

Profili di complessità e di rischio delle “criptovalute”

SOMMARIO: Breve premessa – 1. L’insidiosità delle criptovalute. – 2. Le diverse tipologie di criptovalute. – 3. Il *Bitcoin*. – 3.1. Il sistema *Peer to Peer* (P2P) ed il funzionamento della criptovaluta. – 3.2. La dubbia qualificazione giuridica del *Bitcoin*. – 4. I principali profili di rischio connessi all’utilizzo di *Bitcoin*. – 4.1. L’altissima volatilità ed il rischio di “bolla speculativa”. – 4.2. I rischi connessi all’assenza di tutela legale e contrattuale. – 4.3. L’anonimato e le finalità illecite. – 4.3.1. Il “*cyberlaundering*”. – 4.4. Alcuni profili “residuali”. – 5. Cenni per alcune brevi riflessioni conclusive.

* * *

Breve premessa

La presente trattazione si propone di affrontare, nei limiti del tecnicismo informatico accessibile ad un giurista, il tema delle cosiddette “criptovalute” o “monete virtuali”; un tema complesso ed attuale come pochi altri e dai quali tuttavia si distingue per la capacità di trasmettere ai più l’impressione di un qualcosa di semplice e facilmente comprensibile, essendo invece, nella realtà dei fatti, l’esatto opposto. Per questo motivo si ritiene conveniente ed opportuno iniziare con una pur rapida introduzione di carattere generale volta a fornire alcune necessarie informazioni di premessa. Si proseguirà quindi con l’analisi del funzionamento della “divisa” virtuale maggiormente nota e diffusa illustrandone insidie e pericoli. In conclusione, si tenterà di offrire qualche primo cenno di riflessione corredato di alcuni spunti *de iure condendo*.

1. L’insidiosità delle criptovalute

Secondo la definizione di criptovalute (o “valute virtuali”) fornita dalla Banca d’Italia, queste sono “*rappresentazioni digitali di valore, utilizzate come mezzo di scambio o detenute a scopo di investimento, che possono essere trasferite, archiviate e negoziate elettronicamente*”¹. E’ quindi interessante poter subito evidenziare un primo dato: già nel fornire la suddetta definizione la Banca d’Italia mette in guardia gli utenti rinviando ad una nota a piè di pagina in cui avverte che “*l’utilizzo del termine ‘valuta’ non deve [...] intendersi volto a definire la natura degli strumenti descritti nel presente documento*”. La precisazione, che in un primo momento potrà apparire banale, risulta

¹ *Avvertenza sull’utilizzo delle cosiddette “valute virtuali”, pubblicata da Banca d’Italia il 30 gennaio 2015, p. 1. Si segnala altresì il documento pubblicato il 4 luglio 2014 dall’Autorità Bancaria Europea (EBA), EBA Opinion on ‘virtual currencies’, in cui viene meglio esplicitato il concetto di “rappresentazione digitale di valore”. Si legge infatti che tale definizione “refers to the fact that the value is essentially represented in digital form. This does not exclude the possibility that it may also be physically represented, such as through paper printouts or an engraved metal object. The term ‘digital representation of value’ is close to the monetary concept of a ‘unit of account’ but includes the option to consider VCs as private money or a commodity. It also avoids making reference to a standard numerical unit of account for the measurement of value and costs of goods, services, assets and liabilities, which might (according to some views), imply that it needs to be stable over time”.*

invece assai significativa, tanto da arrivare da sola ad inquadrare l'intero insieme di problematiche (giuridiche e non solo) sottese ad un fenomeno che giorno dopo giorno continua ad espandersi macinando terreno in un mondo virtuale e parallelo. La nota a piè pagina, che è di per sé indice della difficoltà di definizione e di inquadramento giuridico dell'istituto, risulta essere dunque carica di un ulteriore significato ad indicare che quello che ci si accinge a percorrere è un terreno mai battuto prima e che, per intenderlo correttamente, è necessario stare in guardia rifuggendo semplici (pur istintive) semplificazioni.

Apparentemente quello di “moneta virtuale” è infatti un concetto di facile comprensione, che, evocando la nozione e le logiche di funzionamento delle “comuni” monete può indurre l'utente ad un'immediata confidenza e favorire una fiducia che sarebbe quanto mai mal riposta. Siffatto meccanismo associativo rappresenta invero una delle maggiori insidie serbate dal mercato delle criptovalute ai suoi fruitori, raramente preoccupati di approfondirne i concreti principi di funzionamento. Proprio per tale ragione si rendono perciò sempre più indispensabili gli ammonimenti di cui si sono fatte carico le competenti Autorità nazionali ed internazionali.

2. Le diverse tipologie di criptovalute

E' difficile individuare l'esatto numero di valute virtuali ad oggi circolanti. Secondo una stima fornita dall'Unità di Informazione Finanziaria per l'Italia (UIF), nel mondo si arriverebbero a contare addirittura più di 500 criptovalute, alcune tra di loro simili, altre di natura più particolare e con peculiarità proprie. Abbandonando da subito l'utopica idea di elencarle tutte, per il momento ci si accontenterà di richiamare quindi il metodo elaborato dalla Banca Centrale Europea (BCE) al fine di classificare le varie “monete” sulla base del tipo di rapporto che queste intrattengono con le divise legali e, più in generale, con l'economia reale. Una prima tipologia è allora quella delle valute virtuali dette “**non convertibili**” o “**chiuse**”² per via del fatto che esse non producono interazioni con l'economia reale. Queste sono spendibili unicamente nel contesto della comunità virtuale che le accetta per acquistare beni e/o servizi virtuali offerti all'interno della medesima comunità. Bene precisare inoltre che tali monete non possono essere né acquistate né convertite con denaro reale. Conseguentemente, l'unico modo per entrarne in possesso è quello di svolgere specifiche e particolari attività *online* che variano da caso a caso, a seconda del contesto di riferimento. L'ambito in cui ha trovato maggior diffusione questa prima categoria di valuta virtuale è quello dei giochi informatici e, più specificamente, dei *multi-media online game*, ossia quei giochi supportati da computer e console che consentono ai giocatori di interagire tra loro sfruttando la connessione alla rete³. Va da sé che la limitata circolazione, unita alla mancanza di un effettivo potere d'acquisto, fanno sì che l'utilizzo di tali monete produca un impatto relativamente trascurabile sull'economia reale.

Una seconda categoria è poi quella delle valute virtuali “**a convertibilità limitata**” o “**unidirezionali**”, che possono essere acquistate con moneta tradizionale ad un tasso di cambio prefissato (ad esempio mediante bancomat o carta di credito), ma che non sono

² Si veda ancora l'*Avvertenza sull'utilizzo*, cit., p. 1.

³ Alcuni esempi sono forniti dai *Linden Dollars* utilizzati in *Second Life*, i *Nintendo Points* impiegati per i videogiochi *Nintendo* ed i *Facebook Credits* sull'omonimo *social network*.

suscettibili di essere poi riconvertite in denaro reale. Esemplificando, appartengono a siffatta categoria i “punti” di alcune carte fedeltà emesse da supermercati o altre aziende che attraverso questo strumento ottengono vantaggi di varia natura, quali (ad esempio) la fidelizzazione della clientela e l’agevolazione dei pagamenti. I riflessi che l’uso di questo tipo di moneta è in grado di produrre sul corso dell’economia reale sono pertanto certamente più consistenti rispetto a quelli sortiti dalla prima categoria, rimanendo tuttavia ben lontani dai livelli di influenza propri delle monete virtuali “**pienamente convertibili**” o “**bidirezionali**”. Queste ultime, che costituiscono la terza ed ultima categoria, sono perciò quelle di maggior interesse ai fini della presente trattazione, rappresentando le “criptovalute” propriamente intese. Le monete bidirezionali possono infatti essere convertite in valute aventi corso legale in qualsiasi momento, secondo i tassi di cambio (più o meno) ufficiali, potendo essere altresì spese per l’acquisto di beni e servizi reali o virtuali. Peraltro, come si avrà modo di meglio approfondire più avanti, i tassi di cambio di siffatte monete scontano il più delle volte un’elevatissima volatilità, il che rende alquanto rischioso ed imprevedibile l’esito delle operazioni effettuate con questo genere di valute.

All’interno della macrocategoria delle monete “bidirezionali” è poi pure possibile rintracciare ulteriori “sottocategorie”. Si distinguono invero le c.d. valute “**centralizzate**” da quelle “**decentralizzate**”, a seconda che queste siano create da un singolo emittente privato ovvero da un imprecisato numero di utenti dotati di particolari *software*. Ancora, si possono differenziare le c.d. monete “**globali**”, con diffusione planetaria, dalle monete “**locali**”, la cui circolazione è limitata a comunità più o meno ristrette. Infine, si potrebbero individuare ulteriori criteri di differenziazione fondati sulle diverse logiche di funzionamento sottese alle rispettive valute. La complessità dei meccanismi propri di ciascuna di esse rende tuttavia sconveniente avventurarsi in un simile percorso, risultando per contro certo più opportuno limitarsi all’analisi del funzionamento della criptovaluta maggiormente nota e diffusa: il *Bitcoin*.

