soluzione al loro blocco e la propagheranno, quale verrà accettata come la prossima sequenza valida nel Blockchain? Il network accetterà il blocco o la serie di blocchi che ha richiesto il maggior lavoro per essere minata.

Nello scenario in cui un'entità k

controlli il 51% di Hash rate del network[12] si verificherebbe una situazione nella quale *k* sarebbe in grado non solo di minare tutti i blocchi restanti, e quindi di garantirsi il possesso dei rimanenti 21 milioni di bitcoin, ma anche di decidere arbitrariamente quali transazioni possano realmente avere luogo nel network.

Un esempio pratico di ciò che accadrebbe è il seguente:

- *k*, che possiede realmente *x* bitcoin, effettua una transazione verso un'altra entità *k1* per un valore di *x* bitcoin al fine di

acquistare un bene o un servizio.

- Parte del network include la transazione nel suo prossimo blocco e comincia a minarlo.
- *k1* vede che il network ha minato un blocco contenente la transazione di *x* bitcoin verso un suo wallet e invia il bene, o eroga il servizio, che *k* ha acquistato.
- *k*, parallelamente, ha minato da solo un blocco contenente una transazione in cui invia quegli *x* bitcoin verso se stesso.
- Quando *k* propagherà il blocco o la serie di blocchi contenenti la transazione maligna, il network accetterà questi al posto dei

primi, in quanto avranno richiesto maggior lavoro e quindi maggior tempo di processamento.

Il risultato è la perdita del bene o del servizio acquistato per un importo pari a *x* bitcoin da parte del soggetto *k1*. Questo viene considerato, oggi, l'unico attacco in grado di ledere realmente il network Bitcoin.

C'è comunque da tenere in conto che:

- L'attaccante non può effettuare transazioni da wallet di cui non conosce la chiave privata, cioè non può accaparrarsi i bitcoin

posseduti da altri.

- L'attaccante non può creare bitcoin al di fuori del limite di 21 milioni.

INCENTIVI PER IL MINATORE

Il mining è un lavoro difficile e oneroso, che richiede tempo, investimenti, grande dispendio di energia ed è fondamentale per la sussistenza del Bitcoin. Motivo per cui viene riconosciuto un premio ai minatori, ma solo a quelli che riescono a minare un blocco.

Tale premio è formato da due diverse tipologie di incentivo:

- Il primo incentivo consiste nell'assegnazione di una certa quantità di moneta. Vengono assegnati 50 bitcoin per ogni blocco risolto, ma questo valore si dimezza ogni 210.000 blocchi.
- Il secondo incentivo consiste, invece, nell'assegnazione delle commissioni di transazione incluse nel blocco stesso.

Se ogni 210.000 blocchi il numero di nuovi bitcoin viene dimezzato, allora è evidente che l'offerta di moneta è

limitata e si esaurisce in modo geometrico con il passare del tempo, cioè circa ogni 4 anni.

La Figura 2.1 mostra il totale di bitcoin che verranno minati in linea teorica nel corso dei prossimi anni.

Nella Figura 2.2 mostriamo un dettaglio maggiore per le prossime due decadi.

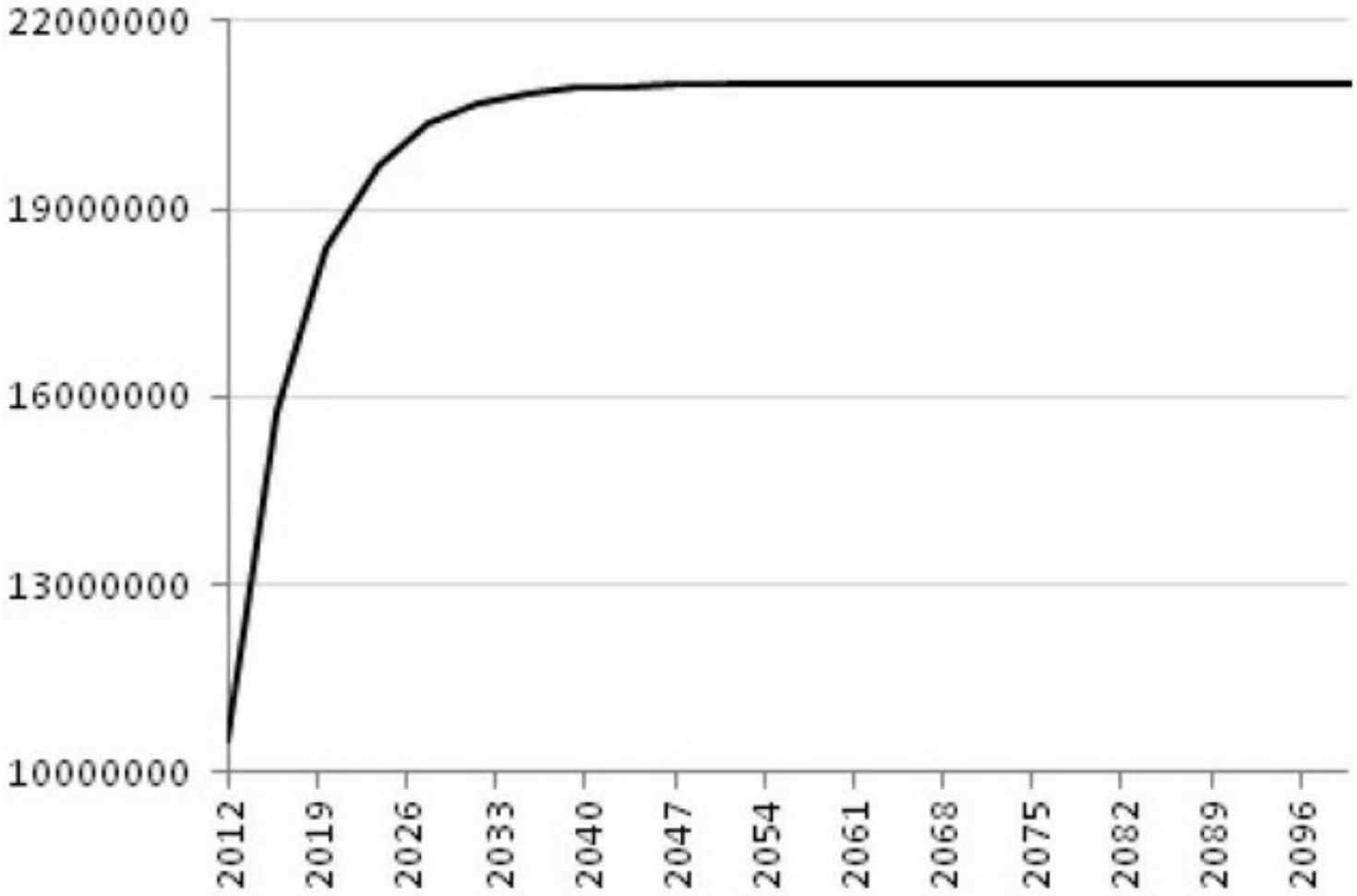


FIGURA 2.1 – Totale bitcoin teorici minati.

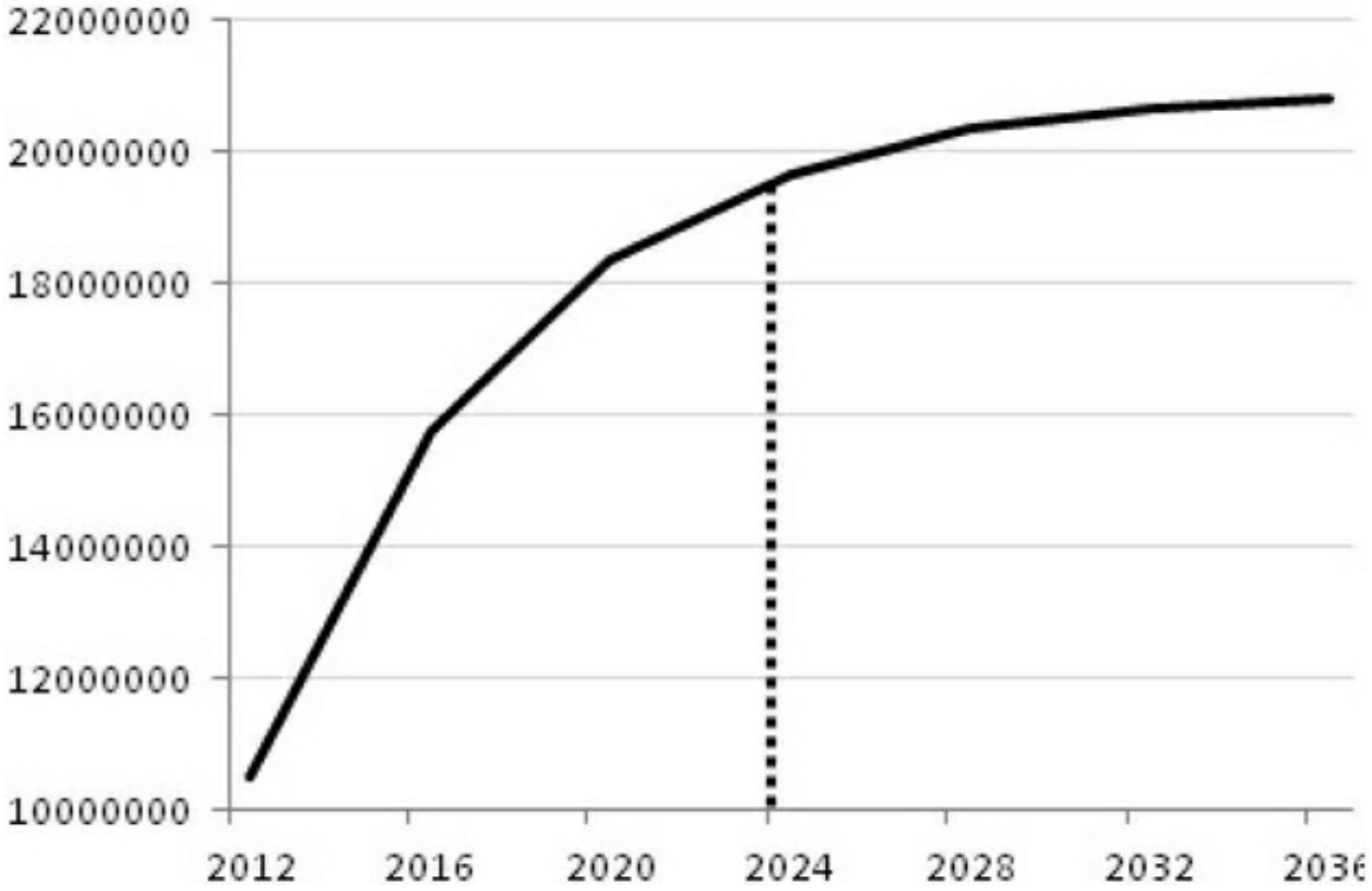


FIGURA 2.2 – Totale bitcoin teorici minati nei prossimi venti anni.

Come potete osservare, la maggior parte della produzione avviene nei primi anni e, già nel 2024, saranno stati prodotti circa 19,5 milioni di bitcoin, cioè il 94% del totale.

Dal 2024 al 2140 verrà completata l'offerta complessiva di 21 milioni di monete.

A che punto siamo della produzione al 21 novembre 2014 (giorno in cui stiamo scrivendo questo capitolo del libro)? Con circa 13.521.050 bitcoin minati siamo al 64,39% e ne mancano ancora 7.478.950. Nella Figura 2.3 è rappresentato il numero totale di bitcoin in circolazione, cioè quelli minati, e la produzione teorica.

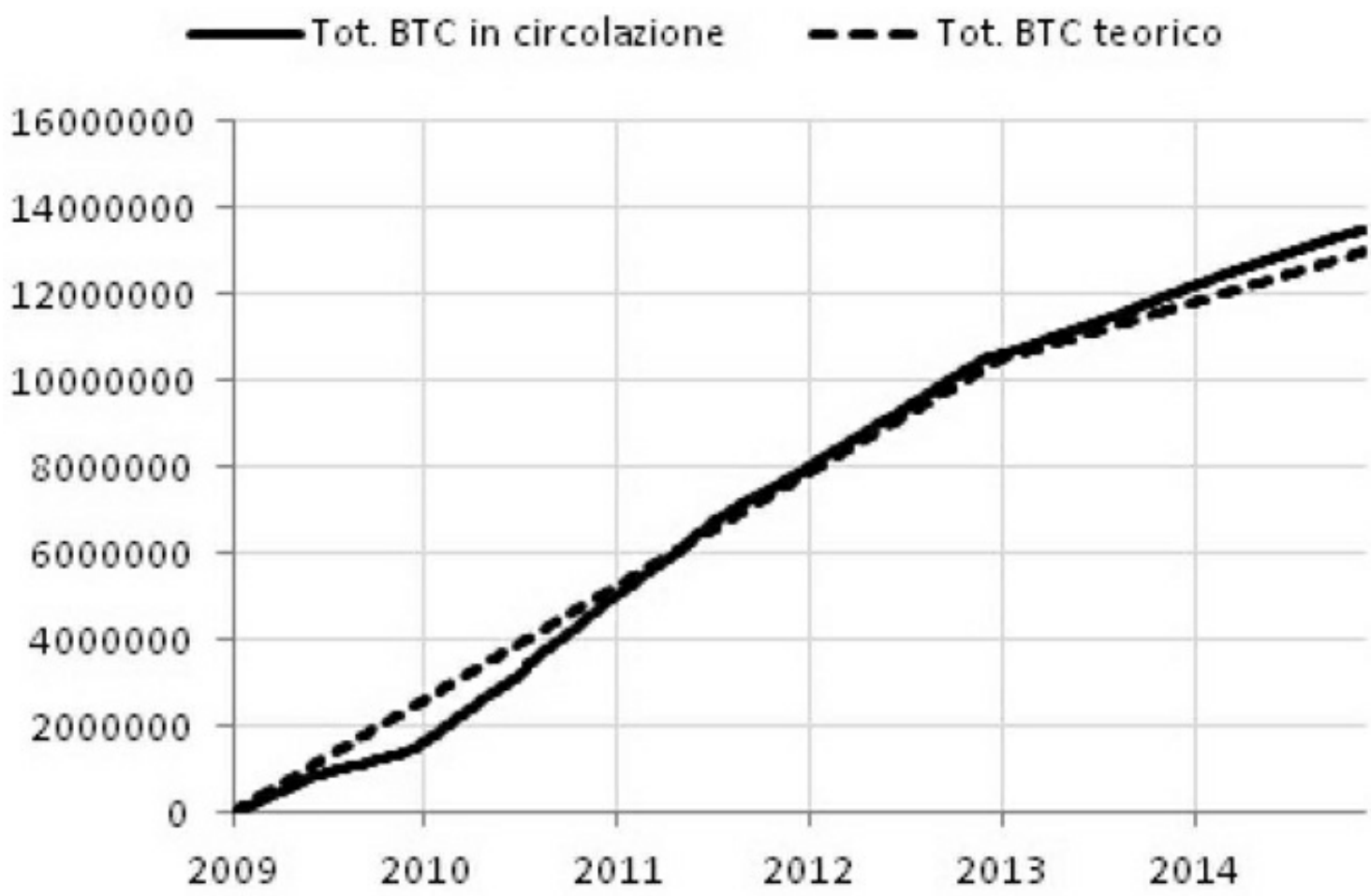


FIGURA 2.3 – Confronto bitcoin reali e produzione teorica.

Dopo la fase iniziale, in cui la produzione effettiva era inferiore a quella teorica, dal 15 maggio 2011 è stata registrata un'inversione. Nel grafico della Figura 2.4 è rappresentato

l'andamento di tale spread, calcolato come differenza tra bitcoin effettivamente minati e bitcoin teorici.

La differenza percentuale di questo spread è in forte crescita dall'inizio del 2013, ed ora è a circa +4% (Figura 2.5).

Come interpretare tale dato? Lo spread testimonia l'efficienza del lavoro dei minatori rispetto al mining teorico. Oltre al fatto che gli investimenti e gli sviluppi nel settore tecnologico sono in crescita e quindi il settore riesce a sovraperformare l'impianto teorico.

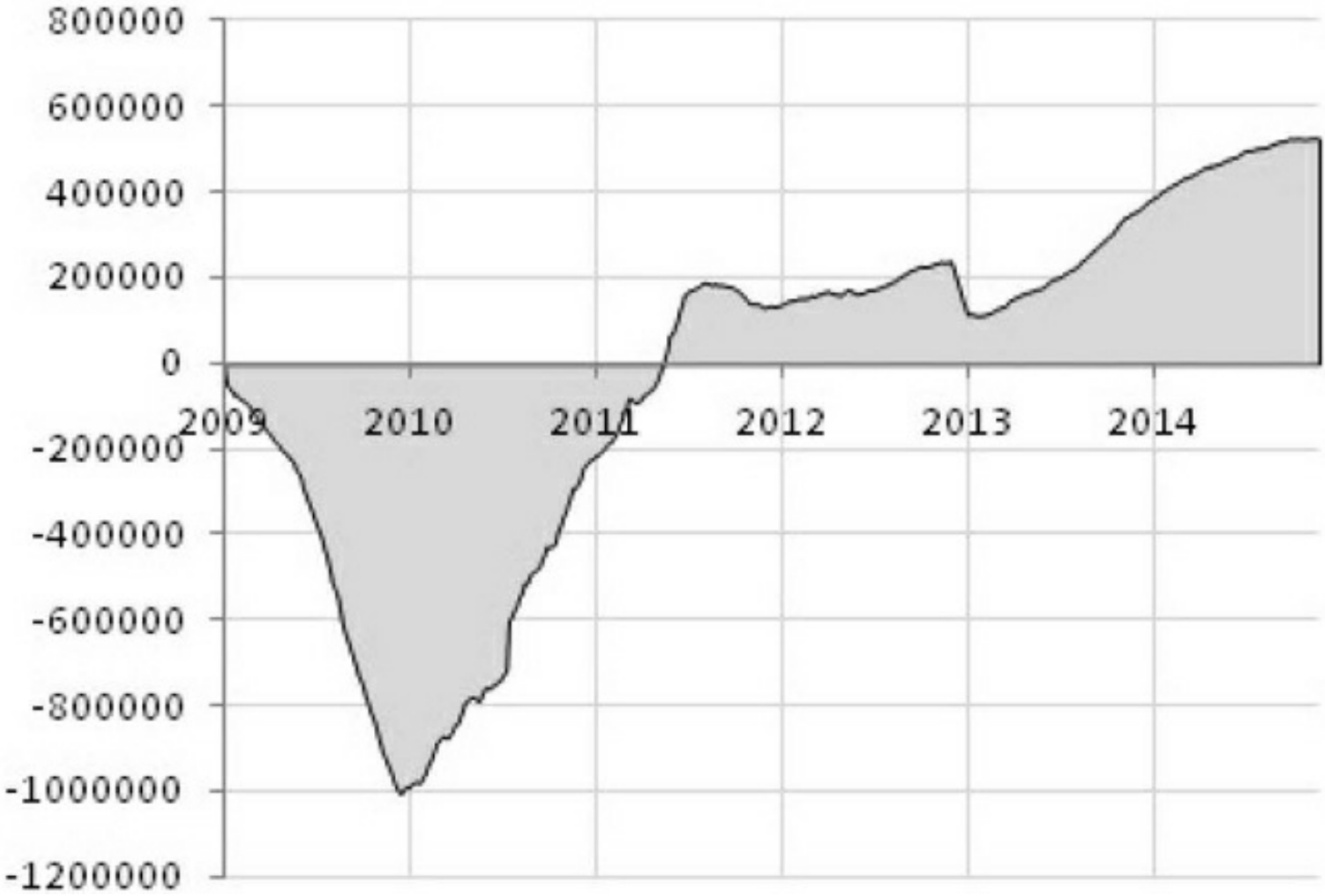


FIGURA 2.4 – Spread bitcoin minati e bitcoin teorici.

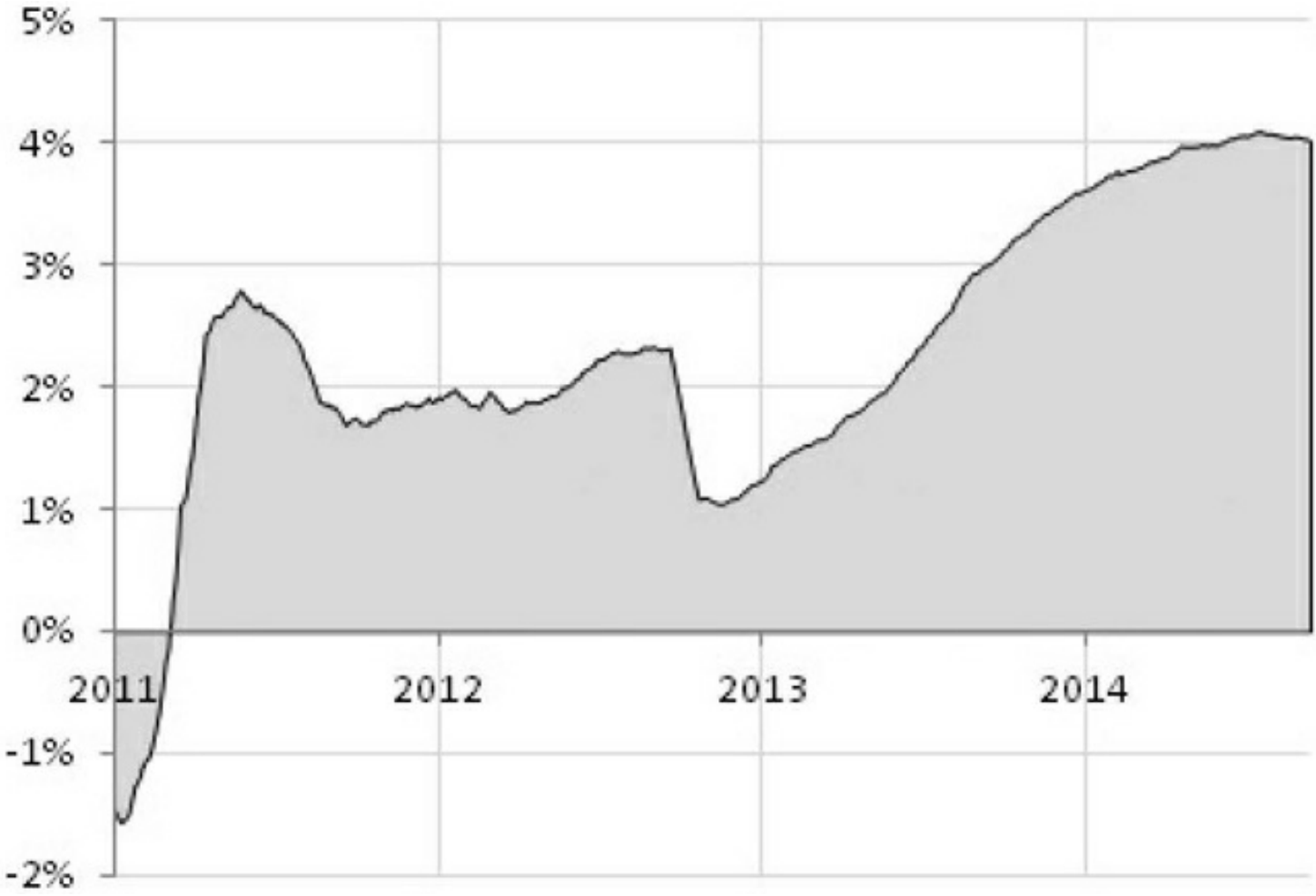


FIGURA 2.5 – Spread bitcoin minati e bitcoin teorici in termini percentuali.

FEE DELLE TRANSAZIONI

Abbiamo visto come la prima forma di incentivo è limitata sia per quantità sia per tempo. Per sostenere i costi dell'attività di mining è necessario che, in futuro, o il prezzo di mercato dei bitcoin salga in modo significativo oppure aumenti la seconda forma di incentivo. Analizziamo in dettaglio questa seconda forma di incentivo prevista per i minatori.

Iniziamo dicendo che le commissioni di transazione non sono obbligatorie, e al tempo stesso i minatori non hanno l'obbligo di processare tutte le transazioni, ma per avere la certezza che queste siano validate, è necessario pagare questo incentivo. Attualmente

molte transazioni sono processate anche senza commissioni, ma con il passare del tempo, e con il decrescere dei bitcoin assegnati in ogni blocco, quasi sicuramente non sarà più così.

Vi mostriamo ora alcuni dati statistici relativi alle transazioni. Partiamo dal numero di transazioni su scala giornaliera nella Figura 2.6.

E aggreghiamo questi dati su scala mensile nella Figura 2.7.

Vediamo infine, nella Tabella 2.1, la situazione su scala annuale. Il trend è palesemente rialzista, a testimonianza che il bitcoin aumenta in consenso e utilizzo.

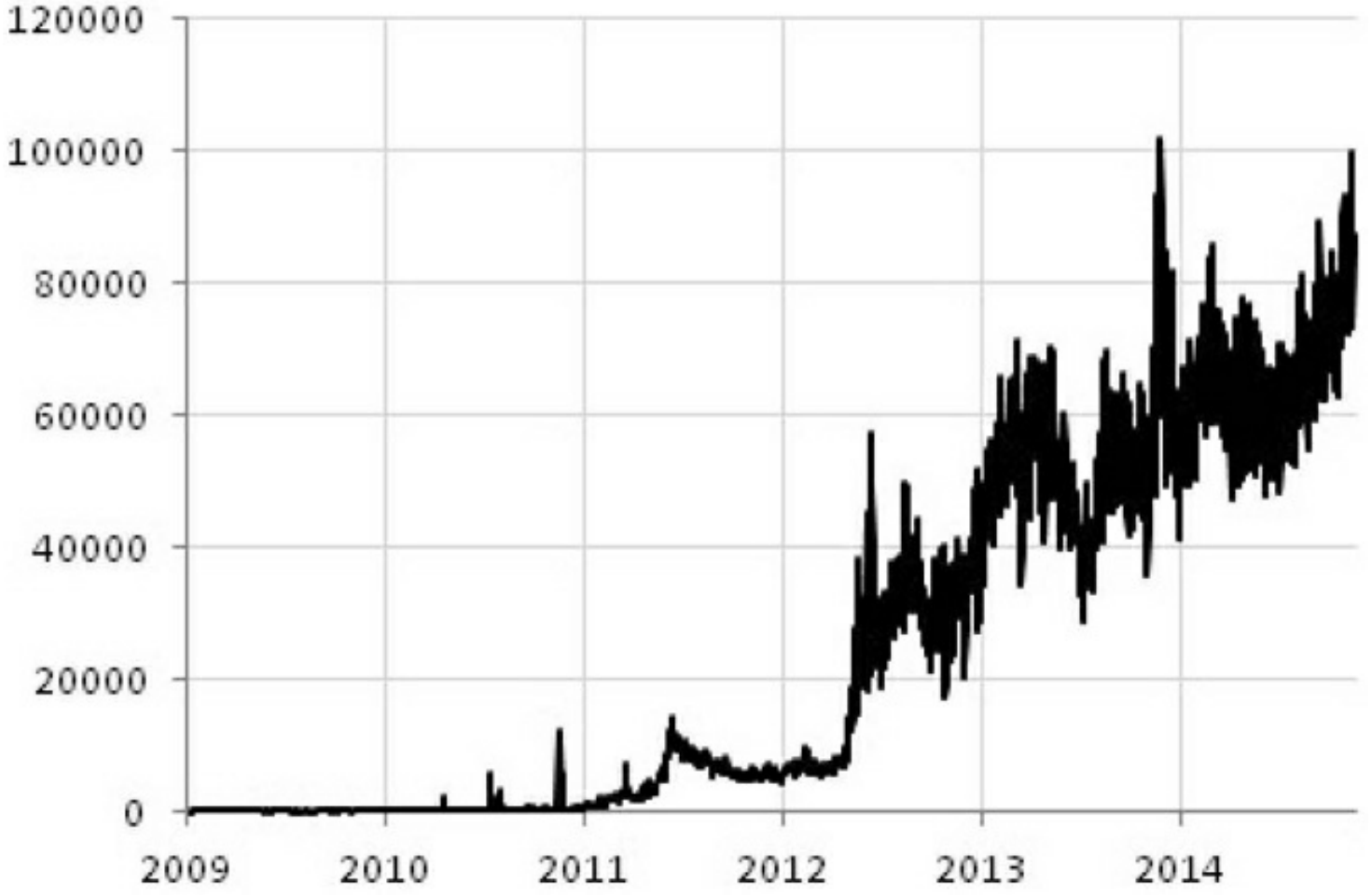


FIGURA 2.6 – Numero di transazioni giornaliere.

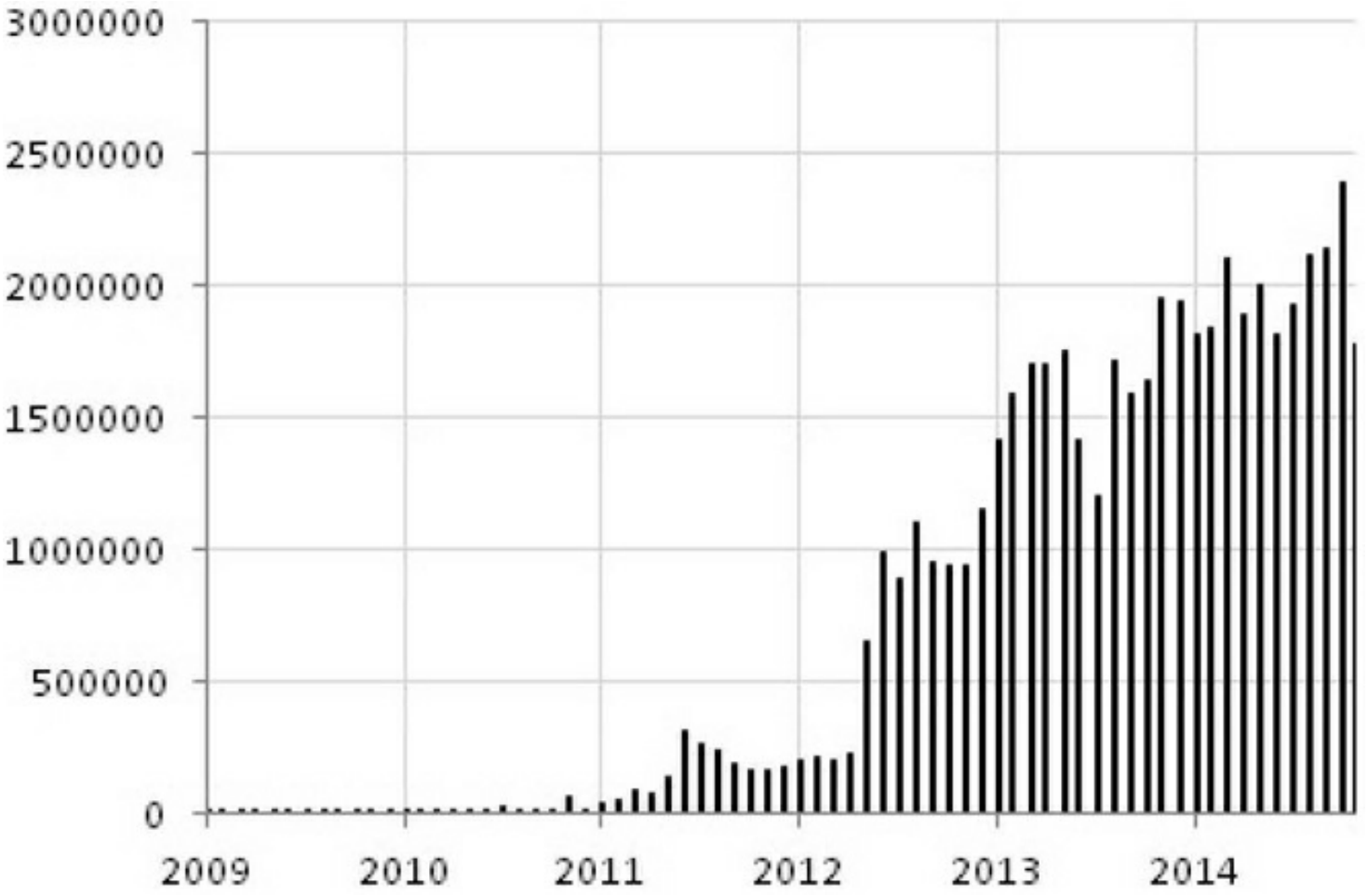


FIGURA 2.7 – Numero di transazioni mensili.

TABELLA 2.1 – Numero di transazioni annuali.

Anno	**Numero di transazioni annuali**
2009	32.687
2010	185.212

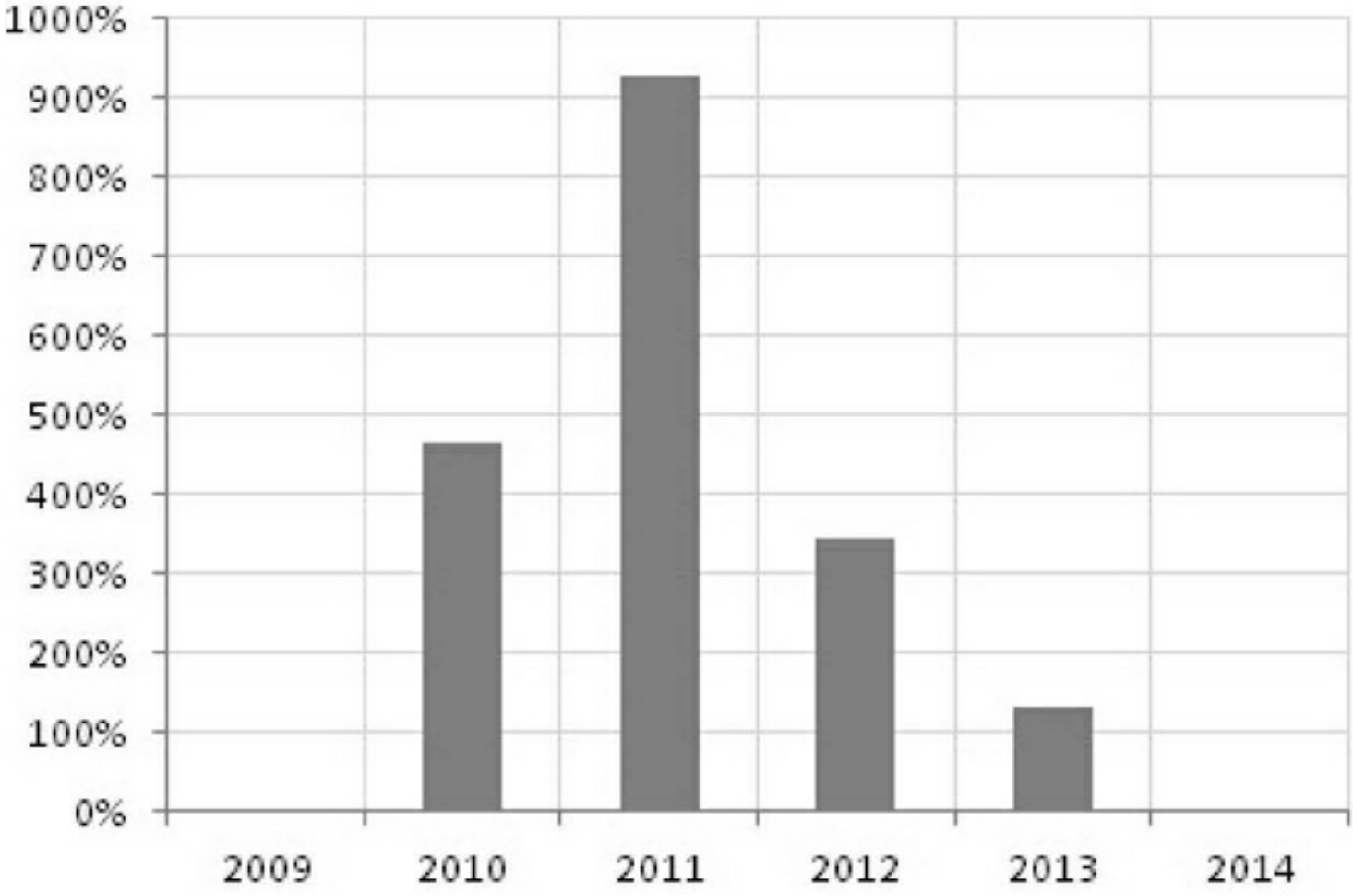
2011	1.900.652
2012	8.447.785
2013	19.638.728
2014 (al 21 novembre)	21.805.485

Analizzando in termini percentuali il numero di transazioni, rileviamo che il maggior incremento percentuale si è avuto nel 2011, anno in cui è cresciuto di oltre il 900%. Invece, nel 2013 abbiamo assistito a un incremento di circa il 130%. I dati relativi al 2014 si fermano al 21 novembre, ma ci segnalano che il trend si conferma in crescita anche per quest'anno (Figura 2.8).

È bene però precisare che il numero

di transazioni in bitcoin, e il relativo controvalore, se confrontati con altri strumenti di pagamento, quali per esempio le carte di credito, sono ancora irrilevanti. Lo potete osservare nella Tabella 2.2, in cui è mostrata una media del numero indicativo di transazioni giornaliere al 31 marzo 2014.

E il relativo volume in dollari nella Tabella 2.3.



FGURA 2.8 – Variazione in termini percentuali del numero di transazioni annuali.

TABELLA 2.2 – Numero medio delle transazioni giornaliere.

Strumento di pagamento	**Numero di transazioni giornaliere**
Visa, Inc.	212.603.000

MasterCard Inc.	93.578.000
American Express Co.	14.521.000
PayPal	7.700.000
Western Union Company	633.000
Bitcoin	65.122
Xoom Corp	25.000

TABELLA 2.3 – Volume medio in dollari delle transazioni giornaliere.

Strumento di pagamento	**Volume in $**
Visa, Inc.	16.518.000.000
MasterCard Inc.	9.863.000.000
American Express Co.	2.434.000.000
PayPal	397.000.000
Western Union Company	216.000.000

Bitcoin	33.400.000
Xoom Corp	15.000.000

Tuttavia, non dimentichiamoci che stiamo parlando di una tecnologia, quella dei Bitcoin, nata da pochissimi anni, con enormi margini di miglioramento e con un vantaggio notevole: i costi di commissione di gran lunga più bassi di tutti gli strumenti di pagamento concorrenti. Vediamo insieme di quanto.

Il primo grafico (Figura 2.9) mostra le fee di transazione in bitcoin su scala giornaliera.

Mentre il secondo grafico (Figura 2.10) le mostra su scala mensile.

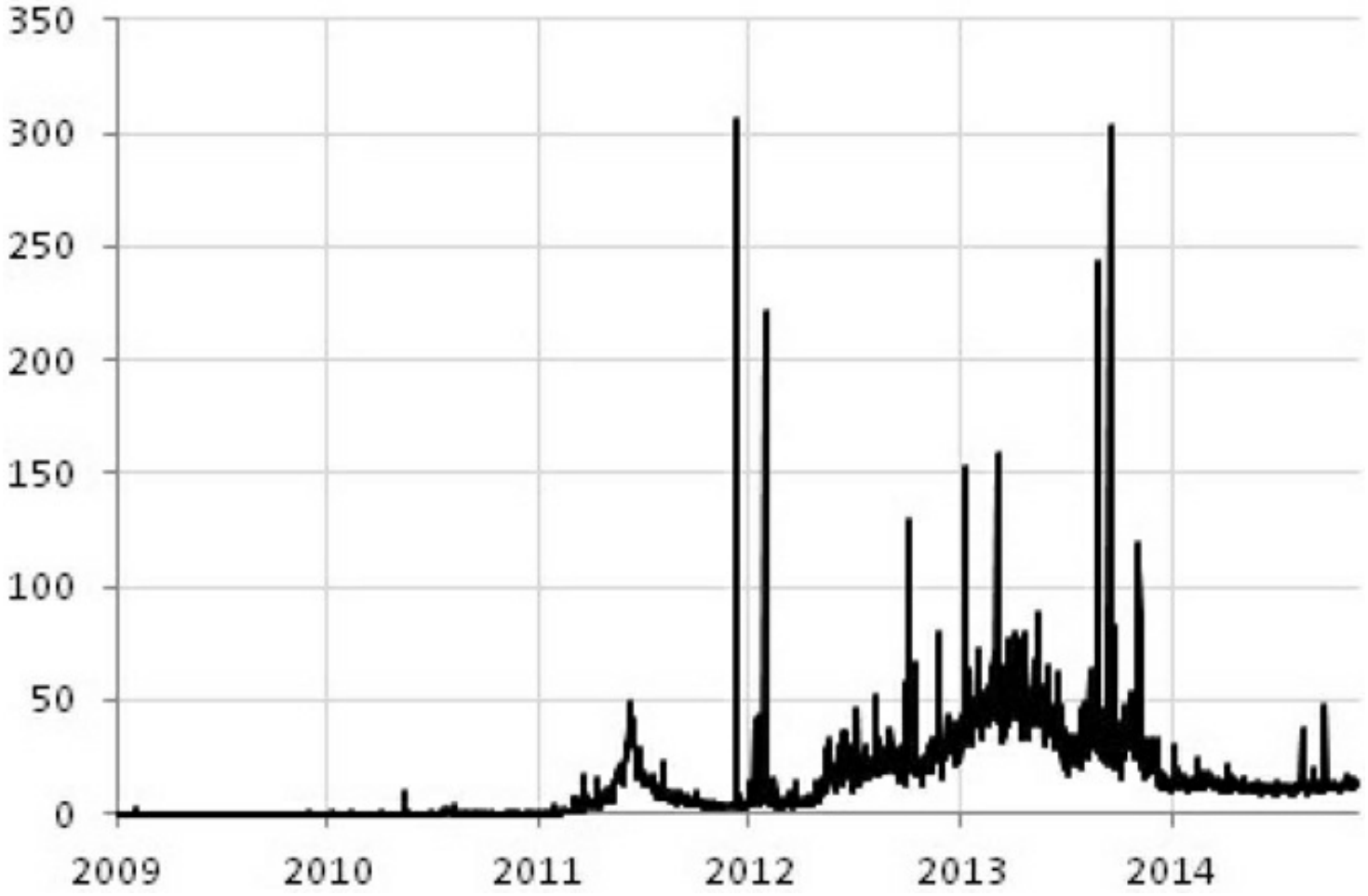


FIGURA 2.9 – Transaction Fee in BTC su time frame giornaliero.

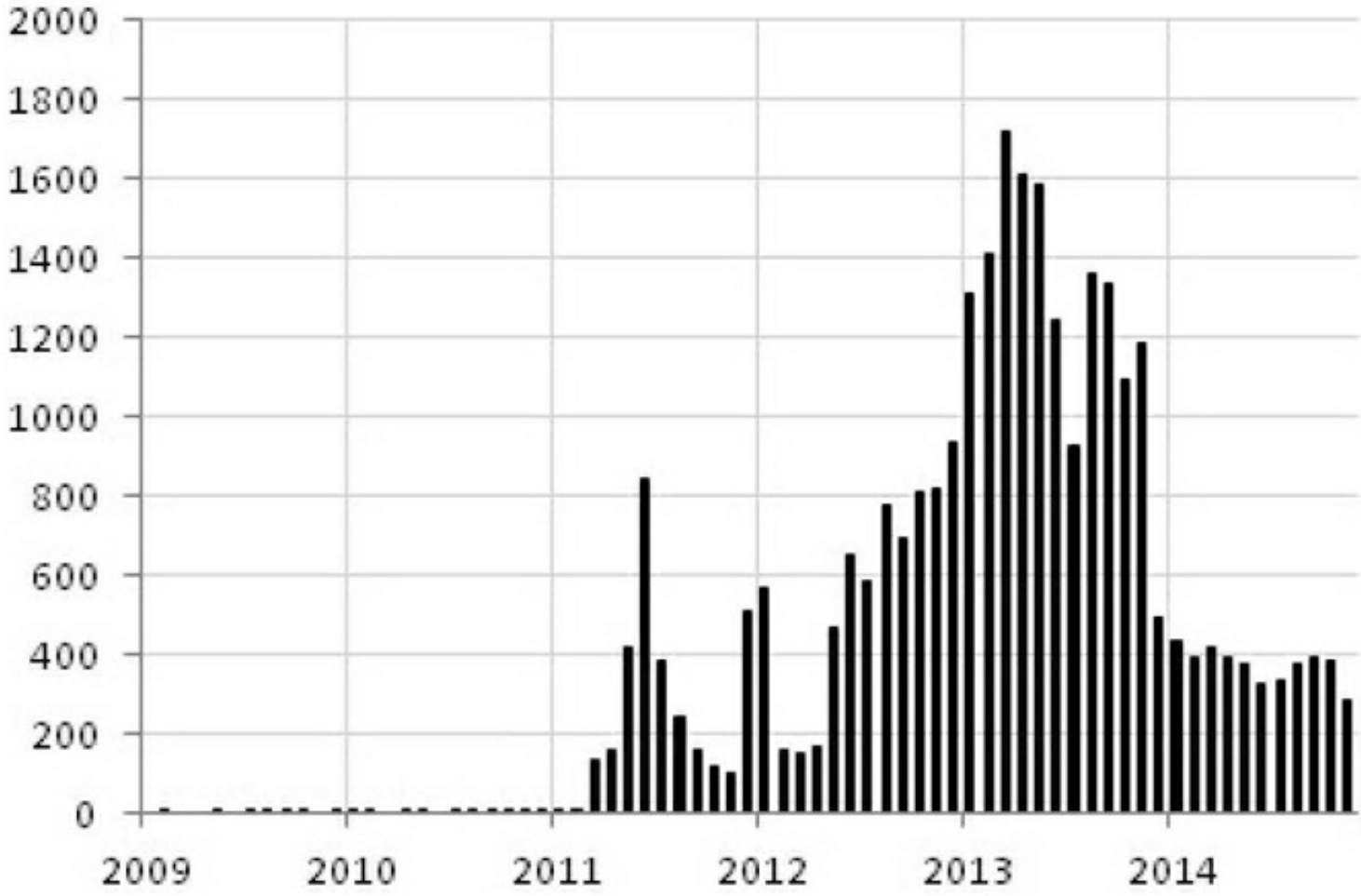


FIGURA 2.10 – Transaction Fee in BTC su time frame mensile.

Mostriamo infine il grafico cumulato (Figura 2.11).

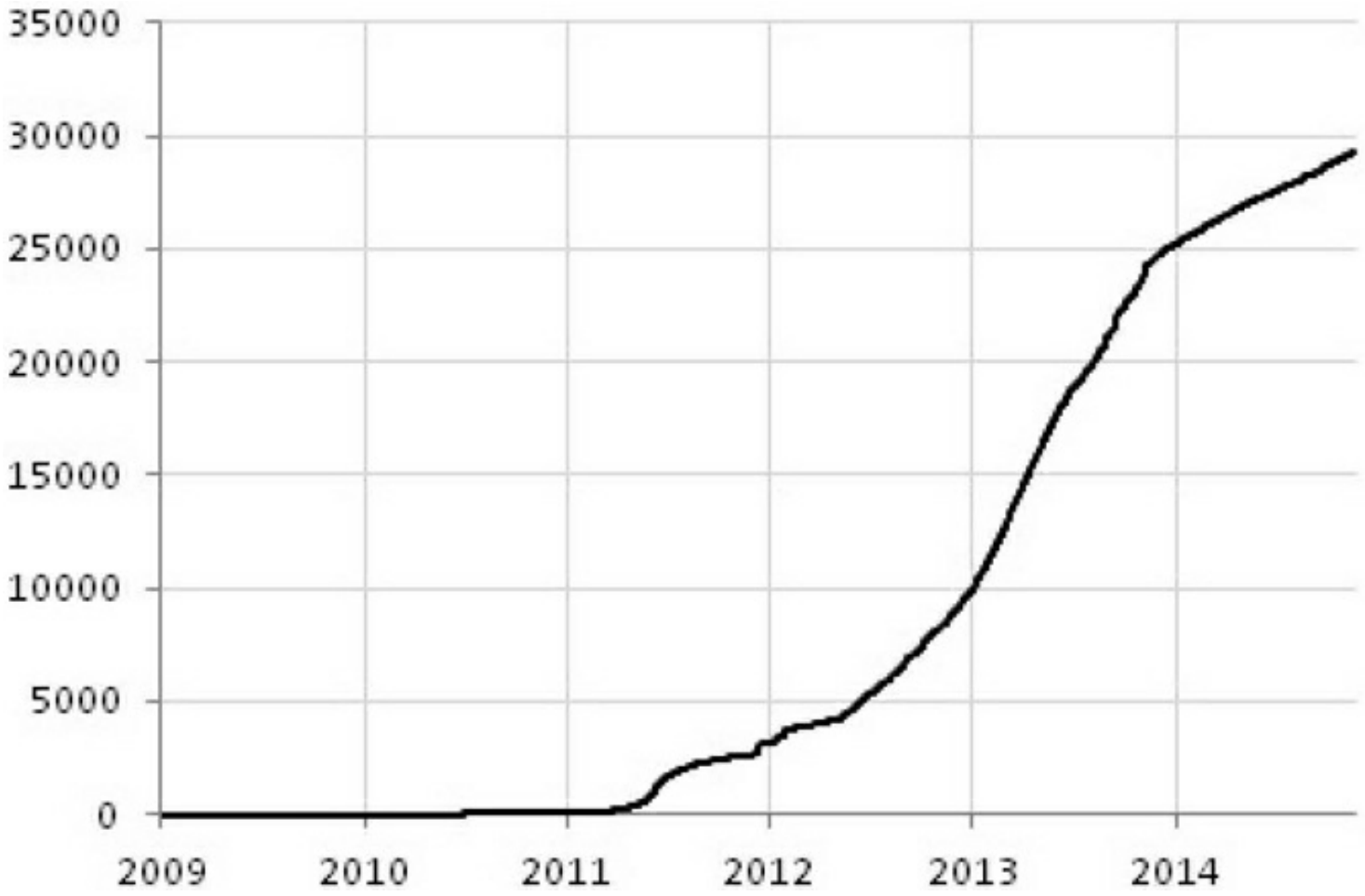


FIGURA 2.11 – Grafico cumulato delle Transaction Fee.

