Capitolo 1

Che cosa sono i bitcoin e le altre criptovalute

Al giorno d'oggi il termine "bitcoin" non sorprende più nessuno. Tutti, anche i nonni e i bambini sanno vagamente che cosa sono e intuiscono che è meglio tenersene alla larga. Ma tutti ne sono anche incuriositi, per le tante leggende, vere e false, buone e cattive che li circondano.

Già il pensiero di poter comprare dei bitcoin e investirci del denaro fisico scatena uno strano mix di acquolina in bocca e mal di testa. Quando poi si viene a scoprire che di criptovalute ne esistono a centinaia e che di soli bitcoin ve ne sono addirittura tre la situazione finisce per generare decisamente un gran mal di testa. A questo punto basta solo aggiungere una goccia di una delle tante storie *horror* che circondano (a volte a ragione) le criptovalute per ritrarsi con un misto di paura e ribrezzo dall'intero argomento.

Ma la curiosità rimane, ed è qui che interviene questo libro. La mia ambizione è quella di togliere il più possibile l'alone di mistero che circonda le criptovalute e consentirvi di maneggiarle, letteralmente "giocarci", accumularle e spenderle riducendo i rischi al livello "questo me lo posso permettere" e, magari, guadagnarci qualcosa (o anche molto, chi può dirlo).

Uno dei primi dubbi che sorgono parlando di bitcoin e criptovalute è capire che cosa sono, da dove vengono, chi li emette. Forse è il caso di partire da un po' di storia del denaro "soft".

In principio era il… conio: una moneta veniva coniata con un metallo più o meno prezioso e il suo valore era stabilito dal suo peso. Semplice. Quando Marco Polo nel XIII secolo compì il suo viaggio

In questo capitolo

- **Dove, come, a chi e quando è nata l'idea dei bitcoin?**
- **Come nasce un bitcoin: il mining**
- **Non solo bitcoin**
- **Ma… si possono anche comprare?**
- **Le offerte iniziali: ICO (Initial Coin Offering)**
- **Le valute in altalena**
- **Le truffe non finiscono mai**

in Cina, vi trovò un'usanza del tutto diversa (tratto da *Il milione*, Capitolo 95, "De la moneta del grande Ka[ne]"):

> Or sappiate ch'egli fa fare una cotal moneta com'io vi dirò. Egli fa prendere scorza d'un àlbore ch'à nome gelso […] e di quella buccia fa fare carte come di bambagia; e sono tutte nere. […] egli ne fa de le piccole, che vagliono una medaglia di tornesegli picculi, e l'altra vale uno tornesello, e l'altra vale un grosso d'argento da Vinegia […] e cosí va infino 10 bisanti. E tutte queste carte sono sugellate del sugello del Grande Sire, e ànne fatte fare tante che tutto 'l tesoro (del mondo) n'appagherebbe. E quando queste carte sono fatte, egli ne fa fare tutti li pagamenti e spendere per tutte le province e regni e terre ov'egli à segnoria; e nesuno gli osa refiutare, a pena della vita.

NOTA

Non è interessante scoprire come l'italiano del tredicesimo secolo non fosse poi così diverso da quello di oggi o, quanto meno, ci risulti comprensibile?

In buona sostanza, il Gran Khan usava come valuta "soft" un materiale di scarso valore, la cartamoneta (Figura 1.1): chi la deteneva poteva cambiare il biglietto con un valore vero. Che cosa garantiva (falsificatori a parte) l'autenticità? Il *sugello*, ovvero il sigillo dell'imperatore. Un'altra cosa. L'imperatore aveva fatto stampare molta più cartamoneta di quella che avrebbe potuto ripagare: tanta da pagare ogni tesoro del mondo. Quindi era una cartamoneta moderna: cambiabile a vista e non basata direttamente su un corrispondente deposito in oro.

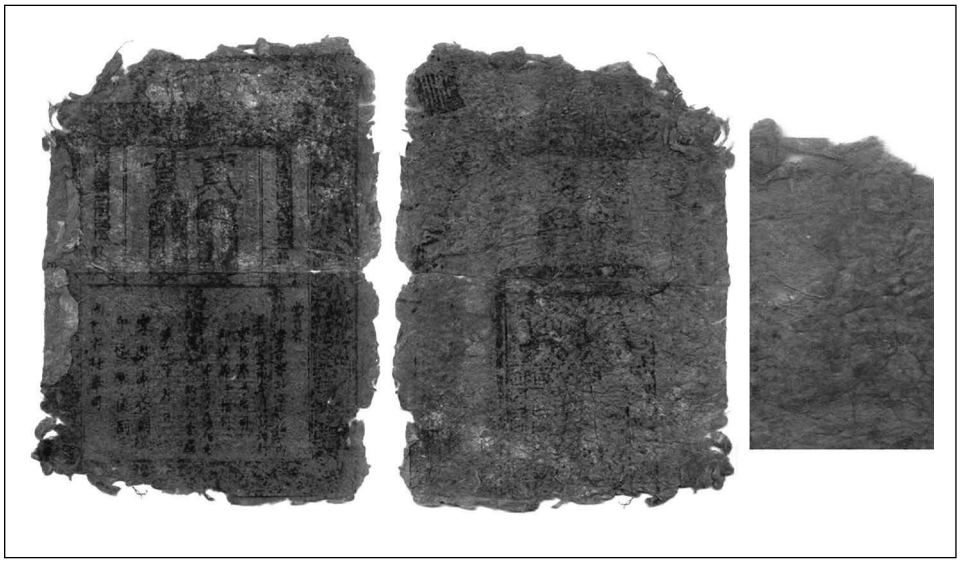


Figura 1.1 Banconota cinese del tredicesimo secolo: non più un valore, ma un titolo il cui unico valore è dato da una garanzia esterna.

Oggi l'euro è fatto (più o meno) così: qualcuno (la BCE) garantisce che se portate in un qualsiasi negozio cinque foglietti con sopra stampati i numeri giusti, diciamo cinque banconote da 100 euro, il negoziante si fidi di quel logo BCE e vi dia un bene solido,

diciamo un computer. Tecniche di stampa a parte, la situazione non è cambiata granché in questi ultimi otto secoli:

foglietto di carta + ente di garanzia = valore

La cosa non vale solo per le grandi istituzioni, ma anche per gli enti privati: se al negoziante faccio vedere una tesserina colorata con un logo noto (VISA, American Express, Mastercard…) e dimostro di esserne il titolare, lui si fida del fatto che prima o poi i miei soldi gli arriveranno, e così mi dà il bene.
Ma questo vuole anche dire che senza l'ente di garanzia, il foglietto o la tessera non hanno più valore: se l'impero viene rovesciato, chi mi garantisce l'incasso del mio foglietto? Se, poniamo, la BCE chiudesse i battenti, chi me li cambierebbe gli euro? Non posso andare a fare la spesa con la tessera del circolo dei modellisti… D'accordo, oggi qualche garanzia di stabilità in più l'abbiamo rispetto al XIII secolo. Ma in buona sostanza, ad attribuire un valore ai nostri soldi, a controllarli, è chi li ha emessi o chi è affidabile nel promettere di metterceli per conto mio.
Ma, qualcuno si è domandato: non sarebbe possibile sottrarre, almeno in parte, il controllo del denaro alla BCE, e in generale alle varie banche nazionali che "battono moneta"?
In fin dei conti che cosa è successo al bene "informazione", intesa nel senso più ampio possibile del termine? Ci fu un tempo in cui le notizie, le telefonate, i brani musicali, i film, le foto… tutto era di proprietà di qualcuno. Oggi abbiamo a disposizione un mezzo, Internet, che nei fatti ha rivoluzionato lo stato delle cose. Non sempre in modo legale, questo lo sappiamo. Ma prendiamo per esempio le notizie. Un tempo erano sostanzialmente "controllate": la *tivvù* diceva che un certo tizio era cattivo, noi, i buoni, andavamo a bombardarlo ed eravamo felici di aver compiuto il nostro dovere. Oggi le fonti di notizie (e di bufale) sono esplose e nessuno (almeno credo) si fiderebbe proprio al 100 percento di tutto ciò che dice il tiggì (Figura 1.2).

