Dipartimento di Economia e Finanza

Cattedra di Diritto dei mercati finanziari

Le evoluzioni della moneta virtuale
prospettive ed incognite legate ai bitcoin

RELATORE

Prof. Mirella Pellegrini

CANDIDATO
Edoardo Burricco
Matricola 669041

CORRELATORE

Prof. Paola Lucantoni

ANNO ACCADEMICO 2016/2017

Introduzione

La rivoluzione informatica ha profondamente mutato ogni settore della vita dell'uomo. L'economia, la finanza e la stessa organizzazione della società vivono ad oggi una fase di grande cambiamento, promossa dalle radicali innovazioni tecnologiche degli ultimi decenni. In questo contesto, una delle più interessanti novità riguarda le evoluzioni dei sistemi di pagamento, su tutte quelle legate alle nuove opportunità offerte dall'informatica, quali le c.d. valute virtuali (o criptovalute). Le valute virtuali hanno difatti catturato via via un sempre maggior interesse, vuoi per l'introduzione di tecniche altamente innovative adottate per le operazioni di pagamento e di trasmissione di moneta, vuoi per la portata rivoluzionaria non solo in ambito economico ma anche sociale e geopolitico. Nell'ottica comune, l'associazione di criptovaluta al nome "Bitcoin" è immediata, quasi scontata: Bitcoin è ad oggi il sistema monetario alternativo più diffuso, nonché il più conosciuto e riconosciuto a livello globale. Basti pensare al sempre crescente numero di rivenditori attivi sui più disparati mercati che hanno iniziato ad accettare la criptovaluta come mezzo di pagamento, coinvolgendo anche *brand* altamente rinomati come Apple, Reddit, Expedia o Wordpress.

Bitcoin è il primo sistema di pagamento basato sul concetto di *distributed ledger technology*, o blockchain: una rete di scambi *peer to peer* in cui non vi è un'autorità centrale incaricata di convalidare e registrare le transazioni. A partire dalla sua creazione nel 2009, Bitcoin ha conquistato un'attenzione crescente presso gli operatori del settore e, complice anche il *boom* osservato agli inizi del 2017 che ha permesso alla valuta raggiungere una quotazione pari a quasi 3.000 dollari, ad oggi deve necessariamente essere considerato una piccola realtà, parallelamente a tutto il mondo delle altre criptovalute, le c.d. *altcoin*. Tuttavia, se da una parte la "moneta 2.0" presenta indiscutibili potenzialità, è altresì necessario valutare con ponderata prudenza le possibili conseguenze che la concorrenza mossa alle valute a corso legale può avere sull'economia globale. Allo stesso modo, il crescente utilizzo delle criptovalute nell'ecosistema criminale richiama l'attenzione sulla necessità di ricondurre questa nuova tecnologia sotto il controllo delle autorità.

L'elaborato punta dunque ad effettuare un'analisi trasversale del "fenomeno Bitcoin", studiandone le suddette potenzialità ed alcuni connessi limiti. Si è scelto di suddividere il lavoro in tre parti. Nella prima, si effettuerà una panoramica del fenomeno nel suo complesso, partendo dalle origini e studiandone l'evoluzione, l'ideologia che ne sta alla base, i meccanismi tecnici di funzionamento e le innovazioni che propone di apportare all'economia. Nei due capitoli successivi, l'analisi procederà su due binari paralleli, approfondendo quelle che, secondo questa trattazione, rappresentano due problematiche chiave di Bitcoin. In primo luogo ci si soffermerà, attraverso un'analisi squisitamente economica, sulla (scarsa) capacità di Bitcoin di espletare efficacemente la funzione monetaria e di potersi dunque affermare come una valida alternativa alle valute tradizionali; si vedrà, in particolar modo, come questa non riesca ad espletare pienamente nessuna delle tre funzioni che una moneta deve svolgere (mezzo di scambio, unità di conto e riserva di valore) A questa si accompagnerà, nel capitolo

seguente, uno studio sul crescente rischio di usi illeciti legati al bitcoin; si porrà specifica attenzione ai fenomeni di riciclaggio e finanziamento al terrorismo, ed alle nuove, pericolose funzionalità garantite dall'avanzamento tecnologico, per concludere infine con un'osservazione delle principali sfide poste agli ordinamenti ed alle problematiche presenti nelle attività di regolamentazione.

Indice

Capitolo 1 – Un mondo Bitcoin

1.1 Cos'è Bitcoin?

Bitcoin è un sistema elettronico di pagamento *peer-to-pe*er, alternativo al tradizionale sistema bancario, che funziona per mezzo del bitcoin, una moneta virtuale creata appositamente per il sistema (abbreviata anche in BTC o XBT)**.** Occorre innanzi tutto sottolineare una prima distinzione: Bitcoin è sia valuta che sistema di pagamento. Questo porta a dover distinguere tra Bitcoin maiuscolo, con cui ci si riferisce alla tecnologia e alla rete, da bitcoin minuscolo, riferito alla valuta-*token* in sé per sé.

L'intento di Bitcoin è quello di permettere l'invio di gettoni in maniera veloce, sicura ed economica attraverso la rete, proponendo dunque un modello decentralizzato, ossia senza l'intervento di alcun soggetto con funzioni di controllo e coordinamento. Bitcoin nasce dalla Rete e per la Rete: è un sistema basato su di un *software open-source*, ossia non protetto da *copyright* e nel quale gli utenti stessi possono apportare migliorie, contribuendo alla sua evoluzione ed al suo perfezionamento, aprendosi anche ad implementazioni "indipendenti" del Protocollo. Inoltre, Bitcoin non ha alcun supporto fisico, le valute possono essere memorizzate in portafogli installati localmente (*wallet*) mediante un apposito *softw*are su dispositivi elettronici (ad esempio pc, smartphone, tablet etc..) o in portafogli *online* la cui gestione è demandata a specifici portali che offrono questo tipo di servizio[1].

L'integrità e l'autenticità delle transazioni sono poi garantite dalla crittografia e dalla blockchain, un registro pubblico e condiviso (liberamente accessibile da ogni utente della rete) sul quale si basa l'intero sistema Bitcoin; in altre parole, la blockchain svolge funzioni simili ad un libro mastro *online*, annotando tutte transazioni mai effettuate e gli utenti partecipanti alla Rete. V'è infine da considerare che, prima dell'iscrizione nel registro, tutte le transazioni vengono verificate da alcuni utenti chiamati *miner,* i quali, come si approfondirà successivamente, vengono ricompensati con l'emissione di nuovi bitcoin.

1.1.1 Anonimato e disintermediazione

Bitcoin promette di superare tutti i limiti del sistema monetario e finanziario tradizionale. Per realizzare il suo fine, Bitcoin poggia essenzialmente su due pilastri: preservare un certo grado di anonimità nel suo utilizzo ed adottare un sistema decentralizzato, che sia totalmente indipendente da qualsivoglia controllo esterno di tipo bancario o governativo.

[1] Cfr. Lemme G. e Peluso S. (2016), "*Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Riv. dir. banc."*, dirittobancario.it, 43.

La sfida principale di Bitcoin è forse proprio quest'ultimo punto, che è alla base dell'esistenza stessa di Bitcoin: proporre un sistema decentrato, che sia del tutto indipendente da intermediari bancari o organismi governativi, senza comprometterne l'efficienza; in altre parole, esso si presenta come una forma radicale di disintermediazione, che comporta la sottrazione di una funzione tipicamente pubblica – la gestone di un sistema di pagamento e della relativa contabilità – ad un operatore tipicamente privato – il settore bancario[2]. È poi grazie alla rete e alla crittografia che Bitcoin consente pagamenti diretti da un utente all'altro (ossia transazioni *peer-to-peer*) in modo efficace, veloce, economico e sicuro. L'ambizione è sicuramente alta: in una sorta di "democratizzazione finanziaria", Bitcoin pone al centro del suo stesso funzionamento la rete nel suo complesso, in cui ogni utente (o "nodo") ha funzioni di controllo e di garanzia delle transazioni; ogni utente con un indirizzo Bitcoin può connettersi alla rete e interagire con gli altri nodi, validare ed autorizzare transazioni, controllare il registro pubblico ed eventualmente segnalare errori al resto della rete. In definitiva, gli utilizzatori di Bitcoin non pongono la fiducia su un ente terzo per la gestione e uso dei propri fondi/guadagni, cosa che ha portato Bitcoin ad essere spesso definito anche come sistema "*trust-less*".

Ma la disintermediazione portata avanti da Bitcoin non si conclude qui. La mancanza di un intermediario o di un ente di controllo centrale assume la sua massima espressione in relazione alla creazione di nuova base monetaria: Bitcoin crea ed emette una nuova moneta, che è completamente fuori dal controllo governativo o bancario. Si potrebbe profilare, in altre parole, il rischio di una pericolosa immissione di nuova liquidità sul mercato, che non è controllata né autorizzata dalle autorità monetarie. Dato questo scenario, è naturale comprendere le preoccupazioni e gli interrogativi attorno agli effetti che Bitcoin possa avere sull'intera macroeconomia.

Bitcoin punta inoltre a garantire una maggiore riservatezza nelle transazioni. Tuttavia, l'anonimità non può considerarsi assoluta; si parla, piuttosto, di "pseudo-anonimità". Sebbene, almeno in apparenza, la tracciabilità non sia sufficientemente forte da risalire all'identità dei singoli operatori, ogni transazione è concretamente e potenzialmente tracciabile. Il sistema funziona tramite un meccanismo di doppia chiave, pubblica e privata. Tutte le transazioni, per essere identificate e successivamente autorizzate, necessitano di entrambe le chiavi, che sono facilmente assimilabili allo *username* alla *password* per accedere alla posta elettronica, ad un *social network*, ad un sistema di *internet banking* o a qualunque servizio *online*[3]. Delle due, solo la chiave pubblica sarà visibile al pubblico. La chiave privata servirà al singolo utente per "confermare" la transazione. Inoltre, per garantire una maggiore sicurezza il sistema predispone la possibilità di generare una serie infinita di coppie di chiavi in capo ad ogni utente (da cui, la crescente difficoltà nell'identificare il soggetto a cui appartengono, di volta in volta, le varie chiavi). La possibilità di risalire al soggetto fisico è poi insita nella stessa blockchain che,

[2] Cfr. Amato M. e Fantacci L., (2016), "*Per un pungo di Bitcoin*", Egea, Università Bocconi Editore, Milano.

[3] Cfr. Amato M. e Fantacci L., (2016), "*Per un pungo di Bitcoin*", Egea, Università Bocconi Editore, Milano.

rendendo pubbliche tutte le informazioni sulle transazioni e le relative chiavi identificatrici, consente di ricostruire tutte le entrate e le uscite di un utente giungendo infine ad identificarlo fisicamente qualora una delle sue transazioni sia in qualche modo legata al mondo reale. Si può dunque asserire che, sebbene le evidenti difficoltà di tracciabilità originate dal sistema, la pseudo-anonimità preserva una possibilità di intervento delle autorità pur provvedendo a tutelare maggiormente la *privacy* degli utenti.

1.1.1 Bitcoin come "contante digitale"

Il sistema Bitcoin ha tuttavia il limite di poter funzionare solo per mezzo del bitcoin valuta; in altre parole, nonostante la nascita di piattaforme di scambio dedicate abbia in parte ovviato a tale problema, gli utenti della rete Bitcoin possono trasferirsi solo e soltanto bitcoin. All'interno di questo contesto, per una piena affermazione di Bitcoin è necessario che la valuta proposta sia in qualche modo preferita alle valute a corso legale, in forza di caratteristiche che maggiormente soddisfino le esigenze dell'utilizzatore.

Prima dell'avvento delle criptovalute, era d'uso comune suddividere la moneta circolante essenzialmente in due categorie, le valute fisiche (come il contante) e le valute elettroniche (come i depositi presso un conto corrente bancario). Il contante ha il pregio di essere facilmente accessibile da chiunque, senza il bisogno di essere titolari di un conto corrente presso una banca o in possesso di dispositivi elettronici. Inoltre, è privo di costi di transazione ed è anonimo, in quanto colui che usufruisce del contante non ha il dovere di indicare la propria identità, né tantomeno il beneficiario o la causale del pagamento. Con l'avvento della moneta elettronica, che si può ricondurre alla creazione della prima carta di credito nel 1958, l'economia ha ottenuto un nuovo sistema di pagamenti che ha introdotto numerosi vantaggi, come quello di un più agevole utilizzo, l'essere infinitamente divisibile e consentire il pagamento a distanza tramite il telefono o internet; d'altra parte, questa tipologia di moneta necessita obbligatoriamente di un coordinamento e una gestione da parte un intermediario e per gli utilizzatori ha lo svantaggio di essere sempre tracciabile. L'intento di Bitcoin è quello di inserirsi a cavallo di queste due monete, di coniugare ed unire a sé i vantaggi dell'una e dell'altra tipologia. Per questo motivo è stato da molti ribattezzato come "contante digitale": Bitcoin tenta di carpire tutte le facilitazioni elettroniche tipiche della moneta "digitale", conservando allo stesso tempo l'anonimità garantita dalla moneta fisica, il "contante", e l'indipendenza dall'intermediazione di un soggetto terzo.

1.1.3 Bitcoin come "oro digitale"

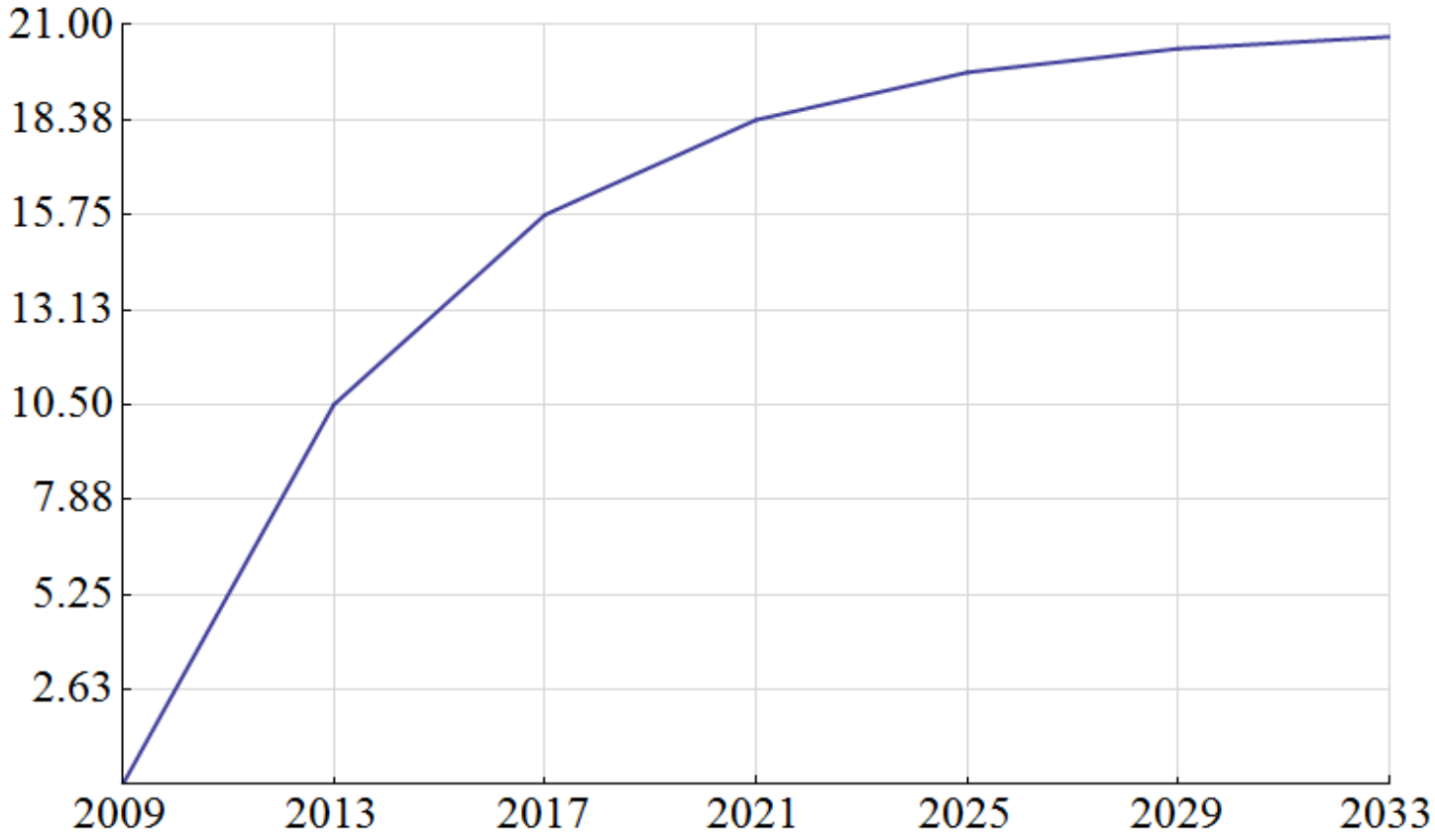
Una delle caratteristiche chiave di Bitcoin nel differenziarsi dalla moneta tradizionale è quella di essere "attivo" del possessore senza essere al tempo stesso "passivo" di qualcun altro. Pur essendo un numero registrato su di un libro contabile (la blockchain), una somma in bitcoin non può essere assimilata ad un credito in quanto non rappresenta un diritto ad ottenere una somma in contanti. Al contrario, sia la moneta scritturale creata dalle

banche commerciali sia la moneta metallica emessa dalle banche centrali comportano un passivo per la banca, ossia un debito che la banca stessa si impegna a convertire in contanti. La moneta elettronica esistente è in realtà un numero che, registrato sul conto corrente di un utente presso una banca, dà il diritto a prelevare in contanti un certo importo equivalente. Anche la moneta emessa direttamente dalle banche centrali rappresenta dunque un passivo per la banca centrale, in quanto quest'ultima si impegna a rispondere del loro valore, regolandone l'emissione per mantenerne relativamente stabile il valore d'acquisto. Da questo punto di vista, il bitcoin è più simile all'oro che alla moneta tradizionale. Anche l'oro, infatti, è attivo di chi lo possiede senza essere passivo di qualcun altro. Questa qualità fa del bitcoin moneta un bene privato, anche a fronte di un sistema di pagamenti che ha natura pubblica e condivisa; il possesso di un bitcoin è il possesso esclusivo di "qualcosa" per la quale il possessore non deve niente a nessuno.

Inoltre, il bitcoin condivide con l'oro un'altra caratteristica chiave, ossia la "scarsità". Mentre per l'oro si parla di "scarsità naturale", per via della sua disponibilità limitata per natura e le difficoltà di estrazione, per bitcoin è stata opportunamente forgiata l'espressione di "scarsità artificiale", proprio per indicarne una componente di limitatezza voluta ed impostata dal suo creatore nel momento della sua stessa progettazione; in altre parole, se l'oro è di per sé scarso, il bitcoin è stato ideato per essere scarso. Ciò è dettagliatamente descritto nel *White paper*, il protocollo-statuto del Bitcoin: la quantità totale di bitcoin in circolazione crescerà gradualmente sino a stabilizzarsi, assumendo inoltre complessità crescenti "nell'estrazione" di nuovi bitcoin mano a mano che ci si avvicina alla cifra prestabilita (quasi a voler replicare le difficoltà di estrazione tipiche dell'oro). La Figura sottostante mostra la crescita nel tempo del numero totale di bitcoin in circolazione: come è possibile osservare, è previsto che la velocità di emissione di nuovi bitcoin dimezzerà ogni 4 anni, per poi rimanere costante e stabilizzarsi, intorno al 2133, alla cifra di 21 milioni di bitcoin esatti (nel secondo capitolo della trattazione si approfondiranno gli effetti direttamente riconducibili a questa scelta). A garantirne l'utilizzo anche per transazioni di piccola entità è la sua capacità di avere fino a 8 decimali (0,00000001[4]). E quando i bitcoin saranno esauriti, poiché si prevede un graduale aumento del controvalore in valuta legale, i decimali potrebbero anche aumentare. Un bene come l'oro, finito, e infinitamente divisibile.

Figura 1 – Evoluzione del numero di bitcoin nel tempo

[4] L'ultima cifra decimale è stata denominata "Satoshi", in onore del suo creatore.



Sotto certi aspetti, la similitudine fra oro e bitcoin può essere forzata. Una critica mossa in tal direzione risiede nel fatto che i bitcoin non sono tangibili e materiali, pertanto non hanno in vero e proprio valore intrinseco: non possono, ad esempio, essere lavorati per creare gioielli od altri oggetti di valore. Tuttavia, si ritiene che il parallelismo possa ragionevolmente essere accettato in ragione delle modalità di conferimento di valore del bitcoin, simili a quelle valide per l'oro. Così come per quest'ultimo, infatti, anche il valore del bitcoin dipende potenzialmente dalla capacità di essere accettato come mezzo di pagamento, oltre che dalla sua scarsità. Sono gli utenti della rete a creare la domanda e, di fatto, a dare valore al bitcoin: esso ha un effettivo potere di acquisto soltanto se c'è qualcuno disposto a ricevere token virtuali in cambio di qualcosa di (più) utile, esattamente come avviene per l'oro[5].

1.2 Fondamenti storici

Il bitcoin è la prima criptovaluta al mondo, non soltanto per mero ordine cronologico ma anche per quanto riguarda l'estensione del mercato. Nato nel 2008 come un'evoluzione (o meglio, una "messa in pratica") del concetto di criptovaluta, Bitcoin ha vissuto quasi un decennio in un crescendo di popolarità, diffusione e crescita del valore, il tutto costellato anche da innumerevoli tensioni e interrogativi.

[5] Cfr. Amato M. e Fantacci L., (2016), "*Per un pungo di Bitcoin*", Egea, Università Bocconi Editore, Milano.

Una maggior comprensione del fenomeno deve necessariamente passare da uno studio delle sue radici storiche, in particolar modo per meglio comprendere successivamente le implicazioni economiche, sociali e politiche attuali e future.

1.2.1 Origini delle cryptovalute

Un primissimo riferimento al concetto di criptovaluta, o criptomoneta, risale al 1982, in uno scritto di David Chaum, "*Blind Signatures for Untraceable Payamentes*", nel quale egli ipotizzava per una primitiva forma di firma digitale (le c.d. "*blind signatures*"), realizzata tramite l'applicazione di una serie di algoritmi. In tal modo, un soggetto poteva ottenere la facoltà di nascondere un certo messaggio prima di firmarlo e "convalidarlo". Lo stesso autore evidenziava le potenzialità di quest'aspetto nel campo dei sistemi di pagamenti, che possono ricondursi alla possibilità di slegarsi dal controllo dalle autorità e all'adozione di forme anonime tramite l'utilizzo di pseudonimi, senza tuttavia trovarne una vera realizzazione pratica.

Le teorizzazioni di Chaum catturarono successivamente gli interessi degli attivisti del Movimento Cyberpunk, che le inclusero nel 1994 nel Manifesto dei Cripto-Anarchici. Gli anarchici del Manifesto identificarono il sistema di crittografia e cifratura proposto da Chaum in uno strumento che potenzialmente potesse essere molto utile nella loro lotta al "potere sovrano". Proprio a tal riguardi, si può leggere che questi può configurarsi come "un modo efficace per riuscire a mantenersi invisibili al Grande Occhio, sfuggendo alla sua ossessione di controllo"[6]. In altre parole, questo sistema è stato considerato come uno strumento funzionale alla lotta dell'individuo nell'affermare la propria sovranità nei confronti dello Stato.

Le idee di Chaum sono state ulteriormente sviluppate, almeno a livello teorico, da Wei Dai nella *mailing list* Cypherpunks, il quale perviene ad una prima ideazione vera e propria di criptovaluta. Egli descrisse un sistema "che consente ad un gruppo di pseudonimi digitali non tracciabili di effettuare vicendevolmente pagamenti in denaro e di assicurare il rispetto di contratti senza aiuti esterni", spiegando come giungere, ad un prototipo di criptovaluta, denominata B-Money, sfruttando una serie di passaggi informatici.

Tuttavia, nonostante i progressi dell'Information Technology e le interessanti potenzialità d'utilizzo delle nuove valute, l'innovativo meccanismo teorizzato si scontrava con l'incapacità di una sua implementazione pratica efficace; il problema più grande riguardava il fenomeno della *double spending* (ossia, il processo mediante il quale si rende possibile duplicare lo stesso gettone e spenderlo due volte).

La portata rivoluzionaria di Bitcoin risiede proprio in questo aspetto: per la prima volta, a partire dalle iniziali teorie di Chaum, si giunge ad un sistema in linea con le idee di Wei Dei ma che al tempo stesso risolve i sopracitati limiti "tecnici", gli stessi limiti che avevano impedito la realizzazione reale di una criptomoneta.

[6] Cfr. Dagnino A. Gulmanelli S. (2003), "*Pop War, il Net Attivismo contro l'Ordine Costituit*o", Apogeo Editore.

1.2.2 Protocollo Bitcoin

Il dominio "Bitcoin" è apparso per la prima volta il 18 agosto 2008, precisamente nell'atto di registrazione di "bitcoin.org" su anonymousspeech.com. Il vero e proprio rilascio è avvenuto pochi mesi più tardi, attraverso la pubblicazione online di "*Bitcoin A peer-to-peer electronic cash system*"[7], un documento sottoscritto da parte di un programmatore sconosciuto, noto con lo pseudonimo di Satoshi Nakamoto. Questo documento è universalmente riconosciuto come il "Protocollo Bitcoin", che pone le fondamenta e disegna le *guidelines* di tutto il progetto. L'identità di colui (o coloro) che si cela dietro Nakamoto è tutt'oggi ancora ignota, nonostante siano state elaborate numerose teorie a riguardo. Tuttavia, Nakamoto ha interrotto il suo diretto coinvolgimento in Bitcoin durante la metà del 2010, trasferendo diversi domini di sua proprietà ad alcuni membri della comunità Bitcoin e consegnando il codice sorgente a Gavin Andersen, il suo più stretto collaboratore.

Il *concept* iniziale del Protocollo è piuttosto elaborato: esso introduce un meccanismo per trasferire denaro digitale senza l'utilizzo di intermediari finanziari o servizi centralizzati, basato quindi su un sistema decentrato *peer-to-peer* puro, in cui un ruolo di primo livello lo assumono i nodi della rete e la crittografia. In particolare, attraverso la crittografia si perviene al tracciamento delle transazioni e alla gestione degli aspetti funzionali (come ad esempio le modalità di generazione della moneta), oltre che alla soluzione del già citato problema della *double spending* attraverso un meccanismo di chiave doppia, pubblica e privata.

Il lancio ufficiale di Bitcoin è invece da ricondurre al 3 gennaio 2009, attraverso il rilascio in rete della prima versione Bitcoin 0.1. In questa occasione, è stato generato il primo blocco di 50 BTC (il cosiddetto "*genesis block*"). Le versioni dalla 0.1.0 fino alla 0.1.5 erano inizialmente supportate solo da Windows 2000, Windows NT e Windows XP. Successivamente al primo rilascio, Satoshi ha lavorato per perfezionare il *client*, correggendo alcuni errori di comunicazione tra i nodi e migliorando l'usabilità del *client* (per esempio, si è deciso di impedire l'inserimento di dettagli e spiegazioni sulle transazioni dei *coin*).

Il primo trasferimento di gettoni avvenne virtualmente tra Nakamoto e Hal Finney (blocco 170 della Blockchain), tuttavia per la prima transazione in termini reali bisogna attendere la fine del 2010, non appena fu resa disponibile la commercializzazione pubblica delle nuove criptovalute. In quel caso, l'oggetto della transazione si manifestò nell'acquisto di due pizze per un ammontare di 10.000 bitcoin, un evento piuttosto curioso che ha portato alla nascita di un "apposito" tasso di cambio pizza/bitcoin.

1.2.3 Segnali di successo

In seguito alla quotazione sul New Liberty Standards, al tasso di cambio con il dollaro statunitense di 1,309 bitcoin per dollaro (ottobre 2009), Bitcoin ha iniziato ad attirare sempre maggior interesse sul mercato globale e

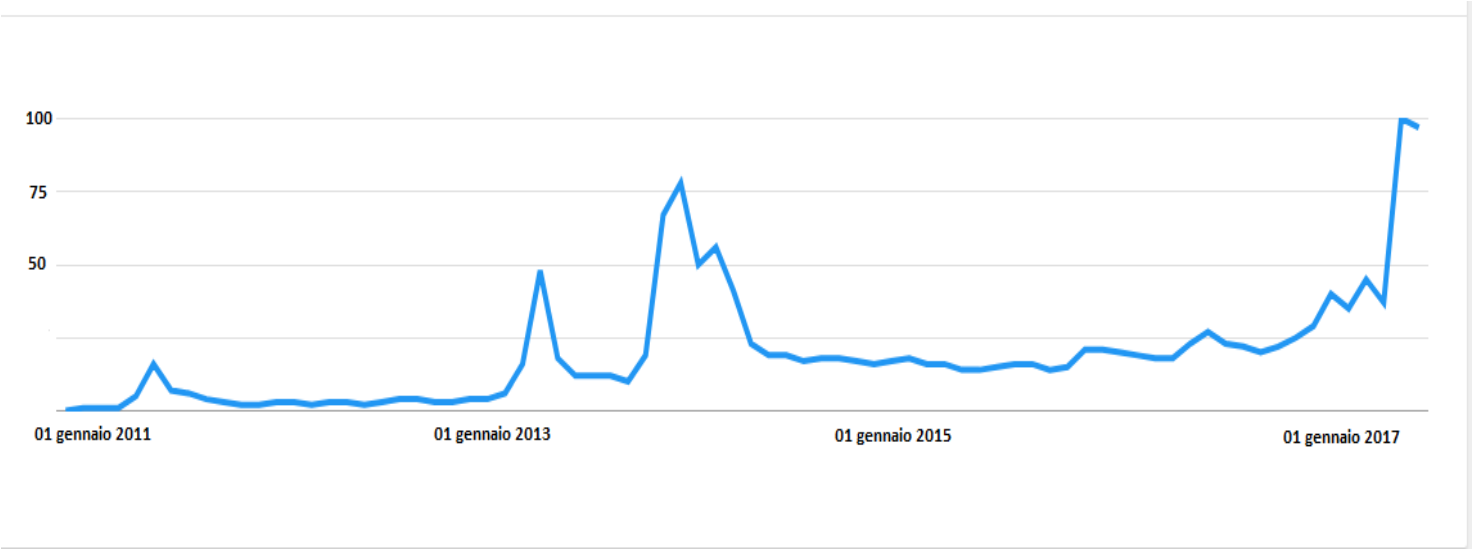
[7] Cit. Jay Palmer Fawcett (2016), "*Bitcoin regulations and investigations: A proposal for U.S. policies*", ProQuest LLC, Ann Arbor.

ad incanalarsi verso un rapido sviluppo. Se in principio Bitcoin era conosciuto unicamente tra una stretta cerchia di sostenitori ed investitori, è ad un anno dalla promulgazione del Protocollo che si è assistito ad un incremento (dapprima timido, poi esponenziale) della sua popolarità. Tale crescente interesse ha portato anche alla costituzione di un numero sempre maggiore di mercati di scambio o piattaforme *online* dedicate, quali Mt Gox (2010) e Kraken (2011). Le piattaforme di scambio hanno consentito l'acquisto o la vendita *online* di una valuta virtuale contro le principali valute legali, offrendo servizi aggiuntivi quali la quotazione dei relativi tassi di cambio, la fornitura di statistiche, la conversione immediata in moneta legale e la custodia del portafoglio digitale. Da queste si devono distinguere le piattaforme di trading, che funzionano come sedi di negoziazione dematerializzate, in cui si raccolgono compratori e venditori di valute virtuali, e che si limitano normalmente a offrire servizi tecnici di supporto alle operazioni di acquisto e di vendita, senza farsi coinvolgere nelle stesse[8].
Ma la diffusione di Bitcoin non si esaurisce unicamente nella moltiplicazione dei mercati e delle piattaforme di scambio. Difatti, parallelamente a questi, sono state istituite una serie di organizzazioni o entità di "supporto", come ad esempio il Bitcoin Improvement Proposal (2011), il cu fine è aumentare l'efficienza delle comunicazioni all'interno della comunità, o la Fondazione Bitcoin (settembre 2012), la quale ha il compito di proteggere e supportare lo sviluppo di Bitcoin.
Durante questi anni, la curiosità sul "fenomeno Bitcoin" ha avuto un forte incremento, coinvolgendo una platea piuttosto variegata (stampa, banche o semplici appassionati) e toccando diversi campi di interesse (informatica e finanza su tutti, ma anche politica, sociologia…). La crescita del numero di investitori e rivenditori dediti all'uso della criptovaluta, unita alle numerose inchieste giornalistiche e studi accademici, sia sul *web* che sui mezzi di divulgazione tradizionali, ha contribuito a questa escalation di attenzione, in una spirale la cui naturale conseguenza è stata l'aumento del valore del bitcoin e della capitalizzazione di mercato. Complice l'intensa attività mediatica, nonché il raggiungimento di una massa critica di utenti-utilizzatori, anche gli stati nazionali hanno sentito il bisogno di studiare e comprendere il fenomeno, anche al fine di trovare un modo per riporlo sotto il proprio controllo, o quantomeno di gestirne gli effetti ed eventualmente sfruttarne le potenzialità.
Se si vuol individuare un punto di svolta, ossia quel particolare momento in cui Bitcoin "sale" sul palcoscenico (almeno per ciò che concerne le istituzioni e la stampa internazionale), si può guardare agli eventi legati alla crisi di Cipro del 2013 ed alle sue conseguenze. La crisi finanziaria aveva obbligato il presidente di Cipro, le istituzioni Europee e il Fondo Monetario Internazionale ad organizzare un piano di salvataggio da 10 miliardi di Euro, con l'obiettivo di rafforzare la debole economia cipriota In cambio dell'aiuto promesso, il governo cipriota si impegnò ad adottare una serie di misure economiche per fronteggiare la crisi. Nel pacchetto di riforme proposte figurava un prelievo forzoso sui conti correnti bancari superiori a 100.000 euro, nonché a

[8] Cfr. Mancini M. (2015), "*Valute virtuali e Bitcoin*", Analisi giuridica dell'economia, Il Mulino, pp. 117-138.

misure volte a contrastare il flusso di denaro in uscita dal paese. Al fine di non alterare il proprio patrimonio, i correntisti (tra i quali figuravano molti risparmiatori stranieri, in particolar modo russi) hanno convertito i propri averi in bitcoin. Questo episodio è ricordato dagli economisti come "effetto Cipro", sia per l'incremento del valore del bitcoin (da 80 a oltre 260 dollari) successivo a questo evento, sia per l'eco che la notizia ha avuto a livello globale (è probabile che molti abbiano sentito parlare di criptovaluta e bitcoin per la prima volta solo in questa occasione) e per la fiducia riposta nel Bitcoin da parte dei ciprioti, seppure in una situazione che non prefigurava un gran numero di alternative.

Figura 2 - Interesse nel tempo[9]



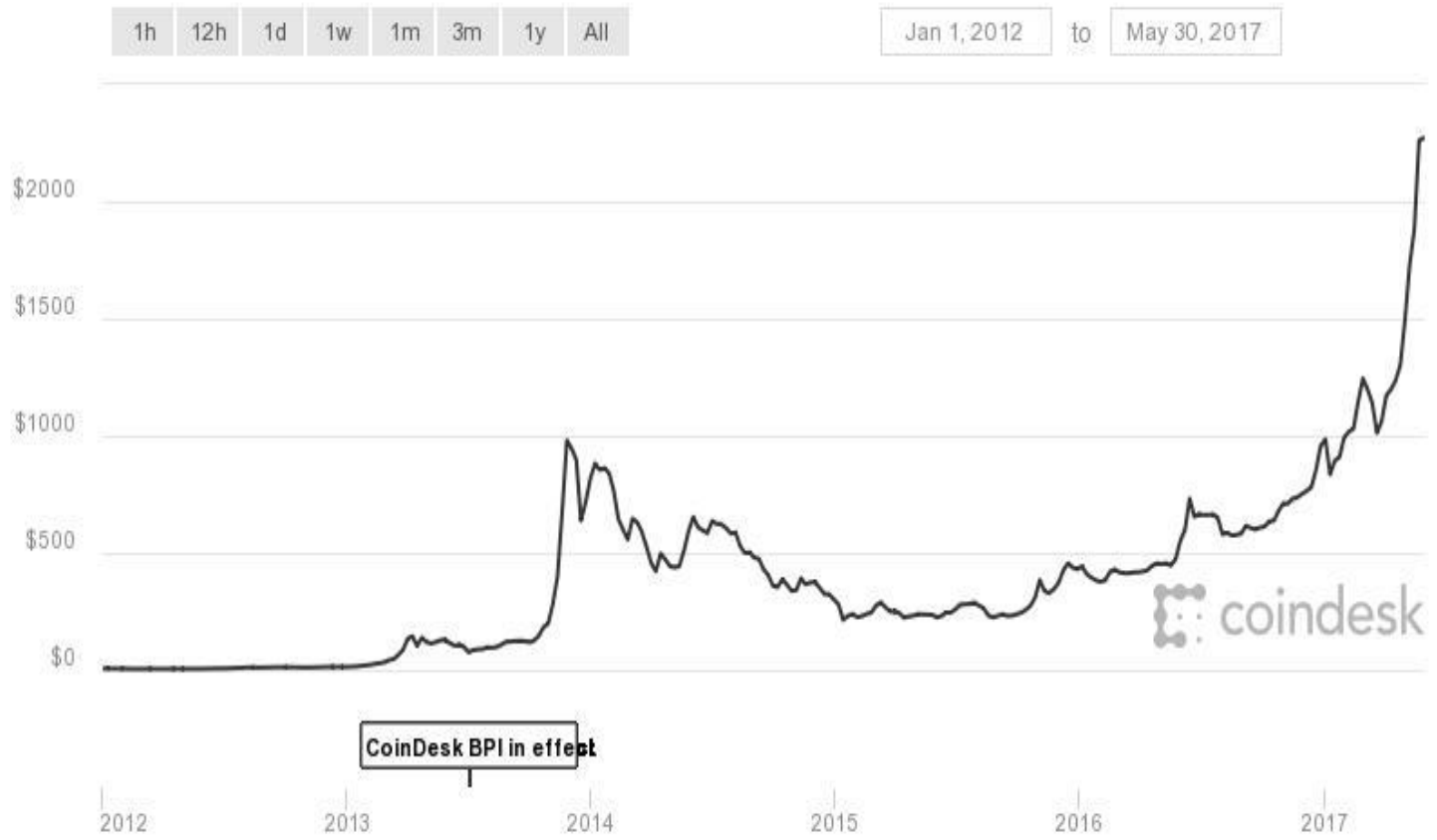
L'evoluzione dell'attenzione attorno a Bitcoin è sintetizzata nella Figura sopra esposta, che mostra i periodi di maggior interesse misurati sulla base delle ricerche effettuate su Google effettuate da tutto il globo. Il valore 100 indica la maggiore frequenza di ricerca del termine mentre 0 indica una frequenza di ricerca del termine inferiore all'1 per cento rispetto alla frequenza di ricerca maggiore.