Il totale delle commissioni pagate è quindi di circa 30.000 bitcoin.

Per completare la nostra analisi è necessario analizzare il totale dei volumi di bitcoin scambiati (Figura

2.12).

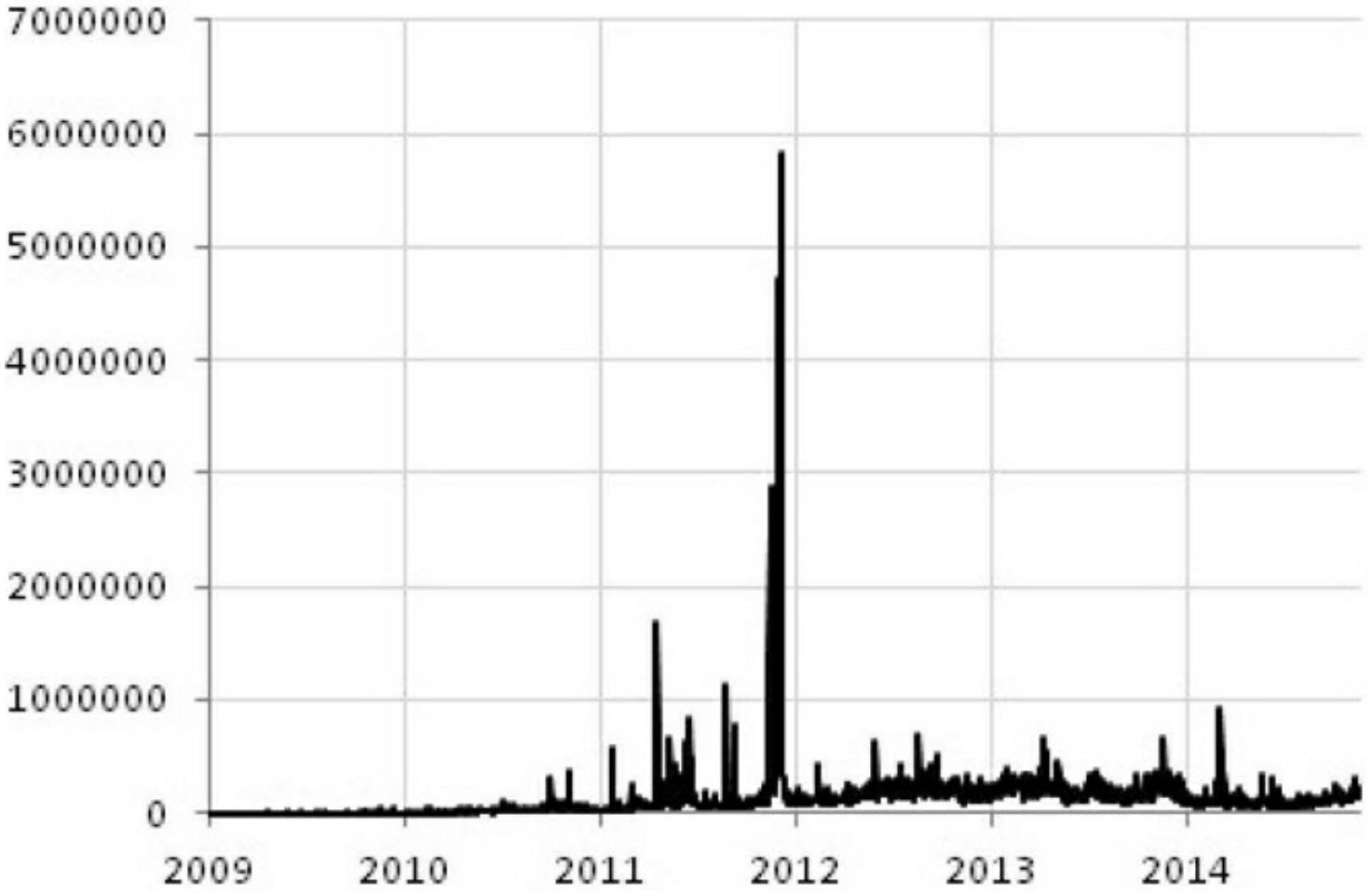


FIGURA 2.12 – Stima dei volumi scambiati.

Passiamo alla curva cumulata (Figura 2.13).

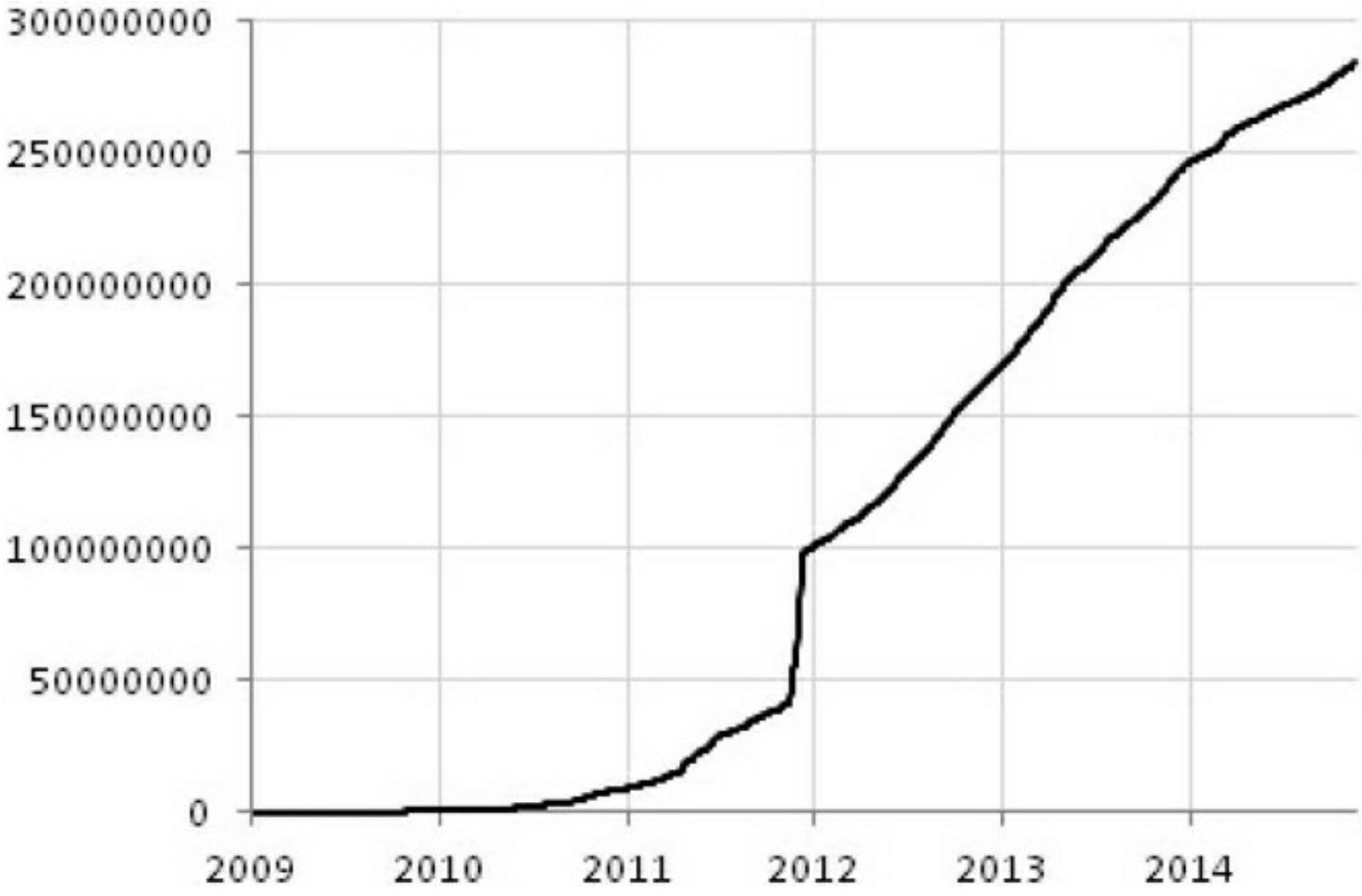


FIGURA 2.13 – Grafico cumulato della stima dei volumi scambiati.

Otteniamo quindi circa 29 milioni di bitcoin scambiati.

Ricordando che il totale delle commissioni è di circa 30.000 bitcoin, dividendo tale numero per la quantità

totale di bitcoin che sono stati oggetto di transazione, otteniamo un valore pari allo 0,10% di gran lunga inferiore alle commissioni mediamente richieste da tutti gli altri strumenti di pagamento. Questo fattore, a nostro avviso, rende il bitcoin uno strumento privilegiato per tutte le transazioni finanziarie e, in particolare, per il commercio online.

---

10. Le prestazioni dei processori e il numero di transistor a esso relativo raddoppiano ogni 18 mesi.
11. L'efficienza energetica dei computer raddoppia all'incirca ogni 18 mesi.
12. Nei primi giorni di giugno 2014, GHash.IO è arrivata molto vicina a detenere la quota del 51%, per poi scendere sotto il 40% nelle

giornate successive.

CAPITOLO 3

L’algoritmo di mining

Andiamo ora a spiegare più nel dettaglio come funziona l'algoritmo di mining.

L'attività di mining consiste sostanzialmente in un gioco di competizione per chi è il primo minatore a trovare la risposta a un problema matematico che risolva il blocco attuale.

Per intenderci, facciamo un piccolo esempio. Ipotizziamo di partecipare a una competizione con altri giocatori, tutti determinati a portarsi a casa il premio in palio. Le regole del gioco sono queste:

- si parte applicando la funzione SHA-256 al messaggio "compra

cento bitcoin" ottenendo il seguente Hash: 5335c303e0981e-00317ec53582de99d9495df45cf7

- si aggiunge al messaggio un valore finale, che prende il nome d i *Nonce*, e si ricalcola la funzione SHA-256, ottenendo un nuovo Hash;
- vince chi per primo trova un nuovo Hash inferiore o uguale a un certo target, il quale deve avere come valore iniziale un certo numero di zeri. Nel nostro esempio ne basta uno.

La strategia che adottiamo è quella di partire da un Nonce pari a 1 che incrementiamo fino a quando non

troviamo un Hash che soddisfi il target. In questo processo di calcolo è, però, richiesta velocità, poiché vince solo il primo giocatore che riesce a trovare la soluzione.

Ecco i nostri calcoli:

- Input: compra cento bitcoin1
  Nonce: 1
  Hash: face26287ca04f2f97ff4d4a702c5c526e3114f6070373aea2fdda
- Input: compra cento bitcoin2
  Nonce: 2
  Hash: 64dd594ceae0d5f1e820a697e0dfb6875db5f2295f5ab957bfb8

- Input: compra cento bitcoin3
  Nonce: 3
  Hash: 7dde2eaa6cff0009c036186c2be1d6486de8ec32896e9846b4e

Proseguiamo con l'incrementare il Nonce fino a quando arriviamo al valore 13:

- Input: compra cento bitcoin13
  Nonce: 13
  Hash: 0e0c03b8ff256deda2efd2b48fe9de685c8e398ba47ae41cc1a77f4b4b5cb7

Questo Nonce produce un Hash che

inizia con il valore zero, se abbiamo individuato per primi la soluzione che soddisfi il target, allora abbiamo vinto!

È bene però precisare che la soluzione non è univoca, applicando infatti un Nonce pari a 1016 si ottiene comunque un Hash che inizia con zero:

- Input: compra cento bitcoin1016
  Nonce: 1016
  Hash: 0d1146506ce813248fa798ec39f8898d3de47a27db6bdcfbf379ac

Quindi è evidente che la velocità nel ricercare una delle possibili soluzioni è l'aspetto peculiare dell'attività di

mining. Infatti, tale attività non è altro che un'operazione di forza bruta (*Brute Force)*, in cui si procede per tentativi applicando tutte le possibili combinazioni, fino a quando un minatore non vince.

Ovviamente il problema del Bitcoin è più complesso, non tanto da un punto di vista logico quanto per la mole di calcoli da svolgere. I passaggi svolti dall'algoritmo di mining sono sostanzialmente identici a quelli fissati nel nostro gioco:

- prende l'header[13] del blocco come input;
- cambia il Nonce;

- applica due volte la funzione Hash (SHA-256);
- verifica che l'Hash sia inferiore al target e, in caso affermativo, si riparte dal punto 1, altrimenti dal punto 2.

La vera differenza sta nel Target.

TARGET

Il Target è un numero estremamente grande, a 256 bit, che può rappresentare 2256 differenti informazioni ed è tipicamente espresso in scala esadecimale.

A titolo di esempio, il Target al 03/04/2014 era il seguente:

- In scala esadecimale: 00000000000000DB9000000000000000000000
- In scala decimale: 5384518863803604621895699672051 2

Il valore del Target si modifica in base alla differenza percentuale tra tempo effettivo e tempo teorico necessario per minare 2016 blocchi.

Il protocollo Bitcoin prevede che il tempo teorico necessario per minare 1 blocco sia pari a 10 minuti, di conseguenza per minare 2016 blocchi

sono teoricamente necessarie 2 settimane come mostrato nella Tabella 3.1.

TABELLA 3.1 – Blocchi minati in diversi intervalli temporali.

Tempo	N° Blocchi
10 minuti	1
1 ora	6
1 giorno	144
1 settimana	1008
2 settimane	2016

Tuttavia il tempo effettivo impiegato dal network, per svolgere la prova di lavoro, può essere più breve o più ampio rispetto a quello teorico.

Il primo caso è quello in cui i minatori siano stati particolarmente bravi e veloci nel minare i blocchi, e questo si traduce in una diminuzione del nuovo Target, rendendo la successiva prova di lavoro più difficile. Il caso opposto è quello in cui i minatori abbiano impiegato un tempo superiore a quello teorico, e in questo caso l'algoritmo incrementa il nuovo Target rendendo la successiva prova di lavoro più facile. L'incremento o il decremento del nuovo Target sono però vincolati, non potendo essere rispettivamente superiori o inferiori di un fattore 4 rispetto al Target attuale. Da quanto appena detto, si deduce che più il Target

è piccolo più è difficile ricercare una soluzione che lo possa soddisfare.

Arriviamo, quindi, a introdurre il concetto di Difficoltà.

DIFFICOLTÀ

La Difficoltà è la misura di quanto sia complicato trovare un Hash al di sotto di un certo Target e queste sono le sue principali caratteristiche:

- il valore iniziale è stato fissato pari a 1;
- non ha un valore massimo;

- non può mai essere inferiore a 1;
- si aggiusta ogni 2016 blocchi, cioè ogni 2 settimane circa;
- è inversamente correlata con il Target;
- è positivamente correlata con l'Hash rate.

In Figura 3.1 è rappresentato il grafico storico (al 21/11/2014) della Difficoltà.

Dal valore iniziale di 1 siamo attualmente arrivati a un valore della Difficoltà che ha superato i 40 miliardi, con una crescita incredibile del 40.300.030.326% in soli 5 anni.

Per una lettura grafica più chiara dobbiamo però utilizzare la scala logaritmica (Figura 3.2). In questo modo

possiamo dividere l'andamento della Difficoltà in tre fasi:

- dal 2009 alla prima metà del 2011: aumento;
- dalla seconda metà del 2011 all'inizio del 2013: stabilità;
- dall'inizio del 2013 fino a oggi: aumento.

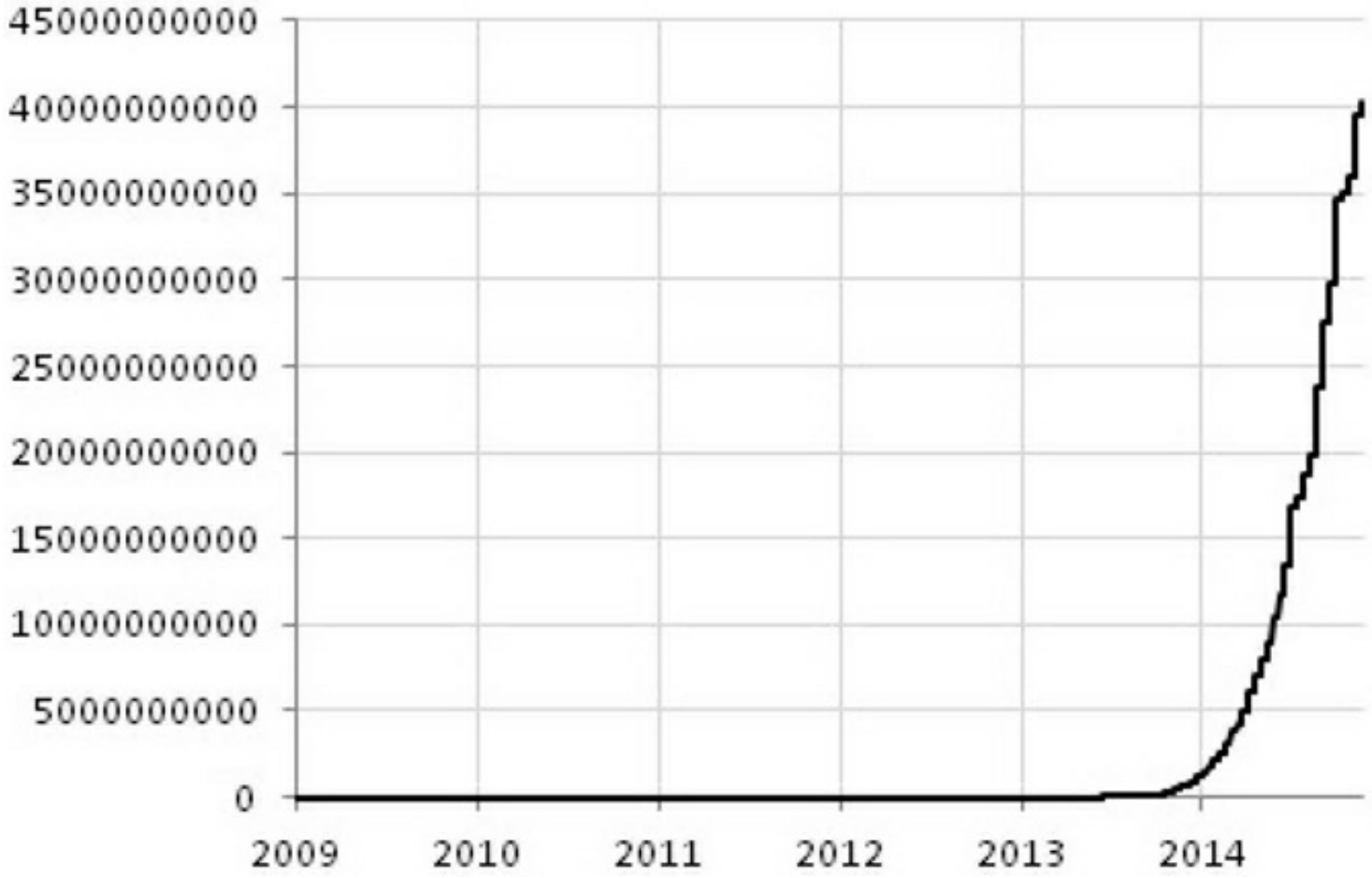


FIGURA 3.1 – Grafico storico della Difficoltà.

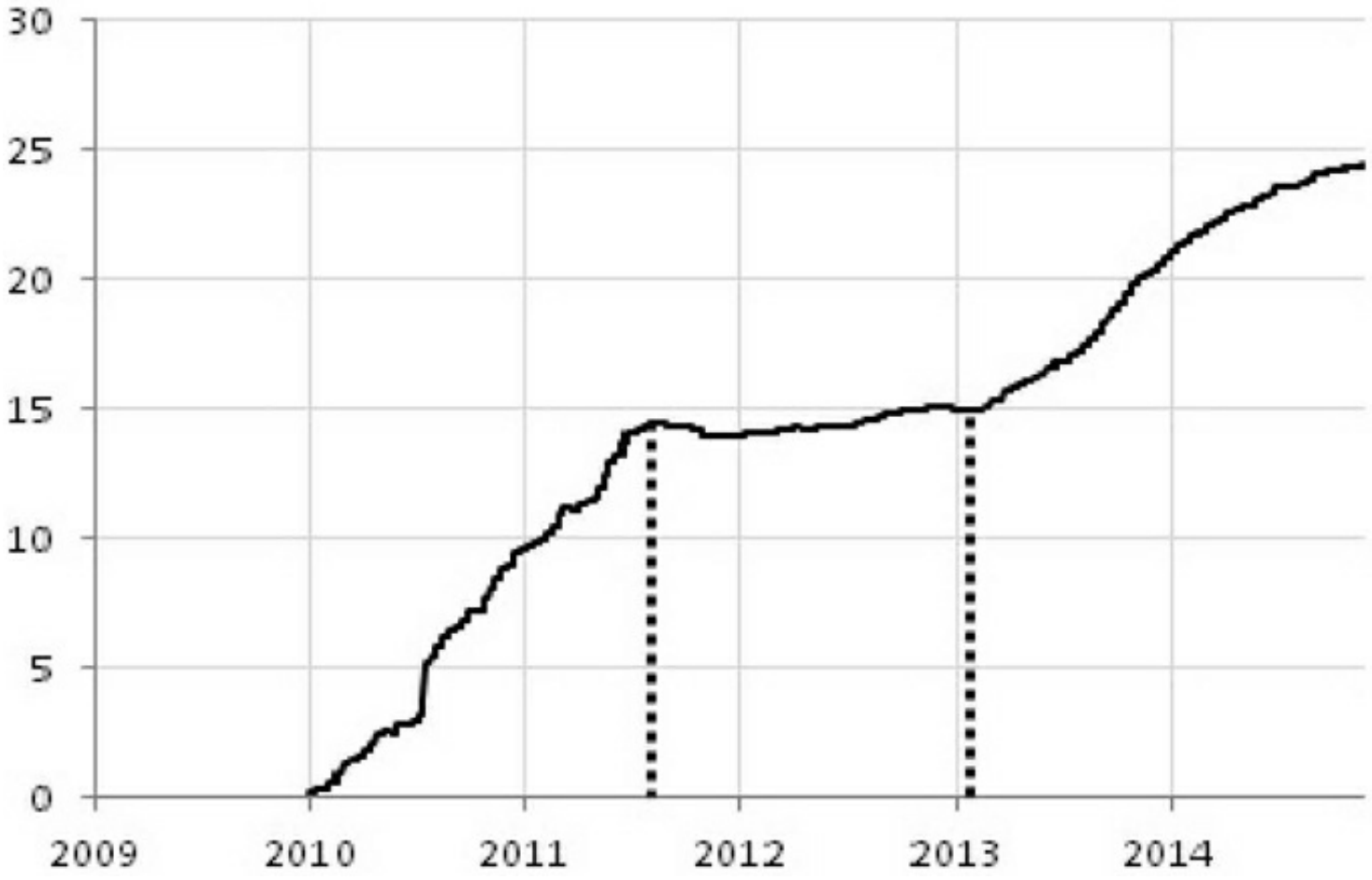


FIGURA 3.2 – Grafico storico logaritmico della Difficoltà.

Dall'analisi grafica passiamo a quella statistica delle variazioni percentuali della Difficoltà (Tabella 3.2). La base dati parte dal 30 Dicembre 2009, giorno in cui si è verificato il primo cambio di Difficoltà, dal valore 1 a 1,18289953.

TABELLA 3.2 – Analisi statistica della Difficoltà.

N° Valori	1788
N° Cambi Difficoltà	149
Media	20,03%
Max (16/07/2010)	300%
Min (01/11/2011)	-18,03%
Dev.st.pop	29,24%
Curtosi	55,89
Asimmetria	6,11

Si tratta di una distribuzione composta da 149 cambi di Difficoltà, con media 20,03% e deviazione standard 29,24%. Il valore massimo è stato del 300% (16

luglio 2010), mentre quello minimo del -18,03% (1 novembre 2011).

La curtosi è positiva e dunque la distribuzione è leptocurtica, cioè più appuntita rispetto alla distribuzione normale. L'asimmetria, anch'essa positiva, ci segnala che il ramo destro della curva è più lungo di quello sinistro. La Figura 3.3 mostra la distribuzione di frequenza.

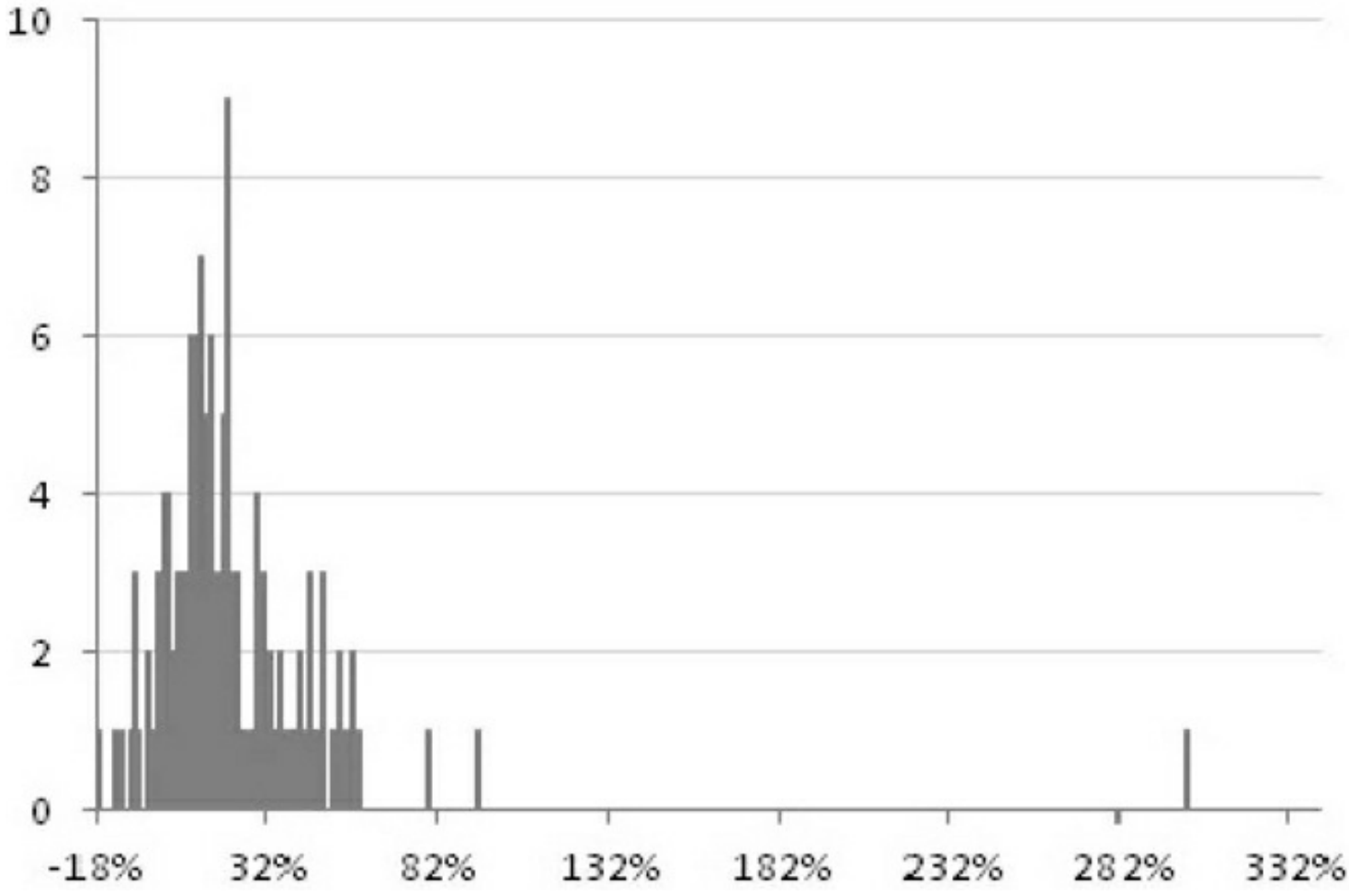


FIGURA 3.3 – Distribuzione di frequenza della Difficoltà.

Proviamo a raggiungere un dettaglio maggiore scomponendo i dati in base all'anno di riferimento, escludendo però il 2009, anno in cui si è registrato un solo cambio di Difficoltà.

Così facendo, otteniamo la Tabella 3.3.

TABELLA 3.3 – Analisi statistica della Difficoltà per anni.

	2010	2011	2012	2013	2014
N° Cambi Difficoltà	33	30	27	31	27
Media	38,3%	18,03%	3,74%	21,84%	14,2%
Max	300%	78,15%	14,89%	46,02%	26,16%
Min	-7,81%	-18,03%	-11,59%	-8,64%	0,98%
Dev.st.pop	50,56%	23,97%	6,07%	11,53%	7,18%
Curtosi	22,27	-0,21	0,20	0,23	-0,89
Asimmetria	4,36	0,73	-0,64	-0,16	-0,31

L'osservazione più importante è legata alla deviazione standard che, dal massimo del 2010, si è significativamente ridotta negli anni successivi. In altri termini abbiamo assistito a un calo di volatilità con conseguente stabilizzazione delle variazioni percentuali della Difficoltà.

Facciamo ora un altro passo in avanti. Sappiamo che la Difficoltà è mediamente aumentata, ma in alcuni casi ha registrato anche valori negativi. Analizziamo separatamente queste due casistiche (Tabella 3.4).

TABELLA 3.4 – Analisi statistica della Difficoltà con distinzione casi positivi e negativi.

	Casi variazione positiva	**Casi variazione negativa**
Percentuale	87,91%	12,09%
N° Cambi Difficoltà	131	18
Media	23,6%	-5,96%
Max	300%	-0,24%

Min	0,09%	-18,03%
Dev.st.pop	29,39%	4,87
Curtosi	59,46	0,24
Asimmetria	6,59	-0,85

Nell'88% dei casi oggetto di studio, la Difficoltà è stata superiore o uguale alla precedente con una media di crescita del 23,6% e un valore massimo del 300%. Mentre nel restante 12% si è avuto un calo della Difficoltà, ma poco significativo, con una media di decrescita del -5,96% e un valore minimo del -18,03%. Con l'analisi statistica abbiamo avuto conferme di quanto intuito dall'analisi grafica, cioè che la Difficoltà è in un chiaro trend rialzista di lungo periodo e i casi in cui

è diminuita sono stati statisticamente poco rilevanti.

TEMPO PER CAMBIO DIFFICOLTÀ

Per i nostri scopi è importante svolgere un'analisi statistica anche riguardo al numero di giorni intercorsi tra i vari cambi di Difficoltà. Storicamente abbiamo avuto 149 cambi di Difficoltà, ma per l'analisi del tempo ne prendiamo in considerazione solo 148. Nella Tabella 3.5 sono consultabili i risultati.

TABELLA 3.5 – Analisi statistica del tempo di cambio di Difficoltà.

N° Valori	148
Media (gg)	12,06
Max (gg)	17
Min (gg)	3
Dev.st.pop (gg)	2,01
Curtosi	2,29
Asimmetria	-0,34

In media si è verificato un cambio di Difficoltà ogni 12 giorni con un minimo di 3 e un massimo di 17 giorni.

Il grafico della Figura 3.4 mostra, sull'asse delle ascisse, il numero progressivo dei cambi di Difficoltà, a partire dal 12 gennaio 2010; mentre,

sull'asse delle ordinate, è rappresentato il numero di giorni intercorsi tra un cambio e il precedente.

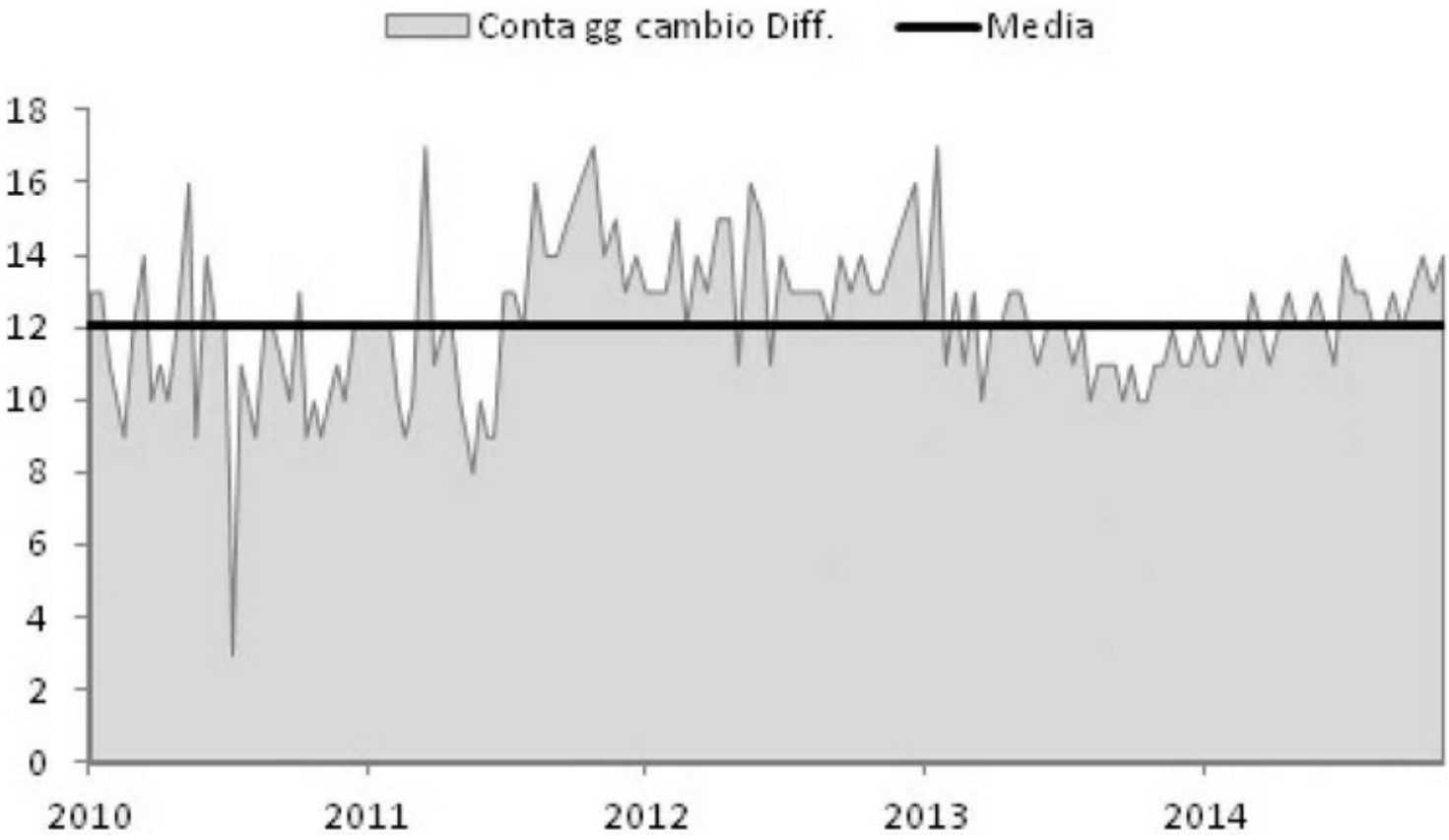


FIGURA 3.4 – Numero di giorni per cambio Difficoltà.

I dati si distribuiscono secondo la curva di frequenza della Figura 3.5.

Questa curva è simile a una

distribuzione normale, come potete osservare dal grafico in Figura 3.6.

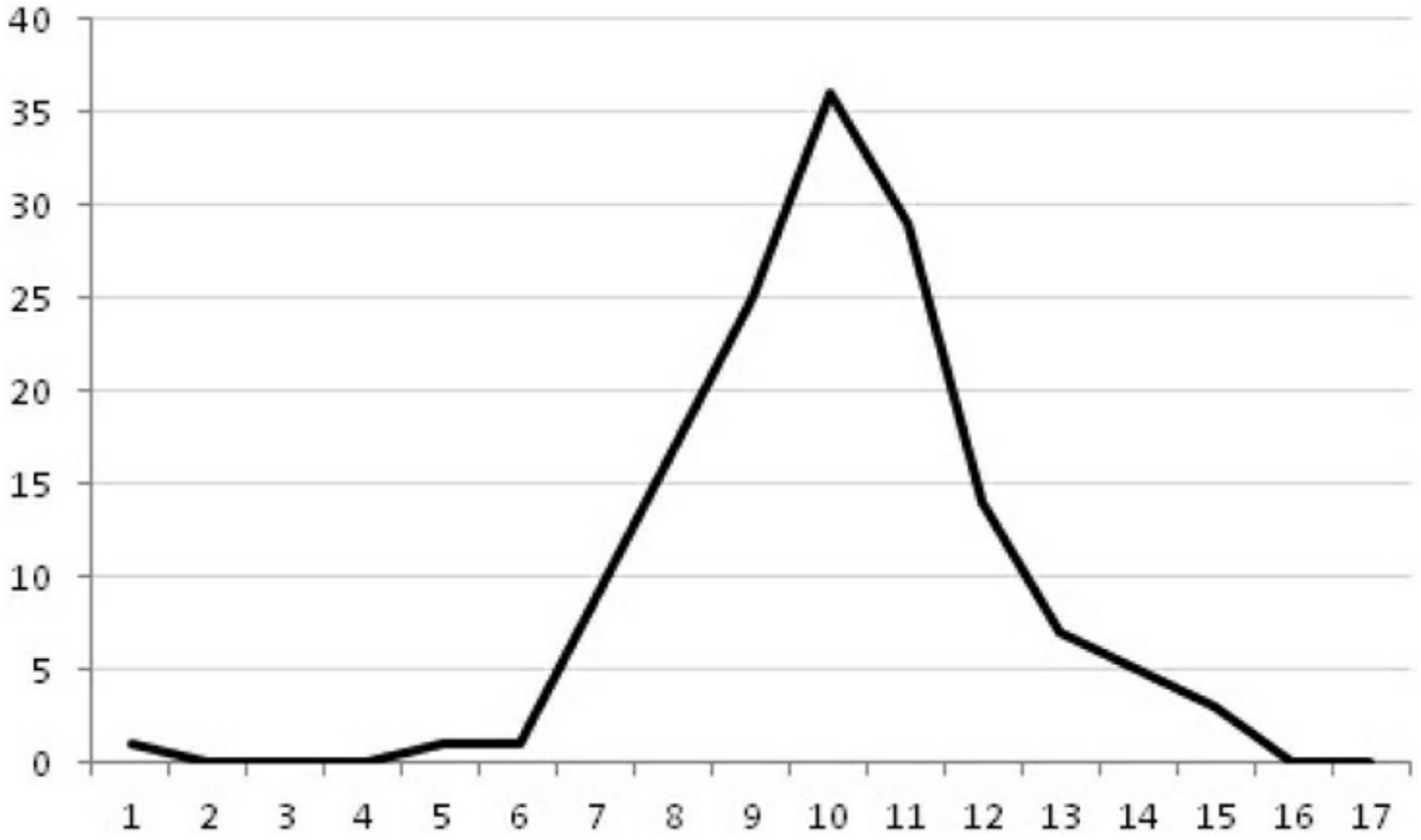


FIGURA 3.5 – Curva di frequenza.

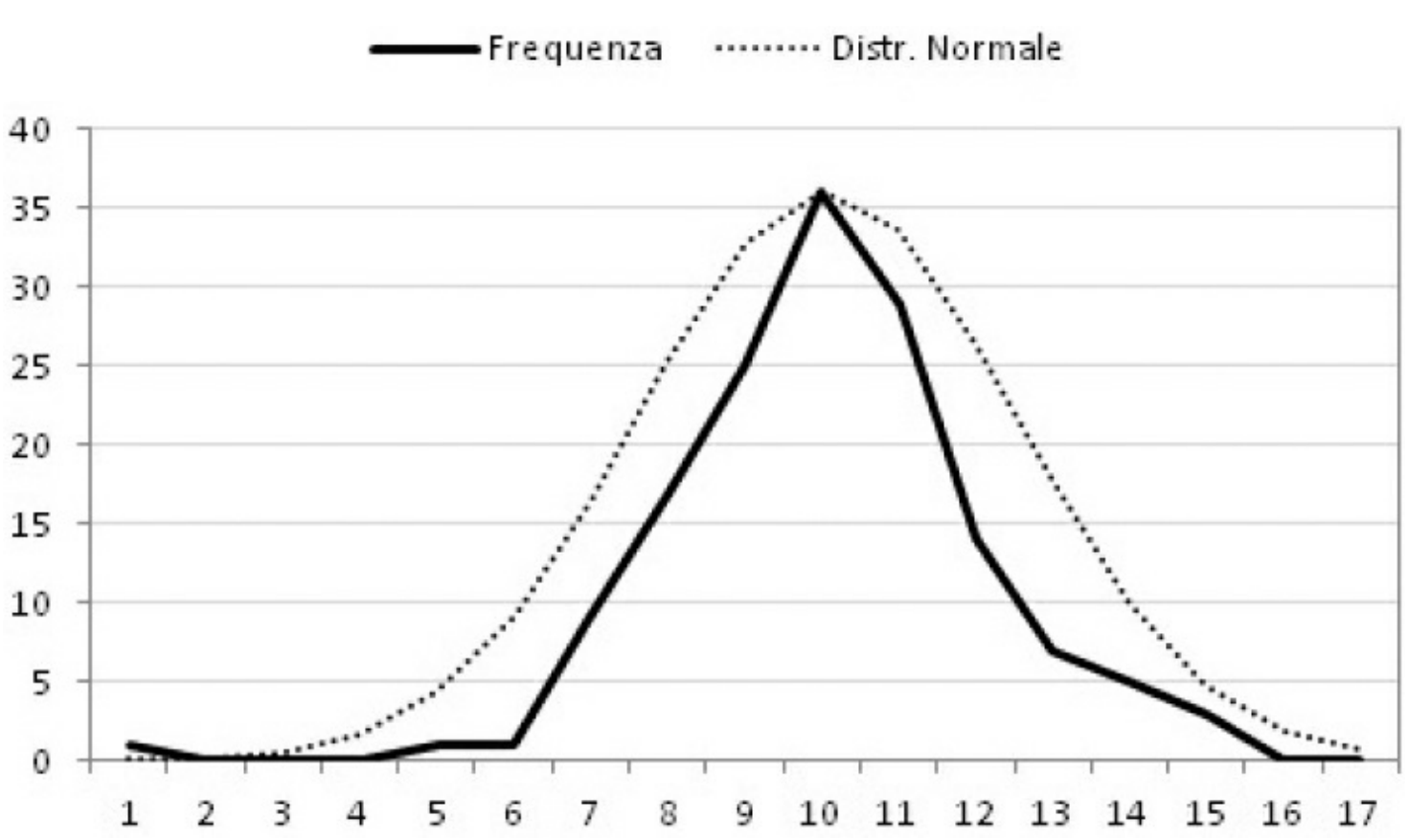


FIGURA 3.6 – Confronto tra Distribuzione normale e frequenza.

Che significa tutto ciò? In concreto, significa che i dati si distribuiscono in modo uniforme intorno alla media e offrono una maggiore stabilità rispetto alle distribuzioni di frequenza osservate per le variazioni percentuali della

Difficoltà. Una distribuzione normale offre particolari vantaggi statistici, uno su tutti: la possibilità di stima della probabilità che si verifichi un determinato evento.

Anzitutto, sappiamo che in una distribuzione normale il 68% dei dati è compreso nell'intervallo tra la media μ meno una deviazione standard σ e la media più una deviazione standard (Figura 3.7).

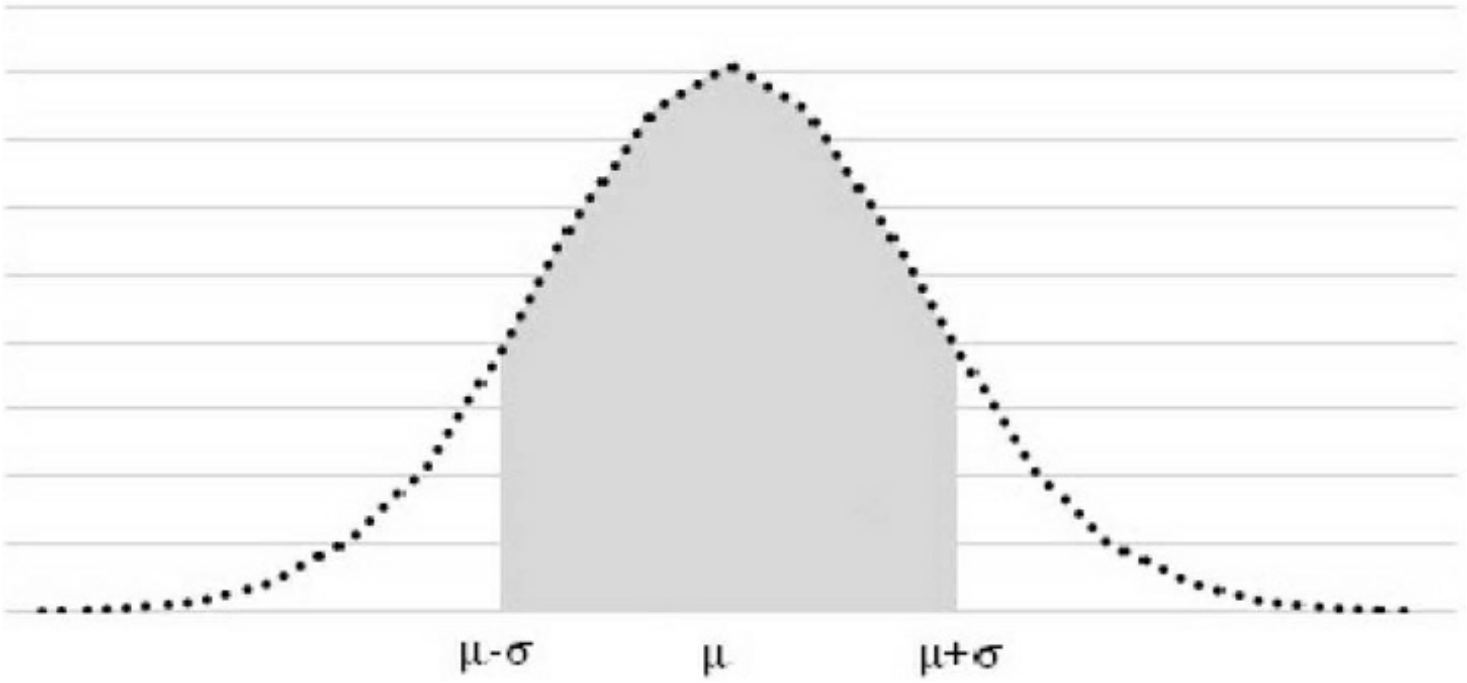


FIGURA 3.7 – Intervallo di confidenza del 68% di una distribuzione normale.

Mentre il 95% dei dati è compreso nell'intervallo tra la media meno due deviazioni standard e la media più due deviazioni standard (Figura 3.8).

