

IL BITCOIN SPIEGATO A MIA MADRE



RICCARDO TORTORA

IL BITCOIN SPIEGATO A MIA MADRE

CON UN'INTRODUZIONE
ALLA BLOCKCHAIN

© 2018 Riccardo Tortora

Tutti i diritti riservati.

www.econominds.it

ilbitcoin@econominds.it

Editing: Marta Mauri

Versione 1.0

Edizione maggio 2018

Le informazioni contenute in questo libro non devono essere considerate una sollecitazione al pubblico risparmio o la promozione di alcuna forma di investimento.

Le indicazioni fornite in questo libro non possono intendersi personalizzate ai sensi del Testo Unico della Finanza rispetto alle caratteristiche del singolo Lettore, trattandosi unicamente di informazione standardizzata rivolta al pubblico indistinto.

L'autore del libro non è al corrente, né potrebbe esserlo, delle competenze, delle esperienze, della situazione finanziaria e degli obiettivi di investimento dei singoli Lettori.

L'obiettivo dell'autore è meramente divulgativo: presentare la moneta digitale e alcuni strumenti finanziari, spiegare in maniera semplice concetti di economia, mettere nella condizione di evitare investimenti imprudenti e pericolosi, nonché far riflettere sui fenomeni trattati.

«Se investi in ciò che conosci, non puoi perdere più di quello che sai.» - Riccardo Tortora

0. PREMESSA

Non sono un milionario in *bitcoin*.

Non sono un milionario in euro.

Non sono uno di quei *trader* che passa le giornate davanti a grafici divisi su più schermi. Ma sì, potrei essere un milionario in yen giapponesi al cambio attuale, ovvero di 0,00763 euro per yen.

Non sono mai stato nemmeno un grande oratore, e nella vita ho sempre

dovuto ascoltare molto per questa mia carenza. Ho dovuto ascoltare gente che, a dir la verità, parlava troppo per quel poco che aveva da dire.

Insomma, se mi chiedeste come sono andate le vacanze, vi risponderei semplicemente: «Bene, grazie. Le tue?». Fate una prova, se mi incrociate in giro.

Ho sempre avuto problemi anche con la scrittura: probabilmente sarei capace di scrivere *Il signore degli anelli* in un foglio protocollo piegato a metà, come si faceva a scuola.

Se con le parole non sono mai andato molto d'accordo, con i numeri fortunatamente è andata meglio. Da

ragazzino ho vinto qualche concorso di logica matematica, classificandomi perfino nelle prime posizioni a livello nazionale.

Vorrei, in realtà, continuare a pavoneggiarmi, ma qui è iniziata e finita la mia carriera di matematico. A volte mi chiedo che fine abbia fatto quel ragazzino...

Mi sono imbattuto nell'economia per caso, se teniamo conto che ho iniziato a sviluppare software all'età di dieci anni e già allora davo per certo il mio futuro da programmatore. Naturalmente oggi faccio tutt'altro, ma anche il programmatore.

Ho iniziato, quindi, a studiare i grafici e i mercati, cercando di capire i meccanismi e le opportunità che questi possono offrire. Ho provato a unire informatica ed economia, sviluppando codici per l'acquisto e la vendita automatica di titoli e azioni.

È stato quando ho pensato di capirci finalmente qualcosa, che ho iniziato a perdere i primi soldi. Ma immagino sia un investimento obbligato, e l'importante è imparare dai propri errori. A onor del vero, però, non credo di aver ancora imparato.

Ma è arrivato il momento di spiegare come è nata l'idea di questo libro.

Era una domenica sera come tante, a cena dai miei. Mia madre Elsa, un'impiegata che reputo di intelligenza superiore alla media, ma che, a essere sinceri, non cucina proprio come detta la diligenza della buona madre di famiglia, a un tratto mi chiede: «Vorrei investire in *Bitcoin*, come faccio?».

Ora, considerato che l'investimento migliore di mia madre è stato un famoso quanto costoso robot da cucina, che attualmente è a prendere polvere sulla credenza accanto ai fornelli, sperando che prima o poi qualcuno colleghi la sua presa alla corrente, l'ho guardata basito. Aveva sicuramente sentito me parlarne,

aveva sicuramente subito il martellamento pneumatico delle trasmissioni di informazione televisiva, aveva sicuramente visto qualche pubblicità online, ma no, non potevo capacitarmene.

Chissà quante madri (o padri) di famiglia, magari anche ottime cuoche e assidue utilizzatrici di famosi robot da cucina, senza sapere di che cosa parlassero, hanno avuto la stessa bizzarra idea...

Ecco perché è nato questo libro: per spiegare in maniera semplice e imparziale che cos'è *Bitcoin* e tutto ciò che gli gira intorno. Ho voluto condire l'argomento con alcuni riferimenti di

economia e finanza base, che ho ritenuto utili per riflettere sui fenomeni discussi.

Per questo motivo, qui, parlerò di *Bitcoin* anche riferendomi alle valute digitali in generale, in quanto credo semplifichino per quanto possibile i concetti a chi si affaccia per la prima volta a questo mondo. Non me ne vogliano i lettori più esperti.

Per questi ultimi, alla fine di ogni capitolo è presente la sezione *Per saperne di più*, dove i lettori più curiosi potranno trovare informazioni più tecniche, e che, al contempo, permetterà agli altri di non rovinarsi la lettura con concetti troppo impegnativi.

1. CHE COSA SONO I BITCOIN?

Avessi un *bitcoin* per ogni volta che qualcuno mi ha fatto questa domanda, probabilmente starei scrivendo sdraiato sulla spiaggia di una qualche isola paradisiaca e non seduto al tavolo della cucina di casa mia, che poi, a dir la verità, è anche il soggiorno.

Prima di introdurre il *Bitcoin* credo si debba partire dal concetto più

generico di moneta.

Potremmo partire dall'Era Mesozoica, magari anche dal Big Bang, ma credo che, per spiegare come la moneta si è evoluta fino ai giorni nostri, possano bastare un paio di semplici esempi.

Il mercato, inteso come rapporto di dare e avere, è un concetto innato dell'uomo. Ci basti pensare come, già da bambini, ci scambiamo i giochi o le figurine. Certo, è molto più facile ricevere che dare, e questa è un'altra peculiarità innata dell'uomo, ma concordiamo tutti su come il baratto sia la base dell'economia umana.

Infatti, immaginiamo per un attimo di essere allevatori di pecore e di avere per vicini solo coltivatori di cavolfiori. Per quanto possano piacerci i cavolfiori, barattare ogni giorno pecore con ortaggi potrebbe non essere così appagante. Ma potremmo comunque trovare utile acquistarli, magari con l'intento di scambiarli con altri beni e servizi.

Tenendo in mente questa possibilità, ci rivolgiamo a un venditore dal quale vorremmo acquistare un nuovo tagliaerba. Gli offriamo alcune pecore di nostra proprietà e i cavolfiori che abbiamo ottenuto dai nostri vicini. Lui potrebbe essere d'accordo e noi torneremmo a casa felici, ma che cosa

succederebbe se, al contrario, il venditore in questione non fosse disposto a barattare il tagliaerba con i nostri due beni? Dovremmo scambiare i beni fino a quando non riusciamo a ottenere quello che serve al nostro venditore di tagliaerba. Direi piuttosto scomodo.

Da questa esigenza è nata la prima moneta merce, ovvero un bene costruito con materiali di valore riconosciuto dal mercato (si pensi all'oro o all'argento) e che proprio per questa caratteristica può essere scambiato con qualsiasi altro bene.

Ottimo, ora possiamo acquistare il desiderato tagliaerba al prezzo di

qualche moneta merce. Non è stato poi così difficile!

Successivamente, sono state introdotte le monete rappresentative, cioè banconote o titoli che di per sé non avevano alcun valore, ma che potevano essere scambiate per date quantità di oro o altri materiali preziosi. È così che insieme alla moneta è nato il risparmio, impensabile al tempo del baratto, dove i beni andavano necessariamente consumati prima del loro deperimento.

Con l'economia in crescita, pensiamo all'Era Industriale, era fondamentale disporre di capitali sufficienti allo sviluppo economico,

anche ricorrendo ai prestiti. Proprio in questo frangente sono nate le banche, soggetti che ancora oggi offrono gestione o depositi per il risparmio e banconote o credito per il prestito di denaro.

Arriviamo quindi ai giorni nostri. La nostra attuale moneta non è rappresentativa di alcuna merce, il suo valore non è collegato né a quello dell'oro, né a quello di nessun altro materiale prezioso. La moneta attuale vale semplicemente quanto è indicato sulla moneta stessa.

Viene spontaneo domandarsi come possa avere valore qualcosa che non è collegato a un bene di riferimento. Chi ci dice che quella banconota vale

davvero 50 euro? E soprattutto, perché?

La risposta a queste domande è una sola: la fiducia. Ebbene sì, suona come una presa in giro e forse lo è, ma la nostra attuale moneta è una moneta fiduciaria.

Che cosa vuol dire? Le banche centrali emettono le monete e si impegnano a mantenere il loro valore stabile nel tempo. A fronte di questo impegno, gli utilizzatori della moneta danno fiducia alla banca centrale e impiegano la moneta nello scambio di beni e servizi. Chi riceve la moneta in pagamento, a sua volta, ha fiducia di poter usare la stessa per acquistare beni

e servizi di pari valore e così via. Ecco perché si chiama moneta fiduciaria: perché il valore reale del pezzo di carta (o di metallo) con scritto «50 euro» è praticamente nullo, ma rappresenta un titolo di scambio per beni e servizi dal valore predefinito e, sulla fiducia, stabile nel tempo.

Il *Bitcoin* è l'ennesima evoluzione della moneta conosciuta, ovvero la moneta virtuale. Non ne si conosce il reale ideatore, o il gruppo di creatori, ma solo lo pseudonimo noto come “Satoshi Nakamoto”.

Il *Bitcoin*, per quanto innovativo, è un progetto che ha ormai dieci anni e utilizza tecnologie ancora più vecchie.

Letteralmente tradotto “Moneta Bit” è una valuta non centralizzata. Non esiste un unico istituto centrale che possiede un registro delle operazioni in *bitcoin*, che ne vigila il valore e che ne garantisce la stabilità nel tempo. Insomma non parliamo più di fiducia.

