Bitcoin, Criptovalute, Blockchain Spiegate Facili

La guida completa alle criptovalute per chi parte da zero

di Cesare Bianchi
con contributi di Roberto Alma

Edizioni GH srl

Prima edizione 2019

Editing: Isabella Proia, Marco Cruciani

libri@cesarebianchi.com
http://libri.cesarebianchi.com

Notizie sul copyright

Per depositare e dimostrare la paternità di questa opera, un checksum SHA256 del file originale di questo libro è stato inserito in una transazione sulla blockchain Ethereum.
Lo zip con il file originale, la firma digitale e le istruzioni su come trovare la transazione e verificare il checksum è reperibile dal sito http://libri.cesarebianchi.com/link

Edizioni GH srl

Immagine in copertina di Torange.biz, concessa con licenza CC BY 4.0

Quando l'ultimo albero sarà stato abbattuto, l'ultimo fiume avvelenato, l'ultimo pesce catturato, solamente allora scoprirete che il denaro non si mangia.

Alanis Obomsawin

SOMMARIO

ARGOMENTO INTERESSANTE, MA IN ESTREMA SINTESI?

Le criptovalute sono un sistema per scambiare denaro in modo semplice, sicuro, economico ed autonomo.

Il sistema è autogestito da una comunità/rete di migliaia di computer nel mondo, la sicurezza è garantita da complessi sistemi matematici, perciò non c'è alcun bisogno di una autorità garante (banca o Stato).

L'invio e ricezione di denaro sono pressoché immediati e le commissioni da pagare sono bassissime, nell'ordine dei centesimi o millesimi di euro.

Si può aprire un "conto" da soli, occorrono due minuti e poi è sufficiente dare a chi ci deve del denaro la propria chiave pubblica, che identifica il nostro conto. Il debitore invierà il denaro verso la nostra chiave pubblica.

Chiunque può perciò avere un numero potenzialmente infinito di "conti correnti" senza dover mai svelare la propria identità.

Gli scambi monetari possono essere tracciabili o non tracciabili, a scelta delle parti. Pertanto è possibile avere il completo anonimato, oppure rispettare tutte le leggi sulla tracciabilità.

Ad oggi le criptovalute sono considerate alla stregua di "valuta estera" e pertanto è legale pagare e farsi pagare usandole. A fini fiscali e contabili il valore dei pagamenti effettuati o ricevuti va calcolato convertendolo in una valuta ufficiale.

Non sono perciò (solo) un fenomeno speculativo ma hanno una effettiva utilità, poiché permettono di scambiarsi denaro, anche a grandi distanze, e in modo sicuro, sganciandosi dalle banche e con provvigioni enormemente inferiori.

Possono includere anche una serie di "servizi" aggiuntivi, sempre gestiti autonomamente ed estremamente economici e sicuri, come ad esempio la registrazione di contratti, i depositi di garanzia, la registrazione di diritti d'autore, la gestione delle votazioni, etc.

Permettono facilmente e confidenzialmente di partecipare a crowdfunding, acquistare e vendere azioni di aziende, ricevere dividendi e partecipare alle votazioni, il tutto garantito da una rete di migliaia di computer, senza doversi fidare di un unico server.

INTRODUZIONE

Ormai anche i sassi hanno sentito almeno di sfuggita il termine "Bitcoin". Per molti è solo un mito, una moneta virtuale su cui alcuni speculano o che è usata dai criminali. Le persone più avanzate hanno forse anche sentito parlare di "blockchain" o addirittura di "smart contract", hanno una vaga idea di cosa siano, e sanno che esistono altre criptovalute oltre al bitcoin. Probabilmente molti pensano che si chiamino "criptovalute" perché sono in qualche modo segrete, cosa che in effetti è vera in alcuni casi (o almeno, alcune garantiscono la segretezza delle transazioni). A nessuna persona dotata di senno verrebbe mai in mente, comunque, di usarle o tanto meno di investirci i propri risparmi. E chi vi investe viene visto con sospetto come quei famosi mercanti di bulbi di tulipano[1] responsabili della prima bolla speculativa della storia.