Figura 1.2 Ci fu, forse, un tempo in cui delle grandi istituzioni ci si poteva fidare. Non ci è dato di sapere il reale contenuto della fialetta di "armi chimiche" grazie alle quali abbiamo raso al suolo l'Iraq, l'antica Mesopotamia, culla della civiltà.

Le stesse telefonate (anche intercontinentali) oggi sono sostanzialmente gratuite: un tap su un contatto WhatsApp e avvio la chiamata, a costo zero. Passando all'illegalità, quanto ci vuole, oggi, con la fibra ottica, a scaricare un film dalla Rete? Dieci minuti? E da dove lo scarico, il film (ragazzi non fatelo…): non lo so neanche, perché lo ricevo da due, dieci, venti fonti diverse, pezzettino per pezzettino e, nel contempo, invio le parti che ho scaricato. È il sistema peer-to-peer: tanti nodi paritetici che si scambiano informazioni (precisissimi frammenti di film) in modo sicuro (quello che mi arriva è un frammento del film che ho cercato, non qualcosa a casaccio).
La tecnologia sulla quale si basano i bitcoin è "figlia" di questo progresso. Bitcoin è una valuta elettronica che nasce, cresce e si fonda sulla Rete. Non ha un ente centrale (non c'è una "BCE" dei bitcoin), non ha un unico certificatore (non c'è neanche un "Gran Khan" che ne certifichi il valore) e non può essere emessa a casaccio. A impedirlo è un algoritmo, un "problema" la cui risoluzione richiede una grande quantità di calcoli, e quindi del tempo. È proprio questo algoritmo a controllare (e quindi a limitare) l'emissione di nuovi bitcoin. Per risolvere il problema, sempre più complesso col passare del tempo, servono computer sempre più potenti. Trattandosi di problemi matematici, il modo più rapido ed economico per risolverli non è impiegare una comune "macchina" da scrivania o portatile, ma "darli in pasto" a macchine dedicate o a schede video (Figura 1.3).

Figura 1.3 Per eseguire i calcoli necessari per "acquisire" criptovalute si usano strane macchine, composte da una normale scheda madre e una grande quantità di schede video di elevata potenza.

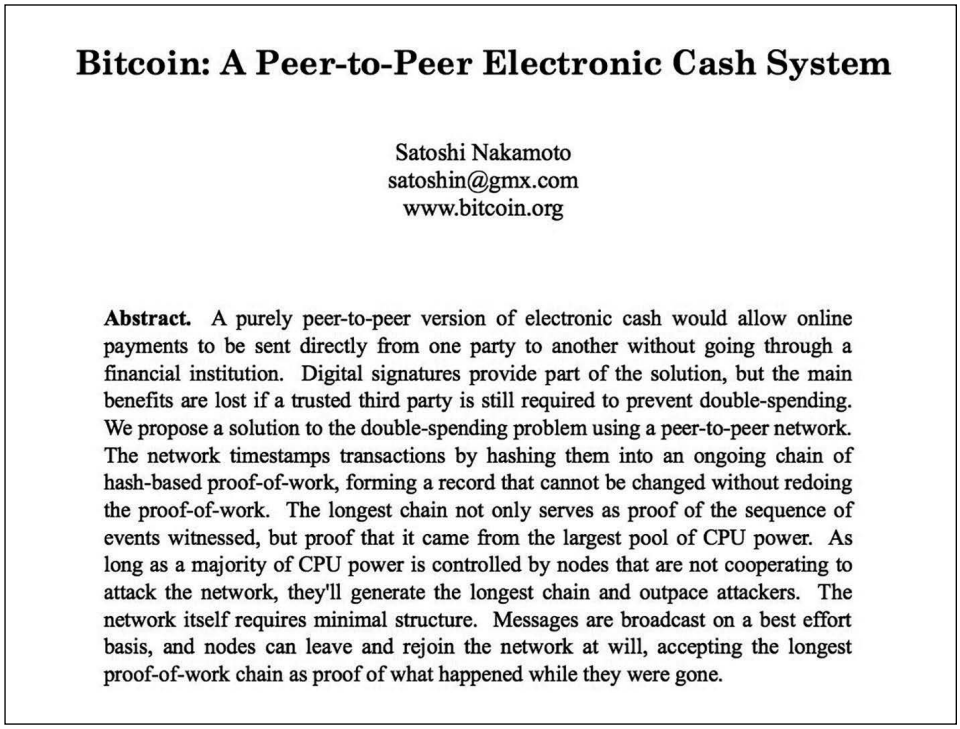
Può sembrare strano, ma le schede video, per loro natura, vengono "costrette" dai videogiochi e dalle applicazioni grafiche a ricalcolare rapidamente e ripetutamente la posizione dello schermo in cui collocare segmenti, colori, sfumature ed effetti grafici. Se il caso fa sì che tu nasca scheda video, sai solo di dover eseguire calcoli: che si tratti di immagini o di problemi da bitcoin… a te sostanzialmente non interessa granché. E così fai quello che le schede video sanno fare meglio: macini numeri. Trovata la soluzione (o avendo contribuito a trovarla) il premio in bitcoin è tuo (o quanto meno in parte).

