LA RIVOLUZIONE DELLE VALUTE VIRTUALI

Scritto da Andrea Romanazzi per ValuteVirtuali.com

Sunto

Gli aspetti tecnologici, la storia delle criptovalute, l'approccio al mondo del trading, i wallet e tutto quello che serve sapere per capire qualcosa di più di questo mondo

Andrea Romanazzi per ValuteVirtuali.com
https://valutevirtuali.com
info@valutevirtuali.com

Indice

Sommario

1. PREFAZIONE

Quando i ragazzi di ValuteVirtuali.Com mi hanno chiesto di scrivere un libro su Bitcoin e le criptovalute nella mia testa c'era già l'idea di fare qualcosa del genere quindi non ho avuto alcuna difficoltà ad accettare ed anche, non ho problemi ad ammetterlo, con un certo entusiasmo.

Sin da quando ho scoperto l'esistenza della tecnologia blockchain, infatti, ho intuito le enormi potenzialità di questo strumento e dopo qualche mese, in cui mi sono dedicato anima e corpo a studiarla, ho subito intuito che era necessario produrre del materiale nella nostra lingua per permettere anche al grande pubblico italiano di accostarsi alla "catena di blocchi" come ormai da anni avviene in tutto il resto del mondo.

Lo squilibrio demografico che caratterizza la società italiana, unitamente a una certa diffusa ignoranza tecnologica e alla mancata conoscenza della lingua inglese, infatti, rappresentano dei grossi ostacoli alla diffusione di Bitcoin e delle altre criptovalute nella nostra società; questo non vuol dire ovviamente che in Italia non ci siano bitcoiners (sarebbe improponibile e per certi versi anche grave), ma è comunque vero che rispetto a molti altri paesi il nostro sta rimanendo indietro anche per quel che riguarda questo aspetto (oltre che per un'infinità di altre cose).

Quando penso all'Italia e alla profonda crisi (non solo economica, ma anche e forse soprattutto culturale) che ormai da decenni la caratterizza non posso fare a meno di credere che se la blockchain rappresenta una grande opportunità, in generale per tutto il mondo, questo è ancora più vero per un paese come il nostro.

Tra tutti i vari motivi, quindi, è proprio questo quello che mi ha portato ad accettare la sfida di scrivere un ebook sulle criptovalute, perché penso sia fondamentale offrire ai lettori un manuale che non sia rivolto agli esperti e agli operatori del settore, ma a tutti coloro che non hanno mai sentito parlare di questa tecnologia (o che la conoscono solo molto superficialmente), di modo da permettere loro di avvicinarsi alla blockchain attraverso un testo scritto in maniera semplice e comprensibile a chiunque indipendentemente dal livello di competenze informatiche che si possiedono.

Questo testo, quindi, è scritto pensando a tutte quelle persone (e non sono poche nel nostro paese) che trovano ancora oggi enormi difficoltà anche solo a configurare una mail su un cellulare o a compiere operazioni che invece chi mastica di tecnologia (senza con questo esserne un grande esperto) esegue quotidianamente senza il minimo sforzo; penso che sia una bella sfida, dal momento che parliamo di una tecnologia estremamente complessa e difficile da comprendere in ogni suo aspetto anche per coloro che già possiedono solide competenze in ambito informatico. Se sarò riuscito o meno a realizzare questo obiettivo, creando una guida che, senza alcuna pretesa, riesca a permettere anche agli utenti meno scafati di comprendere in cosa consista la tecnologia blockchain, lo decideranno i lettori; io posso solo dire che sono molto felice di avere avuto la possibilità di provarci.

Andrea Romanazzi

2. INTRODUZIONE

Spesso mi è capitato di scrivere sui social (e di tanto in tanto lo faccio ancora) che "*le persone che capiscono davvero cosa sia la blockchain in tutto il mondo si possono contare sulle dita di una sola mano*"; il motivo per cui sostengo questa tesi è che parliamo di una tecnologia capace di impattare su ogni campo dello scibile umano, dalla politica all'economia, passando ovviamente per la tecnica (informatica, ma non solo) fino ad arrivare ad ogni settore produttivo (in ambito finanziario, ad esempio, ma anche in quello legale, pedagogico, sociologico, medico, etc).

Per poter comprendere in maniera completa cosa implichi davvero l'invenzione della blockchain per l'umanità, quindi, occorre possedere competenze forti e trasversali in una quantità di settori differenti che solo pochissime menti illuminate possiedono; a scanso di equivoci, quindi, preciso che io non appartengo a questa schiera di menti superiori ma sono solo un umile osservatore che tenta di arrabattarsi come può sulla base delle competenze a propria disposizione. In questo testo, in ogni caso, tenteremo di affrontare tutta questa molteplicità di temi nella maniera più organica possibile tentando al contempo di mantenere il ragionamento su un binario di semplicità e comprensibilità (per renderlo quindi accessibile a chiunque).

L'indice è strutturato in maniera tale da introdurre prima gli argomenti che sono propedeutici ad affrontare tematiche che verranno ulteriormente sviscerate successivamente; originariamente l'idea era di includere in questo testo anche un glossario, durante la prima stesura però ho avuto modo di rendermi conto che sarebbe stato necessario fornire di volta in volta al lettore una definizione dei vari termini utilizzati al fine di facilitare la comprensione di quanto illustrato. Per questo motivo nella stesura finale si è reputato inutile includere anche un glossario.

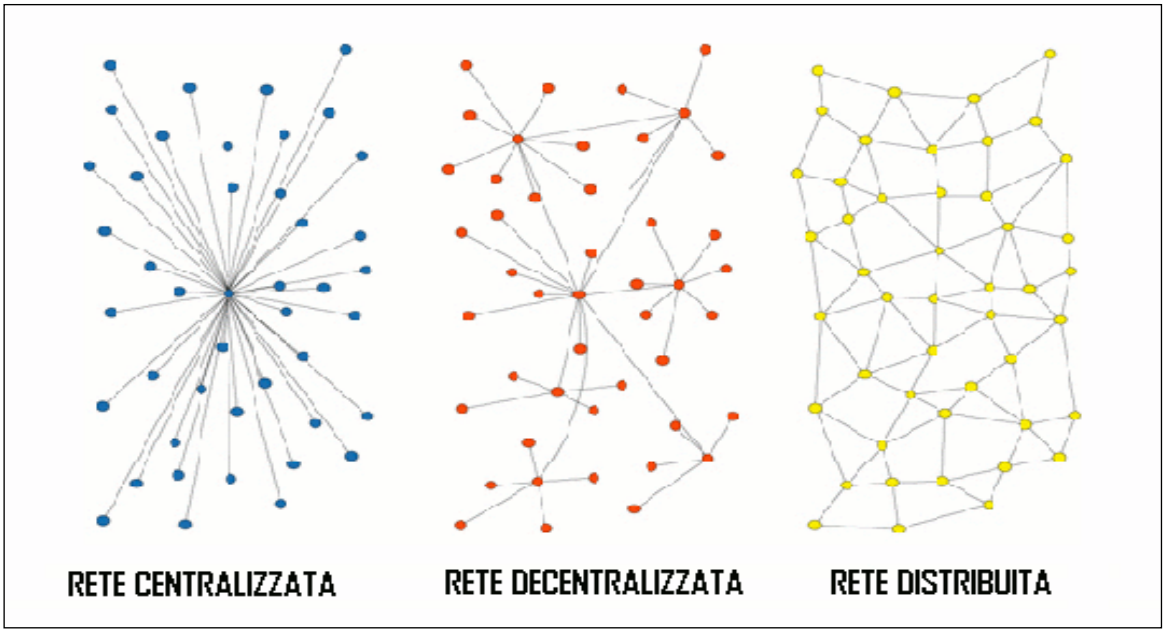
Buona lettura.

3. CHE COS'È LA BLOCKCHAIN

La blockchain, molto semplicemente, non è altro che un data base distribuito; da wikipedia ricaviamo una definizione facile da comprendere di cosa sia un data base, per cui parliamo di "*un archivio di dati strutturato in modo da razionalizzare la gestione e l'aggiornamento delle informazioni e da permettere lo svolgimento di ricerche complesse*". Quindi, traducendo questa definizione in un linguaggio facilmente comprensibile a tutti, stiamo parlando di uno spazio virtuale nel quale è possibile archiviare ogni genere di informazione (economica, ma non solo).

Abbiamo però detto che una blockchain non è semplicemente un data base, ma è un data base distribuito, che cosa significa? Facile, significa che una copia delle informazioni archiviate in questo data base è conservata in ognuno dei computer che fanno parte della rete. Ma se una blockchain non è altro che un data base cosa rende questa tecnologia così rivoluzionaria? Semplice, a rendere così innovativa questa tecnologia è il fatto che a differenza di qualunque altro data base la blockchain è sostanzialmente blindata. Per intenderci, anche il meno esperto di questioni informatiche sa benissimo che qualunque infrastruttura informatica può essere hackerata, non importa quante misure di sicurezza si possano avere, quando un data base è accessibile attraverso il web allora può essere hackerato; questo vale per qualunque archivio su internet, ma non vale per una blockchain.

Il motivo per cui questa infrastruttura non può essere corrotta in alcun modo lo capiremo meglio nel corso dei prossimi capitoli, per adesso limitiamoci a prendere confidenza con questo primo concetto e cioè che una blockchain è sostanzialmente un data base distribuito e blindato. Il fatto, poi, che questo archivio di dati sia "distribuito" ci permette di iniziare a prendere confidenza anche col concetto di "decentralizzazione"; normalmente, infatti, i data base sono "centralizzati" cioè sono di proprietà di un'azienda o di un'istituzione che si occupa di aggiornarli, di renderli accessibili alle persone che possono aver bisogno di consultarli e pone in essere tutte le misure di sicurezza necessarie non solo a prevenire il furto di informazioni ma anche ad evitare che i dati archiviati su quella infrastruttura vengano manipolati e corrotti.



Dal momento, però, che abbiamo detto che la blockchain è un data base distribuito, capiamo bene che non c'è un organo "centrale" che si occupi di fare tutte queste cose, ma che sono tutti i computer della rete che partecipano collettivamente a questi processi. Semplificando un po' possiamo affermare che esistono tre tipi di reti, le "reti centralizzate" (spesso chiamate anche "a stella") nelle quali i dati vengono trasmessi a partire da un punto centrale a tutti gli utenti, le "reti decentralizzate" in cui iniziamo ad avere dei nodi centrali che trasmettono le informazioni tra loro senza una precisa gerarchia e le "reti distribuite" in cui tutti i nodi sono in comunicazione tra loro senza che vi sia una gerarchia definita.

Compresi questi primi concetti abbiamo già modo di intuire per quale motivo la tecnologia blockchain venga comunemente considerata la più grande innovazione tecnologica dopo l'avvento di internet, perché per la prima volta abbiamo a nostra disposizione un data base perfettamente sicuro senza bisogno che vi sia un organo centrale a gestirlo e a garantirne la sicurezza.

3.1 COME FUNZIONA LA BLOCKCHAIN

Nel capitolo precedente abbiamo spiegato che una blockchain è un data base distribuito, adesso proveremo a spiegare come funziona; intanto per rendere più facile comprendere il tutto abbiamo bisogno di fare un esempio concreto e, quindi, parleremo del caso d'uso più tipico che riguarda questa tecnologia e cioè il trasferimento di valore (o denaro) da un utente all'altro. Per trasferire denaro da una persona all'altra siamo attualmente tutti abituati a usare i bonifici; quello che succede, molto semplicemente, è che ogni banca tiene dei registri in cui riporta il saldo complessivo di ogni correntista e le movimentazioni fatte da e verso quel determinato conto.

Quando faccio un bonifico (poniamo caso di 100€) dal mio conto a quello di un'altra persona la mia banca traccia il movimento e segna sul suo registro una transazione di importo pari a -100€ dal mio conto, scala quindi questa somma dal mio saldo complessivo e invia il denaro alla banca della persona a cui lo sto trasferendo.

Questa, a sua volta, farà altrettanto segnando (però questa volta sul proprio registro) un movimento di +100€ e sommandolo al saldo complessivo del correntista beneficiario del bonifico. Con una blockchain succede esattamente la stessa cosa, solo che il registro non lo detiene una banca ma (come abbiamo illustrato nel capitolo precedente) sono tutti i computer che partecipano alla rete ad avere una copia di questo documento; quando invio ad esempio un Bitcoin a una persona (da qui in avanti useremo la sigla BTC per riferirci a Bitcoin come valuta), tutti i computer che partecipano alla rete segnano il movimento sul registro e scalano 1BTC dal mio conto mentre, allo stesso tempo, sommano lo stesso importo a beneficio del destinatario. La prima domanda che a questo punto sorge spontaneo porsi riguarda il fatto che, dal momento che il registro non solo è condiviso da tutti i computer della rete ma è anche pubblico (è cioè accessibile a tutti in consultazione mediante appositi siti chiamati "explorer"), chiunque potrebbe avere accesso alla movimentazione del mio conto ledendo quindi la mia privacy; in realtà i conti (che d'ora in avanti chiameremo "indirizzi") non sono riconducibili a un nome e un cognome (cioè a una persona fisica) ma sono "stringhe" composte da un minimo di 26 a un massimo di 35 caratteri alfanumerici.

Per questo motivo si dice che le transazioni in bitcoin sono anonime. In realtà le cose non stanno nemmeno così, bitcoin infatti non è anonimo ma "pseudo-anonimo"; questo significa, molto semplicemente, che pur non essendo gli indirizzi (cioè, lo ribadiamo, quelli che in banca chiamiamo "conti corrente") intestati a delle vere e proprie persone fisiche è possibile comunque (il che non significa che sia facile, ma solo che è possibile farlo) seguire le tracce informatiche che queste transazioni lasciano sul web fino a risalire all'utenza (cioè al punto in cui l'utente si è collegato a internet o il dispositivo con cui si è collegato) e definire così l'identità della persona fisica che controlla quel determinato indirizzo.

Detto questo torniamo al nostro trasferimento di denaro e introduciamo un'altra differenza rilevante rispetto a quanto avviene nel sistema bancario; mentre quando movimento il mio denaro attraverso una banca questa provvede immediatamente a tracciare ogni transazione e fa altrettanto con ogni altro movimento, in una blockchain le operazioni fatte dai vari utenti vengono "accorpate" ed inserite dentro a dei blocchi. Per capire cosa sia un blocco possiamo immaginarlo come una scatola che contiene le informazioni (indirizzo mittente, importo movimentato, indirizzo destinatario) relative a tutte le transazioni "ordinate" dagli utenti nell'unità di tempo; con Bitcoin, ad esempio, viene generato un blocco ogni 10 minuti.

Chi nel corso della sua vita si sia trovato a fare un inventario non ha difficoltà a comprendere come funzioni questa tecnologia; si tratta quindi di una buona metafora per spiegare come funziona una blockchain.

Quando facciamo un inventario non facciamo altro che prendere tutta la merce che abbiamo in magazzino, riporla all'interno di alcune scatole (numerate in ordine crescente) riportando su un registro il contenuto di ogni singola scatola. Ordinando con criterio le diverse scatole, a inventario terminato, disporrò anche di una "mappa" cartacea che illustra dove si trova ogni singolo articolo all'interno del magazzino; se immaginiamo l'inventario di un ristorante che sta chiudendo l'attività, ad esempio, ci ritroviamo tutti gli utensili della cucina (coltelli, posate, piatti, pentole, bicchieri, etc), conservati in un magazzino e riposti all'interno di scatole. Dato che le scatole sono numerate e che ho riportato sul registro il contenuto di ogni singola scatola, in qualunque momento dovessi avere bisogno, per esempio, dello scolapasta, consultando il registro potrei conoscere la sua esatta posizione. Una blockchain, quindi, può essere immaginata come l'inventario di tutte le transazioni

fatte; in pratica, quindi, non è altro che un enorme registro che riporta la traccia di tutti i blocchi eseguiti dalla rete sin dalla sua nascita.

Mentre tu leggi questo testo, ad esempio, la rete sta processando un nuovo blocco e va ad aggiungerlo al registro di tutti i blocchi processati nel tempo. Il termine "blockchain" tradotto in italiano significa infatti "catena di blocchi" e restituisce bene l'idea di come funzioni tutto questo processo; ogni blocco registrato sulla blockchain è legato (come l'anello di una catena) a quello precedente.

Questo aspetto è fondamentale per comprendere il motivo per cui questa tecnologia è così affidabile, se un soggetto malintenzionato tentasse di manipolare le informazioni contenute in uno dei blocchi già processati dalla rete, infatti, questa modifica provocherebbe una serie di anomalie a catena su tutti i blocchi successivi e gli altri computer della rete, ritrovandosi ad avere a che fare con un documento differente da quello che hanno a propria disposizione, sarebbero capaci di definire la natura malevola dell'operazione bloccandola quindi istantaneamente. I computer che fanno parte della rete non si limitano però a trascrivere le transazioni presenti all'interno di un blocco sulla blockchain, ma le validano; quando il blocco è validato dalla rete non può essere più modificato, la blockchain, quindi, non è solo un registro (o data base) blindato e distribuito ma è anche immutabile. Arrivati a questo punto fermiamoci un attimo per riepilogare i concetti sin qui espressi; quando un utente desidera trasferire del denaro a un altro utente quello che fa è spedire la somma dal suo indirizzo a quello del destinatario. Le informazioni di questa singola transazione vengono inserite all'interno di un blocco insieme alle informazioni relative a tutte le transazioni ordinate negli ultimi dieci minuti, la rete quindi prende in carico il blocco, lo processa, lo valida e lo trascrive sulla blockchain.

Da quel momento le informazioni contenute nel blocco diventano immutabili e non possono più essere modificate; facile no? Bene, nel prossimo paragrafo di questo capitolo andremo ad illustrare in che modo la rete valida e processa i blocchi e soprattutto avremo modo di capire per quale motivo i nodi che fanno parte di questa rete non possono in alcun modo manipolare le informazioni contenute nel blocco che stanno processando. Andremo a definire, in altre parole, chi sono i miners, che tipo di ruolo hanno e perché sono così importanti nel funzionamento di una blockchain.

3.2 IL RUOLO DEI MINERS

Dal momento che questo testo è pensato per tutte quelle persone che non hanno la minima idea di cosa sia Bitcoin, ne di come funzioni e cosa sia una blockchain, fino adesso abbiamo usato dei termini molto generici, proprio per evitare di ingenerare confusione.

Questa tecnologia è però molto complessa e ha una sua terminologia specifica che dobbiamo imparare a conoscere per comprendere pienamente di cosa stiamo parlando; nel paragrafo precedente di questo capitolo abbiamo parlato molto genericamente di nodi, di computer che fanno parte di una rete, di trascrivere i blocchi sulla blockchain e di "validazione" dei blocchi stessi. Adesso

è il caso di entrare più nello specifico e comprendere meglio come tutto questo avvenga, è arrivato, in altre parole, il momento di parlare di mining.

Per prima cosa diamo una definizione comprensibile a chiunque di cosa voglia dire questa parola (traducibile in italiano col verbo "minare") per cui definiamo mining "*il processo di generazione, verifica e validazione dei blocchi*". Ad occuparsi di questo sono delle figure che prendono il nome di "miners" (in italiano li chiameremmo "minatori"); queste figure, centrali per il funzionamento di una rete blockchain, non fanno altro che mettere a disposizione della rete stessa la potenza di calcolo dei loro computer rappresentando quindi ciò che in precedenza abbiamo chiamato "nodi".

Per poter comprendere adeguatamente cosa sia il mining, però, dobbiamo prima introdurre una serie di nozioni che sono essenziali per proseguire il discorso, per cui per prima cosa ricorriamo nuovamente a wikipedia che ci offre una definizione facile da comprendere per chiunque di cosa sia un hash e cioè "*una funzione matematica non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza minore*"; per comprendere cosa sia un hash possiamo immaginare una specie di impronta digitale, per cui, come ogni essere umano ha la propria impronta digitale e non esistono due esseri umani con la stessa impronta digitale (ne mai potranno esistere), allo stesso modo due blocchi che contengono informazioni differenti non potranno mai generare un hash uguale. Per quanto riguarda poi la natura "non invertibile" degli hash questo significa molto semplicemente che, nonostante l'hash venga generato a partire dalle informazioni contenute in un blocco, non è in alcun modo possibile fare il processo inverso, cioè definire il contenuto del blocco partendo dalla semplice osservazione dell'hash.

Le funzioni di hash (bitcoin ne usa una a 256bit, comunemente considerata tra le più sicure in assoluto) lavorano in maniera (per così dire) "scientifica"; con questo intendo dire che se io sottoponessi a una funzione di hash un messaggio del tipo "il sole è splendente ma sul ghiaccio si può scivolare" (i più nerd tra i lettori avranno colto la citazione di un noto film) l'hash che ne ricaverei

sarebbe sempre lo stesso, indipendentemente da quante volte sottoponessi questo messaggio alla funzione di hash e indipendentemente da quanto tempo possa trascorrere tra un tentativo e l'altro. Se però il messaggio variasse anche solo in maniera infinitesimale, ad esempio, se invece di scrivere "può" scrivessi "puo" la frase "il sole è splendente ma sul ghiaccio si puo scivolare" genererebbe un hash completamente differente. In precedenza abbiamo detto che ogni blocco contiene le informazioni di tutte le transazioni ordinate negli ultimi dieci minuti ed è collegato (come in una catena) al blocco precedente; bene, quello che non abbiamo detto è che questo "collegamento" tra ogni blocco che compone la "catena" è realizzato proprio per mezzo delle funzioni di hash.

In ogni nuovo blocco, infatti, viene incluso l'hash del blocco validato subito prima e che finisce quindi col partecipare (insieme con tutte le altre informazioni contenute nel blocco) a formare l'hash del blocco corrente. Facciamo un esempio per capirci meglio e immaginiamo di denominare l'ultimo blocco validato con la lettera A, il blocco in corso di validazione con la lettera B e il blocco che verrà validato subito dopo con la lettera C; quello che succede è che il blocco B include al suo interno l'hash del blocco A, il blocco C includerà quindi a sua volta l'hash del blocco B e così via.

Detto questo facciamo un passo indietro e ritorniamo al punto in cui abbiamo spiegato che gli hash non sono invertibili, la domanda che i lettori più attenti si saranno fatti è: ok, ma se l'hash con cui abbiamo crittografato tutte le informazioni contenute nel blocco non è invertibile, come fa la rete a registrare sulla blockchain i nuovi saldi relativi agli indirizzi? Semplice, procede per tentativi. L'attività di mining appare quindi essere una sorta di gioco matematico, un atto di "brute forcing" ovverosia (come da definizione su wikipedia) "*la risoluzione di un problema attraverso la verifica di tutte le soluzioni teoricamente possibili fino a che si trova quella effettivamente corretta*". Per procedere in questo modo i computer che partecipano alla rete devono eseguire una quantità enorme di calcoli in un arco di tempo che è predefinito (dal momento che abbiamo detto che i blocchi vengono generati ogni dieci minuti) e quando uno dei nodi della rete (il miner) riesce a trovare una soluzione a questo rompicapo la passa anche agli altri nodi, che verificano che tale soluzione sia corretta e, nel momento in cui almeno il 50% più uno dei nodi della rete verificano che lo è, procedono col trascrivere i dati contenuti nel blocco sulla blockchain che, da quel momento, diventano immutabili.

Il miner che vince la sfida e trova la soluzione corretta viene quindi ricompensato con la "vincita" di nuovi BTC (contenuti nel blocco processato) che rappresentano la sua retribuzione per il lavoro svolto. Tutto questo processo, cioè la ricerca di una soluzione al rompicapo matematico (rappresentato dall'hash), il controllo da parte della rete che la soluzione proposta da uno dei nodi sia valida, di modo da raggiungere il consenso necessario (50%+1 dei nodi) ad autorizzare la trascrizione di quei dati sulla blockchain, viene gestito da un algoritmo che prende il nome di "protocollo di consenso" (un tema di cui avremo modo di occuparci meglio nel prossimo capitolo). Se tutto questo, quindi, ti è sembrato complesso ti anticipo sin da ora che le cose si faranno ancora più difficili quando andremo ad illustrare cosa sono e come funzionano i principali protocolli di consenso, incluso ovviamente quello che permette il funzionamento della rete Bitcoin (che prende il nome di POW, acronimo di "proof of work"); per adesso fermiamoci un attimo e riepiloghiamo velocemente le nozioni che abbiamo appreso fin qui.

Abbiamo quindi imparato che una blockchain è un data base all'interno del quale è possibile registrare dei dati, tali dati possono avere (anche, ma non solo) una natura economica e consistere quindi sostanzialmente in un elenco di transazioni tra utenti e dei relativi saldi sui rispettivi conti (indirizzi); a differenza però di quanto accade nel sistema bancario, in cui ogni banca tiene un registro dei propri clienti e ci trascrive sopra di volta in volta ogni singola transazione effettuata, in una blockchain sono tutti i computer che fanno parte della rete che detengono la stessa copia di questo registro e l'aggiornano tutti insieme registrando non le singole transazioni ma la successione

cronologica dei blocchi generati, ognuno dei quali contiene la fotografia di tutte le transazioni effettuate nei dieci minuti precedenti. Ogni blocco contiene una stringa alfanumerica (hash) che lo aggancia al blocco validato subito prima, in questo modo si forma la catena che da il nome a questa tecnologia;

il processo di controllo, verifica, validazione e trascrizione dei blocchi sulla blockchain viene gestito da figure che prendono il nome di miners e che gareggiano tra di loro per pervenire alla risoluzione di un rompicapo matematico che permette di verificare la correttezza delle informazioni contenute in ogni nuovo blocco.

Quando un nodo della rete (miner) risolve il rompicapo, trasmette a tutti gli altri la soluzione valida, quindi la rete verifica che la soluzione proposta sia effettivamente corretta e quando almeno il 50% più uno dei nodi raggiunge il consenso sulla validità della soluzione proposta autorizza la trascrizione del blocco sulla blockchain. Da quel momento le informazioni contenute nel blocco diventano sostanzialmente immutabili. Il miner che per primo ha trovato la soluzione valida riceve dalla rete un compenso per il lavoro (di mining) svolto e si può quindi procedere alla validazione del blocco successivo.

In realtà, a dire il vero, tutte queste informazioni che abbiamo appena riepilogato presentano alcune omissioni e piccole imprecisioni, che avremo modo di colmare e correggere nel prossimo capitolo, quando impareremo a conoscere i principali protocolli di consenso; questo modo di procedere è necessario per evitare di scaricare tutti insieme concetti molto complicati sulle spalle dello sventurato lettore di questo testo, permettendogli così di procedere per gradi e di pervenire a una conoscenza piena di questa tecnologia. Prima di riprendere però il ragionamento in tutta la sua complessità e occuparci dei protocolli di consenso chiudiamo questo capitolo con un paio di paragrafi nettamente più semplici da comprendere in cui sviscereremo per prima cosa quali sono i vantaggi della blockchain e poi introdurremo alcune nuove nozioni indispensabili per prendere di petto il discorso sui protocolli di consenso.

3.3 I VANTAGGI DELLA BLOCKCHAIN

Dopo esserci lambiccati il cervello nei paragrafi precedenti prendendo confidenza con alcuni concetti fondamentali per comprendere meglio la natura della tecnologia blockchain, rilassiamoci un attimo affrontando un tema più leggero e meno tecnico; diciamo sin da subito, anche se a chi mi legge potrebbe sembrare eccessivo, che giudico un solo paragrafo non sufficiente a descrivere compiutamente i vantaggi che questa tecnologia offre all'umanità e che sono convinto che servirebbe anzi un libro a parte per sviscerare completamente l'argomento.

La blockchain, infatti, può essere sostanzialmente applicata in ogni settore e, anche se allo stato attuale è balzata agli onori delle cronache solo per la sua natura prettamente finanziaria, in realtà parliamo di un'innovazione che nei prossimi anni avrà modo di rivoluzionare ogni settore dell'attività umana impattando prepotentemente sulle vite di tutti noi, incluse ovviamente anche quelle di tutti coloro che oggi si schierano orgogliosamente tra i suoi detrattori. Avremo comunque modo, in uno dei capitoli conclusivi, di illustrare più dettagliatamente i vari ambiti in cui la blockchain irromperà col suo carico innovativo, in questo paragrafo concentriamoci invece su quelli che sono i vantaggi innegabili che la caratterizzano.

Per prima cosa, quindi, dobbiamo parlare della trasparenza; per quanto possa apparire persino paradossale, infatti, per una tecnologia che si fonda sulla crittografia, uno degli aspetti più interessanti della blockchain è la sua capacità di rendere accessibili a chiunque le informazioni archiviate. Anche se molti detrattori evidenziano soprattutto la possibilità di rendere completamente anonime le transazioni, ponendo una serie di criticità relative soprattutto a questioni come l'evasione, il riciclaggio di denaro e il finanziamento del terrorismo, la verità (innegabile) è che come ogni grande innovazione tecnologica anche la blockchain può essere usata con ogni genere di finalità; non esiste innovazione tecnologica nella storia umana che non sia stata caratterizzata da questa dualità.

Persino la stampa, giusto per fare un esempio, può essere usata per informare le persone ma anche per indottrinarle (basti pensare ad esempio alla stampa di regime); che cosa avremmo dovuto fare, come genere umano, vietare la stampa per prevenire il rischio di indottrinamento? Sarebbe stato semplicemente folle. Tornando alla blockchain, quindi, è senza dubbio vero che questa tecnologia potrebbe finire col favorire fenomeni come l'evasione, il riciclaggio di denaro e il finanziamento al terrorismo, ma, dal momento che i registri distribuiti sono accessibili a chiunque, può essere anche usata, in virtù della sua grande trasparenza, per prevenire truffe, monitorare fenomeni come il finanziamento ai partiti ed aumentare quindi la trasparenza finanziaria in un gran numero di diversi ambiti; pensiamo ad esempio ai continui scandali che hanno coinvolto il mondo della beneficenza e delle associazioni senza scopo di lucro.

Grazie alla blockchain sarebbe possibile raccogliere fondi e donazioni rendendo completamente trasparente tutto il processo; pensiamo ad esempio ai fondi raccolti a seguito dei tanti, troppi, terremoti che hanno sconvolto l'Italia negli ultimi anni. Ecco, se quei fondi fossero stati raccolti usando una blockchain per gestire le donazioni ogni donatore avrebbe non solo potuto monitorare la somma complessivamente raccolta, ma persino seguire da vicino il modo in cui la sua donazione veniva spesa; nessuno scandalo potrebbe più travolgere alcuna associazione benefica se le raccolte fondi venissero gestite utilizzando una blockchain.

L'anonimato, inoltre, unitamente all'immutabilità del dato archiviato su blockchain rende questa tecnologia un ottimo sistema di voto; pensiamo ai regimi sparsi ovunque per il mondo e agli scandali relativi ai brogli elettorali che si verificano anche in paesi democratici; nulla di tutto questo potrebbe avvenire se si gestisse il voto attraverso una blockchain a patto che, ovviamente, questa fosse pienamente decentralizzata. Una blockchain centralizzata, infatti, implica la possibilità che chi la controlla possa manipolare i dati che vi sono registrati e sarebbe quindi inadatta e pericolosa per gestire un processo di voto; questo non vuol dire che non ci sia spazio o utilità per le blockchain centralizzate (ve ne sono infatti numerose sul mercato), ma significa semplicemente che ci sono cose che possono essere fatte per mezzo di una blockchain centralizzata (in determinati casi limite è persino auspicabile che sia così), mentre ve ne sono altre (come appunto un sistema di voto) che è assolutamente necessario vengano gestite attraverso una blockchain decentralizzata.

L'anonimato, quindi, rappresenta sia una criticità che una risorsa di questa tecnologia, pensiamo, ancora, ad esempio, alla condivisione dei dati sanitari, così utile per la ricerca ma così pericolosa per le persone comuni; tale condivisione è utile perché permetterebbe ai ricercatori di avere un'elevata quantità di dati estremamente preziosi per sviluppare nuovi farmaci e nuove cure, ma è al contempo un pericolo per le persone comuni dal momento che il dato sanitario è uno tra i più sensibili in assoluto. Pensiamo, per fare un esempio, ai malati di AIDS; da un lato è certamente auspicabile che queste persone condividano le loro informazioni sanitarie perché questo permetterebbe ai ricercatori di ricavare informazioni estremamente utili nella ricerca di una cura, d'altro canto, però, nessun malato troverebbe mai auspicabile che diventasse di dominio pubblico il fatto che ha contratto questa patologia.

Ebbene, la blockchain, in virtù della sua trasparenza e del suo anonimato, permetterebbe la condivisione dei dati sanitari in forma completamente anonima, senza che sia mai possibile risalire alla persona fisica a cui quei dati fanno riferimento ma consentendo ai ricercatori di mettere le mani su una mole impressionante di dati su cui lavorare che, sotto il profilo medico, rappresentano una vera e propria manna. L'altro vantaggio importante di questa tecnologia è che snellisce in maniera importante qualunque processo richieda una "validazione", dal momento che non esiste la necessità di un vero e proprio intervento umano per certificare l'informazione, comportando conseguentemente la possibilità di una riduzione importante dei costi necessari a gestire quei determinati processi.

La blockchain, in altre parole, risulta molto meno onerosa per gestire determinati processi di quanto non siano la gran parte dei modelli attualmente in uso; non è quindi un caso che le grandi banche ne siano così attratte e che sostanzialmente tutti i maggiori colossi bancari al mondo la stiano testando con grande interesse. Nonostante quanto sostengano i detrattori, quindi, questa tecnologia presenta innegabili vantaggi e se pure da un certo punto di vista è innegabile che presenti anche delle criticità, rimane comunque incontestabile che la stessa cosa si potrebbe affermare per qualunque grande innovazione tecnologica; anche l'intelligenza artificiale presenta delle criticità (alzi la mano chi non ha mai visto un film come terminator), ma questo non induce nessuno a sostenere che bisognerebbe vietare per legge lo sviluppo delle IA.

Un'altra critica molto comune, poi, tra i detrattori della blockchain è che non esistano casi d'uso concreti per questa tecnologia al di fuori delle applicazioni economiche/finanziarie. Questo è assolutamente falso e, del resto, lo abbiamo appena dimostrato nel corso di queste poche righe; è vero anzi il contrario, che la blockchain trova ambiti concreti di applicazione praticamente ovunque. Come mi piace ribadire spesso, poi, quando discuto di questi argomenti, la blockchain risolve tre grandi temi del nostro tempo che, più precisamente, riguardano la domanda crescente di spazio di archiviazione, potenza di calcolo ed energia elettrica; se per quanto riguarda i primi due aspetti (spazio di archiviazione e potenza di calcolo) la cosa è immediatamente comprensibile a chiunque dal momento che parliamo di una rete di computer che non fa altro che condividere proprio questi due "beni", nel caso della domanda crescente di energia la questione non è altrettanto intuitiva.

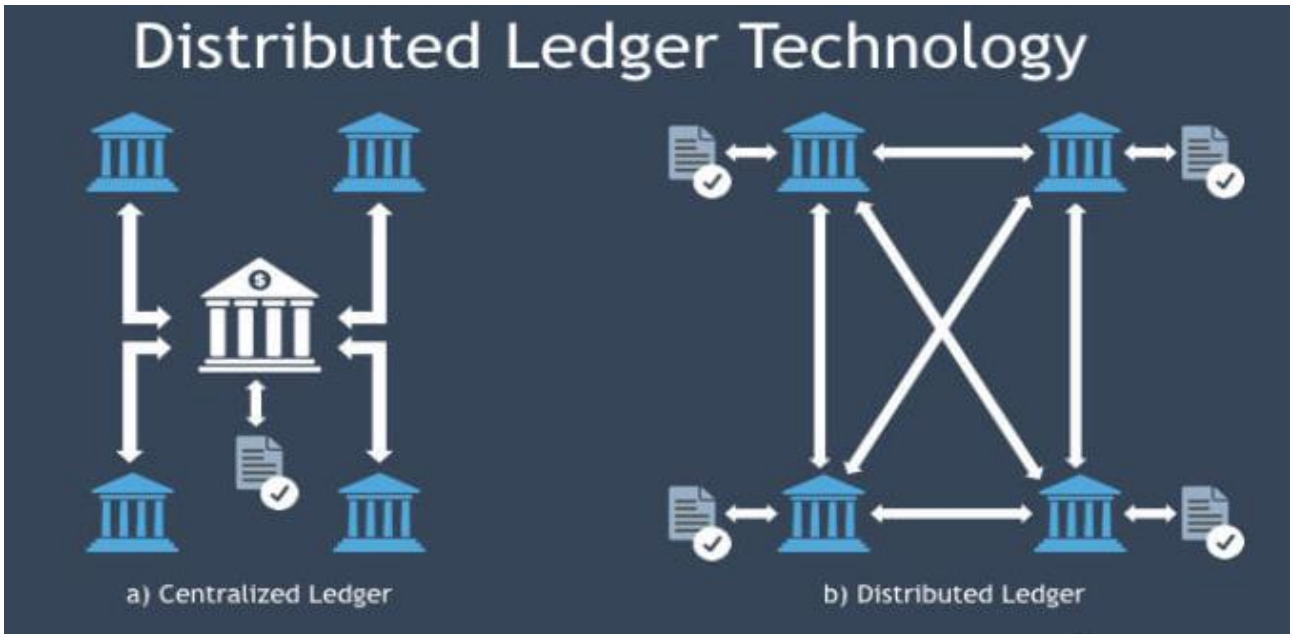
Senza dilungarci troppo, e per concludere, possiamo limitarci a spiegare che il motivo per cui attualmente non riusciamo a sfruttare al meglio la produzione di energia rinnovabile è che le reti con le quali distribuiamo l'energia non ce lo consentono. Le reti di distribuzione, infatti, sono sostanzialmente reti a stella, nelle quali sono pochi grandi produttori a distribuire l'energia; con la blockchain, invece, è possibile mettere in rete l'energia prodotta da una miriade di impianti domestici esattamente come avviene per la potenza di calcolo erogata dai computer ed è quindi possibile, in altre parole, realizzare finalmente delle "smart grid" (griglie intelligenti) a costi economicamente accessibili, sfruttando finalmente al massimo delle loro potenzialità le energie rinnovabili che, per propria stessa natura, sono sostanzialmente illimitate e inesauribili.