1.2.5 Bitcoin e mercati

Parallelamente all'incremento dell'interesse attorno a Bitcoin ed al mondo delle criptovalute, si è assistito ad una continua, seppur in alcuni casi non costante, crescita dei principali indicatori economici. Si parta con l'analizzare l'evoluzione del prezzo del bitcoin, rappresentato dal tasso di cambio dollaro/bitcoin.

[9] Cfr. https://trends.google.com/trends (14/06/2017)

Figura 3 – Andamento del cambio USD/BTC[10]



Come si può facilmente osservare nella Figura 3, seppur con l'alternanza di fasi di espansione e di depressione, Bitcoin è andato ad apprezzarsi nel tempo.

Pur senza analizzare in dettaglio ogni singola oscillazione, è possibile riconoscere tutta una serie di eventi, più o meno collegati al mondo Bitcoin, che spesso spiegano tali variazioni nel prezzo (come la già analizzata questione di Cipro). È inoltre osservabile una certa correlazione fra interesse generato e prezzo del Bitcoin, come è possibile notare confrontando la Figura 3 con la precedente (Interesse nel tempo).

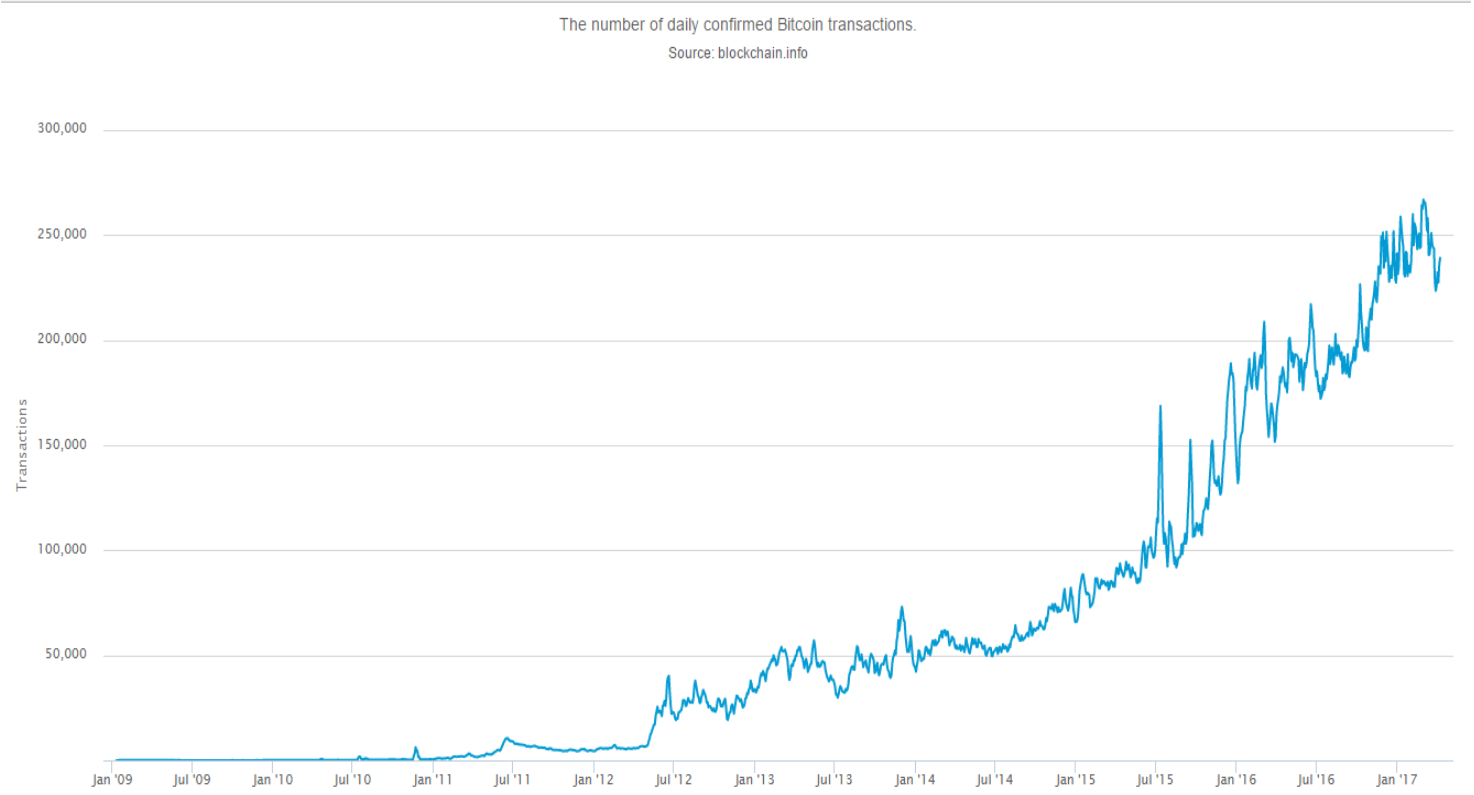
Ad esempio, quando è stato creato il primo bitcoin, il suo valore era ovviamente pari a zero: una valuta risponde alla legge della domanda e dell'offerta, come ogni altro bene, per cui in mancanza di una vera e propria richiesta il suo valore era essenzialmente nullo. Il cambio BTC/USD è rimasto fermo a zero per diverso tempo, almeno finché qualcuno non si è dimostrato disposto a pagare una somma superiore a 0 dollari per acquistare un bitcoin. Cosa poi effettivamente avvenuta nell'agosto del 2010, quando un bitcoin è stato scambiato per 7,69 centesimi di dollaro. Di particolare rilevanza sono inoltre le circostanze che hanno causato l'esponenziale crescita del 2013, il cosiddetto anno della gloria, durante il quale Bitcoin passa dai 31 dollari registrati in febbraio ai ben

[10] Cfr. www.coindesk.com (1/06/2017)

1.153 dollari "toccati" il 3 dicembre dello stesso anno. Oltre agli avvenimenti estivi di Cipro, che come si è visto hanno attirato l'interesse internazionale sulle criptovalute, si possono riconoscere due eventi che, a partire da novembre 2013, hanno permesso a Bitcoin di compiere l'incredibile balzo fino al suo massimo storico del tempo. In primo luogo, il Senato statunitense ha tenuto un'audizione dal titolo "*Oltre Silk Road: potenziali rischi, minacce e promesse delle monete virtuali*" il 18 novembre, all'esito della quale tutti i convenuti conclusero che Bitcoin abbia sorprendenti potenzialità per il futuro. Pochi giorni più tardi, nel corso di una conferenza, Mr. Yi, responsabile della sorveglianza dei flussi finanziari della Cina, ha dichiarato che i cittadini cinesi sono liberi di prendere parte al mercato di Bitcoin e che anzi la Banca Centrale Cinese avrebbe adottato una prospettiva di lungo termine sulla valuta virtuale. Come diretta conseguenza, il portale di scambio BTC China ha duplicato nel giro di pochi giorni il proprio giro d'affari ed il prezzo di Bitcoin ha continuato a salire[11].
Nel biennio successivo, complice una serie di avvenimenti "contrari" a Bitcoin, il valore della criptomoneta ha prima subito un forte deprezzamento (fino a giungere una quotazione anche inferiore ai 300 dollari), seguito poi da una relativa stabilità. Le ragioni del calo possono essere ricercate, ad esempio, nella retromarcia effettuata dalla Banca Cinese riguardo l'autorizzare le transazioni in bitcoin, nonché una serie di falle nella sicurezza informatica e dei mercati. È stato, in definitiva, una sorta di "periodo di assestamento" conseguente alla virtuosa crescita dell'anno precedente, a cui si sono accompagnate nuove incertezze e nuovi interrogativi sull'effettiva sopravvivenza futura della criptovaluta. La caduta del prezzo ha di fatto generato una comune ed erronea convinzione che Bitcoin fosse unicamente una bolla speculativa, un bluff destinato ad una lenta ma inesorabile transizione verso il fallimento ed il dimenticatoio. Tuttavia gli eventi successivi, come si avrà modo di analizzare a breve, sembrano smentire questa affrettata condanna a morte.
Sempre osservando il precedente grafico del tasso di cambio, è possibile notare che il prezzo del bitcoin è stato tutt'altro che stabile. Presenta al contrario una forte componente di variabilità che, come si vedrà in modo approfondito nel secondo capitolo, può tradursi in un limite non da poco nell'affermazione di Bitcoin a livello internazionale. Inoltre, tale variabilità è periodica, ossia a periodi di relativa stabilità se ne susseguono altri, improvvisi, in cui può raggiungere livelli molto elevati.
È opportuno aggiungere che, al fine di comprendere la dimensione della sua diffusione, non basta osservare l'evoluzione del prezzo o della capitalizzazione di mercato nel tempo. È altresì necessario analizzare anche ulteriori parametri, di cui particolare interesse risulta attrarre l'andamento del totale delle transazioni effettuate giornalmente, nonché del numero di utenti che usufruisce del sistema. Difatti, è proprio da questi indicatori che si può avere un'idea sulla capacità della valuta di circolare nel sistema economico ed avere un quadro della sua diffusione nello stesso.

[11] Cfr. Lemme G. e Peluso S. (2016), "*Criptomoneta e distacco dalla moneta legale: il caso bitcoin*", in Riv. dir. banc.,

Figura 4 – Totale delle transazioni giornaliere[12]



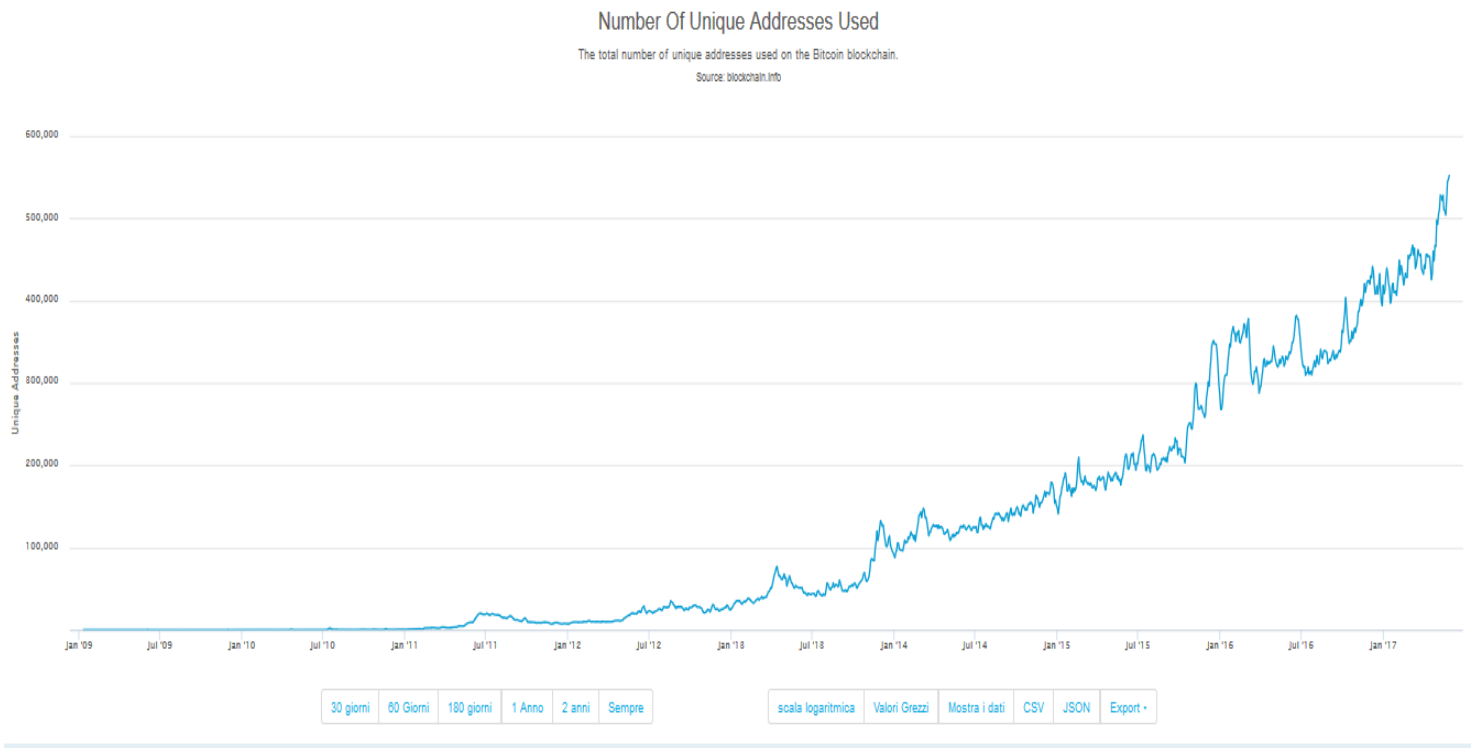
Come evidenziato nella Figura 4, il numero di transazioni giornaliere in bitcoin tende a crescere costantemente nel tempo. Ciò è un dato di particolare interesse se comparato con l'andamento del prezzo, in quanto ivi non si osserva la stessa depressione avuta dal tasso di cambio a partire dall'inizio del 2014. In altre parole, questo suggerisce che la fiducia degli utenti nel bitcoin non è venuta a mancare nemmeno nei momenti più "bui" della sua breve storia. Cosa che, tra l'altro, trova conferma anche nel grafico successivo: al pari del numero di transazioni giornaliere, anche il numero totale di indirizzi bitcoin attivi sulla Blockchain (e quindi, utilizzatori) non ha subìto arresti nella sua opera di crescita.

Figura 5 - Evoluzione del numero totale di indirizzi sulla blockchain[13]

dirittobancario.it, 43

[12] Cfr. https://www.blockchain.com (13/04/2017).

[13] Cfr. https://www.blockchain.com (30/05/2017).



Questi numeri necessitano di essere contestualizzati. Si è sicuramente difronte ad un fenomeno ai suoi albori, caratterizzato da un'espansione tanto notevole quanto instabile, tipica di questa fase. Tuttavia, se comparati con le altre valute "a corso legale", non si può ancora concludere che oggi il sistema sia un'alternativa radicata e diffusa. Sul piano strettamente quantitativo è facile guardare con sussiego al valore dei bitcoin emessi in rapporto a quello delle valute ufficiali: infatti, la capitalizzazione di mercato di bitcoin è meno di un millesimo della quantità di moneta in euro[14]. Si può concludere che, al momento, i livelli di attività di Bitcoin non sono tali da poter avere effetti sull'economia attuale, reale o finanziaria che sia, sebbene la velocità di sviluppo lascia presuppore la possibilità di un ruolo futuro tutt'altro che marginale.

1.2.4 Vulnerabilità

La diffusione di Bitcoin è stata tuttavia costellata anche da incidenti di percorso per così dire "interni" al sistema, che hanno di volta in volta portato gli *stakeholder* ad interrogarsi su nuovi aspetti e nuove problematiche.

Il 6 agosto 2010 è stata individuata una prima, importante vulnerabilità nel protocollo Bitcoin. Le transazioni non venivano correttamente verificate prima di essere incluse nella blockchain e ciò permetteva agli utenti, almeno in linea teorica, di scavalcare le restrizioni di Bitcoin e moltiplicare il numero di monete. Il 15 agosto, la vulnerabilità venne sfruttata; in una sola transazione furono generati 184 miliardi di Bitcoin e inviati a due

[14] Cfr. Amato M. e Fantacci L., (2016), "Per un pungo di Bitcoin", Egea, Università Bocconi Editore, Milano.

indirizzi sulla rete. Fu necessario un intervento diretto che, in poche ore, cancellò la transazione dalla Blockchain, risolvendo il *bug* ed aggiornando il protocollo.

Il fallimento di Mt Gox, una delle principali piattaforme di scambio della criptovaluta che aveva sede a Tokyo, assume un emblematico interesse riguardo alla sicurezza della rete ed ai meccanismi di gestione delle transazioni. Si stima che il cambiavalute giapponese abbia perso quasi 750 mila bitcoin, equivalenti a 350 milioni di dollari dell'epoca. Fin dalle sue origini, Mt Gox si propose come una sorta di intermediario per gli utenti, il primo nella comunità Bitcoin, con il compito di conservare i loro depositi e favorirne le transazioni. Negli ultimi sei mesi di operatività essa aveva gestito circa il 21 per cento di tutte le transazioni Bitcoin, sebbene la sua reputazione in questo periodo fosse già compromessa, avendo dato prova in più occasioni di essere un servizio poco sicuro. La società è stata quindi protagonista di un grosso *crack* nel corso del 2013, che l'ha portata a dichiarare bancarotta nel febbraio dell'anno successivo. Il motivo del fallimento risiede essenzialmente nella vulnerabilità nel sistema di registrazione delle transazioni dell'*Exchange*, che si è rivelato in altre parole esposto a delle continue sortite degli hacker durante tutti i 3 anni di attività. La chiusura di Mt Gox ha dunque catalizzato l'interesse attorno a diverse questioni, tra le quali spicca la mancanza di un comparto di tutele a sostegno degli utenti-investitori: diversamente dal fallimento di una banca tradizionale non esiste una copertura statale per i correntisti bitcoin, né alcuna forma di garanzia od assicurazione.

Nello stesso anno, il famoso caso Silk Road ha aperto a riflessioni sulla natura poco lecita di alcuni utilizzi di Bitcoin. Silk Road (la "via della seta") era un sito *web* (o per meglio dire, del c.d. *"dark web"*) dedito all*'e-commerce* di armi, sostanze stupefacenti ed altro materiale di contrabbando. La particolarità del portale era che si accettavano solamente pagamenti in criptovaluta. Il funzionamento della piattaforma era piuttosto immediato. Gli utenti dovevano inizialmente procurarsi bitcoin come valuta di scambio e creare un indirizzo *email* falso, per poi contraffare il proprio indirizzo IP tramite un apposito *software* in modo da operare in totale anonimato. Sull'interfaccia del portale era presente un lungo elenco di beni e servizi da poter acquistare, associati al profilo utente del venditore e ad un rating circa la sua affidabilità. La consegna dei beni avveniva tramite posta, ma il sito suggeriva di fornire indirizzi di luoghi abbandonati e nomi inventati. Le comunicazioni tra venditore e acquirente non potevano essere tracciate dalle autorità, cosa che permetteva al compratore di negare l'acquisto nel caso di un controllo nei centri di smistamento postale. La chiusura del sito e la conseguente condanna dell'amministratore del sito, Ross Ulbricht[15] (per i reati di associazione a delinquere, frode informatica, distribuzione di false identità, riciclaggio di denaro e traffico di droga) si caratterizza come uno snodo importante nella storia di Bitcoin. È probabilmente in questa occasione che le autorità pubbliche riconoscono

[15] Inizialmente, l'identità di Ulbricht era ignota. Le autorità federali americane hanno impiegato oltre 6 mesi per rintracciare chi si celava dietro lo pseudonimo di "Dread Pirate Roberts".

realmente le potenzialità deleterie della criptomoneta e la necessità di una considerazione più seria e approfondita del fenomeno nonché sulle possibilità di risposta normativa adeguata.

1.2.6 Eventi recenti e sviluppi futuri

A partire dalla seconda metà del 2016, ed in particolare durante la prima metà del 2017, Bitcoin è stato protagonista di una crescita senza precedenti: il valore della moneta virtuale ha toccato i 2800 dollari per *token* nel mese di maggio, raddoppiando il valore registrato appena due mesi prima e facendo ampiamente meglio dei listini di riferimento di Wall Street (lo Standard & Poor's 500 è salito dell'8,8 per cento da inizio anno e il Nasdaq del 16,9 per cento). L'andamento della valuta digitale è comunque sempre caratterizzato da forte volatilità: per esempio, il 25 maggio, nel corso della stessa seduta, bitcoin ha prima guadagnato fino al 12 per cento e poi ha ceduto più di 300 dollari. La nuova fase evolutiva che riconosce nel mondo orientale il principale attore: il Giappone ha riconosciuto ufficialmente il Bitcoin dandogli legittimazione in Asia[16]; la Cina è il secondo mercato Bitcoin al mondo subito dopo gli USA; in Corea si sta verificando un boom di commercianti che accettano Bitcoin e soprattutto di sportelli che utilizzano Bitcoin per trasferire denaro all'estero senza commissioni.

È altresì vero che anche il mercato statunitense potrebbe essere foriero di ulteriori opportunità di sviluppo. Si attende un secondo responso della Sec[17], che potrebbe dare il via libera ad un ETF (*Exchange Traded Fund*, un particolare fondo di investimento quotato in Borsa che di solito investe su indice) legato proprio al bitcoin. Il primo responso, avvenuto agli inizi dell'anno e preceduto da uno studio di oltre 3 anni, è stato negativo. L'idea dell'ETF in criptomoneta è dei gemelli Winklevoss, diventati famosi per la causa civile contro Mark Zuckerberg al quale contendevano la creazione di Facebook. Un contenzioso legale terminato con un accordo finanziario, i cui proventi sono stati investiti dai due fratelli per buona parte sulla moneta virtuale[18]. L'eventuale accettazione da parte delle storicamente severe autorità statunitensi potrebbe condurre ad un'ulteriore fase di diffusione del bitcoin sul suolo americano, con conseguenti effetti anche sulla scena internazionale. Si tratterebbe inoltre di un deciso passo avanti nel riconoscimento di Bitcoin nel mondo della finanza, accompagnandosi alla sempre presente necessità di completare ed adeguare nel tempo la normativa riguardante le criptovalute.

---

[16] Ad aprile 2017 in Giappone è stata approvata la prima legge nel mondo che riconosce Bitcoin e tutte le altre criptovalute come mezzi di pagamento. Si tratta di una legislazione pionieristica, accolta con entusiasmo da aziende ed investitori, che permette l'utilizzo di bitcoin per svariate operazioni commerciali, incluso ad esempio il pagamento delle bollette del gas. Le transazioni in criptovalute hanno già raggiunto punte del 40% del totale delle transazioni finanziarie effettuate.

[17] Securities and Exchange Commission, l'autorità di controllo dei mercari finanziari; è l'equivalente americana della Consob italiana.

[18] Cfr. Pagni L. (2017), "*Bitcoin, quotazione record: il vento d'Oriente spinge la moneta virtuale*", Repubblica, Economia e Finanza, http://www.repubblica.it/economia/finanza/2017/05/30/news/bitcoin-166654682/?ref=RHPPBT-VE-I0-C6-P8-S1.6-T1 .

Parte del futuro di Bitcoin dipenderà da come verrà trattato in ambito legislativo da parte degli ordinamenti di tutto il mondo e da quanto verrà accettata dalle autorità finanziarie come asset di investimento o come moneta. In tal direzione, un ruolo di grande importanza potrà esser giocato dal tentativo delle autorità di contrastare gli usi illeciti di valuta digitale. Difatti, di pari passo con le novità presentate nel campo finanziario, anche nell'ultimo biennio Bitcoin ha avuto un certo risalto per collegamento con la criminalità: in primis si guardi a "Wannacry", il *randosomware*[19] responsabile dell'epidemia globale che criptava i *file*, ed attraverso il quale i pirati informatici hanno richiesto il riscatto proprio in bitcoin.

Un importante dibattito si è invece aperto tra i membri della community riguardo un problema prettamente tecnico, relativo alla capacità massima della rete Bitcoin di elaborazione e validazione delle transazioni. Secondo le simulazioni questo limite è pari, nella migliore delle ipotesi, a circa 350 mila transazioni giornaliere. Il rischio è quello di un sistema che discrimini le transazioni in base alla consistenza delle commissioni (facoltative), creando "code di attesa" sempre più lunghe ed impedendo, in sostanza, le transazioni di piccole quantità. Le proposte per aumentare la capacità di validare transazioni sono essenzialmente di due tipi, ossia "*on-chain*", attraverso l'aumento delle dimensioni dei blocchi, ed "*off-chain*", con sistemi che permettano di fare molte transazioni di segno diverso su canali di pagamento e che si compensino di tanto in tanto sulla blockchain. È evidente che ognuna delle proposte attiri gli interessi economici di soggetti diversi. Bitcoin è stato vicino alla scissione, che avrebbe dovuto portare alla divisione della rete in Bitcoin e Bitcoin Unlimited, nella quale quest'ultimo avrebbe portato all'adozione di un nuovo Protocollo Unlimited capace di livellare la dimensione dei blocchi e, di conseguenza la capacità della rete di validare le transazioni. La scissione non è tuttavia andata in porto, rafforzando la criptovaluta agli occhi degli investitori. Tuttavia, un ennesimo interminabile periodo di trattative e discussioni non è per nulla auspicabile a fronte di un problema che presenterà presto il conto e che necessita quanto prima di una soluzione.

1.3 Impatto sociale, politico ed economico

1.3.1 Ideologia del Bitcoin: la critica al sistema bancario

La teorizzazione, la progettazione ed infine l'implementazione di Bitcoin si legano indissolubilmente al periodo storico in cui esso si colloca, configurandosi infatti come una risposta ai turbamenti sociali, economici e politici del tempo. Come già sostenuto, Bitcoin si pone come sistema di pagamenti alternativo al sistema delle banche e in generale all'uso degli intermediari. Alla sua base vi è un contrasto di fondo degli sviluppatori con la politica

[19] Un *ransomware*, (come ad esempio Cryptolocker, Torrentlocker o CBT-Locker) è un tipo di *malware* che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (*ransom* in Inglese) da pagare per rimuovere la limitazione.

monetaria attuata dalle Banche Centrali, giudicata essenzialmente inefficace nel condurre il proprio compito (ricercare la stabilità dei prezzi, favorire lo sviluppo economico…). Secondo gli sviluppatori ed i sostenitori di Bitcoin le banche appaiono sempre più chiaramente come portatrici di un potere oligopolistico, beneficiarie di aiuti statali immeritati, usurpatrici di un bene comune (la politica monetaria), giustificate dal fatto di svolgere una funzione tipicamente pubblica ma che sembrano sempre meno efficienti a svolgere[20]. Bitcoin è dunque figlio di questa critica, è diretta conseguenza di una politica giudicata fallimentare su tutta la linea, è l'occasione per fuggire alla dittatura imposta dal cosiddetto *Wall Street System*. Ed è difatti proprio durante la crisi finanziaria del 2008 che Bitcoin comincia a muovere i suoi primi passi, ossia quando, specialmente con riguardo all'area Euro, emergono sempre più palesemente i limiti e le incongruenze delle autorità monetarie e delle politiche economiche attuate sino ad allora. In particolar modo, le banche centrali sembrano aver perso il controllo del processo di creazione monetaria a favore di un oligopolio bancario, che rende inefficace ogni politica sistemica e rallentando la circolazione di moneta. Emblematico è il caso europeo ed il *long term refinancing operation* di Mario Draghi: l'immissione di nuova liquidità nel sistema economico non ha prodotto gli effetti desiderati, in virtù di un sistema bancario capace di contrastare quasi totalmente le politiche espansive della BCE; anche a fronte di finanziamenti a tassi prossimi allo zero e per quantità potenzialmente illimitate, le banche non hanno trasformato questo denaro disponibile in finanziamenti all'economia reale e allo sviluppo. L'effetto è che gli scostamenti di breve periodo dalla relazione di lungo periodo fra quantità di moneta e livello dei prezzi hanno mostrato di poter durare indefinitamente.

Il risultato dell'inefficacia delle contromosse adottate dal sistema non ha fatto altro che accentuare le tensioni. Il sistema attuale, nel quale le banche hanno "in ostaggio" il sistema dei pagamenti, crea un'instabilità che viene curata con ulteriore potenziale instabilità. In uno scenario simile, si profila il rischio che moneta, creazione di moneta e politica monetaria non significhino più nulla di determinato. Anzi, lungi dal curare il sistema le azioni che si intraprendono sembrano in realtà volte a salvare posizioni di indebito privilegiate, e di fatto a rafforzarle. L'oligopolio genera e rafforza oligarchie[21].

Da qui, la forza ed il fascino che circonda Bitcoin. Nakamoto e seguaci riconoscono questa malattia del sistema e rispondono proponendo un modello diametralmente opposto a quello in vigore, la cui radicalità trova la sua massima espressione nella loro idea di gestione dell'offerta di moneta. La "medicina" proposta da Bitcoin è tanto semplice quanto drastica: se il sistema bancario si rivela incapace di trasmettere appropriatamente le politiche monetarie, rendendo di fatto inefficace la creazione di moneta, tanto vale rendere l'offerta di moneta completamente esogena rispetto al sistema di scambi che è chiamata a gestire, pre-impostandone l'emissione secondo un determinato sentiero evolutivo e bloccandone la quantità massima ad un ammontare fisso. Sempre

[20] Cfr. Amato M. e Fantacci L., (2016) "*Per un pungo di Bitcoin*", Egea, Università Bocconi Editore, Milano.

[21] Cfr. Amato M. e Fantacci L., (2016) "*Per un pungo di Bitcoin*", Egea, Università Bocconi Editore, Milano.

nell'ottica di Bitcoin, la "scarsità artificiale", quasi a riproporre un modello *gold standard*, è determinante essenziale al conseguimento della stabilità del potere di acquisto, evitando così pericolose svalutazioni della moneta dovute ad un'eccessiva emissione-creazione. La caratteristica del bitcoin di essere un valore attivo del possessore senza essere un passivo per un altro soggetto va letta proprio in quest'ottica: in tal modo si impedisce che la moneta possa essere "creata" dal sistema bancario attraverso la moltiplicazione dei depositi e dunque si priva l'ente centrale di iniettare nuova liquidità nel sistema a seconda delle proprie esigenze. È proprio in questo modo che la moneta è radicalmente esogena, quando nessuno può influire sulla creazione monetaria.
Si tratta di una visione non esente da critiche; in particolar modo, ci si chiede se il privare del tutto la politica monetaria di uno strumento importante quale la creazione monetaria possa essere una soluzione efficace.

1.3.2 Fiducia

Con riferimento alle valute tradizionali, secondo Nakamoto la radice del loro problema risiede nella fiducia posta nell'autorità centrale dedita al loro funzionamento. Attraverso la de-centralizzazione, Bitcoin punta a rendere l'offerta di moneta indipendente dal "fattore umano" e, di conseguenza, indipendente dal rischio di errori che esso porta con sé: i "Bitcoiner" credono che solo la tecnologia possa svolgere un ruolo così delicato quale quello della creazione di moneta[22]. A tal proposito, spesso Bitcoin è definito come un sistema *trust-less*, privo di fiducia*:* dal protocollo Bitcoin si può leggere: "Ciò che serve è un sistema di pagamento elettronico basato su prove crittografiche, invece che sulla fiducia, che consenta a soggetti consenzienti di negoziare direttamente tra loro senza la necessità di un garante terzo". L'idea è dunque quella di fondare un'economia che sia in grado di fare a meno della fiducia, in nome di una maggior libertà dei singoli ed in forza di un protocollo informatico immodificabile. In più, Bitcoin diffonde su fronti sempre più ampi la sua promessa di costruire una vita sociale che prescinda totalmente dalla fiducia. La "mancanza di fiducia" tocca non soltanto le banche commerciali e le autorità monetarie, ma anche le istituzioni, gli organismi di supporto, i teorici sino ad arrivare alle persone comuni.
Tuttavia, in questa sede si ritiene che, piuttosto che ad una generica mancanza di fiducia, si assiste di fatto ad un trasferimento di questa, sotto un duplice punto di vista. In primo luogo, si parla di un trasferimento di fiducia dall'uomo (l'autorità di garanzia), che nell'ottica Bitcoin non è ormai più affidabile, alle leggi della matematica e dell'informatica (ossia alla crittografia e agli algoritmi che stanno alla base del sistema). L'utente è infatti chiamato ad una "prova di fiducia" verso la tecnologia Bitcoin in sé per sé, o se si vuole nei confronti dell'informatica nel suo complesso, e verso l'idea che questi possa essere una soluzione più sicura e più efficiente del sistema umano. In secondo luogo, si assiste ad un trasferimento della fiducia dal singolo alla collettività, in una sorta di fiducia distribuita. Quest'ultimo punto è di grande interesse: si è detto che è

attraverso questa fiducia che Bitcoin assegna alla Rete quel ruolo di primissimo piano di cui si fa promotore. I nodi sono alla base dell'accettazione e della validazione delle transazioni, nonché sono adibiti a proporre ed implementare, tramite votazione ed approvazione a maggioranza, le modifiche al sistema. Si palesa dunque la necessità di un'onestà di fondo non più di un soggetto od un ristretto gruppo di soggetti, ma della Rete stessa nella sua interezza (o quantomeno della maggioranza dei suoi nodi). In altre parole, si tratta di una fiducia rimessa all'idea che un gruppo di persone (tutta la rete Bitcoin) possa avere la capacità di organizzarsi, di autogestirsi, di adattarsi di volta in volta alle contingenze provenienti dal mondo "esterno". A questo si deve necessariamente aggiungere l'atto di fiducia posto nell'altrui accettazione presente e futura della criptovaluta come mezzo di scambio, in mancanza di un vero e proprio vincolo giuridico in tal senso. Questo sistema comporta tutti i naturali limiti intrinsechi delle organizzazioni sociali: anche all'interno della rete Bitcoin sussistono fazioni di diversa ideologia, con interessi economici di natura eterogenea che talvolta possono confliggere e portare il *network* ad una sorta di stallo, causando rallentamenti alla risoluzione di problematiche anche gravi.

1.3.3 Ideologia politica e movimento sociale

La critica perpetuata da Bitcoin non si esaurisce nell'opposizione al sistema bancario. La sfiducia verso l'essere umano e le istituzioni da esso creato porta di conseguenza a generare riserve, in capo a gran parte dei *supporter*, anche nei confronti dello Stato. Sia bitcoin che tutte le altre criptovalute sembrano attrarre l'interesse, di natura prevalentemente politica, di tutta una serie di soggetti con simpatie filo-anarchiche e filo-liberali che vorrebbero privare lo Stato del controllo della moneta[23]; lo stesso intento dei suoi creatori sembra connotare Bitcoin di natura economica liberale, ed in proposito è illuminante una breve citazione di Nakamoto sui i motivi dell'ideazione dell'intero sistema: "*Bitcoin is very attractive to the libertarian viewpoint if we can explain it properly"*.

Una ricerca ha evidenziato che le idee politiche contribuiscono a simpatizzare ed eventualmente adottare Bitcoin. Quasi la metà degli intervistati (47 per cento), che si definisce "*libertarian*", vedono nel Bitcoin uno strumento di liberazione dal potere pubblico, che permette di aggirare regolamentazioni e divieti in un orizzonte che può arrivare a comprendere la "dissoluzione dello Stato" e l'instaurazione del "primo vero libero mercato della storia". Tuttavia, si preme in questa sede avvertire il lettore che ciò non deve condurre ad una politicizzazione *in toto* del Bitcoin: le idee politiche non sembrano essere l'unico fattore scatenate l'utilizzo dello stesso, ed infatti non deve sorprendere che una parte minoritaria, ma non irrilevante, degli utilizzatori non si definisca liberare, bensì socialista (9 per cento), ecologista (7 per cento), genericamente progressista (17 per

[22] Cfr. Nigel Dodd (2017), "*The social life of Bitcoin*", Theory, Culture & Society. ISSN 0263-2764.

[23] Cfr. Nigel Dodd (2017), "*The social life of Bitcoin*", Theory, Culture & Society. ISSN 0263-2764.

cento), o anche anarchica (7 per cento) [24].

L'idea politica di Bitcoin si formalizza attraverso una ricreazione informatica non solo del mondo economico, ma di tutta la società, ritenendo che tale mondo così ricreato non possa che essere migliore.

Questa ideologia è totale e coinvolge i più disparati aspetti della vita dell'individuo e della collettività ed arriva a toccare anche il comparto legislativo. Bitcoin infatti "crea" un proprio diritto, per lo meno nell'ambito delle transazioni commerciali. Si assiste ad una sostituzione della legge come tradizionalmente conosciuta, un'appropriazione di un potere prettamente politico: il codice informatico sostituisce la legge, ne prende il posto nei meccanismi di regolazione del mercato e nei rapporti tra individui tra gli individui, in una spirale che giunge a privare anche la formazione legislativa del tanto bistrattato fattore umano. Si guardi ad esempio al diritto alla *privacy*. Nel modello bancario tradizionale, il garante e le parti coinvolte in una transazione sono gli unici soggetti che hanno accesso alle rispettive informazioni sensibili. Complice la già approfondita sfiducia nel sistema, ogni singola transazione può essere vista, nell'ottica delle parti, come un fulcro di informazioni che il garante può utilizzare per i più svariati fini, leciti o meno. Attraverso la pubblicazione di ogni transazione sulla Blockchain, Bitcoin stabilisce un modo differente nel tutelare il diritto alla *priva*cy, quasi a volersi sostituire alle forme di tutela nazionali. Grazie allo pseudo-anonimato, tutti possono vedere che qualcuno sta spedendo un certo importo a qualcun altro, senza tuttavia poter legare le informazioni della transazione ad un particolare soggetto. Questo meccanismo è simile al livello di informazione pubblicato dalle borse valori, dove il momento e la dimensione delle singole transazioni, il "nastro", viene pubblicato senza dire chi erano i soggetti coinvolti[25]. Sotto quest'aspetto, Bitcoin punta soddisfare le richieste di maggior *privacy* di quell'insieme di utenti che giudicano eccessivo il controllo del sistema

Bitcoin è al tempo stesso assimilabile ad un "movimento sociale": qualunque sia la provenienza politica dei suoi sostenitori, sembra che la "protesta" sia il fattor comune a cui tutti convergono. Come sostenuto, la protesta è rivolta principalmente verso i governi, che non sono giudicati quali autorità affidabili, specialmente a causa della comune tentazione di iniettare nuova moneta nel sistema come espediente politico (pur se questo può causare alta inflazione). D'altra parte, il rischio di una strumentalizzazione populista e demagogica di Bitcoin è dietro l'angolo. A riguardo è illuminante la dichiarazione di Roger Ver, uno dei maggiori investitori della criptovaluta, che sintetizza efficacemente (ed involontariamente) le possibili estremizzazioni di una parte dei più ferventi sostenitori: "Bitcoin priverà i governi dall'abilità di stampare moneta per il solo fine di acquistare carri armati ed armi e bombe per assassinare persone in tutto il mondo".