Il sistema *Bitcoin* è basato su un registro di operazioni su cui sono annotati tutti i trasferimenti di proprietà delle monete, ovvero ogni pagamento. Questo registro è costantemente controllato e verificato dagli stessi utilizzatori di *bitcoin*, non vi è alcuno ente o autorità di controllo esterno.

Questa moneta, completamente

virtuale, è gestita interamente da computer non organizzati sparsi in tutto il mondo. Chiunque posseda un computer può diventare “gestore” di *Bitcoin*, in gergo *miner* (minatore).

Che cosa fanno i *miner*? Verificano che tutte le operazioni effettuate in *bitcoin* siano valide, e in cambio ottengono a loro volta una piccola ricompensa in *bitcoin*. Infatti, i computer collegati alla rete *Bitcoin* lavorano tutti sul registro delle operazioni di scambio di questa moneta. Migliori sono le prestazioni dei computer, più velocemente questi saranno in grado di risolvere i problemi matematici legati al controllo delle operazioni in *bitcoin*.

A differenza della moneta fiduciaria, dove il registro delle operazioni è centralizzato presso la banca a cui prestiamo fiducia, con i *bitcoin* il registro delle operazioni è decentralizzato e tutti i *miner* ne hanno una copia. Non preoccupatevi, il regalo che avete fatto all'amante (o, perché no, anche quello che avete ricevuto) è al sicuro nonostante sia sotto gli occhi di tutti i *miner*. Infatti, le operazioni in *bitcoin* sono criptate e, sebbene siano individuabili i due portafogli virtuali di un pagamento, ovvero quello di chi trasferisce dei *bitcoin* e quello di chi li riceve, i proprietari rimangono anonimi.

Da qui deriva il termine

“criptovaluta”, con il quale si usa chiamare il *bitcoin*.

Ma come si possono spendere i *bitcoin*? Attualmente il loro utilizzo principale è quello speculativo, ovvero acquistare moneta per rivenderla al fine di trarre un profitto sulle sue variazioni di prezzo. Sono, però, anche molto in voga come moneta di scambio per gli acquisti sul *Dark Web*, ovvero la parte sommersa di Internet dove sono presenti mercati neri di qualunque genere. Esiste, fortunatamente, anche un mercato legale per spendere i propri *bitcoin*. Infatti, seppur ancora pochi, alcuni negozi online li accettano come forma di pagamento. Non solo: esistono carte di

debito che consentono di pagare negozianti, purché siano in possesso di POS, in grado di convertire i *bitcoin* in moneta fiduciaria, euro o dollari per esempio, in cambio di una commissione.

Quindi, prima di arrabbiarsi con il proprio panettiere perché non accetta i *bitcoin*, è bene sapere che si è ancora lontani, almeno in Italia, dal poter utilizzare i *bitcoin* nella vita di tutti i giorni come forma di pagamento riconosciuta.



Per saperne di più...

L'unico modo per generare nuovi *bitcoin* è tramite il *mining* (in italiano “l'attività di miniera”, da cui deriva il termine *miner*, che abbiamo visto prima), ovvero mettere a disposizione della rete *Bitcoin* il proprio computer per validare le operazioni in cambio di una piccola quantità di moneta.

I *bitcoin* possono essere scambiati in frazioni, infatti possono essere divisi fino a otto posizioni decimali. La frazione più piccola del *bitcoin* (0,00000001 BTC) prende comunemente il nome di “Satoshi”, in onore del presunto creatore.

Spesso si sente paragonare i *bitcoin* all'oro, ma in realtà l'unica cosa che hanno in comune è che entrambi sono presenti in quantità limitata.

Il sistema *Bitcoin*, infatti, è stato progettato per generare il numero massimo di 21 milioni di *bitcoin*, raggiunti i quali il sistema non produrrà più monete, nemmeno per i *miner*.

2. E LA BLOCKCHAIN?

La Blockchain.

Tutti ne parlano, forse anche più di *Bitcoin*.

Ma perché? Perché la vera rivoluzione la sta facendo proprio lei.

Nel capitolo precedente abbiamo appreso che il sistema *Bitcoin* è basato

su un registro distribuito. Questo registro si chiama, pensate un po', *Blockchain*.

La traduzione letterale è “catena di blocchi”, definizione che descrive al meglio questa tecnologia. Ma cerchiamo di spiegarne il motivo.

Tutte le operazioni in *bitcoin* sono memorizzate sul registro unico, che funziona a tutti gli effetti come un libro mastro contabile su cui si annotano i conti.

Sappiamo che questo libro mastro è aperto a tutti, ovvero: tutti i computer collegati alla rete *Bitcoin* ne possiedono una copia, possono interrogarlo e

ricavarne le informazioni di cui hanno bisogno.

Abbiamo inoltre capito che tutte le operazioni in *Bitcoin*, prima di essere annotate nel registro unico, devono essere verificate dai *miner*, ovvero da quei soggetti che mettono a disposizione la capacità di calcolo del proprio computer per autorizzare le transazioni.

Tutti i computer che posseggono una copia del registro sono detti “nodi”.

Ma come vengono registrate le transazioni?

A differenza di quanto si farebbe su un classico libro contabile, sulla

Blockchain le transazioni non sono registrate una a una ma sono raggruppate in blocchi.

Ogni blocco di transazioni viene poi inviato alla rete *Bitcoin*, dove questo viene autorizzato.

Non esistendo un istituto centrale o un'autorità di controllo, per rendere il meccanismo il più sicuro possibile, i blocchi vengono collegati tra loro in modo irreversibile creando, di fatto, una catena.

Quando un blocco di operazioni è approvato dalla rete *Bitcoin*, ovvero dai *miner* o nodi, questo viene criptato insieme al codice che identifica il

blocco che lo precede. Il blocco approvato successivo si posizionerà subito sopra a quest'ultimo e verrà criptato, a sua volta, insieme al codice identificativo del precedente e così via...

Come già accennato, l'intervento di approvazione è irreversibile: infatti, a differenza dei bonifici bancari che possono essere revocati, un pagamento in *bitcoin* non è annullabile. Perfino nel caso in cui abbiate sbagliato l'indirizzo di pagamento.

Come si acquistano i *bitcoin*?

Iniziamo col dire che i *bitcoin* sono monete completamente digitali, ovvero non potranno mai essere rappresentati da

banconote cartacee. Questo perché ogni operazione deve essere effettuata sulla *blockchain* che ne garantisce l'autenticità. Infatti, se cedessimo dei *bitcoin* a qualcuno sotto forma di banconote, sulla *blockchain* non ve ne sarebbe alcuna traccia e noi rimarremmo, di fatto, proprietari di tutti i nostri *bitcoin*. Insomma, scordatevi di poter aprire il portafoglio per far vedere agli amici del bar quanti *bitcoin* avete, anche perché, poi, vi toccherebbe offrire da bere.

Per acquistare i *bitcoin* ci sono diverse soluzioni. La più diffusa è quella di rivolgersi agli *exchange*, ovvero piattaforme virtuali autorizzate

nelle quali è possibile scambiare *bitcoin* per valute tradizionali, come gli euro. Un *exchange* funziona quasi come un conto corrente: tramite bonifico o carta di credito si ricarica il conto e poi si utilizza il credito per acquistare *bitcoin* al valore di mercato, pagando una piccola commissione. Allo stesso modo è possibile riconvertire i *bitcoin* nella valuta tradizionale. La particolarità degli *exchange* è proprio quella di fornire un conto multi-valuta su cui tenere sia valute tradizionali che *bitcoin*, permettendone lo scambio quando più lo si ritiene opportuno.

Un'altra soluzione, più recente, è quella degli sportelli ATM. Ebbene sì,

sembrano sportelli automatici bancari, ma in realtà permettono di aprire un conto in *bitcoin* e ricaricarlo tramite contanti o carte di credito. I *bitcoin* saranno acquistati al valore di mercato del momento in cui si effettua la ricarica, maggiorato di una commissione che, solitamente, è più salata di quella applicata dagli *exchange*.

Come funzionano i pagamenti in *bitcoin*?

Ogni utente che vuole comprare o vendere dei *bitcoin* non deve aprire un conto corrente, ma un portafoglio virtuale, chiamato *wallet*, dove potrà vedere il saldo e disporre pagamenti.

I *wallet* hanno un indirizzo chiamato *chiave pubblica*, che potremmo paragonare all'IBAN di un conto corrente ordinario, che consente di ricevere i pagamenti. La chiave pubblica è l'indirizzo da comunicare per farsi accreditare i *bitcoin* e sarà l'indirizzo che verrà registrato nella *blockchain* quando effettueremo o riceveremo un pagamento.

Il portafoglio virtuale, però, è composto anche da un altro codice: la *chiave privata*. Questa chiave non deve essere comunicata a nessuno perché è quella che consente l'utilizzo del proprio portafoglio. Non solo è fondamentale non comunicarla, perché

chiunque ne venga in possesso potrà fare ciò che vuole del nostro *wallet*, ma è altrettanto importante non perderla, poiché senza non sarà più possibile accedere al nostro portafoglio di *bitcoin*.

Tornando alla *Blockchain*, i blocchi sono verificati così da impedire agli utenti di trasferire quantità di *bitcoin* che non si posseggono o di spendere più volte la stessa somma.

Com'è possibile? Il fatto che tutte le operazioni in *bitcoin* siano collegate tra loro in questa catena, ne rende impossibile la modifica da parte di malintenzionati, perché per poter modificare una transazione, è necessario

modificare tutte quelle a essa collegate, rendendo l'impresa inattuabile.

Con queste informazioni bene in mente, ora vi faccio una domanda. Quanti di voi metterebbero a disposizione il proprio computer a favore della *Blockchain*? Forse solo i più attenti. Coloro che ricordano quanto letto nel primo capitolo, ovvero che i *miner* sono ricompensati per il loro sforzo.

Ma come vengono ricompensati i *miner*?

Ricordiamo che il termine significa “minatore”, inteso come colui che cerca l'oro. Considerando che i *bitcoin* sono

moneta virtuale, i minatori, in questo caso, sono a tutti gli effetti cercatori di *bitcoin*.

