BITCOIN

FUNZIONAMENTO, PROSPETTIVE DI GUADAGNO E CRITICHE AL SISTEMA

Manuel Carsini

Manuel Carsini

autore dei romanzi "I segreti del tempo che è passato" e "L'aliena"

https://www.amazon.it/segreti-del-tempo-che-passato-ebook/dp/B0161MS7NW
https://www.amazon.it/Laliena-Manuel-Carsini-ebook/dp/B0173RGOPC

BITCOIN: FUNZIONAMENTO,

PROSPETTIVE DI GUADAGNO E CRITICHE AL SISTEMA

MANUALE

Prima edizione: marzo 2018

Sommario

Introduzione

Da alcuni anni si sente parlare di criptovalute (cripto-valute), o crittovalute (critto-valute), come se si trattasse di una rivoluzione epocale a beneficio di tutti e, anche se la cautela è d'obbligo in questi casi e le affermazioni eclatanti sono sempre dietro l'angolo, si può senz'altro parlare di un sistema di pagamento digitale decentralizzato dalle grandi potenzialità, con impatti ancora difficilmente prevedibili sull'economia e sul sociale.

In questo contesto i Bitcoin fanno la loro comparsa quali simbolo e apripista

della suddetta, presunta, rivoluzione, riempiendo, con la loro denominazione e con i loro acronimi, grandi spazi su giornali, telegiornali e Internet. È, ad esempio, recente la notizia di un giovane studente diciannovenne che, dopo avere investito 1.000 dollari in Bitcoin nel 2011, quando era appena dodicenne, si è ritrovato milionario nel giro di pochissimi anni.

D'altronde, osservando uno dei tanti grafici che mostrano il cambio del Bitcoin con il Dollaro o con l'Euro nel corso del tempo, non si può evitare di rimanere a bocca aperta constatando che si è passati dai pochi centesimi di dollaro del 2009 ai quasi 20.000 dollari di fine 2017, precisamente a 18.143,80

dollari americani del 15/12/2017.

Visti i numeri in gioco, ci si interroga, quindi, se i Bitcoin siano protagonisti di una nuova bolla finanziaria, addirittura di un piano speculativo ben congegnato che porterà ad un calo vertiginoso del loro valore da un momento all'altro, oppure se diventeranno, assieme ad altre criptovalute, la moneta del futuro.

Fatto sta che l'interesse che i Bitcoin suscitano richiede approfondimenti, non solo sulla loro affidabilità quali mero prodotto di investimento, ma anche su quell'importantissimo frangente che li riguarda: il mining.

Mentre investire oggi in Bitcoin acquistandoli con moneta tradizionale sonante può essere molto più rischioso

che un tempo, quando un buon investimento poteva avere vita a partire da un capitale irrisorio, guadagnare del denaro per mezzo del mining di Bitcoin sembra essere un'idea ancora piuttosto valida e, tutto sommato, poco rischiosa, a patto di prestare molta attenzione alla natura dell'investimento e ai costi ad esso associati.

In sostanza, fare mining di Bitcoin significa partecipare al processo di "estrazione", di creazione della moneta digitale, che permette di guadagnare la criptovaluta effettuando dei compiti, dei calcoli molto velocemente con hardware la cui complessità spazia da quella del proprio computer di casa a quella dell'ultimo ritrovato elettronico per

svolgere calcoli ad hoc con estrema velocità, tipicamente un ASIC (Application Specific Integrated Circuit).

La crittografia assume un ruolo fondamentale nell'ambito del mining dei Bitcoin e, più in generale, in quello delle crittovalute; non è quindi un caso che quest'ultima nomenclatura, che delinea una classe di monete digitali, richiami bene alla mente il concetto di dati da elaborare in chiave crittografica applicando determinati algoritmi matematici al fine di ottenere altri dati.

A tal riguardo, è importante sapere che il numero di Bitcoin che è possibile generare è limitato ed è pari a circa 21 milioni, ragion per cui, più il tempo

passa, più ci si avvicina alla data in cui non sarà più possibile dar vita a nuovi Bitcoin e, pertanto, non sarà più possibile fare mining di Bitcoin.

La buona notizia è che chiunque può fare mining, se non altro per vedere come funziona questo aspetto del sistema Bitcoin in prima persona, ma chiaramente solo chi disporrà di hardware adeguato potrà farlo in modo professionale, con la speranza di guadagnare concretamente.

L'argomento delle criptovalute, e dei Bitcoin nello specifico, risulta essere interessante anche per via del più generico tema degli investimenti a rischio di perdita del capitale, in quanto

apre il sipario sulle più svariate forme di investimento che promettono ingenti guadagni, rendimenti sicuri a fronte di rischi nulli riguardo al capitale investito.

Nella trattazione del manuale si comprenderà, pian piano, quanto sia davvero difficile guadagnare oggi con le crittovalute e quanto siano quantomeno fuorvianti quelle affermazioni che parlano di facilità di guadagni e di investimento a rischio zero, facendo spesso sembrare l'intera materia come un gioco in cui impiegare con leggerezza i propri risparmi.

Questo manuale tratta l'argomento del Bitcoin da vari punti di vista, con l'obiettivo primario di mostrare un po'

tutte le caratteristiche della criptovaluta del momento, al fine di evidenziare gli aspetti più curiosi, ma anche le problematiche di un sistema probabilmente destinato a rivoluzionare per sempre il concetto stesso di moneta.

Quello dei Bitcoin è, infatti, un mondo molto più vasto di quanto generalmente si creda e lo scopo di questa guida è quello di dare una buona idea di quel che esiste sull'argomento, senza entrare troppo nel dettaglio di ogni punto coinvolto nella trattazione. Il manuale tratta, con un certo dettaglio, il funzionamento tecnico del sistema, le prospettive di investimento, senza scendere troppo in profondità nelle tecniche adottabili per conseguire un

possibile guadagno, e muove anche critiche al sistema man mano che ne delinea i tratti fondamentali.

A chi è rivolto principalmente questo manuale

Questo manuale è rivolto principalmente a chi è interessato a sapere cosa sono i Bitcoin e cosa tale criptovaluta comporti oggi sotto vari aspetti, in termini soprattutto economici, a chi si avvicini all'argomento con curiosità per comprenderne le fondamenta, i principi salienti e le prospettive di guadagno, senza però ricercare un approfondimento su tutto ciò che gravita intorno alla materia, soprattutto riguardo a strategie mirate di investimento, e anzi soffermandosi sugli aspetti negativi con una certa critica al sistema.

Con le informazioni e i suggerimenti

contenuti in questo manuale si riuscirà a comprendere la complessità di un sistema troppe volte considerato come uno strumento magico per fare arricchire chiunque, che invece, al pari di un po' qualunque altro strumento di investimento, è soggetto non solo al rischio di mancato guadagno, ma anche al ben più preoccupante rischio di perdita del capitale investito.

A chi non è particolarmente rivolto questo manuale

Questo manuale non è particolarmente rivolto a chi possiede già molta dimestichezza con il mondo delle crittovalute e, in particolare, con quello dei Bitcoin. Non trattandosi di una guida approfondita su un aspetto specifico dei Bitcoin, non è particolarmente rivolto a chi è alla ricerca di una guida specializzata che tratti a fondo solo uno o pochi aspetti del vasto argomento delle crittovalute, o di una guida che abbia un approccio enciclopedico, rigoroso, esaustivo.

Il manuale getta delle basi per individuare i temi di maggiore interesse

che potrebbero essere approfonditi in altro modo, dando una buona visione d'insieme dell'argomento trattato, ma non si prefigge di scendere eccessivamente nel dettaglio tecnico con approfondimenti, ad esempio, sulla programmazione sottesa al sistema, sul codice sorgente che, nei vari possibili linguaggi di programmazione, sottende l'intera infrastruttura. Non si tratta di una guida per investire in Bitcoin passo passo, né di una guida per sviscerare le funzioni implementate nei programmi informatici che sottendono il sistema.

Capitolo 1: storia, importanza e criticità del Bitcoin

Storia del Bitcoin

L'idea del Bitcoin quale moneta virtuale trova concretezza a fine 2008, ad opera di un certo Satoshi Nakamoto, pseudonimo di un ideatore anonimo che ha fatto e continua a fare molto discutere. I più maliziosi ritengono che il suo anonimato costituisca già una prova del carattere speculativo della criptomoneta che, in effetti, ha consentito di arricchirsi soprattutto ai primi possessori e al suo ideatore in particolare.

In questo contesto c'è addirittura chi ritiene che dietro ad un nome di persona si nasconda una grossa multinazionale o addirittura un Governo straniero,

insomma molto più di quel che si vorrebbe far credere, con risvolti nelle sfere della politica e del sociale.

Al di là dei leciti dubbi, rimane il dato di fatto del documento ufficiale di Satoshi Nakamoto che descrive il Bitcoin nel suo concept. Si tratta di un documento con grafici che descrive la natura peer-to-peer del sistema, dove una potenza di calcolo globale dà vita alla criptomoneta stessa secondo la filosofia del guadagno proporzionale in funzione della potenza di calcolo messa a disposizione dai nodi, ossia da computer ed altri dispositivi di calcolo connessi alla rete peer-to-peer su cui si basa il Bitcoin.

Non ci sono limiti per aderire al

sistema e partecipare al *mining*, ossia alla creazione di nuova moneta: basta scaricare gratuitamente l'apposito software e divenire, in men che non si dica, un nodo della rete Bitcoin. Lo stesso software di connessione al sistema Bitcoin, in genere, consente di creare una chiave privata ed una chiave pubblica che sono necessarie per effettuare e ricevere pagamenti, come si vedrà nel dettaglio in seguito.

Per pagare qualcuno in Bitcoin, tipicamente si utilizza il denaro di cui si è venuti in possesso in una precedente transazione; un nuovo beneficiario sarà destinatario di tale denaro, di cui si è quindi stati beneficiari in precedenza.

Satoshi Nakamoto ha anche dato vita

al cosiddetto "Bitcoin Core" che, come la stessa denominazione suggerisce, costituisce un'implementazione delle funzionalità di base che il sistema dovrebbe avere. Il cuore del sistema, di fatto, consiste nell'attuazione di transazioni tra pari, senza cioè la tradizionale, spesso criticata, posizione dominante di uno o più soggetti quali le banche; segue la stessa filosofia di decentramento l'emissione del denaro, che non è devoluta a soggetti istituzionali, ma ai semplici cittadini.

Si intuisce l'importanza storica di una filosofia del genere, che vuole mettere le persone comuni al centro della gestione monetaria, una vera e propria rivoluzione nel modo di concepire la

valuta, che è così pienamente del popolo e non più dei Governi e delle banche.

D'altra parte, a proposito di Governi, si pensi al fatto che alcuni anni fa si vociferava che la Germania avrebbe accettato il pagamento delle imposte per mezzo di Bitcoin. Tutta la faccenda è, insomma, in divenire e i Governi ne sono ormai pienamente interessati.

Le date importanti che riguardano la nascita del Bitcoin sono il 18/08/2008, quando viene registrato il nome di dominio Bitcoin.org, ma soprattutto il 31/10/2008, quando il documento ufficiale che riguarda i Bitcoin, dal titolo "Bitcoin P2P e-cash paper" , viene pubblicato per la prima volta, e il 03/01/2009, quando nasce il "genesis

block", ossia il primo blocco Bitcoin, contenente 50 Bitcoin.

La prima transazione in Bitcoin è avvenuta il giorno 12/01/2009, con numero di blocco 170; Satoshi Nakamoto inviò denaro in tale criptovaluta ad Hal Finney, anche se si dovrà aspettare il 22/05/2010 per la prima vera transazione pubblica, in cui un certo *laszlo* comprò una pizza pagandola 10.000 Bitcoin, con un cambio di $41. Ebbene sì, con neanche 50 dollari americani, a metà 2010, si poteva acquistare la bellezza di 10.000 Bitcoin.

Il 05/10/2009, a circa un anno dalla registrazione del nome di dominio Bitcoin.org, viene pubblicato il tasso di

cambio del Bitcoin rispetto al dollaro: $1 = 1,309.03 BTC (0,08 centesimi di dollaro a Bitcoin, ossia $0,0008/BTC), con negoziazioni sul mercato New Liberty Standard; è l'inizio di una incredibile prospettiva di ricchezza per chi, di lì a breve, acquisterà moltissimi Bitcoin a pochi centesimi e li rivenderà dopo anni a cifre da capogiro diventando milionario senza sforzi. Del resto, il 12/07/2010, in appena cinque giorni, il tasso di cambio BTC/Dollaro aumenta di 10 volte: si passa da un cambio di $0.008/BTC ad un cambio di $0.08/BTC.

Vantaggi dei Bitcoin

I Bitcoin sono finiti sotto la luce dei riflettori non solo per le fortunate circostanze che hanno permesso a gente comune di arricchirsi con essi, ma anche per la solidità di molte delle idee che sono alla base del loro sviluppo come moneta digitale alternativa a quella tradizionale.

Uno dei vantaggi dell'utilizzo di Bitcoin risiede nell'anonimato, a dire il vero nemmeno assoluto, nella necessità, per il beneficiario di un pagamento, di fornire al soggetto emittente soltanto la sua chiave pubblica. Chi dispone il pagamento, inoltre, non dovrà rilevare

informazioni personali né informazioni legate a carte di credito o altro, informazioni che, se rubate, minerebbero la sicurezza del suo conto.

Si noti, però, a tal riguardo, che l'anonimato nello scambio di Bitcoin tra utenti è tale per i comuni cittadini, ma non per le Forze dell'Ordine, almeno per quel che riguarda le *Permissionless Blockchain* (l'infrastruttura del Bitcoin), ossia le Blockchain senza permesso, a pubblico accesso e liberamente consultabili da chiunque, che non richiedono una accettazione iniziale per potervi operare. In questo caso, infatti, possono essere effettuati dei controlli mirati ad individuare gli utenti che operano dietro i nodi, i beneficiari di

pagamenti, sebbene i loro indirizzi, come si vedrà più avanti nella trattazione, sono le loro chiavi pubbliche che consistono in stringhe criptate; ebbene, partendo da tali chiavi, che in effetti sono in pratica delle stringhe che non contengono informazioni sui dati personali degli utenti, le Autorità possono cercare, all'interno della Blockchain, gli utenti che possiedono le chiavi private tali che ad esse siano associate le suddette chiavi pubbliche. Esiste, infatti, un legame tra chiave pubblica e chiave privata, tale che la chiave pubblica viene ricavata a partire dalla chiave privata in modo univoco.

Una mancanza di tracciabilità può

invece avere luogo per le *Permissioned Blockchain*, che sono private e richiedono un permesso, un'accettazione iniziale per potere essere utilizzate; se non viene fornito l'accesso alle Autorità, non possono davvero essere messe sotto controllo e, pertanto, per esse vige l'idea di anonimato tanto diffusa.

A parte questo, un vantaggio dei Bitcoin, come accennato in fase introduttiva, risiede nella natura peer-to-peer del sistema, che mette in comunicazione dei *pari* senza la necessità di un coinvolgimento di soggetti centrali, quali le banche, visti spesso e volentieri di mal occhio da cittadini divenuti via via più diffidenti

per colpa anche di vergognosi scandali che li hanno interessati.

Un altro vantaggio dei Bitcoin è quello della comodità dei pagamenti, con transazioni che possono avvenire tra soggetti anche molto lontani in modo molto semplice e rapido, con costi molto contenuti, pressoché nulli. I Bitcoin possono, inoltre, essere utilizzati, in tutto il mondo, in negozi, alberghi, ristoranti, bar che li accettano, esponendo magari una dicitura del tipo "Bitcoin accepted here", oltre che nei negozi virtuali di molti siti Web navigabili via Internet.

