Data di pubblicazione: 15 novembre 2016

Bitcoin e antiriciclaggio

di Nina Passarelli

Abstract

L'era *digital* ha ampliato gli orizzonti e ridotto al minimo le distanze. In questo modo tutto è acquistabile in ogni luogo e in qualsiasi momento. E con i *bitcoin* – la moneta virtuale che consente di ottenere beni reali in modo decentralizzato e senza l'ausilio di intermediari finanziari - queste transazioni possono diventare sempre più 'anonime'.

Molti studi recenti sull'argomento si sono focalizzati sul 'fenomeno *bit'* lodandone, in alcuni casi, i vantaggi o aprendo, in altri, inquietanti scenari circa i possibili rischi di riciclaggio e finanziamento al terrorismo. Su queste basi scientifiche l'articolo vuole fornire al lettore un inquadramento e una riflessione su un tema di grandissima attualità.

Profilo dell'autore

Nina Passarelli è laureata in Economia Aziendale presso l'Università della Calabria. Ha svolto il suo lavoro di ricerca per la tesi finale presso la Rheinische Fachhochschule Köln a Colonia (Germania) partecipando, tra l'altro, alla Berlin Crowdsourcing Week, conferenza sullo sviluppo del crowdfunding, del crowdinvesting e sulle misure da adottare a livello normativo e di antiriciclaggio.

Keyword

blockchain, riclaggio

1. Introduzione

Ogni innovazione tecnologica ha in sé un rischio intrinseco, dall'inizio alla fine del suo ciclo di vita, ma, nonostante ciò, il genere umano non può fare a meno di introdurre nuovi sistemi, nuovi ordinamenti, nuovi metodi. Diverso è il grado di novità apportabile: le innovazioni incrementali consistono nel perfezionamento di un prodotto, di un processo o di un servizio rispetto al modello esistente e mirano allo sviluppo della qualità, delle prestazioni, dell'adattabilità dei prodotti, nonché alla riduzione dei costi di produzione o di vendita. Le innovazioni radicali, invece, rappresentano un salto di qualità rispetto ai prodotti e ai processi disponibili e, di norma, sono legate ai risultati di ricerche nei laboratori industriali o di quelli negli enti pubblici o nelle università.

Stabilire se i vantaggi superino i deficit connessi all'ammodernamento è il compito più complesso cui sono chiamati gli Stati moderni. È il caso di *Bitcoin*, innovativo sistema elettronico di pagamento , che ha consentito la creazione del cosiddetto 'contante digitale'[1]. Per capire tale espressione è necessario fare un passo indietro e analizzare le caratteristiche peculiari delle due

monete finora esistenti e operanti nel sistema monetario pre-*Bitcoin*: la moneta 'fisica' e la moneta 'elettronica'. La prima presenta i vantaggi di essere accessibile a chiunque, anche senza l'apertura di un Conto Corrente o il possesso di un dispositivo elettronico; inoltre è anonima, in quanto non è necessario ai fini del pagamento né indicare l'identità del mittente né quella del beneficiario né tantomeno una causale, tutelando così la privacy. La moneta elettronica, invece, ha la prerogativa di essere di agevole utilizzo (basti pensare, ad esempio, al bancomat o alla carta di credito nel portafoglio), non deve essere cambiata alla frontiera e consente il pagamento a distanza, anche in maniera 'programmata' (come nei pagamenti periodici), e, soprattutto, è tracciabile.

Il sistema *Bitcoin* ambisce proprio ad inserirsi a cavallo fra queste due monete, traendone i rispettivi vantaggi, e, per tale motivo, viene definito come 'contante digitale'[2], in quanto consente sia di effettuare pagamenti a distanza sia di essere anonimo (o meglio, come diremo ,'pseudonimo') e di non supportare commissioni di intermediazione. L'ambizione del suo creatore, conosciuto con lo pseudonimo di Satoshi Nakamoto, è quella di costituire una nuova moneta in grado, non solo, di trasferire potere d'acquisto ma di 'crearlo', essendo unità di conto, mezzo di scambio e riserva di valore, indipendente dalla presenza di intermediari finanziari. Da qui la sua natura *peer-to-peer* (P2P) ovvero di rete locale in cui ognuno dei computer collegati, al pari di tutti gli altri, ha accesso alle risorse comuni, senza che vi sia un'unità di controllo dedicata come server[3]; nel caso specifico, quindi, nessuna autorità centrale emette nuova moneta o traccia le transazioni. Tali compiti vengono gestiti collettivamente dalla rete. Questo vuol dire che *Bitcoin* non mira solo a mettere in discussione il sistema dei pagamenti, ma l'intero sistema monetario. Alla stregua delle monete finora note, infatti, è dotato sia di un codice a tre cifre che di un simbolo (simbolo: ฿; codice: BTC o XBT).

La caratteristica che più lo differenzia dalle monete precedenti è il suo essere 'attivo' di chi lo detenga senza comportare il 'passivo' di nessun altro[4]: mentre la moneta scritturale, creata dalle banche commerciali, e quella metallica, emessa dalle banche centrali, costituiscono un credito del possessore a fronte di un debito dell'istituto, *bitcoin*, invece, è, per sua natura, più simile all'oro, essendo un attivo di chi lo detiene senza essere il passivo di nessun altro. Per tale ragione viene spesso definito come 'oro digitale' , in quanto, come l'oro, possiede concreto potere d'acquisto solo nel caso in cui ci sia qualcosa da acquistare e qualcuno disposto a ricevere *bitcoin* in cambio di un bene più utile. *Bitcoin*, come sistema di pagamenti, a differenza dei sistemi e circuiti di credito finora presenti, non consente di trasferire euro, dollari o altre valute, ma solo *bitcoin.* è cioè sistema di pagamento e moneta al tempo stesso. Diversa è anche la sua frazionabilità: mentre le precedenti valute sono divisibili fino al centesimo (10^{-2}), *bitcoin* è frazionabile fino al centomilionesimo (10^{-8}) e il suo più piccolo sottomultiplo, in omaggio al suo inventore, è denominato *satoshi*.

Altro aspetto peculiare di bitcoin è la sua 'scarsità artificiale': come, l'oro, che presenta una scarsità naturale, legata alla quantità disponibile della risorsa e alla sua difficile estrazione, anche per *bitcoin* è stata definita una scarsità 'artificiale'[5], determinata dal protocollo informatico, il cosiddetto *whitepaper*[6] che stabilisce arbitrariamente la sua quantità e rende complessa la sua creazione. La quantità di *bitcoin* nel tempo, quindi, cresce a ritmi decrescenti, fino a stabilizzarsi, a regime, sulla soglia dei 2100 miliardi di *satoshi* (Figura 1)[7]. Lo scopo dei suoi programmatori è mirare, in tale modo, a rimuovere il 'fattore umano', eliminando, grazie alla tecnologia peer-to-peer, la presenza di intermediari finanziari e rendendo questa moneta tecnica, automatica, esogena, decentrata e demandata al controllo degli utenti[8].