Se così non fosse, se chiunque fosse libero o, quanto meno, più libero di emettere bitcoin, accadrebbe quello che accade a ogni valuta troppo stampata: l'inflazione. Troppa valuta circolante porta a una perdita di valore della valuta stessa. Questo è ovvio anche dal punto di vista intuitivo: che cos'è più prezioso? Qualcosa di raro e che tutti vogliono o qualcosa di abbondante e che non interessa granché? Il diamante o il carbone?
A questo punto è chiaro che un'entità come il bitcoin, che non è agganciata a nulla, si basa sul valore che… chi lo usa, ovvero "il mercato" gli attribuisce. Se c'è molta richiesta (se le criptovalute vengono molto comprate e scambiate), il loro valore cresce. Immaginate: avete un bene e volete venderlo. Non fate a tempo a dirlo in giro e l'ingresso vi si riempie di potenziali acquirenti; oppure dopo una settimana dall'annuncio non si è fatto ancora vivo nessuno. Nel primo caso potete alzare il valore del bene finché non avrete un solo (ricco) acquirente. Nel secondo caso dovrete ridurre le pretese. I bitcoin sono sottoposti, anche, alla stessa dinamica: hanno il valore che il mercato attribuisce loro.
"Ok", direte voi, "ma se questi non sono soldi 'veri', che cosa li distingue da una bolla speculativa?". Dubbio più che legittimo. La realtà? Nulla: i bitcoin possono benissimo essere una bolla e forse lo sono proprio. Il 21 aprile del 2017 un bitcoin valeva 1.146 euro. Il 20 aprile 2018 un bitcoin valeva 6.932 euro, 6 volte tanto. Ma a metà dicembre 2017 un bitcoin valeva sui 15 o 16.000 euro, ben 14 volte tanto. Che cosa mai potrebbe fluttuare così tanto? L'esempio che si fa più spesso è… floreale. Avete presente i tulipani? (`https://it.wikipedia.org/wiki/Bolla_dei_tulipani`).
Il tulipano è un fiore… "questa la so, è olandese!". No, non esattamente, è un fiore asiatico, che però è arrivato in Olanda a fine Cinquecento dalla Turchia ottomana. In estrema sintesi, questa raffinatezza esotica piacque molto agli olandesi, che cominciarono a incrociarla e ibridarla per crearne nuove straordinarie varietà. Se una varietà era rara, il suo prezzo saliva e saliva e saliva, fino a toccare (1634) vertici davvero insensati: paghereste voi un singolo bulbo (il *Semper Augustus*) l'equivalente di 200 "maiali grassi"? Peggio ancora: venivano venduti addirittura i bulbi appena piantati o addirittura che si aveva intenzione di piantare. Tempi d'oro per gli *speculatori* (tenete sempre bene a mente questa parola). Immaginate come andò a finire: a un certo punto qualcuno si rifiutò di comprare proprio a un prezzo eccessivo quelle "cipolline", i prezzi prima calarono e in breve precipitarono (Figura 1.4). Qualcuno (chi aveva incassato soldi e non bulbi) divenne ricchissimo e qualcuno (i tanti che avevano sborsato soldi veri per qualche sacchetto di bulbi ormai inesigibili), finì sul lastrico. Ma letteralmente sul lastrico, costretto a nutrirsi dei suoi… costosissimi bulbi.
Ecco, questa è una lezione da tenere a mente. I bitcoin non sono bulbi (non sono nemmeno oggetti fisici), ma celano in loro, potenzialmente, lo stesso rischio "bolla". Avete faticosamente messo insieme… poniamo diecimila euro, pensate di investirli in qualcosa ad alto rendimento, non vi fidate né delle banche né del materasso e comprate (Capitolo 3) dei bitcoin? Il rischio che correte è quello di ritrovarvi in mano nel giro di sei mesi 100.000 euro o magari i vostri vecchi 10.000 o anche solo 1.000 o 100 euro… Come potete notare in questo libro non è allegata una confezione di Kleenex, perché davvero… addio sogni di gloria!

Figura 1.4 Il grafico della "Tulipomania" campeggia nell'appartamento dello speculatore Gordon Gekko in *Wall Street – Il denaro non dorme mai* di Oliver Stone (2010), ©20th Century Fox.

Dove, come, a chi e quando è nata l'idea dei bitcoin?

Voglio mantenere la promessa di non entrare in aridi tecnicismi, non perché non siano intriganti (per qualcuno) ma perché… diciamoci la verità: vi interessa davvero così tanto sapere come vengono stampati o distribuiti gli euro, i dollari o le corone ceche? Probabilmente vi interessa di più sapere come si guadagnano, come si scambiano e dove si spendono. L'operatività, non i dettagli tecnici. O comunque questo è il mio presupposto. A novembre del 2008, sul sito `http://www.metzdowd.com`, "qualcuno" pubblica su una mailing list dedicata alla crittografia ("The Cryptography and Cryptography Policy Mailing List") un testo il cui titolo è *Bitcoin: A Peer-to-Peer Electronic Cash System* (Figura 1.5). Tutto, sostanzialmente, nasce in quel momento. L'autore? Un tale *Satoshi Nakamoto*, uno pseudonimo dietro il quale si cela una persona (o forse più d'una) rimasta tuttora sconosciuta. Sospetti tanti, dichiarazioni anche, ammissioni pure, ma nulla di veramente definitivo. Dobbiamo rassegnarci: almeno per un po', e forse per sempre, non sapremo chi ha "inventato" i bitcoin. Io lo trovo un po' inquietante, ma a dire la verità sono così tante le cose inquietanti al mondo che forse possiamo accettarne un'altra di più.
L'idea fu quella di escogitare un "sistema di transazioni elettroniche che non fosse basato su un fiduciario" (Nakamoto 2008). Il messaggio è esattamente quello di cui parlavamo all'inizio: non abbiamo un imperatore o una banca centrale e neanche una grande società a stampare, garantire, gestire e neanche sovrintendere il valore dei bitcoin. Questo fa sì che la criptovaluta bitcoin sia libera da ogni forma di controllo diretto. Non appartiene a un governo, a un gruppo, a una lobby di banchieri ma "insiste" sulla Rete. Nel 2009 nasce il software open source `Bitcoin-Client` e vengono "minati" (una parola chiave nel mondo delle criptovalute, per un approfondimento si veda il Capitolo 4) i primi 50 bitcoin. È la genesi dei primi bitcoin e infatti il primo blocco di bitcoin viene chiamato *blocco genesi*.



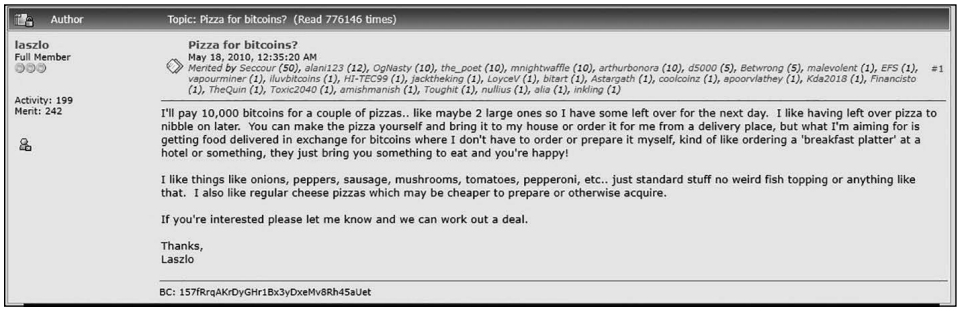
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Figura 1.5 Tutto nacque da qui: il documento all'origine dell'idea e poi della nascita dei bitcoin e di tutte le criptovalute.

Che cosa significa che un software è open-source? Significa che chiunque può controllare che cosa fa e come lo fa. Significa che il suo autore non intende nascondervi nulla: nessun trucco e nessun segreto. Il sistema emette un problema di complessità sempre crescente: chi risolve il problema si "merita" in premio i bitcoin corrispondenti. Sì, ma chi li mette i "soldi" del premio? Nessuno: non c'è un versamento in euro o dollari dietro all'emissione di un bitcoin. Semplicemente tu ricevi una cosa che si chiama "un bitcoin" che il sistema certifica che appartiene a te. Poi il suo valore… è quello che è (ma soprattutto quello che sarà). Chi mai ti darà un centesimo per un bitcoin? Solo un matto. Ma intanto quel bitcoin è tuo. Non vale niente, ma quel "niente" è tuo.
Inizialmente un bitcoin valeva talmente "niente" che davvero non era possibile spenderlo in alcun modo. È impossibile non citare un aneddoto che oggi ha dell'incredibile. Il 18 maggio 2010 (quindi a un annetto dalla comparsa del blocco genesi), tale Laszlo Hanyecz offrì 10.000 bitcoin, ovvero 41 dollari, a chiunque gli portasse un paio di pizze (Figura 1.6), specificando anche come gli sarebbero piaciute: grandi e con peperoni, cipolle, funghi, salsiccia, peperoncino… (no comment… da non napoletano, per me la pizza è solo quella napoletana). Trascorsero quattro giorni, ma poi Jeremy "Jercos" Sturdivant, di 18 anni, accettò il pagamento di 10.000 bitcoin e inviò a Laszlo due pizze grandi di Papa John's. Spesa: 23 dollari. Con somma soddisfazione, Laszlo scrisse: "Solo per dirvi che ho scambiato con successo 10.000 bitcoin per delle pizze" (Figura 1.7).