3. Il *Bitcoin*

Come detto, esistono centinaia di criptovalute, ognuna basata su un diverso e complesso algoritmo crittografico. Tra tutte, la più nota e diffusa è indubbiamente il *Bitcoin*: una moneta virtuale creata nel 2009 da Satoshi Nakamoto, misterioso pseudonimo dietro al quale si annida un fitto mistero circa la reale identità dell’inventore⁴. Purtroppo, per trattare con cognizione di causa le implicazioni legali connesse alla circolazione del *Bitcoin*, il giurista è chiamato a cimentarsi, non senza sforzo, nella comprensione (quantomeno sommaria) dell’algoritmo regolante la celebre criptovaluta.

3.1. Il sistema *Peer to Peer* (P2P) ed il funzionamento della criptovaluta

⁴ Secondo alcune voci si tratterebbe in realtà non di una singola persona, ma di un nutrito gruppo di esperti in varie discipline, quali la crittografia, l’informatica e le transazioni bancarie *online*. Recentemente è stata avanzata l’ipotesi che dietro lo pseudonimo di Nakamoto si celi in realtà l’imprenditore australiano esperto di tecnologia Craig Wright (cfr. L. MCGRATH GOODMAN, *The Face Behind Bitcoin*, disponibile sul sito www.mag.newsweek.com, del 6 marzo 2014).

L'inquadramento del *Bitcoin* in una delle sopraindicate categorie è quello di una valuta "pienamente convertibile", "globale" e soprattutto "decentralizzata". In altre parole, il funzionamento del sistema *Bitcoin* risulta scevro da qualsivoglia forma di controllo accentrata nelle mani di un singolo individuo o di una singola istituzione che ricopra il ruolo equivalente a quello di una banca centrale. L'assenza di un controllore centrale, nonché la mancanza di intermediari e di banche, fanno sì che i costi di utilizzo e di gestione del sistema siano assai contenuti ed equamente suddivisi tra tutti gli utenti, realizzando così quella che si potrebbe definire come la moneta di libero mercato *par excellence*. Il sistema *Bitcoin* si basa infatti su di una rete informatica "*Peer to Peer*" (P2P), formata da un indeterminato numero di "nodi" (ossia di computer) che dialogano tra loro in posizione paritaria, scambiandosi un costante flusso di informazioni che rappresenta il *database* dell'intero sistema. Insomma, ciò che più è importante comprendere è che non esistono rapporti di gerarchia tra i computer con cui i vari utenti accedono al sistema, realizzandosi così un vero e proprio reticolo di rapporti da pari a pari (*peer to peer*) operanti in un regime di completa *disclosure*, in grado di elidere qualsiasi stortura o asimmetria informativa. Come si avrà cura di spiegare meglio nel prosieguo, è manifesto che una simile mancanza di controllo accentrato importerà anche consistenti rischi in termini di sicurezza e certezza dei rapporti di scambio, che inevitabilmente finiscono per diventare parte integrante del sistema.

Scendendo più nel dettaglio, si può affermare che il sistema *Bitcoin*, ossia la rete P2P, si fonda su due "registri" distinti e paralleli; il primo è dato dalla c.d. ***Transaction Chain***, mentre il secondo è noto come ***Blockchain***. Entrambi sono indispensabili al corretto e trasparente funzionamento del sistema, ponendosi dunque in un rapporto di reciproca complementarietà. Semplificando, si potrebbe definire la *Transaction Chain* come quel registro che consente di tenere traccia di tutte quante le transazioni effettuate dall'intero numero di utenti presenti nel sistema, mentre la funzione della *Blockchain* è quella di presidiare sicurezza e correttezza della *Transaction Chain*, evitando che i vari "nodi" della rete (ossia i computer tramite cui gli utenti effettuano transazioni) ed il sistema stesso incorrano in truffe. La particolarità dell'universo *Bitcoin* consiste tuttavia nel fatto che nessuno dei due "registri" sia detenuto e/o controllato da un soggetto terzo in funzione di garante, costituendo invece un patrimonio informativo condiviso da tutti gli utenti ai quali viene così demandato il compito di aggiornare e verificare costantemente entrambe le "catene" (*chain*). Insomma, gli utilizzatori sono allo stesso tempo contabili e revisori non solo delle proprie transazioni, ma anche di tutte le altre che vengono effettuate sulla rete *Bitcoin*.

Ad ulteriormente esplicitare quanto sopra accennato in merito alle due "*chain*" si supponga che Tizio, utente registrato nel sistema *Bitcoin* e titolare di un portafoglio digitale (*e-wallet*), voglia disporre un pagamento a Caio, anch'egli utente del sistema, per un ammontare di 10 *Bitcoin*. Per procedere alla transazione Tizio (meglio, il suo computer – "nodo") invierà alla rete un messaggio contenente l'indicazione del destinatario del pagamento e l'ammontare. A questo punto, ogni altro nodo della rete riceverà il messaggio di Tizio e provvederà a trascriverlo sul proprio registro (*Transaction Chain*), per poi ritrasmettere a sua volta il messaggio agli altri nodi della rete fino a quando questo non abbia avuto una completa e capillare diffusione. Tizio potrà dunque disporre dei suoi *Bitcoin* solo ove sia possibile accertare, ripercorrendo a ritroso l'intero registro di transazioni, che non vi siano "intoppi" nella ricostruzione del

flusso di scambi, ossia che qualcuno, in passato, abbia correttamente ordinato e registrato un accredito sul suo conto di importo pari o superiore a quello di cui oggi egli intende disporre. Volendo provare a spiegare in termini analogici ciò che avviene in maniera digitale, si può immaginare che ogni utente conservi un lunghissimo “mastrino” in cui registra costantemente in “dare” e in “avere” le transazioni che la rete gli comunica essere state effettuate. La differenza che intercorre tra il comune metodo della “partita doppia” e quello del sistema *Bitcoin* consiste nel fatto che, in quest’ultimo, non esistono occasioni in cui si “tirino le somme” dei vari conti calcolandone il saldo, dovendosi di volta in volta ricontrollare a ritroso l’intera catena di pagamenti fino a risalire alla prima transazione in assoluto effettuata sul sistema. Occorre però una precisazione: il controllo analitico a ritroso di tutti gli scambi effettuati viene operato dal singolo utente solo la prima volta che questi si registra sul sistema aprendo un “conto” *Bitcoin*. Infatti, ogni qual volta si decida di creare un nuovo *account*, il computer effettuerà questa operazione che potrà richiedere anche più di ventiquattr’ore per essere completata. Da quel momento in avanti si può dire che il computer del singolo utente terrà per buone e verificate tutte le transazioni precedenti alla sua registrazione, dovendosi preoccupare di registrare e verificare unicamente gli ordini trasmessi sul sistema in momenti successivi, mantenendosi quindi costantemente aggiornato.

E’ questo il principio di funzionamento della c.d. *Transaction Chain*, che incontra tuttavia un grande limite laddove si renda necessario stabilire e controllare anche la cronologia con cui si siano succedute le singole passate transazioni. Per sopperire a siffatta criticità interviene la *Blockchain*. Esemplificando si può affermare che quest’ultima svolge una funzione del tutto analoga a quella che, nel mondo reale, è esplicata dal Registro Immobiliare. Esattamente come nel settore immobiliare infatti ci si rifà alla data di trascrizione del contratto di compravendita per stabilire quale tra più contemporanei acquirenti sia effettivamente titolare del diritto reale, anche nel sistema della valuta digitale occorrerà rifarsi alla *Blockchain*.

Si è anticipato che per effettuare una transazione in *Bitcoin* l’utente Tizio trasmette un messaggio ai singoli “nodi” che compongono la rete, così da informarli dell’operazione in corso. La criticità si annida nel fatto che il messaggio lanciato da Tizio, passando di nodo in nodo, non viene recepito simultaneamente da tutti gli utenti, che non hanno quindi garanzia alcuna del fatto che l’ordine di arrivo dei messaggi sia effettivamente “specchio” di quello in cui le singole transazioni siano state realmente effettuate. Esattamente come avviene per il mercato dei beni immobili, dunque, quello che si pone è un problema di certezza.