3.4 Differenze tra blockchain e distributed ledger technology (DLT)

Spesso può capitare di vedere usati i termini “blockchain” e “DLT” (acronimo di distributed ledger technology) come fossero sinonimi; questo può generare una certa confusione, soprattutto in chi muove i primi passi in questo mondo, favorendo la percezione che si tratti semplicemente di due modi differenti per definire la stessa tecnologia.

Tale confusione è favorita dal fatto che siamo di fronte, in entrambi i casi, a reti P2P che paiono essere decentralizzate e che richiedono il conseguimento di un consenso maggioritario per l’aggiunta di informazioni sul data base distribuito. Quindi sono la stessa cosa? Neanche per sogno, lo sono solo in apparenza. La prima differenza sostanziale è che la blockchain presenta la caratteristica struttura a blocchi, che è completamente assente nella tecnologia DLT; sembra un particolare da poco, ma è estremamente rilevante.

Anche nella tecnologia DLT abbiamo un registro mastro che tiene traccia delle transazioni, ma tali transazioni non sono accorpate all’interno di blocchi concatenati gli uni con gli altri. L’altra differenza assolutamente rilevante è che nella tecnologia DLT normalmente i nodi “validatori” sono sostanzialmente grandi istituzioni (banche, fondi di investimento, etc) mentre quando parliamo, ad esempio, di Bitcoin chiunque può diventare un nodo della rete e validare un blocco (ammesso che disponga della potenza di calcolo necessaria per farlo).



Possiamo quindi affermare, semplificando un po', che la differenza più rilevante tra queste tecnologie è che nella blockchain a validare i blocchi sono i miners, mentre nella tecnologia DLT a fare l'operazione equivalente (la validazione delle transazioni) sono i "nodi validatori". Pur essendo la tecnologia DLT costruita su una rete di nodi P2P e sulla base di un ledger (registro mastro) distribuito, non appare quindi essere perfettamente decentralizzata come invece nel caso di Bitcoin; qui, ragazzi, entriamo negli aspetti prettamente politici di questa tecnologia e iniziamo a intuire che ci troviamo di fronte a un vero e proprio scontro ideologico che divide chi crede che non ci sia alcun bisogno di organi centrali e chi crede al contrario che le grandi istituzioni (centralizzate) conservino una loro rilevanza indipendentemente dallo sviluppo tecnologico.

Il concetto, in altre parole, è che o si crede che la fiducia sia sufficiente riporla nella tecnologia e nei processi attraverso cui la rete può pervenire al consenso, o si crede che comunque e in ogni caso le grandi istituzioni (non solo bancarie, ma anche statali o di qualunque altro genere) siano le sole che godano dell’autorevolezza sufficiente a garantire la fiducia. Siamo quindi evidentemente di fronte a implicazioni di carattere chiaramente politico (e quindi anche ideologico) dal momento che vediamo

contrapporsi due linee di pensiero agli antipodi tra loro, da un lato una visione marcatamente "anarchica" della società, in cui viene a cadere ogni necessità di avere a che fare con le grandi istituzioni (in questo caso economiche), dall'altro un punto di vista in cui si continua a riconoscere la rilevanza e la centralità di quelle stesse istituzioni.

Quale di queste due differenti interpretazioni si imporrà sull'altra? Probabilmente nessuna delle due; di questo almeno io mi sento moderatamente convinto, tanto da poter arrivare a dire che se tra duecento anni ci ritrovassimo di nuovo qui per verificare come sono andate le cose ci accorgeremmo che nessuna di queste due differenti visioni si è dimostrata capace di spazzare completamente via la concorrente.

Queste due tecnologie, in altre parole, sono probabilmente destinate a continuare a coesistere e non è neanche detto, sinceramente, che questo debba essere per forza un male o qualcosa di negativo. Aver introdotto questa distinzione, ma lo vedremo meglio più avanti, ci tornerà molto utile già nel prossimo capitolo, nel quale andremo a vedere proprio come funzionano alcuni dei principali protocolli di consenso e avremo modo di intuire meglio perché blockchain e DLT, contrariamente a quanto in molti si ostinano ancora a fare, sono due termini che non dovrebbero mai e in nessun caso essere usati come sinonimi.

4. I PROTOCOLLI DI CONSENSO

Nel capitolo precedente abbiamo definito cosa sia una blockchain e iniziato a introdurre i principi che ne regolano il funzionamento; abbiamo anche detto, però, che mancava qualcosa e che tutto il ragionamento fatto presentava delle imprecisioni.

Questo perché è impossibile definire il funzionamento di una blockchain senza parlare dei protocolli di consenso; per prima cosa, quindi, ci serve una definizione per capire di cosa stiamo parlando. Preciso sin da ora che l'ecosistema delle criptovalute non è ancora stato capace di proporre delle definizioni univoche e unanimemente accettate da tutti, per questo motivo non è così improbabile che il lettore possa trovare altrove definizioni differenti da quelle proposte in questo testo; in ogni caso definiamo protocolli di consenso "gli algoritmi che definiscono le regole attraverso le quali i nodi della rete sono autorizzati a validare un blocco".

Così come sul mercato esistono una molteplicità di criptovalute lo stesso vale per i protocolli di consenso; in linea di massima ne esistono come minimo una trentina (ma probabilmente sono anche di più), noi qui analizzeremo solo quelli più affermati e che in un certo senso rappresentano la base concettuale su cui se ne sono prodotti di nuovi. Esistono, infatti, anche protocolli di consenso definiti "ibridi" che adottano cioè un approccio che è una via di mezzo tra due altri protocolli, un po' come fanno (giusto per fare un esempio) le auto ibride, nelle quali abbiamo contemporaneamente la presenza sia di un motore a scoppio che di motori elettrici; in questo caso (restando sull'esempio delle auto) non si può dire ne che un'ibrida sia un'auto a benzina, ne che sia un'auto elettrica, è quindi, allo stesso tempo, sia l'una che l'altra cosa e contemporaneamente nessuna delle due.

I protocolli di consenso, quindi, sono il vero e proprio motore della tecnologia blockchain la quale semplicemente non potrebbe funzionare senza questi algoritmi. Nei prossimi paragrafi inizieremo col descrivere il più famoso dei protocolli, quello cioè che regola il funzionamento di Bitcoin, chiamato POW (acronimo di proof of work, in italiano prova del lavoro), ma avremo modo di descrivere anche come funzionano i protocolli che consentono il funzionamento di monete che sono diventate (quasi) altrettanto famose di Bitcoin come nel caso di ETH (che con Casper introdurrà gradualmente il POS, acronimo di Proof of Stake, nel suo protocollo di consenso), Cardano ADA ed EOS (che usano un protocollo sostanzialmente DPOS, acronimo di Delegate Proof of Stake), Ripple e Stellar (che usano sostanzialmente un protocollo BTF, acronimo di Byzantine Fault Tolerance).

Tutti questi differenti protocolli si pongono lo stesso obiettivo, generare il consenso sulla rete per renderla resiliente agli attacchi, ma lo fanno usando approcci anche radicalmente differenti tra loro. L'avvertenza per il lettore è che si tratta di temi mediamente complessi, per cui quella che seguirà nei prossimi paragrafi non è esattamente una lettura rilassante e richiede un po' di concentrazione per seguire il filo di tutto il discorso; la promessa che mi sento di fare, però, è che una volta "scollinati" i prossimi paragrafi il lettore si troverà di fronte una strada tutta in discesa e scoprirà di padroneggiare i concetti fondamentali senza i quali riuscire a comprendere questa tecnologia sarebbe sostanzialmente impossibile.

4.1 Proof of work (POW)

Come non è possibile parlare di blockchain senza parlare di Bitcoin allo stesso modo non è possibile parlare di Bitcoin senza parlare anche del protocollo POW che ne regola il funzionamento; nel descrivere come funziona il protocollo POW abbiamo quindi l'opportunità di riprendere i concetti presentati nel terzo capitolo di questo testo di modo da fare un ripasso complessivo di quanto sin qui descritto e chiarire definitivamente le idee anche del lettore più spaesato.

Abbiamo perciò detto che la blockchain è un data base distribuito in cui tutti i nodi che partecipano alla rete possiedono una copia del registro su cui sono archiviate tutte le transazioni registrate dalla rete stessa sin dalla sua nascita; tali transazioni sono accorpate all'interno di blocchi che la rete processa e valida ogni dieci minuti. Ognuno di questi blocchi è quindi legato (come in una catena) al blocco precedente attraverso un hash. Abbiamo anche definito che un hash è "una funzione matematica non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza minore"; quello che non abbiamo detto è che non tutto il blocco nella sua interezza viene sottoposto alla funzione di hash ma solo una sua parte. Per semplicità abbiamo suggerito di immaginare il blocco come una sorta di scatola che include tutte le transazioni ordinate dagli utenti negli ultimi dieci minuti, ebbene, restando a questo esempio, adesso immaginiamo che su ognuna di queste scatole sia presente una specie di etichetta che ne descrive sinteticamente il contenuto.

Questa specie di etichetta prende il nome di “header” (testa del blocco, in italiano); nella testa del blocco, quindi, sono contenuti una serie di dati e, precisamente, il numero di versione del protocollo, l’hash del blocco precedente, l’hash di un sommario delle transazioni del blocco corrente, una timestamp (cioè data e ora di creazione del blocco) e il grado di difficoltà stabilito per risolvere il “rompicapo” del blocco corrente (del grado di difficoltà avremo modo di parlare a breve). A tutti questi dati ne viene aggiunto ancora uno che prende il nome di “nonce”.

Usiamo quindi ancora una volta wikipedia per ricavare una definizione di cosa sia il nonce e scopriamo che "*in crittografia il termine nonce indica un numero, generalmente casuale o pseudo-casuale, che ha un utilizzo unico. Nonce deriva infatti dall'espressione inglese for the nonce (per l’occasione)*".

Ora, abbiamo avuto modo già in diverse occasioni di dire che i miners partecipano a una gara che consiste in un rompicapo matematico e che solo il miner che vince questa competizione riceve (dopo che almeno il 50% più uno dei nodi della rete ha verificato la validità della soluzione proposta) la ricompensa per aver svolto il lavoro; ma in cosa consiste questo rompicapo? Semplice, la rete definisce un target e il compito del miner è trovare un valore del nonce che restituisca un hash di valore inferiore a quello definito dal target; per riuscirci il miner deve procedere per tentativi, quindi parte generalmente da un valore pari a zero ed aggiunge un’unità fino a quando non trova un valore del nonce adatto a vincere la competizione. Quando questo avviene trasmette tale valore al resto della rete che quindi verifica che la soluzione proposta sia valida e procede alla validazione del blocco trascrivendolo sulla blockchain.

A questo punto approfittiamo anche per chiarire un altro aspetto che fino a questo momento non avevamo avuto modo di affrontare e cioè quello relativo alla difficoltà definita dalla rete per risolvere il nostro “rompicapo”; abbiamo detto che sulla rete bitcoin viene generato un nuovo blocco ogni dieci minuti e che per risolvere il nostro rompicapo è necessario procedere per tentativi elaborando così una quantità enorme di calcoli al secondo.

Ora, quello che succede è che il livello di difficoltà previsto dalla rete per minare un singolo blocco si adatta alla potenza di calcolo che la rete stessa è capace di esprimere di modo che il valore di 10 minuti per la generazione di ogni blocco rimanga costante nel tempo; in pratica man mano che la rete diventa più grande, e quindi conseguentemente aumenta la potenza di calcolo che è capace di esprimere, la difficoltà prevista per trovare un valore del nonce che rispetti il target aumenta, in maniera tale che sia possibile fare in modo che vengano generati sei nuovi blocchi ogni ora (uno ogni dieci minuti) indipendentemente da quanto cresca la potenza di calcolo espressa dalla rete.

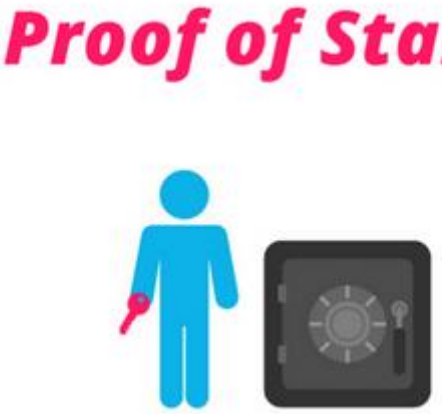
A questo punto diventa facile comprendere un altro aspetto di questa tecnologia e cioè che i Bitcoin non vengono emessi (come avviene con la normale valuta) ma appunto minati, cioè estratti; è esattamente questa la ricompensa che il miner riceve per aver risolto il rompicapo, un ammontare che inizialmente era di 50 bitcoin per ogni blocco validato ma che continua a diminuire con una progressione geometrica ogni 210mila blocchi circa fino a quando non si raggiungerà il limite previsto di 21mln di Bitcoin estratti. Questo processo di dimezzamento della ricompensa dei miners prende il nome di “halving”.

Esiste quindi un limite temporale superato il quale il miners cesserà sostanzialmente di essere tale, nel senso che validando un blocco non estrarrà più un bel nulla e questo, si stima, avverrà intorno all’anno 2140; ma allora, si dirà il lettore più attento, a quella data i miners cesseranno di essere ricompensati per il lavoro svolto? Assolutamente no, perché ogni transazione include anche una piccola commissione che va proprio a beneficio del miner, ad oggi tali commissioni si sommano a quanto estratto dal minatore, dopo la fatidica data del 2140 tali commissioni rappresenteranno invece interamente la ricompensa per il lavoro effettuato (dal momento che pur validando il blocco

non sarà più possibile estrarre alcun Bitcoin, essendo stato raggiunto il limite massimo di 21 milioni di monete).

4.2 Proof of Stake (POS)

Fino adesso abbiamo descritto il funzionamento di una blockchain secondo le soluzioni proposte in Bitcoin, negli anni, però, gli sviluppatori si sono impegnati a sviluppare soluzioni differenti per gestire il consenso all'interno della rete, contribuendo così a dare vita a un eco-sistema piuttosto variegato; il lettore più attento a questo punto inizierà a chiedersi perché se Bitcoin è così sicuro ed affidabile ci sia la necessità di sviluppare monete che funzionino in maniera differente.



Il principale motivo è che il protocollo di consenso POW, che consente il funzionamento della blockchain Bitcoin, comporta un grande dispendio di energia per funzionare; i miners, infatti, come abbiamo avuto modo di spiegare, sono in competizione tra loro per risolvere un "rompicapo" matematico e per farlo procedono per tentativi.

Questo implica che tutti i nodi della rete eseguano contemporaneamente lo stesso lavoro nel tentativo di risolvere il rompicapo e che i loro computer eseguano un'elevata mole di calcoli contemporaneamente, consumando al contempo una grande quantità di energia; il protocollo, non per caso, si chiama infatti "prova del lavoro" e per eseguire quel lavoro è necessario consumare energia. E' proprio per questo che alcuni sviluppatori si sono posti il problema se si potesse creare un protocollo altrettanto sicuro per gestire il consenso sulla rete senza dover consumare un così importante quantitativo di energia; molti tentativi sono stati quindi fatti in questa direzione, dando vita, come accennato, a numerosi differenti protocolli di consenso, tra i quali uno dei più anziani in circolazione è il protocollo POS, acronimo di proof of stake. Una delle differenze principali che caratterizzano le monete basate su POS rispetto a quelle basate su POW è che scompare la figura del minatore; in questi sistemi, infatti, le monete non vengono "minate" ma "forgiate".

Questo implica inevitabilmente che all'interno del blocco da validare non sia presente un quantitativo di monete da estrarre, i nodi che partecipano alle reti POS, quindi, vengono ricompensati sulla base delle sole commissioni sulle singole transazioni; la ricompensa, quindi, rimane comunque un aspetto fondamentale nel funzionamento della rete ed è centrale indipendentemente dal tipo di protocollo che si usa per gestire il consenso. Possiamo quindi affermare, in altre parole, che non può esserci blockchain senza ricompensa.

Ma tentiamo di capire come i sistemi POS gestiscono il consenso; sostanzialmente nel protocollo POW la validazione dei blocchi avviene sulla base della potenza di calcolo che un nodo è capace di esprimere; più alta è la potenza di calcolo di cui si dispone più probabilità ci sono di risolvere per primi il rompicapo matematico. Nei sistemi POS questo meccanismo è sostituito dalla posta in gioco;

quello che succede, in pratica, è che il diritto a validare il blocco (ricevendo così la ricompensa prevista) viene acquisito sulla base della quantità di monete che il nodo vincola nel proprio portafoglio. All'aumentare delle monete che si vincolano, quindi, aumentano anche le possibilità che la rete decida di selezionare quel nodo per validare il blocco corrente; questo pone però implicitamente il rischio che la rete finisca facilmente col diventare centralizzata, dal momento che un ristretto gruppo di nodi, capace di accaparrarsi il grosso della fornitura di monete in circolazione, finirebbe inevitabilmente per essere continuamente selezionato per la validazione del nuovo blocco, accumulando ancora più valuta e consolidando così ulteriormente il proprio "monopolio".

Per scongiurare questo rischio i progetti che usano un protocollo POS usano approcci differenti nella selezione dei nodi validatori, c'è chi adotta un sistema randomizzato (cioè di selezione casuale), chi adotta un sistema di deleghe (lo vedremo meglio nel prossimo paragrafo), chi tiene in considerazioni fattori come l'anzianità dello stakeholder; per quanto riguarda la sicurezza della rete, invece, questa viene garantita attraverso una specie di sistema di multe. Abbiamo detto, infatti, che il nodo per partecipare alla validazione dei blocchi deve vincolare un certo numero di monete; questo "deposito" rappresenta sostanzialmente una garanzia, per cui se il nodo non rispettasse le regole perderebbe la posta in gioco, cioè il deposito.

Dal momento che la possibilità di essere selezionato come nodo validatore aumenta all'aumentare della posta in gioco, i nodi che vogliono guadagnare una maggiore influenza sulla rete devono vincolare importi sempre maggiori e questo implica sostanzialmente un incentivo a comportarsi in maniera corretta perché, in caso contrario, perderebbero l'importo che hanno vincolato.

4.3 Delegate Proof of Stake (DPOS)

Nel paragrafo precedente abbiamo detto che lo scopo del protocollo POS è di gestire il consenso sulla rete evitando un consumo eccessivo di energia; per riuscirci seleziona i nodi validatori sulla base della posta in gioco, cioè sulla base di quante monete ognuno di questi nodi è disposto a vincolare per partecipare al processo di validazione.

Come abbiamo avuto modo di evidenziare, però, nel tentativo di risolvere un problema se n'è creato un altro; se da un lato, quindi, i protocolli POS sono riusciti effettivamente a ridurre in maniera importante il dispendio di energia necessario per far funzionare la rete, dall'altro questo meccanismo rischia di alimentare la centralizzazione della rete, mettendola sostanzialmente sotto il controllo degli utenti più facoltosi che sono anche quelli che possono vincolare il maggior numero di monete per partecipare al processo di validazione.

Di conseguenza ogni progetto che usa un protocollo POS ha introdotto dei meccanismi atti a ridurre questo tipo di rischio; una delle primissime implementazioni in questo senso riguarda la dinamica della delega che ha quindi generato quello che viene chiamato DPOS, acronimo di Delegate Proof of Stake. Per evitare la centralizzazione questo tipo di protocollo ha introdotto una dinamica di voto simile a quella prevista nelle democrazie; se quindi in un sistema democratico si vota per cedere la delega a governare, in un sistema DPOS si vota per cedere la delega a validare un blocco.

Molti dei principali osservatori, però, hanno criticato aspramente questo tipo di approccio bollandolo apertamente come una truffa; in realtà, secondo quanto affermano queste persone, il DPOS è tutto tranne che democratico. Per capire le ragioni di questa critica è necessario

comprendere come funziona questo tipo di protocollo; diciamo subito che nelle blockchain che usano Dpos a provvedere alla convalida delle transazioni sono un gruppo ristretto di "delegati" che vengono eletti dall'intera rete con un sistema molto simile, come abbiamo appena accennato, a quello della democrazia rappresentativa. Il problema, non da poco a ben vedere, è che mentre in una democrazia rappresentativa "uno vale uno" (che non è solo il motto di un noto partito politico italiano, ma un principio per cui il voto di ogni persona ha lo stesso valore, cioè vale uno), nel protocollo DPOS ogni moneta posseduta vale un voto.

Chiunque può quindi facilmente comprendere come questo protocollo di consenso non faccia altro che premiare gli utenti più facoltosi (quelli cioè che possiedono più valuta), i quali inevitabilmente sono nella posizione di esprimere più potere di voto, facendoci di conseguenza cadere di nuovo in un sistema sostanzialmente centralizzato. Proviamo a fare un esempio concreto per capire di cosa stiamo parlando ed ipotizziamo che della rete facciano parte solo quattro persone, che chiameremo Anna, Maria, Claudio e Roberto. Ognuna di queste persone possiede 10 monete l'una ad eccezione di una, Claudio, che ne possiede 40; ora, se sia Anna, che Maria e Roberto votano per delegare Maria mentre Claudio vota per delegare Anna quello che succede è che anche se Maria raccoglie i voti di tre differenti soggetti lo fa per un numero di monete complessivamente pari a 30 mentre Roberto (da solo) vota per un numero di monete pari a 40 e quindi definisce sostanzialmente da solo l'esito della votazione che, nell'esempio in questione, vedrebbe prevalere Anna a scapito di Maria.

Quello che succede nei sistemi che usano Dpos è che i soggetti che possiedono più monete sono quelli che decidono davvero mentre tutti gli altri, rendendosi conto della loro sostanziale marginalità, si limitano a smettere di votare; quello che emerge da questo quadro è praticamente un'oligarchia, un modello cioè in cui i soggetti più ricchi decidono tutto e i soggetti più poveri si ritrovano impossibilitati a far valere il peso del proprio voto persino qualora riuscissero ad aggregarsi tutti insieme. Di conseguenza, affermano i detrattori del protocollo DPOS, le monete che usano questo tipo di sistema per gestire il consenso andrebbero viste come sostanzialmente centralizzate.

4.4 Byzantine Fault Tolerance (BFT)

La questione del consenso è un tema abbastanza vecchio in ambito informatico e precede di parecchi anni la nascita di Bitcoin; capire quindi come si possa costruire la fiducia in un sistema in cui non c'è conoscenza reciproca e nel quale è facile ipotizzare la presenza di attori malevoli (o di componenti che semplicemente non funzionano a dovere), è sempre stato un tema di una certa centralità nell'ambito informatico.

A riprova di quanto questo sia vero basti evidenziare come già nel 1982, ben prima di internet quindi, i matematici Leslie Lamport, Marshall Pease e Robert Shostak ebbero modo di sviluppare quello che oggi è comunemente chiamato "il problema dei generali bizantini"; in questo modo, immaginando la metafora dei generali, i matematici in questione riuscirono a rendere la comprensione del problema alla portata di chiunque. Il problema dei generali (li chiamarono "bizantini" per evitare che qualche popolo potesse risentirsi se vi fosse stato un richiamo a una nazione effettivamente esistente) ipotizza quindi che vi siano delle persone alla guida di diversi schieramenti dislocati in aree differenti tra loro e che i generali a comando di queste forze si ritrovino a dover coordinare un attacco contro una città nemica; il problema nasce dal fatto che i generali in questione possono comunicare tra loro solo attraverso dei messaggi e corrono il rischio che i messaggeri a cui affideranno queste comunicazioni possano essere corrotti dalle forze nemiche e indotti ad alterare il reale contenuto del messaggio.

Facciamo un esempio per capirci e riduciamo le variabili possibili di questo messaggio a sole due possibilità: attacca, ritirati. Ora, se l'ordine vero fosse di attaccare un messaggero corrotto potrebbe

consegnare un messaggio in cui è riportato l'ordine di ritirarsi, rendendo quindi l'assedio meno efficace o, al contrario, se l'ordine fosse di ritirarsi il messaggero corrotto potrebbe consegnare l'ordine di attaccare condannando alla disfatta il generale che eseguisse quell'ordine. Una delle soluzioni più comuni a questo problema viene definita Byzantine-fault-tolerant (BFT) e si basa sul concetto che i messaggi possano anche essere falsificati ma che questo è irrilevante fintanto che il numero dei messaggeri corrotti non si rivela essere pari o superiore a un terzo, si stabilisce, in pratica, una sorta di "soglia" per il conseguimento del consenso (pari quindi al 66% dei nodi che fanno parte di una rete).

Tutto questo, come puoi facilmente capire, funziona tanto meglio quanto maggiori sono le dimensioni della rete; se (restando alla nostra metafora) i generali fossero soltanto due il problema sarebbe sostanzialmente irrisolvibile. All'aumentare del numero di nodi (generali) che devono prendere una decisione aumenta anche la sicurezza del sistema il quale può permettersi persino che un nodo su tre tra quelli che fanno parte della rete sia corrotto (trasmetta cioè informazioni false), senza che questo comprometta in alcun modo il funzionamento della rete, perché tanto ad essere considerata "vera" sarà l'informazione intorno alla quale si è costruito il consenso del 66% dei nodi.

Nei sistemi che usano la BFT per la gestione del consenso, quindi, scompare la figura del miner, sostituito dal "nodo validatore" (l'equivalente del generale) ed anche per questo motivo questo tipo di soluzione è quella più comunemente impiegata nei progetti che sfruttano la tecnologia DLT.

5. Cosa sono le criptovalute

Dopo aver definito cosa sia una blockchain, in che modo si differenzi dalla tecnologia DLT, come funziona il processo di validazione di un blocco e in cosa consistano alcuni dei più comuni protocolli di consenso che rappresentano il cuore di ogni data base distribuito, passiamo ad occuparci più strettamente di criptovalute; tenteremo però di farlo non solo da un punto di vista meramente tecnico, ma anche filosofico, interrogandoci su concetti come quello di "valore" e "denaro".

Detto questo diciamo subito che dare una definizione di cosa sia una criptovaluta non è cosa scontata; nonostante Bitcoin esista da dieci anni, infatti, ed abbia dato vita a un vero e proprio eco-sistema intorno a se, non siamo ancora stati capaci di trovare una definizione comunemente condivisa di cosa sia una criptovaluta.

Basta farsi un giro sul web per verificare come ognuno dei protagonisti di questo mondo (i maggiori sviluppatori, i docenti universitari, i CEO delle aziende che operano in questo settore, etc) abbia avuto modo nel tempo di fornire una propria personale definizione di questa parola, senza che nel tempo emergesse quella capace di mettere d'accordo tutti.

Di conseguenza quello che farò sarà fornire la mia definizione di cosa sia una criptovaluta, avendo cura però (come sto facendo in questo momento) di avvisare il lettore che quella che seguirà non è LA definizione, ma UNA definizione di cosa siano le criptovalute. Personalmente, quindi, dopo qualche anno di riflessione, sono arrivato a definire una criptovaluta come "una unità di dati della quale è possibile stabilire con certezza l'origine, chi ne detiene la proprietà e a cui è possibile attribuire un valore convenzionalmente accettato da chiunque".

Per capire bene di cosa stiamo parlando sarà necessario fare degli esempi concreti; abbiamo già accennato di come sia possibile seguire ogni singola transazione BTC attraverso dei siti web che prendono il nome di explorer, bene, andiamo allora a indagare uno di questi siti. Se cerchiamo "explorer bitcoin" su google uno dei primi risultati è il sito "blockchain.com" che ci mostra, se appena scrolliamo verso il basso, una schermata in cui elenca la successione degli ultimi blocchi validati; cliccando su un qualunque blocco, quindi, possiamo pendere visione di alcune informazioni come ad esempio il numero di transazioni che contiene, il numero progressivo che identifica il blocco (cioè l'altezza del blocco stesso), il valore complessivo delle transazioni che contiene, la timestamp (cioè data e ora in cui il blocco è stato generato) e ancora molte altre informazioni.

Quello che ci interessa notare è che ogni blocco ha un peso, il peso massimo, ma sarebbe meglio parlare di "dimensione massima", di un blocco BTC (giusto per fare un esempio) è di 1MB (anche se la recente introduzione di SegWit ha prodotto un cambiamento in questo senso, ma è un argomento che non avremo modo di trattare adeguatamentein questo testo); all'interno di ogni blocco troviamo i dati relativi ad ogni transazione, quindi possiamo tranquillamente cliccare sopra una a caso per vedere quali informazioni contiene quella singola transazione. Tra i dati a nostra disposizione, oltre ovviamente all'ammontare dell'importo scambiato, abbiamo il blocco all'interno del quale è stata validata, il numero di conferme ricevute, la timestamp, il peso, la dimensione e ancora molto altro.

Perché scrivo tutto questo? Perché sulla blockchain andiamo ad archiviare un dato e quel dato può essere qualunque cosa, può essere ad esempio una cartella clinica di un paziente, può essere il diritto di proprietà su un'automobile, o qualunque altra cosa ci venga in mente. Attualmente, se facciamo l'esempio di Bitcoin, la blockchain registra delle transazioni; ma quelle che stiamo chiamando transazioni sono sostanzialmente dati, informazioni, e quindi possono essere qualunque tipo di informazione.

Una blockchain, in altre parole, non è altro un libro che racconta una storia, più precisamente la storia che racconta è quella della successione cronologica di tutte le transazioni processate e validate dalla rete. Se volessi creare un registro delle automobili immatricolate usando una blockchain alla quale fosse agganciata una criptovaluta potrei farlo facilmente già oggi; in pratica avremmo una moneta che corrisponde alla proprietà di una determinata auto e su quella moneta ci scriveremmo tutti i dati dell'auto (marca, modello, anno di immatricolazione, etc) e i dati del proprietario (anno di acquisto, prezzo di acquisto, nome, cognome, etc). Il giorno in cui l'auto venisse venduta a un nuovo soggetto questi riceverebbe insieme all'auto anche la relativa criptovaluta sulla quale si andrebbero ad aggiungere i dati del nuovo proprietario.

Quello che dobbiamo fare, quindi, è smettere di immaginare una criptovaluta come fosse un biglietto da un dollaro e iniziare ad immaginarla invece (al pari di un blocco) come una piccola scatola; in quella piccola scatola ci puoi mettere qualunque cosa, qualunque tipo di informazione, e a quel punto l'informazione puoi anche scambiarla con un soggetto terzo ed attribuirle un valore sulla base di una convenzione. Quando parliamo di Bitcoin, per esempio, ogni moneta è come una piccola scatola che contiene un'informazione, quindi la domanda a questo punto è: qual è l'informazione che stiamo commerciando quando ci scambiamo un Bitcoin? L'informazione che ci scambiamo è la più essenziale di tutte, il diritto di proprietà su quella scatola (in pratica la moneta)

che ci siamo scambiati; quando io mando un Bitcoin dal mio indirizzo all'indirizzo di un'altra persona l'informazione che viene archiviata sulla blockchain è che quella moneta (non un'altra, non una qualunque di quelle in circolazione, ma esattamente quella moneta) cessa di essere di proprietà del mio indirizzo (e cioè mia) e diventa proprietà di un nuovo indirizzo (cioè della persona che controlla quel nuovo indirizzo). In che modo possiamo essere sicuri della proprietà univoca della moneta? Perché ne possediamo la chiave privata. Di questo concetto, e di altri ugualmente importanti, ci andremo ad occupare nei prossimi paragrafi.

5.1 Cosa conferisce valore a una criptovaluta

Prima di descrivere come funziona una criptovaluta, cos'è una chiave pubblica e una privata, cosa sono i wallet e gli indirizzi, tra le primissime domande che le persone che scoprono questa tecnologia si fanno abbiamo qualcosa del tipo "ok, ma chi stabilisce il valore di una criptovaluta?"; per prima cosa, quindi, tentiamo di rispondere a questa domanda.

La risposta è che a definire il valore di una criptovaluta è il mercato; ma questo vale per qualunque tipo di bene o prodotto, ad esempio: chi definisce il valore dell'oro? Chi è che decide che un grammo d'oro possa essere comprato o rivenduto a quel determinato prezzo? La risposta, ed è la stessa sia che si parli di oro che di criptovalute, è che lo decide il mercato, attraverso gli scambi portati avanti tra chi il bene lo vende e chi vuole comprarlo. Immaginiamo di essere al mercato ortofrutticolo, se sul banco del contadino fosse rimasta una sola mela e due persone volessero comprarla il prezzo della mela lieviterebbe, se ci fossero sempre due persone a voler comprare una mela ma ci trovassimo questa volta di fronte a centinaia di contadini, ognuno dei quali dispone di migliaia di mele, il prezzo si abbasserebbe.

Quindi una delle prime regole sul mercato è che la scarsità genera valore; dal momento che non ci saranno mai più di 21mln di monete chiunque capisce che Bitcoin è un bene caratterizzato da una scarsità naturale, per cui all'aumentare del numero di persone che vogliono comprarlo il prezzo di Bitcoin, in maniera assolutamente naturale, sale. Più gente accetta questa nuova convenzione stabilita da Bitcoin, che cioè si può usare una criptovaluta con una funzione identica a quella del denaro propriamente detto, più il valore di 1BTC finirà col salire di conseguenza.

Del resto siamo sette miliardi di persone, ma ci sono solo 21mln di monete in circolazione, come si fa a soddisfare la domanda di tutta questa gente? Semplice, a differenza di quanto avviene con una banconota da 5€ che deve per forza rimanere integra per avere valore, 1BTC non è un bene fisico, può essere "spezzettato", si possono cioè, in altre parole, possedere frazioni di Bitcoin. Attualmente 1BTC ha un prezzo pari a circa 3.000$, che succede se io non possiedo 3.000$ ma voglio comunque acquistare Bitcoin, ad esempio per un importo complessivo di 300$? Semplice, comprerò un decimo di BTC, cioè 0.1BTC. E se ne volessi comprare (o spendere, il ragionamento è ovviamente lo stesso), solo 30$? Allo stesso modo comprerei (o spenderei) un centesimo di BTC, cioè 0.01BTC.

Stiamo quindi iniziando a capire che il prezzo di 1BTC è definito dal mercato, che essendoci un numero di monete limitato e prestabilito questo crea un effetto scarsità che produce l'aumento di valore e che è possibile acquistare e/o spendere anche frazioni di Bitcoin, e non siamo quindi, in altre parole, costretti a spendere la moneta nella sua interezza.

Quello che è importante capire, in ogni caso, è che il valore di 1BTC, prima ancora che dalle decisioni del mercato, dipende dal diffondersi di una convenzione; all'aumentare, cioè, del numero di persone che accettano la convenzione (accettano cioè di usare Bitcoin come moneta), aumenta inevitabilmente anche il valore. Se domani tutte le persone che accettano Bitcoin come forma di pagamento decidessero che non vogliono più farlo allora il prezzo di Bitcoin crollerebbe per il semplice motivo che non essendo più possibile scambiarlo con altre valute o con un bene, un

prodotto o un servizio, il prezzo crollerebbe inevitabilmente. Lo stesso discorso potremmo farlo per l'oro, ricordandoci però che parliamo di un materiale che non ha il solo scopo di rappresentare una riserva di valore (che in quanto tale può essere scambiata) ma che ha anche un mercato suo (ad esempio tra i gioiellieri); tra i fattori che influenzano, ad esempio, il prezzo dell'oro abbiamo l'inflazione, il che significa che quando il valore di una valuta nazionale diminuisce questo provoca un aumento di valore dell'oro. Perché succede questo? Perché le persone sono convinte che mentre una moneta può deprezzarsi fino ad arrivare a non valere più nulla (vedi ad esempio il caso del Bolivar venezuelano), la stessa cosa non può succedere a un bene fisico come l'oro.

Quello che sta avvenendo con Bitcoin è che la stessa convenzione si sta venendo a consolidare anche per quel che riguarda le criptovalute, tanto che quando una moneta sovrana finisce sotto pressione (abbiamo avuto un caso del genere con la lira turca nel corso del 2018) le persone iniziano a convertire i loro risparmi dalla valuta nazionale alla nuova criptovaluta; durante i giorni più pesanti della crisi della lira turca, infatti, il volume di scambi con Bitcoin in Turchia saliva alle stelle. I detrattori delle criptovalute, sulla base di un'analisi simile, arrivano a sostenere che è proprio questo il motivo per cui il vero valore di Bitcoin è zero, perché si basa sul nulla, su di una semplice convenzione/convinzione. In realtà (ma io non posso che vederla così) si sbagliano profondamente e ci sono numerosi aspetti che non tengono in considerazione e che rendono Bitcoin una riserva di valore migliore dell'oro. Intanto sia l'oro che Bitcoin sono presenti in quantità limitate e predeterminate, in pratica il quantitativo di oro disponibile è limitato, così come lo è il quantitativo di Bitcoin disponibili (non ci saranno mai più di 21mln di monete in circolazione); ma mentre io posso tranquillamente andarmene in giro con 1mln di dollari in tasca convertiti in Bitcoin, andarmene in giro con 1mln di dollari in oro diventa più complicato.

Se voglio conservare 10mln di dollari in oro mi serve un magazzino e delle guardie che prevengano i furti; se voglio conservare 10mln di dollari in Bitcoin quello che mi serve è un dispositivo della grandezza di una chiavetta USB, non mi servono guardie armate per proteggerlo perché posso nasconderlo ovunque e soprattutto perché anche se mi rubassero il dispositivo (o lo perdessi), potrei sempre recuperare i miei soldi usando un "seme di ripristino" (ne parleremo meglio quando ci occuperemo di Wallet).

E' difficile andare al mercato e comprare un chilo di verdura pagando in oro, è facilissimo andare al mercato e comprare un chilo di verdura pagando in Bitcoin; in pratica le criptovalute, almeno sul piano concettuale, uniscono in una sola entità le caratteristiche dell'oro con quelle della moneta.

5.2 Come funziona una criptovaluta

Fin qui abbiamo spiegato che una criptovaluta può essere impiegata non solo per scambiarsi valore (cioè denaro) ma qualunque tipo di dato e/o informazione (una cartella clinica ad esempio, o un certificato di proprietà), abbiamo poi capito che il valore di una criptovaluta lo definisce sostanzialmente il mercato e che tanta più gente utilizza una certa criptovaluta tanto più quella tende ad assumere sempre più valore (a patto che, come accade con Bitcoin, ci sia una quantità di monete pre-determinata e limitata in circolazione).