Sappiamo che il compito dei *miner* è quello di validare le transazioni in blocchi.

Quando un blocco è approvato e aggiunto alla *blockchain*, il *miner* che lo ha trovato riceve dal sistema una ricompensa predeterminata di *bitcoin*. Questa ricompensa non è fissa, ma programmata per dimezzarsi ogni quattro anni. Infatti, nel 2009 ammontava a 50 *bitcoin* per blocco, nel 2013 è diminuita a 25 *bitcoin*, nel 2017 a 12,50 *bitcoin* e così via. La ricompensa per la scoperta di un blocco valido consiste in nuova

moneta, appositamente generata.

I minatori, però, non guadagnano solo i *bitcoin* generati dalla scoperta di un blocco, ma guadagnano anche sulle transazioni.

Infatti, è possibile attribuire delle commissioni alle operazioni in *bitcoin*.

Ma perché pagare una commissione?

I *miner*, guadagnando commissioni dalle operazioni che le prevedono, preferiranno autorizzare le transazioni con le commissioni più alte, dando loro la precedenza. Quindi, se una transazione contiene una commissione alta a favore dei *miner* che la

autorizzano, abbiamo la certezza che sarà eseguita con maggiore celerità.



Per saperne di più...

Ciò che davvero garantisce l'incorruttibilità del sistema *Blockchain* è un meccanismo chiamato *Proof of Work* (PoW), tradotto “prova di lavoro”. Le transazioni in *bitcoin* non vengono approvate da un singolo *miner*, ma dalla rete che collabora sulla *Blockchain*. Il meccanismo di *Proof of Work* definisce un calcolo complesso per la risoluzione degli algoritmi che validano le transazioni.

Perché una transazione sia considerata valida, infatti, deve essere approvata da almeno il 50% + 1 dei *miner*, o nodi. Questo sistema fa sì che, se un malintenzionato volesse

manomettere il registro distribuito delle operazioni, dovrebbe raggiungere più della metà dei computer che lavorano sulla rete *Bitcoin*.

Recentemente si è introdotto un nuovo meccanismo di gestione denominato *Proof of Stake* (PoS), mediante il quale le operazioni vengono convalidate solo da chi detiene, nell'insieme, più della metà del capitale di *bitcoin* circolante. Il sistema *Proof of Stake* rende completamente inutile qualsiasi tentativo di manomissione dei registri, perché, se per modificare i registri bisogna possedere più della metà dei *bitcoin* in circolazione, allora non si avrà più alcun interesse reale nel

manomettere la *Blockchain*.

I concetti, in realtà, sono un po' più complicati di così, ma direi che per adesso può bastare.

Una curiosità: il primo blocco della *Blockchain*, nato il 3 Gennaio 2009 e chiamato “blocco genesi” (*Genesis Block*), ha generato 50 *bitcoin* di ricompensa, ma questi non sono spendibili per un'impostazione del sistema.

3. COME VARIA IL PREZZO DEL BITCOIN?

Sia chiaro, non so dirvi come varierà nel tempo il valore dei *bitcoin*: se lo sapessi, questo libro vi sarebbe costato molto di più.

Se lo avete acquistato pensando che questo capitolo fosse dedicato alle predizioni magiche, tengo precisare che

non si effettuano rimborsi.

In questa sede parleremo “solamente” del meccanismo che ne determina il prezzo.

La mia regola d'oro, che vorrei trasmettere anche a voi, è quella di investire solo in qualcosa che conoscete. È una regola semplice, ma per niente scontata.

Se state leggendo questo libro, vuol dire che avete sentito parlare di *Bitcoin* e magari vorreste investire in criptovalute. Probabilmente qualcuno di voi lo ha già fatto, anche preso dall'euforia che i notiziari e Internet hanno provocato, ma non c'è niente di

più sbagliato dell'aver investito in qualcosa senza essersi documentati a dovere.

Immaginiamo di avere da parte un piccolo risparmio e di volerlo far fruttare.

Abbiamo la possibilità di fare un prestito a due aziende: la prima, che conosciamo bene e di cui siamo anche clienti, è un'azienda solida che utilizzerà i soldi ricevuti per acquistare un macchinario che ne aumenterà la produttività, e per il nostro prestito ci riconoscerà il 5% di interessi; della seconda, invece, non abbiamo mai sentito parlare, né sappiamo come utilizzerà i nostri risparmi, ma sappiamo

che ci riconoscerà il 10% di interessi.

A quale azienda dovremmo prestare i nostri risparmi?

Magari di getto avete pensato alla prima, perché è più sicura e sappiamo che ci ripagherà il prestito con gli interessi. Oppure avete pensato alla seconda, perché, riconoscendoci il doppio degli interessi, è la più profittevole.

La risposta corretta è: dipende.

La prima cosa da fare è sempre quella di informarsi.

Della seconda azienda non abbiamo

mai sentito parlare e non sappiamo come utilizzerà i nostri risparmi? Bene: proviamo a capirlo. Essa, infatti, potrebbe rivelarsi un'ottima azienda con progetti di espansione imminenti e sarebbe un peccato rifiutarle il prestito solo perché non la conosciamo. Al contrario, allo stesso tempo, potrebbe rivelarsi sull'orlo del fallimento e noi rischieremmo moltissimo prestandole i nostri risparmi senza esserci informati della sua situazione.

Nel caso in cui non riuscissimo a recuperare le informazioni necessarie per valutare con la dovuta attenzione, ricordiamoci che sono risparmi faticosamente racimolati, perciò

dovremmo prediligere la prima azienda, perché la conosciamo e ci fidiamo di lei.

Sia ben chiaro che, in entrambe le ipotesi, corriamo sempre il rischio di perdere, in tutto o in parte, i nostri risparmi.

Bene, ora che conoscete la mia regola d'oro, cerchiamo di capire com'è determinato il prezzo dei *bitcoin*.

Se vi è capitato di partecipare a un'asta, il concetto vi risulterà semplicissimo, infatti il prezzo dei *bitcoin* varia in base alla domanda e all'offerta. Possiamo quindi dire che il prezzo dei *bitcoin* è un prezzo di

mercato.

Ma proseguiamo con il nostro esempio per non lasciare dubbi.

Abbiamo affidato i nostri risparmi a una delle due aziende di cui abbiamo parlato poco sopra e siamo tornati a essere allevatori di pecore. Vi ricordate che cosa vendeva il vicinato? Esatto, cavolfiori.

Decidiamo di mettere in vendita una pecora al prezzo di 100 cavolfiori, sperando che sia una buona offerta. Se i giorni passano e nessuno ci ha chiesto la pecora, evidentemente la nostra offerta non ha incontrato la domanda del vicinato. Il prezzo di mercato non è,

dunque, 100 cavolfiori.

Decidiamo allora di abbassare il prezzo della pecora a 60 cavolfiori. Questa volta ci è andata bene, e riceviamo due richieste. Peccato che la pecora in vendita sia solo una! Nessun problema, la vendiamo a chi ci offre di più. Il prezzo di mercato, quindi, non è nemmeno di 60 cavolfiori.

Alla luce di questo, alziamo il prezzo della nostra offerta a 80 cavolfiori, ed ecco che riceviamo un'unica domanda. Vendiamo la pecora al prezzo di mercato di 80 cavolfiori.

In linea teorica, questo semplice meccanismo può essere applicato al

mercato dei *bitcoin*, come a quello dei titoli o delle valute in generale, ma nella realtà dei fatti è molto più complesso. Basti immaginare a quanti operatori trattano contemporaneamente gli stessi affari, mentre noi nell'esempio eravamo da soli senza concorrenza diretta.

Questo ci fa capire come il prezzo dei *bitcoin* sia estremamente volatile, perché dipende da tantissimi operatori che agiscono in modi imprevedibili, o quasi.

Abbiamo capito che il prezzo è dato dalla domanda e dall'offerta, ma come variano domanda e offerta?

I motivi della variazione di domanda

e offerta sono molteplici, ma il più importante, nel caso dei *bitcoin*, è la divergenza di opinione sulle prospettive della moneta.

Insomma, per farla semplice: chi ha dei *bitcoin* e crede che il prezzo di questi crollerà, non vedrà l'ora di liberarsene vendendoli, al fine di evitare perdite ai suoi risparmi. Viceversa, chi è convinto che il prezzo dei *bitcoin* aumenterà, farà di tutto per acquistarli, così da ottenerne un guadagno quando questi varranno di più.

Queste due situazioni fanno sì che il prezzo del *bitcoin* prenda una direzione che, seppur temporanea, scatenerà reazioni diverse tra gli altri operatori.

Infatti, se per esempio il prezzo dovesse scendere, gli operatori potranno vendere i *bitcoin* in loro possesso per paura di perdere parte dei risparmi, oppure comprarne di nuovi visto che il prezzo è sceso e ipotizzano di poterci ricavare maggiori guadagni.

Come vedete, la variazione dipende dalle prospettive che gli operatori hanno sul futuro dei *bitcoin*.

Ed ecco che torniamo all'importanza dell'informazione.

Se conosciamo bene i *bitcoin*, abbiamo letto questo libro e ci informiamo costantemente sulle loro novità, riusciremo a capire come gli

operatori vedono il futuro della nostra moneta virtuale e, di conseguenza, avremo gli strumenti per capire il mercato e il suo prezzo.



Per saperne di più...



Il grafico qui riportato è una rappresentazione della domanda e dell'offerta.

Possiamo individuare due aree: quella a sinistra è l'area della domanda, quella a destra è l'area dell'offerta. Tra le due aree è individuato il prezzo di mercato.

Leggere questo tipo di grafico è più semplice di quel che si può immaginare. Proviamo a capire come.

L'area della domanda individua la quantità di *bitcoin* che il mercato è disposto ad acquistare a una certa cifra. Più è alta la linea in un determinato punto, maggiore è la richiesta di *bitcoin* a quel dato prezzo.

Viceversa, l'area dell'offerta individua la quantità di *bitcoin* che il mercato ha intenzione di vendere al raggiungimento di un certo valore. Anche qui, naturalmente, più alta è la linea, maggiore sono i venditori disposti a cedere i *bitcoin* a un dato prezzo.