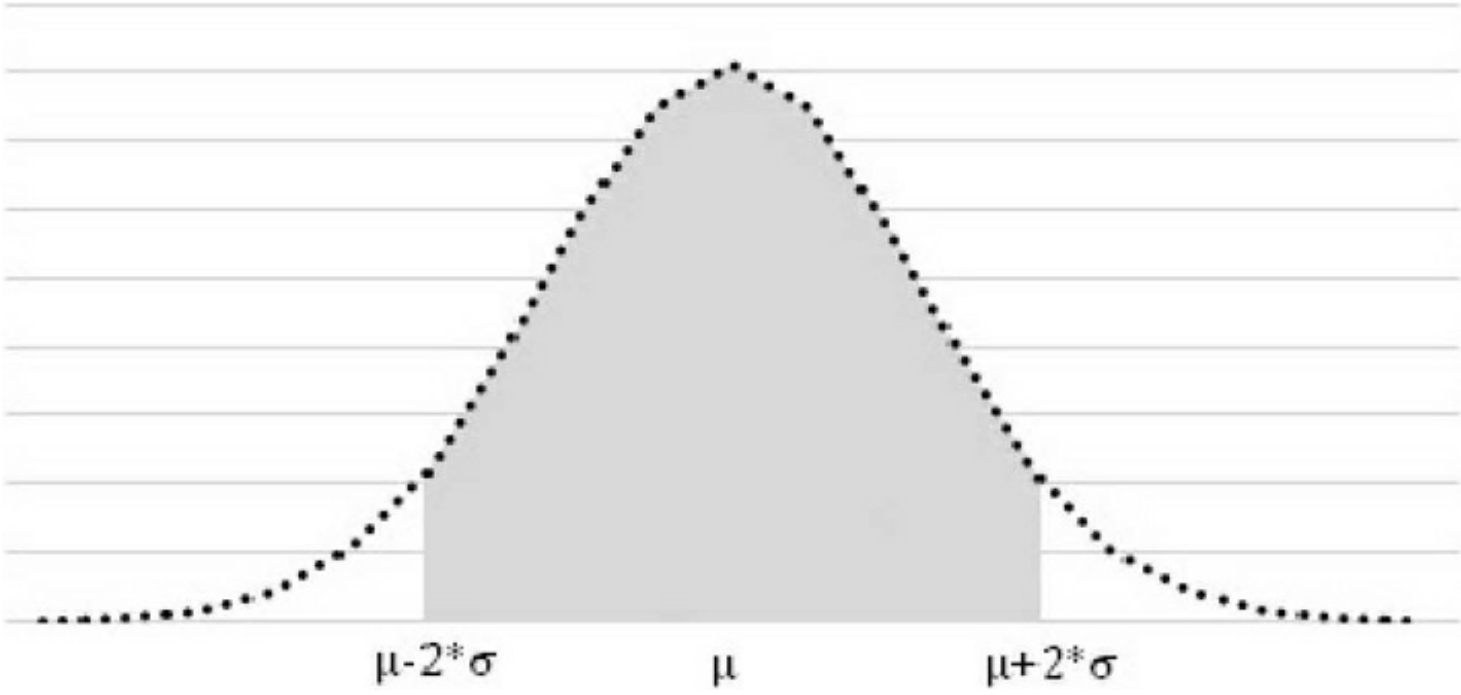


FIGURA 3.8 – Intervallo di confidenza del 95% di una distribuzione normale.

L'analisi condotta sui cambi di Difficoltà ha portato ai seguenti valori:

- media $\mu = 12$ giorni;
- deviazione standard $\sigma = 2$ giorni.

Quindi, senza voler essere particolarmente rigorosi, e ipotizzando

che la distribuzione sia simile a quella normale, possiamo per esempio affermare che la probabilità di avere un cambio di Difficoltà superiore a 14 giorni ($\mu + \sigma$) è pari al 16%:

$$\text{Probabilità} = \frac{(100 - 68\%)}{2} = 16\%$$

Oppure che la che la probabilità di avere un cambio di Difficoltà superiore a 16 giorni ($\mu + 2 \cdot \sigma$) è pari al 2,5%:

$$\text{Probabilità} = \frac{(100 - 95\%)}{2} = 2{,}5\%$$

Si capisce bene che quanto appena esposto ha un ruolo importantissimo ai

fini della stima e della previsione relative al tempo del prossimo cambio di Difficoltà. Vediamo quali interessanti conclusioni è possibile trarre.

Considerate i valori della Difficoltà della Tabella 3.6.

TABELLA 3.6 – Previsione di calcolo della Difficoltà.

Data	Difficoltà	Conteggio giorni
29/10/2014	35.985.640.265	
30/10/2014	35.985.640.265	
31/10/2014	35.985.640.265	
01/11/2014	35.985.640.265	
02/11/2014	35.985.640.265	
03/11/2014	35.985.640.265	

04/11/2014	35.985.640.265	
05/11/2014	39.603.666.252	0
06/11/2014		1
07/11/2014		2
08/11/2014		3
09/11/2014		4
10/11/2014		5
11/11/2014		6
12/11/2014		7
13/11/2014		8
14/11/2014		9
15/11/2014		10
16/11/2014		11
17/11/2014		12
18/11/2014		13
19/11/2014		14

Il giorno 05/11/2014 si è registrato un cambio di Difficoltà e a partire da quello stesso giorno, in base all'analisi statistica precedentemente illustrata, il successivo si verificherà mediamente dopo 12 giorni, con un margine di errore di ± 2 giorni. Se ne deduce che si avrà tra il 15 novembre e il 19 novembre 2014, con una probabilità del 68%. Nella Tabella 3.7 vedete che cosa è successo nella realtà.

TABELLA 3.7 – Valore effettivo della Difficoltà.

Data	Difficoltà	Conteggio giorni
29/10/2014	35.985.640.265	

30/10/2014	35.985.640.265	
31/10/2014	35.985.640.265	
01/11/2014	35.985.640.265	
02/11/2014	35.985.640.265	
03/11/2014	35.985.640.265	
04/11/2014	35.985.640.265	
05/11/2014	39.603.666.252	0
06/11/2014	39.603.666.252	1
07/11/2014	39.603.666.252	2
08/11/2014	39.603.666.252	3
09/11/2014	39.603.666.252	4
10/11/2014	39.603.666.252	5
11/11/2014	39.603.666.252	6
12/11/2014	39.603.666.252	7
13/11/2014	39.603.666.252	8
14/11/2014	39.603.666.252	9
15/11/2014	39.603.666.252	10

16/11/2014	39.603.666.252	11
17/11/2014	39.603.666.252	12
18/11/2014	39.603.666.252	13
19/11/2014	40.300.030.327	14

La Difficoltà è cambiata il 19 novembre, esattamente nel range stimato.

Possiamo applicare lo stesso metodo anche ai valori della Difficoltà, ma poiché la distribuzione delle variazioni percentuali non è di tipo normale, allora dobbiamo utilizzare la disuguaglianza di Čebyšëv.

Questo teorema afferma che, dato un valore reale $\lambda \geq 1$, allora la probabilità che i valori siano compresi nell'intervallo $(\mu \pm \lambda \cdot \sigma)$ è almeno pari

a $(1 - 1 / \lambda^2)$, indipendentemente dalla distribuzione di frequenza.

Di conseguenza, la probabilità che i valori siano compresi in un intervallo entro due deviazioni standard è il 75%, anziché il 95% come nel caso della distribuzione normale. La previsione al 06 novembre 2014 era quindi quella illustrata nella Figura 3.9.

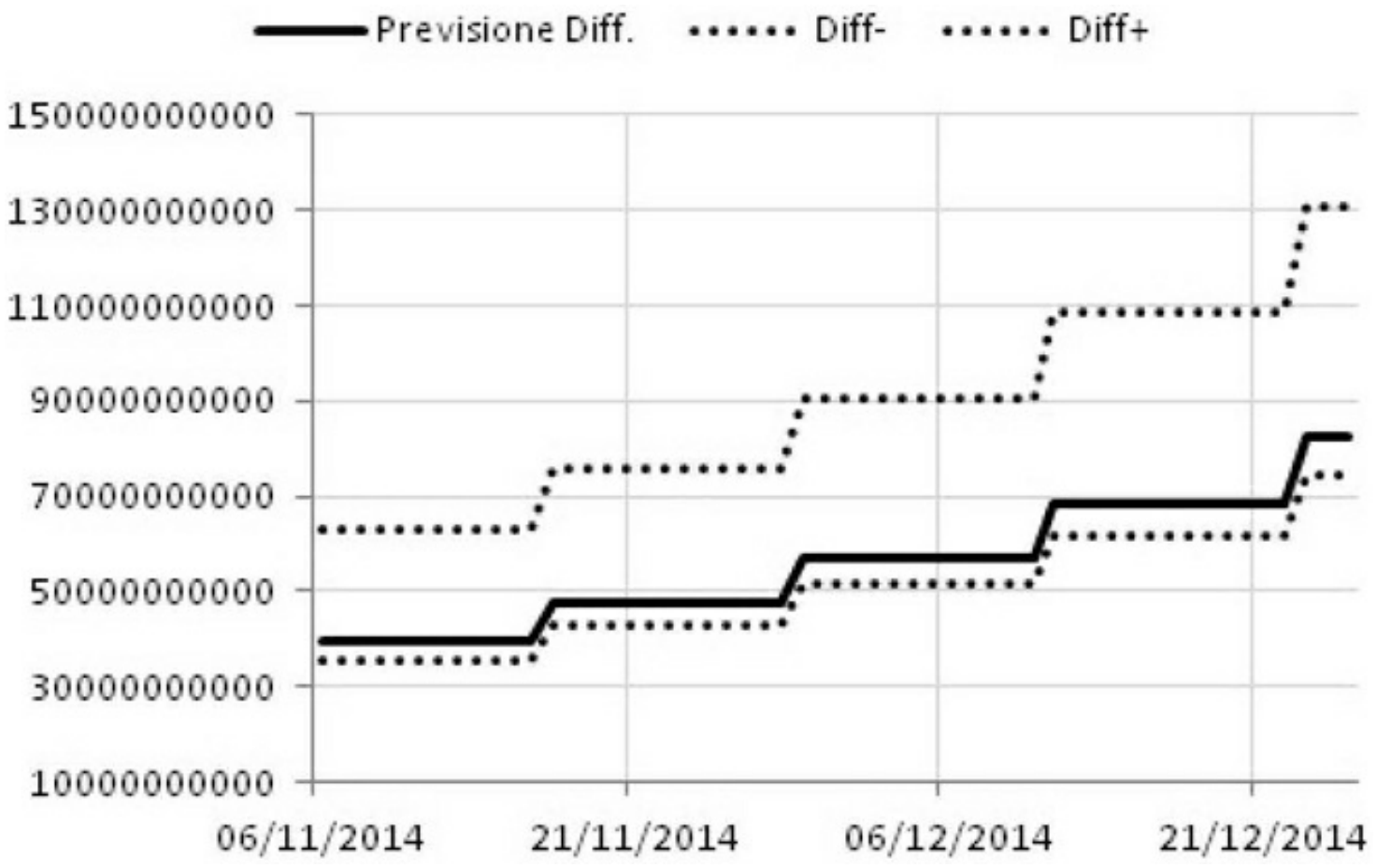


FIGURA 3.9 – Previsione del valore della Difficoltà.

La linea intera di colore nero rappresentata la previsione dei valori dei cambi della Difficoltà, mentre le altre due linee rappresentano la banda di oscillazione di questa previsione. In particolare la linea tratteggiata inferiore

è realizzata applicando la volatilità storica nei casi di variazione negativa della Difficoltà, invece la linea tratteggiata superiore è realizzata applicando la volatilità storica nei casi di variazione positiva della Difficoltà. Abbiamo preferito separare le due casistiche, poiché la rilevanza statistica delle variazioni negative della Difficoltà è bassa.

La previsione per il 17 novembre 2014 era di un valore della Difficoltà a 47.535.738.826 con una probabilità del 75%, secondo la disuguaglianza di Čebyšëv, che fosse compresa tra 42.907.191.328 e 75.479.344.909 (Tabella 3.8).

TABELLA 3.8 – Stima della Difficoltà.

Data	Stima Difficoltà	Banda inferiore	Banda superiore
06/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
07/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
08/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
09/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
10/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
11/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
12/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
13/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
14/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
15/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
16/11/2014	39.603.666.252	35.747.463.427	62.884.449.858
17/11/2014	47.535.738.826	42.907.191.328	75.479.344.909

Come sappiamo dalla Tabella 3.7 il cambio della Difficoltà si è verificato il 19 novembre, con un nuovo valore pari a 40.300.030.327. L'errore tra il valore effettivo e quello stimato è stato del 15% (Tabella 3.9).

TABELLA 3.9 – Delta errore nella stima della Difficoltà.

Data	Difficoltà	Stima Difficoltà	Delta Errore
19/11/2014	40.300.030.327	47.535.738.826	15%

Entrambe le previsioni effettuate si sono dimostrate molto attendibili, ma va ricordato che si tratta sempre e comunque di previsioni, non di certezze.

Da ultimo vi mostriamo un grafico a dispersione (Figura 3.10), che mette in relazione le variazioni percentuali della Difficoltà con il numero di giorni.

Possiamo notare che quando i minatori impiegano più tempo, rispetto ai 14 giorni teorici, per completare 2016 blocchi, la variazione percentuale della Difficoltà è negativa, rendendo più facile la successiva prova di lavoro. Al contrario, quando i minatori impiegano meno tempo di quello teorico, la variazione percentuale tende ad

aumentare, rendendo più complicata la successiva prova di lavoro.

I cambi di Difficoltà che abbiamo rappresentato a grafico sono 148, di cui l'80% si trova sotto alla soglia teorica dei 14 giorni (Tabella 3.10).

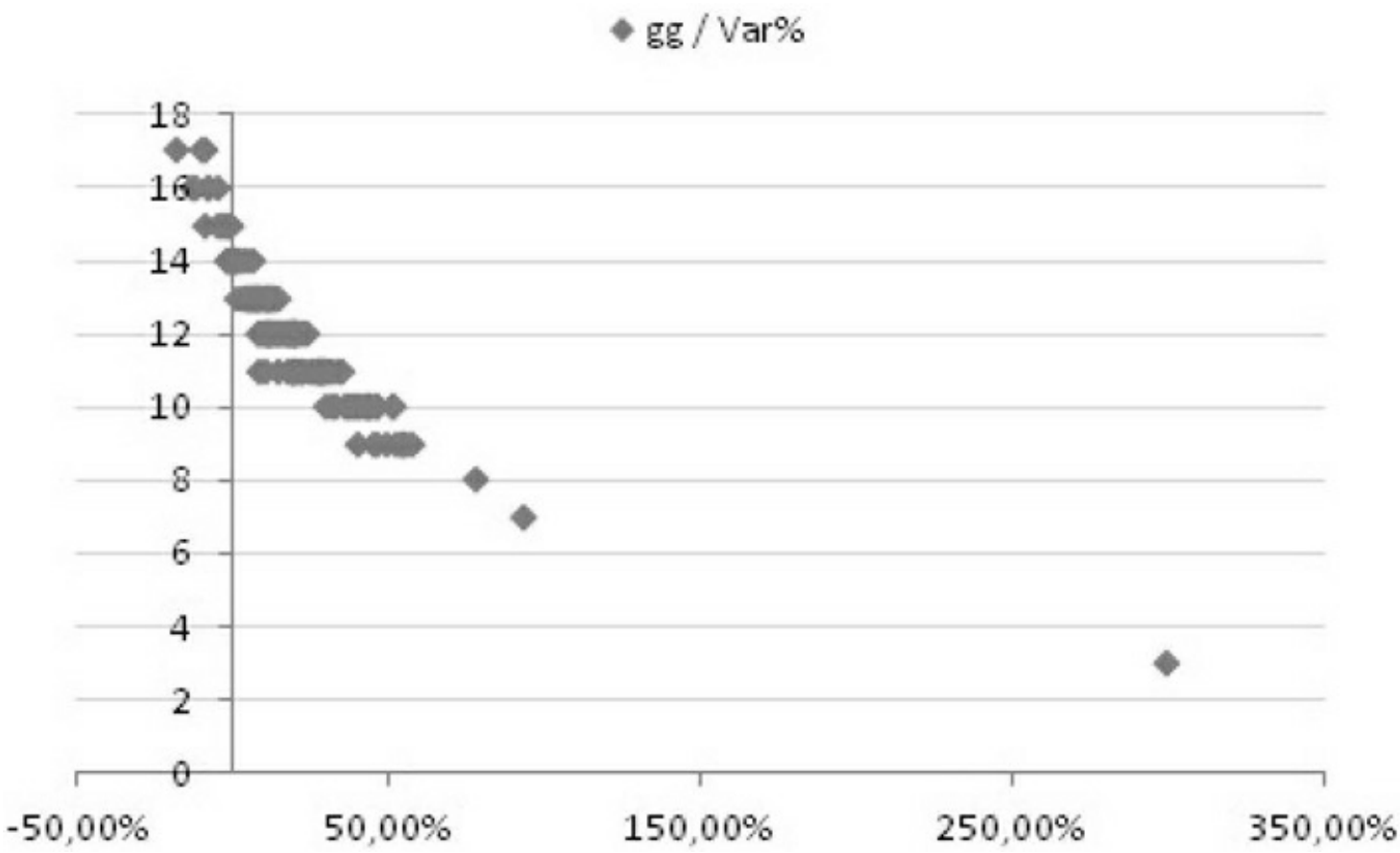


FIGURA 3.10 – Grafico a dispersione giorni/variazione Difficoltà.

TABELLA 3.10 – Percentuale cambi Difficoltà.

	N° giorni	%
< 14	119	80,5%
= 14	14	9,5%
> 14	15	10%

HASH RATE

L'Hash rate è la potenza complessiva, in Giga-Hash al secondo (GH/s), che il network sta eseguendo. Si tratta di un valore enorme, in crescita esponenziale, che ha superato i 300 milioni di Giga-Hash al secondo (Figura 3.11).

Su scala logaritmica si riesce meglio a interpretare il trend in atto (Figura 3.12).

Il grafico della Figura 3.12 mostra come l'Hash rate non sia mai sceso, ma al tempo stesso ha avuto una fase di stabilità di circa due anni, dalla metà del 2011 all'inizio del 2013, seguita da una nuova fase di accelerazione fino ai valori attuali, al 21 novembre 2014, di circa 250 milioni di Giga-Hash al secondo.

I lettori più attenti si saranno già accorti che questo grafico è del tutto simile a quello della Difficoltà che abbiamo mostrato in precedenza (Figura 3.13).

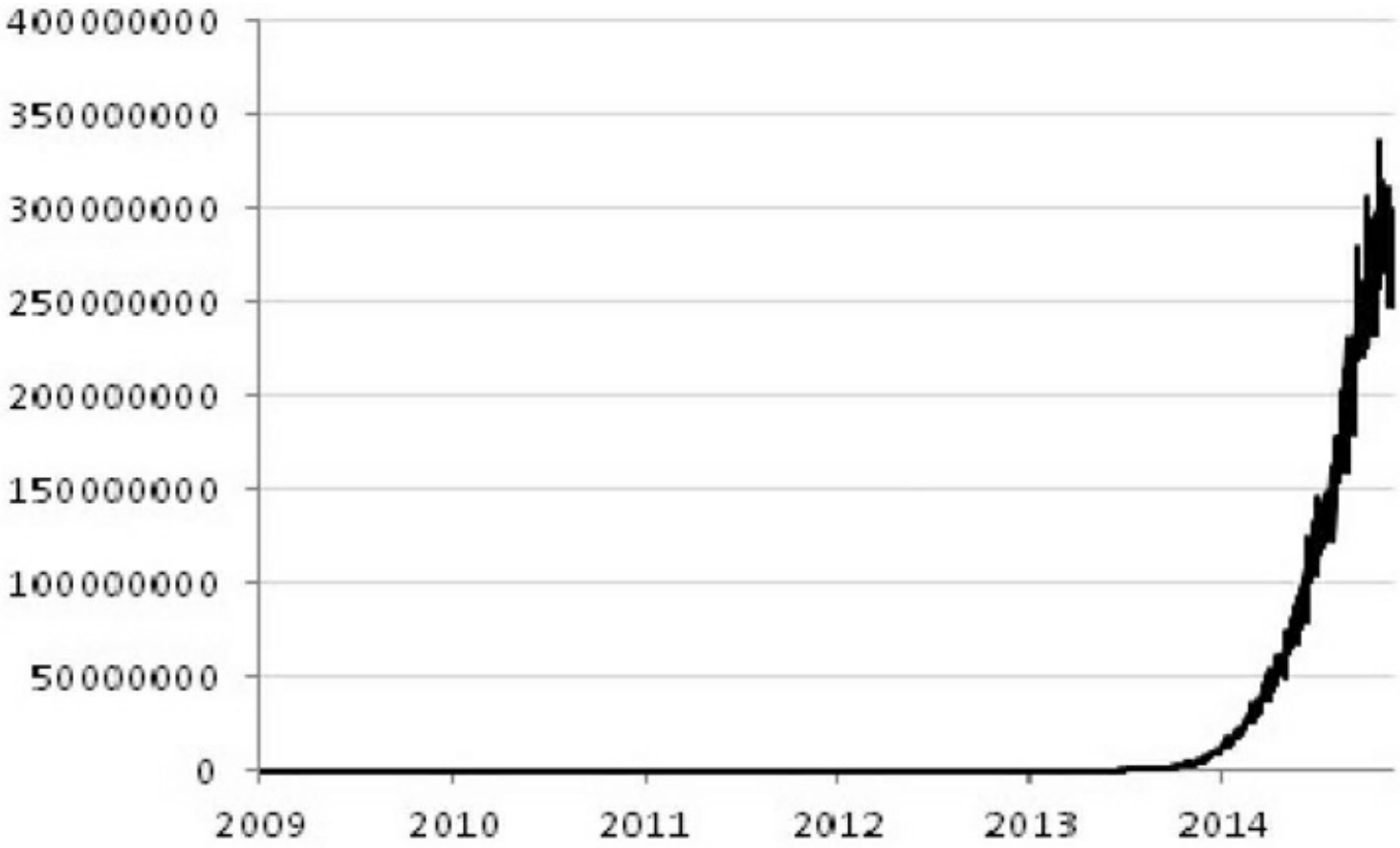


FIGURA 3.11 – La crescita dell'Hash rate (GH/s).

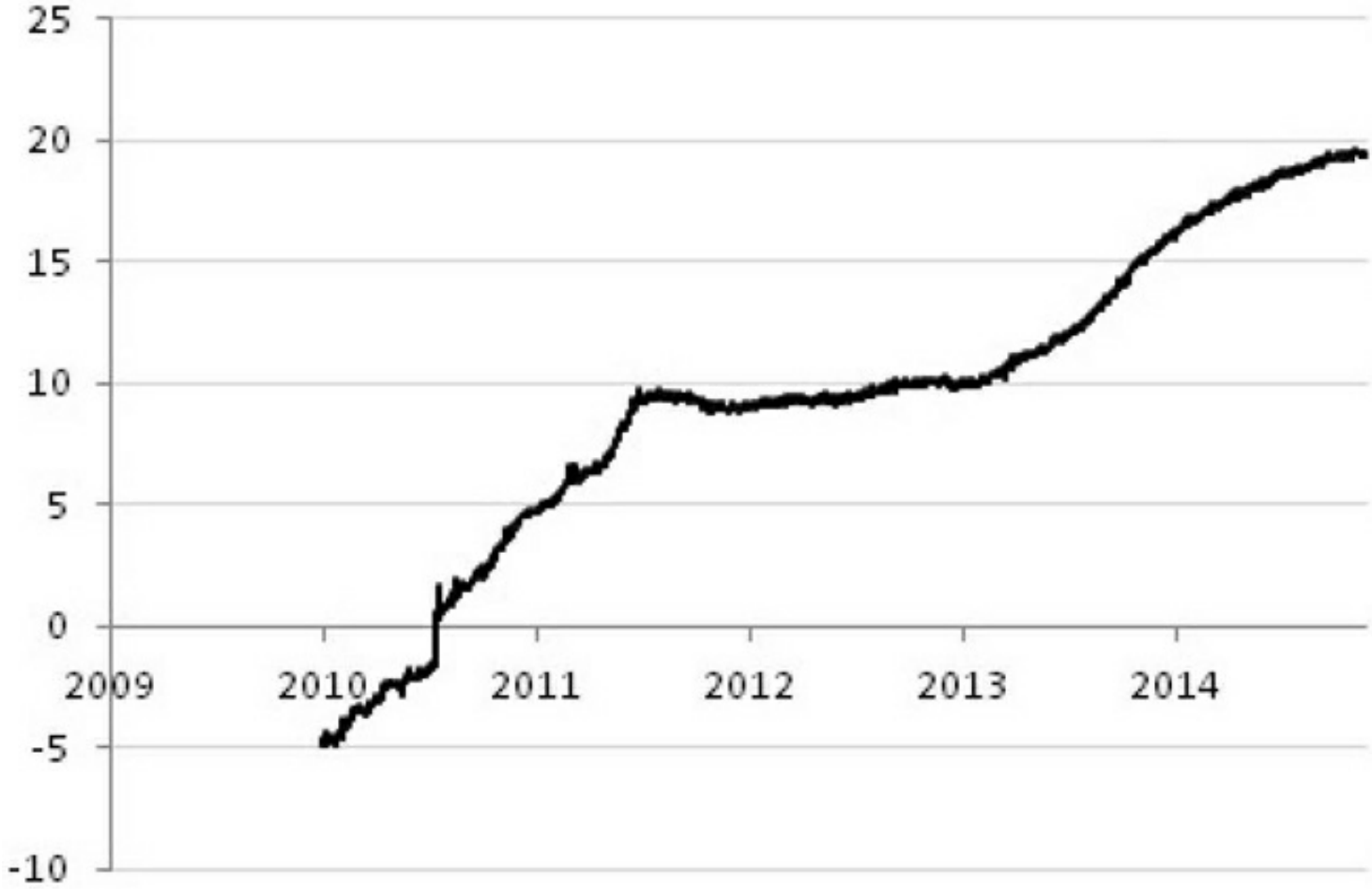


FIGURA 3.12 – Grafico logaritmico dell'Hash rate.

La Difficoltà è positivamente correlata con l'Hash rate e, da un punto di vista statistico, la correlazione di lungo periodo è quasi perfetta e pari a 0,999. È evidente che se nel network aumenta

la potenza di Hash allora è molto probabile che il tempo effettivo per la prova di lavoro diminuisca e sia inferiore a quello teorico, con la conseguenza che verrà aumentata la Difficoltà successiva (Figura 3.14).

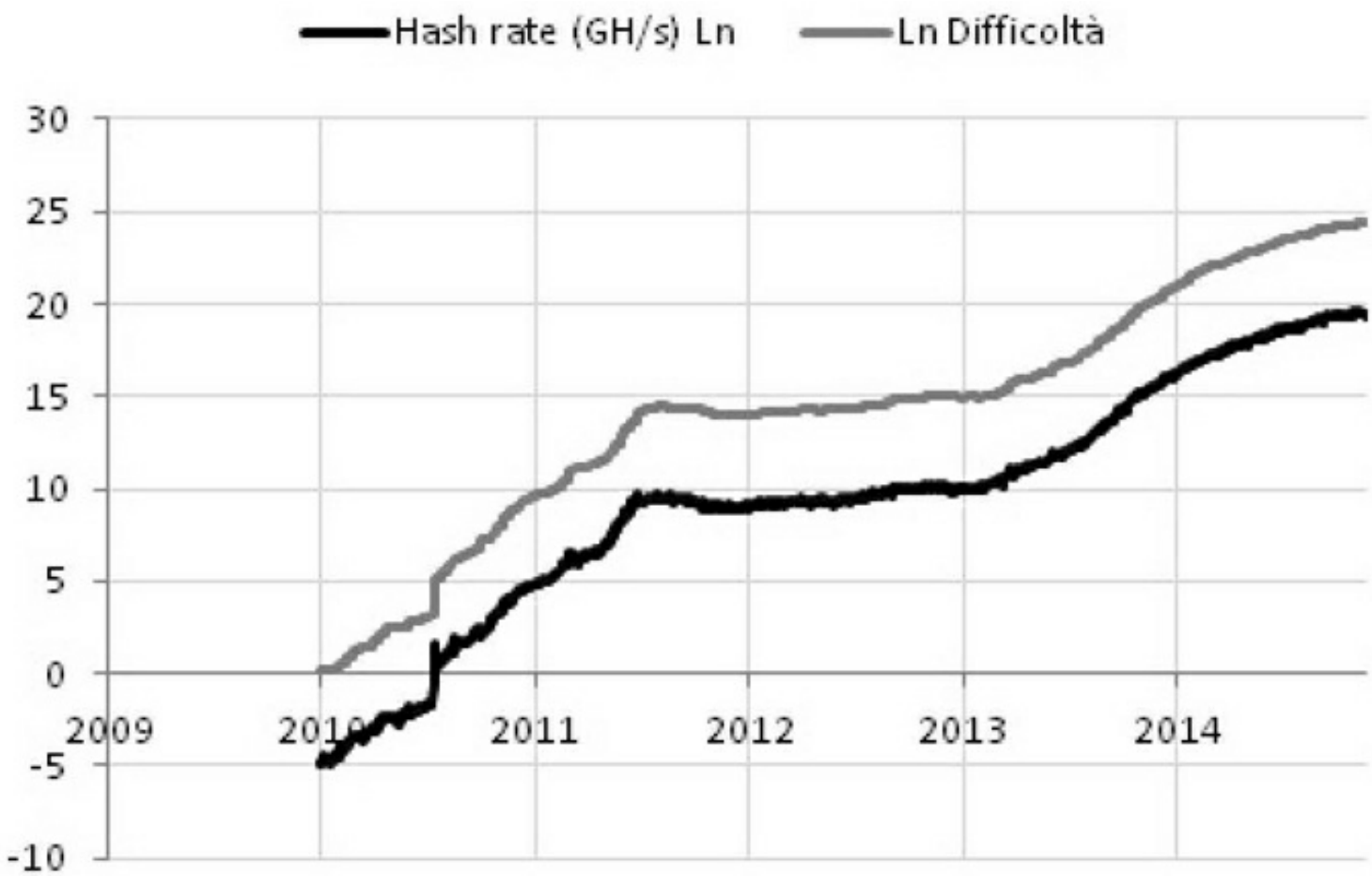


FIGURA 3.13 – Confronto tra Hash rate e Difficoltà su scala logaritmica.

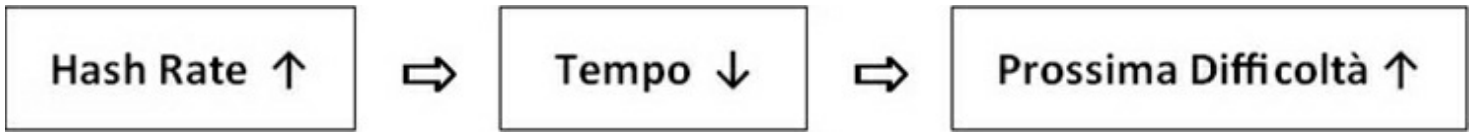


FIGURA 3.14 – Schema a blocchi Hash rate e Difficoltà.

Cerchiamo di analizzare da un punto di vista analitico che cosa succede all'Hash rate quando avviene un cambio di Difficoltà (Tabella 3.11).

TABELLA 3.11 – Analisi statistica dell'Hash rate.

N° Valori	149
Media	25,3%
Max (13/07/2010)	755,2%
Min (27/07/2010)	-60,6%
Dev.st.pop	69,15%

Curtosi	83,76
Asimmetria	8,16

Queste analisi sono state condotte sulle variazioni percentuali dei valori dell'Hash rate, le quali presentano la distribuzione di frequenza della Figura 3.15.

Durante i 149 cambi di Difficoltà, l'Hash rate è aumentato con una media del 25,3%, una deviazione standard del 69,15% e con un valore massimo di ben +755,2% il 13 luglio 2010.

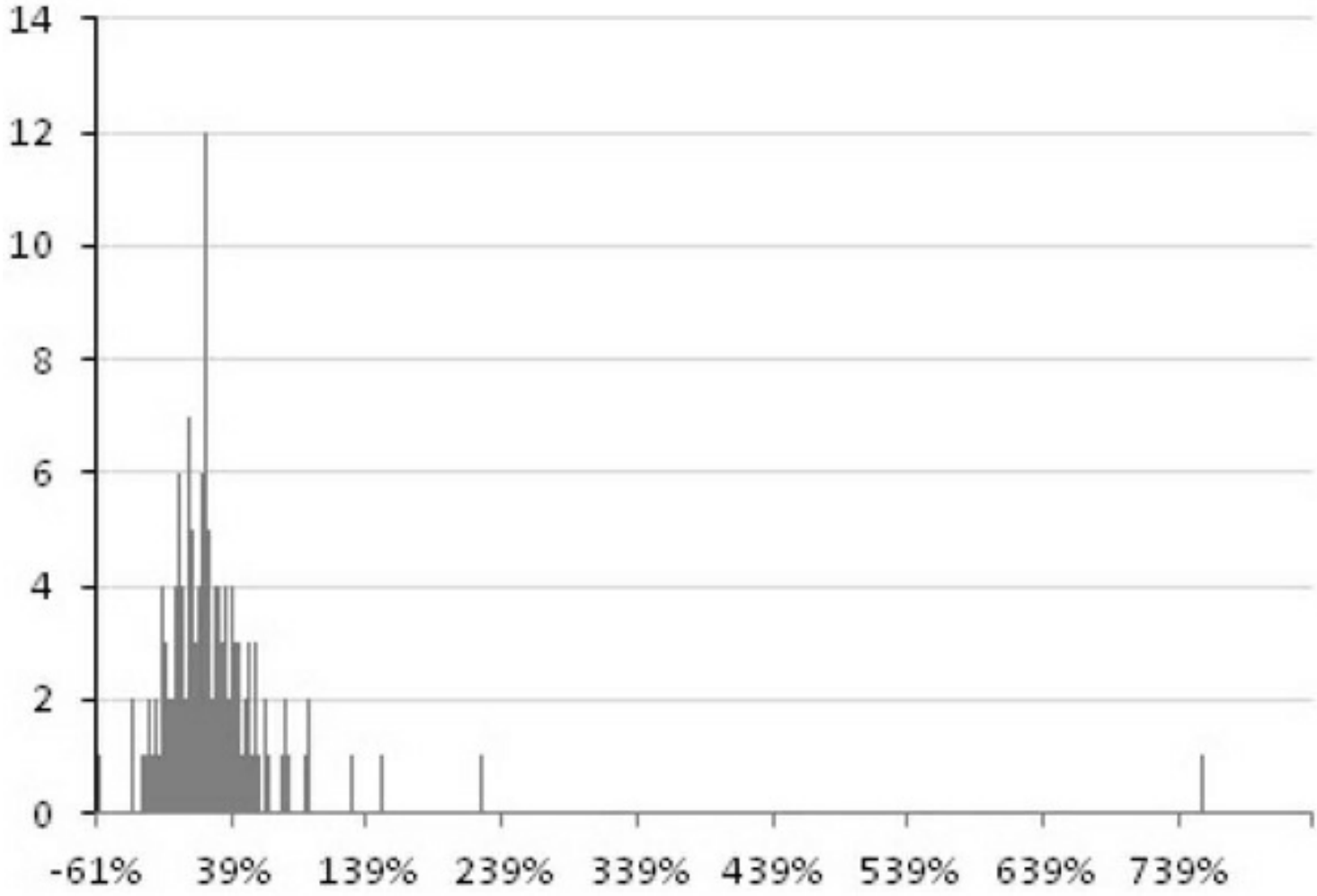


FIGURA 3.15 – Distribuzione di frequenza dell'Hash rate.

Gli indici di forma ci segnalano che la distribuzione è leptocurtica, con curtosi e asimmetria positivi.

Andando più in dettaglio, separiamo le variazioni percentuali positive da

quelle negative, come abbiamo fatto per la Difficoltà. Osservate la Tabella 3.12.

TABELLA 3.12 – Analisi statistica dell'Hash rate con distinzione dei casi positivi e negativi.

	Casi variazione positiva	**Casi variazione negativa**
Percentuale	73,83%	26,17%
N° valori	110	39
Media	39,1%	-13,7%
Max	755,2%	-0,6%
Min	0,1%	-60,6%

In 39 casi, il 26,17% del totale, la variazione è stata negativa con una media del -13,7% e un minimo del -

60,6%, registrato il 27 luglio 2010; mentre, nel restante 73,83%, la variazione è stata positiva con una media significativa del 39,1%.

Queste analisi ci testimoniano come la potenza di Hashing, e di conseguenza il network, sia in continua espansione. Non dimentichiamo che questi numeri non sono altro che lo specchio degli investimenti effettuati, e probabilmente ce ne saranno molti altri. Quello delle valute digitali è un settore in rapida evoluzione, con tassi di crescita elevati grazie alla forte attrazione di capitali.

---

13. L'header di un blocco è dato dalla combinazione di sei fattori: il numero di

blocco, l’Hash del blocco precedente, l’Hash del MerkleRoot, il tempo, il Bits e il Nonce.

CAPITOLO 4

Costo e Fair value del Bitcoin

COSTO DELLA GENERAZIONE DEI BITCOIN

Pensiamo al primo paragone che viene in mente quando si parla di mining: la leggendaria corsa all'oro in California nel 1840. Molte persone con pochi mezzi furono in grado di raccogliere fortune immense. Pensiamo, oggi, a quale infrastruttura multimiliardaria e che tipo di investimento sia invece necessario per poter estrarre e produrre l'oro. Com'è stato per questa industria, con il passare del tempo, anche minare bitcoin si è

rivelato sempre più complesso e difficile. Se nei primi anni un semplice PC domestico era in grado di produrre centinaia di bitcoin al giorno; al momento della scrittura di questo libro, un hardware specializzato, denominato ASIC (Application Specific Integrated Circuit), al costo di diverse migliaia di dollari, è in grado di produrre solamente una frazione di bitcoin al giorno. Questo effetto è legato all'aumento esponenziale della Difficoltà di risoluzione dell'algoritmo che è alla base della creazione di nuovi bitcoin e che abbiamo analizzato nel capitolo precedente. Procediamo ora con la nostra analisi, che ci porterà a stimare il costo di produzione di un bitcoin. Come

prima cosa analizziamo le ASIC attuali. Nella Tabella 4.1 elenchiamo le principali macchine che sono presenti in questo settore e le relative specifiche tecniche.

TABELLA 4.1 – Confronto hardware per il Bitcoin mining.

ASIC UNIT	TerraMiner IV	KnC Neptune	AntMiner S3
Hash Power (GH/s)	2.000	3.000	478
Enegy Usage (W)	2.200	2.200	366
W/GH	1,100	0,733	0,766
Unit Pice ($)	$ 3.999	$ 6.499	$ 540
$/GH	$ 2,00	$ 2,16	$ 1,13

Per semplificare la nostra analisi occorre fare tre ipotesi:

- Tutta la rete Bitcoin è popolata dalla macchina più efficiente (in termini di $/GH): la BitMain

AntMiner S3 ASIC nel nostro caso.

- Un mercato in concorrenza perfetta, costituito da piccoli miner che acquistano la macchina più efficiente sul mercato, appena è disponibile.
- La tecnologia delle macchine di mining, che sono in grado di tenere il passo con la crescente difficoltà mantenendo costante tale rapporto.

Spesa di capitale

Teoricamente, andando a dividere i 220 milioni GH/s (al novembre 2014) in

equivalenti BitMain AntMiner S3 ASIC (478 GH/s ciascuna), otteniamo approssimativamente 460,251 unità, che al prezzo di $ 540 ciascuna danno una spesa totale pari a $ 248,5 milioni.

Assumendo che tale spesa debba essere sostenuta ogni anno per poter tenere il passo con la Difficoltà crescente, e mantenendo così costante il ritmo di produzione attuale (l'ipotesi è molto forte ma riesce a darci un'idea puntuale del costo di produzione ed è facilmente rimovibile aprendo la possibilità a un'analisi di sensibilità), otteniamo una spesa annua pari a $ 248,5 milioni. Al tasso odierno di remunerazione di 25 bitcoin ogni 10 minuti, otteniamo una produzione di

1.314.900 bitcoin minati ogni anno. Questo equivale quindi a un CAPEX[14] per bitcoin pari a:

$$\text{CAPEX} = \$\ 248{,}5 \text{ milioni} / 1{,}3149 \text{ milioni bitcoin} = \$\ 189$$

Spesa operativa

Analizziamo ora i costi operativi di tale soluzione. Con un Hash rate di rete pari a 220 milioni GH/s la rete necessita di 0,766[15] × 220 milioni W= 168.520 kW. Il che equivale a 168.520 kW × 24 ore/giorno × 365 giorni/anno = 1.476.235.200 KWh/anno. Questo

equivale a circa 5,3 milioni di Gj/anno e 887.328 tonnellate di CO_2/anno. Ipotizzando un costo dell'elettricità pari a 70 $/MWh otteniamo OPEX[16] totali pari a $ 103,33 milioni. Prendendo sempre lo stesso dato di produzione annua di bitcoin otteniamo un OPEX per bitcoin pari a:

OPEX = $ 103,33 milioni / 1,3149 milioni bitcoin = $ 79

Costo totale

Sommando quanto trovato dalla nostra analisi dei CAPEX e degli OPEX

otteniamo, infine, un costo di mining per un bitcoin pari a:

$$CAPEX + OPEX = \$\ 189 + \$\ 79 = \$\ 268$$

Questo livello segna un forte supporto per l'eventuale prezzo del bitcoin, ed essendo un costo semplice di produzione occorre aggiungere tutti i costi aggiuntivi e la remunerazione dei produttori. Il pregio di questa analisi è il fatto di essere facilmente scalabile e, modificando le ipotesi della macchina di partenza, è altrettanto agevole ricostruire il costo di produzione per i differenti produttori, a seconda della caratteristiche del loro "parco impianti".

CONFRONTO BITCOIN, ORO E VALUTE

A valle del paragrafo precedente siamo stati in grado di stimare il costo economico della produzione di bitcoin. Cerchiamo ora di dare un'idea di quelli che possono essere, invece, gli impatti socio-ambientali legati alla loro produzione. Spesso, tali impatti vengono dipinti dalla stampa interessata come totalmente catastrofici nei confronti dell'ambiente e si delineano degli scenari disastrosi di enormi macchine fumanti ed energivore che non fanno altro che risolvere problemi per

generare moneta. Pochi, però, hanno provato a fare un raffronto con i costi e gli impatti derivanti dalla produzione di altre forme di moneta. Cercheremo quindi di fornire alcuni dati e delle rapide pennellate per dare un'idea di massima di quanto "impattante" sia la produzione di bitcoin e siamo certi che resterete sicuramente sorpresi dalle conclusioni.

Confronto costi economici

Partiamo dall'analisi economica. È di dominio comune il fatto che, in particolare nei Paesi industrializzati, il costo legato alla produzione di moneta

fisica in metallo per le valute a basso valore nominale (per esempio, le monete da 1 e 2 centesimi ecc.) è superiore al valore della stessa. Ovviamente ciò è dovuto al costo sempre maggiore dei principali metalli che sono alla base della lega utilizzata per la sua produzione (nickel e rame in particolare) (Tabella 4.2). A titolo esemplificativo, il governo dei Stati Uniti d'America spende 1,83 cent di dollaro per produrre la moneta da 1 cent; mentre, per venire alla nostra valuta, nel 2013 l'Irlanda ha speso 11,8 milioni di euro per produrre monete da € 1 per un valore totale di € 7,1 milioni.

Allo stesso modo, i costi sostenuti per la produzione dell'oro sono in

costante e vertiginoso aumento, dovuto sia alla scarsità della risorsa sia alle sempre maggiori difficoltà tecniche da superare per raggiungere nuovi campi di produzione.

TABELLA 4.2 – Confronto costi economici.

Tipologie di produzione	Costo annuale lordo
Produzione oro	$ 105 miliardi
Produzione moneta	$ 28 miliardi
Produzione bitcoin	$ 0,78 miliardi

È immediato constatare che i costi di creazione di questa moneta digitale sono minimali rispetto alle tradizionali "riserve di valore" normalmente

utilizzate, pari circa all'1% e al 3% rispettivamente nei confronti dell'oro e della moneta.

Confronto costi ambientali

Ancora più schiacciante risulta il confronto se si vanno ad analizzare gli impatti ambientali. Ci limitiamo a presentare i dati relativi al consumo di energia e le tonnellate di CO_2 introdotte nell'atmosfera, senza tener conto di tanti altri fattori comunque impattanti per le produzioni tradizionali (spreco di carta, coloranti, additivi chimici dispersi nell'ambiente, morti in miniera ecc.)

(Tabella 4.3).

TABELLA 4.3 – Confronto costi ambientali.

Tipologie di produzione	**Energia usata (GJ)**	**Tonnellate di CO_2**
Produzione oro	475 milioni	54 milioni
Produzione moneta	39,6 milioni	6,7 milioni
Produzione bitcoin	3,6 milioni	0,6 milioni

I dati ci mostrano un impatto ambientale molto limitato del bitcoin rispetto alle riserve di valore tradizionali. C'è inoltre da tenere conto che l'unica fonte utilizzata nella produzione di bitcoin è l'energia elettrica, che si sta spostando

sempre più verso fonti rinnovabili. Progressivamente più alta, poi, sta diventando l'efficienza e il riciclo delle componentistiche delle ASIC. Infine, c'è da ricordare, come mostrato in precedenza, che le macchine per il mining di bitcoin seguono e continueranno a seguire le leggi di Moore e Koomey e che quindi gli impatti ambientali già limitati andranno ulteriormente a ridursi.

Quindi, abbiamo visto come non sia per nulla vero che la produzione di bitcoin sia dannosa per l'ambiente e che anzi, in confronto alla moneta e all'oro, presenti indubbi vantaggi di sostenibilità.

FAIR VALUE DEL BITCOIN

Il valore del bitcoin, come avremo modo di analizzare approfonditamente nel corso del libro, è molto volatile ed è cresciuto di oltre 100 volte nel corso dell'ultimo anno. È spontaneo, quindi, chiedersi se tale fenomeno sia o meno frutto di una bolla speculativa. Prima di poter rispondere a questa domanda, però, risulta necessario cercare di stimare il potenziale Fair value[17] del bitcoin.

Cerchiamo di portare avanti un'analisi che ha l'obiettivo di andare a

stimare il valore corretto da assegnare al bitcoin. Precisiamo, fin da subito, che tale valore è da intendersi come un valore corretto di medio periodo e non è da escludere che, nel breve o lungo periodo, si discosti anche notevolmente dalla quotazione in Borsa, in seguito a logiche speculative. L'analisi prende in considerazione i due valori che il bitcoin racchiude in sé: il valore intrinseco come mezzo di scambio e il valore come riserva di valore.

Fair value come mezzo di scambio

Iniziamo prendendo in considerazione il valore del bitcoin come mezzo di scambio, e concentriamoci in particolare sui suoi possibili utilizzi nel campo dell'e-commerce. Per esempio, ipotizziamo di volere considerare il Fair value del bitcoin se solo un 10% dei pagamenti online iniziasse a essere fatto attraverso di esso. La spesa online dei cittadini americani è pari a 10 miliardi di dollari. Supponendo che un 10% di tutti questi pagamenti siano fatti attraverso bitcoin, otteniamo circa 1 miliardo di dollari di valore. E se prendiamo in considerazione il mondo intero? Il prodotto interno lordo degli Stati Uniti è circa il 20% del PIL

mondiale, quindi, assumendo un grado di penetrazione dell'e-commerce nel resto del mondo e stimando conservativamente il valore, otteniamo un valore di circa 4 miliardi di dollari per il bitcoin su scala mondiale. Questo è certamente un numero derivante da un'analisi ad alto livello, ma aiuta a farci un'idea di questo possibile Fair value.

Consideriamo ora il valore insito nel bitcoin, e derivante dalla possibilità di utilizzarlo come mezzo di trasferimento di moneta. Ciò può essere fatto con estrema facilità e velocemente (tra i 10 e i 50 minuti a seconda che sia una persona conosciuta o meno). Come possiamo quantificare tale valore? Il

settore del trasferimento di denaro è dominato da tre top player: Western Union, MoneyGram e Euronet, ognuno con circa il 20% di quota di mercato. Possiamo ipotizzare che il bitcoin sarà in grado di strappare quote di mercato a questi top player e imporsi grazie ai suoi bassissimi costi di gestione e commissioni.

Cosa implica questo nella valutazione del Fair value? Dato che l'offerta di bitcoin è limitata, chi ne riceve non ottiene solo un mezzo di scambio, ma è come se avesse un piccolo investimento nell'industria Bitcoin. La capitalizzazione media dei tre top player è di circa 4,5 miliardi di

dollari. Questo è sicuramente una buona stima di quello che può essere il valore del bitcoin come mezzo di scambio.

Otteniamo così un primo interessante risultato. Il Fair value totale, come mezzo di scambio del bitcoin, può essere valutato come somma del valore di 4 miliardi di dollari derivanti dall'e-commerce e dei 4,5 miliardi di dollari derivanti dal suo essere un mezzo di trasferimento di moneta:

Fair value bitcoin come mezzo di scambio = $ 8,5 miliardi

Fair value come riserva di

valore

Questa è sicuramente la parte più complessa dell'analisi. Come abbiamo visto in precedenza, possedere bitcoin è come avere una percentuale in un investimento nell'universo Bitcoin, data la limitatezza del numero degli stessi. C'è da aggiungere che questo investimento non paga alcun interesse, e quindi possiamo facilmente assimilarlo a un investimento in un metallo prezioso. È infatti abbastanza evidente, dopo quanto abbiamo già raccontato, come oro e bitcoin abbiano molto in comune: entrambi non pagano interessi e l'offerta è limitata. Al momento il valore dell'oro è di circa 1,3 trilioni di dollari. Può il

bitcoin raggiungere tale valore? Noi ne dubitiamo.

Prima di tutto perché è ancora molto più volatile dell'oro, il che rende l'investimento sicuramente più rischioso e meno attrattivo per investitori avversi al rischio. Inoltre, l'oro ha una reputazione unica di bene rifugio, costruita in più di diecimila anni di storia, ed è sicuramente questa la chiave del successo di questo metallo che è arrivato a valere fino a 60 volte il valore dell'argento. Facciamo un'ipotesi ambiziosa: cioè che il bitcoin riesca ad avvicinarsi alla reputazione dell'argento (il valore delle scorte nei soli Stati Uniti è pari circa a 5 miliardi di dollari) e ipotizziamo, quindi, un valore pari a 4

miliardi di dollari.