Un altro vantaggio dei Bitcoin è quello

della mancanza di restrizioni per i soggetti che li utilizzano; in altre parole, chiunque può usarli senza la necessità di fornire garanzie a chicchessia, senza dovere avere un conto corrente associato, un reddito minimo ecc., e senza limiti di importi massimi di pagamento, che sono invece previsti, ad esempio, per le carte di pagamento bancarie quali le carte di credito e le carte Bancomat.

Problematiche relative ai Bitcoin

Sebbene le crittovalute e i Bitcoin in primis rappresentino una vera rivoluzione per le movimentazioni di denaro, sussistono delle indubbie problematiche che le riguardano e che, potenzialmente, potrebbero addirittura decretarne la fine, prima o poi.

I Bitcoin, da un certo punto di vista, presentano il vantaggio di garantire l'anonimato di chi li detiene, entro certi limiti, ma al contempo è garantito anche il principio di irreversibilità, secondo il quale ogni transazione che li coinvolge non può essere annullata. Ebbene, da un

altro punto di vista questo costituisce uno svantaggio perché, in caso di errori, di ripensamenti o anche del furto di dati che consentano ad un malintenzionato di appropriarsi di Bitcoin altrui, in pratica accedendo illecitamente a chiavi pubbliche e private, non c'è modo, per i legittimi proprietari, di mettere in atto una rivalsa e c'è il rischio concreto di perdere il proprio denaro se non si prendono misure adeguate a scongiurare ogni rischio, quale quella del backup periodico del proprio wallet, che rappresenta, in sostanza, il proprio portafogli virtuale.

Un altro problema dei Bitcoin è rappresentato da un limite massimo

esiguo di transazioni contemporanee che li caratterizza. Mentre, ad esempio, per i pagamenti su circuito Visa non sussistono problemi pratici riguardo a transazioni pressoché contemporanee, dato che tale circuito, in teoria, ne supporta oltre 56.000 al secondo, mediamente 1.667 al secondo, per i Bitcoin le cose stanno molto diversamente poiché è possibile eseguire al massimo, teoricamente, solo 7 transazioni al secondo, a livello globale, una vera inezia che porterebbe a indicibile lentezza qualora il sistema si diffondesse a macchia d'olio nel prossimo futuro. A complicare le cose si aggiunge il fatto che, in pratica, il sistema Bitcoin oggi non riesce a

garantire nemmeno le 7 transazioni al secondo teoriche, ma riesce a gestirne al massimo appena 3 o 4. Si intuisce che le 3 o 4 transazioni al secondo che si riescono a gestire con i Bitcoin fanno sembrare il sistema di tale criptovaluta un giocattolo rispetto a sistemi di pagamento tradizionali quali quello di Visa.

Un ulteriore problema, di carattere pratico, consiste nella portata ridotta della validità della moneta; sono infatti molto pochi gli esercizi commerciali che la accettano e anche su Internet relativamente pochi negozi virtuali la tengono in considerazione per gli acquisti online, anche se il numero di

aziende su Internet che li accetta è in continua crescita.

Sussiste, inoltre, un rischio, sebbene considerato generalmente molto ridotto, che la maggior parte della potenza di calcolo del sistema distribuito dei Bitcoin finisca nelle mani di malintenzionati che riescano così a sovvertire la legalità di tale sistema. In sostanza, fintanto che la maggior parte delle risorse computazionali è nelle mani di utenti onesti, non vi è il rischio di falsificazione dei dati a favore di truffatori e quant'altro, ma non si può essere certi che le cose continuino ad andare bene come adesso.

Un'altra problematica non da poco che scaturisce dal sistema Bitcoin e, nello specifico, dal mining di Bitcoin, è quella dell'enorme consumo di corrente elettrica necessaria a tenere sempre accesi i dispositivi elettronici che fanno computazioni onerose di continuo per dar vita a nuova criptomoneta; tutta questa corrente impiegata ha un impatto non indifferente sull'ambiente, inquina e assorbe risorse che sarebbero molto più utili in altri frangenti compromettendo il già precario stato in cui versa il nostro pianeta.

Ad esempio, si stima che fare mining di Bitcoin, a livello globale, porti ad un consumo energetico orario superiore a quello annuale della città di Milano e,

sempre a livello mondiale, il consumo orario di corrente necessario a fare mining di Bitcoin risulta essere confrontabile con il fabbisogno energetico annuo dell'Ecuador o dell'Oman o del Marocco; ben 159 nazioni di tutto il mondo consumerebbero, in un anno, meno energia di quanto ne sia richiesta dal mining in una sola ora.

A fine 2017, infatti, si stimava un consumo energetico tra 24 e 30 TWh (terawattora, ossia mille miliardi di Wh) per fare mining di Bitcoin, corrispondente a circa lo 0,13% del consumo energetico globale, prendendo per buona la seconda stima.

Con l'aumento esponenziale dei

consumi a cui si è assistito negli ultimi mesi, si teme che il consumo energetico per tale attività aumenti fino a superare quello degli USA entro il 2019 e divenire addirittura confrontabile con quello mondiale entro il 2020. In pratica, se ciò si verificasse, sarebbe come se l'intero pianeta consumasse, ogni ora, il doppio di quanto consumava, all'anno, prima dell'avvento del mining.

Se si guarda alle singole transazioni, sempre a fine 2017 si stimava che ognuna di esse, nel sistema Bitcoin, richiedeva un consumo energetico, per essere attuata, pari a quello richiesto, mediamente, in una casa per una intera settimana.

Un'altra problematica che si può riscontrare riguardo ai Bitcoin è che non si tratta di una valuta ufficiale e quindi bisogna considerare anche l'aspetto fiscale della questione, con adempimenti a tutt'oggi non ancora del tutto chiari; in caso di plusvalenze, di guadagno da rivendita di Bitcoin, ci si dovrà preoccupare anche della tassazione seguendo una normativa specifica ancora in divenire.

Un possibile problema del sistema Bitcoin così com'è concepito riguarda la certezza dei pagamenti che si ricevono; ogni transazione inizia ad essere confermata soltanto dopo circa 10 minuti dalla disposizione di pagamento, ma

prima di diventare definitiva, malintenzionati potrebbero far credere ai beneficiari di aver realmente pagato un certo bene o servizio senza l'intenzione di farlo davvero, pertanto, se si è destinatari di un pagamento, si consiglia di attendere anche un'oretta, prima di ritenersi sicuri di essere al riparo da un certo margine di reversibilità del pagamento.

Per finire, ma non ultimo per importanza, vi è pure un problema relativamente recente, che riguarda un po' tutti i computer, anche quelli che non partecipano al mining e che non hanno nulla a che fare con i Bitcoin: i *miner virus* o *virus miner*; si tratta di malware,

ossia di programmi informatici dannosi che, di nascosto, silenziosamente, forzano un'azione di mining a vantaggio di pochi che sfruttano la potenza di calcolo dei computer altrui per arricchirsi con un sistema computazionale distribuito, un'azione ovviamente illecita perché perpetrata all'insaputa degli utenti, che non immaginano che qualcun altro sfrutti i loro computer per fare soldi.

Si stima che, nel 2017, ben 2,7 milioni di utenti sono stati infettati da tale malware che, inutile dirlo, tra l'altro rallenta anche moltissimo i computer che infetta, data la potenza computazionale necessaria a fare mining . Sembra, insomma, che anche chi non è interessato

al mining e ai Bitcoin possa pagare uno scotto per certi comportamenti illeciti che costituiscono e potrebbero costituire sempre più una serissima problematica relativa ai Bitcoin.

Capitolo 2: il difficile guadagno con i Bitcoin

I Bitcoin, oltre a costituire una opportunità di circolazione di moneta valutabile in modo positivo, hanno anche portato alla luce una problematica di ampio respiro, o meglio hanno pure riesumato un problema concettuale che può affliggere chi apprende le notizie con poco spirito critico: il guadagno facile e senza rischi.

L'idea di guadagnare moltissimo in pochissimo tempo è sempre dietro l'angolo e la facilità con cui alcuni

propongono il tema dei Bitcoin come facile possibilità, per chiunque, di non lavorare più può essere molto pericolosa, anche perché, spesso, si insidia nella mente dei più giovani, i più esposti a certi tipi di malsane tentazioni.

Si fa presto a dire che è facilissimo e immediato guadagnare con i Bitcoin e con le altre criptovalute, ma se davvero le cose stessero in questo modo, come mai sono così pochi i casi di successo e la quasi totalità dei giovani, per guadagnare, deve necessariamente lavorare, e molto spesso pure duramente e purtroppo in condizioni di eterno precariato?

Dovrebbe risultare evidente che il guadagno facile con i Bitcoin,

semplicemente, non esiste, al pari del guadagno facile in Borsa, del guadagno facile nel Trading e così via. Secondo alcuni esperti, anzi, il Bitcoin rappresenta nient'altro che una speculazione, una bolla che, prima o poi, non si sa quando, esploderà trascinando nel baratro molti incauti investitori. Secondo chi non vede di buongrado le criptovalute in generale, il principio alla base di questi sistemi è di tipo speculativo-finanziario e non si basa su alcuna base solida poiché si affida esclusivamente al concetto di mercato, basato semplicemente sull'idea di domanda e offerta.

Il punto cruciale della questione è che, mettendo per un attimo da parte il

"lavoro" del mining, se qualcuno guadagna molto con un certo investimento che non ha per sottostante un lavoro, in questo caso con un investimento in Bitcoin che non ha alcun vero lavoro sotteso, allora, per forza di cose, questo comporterà che una moltitudine di altri investitori in Bitcoin perderà moltissimo. Come si suol dire, la coperta è corta, come avviene per tutte quelle forme di investimento che non sono basate su un reale lavoro, ma su speculazioni e bolle finanziarie.

Il vero, consistente guadagno con i Bitcoin l'ha avuto chi ha investito all'inizio scambiando moneta reale con la criptovaluta a tassi estremamente convenienti ed ha poi, dopo diversi anni,

quando il valore del Bitcoin è schizzato alle stelle in modo incontrollato, cambiato i Bitcoin con moneta reale sonante: pagare un Bitcoin pochi centesimi di Euro nel 2009 per rivenderlo a quasi 18.000 euro nel 2017 è, innegabilmente, un enorme guadagno.

Ad avvelenare il sistema, sempre secondo alcuni esperti in investimenti, vi è il fatto che, chi in passato, dopo il periodo d'oro iniziale, ha guadagnato con i Bitcoin investendo cifre non più trascurabili, successivamente, allettato dalle prospettive di ricavi, relativamente facili da conseguire nei primi anni di vita della criptomoneta, ha reinvestito in Bitcoin somme di denaro via via crescenti, in un circolo vizioso

che, in taluni casi, è in grado di creare addirittura una preoccupante dipendenza paragonabile a quella tipica del gioco d'azzardo, dei casinò, delle slot machine e così via.

La concreta possibilità dar vita ad una dipendenza in questi termini è pericolosa perché, prima o poi, inevitabilmente, porterà al tracollo finanziario; non è infatti possibile che il valore dei Bitcoin aumenti sempre all'avanzare del tempo, è chiaramente impossibile che cresca all'infinito, e quando si presenterà l'inevitabile perdita, vi sarà il rischio altissimo di ritrovarsi con un pugno di mosche in mano.

Allora perché non bollare tutto come un pessimo, pericoloso investimento e snobbare la criptovaluta del momento? Per almeno due buone ragioni: la prima è che non è detto che le cose siano davvero così negative e che investire in Bitcoin risulti fallimentare, la seconda è che può essere davvero molto interessante, a prescindere dall'aspetto dell'investimento, capire cosa sono davvero i Bitcoin, cosa possono rappresentare per il cittadino che vuole avere semplicemente una possibilità in più di effettuare pagamenti, e come un sistema complesso come quello sottostante a tale crittomoneta sia stato implementato.

Vi sono, cioè, diversi motivi per non

liquidare il tutto come una cosa inutile e infruttifera, primo tra i quali quello culturale, dell'informazione su un sistema che può essere interessante analizzare anche da un punto di vista tecnico, oltre che da un punto di vista finanziario.

Non è un caso che le nazioni di tutto il mondo stiano riflettendo sul fenomeno Bitcoin, che i big dell'economia si adoperino a dire la loro su quello che, fino a pochi anni fa, era un sistema di trasferimento di denaro nell'ombra, poco tenuto in considerazione perché considerato poco degno di attenzione. Oggi l'economia mondiale ha compreso la pericolosità di un sistema cresciuto a macchia d'olio in poco tempo, al punto

che alcuni paragonano la febbre da Bitcoin alla febbre da gioco d'azzardo.

L'instabilità economica, politica e sociale che è ormai entrata a far parte delle nostre vite, nonché la sfiducia nella politica e nelle banche, ha spinto molti a guardare al Bitcoin addirittura come ad un bene rifugio, quasi come se si trattasse di oro, del vecchio, caro mattone o di altro bene materiale considerato da sempre come strumento di risparmio sicuro.

La verità è che le criptovalute, e i Bitcoin nello specifico, sono tutt'altro che uno strumento sicuro a cui affidare i propri risparmi senza troppe preoccupazioni, contando sui cambi

sempre più favorevoli di questi ultimi anni.

Scarsità dei Bitcoin

Per bilanciare un po' il pessimismo che trapela da quanto osservato poc'anzi, va considerato che uno dei concetti più interessanti che riguardano i Bitcoin è quello della scarsità: vi è un limite prestabilito alla creazione di moneta, che vede a regime una presenza di 21 milioni di Bitcoin nel 2140.

Questo è dovuto al fatto che il mining, con cui si genera nuova moneta, dà oggi vita ad un premio, per ogni blocco validato, di 12,5 Bitcoin, quindi ogni circa 10 minuti vengono rilasciati nel sistema nuovi Bitcoin.

Il suddetto numero, però, si dimezza ogni 4 anni ed infatti, nel 2012 era pari a

25 anziché 12,5, e anni prima era pari a 50. Questo fa sì che, con il passare del tempo, vengano immessi sempre meno Bitcoin nel sistema, che così non crescerà all'infinito fino ad "esplodere" con un eccesso di moneta.

In questo modo si protegge la moneta dall'inflazione e si compensa il fenomeno della sempre più grande potenza computazionale della rete informatica decentralizzata su cui si basa la criptovaluta.

Capitolo 3: uno sguardo pratico al sistema

Il Bitcoin in pillole

Il sistema sottostante il Bitcoin è piuttosto complesso, almeno tale appare generalmente all'inizio se ci si avvicina ad un argomento articolato quale quello delle criptovalute conoscendone al massimo le caratteristiche ad alto livello, per concetti vaghi e generali, acquisiti fugacemente magari leggendo un articolo di giornale o prestando attenzione all'ultima notizia del telegiornale sull'argomento.

A dirla tutta, non è nemmeno così importante entrare nel dettaglio dell'implementazione dell'infrastruttura su cui si basa il Bitcoin se il proprio scopo è solo quello di investire in tale

crittovaluta facendo trading o sfruttando l'hardware di cui si dispone per fare mining e redigendo così semplicemente, alla fin fine, un prospetto sui costi, sulle uscite di denaro stimabili per ottenere un certo risultato economico e tale risultato sperato, al fine di valutare se vi sia reale convenienza o meno per un investimento di questo tipo.

Molto spesso, chi investe in un determinato settore non ha conoscenza approfondita dell'oggetto dell'investimento, ma una visione generale che comunque basta, o dovrebbe quantomeno teoricamente bastare a prendere le decisioni giuste al momento giusto.

Entrare nel dettaglio può, però, essere

appagante per chi è curioso di capire cosa vi sia dietro alla "moneta del momento" e utile per chi avesse l'esigenza di lavorare attivamente nel mondo delle crittovalute e dei Bitcoin in particolare, ad esempio per contribuire all'implementazione di client che consentano all'utente di interagire con il sistema.