Nel punto in cui le due aree si toccano troviamo il prezzo attuale del *Bitcoin*, ovvero il prezzo di mercato, dove venditori (offerta) e acquirenti (domanda) si incontrano.

Questo grafico non è utilizzato solo per i *bitcoin*, ma per tutti gli strumenti finanziari influenzati direttamente dal mercato, ovvero da domanda e offerta.

4. QUALCUNO HA MAI DAVVERO GUADAGNATO CON I BITCOIN?

Questa è un'altra di quelle domande che probabilmente mi avrebbe fatto arricchire se avessi ricevuto un centesimo di *bitcoin* per ogni volta che mi è stata posta. Se così fosse stato, adesso sarei sicuramente uno di quelli

che ha guadagnato con i *bitcoin*.

Lo so che ve lo state chiedendo, ma no, non ho ricevuto *bitcoin* per queste domande...

Agli inizi *Bitcoin* era una bella idea, ma così lontana dalla realtà che nessuno le dava il peso che ha oggi.

Come sicuramente saprete, quando si parla di innovazioni il tempismo è la cosa più importante. L'idea più brillante può rivelarsi un fiasco totale se presentata nel momento sbagliato.

Prendiamo per esempio il *selfie stick*, il braccio telescopico che con lo smartphone ci permette di scattare foto

in modalità autoscatto: un'invenzione geniale nata dall'esigenza delle nuove tecnologie, penserete. E invece no, il *selfie stick* è stato presentato all'ufficio brevetti nel 1983, poi brevettato nel 1985 con il nome di "Telescopic Extender". Il suo inventore, Hiroshi Ueda, lo aveva progettato per le macchine fotografiche, dotandolo anche di uno specchio per vedere la propria immagine riflessa e potersi inquadrare meglio.

Come potete immaginare, l'invenzione non ebbe alcun successo o, perlomeno, non ebbe il successo che hanno oggi i *selfie stick*. Perché? Tempismo sbagliato. Un'invenzione

rivoluzionaria, ma troppo in anticipo.

FIG. 17a

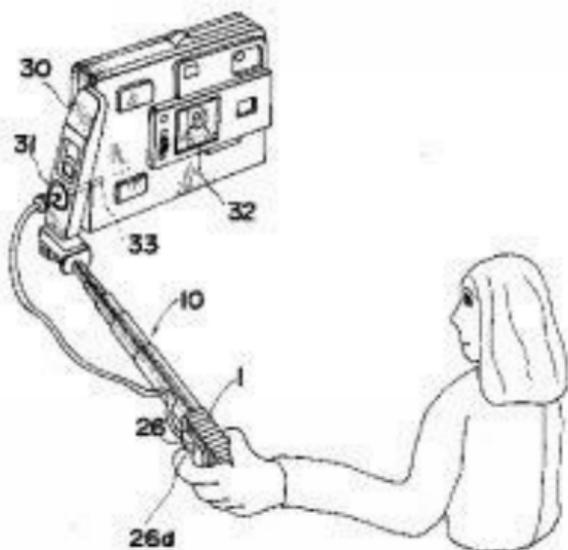


FIG. 17b



FIG. 17c



Per i più scettici ho riportato un estratto del brevetto originale, scaduto nell'anno 1993.

Abbiamo anche l'esempio opposto.

Quando parlo di innovazione cerco sempre di fare riferimento a situazioni comuni che siano facilmente riscontrabili. Come non citarvi, quindi, il caso Facebook?

Facebook è il social network più grande di sempre. Ormai si dà per scontato. Vorrei però farvi riflettere su come sia diventato quello che è oggi.

Prima di Facebook nessuno avrebbe mai utilizzato il proprio nome e

cognome online. Si utilizzavano i *nickname*, o soprannomi. Non perché nessuno li chiedesse, ma perché si sentiva ancora molta diffidenza verso Internet. Facebook ha avuto la fortuna di trovare il momento giusto, nel quale gli utenti erano più in confidenza con la rete, e ha riproposto l'antico nome e cognome. Con la scusa si ritrovava gente che non si sentiva da anni, e così il network continuava a crescere a dismisura.

■ Anche per il *Bitcoin* è valsa la regola del tempismo. È stata un'ottima idea fin dal principio, ma partita troppo in anticipo.

Inizialmente snobbato dai più, si

pensava a un buco nell'acqua. Un'idea già vecchia applicata a un concetto, quello di moneta, molto distante a ciò che si potrebbe pensare come un mercato libero.

Poi, con il tempo, nell'incertezza finanziaria globale, dove tutto il denaro è centralizzato e controllato dai soliti pochi, abbiamo cominciato a guardare al *Bitcoin* con più interesse. Essendo, inoltre, una valuta anonima, è sempre stata al centro degli attacchi e delle minacce informatiche come ottima moneta da riscatto. Per non parlare delle possibilità di riciclaggio di denaro sporco. Anche questo ha certamente contribuito alla sua diffusione.

L'interesse è poi esploso con la pubblicità dei mass media e di Internet, trasformandolo in un fenomeno virale.

Qui è cambiato qualcosa.

A fine 2011 un *bitcoin* valeva circa 5 dollari.

Lo stesso *bitcoin* a fine 2017 è arrivato a valere quattro mila volte di più, circa 20.000 dollari.

Se avessimo comprato 100 *bitcoin* nel 2011 per 500 dollari, sette anni dopo avremmo avuto 2.000.000 dollari in *bitcoin*.

In una situazione di mercato come

quella di *Bitcoin*, quindi, sì, qualcuno ci ha davvero guadagnato.

Ma è stata una situazione molto particolare: si è creato un nuovo mercato, qualcosa che prima non esisteva.

Un mercato, nella sua fase di nascita, non è un mercato regolare. Un mercato regolare ha degli alti e dei bassi, delle trattative. In quello di *bitcoin* no: l'interesse generato dalla nuova moneta digitale era più alto di qualunque quantità di *bitcoin* venduta.

La verità è che fino alla fine del 2017 era difficile perdere investendo in *Bitcoin*, per via delle condizioni di

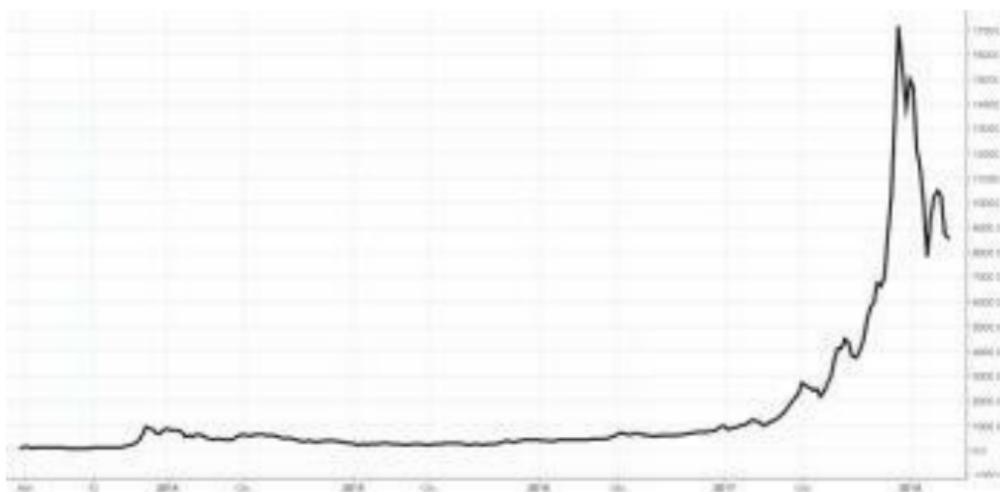
mercato.

Volete sapere quanto è stato guadagnato? Difficile a dirsi. Considerate che un utente mediamente esperto, abituato ai mercati normali, difficilmente avrebbe atteso sette anni per rivendere i suoi *bitcoin*. Si sarebbe accontentato di un 30% di guadagno, magari riacquistando successivamente altri *bitcoin* per ripetere l'operazione.

Diffidate, quindi, di chi si vanta di aver guadagnato quattro mila volte l'investimento. O è un veggente, o si era dimenticato i suoi *bitcoin* sul conto, oppure, più probabilmente, è un simpatico ciarlatano.



Per saperne di più...



Questo grafico rappresenta la variazione del valore di un *bitcoin* nel periodo che va da aprile 2013 a marzo 2018.

Come è facilmente osservabile, partendo dal valore di circa 90 dollari americani del 2013 è arrivato senza troppe incertezze a sfiorare i 20.000

dollari nel dicembre 2017.

Probabilmente l'investitore che ha investito in questo lasso di tempo ci ha guadagnato, ma l'aver scelto il periodo giusto, di per sé, non lo rende un esperto semplicemente perché il mercato non ha fatto altro che salire.

Ma come vedete, un mercato non può andare in una sola direzione...

5. PERCHÉ SI PARLA DI "BOLLA" DEI BITCOIN?

Chissà perché sono passate di moda le Big Babol, quelle gomme da masticare rosa a cui era addirittura dedicato un concorso per chi riusciva a fare la bolla più grossa. Che poi chissà che cosa si vinceva, non credo di averlo mai saputo.

Quello che è certo, è che i tulipani olandesi avrebbero vinto, e se volete capire dove voglio andare a parare, armatevi di pazienza, ch  ora vi tocca un po' di storia...

■Verso la fine del Cinquecento, l'Olanda era impazzita per i tulipani. Con l'avvento della commercializzazione di questi fiori in Europa, gli Olandesi cominciarono a coltivarli. Le qualit  pi  rare divennero beni di prestigio, tanto da essere scambiate alla Borsa di Amsterdam. I prezzi dei tulipani decollarono. Erano talmente richiesti che i fiorai vendevano bulbi in coltivazione o, addirittura, ancora da coltivare, a fronte di un

acconto con saldo a fioritura terminata.

Insomma, nascevano i primi *futures*, ovvero strumenti finanziari per cui venditore e acquirente si impegnano a effettuare uno scambio a una data scadenza con prezzi stabiliti a priori.

Capite bene che chi acquistava un bulbo non ancora coltivato, non poteva che farlo per speculazione finanziaria, ovvero per trarne del profitto.