Fair value bitcoin come riserva di valore = $ 4 miliardi

Fair value finale

Siamo giunti alla conclusione della nostra ambiziosa analisi. Riportiamo di seguito il valore finale calcolato:

Fair value bitcoin totale = $ 12,5 miliardi

Dato un numero di bitcoin, al 21 novembre 2014, pari a 13.521.050 otteniamo:

Fair value bitcoin = $ 925

COSTO E FAIR VALUE A CONFRONTO

Chiudiamo la Parte 2 del libro richiamando quanto visto nei paragrafi "Costo della generazione dei bitcoin" e "Fair value del bitcoin". Nel primo abbiamo analizzato il costo di produzione del bitcoin, e il nostro modello ha calcolato un valore pari a $ 268. Nel secondo, invece, abbiamo portato avanti una complessa analisi del Fair value, trovando un valore pari a $

925. È importante ora vedere come tali valori si siano comportati nei confronti del prezzo del bitcoin. Per semplicità e chiarezza di visualizzazione prendiamo in esame i prezzi dal 1° gennaio 2014 (Figura 4.1).

FIGURA 4.1 – Costo e Fair value del Bitcoin.

Notiamo immediatamente come i due valori da noi calcolati creino proprio un range all'interno del quale il prezzo del bitcoin può oscillare. Tali bande sono già in grado di fornirci previsionalmente un limite massimo e un limite minimo, all'interno dei quali il prezzo può

muoversi. Inoltre, con cadenza annuale o al sopraggiungere di un cambiamento delle condizioni al contorno (macchine più performanti, maggior utilizzo del bitcoin ecc.), è possibile portare avanti una nuova analisi (seguendo esattamente tutti i passi da noi presentati) e calcolare di volta in volta il nuovo costo di generazione e il nuovo Fair value del bitcoin, per tenere tali previsioni sempre allineate al mutevole contesto del mercato.

---

14. Si intendono per CAPEX quei fondi che un'impresa impiega per acquistare asset durevoli nel tempo, per esempio macchinari.
15. Il rapporto W/GH della BitMain AntMiner

S3 ASIC indicato nella Tabella 4.1.

16. Si intendono per OPEX i costi necessari per gestire un prodotto o un business, sono quindi i costi operativi e di gestione.

17. Per Fair value si intende una stima razionale e imparziale del prezzo di un bene o servizio, tenendo conto di vari fattori, tra cui la scarsità, l'utilità, il rischio e il costo di produzione o di rimpiazzo.

PARTE III

Il Trading

Il denaro non dorme mai.

Gordon Gekko, *Wall Street* (1987)

CAPITOLO 5

Mercati OTC e mercato Forex

I MERCATI OTC

Nei precedenti capitoli abbiamo svolto delle analisi statistiche sugli aspetti fondamentali che regolano il funzionamento del network Bitcoin. Abbiamo verificato le variazioni percentuali storiche della Difficoltà, dell'Hash rate e il legame tra queste due grandezze, spingendoci a prevederne anche le possibili evoluzioni.

Prima di svolgere delle analisi sui prezzi, presentiamo il funzionamento e le caratteristiche dei mercati sui quali i bitcoin sono negoziati. I bitcoin sono scambiati su mercati non regolamentati, noti come mercati OTC (Over The

Counter), i quali presentano le seguenti caratteristiche:

- sono mercati decentralizzati;
- sono privi di cassa di compensazione;
- presentano ridotti costi di transazione;
- hanno un rischio maggiore rispetto ai mercati regolamentati.

Questi mercati si distinguono in maniera radicale da quelli tradizionali, per il fatto di essere privi di una localizzazione fisica e perché le negoziazioni avvengono in maniera bilaterale su piattaforme o altri mezzi di

comunicazione. Un mercato regolamentato, quale per esempio il NYSE (New York Stock Exchange), ha una localizzazione precisa, gli scambi avvengono solo nei locali della Borsa, al numero 11 di Wall Street (New York), e attraverso piattaforme elettroniche gestite dall'exchange. Inoltre, i mercati regolamentati presentano una disciplina relativa all'organizzazione, all'operatività e ai requisiti di quotazione. Tali regolamenti sono approvati da un'autorità centrale, che negli Stati Uniti è la SEC (Securities and Exchange Commission), la quale svolge un ruolo di controllo, di vigilanza e di tutela del mercato. In aggiunta, vi è la presenza delle casse di

compensazione, o *clearing houses* (per esempio la The Depository Trust & Clearing Corporation – DTCC), che fungono da sistema di garanzia come controparti centrali, assumendosi il rischio di insolvenza degli operatori che partecipano al mercato. Per svolgere questo ruolo, le casse di compensazione impongono ai partecipanti dei requisiti di adesione, di margine, di risorse patrimoniali e finanziarie. Tale architettura, tuttavia, non elimina il rischio di insolvenza, ma sicuramente lo riduce rispetto ai mercati non regolamentati.

Capite bene che le differenze che abbiamo appena esposto sono

significative, e in estrema sintesi si traducono in un rischio maggiore per l'operatività su mercati OTC rispetto a quella su mercati regolamentati.

Durante la recente crisi finanziaria iniziata nel 2008, colossi quali Lehman Brothers, Bear Stearns e AIG sono miseramente falliti a causa di un'operatività sfrenata e altamente speculativa sui mercati OTC. Il pensiero comune del "*too big to fail*" è stato smentito, e schiacciato dall'evidenza che il cosiddetto rischio sistematico e l'effetto domino possano arrecare danni seri a tutto il sistema finanziario.

Nel mondo dei bitcoin abbiamo già assistito a un clamoroso fallimento, quello di Mt. Gox. Nel caso specifico,

questa azienda aveva una posizione da monopolista, con oltre il 90% del volume mondiale tradato in bitcoin. Questa situazione, abbinata anche a un servizio di scarsa professionalità, ha dato spazio a operazioni di tipo fraudolente e alla scomparsa di oltre 700.000 bitcoin di proprietà dei clienti. Non ci sono, per ora, delle sentenze definitive, ma tutto lascia supporre che ci sia stata un'attività criminale, nata e cresciuta proprio negli anfratti dell'inefficienza del mercato OTC.

Al di là di tutto, si è comunque trattato di un fallimento, uno dei tanti nel corso della storia dell'economia. Così come quanto accaduto a Lehman

Brothers non ha distrutto il sistema bancario, allo stesso modo il fallimento di Mt. Gox non ha distrutto il settore delle valute digitali, ma lo ha spinto alla ricerca di una maggior efficienza e trasparenza.

Come si può osservare dal grafico in Figura 5.1, la discesa dei prezzi di Mt. Gox non ha intaccato l'Hash rate, che ha proseguito il proprio trend al rialzo confermando che l'attività sottostante al trading, cioè il mining, era in salute:

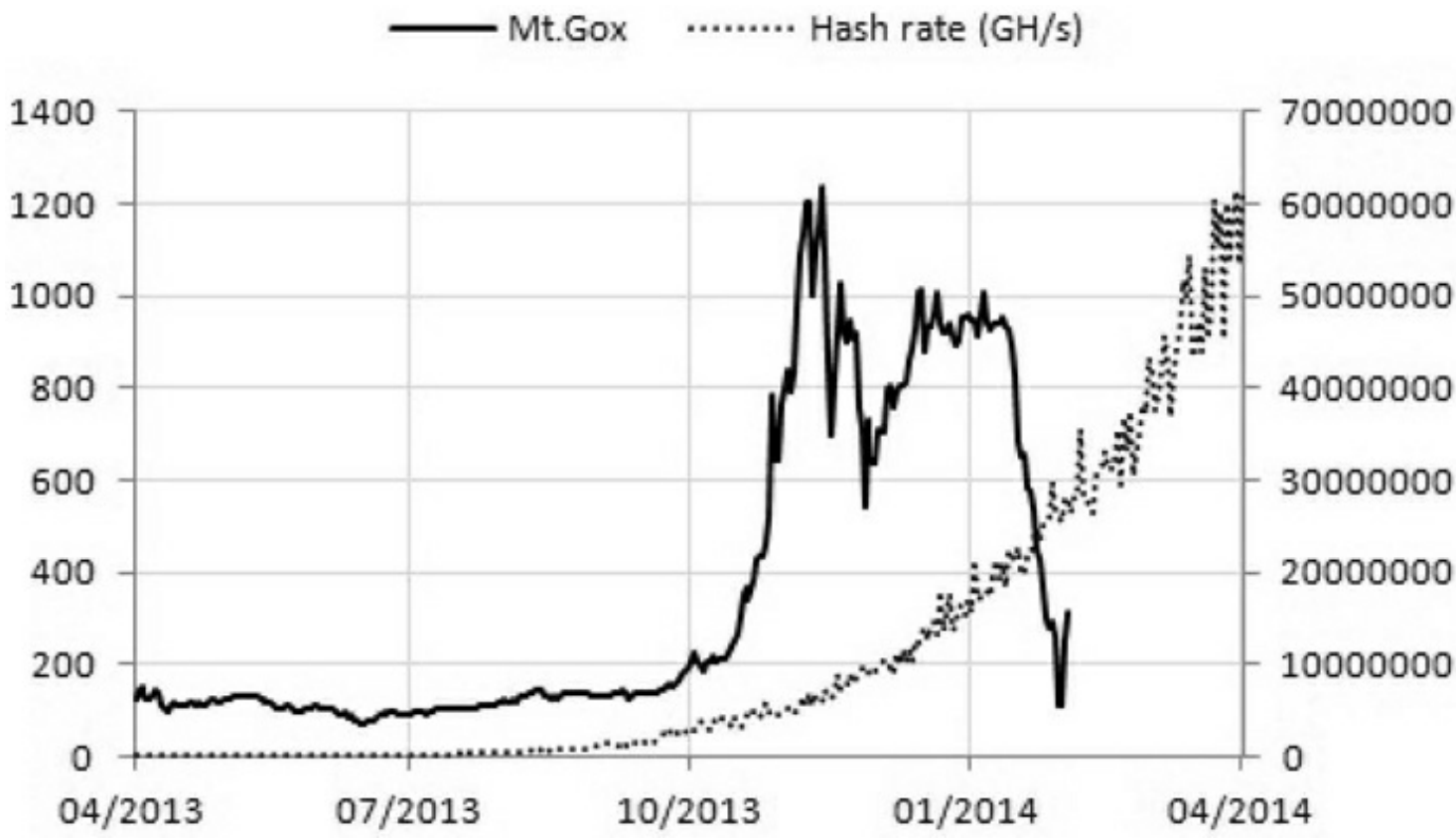


FIGURA 5.1 – Prezzo bitcoin su Mt. Gox e Hash rate.

Al tempo stesso, anche l'attività di negoziazione sugli altri exchange non si è arrestata. Il CoinDesk BPI (Bitcoin Price Index) è un indice pubblicato dal sito www.coindesk.com e sintetizza, in base a determinati criteri, il prezzo del

bitcoin negoziato su vari exchange. Si può correttamente assumere come benchmark in sede di analisi.

Nel grafico della Figura 5.2 confrontiamo, su time frame giornaliero, l'andamento del CoinDesk BPI con il prezzo di Mt. Gox.

I valori di prezzo sono sostanzialmente allineati, con la sola eccezione dei prezzi tradati sulla piattaforma di Mt. Gox a inizio 2014, cioè quando sono emersi i problemi di liquidità di questo exchange. In questa circostanza non era possibile nemmeno svolgere operazioni di arbitraggio, cioè per esempio comprare bitcoin su Mt. Gox e rivenderli su un altro exchange, traendo profitto dalla differenza di

prezzo. Questo perché i conti operativi di questa azienda erano bloccati e non permettevano di effettuare nessuna forma di cash out, né in valuta *fiat* né in bitcoin.

La conclusione di tutto quanto abbiamo scritto si esaurisce nel valutare attentamente il proprio profilo di rischio e agire di conseguenza.

FIGURA 5.2 – Prezzo bitcoin su Mt. Gox e CoinDesk BPI.

Concludiamo questa analisi citando due celebri frasi, per ricordavi che i fallimenti non sempre hanno un'accezione negativa… Dipende dai punti di vista:

Il fallimento è semplicemente l'opportunità di ricominciare, questa volta in modo più intelligente.

Henry Ford

Il successo consiste nel saltare di fallimento in fallimento senza mai perdere l'entusiasmo.

Winston Churchill

IL MERCATO FOREX

Per come siamo abituati a trattarle nella nostra vita quotidiana, le valute sono soggette a un tasso di cambio. Ma non sempre è stato così.

Facciamo un breve salto indietro nella storia e precisamente nel 1944, a Bretton Woods. In questa località, nello Stato americano del New Hampshire, i delegati di 44 Nazioni siglarono degli accordi internazionali ("Bretton Woods Agreement") che sancirono la nascita

della World Bank, del Fondo Monetario Internazionale (FMI) e, fatto ancora più importante, il blocco delle fluttuazioni dei tassi di cambio. Gli Stati aderenti a tale accordo avevano, infatti, il dovere di adottare una politica monetaria volta a stabilizzare il tasso di cambio della propria valuta a un valore fisso rispetto al dollaro americano, che a sua volta era agganciato all'oro con un cambio di $ 35 a oncia. Questi accordi restarono in vigore per quasi 30 anni, esattamente fino al 15 agosto 1971, quando l'allora presidente degli Stati Uniti, Richard M. Nixon, annunciò unilateralmente la sospensione della convertibilità del dollaro in oro.

Nel dicembre del 1971, lo

“Smithsonian Agreement” sostituì gli accordi di Bretton Woods, fissando una fluttuazione massima del ± 2,25% per le valute nei confronti del dollaro americano. Tuttavia, pochi anni dopo, l’elevata inflazione causata dallo shock petrolifero e l’aumento delle pressioni speculative fece abbandonare definitivamente il sistema a cambi fissi dando spazio al sistema a cambi fluttuanti. Da quel momento le valute sono state negoziate liberamente sul mercato Forex (Foreign Exchange Market), secondo le forze di domanda/offerta.

Il Forex è un mercato OTC che presenta delle caratteristiche uniche

rispetto agli altri mercati finanziari, in particolare ricordiamo che si tratta di un mercato delocalizzato con possibilità di tradare 24 ore al giorno, esclusi i weekend. Inoltre, a oggi, rappresenta il primo mercato mondiale per volumi di scambi e anche per numero di partecipanti attivi.

Trattandosi di un mercato OTC delocalizzato, non è agevole stimare l'effettivo controvalore negoziato sul mercato Forex. L'unico dato ufficiale è fornito dalla Banca dei Regolamenti Internazionali (BRI), che periodicamente raccoglie e pubblica i dati forniti dalle principali Banche Centrali del mondo.

In base all'ultimo report disponibile, la media del turnover giornaliero è in

continua crescita e, nel 2013, ha raggiunto il valore di $ 5345 bilioni al giorno (Tabella 5.1).

TABELLA 5.1 – Media dei turnover giornalieri (in bilioni di dollari) sul mercato Forex.

	1998	2001	2004	2007	2010	2013
Market turnover	1239	1527	1934	3324	3971	5345

Si tratta di numeri impressionanti, soprattutto se confrontati con le stime del PIL (Prodotto Interno Lordo) dei primi 10 Paesi sviluppati (Tabella 5.2).

Il PIL mondiale è stato stimato in 47,7 trilioni di dollari nel 2013, cioè il turnover che viene generato mediamente ogni 9 giorni di negoziazione sul Forex.

Ovviamente, il cambio più tradato è

il cross euro-dollaro, con una percentuale di mercato del 24%, seguito dal cross dollaro-yen con un 18% (Tabella 5.3)

TABELLA 5.2 – PIL dei principali Paesi.

Paesi	Trilioni di dollari	%
Stati Uniti	16,8	35,2%
Cina	9,2	19,3%
Giappone	4,9	10,3%
Germania	3,6	7,5%
Francia	2,7	5,7%
Regno Unito	2,5	5,2%
Brasile	2,2	4,6%
Russia	2	4,2%
Italia	2	4,2%

India	1,8	3,8%
Totale PIL Mondiale	47,7	

TABELLA 5.3 – Volumi (in bilioni di dollari) dei principali cross valutari.

Cambi	Bilioni di dollari	%
USD/EUR	1289	24%
USD/JPY	987	18%
USD/GBP	475	9%
USD/AUD	364	7%
USD/CAD	200	4%
USD/CHF	128	2%

Le valute più scambiate, con oltre il 70% dell'operatività giornaliera nel 2013, sono chiamate Majors e

includono:

- dollaro americano (USD),
- euro (EUR),
- sterlina inglese (GBP),
- yen giapponese (JPY),
- franco svizzero (CHF),
- dollaro canadese (CAD),
- dollaro australiano (AUD).

Abbiamo fatto questa breve introduzione al mercato Forex perché i punti in comune con il mercato del Bitcoin sono molteplici.

Come visto nella paragrafo "Transazioni", il bitcoin non presenta tutti i connotati di tipo economico per

essere considerato a tutti gli effetti una valuta, ma dal punto di vista del trading viene già negoziato come se lo fosse. Infatti, viene quotato contro le principali valute *fiat* su mercati OTC aperti 24 ore al giorno 7 giorni a settimana. Da quest'ultimo punto di vista, gli exchange del bitcoin rappresentano un'evoluzione dei tradizionali mercati finanziari, poiché è sempre possibile aprire una nuova posizione o liquidarne una già aperta in qualunque giorno dell'anno.

Un mercato finanziario deve garantire 3 gradi di efficienza:

- Tecnica: capacità di offrire bassi costi di transazione.

- Funzionale: capacità di far incrociare domanda e offerta.
- Informativa: capacità di riflettere sui prezzi tutte le informazioni disponibili.

Per quanto concerne i primi due punti, i mercati bitcoin garantiscono un'efficienza elevata.

Prendiamo per esempio l'exchange Bitstamp: a oggi, offre commissioni che, nella peggiore delle ipotesi, sono pari allo 0,5% del volume tradato, offrendo una liquidità continua con volumi di negoziazione che, da inizio anno, sono stati nell'ordine di 1,7 bilioni di dollari, con una media giornaliera di 9,5 milioni di dollari. L'efficienza informativa è

altrettanto elevata e garantita da numerosi siti e account social che pubblicano in maniera tempestiva news e aggiornamenti.

I principali cross tradati sui vari exchange sono:

- BTC/USD (dollaro americano);
- BTC/CNY (renminbi);
- BTC/EUR (euro);
- BTC/CAD (dollaro canadese);
- BTC/RUR (rublo russo);
- BTC/GBP (sterlina inglese);
- BTC/JPY (yen giapponese).

Questa quotazione è di tipo “certo per incerto”: si scambia un’unità di bitcoin

(certa), assunta come base del cambio, per una quantità variabile di un'altra valuta (incerta). Il tasso di cambio è espresso come rapporto tra due valute:

$$tasso\ di\ cambio = \frac{valuta\ base}{valuta\ secondaria}$$

La valuta certa si trova al numeratore, mentre la valuta incerta al denominatore. Ne deriva che un aumento della quotazione del tasso di cambio significa che la stessa quantità di moneta certa può acquistare una maggiore quantità di moneta incerta. In termini tecnici si dice che la valuta certa si apprezza su quella incerta. Facciamo un esempio per capire

meglio. Ipotizziamo che il primo livello del book di negoziazione sia come nella Tabella 5.4.

TABELLA 5.4 – Primo livello del book di negoziazione in bitcoin al tempo t.

Q Bid	BID	ASK	Q Ask
1,2	620,2	621,5	2,9

Il prezzo Bid (denaro) di $ 620,2 è quello che il compratore è disposto a pagare per acquistare fino a 1,2 BTC, mentre il prezzo Ask (lettera) di $ 621,5 è quello che il venditore è disposto a incassare per vendere fino a 2,9 BTC. Vogliamo aprire una posizione rialzista sul cross BTC/USD, e quindi acquistiamo 1 BTC vendendo nello stesso momento $ 621,5.

Immaginiamo che il mercato si muova a nostro favore, e il nuovo book di negoziazione diventi quello della Tabella 5.5.

TABELLA 5.5 – Primo livello del book di negoziazione in bitcoin al tempo t+1.

Q Bid	BID	ASK	Q Ask
3,5	730,2	731,7	1,4

Da un punto di vista contabile abbiamo avuto i movimenti della Tabella 5.6.

TABELLA 5.6 – Resoconto contabile dell'operazione effettuata.

Valuta certa	Valuta incerta	Segno	Importo certo	Prezzo	Importo incerto
BTC	USD	+	1	$ 621,5	$ 621,5
BTC	USD	-	1	$ 730,2	$ 730,2
		+	0,15		$ 108,7

La situazione opposta rispetto a quella

che abbiamo appena esposto è quella di una diminuzione della quotazione del tasso di cambio. Ciò significa che la valuta certa si deprezza su quella incerta, cioè la stessa quantità di moneta certa può acquistare una minore quantità di moneta incerta.

CAPITOLO 6

Analisi di prezzo del Bitcoin

Nel corso del presente capitolo entreremo nel vivo della nostra analisi, andando ad analizzare con meticolosità la serie storica dei prezzi bitcoin contro il dollaro americano (BTC/USD), a partire dal 17 agosto 2010, giorno in cui si sono avuti i primi scambi sulla piattaforma di Mt. Gox, fino al 30 giugno 2014. La serie storica è stata aggiustata tenendo conto del fallimento di Mt. Gox e della liquidità presente su altri exchange.

La prassi vuole che l'orario di riferimento sul mercato Bitcoin sia le 18:15:05, cioè l'orario in cui è stato generato il Blocco 0. Questo funge sostanzialmente come prezzo di chiusura

di giornata.

Nella Figura 6.1 presentiamo il grafico con granularità giornaliera.

La crescita è stata esponenziale: in soli 4 anni e mezzo il prezzo dei bitcoin è passato da 0,0769 (al 17 agosto 2010) a $ 620 (al 21 novembre 2014), con un'incredibile performance del 464.009%. Stupefacenti, le performance, anche su base annuale, come osserviamo nella Tabella 6.1.

Su tutti spicca l'anno 2013, quando i prezzi sono passati da circa $ 13 a $ 731, con una variazione percentuale del 5.290%. Il 2014, invece, è iniziato nel segno della debolezza e, al prezzo di chiusura del 21 novembre, la performance è di -52%. Nella vostra

vita da trader, avete mai visto qualcosa del genere? Difficile, per non dire impossibile!

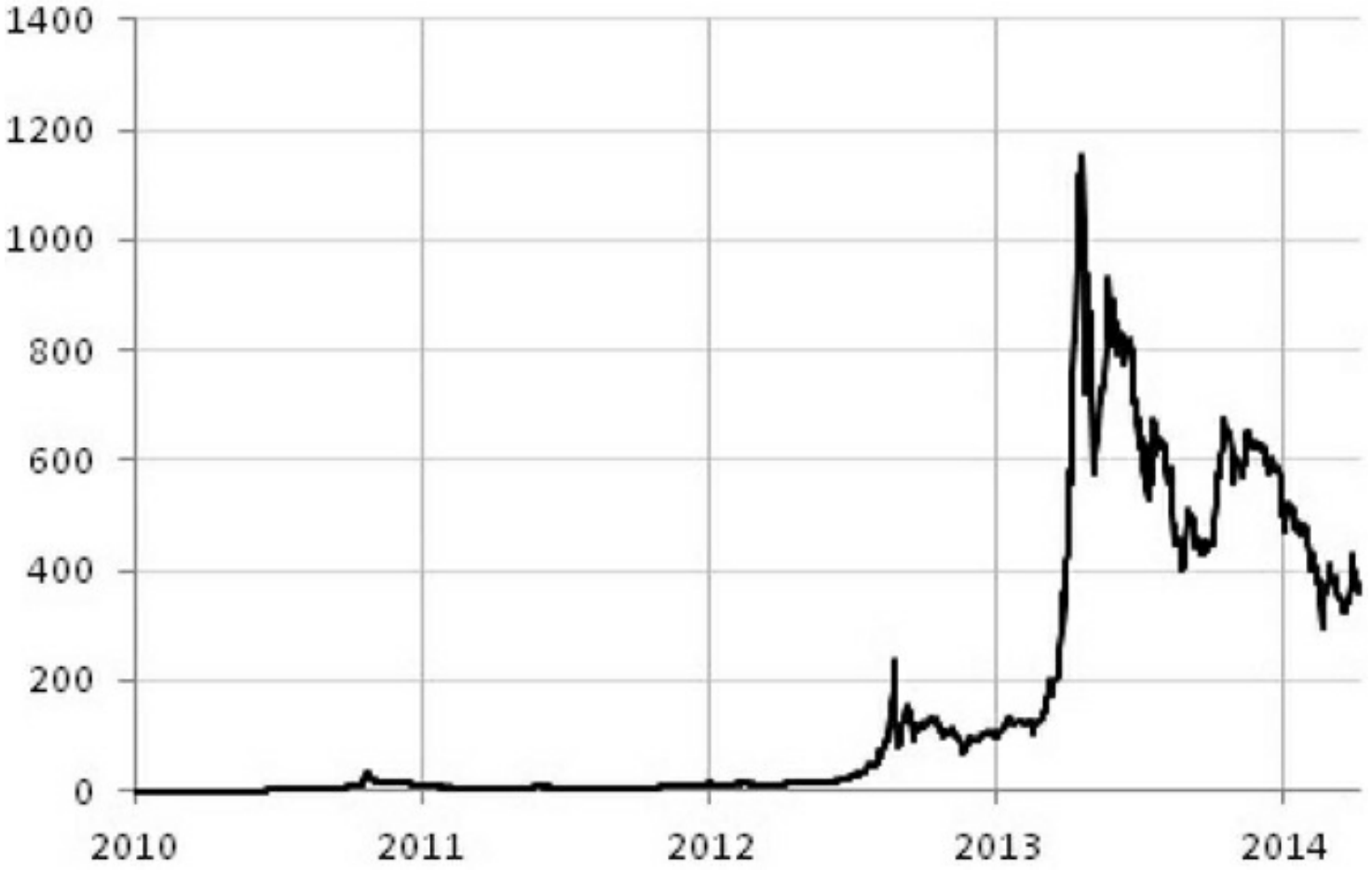


FIGURA 6.1 – Serie storica del prezzo bitcoin in dollari.

TABELLA 6.1 – Performance annuali del prezzo bitcoin.

Giorno	Prezzo in dollari	Var%
17/08/2010 31/12/2010	0,0769 0,299999	+290%
01/01/2011 31/12/2011	0,299999 4,995	+ 1.565%
01/01/2012 31/12/2012	5,2 13,59	+ 161%
01/01/2013 31/12/2013	13,561 731	+5.290%
01/01/2014 21/11/2014	746,9 356,9	-52%

Infatti, siamo di fronte alla performance più strabiliante di tutti i tempi. Nemmeno le bolle speculative più famose hanno raggiunto tali variazioni percentuali.

Avrete sicuramente sentito parlare

della mania dei tulipani scoppiata in Olanda all'inizio del Seicento. L'intero Paese si era follemente innamorato di questo fiore, divenuto un segno di potere e di distinzione sociale. In breve tempo si passò a una situazione di follia collettiva, i prezzi iniziarono a crescere a un ritmo elevatissimo, fino al 1637 quando scoppiò la bolla. A causa della mancanza di dati non è agevole stimare la portata della bolla speculativa. Tuttavia, se ci basiamo sulla standardizzazione dei prezzi creata da Earl Thompson, l'incremento è stato di oltre il 5.900%, prima del drammatico crollo nel febbraio del 1637 (Figura 6.2).

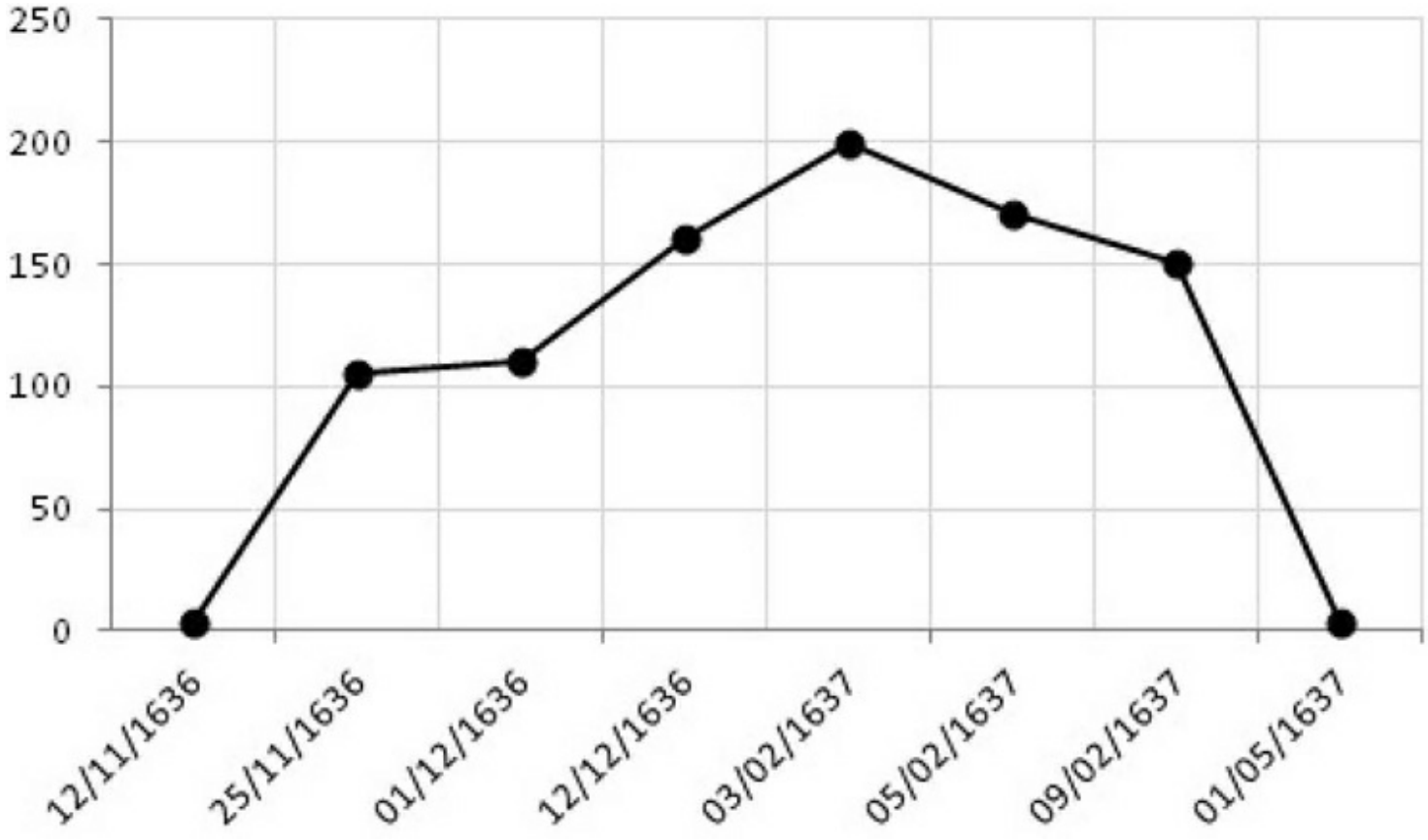


FIGURA 6.2 – La bolla speculativa dei tulipani.

Quella dei tulipani è solo una delle tante bolle che si sono susseguite nel corso dei secoli, ricordiamo anche la bolla della *South Sea Company* e della *Compagnie du Mississippi* nel 1720 e quella delle ferrovie inglesi nel 1840.

Con lo sviluppo dell'economia moderna l'elenco si è decisamente allungato, ricordiamo: la bolla del mercato immobiliare in Florida negli anni Venti, quella del mercato azionario che ha portato al famoso crash del 1929 e quella del titolo Poseidon nel 1970 (Figura 6.3). Questo titolo minerario ha registrato uno dei più grandi rialzi nel settore azionario, con una performance di quasi il 35.000%, per poi crollare e fallire miseramente.

Ricordiamo anche la bolla del mercato azionario in Giappone negli anni Ottanta, che ha spinto l'indice Nikkei verso i massimi del 1989, con un rialzo di oltre il 1.500% (Figura 6.4).

Non possiamo dimenticare le bolle

più recenti e famose: quella dei titoli tecnologici a fine anni Novanta e la bolla dei mutui *sub-prime* del 2008. In particolare, durante la bolla del Nasdaq abbiamo assistito a incrementi di prezzo elevatissimi: per esempio, il titolo Amazon, nella sua fase di start-up, registrò una crescita percentuale di circa il 5.600% in soli due anni, per poi perdere oltre il 90% del proprio valore (Figura 6.5).

Da quanto fino a ora raccontato, una domanda sorge spontanea: siamo di fronte a una nuova bolla speculativa, che riguarda stavolta il bitcoin?

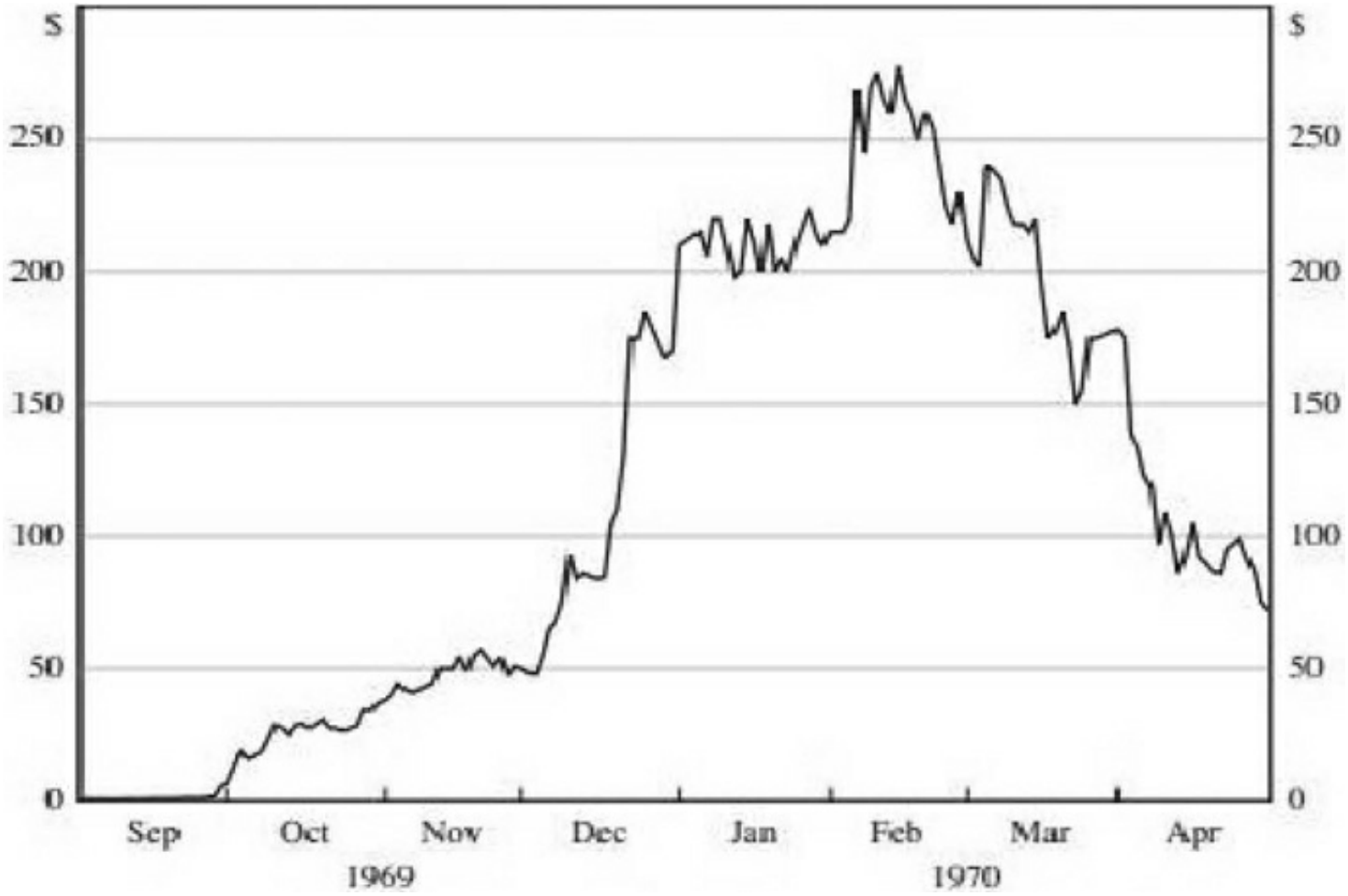


FIGURA 6.3 – Il titolo Poseidon.

FIGURA 6.4 – La bolla dell'indice Nikkei.

Non abbiamo nessuna sfera di cristallo né certezze, solo il tempo infatti sarà in grado di dare le giuste sentenze. Ma di una cosa siamo certi: se siete dei professionisti del trading, o investitori alla ricerca di nuove opportunità, non è possibile ignorare il bitcoin. Il rischio è

sicuramente alto, ma anche i potenziali profitti lo sono.

FIGURA 6.5 – La bolla del titolo Amazon.

Il fattore chiave su cui occorre basare la vostra scelta è la vostra propensione al rischio, e di conseguenza il capitale che volete utilizzare. È nostra intenzione

fornirvi strumenti operativi che siano in grado di supportarvi nel caso sceglieste di avventurarvi in questo nuovo e affascinante settore.

Per completare il nostro breve excursus nella storia delle bolle occorre precisare che non tutte si sono poi trasformate in veri fallimenti. Guardate cosa è accaduto ad Amazon (Figura 6.6).

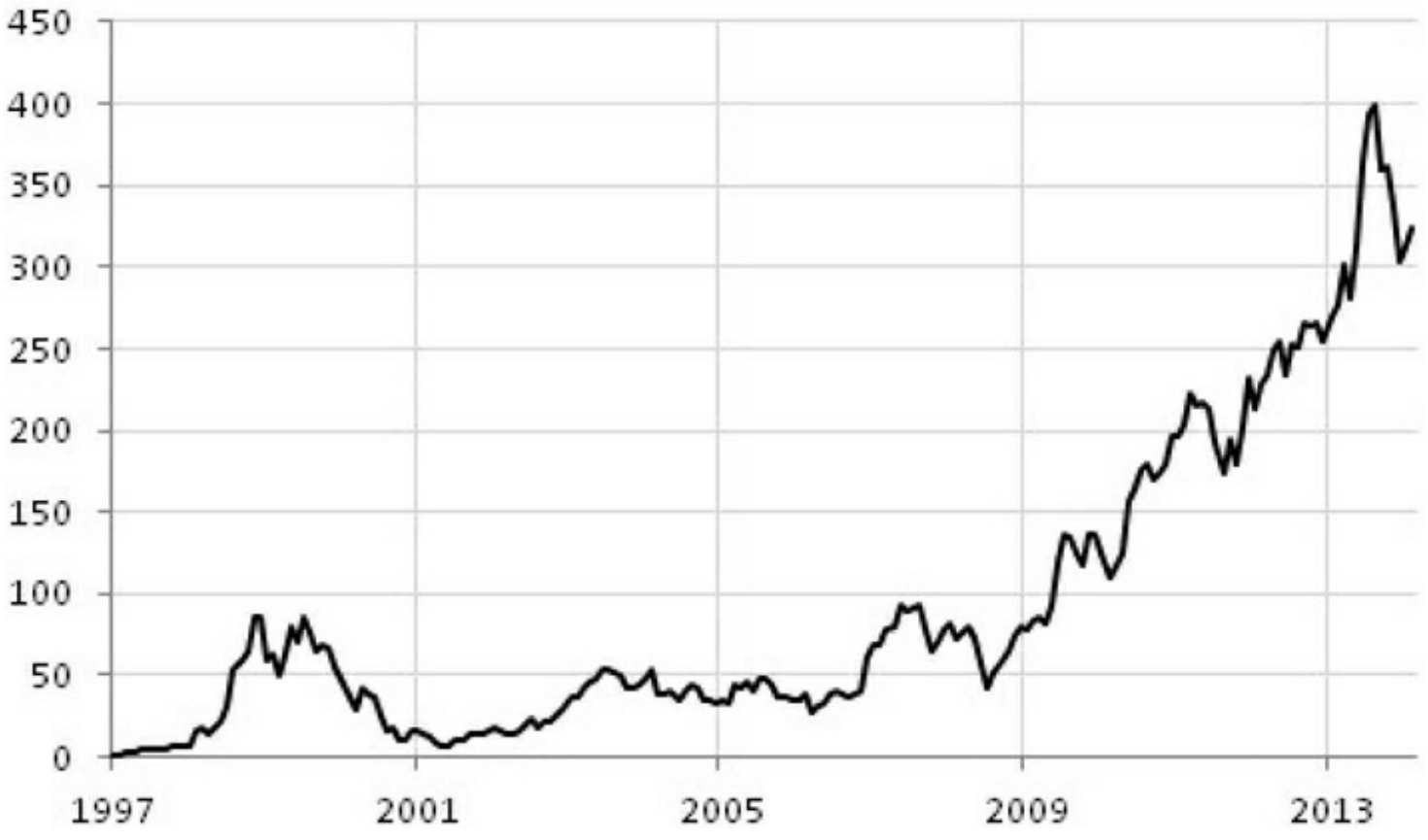


FIGURA 6.6 – Quotazione del titolo Amazon dopo la bolla di fine anni Novanta.

Il suo business era solido e rivoluzionario, il mercato se n'è accorto e ha ripagato.

ANALISI GRAFICA DEL TREND

Procediamo ora ad analizzare meglio il trend di lungo periodo e per far ciò passiamo al grafico su scala logaritmica che ci permette di eliminare le deformazioni di prezzo (Figura 6.7).

FIGURA 6.7 – Grafico logaritmico del prezzo bitcoin.

È evidente che i prezzi sono in continua ascesa e ogni fase di ritracciamento è stata un'occasione di acquisto per il medio e lungo termine. Nel grafico della Figura 6.8 possiamo identificare 6 fasi significative. Andiamole ad analizzare

una per una, nel dettaglio:

- La prima fase (Figura 6.9) è durata 298 giorni, e si è conclusa con il massimo del 10 giugno 2011 a $ 35. La variazione percentuale è stata del 45.445%.
- La seconda fase (Figura 6.10) è durata 164 giorni dal massimo della prima fino al minimo del 21 novembre 2011. I prezzi sono crollati, passando da $ 30 a $ 2,29, con una perdita del 92%.

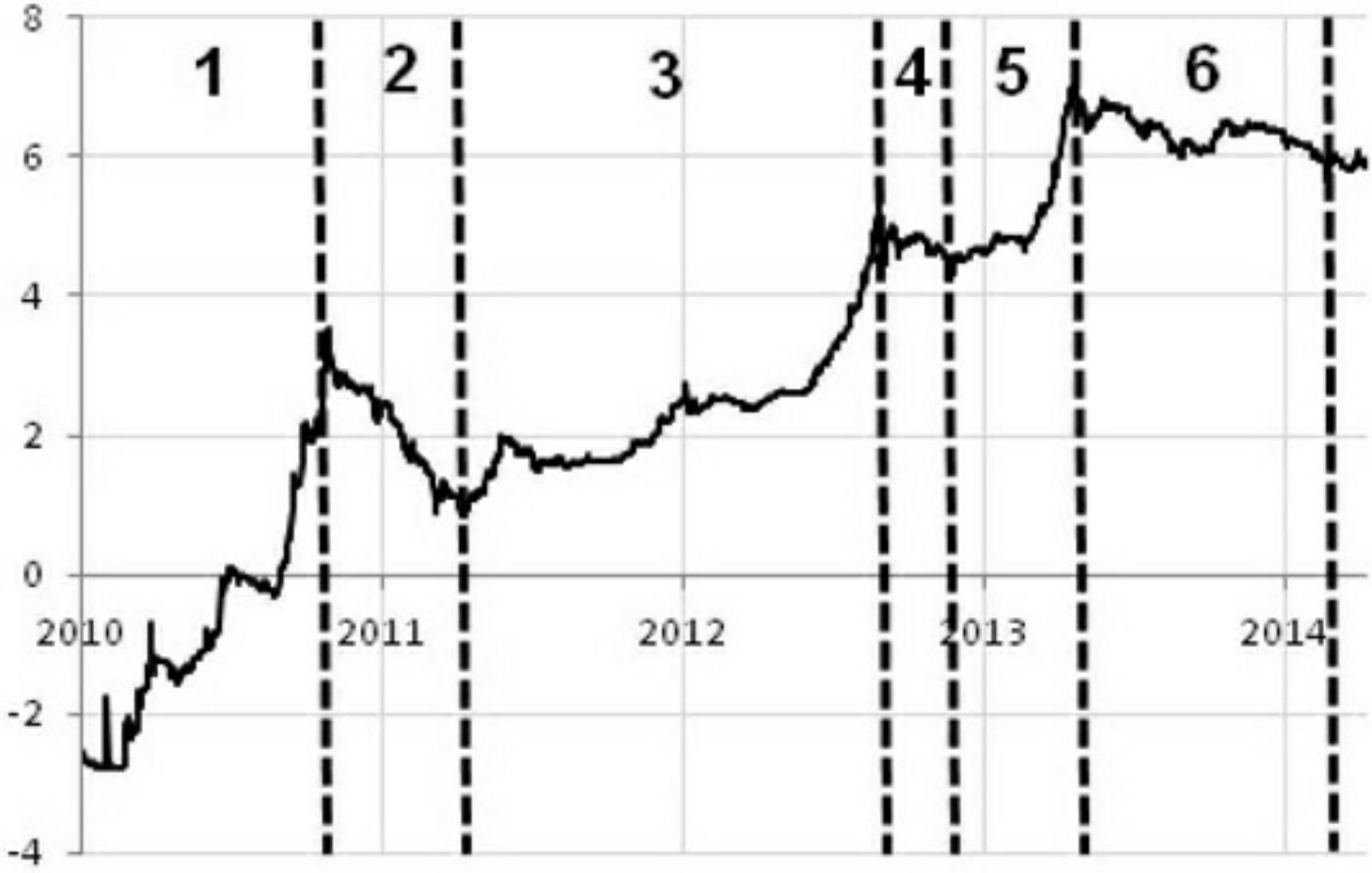


FIGURA 6.8 – Le 6 fasi significative del prezzo.

FIGURA 6.9 – La prima fase.

FIGURA 6.10 – La seconda fase.

- La terza fase (Figura 6.11) è stata la più lunga, ed è durata 505 giorni dal minimo della seconda fino al minimo del 9 aprile 2013. I prezzi hanno registrato un incremento del 10.027%, passando da $ 2,35 a $ 237,99.
- La quarta fase (Figura 6.12) è stata la più breve, ed è durata 87 giorni dal massimo della terza fino al minimo del 5 luglio 2013. I prezzi hanno subito una discesa pari al 66%, passando da $ 198 a $ 67,85.

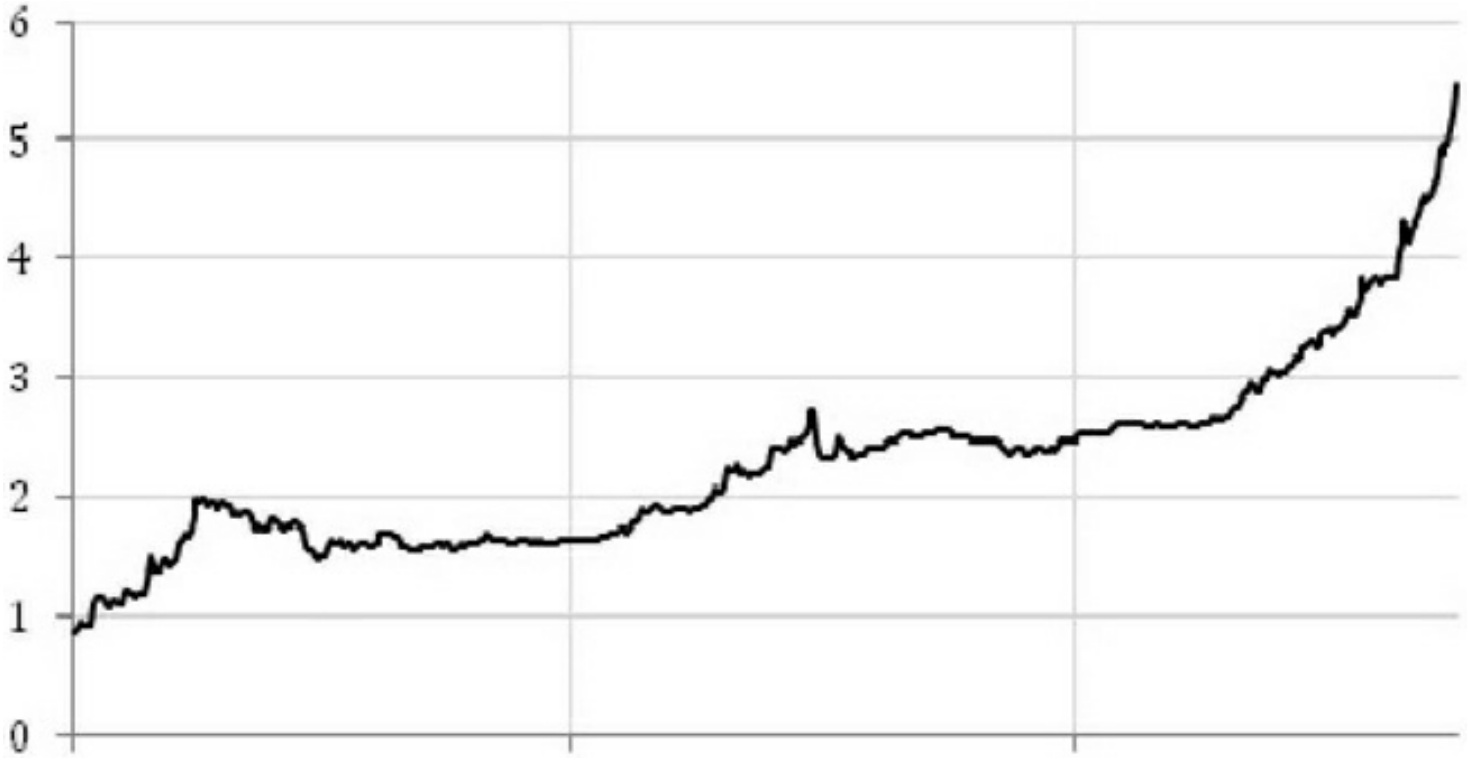


FIGURA 6.11 – La terza fase.