La soluzione al problema viene dunque fornita da quel complesso strumento che è chiamato *Blockchain*. La rete *Bitcoin* suddivide infatti le operazioni in “blocchi”, ovvero gruppi di transazioni che, concatenati l’un l’altro, formano una catena (*Blockchain*) altra e distinta rispetto alla *Transaction Chain*. La regola impone che si considerino perfezionate nello stesso istante le transazioni inserite nel medesimo blocco. Al contrario, quelle non ancora ricomprese in alcun gruppo saranno da ritenersi come ancora non confermate o non ordinate. Ancora una volta si tocca quindi con mano l’essenza della gestione e del controllo “diffusi” e non accentrati, considerando che spetterà ai singoli nodi della rete risolvere le problematiche sottese alle transazioni non

ancora “raggruppate” e ordinate. Riducendosi ancora una volta a fornire una mera semplificazione del complesso procedimento matematico, si può allora affermare che ogni utente (meglio, ogni “nodo”) potrà raggruppare in un unico blocco un certo numero di transazioni ancora non ordinate o confermate, per poi trasmettere la collazione così ottenuta agli altri utenti della rete nella speranza di ricevere la loro approvazione. Come manifesto, dato l’immenso traffico di dati ed informazioni, può ben darsi il caso in cui diversi nodi creino più blocchi (magari in conflitto tra loro) nel medesimo momento, trasmettendoli poi alla rete, che, a questo punto, si troverà nell’“imbarazzo” di dover stabilire quale dei diversi gruppi vada considerato l’anello finale della catena fino a quel momento esistente. La via d’uscita da questa *impasse* è rappresentata (almeno parzialmente) dal fatto che ogni blocco deve contenere in sé la soluzione di alcuni “problemi matematici” di assai difficile soluzione, il che rende stocasticamente difficile che più utenti riescano a risolvere il medesimo problema nello stesso preciso istante, diminuendo così il rischio di contrasti tra “blocchi”. Ad ogni modo, esistono meccanismi e regole che, in caso di simultaneità, stabiliscono quale dei blocchi debba essere preferito ai fini della corretta formazione della *Blockchain*. In buona sostanza, la soluzione di eventuali contrasti ed il conseguente inanellarsi dei “blocchi” conferisce certezza alla sequenza di transazioni e consente dunque il corretto funzionamento dell’intera rete. Tale operazione, che impropriamente definiremo di “controllo” o di “verifica”, è detta “*mining*”⁵ o “*Bitcoin mining*” e costituisce senza alcun dubbio un passaggio chiave dello schema su cui si regge l’intero mondo *Bitcoin*⁶. L’attività di *mining* ha peraltro una funzione anche creativa di moneta virtuale. Ai *miners* che portino a termine una data operazione, contribuendo così ad aumentare la sicurezza del sistema, viene infatti riconosciuta a titolo di “ricompensa” una certa quantità di nuove monete⁷.

3.2. La dubbia qualificazione giuridica del *Bitcoin*

Venendo ad una rapida scorsa delle vesti giuridiche che si è tentato di conferire alla criptovaluta più diffusa al mondo vi è che già nelle prime battute della presente trattazione si evidenziava come le valute virtuali siano genericamente definite alla stregua di “rappresentazioni digitali di valore”. Bene ora precisare ulteriormente come queste non vadano affatto confuse con quella che viene definita “**moneta elettronica**” o

⁵ Sul punto si veda, *ex multis*, N. MANCINI, *Bitcoin: rischi e difficoltà normative*, in *Banca impresa soc.*, 2016, 1, pp. 126 e s., la quale afferma che “*tale verifica viene eseguita attraverso una serie di algoritmi il cui calcolo può essere eseguito da qualunque hardware. Nei primi anni di funzionamento del Bitcoin, chiunque scaricava il programma di mining aveva la possibilità di effettuare tale controllo, giacché anche il singolo utente dotato di un modesto elaboratore era in grado di svolgere il mining. La progressiva diffusione dei Bitcoin ha richiesto sempre più potenza di calcolo ed ha costretto i miners a costituire gruppi di collaborazione: tramite appositi programmi, i pool di miners uniscono la potenza dei propri computer per effettuare più verifiche possibili*”.

⁶ Cfr. il documento attribuito a Satoshi Nakamoto, *Bitcoin: un sistema di moneta elettronica peer to peer*, disponibile sul sito www.bitcoin.org, in cui si afferma che “*il sistema è sicuro fintanto che i nodi onesti controllano collettivamente più potenza CPU rispetto a qualsiasi gruppo collaborativo di nodi attaccanti*”.

⁷ E’ dunque possibile pensare al *mining* come ad uno dei metodi di acquisizione di *Bitcoin*, che si va quindi ad aggiungere alle tecniche più comuni (quali, ad esempio, la conversione di moneta avente corso legale e la vendita di beni e servizi).

“*e-money*”, che (al contrario della moneta virtuale) è suscettibile di precisa identificazione giuridica⁸.

Sin da subito va dunque precisato che le criptovalute (ivi compreso il *Bitcoin*), non hanno corso legale e, pertanto, “*non devono per legge essere obbligatoriamente accettate per l’estinzione delle obbligazioni pecuniarie, ma possono essere utilizzate per acquistare beni o servizi solo se il venditore è disponibile ad accettarle*”. Come poi si è ampiamente ribadito, questo tipo di monete, non essendo né emesso né garantito da banche o altre autorità pubbliche, risulta generalmente privo di regolamentazione: circostanza che rende ancor più arduo il già difficile compito del giurista che si proponga di intagliare una cornice giuridica per questo nuovo fenomeno mediante il ricorso ad istituti assai più risalenti. Sono invero diverse le proposte autorevolmente avanzate per conferire un’accettabile qualificazione a tale inedita fattispecie⁹. Nessuna di esse si rivela tuttavia perfettamente adatta a fungere da veste giuridica per le varie forme di moneta virtuale. Le varie opzioni prospettate spaziano infatti dall’ampia genericità del concetto di “bene giuridico” *ex art. 810 c.c.*, all’esoticità propria di quello di *new property*. Ancora, si è proposto di identificare il *Bitcoin* tramite la definizione di “documento informatico”¹⁰ fornita dal D.lgs. 7 marzo 2005, n. 82 (c.d. Codice Amministrazione Digitale) facendo leva sulle sopracitate tecnologie della *Blockchain* e della *Transaction Chain*. Ulteriore interessante spunto è poi offerto dalla nozione di “strumento finanziario” mutuabile dal c.d. Testo Unico della Finanza. Purtroppo però anche su questo versante le criticità non mancano, atteso che i “mezzi di pagamento” e gli altri strumenti non espressamente previsti dalla norma rimangono esclusi dal novero dei “prodotti finanziari”, di cui lo “strumento finanziario” costituisce una *species*. Se, dunque, sul versante dottrinale, si tende ad escludere che le monete virtuali siano riconducibili all’ambito applicativo del T.U.F.¹¹, nel contesto giurisprudenziale

⁸ Ai sensi dell’art. 55, lett. *h-ter*, della legge 1 marzo 2002, n. 39, attuativa della Direttiva 2000/46/CE, la “moneta elettronica” si definisce come “*un valore monetario rappresentato da un credito nei confronti dell’emittente che sia memorizzato su un dispositivo elettronico, emesso previa ricezione di fondi di valore non inferiore al valore monetario emesso e accettato come mezzo di pagamento da soggetti diversi dall’emittente*”. Come è stato correttamente precisato è bene dunque non confondere il concetto di moneta elettronica con quello di moneta virtuale, in quanto, mentre la prima “*è uno strumento di pagamento memorizzabile su un dispositivo elettronico che presuppone il necessario caricamento sulla carta di fondi già esistenti presso l’emittente, senza comportare la creazione di una nuova moneta nel sistema (es. carte di credito, carte di debito, prepagate, ecc.) e generalmente accettato come mezzo di pagamento da imprese diverse dall’emittente medesimo, la moneta virtuale o denaro digitale (e-cash o cyber-cash) è un tipo di moneta non regolamentata che viene rilasciata e controllata dai suoi sviluppatori*” (E. SIMONCINI, *Il cyberlaundering: la “nuova frontiera” del riciclaggio*, in *Riv. trim. dir. pen. econ.*, 2015, 4, p. 903). Per un’analisi dei punti di contatto tra *Bitcoin* e moneta elettronica, si veda N. MANCINI, *op. cit.*, pp. 126 e s.

⁹ Il riferimento è allo scritto di R. BOCCHINI, *Advisor* per la Commissione ECON Affari Economici e Monetari, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. inform.*, 2017, 1, pp. 31 e s.

¹⁰ Ai sensi dell’art. 1, lett. *p*, del D.lgs. 82/2005, per “documento informatico” deve intendersi “*il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*”.

¹¹ Cfr. R. BOCCHINI, *op. cit.*, p. 34, a parere del quale le monete virtuali sarebbero addirittura escluse dall’applicazione del “sistema MiFID” previsto dalla Direttiva 2004/39/CE relativa ai mercati degli strumenti finanziari. Per completezza, corre altresì l’obbligo di precisare come lo stesso Autore dia conto della possibilità, paventata da taluni, di annoverare il *Bitcoin* nella definizione dei prodotti e servizi finanziari “*coperti dalla disciplina domestica a tutela dell’integrità dei mercati o a protezione dei consumatori*”.

domestico si registra una parziale difformità di vedute, che, lungi dal porsi quale dato dirimente sul punto, è nondimeno idonea a fungere da (ennesimo) elemento rivelatore della diffusa incertezza procurata dall'avvento di queste nuove creazioni informatiche¹². Da ultimo, si sono registrate ipotesi di qualificazione del *Bitcoin* come *commodity* finanziaria (per via delle finalità speculative e/o di investimento di cui sovente è fatto oggetto), ovvero come “mezzo di pagamento” ai sensi della Direttiva 2007/64/CE relativa ai servizi di pagamento, recepita in Italia con il D.lgs. 27 gennaio 2010, n. 11. Con riferimento a quest'ultima proposta è stata nondimeno sollevata la lucida obiezione secondo la quale la corrente interpretazione della summenzionata Direttiva ne limiterebbe la portata ai soli pagamenti denominati in moneta legale¹³.