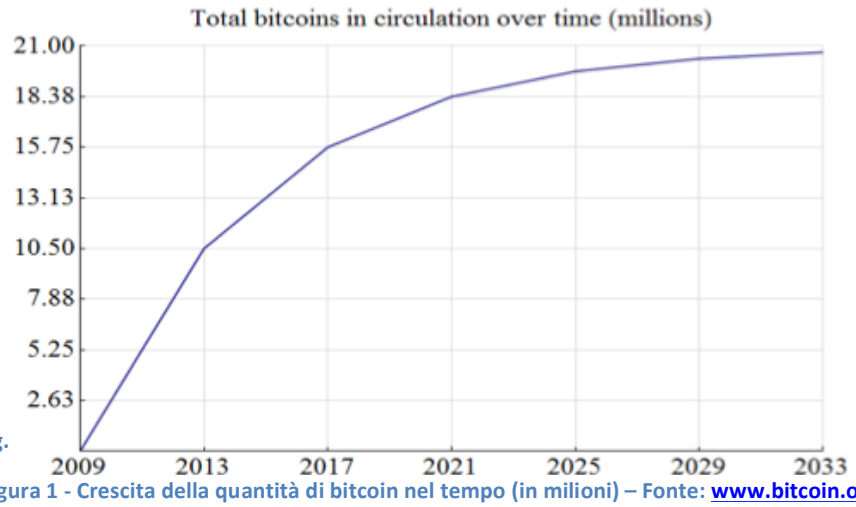

Fig.

Figura 1 - Crescita della quantità di bitcoin nel tempo (in milioni) – Fonte: www.bitcoin.org

La tenuta dei conti, infatti, non è più 'centralizzata', ma è affidata alla rete (*distributed ledger*) e il libro mastro pubblico che registra ognuna delle transazioni *bitcoin* poggia su una struttura dati chiamata *blockchain,* cioè serie concatenata di blocchi. Le operazioni, cioè, vengono raggruppate in blocchi, e, poi, condivise e convalidate da una rete di nodi[9]. La *blockchain*, quindi, è un database distribuito che utilizza la tecnologia *peer-to-peer* e ogni utente, quindi, è in grado di prelevarlo dal web, diventando, così, un nodo della rete. In questo 'libro contabile condiviso' sono registrate tutte le transazioni fatte in *bitcoin* dal 2009 ad oggi, operazioni perfezionate solo nel caso in cui vengano approvate del 50%+1 dei nodi. Grazie a questo sistema di verifica aperto, *Bitcoin* non necessita dell'intermediazione degli istituti di credito per eseguire una transazione e poiché la *blockchain* è di dominio pubblico (con evidenza, dunque, di tutte le transazioni effettuate) si dice che il sistema non è anonimo ma 'pseudonimo'[10].

Parlando di 'sistema di verifica aperto' il problema principale potrebbe risultare quello della salvaguardia della sicurezza delle transazioni. In realtà, però, *Bitcoin* risolve il cosiddetto 'Problema dei generali bizantini'[11], ovvero di come portare a termine un'operazione in sicurezza su una rete che di per sé sicura non è, mediante la criptovaluta, cioè trasferendo *bitcoin* mediante messaggi crittati (Figura 2).

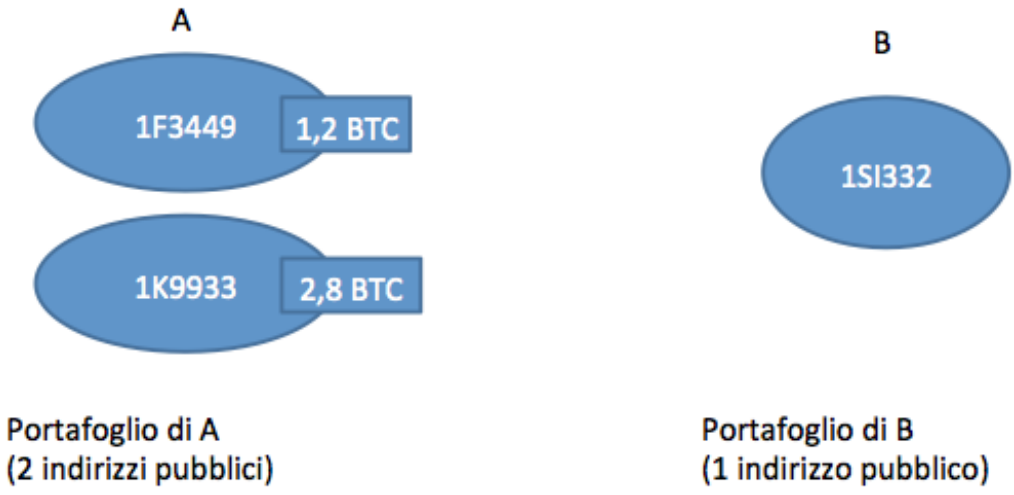

Figura 2 - Transazione in bitcoin.
Fonte: R. Caetano, *Bitcoin. Guida all'uso delle criptovalute*, Milano 2016. Rivisto e modificato da Nina Passarelli, 2016

'A' ha due indirizzi pubblici (chiavi pubbliche)e due indirizzi privati (chiavi private) che controllano i suoi due saldi. Come è possibile notare, la transazione può avvenire tra due o più parti (input/output) e ad ogni input corrisponde un output della transazione precedente (Figura 3)[12].

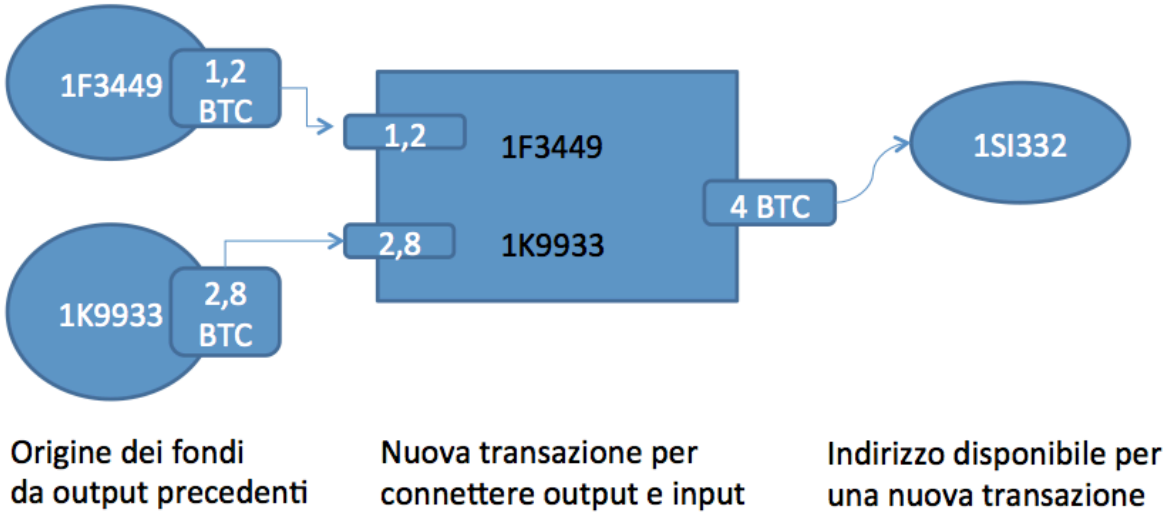

Figura 3 - Transazione Bitcoin che impiega input e output.
Fonte: R. Caetano, *Bitcoin. Guida all'uso delle criptovalute*, Milano 2016. Rivisto e modificato da Nina Passarelli, 2016

Le transazioni, dunque, sono validate se gli output delle transazioni precedenti coincidono con gli input della nuova transazione. Per tale motivo si parla di 'catena di blocchi', infatti, nella *blockchain* è presente l'intera cronologia delle operazioni eseguite dal 2009 ad oggi[13]. Trattandosi di un sistema basato sulla tecnologia *peer-to-peer* per completare la transazione è necessario dimostrare alla rete che 'A' sia il vero mittente (approvazione del 50% più 1 dei nodi) e non abbia alterato o sostituito ciò che sta scambiando.