Adesso che abbiamo spiegato tutto questo tentiamo anche di capire come sia possibile tecnicamente usare una criptovaluta al pari di una moneta e per farlo partiamo dal modo in cui funziona il sistema attuale; normalmente abbiamo tutti un conto corrente in banca, agganciato al conto corrente abbiamo una carta bancomat che ci permette sia (ad esempio) di ricevere l'accredito del nostro stipendio, sia di spendere ovunque i nostri soldi (tendenzialmente anche al bar per pagare un caffè, se non fosse che il costo delle commissioni rende poco vantaggioso per gli esercenti farsi pagare in questo modo).

Con Bitcoin il ruolo che prima aveva la nostra banca (conservare il denaro) viene svolto dai "wallet", dei portafogli virtuali che ci permettono non solo di conservare le nostre criptovalute ma anche di movimentare i nostri soldi usando dispositivi come i computer o gli smartphone in maniera del tutto simile a come facciamo con la nostra carta bancomat. Un modo semplice per capire come funziona Bitcoin, in altre parole, è immaginare che un programma open source installato sul nostro pc di casa o una app per smartphone installata sul nostro telefonino, ci fornisca gli stessi identici servizi che ci fornisce una banca attraverso l'home banking.

Ma facciamo un esempio concreto per capire bene di cosa stiamo parlando; immaginiamo due amici seduti al bar e chiamiamoli Anna e Paolo. Anna ha bisogno che qualcuno le imbianchi casa e Paolo nella vita di mestiere fa l'imbianchino; i due concordano quindi che Paolo tinteggerà la casa di Anna a fronte di un compenso di 2BTC. Dal momento che Anna vuole pagare in Bitcoin e che Paolo non ha la minima idea di cosa siano questi dannati Bitcoin di cui tutti parlano, Anna (da buona amica) si offre di fargli capire come funzionano le criptovalute. Il giorno dopo Anna si reca a casa dell'amico, si collega a internet col computer di Paolo e scarica un programma (il wallet) che Paolo potrà usare per gestire i pagamenti; segue quindi le indicazioni durante il processo di installazione guidata e completati tutti i vari passaggi. Quando finalmente Anna termina di scaricare e installare il primo wallet di Paolo, clicca sul tasto "ricevi" (di modo da visionare l'indirizzo a cui deve mandare i Bitcoin), scatta una foto con il suo smartphone al Qrcode (una specie di codice a barre che contiene le coordinate per raggiungere quell'indirizzo) che il programma le mostra sul monitor ed invia il pagamento pattuito di 2BTC. Tutto questo avviene esattamente come l'abbiamo descritto, come se stessimo utilizzando Paypal, non servono conoscenze particolari per fare un pagamento con Bitcoin, per riceverlo o per avere un proprio wallet; chiunque può usare una criptovaluta per gestire i propri pagamenti, ma come funziona? In che modo viene gestita la transazione? Proviamo a descriverlo in maniera semplice.

Quando Anna ha installato il wallet (cioè il portafoglio virtuale) sul computer di Paolo, una delle prime cose che questo programma ha fatto è stata generare una chiave privata (segreta); subito dopo aver creato questa chiave privata lo stesso programma l'ha usata per generare una nuova chiave, questa volta pubblica, e, infine, ha utilizzato la chiave pubblica per generare l'indirizzo sul quale Paolo ha ricevuto i suoi 2BTC. Le cose iniziano a complicarsi, inevitabilmente, perché stiamo usando parole come "chiave pubblica", "chiave privata" e "indirizzo" senza avere un'idea chiara di cosa queste parole significhino. Per capirci qualcosa di più immaginiamo una cassa che contiene 2 diamanti (i 2BTC che Paolo ha ricevuto), chiusa da un lucchetto, da spedire dalla casa di Anna a quella di Paolo; ora, secondo questo esempio, il lucchetto (che tiene la cassa con dentro i due diamanti chiusa) equivale alla chiave pubblica, i due indirizzi equivalgono alle coordinate della casa di Paolo (a cui vogliamo spedire la cassa) e della casa di Anna (dalla quale parte la cassa) e la chiave privata, infine, equivale ovviamente alla chiave che ci permette di aprire il lucchetto con il quale la cassa viene tenuta chiusa.

Nonostante quindi questi tre dati siano correlati tra loro (l'indirizzo, cioè, si genera a partire dalla chiave pubblica, la quale viene generata a sua volta a partire da quella privata), le funzioni matematiche utilizzate per fare questo processo non sono invertibili e questo permette che sia possibile, partendo dalla chiave privata, risalire alla chiave pubblica e all'indirizzo del wallet, ma non fare il percorso inverso. La chiave privata rimane quindi privata, non c'è modo di ricavarne una a

partire dalla sua chiave pubblica; tornando al nostro esempio, quindi, Paolo riceve sul proprio indirizzo 2BTC, ma cosa succede se decide successivamente di spenderne la metà? E come avviene la transazione? Immaginiamo che Paolo abbia una sorella (Francesca) e che decida di volerle fare un regalo; dal momento che lei ha già un wallet installato sul suo smartphone, Paolo deve solo chiederle il suo indirizzo e quando Francesca glielo gira via mail, subito provvedere ad inviarle 1BTC.

Quello che succede a questo punto è che il wallet procede a creare una nuova transazione, che poi altro non è che un messaggio trasmesso ai nodi che compongono la rete e che registrano le varie operazioni sulla blockchain; possiamo paragonare, per fare un esempio, una transazione ad una specie di scrittura in partita doppia che contiene da un lato i valori degli input (i conti dai quali parte il pagamento ed ovviamente l'entità del pagamento stesso) e dall'altro i valori degli output (i conti beneficiari del pagamento e delle relative somme).

Poco fa abbiamo immaginato la chiave pubblica come un lucchetto che chiude un cassa (con dentro due diamanti, che rappresentavano i nostri Bitcoin), ecco, una transazione la possiamo immaginare anche, più semplicemente, come il messaggio con cui comunichiamo alla rete di spostare la cassa con dentro i due diamanti da un indirizzo all'altro. Ma attenzione che nella cassa ci sono dentro due diamanti, non possiamo quindi prendere un diamante dalla cassa chiusa e lasciarci dentro l'altro; dobbiamo necessariamente aprire la cassa, prendere i due diamanti, riporre un diamante in una nuova cassa con un nuovo lucchetto (destinata a Francesca che sarà l'unica a possedere la chiave per aprirla), mentre il diamante che resta non potremo rimetterlo dove lo abbiamo preso ma andremo quindi anche in questo caso a riporlo in una nuova cassa con un nuovo lucchetto e una nuova chiave che rimarrà ancora nelle mani di Paolo.

In tutto questo manca ancora un aspetto fondamentale e cioè che ogni transazione contiene al suo interno l'output dell'ultima transazione eseguita (esattamente come succede ai blocchi, i quali contengono sempre l'hash del blocco precedente); quello che stiamo facendo, quindi, quando spostiamo una somma in BTC non è altro che firmare con la nostra chiave privata una transazione e cioè un messaggio che contiene l'hash della transazione precedente, la chiave pubblica del destinatario ed ovviamente le informazioni riguardanti la transazione in corso. Tornando alla nostra transazione tra Paolo e Francesca, quindi, è un po' come se Paolo scrivesse un biglietto in cui comunica alla rete che "l'oggetto di questa transazione, pari ai 2BTC precedentemente ricevuti da Anna, va diviso in 1BTC da spedire all'indirizzo di Francesca e 1BTC che torna a Paolo".

Il wallet firma questo messaggio con la relativa chiave privata, in questo modo dimostra alla rete che è proprietario dei fondi archiviati a quell'indirizzo e che ha perciò facoltà di muoverli; la rete lo prende in carico, verifica la correttezza dei dati riportati nel "messaggio" (cioè della nostra transazione) e procede a convalidarli e registrarli sulla blockchain. Non sono possibili errori di sorta in questo sistema, i nodi della rete, infatti, possono facilmente verificare che quanto gli viene comunicato di riportare in blockchain è corretto grazie al fatto che ogni transazione è legata alla precedente attraverso il relativo hash e questo rende sostanzialmente impossibile spendere due volte le stesse monete (o praticare qualunque altra forma di abuso) senza creare un'anomalia facilmente riscontrabile da qualunque nodo.

Verificata la correttezza del messaggio i nodi lo archiviano sulla blockchain (dove diventa immutabile), registrano cioè che la somma di 1BTC che prima corrispondeva alla chiave pubblica che faceva riferimento a Paolo adesso fa riferimento a una nuova chiave pubblica (della quale è Francesca a detenere la chiave privata); il residuo rimanente (sempre 1BTC) torna quindi nella disponibilità di Paolo. Nonostante Paolo veda il saldo del proprio wallet pari a 1BTC, però, non deve cadere nell'errore di pensare che quello rappresenti il residuo dei 2BTC originariamente nella sua disponibilità e rimasti giacenti sull'indirizzo da cui aveva ordinato il pagamento di 1BTC a favore di

Francesca; dal momento che il pagamento fatto da Anna (pari a 2BTC) è finito depositato su quell'indirizzo in un'unica transazione è stato anche speso come un'unica transazione.

Quando la rete restituisce a Paolo il suo resto, quindi, lo va a versare su un nuovo indirizzo e il wallet di Paolo avrà una nuova chiave pubblica e una nuova chiave privata per movimentare quella somma rimanente (di 1BTC). Questo è rilevante perché se Paolo avesse fatto un backup del suo wallet prima di inviare 1BTC a sua sorella Francesca, quel backup non sarebbe più valido; la chiave privata che ha usato per firmare la transazione con cui ha inviato il denaro a sua sorella non è la stessa che gli permette di firmare una nuova transazione scalandola dall'importo di 1BTC che gli è tornato come resto. La cosa potrebbe rappresentare un grosso problema per Paolo qualora per fare questo tipo di operazioni (come vedremo più avanti) usasse un wallet cartaceo (paper wallet), perché successivamente all'ultima transazione effettuata a beneficio di Francesca, a causa di questa dinamica (che prende il nome di "addresses change"), il nostro amico Paolo si renderebbe amaramente conto di non essere mai entrato in possesso della nuova chiave privata per spendere il residuo Bitcoin (che finirebbe quindi perduto).

Quello che dobbiamo capire, in altre parole, è che quando riceviamo un pagamento di, ad esempio, 100BTC non disponiamo fisicamente di 100 monete che possiamo movimentare in maniera indipendente l'una dall'altra, ma disponiamo di una sola chiave pubblica e di una sola chiave privata per sbloccare quei fondi; per poter usare quei 100BTC come se fossero 100 monete che possiamo spendere in maniera indipendente dovremmo disporre di 100 coppie di chiavi pubbliche/private. Per capirci ancora meglio immaginiamo che il nostro amico Paolo abbia deciso di accettare pagamenti in Bitcoin per la sua attività di imbianchino e che adesso si ritrovi già sette diversi pagamenti accreditati da sette indirizzi diversi; Paolo può trovarsi questi 7BTC conservati nello stesso wallet allo stesso indirizzo, ma per movimentarli dispone comunque di 7 coppie di chiavi pubbliche e private.

Possiede quindi una chiave pubblica e una privata per ogni pagamento che ha ricevuto; molte persone, per non rischiare di fare confusione, hanno preso l'abitudine di generare un nuovo indirizzo ogni volta che ricevono un pagamento, in questo modo sono sicure che ad ogni indirizzo corrisponderà una sola chiave pubblica e una sola chiave privata.

Indipendentemente da come si decide di gestire i propri fondi, quindi, è fondamentale capire che anche se quando spendiamo i nostri BTC vediamo solo l'indirizzo a cui li stiamo spedendo, il nostro wallet sta usando una chiave privata per firmare la transazione e comunicare lo spostamento dei fondi alla rete; quella chiave privata c'è, esiste, anche se noi non la vediamo mai, anche se fisicamente non stiamo "firmando" nulla, quella chiave privata è la sola cosa che ci permette di spendere i nostri soldi ed è esattamente per questo motivo che normalmente ci si premura di fare una copia delle chiavi private per avere la sicurezza che, anche se il dispositivo fisico su cui conserviamo le nostre monete andasse perduto, saremmo sempre nella posizione di recuperare il nostro denaro.

5.3 Differenza tra criptovalute, security e utility token

Arrivati a questo punto del quinto capitolo padroneggiamo già un po' di concetti che sono normalmente abbastanza ostici da comprendere; per fare chiarezza e mettere un punto su ciò che

abbiamo imparato prima di passare oltre, tiriamo un attimo le fila del discorso. Abbiamo detto che una blockchain è un data base distribuito che tiene traccia di tutte le transazioni eseguite nel tempo e che a gestire l'archiviazione e l'aggiornamento dei dati c'è una rete di computer sparsa un po' ovunque che riceve una ricompensa per il lavoro svolto.

A garantire gli utenti del corretto svolgimento abbiamo la crittografia e i protocolli di consenso; tutto questo ovviamente ha però un senso solo in un sistema con un numero sufficientemente alto di nodi, capaci di garantire al contempo sia di poter supportare un grande volume di transazioni quotidiane, sia di evitare il rischio che l'eventuale presenza di nodi malintenzionati distrugga o corrompa i dati archiviati sulla blockchain.

Questi sono aspetti fondamentali dietro ogni progetto, alle spalle di Bitcoin, ad esempio, c'è una rete di migliaia di nodi con milioni di persone che ogni giorno spendono, trasferiscono, usano quelle monete; ma che succede se volessi usare le potenzialità di questa tecnologia senza avere alle spalle una rete di nodi decentralizzata che garantisca gli "utenti" che tutto si svolge regolarmente? Posso farlo archiviando i miei dati su un'altra blockchain. Una delle monete più note, ad esempio, è certamente Ethereum (ETH), che però non è solo una moneta ma è una vera e propria piattaforma che ci permette di sviluppare dei progetti (nostri) usando la sua blockchain per archiviare i dati e la sua rete per validarli. Se per esempio una squadra di calcio (in diverse lo hanno già fatto) desiderasse sviluppare una propria criptovaluta, anche solo per gestire la vendita dei biglietti, quello che farebbe sarebbe crearla sfruttando una delle tante piattaforme simili ad Ethereum in circolazione (o Ethereum stessa); è questa quindi la differenza tra una criptovaluta e un token, definiamo criptovaluta una moneta che ha una propria blockchain, mentre definiamo token una moneta che viene "distribuita" e processata su un'altra blockchain. Oltre a distinguere tra criptovalute e token, poi, dobbiamo distinguere anche tra due differenti categorie di token che chiameremo securities token ed utility token; per quanto riguarda questi ultimi, gli utility token possiamo immaginarli come una specie di gettone che ci permette di acquistare beni e servizi attraverso una piattaforma blockchain.

Un esempio di utility token ce lo da la squadra di calcio di poco fa, che invece di stampare il solito biglietto potrebbe sviluppare un utility token da vendere ai tifosi per entrare allo stadio e poi, perché no, rivendibile dai tifosi stessi presso il ristorante dello stadio per godere di un piccolo sconto (offerto dalla società) sui prezzi da listino. Per quanto riguarda invece i securities token, questi assomigliano più a dei veri e propri prodotti finanziari equiparabili sostanzialmente alle azioni di una azienda.

6. Storia di Bitcoin

Nel capitolo precedente abbiamo avuto modo di accennare come, negli anni, Bitcoin abbia iniziato a costruire una sorta di "standard" paragonabile a quello dell'oro per cui ogni volta che l'economia di uno stato inizia a palesare segnali di debolezza possiamo assistere ad un aumento dei volumi di scambio di criptovaluta in quel determinato paese; questo, a ben vedere, è un tratto che caratterizza Bitcoin sin dalla sua nascita.

Era infatti il lontano 2008 quando un personaggio che si firmava sotto pseudonimo fece la sua comparsa proponendo una moneta globale sostenuta da una rete P2P in concomitanza, ed in un certo qual senso in risposta, agli scandali bancari che guadagnavano l'onore delle cronache susseguendosi uno dopo l'altro e rappresentando sostanzialmente l'inizio della grande crisi economica che poi contagerà le economie di tutto il resto del mondo; questo personaggio, di cui dieci anni dopo ancora non si conosce la vera identità, passerà alla storia con lo pseudonimo di Satoshi Nakamoto.

Più precisamente Satoshi fa la sua comparsa nel mese di novembre (2008) pubblicando su "The Cryptography mailing list" (sul sito "Metzdowd.Com") un documento riguardante il protocollo di consenso che consentirà il funzionamento di Bitcoin; pochi mesi dopo (nel 2009) verrà distribuita la prima versione del software a cui iniziano a lavorare anche altri sviluppatori. Poco più di un anno dopo la nascita di Bitcoin (nel 2010) Satoshi si ritira dalla comunità, il suo ultimo messaggio pubblico risale al 2011 e serve a comunicare il passaggio di consegne con Gavin Andresen.

E' forse proprio questa la cosa più strana di questa tecnologia, che la persona che l'ha sostanzialmente inventata (anche se non dal nulla) sia stata capace non solo di rimanere anonima tutto questo tempo, ma abbia addirittura deciso di uscire completamente dalla scena nel giro di neanche due anni dopo aver dato vita alla sua creazione; che Satoshi Nakamoto finisca sui libri di scuola è inevitabile, ci è finito già a dire il vero, non c'è corso presso qualunque università al mondo in cui si parli di blockchain e crittografia senza citare Satoshi.

La cosa importante da capire, quando pensiamo a Satoshi, è che parliamo di una delle menti più brillanti di questo secolo, la matematica che sostiene Bitcoin e ne consente il funzionamento, infatti, è comunemente considerata così evoluta che in molti sono arrivati a sostenere che dietro lo pseudonimo di Satoshi Nakamoto non si celi una sola persona ma bensì un team di hacker dalle solidissime competenze; nemmeno di questo (cioè della natura "collettiva" dietro la figura di Satoshi) abbiamo prove o conferme, per cui la figura di questa persona rimane ancora avvolta nel mistero.

In un bel documentario targato Netflix (Banking on Bitcoin, 2016) possiamo trovare una tra le ricostruzioni più plausibili di come siano andate le cose; a creare Bitcoin, quindi, dovrebbe essere stato uno dei maggiori esponenti del movimento cypherpunk, per cui inevitabilmente uno o più tra Nick Szabo, Hal Finney, Adam Back e Wei Dai. Il cypherpunk, di cui probabilmente quasi nessuno ha mai sentito parlare nel nostro paese, se non forse pochi "appassionati", era un movimento controculturale composto informalmente da persone interessate alla privacy che si proponeva di raggiungere la libertà individuale mediante l'utilizzo della crittografia; l'impostazione ideologica che questi gruppi hanno sempre avuto è stata di carattere libertario oscillando tra l'anarchismo sociale, l'anarco-individualismo e l'anarco-capitalismo.

Ancora oggi, nel 2018, la componente anarchica nel mondo delle criptovalute è chiaramente riconoscibile, nonostante in questo mondo ci siano poi entrate anche grandi banche, istituzioni nazionali, imprenditori e persone comuni che in qualunque modo possono essere definite tranne che anarchiche. Questa tecnologia, in ogni caso, affonda le sue radici in un humus culturale (quello anarchico) che rappresenta ancora oggi il filo conduttore attraverso più di una decade di sviluppo tecnologico. Ma torniamo all'identità di Satoshi, "Banking on Bitcoin" fa una ricostruzione su chi possa essere che a me (e a molto altri), pare essere molto verosimile; dietro lo pseudonimo di Satoshi Nakamoto ci sarebbe proprio Hal Finney (esponente di spicco del cypherpunk made in USA), ammalatosi di SLA nel 2011 e deceduto nel 2014 all'età di 58 anni. Subito alle spalle di Finney tra i più quotati per impersonare il ruolo di Satoshi abbiamo poi Nick Szabo, famoso nel mondo della crittografia per essere l'inventore del concetto di "smart contract" (di cui ci occuperemo meglio quando parleremo di Ethereum) e che già nel 1998 aveva tentato qualcosa di simile con la valuta alternativa chiamata BitGold.

C'è stato anche un momento in cui un imprenditore australiano (Craig Steven Wright) era sembrato poter essere il vero Satoshi ma ben presto anche questa ipotesi è stata scartata. Qualcuno potrebbe a questo punto dire che ovviamente Satoshi ora è sparito, essendo diventato ricco, avrà convertito tutti i suoi Bitcoin in dollari e starà passando il resto dei suoi giorni sorseggiando cuba libre alle Maldive; in realtà quali siano gli indirizzi di proprietà di Satoshi lo sappiamo benissimo, e su questi indirizzi sono bloccati centinaia di Bitcoin che non vengono movimentati da anni. E' questo che ci porta a sospettare che Satoshi possa essere proprio Hal Finney (deceduto nel 2014), perché c'è stato un momento, quando le quotazioni di Bitcoin si sono spinte fino a 20.000$, in cui anche solo 100BTC sono arrivati a valere 2mln di dollari (e sugli indirizzi di Satoshi sono complessivamente bloccati più di 100BTC); il fatto che tutti questi soldi siano rimasti bloccati sui rispettivi indirizzi tutti questi anni senza essere mai movimentati suggerisce l'idea che semplicemente il proprietario di quei Bitcoin (cioè Satoshi) sia venuto a mancare.

Posto che non conosceremo mai la vera identità di Satoshi Nakamoto, che diamo quasi sempre per scontato che sia un uomo ma potrebbe essere una donna, potrebbe essere persino un marziano per quel che ne sappiamo, Bitcoin appare già (in soli dieci anni dalla sua nascita) essere stato capace di sopravvivere al suo inventore; e tutto questo nonostante abbia vissuto momenti molto cruenti nel corso della sua giovane vita. Mentre scrivo questo testo, ad esempio, Bitcoin ha perso circa l'80% del suo valore rispetto agli ultimi picchi del gennaio 2018 e questo porta molti detrattori a sostenere che sia arrivata la sua fine; quello che però i detrattori non dicono è che Bitcoin se l'è vista brutta già diverse volte nel corso della sua storia, mostrando però ogni volta di avere le spalle abbastanza larghe da uscirne più forte di prima. Il primo grande crollo nella storia Bitcoin lo troviamo già nel 2011 quando, dopo una folle corsa che in qualche mese ne gonfiò la quotazione da 0.92$ fino alla cifra esorbitante di 32$ per moneta, le quotazioni Bitcoin crollarono di nuovo intorno ai 2$. "Adesso è finita" dissero gli esperti, "Bitcoin è morto" sentenziarono i giornali; ma le cose non andarono così, l'anno successivo (2012), Bitcoin offrì subito i primi segnali di forza, tornando a quotare intorno ai 7$. Già a metà gennaio, però, un nuovo schiaffone lo spinse giù di quasi il 40%; sembrava comunque trattarsi di una banale correzione, dal momento che l'estate dello stesso anno le quotazioni tornarono vicine ai 15$, se non che una nuova ondata ribassista spinse il prezzo giù di un altro 50%.

Insomma, quando sembrava che Bitcoin non avrebbe mai più recuperato il suo picco storico del 2011 ecco che il prezzo esplose di nuovo segnando, nella primavera 2013, un nuovo massimo vicino ai 50$. Nei mesi successivi BTC riprenderà la sua corsa con nuovi massimi vicini questa volta prima ai 100$ e poi, col nuovo massimo storico registrato ad Aprile 2013, sfiorando i 270$.

Bitcoin è inarrestabile, non si può fermare, arriverà a valere migliaia di dollari, dissero i più entusiasti, e invece Bitcoin tornò giù, soltanto pochi giorni dopo aver toccato il nuovo massimo, attestandosi a quota 67$ nello stesso mese di Aprile. A questo punto i prezzi entrano in una fase laterale, le quotazioni si tengono abbastanza stabili intorno ai 120$ fino alla fine dell'anno quando parte una nuova corsa dei tori che trascina il prezzo fino a 1100$. Wow! Peccato che nel giro di qualche settimana il prezzo torni a precipitare, attestandosi questa volta a quota 500$ e rimanendo in una specie di lateralità per i successivi 18 mesi. Arriviamo così al 2014, altro annus horribilis per la nostra criptovaluta che, nel frattempo, si è arrampicata fino quasi a sfiorare quota 900$; la tempesta perfetta, però, è vicina ed esplode in tutta la sua violenza nel febbraio 2014 quando il più grande scambio al mondo (MtGox) dichiara bancarotta a seguito del furto di 850.000BTC (quasi 800mln di dollari, per intenderci).

La reazione dei mercati a tutto questo è, comprensibilmente, una specie di ecatombe, il prezzo di Bitcoin precipita di nuovo e si attesta in quota 400$, dove rimane fermo per un altro paio di anni. Veniamo quindi a tempi più recenti, quando finalmente a Gennaio 2017 Bitcoin torna a rompere il muro dei 1000$ ed inizia una corsa che lo porterà, tra Dicembre 2017 e Gennaio 2018, a toccare il nuovo massimo storico intorno a quota 20.000$. Da quel momento Bitcoin è rientrato in una nuova fase ribassista, arrivando a toccare minimi intorno ai 3.000$ e dando nuova voce ai detrattori che ancora una volta si sono precipitati ad affermare che "questa volta è proprio la fine"; chi tra i detrattori e i sostenitori avrà l'ultima parola è ancora presto per dirlo, fino ad oggi, però, la storia ci dice che ogni volta che Bitcoin ha bruciato il grosso dei propri rialzi poi nel giro di qualche mese è tornato a segnare nuovi massimi.

Se questo succederà ancora o se è successo per l'ultima volta nel 2017 è presto per dirlo, il tempo ci darà sicuramente una risposta, per cui basta armarsi di pazienza e restare a guardare cosa succederà.

7. Il mercato delle criptovalute

Il mercato delle criptovalute nasce sostanzialmente con Bitcoin; prima non esisteva nulla, ma con la nascita della prima criptovaluta servivano delle piattaforme attraverso le quali gli utenti potessero scambiarsi valute virtuali in cambio di moneta fiat (cioè valuta a corso legale). I primi a riconoscere le potenzialità di questa nuova valuta, ovviamente, furono gli operatori del così detto "dark web", insieme coi gestori del sito silkroad, insomma, dovunque si vendesse qualcosa che non era legale vendere sul web si impose rapidamente questo nuovo standard.

È proprio questo il motivo per cui, persino oggi, alcuni restano convinti del fatto che le criptovalute siano una sorta di denaro al servizio di chi conduce affari loschi, perché inizialmente Bitcoin si diffuse soprattutto in ambienti che, per così dire, non fanno della legalità esattamente la loro bandiera; questa situazione, in ogni caso, era destinata a cambiare molto velocemente. Dal momento che il software Bitcoin è open source la corsa all'oro era partita, iniziarono a nascere sempre nuove monete, alcune delle quali erano sostanzialmente identiche a Bitcoin; le criptovalute, pian piano, iniziavano ad essere accettate quasi ovunque su internet, inclusi alcuni grandi e-commerce dove è sostanzialmente possibile comprare qualsiasi cosa.

Oltre alla necessità di scambiare Bitcoin con valuta FIAT (o, in altre parole, valuta ufficiale), nacque la necessità di scambiare criptovalute con altre criptovalute; gli utenti iniziarono a utilizzare le nuove nate (denominate "altcoin" per definire tutte le altre monete diverse da Bitcoin) per scambiarsele le un con le altre al fine di accumulare altri BTC, stavano venendo fuori i primi "cripto-trader". Dal momento però che le piattaforme che consentivano di scambiarsi criptovalute e valuta a corso legale dovevano rispondere a stringenti norme e regole, un gruppo di sviluppatori, non senza una certa scaltrezza, decise di lanciare un nuovo token (su piattaforma OMNI) che prenderà il nome di Tether (USDT); era nata la prima stable coin, ancora oggi il token con la maggiore capitalizzazione del mercato.

Da quel momento in poi le piattaforme di scambio potevano offrire ai trader uno strumento per ripararsi dalla volatilità di Bitcoin senza fisicamente maneggiare valuta a corso legale ed eludendo così sostanzialmente le norme e le regole previste nei vari paesi per questo tipo di attività; le piattaforme di scambio, infatti, operano sostanzialmente in maniera identica a una banca, di conseguenza, ad esempio, tra le varie norme a cui dovrebbero far fronte c'è l'identificazione degli utenti.

Ma come chiunque può constatare è ancora oggi possibile aprire un conto di trading su molte piattaforme di scambio (anche rinomate) senza fornire alcun documento e quindi in quasi totale anonimato; il mercato intanto è diventato più maturo, oggi esistono un buon numero di piattaforme che consentono di scambiare criptovalute con valuta fiat, che operano nel rispetto delle leggi identificando i propri trader, ma questo non ha fatto sparire le stable coin (come USDT), che invece sono aumentate esponenzialmente di numero negli ultimi mesi (come avremo modo di vedere più avanti). Per quanto riguarda la diffusione delle criptovalute ormai i tempi in cui queste monete si potevano spendere solo sul dark web sono finiti da un pezzo, dopo essere diventate una modalità di pagamento comune su tutto il web (persino sui maggiori e-commerce, come abbiamo avuto

modo di spiegare), di recente, grazie alla diffusione di apposite carte di credito, è diventato facile spenderle presso qualunque negozio delle nostre città.

La diffusione di queste carte (sostanzialmente prepagate) rende possibile usare le proprie criptovalute per prelevare denaro contante da qualunque bancomat di qualunque banca e si stanno iniziando a diffondere anche nuovi sportelli ATM che fanno invece l'esatto contrario, con i quali è possibile cioè comprare criptovaluta usando valuta fiat. Se tutto questo non fosse abbastanza le cose non finiscono qui, Bitcoin è oggi molto diffuso nell'ambito del lusso, un settore sempre pronto nel conquistare nuove nicchie di facoltosi clienti, per cui oggi non solo è possibile comprare un'auto, una barca e praticamente ogni altro genere di articolo di lusso usando le criptovalute, ma è addirittura possibile comprare casa pagandola in questo modo (e proprio in Italia abbiamo avuto negli ultimi mesi almeno un paio di casi di immobili che sono stati pagati in Bitcoin da chi li ha acquistati).

7.1 Ethereum ed ethereum classic

Nelle ultime pagine è diventato ormai chiaro perché parlando di criptovalute abbiamo sempre usato parole come "ecosistema", "mondo" o altre simili, perché parliamo di un vero e proprio universo, popolato da migliaia di progetti (sul mercato ci sono più di 800 criptovalute diverse e addirittura 1200 token); tra tutte queste centinaia di blockchain diverse quella comunemente più nota al grande pubblico (dopo Bitcoin) è senza dubbio Ethereum. Nata su impulso di un giovane sviluppatore, tra i più famosi nel mondo delle criptovalute, Vitalik Buterin (russo di origini ma canadese d'adozione), la prima versione della piattaforma venne lanciata nell'estate 2015.

Buterin, però, aveva avuto l'opportunità di presentare la sua idea già un paio d'anni prima (nel 2013) con la presentazione di un WhitePaper in cui sosteneva la necessità di sviluppare un nuovo linguaggio di scripting per lo sviluppo di applicazioni su blockchain; sulla base di questa prima istanza nacque l'idea di una nuova criptovaluta al cui team di sviluppatori decisero di collaborare anche Mihai Alisie, Anthony Di Iorio e Charles Hoskinson che, a partire dal dicembre 2013, iniziarono a dare fisicamente vita all'idea attraverso una società Svizzera, Ethereum Switzerland GmbH, cui seguì la nascita di una fondazione senza scopo di lucro (la Fondazione Ethereum, sempre con sede in Svizzera). Le prime versioni del software in linguaggio Go e in linguaggio C++ furono rilasciate nel febbraio 2014 mentre risale al bimestre luglio-agosto 2014 la fase di finanziamento (avvenuto raccogliendo BTC) con un crowdsale pubblico online. Il 30 luglio 2015 venne lanciata la prima versione della piattaforma (chiamata Frontier), ed è quindi questa la data in cui possiamo far cadere ufficialmente la nascita di ETH.

Intendiamoci, di criptovalute alternative a Bitcoin ne erano già nate parecchie prima del 2015, e nonostante alcune avessero espresso grandi sforzi per distinguersi rispetto al "fratello maggiore", tutte le monete in circolazione venivano (per certi versi lo sono ancora) considerate come dei cloni di Bitcoin; la nascita di Ethereum (intesa come piattaforma, prima che come moneta) scombina

completamente le carte in tavola. Ethereum, infatti, prima che ogni altra cosa, andrebbe considerata una piattaforma open source di distributed computing pensata non solo per consentire il trasferimento di valore secondo i principi tipici di Bitcoin (una valuta P2P, quindi) ma per consentire di creare, pubblicare e gestire smart contract con la stessa filosofia; per capire di cosa stiamo parlando dobbiamo fermarci un attimo a chiarire cosa siano gli smart contract. Stiamo parlando, molto semplicemente, di "programmi" scritti utilizzando i più comuni linguaggi di programmazione che hanno la caratteristica di essere "auto-eseguibili" cioè, in presenza di determinate condizioni, sono capaci di eseguire compiti specifici; secondo la definizione che ne da wikipedia, quindi, gli smart contract sono "*protocolli informatici che facilitano, verificano, o fanno rispettare, la negoziazione o l'esecuzione di un contratto, permettendo talvolta la parziale o la totale esclusione di una clausola contrattuale*".

Per capirci facciamo un esempio e immaginiamo di dover pagare il nostro fitto di casa usando ETH; normalmente con una banca quello che faremmo sarebbe predisporre un bonifico permanente, di importo pari a quello stabilito per l'affitto, a beneficio del padrone di casa. Ebbene, possiamo fare la stessa identica cosa usando Ethereum come valuta e scrivendo uno smart contract al posto del bonifico permanente. Si tratterebbe, molto banalmente, di un "programma" capace di sbloccare l'erogazione di quanto concordato ogni primo giorno del mese; lo smart contract, quindi, non farebbe altro che verificare la data corrente e, qualora la data del giorno fosse uguale a 1 (se fossimo cioè al primo giorno del mese), sbloccherebbe il pagamento per un importo pari a quello dell'affitto.

Come chiunque può intuire le applicazioni degli smart contract sono potenzialmente infinite e questo ha portato Ethereum ad essere considerata comunemente come la concorrente più temibile per Bitcoin; l'entusiasmo che iniziava a circolare intorno all'idea di Buterin era palpabile, finalmente sembrava possibile sviluppare in maniera tutto sommato facile un progetto di qualunque tipo sfruttando le potenzialità offerte da questa nuova piattaforma.

I nuovi token, quindi, spuntarono fuori da subito (abbiamo detto che attualmente ce ne sono più di mille in circolazione) e nulla sembrava poter arrestare la crescita della creatura di Vitalik. Siamo però arrivati al 2016, la fatidica data dello scandalo The DAO; iniziamo subito col dire che DAO è l'acronomio inglese di decentralized autonomous organization, che tradotto in italiano significa appunto "organizzazione autonoma decentralizzata"; si tratta in pratica di un'organizzazione il cui regolamento è codificato come un programma per computer, sotto il controllo diretto degli "azionisti", trasparente e non influenzata da un governo centrale.

Nel 2016, dicevamo, nacque l'idea di un fondo di venture capital con lo scopo di raccogliere capitali per finanziare progetti che, dopo essere stati preliminarmente valutati da un comitato ad hoc e sottoposti a votazione degli holders, avrebbero potuto ricevere dei finanziamenti offrendo in cambio una partecipazione agli utili; questo fondo prese il nome di The DAO ed il relativo token (omonimo) era sostanzialmente un securities token.

L'idea, sull'onda dell'entusiasmo crescente, ebbe un grande successo arrivando a raccogliere ben 150mln di dollari nel maggio del 2016 e perdendone però subito la metà (70mln di dollari nel giugno 2016) a causa di un attacco informatico che riuscì a violare l'indirizzo sul quale i fondi erano custoditi. Il problema venne gestito con una certa urgenza e già un mese dopo, nel luglio del 2016, fu deciso, a seguito di un voto, di implementare un hard fork nel codice Ethereum e di spostare gli Ether sottratti durante l'attacco in un nuovo smart contract di modo da poterli così restituire agli utenti a cui erano stati rubati; questa idea però minava alla base il concetto di immutabilità della blockchain per cui la comunità di Ethereum si spaccò sostanzialmente in due dando vita all'hard fork che porterà alla nascita di Ethereum Classic (ETC).

Da quel momento, quindi, esistono due catene differenti le cui monete sono identificate dalle sigle ETH (per Ethereum) ed ETC (per Ethereum Classic); il fork però non chiuse definitivamente la questione, lo scandalo The DAO era infatti arrivato alle orecchie della SEC (l'equivalente americano della nostra Consob) che da quel momento accese i riflettori su Ethereum. Dal momento che il token The Dao appariva chiaramente come una securities la procedura con cui li si proponeva e vendeva al pubblico avrebbe dovuto rispettare le normative previste negli USA; gli investitori, in altre parole, erano stati truffati. Anche se ormai pare chiaro a tutti che Ethereum non sia di per se una securities, la questione relativa alla necessità di regolamentare il comparto non si è mai conclusa; due grossi scandali come il fallimento di MtGox e il caso The DAO avrebbero probabilmente ucciso un mercato che non fosse già stato sufficientemente maturo per affrontare uno scenario del genere. Il settore delle cripto, pur essendo innegabilmente uscito indebolito da quanto accaduto, seppe (come ci dimostra la storia) reagire con forza a questi problemi, lasciandoseli alle spalle nel giro di appena un anno, ma senza che dallo spazio di discussione sparisse questa volta la questione relativa alla necessità di introdurre nuove norme per tutto il settore.

7.2 Bitcoin cash e BSV

Abbiamo detto che di tutte le centinaia di criptovalute in circolazione molte condividono in larga misura lo stesso codice di Bitcoin; c'è però una moneta tra le tante che condivide molto più che il codice, condivide la stessa blockchain, è, in altre parole, un vero e proprio hard fork di Bitcoin.

Come abbiamo visto nel paragrafo precedente, infatti, quando i nodi della rete non riescono a trovare un accordo in merito ad alcune decisioni (normalmente di una certa rilevanza) le due fazioni possono dividersi dando vita a due nuovi progetti. E' quello che è successo nel caso di ETH ed ETC, ed è anche la stessa cosa che è successa tra Bitcoin e Bitcoin Cash.

Quando si verifica un hard fork quello che succede è che la blockchain a un certo punto si biforca in due diverse ramificazioni; entrambi i due progetti, quindi, condividono la stessa blockchain fino a un determinato blocco, da quel blocco in poi, però, si genereranno due diverse catene che, pur condividendo la prima parte della loro storia, inizieranno a registrare ognuna le proprie transazioni in maniera indipendente.

