UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

VALUTE VIRTUALI: UTILIZZI ATTUALI E PROSPETTIVE DI SVILUPPO DEI BITCOIN

RELATORE:

CH.MO PROF. FORNI LORENZO

LAUREANDA: MASIN ELEONORA

MATRICOLA N. 1088867

ANNO ACCADEMICO 2016 – 2017

INDICE

INTRODUZIONE

Le moderne tecnologie, supportate da enormi progressi nel campo informatico, hanno un impatto sempre più significativo sull'economia globale, in particolare nella modalità in cui beni, servizi e attività vengono scambiati. Nel corso dei secoli, l'avvicendarsi di differenti valute e metodi di pagamento, generalmente ha contribuito a rendere gli scambi e le transazioni maggiormente efficienti e sicuri.

Il panorama attuale vede l'affacciarsi sul mercato di nuovi alternativi mezzi di pagamento dematerializzati, i quali, rispetto al ristretto ambito delle comunità virtuali in cui erano state inizialmente sviluppati, hanno iniziato a diffondersi sempre più rapidamente e ampiamente nel mondo reale, fino a raggiungere le dimensioni di un fenomeno economico e sociale globale che impone l'attenzione delle autorità e dell'opinione pubblica. Si tratta delle cosiddette valute virtuali, una cui definizione universale deve ancora venirsi a formare, a causa del continuo e rapido mutamento dell'ecosistema in cui si articolano. L'Autorità Bancaria Europea (EBA) ha definito le valute virtuali come rappresentazioni digitali di valore che non sono emesse da una banca centrale o da un'autorità pubblica, né sono necessariamente collegate ad una valuta avente corso legale, ma che vengono utilizzate da una persona fisica o giuridica come mezzo di scambio e che possono essere trasferite, archiviate e negoziate elettronicamente. Queste sono un fenomeno distinto rispetto ai tradizionali strumenti elettronici di pagamento, come carte di credito, carte prepagate e altri strumenti di moneta elettronica, le quali, a differenza delle valute virtuali, si appoggiano, per ogni transazione, ad un conto corrente o ad un intermediario.

Nate negli anni della crisi finanziaria, le valute virtuali, pur essendo accomunate – almeno nelle intenzioni di molti dei loro creatori - da un forte spirito di rivolta verso il monopolio e verso il controllo che gli Stati esercitano sulla moneta, costituiscono un universo estremamente ampio, composito ed in continua evoluzione; infatti, gli schemi di valute esistenti all'agosto 2017 sono 1037[1], più del doppio rispetto a gennaio 2015. All'interno di questo vasto panorama, è dunque necessario tracciare, anzitutto, una linea di demarcazione in funzione del grado di apertura nei confronti dell'economia reale. In primo luogo, secondo una classificazione operata dalla BCE, è possibile distinguere tra:

-valute chiuse o non convertibili: operano solo all'interno di comunità virtuali, quindi la conversione della valuta nella moneta corrente o in altri tipi di valute virtuali, così come l'utilizzo nel pagamento per beni e servizi, al di fuori del dominio virtuale di appartenenza, è

[1] Si tratta, in ogni caso, di un numero in continua evoluzione che può essere aggiornato consultando, ad esempio, il sito web https://coinmarketcap.com.

significativamente ristretto se non nullo (per tali caratteristiche sono quelle, infatti, principalmente utilizzate nei giochi online);

-valute aperte con flussi unidirezionali o a convertibilità limitata: tali unità possono essere acquistate utilizzando moneta legale, e ciò implica un tasso di conversione reale per entrare in possesso della suddetta valuta, ma non possono essere rivendute. Conseguentemente vengono adoperate per comprare beni e servizi virtuali e solo eccezionalmente beni e servizi reali;

-valute aperte con flussi bidirezionali o pienamente convertibili: le unità possono essere acquistate e vendute ad un tasso di cambio fluttuante, utilizzando differenti monete legali. Sono adoperate per acquisire beni e servizi sia reali che virtuali.

Tipicamente, la convertibilità, totale o limitata, di una valuta virtuale è stabilita nelle sue regole di funzionamento, normalmente incorporate nelle procedure del sistema di elaborazione dati, tuttavia è necessario considerare che anche valute virtuali a convertibilità limitata, spesso sono rivendute, in cambio di moneta legale, in mercati secondari o paralleli in cui vengono quotate.

