INFORMATICA GIURIDICA
Collana diretta da Giovanni Ziccardi e Pierluigi Perri

4

Stefano Capaccioli

Criptovalute e bitcoin: un'analisi giuridica

MVLTA PAVCIS AG
GIUFFRÈ EDITORE

Sezione non inclusa

PROLOGO

— Che cosa è il *bitcoin*? (1)

— È una moneta virtuale.

— Sì, ho capito! Ma chi ci sta dietro il *bitcoin*?

— Nessuno.

— Che cosa si intende per nessuno? Qualcuno deve controllarla...

— Nessuno. È un algoritmo.

— Che cosa? Vuoi dire come Terminator? Il mondo quindi sarà gestito solo da macchine?

— Beh, non il mondo, ma forse alcune attività.

— Giusto... (alzando gli occhi) Ma chi controlla l'algoritmo? Qualche scienziato pazzo?

— Si tratta di un progetto *open source* (codice libero).

— Un codice... cosa?

— Sì, codice libero, *open source*. Un programma che può essere scaricato liberamente da *Internet* e farne ciò che vuoi.

— Quindi non c'è bisogno di pagare per il "programma"?

— È gratis perché libero, più dell'aria.

— Che cosa significa?

— Il codice non è solo libero nel senso che è possibile utilizzare il programma gratuitamente. È anche libero nel senso che si può prendere il codice, modificarlo e rilasciare un proprio programma partendo dal *software*.

— Aspetta un secondo! Se posso farlo, allora posso fare i miei *bitcoin*. Che valore ha un *bitcoin* allora?

— No, non è possibile emettere *bitcoin*. Quello che si può fare è inventarsi una nuova valuta. E poi devi provare a fartela accettare dagli altri.

---

(1) Il presente prologo è un adattamento di quello presentato da P. Franco, *Understanding Bitcoin*, Wiley & Sons, 2015.

— Oh, ma questo sarà sicuramente la fine del *bitcoin*. Se riesci a fare il maggior numero di monete, nessuna di loro avrebbe avuto alcun valore.

— Le valute hanno valore a causa delle convenzioni sociali. Il *bitcoin* ha valore perché le persone sono disposte a dare valore ad esso.

— Non credo che tu abbia ragione. Gli Euro o i dollari hanno un valore, lo sanno tutti.

— Beh, se i *bitcoin* non hanno valore sarò lieto di accettare i tuoi *bitcoin* (sorride).

— I *bitcoin* non sono garantiti da nulla e nessuno e perciò non possono avere un valore.

— Né gli euro, né i dollari né i *bitcoin* sono garantiti. Si può dire che tutti sono il frutto di un'allucinazione consensuale. Essi hanno valore perché le persone gli danno valore. Non c'è molta differenza tra loro rispetto al loro valore.

— Non la penso così! È possibile comprare le cose con gli euro o dollari, ma cosa si può acquistare con i *bitcoin*?

— È possibile acquistare quasi tutto con *bitcoin*. Ci sono aziende che accettano *bitcoin* in cambio di valuta a corso legale ed è possibile utilizzare i *bitcoin* per comprare qualsiasi cosa. La conversione di *bitcoin* in valuta a corso legale è solo un'interfaccia tecnica e molte aziende offrono questo servizio. Inoltre, è possibile fare le stesse cose con i *bitcoin* che si possono fare con le valute a corso legale.

— Tipo?

— Per esempio, si può lanciare una campagna di *crowdfunding* attraverso la creazione di un particolare tipo di transazioni *bitcoin*.

— Sembra interessante.

— Ci sono molte altre applicazioni che sono state fino ad oggi impossibili, come ad esempio gestire la proprietà di un bene direttamente dalla rete. Se si desidera acquistare il bene, basta pagare il proprietario con *bitcoin* e il bene diventa automaticamente di tua proprietà perché risulta immediatamente dal database di *Bitcoin*. E ci potrebbero essere ulteriori applicazioni a cui nessuno ha ancora pensato, come del resto con *Internet*.

— Non ci avevo pensato in questo modo.

— Come si suol dire, la valuta è solo la prima applicazione. La tecnologia permette di trasferire il valore in modo sicuro e decentrato e questo può portare a molte nuove applicazioni.

— Quindi il *bitcoin* sarà il futuro?

— E chi lo può dire: è solo un'innovazione dirompente ai suoi albori.

— Sono incuriosito. Mi piacerebbe saperne di più.

— Ottimo! Credo di avere il libro giusto per te...

INTRODUZIONE

SOMMARIO: 1. Le criptovalute. — 2. Prime valute virtuali. — 3. Valuta Virtuale e Valuta Digitale.

1. *Le criptovalute.*

Lo sviluppo dirompente dei sistemi di comunicazione sta portando numerose innovazioni tecniche, tecnologiche e concettuali che scuotono irrimediabilmente gli assiomi e postulati posti a basi di alcune costruzioni giuridiche.

Le criptovalute, monete digitali decentralizzate basate sulla crittografia costituiscono una di queste innovazioni, rispondendo sia alla crisi del sistema finanziario del 2007 sia all'esigenza di una unità di conto legata al mondo oramai interconnesso.

Detta innovazione, differentemente dal *crowdfunding* (1), porta con sé un'immagine distorta da parte degli organi di informazione che hanno sottolineato alcuni aspetti "criminali" (2), fondamentalmente per due ordini di motivi: *i*) scarsa conoscenza del mondo delle valute matematiche che richiede conoscenze tecniche e molto approfondimento *ii*) volontà di sottolineare gli aspetti pruriginosi e pericolosi per aumentare l'interesse dei lettori.

Spesso capita di ricevere domande (3): i *bitcoin* (4) sono illegali?

---

(1) Il *crowdfunding* (dall'inglese *crowd*, folla e *funding*, finanziamento) o finanziamento collettivo in italiano, è un processo collaborativo di un gruppo di persone che utilizza il proprio denaro in comune per sostenere gli sforzi di persone e organizzazioni. È una pratica di micro-finanziamento dal basso che mobilita persone e risorse. Vedi: K. DE BUYSERE, O. GAJDA, R. KLEVERLAAN, D. MAROM, (2012) *A Framework for European Crowdfunding*, http://evpa.eu.com/wp-content/uploads/2010/11/European_Crowdfunding_Framework_Oct_2012.pdf (sito web consultato, e documento disponibile online, il 7 marzo 2015).

(2) Vedi oltre i casi *E-Gold, Liberty Dollars* e *Silk Road*.

(3) C. DUHAIME, *Bitcoin: Virtual Currency, Legal Realities*, in Corporate Risk Canada, August 2014, http://www.duhaimelaw.com/wp-content/uploads/ 2014/08/

Sono utilizzati per riciclare? Sono un "*Ponzi Scheme*" (5)? Sono utilizzati solo per fine criminale? Queste domande rivelano il problema unico che le criptovalute incontrano: la conoscenza degli italiani sulla moneta digitale decentralizzata sembra essere basata sulla finzione piuttosto che sulla realtà. Le nuove valute digitali (come il *bitcoin*) sono una tecnologia globale prorompente e in evoluzione, con una velocità cinque volte maggiore del tempo di reazione aziendale o governativo.

Certamente è difficile tenere il passo dell'evoluzione, partendo proprio dall'assenza di qualsivoglia base giuridica, rischiando di perdere investimenti e di non mitigare i rischi che tali nuovi strumenti introducono.

Il nostro obiettivo è quello di descrivere questo mondo con equidistanza e professionalità per individuare i caratteri distintivi e poi procedere a interpretazione giuridica. Per rappresentare detto mondo occorre ripercorrere la storia di tali criptovalute, gli utilizzi, i vari documenti usciti per poi procedere ad individuare linee interpretative dotate di coerenza e consistenza.

Sottolineiamo fin da ora che le criptovalute non cadono in un vuoto giuridico, non sono fuori dal mondo del diritto e riteniamo non necessaria una legiferazione particolare in quanto le regole esistono e, pur con qualche difficoltà, vanno applicate. L'introduzione di normative specifiche rischia di infrangersi contro la natura "anarchica",

---

Duhaime-Digital-Finance.pdf (sito web consultato, e documento disponibile online, il 7 marzo 2015).

(4) Il *bitcoin* è la prima criptovaluta apparsa. Vedi *infra*.

(5) Lo schema Ponzi (o Ponzi Scheme) è un modello economico di truffa che promette forti guadagni alle vittime a patto che queste reclutino nuovi "investitori", a loro volta vittime della truffa (variante della Catena di Sant'Antonio). La tecnica prende il nome da Charles Ponzi, un immigrato italiano negli Stati Uniti che divenne famigerato per avere applicato una simile truffa su larga scala nei confronti della comunità di immigrati prima e poi in tutta la nazione. Ponzi non fu il primo a usare questa tecnica, ma ebbe tanto successo da legarvi il suo nome. Con la sua truffa coinvolse infatti 40 000 persone e, partendo dalla modica cifra di due dollari, arrivò a raccoglierne oltre 15 milioni. Le caratteristiche tipiche sono: *i*) promessa di alti guadagni a breve termine; *ii*) ottenimento dei guadagni da escamotage finanziari o da investimenti di "alta finanza" documentati in modo poco chiaro; *iii*) offerta rivolta, all'epoca in cui fu architettata la truffa, ad un pubblico non competente in materia finanziaria; *iv*) investimento legato ad un solo promotore o azienda. Si veda anche K. Basu, *Ponzis: The Science and Mystique of a Class of Financial Frauds*, World Bank, Policy Research Working Paper, WPS6967, July 2014 che evidenzia in maniera chiara: "*Contrary to a widely-held opinion, Bitcoin is not a deliberate Ponzi*".

decentralizzata e polimorfa del nuovo strumento, nato per esistere senza una regolamentazione specifica.