Per raggiungere tale scopo 'A' deve dimostrare di avere le chiavi private: ad ogni indirizzo pubblico presente all'interno del portafoglio di A corrisponde una chiave privata mediante la quale può sottoscrivere la transazione usando una 'firma digitale'. Una volta validata dalla rete la transazione è incorporata in modo permanente alla *blockchain* e 'B' riceverà i suoi *bitcoin* (Figura 4)[14].

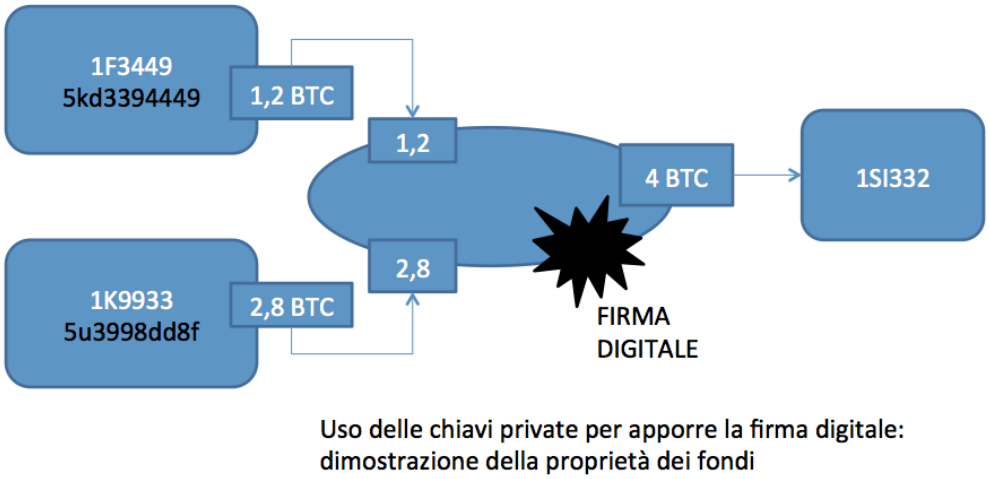

Figura 4 - Schema di validazione del sistema Bitcoin.
Fonte: R. Caetano, *Bitcoin. Guida all'uso delle criptovalute*, Milano 2016. Rivisto e modificato da Nina Passarelli, 2016

In altri termini, Bitcoin utilizza la crittografia a chiave pubblica, cioè un algoritmo crittografico asimmetrico che si serve di due chiavi, generate matematicamente: la chiave privata, impiegata per 'crittografare' o firmare digitalmente il documento, il 'denaro digitale', e la chiave pubblica, che viene usata per 'decrittografare' il messaggio o per verificare la firma. Il legame matematico presente fa le due chiavi fa si che la chiave pubblica funzioni se e solo se esista la corrispondente chiave privata[15]. *Bitcoin* sfrutta degli algoritmi a curva ellittica, *Elliptic Curve Digital Signature Algorithms* (ECDSA)[16], al fine di generare la coppia di chiavi (pubblica e privata); con il procedimento sistemico di calcolo ECDSA è possibile generare una chiave pubblica 'a partire' dalla relativa chiave privata in qualsiasi momento, mentre non è possibile effettuare l'operazione inversa.

Il mittente della transazione deve conoscere l'indirizzo *Bitcoin* del soggetto a cui trasmettere un certa quantità di *bitcoin*. Esso viene calcolato applicando degli algoritmi *hash* crittografici, detti semplicemente *hash,* alla chiave pubblica, e, successivamente, un'altra funzione di hash all'output ottenuto in precedenza[17]. Il detentore di una certa quantità di moneta precedentemente ricevuta che voglia trasferirla a certo destinatario, in altri termini, firma digitalmente un *hash* della transazione precedente e della chiave pubblica del destinatario e aggiunge tali informazioni alla transazione che sta predisponendo. Il più noto *hash* sviluppato dalla *National Security Agency* (NSA) e utilizzato da *Bitcoin* è chiamato SHA256[18] ed è in grado di produrre un codice *digest* di un documento, ovvero una breve stringa di caratteri, in questo caso, 40 (256 bit); un altro noto algoritmo *hash* europeo è invece detto RIPEMD-160 ed è capace di produrre un codice *digest* di 160 bit (ogni alterazione del documento genera un digest differente e non consente la validazione della transazione). Queste due funzioni *hash* vengono applicate alla chiave pubblica e, per identificare la rete di appartenenza dell'indirizzo, davanti ad esso viene aggiunto un 'identificatore di rete'. Al termine dell'indirizzo, invece, viene calcolato e inserito un codice detto *checksum*, impiegato per garantire che l'indirizzo contenga un serie di caratteri validi (se un carattere è errato, la cifra *checksum* sarà errata). In ultimo, all'identificatore di rete, al codice *hash* e al codice *checksum*, viene applicata una funzione BASE58, che ha lo scopo di codificare grossi valori numerici in una stringa alfanumerica di caratteri[19].

Il risultato è un indirizzo pubblico, usato per ricevere *bitcoin* e, una chiave privata che viene impiegata, invece, per spenderli. In sintesi, si genera una chiave privata e il suo indirizzo *Bitcoin* partendo da un grande numero casuale; un algoritmo a curva ellittica ECDSA, crea la coppia di chiavi pubblica e privata partendo dal numero casuale. Viene, infine, generato l'indirizzo *Bitcoin* trasformando la chiave pubblica tramite funzioni *hash* (SHA256 e RIPEMD-160), aggiungendo un codice *checksum* e codificando il tutto con BASE58 (Figura 5).

