Pubblicazione Trimestrale

ISSN: 2279-9737

Rivista di Diritto Bancario

dottrina
e giurisprudenza
commentata

Ottobre/Dicembre

2018

rivista.dirittobancario.it

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

NORME PER LA VALUTAZIONE E LA PUBBLICAZIONE

La Rivista di Diritto Bancario seleziona i contributi oggetto di pubblicazione sulla base delle norme seguenti.

I contributi proposti alla Rivista per la pubblicazione vengono assegnati dal sistema informatico a due valutatori, sorteggiati all'interno di un elenco di ordinari, associati e ricercatori in materie giuridiche, estratti da una lista periodicamente soggetta a rinnovamento.

I contributi sono anonimizzati prima dell'invio ai valutatori. Le schede di valutazione sono inviate agli autori previa anonimizzazione.

Qualora uno o entrambi i valutatori esprimano un parere favorevole alla pubblicazione subordinato all'introduzione di modifiche aggiunte e correzioni, la direzione esecutiva verifica che l'autore abbia apportato le modifiche richieste.

Qualora entrambi i valutatori esprimano parere negativo alla pubblicazione, il contributo viene rifiutato. Qualora solo uno dei valutatori esprima parere negativo alla pubblicazione, il contributo è sottoposto al Comitato Esecutivo, il quale assume la decisione finale in ordine alla pubblicazione previo parere di un componente della Direzione scelto ratione materiae.

2018 | 2019

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

SEDE DELLA REDAZIONE

Università degli Studi di Trento, Facoltà di Giurisprudenza, via Verdi 53,
(38122) Trento – tel. 0461 283836

2018 | 2019

MICHELE BELLINO

I rischi legati al nuovo sistema *bitcoin*: i nuovi intermediari

SOMMARIO: 1. Il problema – 2. Il limitato apporto dell'intervento di materia – 3. I rischi legati ai "nuovi intermediari". – 3.1I rischi per l'utente – 3.2. I rischi per l'efficiente funzionamento del mercato – 4. Considerazioni conclusive

1. *Il problema*

Nel 2009 Satoshi Nakamoto, una figura sulla quale regna un fitto alone di mistero e curiosità, ha rilasciato i codici sorgenti di *Bitcoin*, un sistema informatico che permette l'emissione e lo scambio di una moneta digitale, il *bitcoin*, in maniera totalmente decentralizzata ed indipendente da qualsiasi autorità centrale.

Da quando è stato lanciato, *Bitcoin* ha sempre più fatto parlare di sé. All'entusiasmo per l'aumento del suo valore e all'interesse circa l'innovativa tecnologia che ne è alla base, la *blockchain*, si sono accompagnate tuttavia le preoccupazioni legate ai possibili utilizzi illeciti di questo strumento, i timori riguardanti il formarsi di una bolla speculativa pronta a scoppiare, gli interrogativi sulla sua natura giuridica e sulla possibile regolamentazione dello strumento e dei soggetti che prestano servizi relativi all'utilizzo delle valute virtuali.

A riguardo, bisogna constatare come l'intervento statale non può investire ogni aspetto di *Bitcoin*.

Il codice informatico disciplina l'emissione della moneta, la modalità di validazione delle transazioni, la tenuta di quel particolare registro contabile che è la *blockchain* ed i modi in cui gli utenti possono trasferire i propri *bitcoin*: su questi aspetti nessun legislatore può intervenire.

L'intervento del regolatore invece è possibile e necessario sui punti di contatto tra il circuito delle valute virtuali ed il "mondo reale".

Bitcoin appartiene alle monete digitali che permettono un flusso bidirezionalee che quindi possono essere acquistate e vendute ad un determinato tasso di cambio mediante valuta tradizionale.

Sebbene *Bitcoin* possa funzionare anche senza l'intervento di imprese o intermediari (l'unica attività necessaria alla validazione delle transazioni ed alla tenuta della *blockchain* è il *mining*), lo sviluppo dello strumento ha portato alla nascita di un vasto ecosistema di imprese che forniscono servizi relativi all'utilizzo delle valute virtuali, tra i quali spiccano per importanza gli *exchanges* e i *wallet providers*.

