FRANCESCO GALVANI

# BITCOIN, BENEFIT, BOOM!

Capire e sfruttare le **criptomonete** senza lasciarci le penne.

# BitCoin, Benefit, Boom!

*ovverosia*

Capire e sfruttare le criptomonete senza lasciarci le penne.

# FRANK (FUN)DAMENTALS



www.francescogalvani.com

# INTRODUZIONE

## Bit by bit

Ho scribacchiato per la prima volta a proposito di BitCoin nel 2013 sul mio blog personale. Un articolo esaltato punteggiato da frasi elettrizzate. Roba del tipo: "*BitCoin è più di una nuova moneta, è una rivoluzione democratica e sociale!*". Insomma, col senno di poi sembravo sotto anfetamine.

In verità non avevo capito praticamente nulla di BitCoin. Quasi certamente non ci avevano capito molto nemmeno le persone che si sono complimentate con

me leggendo quelle parole piene di vigore. E altrettanto indubbiamente la stragrande maggioranza della popolazione umana che vive sul pianeta Terra nel 2018 fatica a maneggiare anche solo lo *spelling* di "BITCOIN". Non per propria colpa. Si tratta effettivamente di un caos senza fondo.

Eppure *tutti* ne vogliono far parte e sentono in qualche modo di farne parte.

Il 99% delle conversazioni sulle criptomonete in cui mi imbatto potrebbe essere sintetizzato con un buon margine di successo nella seguente affermazione:

*Non ne capisco granché, ma so per certo che c'è qualcosa di grosso qui.*

*Intanto fingo di padroneggiare l'argomento, vedi mai che qualcuno ci creda.*

Vi ritrovate in questa proposizione? Sì? In caso contrario non potete non ammettere di aver pensato lo stesso origliando quel che si dicevano con alterigia i due tizi al tavolino accanto a voi al bar o i vicini di posto in treno.

C'è *davvero* qualcosa di grosso nel cripto-universo, qualcosa che cambierà il nostro futuro, ma è troppo complicato indagarla per la maggior parte di noi. Quindi ci si limita spesso a riportare opinioni altrui o frasi fatte. Alcuni si dichiarano esperti se per fortuna

sfacciata hanno racimolato qualche soldino o hanno appreso qualche termine tecnico sentito qua e là. Molti evitano del tutto il discorso, visto che hanno perso centinaia di Euro giocando con i BitCoin e non vogliono si sappia troppo in giro.

Eppure *tutti* ne siamo incuriositi.

Sarà per il suo alone di mistero e leggenda, sarà per i suoi segreti iniziatici, sarà perché genera angosce nei potenti, sarà perché annusiamo un ingombrante cambiamento nell'aria come a primavera. Siamo naturalmente sedotti dalle *criptomonete*. Un po' come quando qualcuno urla il nostro nome

nella folla, alla sola parola “BitCoin” ci svegliamo dal torpore e iniziamo ad ascoltare diligentemente, confidando di imparare qualcosa da sfruttare a nostro vantaggio.

Questo libro è quindi per voi, intrigati da BitCoin e fratelli. Per voi che ne avete abbastanza dell’aria fritta e dei tecnicismi scagliati a caso sul tavolo dai guru autoproclamati. Per voi che avete compreso la complessità affascinante di questo universo ma non avete una mappa per orientarvi. Per voi che volete afferrare al volo l’occasione di fare qualche soldino senza però lasciarci il portafogli. Per quelli di voi a cui non bastano le facilonerie esaltate degli

ingenui, ma che intendono piuttosto assaporare il piatto sino in fondo. Accompagnati da qualcuno che educhi a percepire anche le note amare e sapide.

Inizieremo il nostro viaggio accompagnati da una storia entusiasmante che ci condurrà senza scossoni e senza sforzo alla comprensione di cosa sia realmente il denaro e come le diverse sue concezioni abbiano plasmato la storia della nostra specie e la nostra vita. Salvandoci da una terza guerra mondiale ma affondandoci in una crisi terribile nel 2008.

Nella seconda sezione arriveremo ai

BitCoin, figli illegittimi di questo formicolio ideologico. Capiremo cos'è una criptomoneta e, continuando a farci guidare dal piacere della scoperta, scandaglieremo il pozzo sempre più giù, sino a vedere i pistoni che fanno funzionare il motore di BitCoin.

Risaliremo poi sulla terraferma e affronteremo di petto i temi caldi reali, i limiti e le potenzialità delle criptomonete. Come incidono e incideranno sul nostro mondo, sui nostri stati, sull'atmosfera, sulla geopolitica e sulle nostre finanze. Sarà un indispensabile momento di discussione poliedrica tra tecnologia e complessità umanistica.

Arriverà poi il tempo di imparare a *fare soldi con i soldi*. Sfruttando le criptovalute per ricavare un beneficio reale e tangibile in senso finanziario. I cuor di leone potranno a questo punto farsi il risvolto alle maniche della camicia e sporcarsi le mani con il trading più eccitante e spericolato dell'attuale fase economica.

Infine, proveremo a scrutare il futuro. Alzeremo lo sguardo sopra l'orizzonte e oltre le nebbie di oggi. Scoperchiando le nuove sorprendenti criptovalute che sovrasteranno BitCoin e che risponderanno finalmente e senza compromessi ai nostri desideri di democrazia, etica e meraviglia

tecnologica.

Direi che è tempo di iniziare, che ne dite?

Vi chiedo la cortesia di spostare subito le lancette del vostro orologio avanti di qualche secolo.

# SIANO CREATI I SOLDI!

## Una nuova Genesi

“Comandate *Chance*. L’hanno fatto. Come ci aspettavamo da anni, quei bastardi del fronte est hanno alla fine attivato la *cortina TNW (Tactical Nuclear Weapons, bombe nucleari tattiche)*. So che non intendeva farlo, ma dobbiamo attivare il protocollo *New Genesis*. Adesso. Se attendiamo saremo polverizzati in poche ore. Non abbiamo più tempo. LO ATTIVI ORA”.

“Stratega *Marshall*, lo sa che è una strada senza ritorno. Ne abbiamo parlato

centinaia di volte. Se premo quel maledetto pulsante la vita su questo putrido pianeta maleodorante cesserà entro un mese. Non avremo il lusso di un inverno nucleare. Lo capisce o no? Vuole davvero questa responsabilità? Io no. Non sono pronto".

"Perché è un codardo. Come tutti voi della *gens Chance*, ormai siete più ingegneria genetica che DNA biologico. Ne ho abbastanza! Con quegli innesti cromosomici vi hanno salvato dal declino dell'intelletto iniziato 300 anni fa nel XX secolo. Ma a che costo?

Vi hanno resi sì intelligenti, ma fragili. Intimoriti da tutto. Fate carriera più

facilmente di noi umani comuni solo grazie ai voti nei test dell'accademia, ma quello stesso vostro cervello superiore è la vostra rovina! Non sapete prendere decisioni. Siete deboli, conigli spaventati. Non come noi. Noi umani originali.

Ma è ora di finirla... se non si sposta subito dal pannello di controllo la farò trucidare dai miei uomini. Sì, la stiamo sollevando dal comando! Al mio cenno un'intera armata entrerà in questo bunker e lei sarà deatomizzato. SI SPOSTI".

"Ferma! No, non lo faccia! La prego!".

"La smetta di piagnucolare. Sto già digitando il codice di sblocco. È stato

così ingenuo da pensare che la sua mente formidabile sarebbe stata in grado di bloccare i nostri rivelatori di tracce sinaptiche. Illuso. Da anni abbiamo acquisito tutti i suoi schemi e segreti.

Ci siamo. Tra dieci minuti sganceremo le nostre testate sui fronti est e nord, annientandoli. Il tempo necessario a permettere all'astronave con gli infanti di lasciare l'atmosfera superiore e dirigersi verso gli esopianeti del sistema solare *Trappist-1*. Spero abbia salutato i mille. La nave sta decollando ora. La osservi!".

Come tuttavia capitava sovente agli umani del XXIII secolo non

geneticamente potenziati lato intellettivo, la stratega Marshall era stata troppo ottimista. I fronti nemici avevano *già* sferrato l'attacco finale e l'astronave con i neonati si salvò solo per un soffio dal bacio fatale dei missili terra-aria delle forze militari dell'est.

Pochi minuti dopo furono lanciate testate nucleari da 500 Megatoni l'una da tutte le coalizioni dei regni *post-ONU*. La vita sulla Terra collassò quasi all'istante.

La nave spaziale con a bordo gli infanti era stata fortunatamente progettata dagli scienziati della *gens Chance*, quindi dalle migliori menti disponibili nel

2300. Era uno scrigno di perfezione ingegneristica. Nutrici robotiche modello *Child7* potevano vegliare per anni sugli ultimi umani salvati dall'apocalisse, svezzandoli prima e istruendoli poi. Mentre una ragnatela di droni proteggeva giorno e notte la grande arca, circondandola come un cuscino protettivo. Salvandola dai corpi estranei dell'universo *hyper-luce* e riparando ogni possibile falla a motori e scafo.

Dieci anni di navigazione. 39 anni luce. Puntuale come un orologio svizzero, l'astronave arrivò nel sistema Trappist e si settò in ottica geosincrona attorno al pianeta *d*, quello con le migliori

condizioni per la vita. Inviò sulla superficie un vascello con 700 ragazzini di 10 anni.

Altri 300 vennero spediti, con statistico cinismo, verso il pianeta *e*. Gli ingegneri sapevano che per loro le cose sarebbero state più complicate: il pianeta *e* era più freddo del pianeta *d* e le sue onde elettromagnetiche nei venti nella toposfera friggevano qualsiasi circuito tecnologico. Ma questo potenziale martirio dei 300 era necessario.

Gli umani non volevano infatti compiere lo stesso errore fatto con la Terra: l'umanità doveva diffondersi su *almeno* due pianeti per evitare che un solo

evento catastrofico su un pianeta potesse annientarla di nuovo. Serviva un disegno di *backup* robusto. Dividersi su due astri era la strategia statisticamente più robusta per massimizzare la probabilità di sopravvivenza della specie. Anche se in uno dei due pianeti le condizioni erano più difficili dell'altro.

Il vascello dei 300 ebbe giusto il tempo di atterrare sul pianeta *e* prima di vedere i suoi sistemi digitali crepitare come gamberi in padella e guastarsi inesorabilmente per via dei venti elettromagnetici. I 300 erano adesso soli. Ragazzini impauriti. In futuro gli altri 700 avrebbero di sicuro trovato il modo di inviare loro nuovi strumenti

tecnologici resistenti a quei dannati venti, ma per ora dovevano arrangiarsi e sopravvivere col loro puro ingegno. Per decenni, probabilmente.

La vita ripartì. Le nutrici robot avevano insegnato molto ai ragazzi, e questi non ci misero molto a costruire semplici villaggi e un paio di comunità. In fondo c'era ossigeno, piante simili a quelle terrestri, qualche specie animale commestibile, materie prime.

Vide la luce una semplice economia di scambio e una sorta di governo centrale con dieci consiglieri alla pari. Le decisioni comuni erano prese a maggioranza. Sistema semplice, ma

efficace.

Sembrava tutto funzionare alla grande. Finché, dopo una decina di anni di paradiso terrestre, l'edificio sociale iniziò a scricchiolare.

Si erano aperte tre grossissime falle:

- Il **baratto** delle merci non bastava più. Era diventato sempre più complicato stimare, ad esempio, a quante pecore-nane di *Mbolia* corrispondessero 100 kg di grano *katan* primino. Le liti scoppiavano sempre più spesso.

- Si era reso necessario trovare un metodo oggettivo per **multare** i

trasgressori alle leggi comunitarie - senza punizioni corporali, possibilmente. Come valutare le differenti violazioni? Cosa farsi dare dai cittadini colpevoli? Se John coltivava *Crumiskwi* e Bill era un fabbro, quale poteva essere una merce comune a entrambi che poteva essere usata per andare in pari con la legge in modo esatto?

- Anche il pagamento delle **tasse** era diventato ingestibile. Come sopra, persone diverse pagavano i tributi con beni diversi, rendendo impossibile una gestione equa e esatta. Continue polemiche sull'ingiustizia dei diversi

pagamenti stavano minando la comunità e il rischio concreto di una guerra civile era dietro l'angolo.

# La congiura dei *Mins*

Per mesi i consiglieri si riunirono più volte a settimana per trovare soluzioni. Furono proposte varie strategie. Una in particolare risultò interessante e venne applicata.

Si decise che un raro cristallo locale chiamato *Mins* dovesse divenire una sorta di "minimo comune denominatore" negli scambi. I cittadini erano incentivati a darsi da fare per la comunità: per ogni ora di lavoro "socialmente utile" veniva dato loro un *Mins*, che poteva poi essere usato per pagare le tasse o al posto del baratto. I cristalli erano estratti da una squadra scelta al servizio dei dieci

consiglieri. La miniera era custodita dalle uniche guardie armate del regno e il numero di cristalli estratti per settimana era deciso dagli stessi consiglieri.

Pian piano il *Mins* divenne **moneta** stabile e in un paio di anni tutte le tasse e le multe iniziarono a essere risolte con questi cristalli. Ogni scambio tra persone era mediato dai *Mins*.

Qualcuno iniziò ad avere qualche cristallo in più e a poter quindi comprare più merce. Il suo status si elevò di qualche punto rispetto agli altri. Cominciò a essere invidiato. Vedendo questo esempio, la maggior parte dei

cittadini incominciò a darsi un gran da fare per accrescere il proprio benessere allo stesso modo, in un circolo virtuoso che produsse sempre più merci e servizi di qualità sempre più alta.

Sembrò tutto funzionare alla grande per anni, in un *egoistico ma consistente* progresso comune.

Finché due dei dieci consiglieri capirono che potevano *piratare* il sistema a proprio vantaggio. In fondo erano loro stessi a gestire la fornitura dei *Mins*, e potevano quindi appropriarsi dei cristalli in modo diretto senza faticare. Al fine di migliorare il proprio personale benessere.

Fecero così un accordo con una guardia armata e un paio di minatori. Decisero di aprire un'altra entrata seminascosta nella miniera dei *Mins* e di dividere alla pari con gli estrattori corrotti e il militare gli ulteriori cristalli strappati alla terra. La nuova miniera veniva scavata di notte per non destare sospetti.

Dal nulla, 5 persone (di cui due al potere) erano diventate inspiegabilmente benestanti e si misero a vivere una vita di maggiori comodità.

Non poteva durare. Più di qualcuno iniziò a insospettirsi: la comunità era piccola e tutti si tenevano sott'occhio. Uno dei minatori non coinvolti dalla

“congiura dei *Mins*” seguì i due colleghi furfanti dopo il tramonto e scoprì l’entrata secondaria della caverna.

Scoperto il trucchetto convinse tutti gli altri minatori e le guardie a fare lo stesso: aprirono quindi un altro accesso alla miniera da tutt’altra parte e iniziarono a scavare come pazzi ogni notte. Diventarono abbienti dalla sera alla mattina. Qualcun altro si insospettì, ma non poteva dimostrare molto. Le guardie armate erano leste a disincentivare i curiosi.

Tutto bene quindi?

Non esattamente.

Stavolta la quantità di *Mins* estratta era alta. Abominevolmente alta. Questi minatori non avevano la raffinatezza che distingueva la prima cospirazione. Se nel primo caso i due consiglieri avevano usato accortezza facendo scavare i pochi cristalli necessari per migliorare di poco il proprio comfort senza sconvolgere eccessivamente l'economia locale, stavolta non c'erano limiti. Veniva estratto tutto il *Mins* che si trovava.

E si scatenò la tragedia.

I 300 cittadini delle due comunità del pianeta *e* scoprirono il demone dell'*inflazione*.

Maree di *Mins* iniziarono a inondare gli scambi commerciali. C'erano talmente tanti cristalli in giro che, per ovvie ragioni, i prezzi delle merci si alzarono. In fondo chi non voleva sfruttare l'occasione di guadagnare di più per la stessa quantità di prodotto venduta vista la disponibilità di moneta circolante?

In un circolo auto-catalitico di domanda e offerta i beni raddoppiarono di prezzo in pochi anni. Le tasse si alzarono. I consiglieri normalizzarono le multe alla nuova situazione.

Disgrazia totale.

Immaginate per un secondo di aver lavorato per anni come dei muli per

mettere da parte un centinaio di *Mins* per assicurarvi un futuro più tranquillo o per poter comprare quella meravigliosa composizione minerale del famoso designer *Sander*. O per acquistare materiali di qualità più alta per costruirvi un'abitazione più confortevole. Bene. Vi svegliate un bel giorno e scoprite che i vostri 100 *Mins* possono OGGI comprare la metà dei prodotti che potevano acquistare TRE ANNI FA. Perché nel frattempo tutti i prezzi sono raddoppiati.

Dannazione.

Niente composizione artistica di *Sander*. Niente futuro sereno. Niente casa più

confortevole.

Niente. Tutto sparito. Senza motivo. Solo per colpa di un artificio economico con cui voi non c'entrate nulla. Siete disperati e non capite cosa sia successo.

Ma che diamine?

# Fuori dalla metafora, *please*

Fine della prima parte.

Vi ho intrattenuto con una bella storiella *sci-fi-fantasy-finanziaria*. Vi siete divertiti? Lo spero. Avete imparato qualcosa? Se mi dite di no mi arrabbio.

Avete appena appreso un sacco di concetti macro-economici che vi serviranno per comprendere perché esistono le reginette di questo libro che tanto adorate - criptovalute e blockchain – e a cosa dovete stare attenti se volete invitarle al ballo.

Che ci ha insegnato in definitiva la favola dei *Mins*? Un sacco di idee

incastrate tra loro a beneficio narrativo. Sciogliamole e impareremo come funziona lo splendido mondo dei soldi e perché sono emerse le criptovalute. Ok, magari la frase "*splendido mondo dei soldi*" vi riporta alla mente noiosissime ore di economia e storia e vi fa accigliare. Accetto la critica. Ma ve lo prometto, non vi addormenterete stavolta.

Prima idea da portarci a casa: i *Mins* sono **valuta** ma non sono **moneta**. Differenza più estrema di quanto sembri.

La "moneta" (*currency*) è rappresentata dai bei foglietti di carta e gli oggettini circolari di metallo che avete nel

portafoglio. Ma sono solo *una* delle infinite manifestazioni possibili della valuta, che è qualcosa di più ampio e etereo: un deposito di **valore**. Capite bene che questo deposito teorico si può concretizzare come diamine vi pare: soldi di carta o monetine, conchiglie, contratti, sassi blu, pecore nane, pepite d'oro, arancini, palline di Natale, bit. Ogni società ha scelto il suo mezzo prediletto per conservare il valore.

Il che ci porta alla domanda chiave. Perché nel pianeta *e* (e nel nostro pianeta Terra) tutti i popoli hanno sentito prima o poi il bisogno profondo e naturale di inventarsi un sistema di deposito di valore, cioè una valuta?

Nella favola ho svolto i compiti per voi: i popoli hanno questa necessità sia per superare i limiti del baratto, *sia* per permettere ai governi di gestire le società in modo efficiente. L'ho fatta semplice, ma vi assicuro che da decenni – anzi, secoli – gli intellettuali vedono i due scopi come opposti. E la cosa ci interessa parecchio se non vogliamo essere spettatori impreparati dei cambiamenti sociali dati dalle criptovalute! Poi capirete perché.

C'è chi venderebbe la nonnina per difendere la tesi secondo cui la valuta nasce spontaneamente dalle genti per evitare il caos degli scambi, e il suo valore è interno all'*oggetto* stesso usato

come valuta. Secondo questi tizi – i **metallisti**, da non confondersi con i metallari – i *Mins* sono una valuta perfetta perché hanno un loro valore di scambio oggettivo dato dall'essere cristalli rari. Sono una commodity. Anche prima di trasformarli in denaro tutti convenivano all'idea che un kg di *Mins* valesse parecchio e fosse prezioso.

Scommetto sappiate perfettamente cos'è stato sulla Terra il corrispettivo dei *Mins* per la maggior parte dei popoli e della storia.

Sì, le pepite gialle del *Klondike*. L'**oro**. Più o meno tutti conveniamo che l'oro

abbia valore di per sé. È raro, tanto per cominciare. È splendido. Fa felici le donne. È il metallo nobile per eccellenza con cui si possono fare miracoli in elettronica.

Sia chiaro, i metallisti non sono così rimbambiti da non notare che prima o poi quasi tutti i popoli passano dallo scambiarsi oro e monete (dal valore intrinseco oggettivo) a trasferirsi foglietti di carta e monetine metalliche di poco valore, se non simbolico. Ma per loro il concetto non cambia: l'importante è che tutti questi oggettini usati come moneta siano sempre **convertibili** in oro, o nel *Mins* di turno. Poco male se una banconota da 10 Euro

costi in termini di materie prime e produzione non più di 3 centesimi.

Chiaro? Se proprio non si vuole usare direttamente il bene prezioso per gli scambi, per i metallisti l'importante è che da qualche parte ve ne sia un deposito corrispondente alla quantità di denaro circolante.

> *Se ad esempio la banca centrale Europea volesse che in giro per il globo ci fossero 1.000 miliardi di Euro, secondo i metallisti dovrebbe avere in suoi caveau segreti una quantità di oro del valore di 1.000 miliardi.*

In questo modo tutti sono felici e non si

rischia di avere in giro più soldi di quanta ricchezza *reale* essi rappresentino. Un bel modo per tenere i conti in ordine e sentirci tutti bravi padri di famiglia.

Pura teoria accademica inutile? Mica tanto. È probabilmente grazie a una decisione metallista se non abbiamo avuto una terza guerra mondiale.

Cosa?! Frank sei impazzito?!

*No,* almeno stavolta. Facciamo brillare i nostri neuroni ricordandoci le lezioni di storia. Qual è stata la fortuna di Hitler? Perché i tedeschi sono impazziti di colpo e l'hanno votato?

Per lo stesso motivo che fa emergere ogni dittatore: una situazione economica **disastrosa** che esaspera i cittadini. Nella Germania distrutta dalla prima guerra mondiale, per via delle sciagure passate e dei pagamenti agli stati vincitori, l'inflazione divenne estrema. Il deposito di ricchezza delle persone – il *Marco* – si deprezzava alla velocità della luce, rendendo tragico condurre una vita dignitosa. Oggi potevi comprarti gioielli, tra un mese con gli stessi soldi a fatica potevi arrivare ad una pagnotta.

In queste condizioni qualsiasi uomo forte che prometta un futuro radioso ha gioco facile. E Hitler l'ebbe. Con gli

effetti che tutti conosciamo.

# Per un pugno di Dollari

Andiamo avanti qualche anno nella storia.

Verso la fine della seconda guerra mondiale si decretò di non rischiare il ripetersi di queste condizioni da polveriera dei popoli.

Per questo motivo a *Bretton Woods*, nel New Hampshire in USA, 720 delegati di 44 nazioni alleate stabilirono che l'economia globale dovesse essere sì liberista, ma in chiave **metallista**. Basta inflazione esasperata. Basta manipolazione degli scambi monetari per ripagare i debiti statali sulle spalle dei popoli. Ogni moneta nazionale da lì

in avanti doveva essere *bloccata* nel suo valore col Dollaro, e il Dollaro doveva essere sempre *convertibile* in oro.

Ha funzionato? Eccome. Gli stati misero giudizio e il Dollaro divenne la versione monetaria dell'oro. Non a caso fino a pochi anni fa i "*verdoni*" erano la polverina magica che faceva girare il mondo.

Finché non arrivarono le spese pazze americane degli anni '70 (qualcuno ha detto "Guerra del Vietnam"?), finché la Francia non si inventò di voler convertire zizzilioni di Dollari in oro, col rischio di prosciugare tutte le riserve auree statunitensi. A quel punto un Nixon

esasperato dal far quadrare i conti disse al mondo "*Beh, sapete che c'è? Bretton Woods non ci piace più, ognuno vada per la sua strada*". Distruggendo il regime metallista.

Da quel momento non era più necessario che il denaro fosse convertibile in oro, ogni stato nazionale poteva tornare a produrne quanto ne voleva. Non esisteva nemmeno più un tasso fisso di conversione delle valute straniere col Dollaro.

E via a inventarsi turbofinanza, *forex*, inflazioni per risanare debiti. Insomma, il mondo di oggi è frutto di quella decisione.

Nixon in questo caso ha seguito una filosofia opposta al metallismo, cioè il **cartalismo**. Vi ho detto che ci sono due fazioni di intellettuali che si menano di santa ragione (simbolicamente) in economia, no? I cartalisti sono l'altra gang.