Il mio primo contatto professionale con le criptovalute è avvenuto a febbraio 2017, quando ho dovuto studiarle approfonditamente, poiché rivestivo il ruolo di

1 https://it.wikipedia.org/wiki/Bolla_dei_tulipani

riferimento tecnico durante la progettazione della criptovaluta "HOP", ideata per favorire le micro-economie nei centri rifugiati in Austria (progetto sponsorizzato dal Complexity Science Hub Vienna). Da allora la mia curiosità è andata crescendo ed a forza di studiare e sperimentare ho accumulato una discreta cultura sui vari aspetti teorici, tecnici, economici e legali, al punto da aver progettato alcune possibili soluzioni ai problemi che attualmente affliggono le blockchain e ne limitano l'uso.

Ho scoperto un intero mondo, molto interessante e dalle potenzialità enormi, che cambierà radicalmente la nostra società. Non solo perché taglierà finalmente il vincolo tra denaro e stati sovrani (rendendolo di fatto una cosa autogestita dal popolo), ma anche perché fornirà una serie di strumenti per poter gestire in modo decentrato, senza alcuna autorità centrale, tantissimi aspetti della vita sociale (ad es. la firma e registrazione dei contratti, la certificazione dell'identità, la gestione delle garanzie e delle fideiussioni, la registrazione di brevetti e diritti d'autore, il crowdfunding, la gestione delle votazioni, etc.).

Ho deciso di scrivere questo manuale a causa delle tante domande che nel tempo mi sono state poste sull'argomento. Mi è capitato spesso di discuterne e in tanti, tra amici, conoscenti e clienti, mi hanno spesso chiesto chiarimenti. Ho potuto perciò constatare la grande curiosità che c'è sul mondo delle criptovalute, ma anche i tanti fraintendimenti e miti metropolitani che

sono sorti in questi pochi anni, a causa anche della poca conoscenza sia delle basi tecniche sia del funzionamento di queste tecnologie, nonché delle tante opportunità che offrono.

In questa guida cercherò di spiegare in modo semplice come funzionano le criptovalute e più in generale le blockchain, per quali ragioni sono effettivamente utili, come e perché possono essere usate per altri servizi, e perché le persone che ci investono non sono (a volte) dei pazzi o degli speculatori, ma persone che vedono delle effettive opportunità. Cercherò anche di rispondere a molte domande e obiezioni che io per primo facevo (motivo per cui ho tanto studiato) e che sento spessissimo.

Questa guida è strutturata in modo da seguire un percorso graduale, partendo dai concetti base, che saranno poi usati per spiegare i concetti più utili e interessanti. In una prima parte scopriremo perciò le basi tecniche su cui sono state costruite le blockchain e le criptovalute.

Dopo aver affrontato questi concetti un po' ostici ma necessari, nella seconda parte ci occuperemo dei vari usi pratici, sia per gli utenti finali che per le aziende e lo Stato.

Infine, dopo un breve excursus sulla storia delle criptovalute, chiuderemo il manuale con una parte

dedicata a rispondere a vari dubbi e sfatare varie leggende metropolitane.

Il consiglio è perciò di non arrendersi all'inizio, ma fare il necessario sforzo per poter poi comprendere gli interessanti risvolti presentati fino alla fine del manuale.

COSA È UNA CRIPTOVALUTA E COME FUNZIONA

Iniziamo perciò dall'ABC, perché senza avere almeno una infarinatura dei concetti principali e delle tecnologie alla base di questo fenomeno, è impossibile fare un discorso chiaro e comprensibile.

Chi ha già una conoscenza tecnica di base può saltare questo capitolo, che troverebbe di certo banale. Dovrà anzi perdonarmi se a più riprese semplificherò e banalizzerò concetti e procedimenti che so essere in realtà molto più complessi. Il presente non è un manuale tecnico ma appunto una guida per "dummies", e non avrebbe molto senso addentrarsi in dettagli e tecnicismi, per quanto importanti e interessanti possano essere. La selezione di cosa scegliere di semplificare e come farlo è sempre difficile, probabilmente c'è chi storcerà la bocca perché ho banalizzato troppo un certo concetto o perché mi sono addentrato inutilmente in un altro. Per lo stesso motivo userò come esempi solo le tre piattaforme ad oggi (ottobre 2018) più rappresentative, cioè Bitcoin, Ethereum e Monero, per quanto varie altre siano interessanti e degne di nota. Chiedo venia in anticipo.