2. *Il limitato apporto dell'intervento di materia*

Le valute virtuali sono state immediatamente poste sotto la lente d'ingrandimento delle Autorità di vigilanza, delle agenzie di *law enforcement* e della dottrina, che si sono interrogate riguardo ai rischi correlati al loro utilizzo.

Dei rischi correlati all'ecosistema Bitcoin si è occupata approfonditamente l'*European Banking Authority* che, nel suo studio "*Opinion on 'virtual currencies'*"[1], ha individuato circa settanta rischi correlati all'utilizzo delle valute virtuali.

Uno degli aspetti di *Bitcoin* che più hanno destato allarme è lo pseudonimato[2] nelle transazioni.

Ogni transazione in *bitcoin* è trascritta eternamente nella *blockchain*, dalla quale non può essere cancellata o alterata in alcun modo; inoltre, la *blockchain* è un registro accessibile a chiunque: ogni utente è a conoscenza delle transazioni di tutti gli altri utenti.

Sotto questo aspetto, *Bitcoin* è assolutamente meno anonimo rispetto al denaro contante, le cui transazioni sono realmente non tracciabili.

D'altro canto, è chiaro che un sistema del genere pone particolari problemi in materia di privacy: se i nomi delle parti delle transazioni fossero "in chiaro", utilizzare *Bitcoin* sarebbe come condividere con tutti i dati del nostro conto corrente. Per questo, le chiavi pubbliche sono rese anonime: non esiste un registro che colleghi gli indirizzi *bitcoin* (derivanti dalle chiavi pubbliche) ai reali utilizzatori dello strumento.

---

[1] EUROPEAN CENTRAL BANK, "*Virtual currency schemes*", ottobre 2012, p. 14, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (sito web visitato e documento disponibile online il 18/04/2018).

[2] Per una classificazione di questi nuovi attori si veda G. ARANGÜENA, *Bitcoin: una sfida per policymakers e regolatori, in Quaderni di diritto, mercato e tecnologia,* 2014, I, https://www.dimt.it/wp-content/uploads/2014/07/Giulia-Aranguena-DIMT2014_1.pdf (sito web visitato e documento disponibile online il 18/04/2018).

Lo pseudonimato permesso dal sistema, unito alla vocazione globale dello strumento, alla naturale assenza di intermediari nelle transazioni, alla rapidità dei trasferimenti ed al loro basso costo, ha subito destato preoccupazioni[3] riguardo gli utilizzi illeciti dello strumento.

La prima normativa italiana in materia di valute virtuali è stata introdotta proprio in tema di antiriciclaggio con il d.lgs. 25 maggio 2017, n. 90 che, nell'attuare la IV direttiva antiriciclaggio, ha inserito anche le norme contenute nella proposta di modifica della IV direttiva antiriciclaggio attualmente oggetto di discussione in sede europea.

Sebbene l'intervento normativo finalizzato al combattere gli utilizzi illeciti delle valute virtuali sia encomiabile, altre misure sono necessarie affinché l'ecosistema Bitcoin diventi sempre più affidabile e possa svilupparsi in modo organico.

3. *I rischi legati ai "nuovi intermediari"*

Come abbiamo già accennato, l'ascesa del *Bitcoin* e delle criptovalute ha portato alla nascita e allo sviluppo di una serie di imprese che forniscono servizi relativi all'utilizzo delle valute virtuali. Fino al d.lgs. 90/2017, l'attività di questi operatori non era sottoposta ad alcuna disciplina[4] ed era quindi da ritenersi completamente libera.

La normativa attuale, invece, impone a tutti i prestatori di servizi relativi all'utilizzo di valuta virtuale (così come definiti dall'art. 1 co. 2 lett. ff) del d.lgs. 231/07) di iscriversi in una sezione speciale del registro tenuto dall'OAM ai sensi dell'art. 128-*undecies* TUB e assoggetta gli *exchange* agli obblighi della normativa antiriciclaggio.