---

[24] Cfr Bohr J. e Bashir M. (2014), "*Who Uses Bitcoin? An exploration of the Bitcoin community*", Privacy, Security and Trust (PST), Twelfth Annual International Conference on. Toronto, Canada.

[25] Cfr. Nakamoto S. (2008), "*Bitcoin: un sistema di contanti elettronico peer-to-peer*", www.bitcoin.org.

1.3.4 Globalizzazione

L'agevole reperibilità delle infrastrutture tecnologiche occorrenti all'utilizzo e la diffusione capillare della rete internet rendono Bitcoin accessibile ad una vasta platea di utenti, consentendo operazioni anche tra soggetti operanti in diversi paesi. Da qui, emerge la sua natura "globale": non solo Bitcoin offre un sistema di trasferimento di moneta efficiente, sicuro ed economico, ma si propone, anche ideologicamente, come un'ambiziosa valuta "sovranazionale", al di sopra delle comuni spartizioni geopolitiche ed economiche. Il successo di Bitcoin è reale soprattutto in relazione ai costi di transazione ed alle tempistiche per trasferimenti di denaro da un paese all'altro: tradizionalmente, i *transfer* con le valute tradizionali sono molto lenti e costosi, ma risultano ancor meno convenienti se rapportati con le nuove possibilità offerte dalle criptovalute. In più, gli utenti possono beneficiare di tempi di verifica e di regolamento della transazione notevolmente più brevi di quelli normalmente necessari con la moneta scritturale, poiché il completamento del processo è normalmente pari a dieci minuti per le valute virtuali decentrate e può essere addirittura istantaneo per quelle a schema accentrato. Inoltre, tali tempi non subiscono variazioni legate alla distanza geografica fra le parti dell'operazione di trasferimento[26]. Dall'altra parte, il costo di un'operazione eseguita mediante valute virtuali è molto più basso se comparato con quelli che si dovrebbero corrispondere per la prestazione di un servizio di pagamento in valuta "tradizionale". Questi devono coprire solamente i costi di mantenimento, o meglio di compensazione, dei *miner*; non essendoci alcun supporto fisico, questi costi non includono tutta una serie di voci (quali stoccaggio, autenticazione, trasporto e sicurezza) di cui le valute *standard* non possono fare a meno. Si osservino le differenze di costo tra un trasferimento di bitcoin ed un trasferimento di denaro nel sistema tradizionale: in media, i costi per una transazione in Bitcoin oscillino tra lo 0 e l'1 per cento del valore della transazione stessa mentre quelli per una transazione in valuta *standard* arrivino a una percentuale dal 2 al 5 per cento[27]. Oltretutto, i bitcoin sono esenti da rischio di cambio fra divise legali. Ma i benefici non terminano qui, in quanto i costi sopportati dal ricevente sono in genere anche più bassi di quelli del mittente, poiché questi non sopporta in genere alcuna commissione ma deve sostenere solo il costo dell'apertura di un conto in valuta virtuale e di un *wallet* digitale.

In definitiva, la logica sottesa all'elegante disegno organizzativo del Bitcoin è invero quella di un infrastruttura tecnologica che, essendo in grado di operare trasferimenti di valore in maniera continuativa (24 ore su 24, 7 giorni su 7), in un contesto geografico essenzialmente illimitato e senza il bisogno, per l'espletamento delle tradizionali funzioni di supervisione dei processi e verifica della genuinità e validità degli scambi,

[26] Cfr. Mancini M. (2015), "Valute virtuali e Bitcoin", Analisi giuridica dell'economia, Il Mulino, pp. 117-138.

[27] Cfr. Lemme G. e Peluso S. (2016), "*Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Riv. dir. banc."*, dirittobancario.it, 43

dell'intervento di intermediari autorizzati, si presenta come uno strumento - almeno sulla carta - più snello, diretto, efficiente ed economico rispetto ai consueti sistemi di pagamento internazionali[28].

Come ultimo punto, si può sostenere che la copertura globale ponga Bitcoin parzialmente al riparo da quelli che possono essere *shock* locali, quali ad esempio quelli generati da instabilità politiche, catastrofi ambientali e conflitti armati, che invece potrebbero avere effetti anche drammatici sul valore delle valute locali.

1.4 Caratteristiche tecniche

Conoscere Bitcoin significa comprenderne anche il funzionamento da un punto di vista tecnico. Nei seguenti paragrafi sarà data un'infarinatura generale di queste caratteristiche, analizzando il funzionamento della Blockchain e dei portafogli bitcoin, per procedere con le modalità di gestione delle transazioni ed il funzionamento dell'attività di *mining.*

1.4.1 Blockchain

La blockchain è probabilmente l'innovazione più importante di Bitcoin. Essa consiste in un *database* che annovera tutte le transazioni mai eseguite nella rete Bitcoin durante tutta la sua storia, una sorta di registro digitale unico, distribuito, pubblicamente consultabile, permanente e resistente ad alterazioni, mantenuto "in vita" dall'attività congiunta di tutti i nodi del sistema. È possibile vederlo come un'evoluzione del libro mastro, un registro contabile delle sole transazioni in bitcoin. In particolar modo, nella blockchain sono annotate sia l'importo della transazione che la sigla (lo "pseudonimo") corrispondente a chi la compie.

La blockchain è articolata in blocchi di transazioni: ogni nuovo blocco od insieme di operazioni è legato al precedente, formando di riflesso la catena dei blocchi (da cui, appunto, "blockchain"). L'ultimo blocco al termine delle maglie della catena è temporalmente posteriore ad ogni blocco che precede. Avendo accesso al blocco più recente, ogni utente può seguire la catena all'indietro per osservare ogni transazione in bitcoin fatta in precedenza. Tramite questo meccanismo, tutte le transazioni sono perfettamente tracciabili; in questo modo è inoltre risolto per la prima volta il problema della *double-spending* in maniera distribuita, ossia il sistema assicura che soltanto i reali possessori di una somma possano spenderla, servendosi di un meccanismo a firma digitale tramite chiave pubblica, che verrà successivamente spiegato nel dettaglio.

Il funzionamento della blockchain è governato da leggi matematiche e dal *software,* senza dipendere da alcuna entità di controllo centrale, mentre eventuali modifiche a questo non possono essere effettuate da un singolo nodo. Come anticipato, è tutta la Rete che è adibita al suo controllo, a valutare ed eventualmente integrare le

[28] Cfr. Gasparri G. (2015), "*Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*", Diritto dell'informazione e dell'informatica, 31(3), 415-442.

innovazioni proposte da un nodo, tramite un meccanismo di votazione ed approvazione a maggioranza.
L'innovazione apportata dalla struttura della Blockchain è risultata talmente importante e funzionale che diversi individui hanno proposto di utilizzarla anche in altri ambiti, come ad esempio quello politico, giuridico, sociale e scientifico. In qualità di registro pubblico irreversibile ed inalterabile per documenti, contratti, proprietà e beni, la Blockchain può essere utilizzata per contenere informazioni e istruzioni, con applicazioni come gli *smart contract* o *multisignature transaction*. Gli *smart contract* sono contratti informatici in grado di entrare in esecuzione e far rispettare le proprie clausole senza un intervento di un soggetto terzo alle parti. Uno *smart contract* può prevedere una serie di obblighi, clausole, benefici e sanzioni che sono a carico di una o di tutte le parti del contratto, nelle diverse circostanze. A differenza dei contratti tradizionali, questi contratti possono ricevere informazioni come *input* e, dopo un'elaborazione basata sulle regole definite, eseguire delle azioni come *output*. Una delle "nuove" criptovalute che ha incluso l'uso di *smart contract* nella blockchain è Ethereum. Le transazioni *multisignature* sono d'altra parte transazioni che possono essere eseguite solamente se c'è l'autorizzazione da parte di più soggetti. Di particolare interesse sono i *multisignature script,* utilizzati nel commercio *online* per assicurarsi di avere indietro la somma inviata se la merce non è spedita.
Anche in questi casi, il vantaggio introdotto dalla blockchain è quello di non imporre più il bisogno di una terza parte di fiducia per l'esecuzione dei contratti, come un notaio od un intermediario; la piattaforma permette un'esecuzione automatizzata ed affidata alla crittografia, cosa che consente maggiormente di proteggere i partecipanti da rischi di illeciti e che allo stesso tempo riduce le spese di gestione delle pratiche stesse. La blockchain dunque aggiunge una componente non indifferente di maggior trasparenza e di efficienza nella gestione dei costi, nonché anche in questo caso priva l'esecuzione dei contratti della discrezionalità tipica del fattore umano. Alla luce di questa serie di implicazioni, la blockchain può rivelarsi un'innovazione rivoluzionaria per molte tipologie di contratti e numerose attività di *business*.

1.4.2 Wallet e indirizzo identificativo

Il distacco di Bitcoin dal sistema bancario si realizza ulteriormente con la modalità di conservazione di moneta. I bitcoin sono difatti conservati in "*wallet*", una sorta di portafoglio informatico composto da un file criptato accessibile solo possedendo la relativa *password*. Ciò significa, anche in questo caso, che non vi è alcun ente terzo demandato alla gestione ed alla protezione delle monete di proprietà, favorendo il completo controllo da parte degli utenti sui propri bitcoin ed i propri *account*.
Il *wallet* funziona grosso modo come un vero e proprio portafoglio fisico, ove il proprietario conserva criptomoneta anziché le banconote in contanti. Vi sono tuttavia alcune differenze. Non avendo consistenza materiale, il *wallet* digitale è conservato su piattaforme elettroniche, come personal computer, smartphone o tablet; ciò consente al detentore di creare più copie di *backup*, ad esempio su *hard disk* esterni, chiavette USB,

servizi di *file storag*e *online* come Google Drive e Dropbox), e anche se qualcuno trovasse il *wallet* non potrebbe utilizzarlo senza conoscere la *password*. Il lato negativo, a livello di sicurezza, riguarda l'accentramento di ricchezza in un solo *wallet*: a meno che non se ne utilizzino diversi (soluzione con evidenti problemi di gestione), il portafoglio conterrà tutti i bitcoin posseduti e la perdita del file (o della *password*) potrebbe essere molto peggiore dello smarrimento di un portafoglio fisico in cui in genere si conserva solo una piccola quantità di denaro.

Ad oggi è possibile scegliere tra diversi *software* per la creazione di *wallet,* come Electrum o Bither, che si differenziano l'un l'altro per livelli di sicurezza, *privacy*, velocità o altre svariate caratteristiche. Questi *wallet provider* consentono di detenere, conservare e trasferire criptivaluta, favorendo l'esecuzione delle transazioni non solo con gli Exchanger, ma anche con i commercianti che accettano di ricevere valuta virtuale in cambio della fornitura di beni e servizi[29]. Generalizzando, i metodi di gestione dei bitcoin possono essere suddivisi in due categorie. Il primo, definito "*hot storage*" o *online*, prevede che il dispositivo su cui sono salvate gli indirizzi privati dell'utente è lo stesso dispositivo connesso alla rete Internet ed al *network* Bitcoin. A questi si contrappongono i metodi di gestione "*cold storage*", o *offline*, in cui gli indirizzi sono sempre salvate ed utilizzate su dispositivi non connessi alla rete. Per questo motivo, i metodi *hot* sono meno sicuri di quelli *cold,* ma più semplici e veloci nell'utilizzo.

Nei sistemi di hot storage, l'utente deve provvedere ad una registrazione online che, una volta effettuata, consente di ottenere il primo indirizzo personale, o bitcoin *address*, un codice alfanumerico di 33 o 34 caratteri che è a tutti gli effetti ciò di cui un utente ha bisogno per inviare e ricevere pagamenti. L'utente ha anche la facoltà di poter aggiungere al proprio portafoglio altri indirizzi, ognuno con una diversa chiave d'accesso. Per facilitarne l'utilizzo, Bitcoin prevede la possibilità di utilizzare un *QR Code* in sostituzione dell'indirizzo alfanumerico. Per ricevere un pagamento, non servirà altro che fornire al creditore l'*address* o il codice QR, che contiene tutte le informazioni necessarie per completare la transazione.

1.4.3 Le transazioni

Il problema principale di un'economia, a livello sistemico, potrebbe riguardare le transazioni. In un sistema centralizzato, la banca o l'intermediario svolge un ruolo di garante dei pagamenti, assicurando che le transazioni siano svolte in totale sicurezza ed evitando il problema della *double spending*. In altre parole, è la banca che verifica l'identità delle parti, si assicura dell'effettiva disponibilità dei fondi, predispone la transazione e notifica il successo o meno della stessa, nonché tiene registro di tutte le transazioni in capo ad ogni soggetto. Come si è visto, il sistema proposto da Nakamoto è diverso, non prevedendo alcun controllo di questo tipo. Per

[29] Cfr. La Rocca L. (2015), "*La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*", Analisi giuridica dell'Economia, Il Mulino, pp. 201-220.

fronteggiare questo problema, chiamato anche "Problema dei generali bizantini" (come portare a termine un'operazione in tutta sicurezza, operando su una rete non sicura), e garantire comunque la sicurezza delle transazioni, Bitcoin sfrutta la crittografia, ossia un sistema di trasferimenti di bitcoin mediante messaggi criptati. Ogni utente della rete ha quindi due indirizzi pubblici (chiavi pubbliche) e due indirizzi privati (chiavi private), costituiti da una serie di caratteri alfanumerici. Una transazione può coinvolgere due o più parti e ad ogni *input* corrisponde un *output* della transazione precedente.

Le transazioni sono convalidate se gli *output* delle transazioni precedenti corrispondono con gli *input* della nuova transazione. Per tale motivo si parla di "catena di blocchi". Si è detto che il sistema Bitcoin è basato sulla tecnologia *peer-to-peer*: affinché una transazione sia inserita di diritto nella blockchain, è necessario dimostrare che il mittente non abbia alterato o sostituito ciò che sta scambiando tramite l'approvazione del 50 per cento più 1 dei nodi, oltre che verificare che colui che invia bitcoin sia effettivamente chi dichiari di essere e che la comunicazione dell'avvenuto pagamento sia attendibile. In altre parole, chi riceve il pagamento deve avere una prova che, al momento di ciascuna transazione, la maggioranza dei nodi concordi sull'evoluzione temporale della somma di denaro, in modo che non sia affetta da *double spending* e sia effettivamente inviata "per la prima volta"[30].

Per far ciò, il mittente deve dar prova di essere in possesso delle chiavi private: infatti, Bitcoin associa una chiave privata ad ogni indirizzo pubblico presente all'interno del suo *wallet*; utilizzando la chiave privata questi può sottoscrivere la transazione, apponendo una sorta di "firma digitale". Il destinatario della transazione potrà ricevere ed usufruire dei bitcoin solo successivamente alla validazione della rete, grazie al "prezioso" supporto dei cosiddetti "*miner*", dei quali si parlerà in seguito; una volta validata dalla rete, la transazione è definitivamente incorporata alla blockchain. In altri termini, Bitcoin utilizza la crittografia a chiave pubblica, cioè un algoritmo crittografico asimmetrico che utilizza due chiavi generate matematicamente: la chiave privata, impiegata per "crittografare" o firmare digitalmente il "denaro digitale", e la chiave pubblica, che viene usata per "de-crittografare" il messaggio o per verificarne la firma. Il legame matematico presente fra le due chiavi fa sì che la chiave pubblica funzioni sono se esiste la corrispondente chiave privata[31]. Per generare la coppia di chiavi, pubblica e privata, Bitcoin sfrutta degli algoritmi a curva ellittica, gli *Elliptic Curve Digital Signature Algorithms* (ECDSA); tramite questi algoritmi, è sempre possibile "creare" una chiave pubblica legata alla relativa chiave privata, mentre è impossibile fare l'operazione inversa. In sintesi, si genera una chiave privata ed 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 da un numero casuale. Viene, infine, generato l'indirizzo Bitcoin trasformando la chiave pubblica tramite funzioni *hash* crittografiche, aggiungendo il *checksum* (ossia un codice

[30] Cfr. Nakamoto S. (2008), "*Bitcoin: un sistema di contanti elettronico peer-to-peer*", www.bitcoin.org.

[31] Cfr. R. Caetano (2016), "*Bitcoin. Guida all'uso delle criptovalute*", Apogeo, Milano.

impiegato per garantire che l'indirizzo contenga una serie di caratteri validi) e codificando il tutto con una funzione BASE58, che ha lo scopo di codificare grossi valori numerici in una stringa alfanumerica di caratteri.[32] Il risultato è quindi un indirizzo visibile pubblicamente, usato per ricevere bitcoin, ed una chiave privata che viene impiegata invece per spenderli. Al fine di poter trasmettere una certa quantità di bitcoin ad un altro soggetto, il mittente deve conoscere l'indirizzo Bitcoin del ricevente ed applicare alla transazione una funzione di *hash* crittografico. In altre parole, per rispettare la continuità dei blocchi colui che vuole trasferire bitcoin, precedentemente ricevuti da un terzo soggetto, firma digitalmente un *hash* della transazione precedente e un *hash* della chiave pubblica del destinatario ed aggiunge tali informazioni alla transazione che sta predisponendo.

1.4.4 Mining

Il "*data mining",* o semplicemente *mining*, è un processo strettamente legato alla modalità di creazione di bitcoin tramite la validazione delle transazioni. Il *mining* è fondamentalmente l'atto di creare bitcoin, di trovare questo "minerale algoritmico" e coniarlo in *token* utilizzabili. Il processo di *mining* è pertanto remunerativo per coloro che lo intraprendono, eseguendo il *software* di Bitcoin *mining* sui propri computer. In poche parole, il *mining* trasforma elettricità in bitcoin: i computer cercano numeri che non sono ancora stati scoperti e, appena li trovano, possono essere trasmessi come monete nel network. I *miner* generano ricchezza, poi la mettono in circolazione a loro discrezione[33].

Ma si parta con ordine. Come già anticipato, la tenuta dei conti è tenuta di concerto dalla rete e funziona per mezzo della blockchain. Le nuove transazioni in bitcoin sono poste inizialmente sotto lo stato di "non confermato", in attesa della validazione della rete; una volta verificate, vengono raggruppate nei "blocchi" (un blocco contiene di norma dalle 200 alle 300 operazioni, per un peso massimo di 1 MegaByte). È in questa fase che entrano in gioco i *miner*, gli "estrattori", ovvero quei nodi della rete che tentano di risolvere i blocchi. L'attività del *mining* consiste dunque in un procedimento che impiega un nuovo blocco di transazioni come base di calcolo di un problema matematico dalla risoluzione complessa. Solitamente, per trovare la soluzione i *miner* si affidano al metodo *bruteforce*, che consiste nell'analizzare ogni soluzione teoricamente possibile fino a trovare quella corretta; tale sistema richiede un numero molto elevato di tentativi e, seppur sempre efficace, è un metodo risolutivo lento e dispendioso. Nel momento in cui il problema viene risolto, il *miner* invia alla rete una *proof of work*, una sorta di documento di prova, e riceve come ricompensa i nuovi bitcoin più le commissioni (le cosiddette "*transaction fee*") per ogni transazione. Contestualmente, ai blocchi risolti viene associato un

[32] Cfr. Passerelli, N. (2016), "*Bitcoin e antiriciclaggio*", Sistema di Informazione per la Sicurezza della Repubblica, www.sicurezzanazionale.gov.it.

[33] Cfr. Jaromil Roio Denis (2014), "*Bitcoin, la fine del tabù della moneta*", http://effimera.org/bitcoin-la-fine-del-tabu-della-moneta-di-denis-jaromil-roio/.

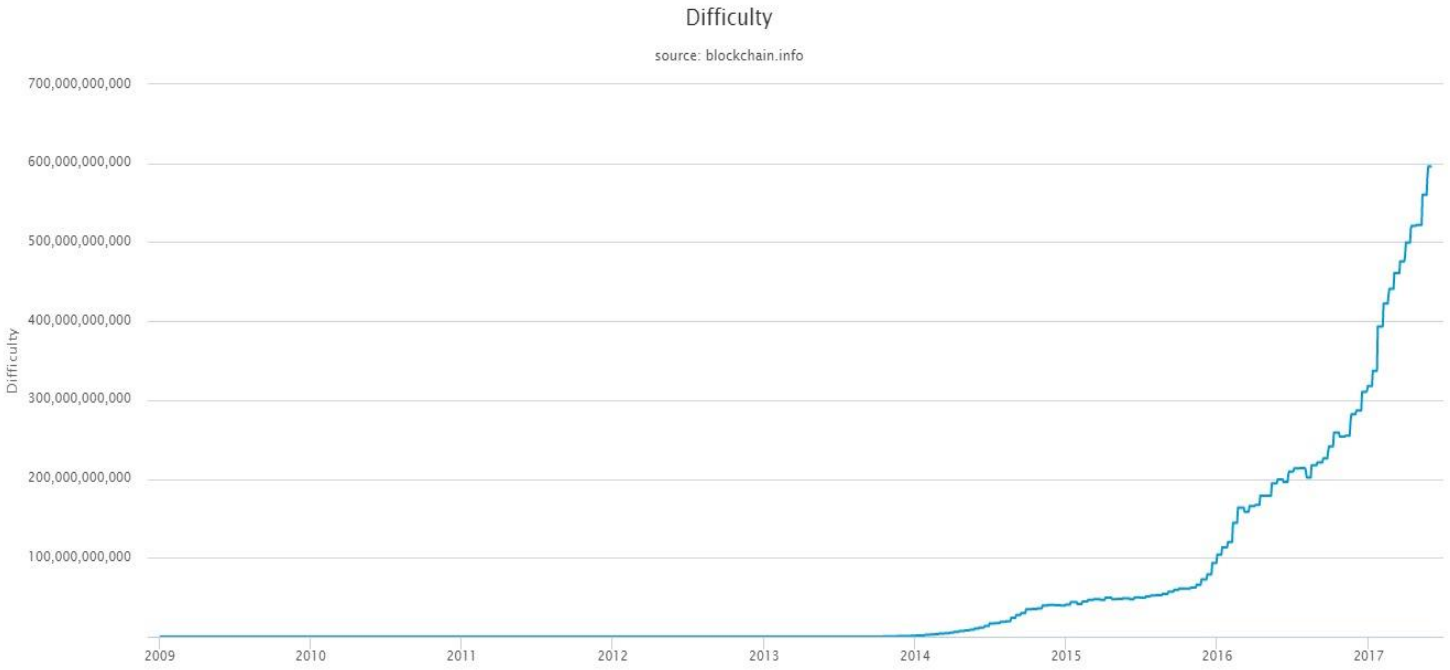
timestamp (marca temporale, fondamentale per avere traccia della cronologia delle transazioni ed evitare il problema della *double spending*) e concatenati definitivamente alla blockchain. L'intero meccanismo di verifica e di convalida dell'operazione avviene in circa dieci minuti. La possibilità che un utente possa ricevere la ricompensa in bitcoin dipende esclusivamente dalla potenza computazionale che egli aggiunge alla rete, in relazione alla potenza computazionale complessiva della rete; in particolare, è il *miner* che ha risolto il blocco per primo ad essere ricompensato.

Entrando nel dettaglio, il problema matematico per i *miner* consiste nel risolvere un'operazione di *hashing* inverso a 256 bit. Nel linguaggio matematico e informatico, l'*hash* è una funzione non iniettiva (e quindi non invertibile) che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita, in questo caso di 256 bit. Il *miner* deve dunque trovare un certo numero per cui l'*hash* di un insieme di dati rappresentante il blocco sia inferiore ad una certa soglia. Questa soglia è chiamata difficoltà di risoluzione dell'*hash*, difficoltà che il sistema rende sempre più elevata aumentando il numero di calcoli necessario per la risoluzione di un nuovo blocco. L'aggiornamento di questo parametro è finalizzato a spronare i *miner* a migliorare costantemente la propria attrezzatura e le proprie tecniche, al fine di poter mantenere una certa soglia di profitto. È dunque un continuo spronare gli attori del mercato all'efficienza. Tale aggiornamento avviene ogni 14 giorni circa, tale da mantenere mediamente il tempo di risoluzione a 10 minuti. La Figura 6 mostra una misura relativa della difficoltà nella risoluzione di un nuovo blocco, la quale è funzione della potenza computazionale (*hashing power*[34]) offerta da tutti i *miner* alla rete.

Figura 6 – Difficoltà di estrazione[35]

[34] *L'hashrate* misura la potenza computazionale ed è definita come il numero di *hash* che un computer, o una rete di computer, può calcolare in un secondo. Esprime, in altre parole, la potenza di calcolo che un nodo mette al servizio dell'attività di validazione delle transazioni ed esprime indirettamente anche la probabilità di riuscire a produrre blocchi validi.

[35] Cfr. www.blockchain.info (1/06/17)



Inizialmente, l'estrazione di bitcoin era effettuata tramite computer ordinari, in un primo momento per mezzo dei comuni processori (CPU) per poi passare all'utilizzo di schede grafiche dedicate (GPU). Queste tecnologie sono divenute ad oggi obsolete per poter sostenere le via via sempre crescenti difficoltà dei calcoli per la risoluzione dei blocchi, Il mercato del *mining* si è evoluto nel senso di giungere alla creazione di computer specializzati, dapprima sfruttando le potenzialità delle *Field Programmable Gate Arrays* (FPGAs) per finire con l'utilizzo di *hardware* dedicati basati sui processori *Application Specific Integrated Circuits* (ASICs): la potenza di calcolo, nel passaggio da ogni tecnologia all'altra, è cresciuta di volta in volta di dieci volte in termini di efficienza[36].

D'altra parte, i costi maggiori che un *miner* deve sostenere, oltre all'acquisto dell'attrezzatura specializzata, sono quelli legati all'energia elettrica, destina sia al diretto funzionamento dei computer, sia agli strumenti dedicati al raffreddamento di questi (poiché, a causa dell'alta attività, sono facilmente esposti a surriscaldamenti). Va da sé che i *miner* scelgano sia di raggrupparsi nelle cosiddette *mining pool*, consorzi industriali nei quali tutti i partecipanti mettono in comune le proprie risorse per poi spartirsi le ricompense, sia di allocarsi in regioni ove il costo dell'elettricità e della manodopera è maggiormente competitivo ed il clima più rigido. Non c'è dunque da meravigliarsi se la gran parte degli impianti industriali dediti al *mining* sia allocata in Cina o in Europa dell'est. Per poter eventualmente competere con gli attori già presenti sul mercato, un potenziale nuovo *miner* dovrebbe inizialmente sostenere un investimento in macchinari altamente specializzati e

[36] Cfr. Bouri et al (2017), "*Bitcoin for energy commodities before and after the December 2013 crash: diversifier, hedge or safe haven*?", Applied Economics, DOI: 10.1080/00036846.2017.1299102.

competitivi; il costo per tali attrezzature sta diventando nel tempo sempre più ingente e questo, al pari della riduzione delle ricompense in bitcoin, sta rendendo questo mercato sempre meno profittevole e, forse, meno concorrenziale[37].

Nella prima fase di creazione di base monetaria, la ricompensa per la risoluzione di un blocco consisteva nell'emissione di 50 nuovi *token*. In seguito, vista la prestabilita natura decrescente dell'offerta di moneta, nel 2012 la ricompensa è stata abbassata a 25 bitcoin e si prevede che verrà dimezzata ogni 210 mila blocchi registrati, finché non sarà raggiunta la quota di 21 milioni di bitcoin in circolazione. A quel punto, sembra che i *miner* verranno remunerati solamente con le commissioni delle transazioni. Questa prospettiva apre interessanti scenari e nuove discussioni: cosa succederà quando il profitto dei *miner* sarà composto dalle sole commissioni? I costi per poter sostenere la potenza computazionale rimarranno teoricamente inalterati, per cui per preservare un certo margine di profitto l'ipotesi più in voga rimane un aumento delle suddette commissioni. Tuttavia, è noto che Bitcoin punti molto sull'economicità dei trasferimenti di moneta ed è lecito domandarsi se questa soluzione possa essere realmente desiderabile per la salute di tutta la *community*.

1.5 Cenni generali sulle altre criptovalute

Il successo del progetto di Satoshi, unito all'allettante prospettiva di guadagno ed una buona dose di creatività, ha aperto ad una massiccia proliferazione di nuove criptovalute, anche chiamate "*alt-coin*" (*alterative coins*), realizzate per i più svariati fini e operative in sempre più eterogenei settori. Basti pensare che, il 1° aprile 2017, il sito coinmarketcap.com annoverava circa 780 diverse monete virtuali ed il loro numero è tutt'oggi in continuo aumento, sebbene alcune di queste siano rimaste sul mercato per un periodo piuttosto breve.

La struttura di queste nuove valute non è molto diversa dallo *standard* realizzato da Bitcoin, infatti nella maggior parte dei casi i programmatori-ideatori hanno preferito implementare piccole differenziazioni rispetto a drastiche modifiche: si possono facilmente riconoscere valute che introducono migliorie tecniche nel protocollo (come, ad esempio, Litecoin), altre che puntano sul rafforzamento dell'anonimato (Monero, Darkcoin) o che si differenziano per la quantità o il taglio disponibile in modo da favorire micro-transazioni (Dogecoin), o ancora valute di recentissima ideazione emesse per favorire l'adozione di comportamenti socialmente od eticamente auspicabili (Zipcoin). Di portata più rilevante sono le innovazioni introdotte da Nautiluscoin e Friecoin: la prima, attraverso la creazione di un apposito fondo di stabilizzazione, tenta di sopperire al problema dell'alta volatilità che normalmente caratterizza tutte le valute virtuali; la seconda invece istituisce una "tassa di stazionamento", ossia un prelievo forzoso del 5 per cento su tutti i depositi dormienti, in modo da favorire un

[37] Si configura, in altre parole, di un caso di barriera economica all'entrata, ossia un aumento dei costi e dei rischi commerciali a carico delle nuove imprese entranti, mentre le imprese già operanti nel mercato beneficiano di elevate economie di scala.

più frequente utilizzo e una maggior circolazione della moneta.

Una nota a parte meriterebbero Ethereum e Ripple, che risultano ad oggi due dei progetti più ambiziosi ed innovativi nell'ambito delle criptovalute dell'ultimo biennio e che stanno attualmente catturando sempre maggiore interesse da parte di numerosi *stakeholder*. Sostanzialmente, come Bitcoin, Ethereum è una piattaforma decentralizzata per transazioni *peer-to-peer,* che tuttavia si concentra principalmente sugli *smart contract;* il bacino di contratti (e potenzialmente di utenti) sottostanti Ethereum è dunque più ampio rispetto a Bitcoin (comprende, ad esempio, anche i contratti di assicurazione o di proprietà intellettuale) ed il sistema funziona attraverso un'apposita unità di conto, gli Ether, che il sistema utilizza per remunerare la realizzazione a tempo dei suddetti contratti. Con una capitalizzazione di mercato pari a quasi 14 miliardi di dollari[38], Ripple è ad oggi la seconda piattaforma più diffusa al mondo e principale "rivale" di Bitcoin. Tuttavia, più che una moneta virtuale, Ripple è un protocollo internet, con cui si possono effettuare e ricevere pagamenti, sulla falsariga di Paypal. A Ripple si può associare un conto corrente di moneta reale, ed è in particolare costituito da un *network,* da una borsa e da una valuta virtuale, anch'essa basata su un codice di crittografia e, come Bitcoin, punta a bypassare l'intermediazione bancaria attraverso un sistema decentralizzato *peer-to-peer*. La differenza principale risiede nel fatto che Ripple offre la possibilità di scambiare diverse valute, garantendo inoltre più elevati meccanismi di sicurezza grazie alla creazione di registri delle transazioni chiamati "Ledger".

La contemporanea presenza sul mercato di questo elevato numero di nuove monete conduce ad una situazione di concorrenza, non solo tra criptovalute e *fiat currencies*, ma anche tra criptovalute stesse. In questo scenario, Bitcoin gode del "vantaggio della prima mossa": se un attore è interessato ad adottare una criptovaluta al posto delle valute tradizionali, il bitcoin è la scelta più ovvia. È la più conosciuta, ha una rete di utenti più estesa ed ha costi di conversione con le valute tradizionali relativamente bassi. D'altra parte, le *alt-coins* possono dar vita a modifiche e migliorie sulla base degli insuccessi di Bitcoin, sfruttando i vantaggi derivanti dal giocare la "seconda mossa"[39]. La sfida affrontata dalle altre criptovalute si sintetizza essenzialmente nel proporre novità capaci di sopperire alla (momentanea?) minor diffusione nel mercato. Le innovative applicazioni proposte da Ripple ed Ethereum, ad esempio, sembrano accogliere un sempre più vivo interesse del mercato, come testimoniato dall'impennata dei valori registrata nella prima metà del 2017.

Se ci si focalizzasse sulla sola capacità di fungere da moneta, è doveroso notare che nella maggior parte dei casi le *alt-coin* soffrono gli stessi limiti di Bitcoin, che si avranno modo di approfondire nel capitolo successivo. Limiti che sollevano comprensibili dubbi sull'effettiva capacità di queste di fungere da moneta alternativa. Inoltre, gli stessi utenti generalmente considerano le nuove *alt-coin* alla stregua di forme di investimento

[38] Cfr. https://www.coingecko.com (18/05/2017).

[39] Cfr. Luther W. L. (2016), "*Bitcoin and the Future of Digital payments*", The Indipendent Review, v.20, n.3, ISSN 1086-1653, pp.397-404.

speculativo piuttosto che come tipico mezzo di scambio. Il motivo è tutto da ricercare nella forte variabilità del loro valore, poiché, equiparate ad attività finanziarie e non a valute vere e proprie, sono dominate dalle dinamiche tipiche dei mercati finanziari, tutt'altro che stabilizzatrici. La mancanza di strumenti di stabilizzazione del potere di acquisto legati alla gestione dell'offerta di moneta contribuisce ad aumentare l'ampiezza delle variazioni dei prezzi (si ricordi che, le valute digitali basate sulla tecnologia blockchain hanno per la stragrande maggioranza un'emissione di moneta esogena e predeterminata). Da queste considerazioni si può supporre che, sebbene la prospettiva di un "sorpasso" da parte di una o più *alt-coin* sia interessante e poggi le basi su solide motivazioni, la sensazione generale tende ad essere di forte scetticismo circa questa possibilità.

Tuttavia, quali sono le implicazioni della concorrenza? La questione ha indotto la dottrina ad interrogarsi sui possibili effetti che la libera concorrenza possa avere sulla qualità del bitcoin e sulla sua funzione monetaria, senza però convergere verso una visione comune; in particolare, ci si chiede se la competizione fra una molteplicità di monete digitali possa comportare un problema o se si incaricherà di far emergere quelle maggiormente capaci di assicurare ai loro utenti un potere di acquisto ragionevolmente costante[40]. In accordo con la corrente keynesiana, la presenza di una pluralità di monete deve essere necessariamente vista come un problema da risolvere ed una situazione da contrastare, in quanto si pone quale ostacolo verso il raggiungimento dell'obiettivo di unificazione monetaria. Di opinione diametralmente opposta è quella parte di dottrina di area liberista che, ispirata alle idee di von Hayek, è favorevole al *free banking*, reputando tale pluralità come un'opportunità ed una ricchezza da promuovere in vista di un miglioramento della competitività non solo del sistema monetario, ma di tutta l'economia globale.

[40] Cfr. Amato M. e Fantacci L., (2016), "*Per un pungo di Bitcoin*", Egea, Università Bocconi Editore, Milano.

Capitolo 2 – Funzione Monetaria

Come si è esaminato nel capitolo precedente, Bitcoin propone una rivoluzione economica tanto radicale quanto ambiziosa. Per scardinare il sistema centrale, Bitcoin si fa forte di un'innovativa tecnologia e di un *token* digitale creato appositamente per il funzionamento del sistema. Fatte salve le potenzialità indubbie della blockchain e della portata delle nuove possibilità associate, l'analisi si deve spostare su binari prettamente economici e comprendere se il bitcoin-unità di conto sia il veicolo adatto per perseguire gli obiettivi prefissati; si deve, in altre parole, capire se il bitcoin abbia la capacità di essere equiparata ad una vera e propria moneta.

Può dunque il bitcoin essere considerato una moneta? Se da una parte le intenzioni dei suoi inventori nell'utilizzare i bitcoin come mezzo di pagamento spingono verso questa conclusione, la dottrina non ha ancora raggiunto un'opinione omogenea. Tale divergenza di vedute sul piano teorico si reitera anche sul piano giuridico, laddove si è ben lontani dal raggiungimento di una comune intesa a livello internazionale su quale sia lo *status* giuridico da attribuire a Bitcoin. Ogni paese inquadra Bitcoin nel proprio ordinamento in modo differente e norme e regolamenti in materia sono in continua evoluzione[41].

Bisogna tuttavia fare una premessa. In economia, con il termine moneta si intende l'insieme di valori utilizzati dagli individui per acquistare beni e servizi[42]; solitamente, si distinguono due tipologie di moneta: moneta merce e moneta a corso legale. Nella prima, si tratta di beni, come l'oro, che hanno un proprio valore intrinseco; le monete a corso legale invece hanno un riconoscimento di valore da parte del legislatore, che ne regola la stabilità e ne assicura l'accettazione come mezzo di pagamento. Sotto questo punto di vista, le valute virtuali sono chiaramente diverse sia dalla moneta merce, sia dalle cosiddette *fiat currency*. Tuttavia, la mancanza di un riconoscimento legislativo o di un valore di utilizzo tangibile non implica necessariamente che bitcoin non possa egualmente svolgere le tre tipiche funzioni di moneta (mezzo di scambio, riserva di valore ed unità di conto) e funzionare alla stregua di una moneta, in virtù di un valore, reale o fittizio che sia, assegnatogli dagli utenti della stessa *community*.

Nonostante queste premesse, la tesi portante del presente elaborato è che il bitcoin non svolga la funzione monetaria in modo sufficientemente completo ed efficiente. Al fine di illuminare il lettore sui motivi che spingono verso questa conclusione, si illustrerà di seguito un'analisi comparativa del bitcoin con le valute tradizionali. L'impostazione scelta consente di valutare singolarmente ognuna delle tre sopracitate funzioni della

[41] Cfr. Lemme G. e Peluso S. (2016), "*Criptomoneta e distacco dalla moneta legale: il caso bitcoin*", in Riv. dir. banc., dirittobancario.it, 43

[42] Cfr. Capoti D., Colacchi E. e Maggioni M. (2015), "*Bitcoin Revolution: La moneta digitale alla conquista del mondo*", Ulrico Hoepli Editore S.p.A., Milano.

moneta, provando ad esplicitare i punti di contatto e le differenze tra le due tipologie di valute, estraendo infine dal confronto i punti di forza e le relative debolezze della criptomoneta.