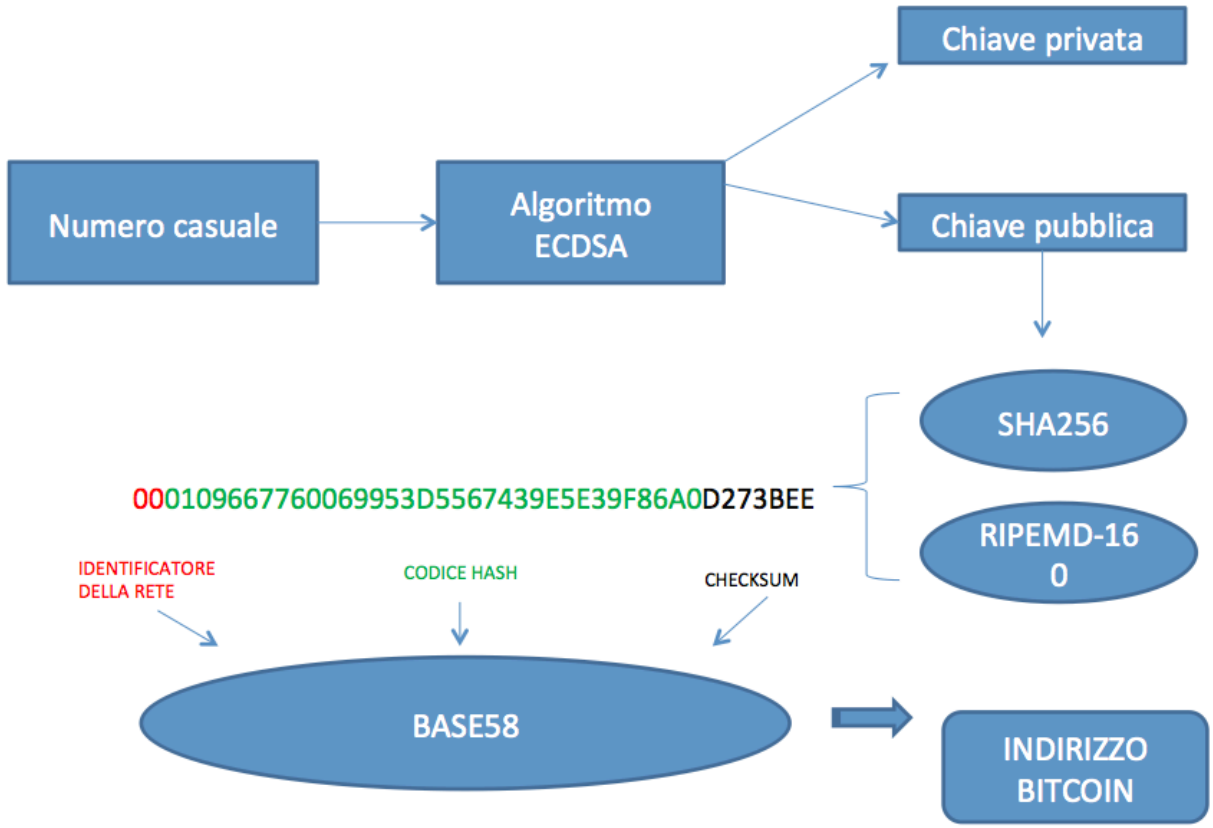

Figura 5 - **Processo di generazione di un indirizzo Bitcoin.**
Fonte: R. Caetano, *Bitcoin. Guida all'uso delle criptovalute*, Milano 2016. Rivisto e modificato da Nina Passarelli, 2016

La trasmissione in *broadcast*, cioè da un sistema trasmittente ad un insieme di sistemi riceventi non definiti a priori, dell'operazione firmata è possibile connettendosi a uno o più nodi della rete stessa. La rete *Bitcoin*, infatti, è costituita da diverse migliaia di nodi, alcuni dei quali vengo chiamati *miner*, cioè minatori, in quanto svolgono la risoluzione di un problema matematico complesso per effettuare la convalida delle transazioni[20], ottenendo, in cambio 25 *bitcoin* per ogni blocco autenticato. Il nodo 'connesso', infatti, diviene parte della rete ed è in grado di inviare e ricevere transazioni; gli altri nodi 'ascoltano' le transazioni trasmesse e le condividono fra loro, in modo tale da essere in grado di gestire una copia di ogni transazione creata e utilizzarla per convalidare nuove operazioni, con la garanzia, così, che il saldo disponibile sia sufficiente prima di inoltrare l'operazione ad altri nodi. Le nuove transazioni sono inizialmente in uno stato 'non confermato', in quanto la rete deve stabilirne la validità (saldo sufficiente e firma digitale); nel caso in cui vengano avvalorate, le transazioni sono raggruppate in un 'blocco' dal miner. Una volta risolto il problema matematico, i blocchi accettati vengono scambiati dai nodi, contrassegnati con un *timestamp*[21] (marca temporale) e concatenati in modo permanente alla *blockchain* (Figura 6).

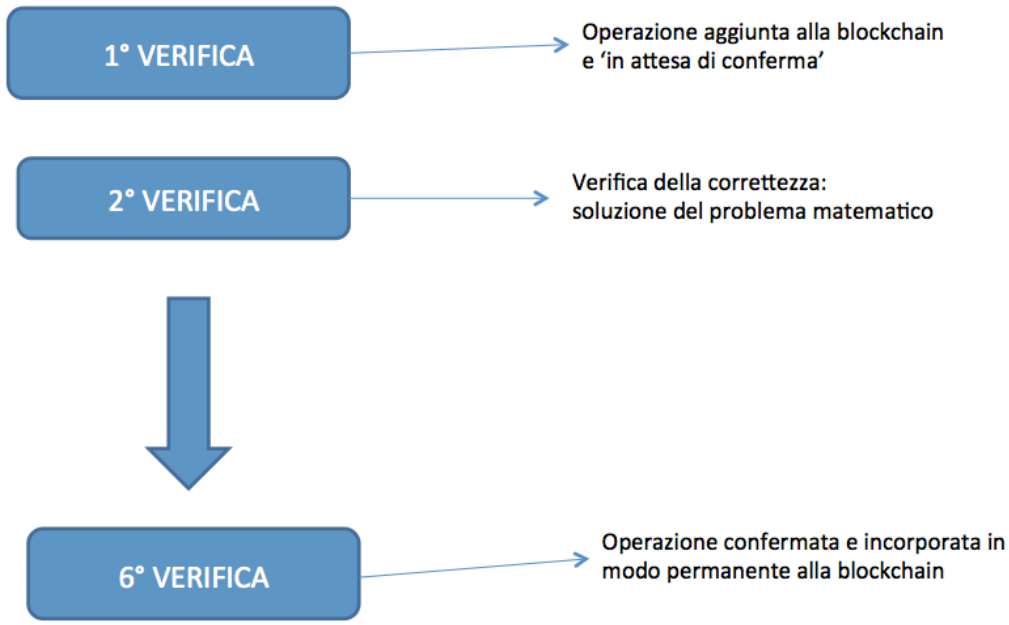

Figura 6 - Meccanismo di verifica

In sintesi, le transazioni possono essere eseguite da tutti i nodi connessi alla rete *Bitcoin*, che è 'decentralizzata' (ogni nodo è indipendente dall'altro e può reindirizzare la connessione qualora uno di questi si disattivasse; non c'è, infatti, un punto centrale fallibile). Al fine di convalidare le operazioni ogni nodo è in grado di gestire una copia dell'intero storico della *blockchain*; ogni blocco comprende un elenco delle transazioni validate ed è collegato al precedente blocco della catena. L'insieme dei nodi costituisce la rete *Bitcoin* ma alcuni di essi si impegnano nell' 'estrazione' (attività di *mining*) di nuovi *bitcoin*, e, perciò vengono chiamati *miner*. L'attività di mining consiste in un procedimento che impiega un nuovo blocco di transazioni come base di calcolo di un problema dalla risoluzione complessa. Nel caso in cui il problema venga risolto, il *miner* invia una *proof of work*, una prova, alla rete e riceve nuovi *bitcoin* più le commissioni dovute per ogni transazione[22]. L'intero meccanismo di convalida dell'operazione avviene in circa dieci minuti.