L'impossibilità di rinvenire la corretta allocazione del *Bitcoin* nell'ordinamento giuridico italiano induce a rammentare come quella della corretta qualificazione giuridica non sia questione di poco momento, atteso, come evidente, che tra le molte implicazioni che essa può sortire vi è anche quella della astratta configurabilità delle fattispecie di reato previste dalle norme dei Testi Unici Bancario e Finanziario. Più precisamente, ci si vuole riferire ai reati di “abusiva attività di raccolta del risparmio” (art. 130 T.U.B.), “abusiva attività bancaria” (art. 131 T.U.B.), “abusiva attività di prestazione di servizi di pagamento” (art. 131-ter T.U.B.) e “abusivismo” per la prestazione di servizi di investimento (art. 166 T.U.F.). E' infatti opportuno ripetere la già citata Avvertenza della Banca d'Italia nella quale si afferma che “*in Italia, l'acquisto, l'utilizzo e l'accettazione in pagamento delle valute virtuali debbono allo stato ritenersi attività lecite; le parti sono libere di obbligarsi a corrispondere somme anche non espresse in valute aventi corso legale. Si richiama tuttavia l'attenzione sul fatto che le attività di emissione di valuta virtuale, conversione di moneta legale in valute virtuali e viceversa e gestione dei relativi schemi operativi potrebbero invece concretizzare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati*”¹⁴. In conclusione vi è da aggiungere che la necessità di pervenire ad un corretto inquadramento giuridico della questione è resa ancor più contingente dalla rapida espansione registrata dalla nota criptovaluta, sia sotto il profilo geografico, che sotto quello dei settori economici interessati¹⁵.

4. I principali profili di rischio connessi all'utilizzo di *Bitcoin*

¹² L'unica pronuncia nazionale che consta essere intervenuta in tema di *Bitcoin* è data dalla sentenza n. 195 pronunciata dalla Seconda Sezione Civile del Tribunale di Verona in data 24 gennaio 2017, in *Banca borsa tit. credito*, 2017, 4, pp. 469 e s., con nota di M. PASSARETTA, *Bitcoin: il leading case italiano*. Il Tribunale di Verona, mostrando adesione ad una non meglio identificata “attenta dottrina”, ha qualificato il *Bitcoin* come uno “strumento finanziario utilizzato per comp[er]ire una serie di particolari forme di transazioni online”.

¹³ Cfr. R. BOCCHINI, *op. cit.*, p. 35

¹⁴ *Avvertenza sull'utilizzo*, *cit.*, p. 2.

¹⁵ Esclusi alcuni Paesi in cui è stata bandita l'operatività in *Bitcoin* (es. Russia, Cina, Islanda, Ecuador e Vietnam), si assiste ad un riconoscimento sempre più diffuso della criptovaluta quale strumento di pagamento anche nell'ambito di ordinari esercizi commerciali. A tal riguardo non sorprenderà, data la sua notoria vocazione tecnologica, che la città di San Francisco (USA) si attesti tra le prime al mondo per numero di attività commerciali *Bitcoin-friendly*.

Le caratteristiche del *Bitcoin* rappresentano al contempo (ed a seconda della prospettiva adottata) punti di forza e di debolezza della criptovaluta *leader* del mercato valutario virtuale. Nelle pagine seguenti verranno quindi affrontate singolarmente le criticità del sistema in commento, approfondendo, ove necessario, le peculiarità dello stesso non ancora illustrate.

Come già si è avuto modo di anticipare, nel corso degli ultimi anni le principali Autorità nazionali ed europee hanno pubblicato *report* ed avvertenze concernenti i principali rischi correlati a diffusione ed utilizzo delle valute virtuali. Saranno dunque siffatti documenti a fungere da base di partenza e chiave di lettura per l'analisi delle problematiche sottese al mondo delle criptovalute. In via di premessa, bene allora specificare come il catalogo dei rischi evidenziati dalla Banca d'Italia, dall'UIF e dall'Autorità Bancaria Europea (EBA), sia da intendersi senza dubbio come un catalogo "aperto", da tenersi costantemente aggiornato al progredire della tecnologia e, con essa, delle "generazioni" di criptovalute¹⁶. Giova precisare inoltre che tutte le varie forme di rischio, per quanto singolarmente analizzate, risultano essere tra loro intimamente connesse, sicché la giustificazione della loro trattazione analitica va ricercata nel beneficio della chiarezza espositiva, rammentandosi purtuttavia che per investigare possibili soluzioni valide *pro futuro* occorre inevitabilmente dotarsi di una visione complessivo-sintetica del fenomeno.

4.1. L'altissima volatilità ed il rischio di "bolla speculativa"

A fungere da capofila di tutti i rischi sottesi all'operatività in criptovalute è indubbiamente quello di carattere finanziario. Il valore delle criptovalute (ed in particolar modo di *Bitcoin*) si caratterizza di fatti per l'elevato tasso di volatilità che, in uno con meccanismi di formazione dei prezzi alquanto "opachi", rende l'esito dell'investimento in valute virtuali piuttosto imprevedibile e rischioso. La forte volatilità incoraggia ed accresce inoltre fenomeni speculativi di cui l'andamento dei prezzi è immediato specchio (cfr. Fig. 1). Occorre poi tener presente che sul mercato sono reperibili strumenti finanziari derivati che, basandosi su un effetto moltiplicatore del loro sottostante, hanno la capacità di elevare a potenza il già consistente indice di volatilità delle criptovalute. Un investitore che decidesse quindi di acquistare un simile strumento, magari allettato dalla possibilità di lauti guadagni in breve tempo, si troverebbe esposto al rischio, quanto mai concreto ed attuale, di vedere polverizzato il proprio capitale di partenza. La drammaticità dello scenario è nondimeno rappresentata dal fatto che la natura "spericolata" di questo genere di operazioni venga spesso ignorata dai soggetti che le pongono in essere, i quali si affacciano sul mercato cripto-valutario sempre più sprovvisti delle necessarie competenze ed accortezze, attirati da pubblicità *online* tutt'affatto che trasparenti. Nei paragrafi successivi si tenterà perciò di porre in evidenza come il tutto sia in parte riconducibile anche ad un problema di informazione e comunicazione, in relazione al quale possono individuarsi diversi responsabili.

¹⁶ E' infatti la stessa Banca d'Italia ad ammonire gli utenti: "il fenomeno è soggetto a rapida evoluzione ed è possibile che valute virtuali di ultima generazione presentino rischi ulteriori rispetto a quelli illustrati" (cfr. *Avvertenza sull'utilizzo*, cit., p. 3).

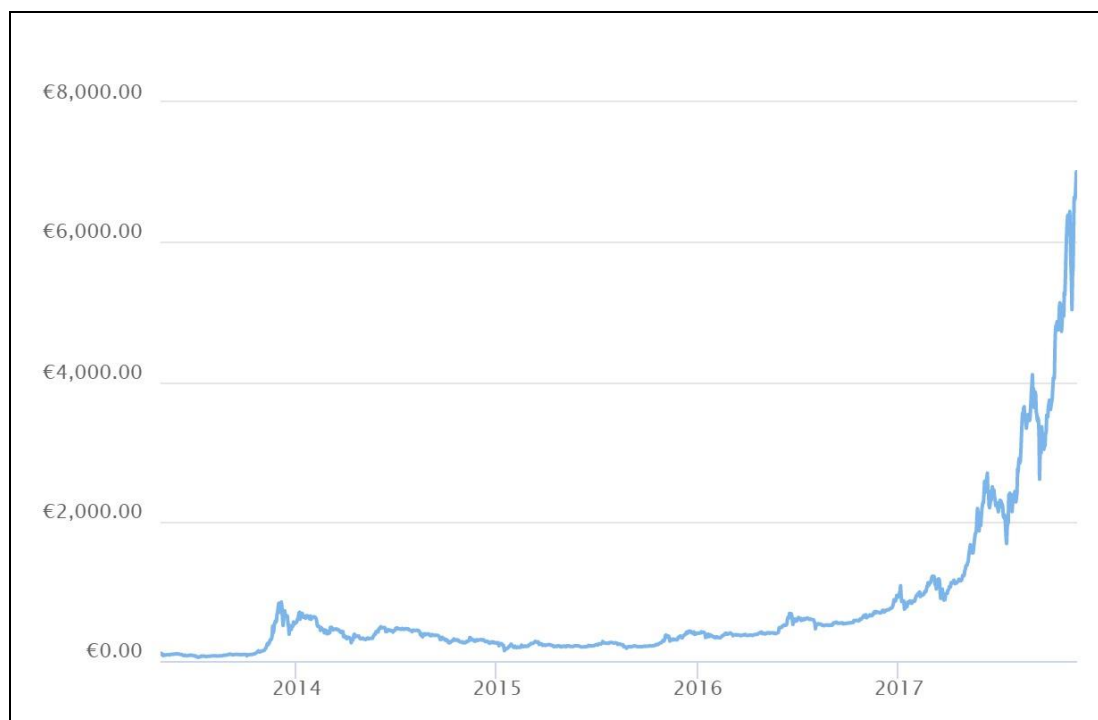


Fig. 1 – Andamento del valore di un Bitcoin espresso in Euro (al 21 novembre 2017)

La stampa (specializzata e non) si fa quotidianamente portatrice di ammonimenti sul pericolo di esplosione di una bolla nel mercato di cambio del *Bitcoin* con le principali divise mondiali¹⁷, segnalando come la criptovaluta in questione sia arrivata a registrare una capitalizzazione di mercato odierna superiore ai cento miliardi di Euro¹⁸. A voler adottare un approccio ottimistico si deve allora auspicare che un simile accrescimento dei volumi di contrattazione della criptovaluta induca i Paesi e le Autorità ad assumere sul fenomeno posizioni più nette di quelle registratesi sino ad ora, scongiurando (o quantomeno limitando) le drammatiche conseguenze che un'esplosione della bolla sicuramente provocherebbe. Peraltro, non è da escludersi che un simile intervento autoritativo possa fungere da acceleratore del temuto sgonfiamento dei prezzi, ove si consideri che un serio apparato regolamentare minerebbe le fondamenta dell'elemento che rende maggiormente appetibile il *Bitcoin*: l'anonimato¹⁹ (cfr. *infra* par. 4.3).