L'analisi svolta in tale scritto prescinde da giudizi sulla validità dello strumento e sulla prognosi di successo di tali strumenti ma per porre le basi interpretative in tale nuovo paradigma (6).

2. *Prime valute virtuali.*

I sistemi di comunicazione e l'interconnessione derivante dalla rete hanno modificato gli schemi concettuali ed il modo di vivere, creando nuovi sistemi sociali in continua evoluzione e rivoluzione, con problematiche derivanti dalla a-territorialità di *Internet* e dalla presenza di un sistema totalmente interconnesso.

Lo stesso *Web* si è trasformato nel corso del tempo: concepito inizialmente per collegare tra di loro vari documenti ipertestuali statici, si è evoluto partendo dalla definizione di *Web* 1.0, afferente al paradigma del *Web* statico. Attraverso l'utilizzo di nuovi linguaggi di programmazione la relazione tra utente e *Web* si è modificata, passando da un atteggiamento passivo ad uno attivo, cambiando l'approccio filosofico e giungendo all'utente che è al tempo stesso fornitore di contenuti (*Web 2.0*, fatto di *wiki*, *social network*, *blog*, *feed*, etc.). Le ulteriori tendenze sono sotto gli occhi di tutti con una propensione ad integrare, concentrare e decentralizzare nello stesso tempo,

In tali evoluzioni sono apparsi "mondi virtuali" interattivi, giungendo ai MMPORG ("*Massive Multiplayer Online Role-Playing*"), giochi di ruolo svolti in rete contemporaneamente da più persone. Alcuni famosi sono *War of Warcraft*® (7) *e Second-Life*® (8).

---

(6) Occorre altresì ricordare che anche i motori di ricerca furono una profonda innovazione ma non è che il primo strumento introdotto abbia prevalso nella competizione, ma può porre le basi per lo sviluppo di un nuovo strumento virale. Non per altro pochi si si ricordano di *Aliweb* (primo motore di ricerca), di *Mozaic* (primo *browser*) o di *Friendster* (primo *social network*).

(7) *World of Warcraft* (letteralmente "il mondo di *Warcraft*", spesso abbreviato in WoW) è un videogioco *fantasy* tridimensionale di tipo MMORPG, giocabile esclusivamente con l'utilizzo di *Internet* e con il pagamento di un canone. Sviluppato dalla Blizzard Entertainment, è stato pubblicato il 23 novembre 2004. *World of Warcraft* è il MMORPG più giocato al mondo, con circa 7 milioni di iscrizioni attive. (Fonte: Wikipedia).

(8) *Second Life* è un mondo virtuale elettronico digitale online lanciato il 23 giugno 2003 dalla società americana Linden Lab a seguito di un'idea del fondatore di

L'evoluzione di tali "mondi" è giunta fino alla creazione di vere e proprie economie virtuali e di sistemi sociali che hanno portato l'interprete giuridico a individuare le norme del diritto positivo applicabili a tali situazioni e a enucleare le norme di riferimento, pur nella consapevolezza che *Internet* è per sua natura

> delocalizzato, a-territoriale e privo di uno spazio e un tempo ben definiti. Esso, infatti, lungi dall'identificarsi con le macchine che lo compongono, è sincronicamente ovunque e in nessun luogo, così da costituire un mondo parallelo al mondo reale (9).

Le difficoltà sono poi incrementate con l'apparizione in tali mondi virtuali (MMPORG) delle prime valute virtuali (10) (*Linden Dollar* di

---

quest'ultima, il fisico Philip Rosedale. Si tratta di una piattaforma informatica nel settore dei nuovi media che integra strumenti di comunicazione sincroni ed asincroni, e trova applicazione in molteplici campi della creatività: intrattenimento, arte, formazione, musica, cinema, giochi di ruolo, architettura, programmazione, impresa, solo per citarne alcuni. (Fonte: Wikipedia).

(9) Cfr. E. Bassoli, *La disciplina giuridica della seconda vita in internet: l'esperienza Second Life*, in *Rivista "Informatica e diritto"*, ITTIG, 2009, I.

(10) Si veda: H. Yamaguchi, *An Analysis of Virtual Currencies in Online Games* (Sept. 1, 2004), http://ssrn.com/abstract=544422 (sito web consultato, e documento disponibile online, il 7 marzo 2015); V. Lehdonvirta, *Real-Money Trade of Virtual Assets: New Strategies for Virtual World Operators (2008)*. Virtual Worlds, Ipe, Mary, ed., pp. 113-137, Icfai University Press, Hyderabad, India (2008), http://ssrn.com/abstract=1351782 (sito web consultato, e documento disponibile online, il 7 marzo 2015); L. V. Orman, *Virtual Money in Electronic Markets and Communities* (June 7, 2010). ICAST Journal of Institute for Communication, Social Informatics, and Technology, Forthcoming; Johnson School Research Paper Series No. 27-2010, http://ssrn.com/abstract=1621725 (sito web consultato, e documento disponibile online, il 7 marzo 2015); S. Ba, D. Ke, *Optimal Pricing and Permissions Strategy for Virtual Good Creators in Second Life* (Sept. 15, 2008), http://ssrn.com/abstract=1271684 (sito web consultato, e documento disponibile online, il 7 marzo 2015); V. Lehdonvirta, *Virtual Item Sales as a Revenue Model: Identifying Attributes that Drive Purchase Decisions*, 9 Electronic Commerce Research, Vol. 9, 97 (2009), http://ssrn.com/abstract=1351769 (sito web consultato, e documento disponibile online, il 7 marzo 2015); D. A. Bray, B. Konsynski, *Virtual Worlds: Multi-Disciplinary Research Opportunities*, 38 The Data Base for Advances in Information Systems, Special Issue on Virtual Worlds, (2007), http://ssrn.com/abstract=1016485(sito web consultato, e documento disponibile online, il 7 marzo 2015); S. T. Kim, *Why Bitcoin?: Structure and Efficiency of Markets for Online Game Currency* (Dec. 18, 2013), http://ssrn.com/abstract=2334000 http://ssrn.com/abstract=1335120 (sito web consultato, e documento disponibile online, il 7 marzo 2015); M. Elias, *Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy* (Oct. 3, 2011), http://ssrn.com/abstract=1937769 http://ssrn.com/abstract=133

Capitolo I
STORIA DELLE CRIPTOVALUTE

1.1. *Storia delle criptovalute.*

L'innovazione delle criptovalute (1) consiste nell'individuazione di un processo che incorpori i principi della crittografia con una valuta digitale decentralizzata e limitata nella quantità totale.

L'introduzione di questi concetti è avvenuta in maniera progressiva, usando le potenzialità della rete, le esigenze che stavano emergendo da parte di alcune comunità congiuntamente allo sfruttamento dello sviluppo tecnologico di *Internet*.

Per giungere al concetto di criptovalute occorre recuperare gli studi e le idee che si sono sviluppate nel corso degli anni, premettendo che il primo lavoro fu pubblicato nel 1982 da David Chaum (2). Nel 1990, Chaum creò la società Digicash (chiusa nel 1999), prima impresa che integrava la crittografia con la moneta, al fine di rendere anonime

---

(1) Per una lista completa delle criptovalute si può visionare: http://en.wikipedia.org/wiki/List_of_cryptocurrencies (sito web consultato, e documento disponibile online, il 7 marzo 2015).

(2) D. Chaum, *Blind Signatures for Untraceable Payments*, in Advances in Cryptology: Proceedings Of Crypto 82 (1982), in http://blog.koehntopp.de/uploads/Chaum.BlindSigForPayment.1982.PDF (sito web consultato, e documento disponibile online, il 7 marzo 2015).

le transazioni con un sistema di emissione centralizzato e di compensazione, forse troppo anticipato rispetto ai tempi.

Molte delle idee sono state sviluppate all'interno dei movimenti *cypherpunk* (3), movimento sorto negli anni Novanta negli USA. Per economia di analisi presenteremo solo alcuni documenti che ne rivelano la filosofia, evitando gli aspetti tecnici non utili ai fini del presente scritto.