In secondo luogo, un'ulteriore distinzione deve compiersi sotto il profilo tecnologico, fra valute virtuali a schema accentrato e valute virtuali a schema decentrato. In entrambi i casi, il modo in cui queste operano include tre elementi: (i) emissione e redimibilità della valuta, (ii) meccanismi di implementazione e rafforzamento delle regole interne relative all'uso e alla circolazione della valuta, (iii) processi di regolamentazione e pagamento. Le prime si avvicinano maggiormente ai sistemi di pagamento tradizionali e sono caratterizzate da uno schema gestito da un unico amministratore, il quale emette la valuta, stabilisce le regole per il suo utilizzo, mantiene evidenza dei trasferimenti effettuati e gestisce la piattaforma elettronica e l'infrastruttura informatica; fra gli schemi accentrati di valuta virtuale, possono annoverarsi, ad esempio, il Ripple e il Second Linden Dollar. Le valute virtuali a schema decentrato invece, tecnicamente più complesse e innovative, affidano l'emissione delle unità di valuta e dello schema a più soggetti operanti collettivamente attraverso la rete in maniera non coordinata; tra queste è possibile menzionare, oltre a Bitcoin - indubbiamente la più importante - Litecoin, Namecoin, Primecoin e Nextcoin. Esistono inoltre, degli schemi ibridi in cui alcune funzioni sono delegate ad un'autorità centrale, mentre altre sono lasciate al mercato in cui i partecipanti interagiscono.

Tale elaborato intende approfondire il fenomeno dei Bitcoin, in quanto, all'interno di questo vasto e complesso universo di valute virtuali, si connota senza dubbio tra i più interessanti e, soprattutto, come quello che, molto probabilmente, entrerà a far parte della nostra quotidianità di consumatori.

CAPITOLO 1. COSA SONO E COME FUNZIONANO I BITCOIN

1.1. STORIA E CARATTERISTICHE

Nel corso dei secoli XIX e XX, la maggior parte delle valute erano convertite in base ad un ammontare fisso di oro o altri metalli preziosi, e andando ancora più indietro nel corso della storia, molte monete erano direttamente coniate in oro o argento. La connessione diretta tra la valuta e il metallo prezioso, assicurata dalle riserve auree e monetarie dello Stato, crearono nella popolazione una certa confidenza e familiarità nei confronti delle valute allora correnti. Tuttavia, tra il 1920 e il 1970, l'adozione del gold standard venne abbandonata dalle maggiori economie del mondo, in parte a causa delle ingenti spese militari necessarie per finanziare la Seconda Guerra Mondiale, ma soprattutto perché la produzione mondiale di oro non riusciva a sostenere i ritmi della crescita economica. Da quel periodo in poi, tutti i Paesi delle maggiori economie istituirono una propria moneta a corso forzoso, il cui valore risiede nella convinzione del popolo che il proprio governo o alternativamente, la banca centrale non aumentino troppo rapidamente l'offerta di moneta, portando a gravi crisi inflazionistiche. Infatti, le varie tipologie di valute a corso legale hanno circolato per centinaia di anni, ma quasi tutte almeno una volta hanno visto ridurre drasticamente il proprio potere d'acquisto a causa dell'inflazione, dovuta all'impotenza delle autorità centrali nei confronti di flebili politiche di finanza pubblica.

Il sistema Bitcoin invece, tenta di superare le criticità legate sia alla moneta a corso legale sia al gold standard, basandosi su una valuta algoritmica caratterizzata da un'offerta deterministica e un tasso di crescita vincolato a delle rigide regole matematiche. Essendo tale valuta controllata da regole crittografiche inserite in un contesto decentralizzato e caratterizzato da codici e applicazioni informatiche estremamente trasparenti, nessun governo o autorità centrale ha quindi il potere di controllare l'offerta di bitcoin.