Il sistema *Bitcoin*, date le sue caratteristiche, ha creato, dunque, una spaccatura tra i suoi sostenitori , concentrati sul potenziale della *blockchain* e sulla natura *peer-to-peer* del sistema visto come strumento di 'democratizzazione finanziaria' e, i suoi detrattori, focalizzati sui possibili rischi riscontrabili in assenza di intermediari finanziari, soprattutto in ottica di riciclaggio e volatilità della valuta virtuale. Tre aspetti risultano essere fondamentali nella valutazione del sistema: 'il modo e la quantità' in cui la moneta viene diffusa, la 'maniera' in cui si distribuisce e gli 'effetti' di tale emissione sui singoli attori.

2. I vantaggi di Bitcoin: la criptovaluta come strumento di democratizzazione finanziaria

Il *whitepaper* di Satoshi Nakomoto, manifesto del sistema *Bitcoin*, fa emergere con forza il potere travolgente di Internet, la sua natura distribuita, collaborativa e 'collettiva', grazie alla rete *peer-to-*

peer, in grado di evitare il ricorso a intermediari finanziari per completare una transazione. Il 'sistema *bit*', inoltre, mira a risolvere il problema della quantità di moneta, in particolare, della cosiddetta 'trappola della liquidità'[23]: dopo la crisi del 2007 la quantità di moneta è aumentata e continua ad aumentare, anche a seguito delle politiche di *quantitative easing* della Banca Centrale Europea (BCE)e degli altri istituti mondiali (come ad esempio la *Federal Reserve* o FED negli Stati Uniti), ma 'non circola', cioè viene accumulata ma non spesa, esercitando una pressione contrattiva sull'economia reale. *Bitcoin* s'inserisce, dunque, in un contesto in cui il sistema monetario è in forte difficoltà di funzionamento e appare quasi fuori controllo.

Uno dei principali vantaggi appare essere legato al funzionamento della *blockchain*, che agevola la disintermediazione: per raccogliere capitale di rischio, infatti, con *Bitcoin*, non occorre quotarsi in Borsa, seguendo le regole del sistema finanziario in essere, ma, si possono effettuare operazioni di *crowdfunding*, il cosiddetto 'finanziamento folla', utili, ad esempio, per le imprese che intendono entrare direttamente in contatto con i propri sovvenzionatori e ottenere il finanziamento mediante un'operazione di compravendita di criptovaluta[24]. Nati dall'intreccio tra innovazione tecnologica e nuovi modelli di business, *Bitcoin* e *Crowdfunding* risultano essere due strumenti di 'democratizzazione finanziaria', in grado di completarsi a vicenda e di sfruttare il potere della rete, che decide in cosa e come investire. Per essi sussiste la stessa filosofia di fondo, ovvero, disintermediare i flussi finanziari e decentralizzarne i meccanismi di controllo al fine di ottenere più trasparenza e democrazia, grazie soprattutto alle reti *peer-to-peer* tra i soggetti che sono coinvolti. Esempi di soluzioni di raccolta di *crowdfunding* basate sulla tecnologia *blockchain* sono Swarm, Koinify e WeiFund[25].

Altro aspetto considerevole per i sostenitori di *Bitcoin* è legato all'abbattimento dei costi di transazione[26]: la maggior parte delle operazioni può essere gestita senza alcuna commissione, a differenza di quanto accade con gli intermediari finanziari. Gli utenti, però, sono incoraggiati a pagare una piccola commissione volontaria in cambio di una 'maggiore velocità di conferma' della transazione e per ricompensare i minatori. Le commissioni sono impiegate a scopo di protezione contro utenti che inviano transazioni per intasare la rete. Il loro funzionamento è ancora in corso di sviluppo e cambierà nel tempo. La commissione non è legata alla quantità di *bitcoin* inviata, infatti, può risultare estremamente bassa (0,0005 BTC per il trasferimento di 1000 BTC) o eccessivamente alta (0,004 BTC per un pagamento di 0,02 BTC). Ad incidere sull'entità della commissione sono la mole di dati della transazione ed il numero di indirizzi in cui è suddiviso l'importo da inviare[27].

La rapidità con cui i *bitcoin* vengono scambiati è un altro elemento che ha consentito il successo e lo sviluppo di questa criptovaluta: la velocità di circolazione dei *bitcoin* è apprezzabile soprattutto pensando alle transazioni verso l'estero (ad esempio i bonifici internazionali), per le quali, attraverso il sistema di pagamenti 'intermediato' possono essere necessari anche più giorni lavorativi per la convalida; con *Bitcoin,* invece, le operazioni possono essere istantanee, nel caso in cui siano a 'zero conferma' (chi vuole ricevere *bitcoin*, cioè, si assume il rischio di accettare una transazione che non è stata ancora confermata dalla *blockchain*) o, in alternativa, impiega circa dieci minuti (operazione confermata dalla rete). In ambo i casi, dunque, la transazione è più veloce rispetto ai tradizionali metodi di pagamento finora utilizzati.

Un'altra caratteristica positiva di *Bitcoin* è l'impossibilità di essere soggetto a confisca: a differenza di quanto accaduto a Cipro nel marzo 2013[28], dove la Banca centrale ha voluto e potuto riprendersi i

depositi non assicurati più grandi di 100 mila dollari per ricapitalizzare se stessa, causando disordini sia tra la popolazione locale che tra i risparmiatori stranieri, con *Bitcoin* questa possibilità è esclusa in quanto si tratta di una moneta decentrata. Nessuna autorità centrale ne ha il controllo e, di conseguenza, non può confiscare tale bene. Tra i fautori del sistema, avversi al tradizionale sistema bancario, questo risulta essere un grande vantaggio ed un'eccellente opportunità di cambiamento.

C'è, infine, un altro aspetto peculiare di questo nuovo sistema rispetto alla nota *fiat money*[29] (la moneta cartacea inconvertibile, generalmente accettata come mezzo di pagamento in quanto dichiarata a corso legale o 'forzoso' dallo Stato che la emette, indipendentemente dal suo valore intrinseco): il 'tempo', variabile cruciale per le monete *fiat,* diventa con *Bitcoin* un fattore neutrale, che non arreca vantaggi o danni per alcuna delle controparti. In altri termini, se non si è più dipendenti dal tempo, non si è più legati a fenomeni come l'inflazione, gli interessi e il *demurrage*[30], cioè il costo associato alla proprietà o al possesso di valuta. La *fiat money* funge, inoltre da 'riserva di valore', per cui, non facendo circolare il denaro si va incontro ad una perdita certa; data la natura *peer* di *Bitcoin* invece, non deve sussistere asimmetria delle risorse, cioè nessuna delle parti deve trarre vantaggio da un fattore, quale può essere il tempo. L'offerta di *bitcoin*, inoltre, è predeterminata (21 milioni) e crescente a ritmi decrescenti, per cui risulta inutile scommettere sulla variabile tempo.

Diversi, dunque, sono gli aspetti positivi riscontrati in *Bitcoin*: solo nel caso in cui tale sistema e moneta al tempo stesso si dimostri migliore dei meccanismi valutari finora esistenti verrà adottata in maniera diffusa dagli agenti economici.