Pensate che per cavalcare l'onda dei tulipani si arrivò addirittura a vendere immobili per acquistare bulbi, nella speranza di guadagnarci.

Il record fu registrato dal *Semper*

Augustus, il bulbo di tulipano più famoso, venduto per la modica cifra di seimila fiorini nella metà del Seicento. Considerate che lo stipendio medio annuo si aggirava intorno ai 150 fiorini. Avete letto bene, annuo.

Ma quanto poteva durare?

Non molto. I commercianti di tulipani, arrivati alle cifre impensabili che avete letto, non potendo più gonfiare il prezzo dei loro fiori, a un certo punto dovettero abbassarlo.

E quando gli investitori di tulipani si accorsero che il valore dei loro bulbi non riusciva a rimanere quello sperato, a loro volta iniziarono a venderli. Così il

prezzo crollò, riducendo molti in miseria. La prima bolla della storia era scoppiata, anno 1637.

Cosa c'entra con i *bitcoin*?

Come abbiamo visto nel capitolo precedente, il valore dei *bitcoin* è aumentato a dismisura nel tempo e, soprattutto nell'anno 2017, ha avuto una crescita esponenziale.

Quando si parla di “bolla” del *Bitcoin* si fa riferimento al suo valore, ovvero al prezzo che si è disposti a pagare per ogni singola moneta digitale in dollari, o in euro.

Il concetto di bolla, o bolla

speculativa, nella finanza attinge proprio dall'idea delle gomme da masticare.

Immaginiamo un concorrente di Big Babol gonfiare più che può la sua gomma da masticare creando una bolla, fino a farla esplodere.

Possiamo facilmente applicare il concetto al mercato del *Bitcoin*, nel quale si è generata una quantità di domanda importantissima. Infatti, in un periodo senza valide alternative di investimento, oltre ai più esperti, molti estranei al settore si sono avvicinati alle monete virtuali anche per la continua pubblicità di tv, giornali e internet, contribuendo all'innalzamento del suo valore. Ricordate il principio di

domanda e offerta di qualche capitolo fa, vero?

Quando si parla di tendenza di mercato, anche se in contesto finanziario come quello del *Bitcoin*, parliamo di *trend*. Se il valore dello strumento finanziario sale, il *trend* è positivo, se scende, il *trend* è negativo.

Il trend di *Bitcoin* è stato quasi sempre positivo, fino al 2018. Questo ha portato a un incremento ingiustificato del suo valore, che alla prima incertezza ha vacillato bruscamente verso il basso. Esattamente come esplode la bolla di gomma per la troppa espansione, lo stesso ha fatto il prezzo dei *bitcoin*,

seppur mantenendo un valore importante. Questo vuol dire che il mercato del *Bitcoin* è sulla via della normalizzazione, perché, ormai lo sappiamo, un mercato non può essere monodirezionale per sempre.

Pensate a quanto pesi il mercato dei *bitcoin*, un mercato che vale centinaia di miliardi di dollari, e pensate a come sia possibile che abbia dovuto aspettare tutti questi anni per essere riconosciuto e per ricevere le prime proposte di regolamentazione. Finché un mercato non è trattato come tale, difficilmente si comporterà come se lo fosse.

E questo è proprio ciò che è successo a *Bitcoin*.



Per saperne di più...

Approfittiamo di questo spazio per deviare un momento dal mondo dei *bitcoin* e parlare della crisi del 2008.

Perché? Perché spesso le crisi partono proprio da una bolla.

Attraverso media, giornalisti, politici e professionisti, tutti abbiamo sentito parlare dei mutui *subprime*. Bene, che cosa sono?

Sono chiamati mutui *subprime* quei mutui che presentano interessi più elevati della norma, che vengono concessi a soggetti che non hanno possibilità di accedere alle normali

condizioni di finanziamento, per la loro alta probabilità di insolvenza.

A partire dal 2000, in America, si è assistito a una crescita esponenziale dei prezzi delle abitazioni, complice anche il basso tasso di interesse dei mutui offerto dalle banche.

Vista la crescita della domanda di abitazioni, e quindi dei loro prezzi, le banche hanno iniziato a concedere prestiti anche a chi normalmente non avrebbe potuto goderne. Le banche avevano la garanzia che, qualora il mutuatario fosse risultato insolvente, avrebbero potuto pignorare l'immobile e rivenderlo.

Non è finita qui: ciò che ha portato ulteriore difficoltà è stata la cartolarizzazione, un altro termine molto in voga fino a poco tempo fa.

Le operazioni di cartolarizzazione consistono, in questo caso, nel trasferire i mutui bancari a società appositamente costituite, che li trasformano in titoli che a loro volta vengono venduti agli investitori.

In questo modo le banche, invece di dover aspettare la durata del mutuo per rientrare degli interessi del prestito, hanno a disposizione altri fondi, ricevuti per il trasferimento dei mutui stessi, che utilizzano per erogare ulteriori finanziamenti.

Le società che hanno ricevuto i mutui dalle banche incasseranno direttamente le rate, e quindi gli interessi, al posto delle banche stesse. Inoltre, trasformano i mutui in titoli, emettendo delle obbligazioni che propongono agli investitori.

A queste obbligazioni è attribuita una valutazione in base alla loro affidabilità e rischiosità, chiamata comunemente *rating*.

Vista la difficoltà di valutazione delle obbligazioni nate da operazioni di cartolarizzazione, in quanto estremamente complesse, ci si affida a società preposte chiamate appunto

agenzie di *rating*.

Come è facile immaginare, questi prodotti finanziari finirono presto per girare il mondo, arrivando anche in Europa.

Le agenzie di *rating*, però, non sembravano avere modelli sufficientemente evoluti per valutare correttamente le obbligazioni. Forse potevano addirittura avere interesse nel classificare i titoli in maniera non corretta, chi può dirlo. Di certo finirono per valutare affidabili anche obbligazioni che non lo erano affatto. Voi mettereste sullo stesso piano di affidabilità i mutui *subprime* e i mutui regolari?

Ad ogni modo, quando i tassi di interesse sui mutui si alzarono, iniziò ad aumentare il tasso di insolvenza dei mutuatari che non potevano più permettersi di pagare le rate.

Al contempo, la domanda immobiliare si abbassò e con essa i prezzi delle abitazioni, ovvero le garanzie dei mutui insoluti.

Scoppiò la bolla immobiliare americana.

Come la crisi raggiunse l'Europa e il resto del mondo è intuibile: con le obbligazioni.

6. QUALI SONO LE POTENZIALITÀ DELLA BLOCKCHAIN?

In Italia si pagano troppe tasse.

Tutti lo dicono, pochi ci riflettono.

Magari chi lo dice non ha mai verificato quante tasse paga e probabilmente non conosce la differenza

tra tasse e imposte, ma in Italia si pagano troppe tasse, comunque.

Le tasse sono quei tributi che vengono corrisposti con lo scopo di ottenere in cambio dei servizi, pensiamo alla tassa sui rifiuti o alla recente tassa sui sacchetti di plastica.

Le imposte, invece, sono quei tributi che vengono calcolati sulla base del reddito generato e corrisposti senza ricevere alcun servizio, ma al fine di coprire la spesa pubblica. Pensiamo all'IRPEF, ovvero all'imposta sul reddito delle persone fisiche.

Ora, unificando i concetti appena appresi e chiamandoli semplicemente

tasse, cerchiamo di capire se in Italia ne paghiamo davvero troppe.

Diciamo che l'Italia è al 34° posto nella classifica della pressione fiscale e tributaria dei Paesi membri dell'OCSE^[1] (dove al primo posto troviamo il Paese con la minore pressione e all'ultimo quello con la maggiore).

L'OCSE è l'Organizzazione per la Cooperazione e lo Sviluppo Economico, un organo internazionale di studi economici per i Paesi membri, che al momento in cui scrivo sono trentacinque.

Esatto, l'Italia è al penultimo posto della classifica OCSE.

So che cosa vi state chiedendo e vi rispondo subito. L'ultimo Paese in classifica è la Francia.

Alla luce di questo, possiamo affermare che in Italia si pagano davvero troppe tasse e, se ripetere questo mantra non dovesse bastare, potete sempre fare bella figura davanti agli amici raccontando quello che avete letto.

Adesso, però, parliamo del primo in classifica.

Il Paese più competitivo per la pressione tributaria tra i membri OCSE è l'Estonia, e lo è da ben quattro anni

consecutivi. Quando ne parlo, tipicamente, la domanda che ricevo subito dopo è: «Ma come, non è la Svizzera?». No, pur essendo ben classificata^[2].

L'Estonia è al primo posto della classifica OCSE perché è il Paese più digitalizzato al mondo^[3].

Dal 2001 ha introdotto l'identità digitale per i suoi cittadini, cosa che ha permesso loro di votare online dal 2005, altro primato da riconoscere a questo Paese.

Inoltre, l'Estonia ha iniziato a studiare la tecnologia della *blockchain*

già dal 2008, riuscendo a renderla operativa dal 2012 in vari settori, come quello sanitario, giuridico o legislativo.

Tutte queste digitalizzazioni si traducono in un importante risparmio di costi e tempo che permettono, anche, una minore pressione fiscale.

La *blockchain* è una tecnologia che ben si presta a rivoluzionare i rapporti fiduciari, la burocrazia classica, i flussi cartacei e il data-entry umano.

Se avete letto il secondo capitolo di questo libro, sono certo avrete compreso a grandi linee come funziona la *blockchain* per *Bitcoin*.

Okay, ricapitoliamo ch     meglio...

La *blockchain* funziona come un registro di dati non centralizzato, ovvero distribuito su tutta la sua rete, e ogni partecipante ne possiede una copia. Il fatto che ne esistano pi  possessori fa s  che il controllo dei dati in esso contenuti sia svolto da tutti i partecipanti, e questo rende la *blockchain* un sistema sicuro, in quanto difficilmente un malintenzionato riuscir  a modificare i dati in tutte le copie dei registri. Inoltre, l'inserimento nel registro di ogni informazione aggiuntiva deve essere autorizzato da tutti i *miner*, ovvero i possessori di una copia.

Bench  sia stata la moneta digitale

più famosa del momento a rilanciare la tecnologia della *blockchain*, quest'ultima può essere utilizzata in moltissimi settori.