Per il cartalismo l'idea che le monete debbano essere sempre e comunque convertibili in un bene (prezioso) è una scemenza masochista che limita l'economia e la creazione di ricchezza. Per loro il denaro non nasce come evoluzione del baratto, ma piuttosto come strumento dei governi e delle banche per permettere alle persone di creare debito, pagare tasse, multe, per

creare opere pubbliche, e così via. Insomma, è un congegno di democrazia, oltre che deposito di valore. E uno stato – o un sovrano – è in fondo il detentore ultimo del diritto di creare denaro, quindi ne può produrre quanto diamine gli pare, se questo permette alla società di funzionare bene.

Se vi sconvolgete e arrabbiate quando sentite dire che "*gli scambi finanziari oggi equivalgono a migliaia di volte il denaro reale*" o che "*bisogna stampare un sacco di nuova moneta per combattere il debito e far ripartire l'economia*" significa che non ragionate da cartalisti. A me va benissimo la vostra posizione, sia chiaro, ma dovete

capire da che parte state della guerra civile tra le due fazioni. Altrimenti come sapete contro chi inveire nei post su Facebook?

Sul pianeta *e* domina chiaramente il metallismo. La concezione dei *Mins* come bene rifugio dotato di valore intrinseco è piuttosto rivelatrice. C'è però stato un comportamento cartalista negativo da parte dei potenti nella manipolazione del mercato a proprio uso e consumo. Un comportamento che prima o poi fa capolino nella storia di molti popoli.

# La fucina di monete

Diciamoci le cose come stanno: dopo la crisi del 2008 siamo tutti un po' infastiditi dal cartalismo e da ciò che comporta la sua filosofia. Oddio, magari fino a 10 minuti fa la rabbia di molti di voi non era indirizzata verso la parola "cartalismo", ma ci siamo capiti.

Abbiamo perso fiducia negli stati e nelle banche centrali. Perché non hanno controllato quel che stava succedendo – anzi, hanno ostentato un *laissez faire* estremo verso le grandi banche d'affari e le loro mastodontiche costruzioni finanziarie totalmente slegate dai beni reali. Perché hanno usato uno sterminio

di soldi dei contribuenti per salvare queste stesse istituzioni mefistofeliche. Perché hanno iniziato a stampare fiumi di denaro per ripagare debiti e per far ripartire l'economia.

Questa mancanza di serietà nei confronti dei cittadini coniugata a furberie di ogni tipo è la faccia **oscura** che a volte il cartalismo ha mostrato nella storia. Semplicemente, questa filosofia mette tanto potere in pochissime mani perché niente è legato a beni tangibili e tutto è discrezionale. Ed è dura per noi fidarci di queste mani, specie quando in passato ci hanno preso in giro.

Sul pianeta *e* l'abuso di potere da parte

di consiglieri prima e di minatori poi è stato fin troppo evidente e ha portato alla terribile e nefasta inflazione che ha rovinato la vita a così tanta gente. Non si scherza col deprezzamento della valuta. La Germania dovrebbe esserne la prova.

In sintesi: per quanto questa dottrina di artificiosità finanziaria apra mercati, permetta di far crescere l'economia col mix di debito + inflazione e di risolvere spesso insostenibili problemi di convertibilità del contante, presenta debolezze pronte a presentare il conto quando i popoli non se l'aspettano. *Not good*.

Quindi che si fa?

Prima di procedere voglio essere certo abbiate compreso esattamente i termini della faccenda. Che è tutto fuorché banale. Se non siamo allineati vi sarà dura apprezzare il valore simbolico e concettuale delle cryptomonete e essere meno vittime delle bufale e dei mascalzoni.

Nei regimi metallisti abbiamo quindi due opzioni:

- Possiamo scambiarci direttamente dei beni con un proprio valore intrinseco – come oro, argento, cotolette.

- Possiamo usare delle valute che siano convertibili in questi stessi

beni a comando. Cioè ogni singola banconota in circolazione si deve riferire a una quantità esatta di commodity materiali stipate in qualche rifugio segreto.

Nei regimi cartalisti le cose vanno diversamente:

- Le monete cartacee (Euro, Dollaro, Franco svizzero) sono inconvertibili in beni rifugio ma hanno corso legale per pura decisione degli stati che le emettono. Il loro valore è cioè deciso a tavolino da qualcuno di potere. Che può diminuire a piacimento tale valore diluendolo

tramite la stampa di più banconote, o aumentarlo acquistando titoli di stato in cambio di denaro contante.

- Questi vettori di pagamento accettati in una comunità ma inconvertibili hanno un nome latino quasi religioso: "***fiat* money**" - *Siano creati i soldi!* Questo la dice lunga sul potere divino nelle mani di pochi, no?

Quando la **fiducia** nell'autorità divina che emette denaro viene meno, si finisce a gambe all'aria. Pensate all'Argentina. Il problema non è stato tanto la crisi del debito e il default. Quanto piuttosto una sotterranea e logorante mancanza di

fiducia dell'intera popolazione verso stato e banche centrali. È questa mancanza di fiducia il vero guaio.

In Argentina lo stato decide a piacimento di non permettere ai propri cittadini di convertire i Pesos in Dollari. In Argentina lo stato svaluta la valuta a proprio gradimento. E i cittadini come risposta non si fidano più della loro nazione. Credono solo a istituzioni private approvate da amici e parenti e, quando possono, le tentano tutte per conservare la propria ricchezza in conti all'estero. Non esattamente le condizioni per far fiorire un'economia.

È questo il messaggio finale del primo

capitolo. Al termine di questo piccolo viaggio in cui avete scoperto le differenti visioni del rapporto tra denaro e società ho una domanda per voi.

Cosa sono in definitiva i soldi?

**Fiducia.** Niente più che fiducia.

Nel cartalismo la nostra ricchezza dipende:

- Dalla fiducia che tutte le altre persone assegnino al denaro lo stesso valore che vi assegniamo noi. Che un Euro sia un Euro per tutti.

- Dalla fiducia che riponiamo negli stati e nelle banche centrali.

Vogliamo credere che domattina questi istituti non raddoppino il numero di contante in circolazione diminuendo all'istante le nostre sudate sostanze.

Nel metallismo:

- Dobbiamo avere fiducia che il valore del bene prezioso che sottende la convertibilità del nostro denaro sia tale per tutti, cittadini e governi.
- Dobbiamo credere che questo stesso bene esista da qualche parte in una quantità compatibile col denaro in circolazione.

Senza questa imprescindibile fiducia nessuno risparmia, nessuno presta soldi. Pochi vogliono lavorare in cambio di denaro. Nessuno vuole conservare troppi soldi in banca. Molti li gettano senza pensarci troppo in immobili su immobili alimentando bolle esasperate e cementificazioni selvagge.

Questo effetto a catena riporta le società al baratto, rende impossibile l'emissione del debito e il pagamento delle tasse. Facendo collassare il sistema.

Forse BitCoin vuole in verità impedire tutto questo?

# In sintesi

- La definizione di "*soldi*" è tutto fuorché pacifica e nel tempo si è prestata alle più aggressive scuole filosofico-finanziarie.

- Benché tutti abbiamo in banca e nel portafoglio svariate monete e banconote, la verità è che non ci interessa particolarmente l'aspetto tangibile del denaro. Quanto piuttosto il suo essere una valuta in grado di fungere da deposito di valore.

- Secondo i metallisti tale valore è assoluto e oggettivo e dipende dalla convertibilità della moneta

(che si può esprimere in oggetti reali o virtuali) in un bene tangibile, quale l'oro. Se una moneta non è convertibile in una commodity reale, non ha valore.

- Viceversa, per i cartalisti il valore di una moneta è relativo e dipende solo dalla sua capacità di consentire il funzionamento di una società economica sviluppata, permettendole di creare debito e di far pagare le tasse. E in generale di far girare il sistema. Per questo il garante ultimo della valuta non è un bene in cui è convertibile, ma il sovrano o la banca centrale.

- Durante il ‘900 i due sistemi si sono alternati per risolvere situazioni storiche spesso drammatiche. Entrambi hanno dimostrato punti di forza e debolezze.

- I decenni recenti sono stati il momento di massima espressione del cartalismo, che ha però portato incidentalmente alla deflagrazione della crisi economica del 2008 e alla successiva recessione.

- Al di là di ogni definizione possibile e di ogni teoria su origine e funzionamento, il pilastro fondante di ogni valuta è uno solo:

la fiducia nelle altre persone e nel sistema.

- Le monete aventi corso legale in un particolare territorio (nazione o gruppo di nazioni) si definiscono "valute *fiat*" dal concetto di "*fiat* money". La parola latina tende a stressare la totale libertà per la banca centrale del territorio in questione di creare a suo piacimento il denaro secondo le necessità di governo dell'economia, in puro e distillato spirito cartalista. Euro e Dollaro rientrano precisamente nella definizione.

- Come vedremo presto, BitCoin & compagni Sono tutto fuorché valute *fiat*. Con tutto ciò che questo comporta.

# BIT MONEY

## Il sacro registro

“Signori, oggi non sono qui per chiedere a taluni di ammettere le proprie colpe e di umiliarsi di fronte agli altri. Non mi interessa. Il passato è passato. È tempo di guardare al futuro. Non sappiamo quando i nostri fratelli del pianeta *d* arriveranno a salvarci. Non sappiamo nemmeno *se* saranno mai in grado di sviluppare circuiti resistenti ai nostri venti elettromagnetici. Quindi dobbiamo arrangiarci. Siamo soli. Lo siamo sempre stati. E proprio per questo

motivo non possiamo perdere tempo ad accusarci l'un l'altro.

La congiura dei *Mins* ha mostrato il peggio della nostra splendente società. Sfruttiamo quello che ci ha insegnato per valutare un nuovo sistema. Moderno, intelligente. In grado di tenere a bada i nostri istinti più bassi e la loro volontà egoistica di appropriarci del bene comune.

Per raggiungere questo futuro fulgido e ripristinare una condizione umana nella nostra economia ho oggi per voi, fratelli consiglieri, una proposta.
Abbandoniamo definitivamente quella mostruosità materiale dei *Mins*. Siamo

capaci di fare di meglio. In fondo sono solo pietre. Ciò che conta non sono i cristalli, ma ciò che **rappresentano**, il loro valore. Io vi chiedo quindi di *astrarre* questo valore dal suo supporto fisico.

Dimentichiamo la sporca materia ma *conserviamo l'informazione* che fino a oggi ha trasportato. D'ora in avanti le transazioni e lo stato non si reggeranno più sul preistorico scambio di pietre. Ma su un unico **registro** infallibile e fulgido in cui, sotto l'egida attenta di un consigliere eletto, saranno annotati tutti i movimenti di denaro.

Niente più cristalli, solo informazione.

Fratelli, se anche voi volete un domani lucido e prospero per il pianeta *e* sapete di dover votare la mia istanza".

La proposta del saggio consigliere *Yivra* venne votata a maggioranza assoluta. Gli altri nove consiglieri non ebbero dubbi. Utilizzare i *Mins* fisici per le transazioni aveva portato solo problemi e **perdita di fiducia** nel governo. I saggi sapevano che ogni scambio di valore pretendeva piuttosto fiducia assoluta da parte dei cittadini. E lo sappiamo anche noi dal capitolo precedente.

Da quel momento quindi, sul pianeta *e* ogni scambio di denaro in cambio di merci, ogni tassa, ogni multa, ogni

transazione doveva essere registrata su un **unico registro** custodito in una cripta nella piazza centrale. Un consigliere era sempre presente per validare l'accordo, e con lui le due parti coinvolte. O una sola parte nel caso di pagamenti al governo delle comunità.

Si decise di continuare a chiamare *Mins* il valore scambiato. Ma era diventata solo una parola. Non c'era più alcun cristallo fisico sul piatto.

Ogni cittadino possedeva un proprio codice numerico personale del tipo "11232443" rilasciato dai consiglieri in modo anonimo e tramite la ricombinazione casuale di cifre in una

giara. Un po' come quando sulla Terra peschiamo i numeri della lotteria da vasi di cristallo. In caso di transazione, sul registro pubblico veniva annotato questo codice associato al codice del ricevente e al valore trasferito. Un *ID* (indice) progressivo assicurava l'ordine nel tempo delle transazioni stesse.

Più o meno come questo:

registro centrale pianeta e

| ID | PAGANTE | MINS | RICEVENTE |
|---|---|---|---|
| 50 | 03243243 | 100 | 34828923 |
| 51 | 33453523 | 20.3 | 32443535 |
| 52 | 43213132 | 0.5 | 75646212 |
| 53 | 11102341 | 12 | 43719205 |
| 54 | 75646212 | 4.5 | 34828923 |
| 55 | 43719205 | 3.3 | 43543334 |
| 56 | 83993247 | 9.7 | 45782983 |
| 57 | 73747387 | 45.4 | 16934092 |
| 58 | 34828923 | 1000.3 | 47373742 |
| 59 | 32443535 | 123.2 | 32823999 |

**Semplice, anonimo, non contraffabile.**

Certo, questo rallentò leggermente le transazioni, ma il fatto tutto fosse pubblico e chiunque potesse calcolare a ritroso il valore associato a ogni codice e la correttezza matematica degli scambi **ripristinò** la fiducia della popolazione

nel sistema. Tutto era adesso chiaro e cristallino. Nessuno poteva fare il furbo e distruggere economia e risparmi personali per via di inflazione dolosa.

Emersero tre cittadini dalle spiccate doti matematiche. Ogni volta in cui qualcuno poneva dei dubbi sulla liceità di qualche compravendita (dubbi del tipo: "*il codice 88393454 non poteva versare 10 Mins al codice 34343534 perché non li possedeva al momento dello scambio con ID 85!*"), veniva interpellato uno a caso di loro.

Il compito del matematico constava nel computare retroattivamente il flusso di cassa del codice incriminato per

verificare la legittimità della transazione accusata.

Aveva o no la persona incriminata in quel momento questi benedetti *Mins* da spendere?

Nel caso in cui fossero emerse irregolarità, i consiglieri dovevano interpellare il cittadino associato al codice anonimo (l'associazione era scritta in un altro registro privato) e multarlo. I soldi di queste multe venivano impiegati per pagare i tre matematici.

Un'organizzazione perfetta. Un sistema matematico e cristallino. **Pubblico ma anonimo**. Inscalfibile. Poteva qualcosa

andare male?

Ehm.

La prossima volta evitate di chiederlo, ok?

Dopo qualche anno, il sistema di "*segnalazione + verifica + multa*" mostrò in modo spettacolare i suoi limiti. Per quanto i matematici avessero inventato ogni possibile stratagemma per creare delle tabelle di sintesi periodiche con i *Mins* posseduti da ogni cittadino al fine di velocizzare i calcoli, la riconciliazione era diventata via via più complicata.

Segnalazioni riferite a indici lontani nel

tempo diventavano via via più difficili da verificare. Peggio ancora, tanti errori di registrazione (quando non vere e proprie frodi!) rimanevano impuniti perché non emergeva alcuna segnalazione!

E per finire in bellezza, il consigliere incaricato di vegliare sul registro trovò il modo di sfruttare di nuovo il suo potere. Facile capire come: lo stipendio dei matematici era quel che era; bastava poco per "oliarli" con qualche *Mins* e far chiudere loro un occhio proprio sui controlli delle transazioni associate al codice del signor consigliere.

Che poteva quindi far comparire

magicamente nuovi *Mins* associati al suo codice tramite transazioni fantasma mai verificate.

Insomma, a quattro anni dal lancio del registro pubblico era divenuto impossibile riconciliare i calcoli tanto erano stati manipolati nel corso del tempo, volenti o nolenti. Erano stati creati dal nulla un sacco di nuovi *Mins* e diverse persone avevano più soldi del dovuto, con i problemi che questo comporta.

Tanta fatica per essere di nuovo al punto di partenza. Qualsiasi sistema venisse inventato per lo scambio di valore, qualcuno in posizione privilegiata era

sempre pronto a sfruttarne le debolezze.

Riassumendo.

Sul pianeta *e* si era passati da un regime metallista (con i *Mins* fisici) a uno cartalista (con *Mins* virtuali esistenti solo come informazione) ma non si era riusciti a risolvere il nodo cruciale della faccenda.

Troppo potere in poche mani. Troppi incentivi per abusarne. E se il groppo da risolvere non fosse il tipo di "supporto" (fisico o virtuale) su cui scorreva la valuta o la sua convertibilità, ma la sua **gestione centralizzata**?

Noi conosciamo bene i problemi che

questa centralità può dare (l'abbiamo sperimentato nel 2008) ma i ragazzi del pianeta *e* dovevano scoprirlo da soli. *Learning by doing*, sentenzierebbero i coach di moda.

Esasperato, il saggio *Yivra* si ritirò per due mesi nell'eremo di *Respr*. Durante questo periodo di raccoglimento rifletté a fondo sull'universo, il flusso della vita e la natura umana così ferina.

Al culmine dell'espansione spirituale ebbe infine l'intuizione che **risolse** definitivamente l'economia degli sfortunati cittadini di *e*.

# La soluzione suprema di Yivra

Corse come un pazzo nella sala consiliare e radunò in fretta e furia tutti gli altri colleghi. Afferrò il maledetto registro pubblico e gli diede fuoco con un gesto di plateale rabbia, di fronte agli sguardi sgomenti degli astanti. Tutti pensarono che il buon *Yivra* fosse totalmente uscito di testa per via del lungo isolamento.

Tutt'altro.

*Yivra* espose la sua nuova e ultima proposta con un tale vigore e carisma iniziatico che trascinò gli altri consiglieri. Lo acclamarono come

salvatore della comunità e misero subito in pratica la sua mozione.

Siete curiosi di conoscerla?

In verità è piuttosto semplice. Com'è spesso semplice ciò che funziona perfettamente e sa resistere al tempo che passa e ai cambiamenti delle società.

Nella nuova proposta rimaneva l'idea del registro pubblico, ma veniva eliminata la sua parte debole e perigliosa, cioè la sua *centralità*. Come? Per quanto possa sembrare folle a prima vista, *Yivra* stabilì che dovevano essere 7 i consiglieri incaricati di vegliare sulla trascrizione delle transazioni. E ognuno di loro

dovesse avere il **proprio** registro su cui trascrivere in modo indipendente dagli altri ogni transazione.

Da quel momento, quando due cittadini volessero dichiarare uno scambio di *Mins*, avrebbero dovuto recarsi nell'aula consiliare e declamare a gran voce i termini della compravendita. I 7 consiglieri sempre presenti erano a quel punto obbligati a trascrivere in tempo reale gli atti sul proprio registro. In modo svincolato dagli altri. Ognuno per proprio conto.

L'informazione era così **decentrata** e **replicata** all'istante.

Per chiudere il cerchio, ogni 12 ore gli

altri 3 consiglieri confrontavano le transazioni della mezza giornata appena trascorsa registrate sui 7 registri. Se emergevano disallineamenti tra loro, si sceglieva come versione ufficiale quella presente nella **maggioranza** dei registri. E si correggevano le righe di quelli sbagliati trascrivendo le informazioni corrette.

Nel tempo e con la crescita della popolazione il numero dei consiglieri dedicati al compito aumentò e si passò da 12 ore a solo 3, così da poter avere una situazione sempre piuttosto aggiornata sulle transazioni nelle comunità e poter contare su una maggiore certezza. Inoltre venne estesa

l’attività anche alle ore notturne, per migliorare il servizio.

Incredibilmente, la pazza idea di *Yivra* salvò l’economia del pianeta e l’intera comunità iniziò a prosperare al punto da non aver più bisogno di essere salvata dai fratelli fortunati del pianeta *d*. In pochi decenni, infatti, gli ex ragazzini ormai adulti, grazie alla prosperità garantita dalla solidità del sistema dei registri decentrati poterono dedicare a tempo pieno una ventina di persone alla ricerca di nuovi materiali per costruire strumenti elettronici resistenti ai campi elettromagnetici deleteri.

Ironia della sorte: il materiale

miracoloso per i circuiti si rivelò essere un cristallo di nostra conoscenza stipato da parecchio in una miniera vicina al villaggio e non più toccato da mano umana da tempo.

I cristalli di *Mins*.

Grazie ai *Mins* nella nuova veste di componenti per circuiti, iniziarono a essere costruiti strumenti elettronici e digitali di ogni tipo, reti di comunicazione e processori sempre più potenti. Al punto da poter trasferire l'intera procedura dei registri pubblici decentrati **online**. Gli scambi a questo punto aumentarono esponenzialmente grazie alla disponibilità continua e

ubiqua dei registri di transazioni e gli abitanti del pianeta *e* iniziarono a colonizzare ogni terra emersa possibile.

Cento anni dopo avvenne l'incredibile: gli abitanti del pianeta *e* crearono astronavi in grado di raggiungere i fratelli sull'altro pianeta e portarono loro la propria tecnologia e la propria struttura finanziaria.

Creando così i semi della futura e gloriosa *Federazione Yivra di Trappist-1*.

The end.

# Vi presento miss blockchain

Va bene, scopro le carte. L'ultima proposta di *Yivra* è in verità qualcosa che ci dovrebbe apparire familiare, anche se non ne sappiamo molto. Ha un nome parecchio interessante e da qualche anno piuttosto in voga. Magari ne avete sentito parlare.

Si chiama **blockchain**.

Ne parlano tutti, vero? In ogni discussione in cui si accenni al tema delle criptomonete e dei BitCoin prima o poi qualche espertone se ne esce con una frase del tipo:

*Eh, ma è così che funziona la*

*blockchain!*

Per la maggior parte della gente che la cita, questa benedetta blockchain resta un oggetto arcano e misterioso, un po' oscuro. Ma voi siete fortunati: grazie alla nostra storiella avete finalmente scoperto che non è nulla di metafisico. Avete capito che è un sistema come un altro per far funzionare una rete di scambi di denaro senza che qualche furbastro ne approfitti.

Il funzionamento profondo della blockchain è infatti lo stesso della nostra bella favola fantascientifica: per essere approvata, ogni transazione di valuta deve essere comunicata a un insieme di attori – ognuno con un proprio registro –

ben felici di valutarne la legittimità. Se non c'è accordo tra di loro, vince la maggioranza. Se in 6 registri di transazioni su 10 emerge che voi possedete 10 *Mins* e negli altri 4 registri no, vincono i 6. Si decide che voi possedete questo denaro e non se ne discute più, caso chiuso.

Tra poco vedremo i dettagli.

La blockchain è **l'anima** del BitCoin. È il processo stesso che rende possibile il 99% delle criptovalute. Senza blockchain non esiste BitCoin, senza registri decentrati non esistono monete elettroniche.

Possiamo addirittura arrivare ad

affermare che, a dirla tutta, non esiste alcuna "moneta fatta di bit". *Il valore dell'intero circuito dei BitCoin esiste* ***solo*** *nell'istante in cui la blockchain elabora un gruppo di transazioni*.

Come una sorta di fenomeno quantistico, la quantità di cripto-soldi che possiedo si manifesta esclusivamente quando i nodi della blockchain osservano e contabilizzano i loro registri. Fuori da questi momenti di analisi, io sono tecnicamente squattrinato.

Fatemelo ripetere in modo ancora più pratico.

Benché usiate dei taccuini elettronici (i *wallet*) per conservare le criptomonete,

vi deve essere chiaro che questi taccuini non contengono in verità **nulla**. Ma proprio niente di niente. Non sono delle cartelle di file digitali che descrivono i singoli BitCoin di vostra proprietà. Non è che se perdete l'accesso al *wallet*, perdete le monete di bit al suo interno. Non funziona così. Tutto ciò che possedete è descritto solo come un elenco di "dare/avere" nei registri decentralizzati alla base della blockchain.

Da questo e dalla storiella del pianeta *e* dovete desumere alcune idee fondamentali sul mondo cripto:

- Per sapere quanti BitCoin io

possieda qualcuno deve calcolare le transazioni da me effettuate dal momento del mio primo acquisto di criptomonete. I portafogli elettronici lo fanno per noi. La blockchain lo fa continuamente per stabilire in modo oggettivo se una cifra che stiamo cercando di spendere sia effettivamente in nostro possesso.

- Quindi **l'intera** blockchain – cioè tutta la rete mondiale che partecipa al circuito BitCoin – sa perfettamente quali siano i miei cripto-averi. Sono pubblici. Tutti possono analizzare le mie transazioni. Strano a dirsi e pure un

po’ inquietante in stile *Black Mirror*, ma è così.