Nel 2008, Satoshi Nakamoto pubblicò sul Web il progetto da lui sviluppato con il titolo "Bitcoin: A peer-to-peer cash system", in cui analizza il sistema di pagamento elettronico peer-to-peer Bitcoin. L'autore, o più probabilmente, gli autori di tale documento non sono ancora stati identificati. La volontà di mantenere l'anonimato affonda le sue radici, infatti, anche nel contesto in cui i bitcoin sono stati fondati, ossia nel periodo più difficile della crisi economico-finanziaria che ha coinvolto l'intero pianeta, proprio quando la fiducia nelle banche e nelle istituzioni era a livelli minimi. La criptovaluta sviluppata da Nakamoto viene eseguita utilizzando un software open-source rilasciato nel 2009 e scaricabile da chiunque.

Bitcoin (codice BTC o XBT) è una moneta digitale che, a differenza della maggior parte delle valute tradizionali, non ricorre ad un ente centrale ma utilizza un database distribuito tra i nodi

della rete che tengono traccia di tutte le transazioni, e sfrutta la crittografia per gestire gli aspetti funzionali, ossia la generazione di nuova moneta e l'attribuzione della proprietà dei bitcoin.
La rete Bitcoin consente il possesso e il trasferimento anonimo delle monete, ed infatti i dati necessari per usufruire dei propri bitcoin sono salvati in uno o più personal computer sotto forma di *digital wallet*. I bitcoin sono trasferiti tramite Internet a chiunque disponga di un indirizzo bitcoin. La struttura peer-to-peer della rete e l'assenza di un ente centrale rende impossibile a qualsiasi autorità il blocco dei trasferimenti, il sequestro dei bitcoin senza il possesso delle relative chiavi o la svalutazione dovuta all'immissione di nuova moneta.
Quindi, le principali caratteristiche su cui si basa questo sistema di enorme successo sono le seguenti:

- Pseudo-anonimo: chiunque può scaricare il software ed iniziare ad effettuare transazioni, senza registrarsi, senza comunicare dati personali e senza svelare la propria identità. È definito pseudo-anonimo in quanto, se non si prendono determinati accorgimenti, c'è la possibilità che le transazioni vengano comunque ricondotte all'identità dell'utente;
- Nessuna autorità centrale: non dipende da nessuna terza parte privata o ente governativo, e, pertanto, il valore dei bitcoin è liberamente contrattato sul mercato. Si tratta quindi di un sistema decentralizzato;
- Inflazione determinata a priori: l'emissione di nuovi bitcoin è determinata dall'algoritmo stesso del programma e non può essere modificata;
- Irreversibile e non falsificabile: una volta che una transazione è stata effettuata ed è inclusa nella blockchain, non può più essere annullata, nemmeno dal mittente;
- Veloce ed economico: in un'ora è possibile trasferire qualsiasi quantità di bitcoin a chiunque nel mondo, a prezzi nell'ordine di centesimo di euro.
- Impossibile da confiscare: soltanto l'utente, attraverso una chiave privata, ha la possibilità di trasferire i propri bitcoin custoditi nel suo *digital wallet*, quindi nessuna autorità esterna può confiscarli o bloccarli senza il permesso.
- Pensato per internet: i bitcoin nascono per essere utilizzati innanzitutto in internet e dunque non soffrono dei difetti e dei problemi di sicurezza che affliggono i sistemi di pagamento tradizionali – come, ad esempio, il mantenere la retrocompatibilità[2] - essendo nati, appunto, prima dell'avvento del Web.

[2] Si definisce retrocompatibilità (backward compatibility) la capacità di interagire con i sistemi precedenti. Ad esempio un software retrocompatibile sarà in grado di aprire correttamente tutti i dati salvati utilizzando la versione precedente.

- Peer-to-peer (rete paritaria o paritetica): modello di architettura logica di rete informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di client o server fissi (clienti e serventi), bensì tutti i nodi sono equivalenti e paritari, cioè possono fungere sia da cliente sia da servente rispetto agli altri nodi della rete; inoltre gli utenti comunicano direttamente e qualsiasi nodo è in grado di avviare e completare una transazione.

Convenzionalmente, il termine Bitcoin con l'iniziale maiuscola si riferisce alla tecnologia e alla rete, mentre il minuscolo bitcoin indica la valuta in sé.