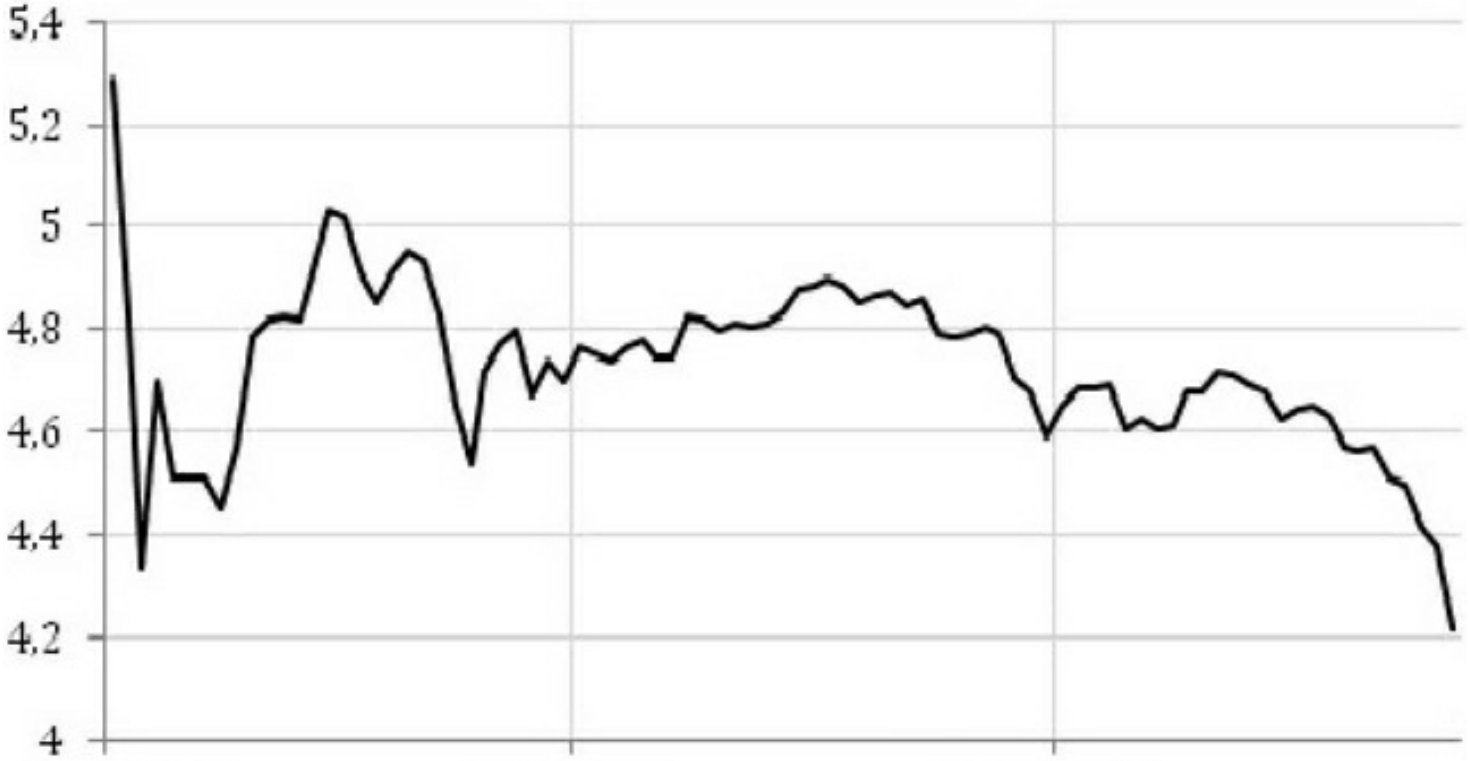


FIGURA 6.12 – La quarta fase.

- La quinta fase (Figura 6.13) è durata 152 giorni dal minimo della quarta fino al massimo assoluto del 4 dicembre 2013 a $ 1151. I prezzi sono cresciuti del 1.560%.
- L'ultima fase (Figura 6.14) è durata 178 giorni, e va dal massimo della quinta al minimo del 10 aprile 2014, con una discesa dei prezzi del 27%.

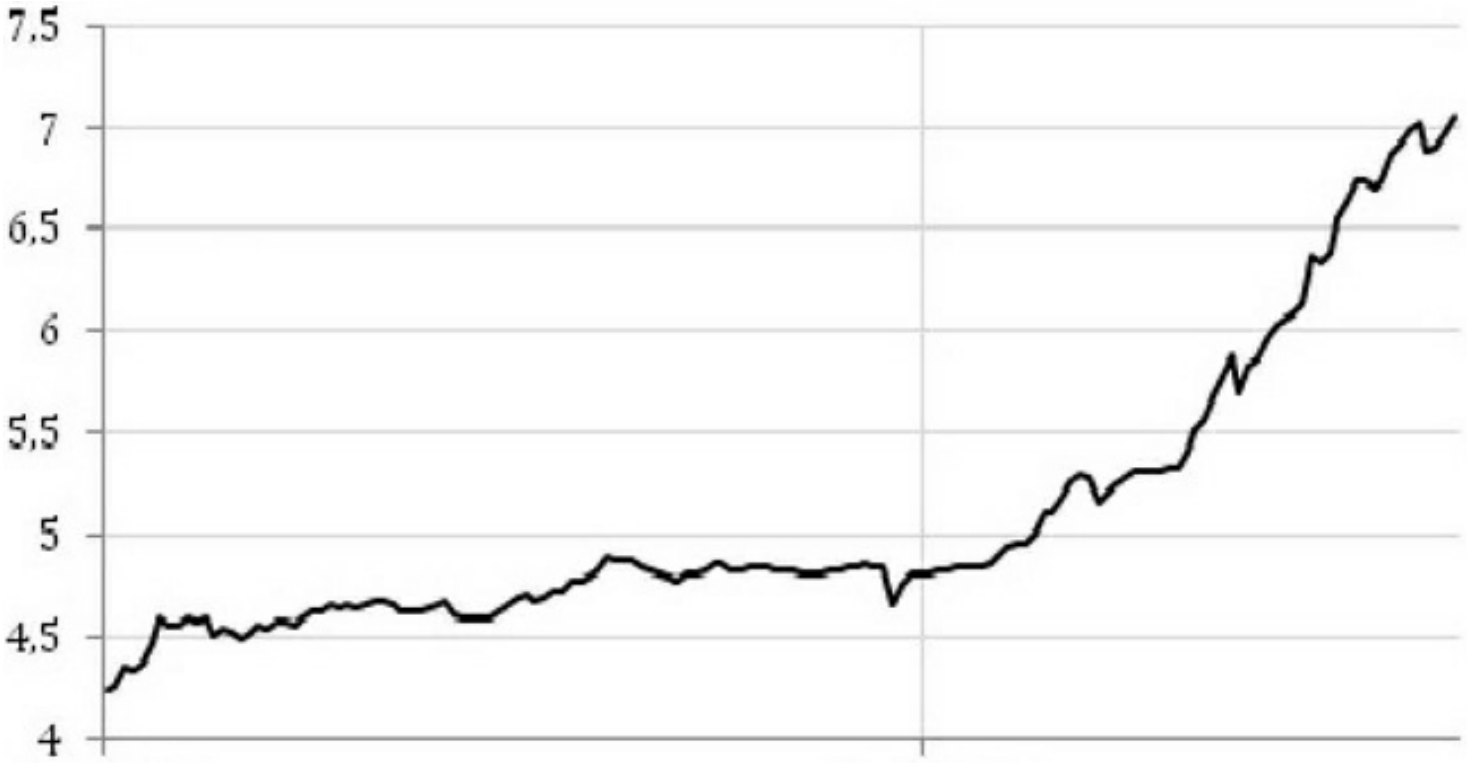


FIGURA 6.13 – La quinta fase.

FIGURA 6.14 – La sesta fase.

Da quest'ultimo minimo è partita una nuova fase del mercato di tipo rialzista, la cui forza sarà ovviamente da valutare in base ai futuri movimenti del prezzo. Al prezzo di chiusura del 21 novembre 2014, la durata è pari a 47 giorni con un

rialzo del 22%.

ANALISI PREZZO-DIFFICOLTÀ

Il grafico in scala logaritmica dei prezzi avrebbe dovuto ricordarvi qualcosa che abbiamo già esposto in precedenza: l'andamento della Difficoltà presentata nel paragrafo "Spesa operativa".

Per maggior chiarezza li mettiamo ora a confronto. Il legame tra queste due variabili è positivo e la correlazione di lungo periodo è quasi perfetta, pari a 0,96 (Figura 6.15).

FIGURA 6.15 – Grafico prezzo-Difficoltà su scala logaritmica.

Esiste un forte legame tra l'andamento dei prezzi e il valore della Difficoltà. Questo non deve stupire, poiché più aumenta la Difficoltà più diventa complicato svolgere la prova di lavoro e ricevere, quindi, l'incentivo che, a

oggi, rappresenta la prima forma di remunerazione per i minatori. In sostanza, il prezzo deve necessariamente essere legato alla Difficoltà, almeno fino a quando non tenderà ad aumentare la seconda forma d'incentivo, cioè le commissioni di transazione.

Cerchiamo di approfondire meglio il concetto analizzando una correlazione a 90 e 365 giorni (Figura 6.16).

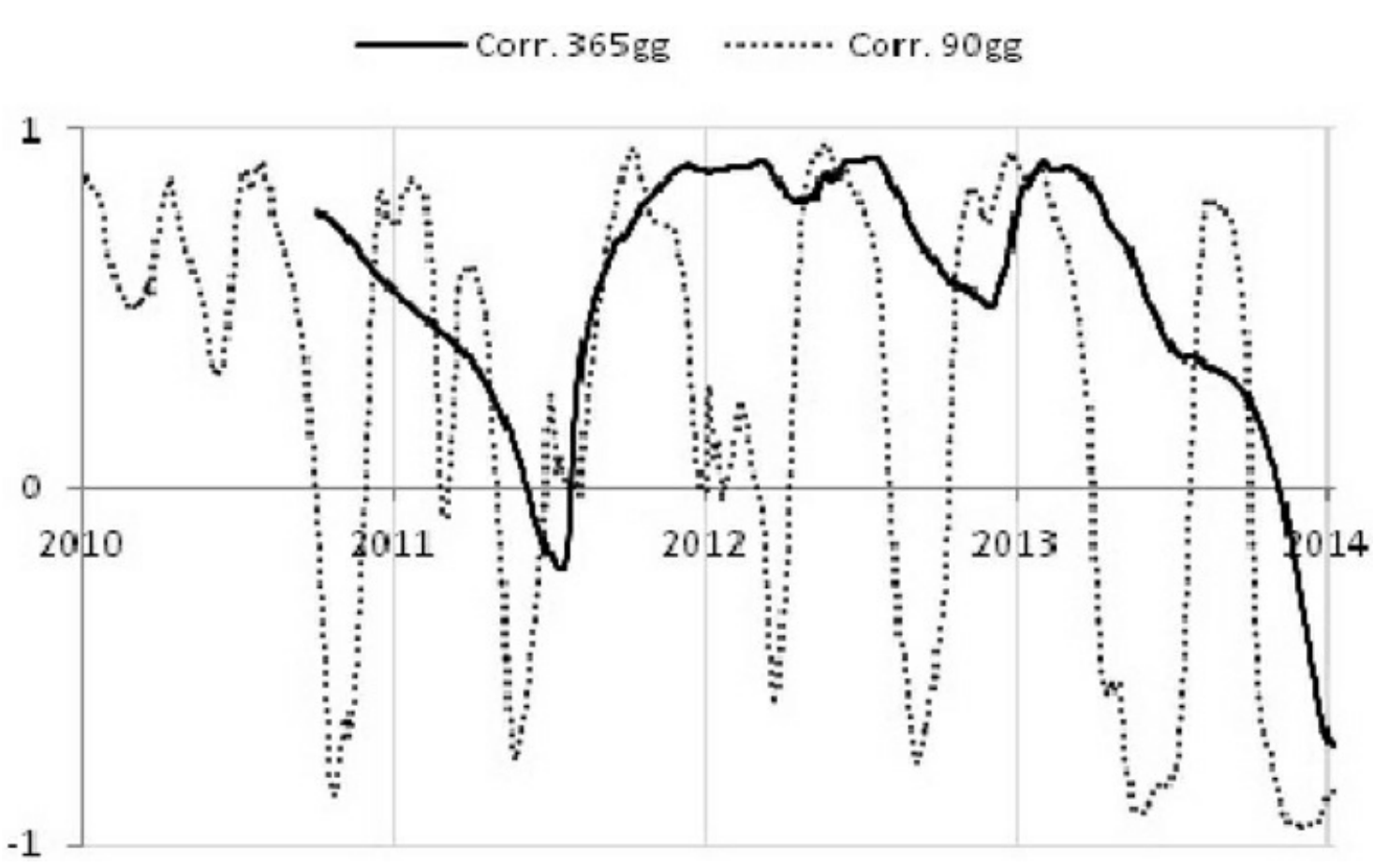


FIGURA 6.16 – Correlazione prezzo-Difficoltà a 90 e 365 giorni.

Queste correlazioni sono di tipo dinamico e ci mostrano che, su base annua, il legame tra prezzi e Difficoltà è stato per la maggior parte del tempo positivo. Va però segnalato che da settembre 2014 la correlazione è

diventata negativa. Ci troviamo, quindi, in un contesto in cui la Difficoltà continua ad aumentare mentre i prezzi restano in un trend ribassista.

In ottica di lungo periodo è improbabile che questa correlazione non ritorni verso valori positivi e, affinché questo si verifichi, i prezzi dovranno necessariamente aumentare. Lo stesso risultato si otterrebbe qualora la Difficoltà iniziasse a diminuire, ma al momento riteniamo questo scenario meno plausibile.

Sempre dalla Figura 6.16 notiamo come le oscillazioni della correlazione trimestrale sono state più frequenti e ampie. Entriamo più nel dettaglio e mettiamo a confronto, su un unico

grafico, la correlazione a 90 giorni e il valore del prezzo su scala logaritmica (Figura 6.17).

Osserviamo come tale grafico presenti sostanziali oscillazioni, ma unite a una certa regolarità generale. Per il momento fermiamo qui la nostra analisi.

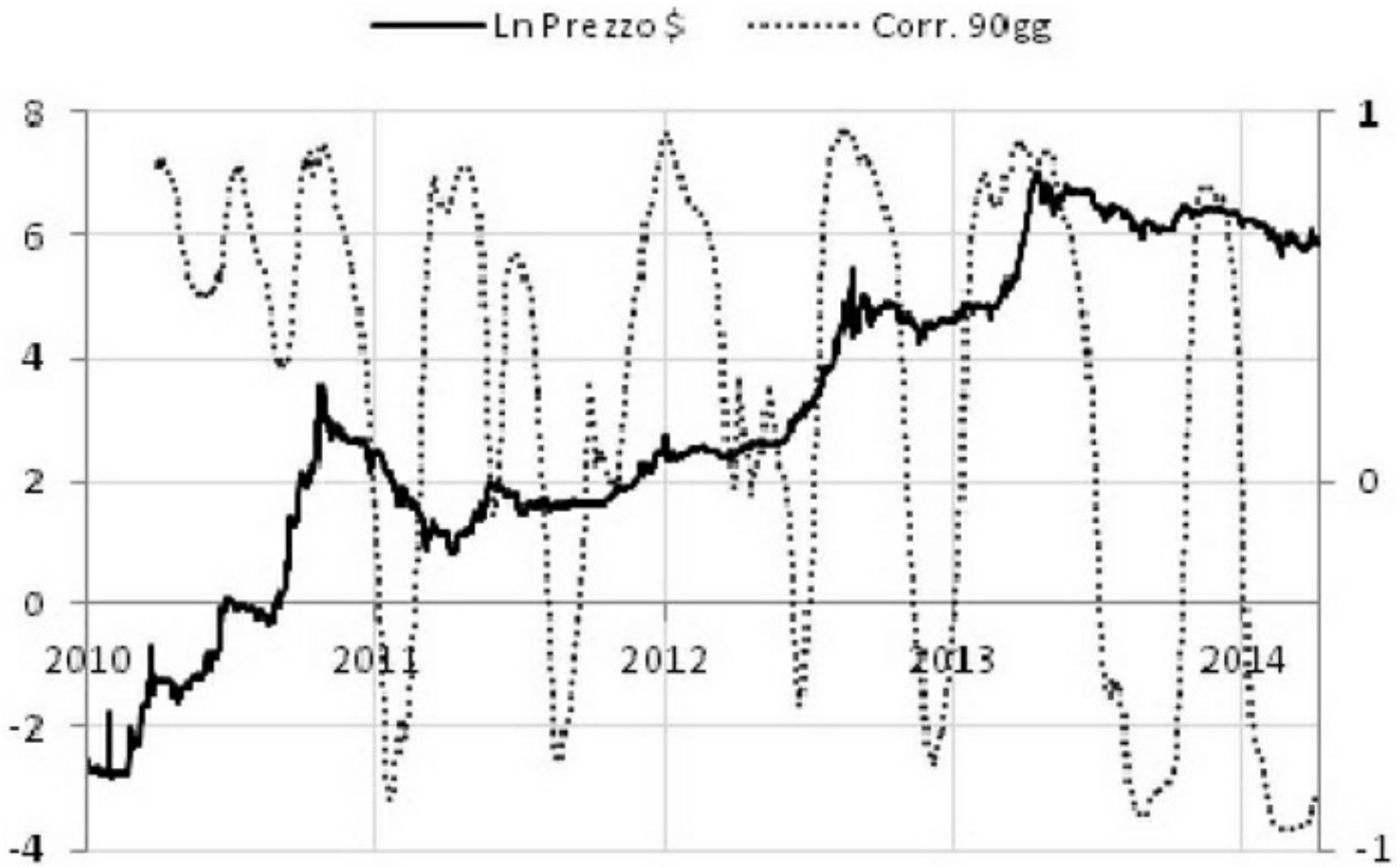


FIGURA 6.17 – Correlazione tra prezzo-Difficoltà a 90 giorni e prezzo in scala logaritmica.

È necessario, infatti, a questo punto, per approfondire lo studio di questo grafico e sfruttarne al meglio le sue potenzialità, introdurre alcuni importanti elementi di Analisi tecnica e, successivamente nel capitolo "Trading system per il Bitcoin", ripartire proprio da qui per costruire un trading system statistico.

ANALISI STATISTICA

Ci proponiamo ora di effettuare una

diversa analisi dei prezzi, non di tipo grafico ma di tipo statistico, e vedremo le ulteriori interessanti conclusioni che essa porterà.

Iniziamo con il calcolare le variazioni percentuali giornaliere sui prezzi di chiusura. La Tabella 6.2 ci segnala che in 776 giorni su 1557 analizzati, cioè il 49,84%, il prezzo di chiusura è stato superiore a quello della giornata precedente.

TABELLA 6.2 – Analisi dei prezzi.

N° Valori	1557
Prezzo ≥ Prezzo precedente	776
% Rialzista	49,84%
Prezzo < Prezzo precedente	781

% Ribassista	50,16%

Da questa statistica emerge che le giornate positive e quelle negative sono praticamente bilanciate. C'è, però, un dettaglio molto importante, come si vede nella Figura 6.18.

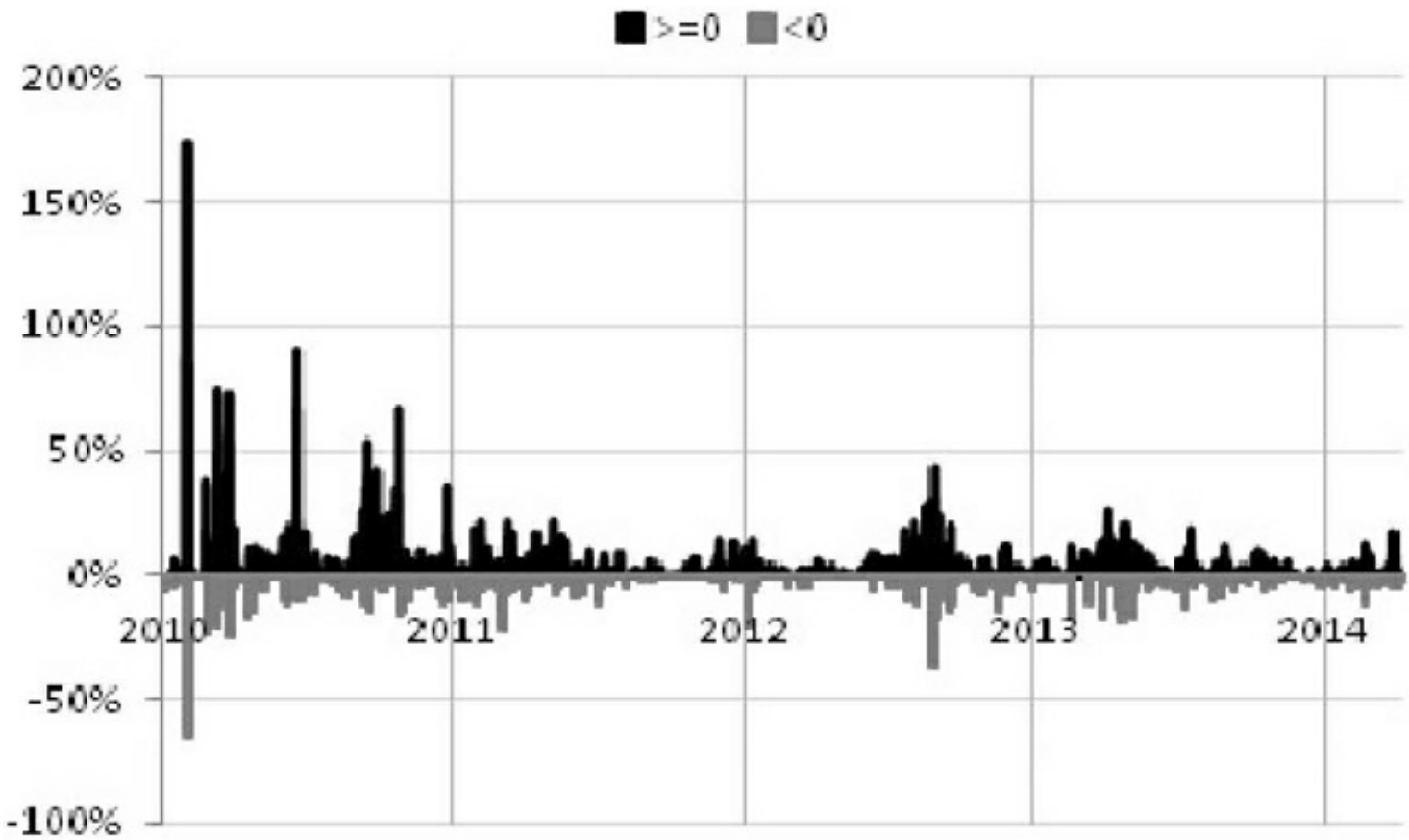


FIGURA 6.18 – Istogramma delle variazioni

positive e negative dei prezzi in termini percentuali.

Le barre in nero, che rappresentano le variazioni percentuali positive, sono in valore assoluto superiori a quelle in grigio, che rappresentano le variazioni percentuali negative. In altri termini, questo significa che nelle giornate positive i prezzi crescono a un ritmo superiore rispetto alla decrescita nelle giornate negative. La media di crescita delle variazioni positive è del 4,96%, contro una media di decrescita delle variazioni negative del -3,19% (Tabella 6.3).

TABELLA 6.3 – Analisi dei prezzi.

	Prezzo ≥ Prezzo precedente	Prezzo < Prezzo precedente
N° Valori	776	781
Media	4,96%	-3,19%
Massimo	173%	0%
Minimo	0%	-64,63%

Tuttavia, tale analisi preliminare risulta poco significativa. Un interesse maggiore deriva dall'analisi delle variazioni di prezzo durante i cambi di Difficoltà. Dal 17 agosto 2010 si sono verificati 127 cambi di Difficoltà, e i prezzi sono variati con le statistiche presenti nella Tabella 6.4.

TABELLA 6.4 – Analisi statistica dei prezzi a

ogni cambio di Difficoltà.

N° Cambi Difficoltà	127
Media	11,16%
Massimo	245,86%
Minimo	-40,47%
Dev. std. pop.	36,59%
Curtosi	13,92
Asimmetria	3,03

La Figura 6.19 mostra la distribuzione di frequenza:

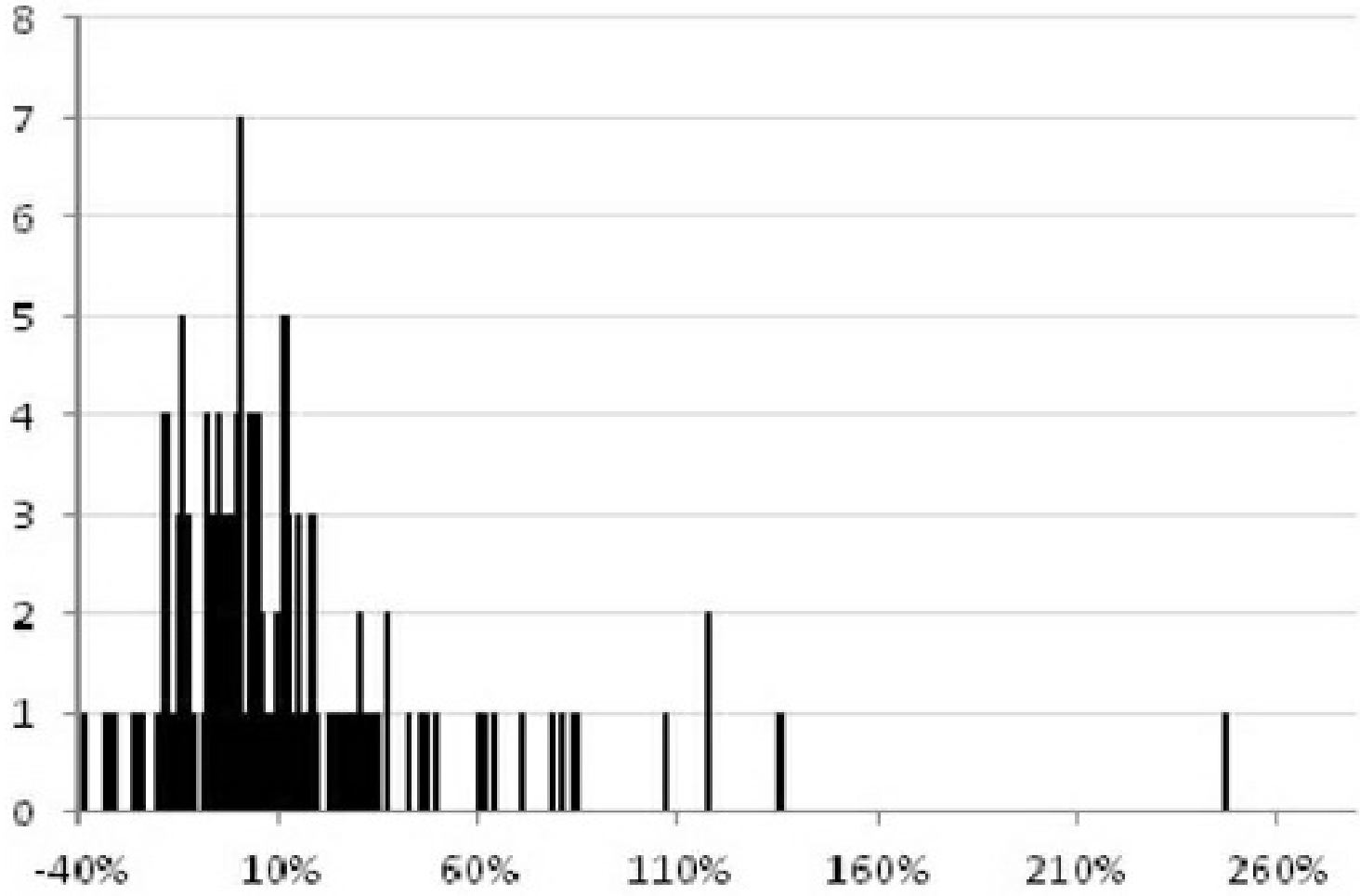


FIGURA 6.19 – Distribuzione di frequenza.

Si tratta di una distribuzione di tipo leptocurtico, di non facile previsione. Spaccando le casistiche in variazioni percentuali negative e positive, si ha la conferma che le distribuzioni non sono né regolari né di facile interpretazione.

I due grafici delle Figure 6.20 e 6.21 mostrano la distribuzione di frequenza per valori minori e per valori maggiori di 0.

La Tabella 6.5 ne mostra i risultati statistici.

Alla luce di tale analisi quantitativa sarebbe sensato fare una sorta di previsione sui prezzi? La risposta è affermativa. L'importante è tenere presente che, seppure su basi statistiche, si tratta pur sempre di una previsione.

L'andamento del prezzo dei bitcoin è influenzato dalla legge della domanda e dell'offerta, così come avviene per tutte le attività negoziate sui mercati finanziari. Il prezzo sale quando la

domanda eccede l'offerta e, al contrario, il prezzo scende quando l'offerta eccede la domanda.

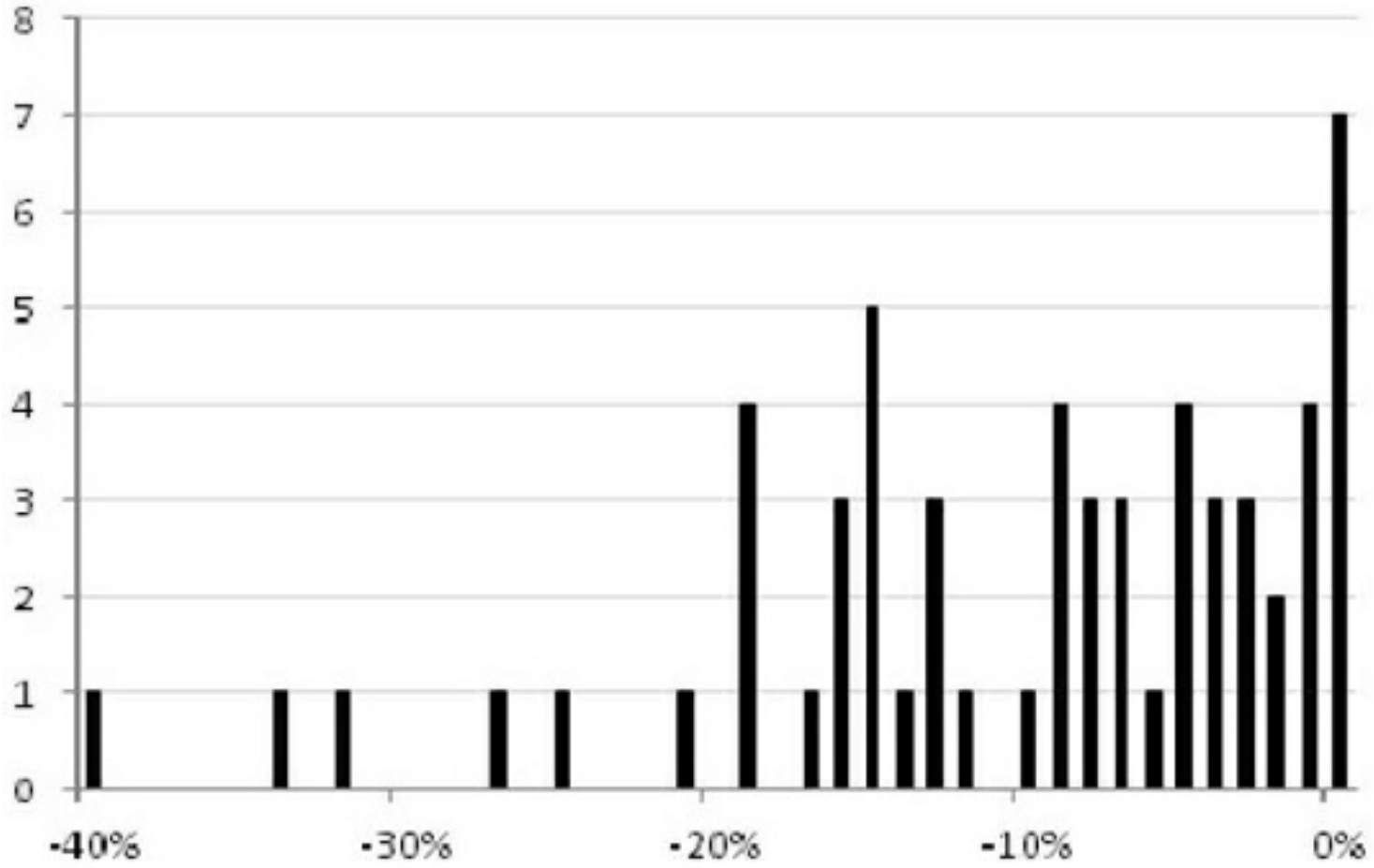
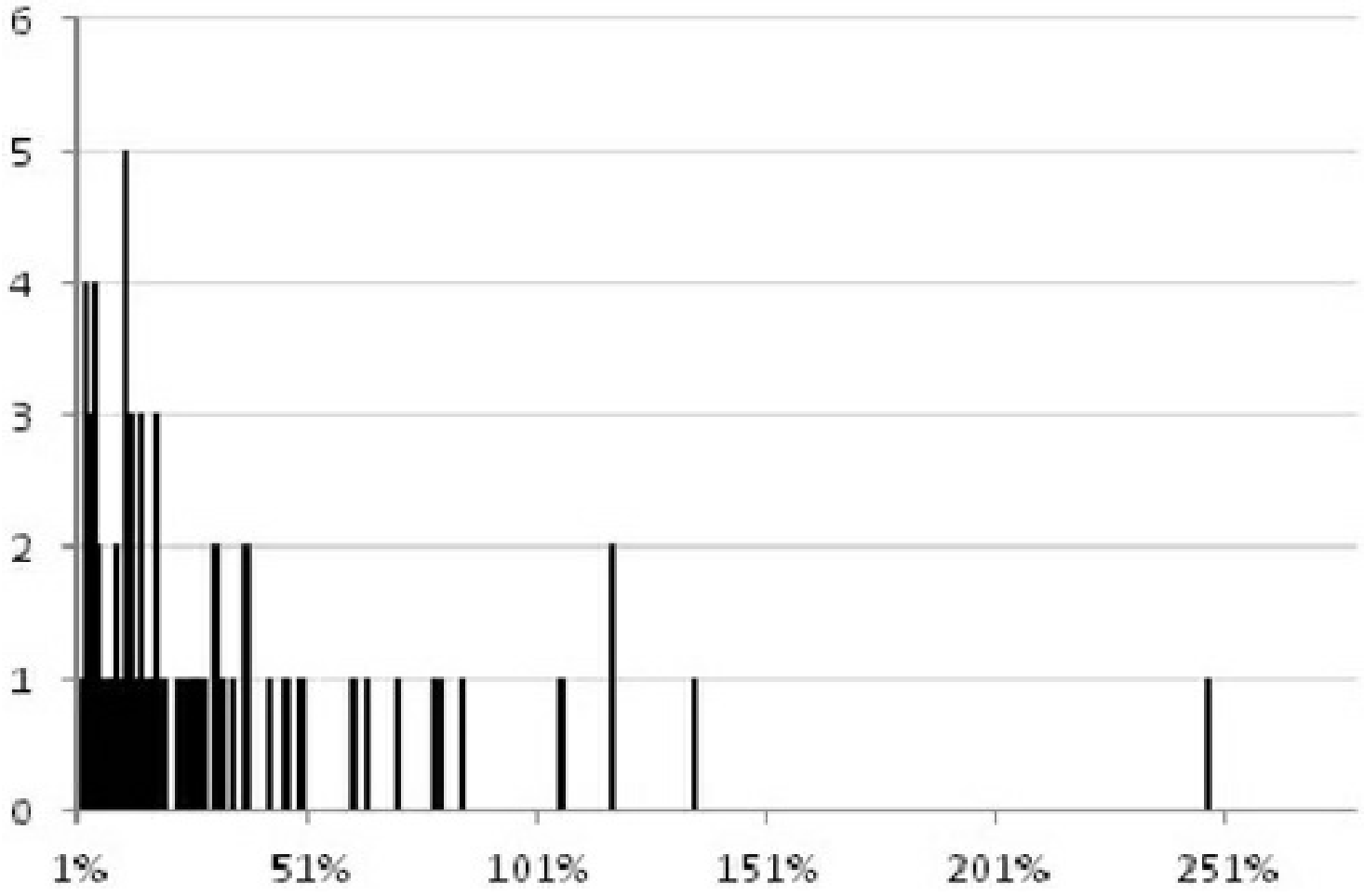


FIGURA 6.20 – Distribuzione di frequenza per valori negativi.



FGURA 6.21 – Distribuzione di frequenza per valori positivi.

TABELLA 6.5 – Analisi statistica dei prezzi a ogni cambio di Difficoltà.

	≥ 0	**< 0**
N° Valori	67	60
% Totale	52,76%	47,24%

Media	31%	-10,99%
Massimo	245,86%	-0,42%
Minimo	0,95%	-40,47%
Dev. std. pop.	40,79%	9,02%
Curtosi	11,45	1,3
Asimmetria	2,93	-1,15

Abbiamo, però, visto come il prezzo sia nel lungo periodo altamente correlato con la Difficoltà. Procediamo, quindi, con l'applicare la disuguaglianza di Čebyšëv, già esposta nel paragrafo "Tempo per cambio Difficoltà". Questo teorema afferma che, dato un valore reale $\lambda \geq 1$, allora la probabilità che i valori siano compresi nell'intervallo $(\mu \pm \lambda \cdot \sigma)$ è almeno pari a $(1 - 1 / \lambda^2)$,

indipendentemente dalla distribuzione di frequenza, e la probabilità che i valori siano compresi in un intervallo entro due deviazioni standard è il 75%.

Con l'ultimo dato a nostra disposizione, del 21 novembre 2014, siamo in grado di svolgere una previsione per i successivi mesi, che illustriamo nella Figura 6.22.

FIGURA 6.22 – Previsione del prezzo.

La linea tratteggiata superiore rappresenta la previsione del prezzo realizzata applicando la volatilità storica nei casi di variazione positiva della Difficoltà, invece la linea tratteggiata inferiore è realizzata

applicando la volatilità storica nei casi di variazione negativa della Difficoltà. Abbiamo preferito separare le due casistiche poiché, come abbiamo visto in precedenza, la rilevanza statistica delle variazioni negative della Difficoltà è bassa. Consideriamo a questo punto conclusa la nostra analisi di prezzo del bitcoin. Per poter, infatti, proseguire nella nostra analisi abbiamo bisogno di introdurre concetti fondamentali di Analisi tecnica. Nel prossimo capitolo inizieremo a fondare le basi che ci permetteranno di progredire nella nostra analisi del prezzo.

CAPITOLO 7

L’Analisi tecnica e il Bitcoin

In questa sezione del libro tratteremo di una disciplina tanto utile quanto affascinante: l'Analisi tecnica. Dopo aver fatto una breve introduzione, ci concentreremo su alcuni indicatori di questa disciplina con il preciso scopo di applicarli al mercato Bitcoin. Come vedrete nel corso del libro, la scelta di questi indicatori non è stata casuale, ma è stata dettata dalla volontà di costruire un metodo il più solido possibile per l'operatività in bitcoin.

Per chi volesse approfondire i concetti esposti vi consigliamo come testo di riferimento quello di John J. Murphy, *Analisi tecnica dei mercati finanziari* (Hoepli).

CHE COS'È L'ANALISI TECNICA?

Nel suo libro *Analisi tecnica dei mercati finanziari*,John J. Murphy definisce l'Analisi tecnica come lo studio del movimento del mercato, o *market action*, tramite l'uso sistematico dei grafici, allo scopo di prevedere la tendenza futura dei prezzi.

Questa definizione pone l'accento su due aspetti: lo studio e la previsione. È attraverso lo studio che siamo in grado di comprendere il movimento dei mercati finanziari, mentre la previsione è rivolta a delinearne i futuri andamenti.

I due aspetti non sono altro che i principali obiettivi dell'Analisi tecnica: rispettivamente, obiettivi di tipo analitico e obiettivi di tipo predittivo. Entrambi sono strettamente legati tra di loro, poiché per svolgere una previsione attendibile è necessario partire da una buona analisi. Gli obiettivi di tipo predittivo vengono perseguiti impiegando le quotazioni passate del mercato e altre grandezze, quali il volume e l'*open interest*. Detto in altri termini, l'andamento futuro dei prezzi viene previsto partendo dal passato.

Vediamo ora anche la definizione di Analisi tecnica che ha fornito Martin J. Pring nel suo libro *Analisi tecnica dei mercati finanziari*. Secondo Pring,

l'arte dell'Analisi tecnica riguarda lo studio dell'azione del mercato e l'identificazione dei punti di svolta, inoltre si occupa di probabilità e non di certezze. Anche da questa definizione possiamo trarre alcune considerazioni interessanti. Anzitutto, la classificazione dell'Analisi tecnica come un'arte. Questa antica parola ha accompagnato nel corso dei secoli la vita dell'uomo assumendo definizioni leggermente diverse. Dal latino *ars*, che indicava un'abilità materiale o spirituale mirata a progettare o costruire qualcosa, fino alla definizione più vicina ai giorni nostri, secondo cui l'arte è la manifestazione delle capacità espressive e creative, e in

particolare di quella capacità di inventare che è propria dell'uomo.

Quello che però ha sempre caratterizzato l'arte è il suo connotato di soggettività, e proprio in questo senso l'Analisi tecnica è strettamente connessa a essa. La soggettività ci porta ad analizzare il passato in modo diverso e, di conseguenza, a svolgere previsioni diverse che avranno una certa probabilità di realizzazione.

Ritornando alla definizione di Pring, un altro aspetto significativo è che l'Analisi tecnica si concentra sull'individuazione dei punti di svolta del mercato, i quali permettono di identificare e classificare le varie tendenze dei prezzi. In altri termini, il

suo obiettivo è quello di determinare le tendenze e le loro inversioni.

LEGGERE I GRAFICI

Nell'Analisi tecnica l'andamento dei prezzi può essere rappresentato utilizzando varie tipologie di grafici, in particolare:

- Grafico lineare (Line chart) (Figura 7.1).
- Grafico a barre (Bar chart) (Figura 7.2).
- Grafico a candele (Candlestick)

(Figura 7.3).

FIGURA 7.1 – Grafico lineare del bitcoin.

FIGURA 7.2 – Grafico a barre del bitcoin.

FIGURA 7.3 – Grafico a candele del bitcoin.

La costruzione di questi grafici prevede innanzitutto l'esistenza di un piano cartesiano, con i due assi che rappresentano il tempo in ascissa (asse delle x) e il prezzo in ordinata (asse delle y). La prima decisione da prendere

riguarda la compressione temporale (*time frame*) da analizzare, cioè l'intervallo tra una rilevazione e la successiva. I time frame più usati sono il mensile (*monthly*), settimanale (*weekly*), giornaliero (*daily*), fino ad arrivare a time frame intraday a 1 ora, 30 minuti, 15 minuti, 1 minuto e *tick by tick*.

Per quanto riguarda il mercato bitcoin, allo stato attuale, riteniamo che abbia senso utilizzare grafici con time frame settimanale o giornaliero, evitando di spingersi su periodi inferiori.

Tra le tipologie di grafici che abbiamo elencato, sia per completezza di informazione sia per facilità di visualizzazione, il migliore è il grafico

candlestick.

Nel prossimo paragrafo ci concentreremo quindi sulla costruzione delle candele.

Candlestick

I grafici a candele hanno una storia antica e vedono la loro nascita in Giappone per mano del leggendario trader Munehisa Homma.

Munehisa Homma nacque nel 1724 a Sakata, dove lavorò gestendo l'attività di famiglia presso il locale mercato del riso. Alla morte del padre si trasferì prima a Osaka, iniziando a fare trading di futures sul riso al Dojima Rice

Exchange, e poi a Edo (l'attuale Tokyo), che stava diventando il più importante mercato dell'epoca. In poco tempo divenne una leggenda vivente nel settore del trading e fu anche insignito del titolo di samurai.

Nel 1755, Homma scrisse 160 regole che hanno dato vita al "*Sakata's Method*", dal quale si fa iniziare la metodologia candlestick. Fu anche il primo a parlare di "psicologia del mercato", mettendo in luce il fatto che i movimenti dei prezzi del riso fossero influenzati dagli aspetti psicologici e si muovessero secondo la rotazione Yang (mercato bull) e Yin (mercato bear).

Nel mondo occidentale, il metodo

delle candele giapponesi giunse solo nel 1989 con la pubblicazione, da parte di Steve Nison, del famoso libro *Japanese Candlestick Charting Techniques*.

Entriamo ora maggiormente nel dettaglio e mostriamo come si costruisce una candela. I dati necessari sono quattro:

- apertura (Open);
- massimo (High);
- minimo (Low);
- chiusura (Close).

Con queste informazioni siamo in grado di costruire una candela, la quale si compone visivamente di un corpo (*Real*

Body), un'ombra superiore (*Upper Shadow*) e un'ombra inferiore (*Lower Shadow*). Il corpo è dato dalla differenza tra prezzo di chiusura e prezzo di apertura. Se questa differenza è positiva, allora la candela rappresenta un movimento rialzista dei prezzi e per convenzione il body è di colore bianco (Figura 7.4). Al corpo aggiungiamo l'ombra superiore, data dalla differenza tra prezzo massimo e prezzo di chiusura, e l'ombra inferiore, data dalla differenza tra prezzo di apertura e prezzo minimo.

Se la differenza tra prezzo di chiusura e prezzo di apertura è negativa, allora la candela rappresenta un movimento ribassista dei prezzi e per convenzione il body è di colore nero

(Figura 7.5). Al corpo aggiungiamo l'ombra superiore, data dalla differenza tra prezzo massimo e prezzo di apertura, e l'ombra inferiore, data dalla differenza tra prezzo di chiusura e prezzo minimo.