2.1 Bitcoin come mezzo di scambio

Una moneta ha il compito di fungere da intermediario negli scambi, ossia da strumento intermedio che permetta di regolare i pagamenti nella compravendita di beni e servizi e nelle altre transazioni commerciali. Essere mezzo di scambio significa svolgere la funzione tramite la quale è possibile scambiare beni e servizi in qualsiasi quantità e tempo: ogni bene viene misurato e riceve una valutazione (un prezzo) in base alle unità di moneta necessarie per acquisirne la proprietà.
Con riguardo a questa funzione, Bitcoin differisce sostanzialmente dalle valute tradizionali sotto diversi aspetti, che ci si preme analizzare punto per punto: costi e tempi delle transazioni, anonimità e trasparenza, mancanza di riconoscimento legale, barriera all'entrata, esternalità di rete, risoluzione delle dispute contrattuali e credito e riserva frazionaria.

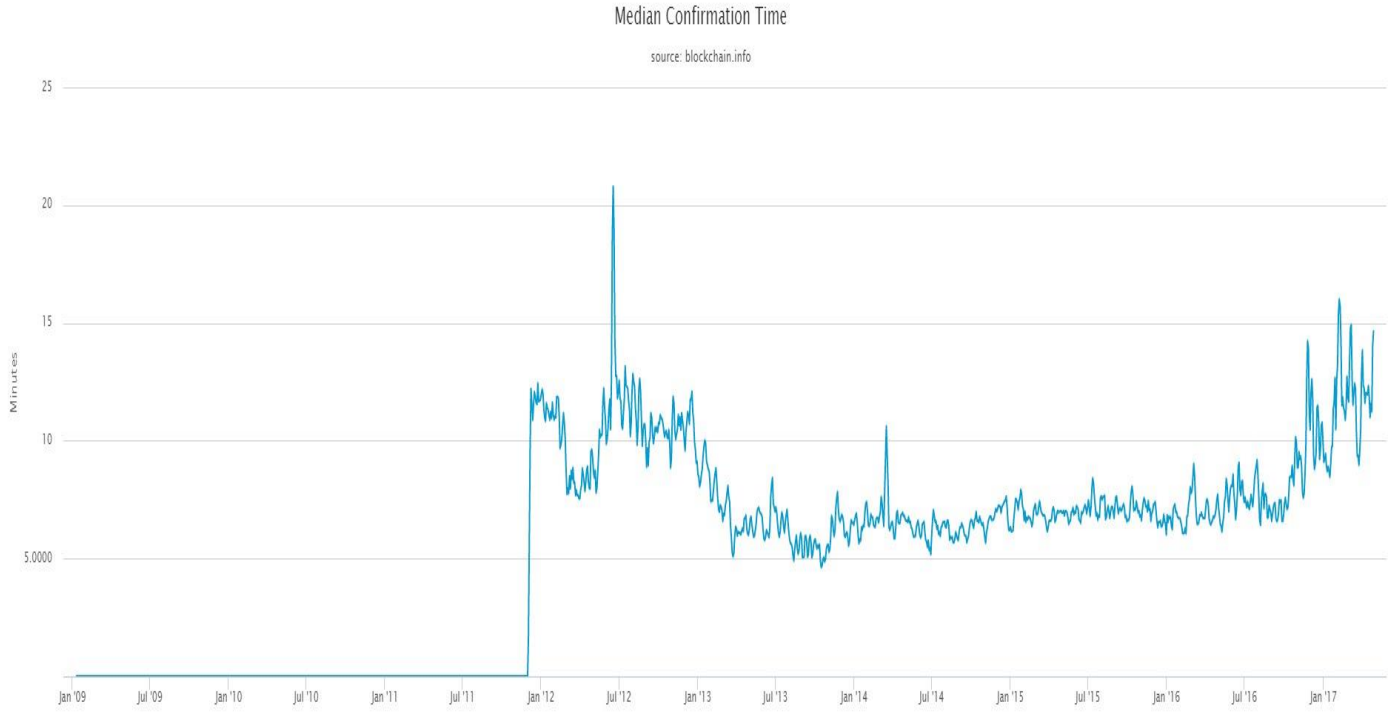
2.1.1 Costi e tempi delle transazioni

Come osservato in precedenza, i bassi costi medi delle transazioni (Figura 7), uniti ai rapidi tempi di conferma e validazione di un'operazione (Figura 8), costituiscono, secondo una parte della dottrina, uno dei vantaggi comparati di maggior spessore del bitcoin. La mancanza di un organismo di intermediazione diretta consente un alleggerimento generale dei costi del sistema, ove le *transaction fee* sono finalizzate alla sola remunerazione dei *miner*. Secondo quanto previsto dal Protocollo Bitcoin, non vi è un'impostazione predeterminata ed obbligatoria dell'ingenza di tali commissioni: la componente di costo delle *fee* è di natura facoltativa, rimessa alla discrezionalità delle parti, ed è volta a stimolare i *miner* ad una più veloce validazione della transazione (in questo modo, in base alla rilevanza dell'importo, le parti acquistano una sorta di "corsia preferenziale"). Si può assumere che le commissioni seguano piuttosto una logica di mercato: il loro prezzo cresce in base alla domanda di maggior rapidità di validazione richiesta dai suoi utenti.

Figura 7: Costo medio percentuale di una transazione[43]

[43] Cfr. https://www.blockchain.com (30/04/2017)

Figura 8 – Tempi medi di conferma di un'operazione [44]



È tuttavia necessario fare un paio di precisazioni, in quanto questo sistema non è esente da difetti. Le

[44] Cfr. https://www.blockchain.com (30/04/2017)

commissioni difatti si pagano in proporzione sia al peso in *bytes* della transazione (che mediamente pesa poco più di 200 *bytes*), sia al numero di indirizzi in cui è suddiviso l'importo da pagare, a prescindere dal fatto che spostino un valore di miliardi di euro o pochi centesimi. Per questo motivo, allo stato attuale non è assolutamente conveniente fare transazioni di basso importo: ad esempio un gelato pagato in bitcoin potrebbe arrivare a costare anche il doppio. Inoltre, se da una parte è vero che per i trasferimenti internazionali il sistema propone tempi di transazione contenuti, è altresì vero che i bitcoin non sono del tutto performanti nei sistemi commerciali tradizionali. Si è detto che i tempi medi per una validazione si aggirano mediamente attorno ai 10 minuti. Questo non sembra essere un problema per l'*e-commerce*; tuttavia, è facile intuire il limite tecnico per gli acquisti nei canali di commercio tradizionali, come i negozi fisici: nessuno aspetterebbe in cassa i 10 minuti necessari per la validazione della transazione, specialmente se di piccolo importo. Ovviare a tale problema, d'altronde, renderebbe necessaria una *fee* più elevata e, di conseguenza, una minor convenienza dell'operazione.
Entrambi i problemi descritti possono disincentivare il consumatore medio nel preferire bitcoin alle valute tradizionali. Nel prossimo futuro, un ulteriore problema potrebbe essere rappresentato da un aumento delle *fee*, dovuto alla concomitanza della sempre costante crescita delle difficoltà nella risoluzione dei blocchi e della frenata nell'emissione di bitcoin come ricompense ai *miner*. Nello scenario più probabile, i *miner* scaricheranno tali "costi" maggiori in capo al consumatore finale tramite il suddetto aumento delle commissioni. Sopperire all'aumento delle commissioni è una questione su cui si continua a dibattere. Ad oggi, una proposta riguarderebbe l'accorpamento di più transazioni nei blocchi: una soluzione che porterebbe sì ad un aumento della difficoltà nella risoluzione degli stessi, ma anche ad un parallelo aumento delle capacità del sistema di processare le diverse operazioni ed addirittura ad un abbassamento delle *fee* richieste. D'altra parte, le maggiori difficoltà possono a loro volta evolversi in una riduzione della velocità di validazione, con relativa riduzione di uno dei vantaggi competitivi più sponsorizzati.
In conclusione, non si può dare un giudizio assoluto circa gli effetti dei costi di transazione sull'affermazione futura del bitcoin come moneta alternativa. Allo stato attuale, la convenienza e la rapidità di validazione della transazione non sembrano portare ad un reale vantaggio comparato del bitcoin sulle *fiat currency*, almeno per ciò che concerne le operazioni commerciali di tutti i giorni. Al più, si può ipotizzare un'affermazione in particolari segmenti del mercato, quali ad esempio i già citati trasferimenti di moneta transfrontalieri.

2.1.2 Anonimità e trasparenza

Come si è visto, l'anonimità (o meglio pseudo-anonimità) consente una maggiore protezione della *privacy* in capo agli utilizzatori di bitcoin, sebbene la tracciabilità non venga del tutto esclusa. Attraverso la blockchain, Bitcoin implementa un sistema pubblico di documentazione e di consultazione di ogni transazione, che rende di fatto possibile risalire agli utenti "fisici", seppur con maggiori difficoltà. Tuttavia, a prescindere dalle reali

intenzioni dei suoi creatori, è indubbio che il sistema abbia attirato sempre più attenzioni da quella parte di utenti dediti ad attività illegali o criminali (come riciclaggio di denaro o narcotraffico), il cui esempio più fulgido è quello della Silk Road. Inoltre, proprio per la riservatezza che è in grado di offrire agli utenti, l'utilizzo di bitcoin sta spopolando anche nel settore del gioco d'azzardo *online*, con un continuo aumento delle piattaforme di poker, bingo, scommesse e lotterie che lo scelgono quale strumento di pagamento privilegiato.

Recenti approfondimenti hanno osservato che l'anonimità di Bitcoin può essere rafforzata, nascondendo più efficacemente le tracce di collegamento tra utenti e bitcoin trasferiti: per ogni nuovo invio o ricezione di pagamento, gli utenti possono ovviare alla tracciabilità ricorrendo ad una particolare strategia, ossia utilizzare via via a nuovi indirizzi per ogni trasferimento. In alternativa, questi possono avvalersi di appositi strumenti informatici, come i servizi di Bitcoin *mixer*. Si parla di meccanismi informatici che consentono di oscurare l'origine di una transazione in Bitcoin (c.d. *anonymiser – anonymisig tool*), di collegare una transazione ad un indirizzo diverso da quello del soggetto che la ha eseguita (c.d. *laundry service mixer*, o *tumbler*) ovvero di celare l'indirizzo IP dell'utente collegato alla rete (c.d. TOR)[45].

Come verrà adeguatamente approfondito nel terzo capitolo della trattazione, la questione degli usi illeciti assume assoluta rilevanza se ci si concentra sui possibili effetti di questi sul prossimo futuro della criptovaluta. A riguardo, le risposte regolamentari degli stati nazionali e delle autorità sovranazionali potrebbero impedire, ostacolare e limitare l'utilizzo di criptovalute. Senza contare che una cattiva reputazione può comportare una maggiore difficoltà nel "convincere" nuovi utenti ed esercizi commerciali ad adottare bitcoin. Vi è poi da considerare che, per evitare di utilizzare bitcoin provenienti da indirizzi "prescritti", in quanto implicati in transazioni illegali, gli utenti potrebbero essere portati a distinguere tra bitcoin "buoni" e bitcoin "cattivi". A lungo andare, siffatta possibilità di scelta all'interno del sistema Bitcoin potrebbe condurre ad adottare una pericolosa logica selettiva, in grado di rallentare se non addirittura arrestare gli scambi[46]. Per tali ragioni, anonimato e trasparenza costituiscono tratti peculiari che possono essere visti come elementi ambivalenti sia a favore che a sfavore dell'uso di Bitcoin rispetto alle valute stan*d*ard.

2.1.3 Mancanza di corso legale

Dal punto di vista giuridico, il termine moneta negli stati moderni identifica esclusivamente la moneta legale a corso forzoso, espressione della sovranità statale o sovrastatale, vale a dire le banconote e le monete denominate

[45] Cfr. La Rocca L. (2015), "*La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*", Analisi giuridica dell'Economia, Il Mulino, pp. 201-220.

[46] Cfr. Gasparri G. (2015), "*Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*", Diritto dell'informazione e dell'informatica, 31(3), 415-442.

nella valuta adottata in ciascun ordinamento, la cui emissione è per solito riservata alle banche centrali[47]. La mancanza di questo specifico riconoscimento legale del bitcoin-unità di conto non può che tradursi in tutta una serie di limiti. Ciò è evidente riguardo alla sua accettazione come mezzo di scambio: in mancanza di un dato obbligo imposto dalla legge, questa è deposta alla libera discrezionalità delle parti coinvolte. In altre parole, il suo uso come moneta non è di per sé proibito, ma è rimesso all'adozione volontaria degli attori, pubblici o privati che siano, che non sono legalmente vincolati ad accettarla. In tal senso, potrebbe essere utile conoscere preventivamente le attività commerciali che nel mondo reale accettano pagamenti in valuta virtuale; questo servizio è stato reso possibile da piattaforme di supporto *online* che offrono la consultazione di mappe, come BitcoinMaps, Bitcoin.travel e CoinMap.org.

A render la situazione ancor più problematica è, infine, la difficoltà generale nell'entrare in possesso di bitcoin: attualmente è infatti possibile ottenere bitcoin solo scambiandoli con una *fiat currency* su una piattaforma dedicata (come ad esempio Exchange), per mezzo di una transazione per la vendita di beni o servizi, od infine attraverso una partecipazione attiva al processo di *data mining.*

La concorrenza tra valute digitali e valute a corso legale può essere profondamente influenzata dallo squilibrio di potere tra *community* bitcoin e autorità monetarie, indirizzandosi verso binari sempre più favorevoli alla supremazia delle valute *standard*. La sponsorizzazione delle monete *standard,* operata dalle autorità governative, contribuisce ad ostacolare l'affermazione della criptomoneta, relegandola al più al ruolo di moneta complementare ed impedendole di giungere a quella ricercata esclusività che al momento è conseguibile solo dalle maggiori valute legali. In altre parole, un individuo non può gestire la propria vita economica facendo leva esclusivamente sulle valute virtuali, mentre è naturalmente possibile farlo con le sole valute legali. L'uso di bitcoin è ad esempio escluso dal pagamento di tutta una serie di attività e servizi di stampo "statale", indispensabili sia per le imprese che per gli individui, quali il pagamento delle tasse o delle utenze. In sintesi, si può sostenere che le valute tradizionali, o meglio le autorità monetarie e statali che le governano, detengono le "regole del gioco" e possono gestire questa concorrenza da una posizione di forza assoluta, configurando una sorta di barriera strategico-istituzionale all'entrata. E difatti, alcune hanno già preso provvedimenti per bannare o regolare bitcoin, o semplicemente hanno adottato misure atte alla dissuasione del suo utilizzo[48].

V'è infine da considerare che i bitcoin non sono soggetti a confisca da parte delle autorità monetarie: a differenza di quanto accaduto a Cipro nel marzo 2013, dove la Banca centrale ha voluto e potuto prelevare fondi dai depositi non assicurati più grandi di 100 mila euro per ricapitalizzare sé stessa, con Bitcoin questa possibilità è esclusa in quanto si tratta per l'appunto di una moneta decentrata. Nessuna autorità centrale ne ha il controllo

[47] Cfr. Mancini M. (2015), "*Valute virtuali e Bitcoin*", Analisi giuridica dell'economia, Il Mulino, pp. 117-138.

[48] Cfr. Luther W. L. (2016), "*Bitcoin and the Future of Digital payments*", The Indipendent Review, v.20, n.3, ISSN 1086-1653, pp.397-404.

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[49].

La difficoltà pratica di confiscare i bitcoin si ripercuote anche nei rapporti creditizi: la criptovaluta si presta particolarmente bene ad essere un "rifugio" per i debitori poiché non può tecnicamente essere oggetto di pignoramento. Ciò tuttavia non pone gli utenti al riparo da operazioni di confisca da parte delle autorità giudiziarie, poiché a seguito di illeciti ed attività fraudolente, è sempre possibile requisire i supporti "fisici" (PC, smartphone…) ove sono conservati i *wallet* e le relative chiavi di accesso e, di conseguenza, anche valuta virtuale. Questa possibilità si è invero verificata in diverse occasioni, come testimoniato dalla requisizione dei bitcoin di proprietà di Ross Ulbritch nel caso Silk Road.

In definitiva, si deve riconoscere che la mancanza di un riconoscimento legale come moneta può configurarsi come un grande ostacolo per la diffusione del bitcoin su larga scala.

2.1.4 Barriera all'entrata

L'adozione di una nuova tecnologia o l'ingresso in un nuovo mercato richiede sempre un certo costo iniziale da sostenere. Nel caso di Bitcoin, l'investimento è prevalentemente di tipo cognitivo: in particolare, a causa della difficoltà di tutto il sistema bitcoin e della tecnologia che esso sfrutta nei pagamenti, esso necessita di un certo grado di familiarizzazione da parte degli utilizzatori a conoscenze che non sono di facile accesso. A differenza del contante (di immediato accesso) e della moneta elettronica bancaria (da anni ampiamente diffusa e resa "a portata" del consumatore medio), per essere adeguatamente compreso e di riflesso utilizzato su larga scala Bitcoin necessita di un livello relativamente elevato di conoscenze informatiche, poiché riguarda sia l'uso di dispositivi elettronici, sia quello di *software*, piattaforme e applicativi specifici[50].

Una seconda "barriera all'entrata" riguarda i costi connessi al passaggio da una valuta già largamente adottata (e di riflesso conosciuta) ad un'altra, meno diffusa. In questo caso viene a palesarsi la necessità di espletare una serie di attività accessorie, funzionali al corretto utilizzo dei bitcoin, quali ad esempio l'aggiornamento dei prezzari od il procurarsi la strumentazione adatta a supportare pagamenti con la criptomoneta, tra l'altro senza dimenticare le evidenti difficoltà nelle modalità di considerazione dei bitcoin in ambito contabile.

Preso atto che al momento le conoscenze tecniche su Bitcoin siano piuttosto modeste, le fattispecie sopra evidenziate possono configurarsi come una barriera all'entrata da non sottostimare, almeno nel breve periodo. Tuttavia, su orizzonti temporali più lunghi, non si può escludere che l'apprendimento di nuove conoscenze

[49] Cfr. Passerelli, N. (2016), "*Bitcoin e antiriciclaggio*", Sistema di Informazione per la Sicurezza della Repubblica, www.sicurezzanazionale.gov.it.

[50] Cfr. Ciaian, P., Rajcaniova, M. & Kancs (2016), "*The digital agenda of virtual currencies: Can BitCoin become a global currency?*", Inf Syst E-Bus Manage 14: 883.

tecniche e il miglioramento delle *skill* informatiche degli utenti possano comportare dei benefici addizionali per la diffusione di Bitcoin.

2.1.5 Economie di Rete

Le economie di rete, altresì dette esternalità di rete, descrivono una situazione in cui l'utilità che un consumatore beneficia dal consumo di un bene è collegata al numero di altri individui che consumano o utilizzano lo stesso bene od un bene compatibile. Si pensi, ad esempio, al telefono: per ogni consumatore, l'utilità dell'apparecchio è proporzionale al numero di altre persone provviste di un telefono compatibile e con cui sia possibile interagire. Questo meccanismo può essere associato anche a Bitcoin: gli incentivi ad utilizzare bitcoin come mezzo di scambio sono condizionati prevalentemente dal numero di utenti esistenti, con riguardo sia al numero di rivenditori, sia allo stesso numero di altri consumatori di beni e servizi che sfruttano Bitcoin per le loro transazioni. È un circolo vizioso: i potenziali utenti saranno meno inclini a procurarsi e ad utilizzare bitcoin se sono pochi coloro che accettano bitcoin e, a loro volta, i venditori e fornitori saranno meno inclini ad entrare "nel sistema" se nella rete ci sono pochi utenti disposti ad utilizzare bitcoin come mezzo di pagamento; ciò anche in virtù dei già citati costi fissi (cognitivi e non) nell'entrare nell'ottica di Bitcoin.

Anche in questo caso, nel breve periodo il numero di utenti della rete può essere un ostacolo all'affermazione di Bitcoin come moneta globale, problema che di contro non coinvolge le valute a corso legale; cionondimeno, ad oggi i dati mostrano una costante crescita del numero di transazioni e di utilizzatori[51], cosa che, complici le implicazioni delle sopracitate esternalità, potrebbe tradursi in un effetto positivo *extra* per la diffusione della valuta.

Occorre precisare che il fenomeno delle economie di rete può avere effetti diversi a livello regionale. Si guardi all'esperienza italiana. Ad oggi, infatti, in parziale controtendenza con i numeri internazionali, in Italia l'affermazione dei bitcoin negli esercizi commerciali sembra non riuscire a "sfondare". I rivenditori che hanno implementato l'accettazione della valuta digitale non hanno trovato un generale positivo riscontro nei clienti. Molti ammettono di aver iniziato ad accettarli e di aver mollato poco dopo a causa dell'assenza di utilizzo da parte dei clienti. Pochi dichiarano di aver effettuato transazioni in Bitcoin, con valori che spaziano dall'irrisorio al migliaio di euro in 3-4 anni. Nessuno racconta di un'impennata nel giro di affari, anzi le esperienze brevi sono le più numerose[52]. A fronte di una diffusione globale, in Italia la mancanza di clienti ha portato non solo ad una mancata crescita di rivenditori *bitcoin-friendly*, ma addirittura ad una riduzione del numero stesso nel tempo.

---

[51] Al riguardo, si rimanda alla Figura 5 della presente trattazione.

[52] Cfr. Frollà A. (2017), "*Bitcoin all'anno zero, italiani ancora diffidenti: pochissimi li acce*ttano", Repubblica Affari & Finanza, Anno 32 n.17, pg.8, stampato.

2.1.6 Risoluzione delle dispute contrattuali

Rispetto alle valute tradizionali, nel sistema Bitcoin una volta che una transazione va in porto ed è inserita nella blockchain, questa diviene di conseguenza irrevocabile. Si parla, non a caso, di irreversibilità delle transazioni. Perciò, cosa succede in caso di contesa, ossia se una transazione è effettuata in modo errato, involontariamente o con intenzioni fraudolente, o se si verifica un caso di inadempimento? Il costo di non avere un intermediario in questo caso è evidente, nulla è stabilito nel caso di transazioni errate. Inoltre, gli operatori che agiscono nell'ecosistema Bitcoin sono, in genere, soggetti non regolamentati e non vigilati, che non devono rispettare alcun requisito patrimoniale né alcun obbligo finalizzato ad assicurare la "*business continuity"*[53].

Allo stato attuale, il *software* può aiutare ad evitare errori di battitura e destinatari sbagliati ma, complice anche la mancanza di una legislazione *ad hoc* in materia, non c'è un'autorità a cui potersi rivolgere in caso di qualunque controversia, che possa riguardare un inadempimento, una frode o molto più banalmente un errore umano. Onde per cui l'unica soluzione sembra essere una correzione volontaria da parte delle stesse parti coinvolte nello scambio. Una soluzione indubbiamente figlia della fiducia posta da Bitcoin nei propri utenti, ma che ovviamente non può che ritenersi incompleta ed inefficace.

L'irreversibilità delle transazioni è stata implementata dagli sviluppatori per garantire commissioni molto convenienti, mercati più ampi e costi amministrativi più bassi, mettendo tuttavia i rivenditori in una posizione di vantaggio nei confronti del consumatore finale (a differenza dei modelli legislativi tradizionali). Del resto, la mancanza di diritti e di meccanismi di tutela agli utilizzatori di bitcoin è uno dei motivi per cui le varie legislazioni, pur adottando approcci differenti nel considerare Bitcoin, convergono nel non considerare le criptovalute alla stregua di monete. Si può dunque concludere che, sebbene in futuro la rete possa implementare servizi aggiuntivi per una maggior protezione degli utenti, tutt'oggi tale mancanza può costituire un rischio per gli utenti della rete e può ridurre la popolarità del bitcoin, in particolar modo presso quell'insieme di utilizzatori per natura più avversi al rischio.

2.1.7 Credito e riserva frazionaria

La fissazione del numero di bitcoin in circolazione ad una quantità fissa e non modificabile rende di fatto impossibile la "creazione" di nuova moneta attraverso il meccanismo della riserva frazionaria.

Questo, a sua volta, fa di bitcoin una moneta che non può essere prestata; in un'economia fondata sul debito, quale quella attuale, l'impossibilità di un accesso al credito rischia di limitare gli investimenti e la crescita dell'economia stessa, onde per cui è lecito aspettarsi una restrizione alla diffusione. Ovviamente, non è impossibile prestarsi bitcoin. Ma il sistema orienta il prestito più verso fini "solidaristici" che economici, ed il

[53] Cfr Mancini M. (2015), "*Valute virtuali e Bitcoin*", Analisi giuridica dell'economia, Il Mulino, pp. 117-138.

sistema, come già analizzato, non offre alcuna garanzia contro debitori inaffidabili. Senza considerare che, entrando nell'ottica del prenditore di fondi, sarebbe poco conveniente indebitarsi in una valuta che è programmata ad apprezzarsi nel tempo.

Una possibile soluzione alla mancanza di un vero e proprio meccanismo di credito orientato all'investimento potrebbe essere la creazione di una nuova moneta fittizia, una sorta di bitcoin virtuale moltiplicabile e convertibile in bitcoin reale. Ma anche in tal caso, si giungerebbe ad un *empasse*: creare tale nuovo *token* virtuale ed evitare problemi di *double spending* necessiterebbe di un organismo centrale che gestisca ed autorizzi le transazioni, ossia sviluppare quello stesso sistema di intermediari centrali che Bitcoin si era prefisso di distruggere[54].

Sotto quest'aspetto si può dunque asserire che gli scenari futuri della valuta sono fortemente a rischio. La mancanza di un sistema di credito può rivelarsi una componente chiaramente negativa nella sopravvivenza della valuta virtuale all'interno del sistema economico per come lo si conosce oggi, che di fatto ha bisogno di investimenti reali per crescere e che spesso sono resi possibili solamente dall'indebitamento.

2.2 Bitcoin come unità di conto

Come qualsiasi altra *fiat currency*, per assolvere la funzione di unità di conto Bitcoin dovrebbe essere in grado di misurare il valore dei flussi e degli *stock* di beni, servizi e attivi patrimoniali nonché il valore di tutte le transazioni economiche, mediante la fissazione dei prezzi, la contabilizzazione dei debiti e dei crediti associati al passaggio di proprietà dei beni o dei servizi senza un contestuale regolamento in moneta[55]. Essere unità di conto significa, in altre parole, impostare un'unità di misura del valore dei beni da scambiare, tale da poter misurare con lo stesso metro tutti i beni disponibili sul mercato.

Per comprendere come ed in che misura Bitcoin assolva a tale compito, si deve in particolar modo far riferimento a due caratteristiche chiave: la divisibilità e la volatilità di prezzo. Come si vedrà, v'è una profonda differenza tra Bitcoin e le altre valute *standard* proprio riguardo a questi due fattori.

2.2.1 Divisibilità

Bitcoin è nominalmente quasi infinitamente divisibile, cosa che rappresenta un tratto peculiare e altamente distintivo della criptomoneta, che implica la possibilità di quotare un prezzo utilizzando fino a 8 cifre decimali (e, al crescere del valore, il sistema potrebbe aggiungere ulteriori cifre decimali). Questa caratteristica volge sicuramente a favore del bitcoin, poiché una buona valuta necessita di poter essere adeguatamente suddivisa per

[54] Cfr. Hanley, Brian P. (2013); "*The false premises and promises of Bitcoin*"; eprint arXiv:1312.2048.

[55] Cfr. Lemme G. e Peluso S. (2016), "*Criptomoneta e distacco dalla moneta legale: il caso bitcoin*", in Riv. dir. banc., dirittobancario.it, 43

prezzare ogni tipo e dimensione di transazione. D'altra parte, questa enorme divisibilità può avere un riscontro negativo sugli utenti, in quanto foriera di confusione e di problemi legati alla comprensione nel comparare i prezzi di beni e servizi (a tal proposito, si spiega la decisione della maggioranza delle valute *standard* di dotarsi solamente due cifre decimali). Quindi, se da una parte l'infinita divisibilità può tradursi in una diffusione maggiore di bitcoin, dall'altra questa diffusione potrebbe essere in parte limitata dalla riduzione della capacità dei consumatori di distinguere accuratamente i prezzi relativi.

2.2.2 Volatilità del prezzo

Tra tutte le caratteristiche identificate in questo elaborato, la volatilità del prezzo è senza ombra di dubbio la differenza più grande che intercorre tra Bitcoin e le valute *standard* più diffuse, quali il Dollaro, l'Euro o lo Yen. Tale caratteristica rischia di compromettere il futuro uso globale della moneta virtuale a valere sulle monete *standard* laddove inficia la capacità di Bitcoin di assolvere efficientemente sia la funzione di unità di conto che quella di riserva di valore[56]. In virtù dell'eccezionalità del fenomeno, si ritiene che esso debba essere esaminato maggiormente nel dettaglio.

Una moneta con una forte volatilità di breve periodo non può essere considerata una buona unità di conto, in quanto le fluttuazioni del prezzo rendono difficile quantificare e bloccare il valore di un prodotto attorno ad un "numero" certo. Queste frequenti oscillazioni conducono a costi diretti ed indiretti in capo sia ai rivenditori che ai consumatori: per i primi, che sì vendono i prodotti finali in bitcoin ma comprano materie prime e semilavorati sempre in valuta *standard*, si tratta di dover continuamente aggiustare i prezzi dei propri listini per evitare una riduzione dei ricavi o una perdita di competitività; per i secondi, ci si riferisce nuovamente alla confusione causata dai cambiamenti repentini dei prezzi ed alla difficoltà di comprendere il reale valore di beni e servizi.

Una volatilità che, tra l'altro, pregiudica anche la capacità di bitcoin di fungere da riserva di valore. Le continue oscillazioni del valore unite ad una forte incertezza sui sentieri evolutivi del valore danneggiano, di fatto, gli stessi possessori di bitcoin, mentre risulta essere un vantaggio per gli investitori che vedono in bitcoin un mero strumento speculativo.

2.2.2.1 Volatilità in numeri.

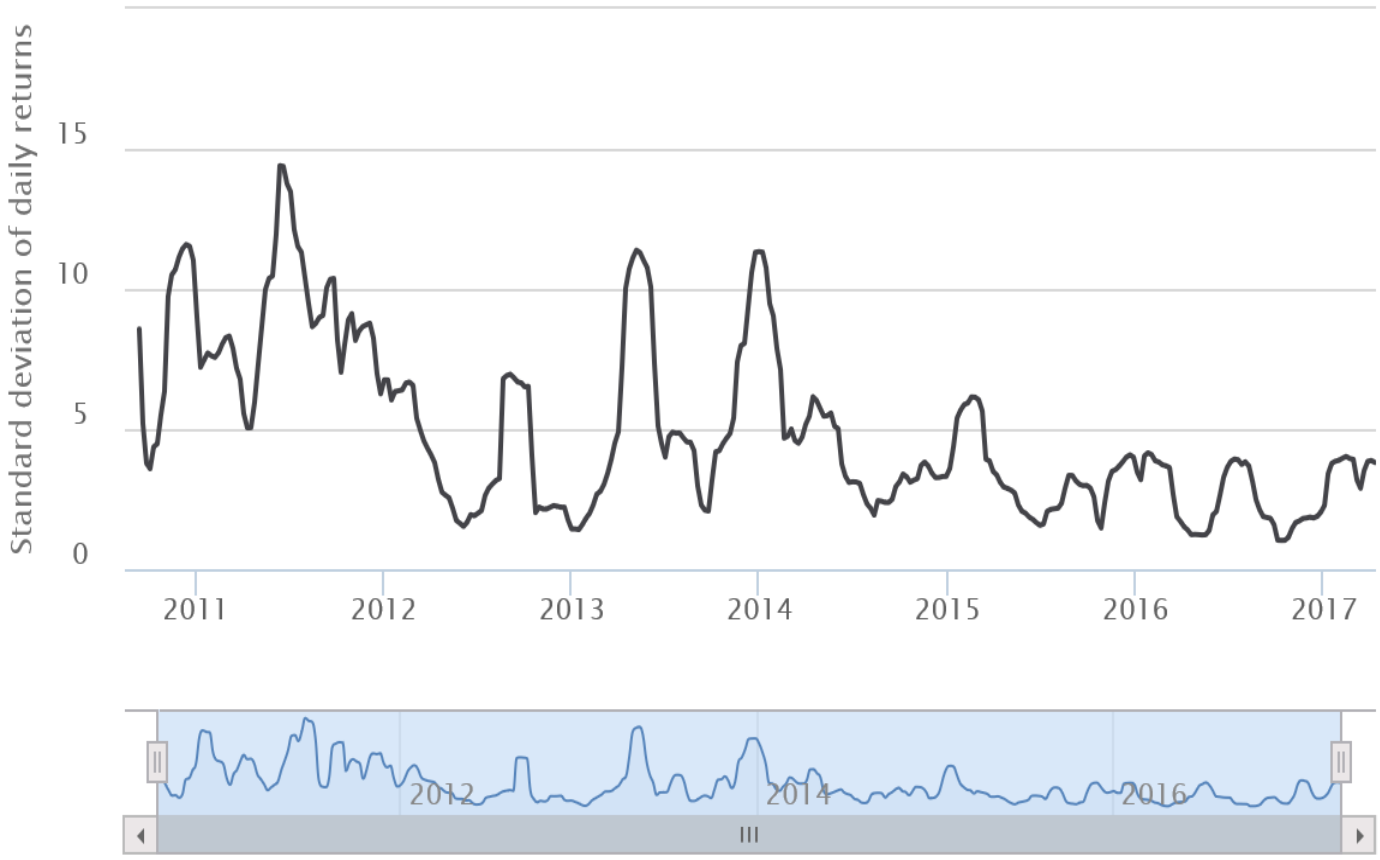
Le imprevedibili variazioni del prezzo del bitcoin portano ad interrogarsi sulla relativa variabilità. Non di rado si è assistito ad apprezzamenti o deprezzamenti nella misura del 50 per cento nell'arco di poche settimane; in più, nei primi 6 anni di vita, il valore del bitcoin è fluttuato in un *range* del ± 8.000 per cento: per dare un'idea dell'importanza di tale numero, basti pensare che nello stesso periodo il dollaro non ha avuto oscillazioni in un

[56] Cfr. Lemme G. e Peluso S. (2016), "*Criptomoneta e distacco dalla moneta legale: il caso bitcoin*", in Riv. dir. banc., dirittobancario.it, 43

range più ampio del 20 per cento.

Nella sottostante Figura 9 è mostrato l'andamento di questa nel tempo, calcolata come deviazione standard mobile dei prezzi giornalieri osservati nei 60 giorni precedenti. Trattandosi di deviazione standard, il grafico mostra le variazioni medie in valore assoluto: nulla dice circa aumenti o diminuzioni del prezzo stesso. Si può notare come, in concomitanza col *crash* del dicembre del 2013, la variabilità abbia subìto un certo ridimensionamento, pur mantenendosi su livelli molti elevati per una moneta[57]. D'altronde, è doveroso considerare che Bitcoin è in ogni caso un fenomeno di relativamente recente creazione, pertanto in una certa misura è anche comprensibile che vi sia un grosso margine di indeterminatezza circa il meccanismo di formazione del prezzo e delle sue evoluzioni future. Motivo per cui si ritiene che, col passare del tempo, il valore possa lentamente acquisire una maggiore stabilità.

Figura 9 – Variabilità a 60 giorni del cambio BTC/USD[58]



[57] Cfr. Bouri et al (2017), "*Bitcoin for energy commodities before and after the December 2013 crash: diversifier, hedge or safe haven*?", Applied Economics, DOI: 10.1080/00036846.2017.1299102.

[58] Cfr: https://www.btcvol.info/ (13/04/2017)

Ciò che invece salta all'occhio è la stessa incostanza della variabilità: non si è difronte solamente ad una volatilità estremamente elevata, ma la stessa assume valori molto diversi nel tempo, seguendo un sentiero costellato di improvvise impennate e cadute che altro non inducono se non ad aumentare ancor di più l'incertezza attorno al reale valore del bitcoin ed ai suoi futuri sentieri evolutivi.

2.2.2.2 Cause della volatilità

Quali sono le determinanti principali della volatilità? Occorre innanzitutto identificare le determinanti principali nel meccanismo di formazione del prezzo. Al pari di qualunque altro *asset*, il prezzo del bitcoin è regolato dalla legge della domanda e dell'offerta. Dal lato della domanda, occorre distinguere, almeno in linea teorica, tra domanda di bitcoin per la compravendita di beni e servizi e domanda per operazioni di natura speculativa. Dal lato dell'offerta, invece, si è visto che il sentiero evolutivo nell'emissione di nuovi bitcoin è già "fissato", cosa che porterà ad un costante apprezzamento del valore della moneta nel tempo; l'offerta di moneta è dunque relegata ai vecchi possessori di bitcoin già "estratti" e nuovi bitcoin che verranno estratti predeterminatamente nel futuro[59].

La domanda di bitcoin legata all'utilizzo della moneta per la compravendita di beni e servizi è solo apparentemente chiara: sebbene tutte le transazioni sono pubblicamente riportate sulla blockchain, il loro numero non rappresenta il totale ammontare di transazioni economiche, in quanto larga parte di queste sono transazioni effettuate per coprire meglio le tracce ed aumentare l'anonimità degli attori. Si tratta, in altre parole, del fenomeno delle micro-transazioni (c.d. *tumbling*). Per spiegare meglio tal concetto, si consideri il seguente esempio: se si volessero inviare un certo numero di bitcoin ad un'altra persona ed aumentare la difficoltà nel tracciamento, questa somma può essere suddivisa in tante piccole quantità ed ognuna inviata attraverso diversi indirizzi prima che possa raggiungere il destinatario.