Author | Topic: Pizza for bitcoins? (Read 776146 times)

laszlo
Full Member

Activity: 199
Merit: 242

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM
Merited by Seccour (50), alan123 (12), OgNasty (10), the_poet (10), mnightwaffle (10), arthurbonora (10), d5000 (5), Betwrong (5), malevolent (1), EFS (1), vapourminer (1), iluvbitcoins (1), HI-TEC99 (1), jackthekingg (1), LoyceV (1), bitart (1), Astargath (1), coolcoinz (1), apoorvlathey (1), Kda2018 (1), Financisto (1), TheQuin (1), Toxic2040 (1), amishmanish (1), Toughit (1), nullius (1), alia (1), inkling (1) #1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

Figura 1.6 Il messaggio con il quale venne acquistato in bitcoin il primo bene fisico.

Che c'è di male, direte… Nulla, proprio nulla. Se non fosse per il fatto che se Laszlo, anziché mangiarsi due pizze ipercondite, si fosse tenuto quei 10.000 bitcoin, oggi varrebbero qualcosa come 75 milioni di dollari. Buon appetito!

Figura 1.7 L'aspetto del "bene fisico" in questione.

C'è un'altra importante espressione che a questo punto non dovrebbe ancora essere chiara: "peer-to-peer". Qualcuno di noi conosce il download peer-to-peer di materiale prevalentemente pirata: video, musica, software… Che cosa significa? Nel caso di, poniamo, un video in download, significa che io uso un software, gli domando di scaricare un certo video e lui si mette alla ricerca, in Rete, di tutti i nodi miei "pari" (peer) che contengono frammenti del video in questione: così ne scaricherò magari 12 frammenti

dal nodo di un tizio australiano, 3 frammenti dal nodo di un tizio veronese, 123 frammenti dal nodo di un tizio tedesco, 63 frammenti dal nodo del mio vicino di casa… fino a completare il video. Ma io stesso sono un nodo e darò 24 dei miei frammenti a un francese, 34 frammenti a un americano, 321 pezzi a un polacco… il tutto sotto il controllo del mio software peer-to-peer. In estrema sintesi ognuno apre il software del suo nodo, il quale mette a disposizione di ogni altro nodo connesso alla Rete quanto ha in suo possesso, "in cambio" di altri frammenti che gli mancano. Chi è il responsabile di questi scambi? Un po' tutti, e nessuno in particolare: è il concetto del peer-to-peer. I nodi (peer) sono dispersi a milioni sul globo e, presi singolarmente, sono pochissimo responsabili del download video che si sta svolgendo.

La rete di nodi peer-to-peer di bitcoin funziona in modo abbastanza simile. I nodi nascono con lo scopo di "minare" nuovi bitcoin: trovarli e guadagnarli. Ma un'altra parte del lavoro dei nodi consiste nel *confermare le transazioni*. Che cosa significa? Se io detengo dei bitcoin (più probabilmente delle "frazioni" di bitcoin) è perché in qualche modo li ho guadagnati e il sistema (dei nodi bitcoin) ha già certificato che in effetti quei bitcoin sono miei. Se voglio trasferire una parte dei miei averi a un altro (per esempio mi sto comprando un sandwich pagandolo in bitcoin), dal momento che non posso dargli un foglietto di carta o una moneta di bitcoin, quello che faccio è informare la Rete (dei nodi) di questa mia intenzione. La Rete riceve la richiesta, verifica che la somma che intendo pagare sia in effetti di mia proprietà, registra la mia intenzione di trasferirla a qualcun altro e, infine, certifica che ora quella stessa somma non è più di mia proprietà, ma del venditore. Quando nel sistema dei nodi vengono rilevate una, due, tre e poi altre conferme della legittimità e correttezza di questa operazione, io non avrò più il corrispettivo in bitcoin del sandwich e il ricevente avrà nel suo portafoglio il mio pagamento. Fine.

Suona complicato? All'atto pratico non lo è affatto: dall'app del mio portafoglio (wallet), che ho sul mio cellulare mi basta inquadrare il codice QR (Figura 1.8) del portafogli del venditore di sandwich, digitare la somma che devo pagare, dare l'OK e attendere l'arrivo delle conferme. Io prendo dalle mani del commesso il mio sandwich e me lo mangio; il venditore ha la somma sul suo portafogli. Finito. E… quello che ho descritto non è il domani, ma già l'oggi. Basta andare a mangiare da Subway (Figura 1.9).

Figura 1.8 Questo è il codice QR del mio portafogli bitcoin. Nel caso in cui il mio libro vi sia piaciuto davvero molto e vogliate farmelo sapere in modo molto, molto apprezzato.

Figura 1.9 Il ristorante SubWay di Brno (CZ) in piazza delle Erbe (Zelný trh), nel quale si può pagare in corone ceche, euro, bitcoin o litecoin. Magari vi trovate là perché siete appassionati di MotoGP o di arte…

A questo punto dovrebbe essere chiaro come il sistema possa funzionare anche senza una banca centrale o un imperatore. A farne le veci è l'intera Rete o, meglio, tutti i nodi peer-to-peer che compongono la rete bitcoin! Allora anche i bitcoin si basano su qualcosa e, in un certo senso, "dipendono" da qualcosa: Internet. Di fatto senza Internet i bitcoin possono essere solo conservati, ma non guadagnati e neanche spesi.

Come nasce un bitcoin: il mining

È tutto abbastanza semplice. Il sistema emette un blocco, contenente un problema (Proof-of-Work), di complessità crescente. Chi troverà per primo la soluzione avrà il bitcoin corrispondente. Milioni di persone in tutto il mondo cercano di risolverlo, da soli o associandosi in gruppi. A un certo punto qualcuno (singolo o gruppo) trova la soluzione e, al solito, la sottopone alla Rete. La Rete confronta problema e soluzione e stabilisce che, in effetti, questo qualcuno ha trovato la soluzione. Arrivano, al solito, una, due, tre, dieci conferme dalla Rete: in effetti questo qualcuno è stato il primo a trovare

la soluzione e il bitcoin è suo. A questo punto il nuovo blocco viene concatenato a tutti gli altri precedentemente emessi, a partire dal blocco genesi, a formare una lunga catena di blocchi, tutti certificati, uno dopo l'altro, dalla Rete: questa catena di blocchi è detta *blockchain*. Essendo basata su un algoritmo crittografico, la blockchain non può essere alterata, nemmeno di un bit, perché la modifica invaliderebbe automaticamente la blockchain stessa e tutti i blocchi che essa contiene. In pratica è proprio la blockchain a fare da "garanzia": è lei "l'imperatore" del sistema bitcoin. E la blockchain è pubblica e in possesso di ogni nodo, pertanto non può essere alterata in alcun modo: si verrebbe scoperti… ma non subito, anche prima.