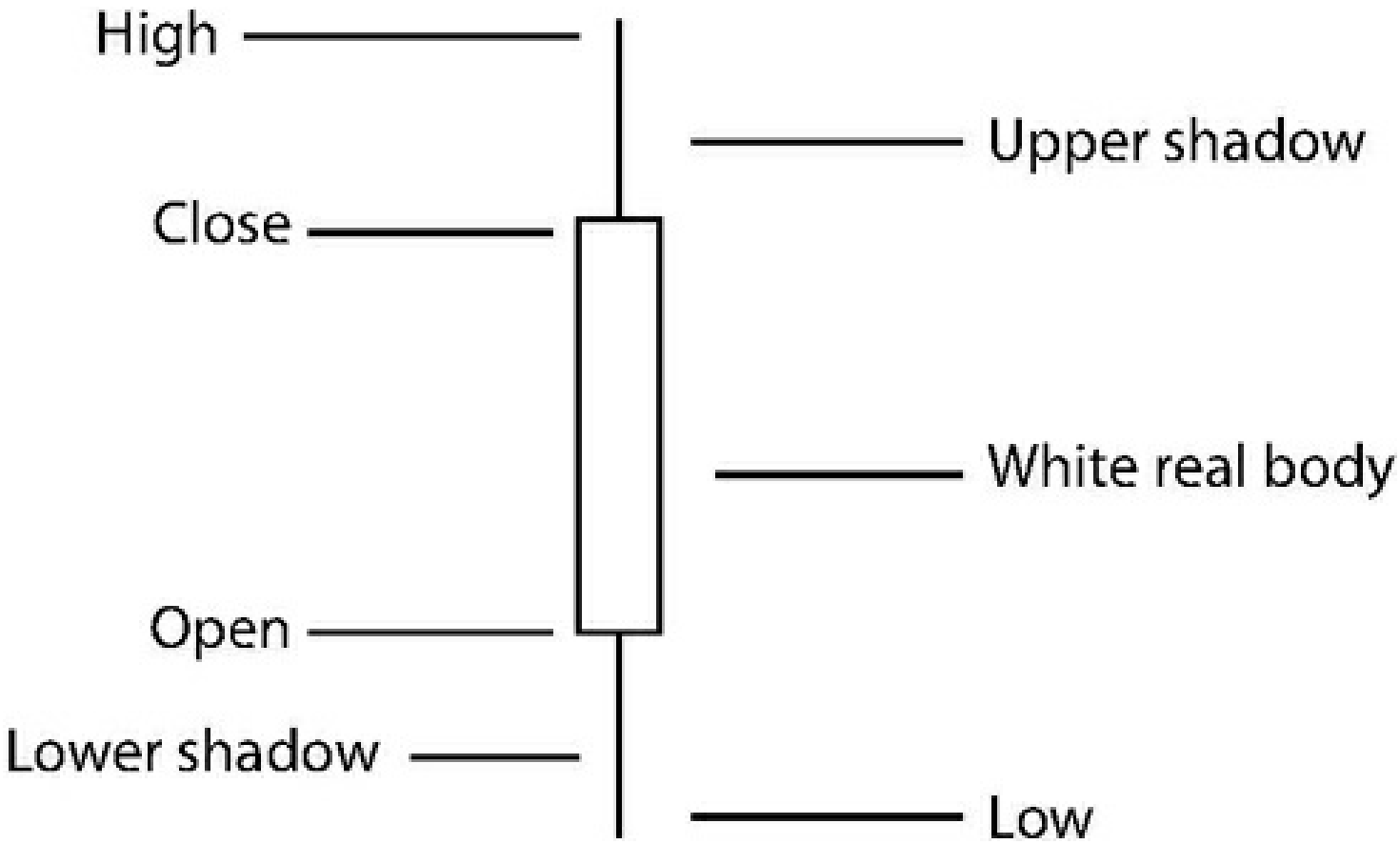


FIGURA 7.4 – Schema di una candela rialzista.

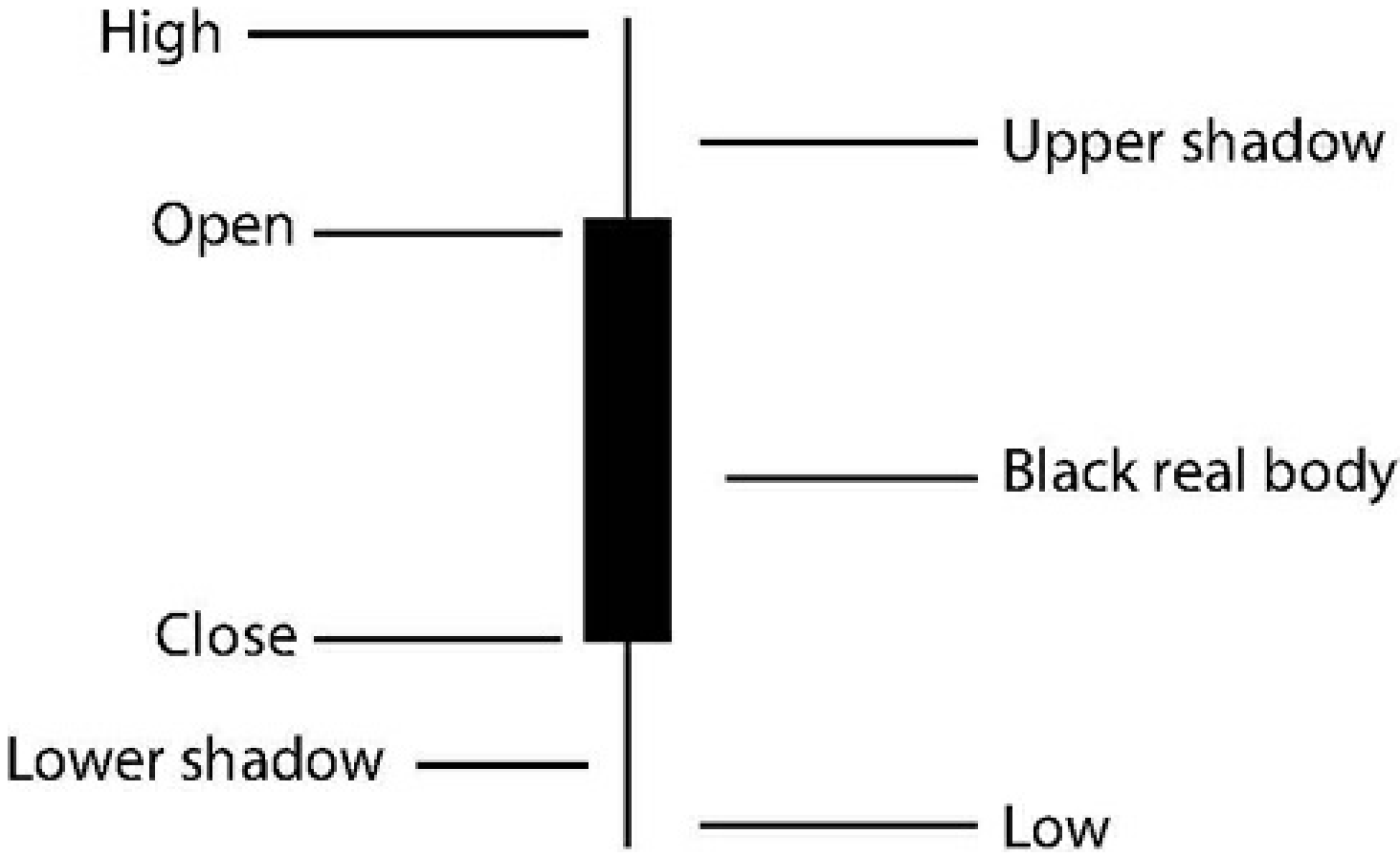


FIGURA 7.5 – Schema di una candela ribassista.

I PRINCIPI FONDAMENTALI DELL'ANALISI TECNICA

In questo paragrafo introduciamo i principi che sono alla base dell'Analisi tecnica, grazie ai quali questa ha la possibilità di studiare e comprendere i mercati finanziari andando ad analizzare i grafici di prezzo mostrati in precedenza.

I presupposti su cui si fonda tutta l'Analisi tecnica sono tre:

- il mercato sconta tutto;
- i prezzi si muovono in un trend;
- la storia si ripete.

Analizziamo insieme questi tre aspetti vedendo le singole implicazioni che ne derivano.

Il mercato sconta tutto

In base a questo presupposto, l'Analisi tecnica ritiene che nei prezzi siano già incorporati tutti quei fattori di tipo fondamentale, politico, monetario ed economico, che ne hanno determinato l'andamento, e anche le aspettative degli operatori circa il futuro del titolo oggetto di studio.

In altri termini, nei prezzi vi è tutto. Sostenere questa affermazione ci porta obbligatoriamente ad assegnare un ruolo chiave ai prezzi e al loro studio. L'Analisi tecnica si sintetizza nello studio del prezzo, con l'obiettivo di capire la direzione del mercato senza dover ricorrere all'analisi delle

motivazioni esterne al prezzo stesso.

Ma cosa fa muovere i prezzi? È molto semplice: la domanda dei compratori e l'offerta dei venditori. L'incrocio tra domanda e offerta porta alla formazione di un certo prezzo per una certa quantità. In generale, possiamo affermare che il movimento dei prezzi riflette i cambiamenti quantitativi della domanda e dell'offerta. In una situazione di equilibrio, con prezzi stabili, l'offerta dei venditori è supportata dalla domanda dei compratori (Figura 7.6)

Sulla base di quanto abbiamo detto, i prezzi aumentano quando la domanda dei compratori è superiore all'offerta dei venditori (Figura 7.7).

Mentre, avremo dei prezzi in discesa

nel caso esattamente opposto, cioè quando l'offerta è maggiore della domanda (Figura 7.8).

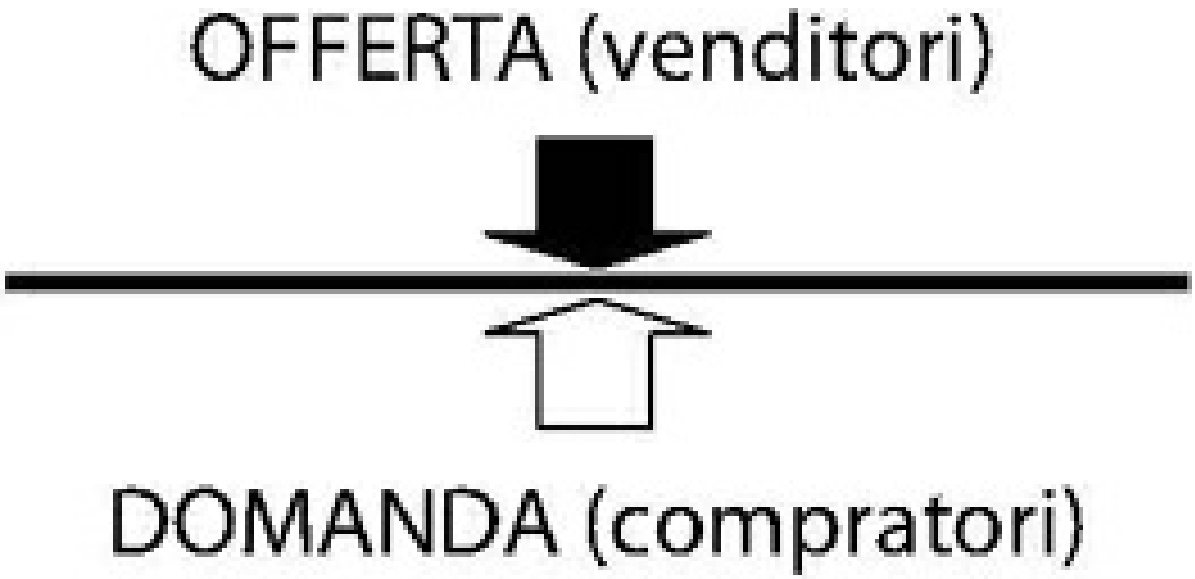


FIGURA 7.6 – Situazione di equilibrio nel mercato.

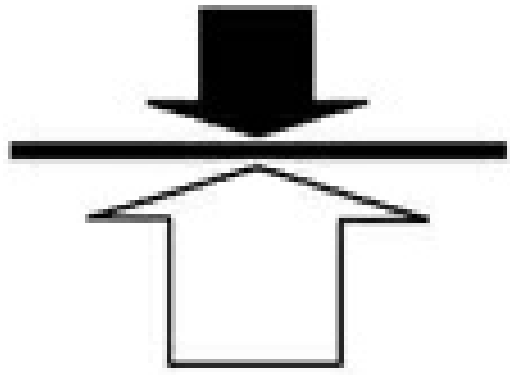


FIGURA 7.7 – Situazione di maggior domanda

nel mercato.

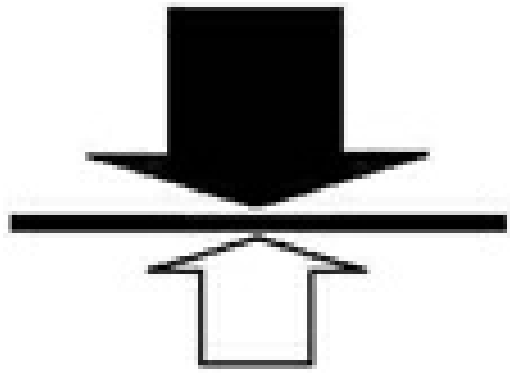


FIGURA 7.8 – Situazione di maggior offerta nel mercato.

All'interno di questa dinamica di costante confronto tra domanda e offerta, i prezzi fluttuano in continuazione alla ricerca di un equilibrio. Tale equilibrio è però instabile.

I prezzi si muovono in un

trend

L'Analisi tecnica ha lo scopo di identificare un trend fin dai suoi primi movimenti, cercando di investire nella sua direzione e fino al suo esaurimento, o meglio fino a quando non ci sono chiari segnali d'inversione del trend stesso. Proprio su questo punto ci ricolleghiamo alla definizione data da Martin Pring secondo cui l'obiettivo dell'Analisi tecnica è quello di determinare il trend e le sue inversioni.

Ma che cos'è un trend? Un trend è una tendenza, cioè l'orientamento di una certa serie di valori a crescere, diminuire o non subire significative variazioni nell'arco di un determinato

periodo di tempo. In Analisi tecnica, il trend non è altro che l'indicazione della direzione dei prezzi.

Guardiamo il grafico del bitcoin per capire con un esempio il concetto di trend (Figura 7.9). Nella prima parte i prezzi hanno una chiara impronta rialzista e si muovono secondo un trend crescente, per poi invertire in modo abbastanza brusco in un trend di tipo ribassista. Nell'ultima parte del grafico i prezzi si sono mossi senza particolari variazioni, all'interno di un trend laterale.

FIGURA 7.9 – Il concetto di trend nel grafico bitcoin.

Per comprendere il trend è necessario analizzare la direzione dei prezzi. Nello specifico bisogna focalizzare la propria attenzione sui punti di massimo e minimo dei prezzi. Un trend rialzista è caratterizzato da massimi e minimi crescenti, un trend ribassista è caratterizzato da massimi e minimi decrescenti e un trend laterale è

caratterizzato da massimi e minimi simili.

Come vedremo nel paragrafo "Supporti e resistenze", questo tipo di analisi è estremamente importante per tracciare livelli di supporto e resistenza attendibili.

La storia si ripete

Come ben sappiamo, per l'Analisi tecnica un ruolo cruciale è dato allo studio dell'andamento dei prezzi, poiché in essi vi è tutto: riflettono un insieme di fattori di varia natura, inclusi anche quelli di carattere psicologico, ed è prevedibile che in determinati momenti

del mercato la storia si ripeta, generando così, dal punto di vista grafico, delle configurazioni tipiche, dette *pattern*.

I *pattern* non sono altro che modelli che si ripetono nel tempo. Se individuati correttamente, possono fornire maggiori probabilità e indicazioni per comprendere l'evoluzione futura delle quotazioni. Alcuni esempi sono le formazioni grafiche quali triangoli, testa e spalle, doppio massimo, *spike, flag* oppure le formazioni a candele, tra cui ricordiamo *engulfing, harami* e *piercing line*. Data l'ampiezza di tale trattazione, per l'approfondimento di tali tipi di figure rimandiamo al testo *Analisi tecnica dei mercati finanziari* di John

Murphy. L'aspetto che a noi preme sottolineare è il fatto che l'esistenza di questi *pattern* rende evidente che nei mercati finanziari vi siano situazioni che si ripetono.

Supporti e resistenze

Il concetto di supporto e resistenza rappresenta uno dei principi cardine dell'Analisi tecnica.

Il supporto è un particolare livello di prezzo attorno al quale le correnti di domanda hanno la capacità di arrestare la flessione dei prezzi. Un livello di supporto sul quale si arresta la discesa dei prezzi fornisce un potenziale segnale

di acquisto, in quanto indica una maggiore presenza di compratori rispetto ai venditori.

Tuttavia, la decisa rottura al ribasso di un livello di supporto rappresenta un segnale di vendita, indicando una presunta incapacità dei compratori nel fronteggiare la forza predominante dei venditori.

Nella Figura 7.10 abbiamo tracciato un livello di supporto che passa per i due minimi di febbraio 2014. Tale supporto è stato violato al ribasso nella giornata del 25 febbraio 2014 con una candela estremamente volatile, ma tale livello è stato recuperato nel corso della stessa giornata ed è poi rimasto

inviolato fino a fine marzo, quando vi è stata la definitiva rottura del supporto con il prezzo di chiusura della candela.

FIGURA 7.10 – Supporto sul grafico del bitcoin.

Invece, la resistenza è un particolare livello di prezzo attorno al quale le correnti di offerta hanno la capacità di arrestare l'ascesa dei prezzi. Un livello di resistenza sul quale si arresta la salita

dei prezzi fornisce un potenziale segnale di vendita, in quanto indica una maggiore presenza di venditori, rispetto ai compratori. Tuttavia, la decisa rottura al rialzo di un livello di resistenza rappresenta un segnale di acquisto, indicando una presunta incapacità dei venditori nel fronteggiare la forza predominante dei compratori. La Figura 7.11 mostra una fortissima resistenza rimasta inviolata per diversi mesi, alla cui rottura, nell'ottobre 2013, è partito un forte movimento ascendente.

I livelli di supporto e resistenza che abbiamo esposto nei precedenti grafici sono di tipo statico, cioè, una volta fissati, il prezzo non varia in base al passare del tempo. Questi livelli

possono però essere anche di tipo dinamico, e in tal caso si parla di *trendline*. Un *trendline* è una linea retta che passa per almeno due punti di massimo o di minimo, con lo scopo di rendere evidente il trend del mercato. Il *trendline* rialzista è tracciato congiungendo almeno due minimi, di cui il secondo è più alto, e funge da supporto dinamico ai prezzi (Figura 7.12).

Il trendline ribassista è tracciato congiungendo almeno due massimi, di cui il secondo è più basso, e funge da resistenza dinamica ai prezzi (Figura 7.13).

FIGURA 7.11 – Resistenza sul grafico del bitcoin.

FIGURA 7.12 – Trendline rialzista sul grafico del bitcoin.

FIGURA 7.13 – Trendline ribassista sul grafico del bitcoin.

Sia per i livelli statici sia per quelli dinamici valgono le seguenti considerazioni:

- l'affidabilità risulta tanto maggiore quanto più elevato è il numero di contatti tra i prezzi e la linea;
- l'inversione di tendenza si

verifica quando viene identificato il definitivo *breakout* (rottura) della linea e prende avvio una nuova fase di mercato.

È facile verificare tali considerazioni sulla base dei grafici che abbiamo mostrato in precedenza (Figura 7.12 e Figura 7.13), nei quali si vede come a ogni contatto tra il prezzo e il supporto/resistenza si rafforza in definitiva quest'ultimo e, a distanza di tempo, il prezzo si ferma nuovamente sui livelli identificati dal supporto/resistenza. Solo a fronte di una decisa rottura si è in grado di assistere al formarsi di un nuovo trend, che a sua volta presenterà nuovi supporti e

resistenze.

IL BITCOIN E LE MEDIE MOBILI

Presentiamo ora alcuni dei principali strumenti che vengono utilizzati nell'Analisi tecnica. Lo strumento sicuramente più utilizzato al mondo sono le medie mobili, vediamo di capire insieme il motivo. Le serie storiche di qualunque dato economico risultano generalmente inficiate da componenti erratiche che contribuiscono a occultare il sottostante andamento tendenziale del

fenomeno oggetto d'analisi. Il problema dell'eccessiva irregolarità della serie temporale può essere risolto attraverso il noto procedimento statistico di perequazione per medie mobili, che consente di restituire alla serie maggiore continuità. L'Analisi tecnica si avvale di questo strumento statistico sia per regolarizzare la serie temporale, processo conosciuto come *smoothing*, sia per individuare segnali operativi di gestione di posizioni speculative. A questo scopo sono utilizzate tre diverse tipologie di medie mobili:

- medie mobili semplici – SMA;[18]
- medie mobili ponderate –

WMA;[19]

- medie mobili esponenziali – EMA.[20]

SMA

La media mobile semplice è senz'altro la più utilizzata e si costruisce banalmente con una media aritmetica di *n* osservazioni, aggiornata nel tempo con l'eliminazione del dato più remoto e l'aggiunta di quello più recente.

Riportiamo la formula di calcolo:

$$SMA_{(t,\,n)} = \sum_{i=0}^{n-1} \frac{P_{t-i}}{n}$$

In generale una media mobile di dominio *n* elimina le componenti erratiche di periodo minore o uguale a n, pertanto medie mobili semplici calcolate su ampi domini operano un più accentuato livellamento della serie perequata. Per questo motivo le medie mobili di periodi lunghi (per esempio, 200 giorni) fungono da supporti/resistenze molto attendibili (Figura 7.14).

FIGURA 7.14 – Grafico del bitcoin con SMA a 20 giorni

WMA

Alcuni difetti del tipo di perequazione semplice sono l'arbitrarietà nella definizione del dominio temporale, nonché l'attribuzione di un peso identico (1 / n) a tutti gli elementi della serie, a prescindere dalla collocazione storica

rispetto all'epoca del calcolo. Può risultare opportuno dunque pesare in modo diverso i prezzi, come viene effettivamente fatto nella media mobile ponderata.

Riportiamo la formula di calcolo:

$$WMA_{(t,\,n)} = \frac{\sum_{i=0}^{n-1} \left(w_i \cdot P_{t-i} \right)}{\sum_{i=0}^{n-1} w_i}$$

La ponderazione riduce il ritardo rispetto alla media mobile semplice. Per l'attribuzione dei pesi della media mobile ponderata si segue generalmente il metodo lineare, moltiplicando l'ultimo termine per n, il penultimo per n-1 ecc.

È evidente che si tratta di uno strumento più adattabile alle esigenze dell'analista ma è esposto all'arbitrarietà della scelta della ponderazione (Figura 7.15).

FIGURA 7.15 – Grafico del bitcoin con WMA a 20 giorni.

EMA

Una ponderazione più raffinata, che

evita la perdita di dati caratterizzante le due precedenti elaborazioni di medie mobili, si ottiene attraverso la perequazione esponenziale. Quest'ultima consente di conservare l'effetto anche dei dati più remoti che, seppur gradualmente ridotto, non è mai annullato (Figura 7.16).

Riportiamo la formula di calcolo:

$$EMA_{(t,\,n)} = \frac{\sum_{i=0}^{n-1}\left(w^{n-i} \cdot P_{t-i}\right)}{\sum_{i=0}^{n-1} w^{n-i}}$$

FIGURA 7.16 – Grafico del bitcoin con EMA a 20 giorni.

Le tre medie a confronto

Mostriamo ora un grafico che pone a confronto i pesi che vengono associati dalle diverse medie alle osservazioni di prezzo (Figura 7.17). È immediato vedere come, rispetto al valore costante della SMA, le altre due medie pongono

maggior importanza, una, sulle ultime osservazioni (la WMA) e, l'altra, oltre che sulle ultime osservazione anche su tutta la storia del prezzo (la EMA).

Riportiamo su un grafico le tre medie qui esposte. Come è possibile osservare nella Figura 7.18, la WMA segue con maggior cura le dinamiche del prezzo, mentre la EMA (dal momento che tiene in conto tutta la storia del bitcoin) segue il prezzo con minore reattività. La SMA si assesta in maniera intermedia tra le due, fornendo a nostro avviso la migliore situazione di compromesso.

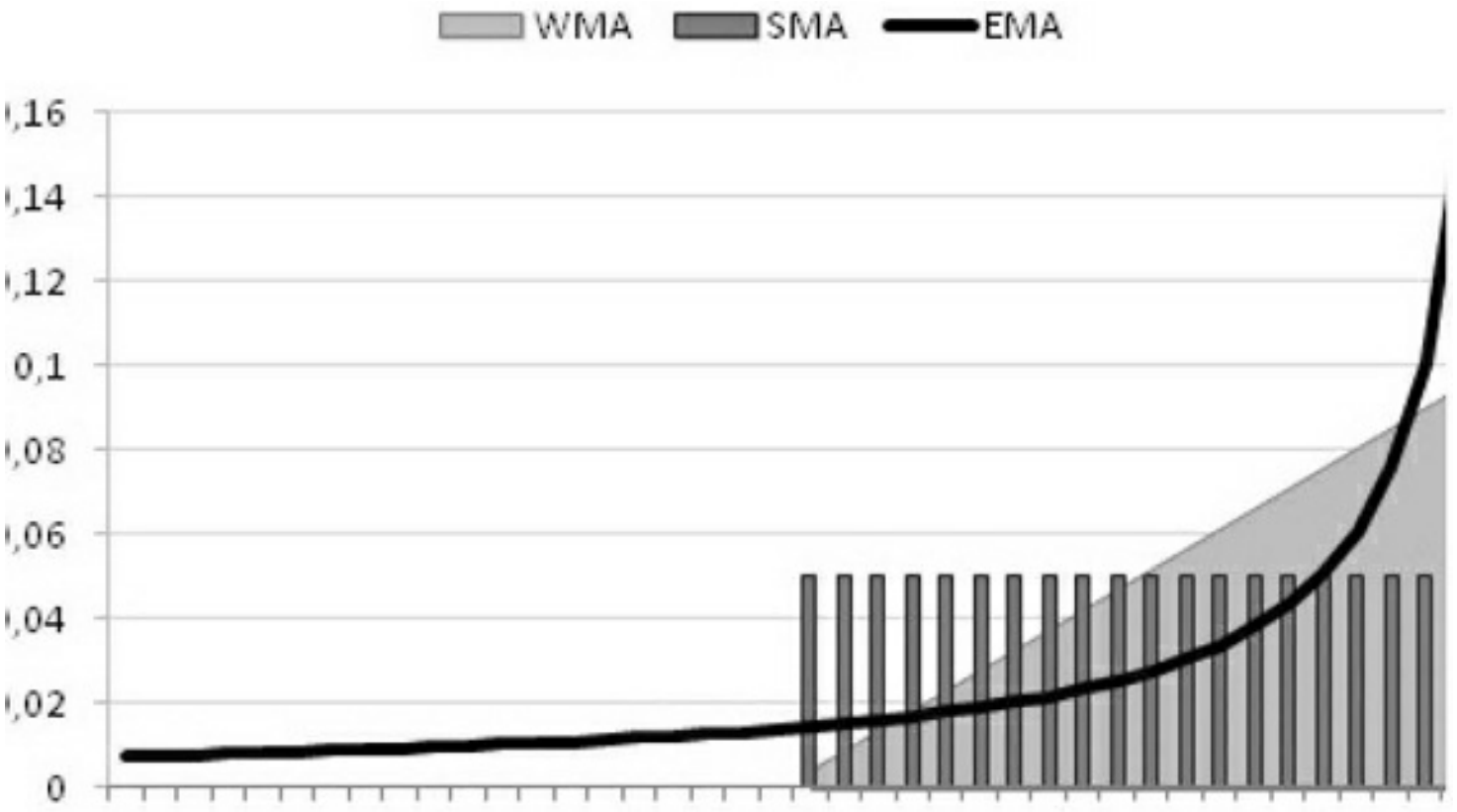


FIGURA 7.17 – Confronto tra i pesi delle medie mobili SMA, WMA e EMA.

FIGURA 7.18 – Confronto SMA (linea

continua), WMA (linea a puntini) e EMA (linea tratteggiata).

Per utilizzare con successo le medie mobili, il fattore più importante da definire è la durata temporale. Occorre subito precisare che non esiste un intervallo temporale ottimale per ogni mercato, ma ognuno risponde in maniera diversa. Infatti, deve essere considerata la particolare variabilità della serie storica analizzata, che è sempre caratterizzata da peculiarità evolutive certamente non sfruttabili con modalità standardizzate. In secondo luogo, deve essere individuato l'orizzonte temporale entro il quale attivare gli interventi speculativi: analisi di breve periodo

richiederanno certamente un dominio più ridotto, che si esprime in un'immagine grafica molto prossima all'effettiva serie di prezzo; mentre, analisi di lungo periodo richiederanno un dominio più ampio e l'immagine grafica della media risulterà più smussata e meno reattiva alle oscillazioni di prezzo. I numeri più utilizzati dagli analisti sono 9, 20, 25, 50, 90 e 200; talvolta vengono impiegati anche alcuni numeri della serie di Fibonacci:[21] 3, 5, 8, 13, 21, 34, 55, 89, 144 (Figura 7.19).

FIGURA 7.19 – Confronto tra SMA 9 giorni (linea sottile), SMA 20 giorni (linea spessa) e SMA 50 giorni (linea tratteggiata).

Solamente utilizzando le medie mobili si possono già impostare alcuni primi semplici *trading system.* Le strategie operative suggerite dall'impiego di medie mobili possono derivare dall'interazione tra una o più medie mobili e il movimento dei prezzi di mercato, o dall'interazione di sole

medie mobili.

Nel primo caso (Figura 7.20), la procedura finalizzata al sistematico raffronto tra la serie storica dei prezzi e la media mobile per la gestione operativa di posizioni speculative prevede il rispetto di due semplici regole:

- Assumere posizioni lunghe (cioè al rialzo) se il movimento dei prezzi taglia dal basso verso l'alto la media mobile.
- Liquidare le posizioni lunghe e assumere posizioni corte (cioè al ribasso) se il movimento dei prezzi taglia dall'alto verso il

basso la media mobile.

Nel secondo caso (Figura 7.21), si prendono posizioni lunghe se una media mobile di breve periodo taglia dal basso verso l'alto una media mobile di più lungo periodo, e viceversa si prendono posizioni corte se una media mobile di breve periodo taglia dall'alto verso il basso una media mobile di più lungo periodo.

FIGURA 7.20 – Caso 1: il prezzo taglia prima dal basso verso l'alto e poi dall'alto verso il basso la media mobile semplice.

FIGURA 7.21 – Caso 2: la SMA a 20 giorni (linea continua) taglia prima verso il basso e poi verso l'alto la SMA a 50 giorni (linea tratteggiata).

Queste tipologie di trading system hanno un indubbio vantaggio nella loro semplicità. Inoltre, hanno come caratteristica principale il fatto di essere

trend follower, cioè delle strategie operative in grado di funzionare bene in un ambiente di forte trend, mentre danno numerosi falsi segnali in caso di mercato incerto.

Terminiamo la nostra trattazione sulle medie mobili riportando un famoso studio della Merrill Lynch riportato da John Murphy,[22] che verificò su un arco temporale di 7 anni, dal 1970 al 1976, il comportamento dei vari tipi di medie mobili su ben 13 mercati di commodities. Il periodo considerava movimenti di prezzo da 3 a 70 giorni. Da questo poderoso studio derivarono tre interessanti conclusioni:

- Nessuna media mobile risultò la migliore per ogni mercato. Infatti, ogni mercato ha la sua media mobile ottimale.
- Le medie mobili di lungo periodo generarono un trading profittevole superiore a quelle di breve. In particolare, la media mobile a otto settimane (40 giorni) con un numero sorprendente di successi.
- La media mobile semplice risultò la migliore superando le performance generate dalle medie ponderate ed esponenziali. Su 13 mercati testati, la media mobile semplice funzionò bene in

10 casi, quella ponderata in 2 casi, mentre l'esponenziale risultò valida solo nel mercato del cacao.

Queste importanti conclusioni ci confermano come anche per il bitcoin sia necessario selezionare una media mobile ottimale.

IL BITCOIN E LE BANDE DI BOLLINGER

Introduciamo alcuni degli studi più importanti di John Bollinger, trader

professionista e uno dei principali studiosi dell'Analisi tecnica. Scopriremo insieme che le sue conclusioni[23] si riveleranno di importanza fondamentale anche per il mercato del bitcoin. I suoi studi sono nati dal forte desiderio di riconciliare e chiudere il gap tra l'Analisi fondamentale e l'Analisi tecnica e lui stesso coniò il termine di "Analisi razionale". Tutti i suoi scritti sono tesi a colmare questa distanza soffermandosi sugli aspetti in comune piuttosto che sulle differenze.

Le Bande di Bollinger

Per costruire le Bande di Bollinger si parte con la misurazione di una tendenza centrale e, successivamente, con una banda superiore e una banda inferiore. Ci poniamo, quindi, le seguenti domande: quale deve essere la misura centrale di tendenza? Come determinare l'intervallo?

Le Bande di Bollinger rispondono che la misura della tendenza centrale debba essere una media mobile semplice e l'intervallo debba essere delineato attraverso una misura della volatilità, utilizzando la deviazione standard (σ), statisticamente definita come scarto quadratico medio o radice quadrata della varianza.

Riportiamo la formula di calcolo:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N} (x_i - \mu)^2}{N}}$$

Entrambe le due misurazioni (media mobile e deviazione standard) vengono calcolate sullo stesso intervallo temporale, che di default Bollinger stesso fissa a 20 giorni.[24]

A tale media mobile viene aggiunto e sottratto 2 volte il valore della deviazione standard, calcolata anch'essa sui 20 giorni precedenti. Così facendo si creano queste due bande (una inferiore e una superiore) che, per costruzione,

contengono sempre al loro interno la media mobile. Schematizzando quanto visto finora, le Bande di Bollinger consistono in:

- una media mobile semplice a N periodi (μ);
- una banda superiore costruita sommando alla media mobile K volte la deviazione standard ($\mu + K \cdot \sigma$);
- una banda inferiore costruita sottraendo alla media mobile K volte la deviazione standard ($\mu \times K \cdot \sigma$).

I valori fissati da Bollinger sono $N = 20$

e $K = 2$ (Figura 7.22).

FIGURA 7.22 – Le Bande di Bollinger sul grafico del bitcoin.

Molti analisti hanno cercato di migliorare l'efficacia delle Bande di Bollinger introducendo medie mobili diverse (per esempio quella esponenziale), ma riteniamo che sia più corretto utilizzarle nella loro versione originale. Questo perché lo stesso

Bollinger testò diverse tipologie di medie mobili, ma non trovò alcun vantaggio. Inoltre, lo scopo della media mobile nelle Bande è quello di fissare un punto di mezzo, mentre con altre diverse medie mobili si introduce comunque un fattore esogeno, che non sempre è facilmente controllabile.

Il punto di forza di queste Bande è la loro capacità di essere in grado di adattarsi a ogni contesto di mercato e mantenere sempre una valida definizione di ciò che è “alto” e di ciò che è “basso”. Da un punto di vista operativo, le Bande di Bollinger danno segnali di acquisto e vendita quando si verificano le seguenti condizioni:

- Se il prezzo esce dalla banda superiore e successivamente vi rientra, si ottiene un segnale di vendita. Questo corrisponde a un rapido aumento del prezzo e a un successivo rallentamento o aggiustamento.
- Se il grafico del prezzo esce dalla banda inferiore e successivamente vi rientra, si ottiene un segnale di acquisto, cioè il prezzo è calato molto velocemente fino ad arrestarsi e potrebbe essere pronto a invertire il trend.

Entrambe queste caratteristiche rientrano nella concezione statistica della

regressione verso la media. Benché alcuni studi confermino che tale fenomeno si verifichi anche sui mercati finanziari, non è però una certezza che i prezzi debbano necessariamente tendere verso la media. Infatti, le Bande di Bollinger possono generare falsi segnali, in quanto per esempio il prezzo potrebbe uscire dalla banda inferiore (superiore), rientrare e continuare il trend discendente (ascendente) (Figura 7.23).[25]

Questo fenomeno è molto comune in situazioni di trend molto forti, e soprattutto si presenta con una frequenza maggiore nei mercati molto volatili. Il mercato del bitcoin sicuramente ne

rappresenta uno dotato di una volatilità elevata e, quindi, tale fenomeno è più frequente rispetto ad altri, come mostrato nella Figura 7.23. Vedremo nel corso del libro come sfruttare al meglio le caratteristiche di questo mercato.

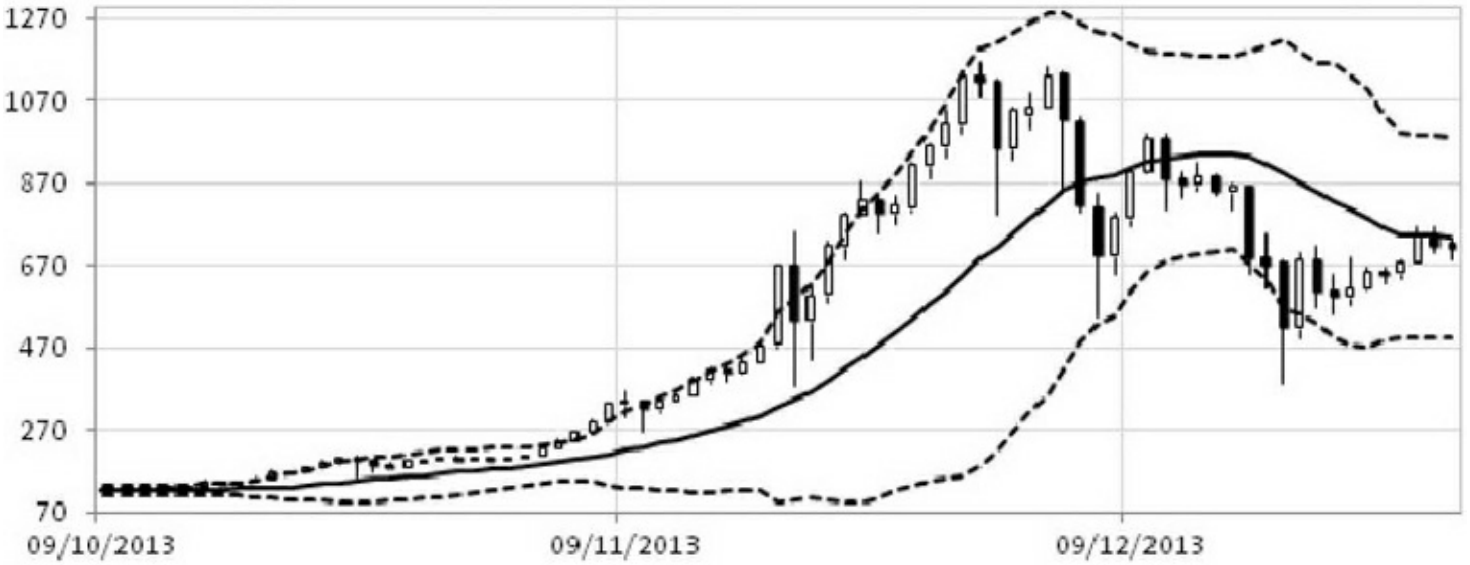


FIGURA 7.23 – Il "*walking on the band*" sul grafico del bitcoin.

Per concludere la trattazione sulle Bande di Bollinger occorre precisare

che sarebbe errato utilizzare semplicisticamente i segnali di acquisto o vendita quando si raggiunge un limite estremo e in quel momento settare il prezzo obiettivo sulla media. Per questi motivi, lo stesso John Bollinger consiglia di utilizzare altri indicatori combinati con le Bande, con lo scopo di aumentarne l'efficacia ed eliminare i falsi segnali. Tali indicatori sono noti come "%b" e "BandWidth", e saranno oggetto di trattazione nei prossimi paragrafi.

Il Percentage B o "%b"

Il "%b" è un indicatore costruito a

partire dalle Bande di Bollinger ed è in grado di dirci dove si trova il prezzo in relazione alle Bande stesse.

Riportiamo la formula di calcolo:

$$\%b = \frac{(Prezzo\ chiusura - BB\ inferiore)}{(BB\ superiore - BB\ inferiore)}$$

Il valore del "%b" è pari a:

- 1 quando il prezzo tocca la banda superiore;
- 0,5 quando il prezzo si trova sulla media;
- 0 quando il prezzo tocca la banda inferiore.

Tuttavia, occorre notare come il valore di “%b” non è vincolato tra 0 e 1. Può accadere che il prezzo sia maggiore (minore) della banda superiore (inferiore). Per esempio, se il valore di “%b” fosse 1,1 vorrebbe dire che i prezzi si trovano sopra la banda superiore di un 10% (Figura 7.24).

FIGURA 7.24 – Il "%b" e le Bande di Bollinger sul grafico del bitcoin.

Questo ovviamente rende tale indicatore immediatamente più fruibile per scrivere dei programmi di trading system rispetto alle sole Bande di Bollinger, le quali sono più utili per un'analisi grafica. Infine, tale indicatore

è molto utile per riconoscere i *pattern* di prezzo.

BandWidth

Il secondo indicatore derivato dalle Bande di Bollinger è il BandWidth.

Riportiamo la formula di calcolo:

$$BandWidth = \frac{(BB\ superiore - BB\ inferiore)}{Media\ Mobile}$$

Utilizzando i valori standard è facile notare che tale valore sia pari a 4 volte il coefficiente di variazione σ / μ.[26]

Questo indicatore è fondamentale per poter individuare le situazioni in cui

la volatilità ha raggiunto un livello così basso da farne prevedere un'inversione imminente nel trend. Il suo utilizzo più semplice è quello di verificare quando tocca il minimo degli ultimi sei mesi, poiché da tale livello è estremamente probabile che la volatilità dei prezzi possa aumentare.

Nella Figura 7.25 si osserva in modo molto chiaro come, a distanza di circa cinque mesi, il BandWidth è arrivato a toccare nuovamente lo stesso punto di minimo, da cui abbiamo avuto un aumento di volatilità dei prezzi. Inoltre, questo grafico ci mostra l'altro fondamentale utilizzo di questo indicatore: la sua capacità di identificare un trend.

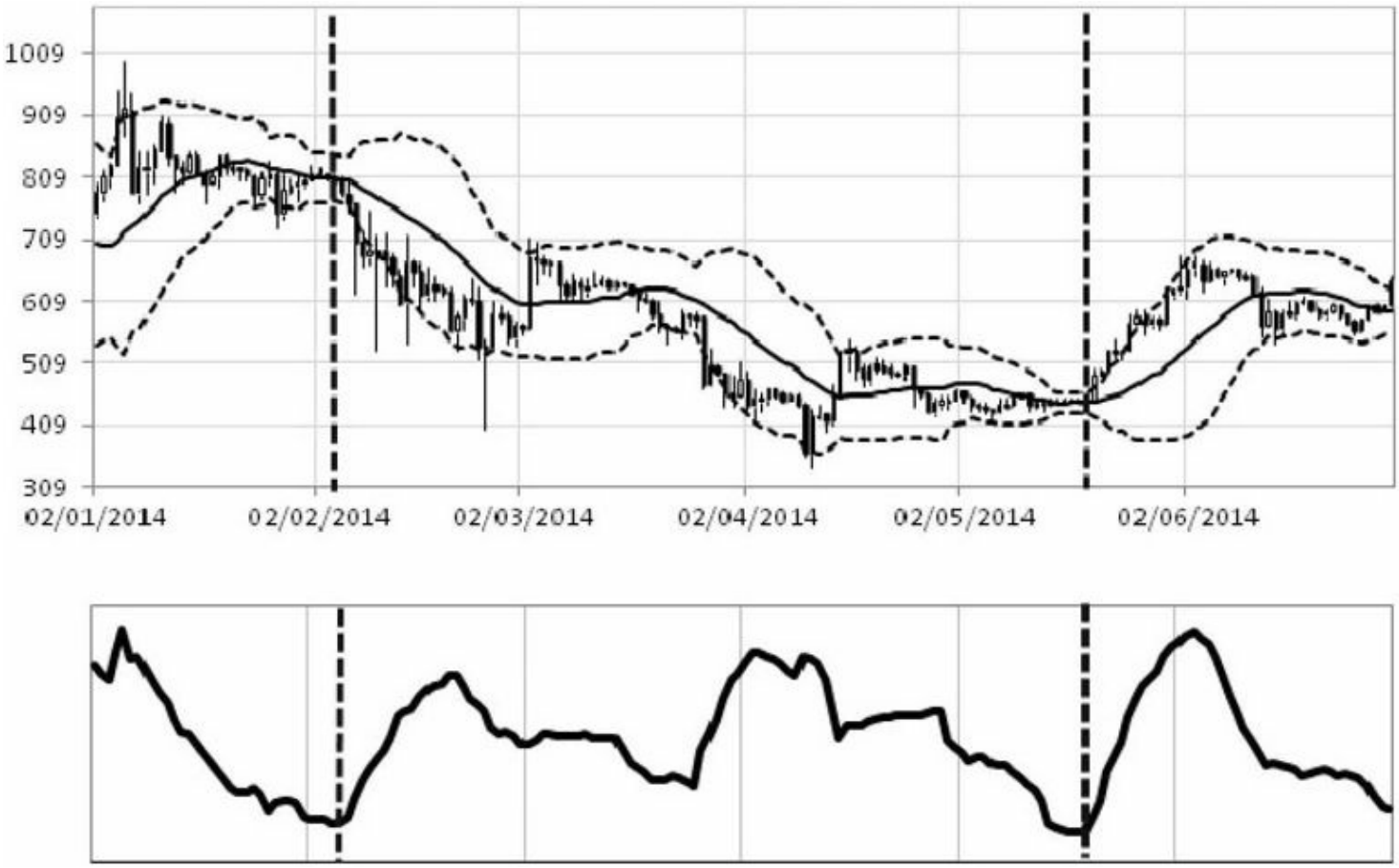


FIGURA 7.25 – Il BandWidth e le Bande di Bollinger sul grafico del bitcoin.

Quasi tutti i più importanti trend nascono quando il BandWidth ha valori piuttosto bassi. La rottura di un trading range da parte dei prezzi, accompagnata da una brusca accelerata del BandWidth, sono spesso le condizioni che indicano

l'inizio di un forte trend. È proprio il caso mostrato nel nostro grafico.

Infine, l'ultima importante proprietà del BandWidth è la sua capacità di identificare la fine di un trend. Se l'inizio è, infatti, sostenuto da un aumento del BandWidth, una sua flessione dà un primo campanello di allarme che il trend è prossimo all'esaurimento.

Terminiamo la trattazione delle Bande di Bollinger mostrando sullo stesso grafico tutti gli indicatori di John Bollinger. Lo facciamo prendendo in considerazione proprio l'esempio più critico, nel quale il prezzo si muove lungo le bande (Figura 7.26).

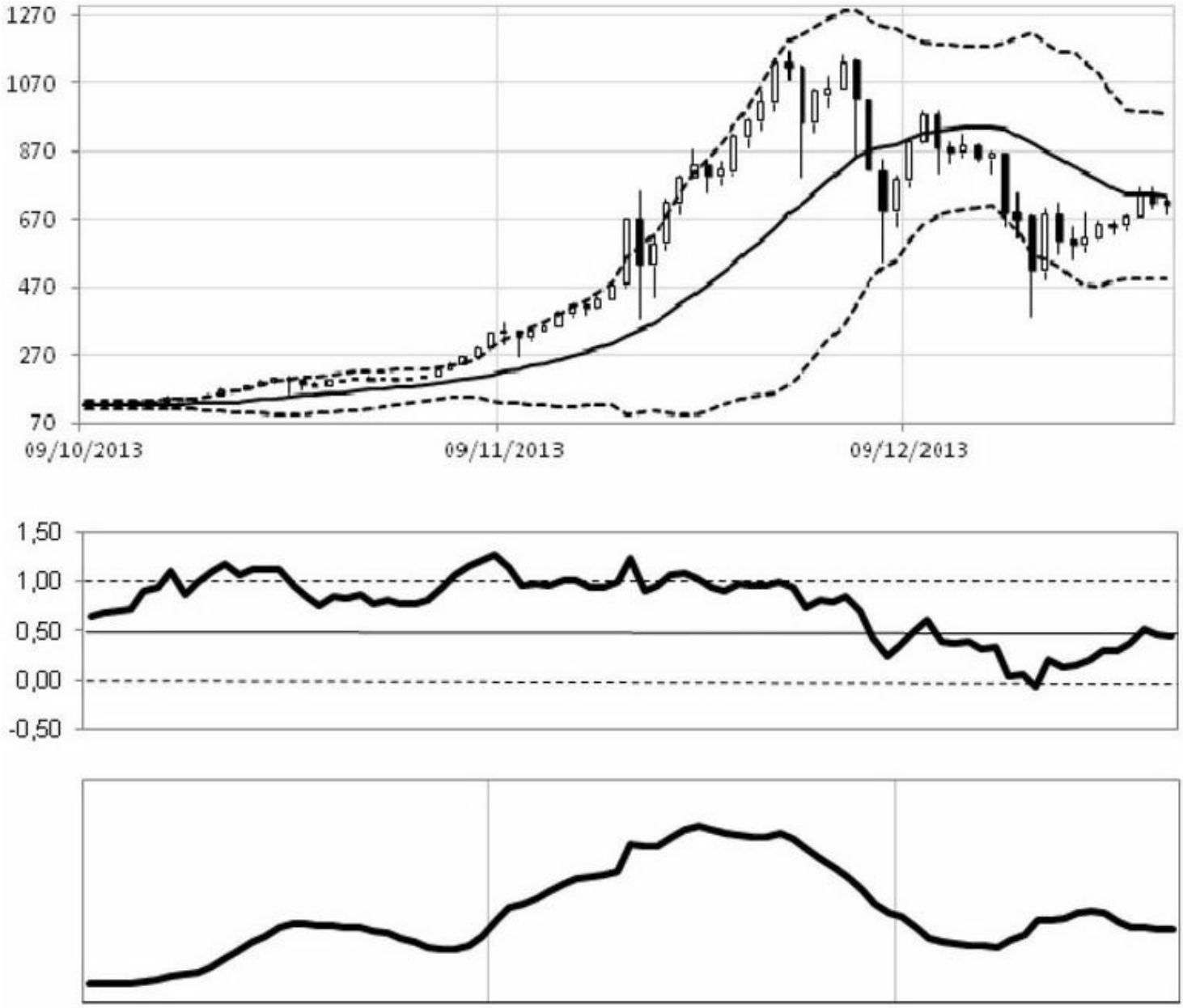


FIGURA 7.26 – Bande di Bollinger, il "%b" e il BandWidth sul grafico del bitcoin.