¹⁷ *Ex multis*, si veda l'intervista al premio Nobel per l'economia Robert Shiller apparsa sul quotidiano *Milano Finanza* del 21 ottobre 2017, pp. 20 e s.

¹⁸ Il fenomeno *Bitcoin* viene spesso paragonato dalla stampa alla celebre bolla speculativa sui prezzi dei bulbi di tulipano occorsa in Olanda nel XVII secolo.

¹⁹ Sul punto appare d'uopo richiamare l'attenta osservazione di R. BOCCHINI, *op. cit.*, pp. 44 e s., che riporta "un'osservazione ripetuta a più riprese da coloro che auspicano una regolamentazione, ma che al tempo stesso ne temono alcuni effetti 'collaterali'. Il timore è che una regolamentazione ricalcata sulle maglie di una attività come quella bancaria possa imbrigliare eccessivamente la caratteristica della duttilità propria delle monete virtuali. Nel considerare questi strumenti alla stregua delle monete elettroniche o nel riservarne l'emissione o intermediazione ai soli istituti autorizzati o addirittura alle Banche centrali, si porrebbe fine all'idea di assenza di emittente centralizzato, di assenza (o bassissimi)

Vi è poi da sottolineare un ulteriore aspetto connesso a questo primo rischio. Occorre infatti ricordare che, a differenza di quanto accade nei mercati finanziari tradizionali, quello delle criptovalute è noto per essere del tutto sprovvisto di regolamentazione e di presidi per i suoi operatori. Ne consegue che non esistano strumenti specifici di repressione di quelle condotte che, se tenute nell'ambito di un mercato regolamentato, sarebbero immediatamente additabili come abusive e manipolative e che invece, per essere perseguibili in tale contesto, andrebbero probabilmente ricondotte a fattispecie proprie della parte speciale del codice penale (quali ad esempio la truffa). La dottrina, sulla scorta della incerta qualificazione giuridica delle valute virtuali, si è spinta ad interrogarsi sulla possibilità di definire "investitori" i soggetti che effettuano operazioni in questo settore; il che rende senz'altro possibile saggiare quanto sia minato il terreno su cui sorge l'intero mercato cripto-valutario. Oltretutto, alla registrata penuria di mezzi punitivi si accompagna quella di strumenti deterrenti con funzione general preventiva in grado di dissuadere i consociati dal porre in essere operazioni fraudolente. Ciò che più sconcerta allora è che, nonostante i segnali di pericolo, si sia creata sul mercato una concezione del *Bitcoin* come "bene rifugio" tale da indurre sempre più soggetti a servirsi (impropriamente) della criptovaluta come riserva di valore in grado di "scudare" il capitale da una perdita di potere d'acquisto²⁰.

4.2. I rischi connessi all'assenza di tutela legale e contrattuale

Uno dei principali *handicap* scontati dai sistemi cripto-valutari è quello di essere pervasi da una generalizzata mancanza di informazione. I sopraccitati dubbi circa la reale identità del fantomatico inventore di *Bitcoin* costituiscono un lampante esempio dell'aura di mistero che avvolge l'intero settore. Se a ciò si aggiunge poi una mancanza di copertura giuridica che dia sostanza e forma al circuito *Bitcoin*, si addiuvine a quello che, a ragione, potrebbe ben definirsi un *far-west* commerciale²¹. Quello delle valute virtuali è un fenomeno subdolo: getta le sue basi nell'informatica, è oggetto di discussioni su *blog* e *forum online*, prolifera e si pubblicizza su internet (strumento

*costi per le transazioni che rendono i Bitcoin particolarmente attraenti, spingendo probabilmente allo sdoppiamento dell'attività degli emittenti tra quella "autorizzata" e quella illecita che si svolge sul c.d. 'deep internet'". L'autorevole opinione dell'insigne giurista Guido Rossi sembra confermare che l'assenza di controllo sia ben lungi dal rappresentare un limite per lo sviluppo della criptovaluta. Tutt'al contrario, spiegava invero Rossi tramite un audace parallelismo con gli strumenti derivati, "l'assenza di controlli in principio non ha impedito al sistema dei derivati di assumere rilevanza" (F. BISOZZI, *Bitcoin, parla Guido Rossi: 'è uno strumento rischioso, è come i derivati, può stravolgere le regole del capitalismo'*, 16 aprile 2013, disponibile su www.huffingtonpost.it).*

²⁰ Come noto la nozione di "bene rifugio" richiama invece caratteristiche assolutamente sconosciute al *Bitcoin* che non può dirsi né portatore di un intrinseco valore reale, né (tanto meno) in grado di mantenere un valore stabile nel lungo periodo. Ancora una volta, un'autorevole conferma in tal senso ci perviene dalla lettura che già dava del fenomeno Guido Rossi, quando affermava: "una volta che il metallo giallo ha iniziato a perdere vistosamente terreno sono venuti meno anche i Bitcoin, a dimostrazione del fatto che ci troviamo di fronte a un bene rifugio fasullo", avvertendo inoltre come i *Bitcoin* rappresentino oggi "degli strumenti finanziari di nuovo conio in grado di stravolgere le regole del capitalismo" (F. BISOZZI, *op. cit.*).

²¹ In merito, appare doveroso richiamare nuovamente il documento elaborato dall'EBA (*EBA Opinion on 'virtual currencies'*, *cit.*, p. 25), ove è dato di potersi leggere che "the regulatory and legal treatment of VCs is unclear and authorities may change their views unexpectedly, at short notice, and the view may not be communicated sufficiently".

oramai appartenente alla nostra quotidianità) trasmettendo così una sensazione di familiarità e di fiducia concretamente mal riposta atteso che sono assai pochi gli utilizzatori della rete che possano definirsi realmente esperti della materia informatica, specialmente ove questa si complichino fino a tradursi in concetti complessi quali sono appunto quelli di *Blockchain* e di *Transaction Chain*. L'immaterialità, la tecnologia, la rapidità, l'assenza di norme e di istituzioni costituiscono una miscela esplosiva che rende (volutamente) imperscrutabile ai più il reale funzionamento dell'ingranaggio. Eppure, "se comprendere è impossibile, conoscere è necessario". Per questo motivo si rendono urgenti i pareri e le avvertenze pubblicate dalle Autorità di riferimento con lo specifico obiettivo di mettere in guardia i meno avveduti.

Le operazioni di acquisto, scambio ed utilizzo delle valute virtuali non sono assistite da quelle tutele di natura legale o contrattuale che contraddistinguono tipicamente l'operatività in valuta legale²². Le transazioni in criptovalute sono tecnicamente irreversibili²³, generalmente non sono supportate né da un contratto né da procedure di reclamo e la reale identità della controparte rimane celata dietro lo pseudonimo scelto da ciascun utente al momento della registrazione²⁴. Come già precisato, l'emissione e la gestione di criptovalute (ivi compresa la loro conversione in divisa tradizionale) non sono inoltre attività soggette a vigilanza da parte della Banca d'Italia né di altra autorità italiana, il che espone gli utenti a rischi altissimi nei casi di condotta fraudolenta, di fallimento o anche semplicemente di cessazione di attività da parte delle piattaforme di scambio, ossia quei "luoghi" di necessaria frequentazione per il soggetto che voglia acquistare e/o rivendere criptovalute contro monete tradizionali. Gli ordinari strumenti di tutela sono poi parimenti assenti quando si tratti di somme denominate in valuta virtuale depositate presso enti terzi, come è stato ampiamente confermato dal noto caso del fallimento della piattaforma "Mt. Gox" avvenuto nel 2014²⁵. Siffatta vicenda, oltre a rivelare la quantità di connessioni esistenti tra criptovalute e diritto fallimentare transnazionale, ha fornito anche un'anteprima di quali e quante sarebbero le catastrofiche conseguenze di un collasso generalizzato del mercato cripto-valutario, rivelandone al contempo l'estrema fragilità. Fino al 2014, infatti, Mt. Gox (con sede a Tokyo) era una delle piattaforme più popolari ed utilizzate del *web* per le operazioni di cambio valuta (c.d. *online exchange*). Basti pensare che nel suo ultimo semestre di attività la suddetta gestiva all'incirca il 21% delle transazioni in *Bitcoin*, offrendo ai suoi clienti prestazioni assai simili a quelle proprie di una tradizionale banca presso cui sia

²² Cfr. R. BOCCHINI, *op. cit.*, p. 44, secondo cui è palese come "il vero caveat nel sistema di utilizzazione della moneta virtuale sia rappresentato proprio dall'assenza di una disciplina di settore che intervenga a regolare, già precedentemente a eventuali momenti patologici, i soggetti emittenti e, soprattutto, un eventuale coordinamento con i sistemi di produzione di valute legali".