1.2. BITCOIN: ASPETTI TECNICI E FUNZIONAMENTO

Badev e Chen sostengono che lo schema Bitcoin, proprio per le sue caratteristiche, consente un facilitato trasferimento di valore tra le parti del sistema di pagamento, l'unità minima del quale è il bitcoin. In sostanza, un bitcoin può essere paragonato ad un gettone senza nessun collegamento ad un bene sottostante o ad una valuta sovrana; possederne un certo ammontare non significa nulla di più se non avere la possibilità di poter muovere questi bitcoin nel loro ecosistema. Quindi, i bitcoin non hanno un loro valore intrinseco, ma quello che gli deriva principalmente dall'uso nel sistema di transazione Bitcoin e dall'aspettativa di conseguimento di utili derivanti da un apprezzamento della valuta.

Di seguito si andranno ad esporre alcune nozioni fondamentali, in modo da poter fornire le basi e favorire la comprensione del sistema di valuta alternativo.

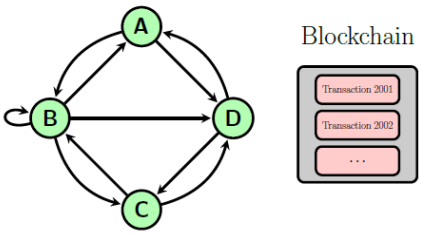

Figura 1.1: Schema Bitcoin.

Nello schema della *Figura 1.1* viene mostrato un pagamento tra i vari utenti della rete Bitcoin. Le frecce indicano i vari pagamenti in bitcoin, mentre i nodi rappresentano le entità o i soggetti coinvolti. Nel linguaggio informatico, si definisce nodo qualsiasi dispositivo hardware del sistema in grado di comunicare con gli altri dispositivi che fanno parte della rete. In particolare, i quattro nodi A, B, C e D interagiscono direttamente l'uno con l'altro, senza necessità di nessun intermediario, al contrario della maggior parte dei sistemi di pagamento tradizionali in cui varie parti, come banche o processori, si collocano tra l'effettuante il pagamento ed il ricevente. Inoltre, come si evince dal diagramma, vi è anche la possibilità che una singola entità, ad esempio B, possa eseguire una transazione in favore di se medesimo. Ogni operazione è cronologicamente registrata dai partecipanti del network in un *public ledger* denominato *blockchain*, cioè una sorta di grande libro mastro. Secondo quanto stabilito dal protocollo Bitcoin, è prevista una ricompensa per la registrazione delle transazioni nella blockchain; ne consegue che i

partecipanti competono tra di loro risolvendo complessi algoritmi crittografici. Tale processo che è ben definito, elegge il vincitore e la blockchain viene così aggiornata. Di particolare rilevanza è il fatto che ogni partecipante detiene una copia di questo libro mastro e il consenso generale dei vari cambiamenti incrementali della blockchain garantisce l'identicità dei ledger. In questo modo, si attua la decentralizzazione e la registrazione delle transazioni. Il procedimento che permette la ricompensa a favore di coloro che effettuano una registrazione nella blockchain include degli incentivi economici: in particolare, una commissione - al momento ancora volontaria - e nuovi bitcoin emessi. Poiché il tasso di transazioni annotate è stabile nel corso del tempo, ne consegue una sostanziale certezza circa il tasso di crescita della valuta, il quale decresce esponenzialmente. Si è quindi arrivati a stimare che l'ammontare totale di bitcoin è circa di 21 milioni e ci si aspetta che tale limite venga raggiunto nel 2140 (https://bitcoin.org/en/faq).

Il processo di transazione Bitcoin è estremamente complesso e gli studiosi sono alla costante ricerca di soluzioni per migliorare la sicurezza, la privacy, la distribuzione del controllo e gli schemi di incentivi. Per esempio, nonostante generalmente ci si riferisca a Bitcoin come un sistema di pagamento quasi istantaneo - in media, infatti, sono necessari 10 minuti affinché la transazione vada a buon fine - Karame et al. (2012) sostengono che non sia idonea per i pagamenti istantanei, poiché questi hanno un tempo di esecuzione nell'ordine dei secondi.

In seguito si tratterà nello specifico il processo di transazione Bitcoin. Poiché la crittografia ha fondamentali implicazioni per la sicurezza e la privacy del sistema Bitcoin, si inizierà con una breve esposizione delle basi della crittografia, successivamente verrà descritta una transazione registrata in un public ledger. In un secondo momento sarà presentato il processo di esecuzione di un pagamento tra due soggetti parti facenti parte del network Bitcoin. Infine, saranno esposte le principali variabili che influenzano il prezzo della valuta.