L'intervento normativo affronta il problema dell'utilizzo illecito delle valute virtuali, mirando a tracciare i flussi di denaro in entrata ed in uscita dal relativo circuito, ma lascia insoluti alcuni problemi legati a questi nuovi intermediari.

---

[3] Financial Action Task Force, in "*FATF Report: Virtual currencies, key definitions and potential AML/CFT Risks*", giugno 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (sito web consultato e documento disponibile online il 18/04/2018).

[4] L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D. Lgs. 90/2017*", in questa *Rivista*, 2018, V.

3.1. *I rischi per l'utente*

I rischi relativi agli *exchange* riguardano, per un primo versante, la loro sicurezza informatica e la sicurezza dei fondi che i clienti gli affidano. Un utente prudente, dopo aver acquistato *bitcoin* tramite l'*exchange*, dovrebbe spostarli su un proprio *wallet* personale, in modo da avere il controllo esclusivo delle chiavi crittografiche funzionali per disporre dei *bitcoin*.

In particolare, una parte di questi *bitcoin*, necessaria per eventuali transazioni quotidiane, dovrebbe essere tenuta su *hot wallet* (portafogli memorizzati su dispositivi collegati alla rete), mentre la maggior parte andrebbe conservata su *cold wallet* (dispositivi che normalmente sono scollegati dalla rete), in modo da minimizzare i rischi derivanti da un attacco informatico.

Tuttavia, gli utenti, quando acquistano criptovalute, spesso non spostano le chiavi private su un *wallet* privato, ma lasciano che a custodirle siano gli *exchange*, che agiscono quindi anche come *wallet*. La differenza tra *wallet* ed *exchange* va sempre più sfumando: il 52% dei *wallet* offre anche servizio di *exchange*.

Gli *exchange* sono spesso al centro delle attenzioni degli *hackers*, che mediante attacchi informatici cercano di sottrarre loro le criptovalute: spesso questi attacchi determinano delle perdite ingenti, a carico degli utenti e dello stesso *exchange*.

Il più famoso *exchange* che, il 24 febbraio 2014, ha dovuto cessare la propria attività a causa di ripetuti attacchi informatici è stato "Mt. Gox": il *default* ha causato la perdita di circa 850.000 *bitcoin* (100.000 del proprio patrimonio e 750.000 degli utenti)[5], pari a circa 350 milioni di dollari al tasso di cambio dell'epoca.

Purtroppo, il caso Mt. Gox non è stato un caso isolato ed altri incidenti hanno coinvolto gli *exchange*.

Un altro significativo incidente coinvolge, nell'estate del 2016, la piattaforma "Bitfinex", la più utilizzata per cambiare *bitcoin* con valuta *fiat*, che subisce una perdita di 200.000 *bitcoin*, pari a circa 72 milioni di dollari.

[5] G. LEMME, S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin*, in questa *Rivista*, estratto dal n. 11, 2016, 25.

A gennaio 2018 è stato *hackerato* "*Coincheck*", che ha subito una perdita di 523 milioni di NEM, pari ad oltre 500 milioni di dollari, ma in questo caso la società si è detta disponibile a rimborsare i clienti con capitali propri.

A febbraio 2018, un piccolo *exchange* italiano, BitGrail, ha subito una perdita di 17 milioni di NANO, una criptovaluta sviluppata da un team americano. Dopo l'incidente il team di sviluppo e l'*exchange* hanno avuto degli scontri fortissimi: sull'intera vicenda indaga la magistratura, mentre la società il 14 marzo ha dichiarato che, alla riapertura del sito, istituirà un fondo cassa dedicato alle vittime del furto di NANO.

Il 7 marzo 2018, "Binance" ha lanciato l'allarme circa alcune attività sospette, bloccando i prelievi: la notizia ha fatto crollare il valore di *bitcoin* da $ 10,700 a $ 9,500 in un'ora.