Questo, al contempo, significa anche che chi possedeva un certo quantitativo di monete prima del fork si ritroverà a possedere un nuovo quantitativo di monete, nella stessa quantità, sulla nuova blockchain; per questo motivo quando si viene a sapere che sta per esserci un fork di una blockchain spesso le criptovalute che saranno oggetto del fork subiscono importanti rialzi, gli investitori infatti sono attratti dalla possibilità di sdoppiare le proprie monete e si precipitano a comprare per partecipare al fork. Se la comunità Ethereum si è rotta sulla strategia da prendere per la gestione dello scandalo The DAO, che cosa ha provocato la rottura della comunità Bitcoin? Un problema noto come "dimensione del blocco"; per comprendere bene di cosa stiamo parlando, dobbiamo però

spiegare prima un concetto abbastanza importante e che prende il nome di “trilemma della criptovalute”.

Un trilemma è un problema in cui solo due delle tre opzioni proposte possono verificarsi contemporaneamente, nel caso delle criptovalute le opzioni del trilemma sono la scalabilità, la sicurezza e la decentralizzazione; di queste tre caratteristiche solo due possono essere soddisfatte pienamente, una delle tre, invece, verrà sempre sacrificata a beneficio delle altre. In pratica, affinché una blockchain sia pienamente sicura e decentralizzata e necessario sacrificare qualcosa alla scalabilità (cioè alla quantità di transazioni che la rete può processare); se si desidera processare un volume alto di transazioni, non potendo sacrificare nulla alla sicurezza, ecco che iniziamo a scadere in un sistema centralizzato (che poi è quello che succede quando sfruttiamo la tecnologia DLT, nella quale abbiamo ottime caratteristiche di scalabilità ma la rete appare sostanzialmente centralizzata).

Quando abbiamo spiegato come funziona una blockchain, spiegando sostanzialmente come funziona Bitcoin, abbiamo detto che viene generato un blocco ogni dieci minuti, che tali blocchi hanno un peso di 1MB e che la difficoltà per minarli aumenta in maniera direttamente proporzionale alla potenza di calcolo espressa dalla rete, di modo da mantenere costante nel tempo la creazione di un nuovo blocco sempre ogni 10 minuti.

Tutta questa dinamica, però, non fa che limitare il numero di transazioni che la rete può processare; per rendere la rete più veloce, quindi, qualcuno iniziò a proporre che si sarebbero dovuti predisporre blocchi più grandi. Ma se facciamo i blocchi più grandi, risposero allora altri, poi ci vorrà troppa potenza di calcolo per minarli e questo taglierà fuori tutti i piccoli minatori facendoci piombare in un sistema sostanzialmente centralizzato in cui pochi grandi minatori controllano sostanzialmente la rete.

In un primo momento si tentò di prevenire la rottura nella comunità implementando una nuova soluzione (chiamata SegWit) che avrebbe dovuto permettere di spostare esternamente al blocco alcune informazioni, liberando quindi spazio per aumentare il numero di transazioni; i problemi erano però solo rinviati e non risolti, questa soluzione non venne infatti giudicata sufficiente a risolvere i problemi di scalabilità della rete e una parte della comunità continuava ad essere fermamente convinta che solo aumentando la grandezza dei blocchi si sarebbero potuti risolvere definitivamente i problemi di scalabilità.

La parte restante della comunità continuò però ad osteggiare questa soluzione ritenendo (neanche a torto a ben vedere) che aumentare la dimensione del blocco avrebbe compromesso la natura decentralizzata di Bitcoin.

SegWit, quindi, non aveva risolto le divergenze nella rete, di conseguenza, nell’agosto 2017, una parte della comunità decise di dare vita a Bitcoin Cash. Come qualunque altra scissione, in qualunque altro ambito, anche quella tra BTC e BCH non è stata molto pacifica; quando una blockchain si spezza in due, infatti, ognuno dei due tronconi nutre l’ambizione di parassitare il gemello, svuotandolo prima dei nodi e poi degli stessi utenti, e la stessa cosa avvenne nel primo hard fork di Bitcoin, con le due comunità che rivendicavano per se il ruolo di vero e unico Bitcoin, accusando l’altra fazione di essere dei truffatori e dei traditori.

A finire al centro delle polemiche più grandi sarà Roger Ver, un americano (è nato a San Jose, in California), classe 1979 ed attualmente residente in Giappone dopo aver patteggiato una condanna a dieci mesi di carcere per aver venduto esplosivi (fuochi d'artificio in realtà) online; si tratta di uno degli investitori storici di Bitcoin, entrato nella comunità intorno al 2011 divenendo uno dei cinque fondatori della bitcoin foundation.

Ancora oggi Ver è uno dei personaggi più controversi e divisivi nel mondo Bitcoin, lungamente considerato come uno dei principali evangelizzatori della creatura di Satoshi (tanto da essersi guadagnato il nomignolo di "bitcoin jesus") dopo aver dato il suo sostegno incondizionato a bitcoin cash ha perso buona parte del suo appeal divenendo oggetto di critiche feroci da parte di larga parte della comunità incluse persone anche molto autorevoli. Comunemente Roger Ver (anche in virtù dell'enorme impegno profuso nel sostenere BCH) viene considerato un po' come la mente che sta dietro alla nascita di questo progetto, cosa che ha suggerito la possibilità che in realtà si tratti di una moneta sostanzialmente centralizzata sostenuta da nient'altro che dagli interessi di coloro che ne sono i reali proprietari tra cui, appunto, lo stesso Ver.

Indipendentemente da come la si voglia vedere, se si reputa quindi l'hard fork di BCH come un colpo di mano o lo si inquadri invece nell'ambito di un più naturale dissenso nell'ambito degli sviluppi possibili da dare a Bitcoin, la nuova creatura iniziava ad avere una sua vita quando a un certo punto, nell'autunno 2018, ecco che si sparge la voce di un nuovo fork, questa volta interno a Bitcoin Cash.

Chi di fork ferisce di fork perisce, verrebbe da dire; questa volta però la comunità non si divide sulla dimensione dei blocchi, ma sull'aspetto relativo all'anonimato delle transazioni. Anche qui abbiamo due fazioni, quella maggioritaria che fa capo a bitmain e che include quasi tutti gli sviluppatori che diedero vita al fork di bitcoin dell'agosto 2017, e una minoritaria facente capo a Craig Wright; è proprio quest'ultimo, infatti, a considerare cruciale per gli sviluppi futuri della moneta concentrarsi su una maggiore privacy delle transazioni (aspetto che invece la maggioranza della comunità non considera prioritario).

Le cose sono ancora troppo fresche per capire cosa succederà, se entrambe le catene sopravviveranno o se una delle due sia destinata a soccombere, per adesso di certo sappiamo che abbiamo due nuove monete che si chiamano Bitcoin cash ABC (che mantiene la sigla BCH) e la creatura nata dallo strappo della minoranza capeggiata da Craig Wright che si chiama invece Bitcoin SV (e che assume la sigla BSV). Contrariamente a quanto sembrava all'inizio, poi, una prima sorpresa è arrivata dall'analisi dell'hash rate (cioè la potenza di calcolo) espressa dalle due catene, con BSV che pur essendo parsa da subito minoritaria nella comunità vanta però (almeno in queste prime fasi) un maggiore hash rate.

7.3 Ripple

Abbiamo già avuto modo di accennare come sul terreno delle criptovalute si consumi uno scontro che è anche ideologico e che contrappone due visioni completamente differenti tra loro, quella che guarda alle grandi istituzioni centralizzate come qualcosa di indispensabile per costruire la fiducia reciproca e, al contrario, quella che guarda a quelle stesse istituzioni come a un carrozzone inutile.

La massima espressione di questo scontro ideologico si incarna in una piattaforma in particolare, Ripple, ed in una criptovaluta, $XRP, probabilmente la moneta più divisiva di tutto il mercato. Nonostante ci siano centinaia di criptovalute al giorno d'oggi solo XRP pare capace di dividere gli appassionati in due gruppi così radicalmente contrapposti e divisi tra chi la odia in maniera viscerale e chi, invece, semplicemente la adora. Il motivo di tutto questo astio? Beh, non è per l'uso della tecnologia DLT (esistono altri progetti che usano la stessa tecnologia ma non raccolgono altrettanto astio) e non è nemmeno per il protocollo di consenso (Ripple usa una variante della Byzantine Fault Tolerance), il motivo, molto più semplicemente è che dietro a questo progetto c'è un consorzio che riunisce alcune delle più grandi banche a livello mondiale.

Ripple, infatti, nasce nel 2012 su impulso di Ripple Labs Inc. in forma di un sistema di trasferimento fondi in tempo reale, capace quindi di permettere lo scambio di criptovalute, valute FIAT, materie prime e, in definitiva, qualunque altro tipo di valore, tra coloro che fanno parte del network; lo scopo dichiarato di questo progetto è di creare una rete capace di consentire transazioni finanziarie globali sicure, istantanee, di qualsiasi importo, con commissioni irrisorie e senza la possibilità di contestare l'addebito (chargeback).

Ad essere completamente onesti, però, la storia di Ripple inizia molto prima del 2012, anche prima di Bitcoin, e può essere fatta risalire al 2004 (quattro anni prima che sulla scena apparisse Satoshi) quando Ryan Fugger (giovane sviluppatore web di Vancouver) ebbe l'idea di RipplePay; questo nuovo sistema di scambio di valuta decentralizzato farà ufficialmente la sua comparsa un anno dopo, nel 2005 con la nascita del sito RipplePay.com. Il concetto intorno cui si sviluppa Ripple negli anni successivi è quello di consentire il trasferimento immediato e diretto di denaro tra due parti e, per fare questo, viene creata la valuta digitale XRP pensata ad hoc per consentire alle istituzioni finanziarie di trasferire denaro con tariffe e tempi di attesa trascurabili.

Ma dal momento che, come noto, tra il dire e il fare c'è di mezzo il mare, il progetto dovrà attendere fino al 2014 per entrare nel vivo, quando la prima banca (la Fidor Bank di Monaco) inizia ad utilizzare Ripple per spostare denaro; i tempi ormai sono maturi e, con l'adesione della prima banca, iniziano ad arrivare nuove partnership, dopo la Fidor Bank di Monaco, a stretto giro di posta, arrivano la Cross River Bank e banca CBW, entrambe con sede nel New Jersey, mentre risale all'anno ancora successivo, nella primavera 2015, la dichiarazione di Western Union di avere intenzione di iniziare le prime sperimentazioni con Ripple. Il 13 giugno 2016 Ripple ottiene la licenza di valuta virtuale dal Dipartimento dei servizi finanziari (la quarta azienda ad aver ottenuto la BitLicense dello Stato di New York) e quasi un anno dopo (nell'agosto 2016) SBI Ripple Asia annuncia la creazione di un consorzio che arriverà ad includere 61 banche giapponesi capaci di rappresentare da sole oltre l'80%

del totale delle attività bancarie di tutto il paese. Arriviamo quindi ai giorni nostri, quando, appena qualche settimana fa (settembre 2018) PNC Financial Services annuncia che utilizzerà il sistema xCurrent di Ripple nei pagamenti internazionali.

Quello che è importante capire è che, a differenza di Bitcoin, Ripple non è un metodo di pagamento, ma un sistema di pagamento; questo significa che attraverso la rete è possibile trasferire la proprietà di qualunque bene (non solo denaro, ma anche oro per fare un esempio), praticamente in tempo reale e con costi sostanzialmente irrisori.

Non entreremo nel merito di come funziona Ripple, ma è importante evidenziare come tutto questo sistema appaia chiaramente pensato su misura per semplificare l'attività interbancaria consentendo agli istituti di credito di scambiarsi grandi somme di denaro (senza spostare fisicamente alcunché ad ogni transazione e senza nemmeno essere costretti a usare XRP per scambiarsi il "valore" oggetto della transazione) e con la possibilità di effettuare tali scambi usando valute FIAT, oro o qualunque altro genere di valore (oltre che le semplici criptovalute) anche senza continuità di forma (invio dollari, ad esempio, e il destinatario finale riceve euro).

Adesso apparirà certamente più chiaro il motivo per cui in tanti odiano Ripple mentre altri, al contrario, la amano; questo progetto non è nato per essere usato dalle persone comuni, è nato per essere usato dalle banche e questo non viene visto di buon occhio da una vasta parte della comunità. Questo non significa ovviamente che Ripple non possa essere usato anche dalle persone comuni, ma la vocazione con cui è nato è di servire le banche, non le persone; il fatto che alle spalle di questo progetto ci siano tanti colossi del sistema bancario, però, è anche il motivo per cui tanti investitori amano questo progetto, che considerano tra i più sicuri (in virtù dei grandi interessi che gli ruotano intorno) tra quelli presenti sul mercato.

Per molti investitori, infatti, che alle spalle di una criptovaluta ci sia una realtà strutturata, una vera e propria corporation, è espressione di maggiori garanzie; ovviamente queste persone preferiscono mettere i loro soldi in mano a degli imprenditori che non nelle mani di una rete di individui dei quali spesso si ignora persino l'identità. Ecco, questa è un'altra distinzione sostanzialmente ideologica tra queste due fazioni che vivono su posizioni radicalmente agli antipodi tra loro, chi crede che le grandi organizzazioni centralizzate siano necessarie, infatti, non vede di buon occhio l'anonimato, mentre al contrario, chi crede che le grandi istituzioni centralizzate siano diventate ormai sostanzialmente inutili vede nell'anonimato qualcosa di positivo e, persino, un diritto inalienabile che ognuno di noi dovrebbe avere facoltà di esercitare.

7.4 Stellar

Tra le piattaforme presenti sul mercato una di quelle che più attira le attenzioni dei maggiori investitori è sicuramente Stellar e questo è paradossale se consideriamo che parliamo del fratello minore di Ripple; le due monete (XRP e XLM) pur essendo imparentate presidiano lo stesso segmento di mercato e sono quindi in competizione tra loro. Le somiglianze sono tante, a partire dal fatto che entrambe sfruttano la tecnologia DLT e possiedono una criptovaluta nativa (che nel caso di Stellar si chiama Lumens, XLM); come XRP anche XLM presenta ottime caratteristiche in termini di scalabilità e rappresenta un punto di accesso al mondo delle cripto per i grandi istituti bancari.

A differenza del suo fratello maggiore, però, Stellar include anche tutta una serie di funzionalità paragonabili a quelle offerte da Ethereum come ad esempio la possibilità di gestire ICO, smart contract e creare token . Il progetto nasce nel 2014 e può essere, come detto, considerato quasi una costola di Ripple dal momento che a fondare Stellar è proprio il co-founder di XRP, Jed McCaleb (insieme all'ex avvocato Joyce Kim); tutto inizia quando, nel luglio 2014, McCaleb crea una fondazione senza scopo di lucro (Stellar Development Foundation) in collaborazione con Patrick Collison (CEO di Stripe).

Oltre che alcune figure chiave inizialmente Stellar condivide con Ripple anche il protocollo di consenso che, però, molto presto avrà modo di mostrare alcune fragilità portando alla decisione di affidare al professor David Mazières di Stanford il compito di ideare un nuovo protocollo che diventerà perfettamente operativo a novembre 2015 e che verrà chiamato SCP (stellar consensus protocol).

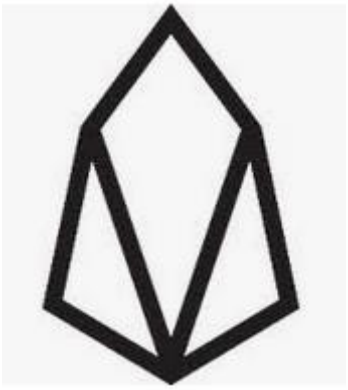
Pur essendo due progetti molto simili Stellar si distingue prepotentemente da Ripple per la sua volontà dichiarata di portare avanti iniziative a carattere sociale tanto da arrivare a porre il suo principale bacino d'utenza in Africa e nel sud-est asiatico, territori nei quali punta a diventare il punto di riferimento per movimentare le rimesse dei migranti; per sostenere questa immagine fortemente orientata al sociale, oltre alla forma di organizzazione no profit, Stellar è da sempre molto attiva nel finanziare imprese sociali e nel garantire accesso al mercato globale ai soggetti non bancabili.

Oggi Stellar è considerata una delle piattaforme più evolute presenti sul mercato; tra le varie funzionalità offerte da questa piattaforma, oltre alla possibilità di scambi transnazionali tra qualsiasi coppia di valute, abbiamo una gestione agevole sia delle ICO che dei relativi token (che da subito possono essere scambiati sull'exchange integrato nella piattaforma), il tutto con commissioni molto basse, in un sistema caratterizzato da altissima sicurezza e con una grande velocità nell'esecuzione delle transazioni. La capacità di associare a una tecnologia di primissimo livello la grande attenzione al sociale ha permesso a Stellar di guadagnarsi le simpatie di un vasto numero di osservatori, a differenza di quanto accaduto a Ripple che pare invece calamitare più che altro diffidenza.

La scelta di strutturarsi come organizzazione senza scopo di lucro, poi, le permette di operare nel totale rispetto delle normative dei vari paesi senza però con questo smarrire la propria vocazione alla decentralizzazione, cosa che inevitabilmente accade quando come forma si decide di adottare quella aziendale. Questa capacità di tenere in qualche modo il piede in due scarpe, tenendosi sempre in bilico tra centralizzazione e decentralizzazione, tra banche e persone comuni, tra business e iniziative di carattere sociale ha permesso a Stellar di raccogliere, negli anni, tanto le simpatie degli utenti quanto i capitali dei grandi investitori; una caratteristica, a mio parere, vincente per chi oggi vuole operare nel mondo delle criptovalute.

7.5 EOS

Arrivati a questo punto dovrebbe essere chiaro che dietro ogni criptovaluta c'è una piattaforma che consente contemporaneamente agli utenti di spendere e movimentare le proprie monete e ai nodi della rete di partecipare alla validazione dei blocchi; alcune di queste piattaforme, come ad esempio Ethereum, si spingono ancora oltre queste funzionalità di base e consentono a chiunque, attraverso una gestione semplificata dei vari processi necessari, di emettere un proprio token (in pratica una vera e propria criptovaluta che però non ha una propria blockchain ma viene processata dalla rete della piattaforma sulla quale è stata creata), scrivere, distribuire e condividere smart contract, scambiarsi criptovalute con valuta fiat o altre cripto (come un vero e proprio exchange) e, particolare che abbiamo omesso nei paragrafi precedenti, creare Dapp.



La parola "Dapp" identifica molto semplicemente quelle che comunemente vengono chiamate "applicazioni decentralizzate"; capire cosa siano questi strumenti è abbastanza semplice. Tutti noi abbiamo installata sul cellulare un'applicazione di qualche tipo, sappiamo quindi benissimo cosa sia un'applicazione e sappiamo che alcune di queste app hanno bisogno di collegarsi a internet per funzionare.

Le Dapp, a differenza di quello che accade con le app che abbiamo sul nostro smartphone, invece che collegarsi a un database per funzionare si collegano a una blockchain; per capire di cosa stiamo parlando basterà fare un esempio banale ed immaginare una qualunque applicazione che consenta il pagamento di un servizio come la consegna di fiori a domicilio.

Un'app di questo tipo ti permette, attraverso internet, di visionare l'offerta del negozio di fiori attraverso una galleria fotografica e, una volta scelto il prodotto che desideri comprare (un mazzo di rose rosse ad esempio), ti permette di concludere l'ordine direttamente online usando i dati della tua carta di credito; concluso il processo di vendita, poi, trasmette l'ordine al negozio di fiori che invia il mazzo di rose all'indirizzo indicato dall'utente durante l'acquisto del prodotto.

Un'app decentralizzata fa tutte queste cose, ma le fa connettendosi a una blockchain; invece che usare i dati della tua carta di credito usa i dati dell'indirizzo di un tuo wallet, anche l'ordine viene trasmesso al negozio di fiori con un messaggio attraverso la blockchain, il tutto, molto semplicemente, viene gestito attraverso gli smart contract.

Qual è il vantaggio di tutto questo? Che le commissioni sono più basse sia per chi compra sia per chi vende. Mentre però è molto comune che le piattaforme presenti sul mercato consentano la creazione di Dapp, le piattaforme che permettono di fare la stessa cosa con un sito web sono ancora poche; tra le poche che offrono questa opportunità quella attualmente più "attenzionata" si chiama EOS. Parliamo di un progetto molto giovane, il suo white paper (il documento che descrive quali sono gli usi della piattaforma e come funziona) risale infatti solo al 2017; come ogni progetto simile, quindi, abbiamo una piattaforma, che viene chiamata eos.io, ed una criptovaluta nativa che prende

il nome di EOS. Inizialmente EOS non era nemmeno una criptovaluta, ma un token erc20; viene in pratica definito così (erc20) lo standard tecnico che bisogna usare per creare dei token sulla blockchain Ethereum. Quello che block one ha fatto (così si chiama la società privata che ha la proprietà del progetto) è stato emettere una ICO per finanziarsi, ha quindi creato un token erc20 e lo ha venduto agli investitori; nello specifico la ICO di EOS ha raccolto la bellezza di 4 miliardi di dollari. Tutto questo è avvenuto in una fase preliminare, sulla base della semplice pubblicazione del white paper; quando poi finalmente (a giugno 2018) è stata rilasciata la piattaforma (come software open source), gli utenti hanno potuto convertire i loro token erc20 nelle nuove monete (EOS). Ma perché EOS sta raccogliendo tutte queste attenzioni? Perché si tratta di un progetto molto ambizioso che punta ad offrire un unico ambiente di sviluppo per la creazione di qualunque tipo di prodotto che funzioni sulla base di una blockchain.

Tra le varie funzionalità offerte da questa piattaforma anche la possibilità di archiviare e ospitare in modo permanente file accessibili da qualsiasi browser web; eos.io, in altre parole, permette di creare siti web decentralizzati (ne parleremo meglio tra poco). La piattaforma eroga agli utenti, in misura proporzionale a quante monete possiedono, sia la larghezza di banda che lo storage sulla blockchain; per farlo utilizza un protocollo di consenso Dpos che permette, tra le altre cose, di partecipare alla governance del progetto esercitando quindi il proprio voto quando richiesto in misura proporzionale alle monete che si possiedono.

E' proprio questo il grande equivoco delle piattaforme che usano un protocollo di consenso Dpos, come abbiamo visto nel quarto capitolo, che la rete partecipa al voto sulla base della regola "una moneta vale un voto", per cui a indirizzare gli esiti dei vari voti alla fine saranno sempre gli utenti più facoltosi. Siamo quindi di fronte a una vera e propria oligarchia, almeno questo sostengono i detrattori di EOS; in ogni caso parliamo di una piattaforma molto evoluta, che permette di fare cose molto interessanti, non ultima la realizzazione di siti web decentralizzati. Sfruttando proprio eos.io, ad esempio, si sta creando una versione decentralizzata di wikipedia che non solo, essendo archiviata su blockchain, è accessibile ovunque e non può essere censurata, ma che retribuisce chi partecipa alla creazione dei contenuti attraverso un token.

Il progetto si chiama everipedia.com ed è già oggi disponibile sul web. Chiunque quindi può navigare su everipedia.com e rendersi conto che l'utente, limitandosi a navigare il sito, nemmeno distingue la differenza tra un sito normale e uno decentralizzato. In questo momento in molti riconoscono alla piattaforma eos.io una serie di punti di forza che vanno dalla capacità di gestire un elevato numero di transazioni in poco tempo (parliamo quindi di scalabilità), flessibilità (perché permette di revocare le transazioni, mentre una vera blockchain dovrebbe essere immutabile) e, soprattutto, viene considerata tra le più facili da usare per gli utenti, ha quindi, in altre parole, un'elevata user friendly che permette anche agli utenti meno esperti e con poche competenze informatiche di usare la piattaforma in tutte le sue funzionalità.

Tutto questo, però, rende eos.io qualcosa di diverso rispetto a quanto siamo abituati a pensare, non siamo più di fronte a una vera blockchain, ne tanto meno questa rete appare realmente decentralizzata; questa è la critica che i detrattori fanno al progetto, una critica che appare sostanzialmente vera. Ma questa considerazione non deve indurci a credere che non ci sia spazio per un progetto come EOS sul mercato; di progetti che usano questo tipo di tecnologia ma che

appaiono sostanzialmente centralizzati in giro ce ne sono parecchi e molti fanno egregiamente il proprio lavoro.

Nonostante l'auspicio, per quel che mi riguarda almeno, è che nel lungo periodo si impongano i progetti realmente e pienamente decentralizzati, riconosco che ci sarà probabilmente sempre spazio per una visione differente di ciò che questa tecnologia può rappresentare; bisogna poi aggiungere che, anche in virtù della grande "usabilità" che questa piattaforma dimostra, eos.io ha comunque il merito di rendere più semplice alle persone comuni avvicinarsi a questa tecnologia, cosa che apporta dei benefici comunque a tutto l'eco-sistema. Più utenti usano le criptovalute, indipendentemente dal tipo di moneta che scelgono di utilizzare, più questo nuovo standard si consolida favorendo una diffusione sempre più capillare di questa tecnologia.

7.6 LITECOIN

Anche se ultimamente pare ci sia la tendenza a dotare le piattaforme di funzionalità sempre più evolute le cose non sono sempre state così; è esistito un tempo in cui a una "povera" blockchain non si chiedeva altro che di processare le transazioni in maniera veloce e a costi irrisori.

Solo di recente le cose sono degenerate (scherzo) ed oggi poco manca che si arrivi a pretendere che una blockchain sappia fare anche il caffè. Tra le monete più "anziane" ancora in vita, dopo Bitcoin ovviamente, abbiamo Litecoin, comunemente considerata una sorta di fratello minore di BTC.

LTC nasce nell'autunno 2011 su impulso di un ex dipendente Google (Charlie Lee), che intuì la necessità di un nuovo tipo di approccio per affrontare alcune criticità che stavano emergendo con Bitcoin; alla nuova moneta, creata a partire dallo stesso codice sorgente di Bitcoin, vennero apportate alcune modifiche (vedremo più avanti quali) e già due anni dopo il suo lancio (nel 2013) aveva attirato le attenzioni dei maggiori investitori internazionali raggiungendo una capitalizzazione di mercato pari a circa un miliardo di dollari (oggi quasi quadruplicata). Ma in cosa LTC si distingue da BTC? Beh, per prima cosa per la fornitura di monete (definita in gergo "supply"), ovvero la disponibilità complessiva di monete che possono essere messe in circolazione; litecoin ha una supply che è circa quattro volte maggiore rispetto a Bitcoin (con un numero massimo di 84 milioni di monete che potranno finire in circolazione posto che, attualmente, ce ne sono in circolo poco più di una cinquantina di milioni). Entrambe usano un protocollo proof of work ma Litecoin usa un diverso algoritmo di hashing che lo rende circa quattro volte più veloce di BTC; a livello concreto questo significa che Litecoin processa un nuovo blocco ogni due minuti e mezzo, laddove con Bitcoin ne servono dieci (LTC, in altre parole, è più veloce, ed anche per questo viene comunemente considerato una versione più leggera di BTC).

Altro particolare non esattamente trascurabile, soprattutto se si desiderano movimentare ingenti somme di denaro, sono le commissioni, che in Litecoin sono mediamente molto più basse e meno soggette a fluttuazioni come invece accade quando si movimentano BTC. Nonostante le differenze tra le due monete siano piuttosto marcate, però, evidentemente non lo sono abbastanza per i

detrattori, che reputano Litecoin sostanzialmente un clone di Bitcoin arrivando a sostenere che, in quanto tale, non abbia alcun motivo concreto di esistere; al netto di quanto possano sostenere i detrattori, ogni moneta ha i propri, il motivo per cui esistono così tante criptovalute credo che sia imputabile al fatto che esiste una sensibilità differente ai diversi tipi di problemi che una blockchain può palesare. Uno dei primissimi obiettivi dichiarati di Litecoin, ad esempio, è ridurre la grande volatilità che caratterizza Bitcoin, cosa che per chi è abituato a possedere BTC potrà non essere importante ma che per molti utenti ha una sua rilevanza.

Ciò che per tante persone non rappresenta un problema (come la volatilità, appunto), per altre può rappresentare un vero incubo; monete differenti, quindi, pongono un'attenzione differente ai diversi problemi, implementando ognuna soluzioni che vanno incontro ad esigenze a loro volta diverse. Ed è proprio dalla molteplicità di esigenze differenti, a mio parere, che deriva la molteplicità di criptovalute che osserviamo sul mercato; in mezzo a tutta questa varietà una moneta con una così grande anzianità come Litecoin, caratterizzata da una ridotta volatilità, basse commissioni e velocità delle transazioni rappresenta, inevitabilmente, un punto di riferimento imprescindibile per larga parte della comunità che opera con le criptovalute.

7.7 MONERO

Abbiamo concluso il paragrafo precedente dicendo che la grande varietà di criptovalute presenti sul mercato è direttamente correlata alla grande varietà di esigenze diverse che gli utenti hanno quando usano una criptovaluta; l'idea iniziale di Satoshi, al netto delle interpretazioni emerse successivamente, era di creare una moneta alternativa, che garantisse l'anonimato delle transazioni e in cui tutti i nodi che partecipavano alla rete, senza alcuna esclusione, potessero riscuotere un compenso per il lavoro svolto.

Ad oggi, però, nemmeno Bitcoin risponde a queste caratteristiche, nemmeno BTC, in altre parole, aderisce pienamente a quella che viene chiamata la "visione di Satoshi". Il primo e più scontato motivo è che Bitcoin non è anonimo, ma pseudo-anonimo, il che significa anche che è possibile seguire le tracce di ogni transazione fino a risalire all'identità della persona che l'ha ordinata.

Vi è poi un motivo più rilevante del mero anonimato che porta BTC a discostarsi in maniera sensibile da quella che viene considerata l'originale "visione" di Satoshi e cioè che Bitcoin, purtroppo, è esclusivo; la corsa al mining, infatti, è diventata una vera e propria corsa all'oro, con i minatori impegnati ad acquistare nuovo hardware con lo scopo di rendere i loro computer sempre più competitivi. Tutto questo ha finito inevitabilmente per tagliare fuori i piccoli minatori favorendo la nascita di vere e proprie industrie che, mettendo in serie centinaia di schede grafiche (GPU), sono capaci di generare una potenza di calcolo semplicemente impressionante; e non stiamo nemmeno considerando quei circuiti integrati (che vengono chiamati ASIC e che arrivano a costare diverse migliaia d'euro) pensati ad hoc per eseguire l'algoritmo di hash di Bitcoin.

Chiunque può facilmente arrivare a intuire che dotandosi di questi dispositivi è possibile aumentare la propria influenza sulla rete semplicemente lavorando sulla potenza di calcolo che si è capaci di

esprimere; ormai da diversi anni non è più pensabile minare BTC col semplice computer di casa per cui a controllare la rete sono quelle che vengono chiamate “mining farm”, vere e proprie fabbriche che fanno del mining il loro core business. Le persone comuni non sono comunque del tutto escluse dal mercato minerario, per contrastare questo tipo di accentramento sono infatti nate delle comunità (chiamate in gergo pool) che consentono agli utenti di aggregarsi insieme per competere con la grande industria mineraria. In tutto questo, chiunque lo capisce facilmente, doveva esserci per forza una moneta alternativa a Bitcoin, con caratteristiche più simili alla visione originale di Satoshi; di criptovalute che aspirano a fare questo (a scalzare cioè Bitcoin dal suo ruolo di regina delle criptovalute) ce ne sono molte, ma quella più rappresentativa, a mio parere, in questo senso è Monero (sigla XMR). La nascita del progetto può essere fatta risalire al 2014 e coincide sostanzialmente con un fork di Bytecoin (BCN) proposto sul forum bitcointalk da un utente chiamato “thankful_for_today”; a prendere in mano la situazione, che sembrava destinata a naufragare nel nulla, arriva, su iniziativa della stessa comunità, un altro utente, chiamato “Johnny Mnemonic”, che pone le basi concrete per la nascita di Monero (che nelle intenzioni iniziali si sarebbe dovuta chiamare BitMonero). Il nome di questa criptovaluta, banalmente, è una parola che, tradotta dall’esperanto, significa “moneta”; il progetto oggi è guidato da 7 membri, 3 ricercatori e 49 sviluppatori (tra i quali i due più in vista sono senza dubbio Riccardo Spagni e Fransisco Cabañas), che si presentano sotto lo pseudonimo comune di Luigi1111.

In conformità con la visione originale di Satoshi, quindi, l’obiettivo dichiarato di Monero è di ottenere l’anonimato delle transazioni; per riuscire ad ottenere questo risultato XMR utilizza una soluzione chiamata “ring signature” (in italiano suonerebbe come “firma ad anelli”) il cui scopo è rendere impossibile risalire a chi abbia firmato una transazione. La ring signature, però, ha evidenziato nel tempo diverse criticità, di conseguenza gli sviluppatori hanno introdotto una nuova soluzione che prende il nome di Ring Confidential Transactions (RingCT) e che permette di oscurare l’importo oggetto della transazione. In questo modo la Ring signature (che permette di nascondere gli indirizzi da cui partono le transazioni), coniugata con la RingCT (che oscura l’importo delle transazioni) e con i così detti “indirizzi stealth” (che provvedono a nascondere gli indirizzi beneficiari delle transazioni) diventa possibile processare le transazioni garantendo al contempo elevati standard in termini di privacy.

Altra caratteristica che rende Monero una moneta molto interessante è la sua capacità di resistere al processo di accentramento della potenza di calcolo; questo avviene perché, prima di tutto, il processo di mining è “ASIC resistente” (non esiste quindi hardware costruito ad hoc per minare questa moneta) e, in secondo luogo, perchè l’algoritmo di hashing usato da XMR (CryptoNight) è profondamente differente da quello usato da Bitcoin e consente veramente a tutti di minare utilizzando sia la CPU (il processore del computer) sia la GPU (la scheda grafica).

Per quanto riguarda invece il problema della scalabilità Monero sembra dimostrare buone caratteristiche di flessibilità in virtù del fatto che, contrariamente a quanto avviene con Bitcoin, la grandezza dei blocchi non è predefinita ma può adattarsi alle esigenze della rete; vi sono però, ovviamente, degli automatismi che prevengono il rischio che l’aumento di dimensione dei blocchi si protragga troppo a lungo.

Ma perché allora Bitcoin vale così tanto più di Monero? Beh, intanto perché è una moneta molto più anzina, ma c'è anche un motivo meno banale di questo e che riguarda il rischio che la diffusione di questa criptovaluta venga osteggiata dagli stati. Non che i governi siano in qualche modo contrari a prescindere alla tecnologia blockchain, esistono anzi diversi progetti realizzati da numerosi stati che puntano a provare questa tecnologia in diversi settori (dalla gestione della pubblica amministrazione all'erogazione di servizi ai cittadini), ciò che i governi però non sembrano disposti a tollerare è proprio l'anonimato.

Monero, ma non è l'unica moneta a farlo, fa dell'anonimato delle transazioni il perno centrale del proprio sviluppo, l'anonimato è praticamente la sua vocazione, questo rappresenta la sua forza e, paradossalmente, la sua debolezza; se da un lato, infatti, ci sono milioni di utenti che pretendono la privacy delle loro transazioni e per i quali una moneta come Monero ha inevitabilmente grande valore, dall'altro lato ci sono i governi che non sembrano intenzionati a tollerare questo livello di privacy a fronte della necessità, così sostengono, di prevenire attività come l'evasione, il finanziamento al terrorismo e il riciclaggio di denaro.

Il timore, quindi, di tutti gli utenti che usano monete come Monero è che presto o tardi possa arrivare un giro di vite da parte dei governi che punti a vietare l'uso delle criptovalute anonime; questo tipo di timore, però, si fonda sull'ipotesi che i governi possano vietare qualcosa su internet, cosa che fino ad oggi raramente si è rivelata esatta.

Prendiamo ad esempio la pirateria informatica, è un reato che prevede pene anche molto severe (dipende dal paese), vietato praticamente in tutto il mondo ma che non impedisce a un film appena uscito nelle sale di finire online nel giro di meno di 24 ore. Per dirlo con parole diverse, quindi, che i governi possano decidere un giorno di arrivare a vietare l'uso di criptovaluta anonima è uno scenario nemmeno troppo improbabile per il futuro, ma rimane ad oggi francamente inverosimile che possano riuscirci concretamente.

7.8 STABLE COIN

Nel paragrafo precedente abbiamo iniziato a prendere in considerazione la possibilità di un grande interesse da parte degli stati e dei governi nella blockchain; questa tecnologia, infatti, con la trasparenza che la caratterizza, rappresenta un punto di svolta importante per quelle politiche che fanno della privazione della privacy finanziaria lo strumento fondamentale di contrasto a numerose condotte illecite, come ad esempio l'evasione o il riciclaggio di denaro.

Questo è il paradosso più grande che caratterizza il mondo delle criptovalute, se da un lato infatti Bitcoin è criticato proprio perché, a detta dei detrattori, favorisce condotte illecite, con la stessa tecnologia si potrebbero però prevenire gran parte di quelle stesse condotte illecite. Al netto delle valutazioni di carattere etico e morale, che pure sono parte integrante della discussione, il punto è che in ogni caso Bitcoin aumenta il livello di riservatezza delle transazioni rispetto a quanto accade nel normale circuito bancario; certamente, ci sono dei punti di ingresso nella rete Bitcoin, le piattaforme attraverso le quali cambiamo la nostra valuta fiat in BTC (ad esempio), che permettono comunque di risalire all'identità della persona a cui fa capo la transazione, ma questo non cambia il fatto che il livello di privacy garantito da Bitcoin è superiore a quello garantito dal circuito bancario.

Basterebbe però semplicemente che, per fare un esempio, ogni indirizzo generato fosse riconducibile all'individuo proprietario del wallet perché tutta la privacy garantita dalla blockchain sparisca in un attimo; se proviamo a immaginare un wallet che generi tutti gli indirizzi a partire dal codice fiscale di un soggetto ecco che tutte le transazioni diventerebbero immediatamente

riconducibili alla persona fisica. Ognuno a quel punto firmerebbe le transazioni con la propria chiave privata, ma ognuna di queste transazioni conterrebbe anche l'hash dell'indirizzo, a sua volta riconducibile al codice fiscale della persona fisica; tutto questo ovviamente ipotizzando un futuro in cui la valuta di carta venga sostituita dalle criptovalute.