- Tuttavia. Esattamente come nella nostra comunità spaziale immaginaria, le transazioni non sono associate al mio nome e cognome, ma a indirizzi **anonimi** espressi come una sequenza di caratteri, un po’ come dei codici fiscali. In questo modo, benché tutto sia pubblico, nessuno può davvero sapere che una certa transazione sia mia. A meno che io non urli ai quattro venti “*hey mondo, l’indirizzo 435435435 sono io!*”. Non è un’idea geniale, ve lo assicuro.

- Nessuno ci vieta di avere un numero alto di questi indirizzi e quindi di rendere ancora più difficile per il pubblico associare determinate spese o entrate alla nostra persona. I taccuini virtuali permettono di gestire *illimitati* codici anonimi.

- Quindi lo scopo dei portafogli elettronici per criptomonete – e degli *exchange*, cioè i siti in cui convertire valute normali da/verso BitCoin – **non è** di conservare fantomatici file contenenti monete elettroniche. Ma piuttosto di darci la possibilità di operare transazioni sulla rete BitCoin al

contempo conservando e trasmettendo gli indirizzi anonimi a noi associati.

- Questi indirizzi anonimi hanno un soprannome tecnico usato dai crittografi da ben prima delle criptomonete: "*chiavi pubbliche*". Si chiamano "pubbliche" perché tutti le possono vedere. Come abbiamo detto, le transazioni nella blockchain sono visibili a chiunque.

- Ma se bastasse conoscere una delle nostre chiavi pubbliche per poter accedere alle nostre sostanze e spendere i nostri soldi sarebbe un

bel problema. Quindi che si fa? BitCoin usa un altro trucchetto ereditato dai maghi della crittografia: le "*chiavi private*". Sono come delle password che conoscete solo voi – e il vostro *wallet*. Se vuoi inviare denaro a qualcuno, devi fornire alla blockchain sia la tua chiave pubblica sia quella privata. La seconda serve alla rete per essere certa che quell'indirizzo pubblico sia di chi sta facendo la transazione. Cioè *che tu sia tu*.

- Al netto di tutto questo: qual è la cosa peggiore possa succedervi nel ruolo di proprietari di BitCoin?

*Perdere* i vostri indirizzi e/o le chiavi private. Non esiste modo per ritrovarle. La rete BitCoin non ha alcuna possibilità di farlo per voi. I primi sono pubblici (ma auguri a riconoscerli tra i tanti) e le seconde sono private. Una volta dimenticate, sono dimenticate.

Andiamo sulla pratica. Date un'occhiata a una tipica transazione nel registro della blockchain:

Il primo indirizzo lunghissimo sotto alla parola "*Transazione*" è il codice univoco di questo particolare trasferimento di BitCoin. Subito sotto avete l'indirizzo di chi sta ricevendo i soldi e a destra un paio di indirizzi del mittente.

> *Uno dei due indirizzi in verità è un codice di change, che è un po' come quando date 5 Euro per comprare un pacchetto di chewing gum da 1 Euro e il cassiere vi restituisce 4 Euro come resto.*
>
> *Quando spendete dei BitCoin dovete usare* ***l'intera*** *cifra ottenuta da una transazione precedente con cui siete stati*

*pagati. In questo caso il mittente ha pagato 10.89 BitCoin e ne ha ricevuti 0.89 come resto. Significa che in passato il mittente ha ricevuto un pagamento da 10.89 BitCoin e ora lo sta usando.*

*I portafogli elettronici di solito mascherano questa complessità!*

# Il cifrario dell'imperatore

Vi ho ingolositi e siamo tutti pronti a tuffarci nell'universo delle cripto-meraviglie. Ma vi chiedo di pazientare cinque minuti. Permettetemi di darvi un contesto storico sui BitCoin, altrimenti avrete una comprensione raffazzonata della cosa.

Vi assicuro che è molto interessante.

Avete visto il magnifico film *The Imitation Game*? Se non l'avete fatto, rimediate subito. Questa superba pellicola narra la storia di *Alan Turing*, scienziato inglese e genio della matematica.

Per molti versi, *Turing* è stato un individuo eccentrico (tra l'altro, chiaramente nello spettro autistico) ed eccezionale. A lui si deve la concezione del calcolatore moderno, cioè tutto ciò che va dal computer agli *smartphone*. Come non fosse abbastanza, per merito suo siamo riusciti a decifrare i codici della macchina *Enigma*, arma infallibile dei nazisti in grado di mascherare tramite **criptaggio** qualsiasi comunicazione da Berlino agli eserciti, compresi gli ordini con gli obiettivi civili e militari alleati da abbattere.

Abbiamo appena scoperto una parola fondamentale: *criptaggio*.

Verbo: *criptare*.

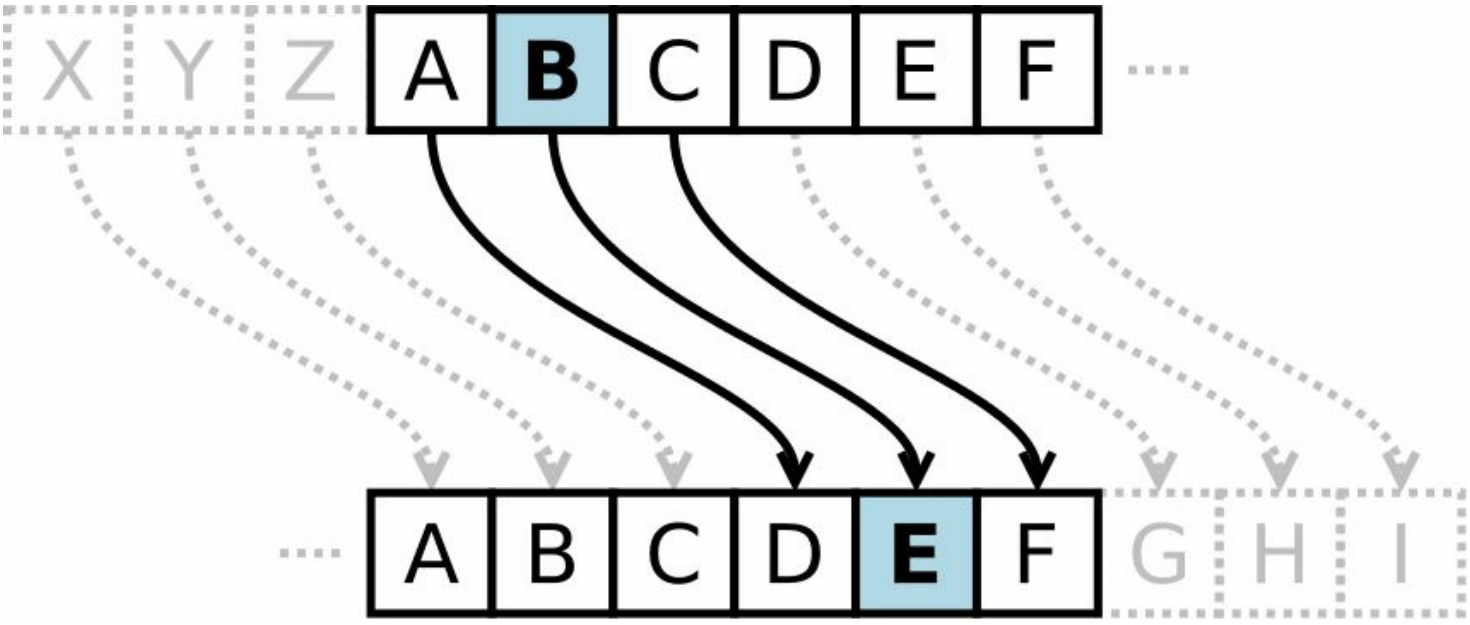
**Criptare** una frase – o un'immagine, un suono o un file – significa renderla **illeggibile** affinché qualsiasi persona che per caso dovesse intercettarla non riuscirebbe a carpirne il significato.

Il più famoso e semplice sistema di criptaggio è il *Cifrario di Cesare* (sì, *quel* Cesare, il tizio pugnalato). Funzionava in modo piuttosto elementare: ogni lettera di una missiva inviata dall'imperatore agli eserciti veniva sostituita da un'altra lettera che nell'alfabeto romano fosse alla distanza di *X* lettere. Dove *X* è un numero deciso di volta in volta.

Usando l'alfabeto italiano possiamo applicare l'algoritmo del *Cifrario di Cesare* per divertirci. Ad esempio, decidiamo insieme che la distanza di lettere deve essere 2. Avendo questa informazione, come criptare la parola: "*ciao*"?

- "C" + 2 = "E"
- "I" + 2 = "M"
- "A" + 2 = "C"
- "O" + 2 = "Q"

Quindi: "*ciao*" diventa "*emcq*".




*Momento quiz: indovinate da dove deriva l'espressione "cripto" nel termine "criptomoneta"?*

Torniamo al nostro amico matematico anti-nazi.

Si stima che senza il genio di *Turing* la seconda guerra mondiale sarebbe durata 2 anni in più. Con i milioni di morti che questo avrebbe comportato. Facendo della fantastoria, è sensato ammettere

che alcuni tra i lettori di questo libro non sarebbero nati se non fosse esistito *Alan Turing*. Impressionante.

*Turing*, grazie alla sua fama di matematico e esperto di codici, nel pieno del secondo conflitto mondiale venne convocato dai servizi segreti britannici presso Bletchley Park, località meglio nota come *Stazione X*. Qui diede sfogo al suo talento combinando il suo progetto del primo computer con alcune intuizioni sulla decriptazione crittografica. Il mix esplosivo permise agli alleati di **de-criptare** le comunicazioni codificate tramite *Enigma* che i tedeschi ignari continuavano a trasmettere tramite

l’etere alle loro truppe.

Posso rassicurarvi su una cosa: il *Codice Enigma* non era per niente facile da svelare come il *Cifrario di Cesare*. Il genio del nostro adorato *Alan* da solo non avrebbe potuto nulla se non fosse stato supportato dalla potenza computazionale di un computer. Il primo computer, tra l’altro. Che oggi farebbe ridere i polli quanto a potenza, ma che all’epoca poteva sostituire stuoli di segretarie e contabili.

Da quel momento, computer e codici crittografici sono andati a braccetto, scatenando una corsa alle armi. I criminali e i militari ossessionati

dall’inventare il codice sempre più indecifrabile, i servizi segreti e gli agenti nel cercare di sgominarlo.

# Gli adorabili nipoti di Turing

Negli anni ’80 un gruppo di nerd ossessionati proprio dai codici diede vita al movimento **cypherpunk**.

Non è un errore di battitura, ho scritto “*cypher*punk”, non “*cyber*punk”. Il prefisso “cypher” è evidentemente collegato al termine **crittografia** – *cryptography*, in inglese. Lo scopo di questi secchioni informatici anarchici era quello di sfruttare le più potenti tecnologie di crittografia per cambiare il mondo in meglio. Dando alle persone il diritto naturale a sicurezza e privacy totali.

Dal manifesto del movimento scritto da *Eric Hughes* negli anni ’90:

> *"Privacy is the power to selectively reveal oneself to the world".*
>
> *“La privacy è il potere di scegliere a nostro piacimento le persone nel mondo a cui rivelare i nostri segreti”.*

Notate l’uso del termine “potere di”. Vi fa capire che lo scopo fondamentale di questi tizi era dare alla gente “*potere*” e “*scelta*”. Un po’ come cantava *Patty Smith*.

Dare potere alla gente significa, tra le altre cose, dotarla di una **moneta** che

non dipenda da governi, banche e altre istituzioni centralizzate. Le persone devono essere libere di scambiarsi denaro senza dipendere da governi, senza lasciare tracce e senza pagare commissioni. Le verifiche delle transazioni devono essere distribuite nella rete e non dipendere da qualche ente particolare. Questo almeno era il DNA del cypher-pensiero.

Sin dal primo vagito del movimento, i chyperpunker volevano quindi realizzare una **criptomoneta**.

E ci hanno provato per anni. Ma in ogni esperimento mancava sempre qualcosa o si è trattato per troppe volte solo di

nobili intenti senza effetti pratici.

Ad esempio.

Nel 1998 il programmatore *Wei Dai* condivise l'idea di *B-Money*, una criptomoneta pensata per far rispettare gli accordi contrattuali tra due persone senza coinvolgere notai o legali. Due dei suoi concetti dovrebbero risultarvi famigliari:

1. B-Money era un protocollo in cui ogni partecipante alla rete doveva mantenere un registro separato delle transazioni contrattuali.

2. Una parte dei partecipanti doveva validare tutte le transazioni mentre

la stessa struttura della rete assicurava l'onestà del meccanismo.

*Yes, è proprio il sistema costruito dagli amici del pianeta e!*

Procediamo a grandi passi verso il 2005 con la proposta di *BitGold*, criptomoneta ipotizzata da tal *Nick Szabo*, nome ultra-conosciuto nella comunità cypherpunk e che più di qualcuno considera il vero creatore di BitCoin. Vi basti sapere che molti dei concetti alla base di BitCoin sono stati presi papali-papali da BitGold.

La storia prosegue e arriviamo alla crisi del 2008 con la seguente deflagrante

**sfiducia** del popolo verso il sistema delle banche centrali. Sfiducia… sfiducia… sfiducia. Mi ricorda qualcosa. Ah sì, è l'opposto di ciò che è il denaro: *fiducia*!

Momento propizio e maturo per i cypherpunker. Il mondo è prontissimo ad accogliere una valuta che non dipenda da istituti centrali e non sia corruttibile. Momento sfruttato alla grande da un certo signore (o signori?) con uno pseudonimo che suona molto giapponese:

**Satoshi Nakamoto**

Il signor *Nakamoto* apparve all'improvviso e sottotono nel 2008 nei

forum dei cypherpunker proponendo la sua idea per una nuova criptomoneta chiamata – provate a indovinare – **BitCoin**!

Nessuno conosceva questo personaggio ma più di qualcuno rispose al suo appello persuaso da un documento tecnico incredibilmente convincente scritto da *Nakamoto* stesso. Questo tizio sconosciuto pareva sapere il fatto suo, e la somiglianza di molti suoi spunti con le idee di BitGold fece il resto nel convincere la comunità ad aderire entusiasta alle sue idee.

Seguirono mesi di sperimentazione e raffinamento del codice di BitCoin e

della sua blockchain. Iniziarono pian piano ad aggiungersi nodi alla rete di sperimentazione fino ad arrivare alla prima calca di entusiasti nel giro di pochi mesi. Qualcuno divenne profeta dei BitCoin, regalandone a migliaia in giro in cambio di pizze.

La rivoluzione era iniziata.

C'è un paragrafo del documento originale di *Nakamoto* che a questo punto dovrebbe collegare nella vostra mente tutti i concetti appresi fin qui:

> *"The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the*

*trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the 'tape', is made public, but without telling who the parties were".*

*"Il modello bancario tradizionale raggiunge un alto livello di privacy semplicemente limitando l'accesso alle informazioni a chi opera le transazioni e alla terza parte fidata che le valida. [Nella Blockchain] la necessità di rendere pubbliche le transazioni a tutti gli attori che vogliono validarle preclude questo sistema di segretezza, ma la privacy può essere comunque ottenuta mantenendo anonime le chiavi pubbliche [cioè gli indirizzi di mittenti e riceventi]. Il pubblico può vedere che qualcuno sta inviando un importo a qualcun*

*altro, ma non può vedere le informazioni che collegano la transazione a una persona specifica. Questo è simile al livello di informazioni diffuse dalle borse delle azioni, dove il tempo e le dimensioni dei singoli scambi sono resi pubblici, ma senza diffondere i nomi degli attori".*

Boom.

# Chi incentiva l'incentivatore

Tutto bellissimo e fantastico. Ma se siete lettori attenti non può esservi sfuggito un dettaglio non banale su cui ho maliziosamente sorvolato.

Sul pianeta *e* nella soluzione di *Yivra* i registri delle transazioni erano in mano a 10 consiglieri (7 trascrittori e 3 che verificavano) che per mestiere dovevano servire il popolo. Non avevano bisogno di essere convinti. Erano pagati per verificare la liceità dei pagamenti. Ma nella blockchain? Come dannazione pensava *Nakamoto* di persuadere qualcuno a impegnarsi in un

tale lavoraccio a favore di tutti gli altri?

Con un metodo semplice:
**incoraggiandolo** con un premio.

Nel mio libro *Digital Deep Marketing* tratto a fondo l'argomento degli incentivi, strumenti necessari per confezionare una strategia di marketing fondata sulla psicologia umana profonda. Qui ci basti capire che le persone rispondono naturalmente a *stimoli*.

Se vuoi convincermi a far qualcosa dammi una carota. Il concetto chiave non è più difficile di così.

*Satoshi Nakamoto* risolse il dilemma in

modo autarchico e piuttosto lineare. Ecco la sua regola:

> *Verifichi le transazioni? Ti becchi nuovi BitCoin freschi freschi.*

Riassumendo: se sul pianeta *e* i consiglieri tenevano i registri e la contabilità ordinata in cambio di uno stipendio e di pubblica visibilità, nella blockchain perfetti sconosciuti lo fanno in cambio di denaro. Nella forma di nuovi BitCoin.

Ora. Da mesi leggo sui social e sui siti aggettivi come “rivoluzionario” associati a questo concetto. Col massimo rispetto per l’intelletto di *Nakamoto*, solo un ingenuo può non

notare in questo criterio l'applicazione più elementare di due assiomi che tutti conosciamo:

- **Incentivi e capitalismo**: per convincerti a far qualcosa ti pago. È il metodo più rapido.
- **Spirito cartalista**: i soldi si possono creare *dal nulla* e non devono essere legati ad alcun bene reale come l'oro. Nel cartalismo puro è il re o la banca centrale che fa sgorgare il denaro dall'aria; nei BitCoin è la blockchain. Il concetto è identico. Ok?

Tutti possono entrare nella blockchain e quindi diventare nodi *validatori* di

transazioni, un po' come i consiglieri del nostro pianeta preferito. Basta scaricare e lanciare sul proprio computer il software scritto da *Nakamoto* e cripto-amici. È open source, quindi gratis.

In questo modo diventate **trascrittori** di **transazioni** e validatori di transazioni. Allo stesso tempo. In cambio del lavoro fatto dal vostro computer e dell'energia elettrica che usate, l'intera blockchain vi ricompensa con nuovi BitCoin.

In definitiva ci sono due ruoli nel mondo dei BitCoin:

1) I **semplici utenti** che si scambiano soldi sotto forma di BitCoin. Per

diventare uno di loro vi basta usare un portafoglio elettronico e caricarvi denaro.

2) Quelli che **validano le transazioni** partecipando alla blockchain. Per farlo occorre scaricare un software e lanciarlo.

Quindi è facile guadagnare nuovi BitCoin! Basta far parte dei tizi che partecipano al secondo ruolo.

No amici, è tutto fuorché facile.

# Numeri, numeri e ancora numeri

*Avviso ai miei adorati lettori: potete leggere questo capitoletto senza obbligarvi a capire tutto. O potete prenderlo come sfida personale.*

*Mi sono dato da fare per evitare il più possibile tecnicismi e complicazioni inutili ma, per quanto io possa impegnarmi, la questione non può essere semplificata oltre una certa soglia. Le criptomonete sono roba complicata.*

*Torniamo a noi.*

Dicevamo. Fosse semplice validare BitCoin saremmo tutti ricchissimi e io

non avrei perso tempo a scrivere un libro.

Tanto per cominciare non è che più gente entra nella blockchain più BitCoin si creano. No no. Il numero di BitCoin è deciso a monte e il sistema ne crea un *tot* ogni 10 minuti. Indipendentemente dal numero di nodi della blockchain. Indipendentemente da quanti registri esistono. La torta è una, più gente c'è e più le fette sono piccole.

**Quanti** BitCoin vengono creati quindi?

Prima di rispondervi tornate a leggere il paragrafo precedente. Ho parlato di un timer che scatta ogni 10 minuti. *Nakamoto* ha infatti deciso che i BitCoin

vengano creati ogni 10 minuti perché proprio ogni 10 minuti viene convalidato un **gruppo** di transazioni. Le due attività sono simultanee.

Sul pianeta *e* la validazione dei pagamenti sui registri e la loro sincronizzazione avveniva ogni 12 ore. Ricordate? Nella rete BitCoin avviene ogni 10 minuti. È lo stesso concetto. Con la sola differenza che nella rete BitCoin questo tempo segna *anche* la creazione di nuove monete.

La blockchain, cioè la rete dei validatori, ogni 10 minuti elabora un *pacchetto* di transazioni richieste da chi vuole scambiarsi BitCoin. Non viene

processato un solo pagamento alla volta perché *Nakamoto* ha ritenuto fosse più efficiente raggrupparli a gruppetti di più transazioni. Ognuno di questi pacchetti si chiama **blocco**. Da cui il nome *blockchain*, cioè "catena di blocchi".

Carino, no?

Ok, ora posso raccontarvi quanti BitCoin vengono creati a cadenza di 10 minuti per ricompensare chi fa il lavoro sporco di validazione delle transazioni.

- A chi ha verificato i primi 210mila blocchi della storia dei BitCoin il sistema ha regalato 50 BitCoin per blocco.

- Ai successivi 210mila, 25 BitCoin per blocco.
- Agli ulteriori 210mila, 12,5 BitCoin per blocco.
- E via così a dimezzare la cifra sinché non si creerà più alcun nuovo BitCoin.

Vi risparmio il calcolo complicato: questo fatto increscioso avverrà nel 2140, l'ultimo blocco sarà il numero 6.929.999 e all'epoca saranno stati creati **21 milioni** di BitCoin.

Vi risparmio un altro calcolo.

Se sappiamo che il dimezzamento del rilascio di BitCoin avviene ogni

210mila blocchi e ogni blocco è processato ogni 10 minuti, tramite la magia dell'algebra elementare possiamo essere piuttosto certi che **ogni 4 anni** il numero di BitCoin si dimezza.

Blocchi emessi ogni 10 minuti = 210.000
10 minuti in un'ora = 6
Ore in un giorno = 24
Giorni in un anno = 365

210.000 / 6 / 24 / 365 = 3.99

Perché proprio queste cifre? Perché l'ha voluto *Nakamoto*. E gli altri muti.

Dovrebbe esservi piuttosto chiaro il motivo per cui il numero di BitCoin totali sarà "tappato" a 21 milioni. Perché *Satoshi* ha deciso di porre un limite massimo alla quantità di

criptomonete che saranno prodotte nella storia?

Ripensate al pianeta *e* nella precedente sezione del libro. Cosa era successo prima della pausa narrativa?

**Inflazione**. Satoshi, ponendo un limite massimo ai BitCoin, vuole evitare a monte l'inflazione.

Nel mondo dei BitCoin nessuno potrà mai di sana pianta decidere di *stampare moneta* per diminuire il debito di uno stato o per qualche strana manovra finanziaria. I BitCoin saranno sempre rilasciati a un ritmo prevedibile e la loro quantità totale futura è prevedibile. Questo da un lato stabilizza il sistema a

monte, dall'altro crea una potenziale dinamica **deflattiva**.

Fermi, non scappate dal disgusto per questo termine! La nozione è più semplice di quanto appaia: mentre le monete *fiat* come Euro e Dollaro tendono per loro natura a esigere un po' di inflazione (in un'economia sana si ritiene dovrebbe essere stabilmente intorno al 2%), BitCoin fa l'opposto. All'atto pratico significa che i nostri risparmi in Dollari o Euro sul lungo termine spontaneamente *diminuiranno* di valore, mentre quelli in BitCoin dovrebbero *aumentare*.

Questo in **teoria**. Ma non fatevi

illusioni: la macro economia fa quel che le pare e noi possiamo controllarla meno di quanto ci illudiamo. Ad esempio, sembra proprio che l'Euro non voglia subire inflazione, nonostante tutti i tentativi della BCE. Si sente una moneta forte e non ci pensa proprio a perdere punti. Che pazzo.

# Mostrami la tua fatica

Torniamo a blockchain. L'avete capito: farne parte è piuttosto facile. Vi scaricate un software gratuito e lo accendete.

Senonché *Nakamoto* è stato un pusillanime non solo nel limitare la quantità di BitCoin che saranno prodotti. Ha ben deciso di rendervi la vita difficile anche su un altro fronte.

Vi presento l'ultima parola complicata di oggi, poi la pianto e vi lascio respirare. Date il benvenuto al signor **proof-of-work** (letteralmente: "*prova del lavoro compiuto*"). Chi è? Cosa fa? A cosa serve? Che diamine c'entra?

30 secondi di respirazione yoga.

Inspirate. Espirate.

Inspirate. Espirate.

Fatto? Continuiamo?

Si parlava di proof-of-work.

Tutto parte da una domanda: *con che criterio scegliere, tra chi verifica le transazioni, gli attori a cui donare i nuovi BitCoin prodotti*?