Gli *hackers*, con vari attacchi *phishing*, avevano rubato le credenziali di accesso di alcuni utenti e il 7 marzo tramite questi *account*, hanno acquistato in massa una criptovaluta chiamata Viacoin, facendone salire vertiginosamente il prezzo[6]; nel frattempo, trentuno utenti di Viacoin, realizzavano enormi profitti, vendendo sui massimi.

Nella stessa giornata Binance ha chiarito che tutti i fondi erano al sicuro[7].

Dagli esempi fin qui riferiti risulta chiaro come sia preferibile gestire da sé le proprie criptovalute, in modo prudente ed avendo una minima conoscenza degli strumenti in questione.

Nel momento in cui un utente delega la custodia della propria criptovaluta ad un altro soggetto, nascono i problemi relativi alla sua tutela: il primo riguarda il furto delle credenziali di accesso al sito del fornitore del servizio (come è avvenuto con il caso Binance); il secondo riguarda le difese informatiche con le quali gli *exchange* si difendono da questi attacchi.

---

[6] P. VIGNA, *Reports of Problems at Crypto Exchange Send Bitcoin Tumbling*, in *The Wall Street Journal*, 7 marzo 2018, https://www.wsj.com/articles/reports-of-problems-at-crypto-exchange-send-bitcoin-tumbling-1520456666.

[7] Binance, https://support.binance.com/hc/en-us/articles/360001547431-Summary-of-the-Phishing-and-Attempted-Stealing-Incident-on-Binance.

Per risolvere il primo problema, il 75% degli *exchange* offre la possibilità agli utenti di abilitare la *two-factor autentication* (2FA)[8] per accedere al proprio conto e il 77% offre la possibilità di utilizzare la 2FA per prelevare fondi dal proprio *account*.

Alcuni *exchange* utilizzano la 2FA anche dal lato amministrativo, affinché nessuno possa rubare le credenziali di accesso all'amministratore per rubare fondi.

Per quanto riguarda la sicurezza delle chiavi crittografiche, la maggior parte degli *exchange* fa ricorso a sistemi di *cold storage.*

Tuttavia, queste misure non bastano, e la strada per realizzare un ambiente sicuro è ancora lunga.

3.2. *I rischi per l'efficiente funzionamento del mercato*

In altri casi – e per un secondo, distinto versante - gli incidenti ed i problemi riscontrati sono meno eclatanti di quelli visti finora, ma comunque sono preoccupanti e costituiscono un nodo da sciogliere con la regolamentazione dell'universo dei prestatori di servizi relativi alle criptovalute.

Spesso gli *exchange* ed i *wallet provider* non sono dotati di un'infrastruttura tecnica all'altezza del traffico cui sono soggetti, e non riescono a gestire i picchi di scambi[9], spesso in corrispondenza di grandi fluttuazioni di valore[10]; in altri casi, si verificano interruzioni del servizio più o meno lunghe, dovuti a malfunzionamenti o ad aggiornamenti e migliorie dell'*exchange*.

Altri problemi riguardano la formazione del tasso di cambio bitcoin/valuta *fiat*, che risulta essere diverso, spesso in maniera considerevole, tra un *exchange* e l'altro; nel mondo della finanza

[8] Nei sistemi protetti da 2FA, l'autenticazione dell'utente avviene in due fasi. Nella prima fase, l'utente deve inserire le credenziali di accesso al sito web; la seconda fase può consistere nel cliccare su un link inviato alla mail dell'utente (ecco perché è importante utilizzare sempre *password* diverse per i propri *account*), nell'inserire sul sito una *password* ricevuta via mail o via sms.

[9] D. FUMAGALLI, *Il Bitcoin rischia di divenire illiquido*, https://www.milanofinanza.it/news/il-bitcoin-rischia-di-diventare-illiquido 201712080834254721

[10] A. SIMEONE, *Dagli albori del Web alla Blockchain: molte luci e alcune ombre*, in https://www.aspeninstitute.it/aspenia-online/article/dagli-albori-del-web-alla-blockchain-molte-luci-e-alcune-ombre.

tradizionale, questo non può accadere, e gli algoritmi impediscono l'arbitraggio[11], mentre nel mondo delle criptovalute le differenze di valore tra un *exchange* e un altro possono essere considerevoli.