Ma, come al solito, vediamo qualche caso concreto.

In Italia esiste il pubblico registro immobiliare, un registro presso il quale sono iscritti tutti gli atti riguardanti i beni immobili. La legge prevede, infatti, l'obbligo di pubblicazione di alcune informazioni come, ad esempio, il trasferimento della proprietà di un immobile o del suo usufrutto.

Immaginiamo di utilizzare la *blockchain* come pubblico registro

immobiliare.

Sappiamo che la *blockchain* è un registro pubblico, per cui le informazioni immobiliari che andremo ad annotare saranno a norma di legge. La *blockchain* non richiede l'intervento umano per la verifica e modifica delle informazioni sugli immobili, quindi chiunque potrebbe trasferire la proprietà del proprio immobile, o concederlo in locazione, in completa autonomia.

L'effettivo possesso dell'immobile e le eventuali ipoteche verrebbero automaticamente verificate dal sistema.

Si avrebbero, inoltre, meno problemi in caso di eredità. Il

testamento potrebbe, infatti, essere un altro possibile impiego per la tecnologia della *blockchain*, dove questo, una volta registrato, sarebbe certo, autenticato e modificabile esclusivamente dal reale autore.

Un altro esempio sono i voti elettorali.

Se a ciascun cittadino è attribuita un'identità digitale, è facile utilizzare la *blockchain* per registrare il voto di ognuno di essi.

La *blockchain* dovrebbe verificare che a ogni identità digitale corrisponda un unico voto, crittografandolo per mantenerlo segreto.

Pensate, si potrebbe votare da qualunque parte del mondo, evitando, per altro, le presunte truffe delle schede elettorali comprate all'estero. Non solo, si avrebbero le statistiche in tempo reale evitando scrutini e azzerando la relativa spesa pubblica.

Un altro caso interessante potrebbe essere quello delle organizzazioni di beneficenza e non governative.

Molto spesso ciò che frena la solidarietà è la mancanza di fiducia. Chi ci assicura che i soldi devoluti in beneficenza andranno effettivamente alle persone bisognose?

Potrebbe farlo la *blockchain*. Infatti,

essendo un registro pubblico, basta poco per rendere tracciabili tutte le operazioni eseguite.

La *blockchain* potrebbe essere impiegata quindi in un sistema di pagamento, tipo il *Bitcoin*, ma con la possibilità di tracciare i flussi di denaro, verificando effettivamente come vengono spese le donazioni.

Fortunatamente, su quest'ultimo punto, qualcuno si è già mosso. Sono nate alcune monete digitali, alternative al *Bitcoin*, anch'esse basate sulla tecnologia *blockchain*, che si propongono proprio tracciare le donazioni fatte alle organizzazioni di beneficenza. Alcune permettono

addirittura di raggiungere i diretti interessati senza passare dalle stesse organizzazioni.

Come si intuisce, le potenzialità della *blockchain* sono davvero molte e molto importanti, ma non finisce qui.

Si stanno studiando i cosiddetti contratti intelligenti, o *smart contract*, programmi che assicurano il rispetto delle clausole di un contratto al verificarsi di determinate condizioni previste dal contratto stesso.

Mi spiego meglio. Prima abbiamo parlato del pubblico registro immobiliare e di come questo potrebbe essere ripensato sotto forma di

blockchain. Uno *smart contract*, in questo caso, potrebbe essere il contratto di compravendita di un immobile. Un contratto le cui regole e condizioni vengono digitalizzate tramite un programma che trasferisce la proprietà dell'immobile dal venditore all'acquirente non appena il pagamento è verificato, intervenendo direttamente sul registro pubblico. Sia il pagamento che il trasferimento dell'immobile sono autorizzati dalla *blockchain*, che ne garantisce la sicurezza e autenticità.

Rimanendo in tema di immobili, pensiamo al contratto di affitto di un appartamento. Dotando l'ingresso dell'appartamento di una serratura

elettronica (come quelle delle stanze d'albergo, per intenderci), lo *smart contract* potrebbe prevedere che, qualora la rata dell'affitto non venisse incassata dal proprietario, la serratura elettronica impedisca l'accesso con la chiave dell'inquilino. Naturalmente finché questi non torni a pagare l'affitto.

Ancora, lo *smart contract* potrebbe essere utilizzato anche nel campo delle assicurazioni. In vista delle ferie, immaginiamo di stipulare una polizza di annullamento volo sotto forma di contratto intelligente. Il contratto verificherà automaticamente lo stato del nostro volo e, qualora venisse malauguratamente annullato,

provvederebbe a rimborsarci quanto pattuito. Certo, è una magra consolazione, lo so.

In sostanza, gli *smart contract* garantiscono il rispetto delle clausole di un contratto dove al momento servono necessariamente figure esterne, come un avvocato o un notaio.

La *blockchain* e gli *smart contract*, in molti settori, possono rendere le informazioni più sicure e più trasparenti, se necessario. Possono far risparmiare tempo e soldi sia pubblici che privati, grazie agli automatismi di verifica dei dati, degli utenti e delle condizioni contrattuali.

Insomma, questa tecnologia ci accompagnerà sicuramente per molto tempo.



Per saperne di più...

Dopo aver elencato le potenzialità degli *smart contract*, può essere interessante vederne insieme anche i punti deboli.

Il primo fra tutti è la riservatezza delle informazioni. Sappiamo bene che la *blockchain* è fondata su un registro pubblico e distribuito. Questa caratteristica rende molto complicato nascondere i dati che transitano sulla *blockchain* e, quindi, all'interno degli *smart contract*.

Gli *smart contract*, come già accennato, sono dei software a tutti gli effetti. Per poter funzionare devono

essere programmati, proprio come un'applicazione per smartphone o per computer. E, come tutti i programmi, non è sempre detto che funzionino perfettamente alla prima versione. Insomma, pensiamoci un attimo, quante volte sono richiesti gli aggiornamenti delle applicazioni che utilizziamo? Spessissimo. Questi aggiornamenti servono a riparare errori di programmazione oppure a incrementare le funzionalità.

Purtroppo con gli *smart contract* non funziona così. Sono sì, dei software, ma non possono essere aggiornati. Se uno *smart contract* contiene un errore, non può essere modificato, ma deve

essere sostituito con un altro *smart contract*.

Il motivo è semplice. Se il contratto intelligente potesse essere modificato a piacimento, anche successivamente alla sua pubblicazione, non sarebbe un contratto con effetti certi. Un esempio? Abbiamo stipulato uno *smart contract* con un intermediario finanziario che ci garantisce il 3% annuo di interessi sulle somme vincolate presso di lui. Immaginate se, una volta trasferite e vincolate le somme, l'intermediario modificasse il contratto azzerando il rendimento annuo garantito. Potrebbe addirittura modificare lo *smart contract* rendendo di fatto il nostro trasferimento

di denaro una donazione a suo favore. Insomma, ci siamo capiti.

Fortunatamente gli *smart contract* sono imm modificabili, ma se si viene a conoscenza di un errore di codice è necessario ricominciare da zero, creando un nuovo *smart contract*. E spesso questi errori escono allo scoperto molto tardi.

Un'altra debolezza, se così si vuol chiamare, è che, se il contratto intelligente necessita di dati che sono estranei alla *blockchain*, è necessario fidarsi del soggetto che li inserisce.

Immaginiamo di avere un contratto che utilizzi i tassi di cambio

dell'Euro/Dollaro. Questi dati, non essendo presenti sulla *blockchain*, dovranno essere inseriti da un soggetto incaricato al quale sarà necessario prestare la propria fiducia.

Su quest'ultimo punto ritengo di dover fare una precisazione. Spesso sento dire che notai e avvocati saranno sostituiti dalla *blockchain* e dagli *smart contract*, ma non trovo ci sia nulla di più sbagliato. Le professioni cambieranno, starà ai professionisti adeguarsi alle nuove tecnologie.

Credo che un contratto, seppur digitale, possa comunque essere ideato e validato da un avvocato o da un notaio, e perché no, da loro anche programmato.

7. OLTRE AI BITCOIN C'È DI PIÙ?

Giunti a questo punto è necessario introdurre le monete virtuali in generale.

Finora abbiamo parlato di moneta virtuale, o criptovaluta, riferendoci per semplicità solo al *Bitcoin*. In realtà, come già accennato in precedenza, i *bitcoin* non sono l'unica moneta virtuale

esistente, semmai sono la prima criptovaluta basata sulla tecnologia *blockchain*. Con l'avvento di *Bitcoin* sono apparse sul mercato – e continuano ad apparire – molte altre monete digitali. Basti pensare che alla prima stesura di questo capitolo erano circa un migliaio, attualmente sono raddoppiate.

A che cosa servono tutte queste monete differenti?

Me lo chiedo anch'io, anche se, purtroppo, la risposta la conosco bene. Quasi a nulla, almeno per il momento. Ma arriviamoci per gradi, come al solito.

Bitcoin nasce come un progetto

innovativo, interessante e ambizioso, fin da subito oggetto di studio da parte di molti sviluppatori e osservatori. Immediatamente, infatti, iniziarono a manifestarsi pareri contrastanti sulla sua struttura e la sua tecnologia, sui suoi punti deboli e punti di forza.

In poco tempo comparvero le prime criptomonete alternative al *Bitcoin*, dette in gergo *altcoin* (dove *alt* sta per *alternative*, “alternativo”, e *coin*, “moneta”). Esse si differenziano dai *bitcoin* per finalità e tecnologie.

■ L'*altcoin* attualmente più diffusa al mondo si chiama *Ether*. Il suo successo è dovuto al fatto che è l'unica moneta a poter essere utilizzata sulla sua

piattaforma, chiamata *Ethereum*. *Ethereum* è la più famosa piattaforma per la creazione di contratti intelligenti, proprio quelli di cui abbiamo parlato nel capitolo precedente.

Ma che cosa c'entra una moneta virtuale con una piattaforma per i contratti intelligenti?

Perché ogni contratto intelligente registrato sulla *blockchain* di *Ethereum* funzioni, deve essere pagata una commissione in *Ether*.