²³ Non è dunque ammessa la possibilità di ripensamenti o correzioni che invece è generalmente contemplata dai servizi di *home banking* approntati dalle tradizionali banche, ove è possibile revocare disposizioni di pagamento (es. bonifici) per un certo lasso di tempo successivo all'inserimento dell'ordine.

²⁴ La Banca d'Italia specifica inoltre che "la mancanza di definizioni, di standard legali e di obblighi informativi renderebbe difficile provare in giudizio di aver subito un danno ingiusto". Avverte infine che "è possibile che l'utilizzo o la conversione di valute virtuali siano soggetti a costi e commissioni non chiaramente indicati" (cfr. *Avvertenza sull'utilizzo*, *cit.*, p. 3).

²⁵ Cfr. G. BOTTERO, *La Borsa dei Bitcoin getta la spugna. Mt. Gox corre verso la liquidazione*, apparso sul quotidiano *La Stampa* il 16 aprile 2014, disponibile sul sito www.lastampa.it.

possibile depositare fondi da lasciare in giacenza nell'attesa di compiere operazioni di *trading*²⁶.

A tal proposito va anzi aperta una piccola parentesi per specificare che esistono due modi per conservare i *Bitcoin*. Il primo (più sicuro) è dato dall'uso di un "portafoglio digitale" (*e-wallet*) salvato sul computer o sullo *smartphone* del singolo utente cui questi può accedere utilizzando le credenziali scelte personalmente al momento dell'apertura del "conto". Una soluzione alternativa consiste invece nel depositare le proprie sostanze su piattaforme di *online exchange* (quale era, per l'appunto, Mt. Gox) e questa seconda tecnica è connotata da un coefficiente di rischio certo elevato in quanto espone i "correntisti" a quello di insolvenza o cessazione di attività della piattaforma senza che vi siano coperture statali delle giacenze analoghe a quelle operanti a garanzia dei clienti degli istituti bancari tradizionali²⁷.

La mancanza di una forma di controllo accentrata ed istituzionalizzata espone (del resto) i detentori di *Bitcoin* a diversi ulteriori rischi: primo fra tutti quello di "perdere" la valuta virtuale archiviata nel portafoglio elettronico a seguito di malfunzionamenti o attacchi informatici²⁸. Non esistendo procedure di recupero delle credenziali di accesso al conto, persino lo smarrimento della *password* potrebbe inoltre produrre le più infauste conseguenze per il soggetto titolare, che si verrebbe così a trovare spogliato della possibilità di gestire le proprie risorse.

E' poi certamente da porre in evidenza che le interazioni tra valute digitali ed economia reale, ossia la possibilità di acquistare beni e servizi tramite la spendita di criptovalute in luogo di moneta avente corso legale, si innescano unicamente su di un'accettazione avente base volontaria. Pertanto, chi detiene somme denominate in criptovaluta non ha alcuna certezza di poterle utilizzare per gli scopi programmati, posto che l'accettazione di valute virtuali da parte di esercenti attività commerciali (o altre controparti) si fonda su accordi che possono esser revocati in qualsiasi momento e senza alcun preavviso.

Le incertezze ed i rischi creati per gli utenti dal vuoto normativo hanno così spinto la dottrina ad interrogarsi su di una possibile estensione analogica delle garanzie apprestate dalle normative in materia di trasparenza e di sorveglianza bancaria e finanziaria. L'ipotizzata estensione ha tuttavia incontrato un ostacolo (apparentemente)

²⁶ Il fallimento della piattaforma giapponese è stato addebitato ad un attacco informatico che ha portato ad una perdita di circa 750 mila *Bitcoin* di proprietà di migliaia di utenti. Al prezzo di mercato odierno il provento dell'attacco *hacker* equivarrebbe a più di quattro miliardi e mezzo di Euro.

²⁷ Come ha avuto modo di precisare Franco Cimatti (Presidente di Bitcoin Foundation Italia) nel corso di un'intervista concessa a *Wired.it*: "*Bitcoin non è fatto per avere conti in servizi terzi, ma per essere ognuno la banca di se stesso*" (<https://www.wired.it/attualita/tech/2014/02/26/mt-gox-fine-bitcoin/>). Bene anche precisare che quella di affidare le proprie somme alle piattaforme di *exchange* è generalmente la scelta prediletta da quei soggetti che acquistano *Bitcoin* con finalità speculative e che scelgono quindi di servirsi delle suddette piattaforme per sfruttare i servizi di *trading* offerti.

²⁸ Emblematico, oltre al sopramenzionato caso Mt. Gox, anche l'attacco perpetrato ai danni del progetto di raccolta fondi "*The DAO*", nel corso del quale sono stati sottratti dagli *hacker* più di 152 milioni di dollari. Il furto è stato perpetrato nel corso di una c.d. *Ico* (*Initial Coin Offering*), ossia quell'operazione attraverso cui un'azienda creatrice di una nuova valuta virtuale la offre in vendita al pubblico per la prima volta. Si segnala sul punto l'intervento di P. VIGNA, *Criptovalute, i segreti delle Ico*, apparso sul quotidiano *Milano Finanza* del 3 ottobre 2017, p. 4.

insormontabile nel presupposto richiesto per l'applicazione delle normative suddette: quello dell'esercizio dell'attività bancaria, che (ai sensi del primo comma dell'art. 10 del T.U.B.) consiste nella raccolta del risparmio tra il pubblico e nell'esercizio del credito. E' pertanto inevitabile propendere per un'esclusione dell'estensibilità analogica di tali normative al mondo *Bitcoin* in cui ancora non constano esserci soggetti esercenti attività bancaria in senso tecnico²⁹. Si ricordi infine che (come precisato dall'UIF) “*i prestatori di attività funzionali all'utilizzo, allo scambio e alla conservazione di valute virtuali e alla loro conversione da/in valute aventi corso legale non sono, in quanto tali, destinatari della normativa antiriciclaggio e quindi non sono tenuti all'osservanza degli obblighi di adeguata verifica della clientela, registrazione dei dati e segnalazione delle operazioni sospette*”³⁰.

Da ultimo, merita sottolineare che la generale incertezza imperante con riguardo sia all'origine che all'esatto funzionamento del sistema *Bitcoin*, rende pure doveroso un approccio diffidente verso lo stesso, che metta in guardia dal rischio che il fantomatico inventore, nel creare il sistema, abbia conservato per sé una posizione privilegiata rispetto a quella dei comuni utenti, tale cioè da consentirgli di intervenire e/o manipolare la rete in maniera discrezionale e arbitraria. Insomma, la diffusa opacità del sistema non consente di escludere con certezza l'esistenza di insidie nascoste che minino la sicurezza e la trasparenza delle operazioni, con ulteriore incremento dei rischi per gli utenti e per l'intero mercato.

4.3. L'anonimato e le finalità illecite

Prima di analizzare i rischi derivanti dagli usi illeciti del sistema *Bitcoin* che vengono favoriti dalle caratteristiche strutturali proprie di quest'ultimo, è utile effettuare ancora qualche pur rapida considerazione preliminare. Il progresso tecnologico è stato infatti ormai da tempo individuato dai criminali come valido alleato per compiere in maniera sempre più sofisticata le più disparate tipologie di illeciti. Tramite i comuni servizi bancari *online* che consentono di scambiare denaro senza alcuna interazione reale il malaffare è in grado di porsi a distanza di sicurezza dalle proprie attività delittuose. Sovente per accedere ai servizi offerti dagli istituti bancari e finanziari si rende tuttavia necessario superare una procedura di autenticazione tesa ad identificare i soggetti coinvolti nella transazione. Ebbene, al fine di sabotare l'efficacia di tali protocolli identificativi i criminali informatici hanno elaborato alcuni *escamotage* atti ad offuscare la reale identità dell'operante attraverso la cosiddetta tecnica di “*spoofing*”, che mette il pirata informatico nella condizione di poter falsificare l'indirizzo “IP”³¹ o addirittura di servirsi abusivamente di profili in uso ad altri utenti, rendendo così impossibile l'identificazione di chi si celi realmente dietro una certa attività.

²⁹ Sul punto cfr. R. BOCCHINI, *op. cit.*, p. 44. Meritevole di menzione è anche il già citato documento *EBA Opinion on 'virtual currencies'*, p. 29, ove si sottolinea che la mancanza di regolamentazione espone gli utenti *Bitcoin* all'elevato rischio di incorrere in un c.d. schema Ponzi: “*the nature of VCs leaves investors more vulnerable to abuse by a Ponzi scheme based on VCs than other, regulated forms of investments. Finally, the user may have no access to redress schemes*”.

³⁰ Cfr. l'informativa diffusa dall'UIF, “*Utilizzo anomalo di valute virtuali*”, p. 1.

³¹ L'indirizzo IP è un codice numerico che serve ad identificare e localizzare in maniera univoca ogni computer o dispositivo connesso ad una rete. Per quanto debba ritenersi impossibile navigare in internet senza un indirizzo IP, è comunque possibile rinvenire nei *web* strumenti di navigazione che consentono di camuffarlo, in modo tale che il dispositivo risulti ubicato in un'altra città o addirittura in un altro Paese.