Bene, ma come fare per risolvere il problema legato al singolo blocco? Si usa un computer. O, meglio, si usava. Al giorno d'oggi il problema è talmente complesso da richiedere l'impiego di intere batterie di speciali computer costituiti da una scheda madre non particolarmente performante, alla quale sono collegate quante più schede video possibili, del modello più veloce possibile e col consumo energetico più contenuto possibile, situati in località climaticamente le più fredde possibili e dove l'energia elettrica costa il meno possibile. Oppure ci sono macchine concepite appositamente per andare a caccia di bitcoin. Immaginatevi interi capannoni (Figura 1.10), pieni di scaffalature dal pavimento al soffitto, pieni zeppi di macchine di mining situate in Islanda, Estonia o, più frequentemente, Cina, che traggono dalla rete elettrica enormi quantità di energia per… estrarre bitcoin. In genere impianti di queste dimensioni affittano potenza di calcolo a chi voglia darsi al mining di bitcoin senza riempirsi la casa di macchine dedicate (e spendere i "guadagni" in bollette elettriche).

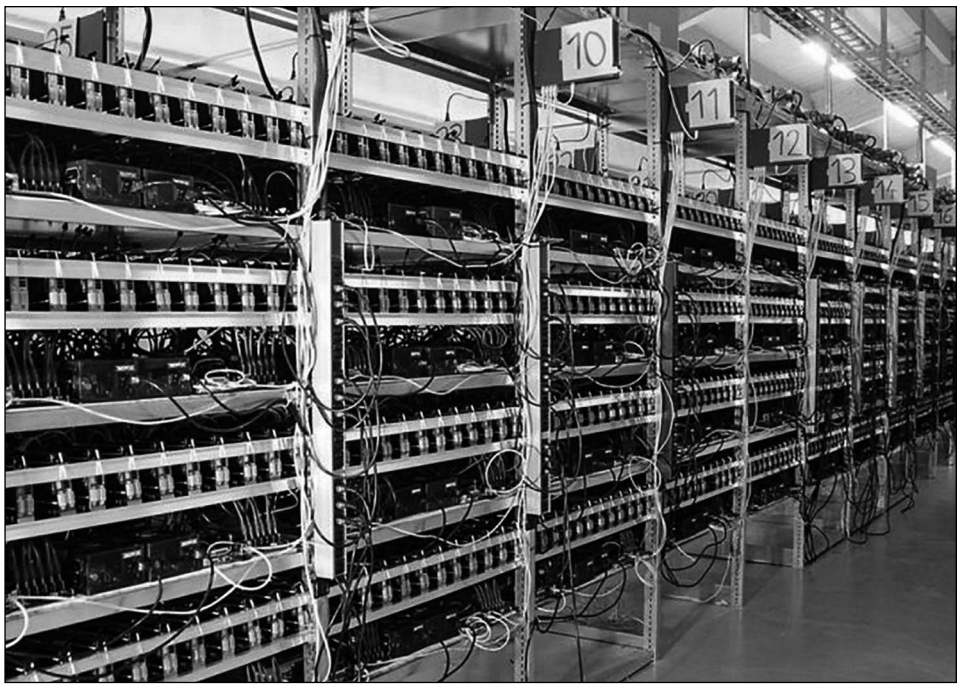


Figura 1.10 Per qualcuno il mining di bitcoin (e affini) è un vero e proprio lavoro: là dove l'energia elettrica è economica e il clima è rigido si impiantano interi "stabilimenti" di mining di bitcoin. Sono le cosiddette mining farm.

Non solo bitcoin

Al giorno d'oggi quasi tutti sanno dell'esistenza dei bitcoin. Magari non sanno esattamente di che cosa si tratta, dove e come si possono trovare, ma almeno il nome bitcoin è entrato nel lessico di tutti, dai pensionati legati al rito del TG ai bambini col loro sguardo fin troppo catturato dal display dell'apparecchio ormai onnipresente e (quasi) onnipotente. La cosa si complica se dal concetto di bitcoin allarghiamo il discorso al mondo delle criptovalute. Quante sono le criptovalute? Innumerevoli. Come innumerevoli? Ebbene sì: praticamente ognuno di noi ha la possibilità di crearsi una sua criptovaluta, ammesso che il suo ego smisurato intraveda in ciò una reale utilità.
Cominciamo col dire che di bitcoin ce ne sono almeno tre: bitcoin propriamente detto (valore attuale sui 7-8.000 euro), bitcoin cash (oltre i 1.000 euro) e bitcoin gold (sotto i 100 euro). Si tratta di bitcoin alternativi nati da operazioni di *fork* ("biforcazioni") che avevano lo scopo di rimediare ad alcuni difetti del progenitore di tutte le criptovalute. Sostanzialmente una certa "pesantezza", dovuta al fatto di trascinarsi dietro una lunga blockchain. La conseguenza di una blockchain pesante? Una transazione (il sandwich di Subway dell'esempio precedente) prima di essere pienamente confermata deve attendere minuti o ore. È vero che un bonifico bancario in euro si prende tre o più giorni "di valuta", ma da una criptovaluta ti aspetti una conferma immediata: io ti pago tot e… 1… 2… 3… ecco che sul tuo portafogli vedi accreditato il mio tot. La transazione deve essere agile e veloce, altrimenti si perde una parte dei vantaggi.
Ogni criptovaluta può seguire sostanzialmente il modello di bitcoin, magari snellendolo, oppure può impiegare un modello del tutto diverso. Si tratta di dettagli tecnici, ma che possono comportare grandi differenze in termini di applicabilità dello specifico sistema. Che cosa significa quest'ultima affermazione? Prendiamo l'esempio di un'altra criptovaluta molto famosa, e con un nome "affascinante": ethereum. La blockchain sulla quale si basa ethereum non è fatta solo per supportare la relativa criptovaluta (che per la precisione si chiama ether) ma più in generale per stabilire la chiusura di un accordo fra due o più parti. Sostanzialmente quell'accordo può certamente essere uno scambio di specifiche somme, ma anche un vero e proprio contratto (*smart contract*); questo, siglato sulla blockchain ethereum, vincola tutte le parti (Figura 1.11).

Figura 1.11 A una blockchain si possono collegare vari tipi di accordi, non solo transazioni economiche. È il caso degli smart contract.

In pratica, se io, A, devo fare un lavoro X per il mio cliente B, lego alla blockchain ethereum la richiesta, il mio lavoro e il compenso pattuito. Nel momento in cui il lavoro X è compiuto, automaticamente la blockchain, trovando che è stata ottemperata la condizione per la quale io debba essere pagato, mi paga. Il tutto senza passare da una banca, senza intermediari e senza "giorni di valuta".
Orbene, quali sono le principali fra queste misteriose criptovalute e perché diciamo che sono le più importanti? Secondo voi che cosa distingue il dollaro americano dallo zloty polacco? Il capitale di valuta circolante, giusto? Sicuramente il dollaro è più importante dello zloty. Ebbene, il capitale circolante dei soli bitcoin (propriamente detti) è oggi di oltre 120 miliardi di euro, più o meno equivalente a un terzo di tutte le criptovalute messe insieme. Se bitcoin fosse uno stato, si collocherebbe fra il Vietnam e la Romania, tanto per dire. Non è esattamente una "cosa da poco", e questo è sicuramente uno dei suoi punti di forza.
Data la volatilità delle quotazioni delle criptovalute, non credo sia il caso di elencarne il valore, una per una, ma un elenco basato proprio sul capitale di mercato credo sia utile, anche perché gli scostamenti di "classifica" fra le prime criptovalute non sono poi così frequenti.