Il Bitcoin, innanzitutto, viene indicato con l'acronimo BTC o con l'acronimo XBT e rappresenta oggi, più di ieri, un'entità digitale dal grande valore, pari a svariate migliaia di Euro, o Dollari se si preferisce; per questo motivo, nella pratica si parla perlopiù di sottomultipli del Bitcoin, la cui più piccola parte è rappresentata da un *Satoshi*, pari a

1/100.000.000 BTC, ossia a un centomilionesimo di Bitcoin.

Semplificando al massimo, il Bitcoin è rappresentato, a basso livello, da stringhe alfanumeriche ciascuna delle quali è presente una sola volta nel sistema concepito ad hoc per tale criptovaluta, che consiste in una infrastruttura informatica distribuita atta a registrare le transazioni che coinvolgono la moneta in maniera decentralizzata, garantendo, tra l'altro, un certo anonimato.

Il Bitcoin, in pratica, è associato ad un insieme di transazioni legate l'una all'altra a mo' di catena. Non a caso si parla, infatti, di "Blockchain", o "catena dei blocchi", proprio per indicare una

catena di transazioni in cui sono coinvolti i Bitcoin.

Il concetto di base è che ogni transazione che coinvolge Bitcoin viene codificata in un blocco della catena con il salvataggio dei riferimenti dei proprietari della moneta, che consistono in indirizzi pubblici, in chiavi pubbliche, e non coinvolgono i nominativi dei soggetti, dato che il sistema garantisce l'anonimato, seppure con dei limiti.

Un passaggio di denaro virtuale da un proprietario all'altro è considerato valido sulla base della firma di un hash e la chiave pubblica del beneficiario della transazione.

In altre parole, se si segue l'esempio

di un acquisto, quando l'acquirente che possiede Bitcoin deve pagare il venditore, applica una firma digitale che ha lo scopo di garantire l'autenticità e l'unicità del pagamento, che non potrà quindi essere riutilizzato per una seconda volta, per scongiurare, così, l'insidioso problema di spese doppie e possibili atti illeciti ad esse correlate.

Il wallet

Il wallet è lo strumento fondamentale dell'utente, visto che gli consente di gestire i Bitcoin tenendo traccia della disponibilità di denaro digitale. In pratica consiste nel portafogli virtuale a cui attingere per effettuare spostamenti di denaro sia in uscita che in entrata.

Nel concreto, un wallet consiste quantomeno in un file dove sono memorizzate delle chiavi private che, di fatto, consistono in codici crittografici aventi una lunghezza di 51 caratteri di tipo alfanumerico.

Per effettuare un pagamento occorre conoscere la chiave pubblica del beneficiario, una stringa alfanumerica

composta da un numero di caratteri compreso tra 27 e 34, che non può comprendere i caratteri '0', 'O', 'I' e 'L'.

Specificando l'importo da trasferire a favore di qualcuno, quindi, con il software che gestisce il wallet è possibile inviare denaro molto agevolmente.

Il wallet nella sua definizione di base che considera solo un elenco di chiavi private da mantenere a tutti i costi segrete, di per sé non necessita nemmeno di un computer o di un qualunque altro dispositivo elettronico in grado di memorizzare dati; è infatti possibile semplicemente scrivere le proprie chiavi private su un foglio di carta da conservare e nascondere con

cura: se si dovessero perdere, si perderebbe irrimediabilmente tutto il proprio denaro.

Appare, quindi, evidente e condivisibile il timore che qualche hacker acceda al proprio wallet digitale per rubarne le chiavi e quindi gestire, a tutti gli effetti, un portafogli altrui come se fosse suo. Il consiglio è quindi quello di mettere in sicurezza tali dati sensibili e di fare attenzione a non dare accesso al proprio computer a persone anche autorizzate per vari motivi: la prudenza non è mai troppa in questi casi.

Vi sono, quindi, due rischi che riguardano il wallet: il rischio di perdita dati e il rischio di furto dati; per scongiurare il primo si può ricorrere a

backup frequenti del wallet, che possono essere fatti molto facilmente e comodamente utilizzando lo stesso software di gestione del portafogli, mentre per scongiurare il secondo si può ricorrere al cosiddetto "borsellino deterministico", che consente la generazione di chiavi crittografiche partendo da un "codice seme".

Nell'ultima circostanza appena esposta, si può memorizzare su un altro dispositivo o al limite sullo stesso computer in uso, ben nascosta, o scrivere su un foglio di carta un'unica stringa, appunto quella del codice seme, a partire dalla quale si potranno ottenere agevolmente le chiavi, così che, anche in caso di furto di dati, il malintenzionato

non potrà accedere alle chiavi, non conoscendo il codice seme segreto che si terrà opportunamente al sicuro.

A proposito di sicurezza e di anonimato, poiché il sistema Bitcoin si basa su una Blockchain che si comporta come un registro pubblico, che può essere consultata per tracciare le transazioni dei vari blocchi, se si vuole proteggere il più possibile il proprio anonimato è opportuno cambiare il proprio indirizzo prima di effettuare una transazione, la qual cosa può essere fatta rigenerando la coppia di chiavi, ossia la chiave pubblica e la chiave privata, utilizzando semplicemente il software di gestione del proprio wallet.

Come guadagnare Bitcoin

Allettati dalle notizie che di recente impazzano in continuazione un po' ovunque, la prima cosa che ci si chiede, su cui si interroga soprattutto chi ha sentito parlare di Bitcoin per la prima volta, è come si possano guadagnare Bitcoin, in modo da avere, alla fin fine, la speranza di guadagnare denaro reale e possibilmente di "fare il colpaccio" e diventare ricchi.

A tal riguardo, è bene precisare sin da subito che, poiché, come si dice, i soldi non crescono sugli alberi, non è possibile guadagnare nemmeno monete digitali quali i Bitcoin con poco o, ancora peggio, nessuno sforzo. Chi si è

arricchito con i Bitcoin, lo ha fatto scommettendo anni fa su un concept di moneta che destava non pochi dubbi oppure venendo a conoscenza della tematica all'inizio, quando il cambio in euro o dollari era così favorevole che non c'era decisamente bisogno di pensarci sopra troppo per lanciarsi in un acquisto di criptovaluta.

Oggi, guadagnare Bitcoin sperando di diventare ricchi è diventato molto più difficile, ma la buona notizia è che, ottenendo Bitcoin in vario modo, si può ancora sperare in un guadagno reale più che soddisfacente.

Il modo più intuitivo di guadagnare Bitcoin è quello di vendere oggetti

oppure servizi e farsi pagare con tale crittovaluta. Sono ormai molti che vendono e comprano utilizzando moneta digitale e molti, in passato, quando ancora il Bitcoin non aveva un valore di cambio stratosferico come quello di oggi, si sono arricchiti facendosi pagare in questo modo, accollandosi il rischio che il tutto si sarebbe rilevato presto una mera bolla speculativa in grado di lasciare in mano solo un pugno di mosche.

Un espediente particolarmente interessante che può tornare utile in alcuni casi, soprattutto se si gestisce qualche sito Web, è quello di richiedere ai visitatori di fare una donazione in Bitcoin, chiaramente facoltativamente,

senza alcuna costrizione e anche senza insistenze; da anni alcuni siti chiedono donazioni di supporto con varie modalità di trasferimento fondi possibili, la più celebre delle quali è probabilmente quella di PayPal, e quindi è possibile comportarsi in modo analogo per guadagnare Bitcoin, anche se una volta, essendoci meno attenzione su tale moneta, che non godeva dei tassi di cambio di oggi, questa strada era molto più percorribile.

Un altro modo piuttosto semplice di ottenere Bitcoin è quello di fare un cambio con gli Euro, in pratica di acquistare la moneta digitale con la moneta tradizionale, di fatto investendo

con il trading di valute. Si intuisce che, per riuscire a guadagnare con questo tipo di investimento, occorre acquistare Bitcoin quando il loro controvalore rispetto all'Euro è il più possibile basso e poi venderli quando il loro controvalore rispetto all'Euro è il più possibile alto. Inutile dire che sussiste il rischio di non riuscire a rivendere i Bitcoin ad un prezzo superiore a quello d'acquisto.

Un altro modo ancora per guadagnare Bitcoin, che è quello forse più stimolante, ma anche quello più difficile da attuare con successo, è quello di ricorrere al mining. Sebbene l'argomento verrà affrontato in seguito nel dettaglio,

è bene sapere sin da subito che, per guadagnare Bitcoin in questo modo è necessario un certo investimento di tempo e di denaro perché fare mining con successo, oggi, richiede tempismo, valutazioni attente e stesure di calcoli certosini, per sperare di riuscire a guadagnare più di quanto si spenda per l'hardware aggiuntivo al classico computer, necessario allo scopo, e per l'energia elettrica necessaria a farlo funzionare di continuo.

Per una buona riuscita dell'operazione, inoltre, è molto importante anche avere la fortuna di cavalcare l'onda quando il cambio è più favorevole, ossia bisogna sperare che i Bitcoin guadagnati con questo sistema siano successivamente

vendibili sfruttando un buon tasso di cambio perché, altrimenti, si rischierebbe di rimanere davvero con un pugno di mosche se la crittovaluta subisse un tracollo per colpa del quale non si riuscisse a ripagare nemmeno l'investimento in hardware e in corrente elettrica.

Il grande problema del mining, oltre a quello esposto, relativo al rischio di perdita di quanto investito per ribassi incontrollati del valore del Bitcoin, è quello della continua obsolescenza dell'hardware che si acquista, che è efficace allo scopo solo per brevi periodi di tempo, tipicamente di una manciata di mesi; dopo tale periodo, il rischio è di doverlo addirittura buttare

perché la complessità crescente del problema matematico sotteso al guadagno dei Bitcoin, unita alla sempre maggiore concorrenza tra minatori, fa sì che sia necessario rinnovare tale hardware con frequenza, comprando più volte dispositivi via via più complessi e potenti, con la difficoltà di rivendere quelli obsoleti al fine di disfarsene recuperando una parte delle spese sostenute.

In pratica, esiste una corsa contro il tempo per sfruttare al massimo l'hardware che, sul momento, offre il massimo in termini di potenza di calcolo, e non va dimenticata la complicazione delle spedizioni internazionali, dato che gli ASIC più

performanti e al contempo economici, vengono tipicamente spediti dalla Cina; ciò significa dover aspettare, anche più di un mese, affinché il pacco arrivi in Italia e anche tenere nel giusto conto le spese doganali a cui gli oggetti sono sottoposti per una importazione in Italia. Il tutto senza contare il rischio di merce difettosa o addirittura non funzionante.

Capitolo 4: la Blockchain e i blocchi alla base del sistema

La Blockchain

Quando si parla di Bitcoin e di mining si finisce inevitabilmente con l'imbattersi nella cosiddetta Blockchain, letteralmente una catena di blocchi, che rappresenta il cuore dell'infrastruttura sottostante la moneta digitale del momento.

Si tratta di una sorta di registro contabile elettronico che tiene traccia di tutte le transazioni effettuate con i Bitcoin, che vengono validate e rese pubbliche per trasparenza, pur mantenendo l'anonimato dei soggetti che le hanno eseguite, almeno ad un certo livello.

Se si fa un acquisto e si paga in

Bitcoin, sarà necessario inserire la transazione all'interno della catena, con il timestamp dell'operazione, ossia la data con l'orario preciso al secondo. Nel dettaglio, i pagamenti vengono registrati mediante delle transazioni, le quali vengono inserite nei vari blocchi della catena, secondo il seguente schema:

pagamenti => transazioni => blocchi => blockchain

Ogni blocco che si va ad aggiungere alla Blockchain ha un legame con il blocco precedente ed è infatti contraddistinto da una stringa alfanumerica che viene ricavata a partire da quella che identifica il blocco

precedente, la qual cosa fa sì che sia estremamente difficile falsificare un certo blocco della catena poiché anche tutti gli altri blocchi successivi dovrebbero essere a loro volta falsificati, ma appunto questa operazione di falsificazione di massa richiederebbe una potenza di calcolo altissima, smisurata.

La Blockchain viene aggiornata con un nuovo blocco ogni circa 10 minuti, grazie alla potenza di calcolo di migliaia di elaboratori che lavorano, anche senza sosta, per validare i blocchi che via via si aggiungono alla catena.

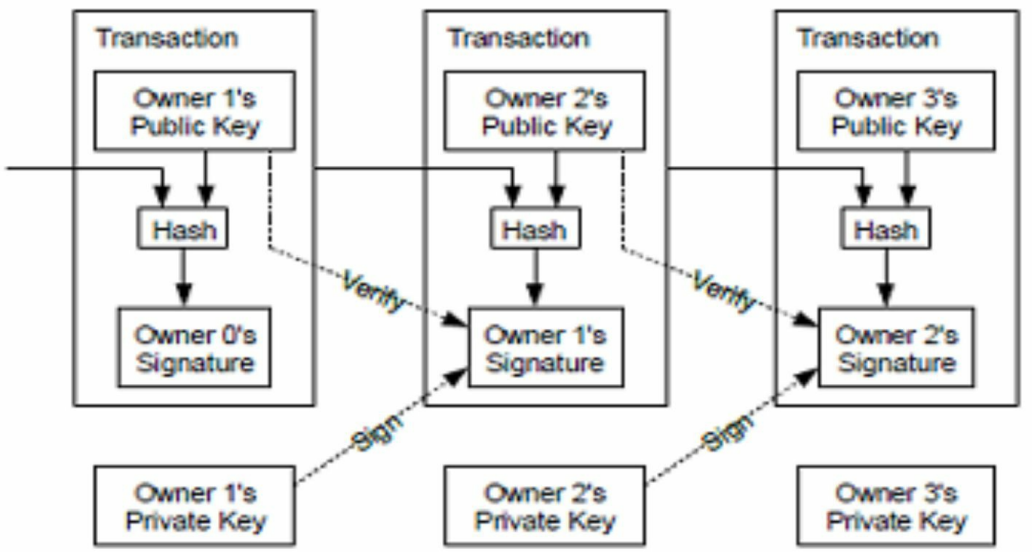
Statistiche aggiornate sulla Blockchain dei Bitcoin possono essere consultate sul sito Blockchain.info. Il 15/03/2018

risulta che un blocco della catena ha una dimensione media di 0,76 MB e che ogni giorno vengono confermate, mediamente, 199,192 transazioni; a tale data risultano già minati, ossia in circolazione nel sistema, quasi 17 milioni di Bitcoin, la Blockchain ha una dimensione che supera 160 GB, vi sono circa 1.500 transazioni a blocco nell'ultimo anno, circa 300.000 transazioni confermate al giorno, si superano i 25 milioni di TH/s di velocità complessiva del network facente mining e si contano quasi 24 milioni di utilizzatori di wallet, ossia portafogli virtuali.

Il sistema alla base dei Bitcoin è sicuro fintanto che la maggiore potenza

di calcolo è nelle mani di utenti onesti che minano senza sovvertire la natura delle cose.

La Blockchain che è alla base del Bitcoin, come da documento ufficiale di Satoshi Nakamoto, è schematizzabile nel seguente modo:



Il grafico mostra che ciascun possessore di Bitcoin può trasferire moneta a un beneficiario firmando digitalmente, con

la propria chiave privata, l'hash della transazione precedente e la chiave pubblica del beneficiario. Si andrà così ad aggiungere un blocco alla fine della catena. Le firme digitali coinvolte in questo processo possono essere sempre verificate al fine di verificare la validità del passaggio di proprietà della criptomoneta, trasferimento che deve essere sempre disposto da un utente che ne sia davvero possessore. Il beneficiario di un pagamento può, quindi, verificarlo effettuando un controllo sulle firme digitali, che consente di verificare la validità dei passaggi di proprietà della criptovaluta.