1.2.1. LE BASI DELLA CRITTOGRAFIA

Il processo di transazione Bitcoin è caratterizzato da (i) un sistema specifico per il pagamento, (ii)dalla crittografia per verificare le operazioni e (iii) dal controllo dell'offerta di bitcoin. Per tali ragioni è frequentemente considerata una criptovaluta.

Bitcoin si basa su due schemi crittografici, quali *digital signature* e *cryptographic hash function*: la prima consente lo scambio di particolari istruzioni di pagamento tra le due parti di una transazione, mentre la seconda viene utilizzata per imporre la disciplina per la scrittura delle transazioni nei public ledger. L'applicazione di questi due specifici schemi non è esclusiva

dei Bitcoin, ma viene ampiamente utilizzata anche nelle comunicazioni commerciali e governative particolarmente riservate e strategiche.

La *digital signature* (letteralmente firma digitale) è una metodologia impiegata per autenticare un messaggio tra l'emittente e il destinatario in modo tale che assicuri:

(i) Autentificazione: il ricevente può verificare che il messaggio provenga realmente dal mittente;

(ii) Non-disconoscimento: il mittente non può negare l'azione di invio del messaggio;

(iii) Integrità: il messaggio non può essere alterato e/o manomesso;

L'attuazione della *digital signature* prevede una *pubblic key encryption* ossia una coppia di chiavi, una pubblica e una privata, che sono generate dal sistema e possiedono delle determinate e specifiche caratteristiche.

La *Figura 1.2* illustra il processo di firma e autenticazione digitale di un messaggio o di un insieme di dati.

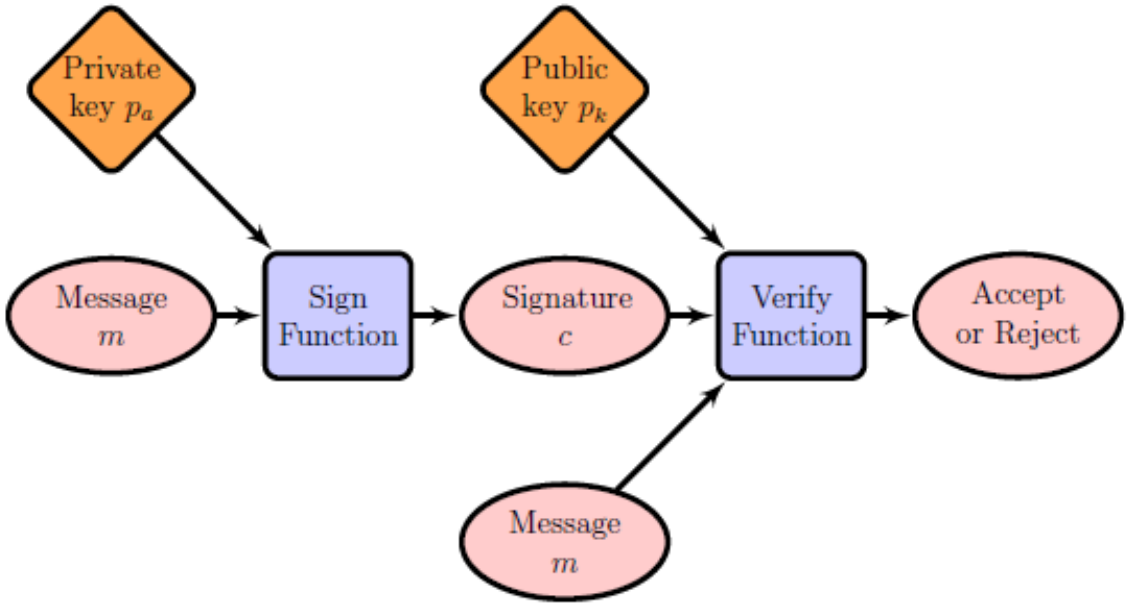

Figura 1.2: Public key encryption.