Ci sono vari sistemi possibili:

1) Dividere i soldi equamente tra tutti i partecipanti alla blockchain? No grazie, se abbiamo milioni di concorrenti significa dare due

spicci a testa. Non è un'idea scalabile al crescere della comunità. Non ne vale la pena.

2) Darli a un solo partecipante in modo casuale o basandosi su qualche altra sua caratteristica? Idea niente male, ma che collima poco con la necessità critica di essere certi che solo le persone *più interessate* partecipino al controllo. Perché solo queste di sicuro daranno attenzione al processo.

Esiste poi una seconda considerazione critica e di non fulminea comprensione per noi comuni mortali.

Ripensiamo al pianeta *e*. Immaginiamo per un secondo che i consiglieri validatori non fossero decisi una volta per tutte ma che chiunque potesse candidarsi al ruolo. Come stabilire chi far entrare e chi no nel momento in cui si fosse inondati di proposte? In modo casuale? Per concorso?

Ma soprattutto: come potevano i nostri essere certi di non portare "nella camera dei registri" un gruppetto di malintenzionati in grado nel tempo di creare una maggioranza di validatori **corrotti** interessati solo a modificare i bilanci monetari a favore loro o dei propri amici?

Vi ricordo che, in caso di incongruenze tra i registri delle transazioni, la regola imponeva di allineare tutti i registri con la versione presente nella *maggioranza* di essi. Se la maggioranza è composta da malintenzionati e contiene quindi informazioni criminali, queste diventano legge.

> *Come la storia ci insegna, anche gli stati moderni non sono poi così bravi a tener fuori dalle stanze del potere i delinquenti, i corrotti, i mafiosi, le persone con un'etica traballante. Anzi. È problematico per definizione impedire le infiltrazioni degli individui peggiori nei sistemi democratici.*

*Lo è nella politica e lo è nei processi come la blockchain.*

L'unico modo per tentare di non far partecipare al gioco chi ha obiettivi fraudolenti è di accompagnare i benefici derivanti dal potere a disincentivi, così da filtrare solo i canditati più interessati e con più interesse a **far funzionare** il sistema.

In concreto:

- Da un lato cerco di persuadere più gente possibile a partecipare alla blockchain promettendo *benefici* da leccarsi i baffi (BitCoin gratis!).
- Dall'altro lato dissuado a partecipare chi vuol farsi solo una

"sveltina" o truffare tutti gli altri. Come? Stabilendo che i BitCoin sono distribuiti solo a chi lavora come un mulo e si impegna più degli altri.

Pensateci. Accettereste mai un lavoro gravoso e con lo stipendio non assicurato? Solo se è la professione dei vostri sogni o solo se ci tenete alla causa. Un criminale getterebbe la spugna dopo poco, specie se la sua probabilità di sporcare i conti dell'azienda si riducesse all'aumentare del numero di dipendenti per via della regola della maggioranza.

Con questa soluzione si ha la buona

certezza di allontanare chi non crede poi tantissimo nella causa e chi spera nei soldi facili "*fregando il sistema*". Perché il sistema ti accoglie e può darti molto, ma prima di tutto ti chiede una grandissima dose di lavoro e non ti assicura un bel nulla. E se vuoi corromperlo devi investire una quantità infinita di fatica perché ti occorre ottenere sempre la maggioranza per operare qualsiasi azione.

Questo bilanciamento è *la* soluzione scelta da *Nakamoto* per convincere a entrare nella blockchain di validazione dei pagamenti in BitCoin solo i più motivati e, in larga parte, onesti.

Se il regalo di BitCoin è l'incentivo positivo, la proof-of-work descrive la parte disincentivante dell'equazione.

La proof-of-work è simile alla cifra finale che si ottiene svolgendo per bene un complicatissimo compito di algebra. Ricordate le equazioni di matematica alle scuole superiori? Lo scopo era risolverle per arrivare a una sola cifra. Un solo numero. Se ci pensate, all'insegnante non serve davvero leggere tutti i passaggi fatti dall'alunno per arrivare alla soluzione. Basta che questa sia **esatta**.

La blockchain è come un'insegnante di matematica disinteressata ai passaggi

utilizzati dagli alunni per risolvere una complicatissima equazione. Le interessa solo sapere qual è stato tra tutti il **primo** della classe che ha trovato la soluzione giusta. Lui vince i BitCoin, tutti gli altri restano a bocca asciutta.

Capite bene non vi sia alcun incentivo a copiare se vince solo il primo. No? Ogni nodo della blockchain lotta per proprio conto e si guarda bene dall'aiutare gli altri. È una guerra senza esclusione di colpi!

Tornando a noi. Ogni 10 minuti arriva a tutti gli attori che partecipano alla blockchain un nuovo blocco di transazioni da elaborare. In quello

stesso istante scatta una gara di lacrime e sangue in cui ogni nodo deve verificare tutti i pagamenti del blocco e *nello stesso tempo* risolvere un compito matematico difficilissimo. Il primo nodo che trova la soluzione vince tutto.

Volete sapere l'aspetto più delizioso di tutto ciò? Il compito matematico difficilissimo è strutturato in modo tale da assicurare alla rete che chi è in grado di risolverlo ha *di sicuro* validato tutte le transazioni in modo attento e corretto. Due piccioni con una fava.

Avete appena capito uno degli aspetti più complicati del funzionamento delle criptomonete! I miei più vivi

complimenti, ragazzi. Potete tirarvela con tutti i vostri amici.

Nel prossimo capitolo vedremo altri dettagli intriganti della faccenda.

# Minatori o contabili?

Quando qualcuno discute di criptomonete sentite sempre parlare di **mining**. Benissimo, il mining è l'attività che *crea* la proof-of-work.

Se la proof-of-work è il numero che ottenete risolvendo il compito in classe, fare mining (o "minare") significa semplicemente *svolgere* il compito in classe. Che nella blockchain è il mix di verifica dei pagamenti e risoluzione di un puzzle algebrico di inaudita difficoltà.

La traduzione letterale di mining è "*estrazione*". Ma è un termine **sbagliato** perché stimola troppo la fantasia in

modo fuorviante. La parola è stata scelta da *Nakamoto* perché ai nerd piacciono un sacco le immagini forti (il minatore che estrae l'oro!) ma è una cavolata. Chi di noi direbbe "*sto estraendo la soluzione di questo bilancio?"*. Frase divertente, ma ci prenderebbero per pazzi.

Dovete piuttosto pensare al mining come all'attività di risoluzione di un problema di **contabilità**. Ok?

*Mining* = risolvere un problema di contabilità.

La rete dei "minatori" delle criptomonete infatti ha uno scopo molto diverso dall'estrarre qualcosa: deve

piuttosto far quadrare i conti sui registri della blockchain. E, mentre lo fa, è obbligata a risolvere un puzzle matematico affinché chi non vuole impegnarsi troppo nella cosa o chi vuol fare il furbetto truccando i conti sia scoraggiato.

Andando al sodo, questa è l'essenza del mining dei BitCoin:

> Guadagnarsi con molta *fatica* la *possibilità* di fare contabilità gratuita per tutti al fine di avere la speranza di essere pagati.

Un po' come essere **stagisti**. Fare tantissimo sforzo per incrementare di poco la remota possibilità di ottenere un

lavoro. Figuriamoci di essere pagati.

Raccontata così è meno romantica e epica la cosa, nevvero? Però è la cruda verità. Le storielle lasciatele agli altri.

Ora piccolo momentino tecnico. Sarò breve-breve.

Tutto il cripto-teatrino nasce per ciò che ormai sappiamo bene: risolvere il problema della validazione delle transazioni senza poter contare su un'autorità centrale che, come un genitore autorevole, consenta o neghi il trasferimento di denaro tra due attori. L'idea di base è che la magia della crittatura e la fatica del mining facciano le veci di questo genitore, rendendo

impossibile manipolare i registri codificati e criptati.

Bene, questo ormai per voi dovrebbe essere più che chiaro. Ma concretamente, com'è fatto il registro decentralizzato nella blockchain? Ve lo siete mai chiesti?

Per quanto sia bizzarro, il registro esiste simultaneamente in **due versioni**:

- Come un grandissimo foglio Excel di bilancio dal peso di più di 100 gigabyte. Un archivio pesantissimo trascritto in ogni nodo della rete e aggiornato ogni 10 minuti dopo la verifica di ogni blocco di transazioni.

- Come un brevissimo codice di 64 caratteri. Anch'esso presente in ogni nodo della blockchain e costantemente aggiornato.

Come diamine è possibile tutto ciò? Perché accade? Come si spiega?

Un passo alla volta.

La prima versione del registro, quella del file **gigante**, penso sia di facile comprensione per tutti. Al suo interno ci sono *tutte tutte tutte* le transazioni di BitCoin dal suo primo vagito. Dal primo pagamento fatto da *Nakamoto*. E tutti nella blockchain devono averne una copia altrimenti non è possibile andare a ritroso per essere certi che ogni attore

abbia davvero i BitCoin che sta usando per pagare qualcun altro. Chiaro, no?

Meno evidente è il motivo del codicino di 64 caratteri. Ora ci arriviamo.

Date il benvenuto al re della blockchain: l'algoritmo di cifratura **sha-256**. Nome alieno ma funzionamento molto terreno. Siamo molto distanti dal *Cifrario di Cesare*, anche se fa qualcosa di simile. Pensate che questo simpatico algoritmo di codifica è capace di trasformare miliardi e miliardi e miliardi di informazioni in un codice molto corto.

Figo, eh?

Per chi è San Tommaso e vuole vedere

per credere, ho appena eseguito per voi l'algoritmo *sha-256* sull'intera *Divina Commedia*.

Ecco il risultato:

2cda53aeba51de19593dc5ec1ff076a860

Qui dentro c'è *tutta* la *Divina Commedia*. Tutta.

Pensate che potreste addirittura inserire tutta l'informazione del mondo in sha-256 e lui vi darà sempre un codice di 64 caratteri.

Che mattacchione.

È un algoritmo ultra-preciso. Basta cambiare **una sola** virgola nella *Divina Commedia* per ottenere un codice

totalmente diverso.

Sembra incredibile e qualcuno mi urlerà "*caspita! È meglio di una compressione zip!*". E direbbe una fesseria. Perché il trucchetto è sottile: sha-256 comprime sì qualsiasi cosa, ma a **senso unico**. Non posso in alcun modo ricreare la *Divina Commedia* partendo dal codice che vi ho incollato poco fa.

Sorry.

Quindi a cosa serve questo benedetto sha-256? Vediamo.

Immaginate di voler dare a qualcuno la possibilità di verificare la vostra password ma senza che lui possa in

effetti vederla. Come potete fare? *Mission impossible*? Affatto: inserite la password in sha-256 e date il codice risultante al vostro interlocutore. A lui basta avere lo stesso codice nel suo archivio per fare un confronto e dirvi: "*ok, la password è giusta!*".

In sostanza, tutta la comunicazione e la verifica avvengono sempre e solo sfruttando versioni criptate della password. Nessuno vede mai l'originale, ma nonostante questo tutti possono convenire che la chiave sia giusta.

Perché *sha-256* darà sempre lo stesso risultato a parità di informazione

inserita. Se tra 4 anni reinserisco tutta la *Divina Commedia* nell'algoritmo, otterrò sempre:

2cda53aeba51de19593dc5ec1ff076a860

I blocchi di transazioni della blockchain sono costantemente trasformati in un codice come il precedente da sha-256. In questo modo è facile per i nodi della rete continuare le proprie ossessive verifiche e confrontarle tra loro. È decisamente più agevole comparare due testi di poche decine di lettere rispetto a intere enciclopedie di pagamenti, no?

> *Il nome tecnico dell'attività di compressione operata da sha-256 si chiama **hashing**. Non chiedetevi*

*cosa significhi, va bene così. Vi basti sapere che una cosa è eseguire l'hashing una volta, una cosa è ripeterlo milioni di volte come richiesto dalla blockchain per generare la proof-of-work. Stressa moltissimo il computer e richiede una montagna di energia.*

Sha-256 nella blockchain si occupa di due cose importanti:

1) È un modo compattissimo per verificare e confrontare tutte le transazioni della storia della blockchain. Sin dal suo primo vagito!

2) Se eseguito molte volte richiede

parecchia “fatica” computazionale e energia. Esattamente i requisiti di una proof-of-work che si rispetti.

Ci siamo. Siete pronti a vedere i pistoni muoversi.

Ecco come funziona in buona sostanza la gara che si ripete ogni 10 minuti nella blockchain:

1) Ogni nodo della rete richiama il codice di 64 caratteri del blocco precedente della blockchain già validato.

2) Crea una sorta di lungo documento in cui scrive 1) questo codice, 2) tutte le transazioni da approvare

nel nuovo blocco, 3) un numero generato a caso. L'algoritmo sha-56 comprime tutto questo e restituisce un codice univoco di 64 caratteri.

3) Il nodo chiede alla rete se questo codice è la soluzione corretta al problema matematico per l'attuale blocco di transazioni.

4) In caso negativo si ripete il ciclo un numero catastrofico di volte sinché qualche nodo non trova la soluzione e vince. In ogni ripetizione ogni nodo cambia il numerino casuale inserito nell'algoritmo al punto 2. Come nel

caso della *Divina Commedia*, basta cambiare una virgola (in questo caso, un numero) affinché sha-256 restituisca un codice totalmente diverso dal precedente.

Questo implica che la compressione di ogni blocco di transazioni avvenga infinite volte e in ogni singolo nodo della rete finché qualcuno non individua per pura "forza bruta" la stringa di codice corretta.

*In verità non esiste una vera e propria stringa di caratteri esatta da individuare ma piuttosto un codice più basso di un certo parametro. Lasciamo perdere, è*

*matematica avanzata.*

È un misto di potenza di calcolo e **fortuna**, perché partecipano così tanti computer alla gara che sei sempre sul filo del rasoio.

Il giochino matematico da risolvere inoltre si adegua alla potenza di calcolo totale della rete che aumenta col numero dei partecipanti: più è alta, più trovare il codice vincente è laborioso perché il problema crittografico diventa più gravoso. In questo modo i disincentivi a partecipare restano sempre alti.

Non avete capito nulla? Non preoccupatevi, gran parte dei dettagli non vi servono, è pura curiosità.

# Blockchain nuda

Avete appena incontrato ottocentomila concetti difficilissimi ma interessanti, auspico. Proviamo a riassumerli in una breve storiella realistica.

Immaginiamo di vivere in un mondo in cui BitCoin è ormai una moneta come un'altra ed è diffuso come l'Euro o come il Dollaro australiano. Supponete di chiamarvi *Arturo* (siamo tutti omonimi!) e di voler acquistare online tramite BitCoin una gigantesca pizza tripla mozzarella strapiena di ogni leccornia. La pizzeria da asporto dal cui portale volete ordinare si chiama *Il Vizio Mortale*. Della serie: uomo

avvisato, mezzo salvato.

1) Sono le 18. Vi collegate al sito de *Il Vizio* e create la vostra pizza mortale con la marea di ingredienti letali che la vostra depravazione vi impone. Cliccate "*paga con BitCoin*" e si apre una finestra in stile PayPal con il vostro portafoglio elettronico. Pagate con BitCoin. Per l'esattezza 0,0011 BTC.

2) La transazione a questo punto è in attesa di essere elaborata dalla blockchain.

*Se l'avete scordato vi ricordo perché abbiamo*

*bisogno di una blockchain. Ringraziatemi poi.*

*BitCoin non può e non vuole contare su un elemento centrale di controllo delle transazioni come Visa o una banca. Quindi non abbiamo nessun "ente terzo" in grado di assicurare a Il Vizio che voi possediate davvero i soldi che volete spendere.*

*Come si risolve? Con un registro pubblico con tutte le transazioni da e verso di voi e qualcuno che usi questo registro per dire ai signori di Il Vizio: "Sì! Arturo ha*

*questi 0,0011 BitCoin da spendere e ora ve li trasferiamo!”. Anche senza punti esclamativi, si intende.*

3) La richiesta di spostamento di 0,0011 BitCoin da uno dei vostri indirizzi a quelli de *Il Vizio* entra in un blocco della blockchain e viene quindi diramata a *tutti* i nodi della rete mondiale interessati a validare il blocco di transazioni in cambio della possibilità di ricevere monetine virtuali sonanti.

4) Un minatore con la potenza di calcolo necessaria e tanta energia da spendere risolve il puzzle matematico legato al blocco che

contiene la vostra transazione e invia la sua elaborazione – cioè la proof-of-work – al resto della blockchain per conferma.

5) La maggioranza della blockchain conferma la bontà della proof-of-work ricevuta e invia un grandissimo “YES, YOU CAN” al tizio fortunato. Vorrei chiarire che si parla sempre di comunicazioni quasi istantanee tra computer, non immaginatevi omini veri o virtuali che chiacchierano.

6) Il computer del tizio inserisce quindi l’ultimo blocco di cui ha trovato la soluzione nella

blockchain e tutti i registri del mondo si aggiornano.

7) A voi e a *Il Vizio* arriva la conferma del trasferimento di BitCoin. Il vostro borsellino elettronico fa un po' di calcoli contabili e aggiorna il vostro conto. Avete ufficialmente 0,0011 BTC in meno rispetto a prima. Al netto di possibili commissioni.

8) Un'ora dopo arriva un fattorino stremato con la vostra pizza gigante da 3 kg.

Ora vi torna tutto, no?

Domanda finale.

Cosa accadrà quando non saranno più creati nuovi BitCoin nel 2140? Chi ricompenserà i validatori della rete?

Risposta un po' banale: le **commissioni**. BitCoin diventerà un circuito un po' più simile a *Mastercard* e chiunque darà qualcosina alla rete in cambio del lavoraccio di verifica dei pagamenti.

Per il resto rimarrà identico ad ora.

Ed ecco a voi un gioviale schema riassuntivo del funzionamento della blockchain:

# FUNZIONAMENTO BLOCKCHAIN CRIPTOVALUTE

Invio un pagamento in BitCoin.

La transazione è inoltrata alla blockchain globale.

I nodi della blockchain impacchettano questa transazione con altre per costruire un blocco.

I nodi competono tra loro per validare per primi il blocco mentre risolvono un problema matematico sempre più difficile tramite hashing.

Il nodo vincitore sigilla il blocco e trasmette la sua proof-of-work all'intera blockchain.

Gli altri nodi verificano la proof-of-work e confermano l'autenticità del blocco.

Il nuovo blocco viene inoltrato all'intera rete, diventando l'ultimo elemento del registro decentrato della blockchain.

La blockchain continua a crescere sia come elenco verificato di tutte le transazioni, sia come versione compatta grazie all'hashing.

BitCoin, Benefit, Boom!

~ Francesco Galvani

# In sintesi

- L'anima di BitCoin è la **blockchain**, cioè la rete decentrata dei registri delle transazioni.
- Tutta la storia di tutti i pagamenti in BitCoin è registrata nella blockchain stessa, che a sua volta viene costantemente verificata e sincronizzata dai miner distribuiti sul globo.
- I BitCoin non sono entità atomiche o file contenenti codici che corrispondono a monete virtuali. Esistono solo nel corso dell'attività contabile operata dalla blockchain.

- Tutto nella rete BitCoin è cifrato secondo un algoritmo potente e (ad oggi) indissolubile: **sha-256**.

- **Satoshi Nakamoto** è il misterioso (o un gruppo di misteriosi) inventore di BitCoin. La sua bravura si è manifestata nel condensare in un insieme coerente e funzionante molte delle ricerche e delle scoperte della comunità cypherpunk entro cui è apparso.

- La blockchain ha due scopi opposti da conciliare: 1) tenere distante chi ha interesse a truffare le transazioni e 2) attrarre una quantità considerevole di nodi in

grado di creare una rete ampia e decentrata di verifica.

- Per risolvere il dilemma *Nakamoto* ha sfruttato una soluzione conosciuta tra gli esperti di sicurezza informatica: la **proof-of-work**. La POW consta nell'obbligare chiunque voglia accedere a una rete a compiere parecchio "lavoro" computazionale per diminuire la probabilità di attacchi maligni. Nella blockchain tale fatica viene ricompensata con nuove monete.

- Le transazioni sono elaborate dall'intera blockchain al ritmo di

un blocco ogni 10 minuti; questo intervallo corrisponde quindi all'emissione di nuovi BitCoin.

- Il numero di monete emanate dal sistema per retribuire il nodo vincitore di ogni blocco viene dimezzato ogni 4 anni. L'ultimo BitCoin sarà forgiato all'incirca nel **2140**.

# Il BUONO, IL BRUTTO E IL CATTIVO

## Dove tecnica e critica si incontrano

Prima di addentrarci nelle altre criptomonete e nei metodi per sfruttare a nostro vantaggio questo incredibile nuovo universo finanziario la mia anima umanista mi obbliga a una breve riflessione con voi, miei adorati lettori.

È *stupido* limitarsi a vedere ogni nuovo fenomeno dalla sola angolatura mediatica esaltata o ingegneristica

imparziale, entrando in fibrillazione come dei cagnolini impazziti di gioia o analizzandolo come dei robot. Nel mondo cripto non esistono solo le opportunità o le "*figate*". Esistono anche tantissimi rischi. Rischi per le nostre tasche e per il nostro fragile mondo.

Se rinunciamo alla visione d'insieme di un fenomeno complesso come BitCoin, in cambio di una breve eccitazione superficiale rischiamo di lasciarci le penne o di fare dei danni. Come sanno bene i nostri amici che hanno bruciato risparmi propri e dei genitori in imprese senza senso o start-up ridicole basate sulla pura esaltazione tecnologica.

Le criptomonete sono realmente qualcosa di eccezionale. Ma altrettanto eccezionale è la stoltezza e la faciloneria con cui se ne parla (e con cui si agisce) online e nelle conversazioni che ho avuto la sfortuna di sentire o leggere negli ultimi mesi.

Ne ho le scatole piene. Non dovete seguire questa massa di anatre starnazzanti.

Dovete volere di più. Ve lo meritate.

# Sicurezza

Sin dal documento programmatico di *Nakamoto* sappiamo che BitCoin nasce espressamente affinché i pagamenti siano pubblici ma anonimi. Esattamente come le transazioni in borsa a cui siamo tutti abituati.

Questo rende l'intero ecosistema sicuro sin dalla sua progettazione per noi utenti. Non esiste il rischio che la blockchain venga *hackerata* e che i nostri dati personali siano resi pubblici alla pubblica gogna. Semplicemente, non sono proprio presenti sulla rete; quindi c'è poco da rubare. Non possiamo dire lo stesso dei normali circuiti di

pagamento come quelli gestiti da banche e istituzioni finanziarie, la cui architettura dipende espressamente da un'associazione conservata nei propri database tra numero del conto e dati personali di un cliente.

Questo non significa che ogni *punto* del circuito BitCoin sia perfettamente a prova di privacy. Anzi. I portafogli elettronici possono essere espugnati, i nostri dati e le password rubate, milioni di Euro in BitCoin saccheggiati. Non esiste un motivo progettuale per cui questi servizi debbano essere più sicuri di un normale conto corrente. Anzi, non esiste un motivo per cui *lo siano*, visto che le banche hanno migliorato per

decenni la loro tecnologia di protezione degli accessi. Le aziende che propongono borsellini elettronici sono invece piuttosto giovani.

La storia delle frodi ai portafogli elettronici di BitCoin è lunga tanto quanto l'esistenza delle criptomonete. L'ultimo caso mirabolante a fine 2017: sono spariti nel nulla ben **63 milioni** di Dollari in BitCoin, rubati dai *wallet* dei clienti dell'azienda *NiceHash*. Soldi di persone vere.

Quali imprecazioni avreste urlato al vostro cassiere se un pirata informatico avesse rubato dal vostro conto corrente tutti i vostri averi? Molto probabilmente

in quel caso avreste riottenuto tutti i soldi perché esistono assicurazioni e contromisure per tali evenienze. Viceversa, i clienti di NiceHash sono rimasti a bocca asciutta.

Ciò detto, il fatto che i portafogli elettronici siano espugnabili non scalfisce la privacy insita nella blockchain e nel DNA di BitCoin. Pane al pane.

# Decentralizzato e deflattivo

Giù le mani: la potenza inarrivabile e il miglior pregio di BitCoin è certamente il suo essere un sistema **decentrato**. Su questo aspetto la criptomoneta stravince rispetto ai sistemi di pagamento tradizionali.