I blocchi

Come accennato, il blocco è l'elemento fondamentale della Blockchain, dove vengono incluse le transazioni che tracciano le movimentazioni di denaro digitale tra nodi.

Ogni blocco è composto da un "header" e da un "body" che contiene le transazioni. L'header presenta i seguenti campi:

- Versione
- PrevHash
- Merkle root
- Timestamp
- Bits
- Nonce

- Numero di transazione

Come si evince dalle denominazioni, l'header ha una funzionalità di identificazione e caratterizzazione del blocco. Il campo "Versione" indica il numero di versione del software impiegato, il campo "PrevHash" contiene l'hash del blocco precedente, il campo "Merkle root" contiene un hash calcolato in funzione degli hash delle transazioni contenute nel blocco, il campo "Timestamp" si riferisce all'ultima transazione del blocco, il campo "Bits" contiene il valore di riferimento, o valore target, utilizzato per calcolare l'hash del blocco, intendendo l'hash dell'header del blocco,

in modo tale che risulti minore del valore di riferimento, secondo la filosofia del problema computazionale che ha una difficoltà praticamente sempre crescente con il tempo, con un valore di riferimento che diviene sempre più piccolo con gli anni, mentre il campo "Numero di transazione" contiene, appunto, il progressivo della transazione.

Una attenzione particolare va prestata al campo "Nonce", di 8 byte, che è fondamentale per il processo computazionale che conduce alla soluzione del problema matematico alla base del mining: il *nonce* è un numero progressivo che va aggiunto in loop alla stringa di base, di partenza per il

calcolo, al fine di trovare l'hash che risulti minore del valore di riferimento, come si vedrà più avanti nella trattazione.

Ogniqualvolta un blocco viene validato dai minatori, viene assegnato un premio la cui entità viene dimezzata ogni circa 4 anni, precisamente ogni 210.000 blocchi validati; il premio previsto nel 2012 era di 50 bitcoin/blocco ed è poi passato a 25 bitcoin/blocco per infine ridursi al valore attuale di 12,5 bitcoin/blocco.

Questo dimezzamento programmato del premio prende il nome di *Halving* e porterà, nel 2140, ad un premio di un solo bitcoin/blocco. A partire da tale

anno non sarà più possibile fare mining poiché si sarà raggiunto il numero massimo previsto di Bitcoin circolanti nel sistema, pari a circa 21 milioni.

Il timestamp

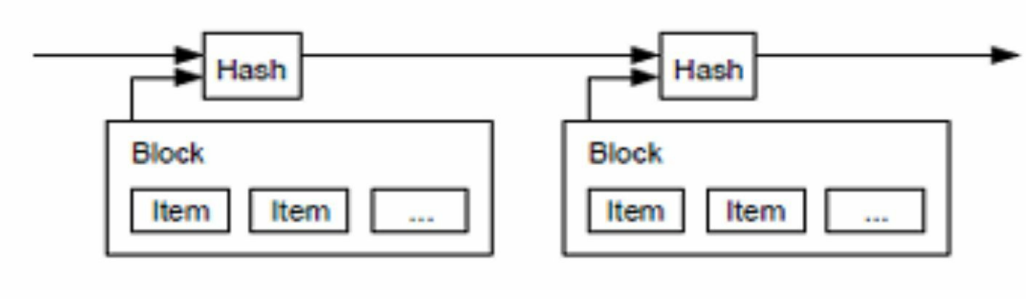
In una struttura come quella poc'anzi descritta, il problema del double-spending si risolve senza l'ausilio di un Istituto centrale da cui scaturisca la moneta, rischioso proprio per il potere centralizzato che avrebbe, al pari delle banche che tanto si criticano; si risolve con il fatto che la maggior parte dei nodi partecipanti al sistema, supposti onesti, approvi una certa transazione come la prima e quindi come l'unica valida in caso di ripetizioni all'interno della Blockchain.

Per meglio capire il concetto bisogna considerare che, se si presentassero due transazioni per lo stesso pagamento, la

prima sarebbe considerata l'unica valida, pertanto sarà la maggioranza dei nodi a decidere quale sia la prima, ossia quella valida. Il beneficiario di un certo pagamento saprebbe, così, che i precedenti possessori di Bitcoin non hanno firmato transazioni precedenti a quella in considerazione, ossia che il pagamento in essere non è già stato validato in precedenti transazioni della Blockchain.

Per raggiungere lo scopo di ordinare temporalmente le transazioni, si fa uso di una marcatura temporale, che viene anche utilizzata per la computazione che è alla base del mining. Si può partire dal seguente schema, tratto sempre dal documento ufficiale di Satoshi

Nakamoto:



Il grafico mostra due dei blocchi che hanno avuto vita nella Blockchain. Il timestamp viene applicato sull'hash di ciascun blocco, e il suo hash, che contiene anche il precedente timestamp, viene pubblicato secondo una successione.

In pratica, si crea una catena di hash, in cui ciascun elemento contiene sia il timestamp del blocco a cui si riferisce, sia il timestamp del blocco precedente, e questo implica che, indirettamente, contenga un'informazione che ingloba

tutti i timestamp precedenti, di fatto aumentando in tal modo la sicurezza del tutto; cambiare illecitamente un timestamp del passato farà sì che vi sia un'incongruenza con i timestamp successivi e che quindi un controllo di validità scopra agevolmente il problema scongiurando il fatto che l'intero sistema possa venire compromesso.

Capitolo 5: il mining

Mining è un termine anglosassone che indica l'azione dell'estrazione, con riferimento al minare nelle cave che porta alla luce oggetti preziosi. Nel caso di Bitcoin, il mining consente di estrarre moneta digitale in senso lato, in quanto si dovrebbe parlare più precisamente di creazione di moneta e di ricompensa per chi ha contribuito a tale compito.

Il mining richiede una enorme complessità di calcolo distribuita, in cui singoli elaboratori, ma soprattutto pool di elaborazione costituiti da centinaia e anche migliaia di computer, eseguono

calcoli matematici di una certa complessità al fine di trovare una soluzione ad un problema matematico in cui si fa uso della crittografia di stringhe.

Secondo un principio che non prevede restrizioni, chiunque può scaricare in locale la Blockchain, ossia l'intero registro delle transazioni in Bitcoin, e mettere a disposizione il proprio hardware computazionale per i calcoli crittografici alla base della creazione di nuova criptomoneta.

Chi fa mining riceve una ricompensa in Bitcoin proporzionale alla sua capacità di calcolo, alla velocità con cui l'hardware di cui dispone è in grado di effettuare i calcoli complessi richiesti

dall'algoritmo in gioco, che prevede come computazione più onerosa quella del calcolo di funzioni hash.

La ricompensa del mining si basa su due pilastri di fondamentale importanza per come è stato concepito il sistema Bitcoin e, più in generale, per come sono state concepite tutte le cripto-valute:

- lavoro reale;
- equità della ricompensa.

Il lavoro è l'elemento cardine che rende il mining una vera e propria attività in cui investire molto tempo e risorse.

A differenza del trading, che richiede

sì un certo impegno e quindi una certa forma di lavoro, ma che si basa sui guadagni sul cambio, cosa che ha una buona componente speculativa, il mining si basa sul lavoro che un individuo dovrebbe svolgere per mettere su un sistema computazionale capace di tenere il passo con i tempi; un lavoro a tutti gli effetti, assimilabile a quello imprenditoriale, che richiede anche particolare attenzione riguardo ai costi da sostenere, che sono dovuti non solo al necessario acquisto di hardware potente, piuttosto costoso, ma anche all'energia elettrica necessaria a tenere acceso tale hardware 24 ore al giorno, tutti i giorni.

Il costo della corrente è infatti un

parametro fondamentale per il calcolo rendimento/costi, rappresenta un punto di attenzione cruciale per chi intende fare mining a livello professionale senza farsi ingannare dai facili guadagni che non tengono conto delle spese sostenute. Il contratto di fornitura elettrica di casa difficilmente farà al proprio caso e sarà molto probabilmente necessario stipulare un contratto con costo al kWh più basso, cosa per niente facile se, ad esempio, non si dispone di un'azienda che è in grado di stipulare con qualche compagnia elettrica contratti molto convenienti in questo senso. Il successo del mining è, quindi, anche una questione di centesimi di euro al kilowattora.

Tutto ciò si sposa con il concetto di equità della ricompensa. In sostanza, più si impiegano risorse adeguate e ci si impegna nel lavoro di mining, maggiore sarà la probabilità di essere remunerati con Bitcoin. Sussiste un'aleatorietà di fondo nel mining, una incertezza del guadagno, anche mettendo per un attimo da parte la volatilità della criptovaluta, la continua variabilità del cambio rispetto ad altre monete reali. Tale incertezza sul numero di Bitcoin che si possono guadagnare è dovuta al fatto che la ricompensa viene data a chi risolve per primo un certo problema matematico che si basa per lo più sul calcolo il più possibile rapido di funzioni hash, e il

caso assume un ruolo cruciale in questo contesto.

La statistica, però, vuole che più le risorse a disposizione sono potenti dal punto di vista computazionale, e quindi più si investe nel mining, maggiori saranno le probabilità di *risolvere blocchi* e quindi di guadagnare ricompense. Bisogna, insomma, dimostrare di aver lavorato seriamente, in modo professionale, con hardware molto potente dal punto di vista computazionale, con apparecchiature costose accese tutti i gironi, 24 ore al giorno, che consumano molta corrente, se si vuol sperare di guadagnare in maniera soddisfacente facendo mining. La ricompensa, che rappresenta il più

grande incentivo al lavoro del mining, è, così, equa perché va a premiare chi si è sforzato di più in termini di tempo e di denaro investiti nell'impresa.

Oggi guadagnare facendo mining da soli e senza investimenti oculati, con il proprio PC o con hardware economico, è pressoché impossibile ed è diventato difficile anche reperire dei client per fare mining con il proprio computer per esercizio, per avvicinarsi alla tematica senza effettuare un investimento serio.

Mentre una volta, all'inizio della vita del Bitcoin, fare mining con il proprio, normale computer di casa era la norma, adesso è pressoché impossibile nella pratica, soprattutto se lo si fa in

solitaria; esiste infatti la possibilità di far partecipare il proprio computer o il proprio hardware ottimizzato ad un *pool*, ossia ad un insieme di macchine di calcolo che, sfruttando il vecchio detto "l'unione fa la forza", risolvono blocchi con una certa frequenza, spartendosi alla fine la ricompensa.

Partecipando ad un pool, si guadagnerà poco ma in modo piuttosto costante, proprio perché il complesso di hardware in gioco risulta essere molto più potente di un singolo elaboratore, ma dividere una ricompensa tra centinaia o migliaia di partecipanti porta a guadagni contenuti per ognuno; chiaramente, più si partecipa ad un pool "attrezzati", ossia con hardware potente,

maggiore sarà la propria parte di ricompensa, in quanto il premio in Bitcoin finale sarà distribuito in proporzione alla potenza di calcolo messa a disposizione da ciascuno.

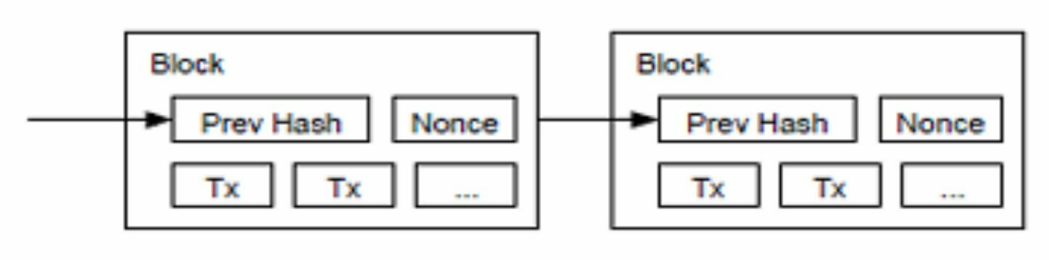
Spesso si consiglia, quindi, di rinunciare alla corsa ai Bitcoin in solitaria e di unirsi ad un pool, ma si tenga presente che, sovente, è anche richiesta una quota di partecipazione per far parte di una grande famiglia, quindi si dovrà avere a che fare con un altro costo da tenere in conto.

Proof-of-work

Come è stato poc'anzi accennato, non si può parlare di mining senza considerare il lavoro reale che c'è dietro; non si può parlare di mining senza introdurre il concetto di proof-of-work, ossia di "prova di lavoro", necessaria per ottenere ricompense in Bitcoin e quindi guadagni concreti dalla propria attività. È questo il famigerato problema matematico di cui si parlava, risolto il quale si ottiene la ricompensa prevista quale incentivo per il lavoro di mining.

Il seguente grafico, sempre tratto dal documento ufficiale di Satoshi Nakamoto, mostra il concetto di proof-of-work che è alla base del mining, o

almeno lo abbozza:



Come si evince, si lavora con funzioni hash e con il *nonce*, termine anglosassone che sta ad indicare "for the nonce", che può essere tradotto in Italiano come "per l'occasione"; si tratta di un numero che può essere utilizzato una sola volta, in genere casuale o pseudo-casuale, ossia generato da un algoritmo deterministico come una sequenza di numeri che presenta, approssimativamente, le stesse proprietà statistiche di una sequenza generata da un processo casuale.

La proof-of-work consiste nella

ricerca di una stringa il cui hash con algoritmo SHA-256 applicato due volte consista in un'altra stringa il cui valore numerico sia minore di un certo numero prefissato, di riferimento, che però varia in funzione della complessità del sistema a cui si è giunti in un certo momento.

La stringa di cui fare l'hash varierà in funzione del nonce, che andrà incrementato di una unità ad ogni passo. Da tutto questo derivano due considerazioni molto importanti:

- la ricerca del risultato giusto, che soddisfa la condizione, è empirica e richiede una grande potenza di calcolo proprio perché presuppone di procedere

"a tentativi", calcolando un numero spropositato di hash di stringhe in cui si varia, man mano, il *nonce* (e non solo, poiché cambia anche, quantomeno, il timestamp);

- il risultato giusto è per forza di cose un numero iniziante con un certo numero di zeri, proprio perché deve essere sufficientemente piccolo da essere minore di un numero che diventa via via più piccolo, all'aumentare della complessità del sistema.

Per capire a fondo la questione bisogna pensare a quello dei Bitcoin come ad un sistema che si "autoregola" nel tempo, che modula la complessità

della soluzione, e quindi della proof-of-work, in funzione della potenza computazionale complessiva che partecipa al sistema in un certo periodo di tempo. In sostanza: più l'hardware per fare mining diviene potente e più aumenta il numero di persone coinvolte nel progetto, più il numero di riferimento, tale che l'hash ne debba risultare minore, diverrà piccolo e quindi più difficile sarà trovare la soluzione al problema matematico, proprio perché più ristretto sarà il campo delle possibili soluzioni; viceversa, qualora il numero di minatori dovesse diminuire, o meglio qualora si abbassasse la capacità computazionale dell'hardware complessivamente in

gioco (circostanza, quest'ultima, per nulla realistica, almeno nel breve-medio periodo), il numero di riferimento diverrà sempre più grande e, per risolvere il problema matematico, basteranno così soluzioni con un minor numero di zeri, più facili da trovare.

La conseguenza di tutto ciò è che fare mining, con il passare del tempo, avrà statisticamente sempre la stessa difficoltà (chiaramente a meno di una varianza, di oscillazioni), perché da un lato, almeno fino ad ora, aumenta sempre la potenza computazionale complessiva, mentre dall'altro il problema matematico diventa sempre più difficile.