Un po' come succede per *Bitcoin*, dove i *miner* si occupano di validare le operazioni, in *Ethereum* i *miner* si occupano, oltre che di validare le

operazioni in *ether*, di far funzionare i contratti intelligenti, ricevendo in cambio un piccolo compenso.

Per farla breve, se volessimo creare il nostro *smart contract*, dovremmo andare sulla piattaforma di *Ethereum*, progettare il nostro contratto definendone il compito e come questo verrà svolto, infine pagare una somma in *Ether* alla piattaforma per renderlo funzionante.

■Quello che abbiamo capito delle criptovalute è che per funzionare devono avere una propria *blockchain*.

Esistono, però, delle monete che sfruttano la *blockchain* di un'altra

criptovaluta, come potrebbe essere quella di *Ethereum*. Queste monete sono chiamate *token*, ovvero gettoni, perché, di fatto, dipendono dalla *blockchain* sulla quale risiedono.

Possiamo paragonare i *token* ai gettoni di un autolavaggio. Ci rechiamo alla cassa e compriamo i gettoni con una moneta riconosciuta, supponiamo gli euro. Sponderemo i gettoni acquistati per uno specifico servizio, ovvero lavare l'automobile. Quei gettoni non hanno valore al di fuori dell'autolavaggio ma sono necessari per utilizzarne i servizi.

Come i gettoni dell'autolavaggio hanno un corrispettivo in euro, i *token*

che sfruttano la *blockchain* di una specifica moneta avranno un prezzo stabilito in quella moneta. Quindi un *token* che usa la *blockchain* di *Ethereum* avrà un valore stabilito in *Ether*, per esempio.

Riepiloghiamo brevemente. Una moneta, in inglese *coin*, è una critpovaluta dotata di propria *blockchain* e quindi è indipendente. Un gettone, in inglese *token*, è un'unità di scambio che si affida a una *blockchain* già esistente.

Fatta questa dovuta e importante precisazione, torniamo a parlare di monete digitali in generale, intendendo

con questo termine anche i *token*, per semplicità. Se volete approfondire l'argomento, a fine capitolo c'è la solita pedante sezione "Per saperne di più".

Iniziamo a intuire come intorno a una moneta digitale possa esistere uno scopo che va oltre quello puramente "di scambio".

Possiamo, quindi, individuare delle categorie di criptovalute specifiche, in base allo scopo per il quale sono state create.

Conosciamo bene, ormai, le criptovalute utilizzate come strumento di pagamento generico. Queste valute possono essere scambiate con altre

monete digitali, come *Bitcoin*, o altre monete legali, come gli euro o i dollari. Ma non solo: possono essere scambiate anche per beni e servizi, ove accettate, come si farebbe con le monete legali, con l'obiettivo di diventarne il sostituto.

Esistono poi criptovalute che vengono corrisposte per usufruire unicamente di specifici servizi o per acquistare determinati beni. Esse non sono direttamente scambiabili con altre monete per pagamenti generici. Per intenderci, è esattamente il caso dell'autolavaggio di cui abbiamo parlato prima: l'acquisto di una certa quantità di valuta mi consente l'accesso a una data quantità di bene o di servizio.

Inoltre esiste una categoria di criptovalute in cui esse sono dette *Security*. Nell'ambito della finanza, con il termine *security* si intendono azioni, obbligazioni e in genere diritti patrimoniali. Le criptovalute *Security*, quindi, rappresentano il possesso, parziale o totale, di un dato bene materiale o immateriale. Sono perciò strumenti finanziari a tutti gli effetti. Possono rappresentare una quantità di merce, il numero di azioni o il diritto di voto in un'organizzazione da parte di chi le possiede.

So che può risultare ostico, quindi facciamo qualche esempio.

Immaginiamo di aver aperto

un'associazione di volontariato che si occupa di beneficenza in vari settori.

Chiunque devolva in beneficenza una somma riceve in cambio delle criptovalute, in base alla donazione effettuata.

Ecco che queste monete virtuali rappresentano il diritto di voto di tutti coloro che hanno contribuito con le proprie donazioni. In uno scenario del genere, chi fa beneficenza potrebbe decidere direttamente in quale settore devolvere l'aiuto. Il meccanismo, per altro, sarebbe molto semplice. Bisognerebbe solo individuare i settori nei quali si vorrebbe fare beneficenza e,

a seguito di una votazione, far defluire le donazioni ricevute nel settore maggiormente votato. Più monete digitali si hanno, più influente sarà la propria votazione.

Una criptovaluta intesa come strumento finanziario potrebbe anche rappresentare un'azienda proprio come fosse un'azione o quota della stessa, prevedendo addirittura di riconoscere dividendi.

Viste le principali categorie di criptovalute è dunque intuibile come potenzialmente si possano creare monete per tutti i servizi.

La quantità di *altcoin* oggi esistente

è enorme.

Non potendo citarle tutte ho preferito non citarne alcuna, se non *Ether*, che era necessaria per spiegare alcuni concetti di questo fenomeno.

Tutte queste *altcoin* sono davvero necessarie?

No, ma ne parliamo nel prossimo capitolo.



Per saperne di più...

Rimbocchiamoci le maniche e torniamo a parlare di *altcoin*, anzi di *smart contract*.

Abbiamo detto che gli *smart contract* possono replicare quasi tutte le condizioni dei contratti “reali”, e che sono utili in moltissimi settori. Bene, volete sapere qual è stato finora uno dei maggiori utilizzi degli *smart contract*?

La creazione di *altcoin*.

Esattamente, avete capito bene. Da una piattaforma di *smart contract* che funziona con pagamenti in *altcoin* è possibile creare altre *altcoin*. Lo so, è

complicato, ma se fosse stato un argomento semplice non avrei iniziato a scrivere questo libro e avrei fatto qualche (molti) weekend fuori porta in più.

Se ci pensiamo un attimo, non è poi così strano immaginare un contratto che permetta lo scambio di merci a determinate condizioni.

E se immaginiamo che quelle merci siano delle monete digitali, ecco che abbiamo il nostro contratto di *altcoin*, tramite il quale gli utenti possono acquistare e scambiarsi la nostra nuova criptovaluta.

In realtà le criptovalute così create

non sono delle vere e proprie monete digitali, ma prendono il nome di *token*, ovvero “gettoni”. Infatti, come nel caso dell’autolavaggio, queste criptovalute non sono scambiabili al di fuori del contratto che le rappresenta.

Questo vuol dire che chi acquisterà dei *token* di un particolare contratto potrà spenderli per usufruire dei servizi previsti da quel contratto specifico, non da altri.

Un po’ come per i gettoni di un casinò. Se acquistiamo dei gettoni al Casinò di Sanremo difficilmente li accetteranno al Casinò di Venezia.

Il fatto che ogni *token* sia utilizzabile

solo nel proprio ambiente, non significa che non possa avere una valutazione di mercato come *Bitcoin* o *Ether*.

Il valore dei *token*, infatti, oscillerà in base alla qualità del progetto e del servizio al quale sono legati, ovvero alla richiesta dello stesso.

Come sappiamo i *token* sono appoggiati sulla *blockchain* di una moneta di riferimento. Il loro valore è collegato, inoltre, al valore della moneta a cui appartiene la *blockchain*.

Il lancio sul mercato di un nuovo *token* è simile alla quotazione in borsa di una nuova società e prende il nome di ICO.

Il termine ICO sta per Initial Coin Offering, ovvero Offerta di Moneta Iniziale, ed è l'operazione con la quale sono messi in vendita per la prima volta i *token* di uno specifico contratto. In questa fase i *token* sono venduti a un prezzo predeterminato dagli stessi creatori, o fondatori del progetto.

Ma a chi sono venduti i *token* durante una ICO? A chiunque ne sia interessato. Infatti, i fondatori di un *token*, prima di mettere in vendita i propri gettoni, spiegheranno il progetto in un documento, specificando anche come i *token* potranno essere impiegati una volta acquistati.

I potenziali investitori valuteranno,

quindi, se il progetto è interessante, se vale la pena acquistare i *token* e se il valore di questi ha possibilità di crescere nel tempo.

8. MI CONVIENE INVESTIRE IN BITCOIN?

Siamo giunti alla faticosa domanda. Cerchiamo, ora, di arrivare anche alla risposta.

Chi ha letto qua e là di *Bitcoin* e dei fantomatici personaggi che con qualche euro sono diventati milionari potrebbe pensare che sia facile guadagnare con le

criptovalute.

Qualsiasi investimento, invece, richiede studio e molta analisi, e non parlo solo di conoscere ciò in cui si vuole investire, ma anche di ciò che si può investire.

La seconda regola da non scordare mai, infatti, è proprio investire solo ciò che ci si può permettere di perdere. Bisogna immaginare i soldi che si vogliono investire come già persi. Siamo davvero sicuri che potremmo farne a meno? È fondamentale, quando si investe, che non si debbano fare rinunce di alcun tipo. Al massimo le rinunce devono essere fatte prima, per risparmiare qualcosina che possiamo

permetterci di perdere, non il contrario. Magari sembra la stessa cosa, ma non lo è.

Questo principio vale sempre, anche se si sta investendo in maniera diversificata. Spesso, chi ha faticosamente messo da parte qualche soldo dà per scontato che, per far fruttare i propri risparmi, essi debbano essere impiegati tutti insieme, nello stesso modo. Non è così, soprattutto in un mercato rischioso come quello delle criptovalute. Lascereste alla mercé di un solo investimento tutti i vostri risparmi? Se si rivelasse fallimentare, avreste perso il frutto di tante rinunce e sacrifici.

Ecco perché la terza regola da imparare prima di pensare a un qualsiasi investimento è quella di diversificare. Diversificare significa impiegare i propri risparmi in più settori differenti, così che, se uno di questi va male, probabilmente avremo investito in un altro che andrà meglio, riducendo il rischio di grosse perdite.

Le regole di cui stiamo parlando non sono numerate per rilevanza; anzi, sono tutte ugualmente importanti, se non fondamentali.

Certo, mi rendo conto che numerarle dà quel senso di disciplina scolastica che un po' fa figo, quindi continuiamo così. La prossima regola, o la prima che

abbiamo presentato all'inizio di questo libro, l'abbiamo già vista ed è conoscere ciò in cui vogliamo investire.