Se immaginiamo al posto dell'euro (con le sue banconote e i suoi circuiti bancari) un cripto-euro (con la sua blockchain) ecco che con questa tecnologia diventa possibile ricostruire ogni minimo spostamento di denaro fatto da una persona; ma non solo, pensiamo ad esempio all'IVA, uno smart contract potrebbe stornare l'IVA di ogni singolo acquisto direttamente a un indirizzo controllato dall'erario. Uno smart contract potrebbe gestire il pagamento di ogni singola imposta e l'utente/cittadino potrebbe facilmente modificarne le condizioni introducendo nuove variabili che consentano, ad esempio, pagamenti rateizzati (o altro tipo di flessibilità sul piano di rientro iniziale).

Tutto questo può essere ovviamente realizzato anche in un sistema che tuteli la privacy degli utenti, ma a quel punto la capacità di prevenire le condotte illecite andrebbe a farsi benedire; i benefici, in entrambi i casi, sono molti e su diversi livelli, per cui non è utopia pensare a un futuro (nemmeno troppo lontano) in cui le criptovalute arriveranno a sostituire il denaro come lo conosciamo. Questo appare sotto molti aspetti inevitabile, mentre appare meno scontato riuscire a capire se questo cambiamento avverrà in un contesto che comunque protegge, tutela e riconosce come un diritto la privacy finanziaria dei cittadini o se si preferirà invece, in nome della legalità, azzerare ogni diritto degli utenti alla privacy. Le criptovalute come le conosciamo oggi, però, non hanno le caratteristiche per produrre un cambiamento del genere nella società; è impensabile, infatti, gestire le transazioni che quotidianamente ognuno di noi fa usando delle monete così volatili.

Quando paghiamo un caffè al bar, ad esempio, il proprietario del bar non deve preoccuparsi che il valore della moneta con cui lo stiamo pagando salga o scenda, quella moneta varrà sempre un euro anche il giorno dopo; con le criptovalute quotate sul mercato oggi questo non è per niente scontato, una moneta che oggi prezza a 100$ domani mattina potrebbe prezzare 67$ e aver bruciato un bel pezzo del proprio valore nel giro di una notte. Ma allora come fanno tutti quelli che accettano pagamenti in Bitcoin? In genere convertono in valuta a corso legale immediatamente dopo aver ricevuto il pagamento (cosa che ovviamente può avere costi anche molto variabili); non è infrequente comunque che chi accetta pagamenti in BTC poi quel denaro lo reinvesta, magari in un'altra criptovaluta. Indipendentemente da cosa si fa, e dallo scopo per cui lo si fa, bisogna capire che se pure è certamente vero che esistono vari modi attraverso cui si può disinnescare la volatilità ogni soluzione ha immancabilmente un costo.

Non si può pretendere che una moneta gravata da una miriade di commissioni, per quanto piccole, possa essere considerata comunemente un buon mezzo di pagamento; certamente per chi gestisce un e-commerce una moneta come Bitcoin rimane una soluzione migliore e più economica rispetto a quelle disponibili fino a poco tempo fa e questo spiega il motivo del successo delle criptovalute come metodo di pagamento sul web. Ma per pagarci il caffè al bar sotto casa è tutto un altro discorso. Come si fa allora a realizzare tutto questo? Come si fa a favorire la transizione dal denaro così come lo conosciamo alle criptovalute con tutti i benefici che ne conseguono? Semplice, tutto questo si può realizzare creando quelle che vengono chiamate "stable coin"; si tratta, molto semplicemente, di criptovalute il cui valore è ancorato al prezzo di una valuta a corso legale.

Oggi esistono decine di criptovalute (in certi casi semplici token) il cui valore è legato al prezzo dell'euro, del dollaro, del dollaro australiano, dello yen giapponese e di molte altre valute FIAT. Molti osservatori negli ultimi mesi hanno dichiarato pubblicamente di considerare il 2018 come l'anno delle stable coin, ed è probabilmente così che questo anno verrà ricordato nel mondo delle criptovalute, perché in questi ultimi dodici mesi il numero delle stable coin in circolazione è letteralmente decuplicato. L'interesse degli stati è alto, ma queste monete rappresentano sostanzialmente un esperimento, si tratta di progetti che sono appena entrati nel vivo e ciò che si sta tentando di capire è come ognuna di queste monete gestirà il rapporto con il relativo sottostante; le soluzioni, immancabilmente, sono diverse e questo favorisce il proliferare di questi strumenti.

Una delle primissime opzioni in campo, la più logica se ci pensiamo, è quella di legare l'emissione dei token ad accantonamenti di pari valore, legando quindi fisicamente il valore di una moneta a quello della valuta fiat che vuole rappresentare. Se creo un cripto-euro quello che devo fare, quindi, è semplicemente accantonare un euro per ogni cripto-euro che metto in circolazione; in questo modo il valore di un cripto-euro deve essere per forza quello di un euro.

Ma ci possono essere soluzioni differenti per perseguire lo stesso scopo, ad esempio io posso impegnarmi a garantire il rapporto di parità tra la criptovaluta e la valuta FIAT di riferimento creando ad hoc delle tensioni sul mercato (rialziste o ribassiste a seconda delle esigenze) e controllandone quindi il prezzo; qui abbiamo fatto solo due esempi, è ragionevole pensare che essendo questa corsa alle stable coin appena iniziata nei prossimi anni nascano soluzioni nuove per gestire questo aspetto fino a che non si imporrà uno standard che rappresenterà l'apripista a un'applicazione concreta di questi strumenti nella vita di tutti i giorni.

Ed è questo quindi, in definitiva, il motivo per cui stiamo assistendo a questo proliferare di stable coin, perché consentono ai vari paesi di sfruttare i vantaggi di una blockchain senza dover con questo rinunciare al controllo sulla leva della politica monetaria.

8. COSA SONO I WALLET

Già oggi che per gestire il nostro denaro abbiamo bisogno di una banca, i nostri soldi appaiono in un certo senso "smaterializzati"; certo, riceviamo periodicamente un estratto conto, però a ben vedere sono solo numeri su un pezzo di carta, fisicamente il denaro non è in nostro possesso.

Quello che succede, nello specifico, è che la banca si fa carico della responsabilità di garantire che una certa somma di denaro appartiene a me. Questa garanzia, quando parliamo di criptovalute, è data dalla blockchain, mentre per quel che riguarda la gestione e la movimentazione delle monete diventa un "problema" dell'utente; chiunque disponga di un servizio home banking lo fa già periodicamente, non c'è bisogno di un impiegato che inserisca una transazione al terminale al posto mio. Per fare tutto quello che prima faceva il nostro conto corrente in un sistema basato su una blockchain useremo un dispositivo che si chiama Wallet (portafoglio, in italiano); un Wallet ha le stesse funzioni di un conto corrente, ci permette di vedere il saldo complessivo, ci permette di gestire le transazioni, di ricevere e inviare denaro, possiamo addirittura farne una copia nel caso il dispositivo attraverso cui usiamo il nostro wallet andasse distrutto.

Esistono però diverse tipologie di wallet, che si distinguono le une dalle altre in termini di sicurezza, proprietà delle chiavi private, facilità di utilizzo e molti altri fattori ancora; nei prossimi paragrafi entreremo meglio negli aspetti tecnici che riguardano le varie tipologie di wallet, quello che ci preme rimarcare adesso è evidenziare ancora una volta come in un sistema basato sulla blockchain scompaia interamente l'utilità delle banche.

Se ogni utente controlla il proprio wallet (cioè il proprio portafoglio), può movimentare in qualunque momento il proprio denaro, è pienamente responsabile di ogni errore fatto nella gestione sia delle transazioni che del proprio wallet, non ha più alcun senso pagare una banca per avere un proprio conto corrente. Le banche, quindi, potranno continuare ad erogare mutui e prestiti, ma lo dovranno fare con i propri soldi (comprandoli quindi, come fa una finanziaria), potranno operare sui mercati, potranno fare tutto quello che hanno sempre fatto, ma non potranno più contare sui risparmi dei correntisti; in questo nuovo sistema, infatti, ogni correntista diventerebbe la propria stessa banca. Non penso che la blockchain finirà col far sparire completamente le banche, ma penso che finirà col rivoluzionare profondamente il modo in cui le banche operano.

Anche ipotizzando la nascita di una criptovaluta di stato (o comunitaria, nel caso europeo), in cui quindi il controllo della moneta rimane nelle manie delle grandi istituzioni centralizzate (banche incluse ovviamente), il denaro dei cittadini a quel punto non transiterebbe più per i conti corrente di una banca ma per gli indirizzi dei rispettivi Wallet; mentre quindi il dibattito italiano è ancora concentrato sulla necessità o meno di tornare a dividere il ruolo di banca commerciale da quello di banca d'affari ecco che a livello internazionale sta nascendo già un modello in cui è proprio la figura della banca commerciale a non essere nemmeno contemplata.

Non è detto che le banche spariscano, ma è abbastanza probabile che se la passeranno male; se pensiamo che con gli smart contract le persone comuni potrebbero creare dei fondi collettivi per erogare prestiti esattamente come fanno banche e finanziarie, ricavando quindi un interesse costante dal proprio investimento, ecco che iniziamo a capire quanto grandi ed importanti siano le sfide che le banche si troveranno a dover affrontare se vorranno continuare a sopravvivere in un mondo ridisegnato dalla tecnologia blockchain.

8.1 WALLET ONLINE

Il fatto che una cosa possa essere fatta gratuitamente non significa che in giro non ci siano persone disposte a pagare pur di non doversi sobbarcare l'impegno che gestire in prima persona quelle cose comporterebbe; portare a spasso il proprio cane, ad esempio, è qualcosa che chiunque fa gratuitamente, senza sognarsi nemmeno lontanamente di poter affidare a un'altra persona quella semplice mansione. Nonostante questo esistono altre persone che, per un motivo o per l'altro, preferiscono pagare qualcuno perché porti a spasso il cane; ecco, con i wallet è la stessa identica cosa. Chiunque può gestire il proprio wallet (ci sono diversi modi per farlo, ma lo vedremo più avanti), eppure tantissimi utenti preferiscono affidarsi a terzi soggetti che lo facciano al posto loro; per quanto questo comportamento possa apparire assurdo se descritto in questo modo in realtà tra i neofiti è molto comune avere un approccio di questo tipo col loro primo wallet.

Invece che acquistare specifici dispositivi, o scaricare pesanti programmi (sempre ammesso che sia possibile farlo) sul proprio computer molte persone per prima cosa utilizzano dei siti internet che servono proprio allo scopo di custodire le loro criptovalute, sono cioè dei Wallet online; quello che questi siti internet fanno è semplicemente custodire le chiavi private degli utenti permettendo l'accesso ai rispettivi fondi attraverso il normale login che qualunque utente è abituato a fare per accedere al proprio account su qualunque sito internet richieda una registrazione.

Questo presuppone, ovviamente, che l'utente nutra una certa fiducia verso il sito internet cui sta affidando le proprie chiavi private, anche perché si ritrova sostanzialmente privo di qualunque protezione; quello che l'utente sta rischiando è di svegliarsi la mattina successiva e scoprire che le proprie criptovalute sono sparite e che magari anche lo stesso sito internet risaluta irraggiungibile. Cosa si potrebbe fare in un caso del genere? Quasi nulla.

A parte questo sono numerosi i siti che negli anni si sono costruiti una grande credibilità e che ormai da tempo gestiscono la loro attività senza incidenti di sorta, con ottimi standard di sicurezza e lasciando gli utenti pienamente soddisfatti. Del resto non esistono particolari competenze necessarie per visitare un sito web, inserire la propria mail, una password sicura e creare il proprio wallet online; i siti che offrono questo tipo di servizi, poi, guadagno le loro belle commissioni su ogni spostamento di denaro quindi non hanno alcun concreto interesse nel permettere furti o tanto meno nell'appropriarsi dei fondi degli utenti.

Una volta aperto il nostro account sul sito di turno, quindi, senza spendere nulla, disponiamo già di un indirizzo Bitcoin (o altra criptovaluta) sul quale ricevere accrediti di denaro; con quell'indirizzo possiamo quindi ricevere un pagamento o possiamo anche inviare denaro (ovviamente prima depositandocelo sopra, quando apriamo il nostro indirizzo il suo saldo è chiaramente pari a zero). I wallet online, quindi, proprio perché sono gratuiti e facili da aprire sono molto spesso il primo approccio che un utente ha con questa tecnologia; difficilmente si può trovare in giro qualcuno che usi Bitcoin e non abbia mai aperto, anche solo per prova, un account su un wallet online. Ovviamente, però, ci sono modi più intelligenti di gestire le proprie criptovalute, come stiamo per scoprire nei prossimi paragrafi.

8.2 PAPER WALLET

Anche se una blockchain è immutabile e blindata questo non deve illuderci che anche i nostri computer lo siano; quando qualcuno prende la decisione di iniziare ad usare le criptovalute per prima cosa dovrebbe entrare nell'ottica di idee che l'anello debole di tutta la catena è il proprio stesso computer (o comunque il dispositivo che usa per conservare le proprie monete).

Nel paragrafo precedente abbiamo visto che ci sono siti internet che si offrono di svolgere proprio questo compito, sono quindi loro a gestire il nostro wallet (incluse le nostre chiavi private) e noi ci limitiamo ad usarle (facilmente e con grande naturalezza, come se fosse una sorta di Paypal); anche in questo caso, nonostante la sicurezza delle nostre monete sia affidata a un soggetto terzo, il punto debole di tutta la catena rimane il nostro dispositivo.

Che io scarichi un programma sul mio pc, una app sul mio smartphone, che usi un sito web di terze parti, che possieda o meno le mie chiavi private, tutto questo diventa sostanzialmente irrilevante se il dispositivo che sto usando viene compromesso da un virus o dall'incursione di un hacker; gestire il tuo portafoglio usando il collegamento wi-fi gratuito della tuo bar preferito, di conseguenza, potrebbe non essere una mossa molto intelligente. Questo rischio esiste sempre e comunque, a meno di non fare una copia delle proprie chiavi private e poi cancellarle da ogni altro dispositivo; è questo il senso di un paper wallet (portafoglio cartaceo in italiano).

Nel momento in cui possiedo una copia delle mie chiavi private, infatti, posso in qualunque momento movimentare quei fondi (posso risalire alla chiave pubblica e all'indirizzo facilmente grazie alla funzione di hash) e quindi posso anche cancellare ogni copia di quelle chiavi da qualunque dispositivo connesso a internet. In questo modo mi assicuro (sulla carta, e non è solo un gioco di parole) che nessuno potrà mai rubarmi quelle chiavi private anche qualora i dispositivi con cui mi connetto a internet venissero compromessi; le cose però non stanno esattamente così, i paper wallet, infatti, per lungo tempo considerati il modo migliore di conservare le proprie criptovalute, non sono in realtà così sicuri come sembrano. Il motivo è che il paper wallet dobbiamo sempre stamparlo, cosa che comporta il rischio che la memoria interna della stampante conservi una copia del documento che conteneva la nostra chiave privata e che un malintenzionato, trovandolo, movimenti i nostri fondi mentre noi siamo convinti e sicuri che nessuno al di fuori di noi possa farlo.

I wallet cartacei rimangono in ogni caso uno dei modi più sicuri per conservare le nostre criptovalute, ma al momento in cui li andiamo a generare dobbiamo essere sicuri di sapere cosa stiamo facendo e di non correre alcun rischio; molti utenti, ad esempio, per generare i loro paper wallet si avvalgono di specifici siti che generano un Qrcode sia della chiave pubblica che di quella privata e lo inoltrano sulla mail dell'utente (o gli permettono di scaricarlo). Fare le cose in questo modo, ovviamente, espone a numerosi rischi. Sono numerose le accortezze che un utente dovrebbe avere per creare in sicurezza il proprio paper wallet, eviteremo di descriverle perché è un argomento potenzialmente

quasi inesauribile, ed anche immaginando che un utente alle prime armi riesca, seguendo precise indicazioni, a creare un paper wallet realmente sicuro (cosa che comunque non richiede chissà quali capacità) il rischio sarebbe poi, in virtù di una piccola dimenticanza, di giocarsi l'intero importo depositato sul wallet cartaceo dopo la prima transazione.

Abbiamo già parlato del meccanismo di "addresses change" e di come avvengano le transazioni, ne approfittiamo adesso per comprendere quanto questa dinamica sia importante da valutare quando gestiamo un portafoglio cartaceo; immaginiamo che io riceva un compenso di 1BTC per aver scritto questo libro e che non avendo la necessità di spendere questi soldi decida di archiviarli in maniera sicura su un paper wallet. Trascorsi un paio di anni mi ritrovo nella necessità di usare quel denaro, quindi uso la mia chiave privata per spendere 0.1BTC in libri. Convinto di quello che ho appena fatto e soddisfatto dell'acquisto ripongo gelosamente il mio paper wallet con dentro i miei 0.9BTC residui; giusto? Sbagliato! Con la mia chiave privata, infatti, ho firmato una transazione pari a 1BTC trasferendone 0.1 all'e-commerce dal quale ho acquistato i miei libri e i rimanenti 0.9 al mio indirizzo.

Il nuovo importo di 0.9 BTC, oltre a poter essere finito in un indirizzo differente da quello originario, necessita di una nuova chiave privata per essere movimentato. Quello che avrei dovuto fare sarebbe stato stampare un nuovo paper wallet per i 0.9BTC residui, con la loro relativa chiave privata; quello che invece ho fatto è stato cancellare ogni traccia della transazione appena fatta e conservare gelosamente la chiave privata della transazione precedente (che però ormai è inutilizzabile per movimentare i miei fondi). Quando parliamo di paper wallet, quindi, prima ancora che la capacità di generare questi portafogli in maniera sicura, è necessario essere certi di conoscere bene il modo in cui questa tecnologia funziona. Sono numerosi, infatti, gli utenti che hanno perso i loro fondi a causa del "addresses change" e, come ormai dovremmo aver capito, questo genere di errori quando ci troviamo ad avere a che fare con una blockchain decentralizzata sono sostanzialmente irreparabili.

8.3 COLD STORAGE

Tenere al sicuro le proprie criptovalute significa sostanzialmente fare in modo di essere gli unici ad aver accesso alle proprie chiavi private; avendo una copia di queste chiavi, infatti, è possibile controllare i propri fondi da qualunque dispositivo. Per ottenere questo risultato, conservare cioè in maniera sicura le nostre chiavi private, è necessario conservarle in maniera tale che non siano accessibili attraverso internet; se le conserviamo su un dispositivo col quale poi navighiamo su internet, infatti, è sufficiente che il dispositivo venga compromesso perché un malintenzionato ci sottragga le chiavi private e, quindi, in pratica, il nostro denaro.

Nel paragrafo precedente abbiamo visto che è possibile conservare le nostre criptovalute su un qualunque pezzo di carta, semplicemente stampandoci sopra le nostre chiavi private; questa procedura richiede però delle accortezze, altrimenti continuerà ad esserci il rischio che le chiavi ci vengano sottratte nel momento in cui il nostro computer dovesse essere compromesso. Usare un paper wallet, poi, richiede di comprendere bene come funzionano le transazioni onde evitare di perdere il controllo dei fondi alla prima operazione fatta o altri incidenti (come ad esempio inviare

BTC a un indirizzo ETH) che pure possono capitare a chi opera senza cognizione di causa. Esiste per fortuna un modo più semplice, che è al contempo anche quello considerato il più sicuro, per conservare le nostre monete senza correre rischi e senza dover avere tutte queste accortezze; sto parlando del così detto "cold storage". Si tratta, in pratica, di dispositivi fisici (concettualmente simili a delle chiavette USB) che vengono chiamati comunemente Hardware Wallet.

Questi dispositivi custodiscono le nostre chiavi private e, di norma, offrono anche una procedura semplificata di backup, per cui ci consentono di fare il ripristino del nostro wallet a partire da ciò che viene chiamato "seme di ripristino"; ovviamente questi dispositivi hanno anche un costo, si possono trovare in commercio a prezzi di poco superiori ai 100€, ma sono un investimento necessario per tutti coloro che possiedono somme ingenti in criptovalute.

Non è neanche lontanamente ipotizzabile possedere anche solo 5mila euro senza aver investito un centinaio di euro in un wallet hardware; questi dispositivi, poi, possono offrire molteplici livelli di sicurezza, inclusa l'autentificazione a due fattori (che richiede quindi una conferma ulteriore per autorizzare ogni movimento di denaro) e sono certamente il modo migliore per conservare le nostre criptovalute. Una comodità maggiore, soprattutto per i trader, deriva dal fatto che ormai molti di questi dispositivi consentono di archiviare tutte le maggiori criptovalute, chi desidera quindi fare un investimento di lungo periodo non è obbligato a conservare le proprie monete sulla piattaforma di scambio ma può tranquillamente conservarle sullo stesso dispositivo su cui conserva, ad esempio, i propri Bitcoin. Ovviamente tutto questo sempre a patto che non si faccia confusione con gli indirizzi; ricordiamo infatti che inviare una somma di una certa criptovaluta all'indirizzo di una blockchain differente è un errore sostanzialmente impossibile da risolvere che inevitabilmente comporta la perdita del proprio denaro.

8.4 WALLET DESKTOP

Arrivati a questo punto capire cosa sia un wallet desktop dovrebbe essere decisamente intuitivo; sono, molto semplicemente, dei programmi che scarichiamo sul nostro computer e che ci permettono di interagire con la blockchain movimentando così i nostri fondi.

Esistono vari wallet di questo tipo, ed ovviamente ogni moneta ha il suo; quando parliamo di "wallet ufficiale" di Bitcoin, ad esempio, stiamo parlando di quello che viene chiamato "bitcoin core" cioè nient'altro che il programma scaricabile per PC, in pratica un wallet desktop. Il problema quando scarichiamo un programma come Bitcoin Core è che per funzionare deve prima scaricare tutta la blockchain e, completata questa operazione, deve anche "sincronizzarsi" (deve cioè effettuare una verifica preliminare di tutte le transazioni registrate); tutto questo richiede ovviamente tempo e per completare l'installazione di un programma come Bitcoin Core possono essere necessari anche più di un paio di giorni.

Ovviamente blockchain più giovani, che abbiano processato meno transazioni, sono più leggere da installare; la blockchain di Bitcoin invece è molto pesante e richiede quindi un bel po' di tempo per essere scaricata e verificata. Per evitare queste perdite di tempo esistono per fortuna dei Wallet Desktop (uno tra i più famosi per Bitcoin si chiama Electrum) che non richiedono di scaricare tutta la blockchain per funzionare e quindi possono essere installati più velocemente. Indipendentemente dal tipo di wallet che si sceglie questo genere di soluzione permette un controllo totale sulle proprie monete; con i wallet desktop è possibile creare un backup del proprio portafoglio, se ne può ripristinare uno vecchio e si possono, ovviamente, gestire le transazioni, ricevere pagamenti e inviarne.

Quello che dobbiamo iniziare a capire è che tutta questa varietà di wallet non sono in competizione tra loro, ma sono strumenti che ogni utente ha a propria disposizione e che usa abitualmente per

gestire il proprio denaro; ogni utente, quindi, possiede almeno un hardware wallet per conservare ciò che riesce a risparmiare, un wallet desktop per gestire i movimenti di denaro che deve fare tutti i mesi (per poi inviare ciò che avanza al proprio hardware wallet) e per spendere piccoli importi di denaro mentre è in giro durante la giornata utilizza ancora altri strumenti (che avremo modo di descrivere tra poco).

Adottare questo tipo di approccio ed avere una gestione razionale dei propri fondi quando si usano le criptovalute è una cosa molto importante; col tempo si impara a tenere separati gli importi che si usano per le spese di tutti i giorni da quelli destinati al risparmio e si acquisisce l'abitudine a non archiviare grosse cifre in un unico modo. Esistono decine di modi differenti per conservare le nostre criptovalute ed il modo più intelligente di farlo è di utilizzare tutte queste modalità differenti, sia perché ognuna di queste modalità diverse soddisfa un bisogno e un'esigenza differenti, sia perché in questo modo non rischieremo mai di perdere tutto ciò che abbiamo nella malaugurata ipotesi di un solo, singolo, incidente.

8.5 WALLET PER SMARTPHONE

Uno dei motivi per cui esistono le criptovalute è che serviva un metodo di pagamento vantaggioso per tutti (sia per chi sul web compra sia per chi sul web vende), sicuro e rispettoso della privacy dell'utente; senza arrivare alle comunque inevitabili questioni di carattere legale, fino a tirare in ballo fenomeni odiosi come l'evasione o il riciclaggio di denaro, a nessuno piace l'idea di essere profilato da un circuito di pagamenti e di vedere i propri dati personali (non solo quindi le transazioni ma anche età, città di residenza, sesso e altre informazioni strettamente private) raccolte accuratamente e rivendute a soggetti terzi (per farne l'uso che più fa comodo).

Le criptovalute esistono perché offrono a chi compra e a chi vende sul web un sistema di pagamento che costa poco e garantisce al contempo il rispetto della privacy degli utenti; nonostante questi aspetti positivi, nonostante il web avesse bisogno di una modalità di pagamento sicura e gli utenti di una modalità di pagamento che rispettasse la loro privacy, nonostante le criptovalute abbiano queste caratteristiche e permettano tutto questo a costi inferiori di quanto accada sui normali circuiti di pagamento, se oggi parliamo chiaramente di rivoluzione blockchain è perché prima ci sono state altre svolte altrettanto epocali. Intanto tutto questo non esisterebbe se non esistesse internet, ne i computer o gli smartphone avrebbero la diffusione e la rilevanza che hanno oggi se non fosse mai stato inventato il web; se possiamo poi stare qui a sprecare parole ipotizzando un futuro in cui le criptovalute abbiano interamente sostituito il denaro come lo conosciamo oggi è solo perché veniamo da 20 anni di sviluppo della telefonia mobile sfociati a loro volta in una rivoluzione tecnologica, quella degli smartphone.

Indipendentemente da internet, quindi, nulla importerebbe di quanto la tecnologia blockchain sia efficace e funzionale se non ci fosse la possibilità di portarsi dietro le proprie criptovalute come se fossero vero e proprio contante che possiamo spendere nelle piccole transazioni quotidiane, come ad esempio pagare pochi euro per una colazione al bar; tutto questo è possibile perché ognuno di noi ha in tasca uno smartphone, e questo dispositivo, ovviamente, può diventare il nostro wallet.

Così come sul computer andiamo a scaricare dei programmi che ci permettono di gestire le nostre monete, la stessa cosa possiamo fare scaricando delle apposite applicazioni sui nostri smartphone.

Ovviamente chiunque può capire che questa soluzione non è indicata per gestire ingenti somme di denaro, lo smartphone si può danneggiare o può essere rubato; certamente possiamo approntare delle misure di sicurezza tali da consentirci un ripristino immediato del wallet prima ancora che un eventuale ladro abbia la possibilità di sbloccare la password del nostro smartphone, in ogni caso è semplicemente il buon senso che ci spinge già normalmente a non portarci in giro grosse somme di denaro ed è ragionevole immaginare che continueremo a comportarci così anche in futuro.

Un wallet per smartphone è un'ottima soluzione per portare con noi piccoli importi, come ad esempio la somma necessaria a pagare un taxi, il biglietto di un museo e il costo di una cena; a meno che non ci siano motivi particolari che lo rendono necessario difficilmente una persona va in giro con più di 200€ al giorno, e quando è costretta a farlo vive la cosa con disagio.

In un sistema basato sulle criptovalute la necessità di portarsi dietro grandi quantità di denaro non esiste, se dovessimo riscuotere di persona un pagamento anche solo di 1000€ non daremmo l'indirizzo del wallet sul nostro smartphone, ma daremo ad esempio quello del nostro hardware wallet; possiamo comunque verificare l'andamento della transazione da qualunque dispositivo e assicurarci che questa venga confermata prima di considerare il pagamento effettuato (sulla blockchain infatti i pagamenti non possono essere revocanti e quando una somma di denaro è stata spostata non c'è modo di annullare il movimento appena registrato).

Siamo quindi dentro a un sistema in cui controlliamo pienamente il nostro denaro, in cui non dipendiamo da soggetti terzi per gestire i nostri conti e i nostri pagamenti, nel quale utilizziamo dispositivi diversi, con diversi scopi, per gestire diverse esigenze sulla base di diversi livelli di sicurezza. Le criptovalute mostrano, come sistema di pagamento, una versatilità enorme, che non è nemmeno lontanamente paragonabile a quella offerta normalmente dalle banche; e del resto viviamo un tempo, per quanto possa sembrare strano dirlo, in cui è diventato più semplice e immediato usare un cellulare per gestire un pagamento qualunque, fosse anche solo comprare il giornale, che non tirare fuori il portafoglio.

Oltre che più comodo è un sistema anche più sicuro; come abbiamo visto, infatti, basta avere un seme di ripristino e impostare una password per accendere il telefono per essere sicuri che anche se ci rubassero il dispositivo potremmo facilmente recuperare le chiavi private del nostro wallet e inviare la somma di denaro che avevamo sul nostro telefono a un indirizzo sicuro.

9. SCAMBIARE CRIPTOVALUTE

Con la nascita di Bitcoin nasceva la necessità di scambiare la nuova criptovaluta con valuta fiat; sin dall'inizio, infatti, chi desiderava capire in cosa consistesse questa nuova moneta aveva solo due modi per farlo, o entrare in possesso di qualche Bitcoin minandolo (cosa che inizialmente era molto più facile di quanto non sia oggi) o farlo comprandolo da qualcuno che lo possedeva già.

Quando poi, col tempo, alcuni commercianti iniziarono ad accettare questa nuova forma di pagamento anche loro avevano la necessità di convertire quel profitto realizzato in BTC in valuta a corso legale; anche i più accaniti sostenitori, quelli che hanno conservato i loro BTC più a lungo, nel corso del tempo hanno avuto anche modo di spenderli.

Oggi spendere le nostre criptovalute è diventato estremamente facile grazie alle carte, che ci permettono di convertire istantaneamente le nostre criptovalute prelevando denaro contante presso qualunque bancomat, ma a tutto questo ci siamo arrivati nel tempo, attraverso un'evoluzione che è durata anni. Come chiunque può immaginare, infatti, inizialmente non c'era nemmeno un vero e proprio mercato come c'è oggi, all'inizio esisteva solo Bitcoin e la maniera più semplice di convertirlo in valuta fiat era di scambiarlo fisicamente con denaro contante; ovviamente il baratto non era un modo molto razionale di gestire la cosa, nacquero così presto le prime piattaforme di scambio, quelle che tutti comunemente chiamano exchange e che oggi ci permettono di scambiare facilmente anche grandi volumi di criptovalute.

Nei prossimi paragrafi andremo a parlare proprio di questo, di come sia possibile scambiarsi criptovalute tra privati, delle piattaforme su internet che consentono di fare questo tipo di operazione e di alcuni particolari siti che ci permettono di scambiare importi anche ingenti di criptovalute con valuta a corso legale garantendoci la totale sicurezza nonostante il fatto che ci ritroviamo ad operare con dei perfetti sconosciuti; tutto questo, in definitiva, fa parte di quello che fino adesso abbiamo chiamato "ecosistema delle criptovalute", una realtà stratificata e complessa di servizi che consentono agli utenti di gestire la loro criptovaluta, di scambiarla e di usarla per comprare beni e servizi.

9.1 LOCALBITCOIN

Se dal primo momento era sembrato scontato che il modo più semplice di scambiarsi criptovalute fosse di persona, andando sostanzialmente a comprare Bitcoin usando il denaro contante, che per costruire un "mercato" di questo tipo (fondato quindi su una sorta di baratto) fosse necessario ricorrere al web era una scelta altrettanto scontata. Il successo stesso di internet, non a caso, era passato anche attraverso tutti quei servizi (ancora oggi ce ne sono decine) che consentono la vendita tra privati, in cui quindi c'è qualcuno che mette un annuncio e qualcun altro che a quell'annuncio risponde.

Con Bitcoin le cose andarono esattamente così, ancora oggi c' è un sito che si chiama Localbitcoins (online ininterrottamente dal 2012) che mette in contatto chi compra e chi vende criptovalute a livello locale; attraverso Localbitcoins (e altri siti simili) la domanda e l'offerta si limitano però ad incontrarsi, hanno cioè un primo approccio, mentre lo scambio di valuta vero e proprio si gestisce di persona, tipicamente in contanti. Nelle grandi città non è difficile trovare qualcuno che voglia comprare anche cifre di una certa rilevanza (fino a qualche migliaio di euro) di criptovalute pagandole con denaro contante, ma non lo è da meno subire tentativi di truffa in questo modo; non sono infatti poche le persone che per aver scambiato le loro criptovalute in questa maniera si sono ritrovate in mano qualche migliaio di euro di soldi falsi.

Quando si procede con questo tipo di scambi, quindi, è sempre preferibile avere le dovute accortezze e non dare mai nulla per scontato; il rischio di trovarsi di fronte a persone intenzionate a truffarci esiste e va sempre tenuto in considerazione. Nonostante possa sembrare poco sicuro questo tipo di scambio è ancora oggi molto in voga, soprattutto perché attraverso questi canali si muove anche l'offerta di lavoro; ci sono infatti molte persone sparse per il mondo che hanno criptovaluta da spendere e vorrebbero investirla su un loro progetto.

Ovviamente non è comune trovare annunci su queste piattaforme per fare il panettiere, ma sono numerosi quelli relativi a lavori di traduzione, realizzazione di siti web e applicazioni per smartphone, oltre che ovviamente a un numero molto elevato di annunci di lavoro inerenti alla blockchain (emettere un token, creare uno smart contract, scrivere articolo per siti specializzati, etc). Tutto questo testimonia la porta rivoluzionaria di questa tecnologia, intorno alla blockchain è nato molto più che un semplice mercato, è nata una vera e propria economia con tanto di posti di lavoro, corsi universitari dai sicuri sbocchi professionali, progetti finanziati per milioni di euro; impensabile oggi come oggi che un tecnologia del genere, con tutte le sue potenzialità ancora non chiaramente espresse, capace di creare dal nulla un'economia che oggi vale miliardi di dollari, fatta di aziende, di posti di lavoro e di salari regolarmente retribuiti ogni mese, possa sparire nel nulla nel giro dei prossimi dieci anni.

L'esistenza di siti come Localbitcoins ci dimostra come la "cripto-economia" (possiamo credo tranquillamente abituarci a chiamarla così d'ora in avanti), contrariamente a quanto sostengono i suoi detrattori, non si fonda sul nulla ma poggia invece su basi concrete ed è sostenuta a diversi livelli; è francamente improponibile pensare che le persone che sono già venute in contatto con questa tecnologia, che hanno capito come funziona e che la usano già abitualmente possano

smettere di farlo nei prossimi dieci anni, mentre non è difficile immaginare che in un arco di tempo simile sempre più persone possano decidere di iniziare ad usare, per i più svariati motivi, una qualunque tra le centinaia di criptovalute attualmente disponibili sul mercato.

9.2 GLI ESCROW

Se in una qualunque grande città al mondo trovare qualcuno che voglia scambiare criptovalute è tutto sommato abbastanza semplice, nei piccoli centri le cose non sono altrettanti facili; nonostante questo io stesso, che pure vivo in un piccolo paese del sud Italia, nel 2016 ho avuto modo di sorprendermi del fatto che c'era una persona a meno di 2km da me che desiderava vendere 3BTC.

A dirla tutta quella persona era anche l'unica in tutta la provincia, quindi si trattava chiaramente di una coincidenza che si trovasse proprio vicino casa mia e magari, perché no, poteva anche trattarsi di un tentativo di truffa (questo non avrò modo mai di saperlo con certezza non avendo risposto a quell'annuncio). A tutto questo bisogna aggiungere che in molti paesi le banche sono, comprensibilmente, reticenti a favorire spostamenti di denaro verso le criptovalute e tendono a bloccare i bonifici in entrata ed in uscita collegati ai conti di alcune grandi piattaforme di scambio; come si fa quindi a scambiarsi criptovalute anche per importi rilevanti attraverso internet e senza rischiare di prendere il proverbiale pacco? Semplice, si usano dei servizi appositi che si chiamano "escrow". Su internet, infatti, ci sono decine di siti che permettono di fare esattamente questo; il sistema è tanto semplice quanto ingegnoso.

Questi siti non sono altro che un catalogo di figure terze che si assumono l'onere di gestire la transazione per conto di tutte le parti coinvolte; ognuno di questi utenti possiede un rating e, ovviamente, richiede un compenso per svolgere un incarico così delicato. La commissione richiesta da ogni escrow varia in base al rating che l'utente ha accumulato, un po' come su e-bay, quindi, il rating definisce la qualità del servizio offerto; è quindi abbastanza ragionevole riconoscere una commissione più alta a quegli utenti che nel tempo hanno concluso il maggior numero di transazioni, per importi di ogni tipo, lasciando sempre pienamente soddisfatte le parti.

Non c'è bisogno di dire che un utente inesperto potrebbe, a seguito di un suo errore, aver imputato la perdita delle proprie criptovalute all'escrow attribuendogli quindi un rating negativo. I motivi per cui un escrow può ricevere un giudizio negativo sono tanti, non solo la malafede, quindi non è così scontato per un utente ricevere un buon rating. Appurato questo, che tipo di attività svolge l'escrow? Semplicemente gli utenti che svolgono questa funzione fanno da ponte tra le due parti, chi vuole vendere i suoi Bitcoin, ad esempio, li invia all'indirizzo dell'escrow il quale, per concludere il processo di vendita, attende di entrare in possesso anche del relativo importo in euro (per fare un esempio) di chi quei BTC li vuole invece comprare. Quando l'escrow si trova in possesso di entrambe le somme di denaro, dopo aver ovviamente trattenuto le proprie commissioni, provvede a inoltrare quanto dovuto ai relativi proprietari e conclude lo scambio; in un sistema di questo tipo l'escrow non è incentivato a truffare le parti dileguandosi col malloppo, perché questo ne minerebbe per sempre la credibilità, impedendogli per altro di continuare a trarre profitto da questa attività.

Con questo sistema, quindi, le truffe diventano estremamente rare e difficili, escluso infatti il rischio che gli escrow possano agire in malafede, dal momento che sono retribuiti per non farlo, se anche una delle parti fosse intenzionata a tentare una truffa non potrebbe mai riuscire a portarla a compimento senza la partecipazione dell'escrow stesso.