1.2. B-money - *Wei Dai.*

L'idea di una valuta virtuale decentralizzata fu descritta per la prima volta nel 1998 da Wei Dai (4) in una *mailing list* di cripto anarchici (5):

> Sono affascinato dalla cripto-anarchia di Tim May (6). A differenza delle comunità tradizionalmente associate alla parola "anarchia", nella cripto-anarchia il governo non è cancellato temporaneamente, ma vietato in modo permanente e inutile in maniera stabile. Si tratta di una comunità dove la minaccia della violenza è impotente perché la violenza è impossibile, e la violenza è impossibile, perché i suoi partecipanti non possono essere collegati ai loro veri nomi o luoghi fisici.
>
> Fino ad ora non è chiaro, anche teoricamente, come tale comunità possa operare. Una comunità è definita dalla cooperazione dei suoi partecipanti, e la cooperazione efficace richiede un mezzo di scambio (denaro) e un modo per far rispettare i contratti. Tradizionalmente questi servizi sono stati forniti dal governo o istituzioni governative e soltanto a entità legali. In questo articolo descrivo un protocollo con cui questi servizi possono essere forniti a e da enti non rintracciabili.

---

(3) Da Wikipedia: "Un cypherpunk è un attivista che sostiene l'uso intensivo della crittografia informatica come parte di un percorso di cambiamento sociale e politico, ad esempio violando archivi riservati per rendere pubbliche alcune verità scomode. Originariamente i cypherpunk comunicavano attraverso una mailing list, in gruppi informali con l'intento di ottenere la privacy e la sicurezza informatica degli account personali, attraverso l'uso della crittografia, contro governi e gruppi economici. I cypherpunk sono organizzati in un movimento attivo dalla fine degli anni '80, con influenze della cultura punk. Esempio di attivismo cypherpunk è il sito Wikileaks di Julian Assange". Tratto da Wikipedia, http://it.wikipedia.org/wiki/Cypherpunk. (sito web consultato, e documento disponibile online, il 7 marzo 2015).

(4) Cfr. http://www.weidai.com/bmoney.txt (sito web consultato, e documento disponibile online, il 7 marzo 2015).

(5) Si presenta traduzione del testo inglese.

(6) Il riferimento è al Manifesto dei Cripto-Anarchici di Timothy May del 22.11.1992, su http://nakamotoinstitute.org/crypto-anarchist-manifesto/ (sito web consultato, e documento disponibile online, il 7 marzo 2015).

Io in realtà descriverò due protocolli. Il primo è impraticabile, perché fa un uso pesante di un canale di diffusione anonimo, sincrono e non comparabile. Tuttavia motiverò il secondo protocollo, più pratico. In entrambi i casi vi è alla base l'ipotesi dell'esistenza di una rete irrintracciabile, dove i mittenti e i destinatari sono identificati solo da pseudonimi digitali (ad esempio chiavi pubbliche) e ogni messaggio è firmato dal mittente e criptato al suo ricevitore.

Nel primo protocollo, ogni partecipante mantiene un database (separato) di quanta valuta appartiene ad ogni pseudonimo. Questi conti definiscono collettivamente la proprietà del denaro, e di come questi conti vengono aggiornati è oggetto di questo protocollo.

1) La creazione del denaro. Chiunque può creare denaro trasmettendo la soluzione di un problema computazionale finora irrisolto. Le uniche condizioni sono che deve essere facile da determinare la quantità di impegno computazionale necessario per risolvere il problema e la soluzione deve esistere altrimenti non esiste alcun valore, né pratico o intellettuale. Il numero di unità monetarie create è pari al costo della potenza di calcolo valutata in base a un paniere standard di merci. Ad esempio se un problema richiede 100 ore per la risoluzione sul computer più economico con un costo di tre panieri standard per le 100 ore di calcolo su quel computer, la soluzione ha un valore di tre panieri standard che verranno accreditati a chi risolve il problema.

2) Il trasferimento di denaro. Se Alice (proprietario della pseudonimo K_A) intende trasferire X unità di moneta a Bob (proprietario della pseudonimo K_B), trasmette il messaggio "Io do X unità di denaro ai K_B" firmato da K_A. Dopo la trasmissione di questo messaggio, tutti addebitano il conto di K_A di X unità e accreditano il conto di K_B di X unità, fatta eccezione che si crei un saldo negativo sul conto di K_A: nel qual caso il messaggio viene ignorato.

3) L'effettuazione dei contratti. Un contratto valido deve includere un risarcimento massimo in caso di default per ciascuna parte partecipante ad esso. Esso dovrebbe prevedere la presenza di una parte che agisce quale arbitro qualora ci fosse una disputa. Tutte le parti di un contratto, tra cui l'arbitro devono trasmettere le loro firme prima che diventi effettivo. Dopo la trasmissione del contratto comprensivo di tutte le firme, ogni partecipante addebita il conto di ciascuna delle parti per l'importo del risarcimento massimo e accredita un conto speciale identificato da un hash (7)

(7) Nel linguaggio matematico e informatico, la funzione *hash* è una funzione non iniettiva (e quindi non invertibile) che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Esistono numerosi algoritmi che realizzano funzioni *hash* con particolari proprietà che dipendono dall'applicazione. Nelle applicazioni crittografiche si chiede, per esempio, che la funzione *hash* abbia le seguenti proprietà: 1) resistenza alla preimmagine: sia computazionalmente intrattabile la ricerca di una stringa in input che dia un *hash* uguale a un dato *hash*; 2) resistenza alla seconda preimmagine: sia computazionalmente intrattabile la ricerca di una stringa in input che dia un *hash* uguale a quello di una data stringa; 3) resistenza alle collisioni: sia

sicuro del contratto per la somma del risarcimento massimo. Il contratto diventa efficace se l'addebito per ogni parte non produce un saldo negativo, altrimenti il contratto viene ignorato e i conti riaccreditati. Un esempio di contratto potrebbe essere simile a questo:

K_A si impegna ad inviare K_B la soluzione al problema P prima del 1/1/2000 0:00:00. K_B si impegna a pagare K_A 100 MU (unità monetarie) prima delle 0:00:00 del 1/1/2000. K_C accetta di eseguire l'arbitrato in caso di controversia. K_A si impegna a pagare un massimo di 1.000 MU in caso di default. K_B si impegna a pagare un massimo di 200 MU in caso di default. K_C si impegna a pagare un massimo di 500 MU in caso di default.

4) La conclusione di contratti. Se il contratto si conclude senza controversie, ciascuna parte trasmette un messaggio firmato "Il contratto con hash SHA-1 H si è concluso senza risarcimenti." o "Il contratto con hash SHA-1 H si è concluso con i seguenti risarcimenti: ..." Dopo la trasmissione di tutte le firme, ogni partecipante accredita il conto di ciascuna delle parti per l'importo del suo risarcimento massimo, rimuove l'account del contratto, quindi accredita o addebita i conti di ciascuna delle parti secondo lo schema risarcitorio in tale evenienza.

5) L'applicazione dei contratti. Se le parti di un contratto non riescono ad accordarsi su una conclusione adeguata anche con l'aiuto dell'arbitro, ciascuna parte trasmette una proposta /risarcimento e gli eventuali argomenti o elementi di prova a suo favore. Ogni partecipante fa una determinazione per quanto riguarda le proposte / risarcimenti, e modifica i suoi conti di conseguenza.

Nel secondo protocollo, i conti sono tenuti da un sottoinsieme dei partecipanti (chiamati server da ora in poi) invece che da tutti. Questi server sono collegati da un canale di diffusione tipo Usenet.

Il formato dei messaggi di transazione su questo canale rimane lo stesso come nel primo protocollo, ma i partecipanti interessati da ogni transazione devono verificare che il messaggio sia stato ricevuto e correttamente elaborato da un sottoinsieme selezionato casualmente di server.

Dal momento che i server devono essere affidabili, è necessario un meccanismo per garantirne l'onestà. Ogni server è tenuto a depositare una certa somma di denaro in un conto speciale da utilizzare come potenziale risarcimento o ricompensa per comportamenti non conformi. Inoltre, ogni server deve pubblicare periodicamente i database della creazione di denaro e le proprietà correnti. Ogni partecipante deve verificare che i propri saldi di conto siano corretti e che la somma dei saldi dei conti non sia superiore alla quantità totale di denaro creato. Questo impedisce ai server, anche in caso di collusione totale, di espandere l'offerta di moneta a costo zero. I nuovi server possono anche utilizzare i database pubblicati per la sincronizzazione con i server esistenti.

---

computazionalmente intrattabile la ricerca di una coppia di stringhe in input che diano lo stesso *hash*

Capitolo II
FUNZIONAMENTO DEL SISTEMA DELLE CRIPTOVALUTE

2.1. *Funzionamento del sistema delle criptovalute.*

La prima applicazione di tali sistemi è costituita quindi dal *bitcoin* (1) (la prima criptovaluta), definita come una valuta paritaria basata su un algoritmo, decentralizzata e digitale la cui implementazione è basata sui principi della crittografia per convalidare le transazioni e la generazione di moneta in sé (2), senza alcun ente emittente.

Il sistema nasce decentralizzato, virtuale, con denominazione propria, gestita e creata attraverso tre elementi:

— un protocollo di comunicazione,

— la crittografia,

— rete *peer-to-peer* che risulta attraverso il protocollo *Bitcoin*.