Infine, altri dubbi riguardano una vera e propria manipolazione del mercato che potrebbe essere in atto a causa di Tether, una criptovaluta emessa da Tether Limited e che si asserisce sia emessa solo a seguito della ricezione, da parte della società emittente, di un dollaro: il tasso di cambio tra Tether e dollaro dovrebbe quindi essere costante e pari ad uno.

Tether dovrebbe quindi permettere agli utenti di utilizzare una criptovaluta stabile anche su *exchange* che non riescono ad avere rapporti con le banche.

La società che emette Tether ha interrotto i rapporti con l'*auditor*, e questo ha ingenerato il timore che non abbia le coperture necessarie a garantire il tasso di cambio paritario tra Tether e dollaro[12]. Se così fosse, il mercato delle criptovalute sarebbe stato drogato, perché l'emissione incontrollata di Tether "scoperti" avrebbe fatto alzare il prezzo del Bitcoin e delle altre criptovalute. Per questo la CFTC americana ha deciso di citare in giudizio Tether e Bitfinex, al fine di fare maggiore chiarezza su questi aspetti[13].

In questa atmosfera, l'*attorney general* di New York ha inviato un questionario a tredici *exchange*, al fine di ottenere informazioni riguardo i loro assetti proprietari e il controllo, le operazioni e le commissioni applicate, le procedure, le interruzioni e le altre sospensioni delle attività, i controlli interni, il rispetto della normativa relativa alla privacy e all'antiriciclaggio.

Scopo dell'iniziativa è quello di assumere informazioni e aumentare la trasparenza e l'affidabilità del mercato delle valute virtuali.

---

[11] V. LOPS, *Bitcoin: piattaforma che vai prezzo che trovi*, in http://www.ilsole24ore.com/art/finanza-e-mercati/2017-12-09/bitcoin-oltre-volatilita-ora-c-e-rebus-prezzo-101938.shtml?uuid=AE6KDePD.

[12] P. SOLDAVINI, "*Cos'è Tether, la criptovaluta legata al dollaro che fa tremare il Bitcoin",* http://www.ilsole24ore.com/art/notizie/2018-02-09/cos-e-tether-criptovaluta-legata-dollaro-che-fa-tremare-bitcoin-182417.shtml?uuid=AELm3WxD.

[13] M. TEREKHOVA, *Tether and Bitfinex subpoenaed by the CFTC*, http://www.businessinsider.com/tether-and-bitfinex-subpoenaed-by-the-cftc-2018-1?IR=T.

4. *Considerazioni conclusive*

Arrivati alla fine di questa panoramica sui rischi correlati all'ecosistema Bitcoin, non ci resta che prendere atto che, nonstante il legislatore italiano sia già intervenuto per arginare gli utilizzi illeciti delle valute virtuali, ancora molto c'è da fare affinché il mercato delle criptovalute possa anche solo pensare di raggiungere il grado di affidabilità dei mercati tradizionali.

In particolare, per fronteggiare le due aree di rischi sopra individuate - bisognerebbe intervenire con maggior forza sui profili relativi alla trasparenza ed alla stabilità finanziaria degli *exchange*, nonché elaborare delle regole circa la loro struttura tecnica e i requisiti di professionalità necessari allo svolgimento di un'attività così particolare ed esposta a rischi, come peraltro era stato già suggerito nel 2014 dall'EBA[14].

Gli *exchange* fanno da anello (debole) di congiunzione tra la valuta virtuale ed il mondo reale: finché il loro operato non sarà trasparente e non si avrà una sufficiente affidabilità degli stessi, le criptovalute non potranno svilupparsi in maniera affidabile per gli utenti.

[14] EUROPEAN BANKING AUTHORITY*, op. cit*., 39 ss.