Questo sistema, ovviamente, non è esattamente il più economico di tutti e probabilmente non è neanche il modo più comodo di scambiare valuta fiat con criptovalute, tuttavia viene usato da migliaia di utenti che ne testimoniano la qualità e l'efficacia ormai da anni.

9.3 PIATTAFORME DI SCAMBIO (EXCHANGE)

Esistono tanti motivi per i quali si può desiderare scambiare criptovalute (con altre criptovalute o con valuta fiat) ed esistono anche tanti modi diversi per farlo; quello che bisogna aver chiaro in testa è che c'è un modo giusto per soddisfare ogni diversa esigenza. Non capire questa semplice cosa, quando si ha che fare con le criptovalute, può portare a spiacevoli inconvenienti; un errore molto comune, ad esempio, è che la funzione di una piattaforma di scambio (o exchange che dir si voglia) sia quella di permettere la conversione delle diverse criptovalute in altre monete o in valuta fiat.

In realtà questo tipo di servizi è nato per permettere l'attività di trading e non per consentire semplicemente di cambiare le proprie monete. Immaginiamo ad esempio un avvocato che accetti di farsi pagare anche in criptovaluta; dal momento che solo pochi clienti decidono di pagarlo in questo modo l'avvocato tende a non spendere quei soldi e alla fine accumula una bella sommetta sul suo indirizzo Bitcoin.

A un certo punto, inevitabilmente, il nostro avvocato vorrà spendere questa somma e magari invece di spendere le sue monete così come sono decide, anche un po' pigramente, che è arrivato il momento di convertirle in euro; qual è il modo più comodo per farlo? Beh, basta aprire un account su una delle più grandi ed affidabili piattaforme di scambio del mercato e trasferire al loro indirizzo i BTC, a quel punto si piazza un ordine di vendita in euro e il gioco è fatto; giusto? Sbagliato! O meglio, non necessariamente le cose si riveleranno così semplici. Nel momento in cui il nostro bell'avvocato tentasse di bonificare sul proprio conto corrente la somma appena convertita in euro potrebbe trovarsi il conto congelato. Perché? Perché non ha letto le regole di compliance! Le piattaforme di scambio, in pratica, forniscono un servizio equiparabile a quello di una banca e soprattutto quelle più credibili lo sono proprio perché sottostanno a tutta una serie di norme e regolamenti che sono originariamente pensati per il comparto bancario.

Ovviamente non tutti gli exchange aderiscono a questo tipo di protocolli, senza che questo implichi che la loro attività sia in qualche modo considerabile illegale, semplicemente dipende dalle diverse norme che i diversi paesi applicano per gestire questo tipo di mercato. In Italia, ad esempio, aprire un exchange richiede di adeguarsi a norme molto stringenti e non è quindi un'attività semplice (e ancor meno economica) da avviare.

Questo complesso di regole, che prende il nome di compliance, prevede, tra le altre cose, oltre all'identificazione degli utenti (motivo per cui oggi come oggi quasi tutte le piattaforme richiedono l'invio dei documenti dell'utente) anche che i fondi depositati vengano utilizzati specificatamente per l'attività di trading; il nostro avvocato pensava di poter semplicemente cambiare i suoi BTC? Il nostro avvocato si sbagliava! Essendo il suo comportamento considerato improprio ed espressamente vietato dal regolamento della piattaforma (si, proprio quello che nessuno legge quando apre un account su un qualunque sito internet) il nostro bell'avvocato si è ritrovato il conto congelato.

Questo non significa che non sia possibile usare una piattaforma di scambio per cambiare i nostri Bitcoin, quello dell'avvocato è solo un esempio dei rischi che una persona pigra corre quando non

fa le cose con la dovuta attenzione, ma esistono numerosi exchange sul mercato, anche tra i maggiori, che non hanno regole così rigide; il nostro avvocato, quindi, è stato anche un po' sfortunato, non che la cosa importi, si è infilato in un bel guaio e ci metterà mesi a tirarsene fuori (ammesso che ci riesca).

Il mondo delle criptovalute, questo dovrebbe essere ormai abbastanza chiaro, è però decisamente refrattario ai regolamenti imposti dall'alto, quindi il fatto che gli utenti (inclusi gli stessi trader) siano costretti a sacrificare la propria privacy per poter operare legittimamente con le proprie monete (dal momento che devono inviare i loro documenti alle piattaforme di scambio per aprire un account) non è esattamente una delle norme più apprezzate all'interno della comunità; a un certo punto gli utenti, sui social e sui forum, attraverso i blog, hanno iniziato a dirsi che non sarebbe stata una cattiva idea costruire un exchange decentralizzato.

Del resto una piattaforma di scambio che cos'altro è se non un registro aggiornato di tutti gli scambi fatti? Esattamente il tipo di dati che possono essere processati attraverso una blockchain, basta che ci sia una rete decentralizzata di nodi che ne garantisca il funzionamento. A questo punto chiunque può intuire perchè in questo preciso momento sul mercato ci sono almeno una decina di piattaforme (con relative criptovalute native al seguito) che offrono esattamente questo servizio; gli utenti possono quindi trasferire le proprie monete su queste piattaforme e fare la propria attività di trading (o limitarsi semplicemente a cambiare le loro monete) esattamente come fanno attualmente con i grandi exchange centralizzati. Dove sta la differenza? Che in questo modo possono farlo in forma anonima e, in molti casi, senza pagare commissioni per ogni operazione che fanno; un bel vantaggio, non c'è che dire.

A rendere tutto questo ancora più facile da realizzare ha contribuito anche una recente innovazione, che prende il nome di "atomic swap", e che consente, in parole povere, di usare uno smart contract per processare uno scambio di valute tra monete appartenenti a catene differenti; in questo scambio lo smart contract si pone sostanzialmente come un vero e proprio escrow (tutela quindi entrambe le parti in causa) assicurandosi di spedire le monete ai relativi indirizzi validi. Immaginiamo che un utente voglia comprare degli ETH usando i propri BTC; uno smart contract prenderà i suoi BTC, si metterà alla ricerca di uno o più utenti capaci di soddisfare la richiesta al prezzo stabilito dall'utente e appena questo sarà possibile si auto-eseguirà saldando le rispettive parti agli indirizzi che ognuna di loro avrà precedentemente stabilito.

Quello degli exchange decentralizzati è uno dei migliori esempi per dimostrare i vantaggi della disintermediazione che, inevitabilmente, coincide anche con un crollo dei costi sostenuti dall'utente finale; la riduzione dei costi, poi, diventa quindi uno straordinario incentivo per convincere sempre più utenti ad abbandonare i modelli centralizzati in favore di quelli decentralizzati ed è per questo che, almeno nel lungo periodo, tutta questa nuova tecnologia basata sulla disintermediazione e la decentralizzazione sembra inesorabilmente destinata a vincere sui modelli (centralizzati) che attualmente regolamentano alcuni dei principali aspetti della nostra vita sociale.

10. INTRODUZIONE AL TRADING DI CRIPTOVALUTE

Inserire in un testo che si occupa di blockchain e criptovalute un capitolo dedicato al trading è, a mio parere, qualcosa di inevitabile; uno dei pregi di questa tecnologia, soprattutto per un paese come il nostro, è che tutti quelli che la scoprono avvertono immediatamente anche l'esigenza di iniziare a capire come funziona il mercato.

I motivi che spingono una persona a iniziare a fare trading di criptovalute possono essere diversi, c'è chi lo fa per pura curiosità, chi per comprendere meglio la stessa tecnologia, chi semplicemente perché intravede la possibilità di guadagnarci dei soldi, in ogni caso è estremamente comune che chi si accosta alle criptovalute quasi contemporaneamente decida di aprire un conto di trading su una piattaforma di scambio.

Questo ha permesso a tantissime persone di acquisire dei primi rudimenti di educazione economica-finanziaria, una forma di istruzione che è quasi completamente assente nel nostro paese e di cui ci sarebbe un gran bisogno; il salto "quantico" che le persone che iniziano ad usare Bitcoin e le altre criptovalute fanno è che dal momento che possiedono il pieno controllo del loro denaro allora possono anche liberamente investirlo. E per il resto, come mi piace affermare ogni volta che ne ho la possibilità, "anche una scimmia può fare profitto facendo trading"; in cosa consiste questa attività? Penso che basti una parola per dirlo e quella parola è "regole"; il trading è un sistema di regole. Tento di essere più chiaro; il valore di una determinata moneta cambia continuamente se messo in riferimento al valore di una seconda moneta, il valore di Bitcoin (ad esempio) cambia continuamente se posto in relazione al dollaro.

Quello che un trader fa è sfruttare queste oscillazioni di valore per trarre profitto, acquista BTC a un prezzo basso (ad esempio a 100$) e rivende a un prezzo più alto (ad esempio 120$); la differenza tra il prezzo di vendita e quello di acquisto rappresenta il profitto (o la perdita) concretizzato con

quella singola operazione. Se compro 1BTC a 100$ e lo rivendo a 120$ ho guadagnato 20$, se al contrario compro 1BTC a 120$ e lo rivendo a 100$ avrò perso 20$.

Nel trading di criptovalute possiamo osservare due grandi tendenze, quella dei trader che operano sempre in coppia con una valuta fiat (comprano ad esempio BTC per guadagnare Dollari) e quelli che commerciano in criptovalute (comprano una qualunque altcoin per guadagnare BTC); chi opera nel primo modo (accumula cioè dollari) è una persona che probabilmente è convinta che la supremazia delle valute fiat non verrà mai scalfita dalle criptovalute, di conseguenza usa le variazioni di prezzo per guadagnare più valuta a corso legale, chi opera invece nel secondo modo (accumula cioè Bitcoin) è una persona convinta che, indipendentemente da quanto succede durante i cicli ribassisti, Bitcoin sia destinato in un'ottica di lungo periodo a continuare ad aumentare il proprio valore toccando sempre nuovi picchi. Indipendentemente dal modo in cui si opera, poi, esistono differenti stili di trading che comunemente vengono identificati come:

1. **Scalping**: significa che il trader apre e chiude numerose transazioni nel corso della stessa giornata, puntando a fare profitto nel minor tempo possibile sfruttando anche le più piccole variazioni di prezzo

2. **Day trading**: in questo caso il trader tende a fare molte meno operazione, raramente si superano le due o tre nell'arco della stessa giornata e come regola di base ogni operazione viene aperta e chiusa rigorosamente entro le 24 ore

3. **Swing trading**: chi fa questo tipo di trading riduce ancora di più il numero di operazioni rispetto al day trader e come regola di base la durata del commercio si allunga da un giorno (durata massima del day trading) fino a una decina di giorni (orientativamente l'arco di tempo massimo entro il quale si dovrebbe chiudere la singola operazione)

4. **Cassettista**: opera più secondo una logica di investimento che non (come negli altri casi) in una logica puramente speculativa; tra quando il cassettista apre un'operazione e quando la chiude possono facilmente trascorrere mesi; difficilmente, inoltre, questo tipo di operatori si ritrova a gestire più di due o tre investimenti contemporaneamente

In linea di massima, comunque, un bravo trader sa adattare la sua operatività a tutti questi quattro stili di trading in base all'andamento del mercato; quindi a seconda del momento il trader decide di adottare uno stile al posto di un altro, lo stesso operatore che oggi fa scalping potrebbe poi improvvisamente adottare una logica da swing trading e poi tornare a fare scalping una volta chiuse le operazioni precedenti.

Come dicevamo, infatti, il trading è sostanzialmente un sistema di regole, una volta impostate correttamente queste regole inevitabilmente si inizia a fare profitto; questo non significa che si diventerà facilmente miliardari, ma semplicemente che si potrà in maniera relativamente facile far fruttare i propri risparmi. La cosa difficile, quando parliamo di trading, non è nemmeno imparare la tecnica (che tutto sommato è accessibile a chiunque), ma avere un controllo pieno della propria psicologia.

Ogni trader è infatti costantemente esposto a una grossa pressione psicologica che lo induce, indipendentemente dalle regole che si è dato, a vendere o a comprare in maniera poco razionale; il punto è che non importa quanto si possa essere bravi, tutti i trader fanno operazioni in perdita, un bravo trader semplicemente accumula più profitto che perdite. Le reazioni a livello psicologico di ogni operatore possono essere diverse e possono cambiare, oltre che da persona a persona, da situazione a situazione; non esistono quindi regole valide per tutti per gestire l'aspetto più impegnativo (che è proprio la dimensione psicologica) dell'attività di trading.

Nei prossimi paragrafi, quindi, oltre che a descrivere il funzionamento di alcuni strumenti fondamentali nell'attività di ogni trader, proveremo a fare anche delle riflessioni più generali su questo tipo di professione per offrire ad ogni lettore un punto di vista amplio e una base abbastanza solida dalla quale partire se desidera cimentarsi in questo tipo di attività.

10.1 COME LEGGERE I GRAFICI

Ritrovarsi a fare trading quando si scoprono le criptovalute è una cosa molto comune, il fatto che chi si accosta a questo tipo di attività lo faccia pensando di diventare immensamente ricco a tempo di record lo è, purtroppo, altrettanto. Anche se chiunque può imparare a sfruttare i cicli del mercato per trarre profitto non è detto che tutti coloro che si cimentano in questa attività raggiungano l'obiettivo; come accennato nel paragrafo precedente, infatti, il trading è un sistema di regole ma dato che queste regole ce le imponiamo da soli il più delle volte finiamo per decidere di contravvenirle. In ogni caso la prima regola che ogni trader deve seguire è "non investire mai più di quanto si sia disposti a perdere"; questo è l'unico modo per evitare che la pressione psicologica cui verremo sottoposti diventi ingestibile. Possiamo comunque imporci tutte le regole del mondo, se però non acquisiamo alcune piccole nozioni di base più che fare trading la nostra attività assomiglierà molto a giocare alla roulette.

La prima cosa che dobbiamo fare, quindi, è imparare a leggere i grafici di borsa che, in gergo, vengono chiamati "grafici a candele giapponesi"; ovviamente l'andamento del prezzo può essere reso graficamente anche da una linea retta, i grafici a candela ci danno però molte più informazioni di quante ne potremmo ricavare osservando una linea.

Il motivo per cui questi grafici si chiamano così è abbastanza intuitivo, i segni grafici (quelli colorati di rosso e di verde) assomigliano infatti a delle candele; la prima cosa che dobbiamo capire per interpretare correttamente questo tipo di grafici è che ogni candela esprime l'andamento del prezzo nell'unità di tempo definita dall'utente. Proprio per questo motivo sentiamo parlare di grafici da un'ora, da quattro ore, da un giorno, da una settimana e via dicendo, perché si intende che ognuna delle candele che compaiono sul grafico rappresenta ciò che è successo al prezzo nell'arco di tempo di un'ora, di quattro ore, di un giorno e così via.

Ora, immaginiamo di leggere un grafico 1D (one day, un giorno), sappiamo che ogni candela rappresenta graficamente quanto accaduto nel corso delle ultime 24h; molto semplicemente, quindi, se la candela è colorata di rosso questo significa che nelle ventiquattro ore il prezzo è calato, al contrario se la candela è colorata di verde significa che il prezzo è salito.

Altri due dati che la candela rappresenta graficamente sono i prezzi di apertura e chiusura che vengono rappresentati dal bordo inferiore e da quello superiore della candela; quando leggiamo una candela rossa (che segnala un calo di prezzo nell'unità di tempo) il bordo superiore indica il prezzo di apertura e quello inferiore il prezzo di chiusura della sessione, quando invece leggiamo una candela verde (che segnala l'aumento di prezzo nell'unità di tempo) è l'esatto contrario, in questo caso quindi il bordo inferiore della candela indica il prezzo di apertura e quello superiore il prezzo di chiusura.

In alcuni casi possiamo osservare delle candele che non sono colorate e assomigliano sostanzialmente a delle croci, questo tipo di candele indicano che il prezzo di apertura è stato

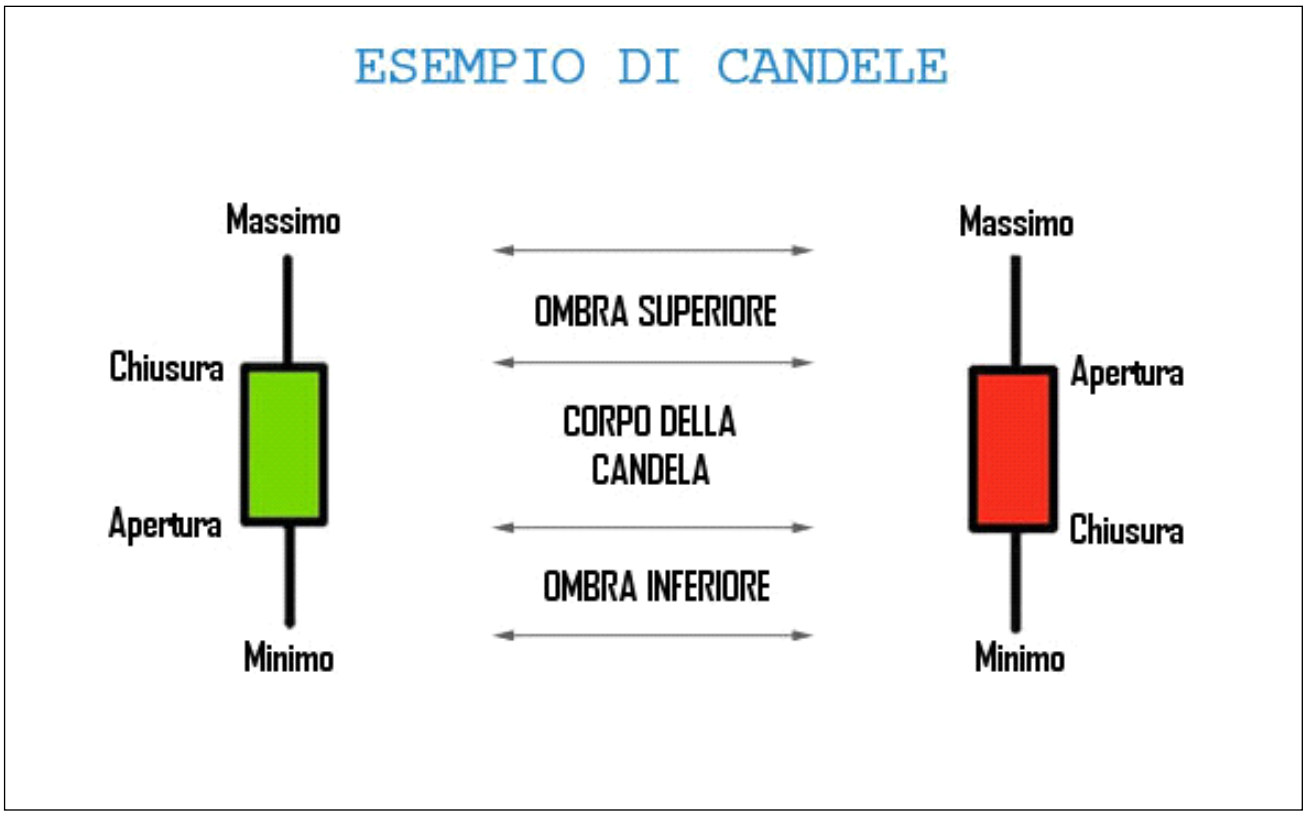
sostanzialmente identico al prezzo di chiusura; i bordi di queste croci (diretti verso l'alto o verso il basso) rappresentano graficamente le variazioni di prezzo (massime e minime) che si sono avute durante la sessione. Riassumendo una candela può essere colorata di rosso (quando il prezzo di chiusura è inferiore a quello di apertura) o di verde (quando il prezzo di chiusura è superiore al prezzo di apertura), il perimetro di queste candele (chiamato in gergo "corpo") rappresenta i livelli di apertura e chiusura nell'unità di tempo, mentre le linee rette che partono dalla cima o dal fondo della candela rappresentano i picchi, rispettivamente massimi e minimi, che si sono toccati nel corso di una sessione.

Facciamo degli esempi pratici e immaginiamo che il prezzo di 1BTC dopo essere partito da una quotazione di 10$ all'apertura abbia toccato un massimo di 15$ per poi chiudere la sessione a 12$, come viene rappresentato tutto questo dalla candela? Semplice, avremo intanto una candela verde (perché il prezzo è salito), simile a un rettangolo il cui margine inferiore è posizionato a quota 10$ (l'apertura) e il margine superiore è posizionato a quota 12$ (la chiusura); dal margine superiore, poi, vedremo partire una linea retta (chiamata in gergo "ombra") che raggiunge quota 15$.

Ancora un esempio ma questa volta immaginiamo che il prezzo di apertura sia 20$ e quello di chiusura 17$ con il minimo di giornata a 15$ e il massimo di giornata a 22$; in questo caso la candela sarà di colore rosso (sessione in perdita), il margine superiore (prezzo di apertura) sarà posizionato a 20$, da qui partirà l'ombra superiore (la linea retta) che rappresenta il massimo di giornata e che toccherà quota 22$, mentre il margine inferiore della candela (prezzo di chiusura) si attesterà a quota 17$, livello da cui partirà l'ombra inferiore (sempre un'altra linea retta) che raggiungerà il minimo di giornata a quota 15$.

Ultimo esempio, infine, una sessione che apre e chiude a 17$, in corrispondenza col minimo di giornata e con un picco massimo raggiunto di 20$; in questo caso la candela assomiglierà a una croce, non avrà quindi alcun colore perché prezzo di apertura e chiusura coincidono, non ci sarà alcuna ombra inferiore perché il minimo di giornata non è mai andato sotto all'apertura ma sarà presente una lunga ombra superiore che si estenderà fino a 20$.

Tutto quello che fino qui abbiamo illustrato a parole lo puoi trovare riassunto nell'immagine sottostante che ti permetterà di comprendere meglio tutta la nuova terminologia che abbiamo introdotto.



10.2 L'ANALISI TECNICA

Anche se non si direbbe in questi pochi paragrafi abbiamo già acquisito diversi concetti fondamentali per fare trading, per intanto abbiamo imparato come si legge un grafico a candele, poi abbiamo iniziato a intuire che fare trading significa crearsi un proprio sistema di regole; questo aspetto è fondamentale perché senza un sistema di regole efficace non riusciremo mai a fare profitto e sbaglieremo tutti i nostri trade.

Lo scopo di queste regole, però, non è quello di permettere di fare profitto quanto piuttosto quello di consentire al trader di alleggerire la pressione psicologica a cui inevitabilmente sarà esposto fino al momento in cui non chiuderà l'operazione; per stabilire invece come concretizzare il profitto ogni operatore si basa su quella che sostanzialmente è una vera e propria "raccolta di segnali".

La prima domanda che ogni persona si pone inevitabilmente quando inizia a fare trading è: che cosa muove il prezzo di una criptovaluta? Trovare una buona risposta a questa domanda significa già aver fatto il primo passo per diventare un buon trader. Il prezzo è mosso principalmente da due fattori e cioè dall'avidità del mercato e dalle notizie che irrompono sul mercato; questi due fattori, nel loro insieme, generano i movimenti di prezzo che ci permettono di fare profitto.

Quando iniziamo ad operare su un determinato mercato, indipendentemente dal tipo di mercato, ogni notizia che lo riguardi può scatenare una reazione di carattere rialzista o ribassista nell'andamento del prezzo; questo vale sempre e vale ovviamente anche per le criptovalute.

Ci sono notizie, come ad esempio la possibilità di un hard fork o il rilascio di una nuova versione della piattaforma (con nuove funzionalità), che scatenano inevitabilmente il rialzo dei prezzi, altre notizie, invece, fanno l'esatto contrario ed affossano il valore di una moneta; se si sparge la notizia che il wallet ufficiale di una certa moneta è difettoso o che una determinata criptovaluta sta per essere esclusa (delistata in gergo) da una grande piattaforma, queste sono notizie capaci di provocare grosse perdite al prezzo di una cripto.

Se capire come e perché le news muovano il mercato è abbastanza facile, più ostico è comprendere il modo in cui l'avidità degli operatori provoca le fluttuazioni del prezzo; per prima cosa quello che dobbiamo capire è che l'andamento dei prezzi non è mai lineare, meglio che come una retta, infatti, faremmo bene a immaginarlo come un'onda che oscilla tra dei minimi e dei massimi.

Quando iniziamo a immaginare l'andamento del prezzo come se fosse un onda iniziamo a inquadrare due differenti tendenze, una di breve periodo in cui il prezzo si muove tra dei minimi e dei massimi all'interno di quello che in gergo viene chiamato "canale" (vedremo più avanti di cosa si tratta), ed allo stesso tempo riscontriamo una seconda tendenza in atto, più di lungo periodo, che vede il prezzo destinato a crescere o diminuire.

Esistono ovviamente diversi strumenti a disposizione dei trader per riconoscere queste tendenze nell'andamento del prezzo (alcune delle quali avremo modo di imparare a conoscere più avanti) ma in linea di massima la dinamica a cui assistiamo è sempre la stessa; dal momento che tutti gli operatori perseguono lo stesso obiettivo (fare profitto) e leggono tutti lo stesso grafico nello stesso momento, quando si verificheranno determinate condizioni tutti gli operatori scatteranno in massa per approfittare dell'occasione ed ecco che, come detto, l'avidità del mercato finisce col muovere il prezzo.

Questo è però vero anche al contrario, le paure del mercato, quindi, possono provocare, in presenza di determinate circostanze, un'ondata di vendite che può portare il singolo trader a subire perdite anche importanti. La capacità di leggere le tendenze del mercato attraverso l'andamento del prezzo su un grafico, di riconoscere i momenti di inversione (sia di breve che di lungo periodo) nell'andamento della tendenza principale (indipendentemente dal fatto che sia rialzista o ribassista), tutto questo passa sotto il nome di "analisi tecnica"; quello che il trader fa, in altre parole, è usare gli strumenti a sua disposizione per definire l'andamento del trend e tentare di fare profitto sulla base delle variazioni di prezzo.

Il brutto dell'analisi tecnica è che non si tratta di una scienza esatta ma più che altro di un calcolo statistico; nessuno dei dati che ricaviamo dalla lettura dei grafici ci da mai delle garanzie, nonostante esistano segnali più rilevanti (e più affidabili) di altri non esistono segnali di trading sicuri al 100%; ogni buon trader, inoltre, oscilla naturalmente tra un approccio di tipo speculativo e uno più moderato basato sull'investimento, di conseguenza per un'operatività completa sul mercato l'analisi tecnica non è sufficiente ma bisogna affiancarle anche l'analisi fondamentale.

Tutti i concetti che stiamo esponendo esistono su ogni tipo di mercato, i grafici si leggono alla stessa maniera sia sul forex che sul mercato delle criptovalute, l'analisi tecnica è la stessa sia che tu stia investendo in azioni sia che tu stia acquistando delle monete, ed anche per quanto riguarda l'analisi fondamentale è un concetto che esiste sempre, a prescindere dal tipo di mercato su cui stiamo operando.

Quando acquistiamo delle azioni, ad esempio, l'analisi fondamentale consiste nella lettura del bilancio dell'azienda su cui stiamo andando ad investire; nel mercato delle criptovalute, questa volta diversamente da quanto avviene negli altri mercati, l'analisi fondamentale si fa raccogliendo informazioni di carattere differente, come per altro avremo modo di vedere meglio in uno dei prossimi paragrafi. Per adesso concentriamoci a conoscere alcuni elementari strumenti che ogni trader normalmente usa nella sua pratica quotidiana per ricercare dei segnali di trading che gli permettano di fare profitto.

10.3 SUPPORTI E RESISTENZE

Abbiamo detto che il prezzo si muove come un'onda all'interno di una tendenza di lungo periodo che può essere bullish (inglesismo col quale in gergo si indicano le tendenze rialziste) o bearish (termine che indica invece le tendenze ribassiste); molto semplicemente in un mercato rialzista il prezzo tende a toccare sempre nuovi picchi, mentre in un mercato ribassista tende a toccare sempre nuovi minimi.

Quando nel mezzo di una tendenza ben definita il prezzo non riesce a toccare un nuovo picco (minimo o massimo che sia), quello è un primo segnale di indebolimento della tendenza e ci indica che potremmo essere in prossimità di un'inversione del trend principale.

Se poi uniamo graficamente i picchi massimi raggiunti dal prezzo con una retta e facciamo lo stesso per i picchi minimi otteniamo graficamente dei livelli importanti a livello di analisi tecnica; questi livelli vengono definiti in gergo supporto (quando parliamo della retta che unisce i picchi minimi) e resistenza (quando parliamo della retta che unisce i picchi massimi).

In maniera molto intuitiva, quindi, quando il prezzo si trova in prossimità di un supporto questo rappresenta un livello difficile da rompere al ribasso e quindi è facile che (nella tendenza di breve periodo) il prezzo stia andando a rimbalzare; allo stesso modo quando il prezzo si trova in prossimità della resistenza, rappresentando quello un livello difficile da rompere al rialzo, è facile che il prezzo cominci a scivolare giù andando a cercare nuovamente il primo supporto utile. Bisogna comunque considerare sempre che tante più volte questi livelli vengono testati (vengono cioè raggiunti dal prezzo) tanto meno diventa probabile che possano reggere all'ondata successiva; quando il prezzo inizia a battere contro una resistenza prima o poi è probabile che riesca a romperla iniziando quindi a salire, e lo stesso vale ovviamente anche per i supporti. In linea di massimi i livelli che fungono da supporto e resistenza possono essere testati non più di due o tre volte prima di essere rotti definitivamente.

In questa dinamica che abbiamo appena descritto ci sono due momenti rilevanti per l'attività di un trader, quando il prezzo si trova in prossimità di quei livelli di prezzo che abbiamo chiamato supporti e resistenze e quando il prezzo infrange questi livelli. Posto che oggi esistono strumenti finanziari che consentono di fare profitto anche quando il prezzo sta calando (vendita allo scoperto), sarebbe preferibile che un trader alle prime armi si concentrasse a fare operazioni tutte al rialzo per poi successivamente, solo dopo essersi fatto una discreta esperienza, integrare anche strumenti più evoluti nella propria operatività.

Il nostro criptotrader neofita, quindi, che desidera realizzare profitto con le variazioni al rialzo del prezzo ha due momenti ideali per aprire una posizione e precisamente quando il prezzo si trova in prossimità di un supporto e quando il prezzo rompe una resistenza; aprire una posizione contando sul rimbalzo in prossimità del supporto è una strategia che permette spesso di fare profitto ma che presenta maggiori rischi dal momento che non è detto che il supporto regga, aprire invece la posizione nel momento in cui viene rotta al rialzo la resistenza è una strategia di trading più moderata, che ci permette di correre meno rischi e che quindi, inevitabilmente, ci offre opportunità di profitto inferiori.

La verità è che in ogni caso, nonostante quanto sia sofisticata la nostra capacità di analisi del mercato, nessuno può realmente predire dove il prezzo sta andando; questo è vero sempre, ancora di più è vero in un mercato come quello delle criptovalute soggetto a continue manipolazioni. Essendo infatti il mercato delle criptovalute (soprattutto per alcune monete) poco liquido alcuni operatori con grandi

capacità finanziarie sono nella posizione di poter provocare manovre speculative che vengono definite in gergo “pump and dump”, accumulano cioè per settimane grandi quantità di monete a un certo prezzo e poi, iniettando enormi volumi di liquidità improvvisamente, favoriscono un rialzo dei prezzi che gli permetterà, successivamente, di rivendere ad altri operatori quanto precedentemente accumulato a un prezzo più basso.

Completata la manovra speculativa e rifilato, dolorosamente, il pacco a tutti gli operatori che si erano fiondati a inseguire quell’improvviso rialzo, il prezzo della moneta, al mancare della liquidità che ne aveva permesso il rialzo, torna a piombare giù (insieme con l’umore degli operatori caduti vittime della manovra speculativa).

Tra le regole che ci si dovrebbe dare quando si fa trading di criptovalute, quindi, abbiamo quella di non operare su coppie illiquide (che generino cioè un volume di scambi inferiore a un minimo che comunemente viene stabilito intorno ai 20BTC al giorno) e quella di investire (solo quel che si è disposti a perdere) sempre su progetti che si conoscono bene e in cui si nutre grande fiducia (per cui tocca studiare le varie piattaforme, realizzare la propria analisi fondamentale e scegliere accuratamente su quali si vuole operare). In ogni caso, prima di passare oltre, usiamo una semplice immagine per fissare quanto abbiamo appena detto; nel grafico a seguire, quindi, vediamo chiaramente che il prezzo si muove all’interno di un “canale” delimitato da due rette che uniscono rispettivamente i picchi minimi (la linea rossa, prende il nome di supporto) e i picchi massimi (la linea nera, prende il nome di resistenza).

Quando a un certo punto il prezzo mostra un primo segnale di debolezza e non si mostra capace di andare a testare nuovamente la resistenza (retta nera) ecco che tenta di rifiatare per qualche tempo in prossimità del supporto; a questo punto assistiamo a un ultimo tentativo di sortita rialzista, poi il prezzo cede di colpo, rompe il livello (già testato diverse volte precedentemente) oltrepassa la retta rossa (il supporto) ed entra in un ciclo marcatamente ribassista nel quale ad ogni nuovo minimo ne segue uno sempre più basso del precedente.

10.4 RELATIVE STRENGTH INDEX (RSI)

Abbiamo detto che ogni trader utilizza, nella sua operatività di ogni giorno, una serie di strumenti che lo aiutano ad analizzare il grafico che sta leggendo; questi strumenti possono essere divisi in due grandi categorie, gli indicatori (che replicano liberamente l'andamento del prezzo sul grafico) e gli oscillatori (che si muovono in un range di valori definito come, ad esempio, quello tra zero e cento). Questi strumenti (tanto gli indicatori quanto gli oscillatori) ci forniscono segnali spesso molto chiari di quello che sta succedendo al prezzo e la loro corretta interpretazione è ciò che fa la differenza tra perdita e profitto; occorre però sempre ricordare che non esistono indicazioni sicure al 100% e che ogni operazione che facciamo sul mercato può potenzialmente finire in perdita (indipendentemente da quanto possa essere ben fatta la nostra analisi).

I segnali di trading, però, non li ricaviamo solo dalla lettura dei dati che ricaviamo dagli indicatori e dagli oscillatori, ma anche direttamente attraverso il grafico del prezzo tracciando noi stessi dei livelli che rappresentano i "supporti" e le "resistenze". Dal momento che per ogni coppia di valute su cui operiamo possiamo modificare l'unità di tempo (rappresentata graficamente dalle candele) abbiamo una molteplicità di segnali differenti a seconda di come settiamo il time frame (così tecnicamente viene chiamata l'unità di tempo espressa graficamente dalla candela). Se per esempio stiamo operando sulla coppia BTC-ETH (cioè compriamo ETH spendendo BTC), i segnali di trading che ricaveremo osservando il grafico settato con un time frame (spesso indicato anche con la sigla TF) di un'ora saranno diversi dai segnali che ricaveremo osservando un grafico con un TF di quattro ore, e così via per i TF superiori (1D cioè un giorno, 1W una settimana, 1M un mese).

Indipendentemente dalla modalità che usiamo per ricavare il segnale di trading intanto dobbiamo sempre partire dal presupposto che il segnale è tanto più solido quanto più è settato in maniera amplia il TF; un grafico con un time frame di una settimana, quindi, offre segnali più solidi di quelli offerti da un grafico con un time frame di un'ora.

Se volessi comprare ETH spendendo BTC quello che farei sarebbe attendere un momento in cui sul grafico 1W si palesa un segnale di trading, iniziare ad osservare il TF inferiore, quello su base giornaliera in attesa di trovare segnali favorevoli all'acquisto anche su questo TF per poi ridurre ulteriormente la finestra temporale a un TF di 4 ore per cercare il punto esatto in cui aprire la mia posizione. Per ridurre il rischio, quindi, non ci basiamo mai su un singolo segnale di trading ma andiamo in cerca di quella che viene chiamata "convergenza" dei segnali; se è vero, come si dice, che "molti indizi non fanno una prova" è anche vero che tanti più indizi si hanno tanto più alte saranno le possibilità di vincere la nostra scommessa. Perché in un certo senso è questo che stiamo facendo, stiamo scommettendo sul fatto che il prezzo si alzerà; tra tutti gli strumenti utilizzati dai trader, quindi, ce n'è uno che sia semplice da comprendere e che sia comunemente usato ed apprezzato dalla maggior parte della comunità? Si, si chiama RSI, acronimo inglese di relative strength index (indice di forza relativa, in italiano).

Si tratta di un oscillatore che si muove continuamente tra un minimo (pari a zero) e un massimo (pari a 100) inventato da John Welles Wilder (che ne illustrò il funzionamento al pubblico nel 1979 col libro "New Concepts in Technical Trading System") e il cui scopo è di aiutare il trader a identificare i punti in cui la forza del trend si sta esaurendo; la formula matematica ci aiuterebbe a

comprendere il perché dall'RSI si ricavino certe indicazioni, in ogni caso questo non cambia l'operatività, per cui, senza complicare troppo le cose, limitiamoci a dire che l'RSI, muovendosi tra un minimo di zero e un massimo di cento, arriva a toccare due fasce in cui l'attenzione del trader aumenta, la fascia 0-30 (che viene definita di ipervenduto) e la fascia 70-100 (che viene invece definita di ipercomprato).

Quando l'RSI attraversa le fasce di ipervenduto e ipercomprato significa che il mercato è in una fase di "eccesso" in cui gli operatori stanno sostanzialmente ostinandosi rispettivamente a vendere e a comprare oltre il ragionevole (siamo cioè in prossimità di una correzione del prezzo in direzione contraria a quella della tendenza principale). Purtroppo per fare profitto non basta precipitarsi a comprare nelle fasce di ipervenduto e vendere nelle fasce di ipercomprato, in base alla forza della tendenza in corso, infatti, l'RSI può rimanere in condizioni "estreme" (di ipervenduto o ipercomprato) per periodi di tempo anche molto lunghi.

Ci sono particolari momenti, però, in cui sull'RSI si producono delle anomalie se paragoniamo l'andamento dell'oscillatore rispetto a quello che leggiamo sul grafico del prezzo. Quando ad esempio vediamo il prezzo segnare un minimo a 20$, risalire fino a 23$, per poi tornare a segnare un nuovo minimo a 17$ quello che leggiamo chiaramente sul grafico del prezzo è che unendo i due minimi ricaviamo una retta discendente (che si muove verso il basso); in certe circostanze, però, succede che in concomitanza dei due minimi sul grafico del prezzo l'RSI segni due picchi che, una volta uniti, formano una retta ascendente (che si muove verso l'alto).