Abbiamo affrontato ampiamente la questione nella prima parte del libro e non ha senso ripetere i dettagli di ciò che già sappiamo. In grandissima sintesi un sistema decentrato ha alcuni vantaggi su uno centralizzato:

- È più robusto. Se cadessero tutti i server di *Visa* all'improvviso vi immaginate la tragedia? Viceversa,

è ampiamente improbabile crollino *tutti* i nodi sparsi per il mondo della blockchain.

- È meno prono alla manipolazione da parte di un'entità fraudolenta. Ripensate alla storia del pianeta *e*: è più agevole modificare un solo registro o 10, 100, 1.000.000?

- Non permette la creazione *ad hoc* di nuovo denaro per ripianare debiti di stati o manipolare l'economia come fanno da sempre le banche centrali. Quindi non consente di mettere in moto dinamiche di **inflazione**.

L'ultimo punto in verità non è né

positivo né negativo. Chi vi racconta che l'inflazione è in assoluto una brutta cosa è un cialtrone. Seguitemi.

Sapete ormai che BitCoin vuole essere *deflattivo* (quindi di natura dovrebbe far aumentare nel tempo il valore dei vostri soldi).

Immaginiamo il caso fantasioso (e improbabile) per cui BitCoin dovesse diventare da moneta di nicchia a valuta fondamentale per intere nazioni come l'Euro o il Dollaro. E supponiamo che all'atto pratico il suo comportamento sia effettivamente deflattivo come da progetto.

Nel tempo, in quanto possessori di una

moneta deflattiva, diventeremmo tutti ricchi visto che non avremmo alcuna inflazione ma, anzi, i nostri soldi lasciati in banca crescerebbero di valore in modo continuo. Fantastico!

E invece no. Sarebbe un **inferno**.

Nel nostro mondo *deflattivo* dominato da BitCoin, se lasciamo i soldi in banca diventiamo ogni giorno più ricchi perché domani i nostri denari varranno più di oggi. O, detta in un altro modo, le merci domani costeranno *meno* di oggi. È la stessa regola espressa in una diversa formulazione.

Ora. In una tale condizione solo un fesso spenderebbe del denaro oggi visto che

tenendolo nel taccuino un giorno in più potrebbe risparmiare qualcosa negli acquisti domani. E tenendolo un anno in più potrebbe addirittura fare un affarone! Mi seguite? Se tutti iniziassero ad applicare questa logica (e *tutti* la applicherebbero, potete starne certi, la gente massimizza le proprie opzioni) l'economia si arresterebbe.

Perché si innesterebbe un ciclo basato sul "*beh, mi conviene rimandare a domani l'acquisto*".

Serrande dei negozi abbassate per mancate vendite. Fabbriche chiuse. Uffici deserti. Posti di lavoro crollati. Disoccupazione. Fame. Tragedie

personali e familiari.

Aggiungiamo a questo bel panorama di serenità un altro tassello: la deflazione è una catastrofe per i debitori (e *tutti* gli stati moderni sono strapieni di debiti). Con un regime deflattivo il valore reale del debito sale costantemente perché il valore dalla moneta in cui è espresso tale debito sale costantemente.

Esempio banale.

Se oggi ti devo 1.000 Euro, in un'economia in deflazione tra qualche anno il valore **reale** del mio debito verso di te salirà a 1.050 o 1.100 Euro, anche se il valore nominale del mio debito rimarrà a 1.000 Euro! Perché nel

frattempo il valore reale che pretendi da me sarà maggiore di oggi.

No buono, visto che la nostra economia globale si basa sul credito.

Seriamente anelate a un mondo del genere?

Troppa inflazione danneggia l'economia perché abbatte la fiducia nel sistema, il risparmio, la capacità di acquisto, la progettualità. Ma zero inflazione, quando non proprio deflazione, crea ancora più danni. Perché scoraggia acquisti, progetti, investimenti e mutui.

In definitiva.

L'idea della deflazione insita nelle

criptomonete è carina se queste restano un oggetto di nicchia. Diventerebbe il suicidio dell'economia se queste dovessero espandersi e diventare valute importanti nella finanza.

Ora che masticate un po' di macroeconomia convenite che l'idea di una banca centrale che attua politiche di inflazione non è poi una calamità come molti esaltati delle criptomonete ci vengono a dire quotidianamente?

Belle le valute decentrate. Ma forse il loro posto non è proprio al centro della scena.

# Oliare

BitCoin promette zero o bassissime commissioni perché i nodi della blockchain sono pagati con la creazione di nuove monete, ricordate? Certo, quando non saranno più generati nuovi soldini (nel 2140) si dovrà fare solo affidamento sulle commissioni, ma per ora si vincono dinari freschi freschi creati dal sistema e nessuno deve sborsare un Dollaro.

In teoria.

Nella pratica non è proprio così. *Nakamoto* ha dato la possibilità agli utenti della rete di pagamento BitCoin di "*prioritizzare*" la verifica della propria

transazione pagando un balzello. Un po' come quando sborsate 10 Euro in più per un volo *low cost* solo per avere l'imbarco rapido o per scegliervi il posto.

Non è proprio una pratica così cristallina in un universo che si propone come l'alternativa etica e democratica allo sporco capitalismo e ai suoi benefici dati a chi ha più soldi rispetto agli altri. No?

Eppure, incredibilmente, esiste questa possibilità. E, ancora più incredibilmente, nel mondo reale dei pagamenti in BitCoin viene usata molto spesso e le commissioni sono molto alte.

Specie se:

- La blockchain è sovraccarica perché in tanti vogliono operare pagamenti in un certo momento (ad esempio quando ci sono grandi fluttuazioni di valore della moneta). E si tratta di un problema sempre più serio.

- Sei un utente che opera tanti piccoli pagamenti. In questo caso vieni espressamente scoraggiato dalla rete e ti si richiedono commissioni sempre più alte.

Volete un'idea delle commissioni? Preparatevi a rimanere a bocca aperta collegandovi a questo link:

http://bit.ly/avg_transactionfee.


Il 22 dicembre 2017, nel picco dello scoppio di una piccola bolla delle criptomonete, avreste dovuto pagare ben **55 Dollari** per operare una singola transazione in BitCoin. A gennaio 2018 fortunatamente ci si è stabilizzati sui 10 Dollari.

Questo è un problema. Immaginate che meraviglia pagare una pizza tripla

mozzarella 12 Euro e aggiungerne 50 di commissioni.

Vediamo un altro tema interessante a proposito dei pagamenti.

Quando pago con la mia carta di credito *Visa*, oltre ad avere commissioni basse (e a carico dell'esercente) ho la buona certezza che uno stuolo di professionisti e di algoritmi intelligenti stia **vegliando** su di me. Non solo in molti casi questi signori umani e digitali bloccano del tutto le transazioni sinché non le approvo espressamente al telefono. Ma possono addirittura restituirmi i soldi – quando non proprio invertire il pagamento – in alcuni casi in cui si

suppone io sia stato derubato.

Con BitCoin scordatevi tutto questo ben di Dio. Quando una transazione è stata validata dalla blockchain e sigillata in un blocco, è andata. Non si torna indietro. Non c'è alcuna reversione possibile. Soldi? Bye bye.

E se perdo la mia normale carta di credito? Posso bloccarla alla velocità della luce. Mentre se dimentico il mio indirizzo BitCoin sono a terra. E se perdo la password (perché magari l'ho scritta su un pezzetto di carta o un file) e qualcuno la trova, **ufficialmente** possiede tutti i miei soldi e nessuno può fare niente.

Vi va bene? Sicuri? A me no.

Ben più di una volta i signori delle carte di credito mi hanno salvato da una brutta nottata di ansia. E in un paio di occasioni ho potuto bloccare alla velocità della luce il bancomat, rimanendo felice possidente di tutti i miei averi.

Si noti che le stesse regole si applicano a tutte le altre applicazioni delle blockchain, quindi anche ai famosi *smart contract* (ne riparleremo).

Questo è un altro maleficio potenziale del decentramento.

# Riccastri

BitCoin nasce per realizzare il sogno di una finanza democratica e equa. In cui non esistano Paperoni e istituzioni con potere immenso o "*too big to fail*". In cui tutti abbiano le stesse possibilità e le transazioni costino nulla o pochissimo.

Abbiamo già visto che l'ultimo obiettivo è stato mancato, per ora. E la visione etica dell'economia? Ha mantenuto le promesse?

Benché la blockchain abbia tutte le caratteristiche tecniche per diventare ciò che *Nakamoto* ha garantito, la sporca realtà dei fatti è piuttosto distante dal mondo ideale a cui tutti i cypherpunker

anelavano a fine anni 2000.

Perché i BitCoin sono soldi. E i soldi seguono una vecchia regola: *piove sempre sul bagnato*. È più di un luogo comune. È una verità statistica che nasce dal funzionamento degli *asset* intangibili.

Ecco una bella tabella presa da *bitinfocharts* pronta a sgonfiare ogni nostra fiducia nella democrazia del sistema-BitCoin. Intanto osservatela, poi la commentiamo.

| SALDO SULL'INDIRIZZO | NUMERO INDIRIZZI | INDIRIZZI SUL TOTALE | VALORE BTC | VALORE DOLLARI | VALORE SUL TOTALE |
|---|---|---|---|---|---|
| 0 - 0.001 | 15352242 | 55.84% (100%) | 2,702 BTC | 31,008,383 USD | 0.02% (100%) |
| 0.001 - 0.01 | 5485769 | 19.95% (44.16%) | 23,403 BTC | 268,617,708 USD | 0.14% (99.98%) |
| 0.01 - 0.1 | 4255941 | 15.48% (24.21%) | 136,247 BTC | 1,563,802,121 USD | 0.81% (99.84%) |
| 0.1 - 1 | 1711056 | 6.22% (8.73%) | 544,751 BTC | 6,252,501,840 USD | 3.25% (99.03%) |
| 1 - 10 | 541390 | 1.97% (2.51%) | 1,438,023 BTC | 16,505,232,461 USD | 8.58% (95.78%) |
| 10 - 100 | 131583 | 0.48% (0.54%) | 4,358,907 BTC | 50,030,334,388 USD | 26.01% (87.2%) |
| 100 - 1,000 | 15686 | 0.06% (0.06%) | 3,699,462 BTC | 42,461,401,218 USD | 22.07% (61.19%) |
| 1,000 - 10,000 | 1506 | 0.01% (0.01%) | 3,328,365 BTC | 38,202,052,201 USD | 19.86% (39.12%) |
| 10,000 - 100,000 | 110 | 0% (0%) | 2,792,497 BTC | 32,051,515,891 USD | 16.66% (19.26%) |
| 100,000 - 1,000,000 | 3 | 0% (0%) | 435,058 BTC | 4,993,475,884 USD | 2.6% (2.6%) |

La tabella raggruppa tutti gli indirizzi dei BitCoin (cioè i conti) in gruppetti. Ogni gruppo consta degli indirizzi con un saldo compreso tra un valore minimo e un massimo. Ad esempio, nella prima riga avete gli indirizzi che contengono da 0 a 0.001 BitCoin. Nella seconda colonna ci viene indicato quanti indirizzi

ci sono in quel *range* di valori. Nella terza vediamo che percentuale occupano tutti quegli indirizzi sul totale dei conti attivi (tra parentesi avete una somma cumulata). A seguire la somma di tutti i BitCoin presenti in quegli indirizzi, il loro corrispettivo in Dollari a gennaio 2018, e infine quanto cuba la somma del valore sul totale.

Se non vi è chiaro qualcosa no problema, ci interessano poche informazioni per stimare l'entità della faccenda.

Una di queste informazioni è che ben **il 55%** degli indirizzi – con buona approssimazione possiamo quindi dire

“il 55% delle persone” – possiede solo lo **0,02%** dei BitCoin quanto a valore. Mentre 3 sole persone possiedono **100 volte tanto** (ultima riga).

Non solo. Con due semplici calcoli possiamo stimare che poco più dello **0,01%** dei possessori di BitCoin (1609 persone) detiene **il 40%** della ricchezza. Basta sommare le ultime tre righe.

Inquietante.

È vero che sono calcoli in parte approssimativi perché la blockchain utilizza vari indirizzi di deposito temporaneo per il suo funzionamento e questo porta la concentrazione reale a essere *leggermente* meno drammatica di

così, ma la realtà dei fatti è che oggi BitCoin segue le orme iper-liberiste di qualsiasi altra moneta.

La stragrande maggioranza della ricchezza appartiene ad una piccolissima e infima schiera di riccastri (tra cui *Nakamoto*), mentre quasi tutti gli altri si devono accontentare delle briciole.

Questa situazione cambierà? Non lo sappiamo.

# Abbiamo un solo pianeta

La concentrazione psuedo-democratica del BitCoin è un problema abbastanza relativo. Il mondo è sempre stato dominato da pochi ricconi. Abbiamo fatto il callo alla cosa e non dovrebbe rovinarci la cena più di tanto.

Ciò che invece dovrebbe farci saltare sulla sedia e causarci un mezzo infarto è l'aspetto in assoluto più drammatico, insensato, stupido, incompreso e congenito della blockchain.

Il suo demente **consumo energetico**.

Ho letto tempo fa varie teorie complottiste secondo cui *Satoshi*

*Nakamoto* non fu in realtà un benefattore. Ma piuttosto un sinistro signore malefico con un chiaro piano per arricchirsi a dismisura e al contempo gettare nella catastrofe ecologica la civiltà occidentale al fine di distruggerla come forma di vendetta.

È un chiaro *non-sense*. Ma all'atto pratico questa teoria allucinata descrive la realtà dei fatti.

*Nakamoto* si sta davvero arricchendo in maniera esasperata – si veda il precedente capitoletto. E al contempo la sua idea di blockchain sta realmente vanificando molti sforzi per salvare la nostra biosfera dall'effetto serra e dal

global warming. Sta concretamente rendendo difficile in molte aree del mondo il passaggio alle – spesso meno performanti – energie rinnovabili.

Se siete stati studenti attenti sapete già perché.

Tutto nasce nel meccanismo machiavellico e satanico dell'hashing ininterrotto e esasperato necessario per generare le proof-of-work nella blockchain. Non rispiego l'intero giochino, mi basta ricordarvi che la caratteristica essenziale di questo puzzle matematico infernale è di diventare **esponenzialmente** più difficile all'aumentare della potenza di calcolo

totale della blockchain.

Che sarebbe a dire che più nodi partecipano all'analisi dei pagamenti e più potenza di calcolo hanno questi nodi sommati, più trovare la proof-of-work diventa computazionalmente assurdamente difficoltoso.

E oggi è già così.

Pensate che la verifica di *una sola* transazione consuma più energia di **otto case** americane nell'arco di 24 ore. UNA-SOLA-TRANSAZIONE. Non un blocco intero di transazioni. Parlo di un singolo pagamento, come l'ordine della nostra pizza.

Nel 2017 la blockchain di BitCoin ha consumato tanto quanto la **Serbia**, un paese di 8 milioni di persone esteso 90 mila km quadrati.

Per chi macina numeri ecologici, sempre nel 2017 il mining di BitCoin ha fatto emettere all'umanità 16 mila kilotoni di Co2.

Più informazioni qui: http://bit.ly/bitcoin_footprint_gov.

E questi numeri non possono che **aumentare** a ritmi sostenuti e assurdi negli anni a venire, all'aumentare della potenza della blockchain. Che per definizione si ingigantisce continuamente man mano che entrano nella

competizione per la proof-of-work nuovi nodi e organizzazioni dotate di super computer e veri e propri stuoli di server dedicati solo a questo scopo.

Lo capite che si rasenta la follia?

Vi è chiaro che tutto questo è insostenibile e che il BitCoin ci sta, di fatto, soffocando?

Da un lato abbiamo gli sforzi esasperati degli stati, delle organizzazioni e di menti eccelse come *Elon Musk* ossessionate dal diminuire i gas serra per salvarci dall'estinzione. Dall'altro ci sono le criptomonete che con algoritmi senza alcuno scopo reale (lo scopo del loro esasperato consumo

energetico è solo di creare proof-of-work; per validare le sole transazioni basterebbe una frazione minuscola di queste risorse) ci potrebbero portare all'ora più buia per la nostra specie.

Fortunatamente si stanno elaborando soluzioni e monete alternative, ma vi deve essere chiaro il grattacapo tragicomico continuamente ignorato.

Stimolo finale: qualche mese fa ho scritto un'analisi su *Quora* a proposito del consumo energetico di BitCoin. A metà 2017 avevo stimato che questa moneta dai pochissimi scambi reali inquinasse 33 volte l'intero sistema di validazione delle transazioni di *Visa*.

Cioè uno dei circuiti che reggono l'intera economia mondiale. Qui la mia risposta con altri dati a supporto: http://bit.ly/frankstyle_bitcoin_consumo.

Di nuovo: decentrato è bello. Ma sarebbe ancora più bello se non inquinasse sproporzionalmente più di un sistema centralizzato.

Si noti che il problema non è la blockchain di per sé, ma la blockchain basata sulla proof-of-work, che per sua natura è dispendiosa e inefficiente. Esistono altri incentivi possibili decisamente più razionali, e molti di loro sono stati già incamerati nelle altre criptomonete. Ne parleremo nell'ultima

sezione del libro.

# Istituzioni e tasse

La natura anonima degli scambi in BitCoin e criptovalute è un grosso dilemma di ordine fiscale e di sicurezza per gli stati nazionali e le società di intelligence.

L'ironia delle criptomonete sta proprio nel permetterci di sapere *cosa* ma senza sapere *chi*. Possiamo vedere spostarsi per la blockchain fiumi di valori e allo stesso tempo non avere alcun mezzo per:

- Sapere a chi far pagare le tasse.
- Controllare cosa stia succedendo e chi stia venendo finanziato.
- Evitare che del denaro finisca in

mano a organizzazioni terroristiche.

- Scongiurare l'ipotesi che qualcuno sfrutti l'anonimato per sponsorizzare reati tramite il *deep web*.

Non è una situazione che può durare per sempre.

Nel 2017 la Cina ha iniziato a fare sul serio chiudendo *exchange*, limitando gli scambi e spingendo per l'eliminazione dell'anonimato. A inizio 2018 la Corea del Sud ha seguito l'esempio. Causando come effetto secondario l'eccezionale crollo di BitCoin di gennaio 2018 visto che nella nazione di *Samsung* la

comunità di cripto-utenti raggiunge livelli di riguardo. Decine di migliaia di coreani sono effettivamente coinvolti nelle monete virtuali.

L'**Unione Europea** si è dimostrata preoccupata per il controllo delle criptovalute e ha aperto un intenso tavolo di discussione in merito, soprattutto per un tema di ordine fiscale e di equilibrio con l'Euro. Non è in effetti particolarmente etico o sicuro che in un territorio esista un'intera economia sommersa di scambi valutari non governabili.

Dovete ricordare che secondo il cartalismo (teoria ancora dominante

nella nostra società) la moneta è soprattutto uno strumento di governo e democrazia. Quindi non è indifferente per una nazione o un gruppo di nazioni avere valute incontrollabili che competono con la principale. Sono viste come falle potenziali che rischiano di aprirsi a dismisura e di rendere impossibile la gestione della società civile tramite emissione e ritiro di contante.

Dubito passerà ancora molto tempo prima che si legiferi sul tema.

Il **Regno Unito** ha risolto la faccenda a monte, decidendo di trattare BitCoin e fratelli come monete “private”.

Ovverosia legali e non tassate negli *exchange*, ma non per questo neutrali rispetto al pagamento dell'IVA sui consumi – la *VAT*. Il che significa che potete tenere tutti i soldini digitali che volete, ma nel momento in cui li usate sul territorio britannico per pagare beni o servizi a qualche esercente dovete pagare l'IVA come chiunque altro.

Si capisce che questo approccio è molto snello come tutto ciò che è anglosassone, ma alla fine è solo una bella teoria che non risolve il problema dei controlli. Se una transazione è anonima e non so né indirizzo di chi paga né quello di chi riceve, come verifico il pagamento dell'imposizione

fiscale sull'esercente?

La linea di pensiero più diffusa punta pertanto ad acciuffare il toro per le corna. Alla fin fine tutto il problema si risolve in una questione: come eliminare il **cripto-anonimato**? Ci sono molte strade percorribili. Ad esempio, una nazione potrebbe permettere a portafogli elettronici e *exchange* di operare sul territorio solo se questi inviano al database dei tributi nazionale i dati fiscali associati a ogni indirizzo BitCoin. In fondo è relativamente facile bloccare un servizio internet in uno specifico territorio se si nota che questo non collabora con le leggi vigenti.

In definitiva.

Si tratta di un tema caldissimo e di non facile soluzione tecnologica, oltre che legale. Tenete le orecchie alzate perché la situazione muterà sempre più in fretta.

# Fluttuazione

Ci prepariamo al prossimo capitolo con una rapidissima analisi finanziaria.

Una moneta vince se funziona da **deposito di valore**, cioè se siamo abbastanza fiduciosi che i nostri risparmi non verranno troppo intaccati nel tempo da fluttuazioni di sorta.

Abbiamo già discusso a sufficienza di inflazione e deflazione. In questo caso però la questione è più terra-terra e a breve termine: accettiamo tutti che l'Euro o il Dollaro subiscano un po' di inflazione, fa parte del gioco e ci sta bene perché si tratta di una dinamica che si sviluppa in tempi molto lunghi. Come

accettiamo deflazioni potenziali, anche nel caso di BitCoin. Quando però la moneta rischia di perdere **il 50%** del proprio valore in poche settimane com'è successo di recente a molte criptovalute, abbiamo un grattacapo di tutt'altra portata.

Una portata che fa pernacchie al rischio di inflazione. Con fluttuazioni così pazze una valuta non può di certo essere considerata papabile per accogliere nel tempo i nostri sudati dinari!

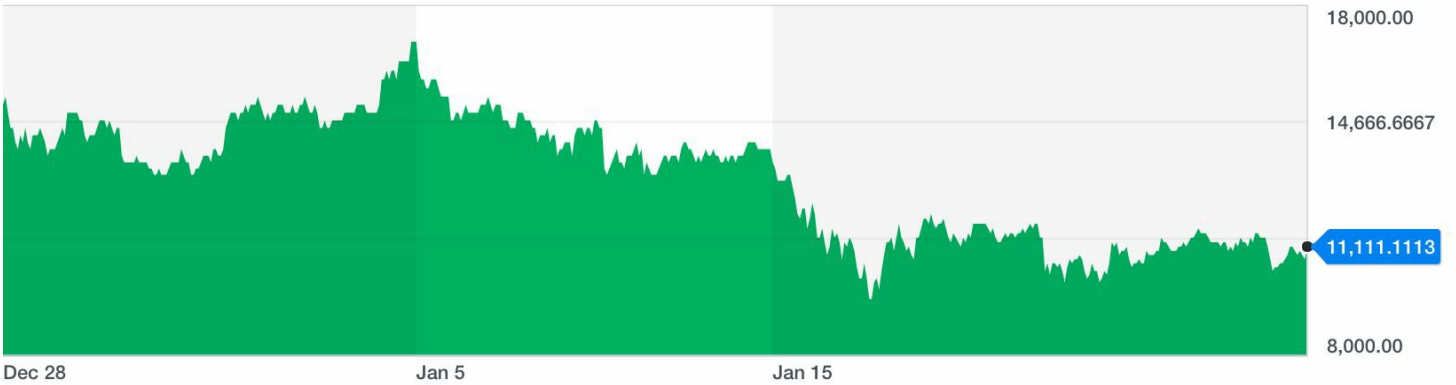
Nessuno con un po' di sale in zucca accetterebbe di vedere dimezzati in un mese i propri averi senza un reale motivo. Intendo dire: se investo o

speculo accetto il rischio di perdere il capitale. È parte del gioco. Ma se non ho fatto nulla di tutto ciò, che scuse ci sono?

Siamo d'accordo, no?

Bene.

Queste sono le fluttuazioni del prezzo di BitCoin versus Dollaro nel mese di gennaio 2018:




In 30 giorni la moneta è oscillata tra

poco più di 9.000 Dollari a quasi il doppio.

In confronto, queste sono le fluttuazioni dell'Euro sul Dollaro nello stesso periodo:


Oscillazione massima da 1,19 a 1,24 Dollari.

Non è proprio la stessa cosa, che ne dite? Da una parte abbiamo una volatilità quasi del 50%, dall'altra del

5%. E vi assicuro che sono stati giorni molto movimentati per entrambe le valute.

Ergo.

Decisamente no, BitCoin **non è** oggi un candidato serio ad accogliere i nostri risparmi. Come riserva di valore fa abbastanza pena. Questo tuttavia non toglie abbia altri meriti!