Lo sviluppo del *bitcoin* si basa sulle innovazioni tecnologiche

---

(1) Per una delle prime analisi in Italia si veda: A. Teti, *Sistemi di pagamento: Bitcoin la moneta del Cyberspazio*, in GNOSIS n. 2/2012: Cfr. http://gnosis.aisi.gov.it/gnosis/Rivista31.nsf/ServNavig/11 (sito web consultato, e documento disponibile online, il 7 marzo 2015). Per un'analisi completa si veda: A. Badev, M. Chen, *Bitcoin: Technical Background and Data Analysis*, Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs Federal Reserve Board, Washington, D.C., 2014-104, http://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf (sito web consultato, e documento disponibile online, il 7 marzo 2015), D. Capoti, E. Colacchi e M. maggioni, *Bitcoin Revolution*, Hoepli, 2015.

(2) Definizione ripresa da http://it.wikipedia.org/wiki/Criptovaluta (sito web consultato, e documento disponibile online, il 7 marzo 2015).

avvenute nell'ultimo periodo, riuscendo a risolvere il problema principale che consiste nel garantire l'affidabilità di transazioni monetarie senza affidarsi ad un ente centrale, quindi attraverso un sistema decentralizzato.

Tutte le esperienze pre-*bitcoin* di valute virtuali e/o digitali prevedevano la presenza di un ente centrale che nello scambio gestiva il *database* con il bilancio e i dati degli utenti: per trasferire le unità di conto (moneta) l'utente si autenticava presso l'ente centrale (in tal caso un *server*) e richiedeva il trasferimento ad un altro utente. Il sistema centralizzato diminuiva dell'importo richiesto il conto dell'utente ed incrementava il conto dell'altro utente garantendo che durante il trasferimento non venisse mai generato o distrutto denaro.

Partendo dall'eliminazione del *server*, il primo problema era quello dell'autenticazione, vale a dire garantire che solo quell'utente fosse in grado di gestire e trasferire il proprio conto.

Il problema è stato risolto con l'utilizzo di una firma digitale. La firma digitale, in informatica, rappresenta l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica. Può essere basata su varie tecnologie, tra cui la crittografia a chiave pubblica.

Il sistema per la creazione e la verifica di firme elettroniche può sfruttare le caratteristiche della crittografia asimmetrica.

Un sistema crittografico garantisce la riservatezza del contenuto dei messaggi, rendendoli incomprensibili a chi non sia in possesso di una "chiave" (intesa secondo la definizione crittologica) per interpretarli. Nei sistemi crittografici a chiave pubblica, detti anche a chiave asimmetrica, ogni utente ha una coppia di chiavi: una chiave privata, da non svelare a nessuno, con cui può decifrare i messaggi che gli vengono inviati e firmare i messaggi che invia, e una chiave pubblica, che altri utenti utilizzano per cifrare i messaggi da inviargli e per decifrare la sua firma e stabilirne quindi l'autenticità.

Per ogni utente, le due chiavi vengono generate da un apposito algoritmo con la garanzia che la chiave privata sia la sola in grado di poter decifrare correttamente i messaggi cifrati con la chiave pubblica associata e viceversa. Lo scenario in cui un mittente vuole spedire un messaggio a un destinatario in modalità sicura è il seguente: il mittente utilizza la chiave pubblica del destinatario per la cifratura del messaggio da spedire, quindi spedisce il messaggio cifrato al destinatario; il

destinatario riceve il messaggio cifrato e adopera la propria chiave privata per ottenere il messaggio "in chiaro".

Nel sistema *Bitcoin* l'utente genera una coppia di chiavi pubblica e privata. Scrive un messaggio che contiene la quantità di unità di conto che vuole trasferire e la chiave pubblica del destinatario. A questo punto firma con la propria chiave privata il messaggio e lo invia. Il destinatario verificando la firma avrà quindi la prova crittografica del mittente, del destinatario e della quantità di unità di conto trasferita.

Il sistema *Bitcoin* utilizza il sistema di firma digitale ECDSA (*Elliptic Curve Digital Signature Algorithm*) (3), con chiavi generate molto lunghe e non pratiche: da ciò l'indirizzo pubblico per identificare il destinatario è l'indirizzo *bitcoin*, attraverso l'applicazione di una funzione (*Base58check*) per avere una codifica dell'*hash* della chiave pubblica. Tramite tale codifica si può verificare la correttezza formale dell'indirizzo al momento del suo inserimento. Esempio di indirizzo: *1mEtPE3PTcnaD1Sa6FdYwE5GWCB2845A4*.

Risolto il problema dell'identificazione, le transazioni avvengono attraverso firme digitali dell'*hash* della transazione precedente con la propria firma e la chiave pubblica del destinatario, in catena (*chain*). Il *bitcoin* è quindi una catena di transazioni, con possibilità di controllare a ritroso i passaggi verificando le firme presenti nelle transazioni precedenti, con impossibilità di modifica, dato che variazioni infinitesimali rendono non valide tutte le transazioni poiché gli *hash* non corrisponderebbero più.

Resta in sospeso il problema del *double-spending*, vale a dire la certezza che deve avere il ricevitore del pagamento che il mittente non abbia inviato l'unità di conto a più persone.

Nel sistema centralizzato, l'ente centrale controlla le transazioni per prevenire tentativi di *double-spending*. In un sistema decentralizzato la soluzione consiste nella condivisione delle transazioni, rendendole pubbliche, vale a dire con la presenza di un unico registro storico condiviso tra gli utenti con un determinato livello di "*consenso*". Il ricevitore deve quindi avere una prova crittografica che la maggioranza degli utenti concordava sulla validità della transazione nel momento della sua inclusione nella catena.

---

(3) Per approfondimenti sul sistema di firma digitale si veda: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf (sito web consultato, e documento disponibile online, il 7 marzo 2015).

Per la datazione delle transazioni è utilizzato un server di *timestamp* (marcatura temporale) distribuito. Ogni *timestamp* include, oltre all'oggetto che deve datare, anche il valore *hash* del *timestamp* immediatamente precedente, creando cosi una catena, con immodificabilità.

Per realizzare un sistema distribuito di *timestamp* in *peer-to-peer*, *Bitcoin* utilizza un sistema *proof-of-work* simile a *Hashcash* (4). All'insieme di oggetti da datare viene aggiunto un numero, chiamato *nonce*, e ne viene calcolato l'*hash* tramite l'algoritmo SHA-256 (5) in maniera iterativa cambiando il *nonce* fino a ottenere un valore *hash* che inizia con un determinato numero di zeri, che variano a seconda della potenza computazionale della rete di modo che la generazione dei *timestamp* sia più o meno regolare.

Per modificare un oggetto in un *timestamp* occorre rifare tutto il lavoro dalla modifica in poi, che necessita di una potenza superiore alla rete nel suo complesso (praticamente impossibile).

Il *timestamp* viene chiamato blocco (*block*) e la catena dei *timestamp* successivi, catena o *blockchain*.

La *blockchain* è un database distribuito pubblico (6) che contiene tutta la cronologia delle transazioni avvenute sulla rete *Bitcoin*, formata da una catena principale e da blocchi "orfani" (che via via vengono abbandonati per involuzione del consenso).

Il lavoro svolto per generare blocchi validi viene svolto da nodi chiamati *miners*.

Di seguito una sintesi del funzionamento della rete *Bitcoin* e del lavoro svolto dai nodi minatori:

1) le nuove transazioni vengono inviate a tutti i *peers*.

2) Ogni *miner* dopo aver controllato la validità formale delle transazioni controlla, le raccoglie in un *block* (blocco) insieme all'*hash* del blocco precedente ed inizia a cercare un *proof-of-work* valido per il nuovo blocco.

---

(4) Cfr. *HashCash* è un sistema basato su "prove" e fu introdotto come uno strumento antispam e come una contromisura contro attacchi di tipo DoS (*Denial-of-Service*). L'articolo è visionabile su A. Back et al., *Hashcash,* 2002, url: ftp://sunsite.icm.edu.pl/site/replay.old/programs/*hash*cash/*hash*cash.pdf (sito web consultato, e documento disponibile online, il 7 marzo 2015).

(5) Cfr. http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf (sito web consultato, e documento disponibile online, il 7 marzo 2015).

(6) La *blockchain* può essere consultata liberamente su: http://bitcoinchain.com e http://bloc[illegible]zo 2015).

Capitolo III
INQUADRAMENTO A LIVELLO INTERNAZIONALE

3.1. *Premessa.*

Le criptovalute sono un fenomeno complesso, internazionale e interdisciplinare e possono inserirsi in molti aspetti della vita economica e sociale, diventando rilevanti per molti aspetti del diritto.

Occorre preliminarmente riflettere che la creazione, il possesso e l'utilizzo delle criptovalute rientra nelle libertà dell'individuo, tale per cui nessun paese occidentale ha dichiarato l'illegalità delle stesse o posto divieti, pur se alcuni paesi extraeuropei hanno messo vincoli (1).