3. I rischi di un nuovo 'ordine' virtuale: dalla volatilità al riciclaggio

Le valute virtuali, tra cui *bitcoin*, costituiscono delle rappresentazioni 'digitali' di valore, utilizzabili come mezzo di scambio o a fini di investimento e vengono gestite elettronicamente. Data la sconfinatezza del *world wide web* risulta sempre più complessa l'attività volta a contrastare fenomeni illeciti, capaci di alterare i circuiti legali dell'economia e della concorrenza. Molti sono i dubbi che circondano *Bitcoin:* in particolare i rischi di riciclaggio e i *cyber* attacchi, la forte volatilità, l'inquadramento normativo e fiscale sono gli aspetti che destano le maggiori perplessità.

L'assenza di intermediari finanziari, baluardo dei sostenitori del sistema di Nakamoto, rischia di dar luogo a operazioni di riciclaggio e finanziamento al terrorismo. Per comprendere tale rischio, basti pensare che gli interventi di contrasto alle transazioni illecite si sviluppano con indagini di polizia giudiziaria[31], con l'approfondimento delle segnalazioni di operazioni sospette inoltrate da intermediari ed operatori finanziari e con i controlli sulle movimentazioni di valuta, aspetti meno controllabili in *Bitcoin* in quanto si tratta di un sistema *open source*, che opera, quindi in assenza di banche o altri organismi centrali (principali mezzi di segnalazione di transazioni illecite). Non meno importanti sono anche le ispezioni ed i controlli nei confronti dei destinatari della normativa antiriciclaggio (intermediari finanziari, money transfer, società fiduciarie, ecc.), con lo scopo di verificare il corretto adempimento dei relativi obblighi (adeguata verifica della clientela, registrazione dei dati e segnalazione delle operazioni sospette) e prevenire l'utilizzo del sistema finanziario per movimentare capitali di origine illecita. Essenziale, poi, è contrastare e prevenire il finanziamento al terrorismo, evitando che sussistano fonti in grado di iniettare liquidità ai principali ambienti a rischio di radicalizzazione.

Il *deep web*[32], la parte di internet che si nasconde al di sotto del *web* in cui si è abituati a navigare, è un 'territorio di bit' poco noto e inaccessibile (servono, infatti speciali software per accedere) che si presta ad operazioni illecite, in particolare in quella porzione detta *dark web*. Non tutto questo web 'nascosto' è implicato in transazioni illegali (sono infatti presenti anche ricercatori d'avanguardia e dissidenti dei regimi totalitari) ma ciò che è certo è che, essendo territorio fertile per gli *hacker* provenienti da tutto il mondo, che comunicano al suo interno seguendo la regola del *peer-to-peer*, le operazioni risultano difficilmente tracciabili e sfuggono con facilità ai controlli. Per tale motivo, la maggior parte degli scambi riguardano droghe leggere e pesanti, armi, prodotti farmaceutici e servizi legati alla compromissione di sistemi informatici e account personali, finalizzati al cosiddetto *cybercrime* informatico. Un esempio di prodotto acquistabile è *Command and Control* (*C&C*) che è un server per il controllo remoto dei malware, difficilmente tracciabile, ed utilizzato per operazioni di 'furto dell'account'. La maggior parte delle transazioni riscontrabili sul deep web/dark web sono pagate in *bitcoin*.

I fondamentalisti islamici dell' *ISIS,* inoltre, sembrano conoscere e sfruttare al meglio i nuovi trend digitali[33], come è emerso dagli studi di una fonte dell'intelligence israeliana, la quale ha fatto emergere una pista relativa proprio al mondo *Bitcoin*, che verrebbe utilizzato come mezzo per il finanziamento delle attività e il reclutamento degli adepti. Secondo l'analista israeliano, infatti, su un sito Internet ritracciato, ci sarebbero state concrete evidenze che una cellula terroristica abbia utilizzato i *bitcoin* come parte delle sue azioni di *fundraising*. Il finanziamento al terrorismo mediante l'uso di *bitcoin* ha destato, perciò, allarmismo nel mondo occidentale, e, in particolare, negli Stati Uniti, in quanto questa nuova moneta digitale rallenterebbe e renderebbe difficili le operazioni di contrasto ai fondamentalisti islamici.

Il rischio di riciclaggio, però, non è l'unico problema emerso nel sistema *Bitcoin*: la forte volatilità dei prezzi[34] è un altro aspetto enfatizzato dai suoi detrattori. La caratteristica principale per valutare una moneta come 'buona' è la stabilità del suo potere di acquisto, che vuol dire che il suo valore deve essere relativamente costante in termini di quantità di beni e servizi che consente di acquistare. Per misurare il potere di acquisto di una moneta è necessario identificare un paniere di beni e servizi di riferimento, come avviene con l'indice dei prezzi al consumo (IPC), indicatore utilizzato dall'Istat per valutare l'inflazione. Per *bitcoin* non esiste un indice analogo in quanto non sussistono ad oggi listini prezzi fissati in tale valuta.

Questo è già un primo indizio di una maggiore volatilità rispetto alla *fiat money*: il 3 gennaio 2009, data della creazione del primo *bitcoin*, questa moneta non aveva valore; un anno e mezzo dopo, il 17 agosto 2010, un *bitcoin* è venduto per 7,69 centesimi di dollaro, superando poi la soglia di un dollaro a febbraio 2011. Il primo picco si ha tra aprile e giugno 2011, quando raggiunge la soglia di 35 dollari, per poi vedere il suo valore dimezzato in una settimana a causa della chiusura della più grande piattaforma di *trading*, Mt. Gox, a seguito di un attacco hacker. Fino ad agosto 2012 si resta sotto la soglia dei 10 dollari per arrivare ad un'ascesa vertiginosa dopo febbraio 2013, quando il cambio viene portato a circa 40 dollari ai primi di marzo e al doppio alla fine dello stesso mese. Il rialzo prosegue, infatti, il 7 aprile 2013 un *bitcoin* vale più di 160 dollari e il 9 aprile tocca il suo massimo a 237 dollari, per poi ricadere in tre giorni a un valore di 76 dollari. Il cambio resta sui 100 dollari per altri sei mesi; ad ottobre 2013, poi inizia un'altra ascesa: da 100 a 200 dollari prima della fine del mese, raddoppia in due settimana e tocca il suo massimo storico il 4 dicembre 2013 con un *bitcoin* scambiato per 1151 dollari, per poi dimezzarsi nuovamente, a causa della decisione della

Banca Centrale Cinese di vietare le transazioni in tale valuta, nel giro di altre due settimane. Le oscillazioni violente proseguono, con il cambio che si tiene intorno ai 5-600 dollari fino ad agosto 2014 per poi iniziare a decrescere restando per tutto il 2015 su un trend di 200-300 dollari[35].