Ad esempio, con una tale variazione, BitCoin ha tutte le carte in regola per essere adorato dagli **speculatori** più accaniti, i signori e gli algoritmi che inseguono la pietra filosofale del guadagno a brevissimo termine permesso dai bruschi cambiamenti del

mercato. Cambiamenti possibilmente a favore dalla propria scommessa, si intende.

E noi? Posto che non possiamo fidarci di BitCoin come riserva di valore, abbiamo qualche possibilità di sfruttarlo per racimolare almeno qualche soldino?

Lo vedremo nella prossima sezione.

# In sintesi

- È nostra responsabilità capire il fenomeno cripto in modo ampio e senza cadere nelle facili esultanze o nella mera strumentalità. Riflettere conviene alle nostre tasche e al nostro pianeta.

- BitCoin è anonimo anche se le transazioni sono pubbliche. La blockchain è quasi indistruttibile ma i nostri *wallet* no. Trattandosi di tecnologie recenti è facile che gli hacker abbiano la meglio. E una volta rubati, i BitCoin sono irrecuperabili.

- Alcuni santoni del settore

brindano alla teorica natura deflattiva di BitCoin, dimenticando che sarebbe una tragedia per il benessere mondiale avere valute importanti deflattive e non inflattive.

- BitCoin nasce per essere democratico, economico e snello. Ma all'atto pratico si nota che senza pagare grosse commissioni la sua rete non processa con particolare gioia le nostre transazioni.

- Anche lato etico c'è molto di che discutere visto che la ricchezza in BitCoin è straordinariamente

concentrata nelle mani di pochissimi e per ora la moneta ha mostrato talento solo come mezzo di speculazione.

- Per via della proof-of-work il consumo energetico di BitCoin è insostenibile e l'inquinamento inaccettabile, specie nel medio e lungo futuro. Questo è probabilmente il maggiore problema della criptomoneta e il fronte su cui riceve più critiche dagli esperti.

- La pacchia dell'anonimia fiscale non può durare a lungo. I maggiori stati del mondo si stanno muovendo

su questo fronte.

- Le fluttuazioni di BitCoin sono incompatibili col suo utilizzo come riserva di valore (conto corrente o conto deposito) ma sono una manna se si vede questa criptomoneta come strumento di speculazione aggressiva.

# FAR SOLDI COI SOLDI

## A vostro beneficio

Molto bene amici, ci siamo fatti traghettare da *Caronte* attraverso il fiume Acheronte delle criptomonete. Abbiamo sterminato tutti (o quasi) i luoghi comuni e le follie popolari. Abbiamo filtrato i grammi d'oro e ne abbiamo fatto tesoro.

Nell'ultima sezione scopriremo il prolifico universo delle altre criptomonete e il futuro, ma prima di tornare a volare alto rimaniamo un po' con i piedi per terra. In particolare,

dobbiamo capire come sfruttare qui e ora a **nostro** vantaggio la tecnologia della blockchain.

Andando all'osso della questione, esistono **due** grosse strade per spremere la "rivoluzione BitCoin" a nostro favore:

1. Installare il software di mining sul nostro computer e diventare **validatori** di transazioni partecipando alla gara della proof-of-work.
    a. Una variante di questa soluzione è partecipare agli "anelli" di validazione. Cioè gruppi di fatica che

compaiono come un unico nodo della blockchain ma in cui ci si spartisce il lavoro tra tanti attori. Se si vince la gara ai BitCoin ci si distribuisce il bottino.

2. Fare **trading** nudo e crudo. In fondo BitCoin è, sulla carta, una valuta come un'altra. Come si fa trading su *Dollaro vs Euro* o su *Yen vs Dollaro canadese*, lo si può fare su *BitCoin vs Euro o vs Dollaro*. Ovviamente tramite una piattaforma che ci consenta di farlo.

Ritengo la prima opzione **fuori**

**discussione**. State leggendo un libro che contiene le mie opinioni pesate, quindi immagino vi interessino anche su questo aspetto. Non esiste oggi un solo motivo per cui per una persona comune abbia senso buttarsi nella battaglia senza prigionieri del mining nella blockchain.

Per varie ragioni:

- Ormai verificare le transazioni è divenuta un'impresa a dir poco irrealizzabile. Anche passando dai "*ring*", cioè dagli anelli di validazione, il carico di lavoro richiesto ai singoli attori è incommensurabile. Tra l'altro, se non si forniscono abbastanza

prestazioni al ring, al momento della potenziale vittoria si ricevono solo le briciole delle briciole.

- Quasi certamente avete un computer o un server nemmeno lontanamente accettabile per entrare in questa lotta. Non potete competere con esperti del mining super corazzati, con alle spalle quasi dieci anni di studi specialistici e in grado di creare per sé stessi delle macchine mostruose in termini computazionali. Siete delle formiche contro dei giganti.

- Per quanto formichine, l'elettricità la pagate pure voi. E anche ammesso siate artisti mondiali nel forgiare Godzilla spaventosi di computazione, prima o poi la bolletta arriva nella vostra bella casellina delle lettere. Su una cosa potete star tranquilli: i BitCoin che *potreste* ricavare dalla gara nella blockchain sono una frazione rispetto alla spesa *sicura* in bolletta.
    - I secchioni interessati alla matematica dei costi e in grado di stimare la potenza di calcolo delle proprie macchine possono divertirsi

con questo simulatore di spesa: http://bit.ly/hashrate_calculato

- Mai e poi mai consiglierò di dare voi stessi, il vostro tempo e le vostre preziose risorse ad una delle attività più stupide e inquinanti inventate dall'uomo. Abbiate o no figli, è imperativo per tutti preservare la biosfera terrestre per chi arriva dopo di noi.

Scartato cioè che è illogico e masochista, resta quindi la seconda opzione di guadagno.

# Tra ragione e emozione

Chi mi segue da qualche tempo conosce il mio amore senza fine per investimenti e speculazioni in borsa. Cioè per il trading.

Vi ho dedicato molti anni, soldi e notti insonni. All'inizio mi sono scottato con un approccio passionale e sono poi ripartito facendomi guidare solo da studio, statistica e numeri. Ho scritto software su software e analizzato montagne di mercati e di dati per trovare le soluzioni di investimento più robuste.

Tralasciando per un secondo i BitCoin, i metodi in assoluto più solidi ed efficaci per investire sul lungo termine con un

buon margine e rischi calcolati sono quelli che ho già descritto nel mio libro del 2017 *Le 3 Formule Segrete per Guadagnare in Borsa*. È qui: http://bit.ly/le3formule.

Molte persone adorabili mi hanno ringraziato per quel libretto perché hanno trovato in esso regole esatte da seguire senza tante interpretazioni. Regole basate sulla pura statistica. Una concezione piuttosto lontana dalle previsioni in stile *Nostradamus* dei grandi santoni degli investimenti che ci riempiono di storie e storielle sull'andamento delle aziende e dei mercati.

Devo altresì ammettere che un paio di lettori sono stati scornati: si aspettavano che il mondo degli investimenti fosse un monte Everest dalla difficoltà inarrivabile; forse per via della quantità assurda di materiale confuso letto e dei commentatori strillanti ascoltati nel tempo. L'idea di una sfida ciclopica li appassionava. Era per loro qualcosa di eroico. Al che, nello scoprire che il miglior modo di guadagnare è riassumibile nella gestione esatta dei soldi, delle proprie emozioni e in tre formule matematiche, sono stati presi da un certo sconforto.

Amici del mondo del fitness, personal trainer e dietologi mi confermano che

assistono giornalmente allo stesso fenomeno: le soluzioni solide, sintetiche e esatte soddisfano tutti *tranne* una piccola percentuale di persone che vedono nell'automiglioramento non un mezzo, ma uno **scopo**. Nel trading funziona allo stesso modo.

In definitiva: per la **maggior parte** dei miei lettori interessati al guadagno nudo e crudo con gli investimenti basta il libro sopraccitato. Non vi serve rischiare con le criptomonete. Ma comprendo che una parte di voi voglia *avventura e palpiti*. Voglia esporsi e azzardare di più per il gusto stesso di avere a che fare con qualcosa di eccitante come il trading sulle

criptomonete.

Ci può stare, è umano e lo comprendo. Io stesso rientro in un certo senso in questo gruppo. Questa è la sezione per voi/noi.

# La scienza del trading

Punto di partenza: BitCoin è **giovane**. Molto giovane. Maledettamente giovane. Nasce nel 2008 e ha oggi solo 10 anni. Anni in cui si è limitato a crescere, come qualsiasi ragazzino che si rispetti.

Il che lo rende una grossissima incognita per tutti quanti. Non esiste un vero *esperto* di trading su BitCoin, non c'è stato per ora il tempo sufficiente perché questa dichiarazione possa essere surrogata dai fatti. Chi si vanta come tale è un ciarlatano. O un ingenuo. Vedete voi cosa preferite.

In senso lato, per elaborare una strategia di trading realmente affidabile servono

tre cose: 1) tantissimi dati, quindi tanti anni pregressi; 2) molti strumenti finanziari per fare dei contro-test alle nostre ipotesi; 3) una relativa maturità del mercato in oggetto al fine di trarre conclusioni con un minimo di stabilità predittiva.

Insomma, ci serve tutto ciò che serve a qualsiasi scienziato: dati e possibilità di verificare le ipotesi. Ahimè, con BitCoin e le altre criptomonete mancano entrambi questi elementi preziosi.

La crescita del valore di BitCoin sul Dollaro è stata, semplicemente, esplosiva ed eccezionale. Se osservate il grafico della sua storia non c'è stato

un solo momento in cui una persona rigorosa avrebbe potuto ricavare qualche regola statistica.

E senza regole statistiche, non si ottengono strategie di trading esatte e **riproducibili**.

Ecco la verità: qualunque persona avesse investito in BitCoin più o meno a caso nel 95% della sua storia avrebbe guadagnato. Spesso una montagna di denaro. In questi casi non vi serve alcun esperto: vi basta prendere un mulo cieco e investire quando l'animale scalcia tre volte di fila. Sono serio. Ci vuol poco a fare i fenomeni quando le cose vanno bene.

Eppure il diavolo sta nei dettagli: sappiamo solo *dopo* una crescita esplosiva che le cose sarebbero andate alla grande. Non prima. Col senno di poi è facile essere dei maghi della finanza. Per lo stesso principio possiamo essere certi che chiunque vi abbia detto di investire in BitCoin a metà 2017 – cioè quando c'è stato il picco di suggerimenti di acquisto – non vi abbia fatto un gran favore. Perché questo periodo rientra nel 5% della storia dei BitCoin in cui anche un genio del trading avrebbe perso.

Di nuovo: in un mercato così immaturo le previsioni sono **insensate** più del solito. Sia previsioni di crescita che di

decrescita. Non serve a niente analizzare a posteriori cos'è successo. Non serve a niente ricavare regole.

E poi c'è la fluttuazione di cui abbiamo già discusso. L'estrema volatilità di questa moneta. Un altro effetto collaterale (positivo o negativo a seconda dei punti di vista) della sua immaturità. Quando si specula la volatilità è qualcosa di tendenzialmente positivo. Ci fa piacere che un titolo oscilli, così possiamo provare a comprarlo quando costa poco e rivenderlo quando sale di valore. Tanto si tratta di momenti vicini nel tempo per via della stessa ampia fluttuazione. Se sbagliamo le previsioni, sbagliamo in

fretta e possiamo perdere poco e rapidamente. Se facciamo soldi, li facciamo in fretta.

Il tempo è infatti un **benefit**: meno ne usiamo per sbugiardare le nostre ipotesi o per guadagnare, meglio è.

Capiamoci, la volatilità dei BitCoin è davvero smisurata. Al punto da mettere a dura prova qualsiasi speculatore che non disponga di sistemi informatici superprofessionali e *commissioni bassissime*. Solo questi due strumenti permettono di fare trading a ritmi così serrati.

E noi? Cosa possiamo fare vista la situazione? Siamo fuori dai giochi?

No.

Vista l'immaturità, la fluttuazione e il mercato inesistente non possiamo seriamente pensare di seguire un metodo esatto di trading sul BitCoin. Non è credibile. Chi vi vuol vendere una roba del genere è un furfante. Cionondimeno ci è concesso di sfruttare alcune **regole d'oro** classiche della finanza speculativa senza anelare a voler imitare *George Soros*. Cercherò di renderle di facile comprensione e dritte all'osso.

Affare fatto? I patti sono chiari? Avete calibrato le vostre aspettative? Mi promettete che non cadrete mai nelle braccia dei "*sistemi di trading per*

*criptovalute*”?

Andiamo.

# Volete davvero diversificare?

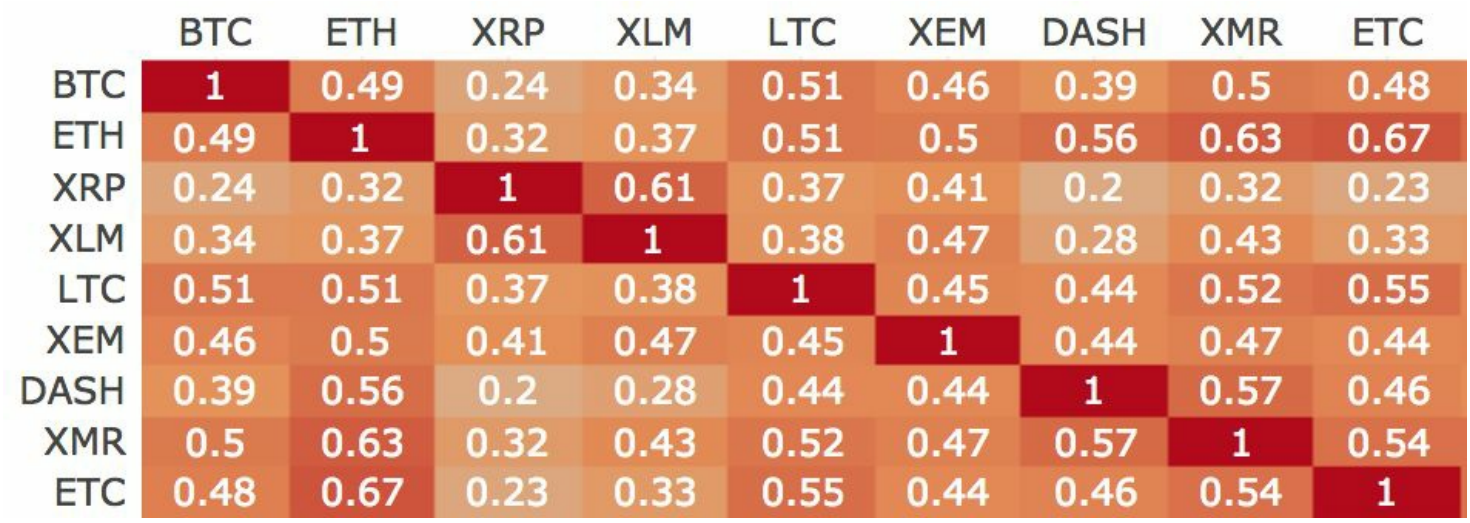
Iniziamo sfatando un mito che pare immortale.

Non vi serve a niente fare trading su **molte** criptovalute. Non esiste un solo motivo per cui dovreste farlo. Sono sicuro vi abbiano sempre detto di *diversificare* il vostro portafoglio e quindi io ora vi stia sembrando un dissennato. Ma una baggianata è una baggianata.

Non ci credete?

Qui potete trovare una bella tabellina sfiziosa che dimostra quanto sia assurdo

diversificare troppo sulle criptomonete. O meglio, quanto sia un modo irrazionale di sentirsi più sicuri: http://bit.ly/crypto_correlations.



| | BTC | ETH | XRP | XLM | LTC | XEM | DASH | XMR | ETC |
|---|---|---|---|---|---|---|---|---|---|
| BTC | 1 | 0.49 | 0.24 | 0.34 | 0.51 | 0.46 | 0.39 | 0.5 | 0.48 |
| ETH | 0.49 | 1 | 0.32 | 0.37 | 0.51 | 0.5 | 0.56 | 0.63 | 0.67 |
| XRP | 0.24 | 0.32 | 1 | 0.61 | 0.37 | 0.41 | 0.2 | 0.32 | 0.23 |
| XLM | 0.34 | 0.37 | 0.61 | 1 | 0.38 | 0.47 | 0.28 | 0.43 | 0.33 |
| LTC | 0.51 | 0.51 | 0.37 | 0.38 | 1 | 0.45 | 0.44 | 0.52 | 0.55 |
| XEM | 0.46 | 0.5 | 0.41 | 0.47 | 0.45 | 1 | 0.44 | 0.47 | 0.44 |
| DASH | 0.39 | 0.56 | 0.2 | 0.28 | 0.44 | 0.44 | 1 | 0.57 | 0.46 |
| XMR | 0.5 | 0.63 | 0.32 | 0.43 | 0.52 | 0.47 | 0.57 | 1 | 0.54 |
| ETC | 0.48 | 0.67 | 0.23 | 0.33 | 0.55 | 0.44 | 0.46 | 0.54 | 1 |

Se non vi è chiaro il suo significato globale rimediamo subito: secondo questi dati le criptovalute si muovono tutte **insieme**. Più una celletta che incrocia il simbolo di due criptovalute tende al colore intenso (cioè più si avvicina a 1, che è il 100%) più le due

monete sono **correlate**. Quando sale una, sale l'altra. Quando crolla una, crolla l'altra.

Da qui la banale conseguenza: se avete acquistato 10 differenti criptomonete (BitCoin, Ethereum, Ripple, BitCoin Cash, Dash, Monero…) perché l'espertone di turno vi ha insegnato a diversificare, e tutte queste belle valutine implodono insieme, che diamine di beneficio vi ha portato questa santissima diversificazione?

NESSUNO. NADA.

Se proprio vogliamo cercare l'aghetto nel pagliaio, risulta che BitCoin e Ripple non siano esageratamente

correlati tra loro visto che presentano un mero 24%. Ma ci scommetto le mie scarpe sportive nuove che si tratta di un effetto transitorio che scomparirà nel tempo. O quantomeno si ridimensionerà. Non sarebbe niente di nuovo sotto il sole. Dinamica vista e rivista.

Da cui la regola: fate trading **solo** su BitCoin o su un'altra delle criptomonete "famose". Se proprio volete aggiungerne una seconda per puro sfizio cercate nella tabella quella con la *correlazione più bassa* rispetto alla valuta già in vostro possesso. Al link http://bit.ly/crypto_correlations trovate molte più criptovalute di quelle presentate nella tabellina di sopra.

# Non in campo aperto

*Come* acquistare le criptomonete? Di solito non è possibile farlo dal vostro conto bancario, anche se avete attivato la funzione di trading.

Il metodo "classico" è di aprire un conto presso un *exchange*, cioè uno dei portaloni web in cui voi caricate Euro con PayPal, bonifico o carta di credito e tramite cui potete poi convertire questa moneta *fiat* in una delle criptovalute disponibili. Gli *exchange* di maggior successo sono di solito quelli che più hanno lavorato sul fronte sicurezza negli ultimi anni: *BitStamp, CoinBase, BitFinex, BTC-e, Kraken* e via così. Vi

basta una ricerca su Google.

Bene. Ora che sapete come fare, vi sconsiglio con tutto me stesso questa strada (!).

Innanzitutto perché fate prima a recarvi a *Lourdes* e a farvi un paio di volte il *Cammino di Santiago* nell'attesa che la vostra richiesta di iscrizione venga presa in carico. Ho provato per voi a registrarmi a quasi tutti questi servizi. Il primo mi ha risposto dopo 3 settimane. Uno si è dimostrato subito attivo per poi bloccarmi l'operatività poco dopo e senza motivi apparenti (auguri col *customer service*!). Gli altri mai pervenuti o risposte sopraggiunte dopo

ere geologiche.

Pensate sia stato sfortunato? Direi di no. Racconti simili arrivano da ogni mio conoscente e da qualsiasi forum online.

Verosimilmente tutti questi *exchange* famosi sono stati sorpresi dal boom delle criptomonete del 2017 e dalle richieste di iscrizione. Ma non sembrano fare molto per arginare i disservizi (nonostante sovvenzioni da capogiro, almeno a leggere la stampa).

In seconda istanza comprare direttamente criptomonete è piuttosto inefficiente. Avete già incontrato il disagio delle alte commissioni (rileggete il capitolo precedente) e la lentezza

delle transazioni, quindi ho poco da aggiungere a questo dato di fatto.

In totale onestà molti *exchange* come CoinBase sfruttano algoritmi di Intelligenza Artificiale per valutare il vostro profilo e permettervi di pre-acquistare BitCoin rapidamente senza passare subito dalla blockchain. È però un trucco temporaneo: prima o poi la vostra transazione dovrà essere approvata dalla blockchain, ma intanto avete un'illusione di velocità.

Questo da un alto tampona il problema, dall'altro però sfiora il ridicolo: tutto il baccano e tutti esaltati per blockchain, proof-of-work, decentramento, hashing,

sha-256, corsa alla computazione più mastodontica, sofisticazione dei problemi matematici, democrazia degli incentivi, varia umanità… e poi alla fine la soluzione più veloce è tornare a un algoritmo automatico centralizzato di verifica dei pagamenti come un circuito *MasterCard* qualsiasi? Ci stiamo prendendo in giro?

Tant'è.

E poi c'è la seconda questione spinosa. Acquistando direttamente criptomonete state partecipando senza saperlo al delirio consumistico di risorse computazionali della blockchain.

*Delirio a cui non **volete** prendere*

*parte visti i disagi ambientali e l'insostenibilità che comporta. Lasciate che i polli si spennino tra loro.*

Ok, tutto chiaro. Quindi qual è la soluzione?

Piuttosto facile in verità, anche se ho paura a rivelarvela.

Ci provo lo stesso, siete lettori intelligenti.

Usate i **derivati**.

TA DAAA! La parolaccia peggiore in finanza! DERIVATI! Ciò che *Warren Buffett* definisce un'arma di distruzione di massa! I nefasti strumenti che hanno

causato la crisi del 2008!

Frank, sei impazzito totalmente o fingi?!

Piano. Riflettiamo un secondo su cosa sia un derivato. Prendo da Wikipedia:

> *Lo strumento derivato o semplicemente derivato in finanza è un contratto o titolo il cui prezzo sia basato sul valore di mercato di un altro strumento finanziario, definito sottostante.*

Di per sé quindi un derivato non è niente di mefistofelico. È un contratto come un altro. Lo attivo quando non intendo acquistare **direttamente** uno strumento finanziario – come un'azione, un'obbligazione o una valuta – per non

avere gli svantaggi derivanti dal possesso, dalla tassazione e dalle transazioni associate, ma voglio comunque **beneficiarne**. E per fare tutto ciò stipulo un accordo con chi questo strumento lo possiede, obbligando costui a rispettare alcune regole.

Regole che possono essere piuttosto banali, ad esempio: "*se lo strumento (come un'azione) cresce 10 Euro, mi dai 10 Euro. Se perde 10 Euro, ti do 10 Euro*". Tutto qui.

Il fatto che i derivati siano stati usati per gli scopi più ignobili non c'entra nulla con la loro straordinaria utilità in senso lato per il sistema liberista. Dovete

mettervi in testa che un derivato di per sé non è buono o cattivo. Sono le regole scritte nel suo contratto e lo strumento finanziario sottostante a fare la differenza.

Per esempio. Nel 2006 o 2007 avrei potuto acquistare facilmente un derivato il cui strumento finanziario sottostante era una matrioska di obbligazioni basate su mutui immobiliari elargiti a persone facilmente insolventi. Derivato a cui poteva essere appiccicata una regola del tipo: "*il possessore di questo derivato godrà di una grossa cedola del 15% annuo, ma perderà tutto l'investimento se il 5% dei mutui saranno insolventi*". Evidentemente in questo caso sarebbe

stata la *mia* ingenua cupidigia (o il mio ottimismo sul mercato immobiliare) il problema, non lo strumento finanziario di per sé. Si tratta chiaramente di un pessimo accordo.

Quindi la ricetta per non essere sbranati da un derivato è piuttosto semplice: prima di acquistarlo dobbiamo capire assolutamente 1) lo strumento finanziario sottostante e 2) le regole di contratto applicate. Se entrambi questi fattori sono chiari, possiamo procedere.

Nel caso dei derivati sui BitCoin di cui stiamo parlando in questo capitolo è tutto piuttosto auto-evidente: lo strumento sottostante è il prezzo di una

criptomoneta in Euro, mentre la regola è un banale comportamento-specchio: "*se BitCoin sale 1 guadagno 1, se cade 1 perdo 1*".

Insomma, come avere un pappagallo finanziario.