Tabella 1.1 Le principali venti criptovalute, in ordine di capitalizzazione di mercato.

Posizione	Sigla	Moneta	Capitalizzazione di mercato (in milioni di euro)
1	BTC	Bitcoin	123.349 M€
2	ETH	Ethereum	51.463 M€
3	XRP	Ripple	27.999 M€
4	BCH	Bitcoin Cash	19.889 M€
5	EOS	EOS	7.685 M€
6	LTC	Litecoin	6.913 M€
7	ADA	Cardano	6.091 M€
8	XLM	Stellar	5.614 M€
9	MIOTA	IOTA	4.888 M€
10	NEO	NEO	4.085 M€
11	XMR	Monero	3.643 M€
12	DASH	Dash	3.112 M€
13	TRX	Tron	2.864 M€
14	XEM	NEM	2.858 M€
15	USDT	Tether	1.866 M€
16	ETC	Ethereum Classic	1.669 M€
17	VEN	VeChain	1.644 M€
18	QTUM	Qtum	1.467 M€
19	OMG	OmiseGo	1.295 M€
20	BNB	Binance Coin	1.280 M€

Non preoccupatevi di memorizzarle tutte o comunque la maggior parte di esse. In questo libro tratteremo solo quelle che capita di incontrare e di trattare più frequentemente, per un motivo o per l'altro: quelle più "popolari". Qualche criptovaluta ha utilizzi molto specifici o è balzata in questo elenco solo casualmente. Altre non rientrano in queste prime venti posizioni, ma capita di averne a che fare. Per esempio bitcoin gold sarebbe al 22° posto di questo elenco, ma capita di raggranellarlo. Lo stesso si può dire di dogecoin, attualmente al 38° posto. Ne parleremo già dal Capitolo 2…

Ma… si possono anche comprare?

Certamente, e pure troppo. Il mondo delle criptovalute pullula di soggetti (persone, iniziative, siti bellissimi ma pericolosi, ma anche siti seri) che vi chiedono soldi veri in cambio di criptovalute. Che riceviate in cambio criptodenaro vero o carta (virtuale) straccia o anche nulla si tratta dell'applicazione del famoso proverbio "Scuotendo l'albero dei [fate voi], qualcuno casca sempre". Questo è uno dei motivi principali per cui ho pensato di scrivere questo libro: permettervi di divertirvi, di avere soddisfazioni o anche patemi d'animo, ma in piena sicurezza. Indicarvi le trappole che troverete disseminate a ogni passo, dare il vostro denaro (intendo quello in euro) in mani fidate e che nel tempo hanno dato prova di serietà, evitando gli inganni e anche gli eccessi. Ricordate sempre: quello delle criptovalute è un mercato volatile; può, anzi deve, regalare soddisfazioni, ma non deve farvi piangere. Non troppo, almeno.
Nel Capitolo 3 parleremo della creazione di un portafogli sicuro, Coinbase, dove potrete versare i vostri euro, trasformarli in criptovalute, ritrasformarli in euro (o dollari) e ritirarli sul vostro conto corrente bancario "tradizionale".

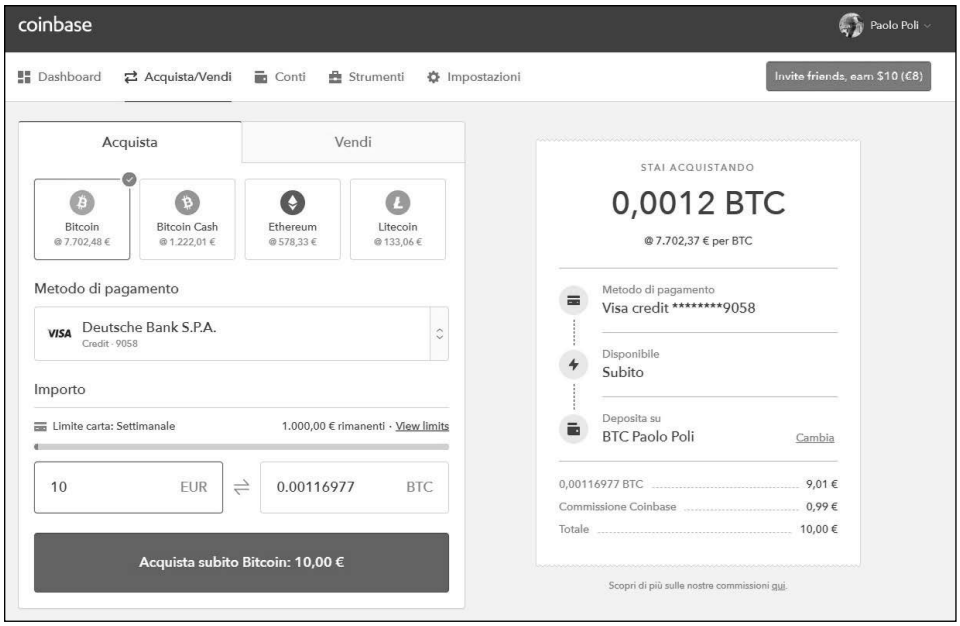


Figura 1.12 Un sito sicuro per acquistare bitcoin. L'operazione è semplice e immediata.

Un tipico esempio di una trappola lo trovate nel paragrafo che segue.

Le offerte iniziali: ICO (Initial Coin Offering)

Per carità, quasi tutte le criptovalute sono nate da un'*offerta iniziale*, ma c'è ICO e ICO, e in genere non c'è modo di distinguerle, almeno inizialmente.

- Per esempio ci potrebbe essere un'organizzazione o un gruppo di persone che sono seriamente intenzionati a creare una nuova criptovaluta che mancava. Chiede il vostro aiuto (soldi) per sostenere la loro iniziativa e dopo aver raccolto qualche milione di euro, può partire con la criptovaluta. Sostanzialmente le intenzioni sono serie, l'iniziativa è seria e, con un po' di fortuna, potete guadagnare molto o anche moltissimo dalla fortuna della nuova criptovaluta.
- Un gruppo di amici di buone speranze lancia una ICO per una nuova criptovaluta da scambiare all'interno di… poniamo un ateneo e poi sia quel che sia. Le intenzioni sono meno solide, le persone coinvolte magari non sono espertissime, ma hanno la vostra fiducia e decidete di aiutarli, non si sa mai. E poi… sia quel che sia, ovviamente. Magari la cosa avrà successo e potreste anche guadagnarci qualcosa (o perdere tutto).
- Ricordo di una criptovaluta, prodeum (Figura 1.13), di origine lituana, lanciata fra luglio 2107 e gennaio 2018. Gli ideatori intendevano "rivoluzionare il settore della frutta e della verdura tramite l'impiego della blockchain Ethereum". Come intendessero farlo? Presto detto: lanciarono una ICO da 6 milioni di dollari, ricevettero alcuni fiduciosi pagamenti (alcuni dei quali erano fasulli, fatti da loro stessi per simulare una certa fiducia del mercato) e poi… chiusero baracca e burattini, intascando quanto era rimasto nella rete (questa volta con la minuscola, era più una rete da olive…) e regalando ai malcapitati una dolce parola... (Figura 1.14).