A livello di costi computazionali, la

difficoltà di trovare una soluzione al problema è esponenziale con il numero di zeri richiesti all'inizio della stringa del risultato. La verifica della validità del risultato, però, può essere fatta computando un singolo hash.

La conseguenza della proof-of-work nei termini suddetti è che, per malintenzionati, non è possibile modificare un blocco senza dover modificare di conseguenza anche i blocchi successivi. Considerando l'immane potenza di calcolo necessaria a dar vita ad un blocco, si intuisce l'enorme difficoltà di dovere dar vita nuovamente a tutti i blocchi successivi per ottenere una coerenza tale da far

tenere in piedi l'atto illecito.

A questo si aggiunge il fatto che la maggioranza che decide la validità della catena non è quella che opera dalla maggior parte degli indirizzi IP coinvolti, ma è quella che opera dalla maggior parte delle CPU coinvolte, la qual cosa porta ad una maggiore equità del sistema: mentre gli IP possono essere facilmente allocati per finalità illecite, è più difficile fare altrettanto con i processori, ossia con i "cervelli" informatici, in pratica con il costoso hardware che entra in gioco.

L'evoluzione dell'hardware per fare mining

Come esposto in precedenza, il vero problema del mining risiede nella utilizzabilità limitata di un certo hardware nel tempo, che spinge a dover fare i conti, riguardo ai guadagni possibili, facendo molta attenzione al costo delle apparecchiature che via via si acquistano per essere in linea con i tempi.

Semplificando un po', si può dire che i dispositivi elettronici che si acquistano oggi per fare mining, iniziano a diventare obsoleti già da domani e il continuo rinnovo degli stessi rischia fortemente di far andare addirittura in

perdita.

Per comprendere l'evoluzione dell'hardware per fare mining nel corso degli anni bisogna chiaramente introdurre il concetto di velocità; ebbene, questa si esprime in hash al secondo, ossia in numero di calcoli di funzioni hash che possono essere eseguiti ogni secondo e oggigiorno si parla perlopiù di decine di TH/s, ossia di Terahash al secondo, che esprimono decine di migliaia di miliardi di hash al secondo, in quanto 1 TH/s = 1.000.000.000.000 di hash al secondo, ossia mille miliardi di hash al secondo.

Il concetto di hash è fondamentale perché riguarda la complessità dell'algoritmo che va applicato per

validare i blocchi della Blockchain; in altre parole, la maggiore complessità computazionale di tale algoritmo consiste nel calcolo dell'hash di un certo insieme di dati, precisamente di un hash di un hash, come si vedrà approfonditamente in seguito.

Oggi è possibile fare mining in modo molto più efficiente che in passato e la capacità computazionale di cui può disporre un singolo minatore è di gran lunga superiore a quella di un decennio fa, quando la diffusione del Bitcoin era agli albori.

All'inizio era sufficiente utilizzare il proprio computer personale per guadagnare Bitcoin attraverso il mining, ma ben presto le cose cambiarono e si

passò, con relativa velocità, all'utilizzo di chiavette USB con circuiteria dedicata al tipo di calcolo richiesto, da dover collegare al computer, molto comode perché autoalimentate, senza cioè la necessità di alimentarle con un dispositivo elettronico esterno, ad hoc, che sarebbe stato costoso ed ingombrante.

Con le CPU (Central Processing Unit, ossia unità di elaborazione centrale) dei computer si potevano raggiungere velocità di pochi MH/s, ossia di pochi milioni di hash al secondo, mentre con le GPU (Graphics Processing Unit, unità di elaborazione delle schede grafiche) di fascia alta si potevano raggiungere velocità intorno ad 1 GH/s, ossia ad un

miliardo di hash al secondo.

Le chiavette USB, invece, consentivano velocità di computazione dell'ordine di decine di GH/s, ossia di decine di miliardi di hash al secondo.

Pian piano le chiavette USB divennero obsolete e si passò all'FPGA, acronimo di *Field Programmable Gate Array*, ossia ad hardware programmabile, e agli ASIC che tutt'oggi si utilizzano. In questo caso, come detto, le capacità in gioco sono dell'ordine di decine di TH/s.

Oggi, se si è alla ricerca di hardware adatto a fare mining con un certo margine di guadagno, si possono consultare alcuni siti Web che mostrano

i ricavi da mining possibili in funzione dell'hardware utilizzato e del costo della corrente elettrica che si è costretti a pagare. Tra questi vi è il sito *NiceHash* che offre, gratuitamente e senza necessità di registrazione, una *profitability calculator* in grado di far capire bene dove si andrebbe a parare utilizzando questa o quella macchina computazionale per fare mining di criptovalute e, in particolare, di Bitcoin.

Per accedere a tale funzionalità basta andare nella sezione del sito "For sellers", istituita appunto per vendere potenza computazionale e guadagnare così Bitcoin o altra criptovaluta con il proprio hardware a disposizione, che può essere un semplice computer, una

semplice scheda video, un complesso hardware dedicato ASIC oppure una vera e propria farm che contempla un insieme di elaboratori.

Nel caso più semplice si può selezionare il riquadro "I want to earn with my CPU or GPU", riferito appunto ad una potenza di calcolo di un computer (CPU) o di una scheda video (GPU).

Selezionando, ad esempio, la suddetta voce, si arriverà ad una pagina in cui si potrà cliccare sul bottone "Calculate profitability" che richiamerà, appunto, la pagina della calcolatrice di stima profitto.

Selezionando, invece, la voce "I want to earn with my ASIC machine", si arriverà ad una pagina in cui si potrà

cliccare sul link "Calculate the profitability of your miner" che richiamerà la stessa pagina della calcolatrice di stima profitto vista in precedenza.

Le stime di NiceHash, aggiornate in automatico più volte al giorno, sono ritenute abbastanza attendibili e possono essere visualizzate in modo molto semplice, ma vi è un punto di attenzione molto importante per non essere fuorviati dai risultati mostrati: questi, purtroppo, non sono sempre relativi ad una data criptovaluta di interesse, il che è anche logico visto che non è possibile impostare la criptovaluta nei vari menù a tendina che vengono mostrati, ma

dipendono da quello che il sistema, in automatico, ritiene essere l'algoritmo di hash, o un insieme di algoritmi di hash, migliore per fare mining con l'hardware dato. Questo può essere visto nel grafico a semicerchio e nei riquadri relativi agli algoritmi visibili verso fine pagina.

A livello pratico, se ad esempio si imposta un calcolo sulla base di una potenza di calcolo basata su una CPU o su una GPU, quel che si ottiene è una stima dei guadagni non per il mining di Bitcoin, ma per il mining di altre criptovalute indicate in basso nella pagina dei risultati. Questo è dovuto al fatto che il sistema ritiene i guadagni da mining di Bitcoin effettuati con CPU o GPU assolutamente irrilevanti, prossimi

a zero, e quindi propone, in modo forse un po' criptico, una stima per altri algoritmi, diversi dall'SHA-256 che è utilizzato dai Bitcoin (e non solo), che vengono utilizzati per altre criptovalute. A confondere ulteriormente le idee vi è il fatto che le stime di guadagno vengono presentate comunque in Bitcoin, anche se tali guadagni si riferiscono al mining di altre criptovalute.

Quel che si deve fare, quindi, per ottenere stime di guadagni relative soltanto al mining di Bitcoin, è farsi una cultura provando diverse soluzioni di hardware e verificare che i guadagni stimati si riferiscano proprio alla crittovaluta Bitcoin e non ad altre.

Per fare qualche esempio pratico, si deve innanzitutto impostare il costo della corrente in kWh, in Euro o in altra valuta, e selezionare un "device", ossia l'apparato di calcolo da utilizzare.

A titolo di esempio, si possono impostare l'hardware "Intel CPU i7-7700K @ 4.70GHz", ossia un computer Intel piuttosto potente, di ultima generazione, e un costo della corrente di 0,20 euro a kWh, che rappresenta un valore di costo tipico per un consumo da parte dell'utenza di un privato, ottenendo come risultato, per il giorno 12/03/2018, un rendimento di 0.00092416 BTC al mese, che corrispondono a 6,88 EUR; praticamente briciole considerando un tasso di cambio Bitcoin/Euro costante,

ma comunque qualcosa che potrebbe costituire un guadagno ancora peggiore in caso di futuro cambio più sfavorevole, o migliore, impossibile sapere di quanto, in caso di una nuova impennata del valore del Bitcoin rispetto alle monete tradizionali.

Facendo un altro esempio per mostrare che le differenze possono essere notevoli anche se si usa un semplice computer domestico, se si imposta l'hardware "AMD CPU Ryzen 7 1700X @ 4.00GHz", si ottiene invece, come risultato, un guadagno stimato mensile di 0.00117464 BTC, corrispondenti a 8,75 EUR; sempre pochi, ma superiori al caso precedente, la qual cosa fa

riflettere sul fatto che l'architettura di un computer AMD di questo tipo si presta maggiormente al mining di quanto lo faccia quella di un computer Intel come quello sopra descritto, con il prezzo del computer AMD in genere inferiore a quello del computer Intel.

Si noti che entrambi i tipi di hardware, come sopra accennato, non sono più idonei a fare mining di Bitcoin e pertanto le suddette stime si riferiscono all'impiego per il mining di altre criptovalute. Generalizzando la questione, diversi tipi di hardware si comportano in modo diverso in funzione della criptovaluta che si intende minare. Eclatante è il caso dell'Ethereum che si

può ancora minare con le GPU delle schede grafiche, mentre tali schede risultano essere oggi inutilizzabili, nella pratica, per il mining di Bitcoin. In alcuni casi, nemmeno tanto rari, può anche capitare che a fare mining si vada in rosso, in perdita perché il costo della corrente supera il rendimento che si otterrebbe minando una certa criptovaluta con l'hardware a disposizione.

Se si cambia decisamente tipo di hardware e si passa ad un ASIC, le cose cambiano molto; selezionando, come device, "BITMAIN AntMiner S9", il più potente ASIC attualmente in commercio per fare mining di Bitcoin, con una

velocità di calcolo di 14 TH/s, ossia 14 Terahash (14 mila miliardi di hash) al secondo, il risultato della stima del guadagno sarà di 0.00804912 BTC al mese, ossia di 59.95 EUR/mese; ancora poco, ma molto di più che se si usasse un normale computer che, come detto, risulta essere ormai del tutto obsoleto per il mining di Bitcoin. Usando una farm di AntMiner S9, acquistabili perlopiù dalla Cina e non senza fatica, i guadagni potrebbero diventare importanti, ma andrebbero ponderati in funzione del costo di tale hardware, a cui si aggiunge, molto spesso, anche quello doganale dovuto all'importazione da Paesi extra UE.

Per fare un ultimo esempio, che può essere interessante per capire come si può affrontare il mondo delle criptovalute andando oltre i Bitcoin, si può impostare, come device, "BITMAIN AntMiner L3+", un ASIC con velocità di calcolo di "appena" 504 MH/s, ossia 504 Megahash (504 milioni di hash) al secondo, ed ottenere come risultato un guadagno mensile stimato di 0.01414715 BTC, corrispondenti a ben 107,07 EUR. È interessante sapere che, pochi mesi fa, il valore del guadagno stimato si attestava sui 1.000 euro, 10 volte più di oggi, ma appunto, come sottolineato più volte, con il tempo diventa sempre più difficile fare mining con successo utilizzando lo stesso hardware.

Scorrendo la pagina del risultato, si noterà che l'algoritmo di hash di riferimento è lo Scrypt, utilizzato dalla criptovaluta Litecoin, una delle più celebri assieme ad Ethereum.

Si noti, infine, che a complicare le cose, come un po' si è accennato nella trattazione, vi è anche il fatto che il guadagno stimato in Euro, in tutti i casi, deriva dal guadagno stimato in Bitcoin e tra i due c'è di mezzo un cambio molto instabile, con tassi molto mutevoli, pertanto il guadagno stimato potrebbe portare, anche in un futuro non molto lontano, ad un "guadagno automaticamente aggiustato" maggiore o minore di quello stimato sul momento, sulla base del cambio che vigerà al

successivo momento della vendita di Bitcoin per ottenere Euro. La conseguenza di questo è che, anche con pochi Bitcoin in tasca, si potrebbe in futuro guadagnare molto, ma è vero anche il viceversa, ossia che, anche con molti Bitcoin in tasca, si potrebbe in futuro guadagnare poco, se non addirittura andare in perdita.

Come acquistare il miglior miner ASIC per Bitcoin

Purtroppo non esiste il miglior miner ASIC per Bitcoin in senso assoluto poiché bisogna tenere in considerazione il costo dell'hardware nel momento in cui si valuta l'acquisto, nonché la sua efficienza, sempre in tale momento. Al passare del tempo, infatti, cambia molto sia il prezzo dell'hardware per fare mining, sia la sua capacità di dare vita ad un rendimento, tanto per cominciare perché la complessità del problema crittografico tende sempre più ad aumentare col tempo; entrambi i parametri si abbassano e occorre valutare di volta in volta quale apparato

elettronico è in grado di fornire il miglior rapporto prestazioni/costo.

Indicativamente, a marzo 2018, l'AntMiner S9 risulta essere un ASIC funzionale per i Bitcoin, me del resto, senza mettere su una farm, con tutti i rischi del caso, e senza partecipare ad un pool, è veramente difficile riuscire a guadagnare con un certo ottimismo.

Ciò premesso, riassumendo, le più importanti caratteristiche di un hardware dedicato al mining, da tenere sempre in considerazione per la propria scelta, fanno riferimento ai seguenti parametri:

- Hash rate, che determina la velocità computazionale dell'hardware, espressa in hash (o multipli) al secondo, un

parametro quindi direttamente proporzionale alla quantità di Bitcoin estraibile in un certo intervallo di tempo.

- Efficienza, che determina il numero di Bitcoin estraibili rapportato al costo da dover sostenere per l'estrazione durante il funzionamento dell'hardware, in sostanza quello della corrente elettrica, che è tutt'altro da trascurare; il consumo di corrente è fondamentale e potrebbe portare a preferire un certo hardware più lento, che offre un minor hash rate, ma che consuma molto meno quando sotto corrente. Per questo motivo, a volte, nei siti Web dei produttori o dei commercianti di hardware per il mining

si fa riferimento alla capacità di conversione di energia elettrica in Bitcoin (tot consumo di energia elettrica porta a tot Bitcoin) per esprimere l'efficienza.

- Prezzo che, indubbiamente, può far scartare alcuni ASIC ritenuti troppo costosi e quindi a maggior rischio di perdita del capitale da investire nel mining. Assieme al prezzo vivo dell'hardware andrebbe considerato anche l'eventuale costo dovuto all'importazione da Paesi che prevedono dazi doganali e l'eventuale costo di riparazione dell' hardware in caso di guasti o di sostituzione dell'hardware in caso di ricezione al proprio domicilio di

un apparecchio difettoso o addirittura rotto.

- Qualità e tempo di vita medio dell'hardware, che, valutati assieme al prezzo, risultano imprescindibili se si vuol fare qualche previsione sensata sui guadagni da mining di Bitcoin.

Capitolo 6: algoritmi di hash e brute force

In generare, è possibile applicare una funzione hash che "trita" una certa stringa, ossia che, partendo da una certa stringa, fornisce per risultato una nuova stringa tale che non sia possibile effettuare una computazione al contrario, che restituisca la stringa originale a partire da quella ricavata mediante hash.

Gli algoritmi di hash sono fondamentali anche a prescindere dalle criptovalute e infatti su di essi si basano meccanismi di sicurezza imprescindibili

nel mondo informatizzato odierno. Vengono utilizzati, ad esempio, per garantire la sicurezza delle password di accesso a sistemi informatici.