In realtà, alcuni organismi internazionali e alcuni Stati hanno promulgato documenti di inquadramento del fenomeno ed è apparsa anche qualche Sentenza. In tale paragrafo esuleremo dalle interpretazioni tributarie che saranno presentate nei paragrafi specifici in maniera funzionale all'interpretazione interna o comunitaria.

Per presentare le varie interpretazioni, sentenze e pronunce abbiamo scelto un criterio cronologico, piuttosto che altre modalità (per paesi o per aree di interesse), poiché riteniamo che in un mondo interconnesso le interpretazioni si sono interrelate le une con le altre, pur con le peculiarità di ogni ordinamento giuridico nel quale sono state emesse.

---

(1) Una panoramica delle normative sulle criptovalute è consultabile su www.merkletree.io (sito web consultato e disponibile online il 7 marzo 2015).

Non considereremo quali rilevanti interviste, comunicati stampa, articoli, discorsi pubblici o *tweet* (2) che riteniamo non idonei (pur avendoli tenuti in considerazione) a questi fini per carenza di ufficialità.

3.2. *Francia: Tribunale di Creteil.*

Il primo documento ufficiale in cui si parla esplicitamente di *bitcoin* è sorprendentemente una Sentenza dell'agosto 2011 del Tribunale di Commercio di Creteil (Francia), Ordinanza dell'11 gosto 2011, R.G. n. 2011R00309, poi appellata alla Corte di Appello di Parigi che ha emesso Sentenza il 28 agosto 2011 n. 11/15269.

Il caso discusso era relativo alla chiusura di un conto corrente da parte della banca nel maggio 2011: la società *Maracaja* (rappresentante di *Mt.Gox* (3) in Francia) aveva aperto un conto presso il *Crédit Industriel et Commercial* (CIC) per lo svolgimento della propria attività e senza un apparente motivo la banca aveva chiuso i conti, con conseguente procedimento di urgenza al Tribunale: la banca sosteneva di aver chiuso il conto in quanto la società *Maracaja* esercitava attività di intermediazione in *bitcoin* non conforme al suo oggetto sociale (che consisteva in "creazione e sviluppo di *software*"), dato che dalle analisi svolte risultavano numerosi bonifici in entrata da parte di persone fisiche per acquisto di *bitcoin* e in uscita riferiti all'acquisto di *bitcoin*. Partendo dal presupposto che il *bitcoin* è una moneta, quindi equiparabile alla moneta elettronica (*monnaie electronique*), la banca affermava che l'intermediazione di *bitcoin* costituisce operazione finanziaria soggetta ad autorizzazione dell'*Autorité de contrôle prudentiel et de résolution* (ACPR) (4) e non essendo la società in possesso di tale autorizzazione, la CIC aveva ritenuto opportuno chiudere i rapporti.

La società *Macaraja* sosteneva che il *bitcoin* è il risultato di un

---

(2) Messaggi di testo brevissimi inviati tramite Twitter®.

(3) MtGox (marchio della società Tibanne Ltd) è stato uno dei principali *player* nel mercato dei *bitcoin* fino alla sua chiusura con apertura di una procedura concorsuale in Giappone.

(4) L'*Autorité de contrôle prudentiel et de résolution* è un organo amministrativo indipendente, senza personalità giuridica, che controlla le attività delle banche e assicurazioni in Francia. È stata fondata nel gennaio 2010 dal decreto no. 2010-76 1, fondendo la Commissione Bancaria, la Autorità di Vigilanza sulle Assicurazioni e Mutui (ACAM), le Commissioni di Controllo sulle Compagnie di Assicurazione e sulle Imprese di Credito e di Investimento (CECEI). Cfr. http://acpr.banque-france.fr/accueil.html (sito web consultato e disponibile online il 7 marzo 2015).

calcolo complesso effettuato da un programma che consiste in una stringa crittografata e non è una moneta elettronica, bensì un bene intangibile come qualsiasi *software*. La società svolgeva attività di intermediazione per la società *Tibanne* (*Mt.Gox*), con attività limitata a operazioni relative agli scambi di *bitcoin* senza che alcun cliente potesse compiere o promuovere pagamenti da un loro conto in banca e che in ogni caso non forniva servizi di pagamento al pubblico, da ciò l'errore della banca con l'aggiunta che nel proprio oggetto sociale sono presenti anche tutte le attività commerciali non regolamentate.

Con sentenza del 6 dicembre 2011, la Corte di Creteil ha dichiarato che l'attività commerciale di *Macaraja* è da considerarsi quale prestazione di servizi di pagamento ed è stata svolta senza applicare le norme di legge che disciplinano tale attività: la banca CIC era quindi giustificata a chiudere il conto.

La Corte d'appello di Parigi ha confermato con Sentenza del 26 settembre 2013 (Pôle 5, ch. 6, n. 12/00161), che *Macaraja* ha svolto attività di intermediario per effettuare una disposizione di pagamento di fondi appartenenti a terzi per conto di terzi, equiparabile ad un servizio di pagamento e che l'attività di intermediazione finanziaria richiede l'autorizzazione dell'ACPR (5). La Corte di Appello, purtuttavia, non si è pronunciata sulla natura giuridica dei *bitcoin*, dichiarando che è "indifferente al risultato del caso per determinare se bitcoin è una moneta elettronica", contrariamente a quanto sostenuto da *Macaraja* (6).

3.3. *FBI Report on* Bitcoin.

Il Federal Bureau of Investigation (FBI) ha pubblicato il 24 aprile 2012 "*Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity*" (7), primo studio strutturato da parte di un ente governativo sul fenomeno.

---

(5) L'ACPR si pronuncerà definitivamente nel 2014: L'ACPR si è pronunciata nel gennaio 2014: Autorité de contrôle prudentiel et de résolution, *Position de l'ACPR relative aux opérations sur Bitcoins en France*, 29.01.2014, n. 2014_P_01, in http://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/201401-Position-2014-P-01-de-l-ACPR.pdf. (sito web consultato, e documento disponibile online, il 7 marzo 2015).

(6) C. Lavardet, *Bitcoin: par ici la cryptomonnaie!*, in Revue Lamy Droit de l'immaterial, Janvier 2014, n. 100.

(7) Federal Bureau of Investigation, "*Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity*", 24 aprile 2012, Cfr.

Detto studio copre gli aspetti investigativi della moneta con l'avvertenza che le valute digitali e virtuali costituiscono una nuova sfida per l'individuazione ed il contrasto di attività illecita, aggiungendo complessità uniche per gli investigatori a causa della sua natura decentralizzata. Il documento presenta i livelli di rischio per le attività illegali che possono essere compiute tramite le valute virtuali decentralizzate, con focus sul *bitcoin*.

L'FBI valuta con livello di rischio medio che, nel breve termine, i *cyber* criminali tratteranno il *bitcoin* come un'altra opzione di pagamento a fianco delle tradizionali e consolidate valute virtuali poiché hanno pochi motivi per abbandonare quest'ultime. La valutazione si basa sulle fluttuazioni del tasso di cambio del *bitcoin* nel 2011 congiuntamente alle segnalazioni limitate che indicano il livello di accettazione di *bitcoin* da parte di criminali informatici.

L'FBI valuta con livello di rischio basso, sulla base della valutazione dell'accettazione di utenti e commercianti, che i riciclatori sfrutteranno i *bitcoin* per riciclare il denaro. Questa valutazione si basa sulle indagini e azioni penali degli individui che sfruttano altre valute virtuali, come *E-Gold* e *WebMoney*.

L'FBI si preoccupa dei reati informatici che possono essere commessi nei confronti degli utilizzatori *bitcoin*, riflettendo che il *bitcoin*, probabilmente, continuerà ad attirare *cyber* criminali che lo ritengono un mezzo per spostare o rubare fondi, nonché un mezzo per finanziare gruppi illegali.

Qualora il *bitcoin* stabilizzi le sue quotazioni e cresca in popolarità, potrebbe diventare uno strumento sempre più utile per le varie attività illecite: in tal caso poiché il *bitcoin* non ha un'autorità centralizzata, l'applicazione della legge dovrà affrontare le difficoltà di rilevamento di attività sospette, di identificazione degli utenti e di ottenere traccia delle transazioni. Il *bitcoin* potrebbe anche attirare logicamente riciclatori di denaro e altri criminali che evitano sistemi finanziari tradizionali, utilizzando *Internet* per effettuare trasferimenti monetari globali.

Sebbene il *bitcoin* non disponga di un'autorità centralizzata, l'FBI valuta con livello di rischio medio che l'applicazione della legge per l'identificazione dei criminali o l'ottenimento di informazione sarà pur sempre possibile se gli "attori" convertono i loro *bitcoin* in una moneta a corso legale. Chi compie tale attività dovrà richiedere l'identificazione

---

http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf (sito web consultato e

Capitolo IV
ASPETTI GIURIDICI

4.1. *Prime riflessioni.*

I documenti apparsi a livello sovranazionale e di alcuni Stati denotano un'estrema difficoltà di analisi, con inquadramenti eterogenei parziali e, per certi versi, contraddittori.