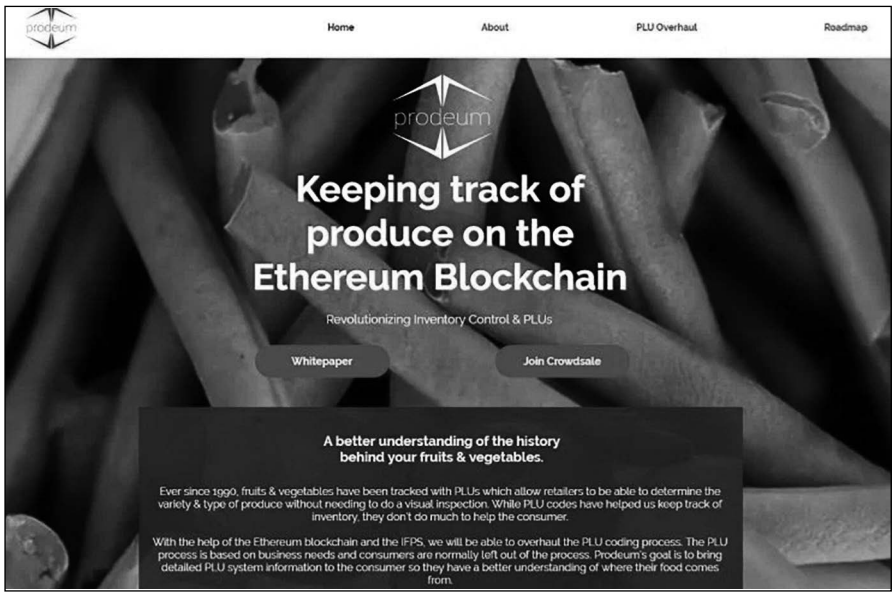


Figura 1.13 Il sito dell'ICO di prodeum si presentava anche piuttosto bene...

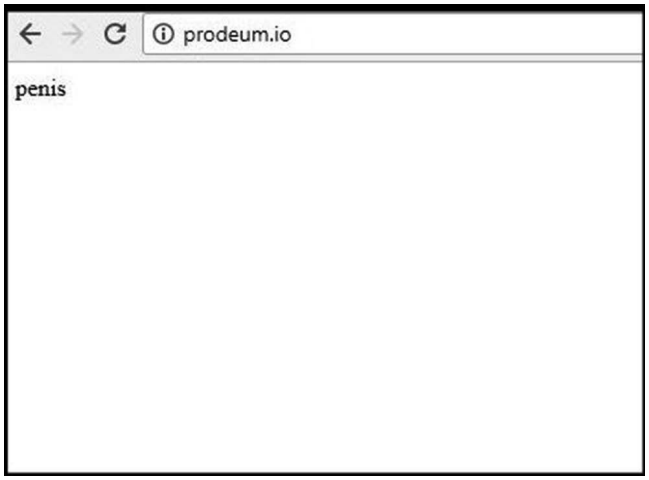


Figura 1.14 ... peccato che sia finito in modo un po' penoso.

E ricordatevi che quest'ultima opzione è abbastanza la norma. Spesso le ICO di buone speranze falliscono o sono vere e proprie truffe nate per raccogliere (i vostri) fondi e sparire. Nel Capitolo 5 troverete alcune indicazioni utili per scommettere sulla fortuna di un'ICO, ma il mio consiglio è: tenetevi alla larga delle tante pubblicità che vi compariranno sulle varie pagine web che parlano di criptovalute.

Le criptovalute in altalena

Il trend delle principali criptovalute è stato, in media, di costante crescita fino a circa metà dicembre 2017. Da allora, si è evidentemente scatenata una tempesta che ha abbattuto il valore di tutte le criptovalute, qualcuna di più e qualcuna di meno. Al momento (aprile 2018) le quotazioni oscillano sui valori di ottobre-novembre 2017 (Figura 1.15).

Figura 1.15 Un anno (aprile 2017 – aprile 2018) di bitcoin: la crescita continua, il picco di dicembre, la crisi e la fase di tenuta.

Ma se nessuno controlla le criptovalute, come è stato possibile abbatterle? I motivi del calo, a mio avviso, sono stati molti.

- Annunci e minacce dei principali governi (Figura 1.16): divieto di traffico di criptovalute (Cina), divieto di mining (Cina e Corea), minaccia di considerare gli acquisti di criptovalute come investimenti, da dichiarare e sui quali pagare le imposte (USA). Questo spinge i possessori di criptovalute a vendere e quindi i prezzi a calare.
- Voglia di realizzo: se a febbraio 2017 ho acquistato un bitcoin a 1.000 euro e a dicembre 2017 vedo che il mio bitcoin ne vale 15.000 o più, *forse* mi viene voglia di realizzare l'investimento, almeno in parte. Se tanti come me vendono i loro bitcoin, il prezzo globale cala.
- Alcune società avevano stretto accordi con VISA per offrire carte di credito in bitcoin e altre criptovalute. A fine anno, VISA ha deciso di non rinnovare questi contratti non essendo più interessata a questo tipo di meccanismo. Come potete immaginare, viaggiare con in tasca una VISA basata su un portafoglio in bitcoin può essere un modo molto comodo per spendere la somma che nel frattempo era maturata. Sono pochi i negozi che permettono di spendere direttamente bitcoin, mentre sono milioni nel mondo gli esercizi commerciali fisici e online che accettano la carta VISA. Qualcosa in questo campo è sopravvissuto: ne parleremo nel Capitolo 3.
- A fine 2017 è successo anche questo: dirigenti di spicco di grossi investitori annunciano misure restrittive nei confronti delle criptovalute; i valori subiscono un ripido calo; magicamente arriva un grosso investitore a fare acquisti di criptovalute nel punto di minimo; immediatamente il prezzo si impenna e il realizzo è immediato. Si dice che a pensare male si fa peccato, ma spesso si indovina…

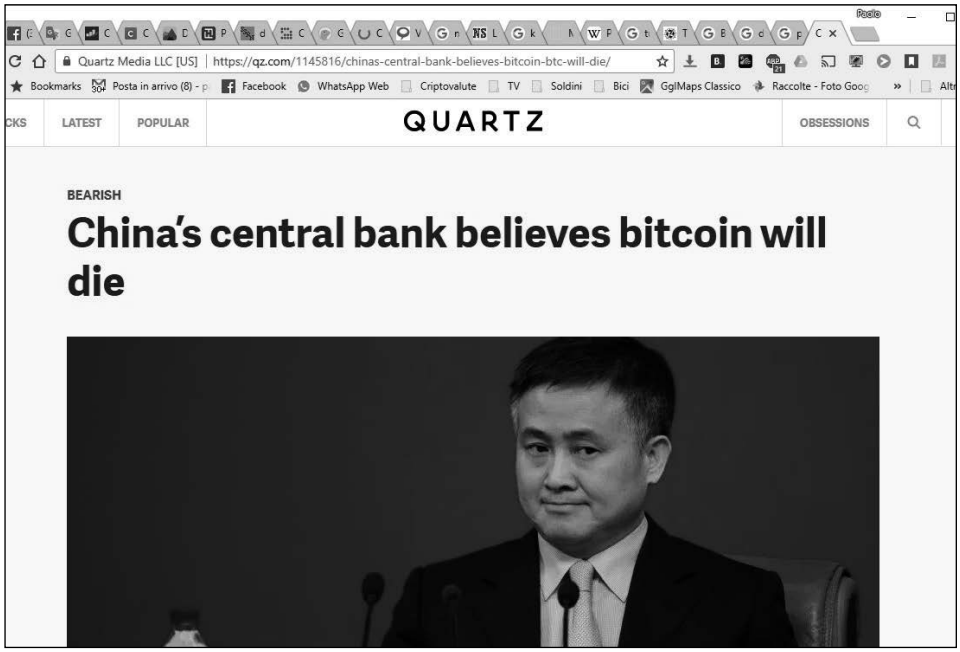


Figura 1.16 A più riprese giungono ad abbattersi sul mondo delle criptovalute vere e proprie "tempeste".