Un esempio interessante di algoritmo di hash è quello dell'MD5, che è stato utilizzato in modo massivo per la protezione delle password dei siti Web. In sostanza, quando un utente effettua un login, una autenticazione inserendo la password, il sistema, la pagina Web dedicata all'autenticazione, nello specifico, calcola la funzione hash MD5 della password inserita nella mascherina e la confronta con la stringa memorizzata nel database che, come è intuibile, consiste appunto nell'MD5 della password calcolato al momento

della registrazione dell'utente. In questo modo, anche se un malintenzionato riuscisse a ricavare la password "tritata" che è custodita nel DB, non riuscirebbe a risalire alla password che dovrebbe inserire nella mascherina per accedere al sistema come un normale utente.

Il fulcro della questione quando si parla di funzioni hash è quindi quello di rendere difficilissimo il processo di individuazione di stringhe a ritroso, scongiurando così il furto di dati sensibili o perlomeno estremamente riservati quali quelli delle password e quelli che scaturirebbero da accessi illeciti a sistemi informatici una volta note tali password; è difficilissimo, ma

non impossibile, in quanto una grande potenza di calcolo, appunto, può far emergere le "stringhe segrete" mediante attacchi *brute force*.

In sostanza, con attacchi di *forza bruta*, dei malintenzionati possono provare a ricavare i dati di interesse provando una miriade di stringhe in input ricavate come combinazioni di lettere il più possibile "esaustive", che coprano cioè lo spazio di tutti gli input possibili nel migliore dei modi.

Le prove consistono nel confrontare gli hash delle stringhe passate al setaccio in input con l'hash di partenza, tipicamente quello memorizzato in un database, e il processo, chiaramente, si interrompe quando si perviene ad un

hash di uno degli input passati al setaccio che dà per risultato proprio l'hash di partenza; tale input rappresenta la soluzione al problema, la stringa segreta individuata a ritroso, tipicamente una password, ma non solo.

Proprio per questa possibilità di riuscire a procedere empiricamente a ritroso, il su citato algoritmo di hash MD5, considerato molto valido al momento della sua introduzione, ha avuto un incontrastabile declino nel corso del tempo, poiché la potenza computazionale via via superiore dell'hardware in commercio ha fatto sì che si riuscisse ad eseguire gli hash molto velocemente e quindi, di conseguenza, che si riuscisse a ricavare

le stringhe di partenza a partire da innumerevoli combinazioni di caratteri per stringhe in input.

Tutto ciò mette in luce l'esigenza di limitare il più possibile la "semplicità" di calcolo degli hash, o meglio la "semplicità" di calcolo, in generale, per arrivare ad un certo risultato, anche forzatamente mediante complicazione delle condizioni da soddisfare per risolvere un certo "problema matematico" come accade per le crittovalute.

Nel caso specifico dei Bitcoin, la funzione di hash utilizzata è l'SHA-256, molto più onerosa dal punto di vista computazionale rispetto all'hash dell'MD5; in questo caso, tra l'altro,

l'hash viene calcolato due volte, ossia si deve computare l'hash di un hash per arrivare al risultato. SHA, per inciso, sta per *Secure Hash Algorithm* e rappresenta una tipologia di funzioni crittografiche di hash che sono state introdotte dalla National Security Agency a partire dal lontano 1993.

Inoltre, per i Bitcoin, la "semplicità" di calcolo degli hash, o ancora meglio la complessità del calcolo viene modulata in funzione dell'andamento della potenza computazionale nel tempo, in modo tale da rendere più difficile o più facile la soluzione rispettivamente all'aumentare o al diminuire della potenza di calcolo distribuita, ossia all'aumentare o al diminuire sia del numero di nodi, e

quindi di utenti che fanno mining, sia, soprattutto, della potenza computazionale del nuovo hardware che man mano viene immesso sul mercato, attualmente costituito da ASIC sempre più veloci.

In sostanza, come già accennato in precedenza e come si approfondirà in seguito, il sistema dei Bitcoin prevede che il risultato di un dato calcolo complesso sia minore di un certo numero che diventa sempre più piccolo all'avanzare del tempo; la brute force che consente di trovare una certa soluzione, quindi, richiederà tempi sempre più lunghi a parità di potenza di calcolo.

Crittografia e Bitcoin

Guardando al sistema dei Bitcoin in modo un po' più rigoroso, si può iniziare a dire che una *funzione crittografica di hash* consiste in un algoritmo che processa in input una stringa di qualunque lunghezza e restituisce in output una stringa di lunghezza prefissata. In altre parole, dato un messaggio m in input, con $h(m)$ si indica l'hash che, in genere, in pratica, comprime l'input in una nuova stringa più corta. Si parla anche, in questi casi, di *digest di messaggio*, in relazione all'output.

Risulta intuitivo che, vista la compressione che può aver luogo, una

funzione crittografica di hash può dar vita a *collisioni*, ossia allo stesso output a partire da input diversi. Affinché una funzione di questo tipo generi degli output davvero utili è necessario che il numero di collisioni sia minimo; in casi limite, se vi fossero moltissime collisioni, infatti, basterebbe un attacco brute force con pochi input , con un numero ridotto di stringhe in ingresso, ossia un attacco ad alta velocità, per ottenere presto il risultato consistente in uno dei possibili messaggi in input.

Nel frangente dei Bitcoin, la suddetta condizione si somma ad altre, importanti condizioni di cui deve godere una funzione crittografica di hash per essere davvero definita tale. Queste,

complessivamente, sono:

- resistenza alle collisioni forte, come spiegato poc'anzi ma in modo più restrittivo: dati due messaggi $m1$ e $m2$, diversi tra di loro, deve essere sempre impossibile che $h(m1) = h(m2)$, qualunque siano i messaggi;

- unidirezionalità input-> output, ossia non deve essere possibile applicare un algoritmo che, partendo dall'output, restituisca l'input; se con un certo m in input si ottiene in output $h(m) = o$, allora non deve essere possibile ricavare una funzione f tale che $f(o) = m$;

- l'hash $h(m)$ deve essere calcolabile

sempre rapidamente per qualunque *m* in input.

A tutto ciò si aggiunge il concetto di robustezza dell'algoritmo in termini di impredicibilità dell'input a partire dall'output, ossia la capacità dell'algoritmo di dar vita ad output completamente diversi , ossia che differiscono, carattere per carattere, in modo casuale, almeno all'apparenza, anche se in input vengono processati messaggi "simili", che consistono in stringhe che magari differiscono per un solo carattere.

Riguardo al sistema dei Bitcoin, nell'ottica appena esposta, applicare la funzione hash SHA-256 a due messaggi

che differiscono solo per un carattere porterebbe a risultati completamente diversi, come nel seguente esempio:

SHA256("test bitcoin 1") =
2520f75da07e9635975ab52b5ffdbcb6bfa

SHA256("test bitcoin 2") =
d6e2eba4c73d2c25f52ff5b64246aa9c02

Si vede chiaramente che, nonostante i due messaggi in input estremamente simili, i due risultati differiscono tra loro a tal punto che, partendo da uno dei due e conoscendo l'input dell'altro, non è possibile "indovinare" il relativo input, non è possibile violare la unidirezionalità di cui sopra; se, ad

esempio, si parte dal secondo risultato (d6e2eba4c73d2c25f52ff5b64246aa9c02 e si sa che l'input del primo risultato (2520f75da07e9635975ab52b5ffdbcb6b è pari a "test bitcoin 1", non c'è modo di sapere che l'input del secondo risultato è pari a "test bitcoin 2", data appunto l'estrema "diversità" dei due output.

Come accennato in precedenza, nel sistema dei Bitcoin la funzione crittografica di hash si applica due volte, ossia va eseguito un calcolo del tipo:

$$\mathrm{SHA256}(\mathrm{SHA256}(m))$$

la qual cosa aumenta il costo computazionale del calcolo e, al

contempo, aggiunge sicurezza in termini di non invertibilità della funzione complessiva che quindi porta ad un risultato a partire dal quale non è possibile calcolare agevolmente il messaggio in input.

La crittografia, nel sistema dei Bitcoin, consente di garantire la sicurezza delle transazioni, la non doppia spendibilità e la possibilità di effettuare pagamenti solo se si è legittimi proprietari di Bitcoin, scongiurando cioè la possibilità di spendere denaro di altre persone.

A parte questo, la crittografia, come accennato in precedenza, può essere utilizzata per mettere al sicuro il proprio

wallet, il proprio portafogli digitale che è necessario per gestire ed utilizzare i Bitcoin. Crittografando i dati del proprio portafogli si può scongiurare il rischio di furto dati che, in questo contesto, si tradurrebbe in un furto di Bitcoin.

Nel sistema dei Bitcoin la crittografia deve garantire i seguenti principi:

- autenticazione, ossia la certezza dell'identità del beneficiario in quanto reale destinatario del pagamento;

- integrità, ossia la validità del pagamento e quindi delle transazioni che vengono man mano inserite nella Blockchain;

- non ripudiabilità, ossia l'impossibilità, per il soggetto pagante, di disconoscere il suo pagamento. Ogni transazione, nel sistema Bitcoin, è incontrovertibile e definitiva.

L'algoritmo che viene utilizzato nel sistema Bitcoin per la firma digitale, che serve a validare le transazioni, è l'ECDSA, una implementazione dell'algoritmo DSA, acronimo di *Digital Signature Algorithm*, sviluppato nel 1991 dall'NSA, acronimo di *National Institute of Standards and Technology*.

Il sistema dei Bitcoin garantisce, così, la trasparenza riguardo alle transazioni, che vengono salvate nella Blockchain in

modo tale che chiunque possa vedere i passaggi di mano della moneta. Ogni volta che vi è un pagamento, una transazione ha vita con la firma digitale dell'hash della transazione precedente, pubblicata, appunto, nella Blockchain.

In questo frangente non è, quindi, possibile modificare una transazione già presente nella Blockchain, poiché, così facendo, cambierebbe l'hash del blocco corrispondente e quindi occorrerebbe cambiare anche tutti gli altri blocchi successivi, che erano stati calcolati ciascuno in funzione dell'hash del blocco precedente.

Chiave pubblica e chiave privata

Prima o poi, quando si cerca di capire il meccanismo su cui si basa la crittovaluta Bitcoin, ci si imbatte inevitabilmente nei concetti di chiavi crittografiche. La chiave pubblica e la chiave privata sono, infatti, concetti cardine di un sistema basato su crittografia e, in pratica, in generale, permettono lo scambio di messaggi riservati tra diversi soggetti, garantendo la segretezza di tali messaggi nei confronti di soggetti terzi che ne avessero accesso.

In sostanza, la problematica si pone qualora il canale di comunicazione sia ritenuto non sicuro e quindi si debba

tenere in conto la possibilità che un certo messaggio venga intercettato da un soggetto che non ne sia destinatario.

Partendo dal principio, esistono due tipologie di cifratura e, quindi, conseguente decifrazione: a chiave simmetrica e a chiave asimmetrica o pubblica; la prima tipologia consente di cifrare e decifrare messaggi mediante l'utilizzo di una chiave che viene trasmessa su un canale sicuro, diverso da quello lungo cui viene trasmesso il messaggio, che è ritenibile non sicuro, mentre la seconda tipologia consente di cifrare e decifrare messaggi mediante l'utilizzo di una chiave pubblica e di una chiave privata che, da un certo punto di

vista, lavorano in modo complementare.

La crittografia a chiave pubblica, impiegata nel sistema dei Bitcoin, supera l'ostacolo della necessaria esistenza di un canale sicuro utilizzabile per fornire la chiave segreta al destinatario del messaggio in piena sicurezza, affinché egli possa utilizzarla per decifrare il messaggio. Infatti, la crittografia a chiave pubblica prevede che un messaggio cifrato con la chiave pubblica possa essere decifrato solo con la chiave privata e viceversa, ossia che un messaggio cifrato con la chiave privata possa essere decifrato solo con la chiave pubblica.

Più precisamente, l'utilizzo dei Bitcoin è regolato da due chiavi: una chiave

privata, generata casualmente, ed una chiave pubblica da essa ricavata per applicazione di una funzione crittografica unidirezionale, quindi non invertibile. Riguardo all'utilizzo di tali chiavi, viene, in pratica, calcolato un hash dell'indirizzo virtuale del beneficiario di pagamenti, che rappresenta la chiave pubblica che consente di ricevere Bitcoin, mentre la chiave privata viene utilizzata per firmare le transazioni che testimoniano il passaggio di denaro tra diversi proprietari.

Va da sé che, mentre la chiave privata deve rimanere sempre segreta e non va quindi mai comunicata ad altri, la chiave pubblica, per ricevere Bitcoin, dovrà

essere comunicata almeno a chi, man mano, intende effettuare dei pagamenti a proprio favore, se non proprio pubblicata. In teoria, gode della massima sicurezza e del massimo anonimato chi non ha mai ricevuto nemmeno un pagamento in Bitcoin poiché, plausibilmente, non ha avuto la necessità di diffondere la sua chiave pubblica e continua a mantenerla segreta al pari della sua chiave privata.

Il processo di generazione della chiave pubblica a partire dalla chiave privata mediante apposito algoritmo crittografico è fondamentale, in quanto le due chiavi hanno la capacità di garantire comunicazioni sicure su un canale in linea di principio non sicuro. Il

mittente del messaggio dovrà cifrarlo utilizzando la chiave pubblica del destinatario, il quale potrà decifrarlo usando la propria chiave privata.

Si può concepire la cosa al contrario e cifrare, nel ruolo di mittente, un messaggio con la propria chiave privata per poi inviarlo al destinatario, il quale potrà decifrarlo con la chiave pubblica del mittente; in questo caso non si fa altro che applicare una firma digitale con lo scopo di dimostrare che il mittente ha inviato tale messaggio che, nello specifico dei Bitcoin, si traduce nello scopo di dimostrare la validità dei pagamenti e quindi delle transazioni che confluiscono nella Blockchain.

Per il sistema Bitcoin, l'algoritmo in

questione, che viene utilizzato per l'impiego della firma digitale, è quello che viene identificato dalla sigla ECDSA, ossia *Elliptic Curve Digital Signature Algorithm*, che garantisce una sicurezza analoga a quella del celebre algoritmo RSA, così denominato dalla iniziali dei cognomi degli ideatori che ne descrissero le caratteristiche nel 1977: Ron Rivest, Adi Shamir e Leonard Adleman.

Firma digitale e transazioni

Come esposto in precedenza, la firma digitale, nel sistema Bitcoin, serve a validare transazioni, ossia ad accertare che i passaggi di mano del denaro siano stati effettuati lecitamente a partire da soggetti che ne avevano davvero disponibilità.

Per i Bitcoin, l'algoritmo utilizzato per applicare la firma digitale è, come poc'anzi accennato, l'ECDSA, ossia l'*Elliptic Curve Digital Signature Algorithm*, che si basa su una curva ellittica Secp256k1, che consente computazioni efficienti.

Tale algoritmo prevede una chiave privata di 256 bit da cui si ricava una

chiave pubblica di 512 bit in modo unidirezionale, non invertibile, ossia tale che, partendo da tale chiave pubblica risulti impossibile ricavare la chiave privata.

Riguardo a questa generazione della chiave pubblica a partire dalla chiave privata, più precisamente la chiave pubblica generata mediante algoritmo ECDSA viene accorciata tramite un doppio hash, prima mediante l'algoritmo SHA-256, poi mediante l'algoritmo RIPEMD-160. Infine si applica un encoding Base58Check, al fine di ottenere una stringa di caratteri standard. A tal proposito, gli indirizzi degli utenti sono hash delle loro chiavi pubbliche, che hanno lunghezza inferiore a tali

chiavi e sono più robusti agli attacchi crittografici.