La funzione "*sign"* combina il messaggio m dell'emittente con la sua chiave privata, al fine di produrre un segno distintivo *c*. Il processo attraverso cui si ottiene c si sostanzia nel firmare il messaggio con l'identità dell'emittente, individuata dalla sua chiave privata p_a. Il destinatario designato quindi, riceve il messaggio firmato, costituito dal messaggio *m* accompagnato dalla firma *c*. Prima di accettarlo egli verifica l'autenticità del soggetto comparando il messaggio e la chiave pubblica attribuita al mittente. Questo viene realizzato attraverso la funzione di verifica, la quale considera come input i messaggi firmati *m* e *c*, unitariamente alla chiave pubblica p_k e produce un output binario statico da accettare o rifiutare. In particolare, la

transazione *m* è firmata con la chiave privata p_a e successivamente trasmessa al network di bitcoin. Tutti i membri del sistema Bitcoin possono verificare che la transazione realmente provenga dal possessore della chiave pubblica p_k, dal momento che le funzioni di firma e verifica sono accessibili al pubblico.

In generale, una funzione crittografica di hash è un algoritmo matematico che prende come input una stringa di dati di lunghezza arbitraria e li trasforma in una stringa binaria di dimensione fissa e predeterminata, chiamata impronta del messaggio o appunto valore di hash. In tale contesto, si considera il messaggio *m* come input e hash *h* come output. La funzione, affinché sia valida e significativa, deve avere le seguenti proprietà:

1. Resistenza alla preimmagine: è computazionalmente intracciabile la ricerca di una stringa di input che dia un hash uguale ad un dato hash, ossia fornito un hash h è estremamente improbabile trovare un messaggio m tale che hash(m)=h.
2. Resistenza alla seconda preimmagine: è computazionalmente intrattabile la ricerca di una stringa in input che dia un hash uguale a quello di una data stringa, cioè dato un messaggio m_1 è difficile riuscire a rintracciare un differente messaggio m_2 tale che hash(m_1)=hash(m_2), infatti un cambiamento anche minimo del messaggio determina un hash completamente diverso.
3. Resistenza alla collisione: è computazionalmente intrattabile la ricerca di una coppia di stringhe in input che diano come output lo stesso hash, ovvero è impossibile trovare due messaggi distinti m_1 e m_2 tali che hash(m_1)=hash(m_2).

Inoltre, la funzione crittografica di hash appartiene ad una famiglia di algoritmi che soddisfano due ulteriori requisiti: (i) è deterministica, infatti il particolare input m originerà sempre e unicamente come output il medesimo h; (ii) è unidirezionale, anche detta non invertibile, in quanto non è possibile ricostruire il documento originale a partire dalla stringa che viene fornita come output. Quindi, nonostante la funzione sia deterministica, l'output è randomico e non prevedibile, questo rende impossibile a qualsiasi soggetto la conoscenza del contenuto del messaggio. Il sistema Bitcoin usa principalmente SHA-256 (Secure Hash Algorithm) elaborato dal National Security Agency (NSA, Agenzia per la Sicurezza Nazionale), organismo governativo degli Stati Uniti d'America che si occupa della sicurezza interno-nazionale, e pubblicato dal NIST, ossia dal National Institute Of Standards and Technology (si veda Badev e Chen 2014).

1.2.2. LA TRANSAZIONE IN BITCOIN

Dal punto di vista tecnico, i bitcoin risiedono in quelli che, nel proprio sistema, sono indicati come *bitcoin addresses* (indirizzi bitcoin). La possibilità di effettuare pagamenti da un particolare indirizzo è regolata e controllata dalla firma digitale, la quale, come già analizzato in precedenza, prevede una chiave pubblica p_k ed una privata p_a. Ogni indirizzo è associato ad un unico pubblico ID, un identificatore[3] alfa-numerico che corrisponde alla chiave pubblica p_k, la cui diretta controparte, la chiave privata p_a, permette il controllo e la gestione dei bitcoin contenuti nello specifico indirizzo. In particolare, ogni pagamento, affinché possa considerarsi valido, deve essere firmato con la propria chiave privata associata a quello specifico indirizzo; quindi, la perdita della stringa alfa-numerica che rappresenta la chiave privata per un dato indirizzo, implica la perdita irreversibile dei bitcoin associati a quel medesimo indirizzo.