Concentrandoci su questo principio, torniamo a parlare di criptovalute.

Nel capitolo precedente abbiamo osservato le diverse tipologie di criptovalute presenti sul mercato. Vediamo adesso di analizzare quali sono le ragioni per cui potremmo pensare di investirci.

L'evoluzione di *Bitcoin* ha destato l'interesse di moltissimi investitori, sia professionisti che improvvisati.

Come già accennato, nel 2009 i

bitcoin non valevano praticamente nulla, ma nel dicembre 2017 un singolo *bitcoin* è arrivato a valere 20.000 dollari americani.

Il crescente interesse in *Bitcoin* ha portato alla creazione di monete virtuali alternative, caratterizzate da diversi intenti.

Chi investe in criptovalute investe puramente per scopi speculativi, ovvero per comprare una valuta a poco e rivenderla a tanto. Non esistono garanzie di riuscita, infatti si potrebbe comprare una criptovaluta a poco e rivenderla a pochissimo.

Come capire, quindi, quando

comprare o vendere una criptovaluta?
Ma soprattutto, quale criptovaluta?

In un mercato come quello che stiamo analizzando non è possibile prevedere con sicurezza come si comporteranno le monete virtuali. Quello che possiamo analizzare, però, è il progetto che vi sta dietro.

Il progetto di *Bitcoin* era, peraltro in un periodo di crisi finanziaria, quello di sostituire la moneta legale centralizzata delle banche. Ecco che, allora, si poteva intuire che l'investimento sarebbe stato ottimo, non sulla base del valore del *Bitcoin* in sé ma dell'idea che rappresentava. Certo, i *bitcoin* potevano rivelarsi anche un fiasco totale, come

potrebbe succedere in futuro, ma se si sposa un'idea perché ritenuta valida, almeno si conosce il motivo per il quale si investe. E se investiamo, lo facciamo con cognizione di causa, perché crediamo in un'iniziativa e non seguendo la massa.

Allora si potrebbe pensare di investire in *altcoin*, dal momento che ogni giorno ne esce una nuova. Esiste un'*altcoin* ormai per qualsiasi cosa, e molte hanno progetti piuttosto interessanti. Il problema di queste monete alternative è che la maggior parte è nata per seguire l'onda di interesse generata da *Bitcoin* ed *Ethereum*. Quindi, seppur presentino bei

progetti teorici, spesso si rivelano dei veri e propri fallimenti.

Le domande che io mi pongo quando vedo una nuova *altcoin* sono poche.

Alle spalle di questa moneta, esiste una organizzazione reale e consolidata?

Molte *altcoin* nascono con l'unico intento di racimolare fondi, senza avere una struttura né un team di lavoro consolidato. Queste monete sono destinate a scomparire nel breve periodo, meglio che lo facciano senza i nostri soldi.

Il progetto è interessante e realizzabile?

Molti progetti sono banali, a volte non se ne comprende nemmeno il reale scopo. Altre volte sono progetti già tentati in altre forme, e si sono rivelati irrealizzabili oppure fallimentari.

È davvero necessario l'utilizzo di una moneta digitale per questo progetto?

Questa è la domanda killer. Difficilmente sono riuscito a rispondermi in modo affermativo. Con la moda delle criptovalute sembra quasi che ogni business debba nascere su una *blockchain* e utilizzare una valuta digitale. Probabilmente un domani questa tecnologia diventerà lo standard per molti settori, ma al momento, per la maggior parte dei progetti che osservo,

non ha alcun senso. Spesso sono copie di progetti già esistenti, che funzionano bene e non utilizzano criptovalute. Quindi perché mai dovremmo investire in una criptovaluta che non offre una soluzione?

La cosa fondamentale è valutare da sé se un investimento può essere più o meno buono. Se non si è in grado di farlo è meglio evitare di investire. Impiegare dei risparmi senza sapere che cosa si sta facendo vuol dire scommettere, non investire. E nessuno dovrebbe farlo.

Molti dicono che chi possiede criptovalute ha interesse nel

promuoverne l'acquisto, mentre chi non ne ha le sconsiglia per lo stesso motivo.

Io, personalmente, ho investito in *Bitcoin* e *altcoin*. Ho diversificato. Ho guadagnato poco, ma non ho mai potuto perdere molto. Ho ancora qualcosa investito in criptovalute.

Vi consiglierei di investire in criptovalute?

Se siete degli investitori professionisti, ovvero con alle spalle tanto studio e formazione, esperienza nei mercati finanziari, sicuramente lo saprete da voi. Per tutti gli altri, no.

9. GLOSSARIO

Altcoin

“Alt” è il diminutivo di *alternative* e “coin” significa “moneta” in inglese. Letteralmente, quindi, un’*altcoin* è una moneta alternativa. Alternativa a che cosa? Al *Bitcoin* naturalmente.

Bitcoin

La criptovaluta più famosa al mondo. Quando si scrive del sistema o del concetto di *Bitcoin*, è utilizzata la lettera maiuscola. Quando il termine

bitcoin è usato per indicare l'unità di moneta, invece, si scrive con la lettera minuscola. Altri dettagli sono spiegati nel primo capitolo, non siate pigri.

Blocco

Insieme di transazioni che vengono raggruppate secondo una grandezza massima predeterminata per poi essere verificate e aggiunte alla *blockchain*.

Blockchain

Registro pubblico non centralizzato di dati, dove le informazioni sono immagazzinate “in blocchi”, verificate e autenticate. La *blockchain* è la tecnologia utilizzata dalla moneta

Bitcoin per registrare tutte le transazioni. .

BTC

È l'unità comune utilizzata per indicare i *bitcoin*, come EUR per gli euro oppure USD per i dollari americani.

Chiave Privata

È un codice che prova la proprietà di un determinato portafoglio virtuale (*wallet*). Questa chiave non deve essere mai comunicata a terzi, in quanto permette l'utilizzo del portafoglio a chi la possiede.

Chiave Pubblica

È l'indirizzo del portafoglio virtuale (*wallet*), come l'IBAN per il conto corrente. Si riferisce, però, alla chiave privata e non alla persona che la possiede. Può essere comunicata a terzi, anche per ricevere pagamenti.

DAO

“Decentralized Autonomous Organization”, organizzazioni in cui proprietà, gestione e controllo sono automatizzati. Sfruttano la tecnologia degli *smart contract* per agire secondo predeterminate regole.

Distributed Ledger

Il “Libro Mastro Distribuito”, ovvero il registro sul quale sono memorizzate tutte le transazioni in *bitcoin*, del quale ogni *miner* possiede una copia.

Ether

Moneta alternativa al *Bitcoin*, seconda per importanza nel mercato delle criptovalute.

Ethereum

Piattaforma per la creazione di *smart contract*, utilizza come moneta di scambio l’Ether.

Exchange

Piattaforma che permette l'acquisto o la vendita di criptovalute in moneta legale, nonché lo scambio tra loro. Gli intermediari sono soliti applicare una commissione a queste operazioni.

Futures

Contratti futuri in cui ci si obbliga a scambiare una prefissata quantità di merce o di valuta a una data e a un prezzo stabiliti in fase di contrattazione.

Genesis Block (Blocco Genesi)

È il primo blocco di transazioni validato di una *blockchain*.

ICO

Con il termine ICO, Initial Coin Offering, si intende l'operazione di lancio di una nuova moneta digitale, che viene venduta per la prima volta al pubblico a un prezzo predeterminato.

Imposte

Tributi corrisposti, sulla base del reddito generato, senza ricevere alcun servizio, ma al fine di coprire la spesa pubblica.

Mercato

Punto di incontro della domanda e dell'offerta, ovvero di acquirenti e venditori.

Miner

Soggetto che presta la capacità di elaborazione di uno o più computer per la verifica delle operazioni eseguite sulla rete *Bitcoin*. Viene ricompensato dalla rete stessa in *bitcoin*.

Mining

Processo di verifica delle transazioni eseguite sulla rete *Bitcoin*. Coloro i quali fanno *mining* sono detti *miner*, ovvero minatori.

Moneta legale

Moneta emessa da una banca centrale – per l’Euro la Banca Centrale

Europea (BCE) – che al contempo ne garantisce il valore.

Mutui subprime

Mutui rilasciati a soggetti che normalmente non avrebbero le garanzie necessarie per riceverli. Per questo motivo sono soggetti a tassi di interesse maggiori rispetto a quelli di mercato.

Nodi

Sono i computer che partecipano alla rete *Bitcoin*, chiamati così perché posseggono una copia del registro mastro. Detti, altrimenti, *miner*.

Rating

Valutazione di un determinato strumento finanziario sulla base della sua affidabilità e rischiosità, spesso rilasciata da apposite società chiamate comunemente agenzie di *rating*.

Somma vincolata

Importo che, una volta depositato presso una banca, o un intermediario finanziario, non può essere prelevato prima di una data scadenza senza il pagamento di una penale.

Smart contract

Letteralmente tradotto in “contratto intelligente”. È un software programmato sulla base di un contratto,

che, al verificarsi delle condizioni concordate in esso, esegue automaticamente la prestazione prevista dal contratto stesso.

Tasse

Tributi che vengono corrisposti con lo scopo di ottenere in cambio dei servizi.

Token

Letteralmente tradotto come “gettone”, è una moneta che sfrutta la *blockchain* di una criptovaluta principale per funzionare.

Trader

Soggetto che compra e vende azioni o strumenti finanziari, con l'intento di trarne profitto.

Volatilità

Termine che indica la tendenza a subire importanti e improvvise variazioni di prezzo.

Wallet

È il portafoglio virtuale dove sono contenuti i *bitcoin* di un determinato utente sulla rete *Bitcoin*. È composto da una chiave pubblica e una privata.

White paper

Documento nel quale è descritto il progetto di una nuova criptovaluta, sia dal punto di vista concettuale che da quello informatico.

[1] Dati del rapporto “2017 International Tax Competitiveness Index Rankings”, stilato dalla Tax Foundation.

[2] Il rapporto “2017 International Tax Competitiveness Index Rankings” posiziona la Svizzera al terzo posto, dopo la Nuova Zelanda.

[3] Wired ha definito l’Estonia la società digitale più evoluta al mondo.