Esistono un sacco di portali online che propongono derivati sulle criptovalute. Rispetto agli *exchange* ci forniscono una montagna di vantaggi:

- Sono **snelli**. Non avendo trafile complicate, approvazioni esasperate di sorta, blockchain e affini e trattandosi di servizi dalla solidità ben precedente alla moda delle criptovalute, la nostra vita

diviene facile. Ci iscriviamo rapidamente e ci basta poco per essere considerati clienti affidabili.

- Sono **economici**. Non dovendo acquistare direttamente le criptomonete non dobbiamo pagare le famose commissioni. Ne abbiamo altre (chi ci dà il servizio non lavora gratis) ma sono di solito inferiori.

- Sono **rapidi** in fase di acquisto e vendita. Non essendo costretti a passare da algoritmi complessi e blockchain non c'è proprio niente da approvare visto che il contratto

è istantaneo e avviene tra noi e l'azienda che sta dietro al portale. Se voglio acquistare 0,5 BitCoin tramite derivato mi basta dirlo al sistema e un secondo dopo il contratto è pronto.

La magia della faccenda sta proprio nel concetto stesso di accordo tra le parti. Con un derivato in nessun momento possiedo davvero i BitCoin. Mi limito a stipulare un contratto velocissimo col sito (che possiede i BitCoin) dicendogli: "*Ascolta bene: se il prezzo della valuta sale di 1 tu mi dai 1, se scende di 1 tu ti prendi 1 dal mio conto. Ci stai?*". Tutto questo con due click.

Ovviamente si tratta di trading, quindi ci sono (come già detto) piccole commissioni e una differenza più o meno ampia tra il prezzo di acquisto e vendita, cioè lo *spread*. Ma si tratta dell'ABC di ogni investimento, non cambia nulla rispetto all'acquisto diretto del bene. Si suppone che prima di aprire il borsellino padroneggiate queste dinamiche essenziali. Di nuovo, basta una ricerca su Google. Il sito di formazione finanziaria *investopedia* è vostro alleato.

Questa particolare tipologia di derivato sulle criptomonete viene comunemente definita **CFD** o *Contratto per Differenza* (*Contract For Difference*).

Con un CFD stipuliamo un accordo col sito in questione che ci assicura che i nostri guadagni e le nostre perdite siano ancorati alla fluttuazione dello strumento finanziario sottostante in modo diretto.

Attenzione: ricordate l'importanza di capire le regole prima di acquistare un derivato e di non strafare. Potreste farvi prendere la mano e attivare una **leva**, che significa moltiplicare di diverse grandezze sia i potenziali profitti sia le vostre perdite.

> *Con una leva posso cioè spendere solo 1.000 Euro per acquistare il derivato ma comandare un valore in BitCoin di ben 50.000 Euro.*

*Quindi moltiplicando potenzialmente di ben 50 volte i miei introiti se le cose vanno bene! Ma, allo stesso modo, moltiplicando di 50 volte le mie perdite se sbaglio previsione.*

Per favore. Capisco sia gustosa, ma lasciate perdere la leva per adesso. E, se proprio non resistete, mantenetela a singola cifra. Non volete davvero rimetterci una montagna di soldi se le cose vanno male.

I più famosi broker di derivati in criptomonete sono, ad esempio: *Plus500, eToro, AvaTrade, IG*. Ma anche conti correnti come quelli di *Fineco* offrono cripto-CFD molto

interessanti.

Infine un tecnicismo. Con un CFD potete scommettere sia a favore di una criptomoneta che a sfavore. Nel primo caso la regola che attivate è diretta – *se BitCoin sale 1 guadagnate 1* – nel secondo è inversa – *se sale 1 perdete 1*. Per una questione tecnica di distribuzione dei ritorni di investimento che non ha senso disquisire in questo volume io vi sconsiglio caldamente la seconda opzione. Semplicemente, nel primo caso avete più probabilità di vincere.

# Chi ben specula

Alla luce di quanto abbiamo visto arriviamo alla strategia di trading più sensata. Che non può essere troppo secchiona e stretta in un momento di immaturità del mercato come accade oggi. Dovete vederla piuttosto come una bussola per orientarvi nel caos, non come un algoritmo esatto. Questo vi deve essere chiaro.

Prima di tutto parliamo di **quanto** investire. Quanto dedicare al trading su BitCoin rispetto al vostro capitale?

Il campo del *money management* è multiforme e amplissimo. Qui ci basta ricordare il principio del *bilanciere*,

che consta nell'allocare la stragrande maggioranza del vostro contante su strumenti **sicuri** come conti correnti, conti deposito o obbligazioni di grandi stati nazionali stabili. Mentre dovete indirizzare al trading, di sua natura rischioso, solo una piccola parte del denaro liquido, *intorno al 20%*.

Perché così poco? Perché la vita è imprevedibile e non possiamo scommettere troppo rispetto alle nostre finanze. Non sappiamo davvero quando avremo bisogno di soldi smobilizzati per urgenze. Non possiamo quindi bloccare troppe risorse in investimenti.

Per approfondire e capire il concetto

rimando al volume *Le 3 Formule*. Non sto complottando per vendervi un libro da pochi dinari. Sto cercando piuttosto di salvarvi la pellaccia con una buona dose di anticorpi riversati in un saggio dedicato allo scopo.

Posto che probabilmente avete già qualcosa di investito in fondi, ETF o azioni, resta di sicuro pochino di questo 20% da dedicare ai BitCoin. E va bene così. Sarebbe folle andare *oltre qualche migliaio di Euro* da bloccare nel gioco delle criptomomente visto che si tratta di un'avventura.

Il tipo di investimento in BitCoin di cui stiamo parlando è **speculativo**, cioè

ottimizzato sul breve termine. Non abbiamo alternative visto il caos delle valutazioni di mercato delle criptomonete e la loro fanciullaggine. Non ci possiamo cioè concedere la relativa serenità di un investimento classico, come quelli che possiamo operare su fondi e ETF.

Ripeto per i duri di orecchie: i consigli che sto per darvi per questa particolare tipologia di speculazione sono da interpretare e applicare con stile, flessibilità e attenzione, non si tratta del codice di *Hammurabi* da divinizzare come oro colato. Il mio **disclaimer** è quindi totale e non voglio poi sentire tante storie: in assoluto *non consiglio* la

speculazione a nessuno che non sia un trader professionista o esperto. In particolare la speculazione su qualcosa di relativamente alieno come i BitCoin. È un argomento difficile che richiede anni di studio e strumenti adeguati, soprattutto psicologici.

> *D'altra parte capisco quanto sia irresistibile approfittare delle criptovalute per divertirsi e arrischiare qualcosa. Mi è altresì chiaro che se non vi do io qualche dritta andrete poi a farvi turlupinare da qualche furbastro con sistemi di investimento suicidi; è troppo difficile tenersi lontani dal miele. Ecco perché ho*

*scritto questo capitolo.*

Ergo.

Continuate la lettura a vostro rischio e pericolo ricordando che si tratta di un **gioco** da casinò. Da intraprendere con testa e protezioni che vi aiuterò a sviluppare.

Se siete ancora qui, iniziamo.

Un buon modo di acquistare e vendere in un mercato così movimentato e volatile come quello delle criptovalute è sfruttare una linea di **supporto** dei prezzi che indichi il trend di movimento e dia una indicazione di massima sulla direzione della moneta verso l'alto o verso il basso. Il sistema in assoluto più

nerboruto, semplice e testato dalla storia è la **media mobile**.

Che è uno strumento piuttosto elementare: ogni giorno basta calcolare la media dei prezzi degli ultimi *tot* giorni - dove "*tot*" è un parametro che dobbiamo stabilire. Potete farlo addittura con Excel.

Più agevole da capire se la disegniamo direttamente su un grafico dei prezzi:


La linea in alto molto frammentata è il prezzo in Dollari di BitCoin, quella sottostante più levigata è la media mobile a 20 giorni. Ogni giorno viene cioè determinato il valore aritmetico intermedio dei prezzi di BitCoin dei 20 giorni precedenti. Per questo è una curva così "liscia".

Capite dal grafico perché viene definita *linea di supporto*? Il suo scopo è di

farci stimare continuamente da che parte stiamo dell'andamento dei prezzi: in salita o in discesa? Solitamente non è mai un gran bel segnale quando il costo di uno strumento finanziario *valica* questa bella curva dirigendosi verso il **basso**: potrebbe certamente oscillare e tornare in su, ma ci sono buone possibilità che sia piuttosto in una maratona discendente suicida.

Per questo la media mobile è un indicatore adorato dagli speculatori. Non è matematica e la predizione non è assoluta (concetto che non esiste nei mercati) ma *statisticamente* ha le sue ragioni.

Che dobbiamo quindi farci con la media mobile? Qualcosa di piuttosto agevole.

Quando il prezzo di BitCoin interseca *dal basso verso l'alto* la media mobile e questa non è in evidente discesa, è probabilmente il momento di **acquistare** un CFD. I più moderati possono attendere qualche giorno per verificare che la tendenza sia reale e non una piccola fluttuazione.

All'opposto, quando il prezzo di BitCoin sta arrivando alla fine di una folle corsa verso le stelle e rimbalza sul soffitto o, magari più sobriamente, quando notiamo che taglia *dall'alto verso il basso* la media mobile e che

questa è inclinata in giù, è presumibilmente venuto il momento di **vendere** il nostro CFD.

A questo dobbiamo aggiungere un'altra condizione: *il limite massimo di perdita* consentita. **Prima** di acquistare dovete decidere quanti soldi potete buttare nel cestino se la vostra strategia dovesse rivelarsi errata. Mantenere in portafoglio una criptovaluta che sta crollando è una pessima idea perché non possiamo davvero sapere quanto è profonda la tana del bianconiglio (cit.).

Stabilite una perdita massima per ogni scommessa di acquisto. Più basso è questo numero, più volte potrete giocare

perché manterrete per più tempo il patrimonio se per tanto tempo le puntate fossero sfavorevoli. Può capitare.

> *La media mobile non ci farà mai acquistare a un minimo o vendere a un massimo. Non funziona così, dobbiamo sempre lasciare qualcosa sul banco. Entreremo in una posizione quando il prezzo è già salito e usciremo poco prima che probabilmente torni a risalire. Pace. La speculazione ha le sue regole.*
>
> *Se siete troppo avari o avete un attaccamento carnale ai soldi questo esercizio non fa per voi.*

Potete usare il livello del *volume* per

verificare se ha senso o no acquistare un CFD. Lo trovate sotto a ogni grafico; questo amichetto vi indica la **quantità** di scambi in un certo periodo. I grandi movimenti verso l'alto o verso il basso di uno strumento finanziario sono molto spesso anticipati e supportati da un innalzamento del livello di questo indicatore. "*Molto spesso*" non vuol dire "*sempre*". Ci siamo capiti?

Ora qualche dettaglio.

*Quale* media mobile usare? Visti gli enormi ondeggiamenti di BitCoin consiglio di testare una media breve: a **10, 20** o al massimo **50** giorni.

Ma dovete capire che nessuna media

mobile sarà sempre perfetta in ogni situazione. In molti casi l'indicatore vi farà acquistare oggi e vendere tra pochi giorni con una perdita per via della volatilità. Eppure vi assicuro che la **consistenza** vince sul lungo termine: se iniziate con una media mobile di – ad esempio – 20 giorni, non dovete assolutamente cambiarla dopo qualche mese di mancata performance perché potrebbe essere proprio quello il momento in cui inizia a funzionare alla grande. I grandi trader non fanno questi errori da pivelli.

Ognuno dei broker di CFD che ho citato poche pagine fa ha un pacchetto grafici di alta qualità tramite cui è facilissimo

attivare l'indicatore della media mobile. Provate a disegnare sul grafico medie a 10, 20 e 50 giorni e cercate di capire, su vari periodi storici e su varie criptomonete, quale orizzonte temporale risponda meglio al vostro stile.

Tenendo ben a mente che una media più *lunga* (come quella a 50 giorni) sarà più **resistente** al "rumore" e ai piccoli increspamenti, ma vi darà anche meno segnali, potenzialmente facendovi perdere dei soldini potenziali. Ovviamente per una media cortissima vale il principio opposto. È tutta questione di *trade-off* e di stile personale. Non esistono merende gratis nel trading!

So che a questo punto volete delle rassicurazioni.

Posso promettervi che con questo indicatore farete un sacco di soldi? No. Posso promettervi che non perderete per cinque volte di fila? No. Posso promettervi qualcosa in assoluto? No, no e no. Se non che la media mobile è una vecchia signora di cui fidarsi, ma ha i suoi acciacchi e non può garantirvi proprio nulla perché è molto religiosa e odia lo spergiuro.

Esistono tanti altri metodi alternativi e strategie sofisticate. Ma ne vale la pena? Il gioco vale la candela? A questo livello di evoluzione di BitCoin siamo

in totale *far-west* e la verità è che non esiste nessuno che possa promettervi alcunché.

Se siete ansiosi di speculare ma avete un grillo parlante nell'orecchio che vi raccomanda di usare giudizio, prima di acquistare davvero un CFD seguendo la media mobile potete per qualche tempo testare la vostra strategia con soldi **virtuali**. Si chiama *paper-trading* ed è la migliore invenzione umana dopo le brioches acero e noci. Ogni broker di CFD propone questa opzione. In alcuni casi si chiama "portafoglio simulato". Divertitevi.

In definitiva.

Se proprio volete investire in BitCoin fatelo speculando con poche e semplici regole, flessibilità, pazienza e spirito sportivo, sapendo che nessuno ha la bacchetta magica e non troverete mai santoni con potere di divinazione.

- Comprate *solo* quando il prezzo della moneta se ne sta bello-bello sopra la vostra media mobile prediletta a 10, 20 o 50 giorni. Non è *rocket-science* ma solo cara e vecchia statistica.

- Cercate di non avere posizioni aperte se il prezzo sta sotto questa curva magica. È piuttosto pericoloso.

- Stabilite un limite massimo alle perdite per singola giocata. E visto che ci siamo, ricordate che sì, è davvero una “giocata”. Come al casinò.

- Potete ottenere una conferma della “*forza*” della direzione del prezzo di BitCoin adocchiando il livello del volume sotto alla maggior parte dei grafici.

- Dedicate a questo sport d’altura una percentuale *piccolissima* di tutti i vostri contanti.

- In generale non esagerate con l’autostima e l’ottimismo: non allocate sull’ammontare degli

investimenti finanziari pazzerelli più del 20% dei vostri liquidi.

- Sfruttate il *paper-trading* per fare esercizio prima di indossare lo smoking e varcare la soglia del casinò.

Riassumo il tutto con una delle mie metafore.

Se volete buttarvi da un biplano fatelo pure. Ma mettetevi quel dannato paracadute infagottato nello zaino dietro al pilota. In questo capitolo avete imparato a farlo aprire in sicurezza.

# In sintesi

- Nella rete BitCoin esistono due ruoli: i miner della blockchain e gli utenti che si scambiano denaro.

- I primi guadagnano presentando la proof-of-work nella battaglia all'ultimo sangue delle validazioni. Ma è un lavoro sporco e esasperato permesso solo se si possiedono tecnologie costose e sofisticate. Alla maggior parte di noi semplicemente non conviene, neanche passando dai "consorzi" di minatori, i ring.

- Tutti noi possiamo sfruttare la rivoluzione in modo più furbo, cioè

col trading.

- Non è uno sport facile e ci vuole parecchia esperienza. Inoltre su BitCoin siamo penalizzati per la scarsa maturità del mercato da cui la mancanza di regole statistiche robuste.

- Il trading su BitCoin si fa speculando *e non* investendo, viste le fluttuazioni notevoli e i punti di domanda sul suo futuro. Investire è una cosa, speculare un'altra. Quest'ultima è un'attività simile all'azzardo e quindi riservata a chi cerca emozioni forti.

- Per chi non è pronto alla

speculazione (e in verità per quasi tutti) è consigliabile dedicarsi a solidi investimenti in fondi e ETF tramite formule consolidate e testate.

- Non occorre seriamente diversificare quando si specula sulle criptomonete tranne rare eccezioni effimere. Si tratta di strumenti finanziari molto correlati tra loro e che si muovono insieme. Sarebbe una diversificazione solo di facciata e non sostanziale.

- È imprudente acquistare direttamente criptovalute da un exchange; è molto più efficiente e

rapido passare da strumenti derivati come i CFD.

- Nella nostra speculazione possiamo sfruttare un indicatore famoso nel trading: la media mobile. Vista la volatilità delle criptomonete conviene mantenersi su medie mobili “corte” a 10, 20 o 50 giorni.

- Se il prezzo della criptomoneta è sotto la media mobile è opportuno star fuori dal mercato. Se è sopra, può aver senso acquistare. Facendo attenzione anche all’inclinazione della media mobile e al volume di scambi.

- La consistenza in questo gioco è tutto, e sapere già quanto si è disposti a perdere vale ancora di più.

# BITCOIN E I SUOI FRATELLI

# Senza domani?

C’è una domanda che fin troppi si pongono preoccupati a proposito di BitCoin: questa regina delle criptovalute è davvero a *prova di futuro*?

La sua capitalizzazione totale direbbe di sì: gli scambi in BitCoin sono a quota 190 miliardi di Dollari. Niente rispetto alle valute *fiat* più importanti, ma parecchio nei confronti degli altri concorrenti. BitCoin gode perciò di un reale vantaggio competitivo e di una accumulazione selettiva degli investimenti che ne ha decretato la posizione dominante, probabilmente per un lunghissimo futuro.

Ma questa leadership è figlia della superiorità reale di BitCoin o piuttosto di alcuni accidenti positivi fortuiti che prima o poi saranno risolti, come la mancata tassazione e controllo da parte degli stati?

C'è di più.

L'oggettiva insostenibilità ambientale di BitCoin e della proof-of-work della sua blockchain quanto può essere sopportata ancora da una società evoluta? Fin quando le nazioni accetteranno un tale irrazionale inquinamento in un momento storico in cui le istituzioni fanno carte false pur di impegnarsi in progetti di riduzione delle emissioni, e lo stesso

Trump è aggredito da ogni fronte per le sue posizioni anti-ambientaliste?

La lentezza esasperata e la facilità di congestione della blockchain sono ammissibili fin quando non si chiede a BitCoin di diventare una moneta "vera" capace di fungere da riserva di valore e strumento di pagamento per la popolazione allargata. Insomma, finché non lo consideriamo un serio competitor di *Visa*. Ma se – come molti cripto-evangelisti auspicano – una massa di persone domani iniziasse a usare seriamente BitCoin oltre ai fini speculativi, quanto reggerebbe il sistema? Quanto sarebbe usabile e scalabile?

Per non parlare poi delle commissioni. Quanto può seriamente fiorire un ecosistema che pretende commissioni via via più alte all'aumentare del traffico? Quanto allegramente una persona può accettare di non avere un "*piano balzelli*" chiaro e trasparente nelle sue spese giornaliere?

Come la prendereste se ogni prelievo al bancomat o ogni pagamento al supermercato o al bar avessero commissioni totalmente casuali che dipendono non dall'entità della spesa ma dal traffico totale della rete di pagamenti?

"*Barista, un caffè grazie, pago in*

*BitCoin”. “Benissimo signore. Il caffè è 1 Euro o 0,0001 BTC, mentre le commissioni per il pagamento a suo carico sono 50 Euro, o 0,006 BTC. In tutto fanno 51 Euro o 0,0061 BTC*”.

Seriamente? Vogliamo questo futuro?

Ritengo che BitCoin sia qui per restare, ma non ho problemi ad ammettere si tratti di una tecnologia non scalabile e piuttosto ottusa. È stata concepita in modo lucidissimo sul breve e medio termine, ma totalmente maldestro sul lungo.

Tutti stimiamo e applaudiamo *Nakamoto*, eppure ci vuole l’onestà intellettuale di riconoscere i limiti del

suo pensiero. Forse lui (o loro) tutto sommato è come noi, non propriamente un genio del calibro di Einstein.

Fortunatamente BitCoin ha scatenato la famosa lampadina delle idee e dal 2010 in poi siamo stati inondati da barlumi di criptopensiero più moderni e a prova di futuro. Menti brillanti di ogni nazione hanno concepito e spesso realizzato miglioramenti di BitCoin e criptovalute alternative che ci terranno probabilmente compagnia per molti anni.

È invece piuttosto prematuro discutere in questa sede di *Lighting Network* e dei miglioramenti architetturali ipotizzati o

in fase di test sullo stesso BitCoin. C'è già stato molto fermento sulla questione al punto che nel corso degli ultimi anni abbiamo assistito a veri e propri sdoppiamenti di BitCoin in altre valute che constano in trasformazioni più o meno rilevanti del BitCoin originale.

Per definire tali interventi si usa il termine informatico **fork**, cioè biforcazioni.

Abbiamo avuto fork sia sul software di BitCoin – con *BitCoin XT*, *BitCoin Classic* e *BitCoin Unlimited* – sia sul funzionamento profondo della blockchain – con i famosi *BitCoin Cash* e *BitCoin Gold*. Ogni fork promette

grossi miglioramenti e risoluzione di problemi rispetto al ramo originale della più famosa criptovaluta al mondo.

Ritengo tuttavia più interessante e produttivo concentrare le nostre risorse mentali su altre criptovalute originali *non derivate* da BitCoin. Si tratta di mondi a volte inattesi e intriganti che rimescolano le carte del cripto-universo e sin dalla loro concezione scommettono su approcci e idee totalmente differenti dal capostipite.

Molte di loro sono *già* a prova di futuro e ci possono regalare un affresco brillante del domani.

Zaini in spalla. Si parte.

# Ethereum

Con una capitalizzazione di 116 miliardi è il degno concorrente di BitCoin. Anche se, a dirla tutta, se BitCoin è un'automobile, Ethereum assomiglia più a una fabbrica in grado di creare qualsiasi oggetto, dalle auto ai grattacieli.

Il suo creatore, *Vitalik Buterin*, nel 2013 era un giovane ricercatore piuttosto invischiato nel mondo delle criptovalute, al punto da accettare con entusiasmo di farsi pagare per il suo lavoro di giornalista tecnologico non in Dollari, ma in BitCoin. Scelta azzardata in un mondo in cui le bollette si pagano

ancora con moneta *fiat*.

Vitalik si è presto accorto dell'insostenibilità e della grettezza del modello BitCoin. Per questo ha iniziato da subito a elaborare e diffondere la sua visione di una blockchain universale più intelligente. Non limitata alle sole transazioni finanziare, ma in grado di gestire la validazione di qualsiasi oggetto digitalizzabile afferente scambi o contratti.

Mr. Buterin non era solo un candido pensatore. La sua eccezionale competenza nello sviluppo software l'ha portato a dare una iniezione di adrenalina all'intero progetto cercando

di concretizzarlo il prima possibile. Grazie ad una prima bozza di codice pubblicata sul famoso portale open-source *GitHub* è riuscito a circondarsi rapidamente di altri programmatori talentuosi e ad ottenere un magnifico finanziamento nel 2014 per il lancio del primo concorrente autorevole di BitCoin. Da lui nominato **Ethereum**.

La modalità da lui sfruttata per ottenere questo finanziamento dalla comunità degli entusiasti di criptomonete è diventata recentemente piuttosto diffusa in giornali e trasmissioni televisive.

Si è trattato di una cosiddetta **ICO** – *Initial Coin Offering*: "offerta

preventiva di monete". Tramite una ICO un'azienda opera in effetti una sorta di prevendita di future criptomonete. Gli interessati forniscono liquidità istantanea agli sviluppatori sotto forma di Dollari in cambio del diritto ad essere tra i primi possessori della futura valuta che la stessa azienda sta forgiando. Con la speranza che questa funzioni e segua le sorti di BitCoin, acquistando valore alla velocità della luce, rendendo tali primi acquirenti ricchissimi.

L'ICO di Ethereum ha permesso ai suoi acquirenti la prenotazione di ben 12 milioni di future cripto-monete, che rappresentano ancora oggi circa il 13%

del parco circolante. Il giochino aveva perciò mostrato da subito il suo potenziale.

L'idea importante da portarsi a casa su Ethereum è che spinge la nozione di blockchain alla sua ennesima potenza. Mentre BitCoin nasce e si sviluppa solamente e orgogliosamente come moneta, Ethereum è multipotenziale sin nel midollo. Sarebbe a dire che la sua blockchain può essere – e vuole essere – sfruttata per **ogni applicazione** possibile in cui sia richiesta la presenza di una terza parte neutrale che faccia da garante. Non solo per il trasferimento di soldi.