Questa elevata volatilità, dunque, renderebbe *bitcoin* una moneta poco affidabile[36] sia come riserva di valore che come unità per la denominazione dei debiti o dei contratti a lungo termine: per esempio, A poteva vendere a settembre 2013 un bene X a un *bitcoin* (che valeva allora circa 100 dollari); dopo neanche due mesi con lo stesso unico *bitcoin* poteva acquistare da B un bene Y del valore di 1000 dollari. B, che dal ricavato della vendita avrebbe voluto acquistare il bene Z, di identico valore di Y (1000 dollari), avrebbe visto però dimezzato, in pochi giorni, il valore del suo *bitcoin*, che sarebbe stato sufficiente, perciò, a pagare solo metà del valore del bene Z. L'utilizzo di *bitcoin* come strumento speculativo più che come mezzo di scambio ne determinano la notevole volatilità, per cui risulta essere una moneta instabile con forte impatto sul 'benessere sociale': il problema di *bitcoin,* infatti, è dato proprio da una delle sue principali caratteristiche, cioè l'offerta di moneta predeterminata a fronte di una domanda variabile. L'impossibilità di adeguare l'offerta alle variazioni della domanda provocano volatilità dei prezzi e dell'attività economica reale con conseguenti perdite di benessere sociale.

L'inquadramento normativo di *bitcoin* costituisce un'ulteriore criticità a cui rapportarsi. Il trattamento giuridico di tale valuta digitale è ancora al suo stadio embrionale e ha fornito diversi riscontri, che hanno evidenziato la difficoltà oggettiva di ricondurre *bitcoin* a fattispecie note e regolamentate.

Un primo approccio sarebbe quello di considerare *bitcoin* come 'moneta': è utilizzata, infatti, come voluto dal suo creatore, come mezzo di pagamento e perciò, normativamente, si potrebbe propendere per ricondurla a tale fattispecie. Per contro però, a differenza della moneta ufficiale, non ha corso legale, non è soggetta a vigilanza e non tutela le operazioni di acquisto o scambio (questo è valevole, però, se si vuole escludere *bitcoin* dal considerarlo alla stregua della moneta a norma della legislazione vigente); sono soprattutto, poi, le caratteristiche funzionali di *bitcoin* (come l'elevata volatilità) che portano a ritenerlo poco vicino alla moneta più sul piano economico che su quello giuridico. Una seconda valutazione assimilerebbe, invece, *bitcoin* alla 'merce', data la sua apparenza di bene immateriale, specifico, infungibile e divisibile. In tal modo, la volatilità non sarebbe più un problema :chi lo riceve sarebbe a conoscenza della variabilità del suo valore, come avviene, per esempio, con un'opera d'arte. La differenza però tra *bitcoin* e ogni altro tipo di merce è che il suo unico valore d'uso è il valore di scambio, con conseguenti fluttuazioni di portata molto più elevata rispetto ad una qualunque altra merce. Si può, poi, assimilare *bitcoin* a 'un valore mobiliare', cogliendone così il suo utilizzo come forma di investimento. Tuttavia *bitcoin*, a differenza di azioni o altri strumenti finanziari non dà luogo ad alcuna obbligazione in capo all'emittente e non comporta nessun altro diritto corrispondente al titolare; in altri termini, non è un titolo di credito. In Paesi come la Svezia, la Germania e l'Italia stessa, però, la strada perseguita dal legislatore è proprio quella di considerarlo alla stregua di un prodotto finanziario[37].

La Banca d'Italia[38], condividendo la posizione dell'Autorità Bancaria Europea (*European Banking Authority* o EBA) ha sottolineato i rischi delle criptovalute, soprattutto se utilizzate come strumento di investimento, e ha fortemente scoraggiato banche o altri intermediari dall'acquistare, detenere o vendere valute virtuali.

Il problema normativo, dunque, presenta molteplici sfaccettature e non è di facile risoluzione. L'ipotesi più plausibile apparirebbe quella di considerare *bitcoin* come strumento di pagamento a corso volontario (l'accettazione di *bitcoin* sarebbe cioè rimessa alla volontà delle parti), nel rispetto del suo carattere *peer-to-peer*.

4. Conclusioni

L'era digitale ha creato un mondo che si muove in parallelo rispetto a quello reale: è il Web, senza confini e limiti temporali, dove tutto può arrivare ad essere gestito in maniera pressoché anonima. L'European Banking Authority si è trovata a monitorare una delle maggiori innovazioni dell'ultimo secolo: la valuta virtuale, che è una rappresentazione di valore non controllata da una Banca Centrale, ma accettata dalle persone fisiche o giuridiche come mezzo di scambio, e, può essere venduta, risparmiata o trasferita elettronicamente. La decentralizzazione fa si che ogni 'nodo' della rete funzioni, allo stesso tempo, in autonomia e sincronia con gli altri, creando una 'catena di blocchi. Le valute virtuali vengono create online utilizzando hardware potenti ed estratte dagli utenti 'minatori' risolvendo algoritmi di calcolo complessi. Un protocollo matematico ne stabilisce l'offerta e ne fissa le regole all'interno del web. Solo piccole quantità di moneta virtuale vengono rilasciate nel corso del tempo, e la potenza di calcolo necessaria per estrarre una unità aumenta nel tempo. I 'minatori' convalidano le transazioni e operano generalmente in forma anonima e in tutto il mondo.

Lo scenario aperto da *Bitcoin* genera al tempo stesso opportunità e rischi: da un lato, come si evince dal *whitepaper* creato da Satoshi Nakamoto, c'è l'ambizione di voler creare una moneta 'migliore', non condizionata dall'intermediazione, e, più in generale, dal fattore umano, per sua natura fallibile. Da qui la natura *peer-to-peer* di questa nuova valuta virtuale, il suo essere 'attivo senza passivo' e *low cost* rispetto ad altri mezzi di pagamento, data l'assenza di intermediari. Rispetto ai sistemi di pagamento tradizionali, *Bitcoin* e le altre valute virtuali hanno generato nuovi tipi di imprese che prima non esistevano. L'uso di *virtual currencies* decentrate offre diverse nuove opportunità di business. Ad esempio, l'attività di *mining* ha generato lo sviluppo di hardware specializzati, di aziende dedicate a quello specifico business. Ulteriori opportunità commerciali sono sorte dagli scambi e dalle piattaforme commerciali, a causa della necessità di convertire *virtual currency* in *fiat money* e viceversa. Le maggiori opportunità di innovazione che si sono riscontrate fanno capo al settore IT ma, anche, a quello dei servizi finanziari.

Per contro *Bitcoin* apre un baratro all'interno di un mondo che cammina in parallelo a quello reale: il Web, data la sua natura scarsamente controllabile e potenzialmente senza confini, risulta essere un terreno fertile per attività criminali o terroristiche, e, i *bitcoin* rischiano di diventare il loro miglior mezzo di finanziamento, soprattutto in mancanza di un ben definito quadro normativo di riferimento. L'Unità di Informazione Finanziaria (UIF), occupandosi di prevenzione e contrasto dei fenomeni di riciclaggio e finanziamento al terrorismo in Italia, è vicina alle posizioni assunte dall'*European Banking Authority* e dalla Banca d'Italia in materia di criptovalute: l'uso per finalità illecite desta le maggiori perplessità verso questo nuovo 'contante digitale', dovuto anche ad alcune segnalazioni di operazioni sospette, effettuate mediante *bitcoin*.