Questo genere di anomalia viene definita "divergenza" e si forma non solo sull'RSI ma anche su altri tipi di oscillatori e indicatori (sempre con la stessa modalità); esistono fondamentalmente due tipi di divergenze, quelle rialziste (che si leggono tracciando una retta che unisce i picchi minimi) e quelle ribassiste (che al contrario si leggono tracciando una rete che unisce i picchi massimi).

Qualunque tipo di divergenza dovessimo notare tra quanto letto sul grafico del prezzo e quanto espresso dall'oscillatore (vale per l'RSI in questo caso ma è la stessa cosa per quasi tutti gli strumenti) ci da un segnale di trading, in particolare se in un mercato rialzista notiamo una divergenza nei picchi massimi abbiamo un segnale di vendita (c'è quindi la possibilità di un'inversione del trend), se invece si produce unendo i picchi minimi abbiamo un segnale d'acquisto.

Più tecnicamente dovremmo distinguere poi le divergenze propriamente dette (due picchi crescenti nella direzione del trend sul grafico del prezzo in concomitanza di due picchi in direzione contraria a quella del trend tracciati dall'oscillatore) da quelle nascoste (in cui la logica è invertita per cui i picchi espressi dal prezzo sono in direzione contraria a quella del trend, mentre l'oscillatore si comporta in maniera inversa); nel grafico seguente, però, andremo ad analizzare solo le divergenze classiche, mentre delle divergenze nascoste ci occuperemo meglio nel paragrafo dedicato al MACD. L'RSI, in linea di massima, ci offre i migliori segnali di trading attraverso le divergenze che si realizzano in prossimità delle fasce di ipervenduto ed ipercomprato; tali segnali sono più solidi quando emergono su TF maggiori (ad esempio 1D e 1W, un giorno e una settimana) e vanno analizzati comunque sempre in relazione agli altri segnali che raccogliamo.

Una divergenza rialzista, ad esempio, costruita su un grafico con un TF di una settimana, in una situazione di forte ipervenduto e in prossimità di un supporto solido è quasi sempre un buon momento per aprire una posizione long (in pratica acquistare le nostre monete per poi rivenderle a un prezzo più alto); più segnali abbiamo che ci spingono all'acquisto più naturalmente saremo predisposti ad aprire una posizione. In ogni caso, per semplificare tutto questo ragionamento, qui di seguito illustriamo graficamente il funzionamento di due classiche divergenze (la prima rialzista e la seconda ribassista); quello che vediamo nel riquadro verde è che il prezzo sul grafico segna tre

nuovi minimi consecutivi mentre invece l'RSI in corrispondenza di quei minimi è crescente (tutto questo è espresso graficamente dalla linea rossa).

Appena il prezzo (e la stessa cosa succede contestualmente all'RSI) rompe la resistenza inizia a crescere e subisce un rialzo di poco superiore (ad occhio e croce) al 30%; subito dopo, però, nel riquadro nero, notiamo che si viene a formare una divergenza ribassista, sul grafico il prezzo segna due nuovi massimi ma la retta che unisce i rispettivi picchi sull'RSI (anche in questo caso evidenziata in rosso) è chiaramente discendente.

Questa volta ad essere rotto è il supporto e il prezzo inizia a scendere. Nell'operatività di un trader, quindi, i cerchi arancioni rappresentano il momento in cui sarebbe stato consigliabile aprire la posizione (i primi due) e chiuderla (gli ultimi due) per ottimizzare il profitto e ridurre gli eventuali rischi; non sempre questo tipo di strategia si mostra infallibile per cui lavorando esclusivamente con le divergenze prodotte dall'RSI finiremo inevitabilmente col cacciarci anche in qualche brutta situazione.

10.5 MEDIE MOBILI

Quello che dobbiamo sempre avere in mente quando facciamo trading è che ogni grafico ci offre segnali di ogni tipo (sia rialzisti che ribassisti, sia di inversione che di continuazione del trend) e sta a noi interpretarli correttamente facendo di volta in volta le diverse valutazioni del caso; quando raccogliamo un segnale usando l'RSI non dovremmo accontentarci di questo ma dovremmo andare in cerca di conferme usando strumenti differenti per assicurarci che anche questi ci forniscano indicazioni positive.

Tra gli strumenti più utili e insieme più semplici da integrare nell'operatività di ogni giorno abbiamo le medie mobili; questi strumenti non fanno altro che ridurre l'effetto derivante da picchi casuali esprimendo l'andamento del prezzo sul grafico sotto forma di una curva.

Esistono diversi tipi di medie mobili, quelle più comunemente usate prendono il nome di media mobile semplice (anche chiamata SMA o aritmetica) che assegna la stessa rilevanza a tutti i valori che il prezzo assume indipendentemente dal fatto che siano più o meno recenti, media mobile ponderata (WMA) che risolve il limite della SMA assegnando una maggior rilevanza alle candele più

recenti, media mobile esponenziale (EMA) che assegna un valore esponenzialmente crescete ai valori di prezzo più recenti e media mobile adattiva, che introduce l'analisi dei volumi nel calcolo necessario a produrre la curva che esprime l'andamento dei prezzi. Indipendentemente dal tipo di media mobile la curva che verrà rappresentata dal grafico avrà sembianze differenti a seconda del "periodo" che avremo settato; una media mobile a 12 periodi, ad esempio, indica che ogni punto tracciato dalla curva rappresenta la media delle ultime 12 candele.

Le medie mobili vengono quindi definite "veloci" e "lente" al crescere del periodo di riferimento; in questo modo una media mobile a 12 periodi (basata cioè sui prezzi delle ultime 12 candele) viene considerata una media mobile veloce e una a 26 periodi (basta sulle ultime 26 candele) viene considerata lenta.

Le medie mobili sono importanti proprio perché possiamo creare più medie mobili con diversi periodi ricevendone diverse indicazioni; in linea di massima i periodi più comunemente usati nell'analisi tecnica per tracciare le medie mobili sono 20-50-100 soprattutto per quel che riguarda la media mobile esponenziale (che è quella che normalmente i trader adoperano di più). Questi strumenti ci offrono un colpo d'occhio sul mercato rapido ed immediato, quando il prezzo si trova sopra una media mobile il trend è ad esempio considerato rialzista (al contrario se si trova sotto è considerato ribassista); si considera inoltre la tendenza tanto più marcata quanto più alto è il periodo della media mobile sopra la quale il prezzo staziona.

Questo perché le medie mobili rappresentano anche valori di supporti e resistenze, tanto più solidi quanto maggiore è il periodo usato per costruire la media mobile stessa; un'altra indicazione molto utile che le medie mobili ci danno è il modo in cui si intrecciano tra loro, che ci dice molto sul futuro andamento del trend. Normalmente quando una media mobile più veloce taglia al rialzo una media mobile più lenta quello è il momento di comprare; quando invece, al contrario, la taglia al ribasso quello è il momento di vendere.

Proviamo a osservare tutto quello che abbiamo detto su un grafico (precisamente un grafico 1D della coppia BTC/XRP), qui abbiamo tracciato tre medie mobili esponenziali a 20 periodi (curva rossa), 50 periodi (curva azzurra) e 100 periodi (curva nera) ed evidenziato (in verde e in nero) due particolari momenti nella storia dell'andamento del prezzo. Andiamo a guardare il primo rettangolo verde, qui ad un certo punto vediamo distintamente la media mobile veloce (quella a 20 periodi, colorata di rosso) tagliare al rialzo le due medie mobili più lente; il prezzo subito dopo torna giù, usa una delle medie mobili più lente come supporto ed entra in un ciclo marcatamente rialzista. Nel secondo riquadro verde assistiamo alla stessa dinamica col prezzo che prima segna un grosso rialzo e successivamente sfrutta la media mobile più lenta come supporto e torna a testare la stessa resistenza che aveva testato col primo rialzo; lo sviluppo della situazione che vediamo dispiegarsi nel riquadro verde è che o il prezzo romperà la resistenza di breve periodo (line arancione) per andare quindi a testare nuovamente quella di lungo periodo (linea gialla) oppure romperà i tre supporti rappresentati dalle tre medie mobili e ripiomberà nella zona dell'ultimo minimo (linea viola) dove con ogni probabilità o tenterà un rimbalzo o inizierà a costruire una divergenza.

Nei riquadri neri osserviamo la stessa dinamica, ma al contrario; nel primo riquadro nero possiamo osservare come la media mobile veloce tagli al ribasso una dopo l'altra le due medie mobili più lente

col prezzo che una volta transitatole sotto inizierà a testare la EMA100 (media mobile esponenziale a 100 periodi, la curva nera nel nostro grafico) esattamente come se fosse una resistenza.

Nel secondo riquadro nero lo stesso scenario si ripete ma con minore vigore, il prezzo sembra infatti tentare di raccogliersi intorno alle medie mobili ma alla fine il ciclo ribassista prevale e il prezzo tocca il suo picco minimo; le medie mobili in generale e quelle esponenziali in particolare sono estremamente utili nell'operatività dei trader e se integrate all'interno di una strategia più amplia ci forniscono indicazioni importanti sul possibile andamento futuro del prezzo.

10.6 MACD

Nei paragrafi precedenti abbiamo iniziato a introdurre l'uso di strumenti che non dovrebbero mai mancare nella cassetta degli attrezzi di un trader; in questa piccola carrellata non poteva quindi mancare il MACD (acronimo di "Moving Average Convergence/Divergence").

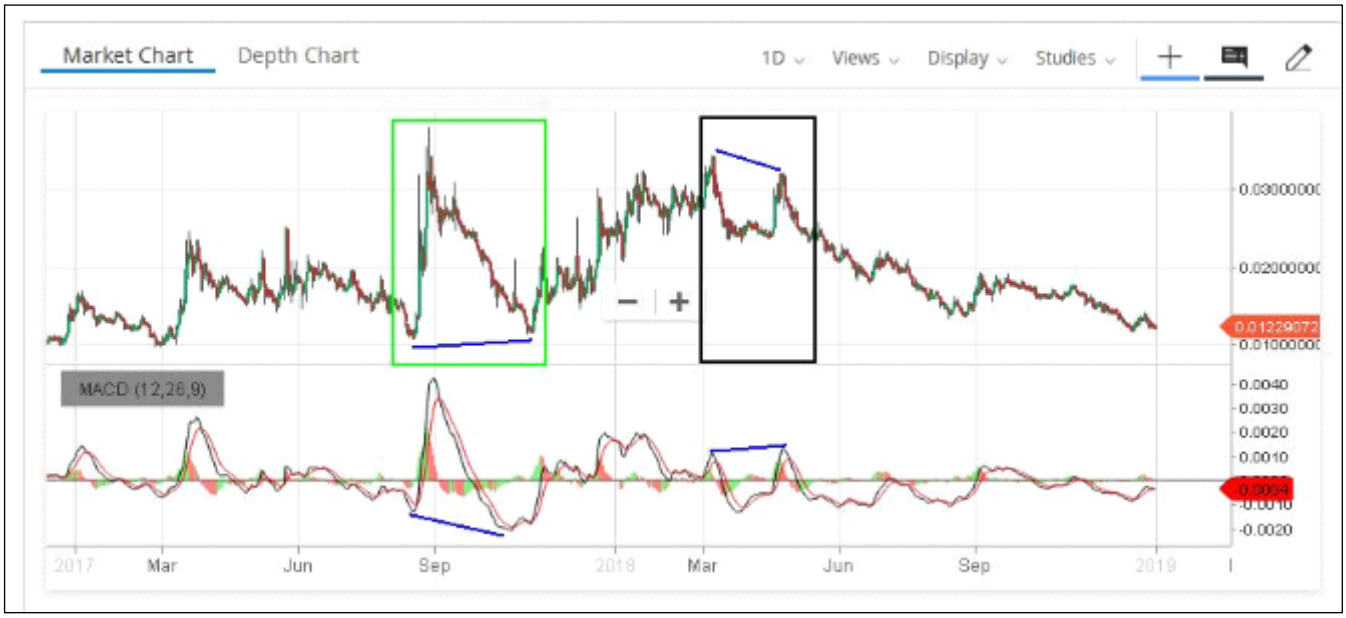
Parliamo di un indicatore considerato estremamente utile da tantissimi trader, che infatti lo integrano abitualmente nella loro operatività, costruito sostanzialmente sulla base dei dati estratti da tre diverse medie mobili esponenziali (a 9, 12 e 26 periodi); uno dei principali usi del MACD è di rintracciare le divergenze. Dal momento che nel paragrafo dedicato all'RSI ci siamo occupati delle divergenze classiche in questo paragrafo ci occuperemo specificatamente di quel particolare tipo di divergenze che vengono definite "nascoste"; la dinamica con cui la divergenza viene costruita è la stessa che abbiamo visto in precedenza, per cui anche questa volta unendo con una retta i picchi massimi (o minimi) tracciati sul grafico del prezzo noteremo delle anomalie (le divergenze appunto) rispetto a quanto notiamo tracciando delle rette che uniscono invece i picchi costruiti dal MACD. Il MACD ci è utile perché ci permette di ricavare più informazioni sulla solidità del segnale di trading, quando infatti notiamo la stessa divergenza sia sull'RSI che sul MACD questa è da intendersi come una prova aggiuntiva della validità del segnale; il MACD ci fornisce poi un altro spunto interessante, essendo infatti graficamente rappresentato dall'andamento di due curve che sono sostanzialmente due differenti medie mobili esponenziali (ema) normalmente evidenziate coi colori blu o nero (per la media mobile più lenta, a 26 periodi) e col colore rosso (per la media mobile più veloce, a 12 periodi), ci permette di ricavare dei segnali di trading sulla base degli incroci tra le due curve.

Quando quindi la media mobile più veloce taglia al rialzo quella più lenta abbiamo un segnale rialzista, al contrario quando invece la media mobile più lenta viene taglia al ribasso da quella più veloce abbiamo un segnale ribassista. In ogni caso, come abbiamo fatto negli altri paragrafi, utilizziamo un'immagine per fissare i concetti principali.

Questa volta abbiamo scattato due fotografie del mercato, evidenziandole con dei rettangoli (di colore verde e nero); nel primo caso (rettangolo verde) vediamo una tipica divergenza rialzista di tipo nascosto, nel secondo caso (rettangolo nero) vediamo sempre una tipica divergenza nascosta, ma questa volta ribassista.

Come possiamo vedere la dinamica è identica a quella che abbiamo descritto nel paragrafo sull'RSI, ma questa volta nel triangolo verde vediamo che non viene segnato un nuovo minimo e che il picco si ferma a un prezzo di poco più alto rispetto a quello raggiunto nel minimo precedente tanto che la linea che unisce i due picchi (colorata di blu) risulta essere ascendente (diretta quindi verso l'alto); troviamo la nostra bella divergenza nascosta unendo i minimi costruiti dal MACD e ricavandone una nuova retta (anche questa tracciata in blu) che si muove invece nella direzione opposta (discendente). L'esito finale, indipendentemente dal fatto che la divergenza sia nascosta o no, è lo stesso, il prezzo inizia a salire e va a testare nuovamente il picco massimo raggiunto in precedenza.

Nel rettangolo nero invece assistiamo a uno scenario ribassista, anche questa volta il secondo picco non riesce a superare quello precedente, ma si ferma un poco prima, tanto che la retta (sempre blu) che tracciamo unendo i due picchi è discendente (tende cioè verso il basso); sul MACD troviamo la nostra divergenza nascosta, unendo i picchi massimi, infatti la nostra solita retta blu questa volta è ascendente (si muove quindi in direzione contraria alla retta che unisce i picchi sul grafico dei prezzi, dal momento che punta verso l'alto).



10.7 ICHIMOKU CLOUD

Gli strumenti che abbiamo descritto fino adesso sarebbero da soli già sufficienti a realizzare una strategia di trading vincente; associando le informazioni che ricaviamo con i supporti e le resistenze a quelle ricavate da medie mobili, MACD ed RSI saremmo già quindi, in linea puramente teorica, capaci di fare trading in maniera profittevole.

Il risultato finale, infatti, non dipende da quanto sono evoluti gli strumenti di cui ci dotiamo, ma da quanto sono ferree le regole di cui ci dotiamo; prima di descrivere un nuovo strumento, tanto utile

quanto semplice nel momento in cui lo si impara ad usare, fermiamoci un attimo a riepilogare alcune delle regole che abbiamo visto e stabiliamone di nuove. Per prima cosa, come abbiamo già spiegato, non si fa trading con importi superiori a quanto si è disposti a perdere; abbiamo anche detto che non dovremmo mai operare su coppie poco liquide (in cui volume di scambi, a titolo orientativo, non supera i 30BTC al giorno) e che dobbiamo sempre investire su progetti che conosciamo e nei quali riponiamo grande fiducia.

Alcune delle regole più importanti da seguire riguardano il momento in cui chiudere l'operazione, può capitare, per fare un esempio, che durante un trade il prezzo rompa un supporto importante e inizi a precipitare molto velocemente a causa di una sorta di effetto panico che travolge gli investitori; molti trader, per far fronte a questa circostanza, si pongono una regola semplice, che consiste nel non vendere mai durante i dump.

Vendere quando tutti stanno vendendo, in altre parole, raramente si rivela essere una buona idea e, il più delle volte, aspettare che il prezzo rimbalzi ci permette di uscire dal trade con perdite inferiori (o addirittura con un piccolo profitto); questo ci porta a una nuova regola che potrà anche sembrare banale ma che consiste essenzialmente nel vendere quando è il caso di vendere. Ci sono momenti in cui il prezzo dimostra chiaramente di essere intenzionato ad andare giù anche pesantemente, in quei momenti un trader furbo accetta di chiudere la posizione con una perdita modesta invece che intestardirsi in un trade che con ogni probabilità inizierà a metterlo presto sotto grande pressione, generando perdite che possono arrivare a percentuali anche importanti prima che la naturale oscillazione del prezzo offra un nuovo punto accettabile di uscita e incastrando il nostro povero trader in un'operazione che può avere una durata di tempo molto più lunga del previsto.

Quando apriamo una nuova operazione (e questa è un'altra buona regola da seguire) dovremmo già avere in testa un'idea abbastanza chiara del prezzo a cui speriamo di vendere e dell'entità massima di perdite che siamo disposti a tollerare se le cose dovessero andare male; questa semplice norma di comportamento ci permette di mettere un freno alle perdite quando le cose vanno male e di consolidare i profitti quando le cose vanno bene. Al netto di queste piccole nozioni, comunque sempre di grande utilità, introduciamo un nuovo strumento che, nonostante in un primo momento possa apparire un po' caotico, ci permette in verità di interpretare molto facilmente e molto velocemente cosa sta succedendo sul mercato; si tratta di un indicatore di slancio che prende il nome di "Ichimoku cloud" letteralmente "nuvole di ichimoku", creato dal giornalista giapponese Goichi Hosoda. Quando un trader che non ne ha mai sentito parlare si trova per la prima volta ad osservare le famose nuvole di Ichimoku normalmente prova una forte sensazione di spaesamento; come possiamo vedere dall'immagine sottostante, infatti, il grafico risulta pieno di segni che occorrerà interpretare nella giusta maniera.

Basterà però molto semplicemente descrivere quello che vediamo nel grafico sottostante per comprendere quanto semplice sia l'uso concreto di questo stupendo indicatore; la prima cosa che notiamo sono quelle aree colorate di verde e di rosso, che sono quelle che vengono appunto denominate "kumo" (o nuvole, in italiano). Il perimetro di queste nuvole è delimitato da delle linee (rappresentate graficamente con un colore più scuro) che prendono il nome di Senkou Span A e Senkou Span B. Possiamo considerare entrambe le Senkou Span (sia la A che la B) come due medie

mobili rispettivamente a 17 periodi (Senkou Span A) e a 52 periodi (Senkou Span B) entrambe proiettate nel futuro di 26 periodi. Sul grafico, poi, distinguiamo ancora due linee, questa volta esterne alle nuvole, evidenziate dal colore rosso e dal colore blu, che rappresentano ancora una volta una coppia di medie mobili; la media mobile più veloce (a 9 periodi) è evidenziata in blu e prende il nome di Tenkan-sen, mentre la media mobile più lenta (a 26 periodi) è evidenziata in rosso e prende il nome di Kijun-sen.

Notiamo poi un'ultima linea di colore più scuro, che replica fedelmente l'andamento del prezzo ma che è posizionata di 26 periodi indietro, che prende il nome di Chikou-span (o linea di ritardo). Questo tipo di indicatore ci fornisce molte indicazioni utili per il trading e soprattutto ci permette di definire con un colpo d'occhio se il prezzo si trova in un trend rialzista o ribassista a seconda che stazioni al di sotto o al di sopra delle nuvole; altre indicazioni ci sono poi fornite dai vari incroci delle diverse medie mobili e dalla posizione della linea di ritardo rispetto alle nuvole che rappresenta un segnale abbastanza attendibile sulla forza del trend in corso.

Come abbiamo già visto, quindi, i momenti migliori per aprire una posizione sono quando le medie mobili più veloci tagliano al rialzo le medie mobili più lente, mentre la posizione della linea di ritardo rispetto alla nuvola viene considerata un segnale di forza che può essere sia rialzista (quando la linea di ritardo fa capolino oltre la nuvola) che ribassista (quando la linea di ritardo ha ormai attraversato al ribasso tutto lo spessore della nuvola emergendo dal lato opposto).

10.8 PARABOLIC SAR

Selezionare tra tutti gli strumenti che un trader ha a propria disposizione un piccolo gruppo ristretto di tool da presentare a chi è completamente digiuno di trading non è una decisione facile da prendere; la mia stessa "cassetta degli attrezzi", per intenderci, include molti altri strumenti oltre a quelli di cui ho avuto modo di parlare come ad esempio i livelli di Fibonacci, i punti Pivot, le bande Fractal Chaos e quelle di Bollinger, l'Elder Ray Index, il Klinger Volume Oscillator e l'On Balance Volume, gli oscillatori stocastici e ancora molti altri. Purtroppo se dedicassimo un paragrafo ad ognuno degli strumenti che un trader può impiegare con profitto per sviluppare la sua strategia questo diventerebbe un testo sul trading, cosa che invece non è; dal momento che ci rimane un ultimo paragrafo da dedicare all'analisi tecnica ho deciso di parlare di uno strumento che si distingue per il rapporto tra semplicità d'uso ed efficacia, il Parabolic SAR (acronimo di "Stop And Reversal").

Molto semplicemente questo indicatore, sviluppato da Welles Wilder, ci permette di comprendere quando un trend è destinato a interrompersi; come vediamo dall'immagine questo strumento viene rappresentato graficamente come una serie di punti che si posiziona sotto la linea del prezzo quando il trend è rialzista e sopra la linea del prezzo quando il trend è ribassista. Una strategia di trading che integri correttamente il Parabolic SAR consiste nell'usare altri strumenti per definire quando siamo in prossimità di un'inversione di un trend ribassista usando il Parabolic SAR come strumento per definire il momento dell'uscita.

Normalmente, quindi, apriremo la nostra posizione quando il Parabolic SAR si trova ancora sopra la linea del prezzo per poi successivamente vederlo diventare rialzista; nel momento in cui il Parabolic SAR tornasse a posizionarsi sopra la linea del prezzo a quel punto avremo il segnale di vendita che aspettavamo. Nell'immagine seguente possiamo facilmente notare come un uso oculato del Parabolic SAR ci permetta di massimizzare il nostro profitto; dal grafico notiamo che, nel rettangolo evidenziato in verde, il prezzo ha piazzato due picchi massimi consecutivi (infatti la retta rossa che li unisce è ascendente) mentre l'RSI ha formato due picchi in direzione opposta all'andamento del trend (infatti la linea rossa che li unisce è discendente).

Basandoci solo sull'uso dell'RSI, quindi, notando la formazione di una classica divergenza ribassista saremmo andati a piazzare la nostra vendita in una fascia di prezzo prossima a quella evidenziata dal rettangolo blu. Se invece avessimo aspettato ancora che il Parabolic SAR diventasse ribassista avremmo venduto circa otto giorni dopo ma a un prezzo che questa volta sarebbe stato compreso all'interno della fascia evidenziata dal rettangolo rosso.

Considerando che tra il punto più basso del rettangolo blu e quello più alto del rettangolo rosso c'è una variazione di prezzo che si aggira intorno al 30% capiamo bene come utilizzare il Parabolic SAR in maniera razionale ci permetta di aumentare anche sensibilmente il nostro margine di profitto. In questo modo iniziamo a capire che non necessariamente dobbiamo stabilire prima il prezzo di vendita ma possiamo anche seguire l'andamento del trend, a patto di avere comunque sempre una strategia che ci permetta di definire il momento giusto per chiudere l'operazione.

Con questo cogliamo quindi l'occasione per buttare li un paio di altre regole preziose; in primo luogo, quindi, la regola che impone di prendere profitto. Se non chiudi mai l'operazione e continui a restare long in attesa di mettere a segno il colpo che ti permetterà di decuplicare il tuo capitale potresti dover aspettare molto a lungo, forse anche per sempre.

Indipendentemente dallo stile di trading che usi, quindi, anche se sei un cassettista e le tue operazioni possono facilmente arrivare a durare mesi, prima o poi arriva comunque il momento in cui se vuoi consolidare il profitto devi vendere; se non vendi mai non incassi mai, sembra facile eppure a tanta gente sfugge. Un'altra regola banale ma non per questo meno importante da seguire è che non si può fare trading in continuazione; già fare qualunque lavoro senza staccare mai non è esattamente una scelta salutare, fare una cosa del genere quando si parla di trading significa semplicemente decidere di volersi auto-consumare.

Come abbiamo avuto modo di ripetere spesso, infatti, il trading è un'attività che ci sottopone a una costante pressione psicologica e se vogliamo fare profitto dobbiamo fare in modo che questa pressione sia tollerabile o lo stress ci indurrà a fare un sacco di errori; per capire quanto questo sia vero basterà analizzare la risposta psicologica che ogni trader ha alla chiusura di un'operazione.

Soprattutto i trader alle prime armi (che ancora non si sono impegnati a padroneggiare le proprie risposte emotive) quando chiudono un'operazione con profitto si esaltano e si sentono come se avessero scoperto il segreto per trasformare il piombo in oro, quando invece chiudono un'operazione in perdita si deprimono e tendono a perdere sicurezza e autostima; questo tipo di reazioni inducono il trader ad aprire in continuazione sempre nuove operazioni e quello che succede, inevitabilmente in un periodo di tempo abbastanza lungo, è che l'operatore alla fine accumula perdite esorbitanti.

Quello che dobbiamo capire è che il trading non è come giocare d'azzardo, tutte le scelte che facciamo devono essere accuratamente ponderate prima di aprire un'operazione anche perché dopo che l'abbiamo aperta non possiamo più fare nulla che non sperare che la nostra analisi si riveli corretta. Una regola importante da darci, quindi, è di prenderci sempre e comunque delle pause tra un trade e l'altro, indipendentemente dal fatto che abbiamo o meno fatto profitto; in questo modo avremo il tempo di metabolizzare tutta la pressione accumulata, studiare gli errori eventualmente commessi nella nostra operazione e cercarcene una nuova ponderando con la massima calma tutte le variabili del caso.

Personalmente, ma la cosa è molto soggettiva, mi impongo un periodo di stop di almeno due giorni tra la chiusura di un'operazione e l'altra, tuttavia io stesso non sempre rispetto questa regola; ci sono infatti fasi di mercato in cui si è incentivati ad accorciare o allungare il periodo di stop tra le due operazioni, ma la regola di base, in ogni caso, è che bisogna prendersi delle pause perché non è consigliabile, ne utile o ancora meno salutare, fare trading tutti i giorni dalla mattina alla sera.

10.9 L'ANALISI FONDAMENTALE NEL MERCATO DELLE CRIPTOVALUTE

In questo capitolo abbiamo introdotto alcuni strumenti comunemente considerati fondamentali per iniziare a fare trading; abbiamo anche spiegato che di strumenti importanti da saper utilizzare ce ne sono ancora molti altri, che non hanno trovato spazio in questo testo ma che dovrebbero essere comunque studiati se si desidera fare trading seriamente.

In ogni caso abbiamo anche avuto modo di spiegare che una strategia di trading valida, capace cioè di generare profitto quando praticata in maniera scientifica, non deve essere necessariamente estremamente complicata e sofisticata, ma può anche essere invece estremamente semplice a patto che sia fondata su regole ferree. Una strategia di trading quindi non si riduce semplicemente agli strumenti impiegati per l'analisi tecnica ma include anche tutte quelle regole (grandi e piccole, operative e non solo) che il trader si auto impone con lo scopo di gestire nella maniera migliore possibile le pressioni psicologiche che questo tipo di attività comporta; dal momento che prima di chiudere un'operazione con profitto, ad esempio, possiamo trovarci a dover sopportare perdite anche di un certo rilievo (perché magari abbiamo anticipato di poco l'effettiva inversione di un trend) aver messo i nostri soldi su un progetto di cui abbiamo una grande fiducia a livello psicologico diventa una grandissima comodità.

Immaginiamo di aver comprato delle monete di cui in realtà non conosciamo nulla sulla base della semplice analisi tecnica (perché ci piaceva il grafico in altre parole) a un prezzo di 10$ e di ritrovarci ventiquattro ore dopo con le stesse monete che sono scese a 8$, come gestiremmo la perdita? Quello che succederebbe è che il dubbio di aver investito in un progetto morente, inutile o sul solito immancabile pacco diventerebbe un tarlo logorante che ci spingerebbe a vendere, magari nel bel mezzo di un dump, magari al prezzo più basso possibile (col danno maggiore possibile); succede più frequentemente di quanto non si possa immaginare.

Se invece avessimo comprato delle monete che conosciamo bene, avendo analizzato nel minimo dettaglio il progetto su cui abbiamo investito il nostro denaro, allora sopportare un crollo da 10$ a 8$ diventa più facile anche, e forse soprattutto, proprio a livello psicologico. Per quanto un trader possa essere bravo nell'analisi tecnica ed essere dotato di un intuito eccezionale, quindi, senza l'analisi fondamentale diventa difficile fare trading di criptovalute; abbiamo già avuto modo di spiegare che sul mercato azionario l'analisi fondamentale può essere intesa come la raccolta di informazioni attraverso la lettura del bilancio dell'azienda, peccato però che quando parliamo di criptovalute il più delle volte non ci sia proprio nessuna azienda, figuriamoci il bilancio.

Ci sono dei fattori che comunque possiamo (e dobbiamo) prendere in considerazione, come ad esempio la capitalizzazione di mercato, o market cap che dir si voglia; per capitalizzazione di una criptovaluta si intende semplicemente l'importo complessivo che ricaviamo moltiplicando il numero di monete in circolazione per il valore (cioè il prezzo) di quelle monete. Un'altra valutazione che dobbiamo fare in questo senso è poi distinguere la supply massima (21mln di monete, ad esempio, se parliamo di Bitcoin) da quella disponibile (o circolante); ci sono ad oggi 17,455mln di monete in circolazione se parliamo di Bitcoin, a fronte di un numero massimo di monete che potranno mai finire sul mercato pari a 21mln.

La quantità di monete in circolazione, in rapporto col numero massimo di monete che la rete ha preventivato, è uno dei fattori che andiamo ad approfondire quando studiamo una nuova criptovaluta; per una vera e propria analisi fondamentale, in realtà, dovremmo essere capaci di smontare il codice della piattaforma open source e capire come è fatta, come funziona e soprattutto se è ben realizzata. Le persone che hanno le competenze per fare una vera analisi fondamentale di un progetto blockchain, che sanno quindi "smontare" la piattaforma e comprendere come funziona, non sono molte; noi persone comuni, che non disponiamo di grandi competenze informatiche, abbiamo quindi altri modi per tentare di capire se possiamo fidarci oppure no.

Le primissime cose che ogni trader di criptovalute vuole conoscere quando investe i suoi soldi riguardano la comunità (intesa non solo come il numero complessivo di nodi che costruiscono la rete ma anche come il numero di utenti che usano quella criptovaluta o quel token) e l'identità delle persone che si occupano di sviluppare il progetto; quando ci troviamo di fronte a una moneta che

ogni giorno viene spesa da migliaia di persone e che viene processata da una propria blockchain attraverso una rete di nodi sufficientemente numerosa e decentralizzata, siamo già moderatamente sicuri di avere a che fare con del buon materiale di partenza.

Ma ci sono altri particolari che ci interessa conoscere, soprattutto relativamente alla squadra di sviluppatori che si occupa di portare avanti il progetto; ogni criptovaluta, se ci fermiamo a pensarci è il minimo, dovrebbe avere un proprio sito ufficiale e all'interno del sito ufficiale deve necessariamente essere presente una sezione in cui vengono menzionate le figure di primo piano all'interno della comunità. Se alle spalle di un progetto c'è un'azienda allora saranno indicate anche figure come il CEO (quello che in Italia chiameremmo amministratore delegato) e i responsabili dei vari dipartimenti (marketing, legale, sviluppo, etc); questo vale ovviamente anche per le monete che alle spalle hanno, invece che un'azienda, una fondazione senza scopo di lucro.

Se poi invece alle spalle di un progetto non c'è ne un'azienda ne una fondazione comunque sul sito web ci dovrà essere uno straccio di sezione "chi siamo" in cui vengano citati, nella peggiore delle ipotesi, gli sviluppatori. Quello che dobbiamo capire è chi sono le persone maggiormente esposte nel progetto, se sono persone serie, se sono persone affermate, stimate o meno, insomma, più ne riusciamo a sapere meglio è.

Ovviamente anche il progetto guidato da una persona per bene, brillante e capace può finire col naufragare, ed anche le persone "famose" ti possono tirare un pacco, ma in linea di massima la qualità di qualunque progetto è sempre legata a doppio filo con la qualità delle persone che se ne fanno carico. Se abbiamo una rete degna di questo nome, decentralizzata, con migliaia di utenti che ogni giorno spendono quella criptovaluta, un team di sviluppatori conosciuto e stimato a livello internazionale, abbiamo tutta una serie di segnali che sono molto utili per costruire quella fiducia che è indispensabile per fare un investimento.

Tutto questo però non basta, occorre conoscere il progetto in maniera più approfondita, capire come funziona e che tipo di opportunità è capace di offrire; per farlo si inizia dalla lettura di un documento (che prende il nome di "withe paper") che tutti i team diffondo ed aggiornano periodicamente, in cui dovrebbero essere riportate (il condizionale è d'obbligo) tutte le caratteristiche e le peculiarità del progetto e che dovrebbe descrivere minuziosamente il funzionamento della tecnologia.

Posto che in ogni caso i withe paper andrebbero intesi più come depliant pubblicitari che come documenti informativi (del resto nessuno metterebbe mai nero su bianco che il proprio progetto è inutile, non funziona o non ha futuro), dalla loro lettura possiamo comunque ricavare informazioni utili; se una determinata moneta, per fare un esempio, usa un protocollo di consenso che conosco già e del quale non mi fido allora avrà poco senso investire su quella criptovaluta.

Se scopro che l'ambizione di questa nuova moneta su cui voglio investire è semplicemente essere l'ennesimo sistema di pagamento basato su blockchain, probabilmente penserò che ci sono monete più anziane ed affidabili da tenere d'occhio e che non sono interessato ad investire i miei soldi su quella che sembra essere soltanto la milionesima copia di una vera innovazione.

Se ancora, per fare un ultimo esempio, scopro che la piattaforma su cui voglio investire, che sulla carta offre decine di servizi molto interessanti (dalla creazione di nuovi token alla gestione degli

smart contract) è ancora molto indietro rispetto alle altre piattaforme che presidiano lo stesso segmento del mercato allora probabilmente prima di investirci i miei soldi sarò propenso a voler aspettare ancora un po' di tempo. Sulla base di tutte queste informazioni che raccogliamo e delle diverse valutazioni che ogni volta direttamente conseguono da ogni diversa informazione raccolta, sviluppiamo una nostra convinzione in merito a un determinato progetto, definiamo di quali monete ci fidiamo di più e di quali di meno, con quali ci sentiamo a nostro agio ad operare e quali invece preferiamo non trattare.

Delle ottocento e passa criptovalute disponibili sul mercato (senza contare i token), sarà sufficiente isolarne una ventina tra quelle che ci piacciono di più e concentrarci a cercare i nostri segnali di trading solo per quelle venti, ignorando tutte le altre; anche così dobbiamo però capire che l'analisi fondamentale è qualcosa che va portata avanti in maniera quotidiana ed include tutta l'attività di informazione e raccolta delle notizie che dobbiamo fare praticamente ogni giorno.

Dal momento che le news muovono il mercato arrivare prima su una news significa prendere un vantaggio sugli altri trader; per riuscirci ci sono una serie di operazioni molto utili da fare come ad esempio seguire sui social gli account degli sviluppatori, iscriversi alle newsletter ufficiali, al canale telegram, partecipare alle discussioni sui forum dove si incontra la comunità; insomma, qualunque canale possa fornirci una notizia in anticipo rispetto agli altri trader dovrà essere aperto e sondato periodicamente.

Una volta che avremo definito un gruppo di criptovalute delle quali ci fidiamo, studiato i loro grafici, raccolto informazioni sulla tecnologia e sulle persone alla guida del progetto, essendo pronti a intercettare qualunque nuova notizia e possedendo una nostra strategia di trading fatta di regole ben precise che dobbiamo semplicemente limitarci a rispettare, allora (e non prima) saremo in possesso di tutti gli strumenti che ci permettono di fare trading di criptovalute con profitto.

11. PROSPETTIVE DEL MERCATO

Nonostante il recente ciclo ribassista abbia bruciato, nel corso degli ultimi 12 mesi, larga parte dei rialzi avuti dall'intero comparto le prospettive per il mondo delle criptovalute nel 2019 e per gli anni successivi paiono essere decisamente rosee; contrariamente a quanto qualcuno possa sostenere, infatti, ci sono già numerosi casi d'uso per questa tecnologia, i vantaggi per la collettività sono incontestabili e sarebbe semplicemente folle pensare che tutto questo possa ritornare nel cilindro del mago e sparire semplicemente nel nulla così come dal nulla è saltato fuori.