In siffatto contesto l'avvento delle criptovalute ha dunque consentito di consolidare meccanismi di perpetrazione del *cybercrime*³² già esistenti, rendendoli addirittura più efficaci grazie alla sicurezza garantita dal regime di anonimato in cui è possibile scambiare le valute virtuali³³. Come già si è avuto modo di accennare (cfr. *supra* par. 4.1), la caratteristica che infatti maggiormente contraddistingue (e rende appetibile) l'utilizzo delle criptovalute è proprio quella di poter effettuare transazioni nel più completo anonimato. Adottando alcune semplici precauzioni gli utilizzatori di *Bitcoin* possono invero tutelare la propria *privacy* in maniera efficace, così da evitare di essere identificati ed identificabili³⁴. E' bene allora non confondere il concetto di "anonimato" con quello di "tracciabilità", atteso che, come sopra analizzato, il sistema mantiene traccia di tutte le transazioni effettuate tramite gli strumenti della *Transaction Chain* e della *Blockchain*. Per mezzo di questi due registri il sistema è infatti in grado di memorizzare ogni transazione insieme all'indirizzo di chi l'ha disposta, ma "gli indirizzi sono per definizione anonimi"³⁵.

La stampa quotidiana rende poi ancor più manifesto che una simile tecnologia presti il fianco ad utilizzi e finalità illecite, con sicuro aggravio dei già difficili compiti repressivi affidati ad autorità giudiziarie e fiscali di tutto il mondo³⁶. E' celebre il caso

³² Quello del *cybercrime* è considerato un "settore della criminalità che opera prevalentemente attraverso 'attacchi' ed azioni di tipo informatico, considerati spesso alla stregua di un 'quasi crimine' a causa della loro natura apparentemente non violenta e la percezione di 'distanza' dovuta all'utilizzo del mezzo telematico" (così E. SIMONCINI, *op. cit.*, p. 898). Per completezza, si precisa che all'interno della macrocategoria dei crimini informatici è possibile individuare due sottocategorie: quella dei "computer crimes" e quella dei "computer facilitated crimes". Nella prima i computer rappresentano gli obiettivi della condotta illecita; nella seconda questi (ed in generale la rete informatica) costituiscono gli strumenti attraverso cui realizzare il reato.

³³ Sul punto, si rimanda a D. BRYANS, *Bitcoin and Money Laundering: Mining for an Effective Solution*, in *Indiana Law Journal*, 2014, 89, pp. 441 e s., ove si legge che le "new virtual currencies, such as Bitcoin, add yet another layer of anonymity by allowing users to transfer value without the collection of any personally identifiable information. Regulations often fail to affect such virtual currencies due to lack of foresight by the regulation writers, creating a legal grey area. Thus, criminals can continue to capitalize on technological innovation to bolster their illegal activities".

³⁴ *Ex multis*, cfr. N. MANCINI, *op. cit.*, p. 136, in cui si chiarisce che "ciascun utente può avvalersi [...] di tanti pseudonimi quanti possono essere i wallets dei quali è titolare senza inviare ad alcun Paese i propri dati identificativi. Ciò risulta possibile poiché le transazioni non necessitano dell'intervento di intermediari, bancari e assimilati, la cui assenza impedisce di fatto che l'utente venga identificato e che i dati dei trasferimenti siano trasmessi all'autorità di uno Stato".

³⁵ R. BOCCHINI, *op. cit.*, p. 45. Per una conferma cfr. anche E. SIMONCINI, *op. cit.*, pp. 907 e s., ove si legge che "gli indirizzi Bitcoin non contengono alcuna informazione che possa consentire alle autorità investigative di individuare i legittimi titolari, siano essi persone fisiche o giuridiche, garantendo loro il completo anonimato" e N. M. KAPLANOV, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation*, in *Temple Law Review*, marzo 2012, p. 5, disponibile sul sito www.ssrn.com, in cui è ben spiegato come a ciascun *account* (indirizzo) sia abbinata una firma criptografica conosciuta dal solo titolare del "conto", mediante la quale quest'ultimo può autorizzare le transazioni in entrata ed in uscita ("At the same time, the payor uses her own private key to approve the payment to the recipient's account. Essentially, the public key is like an email address – public and available to everyone – while the private key is like the password needed to authorize messages (in this case bitcoins) to go in and out").

³⁶ Si veda, ad esempio, l'articolo di R. GALULLO comparso su *Il Sole24Ore* del 29 settembre 2017, *Hackeraggio e ricatto in bitcoin, primi arresti*, in cui si tratta della c.d. inchiesta "virtual money", una delle prime importanti indagini italiane sull'utilizzo della criptovaluta come mezzo di pagamento di riscatti. Più in particolare, secondo i risultati dell'indagine sarebbe stata rintracciata un'organizzazione

“*Silk Road*”, noto sito *web* del mercato nero *online* (c.d. *deep web*), sul quale sono state stimate transazioni per circa 10.000 *Bitcoin* al giorno (corrispondenti al 5% dell’operatività globale in *Bitcoin*) finalizzate all’acquisto di armi, sostanze stupefacenti ed altri beni e servizi illeciti³⁷. Ad ogni modo, l’acquisto di beni e servizi illeciti non costituisce l’unico utilizzo preoccupante della criptovaluta, che viene sovente prostrata alla commissione di reati quali il riciclaggio, l’autoriciclaggio e l’evasione fiscale.

4.3.1. Il “*cyberlaundering*”

L’espressione *cyberlaundering* deriva dalla fusione dei termini *cyber* (coniato dalla letteratura fantascientifica negli anni ’80 del secolo scorso) e *laundering* (ossia “lavanderia/lavaggio”, comunemente utilizzato nel mondo di *common law* in associazione alla parola *money* per indicare il riciclaggio di denaro sporco – *money-laundering*). L’avvento dei computer e della rete internet ha indubbiamente rappresentato un punto di svolta per le ordinarie tecniche di riciclaggio di denaro proveniente da attività illecite, costituendone occasione di semplificazione ed ulteriore diffusione.

Tradizionalmente l’attività di riciclaggio si compone di tre distinte fasi: il c.d. *Placement-stage* (collocamento); il *Layering-stage* (lavaggio) ed infine l’*Integration-stage* (reintroduzione del capitale pulito nell’economia legale). Come si vedrà, la rivoluzione informatica ha inciso in maniera profonda su tutte siffatte fasi, arrivando (in taluni casi) a renderne addirittura superflue alcune. In quest’ottica il *cyberlaundering* può tradursi concretamente in due forme: il “riciclaggio digitale strumentale” ed il “riciclaggio digitale integrale”. La principale differenza consiste nel fatto che “*nel cyberlaundering integrale, a differenza di quello strumentale, la fase di Placement si caratterizza per l’inserimento nel circuito legale dell’economia di capitali di provenienza illecita che già risultano disponibili su conti on-line allo ‘stato digitale’, senza la necessità di alcun contatto materiale tra il riciclatore ed il contante*”³⁸. Dunque, se nel *cyberlaundering* “strumentale” l’apporto tecnologico può inserirsi nella procedura facilitando qualche passaggio, in quello “integrale” il riciclatore è in grado di portare a termine l’intero procedimento di pulitura per mezzo di un’unica operazione effettuata nell’anonimato del mondo virtuale, riducendo così drasticamente i rischi connessi a tale attività e rendendo spesso superflui ulteriori passaggi. In generale, si può affermare che l’operazione di “lavaggio” risulti quella maggiormente facilitata

criminale che inviava virus informatici a computer di privati ed aziende, paralizzandoli. Per rientrare in possesso dei propri dati le vittime avrebbero dovuto pagare una certa somma in *Bitcoin* da acquistarsi sul sito internet di una delle più importanti società di compravendita di criptovaluta che, sempre secondo gli accertamenti dell’inchiesta, avrebbe funto da vertice dell’intera organizzazione criminale.

³⁷ Cfr. N. MANCINI, *op. cit.*, p. 135, ove si fa menzione del citato caso, rammentando che “*al fine di frenare tale utilizzo dei bitcoin, le autorità statunitensi hanno chiuso il sito Silk Road e sequestrato i 170.000 bitcoin dei quali il titolare, nonché fondatore, del sito, Ross Ulbricht, era in possesso, in quanto considerati quali profitto derivante dalle transazioni compiute sulla piattaforma tra il febbraio 2011 e il luglio 2013. La chiusura del sito non ha tuttavia frenato l’utilizzo dei bitcoin, il cui valore, dopo una caduta a picco nel giorno in cui il sequestro venne eseguito, è tornato nuovamente a crescere*”. Per un resoconto sulla tipologia di beni scambiati sul mercato nero, si rimanda ad A. DE SIMONE, *Droga, armi, minori e killer: viaggio nel deep web. Dove tutto è possibile*, 12 aprile 2012, disponibile su www.corriere.it.

³⁸ Cfr. E. SIMONCINI, *op. cit.*, pp. 900 e s.

dall'avvento del *web*, che pure ha già sensibilmente arricchito il catalogo delle attività di “pulitura”³⁹ disponibili.