In pratica abbiamo assistito a un vero ottovolante di valori: bastava che un personaggio di spicco della Federal Reserve americana o qualche ministro europeo o qualche politico dell'Estremo Oriente aprisse bocca e ventilasse una "stretta" sulle criptovalute e partiva un'ondata di svendite e di deprezzamenti. D'altra parte, proprio fra novembre e dicembre a spingere in alto il prezzo dei bitcoin e delle criptovalute in generale è stata una sequenza di notizie positive: l'arrivo di investitori istituzionali (stati o regioni), la possibilità che 1 bitcoin raggiungesse il valore di 5 milioni di dollari… Notizie buone: aumenta la domanda e le quotazioni salgono. Notizie cattive: aumenta l'offerta e le quotazioni scendono. Niente di nuovo, normali dinamiche di domanda e offerta.
Ricorderò sempre e rilancio a voi un'affermazione di gennaio 2018 del presidente russo Vladimir Putin, sempre molto attento al campo delle criptovalute. Cito a memoria e interpreto a senso le sue parole:

> Le criptovalute somigliano troppo a una bolla speculativa. Io ho consigliato ai miei cittadini di non fidarsi e di non gettare in queste attività i loro risparmi, ma di giocarci, e limitarsi a valori sacrificabili. Ma non voglio regolamentare le criptovalute in modo troppo restrittivo. Così facendo, qualcuno perderebbe tutto quello che vi ha investito, con un eccesso di fiducia. Non voglio essere io il responsabile della rovina delle loro famiglie.

Un consiglio? Stampatevi bene in testa queste parole.
Detto questo, a volte le tempeste colpiscono una criptovaluta e non l'altra. Per esempio non tutte le criptovalute garantiscono il pieno anonimato del loro possessore. Per esempio, Ripple è una criptovaluta semiufficiale, sponsorizzata da varie banche. Vari paesi hanno allo studio criptovalute da affiancare a quella tradizionale e nessuno si aspetta che la loro dote principale sia l'anonimato. Altre criptovalute sono un po' più protette e sicure per chi non voglia far sapere proprio a nessuno che cosa fa dei suoi soldi. È il caso di monero. Così capita di assistere a questa sequenza.

1. *Breaking News*: "L'ente statale *tal dei tali* minaccia di imporre tasse sui guadagni da criptovalute".
2. Vendite di criptovalute "trasparenti" e calo del loro valore.
3. Acquisti di criptovalute "riservate" e innalzamento del loro valore.

Dopodiché la notizia non ha alcun seguito effettivo e i rapporti si ristabiliscono: il tutto ha causato solo una "perturbazione" di breve durata. In pratica la criptovaluta più riservata funge da "bene rifugio" per i rischi corsi con la criptovaluta più trasparente. È una dinamica classica, che può essere sfruttata per compiere piccole speculazioni fra una criptovaluta e l'altra. A patto di scommettere su tale dinamica.

Le truffe non finiscono mai

Una costante di tutto l'ambiente "spicciolo" dei siti web che si occupano di criprovalute è la presenza di link pubblicitari. Molto spesso si tratta di rimandi a siti dalla serietà "piuttosto dubbia" (Figura 1.17). Un consiglio: non fidatevi troppo. I rischi in questo mondo sono moltissimi, ma il fine ultimo, quasi sempre, lo scoprite immediatamente:

- vogliono il vostro denaro (in euro) per sostenere il loro impegno nella creazione di una nuova e "rivoluzionaria" criptovaluta (le già citate Initial Coin Offering, ICO);

- vogliono invitarvi a una lotteria (in bitcoin o altro) per raddoppiare il vostro gruzzolo in poche ore;
- vogliono invitarvi a un gioco/sito/sistema che seguirete con cura per giorni e giorni, rimpinzandovi di pubblicità per ricevere qualche "soldino" in criptovalute (Capitolo 2) ma dal quale non vedrete mai il becco di un quattrino;
- vogliono vendervi materiale di mining obsoleto al prezzo del nuovo (vedi Capitolo 4);
- la fantasia per spillarvi denaro o tempo è sempre al lavoro… sicuramente vi sono molti altri modi per attirarvi.

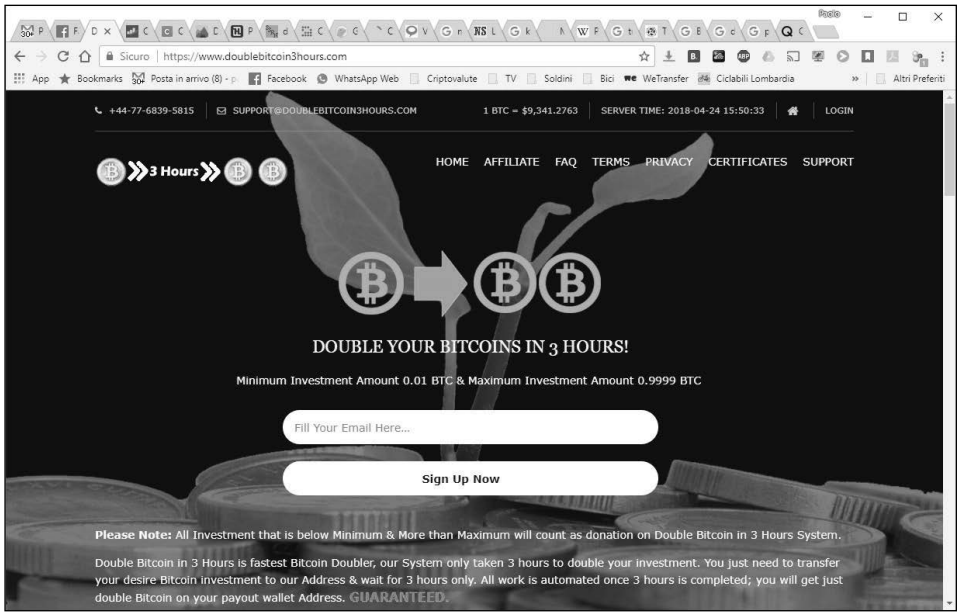


Figura 1.17 Il Web e il mondo delle app è disseminato di trappole.
Evitarle non è difficile: se è troppo bello per essere vero, molto probabilmente NON è vero.

L'ambizione dei prossimi capitoli è quella di offrirvi un "sentiero sicuro", che potrete percorrere con una certa sicurezza e, spero, con grandi e piccole soddisfazioni, senza danni irreparabili o arrabbiature. Aspettatevi comunque di cadere saltuariamente in qualche trappola, quanto meno perché i tempi cambiano, i siti a volte vanno e vengono e nessuno può sapere quanto varranno le criptovalute fra un mese o un anno. Fate sì che eventuali perdite siano superabili con una scrollata di spalle e una buona birra.