Preliminarmente nessun ordinamento giuridico ci risulta che contenga definizioni di moneta, di valuta o di mezzo di scambio, essendo concetti che sono considerati quali assiomi, dati per scontati. Parimenti, la nozione di valuta estera è massimamente definita quale valuta diversa dalla valuta nazionale.

La necessaria premessa tecnica, filosofica e storica delle criptovalute rende chiaro come comprendere il fenomeno sia assolutamente complesso e innovativo, sfidando l'interprete in campo giuridico.

L'introduzione del concetto di criptovaluta pone difatti problemi di inquadramento da un punto di vista giuridico data la sua natura virtuale (1), polimorfa (2), ibrida (3), anonima (4) e ubiqua (5).

---

(1) Sulla tassazione delle economie virtuali, l'Internal Revenue Service si era espressa, con chiarimenti: Internal Revenue Service, *Tax Consequences of Virtual World Transactions*, su http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Tax-Consequences-of-Virtual-World-Transactions (sito web consultato, e documento disponibile online, il 7 marzo 2015), con alcuni contributi di commento utili per il ragionamento: L. Lederman, *Stranger than Fiction: Taxing Virtual Worlds,* in New York University Law Review, 2007, 82, 1620-1672, 1622 e C. Steven, *Real Taxation of Virtual*

Per sgomberare la riflessione da qualsiasi equivoco riteniamo che le criptovalute non cadano in alcun vuoto giuridico o in alcuna terra di nessuno, né potrebbe essere altrimenti. Purtuttavia, il fatto che le criptovalute, quali unità di conto, siano legate inscindibilmente al sistema decentralizzato non aiuta l'interprete che, spesso, viene indotto in errore confondendo i due concetti che però sono e devono essere considerati distinti.

L'attenzione deve concentrarsi sull'unità di conto la cui natura giuridica è abbastanza opaca. Utilizziamo il termine "opacità" in quanto pur intravedendo alcune caratteristiche, nel momento in cui cerchiamo di inquadrarle, i contorni sfumano sovrapponendosi ad altri, sfuggendo.

L'aspetto fondamentale che emerge è costituito dal fatto che dette unità di conto si accodano, innovandoli, ai concetti di *new properties* o nuove proprietà la cui analisi è in continuo divenire, quali possono essere considerati i beni/proprietà/diritti collegati a insieme di *bit*. È necessario svolgere un'analisi su alcuni concetti di senso comune prima di intraprendere la ricerca di definizione.

4.2. *Moneta virtuale, valuta virtuale e criptovalute.*

La Banca Centrale Europea ha analizzato nel 2012 gli schemi di moneta virtuale (6), definendoli provvisoriamente (vista l'estrema variabilità delle caratteristiche fondamentali):

Commerce: Has Second Life Crossed the Line?", Virginia Tax Review, Vol. 28, No. 3, 2008, su http://ssrn.com/abstract=1097793 (sito web consultato, e documento disponibile online, il 7 marzo 2015).

(2) Il polimorfismo delle criptovalute consiste nella loro capacità adattiva a varie esigenze, come del resto emerge dalla natura open-source del codice.

(3) Le criptovalute sono ibride in quanto rispondono a diverse esigenze congiuntamente.

(4) Cfr. R. Fergal, M. Harrigan, *An Analysis of Anonymity in the Bitcoin System*, in arXiv:1107.4524, 2011-07-22, in http://arxiv.org/abs/1107.4524.pdf (sito web consultato, e documento disponibile online, il 7 marzo 2015) e S. Wisniewski, *Taxation of Virtual Assets*, 7 in Duke Law & Technology Review, 2008, 7, 1-18.

(5) Cfr. S.S. Moharana, S. Sai, R.D. Ramesh, *Ubiquitous Virtual Currency,* in IOSR Journal of Computer Engineering (IOSR-JCE), 2013, 9, 2278-8727, and Issue, 2013, 45-49.

(6) Cfr. European Central Bank, *Virtual Currency Schemes*, October 2012, in *http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf* (sito web consultato, e documento disponibile online, il 7 marzo 2015).

> un tipo di denaro regolamentato e digitale, che viene rilasciato e di solito controllato dai suoi sviluppatori e utilizzato e accettato tra i membri di una specifica comunità virtuale.

Gli schemi di moneta virtuale sono molteplici con difficoltà di classificazione e individuazione delle caratteristiche. È possibile, tuttavia, analizzare le interazioni tra moneta virtuale, denaro e economia reale, che può avvenire attraverso:

1) flusso finanziario attraverso scambi di valuta;

2) flusso economico tramite la possibilità di acquistare beni e servizi reali o virtuali.

Prendendo spunto da ciò è possibile individuare:

1) moneta virtuale a regime chiuso: in tali configurazioni gli elementi di interazione sono minimi. Gli utenti di solito pagano un canone di abbonamento per ottenere tale moneta virtuale (che può anche essere guadagnata *on line* al verificarsi di determinate condizioni) e può essere utilizzata solo per acquistare beni e servizi all'interno della comunità virtuale e, almeno in teoria, non può essere utilizzato, al di fuori della comunità virtuale.

2) Moneta virtuale a flusso unidirezionale: la moneta virtuale può essere acquistata tramite moneta reale a un tasso di cambio specifico (determinato dal proprietario della moneta), ma la moneta virtuale non può essere rivenduta e riconvertita in moneta reale. Tale moneta virtuale può essere utilizzata per l'acquisto di beni e servizi virtuali, ma può anche essere utilizzata per acquistare beni e servizi reali.

3) Moneta virtuale a flusso bidirezionale: gli utenti possono acquistare e vendere valuta virtuale in base a tassi di cambio con moneta reale. La valuta virtuale è simile a qualsiasi altra valuta convertibile per quanto riguarda la sua interoperabilità con il mondo reale. Questi sistemi consentono l'acquisto di beni e servizi virtuali e reali.

Per semplicità di analisi, pur con qualche sovrapposizione, è possibile affermare che il concetto di moneta virtuale contiene quello di valuta virtuale e le criptovalute sono un sottoinsieme delle valute virtuali.

4.3. *Moneta Elettronica.*

L'Unione Europea, con la direttiva 2009/110/CE, ha introdotto la regolamentazione della moneta elettronica. Secondo detta direttiva la "moneta elettronica" è un valore monetario rappresentato da un credito nei confronti dell'emittente che sia:

a) elettronicamente memorizzato;

b) emesso dietro ricezione di fondi il cui importo non sia inferiore al valore ricevuto;

c) accettato come mezzo di pagamento da imprese diverse dall'emittente.

Detta definizione evidenzia immediatamente le differenze tra moneta elettronica e moneta virtuale:

1) nei sistemi di moneta elettronica il legame tra quest'ultima e la moneta tradizionale è conservato da un fondamento giuridico: la moneta elettronica è espressa normalmente nella stessa unità di conto (dollari, euro, ecc.).

2) Nella moneta virtuale l'unità di conto può essere una valuta reale o una valuta virtuale (ad esempio *Facebook Credits, Linden Dollars, bitcoins, WII credits, Q Coin, VEN*).

3) Nel caso di valuta virtuale, il tasso di cambio (qualora consentito) per la valorizzazione della stessa è legato esclusivamente alle interazioni tra domanda e offerta.

4) La convertibilità della valuta virtuale in valuta reale non è regolata né obbligatoria e dipende dalla volontà (o dagli schemi contrattuali) dell'emittente.

5) Nel caso di criptovaluta, non essendovi alcun emittente, tale conversione è assolutamente incerta.

In aggiunta, i sistemi di moneta elettronica sono regolamentati e gli emittenti sono soggetti a vigilanza, mentre nei regimi di moneta virtuale può esservi carenza di regole e assenza di vigilanza nei confronti degli emittenti.

I rischi cui l'utente si espone nel possedere moneta elettronica o moneta virtuale sono diversi. La moneta elettronica è principalmente soggetta al rischio operativo associato a potenziali interruzioni del sistema su cui è memorizzata. Le monete virtuali, oltre ad essere esposte a rischi di credito, sono soggette a rischi di liquidità, a incertezza giuridica e rischi operativi per mancanza di regolamentazione e di controllo pubblico (vedi *supra*).

Le motivazioni che possono portare una comunità a emettere una propria moneta virtuale sono molteplici (7) tra cui in forma esemplificativa:

(7) Cfr. K.L. MACINTOSH, *How to Encourage Global Electronic Commerce: The Case for Private Currencies on the Internet*, in *Harvard Journal of Law and Technology*, 1998, 11, 733; *Bitcoin, the Private Digital Currency*,

Capitolo V
RIFLESSIONI GIURIDICHE

Sommario: 5.1. Introduzione. — 5.2. Aspetti di inquadramento delle criptovalute. — 5.3. Proprietà. — 5.4. Protocollo: usi normativi, contrattuali o altro? — 5.5. Trasferimento di criptovalute. — 5.6. Cessione di beni e servizi contro criptovalute. — 5.7. Diritto internazionale privato.

5.1. *Introduzione.*

La panoramica mondiale dei principali documenti e decisioni emesse rileva l'assoluta eterogeneità interpretativa che non permette una definizione e la riflessione presentata sulle nozioni di concetti comuni hanno aperto la strada a alcuni ragionamenti logici e giuridici utili.