Risulta di fondamentale importanza il fatto che, nel sistema Bitcoin, ogni messaggio che esprime una transazione non viene criptato, ma viene inviato così com'è per garantire la trasparenza della Blockchain del sistema; la validità del messaggio viene perciò garantita dalla firma digitale, che si basa sulla cifratura.

La definizione generale di firma digitale considera una coppia di numeri (n, k) con n che indica un *nonce*, dall'inglese "for the nonce", che significa "per l'occasione", ossia un numero in genere casuale o pseudo-

casuale che può essere utilizzato una sola volta, e k che indica la chiave pubblica che viene generata a partire dalla chiave privata del soggetto che appone la firma digitale. Il mittente invia la firma digitale assieme al messaggio.

Ogni firma digitale che viene apposta può essere verificata mediante la chiave pubblica, ma l'autenticità non rappresenta l'unico punto di attenzione: una firma digitale deve anche garantire l'integrità e la non ripudiabilità del messaggio.

In sostanza, si parte da un messaggio *m* e gli si applica un hash che restituisce una nuova stringa. La firma viene applicata a tale output, che costituisce il cosiddetto *digest di messaggio*. È a

questo punto che, concettualmente, c'è la necessità di generare le due chiavi, la chiave privata e la chiave pubblica di conseguenza.

Ricapitolando, per inviare un messaggio firmato digitalmente nel sistema Bitcoin, occorre effettuare l'hash del messaggio *m* e cifrare il risultato con la chiave privata, in modo tale da ricavare la firma digitale che andrà inviata assieme al messaggio. Schematizzando, quindi, si seguono i seguenti passaggi:

- si computa l'hash H = SHA256(*m*);

- si cifra H con la chiave privata Kpriv per ottenere la firma digitale F =

cifra(H, Kpriv):

- si inviano il messaggio *m*, che appunto non è cifrato, e la firma digitale F.

Per validare il messaggio firmato digitalmente, si seguono invece i seguenti passaggi:

- si computa l'hash H = SHA256(*m*);

- si decifra la firma digitale F con la chiave pubblica Kpub per ottenere Hdec = decifra(F, Kpub);

- si verifica se H = Hdec, caso in cui la firma è valida e quindi l'intero procedimento si è svolto con successo.

La chiave pubblica, in realtà, a dispetto della denominazione, non viene necessariamente resa pubblica; diviene pubblica solo quando una transazione viene firmata dal mittente, proprio perché il processo prevede che venga utilizzata la chiave pubblica del mittente per verificare la firma digitale.

In questo contesto, una transazione consiste in un trasferimento di denaro tra due indirizzi, che comporta un cambio di proprietà di Bitcoin. In sostanza, chi dispone di Bitcoin, può trasferire del denaro in tale criptovaluta creando, in modo trasparente, ossia senza magari averne nemmeno cognizione dato che il

software preposto esegue tutto in automatico, un messaggio che costituisce, appunto, una transazione, con l'importo da inviare e l'hash della chiave pubblica del beneficiario, che rappresenta il suo indirizzo, e firma digitalmente tale messaggio con la sua chiave privata.

Sarà cura dei nodi della Rete validare le transazioni validando, di fatto, le firme digitali che vengono inviate assieme ai messaggi . Ogni transazione va quindi accettata in modo definitivo prima di essere inserita nella Blockchain.

Le transazioni possono essere di due diversi tipi: le transazioni P2PKH, acronimo di *Pay-to-PubKey-Hash*, con

cui si trasferisce crittovaluta preesistente da un indirizzo ad un altro, e le transazioni *Coinbase*, con cui vedono la luce nuovi Bitcoin.

Una transazione di tipo P2PKH viene inserita nella Blockchain per essere validata ogniqualvolta un possessore di Bitcoin effettua una pagamento a favore di un beneficiario; dal momento della convalida, il denaro sarà nuovamente spendibile, dal beneficiario che così assume la veste di nuovo possessore.

Poiché nelle transazioni di tipo P2PKH la criptomoneta viene "prelevata" da transazioni precedenti e i pagamenti vengono indirizzati verso gli indirizzi pubblici dei beneficiari, ogni transazione è caratterizzata, in generale,

da un certo numero di input e da un certo numero di output. Si instaura, quindi, una catena che diventa sempre più lunga, in cui gli output di ogni transazione vengono utilizzati come input di transazioni successive.

Se un'intera transazione diviene l'input di un'altra transazione si parla di "transazione spesa", ossia l'intero ammontare di criptomoneta che contiene viene trasferito al beneficiario. Più in generale, un pagamento avrà luogo per una somma diversa da quella della transazione in input; chiaramente, se la somma è inferiore, sarà necessario considerare un resto, un *change* che andrà a confluire in un nuovo indirizzo del beneficiario creato ad hoc.

Capitolo 7: tassazione e adempimenti fiscali riguardo ai Bitcoin

Quando ci si accinge a provare a guadagnare con i Bitcoin, spesso ci si interroga sull'aspetto fiscale della faccenda e, giustamente, come per ogni investimento, bisogna valutare tutti i costi da dover sostenere, quindi anche quelli relativi alla tassazione. Non considerare gli adempimenti fiscali relativi ad un investimento in Bitcoin può portare a conseguenze spiacevoli, tra cui quella di essere inquadrati come

evasori fiscali.

Il recente Decreto Legislativo 90/2017 ha introdotto il concetto di "valute virtuali" nel sistema normativo italiano; contestualmente ha introdotto la figura del prestatore di servizi in relazione all'impiego di valuta virtuale, per adottare la Direttiva UE 2015/859, nota anche come IV Direttiva Antiriciclaggio. Nonostante questo, da un punto di vista pratico, ad oggi non vi è un parere unanime su come i Bitcoin vadano trattati ai fini fiscali.

Data la loro natura e la loro introduzione relativamente recente, i Bitcoin non prevedono una tassazione particolare, su misura, in modo esplicito con una norma chiara ad hoc, e lo stesso

si può dire per le altre criptovalute. Ciononostante, costituendo tali strumenti una opportunità di guadagno, non si può prescindere dalla regola generale che tutto ciò che costituisce un guadagno, una plusvalenza, debba essere in qualche modo tassato.

In sostanza, non è tanto il mezzo con cui si fanno i soldi che determina la necessità di una tassazione, quanto è il fatto di ottenere un certo ricavo da una attività di qualche tipo. Nello specifico, l'Agenzia delle Entrate, con la risoluzione 73E/2018, assimila le criptovalute alle valute estere, che possono anche semplicemente essere impiegate per fare acquisti e non necessariamente, quindi, con fini di

lucro, per ottenere un guadagno da rivendita.

Per le valute estere è prevista una tassazione solo se si supera una certa soglia di valore, proprio perché si ritiene che la detenzione di moneta estera in quantità ridotte sia per il semplice utilizzo, come avviene per l'Euro che si usa normalmente, e non per il guadagno da investimento. In questo frangente, le eventuali plusvalenze realizzate andrebbero dichiarate nella sezione "redditi diversi" del Modello Unico Persone Fisiche.

L'assimilazione, da parte dell'Agenzia delle Entrate, dei Bitcoin alle monete estere, però, non è l'unica considerazione con cui fare i conti: la

sentenza "C-264/2015 CGEU" del 22 ottobre 2015, della Corte di Giustizia delle Comunità Europee, contrasta con la possibilità di assimilare le crittovalute alle monete estere e le assimila, invece, ai tradizionali sistemi di pagamento. È dello stesso avviso la BCE.

Vi è dunque una incertezza derivante da due interpretazioni diverse, che non aiuta certo chi ha deciso di investire in criptovalute.

Comunque, quel che è certo è che la tassazione dei Bitcoin può avere atto solo se il prezzo di vendita è superiore al prezzo di acquisto. Per il resto, date la lacuna normativa e l'incertezza obiettiva sul tipo di tassazione da

adottare, non si può che rimandare la questione al proprio Commercialista di fiducia che, purtroppo a fatica visto quanto poc'anzi esposto, provi a fornire una indicazione pratica sulla base della sua esperienza e professionalità adeguandosi, purtroppo, anch'egli, all'increscioso vuoto normativo.

Tra l'altro, l'imprescindibilità del parere di un Professionista che si assuma la responsabilità del caso è dovuta anche al fatto che il proprio investimento in Bitcoin potrebbe risultare localizzato all'estero, potrebbe cioè essere inquadrato come investimento in un bene conservato fuori dai confini italiani e, per il monitoraggio fiscale previsto dalla legge, gli

investimenti di questo tipo che potrebbero dar vita ad un reddito imponibile nel nostro Paese vanno dichiarati nell'apposito quadro del Modello Unico PF; chi non dovesse adempiere ad un obbligo del genere rischia di subire pesanti sanzioni.

Pensare di passare per investitori anonimi e di evadere, comunque, non è una buona idea poiché lo Stato è in grado di rintracciare le movimentazioni di criptovaluta, può cioè accedere alla Blockchain dei Bitcoin pubblica, che è una *Permissionless Blockchain*, che non richiede cioè una accettazione iniziale per potervi operare, e tracciare i passaggi di mano della criptomoneta

attraverso le chiavi pubbliche dei beneficiari, che, come visto, consistono in stringhe che rappresentano indirizzi.

A partire da tali chiavi pubbliche, le Autorità possono scovare gli utenti che possiedono le relative chiavi private, poiché esiste un legame tra chiave pubblica e chiave privata, secondo il quale la chiave pubblica viene ricavata dalla chiave privata. Le moderne tecnologie informatiche impiegate dalle Forze dell'Ordine hanno già dimostrato di riuscire a tracciare correttamente i movimenti di Bitcoin all'interno della Blockchain.

Capitolo 8: una riflessione sui guadagni milionari con i Bitcoin

I casi in cui un investitore in Bitcoin ha guadagnato in passato moltissimo, in maniera spropositata, sono estremamente rari, spesso del tutto frutto del caso, e la cosa si spiega in modo relativamente semplice; chi ha guadagnato moltissimo, quasi sicuramente ha avuto solo un'enorme fortuna oppure non aveva davvero intenzione di investire, oppure entrambe le cose.

Il fulcro della questione è che, in realtà, chi investe in qualcosa ha poi il problema di capire quando disinvestire. Nel caso dei Bitcoin, chi li ha acquistati nel lontano 2009, per pochi centesimi di dollari, si è trovato presto nelle condizioni di potere disinvestire poiché, già dopo un paio di anni, il controvalore dei Bitcoin era aumentato parecchio. Più il tempo passava, più il valore della criptovaluta aumentava e quindi è molto probabile che, ad un certo punto della storia, si sia effettuato un cambio sì favorevole, ma comunque ben lontano dai picchi del 2017.

Insomma, è molto più probabile che, nel corso dei primi anni di vita della criptovaluta, l'investitore abbia ceduto

alla tentazione di effettuare un cambio favorevole temendo per un successivo ribasso, che già all'epoca si prospettava, dato che non è mai stato un mistero che il tutto potesse consistere solo in una bolla speculativa.

Ecco quindi che chi si è arricchito con decine di milioni di euro, molto probabilmente l'ha fatto perché ha letteralmente dimenticato la questione, perché magari ha fatto l'acquisto all'inizio e poi semplicemente non ha più badato alla cosa fino a quanto, a distanza di molti anni, ha ripreso in mano la situazione, per così dire, ed ha concretizzato un guadagno stratosferico.

Un caso in questo senso è quello di

Kristoffer Koch, uno studente norvegese che aveva scambiato poco meno di 27 dollari in Bitcoin, nel 2009, al fine di capire meglio di cosa si trattasse per redigere la sua tesi di laurea in crittografia informatica. Da quel momento in poi, per anni, lo studente si era praticamente dimenticato dei Bitcoin, che considerava alla stregua di "soldi finti", o forse più semplicemente si potrebbe meglio supporre che non gli abbia dato importanza più di tanto, non controllando più il cambio nel corso del tempo, visto che si era laureato e il capitolo era chiuso. Tra l'altro, l'ormai ex studente, col passare degli anni dimentica anche la password del suo wallet, ossia del suo portafogli virtuale,

necessaria per accedere ai suoi Bitcoin.

Ad un certo punto, la cronaca narra che, complice il furore mediatico che ha accompagnato la criptomoneta per eccellenza in questi ultimi anni, lo studente abbia ripreso in mano le fila del discorso e che, di fatto, sia riuscito a recuperare la password del suo wallet. Risultato: gli oltre 5.000 Bitcoin in suo possesso gli hanno fruttato la bellezza di 886.000 dollari al cambio nel 2013.

Si tratta dunque di un guadagno enorme ma, ritornando al concetto iniziale: quanto avrebbe guadagnato questo fortunato studente se avesse aspettato qualche altro anno anziché incassare e comprarsi un appartamento poco dopo il recupero della sua

password? Quasi 900.000 dollari rappresentano una cifra enorme, ma sono ben poca cosa rispetto alle decine di migliaia di dollari a Bitcoin che il fortunato studente avrebbe potuto guadagnare se solo si fosse ricordato della password qualche anno dopo, magari proprio nel 2017, quando il cambio Bitcoin/Dollaro è arrivato a circa 1 BTC = $ 18.000.

E se invece lo studente si fosse ricordato la password e avesse dato importanza alla cosa qualche anno prima del 2013? Beh, magari un guadagno dell'ordine del migliaio di dollari sarebbe stato visto come estremamente profittevole e a quel punto non ci sarebbe stato alcuno scalpore e non si

sarebbe, così, mai giusti all'enormità della cifra di quasi $ 900.000.

Ecco quindi la forza della riflessione iniziale, secondo la quale i guadagni enormi con i Bitcoin, nella maggioranza dei casi, se non nella totalità, sono stati fatti senza reale cognizione di causa, con moltissima fortuna e/o senza una reale intenzione di investire.

Va anche notato che, nello stesso anno 2013, mentre ad aprile 2013 il cambio era 1BTC = $266, poco dopo è divenuto 1BTC = $50, abbassandosi quindi notevolmente, il che fa capire la difficoltà di individuare il momento migliore per vendere Bitcoin e guadagnare concretamente, oltre alla difficoltà di guadagnare qualcosa e non

perdere invece tutto. Si tratta, insomma, di fluttuazioni enormi anche nel breve periodo: da un giorno all'altro si può guadagnare moltissimo, ma anche perdere moltissimo.

A tutto ciò si aggiunge un'altra considerazione, tutt'altro che secondaria: quando si è presentata la possibilità di investire in Bitcoin, erano comunque disponibili altre possibilità di investimento. Realisticamente, mettendo da parte la fortuna, un investitore, in linea di principio, senza sapere cosa gli avrebbe potuto riservare il futuro, avrebbe dovuto puntare non solo sui Bitcoin, ma anche su tutte le altre forme di investimento possibile, o per lo meno su un buon numero di esse, ritenute

degne di attenzione, il che si sarebbe potuto rivelare come una ingente perdita. In altre parole, è facile dire a posteriori, a cose fatte, che bastava investire in Bitcoin per diventare ricchi sfondati, quando, in realtà, investire molto e su più fronti, di norma porta alla perdita del proprio capitale e non al guadagno sfrenato.

Si ritorna al concetto di estrema fortuna anzi espresso, che porta alla naturale conseguenza che investire oggi in Bitcoin è una pratica piuttosto rischiosa che può sì fare guadagnare ancora, ma che può pure far perdere non poco, anche visto e considerato che oggi acquistare un solo Bitcoin richiede un certo capitale di migliaia di euro e che,

anche se si acquistassero Bitcoin quando il controvalore in euro scendesse a poche centinaia di euro, ci sarebbe comunque il rischio che il Bitcoin continui a perdere terreno attestandosi, definitivamente, a valori ben al di sotto di centinaia di euro.