Le stesse banche, per altro, non stanno facendo mistero di voler esplorare le potenzialità offerte dalla blockchain per cui sembra francamente improponibile accogliere anche solo parzialmente il punto di vista dei vari detrattori secondo i quali siamo di fronte a una moda passeggera. Paradossalmente neanche un paio di giorni fa leggevo l'ennesimo articolo su un noto giornale economico a tiratura nazionale in cui l'ennesimo osservatore di turno paragonava per l'ennesima volta le criptovalute alla famosa bolla dei tulipani del 1636; tutto questo appare chiaramente ridicolo e non basta sovrapporre un paio di grafici per tirarsi fuori dall'imbarazzo che fare affermazioni così cialtrone inevitabilmente comporta.

Le bolle, propriamente dette, si formano in un arco di tempo ragionevolmente breve e altrettanto velocemente esplodono per poi non riformarsi più; possiamo notare un comportamento di questo tipo in monete come Bitcoin (o altre, tra quelle a maggiore capitalizzazione del mercato) solo se accettiamo di isolare quanto accaduto negli ultimi 15 mesi e pretendendo di ignorare tutto il resto.

Se il mercato, invece, dovesse dimostrare di essere capace di reagire come avvenuto in passato, non solo le maggiori monete appaiono destinate a recuperare le perdite fin qui accumulate nel corso del 2018 ma sembra addirittura plausibile che possano toccare nuovi massimi storici; quello che dobbiamo veramente chiederci quando decidiamo che potremmo essere interessati a investire in criptovalute è se pensiamo che la tecnologia blockchain possa ricavarsi sempre maggiore spazio nei prossimi anni oppure no. Se ci fermiamo un attimo a pensare a come sarà il mondo tra 10, 15 o 20 anni allora diventa difficile ipotizzare che le tecnologie blockchain e DLT possano semplicemente sparire dalla circolazione; queste innovazioni, infatti, hanno già tutte le caratteristiche necessarie a farci capire che non sono affatto destinate a sparire ma che anzi appare più probabile finiscano con l'imporsi definitivamente in un'ottica di lungo periodo. Se pensiamo ad altre tecnologie del passato che hanno poi finito col rivoluzionare il nostro presente ci rendiamo conto di quanto il tempo giochi un ruolo cruciale quando parliamo di questi argomenti; l'inventore delle stampanti 3D, ad esempio, inizialmente faticò non poco a trovare qualcuno che fosse interessato a quella tecnologia dal momento che sembrava a tutti costare troppo e avere poche applicazioni pratiche.

Oggi, però, le stampanti 3D hanno rivoluzionato largamente il mondo della produzione industriale. Le stesse auto elettriche, per fare ancora un altro esempio, sono state bollate lungamente come uno sfizio per ricchi, comunemente considerate per tanti anni troppo costose e difficili da ricaricare perché potessero diffondersi sul mercato; oggi sono invece additate da tutti come le eredi più plausibili per la mobilità privata nell'immediato futuro.

Tutto questo sembra destinato a ripetersi con le criptovalute, una tecnologia largamente snobbata da tanti "esperti" di turno che però, forse perché in conflitto di interessi, forse per meri limiti

anagrafici, non sembrano capaci di comprendere pienamente la portata rivoluzionaria che una tecnologia come la blockchain si porta dietro. Immancabilmente, quindi, parlando col detrattore di turno, soprattutto di questi tempi, quello che potremo notare è che il nostro caro amico si "attaccherà" letteralmente ai grafici per dimostrare che il calo di prezzo è così importante da decretare automaticamente la morte del mercato; non sentirà ragioni, non accetterà spiegazioni, mostrerà con sicurezza assoluta tutte le caratteristiche più inquietanti del grafico Bitcoin, evidenziando anche il più piccolo segnale ribassista per prendersi la ragione.

Quello che queste persone non hanno capito è che normalmente chi opera con le criptovalute del prezzo in un momento X se ne infischia beatamente; c'è stato un momento, ad esempio, in cui Bitcoin precipitò a 2$ dopo aver toccato quota 32$. Ebbene, sfido chiunque oggi a non desiderare di aver comprato anche solo una decina di monete al prezzo di 32$; certamente chi ha comprato su quel picco ha avuto mesi molto stressanti successivamente, durante i quali ha accumulato perdite dolorose, ma chi ha accettato di giocare la partita in un'ottica di lungo periodo ha avuto modo successivamente di togliersi grandi soddisfazioni.

Il prezzo, quando parliamo di criptovalute, è sempre da considerarsi irrilevante e contingente, non è importante, in altre parole, il prezzo che vediamo oggi ma quello che vedremo tra tre anni. Siccome a fare la differenza con le criptovalute è prima di tutto l'adozione, tutto dipende cioè da quante persone accettano di usare questa tecnologia, la domanda che dovremmo farci prima di ogni altra e se tra cinque anni il numero di persone che utilizzano Bitcoin sarà aumentato o diminuito e la risposta a questa domanda, inevitabilmente, sulla base di quello che abbiamo visto negli ultimi dieci anni, appare chiaramente essere che il numero di utenti è destinato ad aumentare (e neanche poco). Molte delle persone che io stesso conosco, giusto per fare un esempio, potrebbero benissimo iniziare ad usare questa tecnologia nei prossimi dieci anni; faccio anzi fatica a capire perché non la stiano già ora usando.

Tutto questo non significa, ovviamente, che non ci saranno nuovi crolli anche per il futuro e che sia possibile escludere a priori qualche decesso eccellente tra le maggiori criptovalute, con monete che oggi hanno una capitalizzazione importante e che potrebbero invece tra qualche anno, per i più svariati motivi, sparire completamente dal mercato ed estinguersi; ma da qui a pensare che sarà tutto il mercato a sparire ce ne passa. Se guardiamo quindi al numero di utenti quello che capiamo è che la corsa del 2017, che ha fatto volare bitcoin fino a quotazioni da 20.000$, appare quasi essere un piccolo antipasto in considerazione del numero ancora ridotto di persone che usa questa tecnologia e del basso impatto che i capitali così detti "istituzionali" hanno avuto su quel rialzo; quando questa fase si concluderà, quindi, e tornerà ad aumentare (come in un certo senso pare stia già succedendo nelle ultime settimane) l'interesse degli utenti, favorendo conseguentemente l'aumento del numero di utilizzatori di questa tecnologia e l'afflusso di grandi capitali "istituzionali" sul mercato, avremo modo di tornare a vedere le principali monete avere rialzi da capogiro.

Non è quindi, per intenderci, questione di capire se succederà o meno, si tratta solo di capire quando succederà.

11.1 USI POSSIBILI DELLA BLOCKCHAIN E DELLE CRIPTOVALUTE

Personalmente ho avuto modo di intuire sin quasi da subito che con ogni probabilità il termine "criptovaluta" non era il più indicato da utilizzare dal momento che tende a generare confusione nel grande pubblico; oggi come oggi, infatti, è diventato molto complicato togliere dalla testa delle persone che quando parliamo di blockchain non parliamo solo di denaro.

Non è quindi un caso se quando ho provato a dare una definizione di cosa sia una criptovaluta, all'inizio di questo libro, ho scritto che si tratta di "una unità di dati della quale è possibile stabilire

con certezza l'origine, chi ne detiene la proprietà e a cui è possibile attribuire un valore convenzionalmente accettato da chiunque".

Attenzione quindi, perché abbiamo parlato chiaramente non di denaro ma di "unità di dati"; sulla blockchain ci possiamo registrare qualunque cosa, il fatto che oggi si tenda a registrarci principalmente delle transazioni è puramente incidentale. Dal momento che le caratteristiche della blockchain sono di essere immutabile, trasparente, accessibile e rispettosa della privacy degli utenti appare chiaro che una delle prime applicazioni possibili riguarda la digitalizzazione dei sistemi sanitari dei vari paesi; con questa tecnologia, quindi, ogni paziente potrà condividere i propri dati sanitari, mantenendone il controllo, decidendo di condividerli con la comunità scientifica ma sempre in forma anonima.

Ovviamente quei dati, soprattutto in un settore come la sanità, avranno inevitabilmente un valore e quindi non è difficile ipotizzare che possano venire commercializzati usando proprio una criptovaluta per retribuire tutti quegli utenti che dovessero decidere di condividere i propri dati sanitari.

Quello che dobbiamo capire è che in questo sistema la fiducia è tutto e che la fiducia viene garantita dalla rete non solo grazie alle regole imposte dagli algoritmi ma anche grazie al meccanismo stesso della ricompensa che è, a ben vedere, parte integrante di questa tecnologia; dal momento che per costruire la fiducia serve la ricompensa e che è più facile elargire questa ricompensa usando una criptovaluta che valuta FIAT, diventa implicito come non possa esistere blockchain senza ricompensa e, di conseguenza, non possa esserci ricompensa senza una criptovaluta che serva proprio a questo scopo. In ogni caso le applicazioni della blockchain sono tantissime, a livello potenziale, è vanno dalla gestione dei diritti di proprietà alla gestione di un registro dei brevetti, con questa tecnologia si può gestire e monitorare costantemente il pagamento delle imposte, si può gestire la mobilità pubblica usando un token di utilità al posto dei normali biglietti e migliorando così la capacità di analisi dei dati relativi a come gli utenti usano i mezzi pubblici; la blockchain può essere usata per aumentare la fiducia e la sicurezza di filiere come quella alimentare (attraverso la tracciabilità dei prodotti) e quella del farmaco, può essere usata per creare nuovi prodotti finanziari (fintech) o in ambito legale (legaltech).

Insomma, più uno ci pensa più si rende conto che le applicazioni sono potenzialmente infinite; sul piano energetico, ad esempio, uno dei motivi per cui molti paesi non riescono a sfruttare pienamente le risorse rinnovabili è che per farlo bisognerebbe abbandonare le reti di distribuzione così come sono costruite e passare alle smart grid (reti intelligenti) che non sono altro che reti di distribuzione decentralizzate.

Grazie alla sinergia tra blockchain e criptovalute, quindi, diventa finalmente possibile creare delle smart grid a prezzi contenuti, con l'energia prodotta da tutta la rete decentralizzata che viene distribuita dove serve, nelle quantità che serve, messa in rete automaticamente dagli utenti e saldata di volta in volta attraverso uno smart contract creando un vero e proprio mercato decentralizzato dell'energia.

La tecnologia blockchain, inoltre, soddisfa due aspetti che diventeranno sempre più cruciali nei prossimi anni e cioè la domanda crescente di spazio di archiviazione virtuale e di potenza di calcolo; digitalizzare la pubblica amministrazione di tutti i paesi, facendo sparire definitivamente

l'archiviazione cartacea, produrrà una domanda crescente di spazio di archiviazione oltre che costi di gestione che possono essere facilmente ridotti sfruttando una rete decentralizzata di computer.

Chiunque può capire, poi, che man mano che le intelligenze artificiali diventeranno sempre più evolute, sarà necessaria una grande potenza di calcolo per farle funzionare pienamente e questa potenza di calcolo potrebbe essere tranquillamente ceduta dai computer che fanno parte di una rete esattamente come oggi succede col mining.

Salute e trasporto pubblico, gestione della pubblica amministrazione, sistemi di voto, filiera del farmaco ed agroalimentare, sistema finanziario e giuridico, sistemi di comunicazione e chat, sviluppo di nuove tecnologie, tutela della privacy, distribuzione di beni come energia, spazio di archiviazione virtuale e potenza di calcolo, non c'è un solo singolo settore dell'attività umana che non possa trarre giovamento dalla tecnologia blockchain; a chi dovesse chiedere, quindi, quali sono i campi di applicazione di questa innovazione tecnologica l'unica risposta sensata da dare sarebbe "tutti".

Semplicemente in tutti i campi, in ogni aspetto della società umana, in ogni ambito produttivo la tecnologia blockchain avrà modo di irrompere nel prossimo futuro rivoluzionando in maniera radicale il nostro modo di concepire la realtà così come, a suo tempo, ebbe modo di fare la nascita di internet.

11.2 Nascita di un nuovo paradigma

La vera forza della tecnologia blockchain è che produce inevitabilmente un cambio di mentalità epocale in chi la usa; il nuovo modello decentralizzato, infatti, apre le porte a un mondo nuovo, profondamente diverso da quello che conosciamo oggi.

Per tanto tempo, in altre parole, ci è stato detto che la tecnologia, l'automazione industriale, la robotica e le intelligenze artificiali avrebbero distrutto i nostri posti di lavoro, quelli che richiedevano minori qualifiche, quelli che normalmente fanno le persone comuni; beh, da quello che possiamo vedere oggi a essere stati spazzati via dalla tecnologia sono i posti di lavoro di persone che si percepivano intoccabili (politici, banchieri, etc). Il salto di mentalità che questa tecnologia produce è inevitabile, chiunque si ritrovi ad usare Bitcoin a un certo punto non può fare a meno di constatare che se si può gestire una cosa complessa come la moneta in maniera decentralizzata allora si può gestire in questo modo qualunque cosa, inclusi interi paesi.

Per questo motivo, come abbiamo già avuto modo di accennare, appare chiaro a tutti che quando parliamo di blockchain stiamo anzi tutto parlando di politica e soprattutto parliamo di un modello che appare chiaramente di ispirazione anarchica; la tecnologia blockchain, infatti, presuppone l'assenza di un governo centrale, ma non presuppone l'assenza di regole, anzi, è vero l'esatto contrario. Perché possa esserci fiducia in un sistema decentralizzato le regole devono essere ferree e chiare a tutti così come lo sono le regole definite da ogni protocollo di consenso; quello che avviene, semplicemente, è che invece di esserci grandi istituzioni centralizzate (corruttibili per loro stessa natura) a far rispettare le regole abbiamo un sistema di algoritmi basato sulla matematica che è trasparente e incorruttibile.

Chiunque quindi, appena ha modo di studiare anche solo superficialmente questa tecnologia, si rende conto che siamo di fronte a un paradigma completamente nuovo, che contesta radicalmente quello basato sulle grandi istituzioni centralizzate e propone un modello in cui lo stesso ruolo che prima ricoprivano le grandi istituzioni viene adesso ricoperto dagli stessi cittadini in maniera decentralizzata.

Quando ho scoperto l'esistenza di Bitcoin, dopo che ho avuto modo di studiarlo per qualche tempo, ho iniziato a dire che mi sarebbe piaciuto cambiare la costituzione da "l'Italia è una repubblica democratica fondata sul lavoro" a "l'Italia è una repubblica decentralizzata fondata sulla piena occupazione"; sembra una modifica di poco conto, ma implicherebbe un cambiamento radicale nel modo in cui viene gestito questo paese.

Se poi andiamo ad analizzare le caratteristiche principali di una blockchain ci accorgiamo che corrispondono perfettamente alle caratteristiche che deve avere un sistema di voto; la blockchain, infatti, è trasparente (nel senso che chiunque può controllare e verificare i dati che contiene), è immutabile (quando il dato viene quindi registrato non può più essere modificato) ed è anonima (possiamo quindi evitare che si riconduca un indirizzo a una determinata persona fisica). Dal momento però che questo nuovo sistema di voto avrebbe costi sostanzialmente irrisori ecco che già ci troviamo di fronte a un modello più efficiente per gestire la democrazia; e siccome votare con la blockchain costa così poco (non servono scrutinatori, non servono presidenti di seggio, non devi mobilitare le forze dell'ordine per un fine settimana, non consumi carta, matite, etc) nulla ci vieta di arrivare a pensare che un domani potremo esprimere il nostro voto in maniera diretta ed istantanea su qualunque cosa. Quando però ci dovessimo trovare in un modello in cui ogni cittadino può fare una proposta e vederla approvata in breve tempo a seguito di un voto popolare (secondo le regole democratiche) ecco che inevitabilmente inizieremmo a chiederci a cosa possano servirci ancora i governi e gli stessi parlamenti.

Ogni volta che ragioniamo di tecnologia blockchain, se accettiamo di portare il discorso alle logiche estreme conseguenze, finiamo sempre, immancabilmente, con l'immaginare un nuovo modello in cui viene a cessare la necessità delle grandi istituzioni (non solo banche, ma gli stessi governi e persino i parlamenti) e i processi democratici finiscono finalmente pienamente sotto il completo controllo dei cittadini; il fatto che si reputi questo più o meno auspicabile è molto soggettivo, il fatto invece che la tecnologia blockchain ci inviti a pensare a questo nuovo tipo di modello appare sostanzialmente ineccepibile.

Ovviamente oggi non c'è modo di dire come andranno le cose e come evolveranno nel prossimo futuro, ma ci sono alcune cose che possiamo facilmente preventivare sin da oggi, prima tra tutte che non è possibile decidere di sfruttare la tecnologia blockchain senza sdoganare definitivamente anche Bitcoin; il pacchetto, per intenderci, è un all inclusive, per cui o prendi tutto o prendi niente.

Nel momento in cui gli stati iniziassero ad usare assiduamente questa tecnologia starebbero implicitamente e sostanzialmente legittimando l'esistenza di Bitcoin e dei vari metodi di pagamento completamente decentralizzati; quando questo accadrà il risultato sarà che gli stati inizieranno a perdere progressivamente il controllo sulla leva monetaria.

Se immaginiamo poi un contesto in cui i governi e le grandi istituzioni perdono il controllo della leva monetaria immaginare che da lì a breve possano perdere il controllo anche sulla leva politica non diventa così utopistico; in ogni caso, quando tutto questo avverrà, perché appare assolutamente ragionevole che avvenga, saranno i popoli a decidere (si spera liberamente) se reputano di aver ancora bisogno di parlamenti, governi e grandi istituzioni centralizzate o se invece (come io auspico e insieme a me larga parte degli appassionati di criptovalute) preferiranno farne a meno decidendo

che vogliono gestire liberamente e direttamente i rispettivi paesi cambiando quindi radicalmente e per sempre la percezione che oggi abbiamo degli stati.

11.3 I limiti delle criptovalute

Fino adesso abbiamo usato toni molto entusiasti per descrivere il mercato delle criptovalute, non sarebbe stato però corretto omettere di descrivere anche i limiti che questa tecnologia mostra ancora di avere; anche se qualcuno ogni tanto taccia gli appassionati di criptovalute di essere quasi un culto, fondato su dogmi e incapace di vedere i limiti e le criticità che questa tecnologia lascia intravedere, in realtà sono proprio coloro che la blockchain la conoscono che non mancano di evidenziarne gli aspetti più critici.

Gli aspetti più delicati, infatti, emergono subito chiaramente nel momento in cui si affronta in maniera più sistematica lo studio dei protocolli di consenso; nonostante infatti esistano decine di soluzioni differenti il protocollo di consenso perfetto ad oggi ancora non è stato inventato e probabilmente non lo sarà mai. Prendiamo il protocollo POW, ad esempio, che consente il funzionamento di Bitcoin, questo richiede, per funzionare adeguatamente, sempre maggiore potenza di calcolo e sempre maggiore energia; questa dinamica produce un progressivo allontanamento dei piccoli minatori dalla rete BTC che inizia quindi a restringersi a tal punto da lasciare già oggi intravedere un futuro in cui Bitcoin potrebbe apparire sostanzialmente centralizzato.

Se pochi minatori, poi, riuscissero ad arrivare al punto di sviluppare il 51% della potenza di calcolo disponibile sulla rete allora la rete stessa diventerebbe molto meno sicura e sarebbe sostanzialmente nelle mani di un ristretto gruppo di persone; altri protocolli di consenso tentano di bypassare questo problema introducendo regole diverse, ma finendo col produrre poi anche nuove storture. I protocolli POS e DPOS, per fare un esempio, mostrano già chiaramente di prestare il fianco alla nascita di una possibile oligarchia, un modello in cui gli utenti più facoltosi esercitano un maggior potere di voto, con la logica conseguenza che le catene che funzionano utilizzando questi protocolli di consenso difficilmente possono essere percepite come realmente decentralizzate (e se lo sono in questo momento nulla vieta che cessino di esserlo in futuro).

Ad impedire che da questo nuovo modello emerga anche una nuova elite di ultra-ricchi, capace di fare il bello e il cattivo tempo, allo stato attuale delle cose è proprio la grande varietà di progetti in circolazione; se tuttavia questa varietà dovesse iniziare a ridursi negli anni, lasciando emergere un nuovo possibile standard, le cose potrebbero cambiare ed anche rapidamente. Per capire bene di cosa stiamo parlando sarà utile fare un paragone con internet; anche questa tecnologia ci sembrava aprire, in passato, potenzialità infinite ed oggi, a distanza di più di vent'anni, appare chiaro che non tutte le promesse si sono trasformate in realtà.

Una volta, poi, internet era caratterizzata da maggiore varietà, pensiamo ad esempio all'ecosistema dei motori di ricerca, un tempo ne esistevano decine, poi da questa molteplicità è emerso uno standard (rappresentato da Google) e con la nascita di questo nuovo standard è emerso anche quello che oggi appare sostanzialmente essere un monopolio. L'enorme, forse anche eccessiva, influenza che Google e pochi altri colossi esercitano sul web sta rendendo il web un luogo sempre meno libero rispetto a come lo abbiamo conosciuto e percepito alle origini, in cui stiamo progressivamente perdendo il controllo sui nostri dati personali e nel quale sono ormai gli algoritmi (decidendo la disposizione con cui i contenuti vengono presentati) a decidere per conto degli utenti cosa sia opportuno leggere e cosa no. Allo stesso modo la progressiva marginalità delle piattaforme di blogging, schiacciate dallo strapotere di un gruppo ristretto di social network, sta ponendo le basi

perché scompaia il diritto di espressione sul web; se infatti nessuno poteva immaginare di imporre cosa qualcuno potesse scrivere o non scrivere sul suo blog, oggi i grandi social si arrogano il diritto (spesso unilateralmente) non solo di bannare esplicitamente gli utenti (chiudendo i loro account) ma anche di occultarne i contenuti facendoli sparire dai risultati di ricerca (il così detto shadow banning). Tutti questi limiti che sono emersi su internet li abbiamo potuti constatare proprio nel momento in cui la grande varietà di servizi differenti che aveva caratterizzato il web ai suoi albori ha iniziato a ridursi, favorendo la nascita di veri e propri imperi che oggi operano in condizioni di sostanziale monopolio; bisognerebbe essere quindi miopi (e forse anche stupidi) per non arrivare a temere che una dinamica del genere possa emergere anche nell'ambito della tecnologia blockchain.

Diverso invece il discorso per quel che riguarda l'annoso problema della volatilità, se da un lato è infatti certamente vero che monete così volatili non si prestano bene a diventare unità di conto non è difficile immaginare che le valute FIAT possano sopravvivere proprio per svolgere questa funzione; ogni utente, poi, elabora una propria strategia per difendersi dalla volatilità. I trader, ad esempio, sono soliti aprire posizioni short su bitcoin usando il 50% del loro capitale, in questo modo evitano che movimenti improvvisi e violenti del prezzo possano danneggiarli economicamente; immaginiamo ad esempio che io abbia 2BTC e che il prezzo sia attualmente attestato a 10.000$.

In tasca mi trovo quindi 20.000$; quello che farò sarà semplicemente holdare 1BTC e usare il secondo BTC per shortare (cioè vendere allo scoperto). In questo modo se il prezzo salisse del 10% questo profitto verrebbe azzerato dall'operazione short, ma lo stesso varrebbe per le perdite, se il prezzo crollasse del 10% questa perdita sarebbe sanata dall'apertura della posizione allo scoperto. Indipendentemente dalle oscillazioni del prezzo, quindi, il mio saldo finale sarà sempre di 20.000$ (al netto delle commissioni, un costo certo, ma tollerabile per proteggersi dalla volatilità).

Chi poi ha avuto l'opportunità di essere pagato in criptovaluta, a me è successo un paio di volte, capisce bene che ad ogni pagamento sarà necessario fare delle valutazioni relativamente all'andamento del prezzo; se quindi avremo il timore che il prezzo possa crollare cambieremo immediatamente il nostro pagamento in un'altra valuta, se però la nostra convinzione è che il prezzo sia destinato a salire saremo felici di holdare le monete che abbiamo ricevuto.

La volatilità, quindi, oltre ad essere un limite è anche un'opportunità, chi opera con le criptovalute, infatti, non teme questo tipo di caratteristica ma ha imparato ad apprezzarla. Infine, come abbiamo avuto già modo di accennare in uno dei capitoli precedenti, questa tecnologia potrebbe anche tramutarsi in una specie di incubo distopico se immaginiamo un contesto in cui ad imporsi sia un modello di blockchain centralizzata nel quale l'anonimato degli utenti cessasse di essere tutelato; in questo caso, inevitabilmente, ci troveremmo a vivere in un mondo in cui i governi avrebbero assoluto controllo su ogni aspetto della nostra vita, una sorta di grande fratello orwelliano che non rappresenta certamente l'aspirazione massima di qualunque persona dotata di un minimo di intelligenza. Come ogni grande innovazione umana, quindi, anche quando parliamo di blockchain il giudizio non potrà essere aprioristicamente positivo o negativo, ma tutto dipenderà da come decideremo di utilizzare questa tecnologia; del resto, se ci fermiamo un attimo a riflettere su una qualunque delle grandi tecnologie che hanno cambiato il mondo (dalla stampa alla tv, passando per l'auto fino ad arrivare a internet), ci accorgiamo che sono state usate sia con finalità positive che con finalità negative.

La TV in Italia, giusto per fare un esempio, ha avuto un ruolo importante nei processi di alfabetizzazione della popolazione (attraverso programmi come “non è mai troppo tardi” che insegnarono letteralmente agli italiani a leggere e scrivere) e nel costruire definitivamente una lingua comune in un paese dove ancora la facevano da padrone i dialetti; lo stesso strumento, però, è stato usato non solo per “elevare” le masse ma anche per (scusatemi il termine) rincoglionirle. Basta guardare la quantità spropositata di spazzatura che i nostri canali televisivi ci propinano ogni giorno per capire come non si possa attribuire a questa tecnologia (quella televisiva) un giudizio univocamente positivo o negativo, ma occorra invece distinguere di caso in caso, di volta in volta, se il modo in cui usiamo la televisione ha un valore oppure no.

Ricapitolando, quindi, la blockchain ha diverse criticità, prima tra tutte una tendenza alla centralizzazione che appare già oggi essere marcata in quasi tutti i progetti esistenti sul mercato; indipendentemente dai limiti e dalle criticità che questa tecnologia mostra, sta a noi decidere come vogliamo usarla, se per costruire un mondo migliore o se preferiamo invece usarla per rendere le cose ancora peggiori di quanto non siano già. Questo possiamo dirlo con certezza già oggi, definire invece come evolveranno le cose nei prossimi 20 anni è attività che lasciamo volentieri ai cartomanti.

12. Utilità e punti di riferimento

Appassionarsi alle criptovalute, indipendentemente dal fatto che si decida di fare anche trading, implica che bisogna iniziare ad informarsi assiduamente sulle cose che succedono in questo mondo; se già normalmente in qualunque settore informarsi è diventata un'attività impegnativa, nel settore delle criptovalute raccogliere le notizie può diventare addirittura estenuante.

Ogni giorno, infatti, nascono nuovi progetti, nuove soluzioni a vecchi problemi e vengono diffuse notizie che dobbiamo necessariamente seguire; per informarci adeguatamente, quindi, dobbiamo avere dei punti di riferimento chiari. Per prima cosa dovremmo calarci nell'ottica di idee che i grandi giornali (così detti mainstream) non sono la migliore fonte per mantenersi informati quando parliamo di cripto; molto spesso, infatti, chi scrive sui grandi giornali lo fa "per contratto" viene quindi cioè invitato a scrivere di un argomento in voga al fine di soddisfare la domanda degli utenti senza che però possieda solide competenze per scrivere di quel dato argomento.

Ecco spiegato il motivo per cui sui maggiori giornali capita spesso di leggere imprecisioni, cose scorrette o veri e propri sfondoni di quelli che non farebbe nemmeno un bambino di dodici anni; nel tempo, fortunatamente, sono nati numerosi siti e blog di carattere informativo/divulgativo che si occupano esclusivamente di criptovalute e sui quali a scrivere sono persone che magari non saranno famose ma che conoscono molto bene questa tecnologia e la seguono ormai da anni.

Per correttezza preferisco evitare di menzionare questi siti, chiunque può comunque facilmente fare una ricerca online e selezionare quei quattro o cinque siti, comunemente considerati credibili da tutta la comunità, attraverso i quali informarsi; del resto una persona che ama il calcio, ad esempio, per informarsi compra un giornale sportivo non uno che si occupa di politica e cronaca, allo stesso modo se ci si vuole informare seriamente sulle criptovalute non bisognerebbe leggere i giornali economici ma affidarsi a siti specializzati che trattano questo tema ormai da anni e che si avvalgono della collaborazione di persone che questa tecnologia l'hanno studiata e non si sono limitate invece a leggere in venti minuti un paio di pagine su wikipedia.

In ogni caso il principale punto di riferimento per la comunità che opera con le criptovalute è il forum bitcointalk, sul quale si può trovare ogni genere di informazione e una soluzione ad ogni tipo di problema; la comunità, poi, è sempre molto proattiva e attenta ad aiutare gli utenti alle prime armi, a patto ovviamente che i neofiti dimostrino di volersi impegnare, cercando attivamente le informazioni di cui hanno bisogno, evitando di pretendere la famosa "pappa pronta".

Per informazioni sulle monete e i token presenti sul mercato, per conoscere gli indirizzi dei siti web ufficiali, informazioni sulla supply e sugli exchange che permettono di operare con una determinata moneta il punto di riferimento per tutta la comunità è invece coinmarketcap. Per avere informazioni sulle news di carattere tecnico, sui nuovi rilasci previsti, i recenti sviluppi tecnici, eventuali hard fork previsti ed ogni altra informazione squisitamente tecnica è molto comune avvalersi di un sito chiamato coinmarketcal, molto apprezzato soprattutto dai trader.

Siti come reddit, poi, sono a tutt'oggi molto frequentati dagli appassionati di criptovalute ed ogni progetto ha normalmente la sua pagina su questo sito; poi ci sono ovviamente newsletter e i canali di comunicazione ufficiali delle varie monete. Anche i social sono importanti, quindi oltre che seguire

gli account ufficiali dei vari progetti dobbiamo iniziare a seguire anche i singoli sviluppatori che spesso proprio attraverso i social hanno modo di condividere vere e proprie chicche; inoltre al giorno d'oggi è diventato molto comune che i trader condividano la loro operatività attraverso i social network, finendo così col fare anche un'attività che è sostanzialmente didattica.

Il consiglio, quindi, tanto più per chi vuol fare trading, è di selezionare un gruppo di trader di propria fiducia (sulla base della qualità delle analisi che sono capaci di produrre) e seguirli sui vari social tentando sia di comprendere la loro strategia di trading sia di ricavarne, quando possibile, qualche piccola dritta. Assumendo tutte queste piccole abitudini inizieremo pian piano ad orientarci trovando delle figure che rappresentino per noi un punto di riferimento, delle quali abbiamo fiducia piena e che ci permetteranno di ottimizzare il poco tempo che abbiamo a disposizione per poterci informare.

13. CONCLUSIONI

Siamo quindi giunti alla fine di questo nostro viaggio nel mondo della tecnologia blockchain ed è il momento di tirare le somme di questo percorso; ovviamente una lettura di un testo del genere non è sufficiente a costruire una conoscenza profonda di questo tipo di tecnologia ma dovrebbe comunque consentire a chiunque, indipendentemente dalle proprie competenze tecniche, di iniziare un percorso di comprensione più grande sulla base dei primi, basilari concetti acquisiti dalla lettura di questo libro.

Conoscere sommariamente come funziona la tecnologia blockchain, infatti, non significa conoscere il mercato; anche se in giro può capitare frequentemente di sentire che tutte le "altcoin" non sono altro che cloni di Bitcoin, le cose non stanno affatto così e per conoscere una determinata criptovaluta occorre prima studiarla.

Dal momento che sono diversi i protocolli di consenso, diversi gli algoritmi di hash, diverse le caratteristiche della rete, di conseguenza è inevitabile che ogni progetto finisca con l'avere peculiarità uniche e in qualche modo persino esclusive. Per poter dire di comprendere davvero la blockchain, quindi, è inevitabile dover dedicare un po' di tempo a uno studio approfondito delle maggiori criptovalute presenti sul mercato; non sarà, in ogni caso, tempo sprecato dal momento che, e questo mi sento di poterlo garantire, nei prossimi anni questa tecnologia impatterà pesantemente sulla nostra quotidianità arrivando a ridisegnare il mondo come lo conosciamo, esattamente come, qualche decennio fa, la nascita e la crescita vertiginosa di internet aveva già fatto.

Chiunque, quindi, si sia mai ritrovato a pensare con rammarico alla nascita di internet, rimpiangendo di non aver saputo cogliere sin da subito le opportunità che quella nuova tecnologia stava offrendo, non può permettersi il lusso di perdere di nuovo anche questo treno o si ritroverà a pentirsene amaramente nei prossimi anni; che potesse ritornare in così breve tempo un'opportunità del genere dopo la grande rivoluzione di internet, sinceramente, andrebbe inteso come qualcosa di più unico che raro, una coincidenza che solo molto raramente abbiamo visto capitare nel corso della storia dell'umanità.

E' vero che ormai lo sviluppo tecnologico è diventato esponenziale, è vero anche che la tecnologia si muove molto più velocemente di quanto noi esseri umani possiamo fare, ma attualmente esiste forse un solo ambito possibile che potrebbe rivelarsi capace di impattare in maniera così prepotente sulla nostra quotidianità, ed è rappresentato dalla genetica.

Quello che sto sostenendo, in altre parole, è che non è detto che nei prossimi 50 anni ci si ripresenti di nuovo la possibilità di "cavalcare" una nuova tecnologia così rilevante sin dai suoi esordi; è già straordinario che la stessa generazione abbia avuto la possibilità di vivere due momenti così epocali (con internet prima e con la blockchain poi), difficile immaginare che nei prossimi anni ci si ripresenti ancora una terza opportunità in questo senso.

Se guardiamo alle nostre spalle, infatti, possiamo facilmente notare che i momenti nella storia dell'umanità in cui lo sviluppo tecnologico ha segnato svolte così epocali come quelle a cui assistiamo oggi si contano sulle dita di una sola mano; dovremmo quindi considerarci molto

fortunati per aver potuto assistere in un così breve periodo di tempo alla nascita e alla diffusione di due tecnologie come internet e la blockchain potenzialmente così rivoluzionarie. La sfida, arrivati a questo punto, consiste più che altro nella forma che riusciremo a dare a questa nuova rivoluzione tecnologica, se saremo, in altre parole, capaci di usare questo tipo di tecnologia per rendere il mondo un posto migliore o se, nonostante e per certi versi persino a scapito della tecnologia stessa, continueremo a replicare sempre gli stessi errori; in ogni caso tutto questo dipende strettamente da noi e dalle scelte che prenderemo (come popolo, come cittadini) nei prossimi anni.

Accettare, come sembra stia diventando molto comune purtroppo, di perdere il nostro diritto alla privacy sacrificandolo all'altare della sicurezza e della legalità, infatti, nel lungo periodo potrebbe rivelarsi una pessima scelta capace di generare, a catena, una serie di effetti estremamente deleteri con conseguenze che oggi sono difficili da immaginare; che cosa succederà, se avremo il coraggio di usare questa tecnologia per mettere al centro del mondo le persone, gli individui, invece che limitarci a metterli sotto controllo permanente ce lo potrà dire solo il tempo, noi, dal canto nostro, possiamo solo aspettare per vedere cosa succederà ed impegnarci già oggi affinché le persone comuni capiscano l'importanza e le potenzialità offerte dal nuovo modello decentralizzato che sta emergendo sempre più chiaramente con la nascita della tecnologia blockchain.

14. CREDITS

Trovo necessario chiudere questo libro con alcuni ringraziamenti che reputo essere doverosi; per prima cosa, quindi, ringrazio la redazione di ValuteVirtuali.Com che questo libro l'ha commissionato e con la quale collaboro ormai da diversi mesi. Ringrazio ovviamente tutti coloro che quotidianamente si impegnano a realizzare nuovi contenuti per Wikipedia (dalla quale abbiamo attinto diverse definizioni in diversi passaggi di questo libero), che fanno ormai da anni un lavoro fantastico e in maniera completamente disinteressata. In secondo luogo credo che sia doveroso ringraziare tutti gli sviluppatori che, ogni giorno, dedicano una parte del loro tempo e le loro competenze a creare software open source che permette ad ognuno di noi di fare il proprio lavoro con professionalità senza dover spendere cifre spropositate per acquistare le licenze.

Un grazie particolare anche a tutti i divulgatori (non solo a quelli che si occupano di blockchain) che creano continuamente nuovi contenuti per il web e che tali contenuti li distribuiscono gratuitamente permettendo ogni giorno a milioni di persone guidate da una sana curiosità di vivere un percorso di apprendimento e approfondimento continui. Di conseguenza vorrei anche ringraziare tutte le persone che stanno dall'altra parte della barricata, gli utenti quindi, quella massa informe di individui che ogni giorno usa internet per informarsi, crescere e studiare e non solo per ammazzare il tempo; tutte quelle persone, quindi, che rappresentano la vera coscienza critica e l'intelligenza collettiva di questa società.

Ogni volta che mi lancio in un nuovo progetto, poi, c'è un gruppo musicale che mi fa da colonna sonora durante i giorni che servono per completarlo, è stato così anche per la scrittura di questo libro, durante la quale c'è stata una band di tre grandissimi musicisti che mi ha fatto compagnia attraverso le lunghe ore passate a scrivere al computer; ringrazio quindi i "Too many zooz" che ho avuto modo di scoprire e apprezzare proprio mentre mi cimentavo nella scrittura di questo libro e che vi invito ad ascoltare perché fanno davvero una musica fantastica. Un ringraziamento particolare va poi a quelle centinaia di persone (troppe per citarle tutte) che sono il mio punto di riferimento nella cripto-economia, ai trader che stimo e che ogni giorno condividono sui social la loro operatività, agli esperti (quelli veri) di crittografia e di economia che mi permettono di continuare ad orientarmi in un mondo che si muove sempre troppo velocemente e che con cadenza quotidiana mi permettono di scoprire e conoscere cose sempre nuove.

Un ultimo ringraziamento, infine, agli utopisti, ai pazzi, a coloro che non si rassegnano a questo mondo così come lo conosciamo e che stanno dedicando la loro vita a creare ed ipotizzare modelli più sani e più giusti per organizzare la nostra società; sono loro, a mio parere, il vero sale della terra.