La domanda di bitcoin legata a fini speculativi è altresì composta da tre fattispecie. Una parte degli utenti specula sulla moneta poiché ritiene che Bitcoin sia il futuro della moneta e che dunque, anche in virtù dell'offerta di moneta fissa e del continuo apprezzamento nel tempo, l'accumulo della stessa non possa che condurre ad esponenziali incrementi di ricchezza. D'altra parte, una folta schiera di investitori utilizza bitcoin per cercare di ottenere profitti dalla forte instabilità del prezzo, attraverso repentine e numerose operazioni di compravendita; non di rado si è assistito ad azioni prettamente speculative da parte di un gruppo di investitori che, comprando o vendendo in blocco una consistente quantità di moneta, hanno significativamente impattato sul prezzo, proprio al fine di trarre successivamente profitto da riacquisti o rivendite a prezzi più vantaggiosi. Non da meno è il rischio di manovre volte a influenzare attivamente il prezzo, attraverso intenzionali

[59] Cfr. Bouri et al (2017), "*Bitcoin for energy commodities before and after the December 2013 crash: diversifier, hedge or safe haven*?", Applied Economics, DOI: 10.1080/00036846.2017.1299102.

divulgazioni di informazioni riservate, *rumor* o addirittura notizie false. Speculazione che si presenta, infine, in tutte quelle operazioni di arbitraggio tra più piattaforme: è stato difatti osservato che il mercato dei bitcoin è tutt'altro che *arbitrage free*, con le diverse piattaforme di *trading* che offrono prezzi di acquisto e di vendita anche notevolmente diversi tra loro. Si guardi ad esempio la figura sottostante, che mostra le differenze di prezzo (in dollari) di un bitcoin su diversi mercati. Il prezzo proposto varia considerevolmente di piattaforma in piattaforma, addirittura tra Gdax e Localbitcoins vi è una differenza di 541 punti base, pari al 22 per cento.

Figura 10- Prezzi operati fra più piattaforme di *trading*[60]

BTC/Name	Price	24h Change	24h Volume (BTC)	Exchanges
USD	2,472.63319146	0.55%	131,529.00	
Bitfinex	2,455.10000000	1.64%	52,979.18	Bitfinex
Gdax	2,434.32000000	-3.26%	34,853.67	Gdax
BTC-e	2,479.00000000	1.79%	25,871.18	BTC-e
Kraken	2,544.00000000	3.35%	13,727.96	Kraken
Cex.io	2,748.32850000	2.33%	3,996.24	Cex.io
QuadrigaCX	2,610.73000000	6.43%	70.18	QuadrigaCX
The Rock Trading	2,847.00000000	7.57%	22.11	The Rock Trading
XBtce	2,479.00000000	0.00%	6.37	XBtce
Bitsquare	2,500.00000000	-3.11%	2.10	Bitsquare
Localbitcoins	2,975.40000000	7.46%	0.00	Localbitcoins

Per quanto riguarda l'offerta di moneta, come anticipato essa si muove su due binari diversi: da una parte vi sono i possessori di bitcoin già estratti, la cui offerta è legata alla loro predisposizione ad utilizzare bitcoin come mezzo di scambio; dall'altra, vi sono i nuovi bitcoin estratti dai *miner*. Se il mercato fosse in perfetto equilibro, il prezzo del bitcoin dovrebbe essere eguale al costo marginale di produzione, ossia il costo dell'energia elettrica (individuata come unica, o quantomeno prevalente, componente di costo del processo di estrazione)[61]. Tuttavia, alcuni studi (Boeri et al. 2016) hanno dimostrato che la correlazione fra il prezzo di un bitcoin e il costo dell'elettricità è troppo debole per poter definire un collegamento sufficientemente valido, asserendo in altre parole che anche il mercato dei bitcoin non è in concorrenza perfetta.

Poiché numero delle transazioni e predisposizione all'uso da parte dei detentori possono essere ragionevolmente stimabili, da questo quadro sembra emergere che la variabilità sia legata maggiormente alle attività degli

[60] Cfr. www. http://etherwisdom.com/bitcoin (26/05/2017).

[61] Cfr. Hayes A. S. (2016), "*Cryptocurrencies Value Formation: An Empirical Study Leading to a Cost of Production Model for Valuing Bitcoin*", Telematics and Informatics. Doi: 10.1016/j.tele.2016.05.005.

speculatori: comportamenti, come quello appena descritto, sono sicuramente una delle componenti più imprevedibili nel meccanismo di formazione dei prezzi. V'è tuttavia da considerare un ulteriore fattore, tutt'altro che trascurabile: sia la domanda che l'offerta di moneta sono fortemente influenzate dalle aspettative future[62]. Aspettative che si formano e si adattano di volta in volta agli avvenimenti del mondo esterno, relativi ad aspetti economici, politici, giuridici o che semplicemente pongono Bitcoin sotto una maggiore esposizione mediatica. Si possono, ad esempio, riconoscere una serie di eventi geopolitici, quali la già citata crisi economica di Cipro o l'elezione di Donald Trump in America, che hanno in qualche modo condotto ad un apprezzamento del bitcoin sul dollaro. D'altra parte, si guardi al crollo del prezzo osservato in concomitanza con la decisione del Governo Cinese, nel tardo 2013, di proibire agli intermediari finanziari l'uso sotto ogni forma di bitcoin ed a vincolarne le possibilità di utilizzo. Non da ultimo, v'è da sottolineare l'imprevedibilità degli effetti degli avvenimenti esterni: Si guardi ad esempio all'attacco informatico più recente, WannaCry, ha tenuto ostaggio di centinaia di migliaia di file nell'attesa del pagamento di un riscatto da circa 300 o 600 dollari in Bitcoin. Ci si sarebbe aspettato una caduta del prezzo, legata alla cattiva reputazione che deriva dall'accostamento della criptovaluta con il mondo del *cybercrime*; invero, per far fronte a queste richieste ed al rischio di un futuro incremento dei *ransomware*, molte aziende stanno facendo scorta di denaro digitale, livellando la domanda e, di conseguenza, anche il prezzo stesso della valuta.

Emerge un quadro interessante ma tutt'altro che rassicurante: il prezzo del bitcoin è esposto alle contingenze esterne molto più di un qualunque altro *asset*, in un legame spesso di difficile lettura.

2.2.2.3 Soluzioni alternative

L'incidenza del problema della liquidità è stata riconosciuta anche dagli stessi ideatori e sostenitori di Bitcoin, ma non mancano soluzioni alternative tese a ridurre i rischi e gli effetti della volatilità. Per le valute *standard* esistono meccanismi di stabilizzazione sia dal lato della domanda che dal lato dell'offerta; la domanda è stabilizzata dal fatto che le valute legali hanno, appunto, valore legale per il pagamento di tutti i debiti, pubblici e privati, e segnatamente per il pagamento delle tasse; l'offerta è altresì stabilizzata dall'opera delle banche centrali, che hanno il compito di adottare politiche monetarie per salvaguardare il potere d'acquisto. Tali stabilizzatori pongono un pavimento ed un tetto alle oscillazioni delle monete ufficiali, evitandone l'eccessivo deprezzamento (deflazione) o apprezzamento (inflazione)[63]. Per Bitcoin questi stabilizzatori non esistono, per cui si deve guardare ad altri modi per attenuare il problema. Difatti, un vantaggio del sistema Bitcoin risiede proprio nella sua natura *open-source*, che lascia ampio margine all'innovazione e all'implementazione di

[62] Cfr. Bouri et al (2017), "*Bitcoin for energy commodities before and after the December 2013 crash: diversifier, hedge or safe haven*?", Applied Economics, DOI: 10.1080/00036846.2017.1299102.

[63] Cfr. Amato M. e Fantacci L., (2016), "*Per un pungo di Bitcoin*", Egea, Università Bocconi Editore, Milano.

modifiche e a tal fine risulta estremamente sofisticato. Per risolvere il problema della stabilità, nella *community* sono rintracciabili diverse soluzioni, a volte solamente teorizzate, ed in questa sede ci si vuol soffermare essenzialmente su due specifici "meccanismi".

Una prima soluzione riguarda la nascita di piattaforme dedicate che, ricavando informazioni in tempo reale dal mercato valutario, possono aiutare i venditori nella fissazione dei prezzi ed ampliare le opportunità di spesa dei consumatori. Avvalendosi di tali piattaforme i venditori possono fissare i prezzi in una valuta e far visualizzare al consumatore tali prezzi in simultaneo e continuo aggiornamento in più valute, bitcoin compresi, ai tassi di cambio correnti. Questo sistema consente il monitoraggio dei prezzi in bitcoin per tutti gli attori del mercato in tempo reale a costo zero[64].

Una seconda alternativa è invero rappresentata dalle piattaforme di scambio istantaneo, le quali consentono al venditore di accettare pagamenti in criptomoneta, senza riceverla in concreto. Tali piattaforme si configurano come dei soggetti intermediari, i quali scambiano bitcoin pagati dai consumatori con una valuta *standard* da inoltrare ai venditori. In questo caso si assiste ad un trasferimento del rischio di cambio in capo proprio all'intermediario: non ricevendo di fatto alcun bitcoin, i venditori evitano in questo modo il rischio connesso alle fluttuazioni della valuta in cambio di una piccola commissione.

Nonostante queste parziali soluzioni, si deve riconoscere che il bitcoin rimane estremamente esposto all'eccessiva volatilità, che mina la sua capacità di fungere da unità di conto: in altre parole, non v'è adeguata efficienza nell'opera di prezzare adeguatamente beni e servizi nell'economia. Ma ciò non esclude la possibilità che in futuro, grazie allo sviluppo di nuove opzioni innovative, l'impatto di tale aspetto possa essere ulteriormente ridimensionato.

2.3 Bitcoin come riserva di valore

La terza funzione che una moneta deve svolgere è quella di riserva di valore, ossia deve riuscire a conservare il proprio valore nel tempo e poter essere detenuta per un utilizzo futuro senza correre il rischio che vi sia perdita di valore o di potere d'acquisto. Questa stabilità consente *de facto* la facoltà ad un attore di poter scambiare bitcoin in momenti diversi, nonché di poter accumulare ricchezza e mantenerla nel tempo. Per ciò che concerne le *fiat currency*, la stabilità del potere d'acquisto è garantita dalla autorità di politica monetaria, quali le banche centrali, ed alla loro opera anti-inflazionistica (ad esempio tramite la regolazione dell'offerta monetaria). Si è già visto di come il bitcoin non goda di questa prerogativa, bisogna dunque vedere se questi possa garantire la conservazione del valore a prescindere dalla presenza degli stabilizzatori delle Banche Centrali. La questione diventa fondamentale laddove è possibile rilevare che si può avere una riserva di valore che non funga da

[64] Cfr. Lemme G. e Peluso S. (2016), "*Criptomoneta e distacco dalla moneta legale: il caso bitcoin*", in Riv. dir. banc.,

strumento di pagamento, ma non si può avere uno strumento di pagamento che non abbia una seppur minima capacità di conservare il proprio valore nel tempo[65]. Anche in questo caso, svolge una funzione critica (e non propriamente positiva) la presenza di una volatilità pericolosamente elevata, di cui si è già discusso. Oltre ciò, si considereranno anche aspetti quali la sicurezza informatica, la spirale deflazionistica e l'accumulo di ricchezza.

2.3.1 Sicurezza della Rete

Una delle critiche più aspre mosse a Bitcoin riguarda la sua sicurezza, che non si riferisce soltanto alla sua componente informatica ma è piuttosto relativa a tutto ciò che incide sulla complessiva capacità di preservare il valore ed il possesso dei bitcoin degli utenti. Si vuol guardare, in sostanza, alla sicurezza dell'intera rete di scambio Bitcoin, con riguardo sia ai protocolli informatici che ne stanno alla base, sia ai meccanismi di funzionamento, sia ai diversi rischi a cui sono esposte le piattaforme di scambio.

Si deve innanzi tutto premettere che, rispetto a bitcoin, le valute *standard* hanno un meccanismo di difesa sicuramente più efficace, potendo essere protette sia attraverso la difesa "fisica" (ad esempi grazie all'uso di una cassaforte o nascondendo le banconote "sotto il materasso"), sia attraverso depositi presso gli istituti bancari. Il bitcoin è un bene virtuale e non gode di questa possibilità; in altre parole, il bitcoin deve essere giocoforza conservato su specifici portafogli virtuali. Conservare bitcoin sulla rete comporta tutti i rischi derivanti dalla sicurezza della rete informatica stessa, ed in effetti, in passato molti utenti hanno perso parte delle loro valute virtuali attraverso truffe[66] o furti operati sul *web*[67]. Restando in tema di sicurezza informatica, un settore

---

dirittobancario.it, 43;

[65] Cfr. Lemme G. e Peluso S. (2016), "*Criptomoneta e distacco dalla moneta legale: il caso bitcoin*", in Riv. dir. banc., dirittobancario.it, 43;

[66] Secondo alcuni critici, Bitcoin deve essere letto come un elaborato schema Ponzi, il quale richiede che le persone investano i loro soldi per pagare altre persone che hanno già pagato, e sono in attesa del loro guadagno, in uno schema "piramidale". Solitamente, è un tipo di struttura non sostenibile e destinata a collassare su sé stessa, non riuscendo a ripagare gli investimenti o venendo scoperta dalle forze dell'ordine, e si configura dunque solo come truffa. Tuttavia, tale struttura non sembra tuttavia essere particolarmente adatta a Bitcoin. Sebbene, come uno schema Ponzi, sembri promettere elevati guadagno ad una vasta platea di soggetti poco edotti dal lato finanziario ed informatico, in realtà non c'è un soggetto centrale che abbia iniziato la truffa; inoltre, quando si acquistano bitcoin, non si riceve una promessa di futuri guadagni, bensì gettoni (virtuali) che si possono utilizzare da subito per qualsivoglia finalità. È tuttavia opportuno segnalare che queste considerazioni non valgono per alcune altcoin, che in realtà sembrano create in una maniera molto simile a quella di uno schema Ponzi.

[67] A tal proposito, Bitcoin.org suggerisce di adottare alcune precauzioni per una protezione basilare del proprio *wallet*: a) fare backup di tutto il portafoglio; b) criptare i *backup online*; c) conservare i *backup* in molteplici posti sicuri, come chiavette USB o in documenti cartacei, in modo da non correre il rischio di perdere le relative chiavi; d) eseguire dei *backup* periodicamente; e) utilizzare una *password* alfanumerica complessa.

particolarmente attivo è quello dei *malware*[68]. Questi sono utilizzati dai pirati informatici per attaccare i sistemi che memorizzano indirizzi bitcoin e le chiavi private, compromettendone la sicurezza e rubando i bitcoin conservati nei relativi *wallet*. Altre tipologie invece sfruttano le schede grafiche ed i processori dei computer attaccati per effettuare operazioni di *mining*, sebbene casi del genere siano diminuiti vistosamente in virtù dell'aumento della potenza computazionale richiesta per minare.

Tuttavia, il semplice furto informatico di criptovaluta non è l'unica fattispecie che necessita di attenzione. Alcuni studi hanno stabilito che le falle nel sistema di sicurezza costituirebbero il motivo portante per il quale il 45 per cento circa delle piattaforme di scambio di bitcoin chiude in uno o due anni, la cui conseguenza è, ancora una volta, la perdita di bitcoin. Pare infatti che di queste piattaforme oltre il 46 per cento dichiari fallimento senza rimborsare agli utenti le perdite subite[69].

L'enfasi di questa analisi deve essere spostata sulla sicurezza della rete nella sua interezza. La questione non è di facile lettura e presenta numerose problematiche che possono rientrare nella categoria. Di seguito, verranno brevemente esaminate quelle più rilevanti.

2.3.1.1 Monopolio dei *miner*

Una circostanza che desta notevoli preoccupazioni è quella comunemente nota come "rischio del 50 per cento più 1", ossia che un soggetto (o più realisticamente un'associazione di essi, le *mining pool*) arrivi ad estrarre giornalmente più della metà dei bitcoin in circolazione. Questo fenomeno può potenzialmente portare ad una situazione di accentramento di "potere" in mano a pochi, esponendo dunque la comunità Bitcoin al rischio di un'influenza dominante sull'intera Rete, una sorta di monopolio-oligopolio, a danno della decentralizzazione e della democraticità ricercata nel Protocollo. Un controllo simile può portare ad operazioni di *double spending* dei *token*, a furti informatici da parte della maggioranza o semplicemente a rovinose cadute del valore del bitcoin. Difatti, almeno in teoria, ottenere la maggioranza del "*network power*" potrebbe permettere la duplicazione dei *token*, di ostacolare la validazione delle transazioni e magari di riscrivere la storia delle transazioni passate[70], il tutto per interessi personali e fraudolenti. In questi casi, il 50 per cento è il minimo teorico per avere la certezza di riuscirci, ma con poco meno la probabilità è comunque non indifferente. Una dei più estesi *pool*, chiuso nell'ottobre 2016, è stata Ghash.io, più volte vicinissimo ad ottenere il 51 per cento della

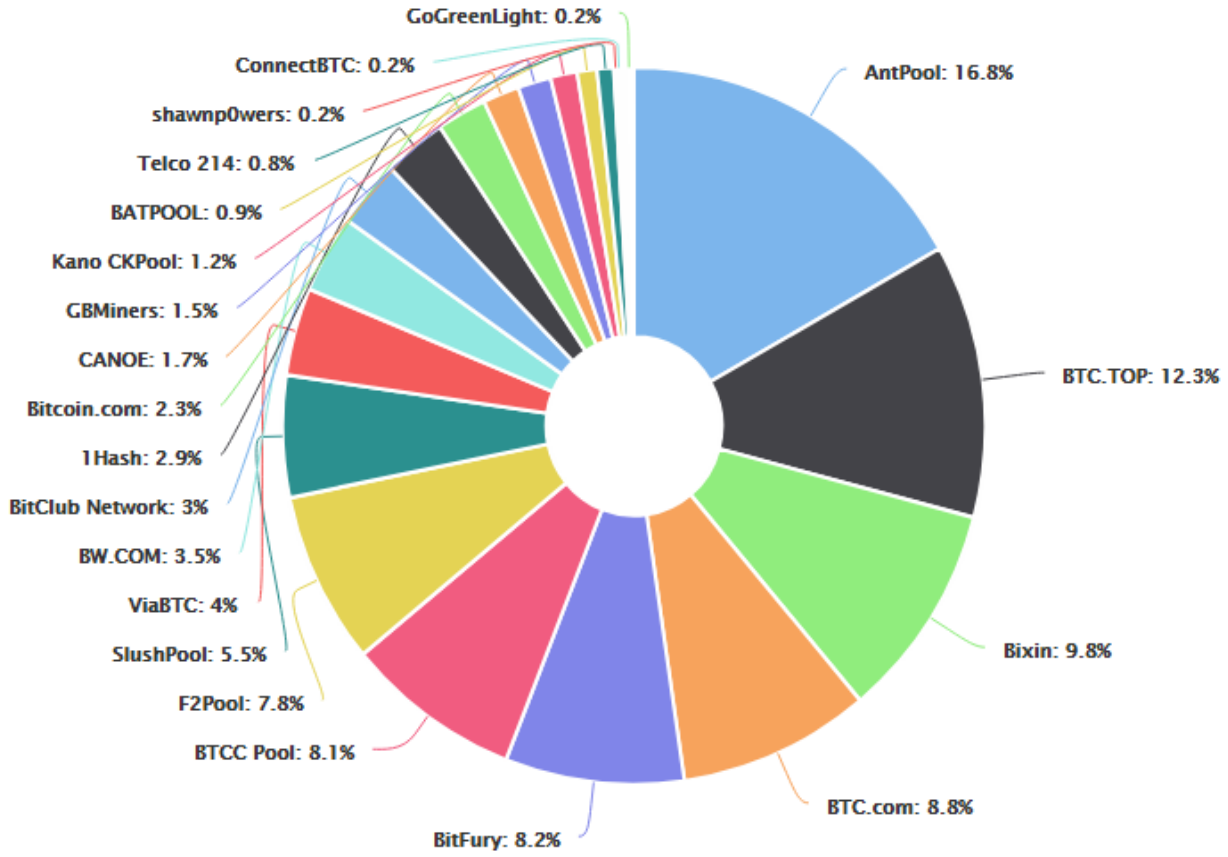
[68] I *malware* sono programmi informatici usati per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata.

[69] Cfr. Ciaian, P., Rajcaniova, M. & Kancs (2016), "*The digital agenda of virtual currencies: Can BitCoin become a global currency?*", Inf Syst E-Bus Manage (2016) 14: 883.

[70] Un caso simile si è verificato per Dao, una piattaforma autonoma creata da Ethereum. La piattaforma aveva raccolto 150 milioni con il crowdfunding, ma a seguito di attacco informatico ne sono stati rubati 50. Dao è fallita ed Ethereum, per cancellarne traccia, ha riscritto tutte le transazioni della propria Blockchain, cambiando di fatto il passato.

potenza di *hashing* della rete. La società è riuscita a raggiungere la soglia del 42 per cento della rete nel gennaio 2014, per poi avvicinarsi alla preoccupante soglia del 50 per cento non più di tre mesi più tardi. Tuttavia, al netto di accordi non noti fra più consorzi, allo stato attuale non sembra esserci un soggetto che abbia una concentrazione di potere notevolmente maggiore rispetto ad altri (come osservabile nella figura successiva, che mostra la percentuale di mercato dei gruppi di minatori più popolari).

Figura 11 – Distribuzione capacità di *hash*[71]



V'è da puntualizzare che le *mining pool* non nascono, almeno all'apparenza, con l'obiettivo di controllare o manipolare il funzionamento della rete Bitcoin. L'aggregazione di più individui risponde difatti alle più elementari logiche economiche, in quanto viene a formarsi una società con maggiore potenza computazionale e, di conseguenza, oltre a ridurre i costi individuali di ogni associato, aumenta le possibilità di "vincere" la ricompensa. Data la serrata concorrenza, un *min*er che opera individualmente, scontrandosi con una barriera economica all'entrata, si espone al rischio di non riuscire mai a risolvere un blocco per giorni al netto di costi

[71] Cfr. https://www.blockchain.com (01/06/2017).

fissi inevitabili. Di conseguenza, anche in ragione della crescente difficoltà nel risolvere i blocchi e del continuo adeguamento delle attrezzature informatiche richiesto, il *miner* solitario è una figura che tende nel tempo ad essere estromessa dal mercato. Da un punto di vista di efficienza economica, la creazione di società di *miner* sembra dunque essere proprio la soluzione preferibile.

Bitcoin implementa un sistema di incentivi-disincentivi per fronteggiare l'attacco del 50 per cento più 1. Si sostiene, in concreto, che un potenziale attacco della maggioranza alla Rete non sarebbe per nulla auspicabile, poiché una destabilizzazione di Bitcoin potrebbe causare una caduta del valore della moneta, lo stesso bene "obiettivo" dell'attacco, ed alimentare sfiducia nel sistema. La questione è stata affrontata in via preventiva anche nello stesso Protocollo Bitcoin, ove si può leggere: "Gli incentivi (le ricompense ai *miner*) dovrebbero incoraggiare i nodi a rimanere onesti. Se un attacco esterno fosse capace di radunare maggiore capacità di calcolo di tutti gli altri nodi, dovrebbe decidere se utilizzare tale capacità per frodare gli altri utenti riprendendosi i propri pagamenti, o piuttosto per generare nuovi gettoni. Sarebbe per questi più conveniente giocare secondo le regole, visto che esse avvantaggiano l'attaccante con nuovi gettoni in quantità maggiore rispetto a chiunque altro, piuttosto che distruggere il sistema e quindi la validità delle proprie monete"[72].

Un punto di vista condivisibile ma che non risolve del tutto la questione, soprattutto in relazione a tre punti. In primo luogo, queste aggregazioni espongono il sistema ad un ulteriore rischio di sicurezza dell'intero sistema; si pensi ad un hackeraggio di uno solo di questi *pool* ed alle possibili conseguenze: una fetta non indifferente della rete può essere messa a rischio con una sola mossa. In secondo luogo, non si è al riparo dal cosiddetto *selfish mining attack*. Si tratta di quel particolare caso in cui un grosso *pool*, giocando con i ritardi con i quali presenta agli altri nodi i blocchi trovati e generando dei conflitti, riesce ad accaparrarsi una percentuale maggiore dei bitcoin generati col *mining*, ovviamente a scapito di tutti gli altri minatori e causando loro una perdita di profitto. Questo può automaticamente invogliare una parte dei minatori meno efficienti all'abbandono del mercato o, paradossalmente, ad unirsi al *pool* stesso, con un abbassamento del livello di concorrenza e di efficienza di tutto il sistema di *mining*. Infine, il sistema incentivi/disincentivi del Protocollo ben si applica agli attacchi di grande portata, ma non sembra avere la stessa forza persuasiva nei confronti di operazioni di *double spending* di piccole dimensioni.

2.3.1.2 Potere e sicurezza informatica delle piattaforme di *exchange*

La proliferazione delle piattaforme di scambio dedicate ha indotto ad interrogarsi sulla reale sicurezza delle stesse, in particolar modo riguardo alla sicurezza informatica e al potenziale accentramento di potere in mano ai gestori. Le piattaforme di scambio di bitcoin nascono con l'intento di rendere possibili le transazioni tra utenti, permettendo la conversione di criptovaluta nelle maggiori valute globali e consentendo la conservazione del

[72] Cfr. Nakamoto S. (2008), "*Bitcoin: un sistema di contanti elettronico peer-to-peer*", www.bitcoin.org.

proprio *wallet online*. Ma, come precedentemente accennato, la conservazione di bitcoin in *wallet online* comporta un rischio di sicurezza aggiuntivo rispetto alla cosiddetta "*cold storage*", poiché sorge un rischio di hackeraggio della piattaforma e di furto di credenziali. Si tratta, in questo particolare caso, di un problema associato alle singole piattaforme piuttosto che ai meccanismi di funzionamento di base di Bitcoin nel suo complesso. Il caso Mt Gox può essere ancora una volta di ottimo esempio per specificare questo punto. Il suo fallimento è sostanzialmente dovuto ad una vulnerabilità nel proprio sistema di registrazione delle transazioni, che d'altra parte non è stato riscontrato nelle altre piattaforme di *exchange*. In altre parole, il problema ha coinvolto la sola Mt Gox, riversando gli effetti negativi sui propri correntisti e non in modo diffuso sul funzionamento di tutto il *network*.

Un ulteriore rischio connesso all'aumentare dell'utilizzo dei bitcoin e parallelo a quello della sicurezza è legato all'eccessiva libertà delle piattaforme di scambio dedicate. Le piattaforme di *exchange* ad oggi non sono adeguatamente regolamentate, a differenza delle borse valori tradizionali che godono di una normativa atta sia a tutelare l'investitore che a limitare gli accentramenti di potere. A questi organismi sono invero concesse condizioni di elevatissima (se non totale) discrezionalità rispetto alle operazioni da compiere, unite ad un relativamente basso grado di trasparenza richiesto. La questione assume specifica importanza riguardo agli effetti che tale potere può avere sul mercato di Bitcoin. L'accrescimento del numero e del volume medio delle operazioni in valuta virtuale contribuisce ad accentrare un'enorme mole di ricchezza presso queste piattaforme e, poiché si è in presenza di organismi in qualche modo esterni o di supporto a Bitcoin, nulla vieta che i gestori possano perseguire interessi diversi da quelli dell'intera *community*. Di conseguenza, l'interrogativo che ci si può porre riguarda l'eventuale campo di azione di queste ultime, specialmente per quanto riguarda la gestione dei portafogli digitali dei correntisti. In sostanza, si profila il rischio che alcune piattaforme possano studiare ed adottare soluzioni atte a praticare attività di tipo prettamente bancario, venendo meno all'ideologia di base di Bitcoin stesso. Anche *l'exchange* è, in effetti, un organismo centralizzato, con degli interessi non distribuiti e perciò potenzialmente spinto verso logiche di mercato.

La mancanza di una vera e propria disciplina rende dunque gli investitori molto più vulnerabili a perdite di ricchezza, senza contare che l'investitore si espone anche ai potenziali comportamenti fraudolenti dei gestori e agli eventuali fallimenti degli stessi. Come è stato già osservato, non esistono meccanismi di salvataggio di natura statale, né agenzie di *rating* che possano quantificare il rischio di insolvenza di una piattaforma e supportare gli investitori nella valutazione dei rischi. In caso di fallimenti, la tutela dell'individuo è demandata, ancora una volta, a tutta la *community* Bitcoin. Così come per la risoluzione di controversie tra due utenti, anche in questo caso l'onere grava sulla capacità di autogestirsi della rete, che ha il compito di trovare, di volta in volta, una soluzione quanto più equa ed efficiente possibile.

2.3.2 Spirale deflazionistica

Le valute *standard* sono di norma inflazionistiche, ossia il loro valore reale va a ridursi col passare del tempo. Ciò è principalmente dovuto all'aumento nel tempo della quantità di moneta in circolazione, che va a ridurre l'abilità della valuta stessa di fungere da riserva di valore. Bitcoin sceglie, piuttosto ambiziosamente, di definire *ex-ante* i sentieri evolutivi della quantità di moneta in circolazione. Nel Protocollo Bitcoin sono infatti decise la quantità di *token* emessi ed i ritmi di emissione, prevedendo inoltre un tetto massimo di moneta "estraibile" e quindi circolabile. Come si è visto, questa è una politica economica completamente opposta a quella delle principali autorità monetarie mondiali, tanto criticata dai "*bitcoiner"*, che punta a privare la valuta virtuale della componente inflazionistica e delle ingerenze di politiche monetarie esterne.

Gli effetti di questa scelta sono facilmente intuibili: se a fronte di un probabile aumento futuro della domanda il numero totale di bitcoin sarà sempre limitato alle famose 21 milioni di unità, senza apparenti possibilità di modifiche, non può che profilarsi un futuro deflazionistico per la moneta; in altre parole, piuttosto che perdere valore il bitcoin ha la tendenza ad apprezzarsi nel tempo (a meno che la *community* non deliberi in futuro un incremento di bitcoin in circolazione). La crescente difficoltà nell'estrazione di bitcoin è un ulteriore prova a sostegno di questa tesi: se risolvere un blocco e ricevere un dato ammontare di bitcoin come ricompensa diventa nel tempo più complesso ed oneroso, è necessario che i *miner* siano sempre incentivati a continuare a dedicarsi a tale attività; un apprezzamento della ricompensa (che nominalmente è certa ma decrescente nel tempo) spinge in tal direzione. Inoltre, se una creazione addizionale di bitcoin sembra impossibile, la deflazione è amplificata dalla possibilità di distruzione di bitcoin estratti: si pensi, ad esempio, alle quantità di moneta tuttora inutilizzate negli indirizzi comunemente detti "*sink*", ovvero dimenticati ed in disuso.

Questa tendenza deflazionistica può avere un duplice effetto. Da una parte, genera inequivocabili benefici per i possessori, che potranno accumulare maggior ricchezza nel tempo; dall'altra, l'aspettativa che si verifichi una simile circostanza porterebbe gli utenti ad accumulare bitcoin a fini speculativi, piuttosto che a far circolare la moneta, riducendone presenza ed uso nei mercati. Si profilerebbe in tal caso un uso del bitcoin come bene rifugio, capace di richiamare ancora una volta il paragone con l'oro, ma che di fatto potrebbe fungere da freno alla crescita economica e allo sviluppo.

Difficile leggere gli effetti di questo scenario deflazionistico in senso strettamente sfavorevole o favorevole; se è vero che l'assenza di inflazione potrebbe in astratto favorire la popolarità di Bitcoin sulle valute *standard* è anche vero che la vocazione alla deflazione potrebbe al contrario sfavorirla facendo da contrappeso, poiché

rischia in ogni caso di comprometterne la capacità di operare in modo efficace come riserva di valore, soprattutto tenendo conto della volatilità dei prezzi[73].

2.3.3 Accumulo di moneta e speculazione

L'affermazione del Bitcoin nel mondo dei pagamenti si scontra con un effettivo basso utilizzo del bitcoin negli scambi commerciali, in favore di attività di investimento speculative e di accumulazione di ricchezza. Si tratta di fattispecie strettamente legate rispettivamente alla spirale deflazionistica di cui si è discusso in precedenza.

La capacità del bitcoin di svolgere la funzione di riserva di valore ha conseguenze da non sottovalutare. Come si è visto, sebbene il numero di transazioni sia in continuo aumento, tale numero risulta essere piuttosto contenuto se rapportato alle transazioni svolte giornalmente nelle valute tradizionali. A ciò, bisogna aggiungere il fenomeno delle micro-transazioni, che "maschera" il reale numero di operazioni in criptovaluta. La ragione di questa relativa scarsità non è tanto da ricercare nella quantità di bitcoin in circolo, quanto più sulle finalità dei suoi detentori. Sta di fatto che una moneta che continua ad apprezzarsi nel tempo non sembra essere potenzialmente ottimale ad essere ceduta e scambiata, bensì sottostà positivamente ad una logica di accumulazione in vista di un accrescimento della ricchezza personale. Tuttavia, un tale scenario è poco desiderabile, principalmente per due ragioni.

In condizioni normali, la politica monetaria ha infatti la possibilità di agevolare la crescita economica sia aumentando l'offerta di moneta in circolazione sia abbassando i tassi di interesse. Da questa operazione ne consegue che le imprese sono incentivate ad indebitarsi e quindi ad investire e, nel contempo, si riduce la propensione delle famiglie al risparmio, aumentandone la propensione al consumo. Tuttavia, in una situazione in cui gli attori prediligono detenere moneta piuttosto che immetterla nel mercato, si contravviene ad una spirale contrattiva dei consumi e degli investimenti, rallentando la ripresa ed impedendo la crescita dell'economia reale (ci si riferisce a quel fenomeno comunemente noto come "trappola della liquidità"). Parallelamente, la moneta immessa nel sistema che non viene spesa, rappresenta un potenziale pericolo per la stabilità del sistema economico. La moneta accumulata può difatti essere improvvisamente reinserita nel sistema in blocco, generando iperinflazione.

In seconda istanza, si può pervenire ad una situazione di concentrazione di ricchezza in mano a pochi che, oltre a contrastare con la "democratizzazione finanziaria" del sistema economico promulgata da Bitcoin, potrebbe essere estremamente pericolosa, semplicemente per il potere di pressione che implicherebbe sui potenziali utilizzatori (per scambi e prestiti) da parte degli effettivi possessori[74]. Ma si proceda per gradi. Si è detto che la

[73] Cfr. Lemme G. e Peluso S. (2016), "*Criptomoneta e distacco dalla moneta legale: il caso bitcoin*", in Riv. dir. banc., dirittobancario.it, 43

[74] Cfr. Amato M. e Fantacci L., (2016), "*Per un pungo di Bitcoin*", Egea, Università Bocconi Editore, Milano.

predeterminazione della moneta porta effetti deflattivi, ossia che, a fronte di un (auspicato) aumento della domanda di moneta, il valore del bitcoin si apprezzerà nel tempo. In questo contesto, coloro che ne trarrebbero maggior guadagno sarebbero i *miner* "storici", all'epoca ricompensati con un numero maggiore di bitcoin. È verosimile ritenere che la prospettiva di un aumento di valore del bitcoin abbia generato la tendenza a tesaurizzarlo, rendendolo scarso rispetto alle potenziali transazioni e quindi auto-avverando la profezia di apprezzamento. Facendo riferimento alle statistiche più attendibili, sembra che l'andamento sia proprio questo. Al 3 dicembre 2013, utilizzando un prezzo di 1.000 $ ed ipotizzando che vi siano 12 milioni di bitcoin in circolazione, ecco cosa si ottiene: 47 individui posseggono il 28,9 per cento dei circa 12 milioni di bitcoin coniati sinora. Altri 880 posseggono il 21,5 per cento. Il che significa che 927 persone controllano metà dell'intera capitalizzazione di mercato della valuta digitale. Altre 10.000 persone controllano circa un quarto. E agli altri (circa un milione di persone) rimangono le briciole (500.000 bitcoin sono fuori circolazione, o perché sono stati sequestrati dal governo o perché i proprietari hanno smarrito la *password*)[75].

Un tale quadro di accentramento di ricchezza è quindi tutt'altro che desiderabile e l'affermazione a livello diffuso di Bitcoin, peraltro nato con un'ideale (almeno sulla carta) solidaristico e democratico, potrebbe esser in tal caso esser rifiutata. L'eccessiva capacità della valuta virtuale di apprezzarsi nel tempo potrebbe avere effetti deleteri su un'utopica economia esclusivamente fondata su Bitcoin ed è indubbio che l'attenzione delle autorità governative dovrà focalizzarsi sulla prevenzione di suddetti scenari.

2.4 Sintesi

Dall'analisi comparativa effettuata, risulta davvero difficile parificare il bitcoin ad una moneta tradizionale su un piano prettamente economico. In accordo con la posizione assunta dalla Banca Centrale Europea[76], esse assolverebbero soltanto parzialmente alle tre classiche funzioni monetarie necessarie.

Con riguardo alla prima funzione, ossia la capacità di fungere da mezzo di scambio, le problematiche più importanti sono legate non soltanto alla mancanza di un riconoscimento legale, che appunto pone la sua adozione alla spontaneità degli attori, ma soprattutto alla mancanza di un'adeguata struttura di diritti e tutele nei confronti degli utilizzatori è un freno ad un ipotetico riconoscimento legale. Gli attori, in assenza di una vera e propria normativa dedicata, non possono sentirsi al riparo da comportamenti fraudolenti e da perdita di ricchezza, ad esempio legate al fallimento di un mercato, cosa che invero si è verificata in più occasioni. Ed in effetti attualmente non ci sono e non possono essere date garanzie sulla sicurezza del sistema nel suo complesso. Inoltre, si è visto che anche le caratteristiche che potenzialmente potrebbero garantire un vantaggio competitivo

[75] Cfr. Wile R. (2013), "*927 People Own Half of All Bitcoins*", Business Insider, 10 dicembre, http://www.businessinsider.com.

[76] Cfr. Banca Centrale Europea (2014), "*Virtual Currency Schemes – a further analysis*", disponibile su: www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

considerevole, come il basso costo delle transazioni o la pressoché infinita divisibilità, in realtà nascondono insidie che tendono a controbilanciare gli effetti positivi. La stessa rapidità delle validazioni, ampiamente pubblicizzata come punto di forza del Sistema Bitcoin, non risulta pienamente efficiente nelle transazioni per così dire "quotidiane"; inoltre, la crescente difficoltà nella risoluzione dei blocchi da parte dei minatori espone ad un rallentamento di pratiche di inserimento delle transazioni nella blockchain e, in relazione, ad probabile un minor utilizzo nelle pratiche commerciali.

Non mancano dubbi anche sulla capacità del bitcoin di preservare il proprio valore nel tempo e di configurarsi sia come unità di conto che come una riserva di valore affidabile. Si è visto come l'esponenziale volatilità del tasso di cambio sia, con ogni probabilità, la differenza maggiore che intercorre con le monete tradizionali e che risulta essere il limite più grande nell'affermazione futura di Bitcoin, anche in virtù di un'assenza di meccanismi di stabilizzazione (quale ad esempio potrebbe essere la regolazione dinamica dell'offerta di moneta). Il valore del bitcoin, inoltre, è pericolosamente esposto a comportamenti speculativi ed agli eventi politici, giuridici ed economici esterni al mondo Bitcoin (che sono, tra l'altro, di difficile lettura). Infine, rispetto alle valute a corso legale, si osserva un maggior rischio inerente alla sicurezza della Rete, legato sia a fattori esterni, come attacchi informatici alle piattaforme di scambio, sia interni alla stessa Rete, come comportamenti fraudolenti dei gestori delle piattaforme di scambio o relativi all'acquisizione di posizioni monopolistiche.