Le interpretazioni giuridiche delle innovazioni informatiche rischiano di essere sempre incomplete e parziali, anche perché occorre entrare nella logica della programmazione e della creazione di tali mondi virtuali e realtà virtuali: torna alla mente il pensiero di Lessig (1): "*il codice è la legge*" con inevitabile conseguenza che le regole del *software* sono semplici e brutali: chi controlla il *software* stabilisce le regole (2).

Il sistema delle criptovalute è costruito per non necessitare di altre regole se non quelle definite dal codice, che sono autosufficienti, complete e coerenti per il perfezionamento di una transazione. Nel momento in cui si entra nel "mondo" *bitcoin* e delle criptovalute in genere, si accetta tacitamente, ma espressamente quel codice, quell'insieme di regole scritte nel *software* e che, quindi, integrano i contratti che ne originano.

---

(1) L. Lessig, *Code and other laws of cyberspace*, Basic Books 1999.

(2) J. Grimmelmann, *Anarchy, Status Updates, and Utopia*, Pace L. Rev., http://ssrn.com/abstract=2358627 (sito web consultato, e documento disponibile online, il 7 marzo 2015).

Con l'accettazione, quel codice quindi diventa elemento esterno vincolante per le parti e crea un sistema che non necessita altro che se stesso per effettuare le transazioni. Detto aspetto, di rilevante importanza, deve essere tenuto in debita considerazione quando si introduce il tema della regolazione del sistema delle criptovalute.

La premessa tecnica è a questo punto utile per lo sviluppo del ragionamento, anche perché interpretare detta materia, in assenza sia della filosofia di fondo sia del funzionamento tecnico e informatico porta a risultati parziali, errati ed erronei.

Mentre il sistema è autosufficiente, la criptovaluta, come abbiamo visto è e, congiuntamente, non è una serie di concetti giuridici, ma configura l'uno piuttosto che un altro a seconda dello schema giuridico di riferimento.

L'architettura informatica delle criptovalute indica un futuribile sviluppo che potrebbe scuotere molti sistemi giuridici fino a qui dati per scontati e, in particolar modo, tutti quelli che presuppongono la presenza di un ente centralizzato, su cui una o più parti confidano per l'esecuzione di una transazione.

L'automatismo della rete *peer-to-peer* e il lavoro dei "*miners*" (il codice di Lessig) non consiste nel validare le transazioni attraverso valutazioni di merito, sul pregio della transazione o validità della stessa: si limitano a risolvere equazioni e funzioni al fine di verificare la disponibilità dell'unità di conto del mittente, la validità della sua firma e l'apposizione di un "*timestamp*". Non entrano nel merito, nel pregio giuridico, nel contenuto della transazione.

La transazione quindi è e resta autonomia privata, senza che terzi entrino o possano entrare nel merito della stessa. Una nuova complicazione è l'irrevocabilità della stessa, vale a dire che quando è firmata ed inserita nel sistema, la transazione è irretrattabile, non revocabile in alcun modo ed in alcuna maniera.

La genericità di tali affermazioni rende il compito assolutamente arduo per l'interprete, visto che le modalità di svolgimento di una transazione, così come il loro contenuto sono assolutamente infinite e con risvolti assolutamente diversi.

Un esempio su tutti: i *colored coins*. La definizione data in precedenza indica come l'unità di conto venga "colorata" per essere collegata ad un sottostante, quale un bene, un titolo o altro, con un database di metadati che sia in grado di collegare quel *colored coin* al sottostante.

In tale maniera l'unità di conto "*colored*" diventa un titolo rappresentativo di merci, o di titoli, di azioni e di titoli di credito seguendo le

regole proprie: potrebbe essere però collegato ad un servizio (un evento a teatro, credito telefonico, un film in streaming) ed in tal caso assumerebbe la configurazione di titolo di legittimazione, ma se è collegato un credito pecuniario diventa un credito.

Queste riflessioni indicano ulteriormente che rinchiudere in un concetto giuridico le criptovalute è riduttivo e pericoloso: occorre lasciare aperto il concetto e procedere a interpretazioni specifiche in ogni settore del diritto dopo aver ben compreso l'oggetto di analisi.

Il settore è in fase embrionale tale per cui la maggior parte delle interpretazioni effettuate si basa sul "prodotto" più famoso e diffuso: il *bitcoin*. In tal caso può essere (semplificando) analizzato quale unità di conto convertibile (3) e quindi presenta meno (!) problemi interpretativi, poiché l'oggetto di analisi è limitato.

Nel prosieguo ci limiteremo a analizzare le unità di conto delle criptovalute simili al *bitcoin*.

Dai documenti analizzati emergono definizione tecniche e giuridiche abbastanza eterogenee, perché eterogeneo è il mercato ed il settore. Ad oggi è abbastanza limitato, ma le implicazioni giuridiche che ne originano sono estremamente sfidanti.

I documenti presentati definiscono le criptovalute in maniera funzionale agli scopi per i quali sono stati emessi, confondendo valute virtuali, valute digitali, criptovalute e *bitcoin*. Lo sforzo del FAFT di definire un quadro comune riconosce detta problematica, cercando di dare un linguaggio comune agli sforzi antiriciclaggio.

Qualsiasi definizione giuridica si scontra inevitabilmente anche con l'ambiguità tra rete (*Bitcoin*) e unità di conto (*bitcoin*) che sono due facce della stessa medaglia, ma un'eventuale definizione dell'una può entrare in contraddizione con l'altra.

Riprendendo l'approccio "atomistico" le criptovalute presentato caratteristiche assimilabili a:

1) moneta, in quanto rispondono alle definizioni classiche economiche della stessa.

2) Valuta estera, in quanto non ha corso legale nella Nazione/e quindi è valuta estera per tutti.

3) *Commodity*, in quanto bene fungibile prodotto da un'attività umana e riconosciuto da una determinata comunità quale valore.

---

(3) Oggi nell'accettazione dell'unità di conto da parte del venditore di beni e servizi si analizza il cambio tra *bitcoin* e valuta a corso legale per attribuire la quantità di unità di conto per il bene e servizio ceduto.

4) Strumento Finanziario (*Securities*), in quanto la propria valutazione dipende dalla domanda ed offerta ed è scambiato in un mercato.

5) Beni Immateriali, dato che non esistono fisicamente.

6) Diritti di Baratto, dato che possono essere barattate con beni e servizi espressi in quella data unità di conto.

7) Sistema di pagamento, dato che può avere detta funzione.

E la loro definizione cambia nei vari contesti, similmente agli altri mezzi di scambio che non siano valute *fiat*.

Nel caso dell'oro, possiamo notare, che ha tre funzioni: *i*) moneta, *ii*) capitale e *iii*) materia prima e, a seconda dello schema di riferimento, cambia totalmente l'interpretazione giuridica e gli schemi applicabili (4). Da ciò è possibile, quindi, date anche le altre esperienze, indicare nei vari schemi di riferimento, le norme applicabili, con una doppia interpretazione:

— oggettiva: natura giuridica delle criptovalute in tale schema giuridico di riferimento;

— soggettiva: applicabilità di tali norme interpretando l'attività che quel determinato attore svolge nel sistema delle criptovalute.

Alcuni campi di indagine richiederanno la doppia analisi, sia da un punto di vista soggettivo sia oggettivo, altri solo uno.

Tale distinzione è utile per affermare che l'utente finale non è soggetto ad alcuna restrizione e che l'utilizzo a fini privati di criptovalute non è vietato da alcuna norma in Italia (5) né in Europa. La detenzione, l'utilizzo, l'acquisto e la cessione non sono soggette ad alcuna restrizione né ad alcuna comunicazione.

Detto aspetto risponde alla libertà che ogni individuo ha di acquistare qualsiasi bene che non sia vietato da norma imperative di legge e di disporne, senza alcuna limitazione.

Lo svolgimento di attività legate al mondo delle criptovalute impone una profonda riflessione delle normative applicabili, dei limiti

---

(4) S. Capaccioli, *Commercio all'ingrosso di metalli preziosi: inquadramento Amministrativo e Tributario*, Diritto e Pratica Tributaria, Edizioni CEDAM, Vol. LXXXI - n. 5/2011 p. 1025-1047.

(5) "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" in Banca d'Italia, *Avvertenza sull'utilizzo delle cosiddette "valute virtuali"*, 30 gennaio 2015, in http://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf (sito web consultato, e documento disponibile online, il 7 mar

Capitolo VI
IMPOSTA SUL VALORE AGGIUNTO

6.1. *Imposta sul Valore Aggiunto (IVA).*

L'inquadramento IVA (1) delle *criptovalute* e dei *bitcoin* deve essere necessariamente affrontato in chiave europea, poiché la normativa interna (D.P.R. 26 ottobre 1972 n. 633) trova la sua fonte interpretativa nelle direttive Iva della Unione Europea ed in particolare la Direttiva n. 2006/112/CE, pubblicata l'11 dicembre 2006 nella Gazzetta Ufficiale dell'Unione europea (in vigore dal 1° gennaio 2007).