Comunemente, i soggetti coinvolti in una transazione di bitcoin possiedono più indirizzi e sono soliti identificarne la totalità con il semplice nome "portafoglio", cioè un insieme di *bitcoin addresses* la cui proprietà è in capo ad un'unica persona. Infatti, ogni transazione solitamente coinvolge multipli indirizzi sia per il mittente, sia per il destinatario. Nonostante ogni operazione venga registrata nella blockchain e questa sia pubblica, non è comunque possibile osservare direttamente il percorso degli scambi e i vari cambi di proprietà. Il seguente esempio illustra chiaramente questo concetto: lo schema nella *Figura 1.3*, che illustra una transazione avvenuta il 15 gennaio 2015, riporta 14 indirizzi invianti (indicati in verde) e 12 riceventi (indicati in blu), ma questo non permette di dedurre il numero esatto di entità coinvolte: potrebbe trattarsi sia di un'unica persona che possiede i 14 sending adress, sia di 14 soggetti distinti.

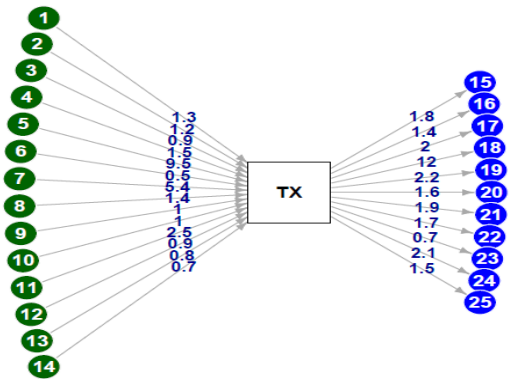

Figura 1.3: Indirizzi in una transazione bitcoin.

Una qualsiasi transazione Bitcoin mette in atto una serie di meccanismi al fine di garantire che: (a) la verifica di ogni transazione venga effettuata da più soggetti coinvolti nel network; (b) la

[3] Per avere un'idea più concreta, un esempio di identificatore è il seguente: 1JArS6jzE3AJ9sZ3aFij1BmTcpFGgN86hA.

registrazione di ogni transazione sia discretizzata, cioè che ciascuna venga linearmente ordinata per mezzo di un segno consecutivo nel tempo; (c) i partecipanti competano tra di loro e vengano ricompensati per la registrazione di una transazione e (d) che ogni movimentazione sia sottoposta ad un controllo incrociato da parte di più nodi (=soggetti).

Di seguito sarà illustrato il processo di una transazione Bitcoin mettendo in luce le proprietà appena menzionate.

Si supponga che Silvia desideri inviare a Marco 1 bitcoin utilizzando il network Bitcoin. Innanzitutto è necessario che ciascuno possieda un indirizzo bitcoin, il quale verrà rispettivamente denominato address^{Silvia} e address^{Marco}. Successivamente Silvia dovrà emettere e autenticare digitalmente un messaggio di tale tipo: "*address^{Silvia} is sending address^{Marco} 1 bitcoin*"; come già detto, ogni indirizzo bitcoin è identificato da una specifica chiave pubblica, quindi il messaggio appena citato può essere agevolmente rappresentato dalla *Figura 1.4*.

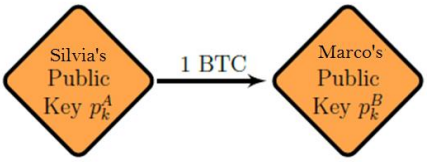

Figura 1.4: Esempio di una transazione.

Non appena Silvia avrà firmato e autenticato con la sua chiave privata, il messaggio relativo all'operazione, ad ogni soggetto appartenente alla rete Bitcoin sarà la possibilità verificare e accertare che sia stata realmente Silvia ad inviare quel messaggio e che questo non sia stato manomesso. Inoltre, la firma digitale costituisce una garanzia del fatto che nessun altro, eccetto Silvia, possa aver firmato il messaggio, e le impedisce anche di negare la propria azione.