Le conclusioni a cui si è giunti sembrano tra l'altro avallate da un report pubblicato, successivamente ad un (ennesimo) crollo del valore nel giugno 2017, da Morgan Stanley, il quale condanna il Bitcoin e sostiene che le criptovalute non potranno affermarsi in futuro né come delle interessanti forme di investimento finanziario, né tantomeno come una valida moneta. Secondo l'istituto bancario, il bitcoin propone una moneta scomoda per i pagamenti di beni e servizi che non potrà reggere il confronto con la praticità e la solidità oggi garantita dalle carte di debito e credito.

Tuttavia, vi sono altri scenari ove la criptomoneta può giocare un ruolo più importante anche nell'immediato futuro. Ci si riferisce in particolar modo a quei paesi in cui la valuta nazionale è debole e soggetta a forti scosse inflazionarie, come per esempio Argentina e Venezuela, oppure a paesi dove il sistema bancario non è radicato, come alcuni stati africani. In Kenya, ad esempio, la gran parte della popolazione non è cliente di alcuna banca ma possiede un telefono cellulare; in concomitanza con una valuta nazionale instabile, gli utenti potrebbero optare di utilizzare i propri cellulari per scambiarsi appunto criptomonete[77].

[77] Cfr. Luther W. L. (2016), "*Bitcoin and the Future of Digital payments*", The Indipendent Review, v.20, n.3, ISSN 1086-1653, pp.397-404.

Capitolo 3 – Usi illeciti e riciclaggio

Se nel capitolo precedente si è analizzato come Bitcoin non possa facilmente essere parificato ad una moneta, in questa sede si procederà ad approfondire il suo legame con la criminalità. Sebbene nella maggior parte degli ordinamenti Bitcoin non sia considerato illegale in sé per sé, alcune sue caratteristiche peculiari, quali la maggior difficoltà nel tracciamento dettata dalla pseudo-anonimità e l'assenza di un organismo centrale, ne fanno un mezzo di scambio che oggettivamente ben si presta ad utilizzi poco leciti. Come mostrato dai casi Silk Road e Liberty Reserve[78], le diverse operazioni criminali che sfruttano la criptovaluta sono numerose e ben ingegnate. Si riconoscono, a riguardo, atti di compravendita di materiale illecito (pedo-pornografia, armi, sostanze stupefacenti...), od attività che si inseriscono nella categoria del *cybercrime* (frodi informatiche, furto di identità o di informazioni riservate, od addirittura il reclutamento di assassini), senza dimenticare pericolose operazioni di finanziamento al terrorismo (*money dirtying).* Inoltre, le criptovalute possono configurarsi come un'eccellente strumento per l'evasione fiscale.

Ciò che preme maggiormente in questa sede è approfondire il rischio legato alle pratiche di riciclaggio di denaro (*money laundering*) mediante Bitcoin e, più in generale, le valute virtuali. Nel proseguo della trattazione si entrerà maggiormente nel dettaglio sui sopracitati temi, in particolar modo circa la connessione tra Bitcoin e le moderne tecniche criminali, le problematiche relative alla prevenzione ed alla repressione delle attività di riciclaggio e delle risposte normative finora adottate.

3.1 Riciclaggio nell'era contemporanea

3.1.1 Reato di riciclaggio e modalità di intervento

Il riciclaggio di capitali rappresenta quell'insieme di operazioni di re-immissione di denaro nel circuito dell'economia legale, la cui origine è associata ad attività di stampo criminale. Nell'economia contemporanea, i fenomeni legati al riciclaggio di denaro hanno effetti tutt'altro che marginali sull'economia, poiché alterano le condizioni di concorrenza, il corretto funzionamento dei mercati ed i meccanismi di allocazione delle risorse. Si stima che l'impatto sulla sola economia italiana possa oscillare tra l'1,7 per cento e il 12 per cento del PIL, a seconda dei criteri di misurazione.

Solitamente, si identificano tre fasi di riciclaggio: a) fase di *placement*: i criminali si liberano del denaro contante, spesso di piccolo taglio e che deriva dalla vendita di stupefacenti o da altre attività illecite, utilizzando una serie di operazioni (deposito, cambio, trasferimento, acquisto…). In questa fase, nota anche come

[78] Piattaforma di scambio che fungeva da deposito di ingenti somme convertite in moneta digitale, accusata dalla Procura di New York di aver contribuito al riciclaggio di ben sei miliardi di dollari.

"*immersion*", i capitali ottenuti illegalmente vengono raccolti ed allocati presso degli intermediari finanziari oppure in beni acquistati sul mercato, grazie alla complicità di un prestanome; b) fase di *layering*: consiste nel "lavare" il denaro sporco, ossia effettuare operazioni finanziarie per ostacolare la ricostruzione investigativa dei flussi finanziari da parte delle forze dell'ordine e mascherarne l'origine criminale; c) fase di *integration*: consiste nella reintroduzione dei capitali nell'economia legale per mezzo di prestazioni fornite da professionisti altamente specializzati come notai, commercialisti, istituti bancari e altri tipi di intermediari finanziari. Solitamente, questi soggetti sono situati in Paesi con una legislazione debole sotto il profilo dell'antiriciclaggio e molto attenti alla salvaguardia del segreto bancario (i c.d. paradisi fiscali). Inoltre, l'utilizzo di prestanome e società di comodo aiuta i criminali ad ostacolare le indagini atte ad accertare la reale titolarità della ricchezza.
La lotta al riciclaggio è tipicamente articolata in due sistemi, ossia sistema di contrasto e sistema di prevenzione. Il primo prevede l'utilizzo di strumenti propri del diritto penale, quali reclusione, sanzioni amministrative e confisca dei beni, il tutto con la finalità di reprimere le attività di riciclaggio, l'impiego di denaro di provenienza illegale e l'auto-riciclaggio. In Italia il riciclaggio è un reato previsto dall'articolo 648-bis del Codice Penale; è colpevole di reato colui che "sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo" e chi ostacola l'identificazione della loro provenienza delittuosa. La materia è inoltre regolata dal d. lgs. n. 56 del 20 febbraio 2004 e dal decreto n. 141 del 3 febbraio 2006, oltre che dalla la direttiva 2005/60/CE tradotta nel decreto legislativo 231/2007. Le attività di prevenzione, invece, mirano ad intercettare in maniera anticipata le infiltrazioni criminali nel sistema economico legale e si fondano sulla collaborazione fra le autorità pubbliche e gli operatori privati; questa collaborazione è incentivata dalla volontà dei privati di mitigare i rischi legali e di reputazione che deriverebbero da un coinvolgimento, anche inconsapevole, in pratiche criminali. Altrettanto importante è la raccolta di dati e informazioni sensibili relative alle transazioni ed alle parti coinvolte, soprattutto se in queste intercorrono diversi soggetti intermedi, quali possono essere agenti di cambio o piattaforme di scambio. Inoltre, è necessario monitorare continuamente le suddette transazioni, le tipologie di rapporti tra le parti coinvolte ed i volumi delle operazioni. Per contenere il rischio potrebbe infine essere opportuno introdurre un sistema di limiti, come ad esempio il divieto di accettare pagamenti in contanti per operazioni di importo superiore ai 2.999 euro[79], oppure quantità massime di prelievo dagli sportelli bancari. È infine essenziale che tutti i dati "sospetti" acquisiti dagli operatori privati siano prontamente messi a disposizione delle autorità competenti, quale l'agenzia nazionale antiriciclaggio del Paese di riferimento, al fine di adottare le più adeguate misure di intervento.

[79] Cfr. D.Lgs. n. 231/2007, art. 49.

3.1.2 Evoluzione

Nel tempo si è assistito ad un'evoluzione delle tecniche di *money laundering*, legate alla dissimulazione di capitali di origine o finalità illecita: si utilizzano spesso, per scopi criminali, tecniche sofisticate, sviluppate grazie all'innovazione finanziaria, alla globalizzazione dei mercati ed alle potenzialità consentite dalle moderne tecnologie informatiche[80]. Da sempre, infatti, tra criminali ed autorità è in atto un continuo "gioco al rincorrersi", che vede i primi tentare di ideare di volta in volta nuove strategie per perseguire le proprie finalità ed i secondi tentare di riconoscere, prevenire e contrastare tali meccanismi. Allo stato attuale, questo gioco è reso ancor più dinamico dallo sviluppo tecnologico, nel quale Internet ha assunto assoluta importanza ed ha permesso di percorrere strade inedite da contrapporre ai classici *modus operandi* dei criminali. La stessa rete può incidere secondo diversi gradi: può configurarsi come mero strumento-veicolo, il cui ruolo è principalmente quello di sostituire il corriere fisico con un computer nella fase di *placement* (riciclaggio digitale strumentale), oppure può assurgere ad *input* per la creazione di nuovi stratagemmi per il riciclaggio di denaro, capaci di coinvolgere anche le fasi di *layering* ed *integration* (riciclaggio digitale integrale)[81].

La sfida per il legislatore e le autorità deve altresì partire necessariamente da una conoscenza approfondita dell'ambito in cui queste attività si inseriscono. Il continuo avanzamento tecnologico favorisce difatti un contesto nel quale le organizzazioni criminali possono congetturare molteplici stratagemmi, sfruttando le cosiddette "aree grigie" della legislazione, che potenzialmente consentono operazioni *de fact*o criminali ma giuridicamente di difficile soluzione ed operativamente di altrettanto difficile contrasto.

Nei sistemi di prevenzione, una speciale attenzione va posta sui mezzi di pagamento che possono essere impiegati nell'esecuzione di transazioni finanziarie finalizzate al riciclaggio. Anche il settore dei servizi di pagamento ha subito una trasformazione nel tempo, investito dalle innovazioni apportate dalle tecnologie informatiche e di trasmissione di dati. Le stesse criptovalute rappresentano uno snodo importante di questi sentieri evolutivi, un servizio di pagamento dalle accresciute funzionalità e costituito da un rapido quanto preoccupante sviluppo; pertanto, esse necessitano di essere inglobate nel più ampio disegno di lotta al riciclaggio e al finanziamento del terrorismo, ed occorre inoltre di dotarsi delle conoscenze e degli strumenti idonei a riconoscere ed a contrastarne gli usi per finalità illecite. In effetti, la pericolosità di questi strumenti sta nella loro capacità di configurarsi, nella maggior parte dei casi, come fattispecie di riciclaggio digitale integrale: le valute virtuali non sono semplicemente uno strumento di *placement*, ma permettono l'ideazione di sempre più

[80] Cfr. La Rocca L. (2015), "*La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*", Analisi giuridica dell'Economia, Il Mulino, pp. 201-220.

[81] Cfr. Florindi E. (2016), "*Deep web e bitcoin: Vizi privati e pubbliche virtù della navigazione in rete*", Imprimatur Editore.

complesse ed inedite strategie che coinvolgono tutte le fasi di riciclaggio e che rendono in concreto ancor più complessa l'attività di prevenzione e di contrasto.

3.1.3 Deep-web e dark-web

Si è anticipato di come l'avvento dell'informatica abbia rivoluzionato le attività criminali. Si rende ora necessario far cenno al *deep web,* in quanto rappresenta un contesto particolarmente ideale, un terreno fertile sul quale si sviluppano le nuove tecniche di riciclaggio (anche per mezzo delle criptovalute), oltre che per altre categorie di reati informatici.

Con il termine *deep web* ("*web* sommerso") si indica quella parte della rete che non è di immediato accesso attraverso i comuni motori di ricerca. Dal d*eep web* deve essere distinto il *dark web*, un ulteriore sottostrato del *we*b, il cui accesso è relegato all'utilizzo di strumenti specifici, quali *browser* dedicati come TOR (*The Onion Router*); si tratta della parte più profonda del *deep web,* costituita da contenuti che sono volontariamente tenuti nascosti ai normali navigatori. Connettendosi a TOR, l'utente passa per 3 diversi nodi, presi casualmente dalla rete, prima di arrivare all'indirizzo di destinazione scelto. Ognuno di questi nodi conosce solo l'indirizzo da cui prende i dati e quello a cui passarli, in modo che nessun nodo possa ricostruire per intero tutta la catena di connessione. Questo stratagemma rende una connessione con TOR totalmente anonima e permette agli utenti di navigare in rete senza la paura di esser tracciati.

Al pari delle criptovalute, il *deep web* non è illegale, come d'erronea convinzione comune. Sono in realtà presenti numerosi indirizzi *web* di natura lecita ma non direttamente indicizzati od indicizzabili dai motori di ricerca, come ad esempio pagine ad accesso riservato o contenuti non testuali. In altre parole, per accedervi è necessario conoscere una *password* od il relativo *link*. Tuttavia, appare chiaro che il medesimo strumento possa essere utilizzato per nobili finalità o per altri scopi molto meno onorevoli. E difatti, si stima che il 90 per cento degli indirizzi *web* attivi sul *dark web* siano piattaforme dedite ad attività illegali od immorali, le quali sono tra l'altro finanziate principalmente con criptovalute (tra cui spiccano Bitcoin, Monero e DarkCoin). La ragione è da ricercare nella capacità del *deep web* di "nascondere le tracce", consentendo agli utenti una maggior protezione della propria identità e dei propri movimenti; l'uso delle criptovalute è da leggere proprio in tal senso, ossia esaltano ancor di più questi aspetti, ed in ragione si ritiene che queste, data la connessa difficoltà nel tracciamento e nella mancanza di obblighi informativi sulle controparti delle operazioni, sembrano essere il perfetto mezzo di scambio per questo tipo di commerci.

I mercati operativi sul *dark web* commerciano abitualmente droghe, materiale pedo-pornografico, oggetti rubati, armi, prodotti farmaceutici illegali e prodotti contraffatti, e finanziano attività legate al terrorismo o generalmente riconosciute inerenti al cosiddetto *cybercrime*, quali furto di identità ed informazioni personali, traffico di organi, estorsione…etc. Un esempio di prodotto acquistabile è *Command and Control* (C&C), un

server per il controllo remoto dei *malware*, difficilmente tracciabile ed utilizzato per operazioni di "furto dell*'account*"[82]. Nel 2014 il volume delle transazioni di natura illecita è stato valutato superiore ai 650 mila dollari al giorno, ai quali si aggiungono i traffici su almeno 50 diversi negozi *online* non identificati[83]. La soppressione definitiva di questo sistema di *online market* rappresenta una sfida all'apparenza impossibile per le forze dell'ordine, in ragione di due motivi: in primo luogo, il riconoscimento e l'intercettazione degli stessi (e dei relativi amministratori, usualmente coperti da pseudonimi e non direttamente tracciabili) è un'operazione di non facile accesso, proprio per la natura pressoché anonima del *dark web*; in secondo luogo, la chiusura di una piattaforma è solitamente seguita da una profilazione di nuovi *website*, pronti ad accaparrarsi la quota di mercato persa dalla precedente. Il caso Silk Road insegna: una volta soppresso il sito *web* e condannato il suo amministratore, sono apparsi *online* una lunga serie di siti fotocopia che hanno occupato quel segmento di offerta di droga, armi e quant'altro venuta meno dalla chiusura delle attività di Silk Road.

3.2 Strategie mediante Bitcoin

Nel sistema Bitcoin, l'assenza di intermediari finanziari, unito alla natura "pseudonima" delle transazioni, rischia di favorire operazioni di riciclaggio, oltre che di finanziamento al terrorismo, in quanto viene a mancare quell'organismo che, nell'economia tradizionale, funge da controllore e segnalatore di attività sospette alle autorità competenti. Al contempo, con un sistema finanziario che presenta interconnessioni su scala globale è facile nascondere e trasferire fondi in tutto il mondo creando in maniera semplice e rapida una struttura stratificata di società di comodo che operano attraversando le frontiere e le giurisdizioni, rendendo così estremamente difficile rintracciare l'origine del denaro[84].

Un'organizzazione criminale può difatti facilmente adoperare i bitcoin per trasformare il denaro proveniente da attività illecite in moneta reale e soprattutto pulita. Si tratta di operazioni piuttosto sofisticate ed apparentemente molto efficienti nel nascondere ogni traccia alle forze dell'ordine. Ad esempio, attraverso un opportuno *software* che falsifica la geolocalizzazione e che permette all'utente di essere "virtualmente" in un altro Paese, le cosche criminali possono trasferire soldi sporchi da carte prepagate (abilmente intestate ad un prestanome) sulle piattaforme di scambio Bitcoin in modo da acquistare criptomoneta. A questo punto, i bitcoin vengono trasferiti su diverse piattaforme mediante una molteplicità di transazioni e verso acquirenti sparsi in tutto il globo. Con

[82] Cfr. Passerelli, N. (2016), "*Bitcoin e antiriciclaggio*", Sistema di Informazione per la Sicurezza della Repubblica, www.sicurezzanazionale.gov.it.

[83] Cfr. Jay Palmer Fawcett (2016), "*Bitcoin regulations and investigations: A proposal for U.S. policies*", ProQuest LLC, Ann Arbor.

[84] Cfr. Commissione Europea (2016), "*Proposta di Direttiva del Parlamento Europeo e del Consiglio che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica la direttiva 2009/101/CE*", Strasburgo, COM (2016) 450 final, 2016/0208 (COD).

questo stratagemma, l'organizzazione riesce a piazzare sul mercato ingenti somme di denaro sporco in modo anonimo, dislocandolo ad esempio verso società di comodo atte alla ripulitura, ricevendo in seguito moneta pulita e irrintracciabile.

Di seguito, verranno analizzati singolarmente alcuni degli aspetti più comuni delle pratiche di riciclaggio mediante bitcoin. Generalmente, queste pratiche puntano a nascondere la fonte dei capitali criminali, nonché a mascherare il vero proprietario del portafoglio Bitcoin. Numerose agenzie governative ed istituzioni finanziarie hanno esaminato questi metodi al fine di vagliare soluzioni efficaci per ostacolare le attività criminali sottostanti l'utilizzo di bitcoin e, in generale, molte altre *alt-coin*[85].

3.2.1 Transazioni peer-to-peer

Le transazioni *peer to peer* sono transazioni svolte direttamente tra due parti, che non prevedono l'intervento di un organismo terzo che si interpone nello scambio. La più popolare piattaforma di scambi *peer-to-peer* sul *web* è Local Bitcoins[86], la quale concede l'opportunità agli utenti di comprare e vendere criptomoneta attraverso un meccanismo di coordinamento delle vendite sul sito, senza tuttavia prendere direttamente parte alla transazione. In sostanza, Local Bitcoins tende a espletare quella che è la modalità di trasferimenti "originale" predisposta dal Protocollo Bitcoin. Tuttavia, ivi si assiste ad un regime di commissioni, adottate individualmente dagli utenti, molto elevato: si parla di un costo che varia mediamente tra il 10 ed il 15 per cento, a fronte di commissioni dell'1 o 2 per cento richieste dalle comuni piattaforme abilitate[87]. Questa disparità nelle commissioni è un tipico segnale che può far sospettare operazioni di riciclaggio. Si può infatti trattare di attività utilizzate nella fase di *integration recycling,* che in altre parole puntano a giustificare legalmente un'entrata (la commissione) che in realtà deriva da denaro sporco. Queste quote di provvigione di solito non sono fisse, al fine di evitare l'identificazione di uno schema di riciclaggio usuale da parte delle forze dell'ordine.

La natura di questo tipo di transazioni permette ai soggetti di convertire una grande quantità di contante di provenienza illecita in bitcoin. Il meccanismo è piuttosto semplice: una classica transazione *peer to peer* è condotta di persona, ove due soggetti si incontrano, solitamente in un posto pubblico e opportunamente coperto da rete Wifi, e finalizzano un trasferimento di bitcoin al tasso di mercato corrente più il sovrapprezzo della commissione. Il venditore ottiene gli estremi del *wallet* a cui trasferire criptomoneta dallo stesso acquirente e, una volta ottenuta l'iscrizione del *transfert* nella blockchain, egli riceve in pagamento la valuta legale in contanti. In questo tipo di transazioni, non sono raccolte alcun tipo di informazioni sulle parti e sulla

[85] Cfr. Mandjee T. (2016), "*Bitcoin, its Legal Classification and its Regulatory Framework"*, 15 J. Bus. & Sec. L. 157, Available at: http://digitalcommons.law.msu.edu/jbsl/vol15/iss2/4.

[86] www.localbitcoins.com

[87] Cfr. Jay Palmer Fawcett (2016), "*Bitcoin regulations and investigations: A proposal for U.S. policies*", ProQuest LLC, Ann Arbor.

provenienza dei capitali sottostanti il trasferimento. In tal modo, il compratore riesce a immettere denaro illecito nel sistema finanziario senza peraltro attirare l'interesse delle autorità antiriciclaggio. I trasferimenti *peer to peer* sono inoltre sfruttati dai criminali che ottengono bitcoin dalla vendita di beni e servizi illeciti sul *dark web*: per mantenere l'anonimato, spesso i criminali evitano le piattaforme di scambio dedicate e sfruttano questo tipo di transazioni e, per convertire rapidamente bitcoin prima che il tasso di cambio possa essere meno conveniente, sono disposti a far fronte alle commissioni generalmente molto più elevate citate pocanzi.

In aggiunta alle operazioni svolta di persona, sono state via via implementate nuovi schemi *peer to peer*. Per esempio, quando venditore ed acquirente si trovano in posti geograficamente lontani, questi ultimi possono definire il pagamento attraverso un deposito di valuta *standard* nel conto corrente bancario del venditore, inviare un *wire transfer* od anche un vaglia postale, mentre alcuni venditori hanno iniziato ad accettare pagamenti in *gift card* (in valuta legale) e trasferimenti attraverso PayPal. Metodi come questi certamente comportano un rischio maggiore in capo all'acquirente; a tal proposito, Local Bitcoins ha implementato un meccanismo di *feedback* sul proprio sito *web*, per dare agli utenti un'informazione aggiuntiva circa l'affidabilità della controparte.

In definitiva, il potenziale rischio di un uso distorto delle transazioni *peer to peer*, con finalità di riciclaggio, è da valutare con cautela. Recenti ricerche hanno rivelato un'inquietante diffusione di queste pratiche su tutto il globo, tanto che le transazioni eseguite tramite il solo Local Bitcoins coinvolgono utenti presenti in 249 paesi, nonché più di 73 mila città americane[88].

3.2.2 Trasferimenti oltreoceano

Attraverso la conversione di moneta tradizionale in bitcoin, la criminalità organizzata ha trovato un sistema per rimpatriare e trasferire capitali all'estero, come quelli stanziati nei paradisi fiscali, senza dover temere la rilevazione e l'interdizione da parte delle forze dell'ordine. Al contrario, i capitali di origine illecita possono essere facilmente convertiti in bitcoin in quei paesi ove sussistono limitati controlli antiriciclaggio, per essere poi riconvertiti in patria. In più, questo meccanismo può facilitare il trasferimento di fondi ad organizzazioni terroristiche.

Uquid[89], una compagnia con sede in Gibilterra che tratta conversione di bitcoin, rappresenta un esempio di come un'organizzazione possa avere possibili implicazioni di riciclaggio. La società offre ai suoi utenti una carta prepagata VISA, ricaricabile in bitcoin, senza necessità di dover garantire tutti gli obblighi informativi necessari alle forze dell'ordine per intercettare capitali di dubbia origine. Il problema in questo caso risiede nella

[88] Cfr. Jay Palmer Fawcett (2016), "*Bitcoin regulations and investigations: A proposal for U.S. policies*", ProQuest LLC, Ann Arbor.

[89] https://uquid.com/

giurisdizione: in virtù di operazioni tra più paesi, le transazioni possono essere al di fuori del raggio di azione delle autorità che vogliono attivamente contrastare i fenomeni di riciclaggio, sia da un punto di vista investigativo che interventistico.

3.2.3 ATM Bitcoin

Sebbene in misura inferiore rispetto alle altre metodologie, anche gli ATM (*Automated Teller Machine*) possono essere strumenti utilizzati per operazioni di riciclaggio. Gli ATM del circuito Bitcoin non devono essere confusi con i bancomat tradizionali, piuttosto sono distributori in cui introdurre contanti per ottenere in cambio l'accredito di bitcoin sul proprio *wallet* personale o viceversa. La prima postazione è stata introdotta nel 2014, mentre già nel 2016 se ne contavano almeno 640 in uso in tutto il mondo. In Italia, il primo ATM è stato inaugurato a Roma, presso il Luiss Enlabs alla Stazione Termini.

Tramite gli ATM, gli utenti possono ottenere bitcoin in modo anonimo ed utilizzarli successivamente per l'acquisto di beni o servizi illegale, contribuendo alla crescita dell'economia sommersa sul *dark web*. Il vero problema risiede nelle legislazioni dei vari Stati, che spesso non fanno ricadere gli ATM del circuito Bitcoin sotto la normativa antiriciclaggio, non applicando le adeguate verifiche della clientela e di raccolta di dati sensibili.

In alcuni Stati americani, gli ATM devono essere obbligatoriamente registrati come MSB *(money service business*)[90] e dunque rispondono alle stesse norme antiriciclaggio applicate a questa specifica tipologia di attività. Tuttavia, a prescindere dalle informazioni richieste a norma di legge, gli obblighi che molti di questi sportelli richiedono sono spesso facilmente aggirabili. Pur ricadendo nella normativa, alcune compagnie di ATM richiedono solamente il numero di telefono del consumatore, che può benissimo esser nascosto con una scheda prepagata e completamente anonima. Altre compagnie richiedono una fotocopia del documento di identità, ma documenti falsi possono essere facilmente ottenuti sul *dark web* o da altri sistemi illeciti e gli sportelli raramente hanno l'abilità di riconoscerne l'effettiva autenticità.

[90] Per *money service business* si identificano quegli organismi che trattano la trasmissione o la conversione di denaro. La definizione è stata formulata per distinguerli dalle banche tradizionali, che normalmente provvedono agli stessi servizi in forma accessoria all'attività bancaria. Ogni MSB ha una diversa configurazione legale a seconda dello Stato di appartenenza, ma generalmente prevede la presenza di una specifica licenza ad operare, include ogni business di trasmissione di moneta e provvede a fornire le conversioni in valuta estera. Inoltre, hanno specifici obblighi informativi per quanto riguarda la normativa antiriciclaggio (AML, *Anti Money Laudering*).

3.2.4 Pratiche di tumbling

Per aumentare il livello di riservatezza delle transazioni, gli utenti possono ricorrere a pratiche di *tumbling*, le c.d. micro-transazioni, che di fatto permettono di offuscare ancor di più le informazioni reali relative alle parti coinvolte nell'operazione. Si è difatti visto che, pur consentendo un alto grado di protezione dei dati degli utenti, le transazioni in bitcoin sono pubblicamente visibili sulla blockchain e in linea teorica è sempre possibile trovare quel punto di contatto tra il mondo virtuale ed il mondo reale. Attraverso le pratiche di *tumbling*, condotte prevalentemente sul *dark web* ed attuate grazie al supporto di specifici intermediari chiamati "*tumbler*" (Bitcoin Fog, BitMixer, SatoshiDice…), un soggetto può spacchettare un consistente ammontare di valuta virtuale in una moltitudine di modeste dimensioni. In tal modo si avranno tante transazioni di piccolo importo piuttosto che un unico consistente trasferimento, che per sua natura può più facilmente richiamare l'attenzione delle autorità. In più, questo sistema offre un certo "effetto diversificazione": il rischio che una singola micro-transazione possa essere intercettata dalle forze dell'ordine pesa in maniera poco significativa sul totale dell'importo. Lo scaglionamento si ripercuote anche nelle attività di prelievo: suddividere nel tempo le conversioni di bitcoin ed i ritiri di moneta legale impedisce agli investigatori di identificare uno schema temporale nei movimenti e favorisce, ancora una volta, l'offuscamento delle attività.

Le commissioni per i servizi di *tumbling* si stimano pari ad una percentuale compresa tra il 5 ed il 15 per cento e dipendono essenzialmente dal volume dei trasferimenti ed il grado di frammentazione dell'operazione. L'uso di più *wallet* su cui suddividere o da cui inviare l'importo è invece un servizio aggiuntivo, poiché comporta una più efficace copertura delle informazioni sensibili a fronte di un costo più elevato, sempre tradotto in uno *spread* sommato al tasso di cambio. Per le forze dell'ordine, il problema principale delle tecniche di *tumbling* risiede dunque nel fatto che offuschino la blockchain, rendendo più difficile rintracciare la fonte originale del pagamento nonché riconoscere le stesse operazioni sospette. Si tratta, in altre parole, di un meccanismo di *layering recycling* altamente efficiente.

3.2.5 Transazioni sul dark web

Come già analizzato nel paragrafo precedente, l'avvento del *web* (ed in particolare del *dark web)* ha avuto un notevole impatto sul mondo criminale. Nel concreto, oltre ad essere il "luogo virtuale" ideale ove le organizzazioni criminali possono generare profitti da attività illecite, il *dark web* consente di: a) ottenere tutta una serie di strumenti accessori alle operazioni di riciclaggio, quali ad esempio documenti di identità cartacei falsi, od attuare operazioni di "*spoofing*", ossia operazioni di falsificazione dell'identità attraverso l'alterazione del proprio indirizzo IP, attraverso l'utilizzo abusivo di *username* e *password* di altri utenti, o ancora attraverso il camuffamento di file nocivi per renderli irriconoscibili come tali; b) sfruttare la maggior riservatezza offerta dal connubio con le criptovalute per facilitare le operazioni di *placement recycling* e per trasferire, senza una

reale preoccupazione delle forze dell'ordine, grossi flussi monetari di e da paradisi fiscali; c) convertire rapidamente i bitcoin ottenuti da siffatte attività criminali, tendenza che sembra tra l'altro confermare la scarsa propensione del bitcoin ad essere riserva di valore; d) ampliare l'efficienza delle operazioni di *layering recycling* in virtù della maggiore difficoltà delle forze dell'ordine nelle operazioni monitoraggio ed impreziosire il bagaglio di stratagemmi per le operazioni di *integration recycling*.

Per quanto riguarda Bitcoin nello specifico, v'è da notare che in seguito alle indagini su Silk Road ed alla confisca di tutti i bitcoin di proprietà a Ross Ulbricht, i criminali hanno iniziato a dubitare della pseudonimità di Bitcoin, spostando i propri interessi su altre criptovalute che possano concedere loro una maggior riservatezza, come ad esempio Monero. Questa valuta difatti incorpora operazioni di *tumbling* in automatico, al fine di rendere le transizioni ancor meno tracciabili. Molti mercati operativi sul *web* stanno aggiungendo la possibilità di accettare pagamenti in monero in concomitanza con bitcoin, rendendo inoltre attuabili gli scambi tra le due criptovalute; ne è un esempio AlphaBay, dedito alla vendita di stupefacenti: accettandola come strumento di pagamento, ha permesso a Monero di quintuplicare il proprio valore nell'arco di un anno.

3.2.6 Strategie alternative: Purse.io e gioco d'azzardo

Al di là delle pratiche di riciclaggio finora analizzate, quella relativa agli scambi che coinvolgono beni di proprietà e bitcoin risulta essere di particolare sagacia. Si tratta di operazioni di vendita di oggetti in cambio di criptomoneta, facilitate da piattaforme di recente formazione come Purse.io e similari. Purse permette di ottenere bitcoin tramite transazioni *peer to peer* non registrate, globali ed anonime attraverso la manipolazione delle vendite su Amazon, il famoso negozio *online*, che di norma non accetta bitcoin come mezzo di pagamento. Il meccanismo adottato da Purse si basa sulle *wish list*, un'opzione di Amazon che permette ai propri utenti di creare una lista degli oggetti "desiderati", da acquistare personalmente in futuro o da accettare in forma di regalo altri utenti. Coloro che vogliono entrare in possesso di bitcoin non devono far altro che acquistare un oggetto presente nella *wish list* di un altro utente e ricevere da questi bitcoin; la *mission* di Purse è proprio quella di offrire un punto di contatto tra i soggetti che vogliono vendere bitcoin in cambio di beni acquistabili tramite Amazon. La piattaforma, al fine di favorire queste transazioni, implementa un'interfaccia che replica le *wish list* presenti su Amazon.

Lo stratagemma che coinvolge Purse consente di proteggere le identità delle parti e le informazioni sensibili sulla transazione, che di fatto non vengono diffuse alle forze dell'ordine, ed inoltre non implica la raccolta di tutti i dati richiesti in ottica di antiriciclaggio, poiché né Amazon né tantomeno Purse sono soggetti a specifici obblighi informativi. In sintesi, questo schema permette la cessione di bitcoin da parte di coloro che vogliono privarsene in cambio di beni di vario genere, tendenzialmente beni facilmente rivendibili; d'altra parte, vista la mancanza dei sopracitati obblighi informativi, questo sistema configura un meccanismo per ottenere bitcoin in

modo sostanzialmente occulto da parte di coloro che vogliono sfruttare il mercato di beni illeciti del dark web. Tuttavia, il sistema delle commissioni mediamente adottato è particolarmente oneroso: gli utenti che cedono bitcoin tendono ad inserire degli *spread* addizionali piuttosto elevati per remunerare il servizio, pari anche al 15 per cento della transazione.

D'altro canto, i bitcoin si stanno rapidamente affermando come mezzo di pagamento prediletto nelle operazioni di riciclaggio che coinvolgono il gioco d'azzardo ed i casinò *online.* Il mercato dell'*online gambling* è in continua crescita, e l'industria ha da tempo aperto le braccia agli utenti Bitcoin (specialmente per quanto riguarda il poker *online* ed i dadi). Questa crescita esponenziale è legata sia alle agenzie di gioco già presenti sul mercato che hanno iniziato ad accettare criptovaluta, sia all'istituzione di nuovi casinò *online* che accettano esclusivamente Bitcoin o altre criptovalute, quali Primedice e Bitcoincasino.

Le piattaforme di gioco virtuali sono dei luoghi ideali per far circolare denaro proveniente da attività illecite, finalizzato alla corruzione o al riciclaggio senza dare troppo nell'occhio. La difficoltà nel monitorare gli spostamenti di denaro derivano soprattutto dall'estesa ramificazione di queste piattaforme, che è poi quella di cui si avvalgono le organizzazioni criminali, le quali dislocano in stati esteri i *server* per la raccolta delle giocate e la gestione delle stesse, spesso aggirando le normative statali che regolano il settore. In altre parole, queste ramificazioni prevendono che il *server* di un casinò *online* si trovi in uno Stato, la sede legale dell'azienda in un altro, e in un altro ancora la sede operativa. Inoltre, per le forze dell'ordine è difficile individuare l'ubicazione del giocatore, il quale può dislocare la propria attività in una giurisdizione diversa rispetto a quella fisica, facendo così perdere le proprie tracce.

I casinò *online* sono esposti ad una vasta gamma di strategie criminali. Per esempio, un prestanome introduce anonimamente sul proprio conto *online* una somma di denaro sporco per poi perderlo nei confronti di altri giocatori criminali, che in questo modo riescono a ripulire il denaro giustificandolo come vincita da gioco d'azzardo. Le organizzazioni criminali internazionali potrebbero inoltre hackerare il sistema per truccare giochi e indirizzare le vincite verso i membri dei gruppi stessi, nonché utilizzarli per pagare tangenti ai pubblici ufficiali in modo occulto.

3.2.7 Collegamenti con il terrorismo

Le attività di riciclaggio di denaro e le attività di finanziamento al terrorismo presentano diversi punti di contatto, tali da rendere le une strettamente connesse con le altre: difatti, queste transitano nei medesimi punti del circuito finanziario globale e spesso si avvalgono delle stesse tecniche e strumenti, che puntano a nascondere l'origine e la destinazione dei flussi di denaro coinvolti. Nell'era *digital*, le criptovalute sono uno strumento che ha acquisito importanza anche nell'ambito della lotta al terrorismo. I meccanismi di trasferimento di moneta anonimi hanno difatti favorito il fiorire di tecniche di diversificazione nelle fonti di finanziamento delle

organizzazioni terroristiche, come l'Isis, che fino a pochi anni fa ricorrevano principalmente ai traffici di stupefacenti e di armi, nonché alle estorsioni ed ai sequestri di persona. Secondo alcuni studi svolti dalle autorità israeliane, i fondamentalisti islamici sembrano conoscere relativamente bene le opportunità offerte dalle criptovalute per muovere capitali sottotraccia. Una fonte dell*'intelligence* israeliana, citata dal quotidiano "Haaretz", fa emergere un'inquietante pista relativa al mondo di bitcoin, che verrebbe utilizzato come canale per il finanziamento delle attività e come terreno di reclutamento (al pari dei *social network*)[91], nonché come strumento di *fundraising*. La possibilità di servirsi delle criptovalute per il finanziamento del terrorismo è un argomento che è stato ampiamente dibattuto su diverse testate giornalistiche, in particolar modo americane, creando un più che fondato allarmismo. Pare difatti che anche sul territorio americano ed europeo siano presenti i cosiddetti finanziatori del terrore, allo stesso modo in cui è stato riscontrato che, anche in un contesto occidentale, esistano sostenitori dell'Isis capaci persino di arruolarsi e di partecipare attivamente ad azioni terroristiche. Il rischio riguarda principalmente questi soggetti, che possono sfruttare le criptovalute e le connesse piccole falle nei sistemi legislativi proprio per muovere capitali dai paesi occidentali in favore dell'Isis, contribuendo ad aumentarne il potere economico e la pericolosità.

Il GAFI (Gruppo di Azione Finanziaria Internazionale), attraverso un'analisi condotta nel 2014, ha portato alla luce un inquietante caso che testimonia il collegamento tra Bitcoin ed estremisti islamici. Il 28 agosto 2015 Ali Shukri Amin, studente 17enne dalla Virginia (Usa), è stato condannato a 11 anni e 7 mesi per aver incitato altri giovani ad unirsi all'Isis attraverso Twitter ed un blog personale. Il teenager si era dichiarato colpevole davanti a un tribunale federale per aver fornito sostegno materiale allo Stato Islamico sul *web*, fondendo istruzioni su come utilizzare bitcoin per mascherare la fornitura di fondi finanziari ai jihadisti.

Il GAFI ha colto l'occasione di portare alla luce la crescente preoccupazione generale che aleggia tra le autorità giudiziarie di tutto il mondo, in relazione all'uso delle valute virtuali da parte delle organizzazioni terroristiche. Il mondo ha visto crescere a dismisura, ricorda il *report*, l'uso di siti *web* affiliati alle organizzazioni terroristiche per promuovere il ricorso ai bitcoin e *chat* tra estremisti sulle monete virtuali[92].