E' dunque manifesto che il settore del *cyberlaundering* rappresenti un terreno assai fertile per il proliferare degli usi illeciti del *Bitcoin* e, più in generale, delle valute virtuali. Basti considerare che la conversione della provvista illecita (ad esempio provento di evasione fiscale) in valute virtuali (a loro volta suscettibili di ulteriore negoziazione) ostacola l'identificazione della provenienza delittuosa, integrando così la fattispecie di riciclaggio *ex art. 648-bis c.p.* Occorre poi tenere a mente che con l'adozione della legge 186/2014 e, dunque, con l'introduzione dell'*art. 648-ter1 c.p.* (Autoriciclaggio), il legislatore ha inteso sottoporre a sanzione penale anche l'“autoriciclatore”, ossia quel soggetto che, “*avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa*”. Bene rammentare peraltro che tra le principali novità introdotte dalla legge 186/2014 vi è anche la modifica dell'*art. 25-octies* del d.lgs. 231/2001, tradottasi nell'inclusione del nuovo delitto di autoriciclaggio tra i reati presupposto della responsabilità amministrativa da reato degli enti⁴⁰.

Preme infine evidenziare che il d.lgs. 231/2007 (c.d. legge antiriciclaggio) non contempla in alcuna delle categorie⁴¹ di cui agli artt. 10 e ss. i soggetti che operano a vario titolo nel settore delle criptovalute. Ne deriva che i soggetti esercenti un'attività connessa all'utilizzo, allo scambio, alla conservazione o alla conversione di valute virtuali in moneta legale, andando esenti dall'applicazione della normativa antiriciclaggio, non sono tenuti all'osservanza degli obblighi di adeguata verifica della clientela, alla registrazione dei dati e alla segnalazione delle operazioni sospette all'UIF⁴².

Insomma, il sistema *Bitcoin* può davvero rappresentare un “paradiso virtuale” in cui andare impuniti grazie al completo anonimato garantito in egual misura al piccolo criminale come alla grande società. Ciò nondimeno, si è obiettato che l'anonimato

³⁹ Si pensi, ad esempio, alla possibilità di accendere conti correnti bancari anonimi, di costituire servizi di *hot-line* telefoniche, oppure ancora quella di ricorrere a siti e piattaforme di gioco d'azzardo *online*.

⁴⁰ La dottrina si è interrogata sulla possibilità di servirsi della fattispecie di cui all'*art. 648-ter1 c.p.* per includere alcuni reati tributari nel novero dei reati presupposto *ex d.lgs. 231/2001*. Un limite in tal senso è (come noto) dato dal requisito dell'idoneità in concreto della condotta a camuffare l'origine delittuosa della provvista illecita. Nondimeno, ogniqualvolta l'amministratore di una società effettui, nell'interesse o a vantaggio di quest'ultima, operazioni distrattive (anche *online*) volte a mascherare l'illecita provenienza della *res*, sarà possibile estendere anche all'ente la nuova fattispecie di “*self-laundering*”. Sul punto, si veda più diffusamente E. SIMONCINI, *op. cit.*, pp. 912 e s.

⁴¹ *Id est* società di gestione, intermediari finanziari, professionisti, revisori contabili ed altri.

⁴² Cfr. *supra*, par. 4.2, nota 25. Da rammentare quanto affermato dalla Banca d'Italia, ossia che nel nostro Paese “*l'acquisto, l'utilizzo e l'accettazione in pagamento delle valute virtuali debbono allo stato ritenersi attività lecite; le parti sono libere di obbligarsi a corrispondere somme anche non espresse in valute aventi corso legale. Si richiama tuttavia l'attenzione sul fatto che le attività di emissione di valuta virtuale, conversione di moneta legale in valute virtuali e viceversa e gestione dei relativi schemi operativi potrebbero invece concretizzare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati*” (cfr. *Avvertenza sull'utilizzo, cit.*, p. 2).

(meglio lo “pseudonimato”) sarebbe in grado di operare solo fin quando l’utente non decida di convertire la criptovaluta in divisa avente corso legale con accredito diretto in conto corrente bancario dall’intestazione conosciuta o comunque conoscibile dalle autorità. Critica certo non destituita di fondamento giacché l’opera di intermediazione di un istituto bancario è senz’altro idonea a ripristinare una riconducibilità soggettiva della transazione. I *cyber*-criminali possono tuttavia spesso fare affidamento sulla disponibilità di conti correnti intestati a soggetti “prestaconto” (c.d. “*money mule*”), che, una volta ricevuto l’accredito delle somme, procedono al loro incasso e successivo trasferimento al reale destinatario⁴³.

4.4. Alcuni profili “residuali”

Quelle esposte nei paragrafi precedenti costituiscono le maggiori criticità proprie del sistema *Bitcoin*. Esistono poi alcuni profili residuali che, ancorché non preminenti, sono comunque meritevoli di menzione. Si tratta, in primo luogo, di quello che una certa dottrina ha definito come “rischio di sviamento della concorrenza”, consistente nel fatto che il sistema *Bitcoin* avrebbe “*aperto il mercato a (moltissimi) prestatori di servizi di pagamento, i quali, in assenza di vincoli normativi, riescono ad alleggerirsi di maggiori costi operativi e ad offrire trasferimenti di fondi a prezzi più bassi*”⁴⁴, alterando così i tradizionali assetti concorrenziali di mercato. Un ulteriore ed interessante aspetto potrebbe poi scaturire dalla lettura del caso *Bitcoin* come un fenomeno sociale esplosivo in un contesto storico di profonda sfiducia nel sistema economico e nelle relative istituzioni. Il *Bitcoin* interpretato dunque come “filosofia di ribellione” a quell’*establishment* verso cui il cittadino medio, in un prolungato periodo di crisi finanziaria, ha maturato un’insofferenza sempre crescente. In tal senso la congiuntura economica sfavorevole potrebbe contribuire al successo della moneta virtuale alimentando la preferenza per un sistema in cui le transazioni si perfezionino senza il necessario intervento di istituti di credito.

5. Cenni per alcune brevi riflessioni conclusive

Le criptovalute costituiscono paradigmatica dimostrazione di quanto sia difficile operare un equo bilanciamento tra sicurezza e libertà nella società attuale. La diffusione su scala mondiale delle monete virtuali ha fatto emergere con grande prepotenza la necessità di una loro regolamentazione, senza però che vi sia ancora unanimità di vedute sulle concrete modalità di intervento. Tra le varie proposte registrate in dottrina si annovera invero anche l’introduzione di un’obbligatoria procedura identificativa per le transazioni oltre un certo valore-soglia, ed attraverso le quali attestare la riconducibilità della transazione al titolare del portafoglio digitale. A parere di chi scrive, siffatta proposta sconta nondimeno il limite dell’essere facilmente eludibile, consentendo di andare esenti da identificazione tramite una semplice “frammentazione” delle transazioni che risultino così, singolarmente considerate, al di sotto del valore limite. Ciò che allora varrebbe forse a rendere il *Bitcoin* uno strumento meno promiscuo sarebbe una procedura di registrazione ed identificazione obbligatoria per chiunque

⁴³ Precisa E. SIMONCINI, *op. cit.*, p. 901, che un prestaconto “*potrebbe anche essere un’identità virtuale fittizia, creata mediante la produzione di un documento falso usato per intestare il conto di appoggio*”.

⁴⁴ Così R. BOCCHINI, *op. cit.*, p. 43, che soggiunge come il *Bitcoin* si sia attestato tra i primi dieci *network* di *e-payment* al mondo, dopo Visa, Mastercard, Paypal, ecc.

voglia creare un portafoglio digitale; ossia, non subordinare la tassativa *disclosure* dell'identità all'inserimento di un ordine dal controvalore particolarmente elevato, ma prevederla come *condicio sine qua non* per poter operare in generale sul sistema *Bitcoin*. E' manifesto come la vera insidia derivi dalle implicazioni che un simile obbligo importerebbe, non ultima quella di individuare un soggetto preposto al controllo della veridicità dei dati forniti. Peraltro, andrebbe ponderata altresì la ricaduta che una simile regolamentazione produrrebbe sul corso dei prezzi di *Bitcoin*, che, come detto, trova nell'anonimato una delle proprie principali "giustificazioni". Si consideri poi che la diffusione globale raggiunta dalle criptovalute renderebbe necessario un coordinamento legislativo tra molti Paesi, giacché ad un disallineamento normativo conseguirebbe la nascita di nuovi "paradisi" in cui poter operare a condizioni vantaggiose, con conseguente frustrazione degli sforzi normativi.

Le criptovalute sono allora da demonizzare in assoluto? Se regolamentate e "domate" potrebbero addirittura rappresentare, grazie alla tecnologia *Blockchain*, il più efficace alleato nella lotta all'evasione fiscale. La rete ed i suoi prodotti rappresentano il futuro e non è certo osteggiandoli che si potranno eliminare (o quanto meno attenuare) i rischi connessi. Le difficoltà sorgono dalla complessità delle realtà fattuali ancora non sufficientemente esplorate e comprese. La maturazione del momento per nuovi interventi normativi necessita perciò di una migliore e più completa comprensione delle realtà, manifesto essendo che una normativa necessita della comprensione dei fatti e quindi delle fattispecie da disciplinare (tanto più se da sanzionare anche penalmente).