Il caso più ovvio di una blockchain non propriamente finanziaria è in ambito legale. Nel mondo pre-Ethereum non abbiamo molte alternative a avvocati, notai e studi legali quando dobbiamo stipulare un contratto e essere poi certi che le sue condizioni vengano rispettate. Con Ethereum non ci serve niente di tutto ciò. La sua blockchain non solo è il garante oggettivo, *super-partes* e neutrale per definizione (per sua stessa architettura non può manipolare o sparigliare le carte). Ma trattandosi di un software avanzato può essa stessa innescare le operazioni che normalmente si attivano quando una parte non rispetta ciò che ha firmato.

In totale onestà c'è un po' di confusione in giro su questo aspetto. I guru e gli "strateghi" si sbracano a forza di lodi e paroloni in blog, alla macchinetta del caffè e su YouTube a proposito di questi contratti digitali tecnicamente definiti *smart contract*. Ma non ho sentito un solo esempio verosimile. Insomma, solito stile da venditori di aria fritta.

Proviamo a fare chiarezza con un caso reale.

Immaginiamo di vivere in un mondo in cui Ethereum sia uno standard legale. Supponiamo io voglia acquistare una casa con un mutuo; vado dalla mia banca di fiducia e accetto il preventivo. Mi

viene chiesto se preferisco passare da un avvocato/notaio o dalla blockchain. Opto per la seconda per via delle spese nettamente inferiori e per la rapidità di esecuzione. Tramite uno *smart contract* attiviamo nella rete di Ethereum delle **regole** che definiscono il mio legame con la banca e con il mutuo da me richiesto.

A questo punto la rete Ethereum inizia a lavorare per me e per la banca verificando incessantemente le condizioni inserite e le azioni da compiere.

Le regole continuamente calcolate e testate dalla blockchain possono essere

semplici come "*adegua la rata al tasso BCE*" o sofisticate come "*alla quinta rata non pagata trasferisci la proprietà della casa all'ente X, sposta Y soldi dal conto del cliente alla banca e blocca il suo wallet sinché non riprende il pagamento*". Si può andare ben più in là: se la porta di casa ha un lucchetto digitale biometrico o con chiave elettronica, la rete può automaticamente bloccarne l'accesso per l'inquilino insolvente sino a nuovo ordine.

Si noti che tutto questo sarebbe totalmente automatico e costituzionale per via dell'affidabilità e imparzialità intrinseca della blockchain. Un tale utilizzo della cripto-rete permetterebbe

di eliminare buona carte dei cavilli, delle spese legali e dell'operatività infausta legata a ogni contrattualistica civile. Un vero cambiamento di paradigma. Brutta notizia per avvocati e notai, splendida news per noi.

A forza di rovistare la rete col lanternino in cerca di qualche start-up che avesse proposto almeno un accenno di servizio di questo tipo ho scovato *Propy*. Questi ragazzotti (capeggiati da una tizia a dir poco tosta) si stanno proponendo nientepopodimeno che come sostituti del registro del catasto e di tutta l'infinita contrattualistica indispensabile nella compravendita internazionale di case. Il loro garante è una blockchain in

stile Ethereum, quindi a base di smart contract. Propy è tutt'ora in fase di lancio e niente è certo, ma sul loro portale propongono già una bella offerta di immobili a San Francisco, Los Angeles, Dubai, Auckland e Pechino.

La proposta di Propy non si può definire proprio cristallina, specie per le implicazioni giuridiche. Da questo paragrafo trovato sul loro sito possiamo però percepire la commistione di speranza e realismo entro cui questo intero cripto-mondo si culla (traduco dell'inglese):

> *Propy mira a risolvere i problemi delle transazioni immobiliari*

*internazionali creando un nuovo servizio unificato e una piattaforma globale. Inizialmente il registro di Propy rispecchierà fedelmente i catasti locali in cui sono registrati i trasferimenti di beni immobili.*

*A lungo termine, tuttavia, la nostra aspettativa è che le giurisdizioni cittadine adotteranno il registro di Propy come loro catasto ufficiale in modo tale che il semplice inserimento di un immobile sul registro di Propy costituisca in effetti il trasferimento legale della proprietà [senza la necessità di*

*ulteriori azioni e contratti cartacei o con altri enti].*

Insomma: per quanto ce la raccontiamo, oggi gli smart contract sono ancora nel mondo ideale. Ma qualcuno inizia a crederci davvero.

Torniamo a Ethereum.

Trattandosi di un network multipotenziale, anche Ethereum ha prodotto una sua criptovaluta, l'**Ether**. Ha alcune notevoli differenze con BitCoin:

- I blocchi vengono processati ogni 15 secondi e non ogni 10 minuti come per BitCoin. Quindi Ether è per suo stesso disegno più rapido

nella verifica delle transazioni.

- Non è deflattivo: il rilascio di nuove monete non si dimezza ogni 4 anni.

- Le commissioni sono generalmente molto più basse. A dicembre 2017 la commissione mediana si aggirava sui 33 centesimi di Dollaro, decine e decine di volte inferiore a BitCoin.

E soprattutto, per nostra grande gioia, Ethereum ha un grandissimo obiettivo morale e intellettivo: abbandonare nel medio termine la follia del proof-of-work e tutti i costi energetici e ambientali che impone. Arrivando a un

modello alternativo: la **proof-of-stake** ("prova di partecipazione").

Non intendo dedicare un intero capitolo alla proof-of-stake, quindi limitiamoci a comprenderne l'ossatura ideologica. Se nella proof-of-work venite ricompensati con nuove monete in proporzione alla vostra quantità di **fatica** computazionale e al dispendio elettrico, nella proof-of-stake le cose sono più semplici. La rete vi "paga" valutandovi con un mix di criteri decisi **a priori** e non determinati dalla vostra bravura nel risolvere puzzle matematici. Criteri come: casualità di assegnazione, anzianità di utilizzo o di possesso di monete, potenza tecnica potenziale della vostra infrastruttura

informatica, voto all'interno di una schiera di delegati (concetto spaventosamente simile alla storiella del pianeta *e*). E via così.

Se non siete sociopatici e il vostro scopo non è ridurre l'atmosfera a un forno a microonde, probabilmente siete spontaneamente più attratti dalla proof-of-stake rispetto alla proof-of-work. E vi stimo per questo. Dovete però capire che la faccenda è prodigiosamente complicata allo stato attuale e tutto è un gran polverone e un ribollire.

Ethereum, ad esempio, per ora ha una sorta di modello misto. Ma il suo scopo a medio termine è superarlo in ottica

proof-of-stake pura grazie ad un concetto ancora più ingarbugliato definito **Casper**, come il fantasmino del film. Con Casper, la probabilità che voi, nel ruolo di nodi della blockchain, siate ripagati con monete e transazioni è direttamente proporzionale a quanti Ether (che vi ricordo essere la valuta di Ethereum) *bloccate* per la durata della validazione dei blocchi. Un po' come con un conto deposito: più soldi immobilizzate per più tempo, più la rete sarà disponibile a ricompensarvi.

Il concetto di "*stake*" (partecipazione) della proof-of-stake in fondo è tutto qui. La rete ti premia sulla base di **quanto ci tieni** alla causa al punto da bloccare i

tuoi averi per essa. Mentre la proof-of-work è più muscolare: ti ricompensa sulla base delle tue misure. Pensatela come volete, ma ritengo il primo modello più atto a disincentivare fraudolenti e furbastri rispetto al secondo.

Per i fan tecnici della questione “proof-of-stake” consiglio questa ulteriore lettura: http://bit.ly/proof-of-stake-faqs.

# Ripple

Se la forza di Ethereum è il suo proporsi come piattaforma universale, Ripple sta appollaiato dall'altra parte del continuum. Si vende cioè come uno specialista assoluto. Specialista delle **transazioni tra** le grandi istituzioni finanziarie.

Il problema di partenza è molto sentito: oggi un pagamento internazionale tra banche e affini può richiedere *giorni* e ha costi piuttosto elevati, che inevitabilmente si scaricano sui clienti in termini di commissioni e tempistiche esagerate. Tutto sommato se si tratta di grossi trasferimenti di denaro le cose

sono accettabili, ma nel caso di micro-transazioni non ha assolutamente senso.

Ripple sta provando a dare una soluzione nerboruta basata sulla sua blockchain e la sua criptovaluta. Le istituzioni possono usare queste monete virtuali per ottenere liquidità istantanea, ci penserà poi lo stesso Ripple a fare da "ponte" tra le valute *fiat* in entrata e in uscita dalla transazione.

Insomma: se oggi due banche ci mettono giorni per scambiarsi centinaia di migliaia di Dollari in un trasferimento internazionale, tramite Ripple il pagamento sarà istantaneo (4 secondi stimati) perché la moneta stessa e il suo

circuito faranno da vettore tra le due realtà.

Molti commentatori dotati tracciano il parallelo tra Ripple e la rete *Hawala*, un sistema di trasferimento internazionale di denaro decisamente analogico impiegato nel mondo islamico sin dall'ottavo secolo. L'Hawala è propriamente descritta come un sistema di trasmissione di denaro *senza trasferimento* di denaro.

Un controsenso? No. Un'idea fantastica.

Supponiamo siate a Dubai e vogliate inviare a un vostro amico di Mumbai 100 Dollari (in valuta locale) tramite la rete Hawala. Per prima cosa dovete

recarvi da un agente locale a Dubai, un cosiddetto *hawaladar* e fornirgli il denaro e un codice segreto in stile password da voi deciso. Inviate lo stesso codice al vostro conoscente. L'agente di Dubai contatta quindi un suo collega a Mumbai, che avvisa a sua volta il vostro amico: "*c'è denaro per te!*". A questo punto l'amico si reca dall'hawaladar di Mumbai, comunica la password a mo' di verifica e incassa il dovuto in valuta locale meno un costo di commissione. La vostra transazione è conclusa, e i due hawaladar si accorderanno in seguito per il trasferimento reale dei soldi.

Adoro i corsi e i ricorsi storici.

# Cardano e Iota

Queste non sono criptomonete troppo famose e la loro capitalizzazione è ancora contenuta. Ma sono di gran lunga più interessanti degli altri concorrenti di BitCoin non trattati in questo libro, come *BitCoin Cash* e *LiteCoin*. E ci possono dire molto sul nostro domani. Per questo motivo ho deciso di dedicare a loro l'ultima parte di questa sezione del volume.

Partiamo da **Cardano**.

Se BitCoin è una blockchain di prima generazione e Ethereum di seconda, Cardano si adorna di modestia dipingendosi come di *terza* generazione.

Nientedimeno. Ma ha probabilmente buoni motivi per essere così poco sobrio nella sua certificazione di autostima.

Nato in seno alla fervente comunità di Ethereum, Cardano si è presto distaccato per i suoi intenti ancora più splendenti e sfidanti. Prima di tutto si tratta dell'unica criptovaluta manifestamente votata al metodo scientifico: ogni suo aspetto tecnico e teorico viene vagliato costantemente in stile **peer review** da uno stuolo di ricercatori, sempre ben felici di segnalare debolezze e potenziali ostacoli.

Quindi *solidità concettuale* come

binario principale. Se ritenete si tratti di puro esercizio di stile è meglio rileggiate il capitolo dedicato alle sviste progettuali che stanno minando il futuro di BitCoin.

Cardano ovviamente implementa la proof-of-stake e non la proof-of-work (avevate dubbi?), e lo fa con un'architettura ancora più sofisticata degli altri come Ethereum con Casper.

Il sistema permette agli attori della blockchain di non essere costretti a ricopiare e mantenere sincronizzato tutto il registro su ogni nodo. Allo stesso tempo consente di minimizzare a livelli estremi il consumo energetico totale

grazie ad una rete globale composta da tante piccole reti governate da leader locali. Ogni leader ha la responsabilità di verificare e validare le transazioni della collezione di nodi a lui assegnati. E solo se tutto è confermato in locale può inviare alla blockchain mondiale le transazioni.

Questo sotto-raggruppamento computazionale tende a essere di gran lunga più efficace di una blockchain pura in cui tutti i nodi mondiali sono allo stesso livello, ma è di più complessa creazione e gestione. Vedetelo come un modello misto tra gli efficientissimi sistemi centralizzati delle istituzioni che maneggiano valute *fiat* e la democrazia

classica delle criptovalute.

Non solo Cardano sulla carta è una scheggia in termini di validazione delle transazioni e non avrà mai – si spera – i guai di imbottigliamento di BitCoin e affini. Ma questa sua architettura semidistribuita lo rende pure energeticamente super-efficiente e tutt'altro che sprecone di risorse. A beneficio in prima istanza delle commissioni, che saranno verosimilmente sempre molto contenute.

In ultima istanza, gli obiettivi sproporzionati di Cardano si manifestano anche nella sua visione di diventare una sorta di "*meta-moneta*

*virtuale*", capace cioè di proporsi come mediatore tra ogni possibile scambio tra *qualsiasi* criptovaluta mondiale presente e futura. Necessità tutt'altro che malcelata dagli utenti, che sono oggi costretti a transitare da vari *exchange* differenti (con relativi balzelli) quando vogliono convertire un BitCoin in un'altra moneta meno famosa.

Caro Cardano, sarai pure poco umile, ma ci piaci.

Terminiamo con **Iota**, una criptovaluta piuttosto pazzerella e in un certo senso assurda.

Con Iota siamo alla minimizzazione più totale e verace. Software asciutto,

consumi da pettirosso, validazioni minime, blockchain fondamentalmente inesistente. Se fossimo dei precisetti avremmo più di qualche scrupolo a definirla davvero una criptovaluta. Ciò non toglie che lo sia.

Partiamo dall'elemento a prima vista illogico e contrario a gran parte di quello che abbiamo imparato nelle scorse pagine. Iota *non ha* una blockchain. O meglio, ce l'ha, ma coincide con gli utenti comuni. Vi ricordo infatti che ogni criptomoneta opera una netta distinzione tra chi vuole trasferire soldi o attivare contratti e chi li valida. I primi sono gli utenti, i secondi i nodi della blockchain, non se

ne scappa. Con Iota invece i due concetti **si miscelano**.

È piuttosto elettrizzante a dire il vero. Tra tutte le criptomonete, Iota è l'unica che abbia solleticato entrambe le mie anime: quella dello sviluppatore tecnofanatico e quella dell'umanista sociologo.

Il trucco di Iota si chiama **Tangle**, ed è l'ultimo termine che imparerete in questo libro. Potete tirare un sospiro di sollievo! Questo algoritmo matematico assicura un flusso esatto di *dare-avere* tra tutti gli utenti della piattaforma in modo che nessuno possa fare il furbo, senza però rinunciare alla sicurezza

delle blockchain e alla rapidità delle reti decentrate.

Riducendo la spiegazione al minimo sindacale, se volete operare una transazione con Iota il vostro *wallet* (o la vostra app, molto più verosimilmente in questo caso) deve prima **verificare** due transazioni di altri utenti. Tutto qui? Yes. E no, non serve che su ogni dispositivo ci sia la copia dell'intero registro di transazioni come nelle altre criptomonete.

Perché questo congegno meraviglioso funzioni è prima necessario che Tangle sia perfettamente messo a punto. Un concept di questo tipo viaggia sul filo

del rasoio della sofisticazione tecnologica estrema perché scarica sull'algoritmo la valutazione dell'affidabilità degli utenti a cui far vagliare di volta in volta le transazioni. Ma siamo in dirittura di arrivo su questo fronte, sempre più ricercatori brillanti – tra cui molte teste d'eccezione dell'*MIT* – stanno convergendo su Iota e la risoluzione dei bug procede a ritmo serrato.

Pensate alle **conseguenze** di un approccio del genere.

Con Iota abbiamo una *vera* valuta che tuttavia non necessita né di mining, né di grosse fatiche, né di attori dedicati alla

sola validazione. Attori che in qualche modo negli altri sistemi devono sempre essere incentivati e sussidiati. Attori che senza colpa creano le condizioni per colli di bottiglia e costringono algoritmi complicati come Cardano a creare sotto-reti di inaudita complessità topografica.

Con Iota avviene l'esatto opposto di quello a cui siamo abituati con le blockchain: se generalmente alla crescita degli utenti una cripto-rete si ingolfa e deve convincere sempre più persone a partecipare alla blockchain per compensare (ricordate le transazioni altissime di BitCoin!), con Iota all'aumentare degli utenti la rete si **velocizza** perché all'atto pratico ogni

nuovo cliente è un centro di elaborazione ulteriore! Si tratta del cosiddetto *network-effect*, lo stesso principio che ha reso Facebook un'azienda che macina fantastiliardi.

Ultima riflessione: Iota si può permettere di avere **zero** commissioni. Sembra un discorso politico di Silvio Berlusconi, ma è la mera conseguenza dell'architettura di Tangle.

Iota ha nel suo nome "I.O.T", cioè *Internet of Things* ("internet delle cose"), nasce infatti per essere immersa in elettrodomestici, automobili, case, negozi, utensili intelligenti e connessi.

Potete immaginare il vostro frigorifero

che, tramite Iota, ordina e paga il latte su Amazon. O un distributore di *Coca-Cola* che non necessità di essere collegato a una qualche società finanziaria per accettare il vostro bancomat.

La mancanza di blockchain e l'agilità del software di Iota consente di sognare un mondo in cui Tangle è sparso in ogni dispositivo elettronico, anche in quelli di potenza ridicolmente bassa. Ogni oggetto presente in questo mondo è potenzialmente intelligente, programmabile e autonomo, anche nelle sue transazioni – non solo economiche. Gli basta un minuscolo chip e una connessione dati *mobile* a basso consumo come il 5G.

Ammettiamolo. Se con BitCoin il futuro è un po' oscuro e controverso, con Iota è, semplicemente, eccitante.

# In sintesi

- **BitCoin** è stato progettato con una grande lucidità sul breve termine ma non sul lungo. A meno di 10 anni dalla sua nascita e nonostante il suo dominio in termini di mercato è già vecchio e barcollante su molti aspetti.

- Il proof-of-work estremo di BitCoin è di sua natura insostenibile in un mondo di risorse limitate e in cui la produzione di energia è la prima causa di inquinamento, addirittura più dell'allevamento e dei trasporti.

- La facilità con cui la sua blockchain si satura e le altissime commissioni per oliarla creano colli di bottiglia nel suo utilizzo come valuta reale.

- Per superarne i limiti sono stati proposti dei fork, ma molte istituzioni e persone hanno preferito piuttosto ripensare da zero la questione con nuovi approcci più freschi alle criptovalute.

- **Ethereum** è la blockchain universale, concepita per ospitare qualsiasi applicazione civile, sociale, legale e finanziaria che

necessiti di avere un referente terzo neutrale a cui far affidamento per l'esecuzione di accordi, transazioni e contratti. Questi ultimi definiti smart contract.

- Ha la sua personale criptovaluta denominata **Ether**.

- Ethereum sta evolvendo verso un puro approccio proof-of-stake, in grado di incentivare la blockchain al suo lavoro senza sprechi di risorse computazionali e energetiche. L'incarnazione prossima ventura si chiama Casper.

- **Ripple** è una criptovaluta verticalizzata sul trasferimento di

denaro a livello internazionale tra istituzioni finanziarie e banche. Sfrutta la sua blockchain per consentire transazioni massive rapide e sicure ponendosi come ponte tra gli attori.

- **Cardano** sgorga dal mondo della ricerca e fa dell'oggettività scientifica e della sofisticazione ingegneristica la sua forza. Propone un'architettura a sotto-reti che disegna una blockchain snella e efficiente. Punta inoltre a diventare la "lingua franca" nelle conversioni tra le criptomonete.

- **Iota** è l'unica criptovaluta a non

aver bisogno di una blockchain grazie al protocollo Tangle e alla verifica distribuita delle transazioni. Gli stessi utilizzatori finali sono i miner. Questo le consente di avere un impatto computazionale tendente allo zero, una velocità estrema e di poter essere ibridata con qualsiasi oggetto della futura “internet delle cose” (*Internet of Things*).

# DOVE VADO ADESSO?

Ne abbiamo viste delle belle.

Mondi spaziali remoti, individui saggi e individui corrotti, cristalli misteriosi, civiltà esplose.

Trucidi scontri filosofici sul senso del denaro capaci di plasmare a colpi di ideologie e accordi globali il mondo in cui viviamo. Un misterioso individuo apparso sui forum online nel 2008 e adorato dai suoi adepti come un messia. Le sue sorprendenti teorie in grado di miscelare tecnologie di ogni complessità per forgiare la prima valuta totalmente

virtuale.

Utopie anarchico-democratiche deflagrate contro l'ineffabile complessità della realtà. La nuova classe dei ricchissimi cripto-possidenti anonimi. Una delle più grandi minacce ecologiche al nostro pianeta in larga parte sconosciuta. Crasi tra tecnologia e umanesimo per vaccinarci contro la facile esaltazione degli ingenui.

Machiavellici congegni di speculazione per spremere a nostro favore l'imprevedibilità dello strumento finanziario più giovane della storia. Guizzi di genio di pensatori intenti a modellare per noi un futuro in cui

potremo finalmente far lavorare le criptomonete per noi. E *non* noi per loro.

Dopo un tuffo in apnea di tale calibro tra discipline di ogni tipo, cosa ci resta?

La **curiosità** che questo libro vi ha – auspicabilmente – infiammato.

Con le mie parole non intendevo per nessuna ragione al mondo cercare di risolvere e di descrivere *tutto* il reame infinitamente ramificato delle criptovalute e dei sintomi che le sottendono. Molti libri prima di questo ci hanno provato, per poi ritrovarsi tristemente superati a distanza di sei mesi. Ho preferito piuttosto puntare il

vostro sguardo e la vostra sensibilità verso le grosse arterie entro cui questo universo quasi irreale si sta muovendo. E sulle sue cause psicologiche, sociali, etiche, tecniche, legislative, filosofiche.

Mi illudo di avervi consegnato tramite questo volume una *mappa* da cui decollare per esplorare i meandri dei regni che più vi hanno intrigato. E, soprattutto, una scacchiera per incasellare ciò che verrà, spesso non così semplice da ghermire senza delle coordinate di riferimento.

Se avete apprezzato le mie righe potete seguirmi su *Quora Italia*, spesso rispondo a domande relative a finanza e

criptovalute: https://it.quora.com/profile/Francesco-J-Galvani.

Nel corso dei capitoli vi ho più volte consigliato di sfruttare l'occasione per comprendere più a fondo il mondo degli investimenti, ben oltre BitCoin o Ethereum. Il nostro sistema educativo lo ignora totalmente mettendo la nostra tranquillità finanziaria futura a repentaglio. Il mio libro *Le 3 Formule Segrete per Guadagnare in Borsa* (http://bit.ly/le3formule) può aiutarvi, ma siete invitati a rintracciare qualsiasi materiale possa guidarvi.

Ci sono fonti autorevoli e sempre

aggiornate per rimanere sincronizzati con le novità delle criptomonete. La mia prediletta da anni è *Investopedia*, ha un'intera area dedicata a tutto ciò che è "cripto": https://www.investopedia.com/bitcoin/.

Non vi basta? Il fenomeno è talmente "hot" e il materiale talmente abbondante che una ricerca su Google in genere vi assicura risultati di qualità.

Se invece avete bisogno di chiarimenti o vi va di aprire un canale con me, niente di più semplice: su www.francescogalvani.com avete tutti i riferimenti del caso. Ci tengo. Se vi va di lasciare su Amazon una vostra

personale recensione a questo libro ne sarei felicissimo – al di là delle stelline, si intende! :)

Grazie per avermi permesso di accompagnarvi in questo viaggio. Per me è stato entusiasmante.

*Frank*

# L'AUTORE

*Quant* trader, sviluppatore in ambito *Artificial Intelligence*, professionista nella comunicazione e autore, **Francesco Galvani** è da sempre un ambientalista convinto, innamorato della mente e del cosmo, musicista per diletto.

Per il suo personale approccio alla divulgazione nel 2017 è

stato inserito tra i *top author* di *Quora Italia*. In precedenza ha conquistato premi internazionali e riconoscimenti per il suo focus tecnologico nel *digital marketing*.

Sfrutta le sue competenze statistiche, psicologiche, economiche e informatiche per indagare e dissotterrare i **principi fondanti** di molti fenomeni complessi arrivando all'essenziale. Ama ragionare

per concetti chiave e non per parafrasi, idee preconfezionate e buon senso altrui.

Il suo stile è smaccatamente ispirato alla leggerezza dei divulgatori americani. Per questo avvolge pensieri serissimi con battute, iperboli e paradossi.

Questi suoi due obiettivi si incarnano nel progetto **Frank (Fun)damentals**, che vive sul sito francescogalvani.com, in

seminari, consulenze e prodotti editoriali.