Nel secondo volume entreremo più nel dettaglio delle caratteristiche tecniche e del funzionamento dei vari tipi di blockchain ed affronteremo ad esempio gli Smart Contract, le Zero-knowledge Proof, le ICO, le DAO, le DApp, nonché gli aspetti legali e le potenzialità di tutte queste nuove tecnologie e paradigmi, che rivoluzioneranno il concetto stesso di "azienda" o "organizzazione" ed il funzionamento non solo delle banche, del commercio e della finanza, ma anche della vita organizzativa e sociale a tutti i livelli.

Nel terzo volume vedremo come la pubblica amministrazione può sfruttare queste nuove tecnologie per snellire la burocrazia, semplificare la vita ai cittadini e ridurre drasticamente i costi e i tempi necessari per svolgere tantissime operazioni. Tuttavia, per poter arrivare a conoscere e comprendere tutto questo nuovo mondo complesso, dobbiamo partire dalle basi.

Hashing

Iniziamo da un concetto un po' difficile ma che è proprio alla base di tutto questo mondo "criptico". E comunque no, il fumo non c'entra nulla.

Una funzione di hashing è un procedimento che permette, a partire da un qualsiasi oggetto informatico (in genere un file, ma anche un numero o una stringa di lettere tipo "Comprare il latte") di calcolare un numero ad esso associato. La caratteristica delle funzioni di

hashing è che se si applicano nuovamente allo stesso identico oggetto (stesso file, stesso numero o stessa stringa) daranno sempre lo stesso identico numero. L'altra caratteristica fondamentale è che a partire dal numero calcolato (cosiddetto "Hash") è impossibile risalire all'oggetto iniziale. Ultime caratteristiche importantissime sono che la probabilità di ottenere lo stesso numero da due oggetti diversi è molto molto bassa, e che cambiando di pochissimo l'oggetto (ad es. "Comprato il latte") l'hash che ne risulta è totalmente diverso.

E quindi a cosa serve? Semplice: a verificare che un oggetto sia esattamente lo stesso. Ad esempio, se mando un documento ed ho paura che qualcuno possa modificarlo strada facendo, posso calcolarne l'hash e comunicarlo separatamente al ricevente. Quando riceverà il documento, non dovrà far altro che calcolare l'hash del documento ricevuto e controllare che sia lo stesso che gli ho mandato io. Se è uguale, può avere la certezza che il documento non è stato toccato ed è esattamente quello che gli ho mandato io, fino alle virgole e agli accenti.

Vale la pena aggiungere che le funzioni di hashing correntemente usate danno come risultati dei numeri molto molto grandi (dell'ordine di 10 seguito da 154 zeri), in modo da garantire la quasi impossibilità di ottenere lo stesso numero ("collisione").

La blockchain

L'oggetto alla base di tutte le criptovalute è la blockchain. Molti pensano che sia stata creata apposta per le criptovalute, in realtà è un concetto molto semplice che era già stato adottato in contesti differenti (ad es. la "conservazione sostitutiva"[2]).

È basata sulle funzioni di hashing di cui sopra. L'idea è molto semplice e serve a poter dimostrare che un file (d'ora in poi parlerò genericamente di file per indicare qualsiasi oggetto informatico) esisteva in un certo momento.

Poniamo che ogni giorno ad un ufficio brevetti arrivano 1000 richieste. Ogni 10 richieste, un computer crea uno zip (cioè un archivio compresso) delle richieste arrivate, ne calcola l'hash, e lo scrive in un file. Tale file verrà incluso nello zip successivo, e così via. Se pertanto voglio togliere o modificare un file in uno zip, il suo hash sarà diverso, perciò dovrò modificare anche lo zip successivo, che però a quel punto avrà un hash diverso, etc.

Questo crea una catena (chain) di hash relativi allo zip (blocco) precedente, che sono inclusi nel blocco successivo. A lungo andare, diventa praticamente impossibile cancellare il fatto che un certo brevetto era stato presentato tale giorno più o meno a tale ora (o che comunque, di sicuro, quando tale blocco era stato chiuso, tale richiesta esisteva ed era pervenuta), o modificarne il

2 https://it.wikipedia.org/wiki/Conservazione_sostitutiva

L'anteprima del libro finisce qui.

Dal 5 gennaio sarà in vendita presso tutti i canali online, in formato sia cartaceo che ebook, e sarà ordinabile in tutte le librerie.