Continuando l'iter di riflessione, un altro caso fortunato è quello di una persona che, il 22/05/2010, accettò di farsi pagare due pizze in Bitcoin dal programmatore Laszlo Hanyecz, che aveva anche lavorato al codice sorgente del sistema e che pensava di spendere, con 10.000 Bitcoin, appena 41 dollari.

Da quel primo acquisto in Bitcoin si parla di "Pizza Index" per indicare il

mutamento di valore delle due pizze acquistate nel tempo; si è, così, passati da un Pizza Index di $41 di maggio 2010 ad un Pizza Index di $15.500.000 di aprile 2017. Il 22 maggio di ogni anno, inoltre, viene indicato come "Bitcoin Pizza Day", per commemorare la transazione "sbalorditiva" con il senno di poi, nonché il primo acquisto fatto pagando con Bitcoin; in tale giorno, molti rivenditori di pizza di tutto il mondo fanno sconti a chi paga in Bitcoin.

Per la cronaca, a luglio 2010 si poteva acquistare un Bitcoin a 5 centesimi di dollaro.

Si dovrebbe intuire, quindi, il rischio di bolla speculativa tanto invocato dagli

analisti finanziari che studiano le soluzioni delle criptovalute; alcuni di questi paragonano il fenomeno Bitcoin a quello della bolla del 2002 relativa alle Internet Company e a quello della bolla del lontano 1637 relativa ai bulbi di tulipani.

Anche la Federal Reserve e la BCE hanno espresso forti preoccupazioni per questa situazione che coinvolge le criptovalute e si è insidiato pure il sospetto che a controllare, a pilotare in qualche modo il cambio, vi siano dietro degli speculatori ben organizzati con al seguito piccoli risparmiatori illusi da prospettive di guadagni facili.

La domanda, quindi, nasce spontanea:

come riuscire a guadagnare anche se il valore del Bitcoin diminuisce? Come si potrebbe affrontare un eventuale crollo del valore del Bitcoin?

Spesso alcuni sedicenti esperti insistono sul fatto che si possa guadagnare con i Bitcoin facendo trading online anche se il valore della criptovaluta è in discesa, affermando cioè senza mezzi termini che, con i Bitcoin, si possa guadagnare in ogni caso, sempre.

Ovviamente questo non è possibile perché, se da un lato è vero che acquistando Bitcoin quando il loro valore è in discesa con l'idea di rivenderli successivamente quando il loro valore sarà in salita è un concetto

valido, forte di una sua logica, è altrettanto vero che nessuno garantisce che vi sarà un momento futuro in cui il loro valore, effettivamente, aumenterà rispetto a quello di acquisto; il fatto che ciò sia successo in passato non implica assolutamente che possa verificarsi in futuro, quindi il rischio è che la diminuzione di valore sia definitivo, con perdita del capitale investito.

Fare trading online, tra l'altro, non è semplice nemmeno in termini di scelta della piattaforma di trading da utilizzare; va da sé che è innanzitutto necessario scegliere una piattaforma autorizzata che sia affidabile, gestita da personale qualificato, serio, che agisca nel pieno rispetto delle normative in materia.

Imparare ad usare questi strumenti non è difficile, ma richiede una certa attenzione e, in effetti, con la piattaforma di trading vengono in genere forniti un supporto gratuito 24 ore su 24 e un tutor di guida e viene data la possibilità di iniziare a fare trading con una piccola somma di denaro.

Un lato indubbiamente positivo nell'approccio al trading sicuramente c'è e riguarda la possibilità di analizzare, in tempo reale, grafici sull'andamento del valore del Bitcoin. Non che tali grafici non siano consultabili gratuitamente con una rapida ricerca sui principali motori di ricerca, ma interessandosi al Bitcoin ad un certo livello, utilizzando un certo framework, risulta semplice avere tutto

ciò che è utile a portata di mano.

Come si evince dal grafico (prelevato il 12 marzo 2018 dal sito *IQ Option*), scaturito dalle quotazioni fornite da *Levarate*, dal 19/09/2012 al 12/03/2018, non si è assistito affatto ad un continuo aumento di valore del Bitcoin rispetto all'Euro, anzi si può notare che proprio verso la parte finale del diagramma si assiste ad una pressoché continua perdita di valore del

Bitcoin. Questo significa che chi avesse acquistato Bitcoin nella prima metà di dicembre, oggi sarebbe, molto probabilmente in perdita, seppure vi sia un trend al rialzo per gli ultimi giorni considerati.

Il seguente dettaglio del grafico dovrebbe mostrare meglio quanto riportato:

Si tratta di un'estrazione del trimestre che va dal 12/12/2017 al 12/03/2018,

che mostra, appunto, che chi, poco prima, ha acquistato Bitcoin, potrebbe aver perso del denaro, anziché guadagnarlo, e se si pensa che questi andamenti bruschi verso l'alto o verso l'alto, frutto di grande volatilità, possono verificarsi in qualunque momento, anche dopo mesi o anni, si intuisce il rischio di perdita, oltre che di guadagno, che riguarda i Bitcoin.

Quantitativamente parlando, per fare un esempio di analisi, il minimo del 05/02/2018 è relativo ad un cambio Bitcoin/Euro di 6.937,08, mentre il massimo del 16/12/2017 è relativo ad un cambio Bitcoin/Euro di 19.345,49, mentre il cambio al 12/11/2017 è di 5.878,13, con un trend in crescita e

valori superiori a quello del minimo, il che significa che chi ha acquistato Bitcoin dal 13 al 16 novembre 2017 con l'idea di venderli nel brevissimo periodo avrebbe sicuramente perso per rivendite effettuate entro il 05/02/2018.

Bisogna, insomma, vedere su che "fronte" del grafico ci si trova per rendersi conto se il proprio investimento stia davvero rendendo qualcosa, e tale fronte può essere sfavorevole in qualsiasi istante si faccia l'analisi, mettendo da parte la semplicità dell'esempio che mostra una situazione sfavorevole nel breve periodo. Tra l'altro, il trend negativo può essere molto "brusco" e portare a perdite continue col passare del tempo, nei casi

peggiori fino a non lasciare spazio ad una inversione di trend che quantomeno limiti le perdite.

Riferimenti e altri libri dell’autore in vendita

Altri libri dell'autore in vendita

Manuali

In vendita su Amazon il manuale:

Miglioramento della Memoria con Tecniche di Memorizzazione Veloce

Sinossi:

L'argomento del potenziamento della memoria è divenuto molto popolare soprattutto in questi ultimi anni, segno di un malessere che vede molte persone in difficoltà per non sentirsi abili nel

memorizzare nozioni, concetti, nomi e numeri che servono nella vita quotidiana.

Il disagio di non sentire adeguate le proprie capacità mnemoniche si riflette, dunque, sulla vita di tutti i giorni e, spesso, dà pure vita ad una certa frustrazione che sfocia in rassegnazione e pessimismo cronico perché ci si sente incapaci di ricordare cose, talvolta anche importanti, che si ritiene che altri ricordino bene, e questa sensazione si sente spesso in modo accentuato quando si è studenti e ci si trova davanti ad esami difficili da sostenere con la testa che “non fa quel che dovrebbe”.

Le capacità cognitive in generale, ossia non solo la capacità di memorizzazione, ma anche la capacità di concentrazione, la capacità di comprensione e la prontezza mentale nelle sue varie sfaccettature, costituiscono, quindi, per molti, un aspetto della propria esistenza da migliorare il più possibile, per risultare più efficienti nella vita quotidiana, per allontanare lo stress generato dal sentirsi poco capaci a livello mentale e per dare così pure sollievo alla propria autostima.

Questo manuale tratta l'argomento delle tecniche sinergiche per il potenziamento delle capacità cognitive, delle abilità mentali, soffermandosi sulle

mnemotecniche, sull'allenamento della materia grigia e sulle piante più usate in fitoterapia per il rafforzamento della memoria. La chiave per ottenere risultati tangibili risiede infatti nell'unione di più metodologie da mettere in atto per il raggiungimento di un obiettivo comune.

In vendita su Amazon il manuale:

Tecniche di lettura veloce e comprensione rapida

Sinossi:

L'argomento della capacità di lettura veloce è divenuto molto popolare

soprattutto in questi ultimi anni, complice l'enorme quantità di informazioni che ogni giorno bombardano chiunque, soprattutto su Internet.

A volte ci si sente anche a disagio per non sentire adeguate le proprie capacità di lettura e di comprensione, con l'insorgere, in alcuni casi, di una certa frustrazione che sfocia in rassegnazione e pessimismo cronico perché ci si sente incapaci di elaborare a dovere tutte le nozioni che capitano a tiro e questa sensazione si sente spesso in modo accentuato quando si è studenti e ci si trova davanti ad esami difficili da sostenere in breve tempo, molto spesso

realmente insufficiente per leggere bene tutto il materiale didattico.

Le capacità di lettura e di comprensione rappresentano, quindi, per molti, un aspetto della propria esistenza da migliorare il più possibile, per risultare più efficienti nella vita quotidiana, per allontanare lo stress generato dal sentirsi poco capaci a livello mentale e poco ferrati a livello culturale, e per dare così pure sollievo alla propria autostima.

Questo manuale tratta l'argomento delle tecniche di lettura veloce e comprensione rapida, quest'ultima legata indissolubilmente alla lettura, ma

anche alla capacità di memorizzazione, senza la quale ciò che viene letto e viene compreso non può essere realmente appreso e ricordato.

In vendita su Amazon il manuale:

Matematica Ragionata per il Calcolo Mentale Veloce

Sinossi:

La matematica ha sempre accompagnato l'uomo nella sua vita, e lo accompagna a maggior ragione tutt'oggi, non solo ogni volta che occorre eseguire un calcolo aritmetico, ma anche in considerazione

delle manifestazioni della natura che lo circondano, che spesso impiegano schemi matematici ben precisi per formarsi e svilupparsi.

Gli algoritmi di calcolo mentale veloce sono utili strumenti per semplificare alcuni calcoli mediante dei “trucchi matematici”, delle “scorciatoie”, che si basano sia su semplici ragionamenti ed applicazioni di proprietà di base dell’aritmetica, sia su metodologie più o meno complesse atte a velocizzare al massimo l’esecuzione dei calcoli evitando di essere costretti ad eseguirli su fogli di carta.

A titolo di esempio, calcolare a mente il

quadrato del numero 63 può essere piuttosto agevole calcolando semplicemente il quadrato di 60 e sommandogli il numero fisso 9 e sei volte il numero 60, calcolando, cioè, semplicemente la somma 3600+360+9, ottenendo così il risultato 3969. Niente, quindi, che non possa essere calcolato velocemente a mente, anche senza un particolare allenamento mentale.

Questo piccolo manuale tratta casi come quello appena esposto e si prefigge lo scopo di fornire al lettore molti semplici e dettagliati esempi di applicazione di calcoli mentali veloci, facendo soffermare l'attenzione, in particolar modo, sui quadrati dei numeri e sulle

moltiplicazioni dei numeri. Assieme a tecniche di allenamento mentale, si potrà così avere una marcia in più che, se non altro, sia da spunto per avvicinarsi al magnifico mondo della matematica partendo da concetti di semplice comprensione utili e in parte anche divertenti.

Romanzi

In vendita su Amazon il romanzo:

L'Aliena

Sinossi:

Durante un violento temporale che si

abbatte su Roma e dintorni, Andrea è di ritorno da Tivoli in auto, quando è costretto a lasciare la consueta strada principale per deviare il suo viaggio attraverso una stradina di campagna sconosciuta. La sua vecchia automobile si ferma all'improvviso nel bel mezzo dell'acquazzone e, davanti ai suoi occhi, si delinea la figura di una ragazza misteriosa che sta immobile e silenziosa sotto la pioggia battente con un ombrello rotto in mano. Dopo uno spiacevole incontro in una taverna lì nelle vicinanze, dove il ragazzo si reca, assieme alla ragazza, per cercare aiuto, e dopo una breve fuga in auto, Andrea perde di vista la ragazza ma non riesce a dimenticarla i giorni successivi,

essendone rimasto ossessionato. Nei giorni a seguire, i pensieri del ragazzo vengono monopolizzati da quella figura misteriosa, alla ricerca di risposte in una Roma sbiadita, decadente, e al contempo potenzialmente magnifica. Nel frattempo, il massimo esperto mondiale di ufo ed alieni annuncia che il 21 dicembre 2021 farà una rivelazione che cambierà il mondo.

Una storia drammatica con elementi di fantascienza, densa di mistero, incentrata sui temi dell'alienazione, della diversità e della percezione della realtà, dove una buona dose di avventura, necessaria per la ricerca della verità, si sposa con le riflessioni e gli interrogativi che

nascono dalla contraddizione tra le potenzialmente fallaci certezze che vengono propinate dall'alto, spesso corroborate dal comune vedere e sentire, e la consapevolezza della percezione personale della realtà con le sue diversità.
Una storia a tratti romantica, sui buoni sentimenti e sulla speranza, che narra una certa condizione umana tra degrado sociale e fiducia nel riscatto, toccando il tema degli ufo e degli alieni.

*** GENERI: drammatico con cenni di fantascienza e di romanticismo ***

In vendita su Amazon il romanzo:

I Segreti del Tempo che è Passato

Sinossi:

Si può amare qualcuno che non sia un bell'avvocato in carriera o un ricco proprietario di una multinazionale o un affascinante uomo d'affari che vive a Londra o a New York? Qualcuno non ricco e potente e nemmeno bello e dannato, con cui magari si interagisce solo a singhiozzo e con piccoli, teneri gesti? E ci si può sentire diversi e a disagio, come voci fuori dal coro, semplicemente perché non si ha un'idea dell'amore stereotipata e non si riesce ad amare come fanno quasi tutti gli altri?

Ambra è una ragazza sbarazzina e ironica di 28 anni, una giovane donna sognatrice innamorata della fotografia che ha un grosso problema: è bellissima, e quindi molto corteggiata, soprattutto dal suo amico avvocato Marco, ma ha grande difficoltà ad intessere relazioni con l'altro sesso. Il suo cuore, da tempo immemore, non è più capace di amare nessun uomo. Un terribile passato ha segnato la sua esistenza, spensierata e disinteressata all'amore solo all'apparenza. Assieme agli affetti di Jennifer, la sua migliore amica, e del suo strampalato nonno, e fra i comportamenti bizzarri di vari personaggi che la accompagneranno

nella sua routine quotidiana avente per sfondo la magnifica città di Roma, Ambra cercherà con tutte le sue forze di ritrovare la fiducia nel genere maschile e, soprattutto, in se stessa. Un misterioso ragazzo spuntato all'improvviso dal nulla, un improbabile scrittore di romanzi chick-lit con cui sarà costretta ad interagire tra battibecchi e incomprensioni, potrebbe dare un contributo decisivo alle sue convinzioni, minandole e favorendo così il punto di svolta tanto indesiderato a parole, quanto bramato nel profondo dell'animo. Ma anche questo personaggio nasconde forse un passato terribile…

Un approccio da commedia romantica

dove umorismo, stramberia, sogno e un pizzico di dramma e di mistero si mescolano per dar vita ad un romanzo chick-lit un po' fuori dai canoni, in cui l'amore è trattato in maniera molto delicata, visto con gli occhi di una ragazza sognatrice e un po' sopra le righe, ma anche forte, grintosa, determinata e coraggiosa, proprio come una ragazza dei nostri tempi.

*** GENERI: contemporary romance, commedia romantica, chick-lit atipico ***

Riferimenti e contatti

Pagina Amazon dell'autore:

http://www.amazon.it/s?_encoding=UTF8&field-author=Manuel%20Carsini&search-alias=digital-text

Email dell'autore:

manuel.carsini@hotmail.com