Le caratteristiche che rendono le criptovalute utilizzabili nell'ambito della frode, del terrorismo, del riciclaggio di denaro sporco e del crimine organizzato, designano una delle maggiori sfide per le

forze dell'ordine, le autorità di regolazione e i governi nazionali. L'ambizione di dar luogo a trasferimenti di denaro veloci, sicuri e con costi di transazione minori rispetto all'attuale *fiat money* in tutto il mondo porta con sé il rischio di facilitare e offuscare transazioni legate ad attività criminali, incluso il riciclaggio di denaro e il finanziamento al terrorismo, il commercio di droghe e la frode su scala globale. Tale pericolo va affrontato e combattuto con regolamenti e leggi ad hoc, al fine di sfruttare i vantaggi della tecnologia *blockchain*.

Questa visione sembrerebbe essere ancora lontana da quella attuale: nella società contemporanea sta iniziando a farsi strada l'idea che le monete virtuali possano essere connesse ai reati 2.0, al cosiddetto *cyber crime*, capace di muoversi, soprattutto all'interno della fitta rete del *dark web*. Non solo alle autorità competenti serviranno nuovi, adeguati strumenti per far fronte a questo scenario 'digitale', ma anche le aziende dovranno imparare a tutelarsi adeguatamente nei confronti dei rischi connessi alle valute virtuali.

Nel caso in cui *Bitcoin* voglia porsi come valuta 'alternativa' e al tempo stesso sistema di pagamento sostitutivo di quello attuale, dovrà essere in grado di implementare i vantaggi della 'catena di blocchi' e di rendere sempre più la rete come il meccanismo *peer-to-peer* di 'autodifesa' delle transazioni.

Note

(ultimo accesso ai link segnalati: 14 novembre 2016)

[1] *Bitcoin* con l'iniziale maiuscola indicherà la tecnologia di pagamento e registrazione crittografica di informazioni; *bitcoin* con l'iniziale minuscola farà riferimento invece alla moneta creata e messa in circolazione da quella tecnologia.
M. AMATO, L. FANTACCI, *Per un pugno di bitcoin. Rischi e opportunità delle valute virtuali,* EGEA Università Bocconi Editore, Milano 2016

[2] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[3] C. ASTARITA, *Cos'è Bitcoin, cinque cose da sapere,* in «Panorama», 12 aprile 2013, http://www.panorama.it/economia/soldi/bircoin-cinque-cose-da-sapere/.

[4] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[5] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[6] S. NAKAMOTO, *Bitcoin, a peer-to-peer electronic cash system*, www.bitcoin.org.

[7] *Total bitcoins over time*, https://blockchain.info/charts/total-bitcoins.

[8] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[9] R. CAETANO, *Bitcoin. Guida all'uso delle criptovalute*, APOGEO, Milano 2016

[10] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[11] A. ANTONOPOULOS, *Il problema dei generali bizantini e il suo impatto sull'economia (meglio noto come bitcoin),* Consulenza Finanziaria, http://www.consulenza-finanziaria.it/problema-dei-generali-bizantini-e-il-suo-impatto-sull-economia-meglio-noto-come-bitcoin/.

[12] Caetano, *Bitcoin*, cit.

[13] BITCOIN PROJECT 2009-2016, *Come funziona Bitcoin*, Bitcoin, https://bitcoin.org/it/.

[14] Caetano, *Bitcoin*, cit.

[15] Caetano, *Bitcoin*, cit.

[16] D. JOHNSON, A MENEZES, S. VASTONE, *The elliptic curve digital signature algorithm* (ECDSA), Certicom Corporation 2001, http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf.

[17] Caetano, *Bitcoin*, cit.

[18] P. FRANCO, *Understanding Bitcoin*: *Cryptography, Engineering and Economics*, Wiley, 2015

[19] Caetano, *Bitcoin*, cit.

[20] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[21] S. HABER, W.S. STORNETT, *How to timestamp a digital document*, in «Journal of criptology», 1991.

[22] M. BERNASCHI, E. MASTRASTEFANO, *Una descrizione (quasi) informatica del funzionamento di bitcoin,* EticaEconomia, 2014, http://www.eticaeconomia.it/una-descrizione-quasi-informatica-del-funzionamento-di-bitcoin/.

[23] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[24] P. FORMICA, *L'alleanza tra crowdfunding e Bitcoin apre scenari nuovi,* in «Il Sole24ore 2014», http://www.ilsole24ore.com/art/notizie/2014-02-02/l-alleanza-crowdfunding-e-bitcoin-apre-scenari-nuovi-081728.shtml?uuid=AB93fxt.

[25] F. ALLEGRENI, *Crowd4fund:Crowdfunding e Bitcoin sempre più vicini. Intervista a Carlo Zanaboni (Sogni fuori dal cassetto)*, Key4biz 2015, https://www.key4biz.it/crowd4fund-crowdfunding-e-bitcoin-sempre-piu-vicini-intervista-a-carlo-zanaboni-sogni-fuori-dal-cassetto/134661/.

[26] A. SIMEONE, D. MANCINI, A. IANIRO, *Bitcoin- Guida all'uso*, Exeo Edizioni 2014

[27] Caetano, *Bitcoin*, cit.

[28] M. APPE, *Bitcoin - Vantaggi e rischi*, Marco Appe-Informatica e Tecnologia, http://marcoappe.com/bitcoin-vantaggi-e-rischi.

[29] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[30] M. CHIRIATTI, *Con i bitcoin il tempo non è più denaro,* Il Sole24ore, 2015, http://www.econopoly.ilsole24ore.com/2015/08/01/con-i-bitcoin-il-tempo-non-e-piu-denaro/.

[31] GUARDIA DI FINANZA, *L'attività della guardia di finanza nella lotta al finanziamento del terrorismo,* 2016, http://www.gdf.gov.it/stampa/ultime-notizie/anno-2016/agosto/l2019attivita-della-guardia-di-finanza-nella-lotta-al-finanziamento-del-terrorismo.

[32] E. SPAGNUOLO, *Cinque cose da sapere sul deep web,* in «Focus», 2014, http://www.focus.it/natura/cinque-cose-da-sapere-sul-deep-web.

[33] G. VAGNONE, *Il terrorismo islamico nell'era di internet, fra bitcoin e dark web,* Eastonline, 13 febbraio 2015, http://www.eastonline.eu/it/opinioni/open-doors/il-terrorismo-islamico-nell-era-di-internet-fra-bitcoin-e-dark-web.

[34] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[35] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[36] M. MAGRINI, *Bitcoin, tutti i rischi della cybermoneta*, in «L'Espresso», 9 dicembre 2013, http://espresso.repubblica.it/visioni/tecnologia/2013/12/09/news/non-e-tutto-bitcoin-quello-che-luccica-1.144857.

[37] Amato, Fantacci, *Per un pugno di bitcoin,* cit.

[38] BANCA D'ITALIA, *Comunicazione del 30 Gennaio 2015- Valute virtuali,* 2015, https://www.bancaditalia.it/pubblicazioni/bollettino-vigilanza/2015-01/20150130_II15.pdf.

Bibliografia

M. AMATO, L. FANTACCI, *Per un pugno di bitcoin. Rischi e opportunità delle valute virtuali*, EGEA Università Bocconi Editore,Milano 2016

M. BERNASCHI, E. MASTRASTEFANO, *Una descrizione (quasi) informatica del funzionamento di bitcoin,* EticaEconomia, 2014

R. CAETANO, *Bitcoin. Guida all'uso delle criptovalute*, Apogeo, Milano 2016