---

(1) Il presente capitolo è una rielaborazione di alcuni articoli: S. Capaccioli, *Criptovalute, bitcoin e IVA* su "Il Fisco", n. 27/2014 Edito da Il Fisco - WKI Ipsoa pp. 2671-2678, S. Capaccioli, *VAT & bitcoin*, su EC Tax Review, Kluwer Law, Volume 23 (2014), Issue n. 6., S. Capaccioli, *Value Added Tax & bitcoin: a summary*: in Bitcoin Magazine 09.09.2014, http://bitcoinmagazine.com/16197/value-added-tax-vat-*bitcoin*-summary/ (sito web consultato, e documento disponibile online, il 7 marzo 2015) , S. Capaccioli, *VAT & BITCOIN: Update from Bruxelles*: in *Bitcoin* Magazine - 26.09.2014 — http://bitcoinmagazine.com/16810/vat-*bitcoin*-update-bruxelles/ (sito web consultato, e documento disponibile online, il 7 marzo 2015), S. Capaccioli i, *VAT & bitcoin — are bitcoin exchange transactions exempt from the VAT Directive?,* in Blog of Durham European Law Institute, June 24, 2014 https://delilawblog.wordpress.com/2014/06/24/vat-bitcoin-are-bitcoin-exchange-transactions-exempt-from-the-vat-directive/ (sito web consultato, e documento disponibile online, il 7 marzo 2015).

Detta direttiva costituisce la riscrittura (*recasting*) della Direttiva n. 77/388 del 17 maggio 1977 (più nota come VI direttiva), ai soli fini di chiarezza e razionalizzazione per tener conto delle diverse modifiche intervenute nel corso degli anni.

La direttiva è un atto obbligatorio per la necessità di pervenire ad un determinato risultato, lasciando la scelta ai singoli Stati destinatari delle misure più idonee per il raggiungimento dello stesso, necessitando, quindi, di atti normativi nazionali che permettano il loro recepimento nell'ordinamento interno.

La matrice comunitaria dell'IVA porta necessariamente ad un'analisi delle interpretazioni svolte nei vari Stati Membri per verificare le varie posizioni e la consistenza delle stesse.

Sull'argomento del trattamento IVA delle criptovalute vi è stata molta esitazione all'inizio, con alcune affermazioni e successive retromarce (quale ad esempio, l'affermazione del Ministero Britannico di assimilazione a *voucher* con assoggettamento ad Iva poi ritirata visto che il bene e/o il servizio non è identificato né identificabile a priori e non vi è nessun emittente).

Ad oggi, pende presso la Corte di Giustizia dell'Unione Europea (2) la questione pregiudiziale sul trattamento Iva dei *bitcoin* a norma dell'art. 267 TFUE da parte della Corte Suprema Amministrativa Svedese.

Prima di affrontare il merito della questione pendente presso la Corte di Giustizia riteniamo necessario passare in rassegna tutte le interpretazioni fino ad oggi apparse in merito a tale argomento, compreso il *Ruling* che ha originato il rinvio pregiudiziale.

La direttiva IVA 112/2006/CE stabilisce che le prestazioni di servizi sono definite all'art. 24 come qualsiasi operazione che non costituisce una cessione di un bene, categoria residuale interpretata dalla Corte in maniera estensiva. Non per altro, l'art. 25 della Direttiva 112/2006/CE precisa che la prestazione di servizi può consistere, tra l'altro, in una cessione di beni immateriali, rappresentati o meno da un titolo.

Le prestazioni di servizi effettuate a titolo oneroso, effettuate da un soggetto passivo che esercita in modo indipendente un'attività economica, sono imponibili Iva ed è fuori discussione che la cessione di criptovaluta costituisca un servizio consistente nella cessione di beni

---

(2) La questione è pervenuta in Corte di Giustizia dell'Unione Europea il 2 giugno 2014, contrassegnato da C-264/14 Hedqvist.

immateriali e non rientri nei servizi prestati per via elettronica di cui dell'art. 56, comma 1 lett. *k*) ed allegato II, della direttiva.

Alcune transazioni sono esentate da IVA: le esenzioni IVA sono previste nella direttiva IVA e quelle rilevanti a questi fini sono contenute dell'art. 135.1:

> 1. Gli Stati membri esentano le operazioni seguenti: (...)
> *b*) la concessione e la negoziazione di crediti nonché la gestione di crediti da parte di chi li ha concessi; (...)
> *d*) le operazioni, compresa la negoziazione, relative ai depositi di fondi, ai conti correnti, ai pagamenti, ai giroconti, ai crediti, agli assegni e ad altri effetti commerciali, ad eccezione del recupero dei crediti;
> *e*) le operazioni, compresa la negoziazione, relative a divise, banconote e monete con valore liberatorio, ad eccezione delle monete e dei biglietti da collezione ossia monete d'oro, d'argento o di altro metallo e biglietti che non sono normalmente utilizzati per il loro valore liberatorio o presentano un interesse per i numismatici;
> *f*) le operazioni, compresa la negoziazione ma eccettuate la custodia e la gestione, relative ad azioni, quote parti di società o associazioni, obbligazioni e altri titoli, ad esclusione dei titoli rappresentativi di merci e dei diritti o titoli di cui all'articolo 15, paragrafo 2; (...).

La questione verte sull'interpretazione di tale articolo e se la cessione di criptovaluta rientri o meno in una di queste esenzioni.

6.2. *Primo* Ruling *in Svezia.*

L'Autorità Svedese per il Ruling ha affrontato la problematica, con la Decisione (3) 2013-10-14 (ref. 32-12./I) relativa al commercio di *bitcoin* (*Mervärdesskatt: Handel med bitcoins*). In particolare, l'oggetto dell'interpello consisteva nella richiesta se l'acquisto e la vendita di *bitcoin* (cambio di *bitcoin* da e verso la Corona Svedese) fossero soggetti ad Iva.

Il contribuente riteneva tali transazioni non assoggettabili all'Iva (anche perché la soggezione al tributo renderebbe i *bitcoin* inutili come moneta), mentre l'Autorità Tributaria, nonostante prendesse atto che le attività di cambio tra *bitcoin* e Corona Svedese non implicassero alcun attività di consumo, riteneva tali transazioni quali servizi imponibili Iva,

---

(3) SKATTERATTSNAMNDEN, *Mervärdesskatt: Handel med bitcoins,* 14.10.2013 in http://skatterattsnamnden.se/skatterattsnamnden/forhandsbesked/2013/forhandsbesked2013/mervardesskatthandelmedbitcoins.5.46ae6b26141980f1e2d29d9.html (sito web consultato, e documento disponibile online, il 7 marzo 2015).

non essendo coperti da alcuna esenzione, dato che i *bitcoin* non sono moneta legale.

La Decisione, pur non entrando nella qualificazione giuridica delle criptovalute, si basa sul presupposto che l'esenzione Iva deve essere interpretata alla luce dell'articolo 135.1 della direttiva Iva 2006/112/CE e sulla base della Sentenza della Corte Europea (caso C-172/96, *First National Bank of Chicago*) e dallo Studio della BCE la Decisione rileva come le operazioni di cambio non implichino l'addebito di alcuna commissione per il servizio di scambio. Inoltre, nonostante l'assenza di corso legale, la Corte Europea (Sentenza 7/78 Thompson et al. relativo ai *krugerrand*) ha constatato come il concetto di mezzo legale di pagamento e l'equivalenza alla moneta siano riferiti all'accettazione di tali strumenti in un mercato monetario, anche in presenza di dubbi sulla validità del corso legale.

L'assenza di una definizione nella Direttiva Iva del termine "moneta" porta all'interpretazione della stessa quale mezzo di pagamento, con l'ulteriore domanda se la dizione prevista nell'art. 135.1. lettera *e*) "con valore liberatorio" prevista per "banconote e monete", si riferisca anche alle valute. La presenza dell'eccezione delle "monete e dei biglietti da collezione" che certamente hanno corso legale, ma non sono normalmente utilizzati come tali perché sono oggetti da collezione, indica che il concetto di corso legale sia riferito solo alle monete ed alle banconote. Ciò esclude il concetto di "divisa" dalla necessità del corso legale.

Sulla base di queste riflessioni e prendendo spunto dal fatto che:

— l'intermediazione di *bitcoin* richiede requisiti similari ai servizi finanziari,

— i *bitcoin* sono un mezzo di pagamento utilizzato in modo simile alla moneta a corso legale,

— i *bitcoin* presentano forti analogie con moneta elettronica.

L'Autorità Svedese per il *Ruling* ha ritenuto che le transazioni di *bitcoin* debbano essere considerate operazioni relative a divise di cui all'articolo 135.1. lett. *e*), coerentemente con le finalità delle deroghe di cui all'articolo 135.1. (evitare le difficoltà di applicazione Iva connesse con i servizi finanziari). L'Autorità Tributaria Svedese ha appellato detto *Ruling* alla Corte Suprema Amministrativa che ha risolto il caso con rinvio pregiudiziale alla Corte di Giustizia, che analizzeremo successivamente.