[91]Cfr. Vangone G. (2015), "*Il terrorismo islamico nell'era di Internet, fra bitcoin e dark web*", Eastonline, http://eastwest.eu/it/opinioni/open-doors/il-terrorismo-islamico-nell-era-di-internet-fra-bitcoin-e-dark-web .

[92] Cfr. Galullo R. e Mincuzzi A. (2017), "*Bitcoin, il riciclaggio invisibile di mafie e terrorismo internazionale*", Il sole 24 ore, disponibile a: http://www.econopoly.ilsole24ore.com/2016/07/08/bitcoin-e-antiriciclaggio-i-primi-passi-delleuropa-per-un-quadro-legislativo/.

3.3 Nuove sfide

3.3.1 Necessità di una definizione uniforme

Le valute virtuali rappresentano un fenomeno globale, che travalica le frontiere nazionali, e, come tale, richiederebbe la definizione di un quadro regolamentare il più possibile uniforme e condiviso a livello mondiale[93]. La questione diviene più critica se relazionata a diversi punti. La struttura decentrata della maggior parte degli schemi di attuazione di operazioni di riciclaggio, come osservato ad esempio nel gioco d'azzardo, impedisce alle singole autorità nazionali di imporre strategie di prevenzione e contrasto pienamente efficaci. Ciò in quanto le singole legislazioni mal si prestano a regolare situazioni ove intervengono entità disperse in diversi Stati; inoltre, la difficoltà raggiunge il suo apice se si guarda alla collocazione geografica degli operatori dell'ecosistema bitcoin, che spesso sfruttano giurisdizioni che non hanno un'adeguata normativa antiriciclaggio. In effetti, come è stato già osservato, le valute virtuali convertibili possono essere più facilmente utilizzate per finalità illecite rispetto alle valute tradizionali proprio in quanto consentono una trasferibilità globale più veloce e più difficilmente monitorabile dalle autorità. Da qui, il rischio che le organizzazioni criminali possano avvantaggiarsi da questi squilibri di "severità" negli ordinamenti.

La richiesta di un'armonizzazione degli ordinamenti è dovuta proprio a questa incidenza globale di Bitcoin, che deve esplicarsi non soltanto nelle misure per così dire "operative", ma deve necessariamente partire dall'adozione di una definizione il più possibile condivisa di criptovaluta. Si deve iniziare, in altre parole, con una determinazione univoca della natura di Bitcoin, per proseguire, in seguito, con l'impostazione di uno schema normativo condiviso adatto a contrastarne gli usi illeciti. Una definizione comune che può quindi sollevare il legislatore dell'annoso problema di dover forzatamente ricondurre le criptovalute sotto istituti giuridici già esistenti, che non risultano essere pienamente compatibili anche in virtù della natura "ibrida" di questi strumenti.

In effetti, di volta in volta Bitcoin è stato assimilato alla moneta, alle merci, ai prodotti finanziari, ai beni digitali o agli effetti commerciali. Ciascuno di questi tentativi si basa su interessanti analogie, ma si scontra d'altro canto con sostanziali differenze che impediscono di approdare ad un quadro normativo univoco e convincente[94]. Si è già ampiamente analizzato di come il protocollo ideato da Nakamoto, specialmente sul piano economico, difficilmente possa essere considerato come moneta; soffre infatti di importanti limiti in relazione alle sue caratteristiche funzionali (su tutte, la volatilità). Vista anche la sua natura dematerializzata, parte della dottrina ha provato a ricondurre la criptovaluta sotto la natura di moneta elettronica, asserendo che potesse configurarsi

[93] Cfr. Mancini M. (2015), "*Valute virtuali e Bitcoin*", Analisi giuridica dell'economia, Il Mulino, pp. 117-138.

[94] Cfr. M. Amato, L. Fantacci, (2016) "*Per un pungo di Bitcoin*", Egea, Università Bocconi Editore, Milano.

come un suo particolare sottoinsieme. A ben guardare, Bitcoin non può ottenere questo riconoscimento in quanto, in accordo con le disposizioni della BCE sulle monete elettroniche, non risponde pienamente ai tre criteri identificativi. In particolare, l'attività di produzione di criptovaluta avviene mediante operazioni di *mining*, che non sono vincolate alla ricezione di fondi di valore equivalente a quello monetario emesso. Si potrebbe in alternativa considerare il bitcoin come una merce, così come inquadrato nell'ordinamento francese, data la sua apparenza di bene immateriale, specifico, infungibile e divisibile. La differenza con ogni altri tipo di merce questa volta risiederebbe nel fatto 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[95]. Infine, un ultimo approccio consisterebbe nell'inglobare bitcoin nella definizione di valore mobiliare, in modo da coglierne anche il suo utilizzo come forma di investimento. Ma anche in questo caso il paragone non regge poiché, a differenza dei comuni strumenti finanziari, bitcoin non è mai passivo di un soggetto, non si configura come titolo di credito e non concede nessun diritto in capo al titolare. Ad esempio, in Italia questa difficoltà di ricondurre, alla stregua dei principi generali del vigente ordinamento, le valute virtuali a una qualificazione giuridica appagante, che prescinda dalle loro plurime possibili modalità di impiego, ha indotto gli studiosi a ricondurre la fattispecie a istituti molto generali, come quello di bene giuridico immateriale, nell'ampia nozione di cui all'art. 810 del codice civile, o quello di documento informatico, vale a dire di rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, nella definizione resa dal d.lgs. 7 marzo 2005, n. 82.

In sintesi, la sfida lanciata dalle criptovalute non sembra ad oggi completamente recepita dagli ordinamenti nazionali proprio alla luce di quest'ultimo punto, poiché investigatori e forze dell'ordine sono prevalentemente portati ad adattare le leggi in vigore ad una fattispecie su cui aleggia una forte componente di incertezza giuridica. Ad oggi, l'ordinamento tedesco è forse l'unico che abbia affrontato in modo compiuto il problema della qualificazione giuridica di Bitcoin. La mancanza di una legislazione globale uniforme pone inoltre problemi di intervento e di indagine, come già analizzato per i trasferimenti effettuati in criptovaluta per rimpatriare capitali esteri. Questa situazione di totale incertezza giuridica costituisce un fattore che agevola la possibilità di un uso distorto delle criptovalute per la realizzazione di attività criminali. Si sostiene, in altre parole, che per risolvere tale *empasse* possa essere necessario valutare la creazione di un istituto giuridico *ex-novo*, il più possibile adeguato alla natura delle criptovalute e che punti a contenere le asimmetrie presenti tra gli ordinamenti.

Un passo avanti, almeno per ciò che concerne il riconoscimento della natura delle valute virtuali, condiviso quantomeno a livello comunitario, è riscontrato nella proposta di modifica alla IV direttiva antiriciclaggio del febbraio 2017. In questa, si introduce una modifica dell'articolo 3, con l'aggiunta del punto 18, nella quale si

[95] Cfr. Passerelli, N. (2016), "*Bitcoin e antiriciclaggio*", Sistema di Informazione per la Sicurezza della Repubblica, www.sicurezzanazionale.gov.it.

identificano le valute virtuali come "una rappresentazione digitale di valore che non viene emesso da una banca centrale o da un'autorità pubblica e non necessariamente collegato a una moneta a corso legale, ma è accettato da persone fisiche o giuridiche come mezzo di pagamento e può essere trasferita, immagazzinata o scambiata elettronicamente".

3.3.2 Assistenza agli organismi di law enforcement

Uno dei problemi che più affligge le forze dell'ordine ed i sistemi legislativi riguarda la mancanza di risorse e di conoscenze specifiche per affrontare efficacemente la nuova sfida posta dalle criptovalute e dal *dark web*. La difficoltà risiede essenzialmente nella mancanza di un adeguato addestramento per riconoscere e contrastare le nuove tecniche utilizzate dai criminali in ambito di illeciti finanziari. Occorre poi servirsi di *software* avanzati e strumenti all'avanguardia per poter indagare con successo sulle operazioni svolte sfruttando le nuove tecnologie ed il vasto e complesso modo del *web*. Attrezzature che necessiterebbero anche di un continuo ricambio e rinnovamento, che permettano di seguire i sentieri evolutivi della tecnologia e non figurarsi altresì come un punto di debolezza. Ciò che si ritiene necessario è, in particolar modo, il supporto fornito da un'entità centralizzata che raccolga e conservi dati sulle informazioni strategiche riguardo le valute digitali. Informazioni che, tra l'altro, dovrebbero essere diffuse ad ogni livello (statale, regionale e locale) delle forze dell'ordine.

In questo contesto, si è evidenziata una crescente rilevanza delle imprese private nelle indagini digitali, spesso finanziate dalle stesse autorità governative; il loro compito è essenzialmente quello di incrementare il livello conoscitivo delle forze dell'ordine circa i nuovi metodi di riciclaggio che vengono di volta in volta alla luce e sfruttare i dati posseduti per realizzare modelli di analisi dei traffici in bitcoin al fine di riconoscere gli svariati schemi propri delle operazioni di riciclaggio. Si pensi ad esempio al meccanismo adoperato dai criminali nel *business* del gioco d'azzardo *online*. Nuove strategie continuano ad emergere giorno dopo giorno, andando di pari passo con un avanzamento tecnologico che offre sempre nuove opportunità capaci di inserirsi laddove spesso la legislazione non sembra arrivare. Il compito, in altre parole, è quello di ridurre il *gap* tecnologico-cognitivo e permettere alle autorità un tempestivo intervento, se non addirittura a prevedere ed anticipare tali nuovi schemi di riciclaggio.

Un esempio è offerto da un *software* frutto della *partnership* tra il Dipartimento della Sicurezza Interna degli Stati Uniti e Sandia National Laboratories[96]: la nuova tecnologia sviluppata potrebbe assistere le forze nell'ordine attraverso il monitoraggio della blockchain, finalizzato ad individuare i suddetti schemi di lavaggio di denaro sporco, oltre che attività di *cybercrime* e commerci illegali sul *dark web*. Si tratta, in sintesi, della

[96] I Sandia National Laboratories sono due grandi laboratori dell'United States Department of Energy, che si occupano di questioni di sicurezza nazionale per conto della National Nuclear Security Administration.

creazione di un'interfaccia grafica che permetta una comparazione dei flussi monetari osservati dalle forze dell'ordine con gli algoritmi trovati da Sandia, volti a riprodurre schemi di operazioni illecite osservati in passato. In questo modo, si può rendere possibile aggirare gli effetti di offuscamento delle pratiche di *tumbling* e pervenire ad una parziale de-anonimizzazione delle transazioni bitcoin.

Al pari di Sandia National Laboratories, anche altre entità hanno provveduto ad ideare *software* utilizzabili nelle indagini, finanziate dalle autorità governative. Si tratta di prodotti che solitamente offrono sofisticate analisi della Blockchain e delle transazioni Bitcoin per supportare le forze dell'ordine; si citano, al riguardo, Block Seer, Ledger Labs, Elliptic e Chainalysis.

3.2.3 Equilibrio tra regolamentazione e libertà di innovazione: il caso Bitlicense

La sfida per i legislatori attuali, come sempre, consiste nel trovare soluzioni efficaci senza frenare la crescita di nuovi mercati e affari: un approccio troppo rigido nei confronti di questa nuova tecnologia può tradursi in una limitazione delle offerte di servizi e prodotti connessi alle criptovalute, aumentandone i prezzi, calandone la qualità e creando possibili situazioni di cartello. A questo bisogna necessariamente aggiungere anche lo sviluppo di attività professionali e l'offerta di prodotti e servizi a cui potrebbe facilmente accedere chiunque, non soltanto i clienti di istituti bancari. Alla luce di queste considerazioni, l'obiettivo principale delle linee guida dovrebbe essere quello di trovare il giusto equilibrio fra il garantire lo sviluppo di sistemi che possono aumentare l'efficienza dei mercati finanziari ed incoraggiare lo sviluppo economico, e la necessità di salvaguardare l'integrità stessa dei mercati, ponendo limiti, regole di prevenzione e repressione dei comportamenti potenzialmente dannosi. D'altro canto, a fronte di effetti positivi in termini di innovazione finanziaria e di sistemi di pagamento alternativi per i consumatori, le valute virtuali possono influire negativamente sulla politica monetaria, sulla stabilità finanziaria e sulla sicurezza del sistema economico-sociale.

Nella breve storia di Bitcoin, vi è già stato un caso di una legislazione troppo restrittiva che ha ostacolato il fiorire del mercato. Nel 2015 il Dipartimento dei Servizi Finanziari dello Stato di New York ha codificato lo Statuto per la regolamentazione delle attività professionali in valute digitali, definito Bitlicense. Lo Statuto introduce specifici requisiti di registrazione e di licenza per ogni organismo, piattaforma o mercato che sia, che tratti con i bitcoin. Esso inoltre riconosce una lunga serie di attività che rientrano nel campo di applicazione della normativa. Difatti, sotto la definizione di "*virtual currency business activity*" rientrerebbero: lo svolgimento di attività di ricezione e trasmissione di valuta virtuale; la conservazione, la custodia od il controllo di valuta virtuale per conto di altri soggetti, l'attività professionale di acquisto e vendita di valuta virtuale; la prestazione del servizio di cambio valuta virtuale in valuta avente corso legale e viceversa; l'emissione,

l'amministrazione ed il controllo di valuta virtuale[97]. Ovviamente, il regime imposto da Bitlicense si applicherebbe solo nel caso in cui queste attività si coinvolgano lo Stato di New York od i soggetti ivi residenti. Per ottenere la licenza, i requisiti previsti sono molto simili a quelli già presenti per le "*money service business*", ma mediamente più stringenti. In particolar modo, gli *exchange* abilitati hanno l'obbligo di raccogliere numerose informazioni sulle parti delle transazioni e di segnalare, in ottica di antiriciclaggio, tutte le transazioni che eccedono i 10.000 dollari al giorno per persona e per volume e, più in generale, di inoltrare alle autorità competenti tutte le sospette operazioni di riciclaggio, evasione fiscale od altre attività criminali.

Il progetto Bitlicense ha tuttavia fallito, almeno in parte, i propositi iniziali; in altre parole, si è rivelato eccessivamente restrittivo, tale da ridurre drasticamente il numero di organismi in attività. Molte delle imprese operanti nell'industria delle valute digitali hanno espresso preoccupazioni riguardo gli eccessivi oneri informativi, nonché ritengono che Bitlicense limiti fortemente la capacità di innovazione dei mercati emergenti. E i numeri sembrano avallare questa lettura: ad oggi, solo tre organizzazioni hanno ricevuto la licenza e operano regolarmente come piattaforme di scambio Bitcoin. Il sito Coindesk.com ha monitorato il numero delle entità coinvolte nelle criptovalute e soggette a Bitlicense. Si può notare che nell'agosto 2015 il sito ha contato solo 9 *exchanger* che si erano realmente applicati per ottenere la licenza, mentre 15 hanno cessato del tutto le operazioni nello Stato subito dopo l'approvazione di Bitlicense[98], per spostarsi realisticamente negli Stati confinanti.

3.4 Quadro Legislativo

I rischi finora esposti hanno messo in allarme le Autorità internazionali ed europee, quali il Gruppo d'Azione Finanziaria Internazionale, l'Autorità Bancaria Europea (EBA) e la Banca Centrale Europea (BCE). Di seguito si provvederà a dare un quadro generale delle posizioni e dagli interventi normativi finora effettuati.

3.4.1 Gli interventi del GAFI

A livello internazionale, è stato instituito il Gruppo di Azione Finanziaria Internazionale (GAFI)[99], un organismo intergovernativo che sviluppa e propone strategie di protezione del sistema finanziario dalle attività di riciclaggio e dal finanziamento al terrorismo, nonché favorire la coordinazione dei diversi ordinamenti

[97] Cfr. La Rocca L. (2015), "*La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*", Analisi giuridica dell'Economia, Il Mulino, pp. 201-220.

[98] Cfr. Jay Palmer Fawcett (2016), "*Bitcoin regulations and investigations: A proposal for U.S. policies*", ProQuest LLC, Ann Arbor.

[99] Altresì conosciuto come Financial Action Task Force (FATF), è un ente intergovernativo con sede a Parigi, composto da 36 membri di rappresentanza di Stati e organizzazioni regionali e fondata nel 1989 su iniziativa del G7. Alle attività del FATF/GAFI partecipano inoltre rappresentanti di organismi finanziari internazionali quali il FMI, la BCE e l'ONU.

mondiali in materia. Il GAFI opera per mezzo di raccomandazioni, elabora *standard* riconosciuti a livello internazionale per il contrasto di attività illecite e ne studia i *trend* e le evoluzioni, in modo da fornire assistenza agli organismi governativi nella loro lotta alla criminalità. Trattasi di raccomandazioni, che non hanno diretta valenza legale. Sono tuttavia utili nel fornire ai governi uno strumento ausiliare aggiuntivo di grande utilità e capace di influenzarne attivamente le politiche legislative, soprattutto in quei paesi che presentano problemi strategici nei loro sistemi di prevenzione e contrasto[100].

In ogni Stato è inoltre istituita un'unica agenzia antiriciclaggio, chiamata *Financial Intelligence Unit* (FIU), dotata di autonomia operativa e gestionale e specializzata nell'analisi finanziaria delle informazioni sia ai fini prudenziali, sia ai fini della prevenzione e del contrasto delle attività di riciclaggio o ai casi legati al finanziamento al terrorismo sul territorio di appartenenza. In Italia, questo compito è assegnato all'Unità di Informazione Finanziaria (UIF), istituita presso la Banca d'Italia dal d. lgs. 21 novembre 2007, n.231 (Decreto antiriciclaggio) che a sua volta recepisce la direttiva europea 2005/60/CE. I compiti assegnati alla UIF sono principalmente i seguenti: a) ricevere ed analizzare le segnalazioni di operazioni sospette e le informazioni rilevanti inerenti a tali attività; b) ricercare e studiare le nuove tecnologie adoperate e le tecniche di riciclaggio; c) elaborare indicatori di anomalia, volti ad agevolare l'individuazione delle operazioni sospette; d) inviare alle autorità competenti il flusso di informazioni raccolte al fine di un intervento legislativo ed operativo. Con riguardo a quest'ultimo punto, l'art. 41 del suddetto decreto legislativo prevede una stretta collaborazione con la Guardia di Finanza e la DIA (Direzione Investigativa Antimafia), al quale la UIF è incaricata di inviare le segnalazioni ricevute (corredate di un apposita relazione tecnica), nonché con l'Autorità Giudiziaria, ai quali comunica i fatti di possibile rilevanza penale.

Un primo riferimento alle valute virtuali da parte del Gruppo di Azione Finanziaria Internazionale è riconducibile ad un *report* promulgato nel 2013. In questo frangente, le valute virtuali erano solamente menzionate, senza tuttavia ricevere una vera e propria definizione o altresì una specifica trattazione.

Il GAFI ha tuttavia ripreso la questione e, con la pubblicazione di un *report* nel 2014, ha sottolineato la pericolosità delle criptovalute, con specifico riferimento a Bitcoin; difatti nel *report* si può leggere: «Le valute virtuali e i bitcoin in particolare sono l'ondata del futuro per i sistemi di pagamento e forniscono un nuovo e potente strumento per i criminali, terroristi, finanzieri ed evasori, consentendo loro di far circolare e conservare fondi illeciti, fuori dalla portata del diritto»[101]. L'obiettivo dichiarato dal Gruppo consiste nell'implementazione

[100] Cfr. La Rocca L. (2015), "*La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*", Analisi giuridica dell'Economia, Il Mulino, pp. 201-220.

[101] Cfr. GAFI/FATF Report (2014), "*Valute Virtuali, definizioni chiave e potenziali rischi in ambito antiriciclaggio e finanziamento del terrorismo*", http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

di misure di prevenzione proporzionate da parte dei soggetti obbligati, a cui devono provvedere gli ordinamenti nazionali con disposizioni legislative *ad hoc* ma coerenti con il quadro delineato a livello internazionale. Il GAFI riconosce quindi l'importanza e la pericolosità delle valute virtuali, specialmente quelle convertibili e centralizzate, identificandone i rischi e le misure di contenimento più adeguate. Nel *report* è presente un'ampia trattazione della questione, nel quale le valute virtuali sono definite come una tipologia di *Internet-based payment service* e sono classificate in base alle caratteristiche e alle modalità di funzionamento. Il Gruppo individua i soggetti che operano nel sistema delle valute virtuali, identifica i rischi che esse comportano dal punto di vista antiriciclaggio e descrive alcuni casi di investigazioni inerenti ad attività illecite commesse attraverso l'utilizzo di questi strumenti[102]. Non meno importanti sono, infine, le ispezioni ed i controlli nei confronti dei destinatari della normativa antiriciclaggio (intermediari finanziari, *money transfer*, società fiduciarie...), con lo scopo di verificare il corretto adempimento dei relativi obblighi (adeguata verifica della clientela, registrazione dati e segnalazione delle operazioni sospette) e prevenire l'utilizzo del sistema finanziario per movimentare capitali di origine illecita[103].

3.4.2 L'opinion dell'EBA

L'European Banking Authority (EBA) ai sensi dell'art. 9 del Regolamento UE n. 1093/2010, del 24 novembre 2010, è un organismo di vigilanza europeo che ha il compito di monitorare le attività finanziarie nuove ed esistenti e adottare orientamenti e raccomandazioni volti a promuovere la sicurezza e la solidità dei mercati e la convergenza delle prassi di regolamentazione.

L'EBA ha iniziato ad interessarsi alle criptovalute a partire dal settembre 2013, conducendo un primo studio che ha condotto alla pubblicazione di un *warning* per i consumatori nel dicembre successivo. Oggetto del *warning* erano le perdite economiche che sarebbero potute seguire all'utilizzo di valute virtuali come sistema di pagamento. Pochi mesi più tardi, nel luglio 2014, l'EBA ha promulgato la propria "*opinion on virtual currencies*"[104], nella quale l'autorità ha espresso un giudizio fortemente critico sulle criptovalute: sulla base di un'accurata analisi costi/benefici, l'EBA ha sostenuto che i rischi derivanti dall'uso delle valute virtuali superassero, all'epoca, i vantaggi che gli utilizzatori avrebbero potuto ricavare da un loro utilizzo, sollecitando inoltre le Istituzioni europee a promuovere una duplice risposta regolamentare.

---

[102] Cfr. La Rocca L. (2015), "*La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*", Analisi giuridica dell'Economia, Il Mulino, pp. 201-220.

[103] Cfr. Passerelli, N. (2016), "*Bitcoin e antiriciclaggio*", Sistema di Informazione per la Sicurezza della Repubblica, www.sicurezzanazionale.gov.it.

[104] Cfr, EBA (2014), "*Opinion on virtual currencies*", disponibile su: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

L'approccio suggerito dall'EBA si predispone su due binari, di lungo e di breve periodo. In un'ottica di lungo periodo, l'EBA ha proposto di adottare un quadro normativo quanto più possibile armonizzato, al fine di contenere i rischi individuati; viene a tal fine raccomandata l'introduzione di una specifica regolamentazione attraverso uno schema di *governance authority*, incaricata di stabilire regolare l'utilizzo della criptovaluta ed assicurare l'integrità del sistema. Si profila inoltre un regime autorizzativo per i partecipanti al mercato delle criptovalute, con requisiti di capitale e di vigilanza volti a mitigare i rischi connessi al suddetto segmento di mercato. Nel disegno di lungo periodo, le istituzioni finanziarie che vogliano prestare servizi in valuta virtuale dovrebbero, infine, separare le attività svolte in valute virtuali e quelle svolte sui sistemi di pagamento tradizionali. Contemporaneamente al perseguimento delle finalità di lungo periodo, l'EBA ha invitato le istituzioni europee a mitigare i rischi che derivano dall'interazione delle criptovalute ed il sistema finanziario; nello specifico, si suggerisce di far ricadere sotto la disciplina comunitaria di antiriciclaggio e di contrasto al finanziamento del terrorismo anche gli organismi che offrano servizi di conversione fra valute virtuali e valute reali. Infine, sempre in un'ottica di breve periodo, l'EBA, dopo aver pubblicato un'avvertenza rivolta agli utenti per renderli edotti dei rischi derivanti dal comprare, detenere o scambiare valute virtuali, ha invitato le Autorità di vigilanza degli Stati membri a scoraggiare gli intermediari vigilati dall'acquistare, detenere o vendere valuta virtuale, fintantoché quest'ultima non sia stata regolamentata[105].

3.4.3 Interventi comunitari

La crescente diffusione del terrorismo internazionale, unita alle nuove modalità di finanziamento dello stesso ed alle pratiche di occultamento dei capitali di origine delittuosa, ha indotto la Commissione Europea ad una riflessione per accrescere le capacità di contrasto a questi fenomeni. Il risultato è stata la presentazione di un Piano d'azione per rafforzare ulteriormente la lotta contro il finanziamento del terrorismo, incentrato su due principali linee d'intervento: a) individuare e prevenire i movimenti di fondi e di altri beni effettuati dalle organizzazioni terroristiche e dai loro fiancheggiatori; e b) smantellare le fonti delle entrate delle reti terroristiche colpendone le capacità di raccolta fondi[106].

A tal proposito, la Commissione Europea, nel febbraio 2017, ha pubblicato una proposta di modifica della Direttiva 849/2015 (IV direttiva antiriciclaggio) e, coerentemente alla "Risoluzione sulle valute virtuali" approvata il 25 maggio 2016 dal Parlamento Europeo, ha riconosciuto il ruolo assunto dalle valute virtuali all'interno dell'ecosistema criminale. Le maggiori modifiche apportate alla Direttiva 849/2015 riguardano

[105] Cfr. Mancini M. (2015), "*Valute virtuali e Bitcoin*", Analisi giuridica dell'economia, Il Mulino, pp. 117-138.

[106] Cfr. Pezzuto A. (2017), "*Profili evolutivi della legislazione in materia di antiriciclaggio e contrasto al finanziamento del terrorismo*", disponibile al sito: http://www.dirittobancario.it/approfondimenti/antiriciclaggio/profili-evolutivi-della-legislazione-materia-di-antiriciclaggio-e-contrasto-al-finanziamento .

essenzialmente l'inclusione delle piattaforme di cambio di valute virtuali tra i soggetti obbligati, la fissazione di valori limite di transazione più bassi per alcuni strumenti prepagati, il rafforzamento dei poteri delle FIU nazionali, il potenziamento dei controlli nei confronti dei paesi terzi ad alto rischio e la raccolta di maggiori informazioni sulla titolarità effettiva.

Nello specifico, la Commissione propone di inglobare nell'ambito di applicazione della suddetta direttiva antiriciclaggio anche le piattaforme di scambio di valute virtuali (gli organismi di *exchange*) ed i prestatori di servizi di portafoglio digitale (*custodian wallet provider*). Piuttosto che ad una regolazione diretta delle valute virtuali, l'attenzione si è quindi incentrata su alcuni specifici operatori del settore, che possono rappresentare la determinante essenziale per un intervento efficace e risolutivo, poiché raccolgono una non indifferente mole di dati sensibili derivanti dagli strumenti di pagamento "tracciati" (bonifico, carta di credito...). Allo stato attuale, le politiche di antiriciclaggio sono adottate su base volontaria degli organismi di *exchange*, che tuttavia risultano controproducenti se non sono condotte all'interno di una regolamentazione che obblighi la trasmissione delle informazioni e delle operazioni sospette alle autorità competenti.

La chiave dell'intervento risiede dunque nel far cessare l'anonimato associato a questi scambi e permettere alle forze dell'ordine di entrare a conoscenza delle situazioni pericolose; per raggiungere tale scopo, si è proposto di allargare i comuni obblighi di adeguata verifica della clientela anche alle piattaforme che permettono il cambio di valute virtuali in valute legali. In questo modo, gli *exchanger* diventano soggetti obbligati ai sensi della direttiva antiriciclaggio: devono raccogliere, elaborare e registrare i dati personali, e in alcuni casi condividerli con autorità pubbliche (come le unità di informazione finanziaria) o con soggetti privati all'interno dello stesso gruppo; inoltre la normativa richiede che gli *exchanger* debbano essere in possesso di una forma di approvazione da parte delle autorità nazionali, sebbene si delega alla discrezionalità degli ordinamenti nazionali la scelta di adottare un meccanismo di licenza o di semplice registrazione. La stessa normativa si applica ai *wallet provider*, quei soggetti che offrono servizi di *hot storage*, necessari per conservare le valute virtuali sui portafogli *online*.

Si passa, poi, ad una precisazione della natura degli organismi a cui si rivolge la normativa. Gli *exchanger* sono definiti come prestatori di servizi impegnati principalmente e professionalmente nel settore dei servizi di cambio tra valute virtuali e valute a corso legale (nuova lettera (g) in cui al punto (3) dell'articolo 2 (1)). In questa prospettiva, e basandosi anche sull'analisi svolta dalla Banca Centrale Europea (*Virtual currency schemes, a further analysis*[107]) sui regimi di valuta virtuale, la Commissione distingue fra *exchanger* "puri" e piattaforme di

[107] Si tratta di uno studio condotto nel mese di ottobre 2012 pubblicato dalla Banca Centrale Europea, ove quest'ultima ha dichiarato apprezzamento per la creatività e innovazione riconoscendo dietro al protocollo di Nakamoto la presenza di rilevanti fondamenta dai punti di vista teorico-economici. Nello stesso documento la BCE rende nota la perplessità in termini di potenziale uso illecito dei gettoni virtuali da parte di utenti anonimi, avvisando che procederà regolarmente a indagini periodiche volte ad arginare simili usi.

trading. Gli *exchanger* (ad esempio Kraken) offrono servizi di *trading* agli utenti prezzando i tassi di cambio con cui *l'exchanger* acquisterà o venderà valuta virtuale contro le principali valute (dollaro statunitense, yen giapponese, euro) o contro altre valute virtuali. Si tratta per la maggior parte di imprese non finanziarie, che possono essere affiliate agli emittenti di valute virtuali o a terze parti. Solitamente, gli *exchanger* accettano una vasta gamma di opzioni di pagamento, quali contanti, bonifici e pagamenti con le altre valute virtuali. Inoltre, alcuni forniscono anche una serie di servizi accessori, quali ad esempio la possibilità di fungere da *wallet provider*, o fornire statistiche sulle evoluzioni del prezzo, sui volumi scambiati e sulla volatilità, nonché servizi di conversione ai commercianti che accettano le valute virtuali come strumento di pagamento. D'altra parte, le piattaforme di *trading* (ad esempio Local Bitcoins) funzionano come mercati, ossia sono uno strumento per mettere in contatto gli acquirenti e i venditori di valute virtuali, fornendo loro una piattaforma su cui possono acquistare e vendere tra loro. Infatti, a differenza degli *exchanger*, le piattaforme di *trading* non operano da intermediari diretti, non acquistando e/o vendendo in proprio. Alcune piattaforme di *trading* danno inoltre la possibilità di individuare potenziali controparti nelle vicinanze.

In ultima istanza, si segnala un ulteriore novità. Si prevede l'aggiunta di un secondo paragrafo nell'articolo 65, volta ad aumentare il potere delle FIU che si traduce, nello specifico, con l'attribuzione di poteri per istituire e mantenere un database centrale su cui registrare le identità degli utenti e gli indirizzi del portafoglio.

Tuttavia, questo non è che il primo passo di un lungo percorso verso una legislazione completa ed esaustiva della materia, che presenta lacune in virtù di quella parte di operazioni in valute virtuali che non si appoggiano alle sopracitate piattaforme. Come sottolineato anche dalla Commissione nelle note esplicative: "l'inclusione di piattaforme di *exchange* virtuali e di fornitori di *wallet* di custodia non risolverà totalmente la questione dell'anonimato collegato alle operazioni in valuta virtuale, dato che grande parte dell'ambiente delle valute virtuali rimarrà anonimo perché gli utenti possono anche effettuare transazioni senza utilizzare piattaforme di *exchanger* o di prestatori di *wallet* di custodia".

3.4.4 Posizione della Banca d'Italia e normativa fiscale italiana

La corsa del Bitcoin finisce, per la prima volta, sotto i riflettori della Banca d'Italia nel rapporto di stabilità finanziaria del 2014, ove si esplicitano le preoccupazioni sulle criptovalute, con specifico riguardo a Bitcoin, peraltro riprendendo posizioni condivise a livello comunitario; queste preoccupazioni riguardano principalmente il possesso e l'uso di criptomoneta, in particolar modo in ragione della mancanza di qualsivoglia forma di tutela degli utilizzatori.

Inoltre ha effettuato una comparazione tra Bitcoin e la moneta elettronica riconosciuta dall'ordinamento europeo, escludendo una possibile inclusione del primo nell'istituto giuridico della seconda.

La Banca d'Italia è tornata sull'argomento il 30 gennaio 2015, attraverso la divulgazione di un "Avvertenza sull'utilizzo delle cosiddette valute virtuali" sul proprio sito *online*, in contemporanea con una Comunicazione al sistema bancario. La posizione della Banca d'Italia presenti molti punti in comune con *l'opinion* divulgata dall'EBA, precedentemente analizzata, in particolar modo aderisce a quella visione delle valute virtuali come "rappresentazioni digitali di valore". L'obiettivo primario è indurre i soggetti vigilati ad adottare comportamenti ispirati alla massima cautela e ad assumere solo rischi consapevoli e ben ponderati. Difatti, l'acquisto, uso ed accettazione di pagamenti mediante criptovaluta non sono da considerare attività illecite, tuttavia si richiama nuovamente l'attenzione sugli stessi rischi, quali ad esempio elevata volatilità del valore, i rischi di perdite e l'assenza di tutele. Ma la Banca d'Italia pone particolare enfasi sull'incertezza che aleggia attorno alle valute virtuali, riconoscendo inoltre che il fenomeno è in continua evoluzione e ciò non permette un'identificazione esaustiva di tutti i possibili effetti che possono derivare dal suo utilizzo; si può leggere non si esclude che "l'uso di valute virtuali possa esporre l'utilizzatore a rischi ulteriori, derivanti dalle caratteristiche della specifica valuta virtuale utilizzata. Inoltre, il fenomeno è soggetto a rapida evoluzione ed è possibile che valute virtuali di ultima generazione presentino rischi ulteriori rispetto a quelli illustrati"[108].

Detto ciò, in accordo con l*'opinion* dell'EBA, la Banca d'Italia scoraggia le banche e gli altri intermediari vigilati dall'acquistare, detenere o vendere valute virtuali, sia in virtù dell'assenza di adeguati presidi e di un quadro legale certo circa la natura giuridica delle valute virtuali, sia poiché le concrete modalità di funzionamento degli schemi di valute virtuali possono integrare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati. In altre parole, specie in assenza di una puntuale presa di posizione da parte dell'ordinamento e di una scelta politica ben definita, le concrete modalità di funzionamento di bitcoin potrebbero ricadere negli ambiti di quelle determinate attività (es. bancaria) che la legge italiana riserva a determinati soggetti legittimati, titolati e qualificati sia dal punto di vista delle disponibilità patrimoniali e del capitale di vigilanza, che dal punto di vista della *compliance* nei confronti dei clienti.

Nel raccomandare particolare prudenza, si stabilisce che gli intermediari che vogliano trattare criptovaluta debbano portare l'orientamento della Banca d'Italia a conoscenza degli utenti, prima di intraprendere operazioni con essi. Inoltre, anche la Banca d'Italia auspica ad avere un quadro normativo omogeneo, che sia comune fra tutti gli istituti bancari e le varie nazioni appartenenti all'Eurozona. Ciò per evitare che la partecipazione degli intermediari vigilati al mercato delle criptovalute, in un contesto non ancora esaustivamente regolamentato, possa causare un aumento dei rischi per la stabilità di tutto il sistema finanziario e del sistema dei pagamenti.

[108] Cfr. Banca d'Italia (2015), "*Avvertenza sull'utilizzo delle cosiddette valute virtuali*", disponibile all'indirizzo: https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf .

L'iniziativa della Banca d'Italia si muove dunque preventivamente sul piano della *soft law*, non ponendo alcun obbligo e divieto, bensì utilizzando un richiamo alla prudenza ed alla consapevolezza dei rischi, nonché esternando loro la *policy* interna e preavvisandoli che un eventuale coinvolgimento nel mercato delle valute virtuali potrebbe essere controbilanciato dall'assunzione da parte dell'Autorità di vigilanza di specifiche misure di carattere prudenziale, volte a prevenire e contenere il rischio[109]. L'unica parte della comunicazione che ha carattere prescrittivo è quella riguardante gli obblighi informativi sull'orientamento della Banca d'Italia già accennati, oltre che l'ovvia conferma che chi farà uso delle criptovalute dovrà rispettare le norme presenti per le normali valute legali.

Sul piano fiscale, la questione relativa alle modalità di considerazione delle criptovalute ha trovato una prima regolamentazione ufficiale nella risoluzione 72/E/2016 con cui l'Agenzia delle Entrate, in linea con i recenti orientamenti della Corte di Giustizia dell'UE, illustra il trattamento fiscale da applicare a chi svolge attività di acquisto e cessione di moneta virtuale in cambio di valuta *standard*. Per i clienti persone fisiche che detengono i bitcoin al di fuori dell'attività d'impresa, si ritiene che si tratti di operazioni a pronti che non generino redditi imponibili, poiché manca la finalità speculativa. In questo caso, ne deriva che gli operatori non sono tenuti agli adempimenti tipici dei sostituti d'imposta e, si precisa, che a queste operazioni non si applica l'Iva. Resta oltremodo ferma la facoltà dell'Agenzia di acquisire le liste della clientela per le opportune verifiche nell'espletamento delle normali attività di controllo.

Per ciò che concerne le attività di intermediazione di valute tradizionali con bitcoin, svolta in modo professionale ed abituale, queste non scontano l'Iva in quanto il loro operato rientra tra le operazioni relative alle monete e alle banconote; tuttavia, costituiscono attività rilevante di IRES ed IRAP, al netto dei relativi costi inerenti a detta attività. Per valutare i bitcoin di cui la società dispone a fine esercizio occorre considerarne il valore normale, cioè la miglior quotazione disponibile sul mercato in quel momento. In particolare, si è ritenuto che l'attività remunerata attraverso commissioni pari alla differenza tra l'importo corrisposto dal cliente e la suddetta miglior quotazione reperita sul mercato, debba essere considerata ai fini IVA quale prestazione di servizi esenti ai sensi dell'art. 10 D.P.R. n. 633/1972.