È interessante notare come, nei casi in cui il prezzo sviluppi un forte trend, le Bande di Bollinger superiore o inferiore

fungono da pista per i prezzi. In questi casi il "%b" è stabile intorno al valore 1 e il BandWidth mantiene anch'esso un trend rialzista. Il declinare del BandWidth dà, come già detto, il primo segnale di allarme che il trend è vicino alla fine e, come si può facilmente verificare dal grafico, anche il "%b" inizia a scendere.

IL BITCOIN E IL WILLIAMS %R

Introduciamo un importante indicatore di trading sviluppato da Larry Williams:[27]

il Williams Percentage Range (%R). Tale indicatore rientra nella categoria degli oscillatori.[28]

Con tale definizione ci si riferisce a elementari elaborazioni quantitative della serie dei prezzi volte a isolare determinate caratteristiche di velocità, forza o volatilità delle quotazioni rispetto al rapporto tra forze bullish (in acquisto) e bearish (in vendita). Un esame analitico di tutti gli oscillatori codificati progressivamente dalla letteratura dell'Analisi tecnica richiederebbe un intero volume. Questa considerazione, unita al fatto che spesso i vari oscillatori forniscono indicazioni altamente correlate, ci inducono a

presentare in questo paragrafo il più famoso di tutti gli oscillatori. Introduciamo subito la formula del %R:

$$Williams\ \%R = \frac{(Massimo\ tra\ Massimi(n) - Prezzo\ Chiusura)}{(Massimo\ tra\ Massimi(n) - Minimo\ tra\ Minimi(n))} \cdot (-100)$$

Il Williams %R riflette il livello della chiusura rispetto al massimo tra i massimi toccati dal prezzo e va a confrontare tale misura rispetto al più ampio range degli ultimi *n* periodi. Larry Williams settò il valore *n* dei periodi di osservazione a 14. Tale valore viene, infine, moltiplicato per -100, al fine di dare all'oscillatore una lettura visiva concorde al movimento del prezzo.

Per costruzione, questo indicatore

oscilla quindi tra 0 e -100. Se il suo valore è compreso tra -80% e -100%, significa che ci troviamo in una situazione di ipervenduto, nelle quali il prezzo di chiusura è molto vicino al minimo e le forze in vendita prevalgono rispetto a quelle in acquisto.

Un valore compreso tra 0% e -20% indica una situazione di ipercomprato, nelle quali il prezzo di chiusura è molto vicino al massimo e segnala che i compratori prevalgono rispetto ai venditori. L'indicatore è composto da due linee orizzontali che tagliano appunto le soglie del -20% e dello -80%.

Dalla Figura 7.27 si può subito notare come il valore dell'oscillatore in

zona di ipercomprato non sia necessariamente un segnale bearish. Infatti, il prezzo del bitcoin resta per lungo tempo ipercomprato senza mai rintracciare. Queste letture di valori costanti nelle due zone estreme danno il segnale che un forte trend è in atto.

FIGURA 7.27 – Williams %R sul grafico del bitcoin.

Ricordate la Figura 7.23, in cui il prezzo faceva "*walking on the band*"? Nella Figura 7.28 vediamo sullo stesso grafico quale indicazione ci avrebbe fornito il Williams %R.

Il forte trend rialzista era stato

anticipato dall'indicatore di Larry Williams che, una volta entrato nella zona di ipercomprato, è rimasto stabilmente sopra il valore -20 per tutta la durata del trend.

La lettura generale, per tutti gli oscillatori che segnalano zone di ipercomprato e ipervenduto, è quella per cui il segnale si genera quando l'oscillatore inizia a uscire da queste zone estreme. Si attiva, quindi, un primo campanello di allarme, ma occorre sempre aspettare che tale movimento sia seguito da un movimento concorde del prezzo che confermi l'inversione nel trend.

FIGURA 7.28 – Williams %R sul grafico del bitcoin in forte trend.

Una lettura di valori estremi potrebbe suggerire che il movimento dei prezzi è troppo esteso, o si è verificato in un tempo troppo ristretto rispetto alla sua entità, e perciò diviene probabile una correzione.

Per ottenere informazioni pulite da questo indicatore è necessario associarlo all'interno di un trading system insieme ad altri indicatori che possano fungere da filtro per aiutarci a distinguere se siamo in presenza di una fase di inversione o di continuazione del trend.

IL BITCOIN E IL PARABOLIC SAR

Trattiamo ora un indicatore estremamente utile e originale, sviluppato da John W. Wilder jr. e

pubblicato nel libro *New Concepts in Technical Trading Systems* del 1978. Si tratta dell'indicatore Parabolico, noto anche come SAR (Stop And Reverse).

La caratteristica unica di questo strumento è l'assenza di base temporale, cioè la sua costruzione non si basa su parametri di tempo ma su variazioni di volatilità dei prezzi. Nel paragrafo "Trading system con il Parabolic SAR" vedremo che per costruire una media mobile è indispensabile definire un periodo di calcolo e la stessa cosa avviene per quasi tutti gli altri indicatori di Analisi tecnica, ma non per il parabolico. Infatti, il SAR prevede come input solo un fattore di accelerazione (AF = Acceleration Factor) compreso

tra 0,02 e 0,20 con incremento (Step) pari a 0,02. La formula è di tipo iterativo e si costruisce sommando al SAR precedente la differenza, moltiplicata per il fattore di accelerazione, tra il punto estremo (il massimo o il minimo del range precedente) e il SAR precedente.

Riportiamo la formula di calcolo:

$$SAR_{t+1} = SAR_t + AF \cdot (EP_{trade} - SAR_t)$$

$$0{,}02 < AF < 0{,}2$$

Da un punto di vista grafico, il SAR si presenta come una serie di punti posizionati al di sopra o al di sotto dei prezzi. Nella Figura 7.29 un esempio sul grafico del bitcoin.

FIGURA 7.29 – Il Parabolic SAR sul grafico del bitcoin.

È intuitivo comprendere che se i punti del SAR si trovano al di sopra dei prezzi, segnalano un trend di tipo ribassista (down trend) e in questa situazione l'indicatore funge da resistenza dinamica ai prezzi (Figura 7.30).

Mentre quando i punti del SAR si trovano al di sotto dei prezzi, segnalano

un trend di tipo rialzista (up trend) e in questa situazione l'indicatore funge da supporto dinamico ai prezzi (Figura 7.31).

Un trend resta in essere fino a quando non si verifica un nuovo taglio dei prezzi sull'indicatore SAR. Nello specifico, si passa da un trend ribassista a uno rialzista quando i prezzi rompono dal basso verso l'alto il valore del SAR precedente e da un trend rialzista a uno ribassista quando i prezzi rompono dall'alto verso il basso il valore del SAR precedente. In questo senso, il SAR si definisce un *true reversal system*, cioè un sistema di trading tale per cui ogni punto di stop è anche un punto di inversione.

FIGURA 7.30 – Il Parabolic SAR sul grafico del bitcoin in down trend.

FIGURA 7.31 – Il Parabolic SAR sul grafico del bitcoin in up trend.

Come si può notare dai grafici che abbiamo presentato, il valore del SAR non torna mai indietro ma si muove e si incrementa a ogni barra e solo nella direzione del trend. Per esempio, se siamo in direzione long allora il SAR si muoverà verso l'alto a ogni barra (questa è una funzione del tempo) con una distanza che dipende dal movimento dei prezzi (questa è una funzione del prezzo).

Le variazioni del SAR iniziano in modo graduale, per poi incrementarsi al crescere del fattore di accelerazione, assumendo una forma che ricorda un ramo di parabola.

Il pregio del SAR è di essere un

indicatore direzionale che tende a seguire in modo preciso il movimento dei prezzi, qualora questi si muovano con un trend ben definito. Proprio per questa ragione, riteniamo che il parabolico sia un valido strumento per l'operatività di trading in bitcoin.

---

18. SMA: Simple Moving Average.
19. WMA: Weighted Moving Average.
20. EMA: Exponential Moving Average.
21. Matematico italiano di nome Leonardo Pisano, figlio di Guglielmo dei Bonacci (da cui l'appellativo "Fibonacci" che deriva infatti da *filius Bonacci*). A lui si deve lo studio della famosa successione di numeri interi positivi in cui ciascun numero è la somma dei due precedenti.

22. Nel libro *Analisi tecnica dei mercati finanziari*.
23. Tratte dal libro *Bollinger on Bollinger Bands*.
24. Venti giorni sono approssimativamente il numero di giorni di trading in un mese.
25. Fenomeno chiamato "*walking on the band*".
26. Infatti si ha $[(\mu + K \cdot \sigma) - ((\mu - K \cdot \sigma)] / \mu = (2K \cdot \sigma) / \mu$ che per un valore di K=2 dà proprio $4 \cdot \sigma / \mu$.
27. Nel 1987, durante la "World Cup Championship of Futures Trading", Larry Williams ha guadagnato oltre un milione di dollari partendo con un conto di soli $ 10.000, realizzando un'incredibile ritorno sull'investimento del 10.900%.
28. Il nome si riferisce in modo particolare al tipico andamento di oscillazione in una banda delimitata da due estremi di questi indicatori. Talvolta tali estremi sono predefiniti e

assumono valori da 0 a 100 oppure da +1 a -1.

CAPITOLO 8

Trading system per il Bitcoin

In questo capitolo svilupperemo dei sistemi di trading automatici applicando gli strumenti di Analisi tecnica che abbiamo esposto nel capitolo precedente.

Procederemo per gradi, partendo dalla definizione delle regole e delle misure statistiche che serviranno per valutare le performance, per poi passare all'applicazione di semplici trading system basati sul cross di due medie mobili, sulle Bande di Bollinger, sull'oscillatore di Larry Williams e sul Parabolic SAR. Come sappiamo, ogni strumento presenta delle specifiche regole operative con chiari connotati di oggettività. L'errore più frequente che

un trader può commettere è quello di non rispettare in maniera rigorosa tali regole, lasciandosi condizionare dal proprio "ego", con la conseguenza di un aumento di soggettività nel trading e con la possibile distorsione del segnale stesso. Il vantaggio di utilizzare un trading system è proprio quello di garantire l'oggettività, semplificando il tutto con un segnale di ingresso per una determinata quantità e uno di uscita. In questo contesto, il trader deve solo lavorare sull'ottimizzazione dell'algoritmo, cioè sulle regole che compongono il trading system, eseguendo in modo oggettivo i segnali generati.

Non fraintendete però quello che

abbiamo appena scritto: i trading system non rappresentano la scelta definitiva per il trading, ma solo un mezzo efficiente per eliminare la componente psicologica. Inoltre, precisiamo che si tratta di un campo di lavoro che richiede competenze avanzate di Analisi tecnica, ma soprattutto di statistica e programmazione.

Pertanto, lo scopo che ci prefiggiamo è quello di mostrarvi come sia possibile tradare in maniera automatica anche sul mercato Bitcoin, fornendovi indicazioni e spunti per approfondire in maniera opportuna e professionale questo ambito di attività. Inoltre precisiamo che per ottenere dei

trading system robusti è indispensabile combinare diversi indicatori tra loro. Solo per semplicità di trattazione, nel corso del capitolo ci concentreremo ad analizzare trading system composti da un solo indicatore lasciando al lettore l'onere di approfondire in maniera accurata tali studi.

Le regole generali per tutti i trading system che presenteremo in questo capitolo sono le seguenti:

- Se il segnale viene generato il giorno *t* si entra in posizione a mercato al prezzo di apertura (Open) del giorno *t*+1:

$$\text{Segnale}_{(t)} \Rightarrow \text{Esecuzione del Segnale}_{(\text{Open}_{(t+1)})}$$

- La quantità di bitcoin che verrà comprata o venduta a mercato è calcolata dividendo il capitale disponibile al giorno t per il prezzo di chiusura (Close) sempre del giorno *t*:[29]

$$\text{Quantità}_{(t+1)} \Rightarrow \frac{\text{Totale Capitale disponibile}_{(t)}}{\text{Prezzo Close}_{(t)}}$$

- Inoltre, assumiamo i costi di slippage[30] pari all'1%. Tale valore è stato scelto così alto in via cautelativa e per rispecchiare l'elevata volatilità del mercato

Bitcoin. Risulterà, quindi, che gli effettivi prezzi di ingresso e di uscita di tutte le operazioni saranno calcolati nel seguente modo:

$$\mathrm{Pacquisto}_{(\mathrm{effettivo})} = \mathrm{P}_{(\mathrm{open})} + (1\% \cdot \mathrm{P}_{(\mathrm{Open})})$$

$$\mathrm{Pvendita}_{(\mathrm{effettivo})} = \mathrm{P}_{(\mathrm{open})} - (1\% \cdot \mathrm{P}_{(\mathrm{Open})})$$

- Ipotizziamo, per uniformità di trattazione, che siano pari a zero i costi di commissione. Tale ipotesi non inficia, se non superficialmente, la nostra analisi, in quanto i costi di commissione sono comunque molto bassi sul mercato Bitcoin e

possiamo considerarli già compresi nei costi di slippage.

- L'intervallo temporale della serie storica di prezzo[31] che prenderemo in considerazione sarà dal 21/05/2012 fino al 21/11/2014 con time frame giornaliero.

Occorre infine presentare le modalità con le quali è possibile analizzare e studiare in maniera obiettiva i diversi trading system, andando a capire quali siano i punti di forza e di debolezza di ognuno.

Per valutare in maniera appropriata i risultati di una strategia di trading è indispensabile utilizzare delle misure

statistiche. Nel corso dei prossimi paragrafi, a valle dell'applicazione dei vari trading system, provvederemo a utilizzare le seguenti misure in modo da fornire una tabella standard e obiettiva di valutazione:

- Gross Profit: è la somma di tutti i profitti.
- Gross Loss: è la somma di tutte le perdite.
- Total Net Profit: è la differenza tra Gross Profit e Gross Loss. Se la differenza è positiva allora il trading system ha generato un profitto, in caso contrario una perdita.

- Profit Factor: è il rapporto in valore assoluto tra Gross Profit e Gross Loss. Questo rapporto esprime il rischio associato a un determinato ammontare di profitto. Deve essere almeno maggiore di 1. È da preferire un valore elevato poiché significa che a un aumento del rischio corrisponde un aumento più che proporzionale del profitto.
- Number of Winning Trades: è il numero di trade a profitto.
- Number of Losing Trades: è il numero di trade in perdita.
- Total Number of Trades: è il numero totale di trade.

- Percent Profitable: è il rapporto tra numero di trade a profitto e il numero totale di trade. Non rappresenta però una voce determinante nella valutazione dell'affidabilità di un trading system.
- Average Winning Trade: è la media del profitto generato dai trade positivi.
- Average Losing Trade: è la media della perdita generata dai trade negativi.
- Ratio AvgWin/AvgLos: è il rapporto tra Average Winning Trade e Average Losing Trade. È da preferire un valore elevato,

poiché significa che a un aumento del rischio medio corrisponde un aumento più che proporzionale del profitto medio.

- Average Bars in Winning Trades: è la durata media in termini di tempo dei trade a profitto.
- Average Bars in Losing Bars: è la media in termini di tempo dei trade in perdita.
- Max Drawdown: è il massimo valore di declino dell'Equity Line (linea dei profitti).
- Return on Account: è la percentuale di valorizzazione del capitale investito.
- Percent of Time in the Market: è la percentuale di tempo con

posizioni aperte. Un valore elevato di questa percentuale corrisponde a un maggior rischio.

L'elenco non è completo nel senso che esistono numerose altre statistiche, ma riteniamo che queste siano le più attendibili per gli scopi che ci siamo prefissati in questa sezione del libro. Siamo ora pronti per procedere con lo studio dei diversi trading system.

TRADING SYSTEM CON LE MEDIE MOBILI

Sulla base di quanto presentato nel paragrafo “Il Bitcoin e le medie mobili” impostiamo ora un trading system che utilizza il crossover tra una media mobile lenta e una veloce. I parametri selezionati sono i seguenti:

- media mobile semplice a 5 giorni;
- media mobile semplice a 10 giorni.

Il trading system segue le seguenti regole:

- ingresso long (chiudendo eventuali posizioni corte) quando

la media mobile semplice a 5 giorni taglia dal basso verso l'alto la media mobile semplice a 10 giorni;

- ingresso short (chiudendo eventuali posizioni lunghe) quando la media mobile semplice a 5 giorni taglia dall'alto verso il basso la media mobile semplice a 10 giorni.

Questo trading system, per costruzione, resta sempre a mercato. Vediamo nella Figura 8.1 come e quando viene generato un segnale di ingresso.

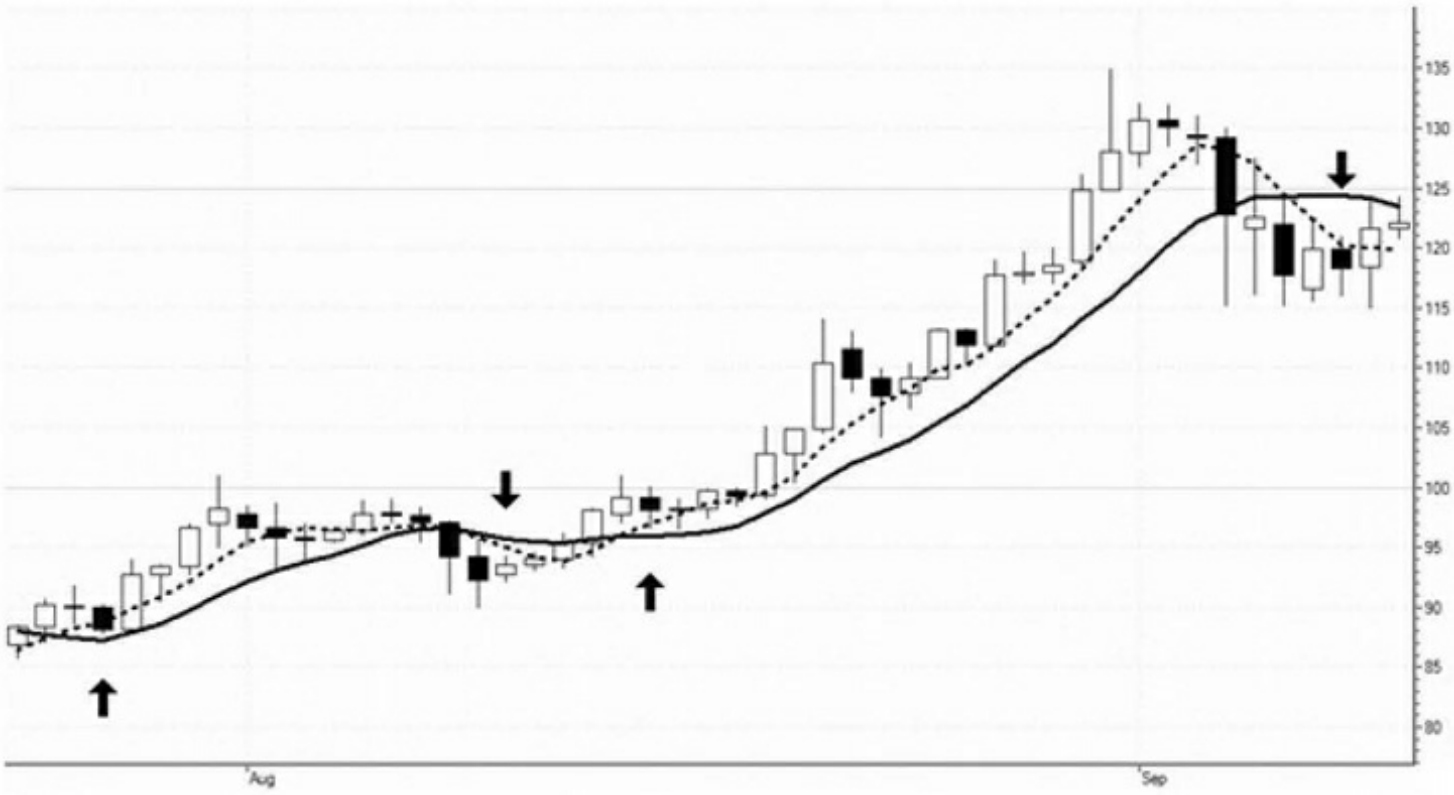


FIGURA 8.1 – Trading system con le medie mobili: SMA a 5 giorni (linea tratteggiata) e SMA a 10 giorni (linea continua).

Durante i primi giorni dell'agosto 2013, a seguito del taglio dal basso verso l'alto della media mobile semplice a 5 giorni, il trading system ha lanciato un segnale di acquisto (posizione long). La posizione viene mantenuta con profitto

per circa due settimane, quando un nuovo taglio, questa volta dall'alto verso il basso, fa chiudere in profitto la posizione long e contemporaneamente viene lanciato dal trading system un segnale di vendita (posizione short).

Questa nuova posizione viene chiusa in leggera perdita dopo poche sedute, quando il nuovo segnale rialzista apre un long e la posizione viene tenuta per quasi un mese portando un profitto notevole.

Performance report medie mobili

Nella Tabella 8.1 presentiamo le statistiche del trading system con le medie mobili per vedere come si è comportato nell'intervallo temporale preso in considerazione. Il capitale iniziale investito è pari a $ 10.000.

TABELLA 8.1 – Risultati del Trading system basato sulle medie mobili.

Statistiche	All Trades	Long Trades	Short Trades
Gross Profit	$ 437.540	$ 361.027	$ 76.513
Gross Loss	$ -221.233	$ -155.930	$ -65.302
Total Net Profit	$ 216.307	$ 205.097	$ 11.211
Profit Factor	1,978	2,315	1,172
Number of Winning Trades	20	12	8
Number of Losing Trades	40	18	22
Total Number of Trades	60	30	30
Percent Profitable	33%	40%	27%
Average Winning Trade	$ 21.877	$ 30.086	$ 9.564
Average Losing Trade	$ -5.531	$ 8.663	$ -2.968
Ratio AvgWin/AvgLos	3,955	3,473	3,222
Average Bars in Winning Trades	26,15	30,83	19,13
Average Bars in Losing Bars	6,60	6,33	6,82
Max Drawdown	$ -66.332	$ -74.043	$ 42.323
Return on Account	326,10 %	277 %	26,49 %
Percent of Time in the Market	95,19 %		

Questo trading system ha generato 60 segnali, divisi equamente tra long e short, di cui 20 sono stati chiusi a profitto e 40 in perdita. Ne deriva che la percentuale di profittabilità è estremamente bassa e pari al 33%.

Tuttavia, il Total Net Profit è di ben $ 216.307, perché l'utile medio ($

21.877) supera ampiamente la perdita media ($ -5.531). Il massimo Drawdown è risultato pari a $ -66.332.

L'andamento dell'Equity Line monetaria, nella Figura 8.2, ci evidenzia come la performance maggiore sia derivata dalle operazioni effettuate a fine 2013.

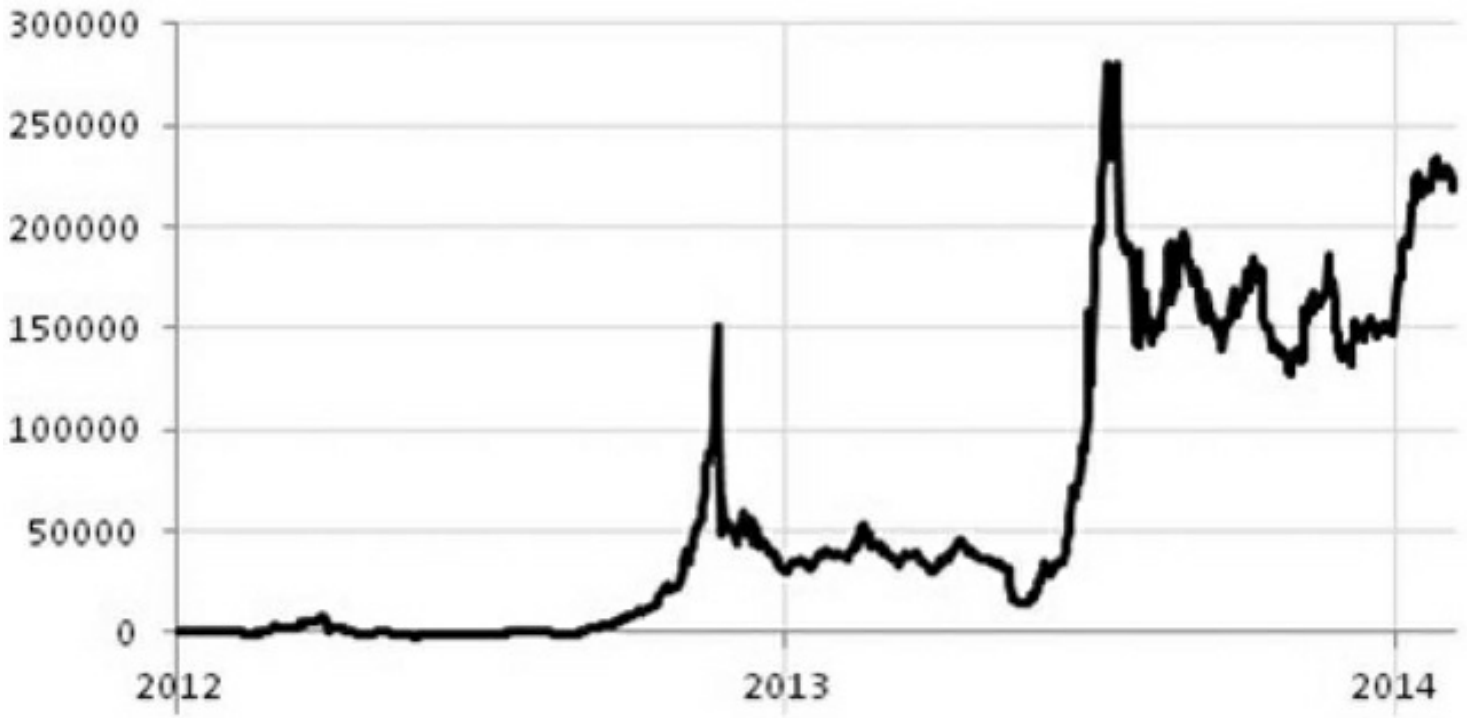


FIGURA 8.2 – Equity Line del trading system con le medie mobili.

TRADING SYSTEM CON LE BANDE DI BOLLINGER

Costruiamo ora un trading system che utilizza le Bande di Bollinger. I parametri selezionati sono i seguenti:

- periodo di osservazione = 20 giorni;
- costante $K = 2$.

Il trading system segue le seguenti regole:

- ingresso long (con chiusura di eventuali posizioni corte) quando il prezzo rompe la Banda superiore di Bollinger;
- ingresso short (con chiusura di eventuali posizioni lunghe) quando il prezzo rompe la Banda inferiore di Bollinger.

Questo trading system, per costruzione, resta sempre a mercato. Vediamo sulla Figura 8.3 come e quando viene generato un segnale di ingresso.

FIGURA 8.3 – Trading system con le Bande di Bollinger.

Il 3 marzo 2014 il prezzo ha rotto con decisione la Banda superiore di Bollinger e il trading system genera un segnale di acquisto alla rottura della Banda al prezzo di $ 685. Non si dimostra essere un'operazione vincente, infatti pochi giorni dopo (il 21 marzo 2013) la posizione viene chiusa alla

rottura della Banda inferiore, al prezzo di $ 569. Tuttavia, sulla base delle regole che abbiamo fissato, non viene semplicemente chiusa la posizione long ma viene aperta immediatamente anche una posizione short. In altri termini abbiamo fatto un *stop and reverse*. Questa posizione si è dimostrata profittevole e viene chiusa a $ 523 il 16 aprile, data in cui si entra di nuovo long.

Performance report Bande di Bollinger

Presentiamo ora le statistiche del trading system con le Bande di Bollinger per

vedere come si è comportato tale sistema lungo l'intervallo temporale da noi preso in considerazione. Il capitale iniziale investito è pari a $ 10.000.

TABELLA 8.2 – Risultati del Trading system basato sulle Bande di Bollinger.

Statistiche	All Trades	Long Trades	Short Trades
Gross Profit	$ 576.558	$ 570.884	$ 5.675
Gross Loss	$ -34.550	$ -3.140	$ -31.410
Total Net Profit	$ 542.009	$ 567.744	$ -25.735
Profit Factor	16,688	181,813	0,181
Number of Winning Trades	11	6	5
Number of Losing Trades	9	4	5
Total Number of Trades	20	10	10
Percent Profitable	55 %	60 %	50 %
Average Winning Trade	$ 52.414	$ 95.147	$ 1.135
Average Losing Trade	$ -3.839	$ -785	$ -6.282
Ratio AvgWin/AvgLos	13,65	121,21	0,18
Average Bars in Winning Trades	65,82	75,00	54,80
Average Bars in Losing Bars	19,78	21,75	18,20
Max Drawdown	$ -19.606	$ -2.835	$ -28.667
Return on Account	2764 %	2026 %	-89 %
Percent of Time in the Market	97,7 %		

Questo trading system ha generato 20 segnali, divisi quasi equamente tra long e short, di cui 11 sono stati chiusi a profitto e 9 in perdita. Ne deriva che la percentuale di profittabilità è pari al 55%.

Il Total Net Profit è di ben $ 576.558, con un utile medio ($ 52.414)

che supera ampiamente la perdita media ($ -3.839).

Il massimo Drawdown è risultato pari a $ -19.606.

Presentiamo nella Figura 8.4 l'andamento dell'Equity Line monetaria.

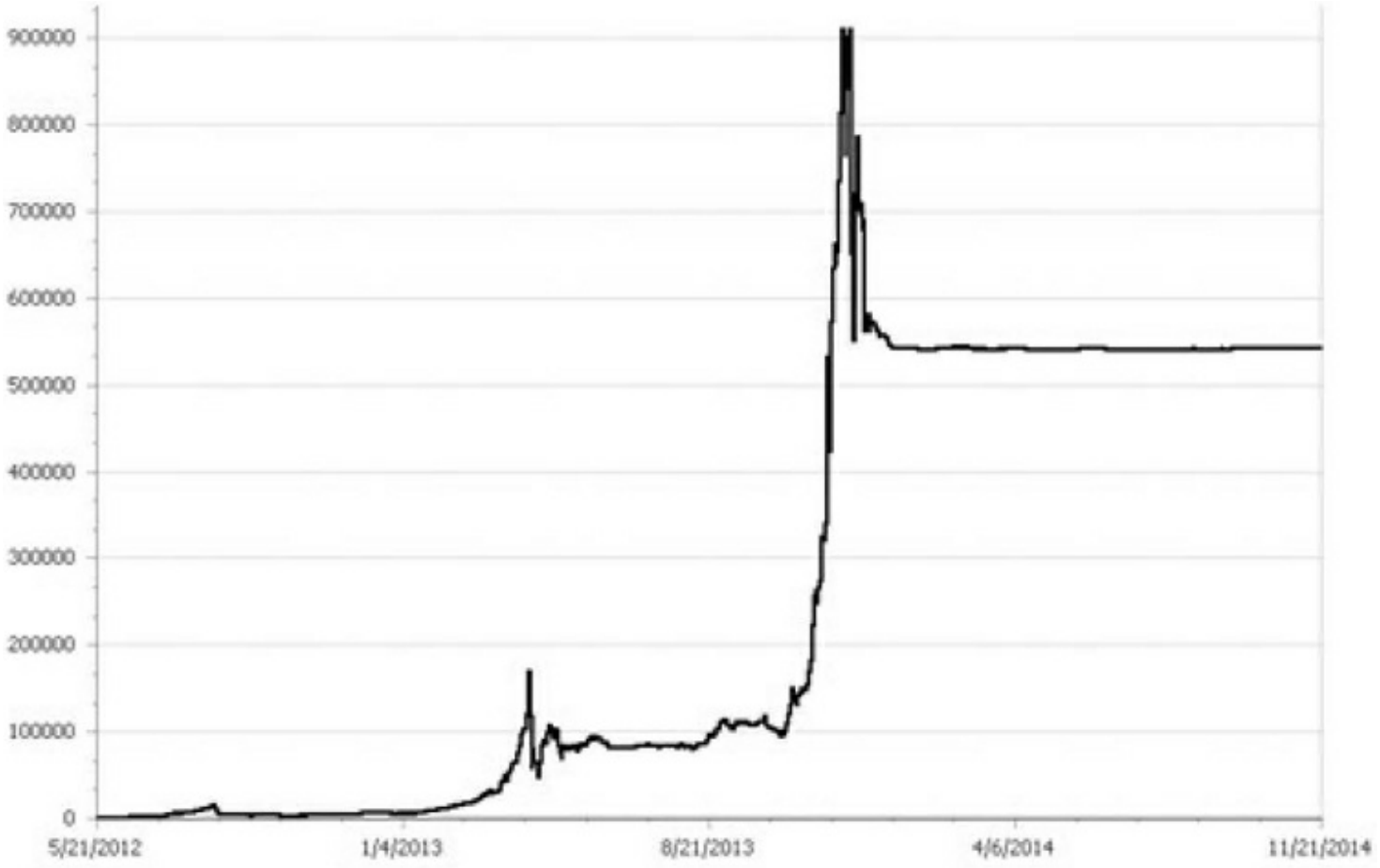


FIGURA 8.4 – Equity Line del trading system con le Bande di Bolliger.

TRADING SYSTEM CON IL WILLIAMS %R

Passiamo ora alla costruzione di un trading system che utilizza il Williams %R. I parametri selezionati sono i seguenti.

- periodo di osservazione = 14 giorni;
- livello di ipercomprato = -20%;
- livello di ipervenduto = -80%.

Il trading system presenta queste regole:

- ingresso long (con chiusura di eventuali posizioni corte) quando il Williams %R rompe dal basso verso l'alto il livello di ipercomprato;

- ingresso short (con chiusura di eventuali posizioni lunghe) il Williams %R rompe dall'alto verso il basso il livello di ipervenduto.

Abbiamo settato questo trading system in maniera esattamente opposta a quanto proposto inizialmente dal suo ideatore poiché, sul mercato Bitcoin, i trend tendono a perdurare nel tempo in modo più significativo rispetto a ogni altro mercato. Lasciamo al lettore l'onere di verificare come si sarebbe comportato secondo le regole standard stabilite da Larry Williams. Questo trading system resta, per costruzione, sempre a mercato. Vediamo sulla Figura 8.5 come e quando

viene generato un segnale di ingresso.

FIGURA 8.5 – Trading system con il Williams %R.

Il 28 aprile il Williams %R è sceso sotto il livello -80%, generando un segnale di vendita a $ 430. Tale operazione è stata chiusa in perdita il 21 maggio, a $ 489 e, contestualmente, viene aperta una posizione long allo stesso livello di prezzo. Tale posizione

viene mantenuta fino al 13 giugno, quando in seguito alla rottura del livello -80% il trading system genera il segnale di uscita con un significativo profitto.

Come ormai siamo in grado di comprendere il trading system non si limita a chiudere la posizione long ma, restando sempre a mercato, apre immediatamente una posizione short allo stesso livello di prezzo che viene chiusa il 1° luglio a $ 642. La posizione long successiva che si genera viene infine chiusa il 26 luglio 2014 a $ 600, data in cui si entra short, e alla data finale (scelta per il test del nostro trading system) siamo ancora in posizione short con il bitcoin che ha raggiunto i $ 350.

Performance report Williams %/R

Presentiamo ora le statistiche del trading system con il Williams %R per vedere come si è comportato tale sistema lungo l'intervallo temporale da noi preso in considerazione. Il capitale iniziale investito è pari a $ 10.000 (Tabella 8.3).

TABELLA 8.3 – Risultati del trading system basato sul Williams %R.

Statistiche	All Trades	Long Trades	Short Trades
Gross Profit	$ 760.827	$ 714.456	$ 46.371
Gross Loss	$-51.440	$ -26.397	$ -25.042
Total Net Profit	$ 709.387	$ 688.059	$ 21.329
Profit Factor	14,791	27,066	1,852
Number of Winning Trades	12	6	6
Number of Losing Trades	11	6	5
Total Number of Trades	23	12	11
Percent Profitable	52%	50%	54%
Average Winning Trade	$ 63.402	$ 119.076	$ 7.728
Average Losing Trade	$ -4.676	$ -4.400	$ -5.008
Ratio AvgWin/AvgLos	13,558	27,066	1,543
Average Bars in Winning Trades	58,33	74,33	42,33
Average Bars in Losing Bars	19,91	15,83	24,80
Max Drawdown	$ -23.602	$ -18.069	$ -16.286
Return on Account	3006%	3808%	131%
Percent of Time in the Market	98,25 %		

Questo trading system ha generato 23 segnali, divisi equamente tra long e short, di cui 12 sono stati chiusi a profitto e 11 in perdita. Ne deriva che la percentuale di profittabilità è pari al 52%.

Il Total Net Profit è di ben $ 760.827, con un utile medio ($ 63.402)

che supera ampiamente la perdita media ($ -4.676).

Il massimo Drawdown è risultato pari a $ -23.602.

Nella Figura 8.6, infine, presentiamo anche per questo trading system l'andamento dell'Equity Line.

TRADING SYSTEM CON IL PARABOLIC SAR

Concludiamo la nostra trattazione sui trading system costruiti con gli indicatori di Analisi tecnica presentando quello sul Parabolic SAR. Il parametro

selezionato è il seguente:

- AF = 0,02.

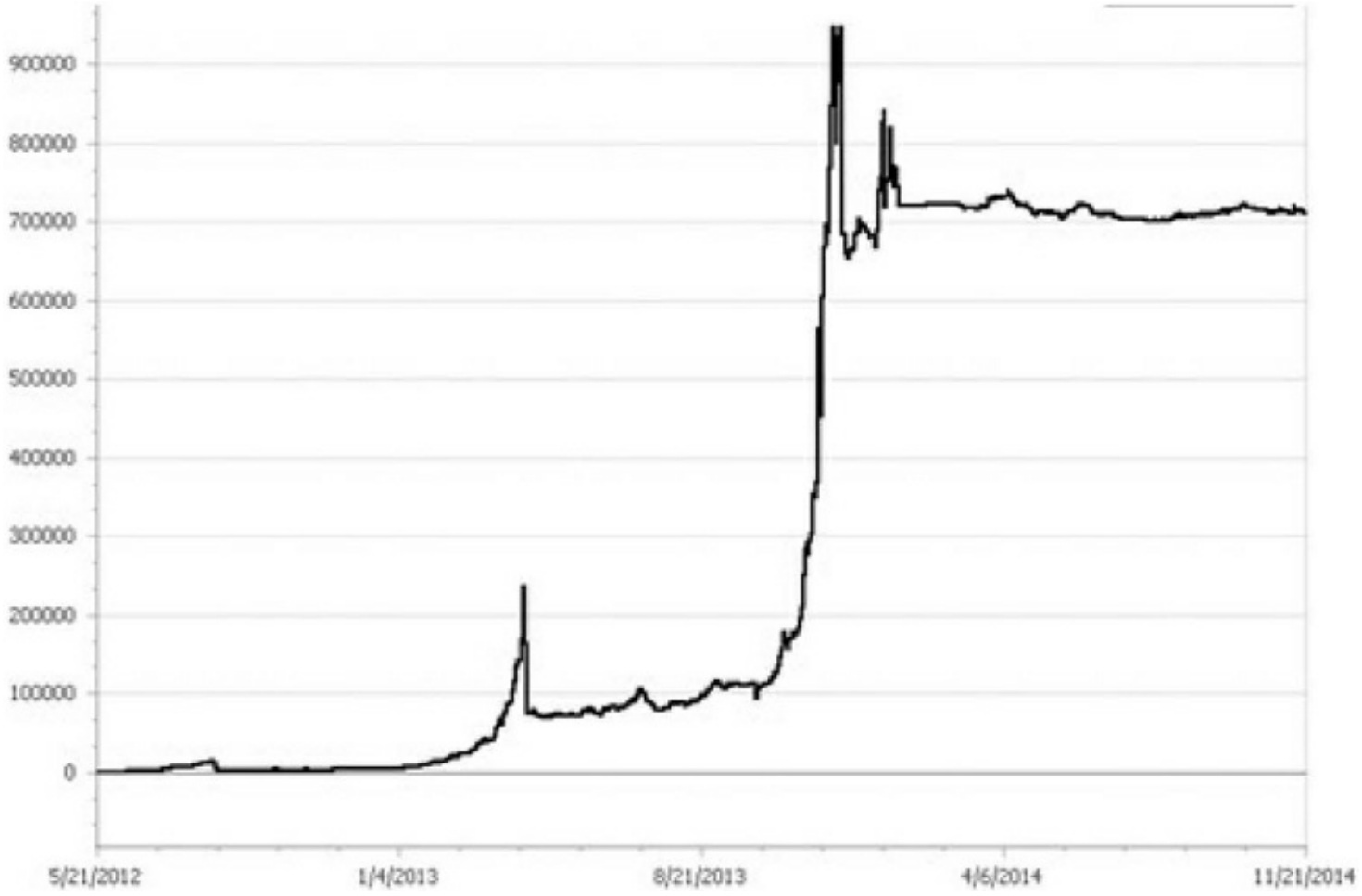


FIGURA 8.6 – Equity Line del trading system con il Williams %R.

Il trading system segue le seguenti regole:

- ingresso long (ribaltando eventuali posizioni corte) quando

il livello di prezzo rompe al rialzo l'indicatore SAR;

- ingresso short (ribaltando eventuali posizioni lunghe) quando il livello di prezzo rompe al rialzo l'indicatore SAR.

Anche questo trading system, per costruzione, resta sempre a mercato. Vediamo nella Figura 8.7 come e quando viene generato un segnale di ingresso.

Durante i primi giorni di ottobre 2014 il prezzo del bitcoin interrompe il trend ribassista che ha caratterizzato il mese di settembre e il trading system genera un segnale di acquisto. La posizione viene mantenuta per un paio di

settimane e chiusa in profitto. Nello stesso istante la rottura al ribasso del SAR genera un segnale di vendita, e anche questo trend viene catturato con successo fino a quando l'ulteriore rottura del SAR al rialzo ci fa ribaltare nuovamente la posizione.

FIGURA 8.7 – Trading system con Parabolic SAR.

Performance report Parabolic SAR

Presentiamo le statistiche del trading system con il SAR per vedere come si è comportato tale sistema lungo l'intervallo temporale preso in considerazione. Il capitale iniziale investito è pari a $ 10.000 (Tabella 8.4).

TABELLA 8.4 – Risultati del trading system basato sul Parabolic SAR.

Statistiche	All Trades	Long Trades	Short Trades
Gross Profit	$ 190.685	$ 115.161	$ 75.524
Gross Loss	$ -94.805	$ -48.528	$ -46.277
Total Net Profit	4 95.880	$ 66.633	$ 29.247
Profit Factor	2,011	2,373	1,632
Number of Winning Trades	31	18	13
Number of Losing Trades	23	9	14
Total Number of Trades	54	27	27
Percent Profitable	57,41 %	66,67 %	48,15 %
Average Winning Trade	$ 6.151	$ 6.398	$ 5.810
Average Losing Trade	$ -4.122	$ -5.392	$ -3.306
Ratio AvgWin/AvgLos	1,492	1,187	1,758
Average Bars in Winning Trades	23,03	23,17	22,85
Average Bars in Losing Bars	10,61	12,33	9,50
Max Drawdown	$ -46.200	$ -32.167	$ -29.892
Return on Account	207,53%	207,15%	97,84%
Percent of Time in the Market	99,34%		

Questo trading system ha generato 54 segnali, divisi equamente tra long e short, di cui 31 sono stati chiusi a profitto e 23 in perdita. Ne deriva che la percentuale di profittabilità è superiore al 50%.

Il Total Net Profit è di $ 190.685, e l'utile medio ($ 6.151) supera

ovviamente la perdita media ($ -4.122).

Quindi, sebbene il profitto totale sia minore rispetto a quello generato dal trading system con le medie mobili, nel complesso il SAR si è dimostrato più equilibrato.

Il massimo Drawdown è risultato pari a $ -46.200. L'andamento dell'Equity Line monetaria ci evidenzia come la performance maggiore sia derivata dalle operazioni a cavallo tra il 2013 e il 2014 (Figura 8.8).

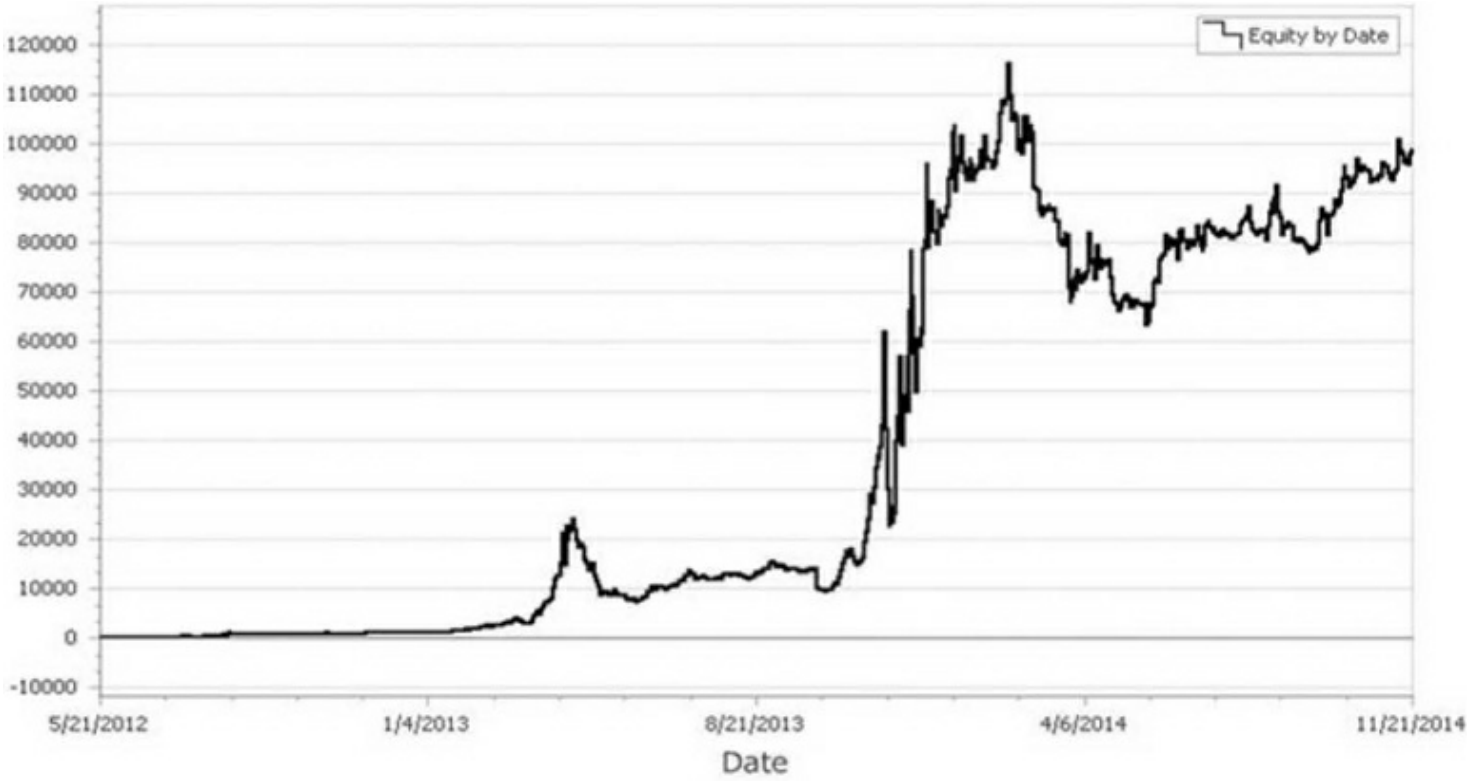


FIGURA 8.8 – Equity Line del trading system con il SAR.

TRADING SYSTEM STATISTICO

Per presentare il nostro trading system statistico riprendiamo la Figura 6.17,

che mostrava la correlazione tra prezzo-Difficoltà a 90 giorni.

Forti delle competenze acquisite nel capitolo precedente sull'Analisi tecnica, siamo perfettamente in grado di notare come l'andamento della correlazione prezzo-Difficoltà si caratterizzi per *spike* (o formazioni a "V") ben definiti. Come abbiamo visto, gli *spike* sono figure di inversione di tendenza e in particolare prendono il nome di Top V Reversal quando invertono il trend da positivo a negativo e di Bottom V Reversal nel caso opposto.

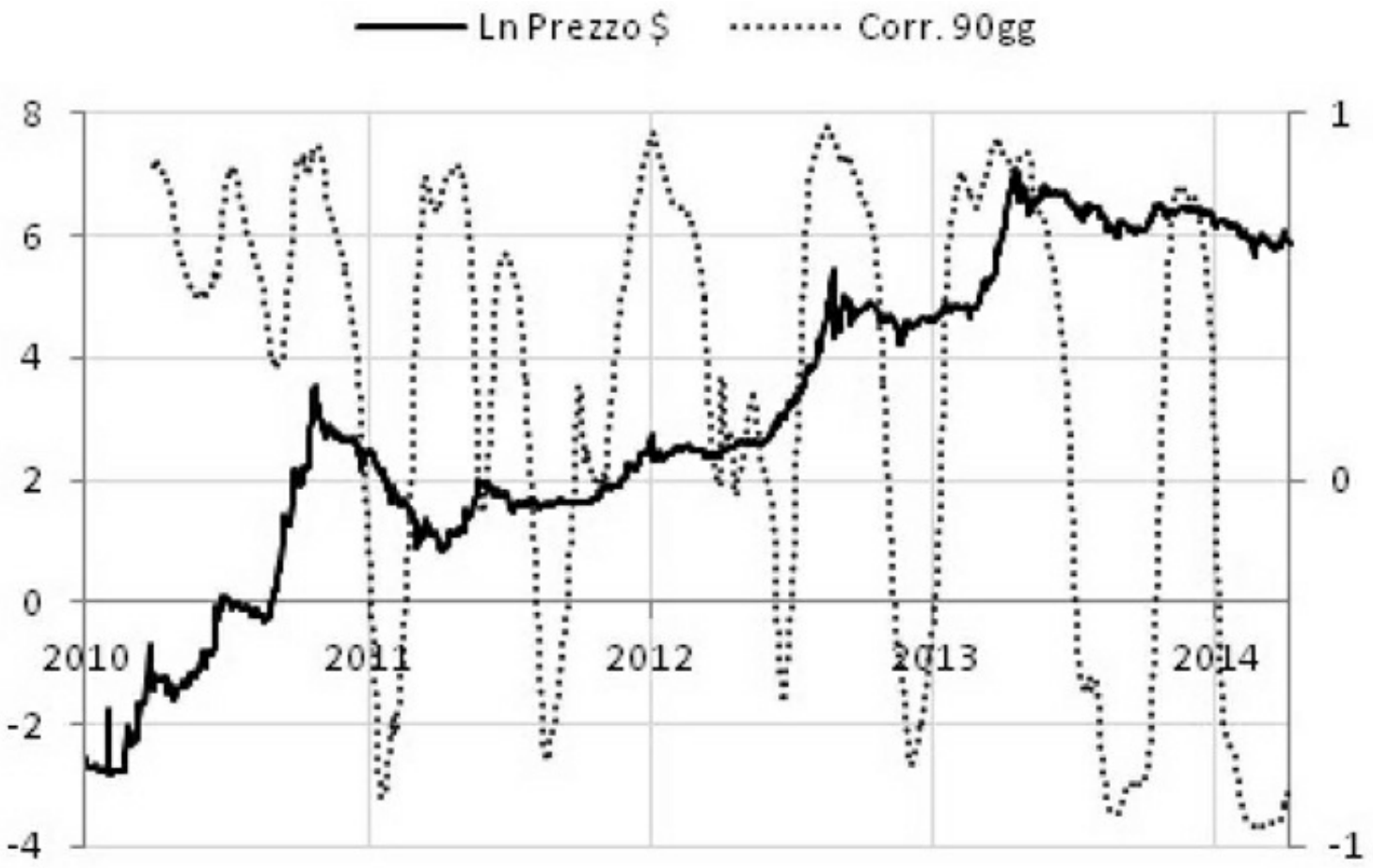


FIGURA 8.9 – Correlazione tra prezzo-Difficoltà a 90 giorni e prezzo in scala logaritmica.

Cerchiamo ora di impostare un sistema di trading che ci permetta di sfruttare i segnali proposti da queste configurazioni grafiche. Queste sono le regole:

- il grafico della correlazione ha una lettura simile a quella di un comune oscillatore di analisi tecnica, come per esempio l'RSI (Relative Strength Index);
- l'ingresso long si genera quando la correlazione ritorna in trend positivo (> -0,5) dopo che è stata in area di ipervenduto, che fissiamo inferiore a -0,5;
- il punto di uscita si genera quando la correlazione ritorna in trend negativo (< 0,5) dopo che è stata in area di ipercomprato, che fissiamo superiore a 0,5.

In base a queste ipotesi il sistema lavora solo nella direzione rialzista,

concentrando i segnali esclusivamente sul valore dell'indicatore di correlazione. In Tabella 8.5 potete vedere i risultati.

Sono stati effettuati solo 5 trade, con un tempo totale di esposizione a mercato pari a 633 giorni, cioè il 43% dei 1469 giorni disponibili per l'operatività.

Per valutare correttamente il profitto generato ipotizziamo di investire in ogni trade un valore di $ 10.000. Nella Tabella 8.6 vedete i risultati.

TABELLA 8.5 – Risultati del trading system basato sulla correlazione prezzo-Difficoltà a 90 giorni.

Trade		Buy		Sell	P&L	P&L %	Time
1	30/09/11	$ 5,35	31/12/11	$ 5	$ -0,36	-7%	92
2	23/04/12	$ 5,22	24/10/12	$ 11,82	$ 6,6	127%	184
3	09/02/12	$ 23,7	09/06/12	$ 98,47	$ 74,77	315%	121
4	13/08/13	$ 107,3	25/01/14	$ 806	$ 698,7	651%	165
5	30/05/14	$ 609,03	09/08/14	$ 588,61	$ -20,42	-3%	71

TABELLA 8.6 – Risultati del trading system basato sulla correlazione prezzo-Difficoltà a 90 giorni.

Trade	USD	BTC	USD finale	P&L
1	$ -10.000	1869,16	$ 9336	$ -664
2	$ -10.000	1916,45	$ 22.652	$ 12.652
3	$ -10.000	421,94	$ 42.549	$ 31.549
4	$ -10.000	93,2	$ 75.117	$ 65.117
5	$ -10.000	16,42	$ 9.665	$ -335
			Totale	$ 108.320
			Totale %	1.083%

Questo trading system ha generato $ 108.320, con un ritorno del 1.083% sull'investimento.

Ai lettori più attenti non dovrebbe essere sfuggito il fatto che una strategia "*buy and hold*" avrebbe generato

maggiori profitti (Tabella 8.7).

TABELLA 8.7 – Risultati della strategia "buy and hold".

	Buy		Sell	P&L	P&L %	Time
30/09/2011	$ 5,35	21/11/2014	$ 356,9	$ 351,55	6.571%	1148

Investendo $ 10.000 si sarebbe generato un profitto di $ 657.100.

Il fortissimo incremento rialzista di lungo periodo favorisce in modo evidente questo tipo di strategia, la quale però ha il difetto che, dopo aver aperto la posizione, il tempo a mercato è pari al 100%. In altri termini, si è sempre a mercato e in balia della volatilità dei prezzi, avendo tutto il capitale investito bloccato. Questa è una variabile che deve essere assolutamente

considerata nel momento in cui si sviluppa una strategia di trading.

Quello che abbiamo esposto è ovviamente un semplice *trading system*, che può essere migliorato e ottimizzato, così come è necessario applicare delle regole di money management.

Guardate banalmente cosa succede se consideriamo di reinvestire sempre gli utili generati, partendo sempre con l'investimento di $ 10.000 (Tabella 8.8).

TABELLA 8.8 – Risultati del trading system basato sulla correlazione prezzo-Difficoltà a 90 giorni con ipotesi di reinvestimento.

Trade	USD	BTC	USD finale	P&L
1	$ -10.000	1869,16	$ 9336	$ -664
2	$ -9.336	1789,28	$ 21.149	$ 11.813
3	$ -21.149	892,38	$ 87.873	$ 66.723
4	$ -87.873	818,95	$ 660.076	$ 572.203
5	$ -660.000	1083,82	$ 637.945	$ -22.132
			Totale	$ 627.945
			Totale %	6.279%

L'utile generato è salito a $ 627.945, con una performance del 6279% sul capitale iniziale. L'Equity Line è mostrata nel grafico della Figura 8.10.

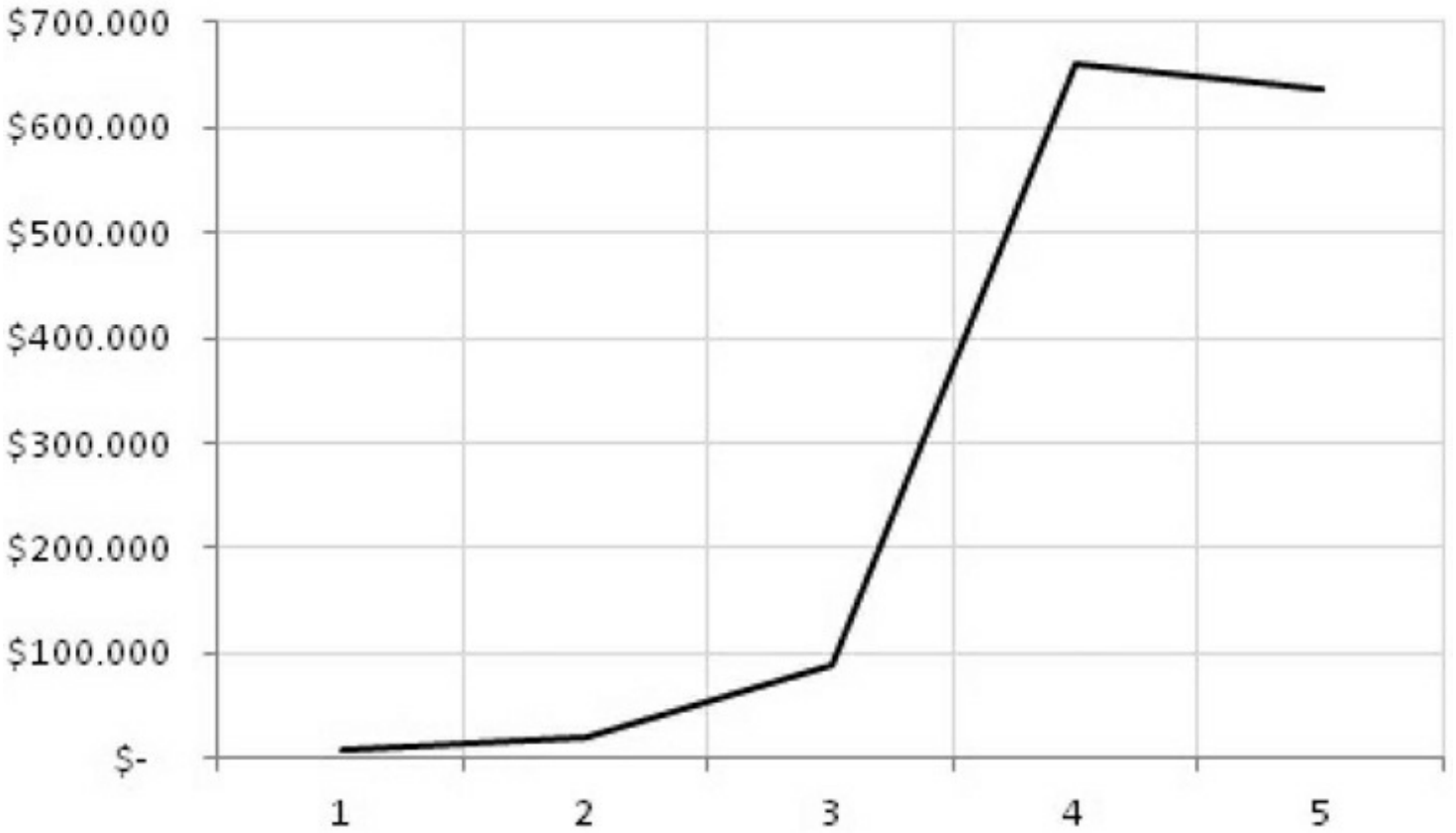


FIGURA 8.10 – Equity Line del trading system con ipotesi di reinvestimento.

Da un punto di vista statistico, questo trading system offre però poche garanzie di affidabilità poiché ha generato solo 5 segnali operativi.

Per incrementare l'operatività si può passare a utilizzare una correlazione a 30 giorni (Figura 8.11).

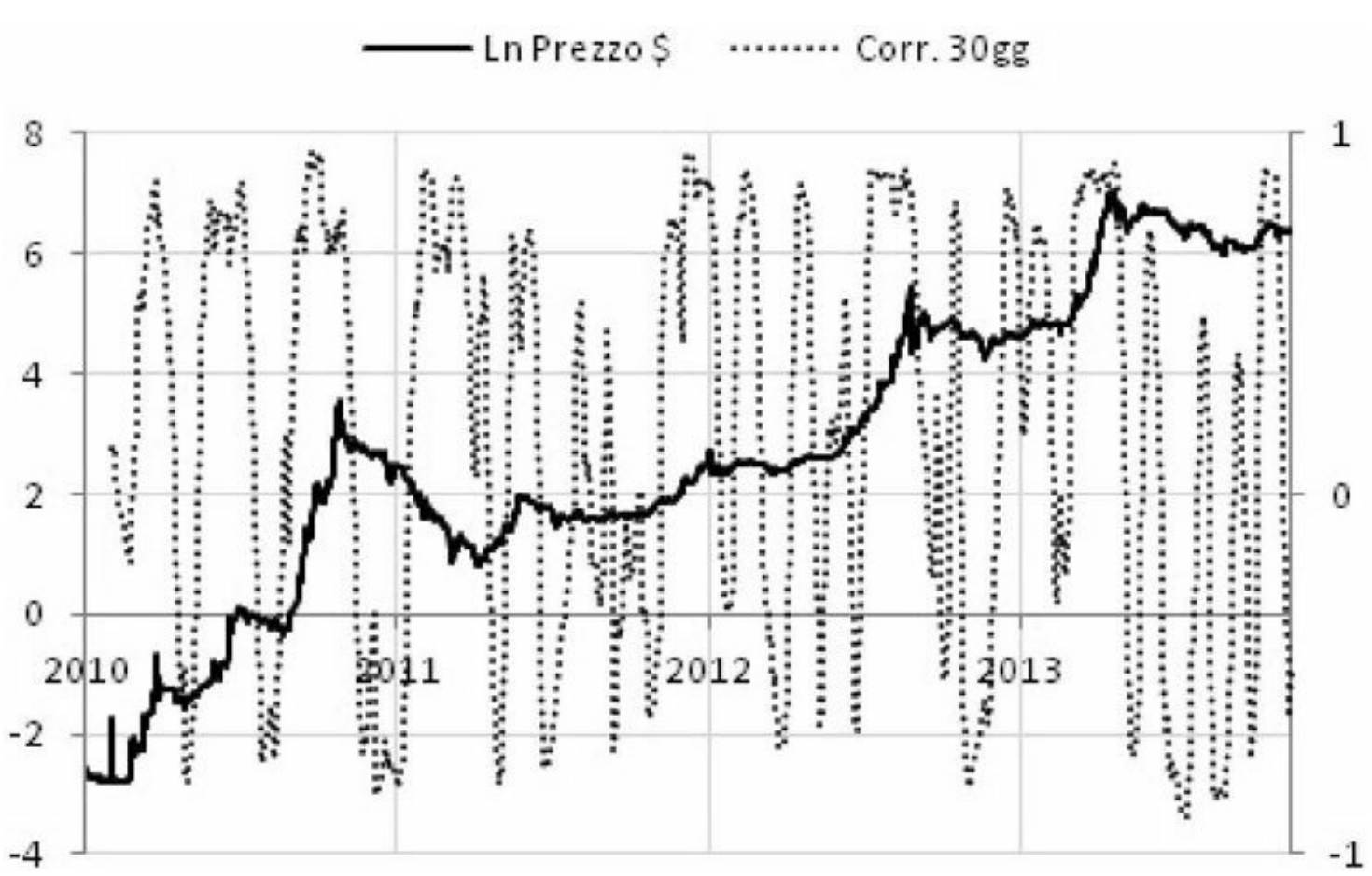


FIGURA 8.11 – Correlazione tra prezzo-Difficoltà a 30 giorni e prezzo in scala logaritmica.

In questo caso il grafico della correlazione ha maggiori oscillazioni rispetto a quello precedente e per questo motivo è sensato ridurre il range dei punti di ingresso e uscita.

Queste sono le regole del trading system:

- l'ingresso long si genera quando la correlazione ritorna in trend positivo (>-0,25) dopo che è stata in area di ipervenduto, che fissiamo inferiore a -0,25;
- il punto di uscita si genera quando la correlazione ritorna in trend negativo (<0,25) dopo che è stata in area di ipercomprato, che fissiamo superiore a 0,25.

L a Tabella 8.9 riporta i risultati di questa strategia.

Il tempo a mercato è stato pari a 810

giorni, cioè il 53% dei 1529 giorni oggetto dell'analisi, con un profitto totale generato pari a $ 323.476, ipotizzando di investire sempre $ 10.000 in ogni trade (Tabella 8.10).

Tale profitto aumenta in modo esponenziale in caso di reinvestimento dell'utile generato (Tabella 8.11).

Dall'investimento iniziale di soli $ 10.000 si sarebbe generato un profitto di quasi 25 milioni di dollari con una performance del 249.099%.

TABELLA 8.9 – Risultati del trading system basato sulla correlazione prezzo-Difficoltà a 30 giorni.

Trade		Buy		Sell	P&L	Time
1	26/12/2010	0,27	28/02/2011	0,95	251,6%	64
2	03/04/2011	0,80	24/06/2011	16,75	1994,3%	82
3	29/08/2011	9,48	13/11/2011	3,10	-67,3%	76
4	22/12/2011	3,99	29/01/2012	5,76	44,3%	38
5	03/03/2012	4,78	23/03/2012	4,83	1,0%	20
6	13/04/2012	4,94	22/04/2012	5,33	7,8%	9
7	09/05/2012	5,10	28/08/2012	11,38	123,3%	111
8	14/09/2012	11,75	15/10/2012	12,03	2,4%	31
9	19/11/2012	11,80	16/12/2012	13,67	15,8%	27
10	30/12/2012	13,57	27/01/2013	18,00	32,6%	28
11	11/02/2013	24,20	22/04/2013	123,52	410,5%	70
12	25/05/2013	132,69	07/06/2013	110,30	-16,9%	13
13	16/07/2013	97,01	19/08/2013	102,07	5,2%	34
14	29/09/2013	128,10	16/12/2013	709,00	453,5%	78
15	05/01/2014	896,00	27/01/2014	777,00	-13,3%	22
16	10/03/2014	621,99	24/03/2014	572,00	-8,0%	14
17	24/04/2014	491,60	03/05/2014	434,50	-11,6%	9
18	21/05/2014	494,87	21/06/2014	590,99	19,4%	31
19	02/07/2014	654,00	27/07/2014	592,51	-9,4%	25
20	24/10/2014	358,46	21/11/2014	356,90	-0,4%	28

TABELLA 8.10 – Risultati del trading system basato sulla correlazione prezzo-Difficoltà a 30 giorni.

Trade	USD	BTC	USD finale	P&L
1	$ -10.000	37.037,17	$ 35.157	$ 25.157
2	$ -10.000	12.503,13	$ 209.429	$ 199.429
3	$ -10.000	1054,73	$ 3269	$ -6731
4	$ -10.000	2505,02	$ 14.429	$ 4429
5	$ -10.000	2092,07	$ 10.105	$ 105
6	$ -10.000	2022,39	$ 10.777	$ 777
7	$ -10.000	1962,29	$ 22.332	$ 12.332
8	$ -10.000	851,06	$ 10.238	$ 238

9	$ -10.000	847,46	$ 11.581	$ 1581
10	$ -10.000	736,92	$ 13.265	$ 3265
11	$ -10.000	413,30	$ 51.049	$ 41.049
12	$ -10.000	75,36	$ 8312	$ -1688
13	$ -10.000	103,08	$ 10.522	$ 522
14	$ -10.000	78,06	$ 55.347	$ 45.347
15	$ -10.000	11,16	$ 8672	$ -1328
16	$ -10.000	16,08	$ 9196	$ -804
17	$ -10.000	20,34	$ 8838	$ -1162
18	$ -10.000	20,21	$ 11.942	$ 1942
19	$ -10.000	15,29	$ 9060	$ -940
20	$ -10.000	27,90	$ 9956	$ -44
			Tot	$ 323.476
			Tot %	3235%

TABELLA 8.11 – Risultati del trading system con reinvestimento.

Trade	USD	BTC	USD finale	P&L
1	$ -10.000	37.037,17	$ 35.157	$ 25.157
2	$ -35.157	43.957,03	$ 736.285	$ 701.128
3	$ -736.285	77.658,15	$ 240.663	$ -495.622
4	$ -240.663	60.286,37	$ 347.250	$ 106.587
5	$ -347.250	72.647,10	$ 350.886	$ 3636
6	$ -350.886	70.962,80	$ 378.139	$ 27.254
7	$ -378.139	74.201,88	$ 844.469	$ 466.330
8	$ -844.469	71.869,73	$ 864.593	$ 20.124
9	$ -864.593	73.270,71	$ 1.001.279	$ 136.687
10	$ -1.001.279	73.786,36	$ 1.328.154	$ 326.874
11	$ -1.328.154	54.892,59	$ 6.780.059	$ 5.451.905
12	$ -6.780.059	51.096,98	$ 5.635.742	$ -1.144.316
13	$ -5.635.742	58.094,45	$ 5.929.700	$ 293.958
14	$ -5.929.700	46.289,62	$ 32.819.339	$ 26.889.639
15	$ -32.819.339	36.628,73	$ 28.460.521	$ -4.358.818
16	$ -28.460.521	45.757,20	$ 26.173.118	$ -2.287.402
17	$ -26.173.118	53.240,68	$ 23.133.075	$ -3.040.043
18	$ -23.133.075	46.745,76	$ 27.626.278	$ 4.493.203
19	$ -27.626.278	42.242,02	$ 25.028.816	$ -2.597.462
20	$ -25.028.816	69.823,18	$ 24.919.892	$ -108.924
			Tot	$ 24.909.892
			Tot %	249.099%

Se riportiamo su grafico i risultati di questa strategia otteniamo l'Equity Line della Figura 8.12.

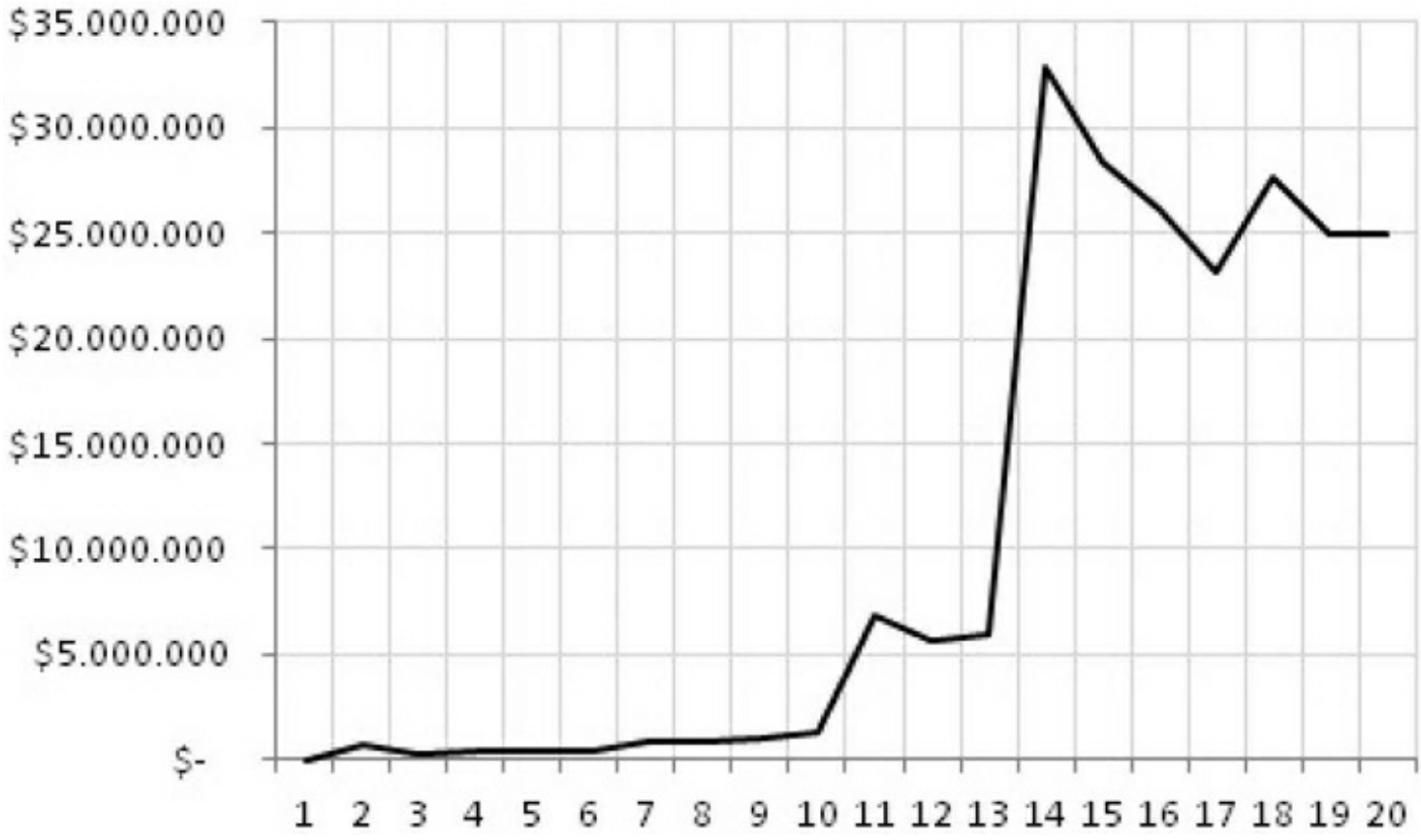


FIGURA 8.12 – Equity Line del trading system con ipotesi di reinvestimento.

Il grafico logaritmico dell'Equity Line ci mostra in modo più chiaro come la crescita sia stata abbastanza lineare con i maggiori incrementi percentuali registrati con i deal numero 2, 11 e 14 (Figura 8.13).

Termina qui la nostra trattazione di questo potente trading system statistico basato sulla nostra osservazione della forte correlazione tra prezzo e Difficoltà. Data la struttura generale del sistema Bitcoin riteniamo, con sufficiente certezza, che tale possa rimanere valido anche nel prossimo futuro.

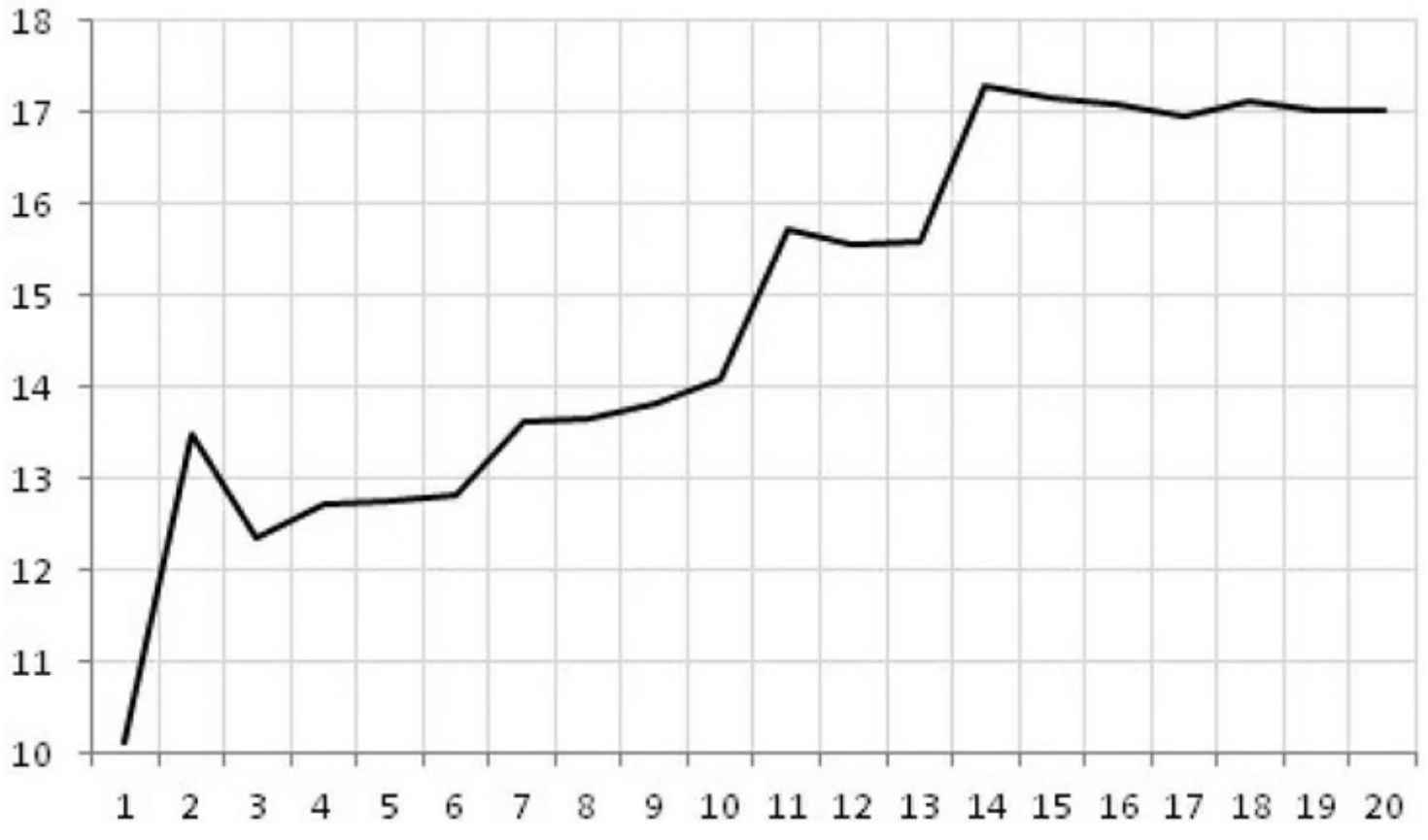


FIGURA 8.13 – Equity Line su scala logaritmica del trading system con ipotesi di reinvestimento.

---

29. Per i lettori esperti di money management stiamo applicando la strategia *Position sizing - Fixed Percent* con percentuale pari al 100%.
30. Per costo di *slippage* si intende il costo nascosto dovuto alla differenza che si registra tra il prezzo di mercato e il prezzo effettivo di esecuzione.
31. Costruita con i prezzi negoziati sull'exchange Bitstamp.

APPENDICE

Uno sguardo al futuro

Tutti sanno che una cosa è impossibile da realizzare,
finché arriva uno sprovveduto che non lo sa e la inventa.

Albert Einstein

Come evidente, il tema fin qui trattato è assai attraente, quanto complesso e innovativo, anzi rivoluzionario. Sulla scena mondiale, il debutto relativamente recente del

Bitcoin prova a rubare il ruolo da protagonista alle varie valute ufficiali, insidiando a livello internazionale i già precari equilibri economici. Difatti, la nuova moneta digitale, tra gli alti e bassi di quotazioni al cardiopalma, fa registrare una continua e vertiginosa crescita in termini di scambio in Rete. Segno che la fiducia cresce e si vede dai numeri. Ma fare previsioni a lungo termine, cioè da qui al 2140 (data in cui la Rete genererà il suo ultimo bitcoin) sarebbe come dare i numeri al lotto, meglio quindi stare con i piedi per terra e valutare i dati reali.

Perché la complessità del fenomeno Bitcoin rende le cose più difficili di quanto non lo siano state negli anni

Settanta, quando un pionieristico progetto informatico per la difesa militare degli Stati Uniti d'America (progetto "Arpanet") diede il via allo sviluppo di un sistema di interconnessione globale tra reti informatiche, che a oggi costituisce il principale mezzo di comunicazione di massa del nostro pianeta (Internet). Grazie a questo sistema, l'utente usufruisce di una serie di contenuti informativi, servizi e possibilità pressoché infinite, oltreché inimmaginabili a quel tempo.

A volere azzardare un paragone, quello in oggetto è un fenomeno di una portata straordinaria quasi quanto lo

sbarco sulla Luna. Pietra miliare di ciò che oggi è quasi praticamente realtà: il turismo spaziale. Qualcuno, probabilmente, obietterà che sia le missioni spaziali sia Internet sono entrambi frutto di un progetto governativo; mentre il Bitcoin, figlio di un enigmatico signor sconosciuto, è peraltro osteggiato dagli Stati centrali e dal sistema finanziario ufficiale. I suoi detrattori ne sottolineano difatti le non poche criticità, paventando rischi e pericolosità per tutto il sistema economico mondiale. A loro dire, un fenomeno, quindi, per certi versi anarchico, destinato a morire a breve. Ma se così non fosse? Se in futuro fossimo costretti a considerare il Bitcoin

uno spartiacque, tanto da dividere gli avvenimenti globali in un prima e dopo Bitcoin (*Ante* e *Post Bitcoin)*? Se la "reazione" non fosse che una forma estrema di autodifesa dell'ordine pre-costituito?

Perché, ripercorrendo le tappe delle startup più influenti del nostro tempo, ci si accorge come molte tra queste (Google, Amazon, YouTube, PayPal, eBay e Apple solo per citarne alcune) siano state agli esordi osteggiate duramente e per lungo tempo da tutte le più influenti lobby mondiali, tacciate di crimini vari e spregiudicate illegalità. Anche You-Tube, dicevano con supponenza i miopi cronici, avrebbe

chiuso i battenti dando il via a una valanga di risarcimenti danno per violazione di copyright. Oggi, invece, è una vetrina fantastica, rappresentando il concetto di televisione 2.0. E che dire di Jeff Bezos, fondatore di Amazon, schernito dai Big dell'editoria di tutto il mondo? A cominciare dall'illustre *New York Times*, che sosteneva sfacciatamente che, con il suo progetto, non sarebbe stato in grado di vendere la copia digitale di un libro neanche a un proprio parente. Sappiamo bene come è andata a finire.

Piccole startup hanno cambiato il nostro modo di guardare il mondo. E di viverlo. Startup nate da uomini visionari, spesso nell'angusto spazio di

un garage. Uomini dallo sguardo lungo e dal cuore indomito. Con in testa idee con le ali. Tra le mani la tastiera di un PC formato futuro, da condividere con quanti ci credono. Un'idea di un futuro, a volte, scomodo ai più, ma che comunque non è possibile arrestare. Sicuramente non a suon di divieti, come tentano di fare con i bitcoin.

Invece, chissà. Perché la stessa buona sorte di Amazon potrebbe toccare anche ai bitcoin. Saremmo così davanti a un'altra grande scommessa. Una moneta digitale globale sottratta al controllo di governi e banche centrali, quindi alle manovre monetarie, non inflazionabile, non falsificabile, dotata

di un registro trasparente e in tempo reale delle transazioni in atto.

Chi dice che il bitcoin è la moneta del "*dark web*" potrebbe dover fare i conti con la Storia. Che dire per esempio del dollaro? Forse che questa valuta ha perso credibilità per il fatto che miliardi di dollari vengono sottratti annualmente al controllo degli Stati nel momento in cui si stampa moneta falsa, magari per riciclarla in circuiti illegali? Tesi difficile da sostenere. Il dollaro, l'euro, lo yen e il rublo non hanno più credibilità internazionale, ma non perché sono stati utilizzati nel circuito illegale della criminalità organizzata, bensì perché le stesse Banche centrali hanno delegittimato le proprie valute con

operazioni folli e fuori controllo, attuando politiche monetarie al limite del suicidio economico.

Chi sostiene che il bitcoin verrà "bannato" e i suoi utilizzatori messi alla gogna, presenta la sindrome da pregiudizio, o perlomeno non è sufficientemente informato. Perché non si può "bannare" né distruggere. Per eliminarlo bisognerebbe azzerare Internet, motore del suo proliferare, cosa pressoché difficile solo da immaginare. Indietro non si torna.

A frenare ci provano quegli Stati che limitano l'accesso a Internet, cercando invano di strozzare il futuro e la ricerca della libertà nelle sue varie espressioni.

Libertà che pur vuol dire credere o non credere nel valore Bitcoin, quale nuovo mezzo di pagamento e valuta di riserva. Volendo spingerci oltre, in tutta libertà c'è perfino chi immagina il bitcoin come moneta di Stato. D'altronde ogni moneta ufficiale non si basa forse sul concetto di fiducia?

Naturalmente, il cambiamento in atto è prima di tutto culturale, poi socio-economico. Internet con i suoi Twitter e social network, ma anche con le monete digitali, è la faccia della globalizzazione post-modernità. Perché se Internet ha connesso menti e cuori del pianeta, il bitcoin (o qualsivoglia moneta digitale), simbolo dell'innovazione e della protesta contro banche e politiche

monetarie fallimentari, coerentemente lo completa e rafforza, ponendosi come strumento di scambio commerciale funzionale a un sistema aperto, flessibile, in divenire.

A sostenere la nuova moneta digitale sono, di sicuro, le menti più aperte e soprattutto i giovani. Sotto la loro spinta vanno via via adeguandosi un numero crescente di attività commerciali.

Sono ormai decine di migliaia (76.000 merchant) ad accettare i bitcoin. E sono centinaia le startup nel mondo che stanno sviluppando progetti innovativi basati sul protocollo Bitcoin: basti pensare che nel Q3 2014 sono stati investiti 285 milioni di dollari. Una

cifra notevolmente superiore a quella investita dai privati al tempo della creazione di Internet!

Alcune startup, per esempio, hanno creato exchange come Bitstamp e Kraken, altre si sono lanciate sui wallet (Blockchain e Xapo) o sui sistemi di pagamento (Coinbase, BitPay e GoCoin). Altre ancora focalizzano la loro attenzione sul mining e sui servizi di cloudmining (CEX. IO, KnCMiner, CoinTerra e il nostro www.cloudminingbiz.com), o creano veri e propri ATM point per prelevare o cambiare Bitcoin (Lamassu e Robocoin).

Certo si sa che di startup ne nascono decine di migliaia all'anno, sebbene

l'indice di sopravvivenza non sia in proporzione.

Ecco, invece, cosa fanno i colossi (ex startup) del settore. Dell è diventata la più grande compagnia al mondo ad accettare bitcoin, PayPal, il colosso dei pagamenti online, la piattaforma più utilizzata al mondo, ha ben intuito che non integrare i pagamenti in questa valuta sarebbe stato commettere lo stesso errore che ha commesso Blockbuster con i contenuti digitali. Chi? Sì, Blockbuster, la più grande catena al mondo di noleggio film degli anni Novanta, scomparsa tragicamente per non aver compreso il cambiamento epocale in atto. PayPal ha invece saputo

cavalcare il futuro, tant'è che integrerà non solo il pagamento in bitcoin, ma lo permetterà sul sito di compravendita oggetti più grande del mondo, eBay.

Qualche altro colosso? Dish Network, Expedia, Monoprix, Newegg, Overstock e TigerDirect, che generano insieme 85 miliardi di dollari di revenues annuali. Invece, Apple per il momento sta alla finestra in una posizione incerta: dapprima lo accetta poi lo nega, parrebbe disorientata. Dovrà prima o poi decidere da che parte stare. Senza trascurare l'operato di Google (Android), che ha strizzato l'occhio al bitcoin innumerevoli volte. E si vocifera che i fondatori di Google ne siano appassionati utilizzatori.

Non è tutto. Si parla già di Bitcoin 2.0. E di innovazioni legate al Blockchain, che a detta di molti è la più grande innovazione in assoluto. Più dello stesso Bitcoin. Si tratta, come abbiamo già visto nel Capitolo 2, di un registro pubblico informatico nel quale possono essere memorizzate le informazioni più svariate possibili. Come fosse un notaio informatico che lavora 24/7 instancabilmente, incessantemente e praticamente a costo zero. Possibili utilizzi? Dal registro immobiliare agli atti notarili, dalle sentenze a tutti i tipi di pagamenti e trascrizioni aventi efficacia di legge. L'unico freno all'innovazione pare

essere la fantasia stessa.

A questo punto del nostro lavoro, condotto senza pretese di esaustività, auspichiamo di essere riusciti a suscitare l'interesse di chi legge su un tema tanto discusso quanto affascinante. Nel sollecitare la lettura del presente manuale, invitiamo ad avvicinarvi alla nuove monete digitali con un atteggiamento libero da pregiudizi ma allo stesso tempo responsabile e consapevole dei rischi, limiti e opportunità di un settore ancora agli albori. D'altronde, lo sviluppo del pensiero critico è la base di ogni reale conquista. Da lì comincia l'avventura dell' "*homo faber fortunae suae*".

Alea iacta est

Il dado è tratto!

GLOSSARIO

Address: è la chiave pubblica di un portafoglio in Bitcoin ed è formata da una stringa di caratteri alfanumerici utilizzata per ricevere o inviare le transazioni.

ASIC: è uno specifico circuito integrato di chip in silicio, costruito per

svolgere una precisa attività. Nel caso del Bitcoin, sono progettate per processare funzioni Hash con l'algoritmo SHA-256.

Bitcoin: è un sistema di pagamento peer-to-peer e una moneta digitale. Convenzionalmente la parola "bitcoin", scritta in maiuscolo, si riferisce alla tecnologia del network, mentre la parola "bitcoin", scritta in minuscolo, si riferisce alla valuta stessa.

Bitcoin Price Index (BPI): è un indice pubblicato dal sito www.coindesk.com e sintetizza, in base a determinati criteri, il prezzo del bitcoin negoziato su vari exchange.

Blocco: è un'unità che compone il Blockchain e contiene tutte le transazioni

confermate durante il periodo di generazione del blocco stesso. In media ogni 10 minuti viene generato un nuovo blocco e aggiunto in modo cronologico al Blockchain.

Blockchain: è un registro pubblico di tutte le transazioni in bitcoin. Si tratta di una "catena di blocchi", questo perché ogni blocco, che la compone, è per costruzione collegato con il precedente. Da un punto di vista informatico, il Blockchain si definisce come un database memorizzato e distribuito su ogni macchina che fa parte del network Bitcoin.

BTC: è l'abbreviazione della valuta bitcoin. Talvolta si può trovare anche

l'abbreviazione XTB.

Chiave privata: è una chiave crittografica utilizzata in un sistema di crittografia asimmetrica. La chiave privata deve essere custodita gelosamente. Nel sistema Bitcoin la chiave privata si compone di un codice alfanumerico associato a ogni wallet.

Chiave pubblica: è una chiave crittografica utilizzata in un sistema di crittografia asimmetrica. La chiave pubblica può essere scambiata anche su un canale non sicuro. Nel sistema Bitcoin la chiave pubblica è rappresentata dall'address.

Conferma: affinché una transazione in Bitcoin sia valida è necessario che venga confermata dal network attraverso

l'attività di mining.

Crittografia: è un insieme di tecniche che consentono di trasmettere un messaggio mantenendolo segreto a tutti, tranne alle persone che possiedono le chiavi per decifrarlo. Si parla di crittografia simmetrica quando si utilizza la medesima chiave per cifrare e decifrare un messaggio, e di crittografia asimmetrica quando si utilizzano chiavi diverse.

Difficoltà: è la misura di quanto sia complicato trovare un Hash al di sotto di un certo target. Nel sistema Bitcoin la Difficoltà non può essere inferiore a 1 e viene aggiustata ogni 2016 blocchi, cioè mediamente ogni 12 giorni. Si tratta di

un valore inversamente correlato con il target e positivamente correlato con l'Hash rate.

Double spending: è un problema che si verifica quando un bitcoin viene speso più di una volta dallo stesso proprietario.

Genesis block: è il primo blocco che compone il Blockchain ed è stato generato alle ore 18:15:05 del 3 gennaio 2009.

Fair value: è una stima razionale e imparziale del prezzo di un bene o servizio tenendo conto di vari fattori, tra cui la scarsità, l'utilità, il rischio e il costo di produzione o di rimpiazzo.

Fiat currency: è la moneta tradizionale che deriva il suo valore

essenzialmente da un'autorità e dalla fiducia della gente. Di conseguenza, è un valore fiduciario, cioè non determinato dal valore intrinseco di un materiale, quale per esempio l'oro e l'argento.

Funzione Hash: è una funzione che trasforma un messaggio di lunghezza arbitraria in un codice alfanumerico di lunghezza prefissata, che prende il nome di Hash, Digest o impronta del messaggio. La funzione Hash utilizzata nel sistema Bitcoin è l'algoritmo SHA-256.

Hash rate: è la potenza complessiva in Giga-Hash al secondo (GH/s) che il network Bitcoin sta eseguendo.

Incentivi: per il lavoro svolto dai

minatori viene riconosciuto un "rimborso", che si compone di nuovi bitcoin e commissioni di transazione incluse in ogni blocco. Vengono assegnati 50 bitcoin per ogni blocco risolto, ma questo valore si dimezza ogni 210.000 blocchi.

Input: è quella parte di una transazione in bitcoin che identifica l'origine della transazione stessa. Tipicamente si tratta di un address, salvo il caso in cui si tratti di bitcoin di nuova generazione.

Mining: è il processo con cui si verificano e registrano tutte le transazioni in bitcoin, ma è anche l'attività che permette di coniare nuovi bitcoin. Il numero massimo a

disposizione è pari a 21 milioni e tale offerta verrà completata entro il 2140.

Network: il sistema Bitcoin è organizzato in nodi secondo una rete distribuita, decentralizzata e paritaria. Il Network Bitcoin è costruito quindi di tipo P2P (peer-to-peer).

Nonce: è una stringa casuale di dati che viene utilizzata nel processo di hashing di un blocco. Viene utilizzato un Nonce diverso per ogni tentativo di hashing, con lo scopo di soddisfare il target richiesto nel processo di mining di un blocco.

OTC: i bitcoin sono negoziati sui mercati non regolamentati, noti come OTC (Over The Counter). Questi

mercati sono decentralizzati, privi di cassa di compensazione e presentano un rischio maggiore rispetto a quelli regolamentati.

Output: è quella parte di una transazione in bitcoin che identifica l'address di destinazione della transazione stessa.

SHA-256: è l'algoritmo di hashing utilizzato nel sistema Bitcoin. Questo algoritmo restituisce un Hash a 256 bit.

Target: è un numero estremamente grande, a 256 bit, il cui valore si modifica in base al tempo effettivo e teorico necessario per minare 2016 blocchi. Più il target è un numero piccolo e più è difficile ricercare una soluzione che lo possa soddisfare.

Wallet: è un portafoglio elettronico che memorizza tutte le credenziali digitali per accedere, spendere e trasferire i bitcoin. Esistono tre tipologie di wallet: desktop, smartphone e web wallet.

GLI AUTORI

Davide Capoti: Laureato in Economia delle istituzioni internazionali e in Giurisprudenza presso l'Università Bocconi di Milano. Membro dell'International Federation of Technical Analysts (IFTA) e socio della Società Italiana Analisi Tecnica (SIAT).

Attualmente è trader istituzionale sui mercati delle commodities per uno dei primari player del settore. Ha inoltre maturato una specializzazione come portfolio manager su azionario, strumenti derivati e Forex. Co-fondatore di una delle prime startup italiane nel settore delle valute digitali (www.cloudminingbiz.com e www.coinbiz.com). A maggio 2014 ha tenuto la prima conferenza in Italia sul Bitcoin, presso l'ITF di Rimini.

Emanuele Colacchi: Laureato in Ingegneria presso l'Università La Sapienza di Roma. Iscritto all'albo dell'Ordine degli Ingegneri della provincia di Roma. Attualmente è trader

istituzionale sui mercati delle commodities per uno dei primari player del settore. Ha, inoltre, maturato una specializzazione su mercato azionario con operatività sia da trading system che discrezionale. Docente per FinecoBank SpA, una delle principali banche dirette in Europa. Si occupa anche di ricerca e analisi quantitativa nel settore delle valute digitali per una delle prime startup italiane del settore (www.cloudminingbiz.com e www.coinbiz.com).

Matteo Maggioni: Laureato in Economia delle istituzioni e dei mercati finanziari presso l'Università Cattolica di Milano. Membro dell'International

Federation of Technical Analysts (IFTA) e socio della Società Italiana Analisi Tecnica (SIAT). Attualmente è trader istituzionale sui mercati delle commodities per uno dei primari player del settore. Ha, inoltre, maturato una specializzazione in strumenti derivati su indici azionari e obbligazionari in ottica di breve e brevissimo periodo. Docente per FinecoBank SpA, una delle principali banche dirette in Europa. Si occupa anche degli sviluppi delle valute digitali, sia come crypto-trader che come co-fondatore di una delle prime startup italiane del settore (www.cloudminingbiz.com e www.coinbiz.com). A maggio 2014 ha tenuto la prima conferenza in Italia sul

Bitcoin, presso l’ITF di Rimini.

Informazioni sul Libro

Dopo il Bitcoin nulla è più come prima. Quasi uno spartiacque. A livello mondiale, cresce la fama e la diffusione della moneta digitale “non ufficiale”, quale rivoluzionario sistema di pagamento online con cui è possibile acquistare beni reali e servizi.

Ma non solo. Il Bitcoin rappresenta anche una forma di investimento a lungo termine. Transazioni commerciali e finanziarie sono così sottratte al controllo di banche centrali e governi nazionali. Perché la moneta digitale decentralizzata, nata non a caso da Internet, spezza e libera dai vincoli delle banche e dei vari intermediari finanziari.

Comunque la si pensi, il cambiamento è in atto, inarrestabile, nonostante le preoccupazioni crescenti di istituti di credito e Stati nazionali. Nell'interconnesso villaggio globale il tempo corre in avanti e la fiducia sale: il Bitcoin è scambiato con un ritmo da contagio, quasi una nuova corsa all'oro,

che rappresenta di certo una grande opportunità per i più informati. Opportunità che il libro vuole offrire a un più vasto pubblico, non presentandosi solamente come manuale tecnico per i professionisti del settore.