Conclusioni

Nell'era della crisi economico-finanziaria, Bitcoin si propone come un sistema monetario alternativo intenzionato a scardinare gli equilibri economici, politici e persino sociali. La sfida è impostata specialmente come una radicale critica alle Banche Centrali ed a tutti gli organi di controllo centrali, rei di aver avvelenato

[109] Cfr. La Rocca L. (2015), "*La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*", Analisi giuridica dell'Economia, Il Mulino, pp. 201-220

l'economia globale mediante la manipolazione dell'offerta monetaria, ritenuta inefficiente e oltremodo legata a logiche affaristiche. Attraverso un sistema di transazioni *peer-to-peer*, regolato da un protocollo informatico, Bitcoin si presenta, simultaneamente, come una valuta-unità di conto ed un sistema di pagamento indipendente da ogni controllo centralizzato, ponendo al centro del suo funzionamento l'intera community degli utilizzatori (altresì detti "nodi" della rete).

Tuttavia, lo scenario aperto da Bitcoin e dalle altre valute virtuali genera allo stesso tempo delle opportunità e dei rischi. L'obiettivo dichiarato di questa trattazione era infatti quello di analizzare alcuni punti deboli di Bitcoin. A tal fine, nel secondo capitolo è stata impostata un'analisi comparativa del Bitcoin con le valute a corso legale, al fine di dimostrare, da un punto di vista prettamente economico, che questi può difficilmente imporsi in futuro come moneta alternativa: dal confronto effettuato, il *token* bitcoin non sembra poter essere abbastanza forte da esser parificato alle valute a corso legale, poiché non espleta pienamente le comuni funzioni di una moneta, quali mezzo di scambio, unità di conto e riserva di valore. Una particolare menzione deve essere posta sull'eccessiva volatilità del prezzo della valuta, connessa ad una serie di dubbi riguardanti la sicurezza informatica e sulle (mancate) tutele garantite agli utilizzatori.

Dallo studio effettuato nella prima e nella seconda parte della trattazione, si può asserire che il futuro di Bitcoin non risiede tanto nelle caratteristiche del *token*, quanto più sulle novità introdotte dalla tecnologia che ne sta alla base. Le inedite funzionalità della blockchain, in particolare, ben si prestano ad applicazioni di svariato tipo e che possono offrire un contributo tangibile allo sviluppo in campo giuridico, commerciale ma anche sociale, ed un chiaro esempio è fornito da alcune nuove *alt-coin* entrate sul mercato successivamente a Bitcoin. Invero, date le difficoltà nel qualificare bitcoin come una moneta in senso lato, si potrebbe al più parlare di moneta complementare, ossia uno strumento di commutazione con cui è possibile scambiare beni e servizi che si affianca il denaro ufficiale. La base a fondamento della moneta complementare non è la sua dimensione pubblica e legale, ma quella più propriamente contrattuale degli accordi, anche di tipo associativo, a sostegno della sua emissione ed accettazione quale mezzo di pagamento. In altre parole, le monete complementari aderiscono alla definizione antica di denaro, ossia un accordo all'interno di una comunità che accetta di utilizzare qualcosa come bene di scambio riconosciuto, ed in quest'ottica Bitcoin sembra potersi inserire discretamente bene. L'emissione di valute complementari può essere operata da diverse tipologie di soggetti, quali ad esempio cooperative, associazioni, ma anche aziende che offrono un servizio a cui aderiscono persone fisiche ed altre aziende. Si pensi ad esempio al Sardax, una moneta complementare nata nel 2009 in Sardegna molto simile al Bitcoin per la caratteristica di poter circolare soltanto sul *web*, seppur utilizzabile soltanto dalle piccole e medie imprese con funzione di mutuo soccorso.

Il secondo problema analizzato riguarda il crescente uso illecito di Bitcoin, e di molte altre criptovalute, all'interno di pratiche di riciclaggio di denaro sporco e di finanziamento al terrorismo. La questione riguarda

essenzialmente il luogo ove si svolgono queste transazioni, il *dark web*, che per sua natura rende altamente difficile, se non impossibile, il monitoraggio di ogni singola operazione finalizzato a riconoscere ed a tracciare i capitali delittuosi. È stata osservata, difatti, una diversificazione sempre più sofisticata delle tecniche adottate all'interno dell'ecosistema criminale per riciclare i proventi illeciti e per occultare i movimenti di capitali. Appare dunque sensata, almeno in ottica di breve periodo, la decisione della Commissione Europea di concentrare l'intervento normativo sui nodi che legano il mondo virtuale ed il mondo legale, gli *exchanger*, allargando a questi i comuni obblighi di adeguata verifica della clientela, di registrazione dati e di comunicazione delle operazioni sospette alle autorità competenti.

Tuttavia, l'intervento della Commissione Europea deve essere considerato solamente come l'inizio del processo di regolamentazione del mondo delle criptovalute. Permangono difatti questioni ancora irrisolte. In primo luogo, bisogna osservare che la maggior parte delle operazioni occulte si svolte al di fuori dei traffici gestiti dagli organismi di *exchange*. In secondo luogo, come accolto anche da una seconda *opinion on virtual currencies*[110] dell'EBA indirizzata alla Commissione, al Parlamento e al Consiglio dell'Unione Europea, la possibilità di lasciare ai singoli Stati Membri la scelta di assoggettare le valute virtuali ad un regime di licenza o di registrazione rischia di minare lo scopo della direttiva e delle sue modifiche; occorrerebbe, pertanto, far luce su quale tra i due regimi sia il più adatto a realizzare lo scopo della direttiva e, ove ciò non sia possibile, di chiarire almeno i requisiti minimi dei regimi di licenza o di registrazione nazionali. Infine, spostando l'attenzione dal quadro europeo a quello internazionale, occorre precisare che, data la natura globale delle criptovalute, ogni sforzo può risultare vano senza un inquadramento normativo comune tra tutti gli ordinamenti. A tal proposito, ci si trova particolarmente in accordo con le posizioni assunte dall'EBA, e si sostiene che l'introduzione di un organismo non governativo che regoli e controlli l'utilizzo di un *virtual currency scheme* sia assolutamente necessario, supportato inoltre dalla creazione di un istituto giuridico *ad hoc* il più possibile condiviso a livello internazionale ed adatto alla natura delle valute virtuali.

Per concludere, nelle attività di prevenzione e monitoraggio si profila un ruolo di crescente rilevanza per le agenzie di supporto private, quali ad esempio Elliptic e Chainalysis, in forza di conoscenze specifiche e *software* dedicati al riconoscimento degli schemi di riciclaggio che spesso mancano alle forze dell'ordine.

[110] Cfr. EBA (2016), "*Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)*", disponibile al sito: https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD.

Riferimenti Bibliografici

Amato M. e Fantacci L., (2016) "*Per un pungo di Bitcoin*", Egea, Università Bocconi Editore, Milano;

Banca d'Italia (2015), "*Avvertenza sull'utilizzo delle cosiddette valute virtuali*", disponibile all'indirizzo: https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf;

Bohr J. e Bashir M. (2014), "*Who Uses Bitcoin? An exploration of the Bitcoin community*", Privacy, Security and Trust (PST), Twelfth Annual International Conference on. Toronto, Canada;

Bouri et al (2017), "*Bitcoin for energy commodities before and after the December 2013 crash: diversifier, hedge or safe haven*?", Applied Economics, DOI: 10.1080/00036846.2017.1299102;

Caetano R. (2016), "*Bitcoin. Guida all'uso delle criptovalute*", Apogeo, Milano;

Cano A. (2014), "*Problemi evolutivi e nuove prospettive in tema di riciclaggio di denaro, beni o altre utilità*", inCassazione Penale 2014, fasc. 6;

Capoti D., Colacchi E. e Maggioni M. (2015), "*Bitcoin Revolution: La moneta digitale alla conquista del mondo*", Ulrico Hoepli Editore S.p.A., Milano;

Ciaian, P., Rajcaniova, M. & Kancs (2016), "*The digital agenda of virtual currencies: Can BitCoin become a global currency?*", Inf Syst E-Bus Manage (2016) 14: 883;

Commissione Europea (2016), "*Proposta di Direttiva del Parlamento Europeo e del Consiglio che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica la direttiva 2009/101/CE*", Strasburgo, COM (2016) 450 final, 2016/0208 (COD);

Dagnino A. Gulmanelli S. (2003), "*Pop War, il Net Attivismo contro l'Ordine Costituit*o", Apogeo Editore;

De Collibus F. e Mauro R. (2016), "*Hacking finance. La rivoluzione del bitcoin e della blockchain*" - Agenzia X;

EBA (2016), "*Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)*", disponibile al sito: https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD;

Faiella S. (2014), "*Riciclaggio e crimine organizzato transnazionale*", Giuffrè;

Florindi E. (2016), "*Deep web e bitcoin: Vizi privati e pubbliche virtù della navigazione in rete*", Imprimatur Editore;

Galullo R. e Mincuzzi A. (2017), "*Bitcoin, il riciclaggio invisibile di mafie e terrorismo internazionale*", Il sole 24 ore, disponibile a: http://www.econopoly.ilsole24ore.com/2016/07/08/bitcoin-e-antiriciclaggio-i-primi-passi-delleuropa-per-un-quadro-legislativo/.

Gasparri G. (2015), "*Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*", Diritto dell'informazione e dell'informatica, 31(3), 415-442;

GAFI/FATF Report (2014), "*Valute Virtuali, definizioni chiave e potenziali rischi in ambito antiriciclaggio e finanziamento del terrorismo*", http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf ;

Hanley, Brian P. (2013); "*The false premises and promises of Bitcoin*"; eprint arXiv:1312.2048;

Hayes A. S. (2016), "*Cryptocurrencies Value Formation: An Empirical Study Leading to a Cost of Production Model for Valuing Bitcoin*", Telematics and Informatics. Doi: 10.1016/j.tele.2016.05.005;

Jay Palmer Fawcett (2016), "*Bitcoin regulations and investigations: A proposal for U.S. policies*", ProQuest LLC, Ann Arbor;

Jaromil Roio Denis (2014), "*Bitcoin, la fine del tabù della moneta*", http://effimera.org/bitcoin-la-fine-del-tabu-della-moneta-di-denis-jaromil-roio/ ;

La Rocca L. (2015), "*La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*", Analisi giuridica dell'Economia, Il Mulino, pp. 201-220;

Lemme G. e Peluso S. (2016), "*Criptomoneta e distacco dalla moneta legale: il caso bitcoin*", in Riv. dir. banc., dirittobancario.it, 43;

Luther W. L. (2016), "*Bitcoin and the Future of Digital payments*", The Indipendent Review, v.20, n.3, ISSN 1086-1653, pp.397-404;

Mancini M. (2015), "Valute virtuali e Bitcoin", Analisi giuridica dell'economia, Il Mulino, pp. 117-138;

Mandjee T. (2016), "*Bitcoin, its Legal Classification and its Regulatory Framework*", 15 J. Bus. & Sec. L. 157, Available at: http://digitalcommons.law.msu.edu/jbsl/vol15/iss2/4;

Nakamoto S. (2008), "*Bitcoin: un sistema di contanti elettronico peer-to-peer*", www.bitcoin.org ;

Nigel Dodd (2017), "*The social life of Bitcoin*", Theory, Culture & Society. ISSN 0263-2764;

Pagni L. (2017), "*Bitcoin, quotazione record: il vento d'Oriente spinge la moneta virtuale*", Repubblica, Economia & Finanza, http://www.repubblica.it/economia/finanza/2017/05/30/news/bitcoin-166654682/?ref=RHPPBT-VE-I0-C6-P8-S1.6-T1;

Passerelli, N. (2016), "*Bitcoin e antiriciclaggio*", Sistema di Informazione per la Sicurezza della Repubblica, www.sicurezzanazionale.gov.it ;

Pezzuto A. (2017), "*Profili evolutivi della legislazione in materia di antiriciclaggio e contrasto al finanziamento del terrorismo*", disponibile al sito: http://www.dirittobancario.it/approfondimenti/antiriciclaggio/profili-evolutivi-della-legislazione-materia-di-antiriciclaggio-e-contrasto-al-finanziamento ;

Razzante R. (2014), "*Il riciclaggio come fenomeno transnazionale. Normative a confronto*", Giuffrè;

Vangone G. (2015), "*Il terrorismo islamico nell'era di Internet, fra bitcoin e dark web*", Eastonline, http://eastwest.eu/it/opinioni/open-doors/il-terrorismo-islamico-nell-era-di-internet-fra-bitcoin-e-dark-web ;

Wile R. (2013), "*927 People Own Half of All Bitcoins*", Business Insider, 10 dicembre, http://www.businessinsider.com.

Riassunto

Una delle più interessanti novità apportate dalla rivoluzione informatica riguarda le nuove opportunità nate nel campo dei sistemi di pagamento, su tutte quelle legate alle c.d. valute virtuali (o criptovalute). Le valute virtuali hanno difatti catturato via via un sempre maggior interesse, poiché introducono tecniche altamente innovative per le operazioni di pagamento e di trasmissione di moneta, elevandosi inoltre a portatrici di idee radicalmente rivoluzionarie non solo in ambito economico ma anche sociale e geopolitico.

Bitcoin è il sistema di pagamento alternativo più diffuso ed è basato sul concetto di *distributed ledger technology*, o blockchain: una rete di scambi *peer to peer* in cui non vi è un'autorità centrale incaricata di convalidare e registrare le transazioni; è inoltre un sistema basato su di un *software open-source*, ossia non protetto da *copyright* e nel quale gli utenti stessi possono apportare migliorie, contribuendo alla sua evoluzione ed al suo perfezionamento. Nato nel 2009 attraverso la pubblicazione *online* di un Protocollo informatico ad opera dello sconosciuto programmatore Satoshi Nakamoto, la valuta virtuale ha conquistato un'attenzione crescente presso gli operatori del settore e, complice anche il *boom* osservato agli inizi del 2017 che ha permesso alla valuta raggiungere una quotazione pari a quasi 3.000 dollari, ad oggi deve necessariamente essere considerato una piccola realtà. Seppur con l'alternanza di fasi di espansione e di depressione e sebbene non sia comparabile alle valute virtuali in quanto a diffusione ed utilizzo, Bitcoin è andato continuamente ad apprezzarsi nel tempo e, parallelamente, è osservabile una crescita ininterrotta (nemmeno nelle fasi più "buie" della sua breve storia) dei principali indicatori economici, come ad esempio il numero di indirizzi bitcoin della rete o di transazioni giornaliere, nonché dell'interesse mediatico, dottrinale e giuridico.

L'innovazione più dirompente è sicuramente la sopracitata blockchain, una sorta di libro contabile virtuale che tiene nota di tutte le transazioni effettuate in bitcoin. La blockchain è pubblicamente consultabile, ogni transazione è perfettamente visibile e, seppur protetta dallo pseudonimo, è sempre possibile tracciare l'identità delle parti coinvolte, quantomeno in via teorica. Inoltre, al di là della funzione attribuita da Bitcoin, la blockchain si presta ad innumerevoli altre applicazioni, spesso sfruttate da altre criptovalute nate successivamente, poiché aggiunge una componente non indifferente di maggior trasparenza e di efficienza nella gestione dei costi attraversi la crittografia.

Proprio con riguardo a quest'ultima, Nakamoto è riuscito a proporre per la prima volta un sistema che risolva il problema della *double spending* (ossia, il processo mediante il quale si rende possibile duplicare lo stesso gettone e spenderlo due volte) in modo distribuito, senza ricorrere a nessun organismo centrale come un intermediario. Il sistema si avvale di un meccanismo di chiave doppia, pubblica e privata: utilizzando la chiave privata questi può sottoscrivere la transazione, apponendo una sorta di "firma digitale". Il destinatario della transazione potrà ricevere ed usufruire dei bitcoin solo successivamente alla validazione della rete, grazie al

"prezioso" supporto dei cosiddetti "*miner*". L'attività di validazione delle transazioni è strettamente connesso con il meccanismo di emissione (o "estrazione") monetaria, chiamato *mining process*. I minatori sono nodi che mettono la loro potenza computazionale a disposizione della rete e, attraverso la risoluzione di un problema matematico, validano un blocco di transazioni e vengono ricompensati attraverso un'elargizione di nuovi bitcoin, "appena creati". Un fenomeno piuttosto comune è l'associazione di *miner* in consorzi, i cosiddetti *mining pool*, volti a contenere i costi dati dai crescenti bisogni di potenza computazionale ed energia elettrica. Tuttavia, in linea teorica i *mining pool* pongono il sistema al rischio di un controllo monopolistico di tutta la rete da parte di coloro che "estraggono" la maggioranza dei bitcoin. Questo rischio è stato affrontato anche dallo stesso Protocollo, attraverso un sistema di incentivi/disincentivi, che tuttavia non ne pone completamente al riparo la rete.

Le operazioni di ricompensa continueranno fintantoché non sarà raggiunta la quota di 21 milioni di bitcoin in circolazione. Difatti, la quantità di moneta in circolo è stata preventivamente decisa e bloccata attorno ad un ammontare certo. Quest'ultima decisione è spiegata dall'ideologia su cui si poggia tutto il Sistema. Bitcoin si pone come un'alternativa al sistema delle banche e in generale all'uso degli intermediari. Alla sua base vi è un contrasto di fondo degli sviluppatori con la politica monetaria attuata dalle Banche Centrali, giudicata essenzialmente inefficace nel condurre il proprio compito (ricercare la stabilità dei prezzi, favorire lo sviluppo economico…). Secondo i sostenitori di Bitcoin, le banche appaiono sempre più chiaramente come portatrici di un potere oligopolistico, beneficiarie di aiuti statali immeritati, usurpatrici di un bene comune (la politica monetaria), giustificate dal fatto di svolgere una funzione tipicamente pubblica ma che sembrano sempre meno efficienti a svolgere. Per ovviare a tali problematiche, Bitcoin propone una soluzione radicale: rendere la moneta completamente esogena al sistema di scambi che è chiamata a gestire e privarla dal controllo "umano". La caratteristica del bitcoin di essere un valore attivo del possessore senza essere un passivo per un altro soggetto va letta proprio in quest'ottica: in tal modo si impedisce che la moneta possa essere creata dal sistema bancario attraverso la moltiplicazione dei depositi e dunque si priva l'ente centrale di iniettare nuova liquidità nel sistema a seconda delle proprie esigenze. L'indipendenza dal controllo umano è inoltre frutto dell'idea che questi non sia tanto affidabile quanto possa esserlo il *software* informatico: Bitcoin predilige l'affermazione di un sistema *trust-less*. Ciononostante, in questa sede si ritiene che, piuttosto che ad una generica mancanza di fiducia, si assiste di fatto ad un trasferimento di questa, sotto un duplice punto di vista. In prima istanza, si tratta di un trasferimento di fiducia dall'uomo all'informatica: in sostanza Bitcoin chiede che gli utilizzatori "si fidino" del codice sorgente, del suo meccanismo di funzionamento imparziale e neutrale, incapace di piegarsi alle logiche monopolistiche tipiche delle Banche Centrali. In seconda istanza, si segnala un trasferimento dall'individuo alla collettività, rappresentata da tutta la *community*. Quest'ultimo punto è di interesse centrale, poiché alla Rete è stato concesso un ruolo di primissimo piano. Si palesa dunque la necessità di un'onestà di fondo non più di un

soggetto od un ristretto gruppo di soggetti, ma della *community* nella sua interezza (o quantomeno della maggioranza dei suoi nodi). In altre parole, si tratta di una fiducia rimessa all'idea che un gruppo di persone (tutta la rete Bitcoin) possa avere la capacità di organizzarsi, di autogestirsi, di adattarsi di volta in volta alle contingenze provenienti dal mondo "esterno".

Il distacco di Bitcoin dal sistema bancario si realizza ulteriormente con la modalità di conservazione di moneta. I bitcoin sono difatti conservati in "*wallet*", una sorta di portafoglio informatico composto da un file criptato accessibile solo possedendo la relativa *password*. Ciò significa, anche in questo caso, che non vi è alcun ente terzo demandato alla gestione ed alla protezione delle monete di proprietà, favorendo il completo controllo da parte degli utenti sui propri bitcoin ed i propri *account*. I *wallet* sono conservabili su supporto fisico (*cold storage)* e su supporto virtuale (*hot storage*), circostanza che, anche in virtù di una maggiore esposizione a furti informatici, ha visto nascere una serie di società e di piattaforme dedicate che offrono servizi di gestione e di protezione dei portafogli *online*.

Tuttavia, a fronte di indiscutibili potenzialità, il sistema Bitcoin è affetto da diverse problematiche, che possono costituire un limite alla sua diffusione e necessitano una più approfondita analisi. Innanzitutto, il quesito converge sulla capacità del bitcoin-*token* di svolgere correttamente la funzione monetaria, in modo da potersi positivamente affermare in futuro come una vera e propria moneta. Il problema risiede essenzialmente nella natura ibrida del bitcoin, poiché non è assimilabile ad una moneta merce, priva com'è di qualsivoglia valore intrinseco, né tantomeno ad una moneta a corso legale, poiché manca il riconoscimento da parte del legislatore che ne regola la stabilità e ne assicura l'accettazione come mezzo di pagamento. Ciò non toglie, in linea di principio, che il bitcoin non possa comunque di assurgere, potenzalmente, ad essere una buona moneta. Per comprendere se sia effettivamente possibile accettare una simile parificazione, si è deciso di impostare un'analisi comparativa con le maggiori valute a corso legale, in relazione alle tre funzioni tipiche svolte da una moneta (mezzo di scambio, unità di conto e riserva di valore). Ciò al fine di identificare i punti di forza e di debolezza relativi della valuta virtuale.

Il quadro che ne deriva, tuttavia, è tutt'altro che positivo. In accordo con la posizione assunta dalla Banca Centrale Europea ("*Virtual Currency Schemes – a further analysis*"), il bitcoin assolverebbe soltanto parzialmente alle tre sopracitate funzioni monetarie necessarie. Le problematiche riconosciute sono legate non soltanto alla mancanza di un riconoscimento legale, che appunto pone la sua adozione alla spontaneità degli attori, ma soprattutto alla qualità di preservare il proprio valore nel tempo e di configurarsi come una riserva di valore affidabile. La mancanza di un'adeguata struttura di diritti e tutele nei confronti degli utilizzatori è un freno ad un ipotetico riconoscimento legale. Allo stato attuale, il *software* può aiutare ad evitare errori di battitura e destinatari sbagliati ma, complice anche la mancanza di una legislazione *ad hoc* in materia, non c'è un'autorità a cui potersi rivolgere in caso di qualunque controversia, che possa riguardare un inadempimento,

una frode o molto più banalmente un errore umano. Onde per cui l'unica soluzione sembra essere una correzione volontaria da parte delle stesse parti coinvolte nello scambio. Gli attori, inoltre, non possono sentirsi al riparo da frodi e inadempimenti e dalle conseguenti perdite di ricchezza. Si pensi ad esempio al fallimento di una piattaforma di mercato, circostanza che si è verificata in più occasioni, o ad attacchi informatici. Ed in effetti attualmente non ci sono e non possono essere date garanzie sulla sicurezza del sistema nel suo complesso, sebbene la *community* bitcoin si stia evolvendo per garantire una sempre maggior protezione dei suoi utenti.

L'esponenziale volatilità del tasso di cambio è, con ogni probabilità, la differenza maggiore che intercorre con le monete tradizionali e che risulta essere il limite più grande nell'affermazione futura del bitcoin. Una moneta con una forte volatilità di breve periodo non può infatti essere considerata una buona unità di conto, in quanto le fluttuazioni del prezzo rendono difficile quantificare e bloccare il valore di un prodotto attorno ad un "numero" certo. Una volatilità che, tra l'altro, pregiudica anche la capacità di bitcoin di fungere da riserva di valore. Le continue oscillazioni del valore unite ad una forte incertezza sui sentieri evolutivi del valore danneggiano, di fatto, gli stessi possessori di bitcoin, mentre risulta essere un vantaggio per gli investitori che vedono in bitcoin un mero strumento speculativo. Proprio in ragione di ciò, occorre osservare che il bitcoin è spesso utilizzato con finalità diverse dalla semplice regolazione di scambi commerciali: con le dovute ponderazioni, il numero di transazioni in bitcoin risulta relativamente basso rispetto alle transazioni svolte nelle valute a corso legale. Difatti, si presume che la maggior parte degli utenti predilige sia gli investimenti speculativi, volti a trarre profitto dalle forti oscillazioni di prezzo, sia l'accumulazione di moneta. Infatti, se a fronte di un aumento futuro della domanda il numero totale di bitcoin sarà sempre limitato alle famose 21 milioni di unità, non può che profilarsi un futuro deflazionistico; in altre parole, piuttosto che perdere valore, come la maggior parte delle valute a corso legale, il bitcoin avrà la tendenza ad apprezzarsi nel tempo. Questa capacità renderebbe il bitcoin, al pari dell'oro, più utile in ottica di accumulazione che di circolazione nel sistema economico, con conseguenti effetti negativi sulle prospettive di crescita e di sviluppo dello stesso.

Inoltre, si osserva che anche le caratteristiche che potenzialmente potrebbero garantire un vantaggio competitivo considerevole, come il basso costo delle transazioni o la pressoché infinita divisibilità, in realtà nascondono insidie che tendono a controbilanciare gli effetti positivi. Da un lato, le commissioni si pagano in proporzione sia al peso in *bytes* della transazione, sia al numero di indirizzi in cui è suddiviso l'importo da pagare, a prescindere dal fatto che spostino un valore di miliardi di euro o pochi centesimi; questo rende le transazioni di piccolo importo solitamente poco convenienti. D'altra parte, l'enorme divisibilità può avere un riscontro negativo sui consumatori, in quanto foriera di confusione e di problemi legati alla comprensione nel comparare i prezzi di beni e servizi. Infine, la stessa rapidità delle validazioni, ampiamente pubblicizzata come punto di forza del Sistema Bitcoin, non risulta pienamente efficiente nelle transazioni per così dire "quotidiane"; inoltre, la crescente difficoltà nella risoluzione dei blocchi da parte dei minatori espone ad un rallentamento di pratiche

di inserimento delle transazioni nella blockchain e, in relazione, ad probabile un minor utilizzo nelle pratiche commerciali.

Date le difficoltà nel qualificare bitcoin come una moneta in senso lato, si potrebbe al più parlare di moneta complementare (es. il Sardax), ossia uno strumento di commutazione con cui è possibile scambiare beni e servizi che si affianca il denaro ufficiale. La base a fondamento della moneta complementare non è la sua dimensione pubblica e legale, ma quella più propriamente contrattuale degli accordi, anche di tipo associativo, a sostegno della sua emissione ed accettazione quale mezzo di pagamento. L'emissione di valute complementari può essere operata da diverse tipologie di soggetti, quali ad esempio cooperative, associazioni, ma anche aziende che offrono un servizio a cui aderiscono persone fisiche ed altre aziende. Infine, vi sono altri scenari ove la criptomoneta può giocare un ruolo più importante anche nell'immediato futuro. Ci si riferisce in particolar modo a quei paesi in cui la valuta nazionale è debole e soggetta a forti scosse inflazionarie, come per esempio Argentina e Venezuela, oppure a paesi dove il sistema bancario non è radicato, come alcuni stati africani. In Kenya, ad esempio, la gran parte della popolazione non è cliente di alcuna banca ma possiede un telefono cellulare; in concomitanza con una valuta nazionale instabile, gli utenti potrebbero optare di utilizzare i propri cellulari per scambiarsi appunto criptomonete.

Un secondo, grande problema riguardante il sistema Bitcoin riguarda il suo sfruttamento all'interno dell'ecosistema criminale. Nel tempo si è assistito ad un'evoluzione delle tecniche di *money laundering*, legate alla dissimulazione di capitali di origine illecita o per finalità illecite. Contestualizzando, la lotta al riciclaggio è tipicamente articolata in due sistemi, ossia sistema di contrasto e sistema di prevenzione. Il primo ha finalità di repressione delle attività di riciclaggio, dell'impiego di denaro di provenienza illegale e dell'auto-riciclaggio. Le attività di prevenzione, invece, mirano ad intercettare in maniera anticipata le infiltrazioni criminali nel sistema economico legale. Altrettanto importante è la raccolta di dati e informazioni sensibili relative alle transazioni ed alle parti coinvolte, soprattutto se in queste intercorrono diversi soggetti intermedi, quali possono essere agenti di cambio o piattaforme di scambio. Inoltre, è necessario monitorare continuamente le suddette transazioni, le tipologie di rapporti tra le parti coinvolte ed i volumi delle operazioni.

La rivoluzione informatica ha invero aperto ad una molteplicità di nuovi stratagemmi per aggirare le legislazioni antiriciclaggio in vigore. La maggior parte di queste operazioni si articola sul *dark web*, un sottostrato nascosto del *web*, che consente una maggior protezione della identità e dei movimenti dei navigatori ed è accessibile solo attraverso specifici *broswer* (come ad esempio TOR). Si stima che il 90 per cento degli indirizzi *web* attivi sul *dark web* siano piattaforme dedite ad attività illegali od immorali, le quali sono tra l'altro finanziate principalmente con criptovalute. Nel sistema Bitcoin, l'assenza di intermediari finanziari, unito alla natura pressoché anonima delle transazioni, rischia di favorire operazioni di riciclaggio, oltre che di finanziamento al terrorismo, in quanto viene a mancare quell'organismo che, nell'economia tradizionale, funge da controllore e

segnalatore di attività sospette alle autorità competenti. Al contempo, con un sistema finanziario che presenta interconnessioni su scala globale, è facile nascondere e trasferire fondi in tutto il mondo creando in maniera semplice e rapida una struttura stratificata di società di comodo che operano attraversando le frontiere e le giurisdizioni, rendendo così estremamente difficile rintracciare la vera origine del denaro per le forze dell'ordine. Il connubio bitcoin - *dark web* permette ai criminali di ideare strategie che coinvolgono tutte le fasi dell'attività di riciclaggio (riciclaggio digitale integrale). Si guardi, ad esempio, alle operazioni svolte tramite piattaforme come Local Bitcoins, che permettono transazioni *peer to peer* anonime abilmente sfruttate dai criminali per liberarsi del denaro di provenienza illecita in cambio di bitcoin (*placement recycling*); nel mentre, attraverso le c.d. operazioni di *tumbling,* i criminali riescono ad ostacolare la ricostruzione investigativa dei flussi finanziari da parte delle forze dell'ordine e mascherarne l'origine criminale (*layering recycling*); infine, si reintroducono i capitali nell'economia legale sfruttando, ad esempio, alcune piattaforme di gioco d'azzardo *online* e giustificare le rendite come vincite.

La sfida per le autorità e per le forze dell'ordine si articola su più punti. In primo luogo, è riscontrata una generale mancanza di risorse e di conoscenze specifiche per affrontare efficacemente la nuova sfida posta dalle criptovalute e dal *dark web*. La difficoltà risiede essenzialmente nella mancanza di un adeguato addestramento e dei *software* specifici per riconoscere e contrastare le nuove tecniche utilizzate dai criminali in ambito di illeciti finanziari. Sotto quest'ottica, un ruolo di crescente rilevanza potranno ritagliarselo le agenzie di supporto private, quali ad esempio Elliptic e Chainalysis. In secondo luogo, la struttura decentrata della maggior parte degli schemi di attuazione di operazioni di riciclaggio, come osservato ad esempio nel gioco d'azzardo, impedisce alle singole autorità nazionali di imporre strategie di prevenzione e contrasto pienamente efficaci. Ciò in quanto le singole legislazioni mal si prestano a regolare situazioni ove intervengono entità disperse in diversi Stati; inoltre, la difficoltà raggiunge il suo apice se si guarda alla collocazione geografica degli operatori dell'ecosistema bitcoin, che spesso sfruttano giurisdizioni che non hanno un'adeguata normativa antiriciclaggio. Quel che è necessario è un'armonizzazione degli ordinamenti, che deve esplicarsi non soltanto nelle misure per così dire "operative", ma deve necessariamente partire dall'adozione di una definizione il più possibile condivisa di criptovaluta. Si deve iniziare, in altre parole, con una determinazione univoca della natura di Bitcoin, per proseguire, in seguito, con l'impostazione di uno schema normativo condiviso adatto a contrastarne gli usi illeciti. Una definizione comune che può quindi sollevare il legislatore dell'annoso problema di dover forzatamente ricondurre le criptovalute sotto istituti giuridici già esistenti, che non risultano essere pienamente compatibili anche in virtù della natura "ibrida" di questi strumenti. Si sostiene, nella pratica, che possa essere necessario valutare la creazione di un istituto giuridico *ex-novo*, il più possibile adeguato alla natura delle criptovalute e che punti a contenere le asimmetrie presenti tra gli ordinamenti. In ultima istanza, l'obiettivo principale delle linee guida dovrebbe essere quello di trovare il giusto equilibrio fra il garantire lo sviluppo di

sistemi che possono aumentare l'efficienza dei mercati finanziari ed incoraggiare lo sviluppo economico, e la necessità di salvaguardare l'integrità stessa dei mercati, ponendo limiti, regole di prevenzione e repressione dei comportamenti potenzialmente dannosi.

I rischi finora esposti hanno messo in allarme le Autorità internazionali ed europee. Il GAFI (Gruppo di Azione Finanziaria Internazionale), attraverso la pubblicazione di un *report* nel 2014, ha sottolineato la pericolosità delle criptovalute, con specifico riferimento a Bitcoin; difatti in questi si può leggere: «Le valute virtuali e i bitcoin in particolare sono l'ondata del futuro per i sistemi di pagamento e forniscono un nuovo e potente strumento per i criminali, terroristi, finanzieri ed evasori, consentendo loro di far circolare e conservare fondi illeciti, fuori dalla portata del diritto». L'obiettivo dichiarato dal Gruppo, perseguito attraverso raccomandazioni atte ad influenzare gli interventi normativi nazionali ed a favorire la sopracitata armonizzazione, consiste nel favorire di misure di prevenzione proporzionate da parte dei soggetti obbligati, a cui devono provvedere gli ordinamenti nazionali con disposizioni legislative *ad hoc* ma coerenti con il quadro delineato a livello internazionale.

Di pari passo, anche l'EBA ha iniziato ad interessarsi alle criptovalute a partire dal settembre 2013, per promulgando una propria "*opinion on virtual currencies*" nel luglio 2014: sulla base di un'accurata analisi costi/benefici, l'EBA ha sostenuto che i rischi derivanti dall'uso delle valute virtuali superassero, all'epoca, i vantaggi che gli utilizzatori avrebbero potuto ricavare da un loro utilizzo, sollecitando inoltre le Istituzioni europee a promuovere una duplice risposta regolamentare. L'approccio suggerito dall'EBA si predispone difatti su due binari, di lungo e di breve periodo. In un'ottica di lungo periodo, l'EBA ha proposto di adottare un quadro normativo quanto più possibile armonizzato, al fine di contenere i rischi individuati; viene a tal fine raccomandata l'introduzione di una specifica regolamentazione attraverso uno schema di *governance authority*, incaricata di stabilire regolare l'utilizzo della criptovaluta ed assicurare l'integrità del sistema. Si profila inoltre un regime autorizzativo per i partecipanti al mercato delle criptovalute. Contemporaneamente, nel breve periodo l'EBA ha invitato le istituzioni europee a mitigare i rischi che derivano dall'interazione delle criptovalute ed il sistema finanziario; nello specifico, si suggerisce di far ricadere sotto la disciplina comunitaria di antiriciclaggio e di contrasto al finanziamento del terrorismo anche gli organismi che offrano servizi di conversione fra valute virtuali e valute reali.

La posizione della Banca d'Italia presenti molti punti in comune con *l'opinion* divulgata dall'EBA, in particolar modo accoglie quella visione delle valute virtuali come "rappresentazioni digitali di valore" e condivide l'obiettivo primario di indurre i soggetti vigilati ad adottare comportamenti ispirati alla massima cautela e ad assumere solo rischi consapevoli e ben ponderati. Difatti, l'acquisto, uso ed accettazione di pagamenti mediante criptovaluta non sono da considerare attività illecite, tuttavia si richiama nuovamente l'attenzione sugli stessi rischi. In ragione di questi, la Banca d'Italia scoraggia le banche e gli altri intermediari vigilati dall'acquistare,

detenere o vendere valute virtuali, sia in virtù dell'assenza di adeguati presidi e di un quadro legale certo circa la natura giuridica delle valute virtuali, sia poiché le concrete modalità di funzionamento degli schemi di valute virtuali possono integrare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati.

Si tratta in ogni caso di meccanismi di *soft law*. Per un intervento legislativo più diretto, a livello comunitario, bisogna attendere l'approvazione della proposta di modifica alla Direttiva 849/2015, con la quale la Commissione propone di inglobare nell'ambito di applicazione della normativa antiriciclaggio anche le piattaforme di scambio di valute virtuali (gli organismi di *exchange*) ed i prestatori di servizi di portafoglio digitale (*custodian wallet provider*). Piuttosto che ad una regolazione diretta delle valute virtuali, l'attenzione si è quindi incentrata su alcuni specifici operatori del settore, che possono rappresentare la determinante essenziale per un intervento efficace e risolutivo, poiché raccolgono una non indifferente mole di dati sensibili derivanti dagli strumenti di pagamento "tracciati". Al fine di armonizzare gli ordinamenti europei e mitigare l'incertezza attorno alla materia, è stata inserita una menzione alla natura delle valute virtuali, definite come una "rappresentazione digitale di valore che non viene emesso da una banca centrale o da un'autorità pubblica e non necessariamente collegato a una moneta a corso legale, ma è accettato da persone fisiche o giuridiche come mezzo di pagamento e può essere trasferita, immagazzinata o scambiata elettronicamente".

Tuttavia, l'intervento promosso dalla Commissione Europea deve essere considerato solamente come l'inizio del processo di regolamentazione del mondo delle criptovalute. In primo luogo, bisogna osservare che la maggior parte delle operazioni occulte si svolte al di fuori dei traffici gestiti dagli organismi di *exchange*. In secondo luogo, come accolto anche da una seconda *opinion on virtual currencies* dell'EBA, la possibilità di lasciare ai singoli Stati Membri la scelta di assoggettare le valute virtuali ad un regime di licenza o di registrazione rischia di minare lo scopo della direttiva e delle sue modifiche; occorrerebbe, pertanto, far luce su quale tra i due regimi sia il più adatto a realizzare lo scopo della direttiva e, ove ciò non sia possibile, di chiarire almeno i requisiti minimi dei regimi di licenza o di registrazione nazionali. Potrebbe inoltre risultare necessario introdurre un organismo non governativo che regoli e controlli l'utilizzo di un *virtual currency scheme*, supportato inoltre dalla creazione di un istituto giuridico *ad hoc* il più possibile condiviso a livello internazionale ed adeguato alla natura delle valute virtuali.