Prima di eseguire la transazione, il protocollo Bitcoin impone la verifica di due distinti aspetti del messaggio *"address^{Silvia} is sending address^{Marco} 1 bitcoin"*. In primis, è realmente Silvia ad aver trasmesso il messaggio? (Si noti che in questa fase iniziale, l'autorizzazione di Marco non è richiesta né per l'avvio né per la registrazione della transazione). La risposta è affermativa in quanto, come già esposto, lo schema della firma digitale attribuisce solo al proprietario della chiave privata la facoltà di poter autenticare e firmare il messaggio. In secondo luogo, l'indirizzo emittente possiede fondi a sufficienza da garantire il buon fine dell'operazione? La risposta è nuovamente affermativa in quanto essendo un sistema decentralizzato è in grado di sostituire le terze parti intermediarie e mantenere tutte le informazioni necessarie, tra cui la reale disponibilità di fondi.

In seguito a questa verifica iniziale, alcuni tra i partecipanti al network bitcoin, i *miners*, iniziano a competere tra di loro per registrare la transazione nella blockchain. Una volta determinato il vincitore la registrazione dell'operazione si considera conclusa e a questi spetterà una ricompensa in bitcoin. Il vincitore è il nodo che per primo riesce a risolvere un compito che si

basa sull'uso di schemi crittografici, in particolare la funzione di hash. Inizialmente, un blocco di nuove transazioni appena trasmesse viene usato come input nella funzione crittografica di hash per ottenere un hash che prende il nome di digest. Questa insieme al nounce - una stringa alfa numerica arbitraria che può essere utilizzata una sola volta - e con l'hash del blocco precedente, diventa input di un'ulteriore funzione di hash in grado di aggiungere un nuovo blocco alla blockchain. Il primo soggetto in grado di trovare un nounce con le proprietà richieste dalla funzione crittografica, invia l'informazione agli altri partecipanti e successivamente il libro mastro (ledger) viene aggiornato. Questo schema brevemente descritto, è l'attuazione di Hashcash, un tipo di sistema proof-of-work il cui obiettivo è assicurare che i computer utilizzino un numero definito di risorse computazionali per risolvere una data mansione.

I nodi in grado di eseguire tali complicati processi, nell'ecosistema Bitcoin, sono conosciuti come *miners* e sono incentivati da una ricompensa prevista dallo stesso Nakamoto nel protocollo Bitcoin. Questa si sostanzia in un ammontare di nuovi bitcoin e, in misura significativamente minore, in commissioni e tariffe pagate volontariamente dagli iniziatori di una qualsiasi transizione (si veda Badev e Chen 2014).

1.3. LA FORMAZIONE DEL PREZZO

Partendo dal presupposto che i bitcoin sono una valuta relativamente giovane, il meccanismo di formazione del prezzo non è ancora stato compreso nei suoi minimi particolari. Gli studi esistenti nella letteratura suggeriscono l'esistenza di tre driver determinanti il prezzo dei bitcoin: (i) le forze di mercato nella domanda e offerta dei bitcoin, (ii) attrattività dei bitcoin e (iii) gli sviluppi globali macroeconomici e finanziari. In questa sezione si seguirà l'approccio utilizzato da Kancs, Ciaian e Rajcaniova (2016) nel loro elaborato per la Commissione Europea e si illustreranno brevemente le conclusioni a cui sono giunti in seguito a studi econometrici.

1.3.1. DRIVER #1: FORZE DI MERCATO NELLA DOMANDA E NELL'OFFERTA

Secondo Buchholz, uno dei driver principali del prezzo dei bitcoin è l'interazione tra domanda e offerta sul mercato stesso. Come affermato dalla teoria quantitativa della moneta, l'offerta è determinata dallo stock totale dei bitcoin in circolazione, mentre la domanda è rappresentata dall'ampiezza dell'economia Bitcoin (ad esempio l'uso negli scambi) e dalla velocità di circolazione. La velocità Bitcoin misura la frequenza con la quale un'unità di bitcoin è utilizzata per acquistare un bene o un servizio. Tale teoria implica che il prezzo della valuta decresce all'aumentare della velocità di circolazione e dello stock, mentre aumenta con il parallelo incremento dell'ampiezza dell'economia e del livello generale dei prezzi. La domanda è influenzata primariamente dal valore dei bitcoin come mezzo di scambio; infatti, questi non

possiedono un valore intrinseco, proprio come le monete correnti. Quindi, mentre per esempio, la domanda di dollari è influenzata sia dal loro valore intrinseco, sia dal valore degli scambi futuri, la domanda di bitcoin può essere condizionata solo da quest' ultimo aspetto. L'offerta invece, è data dall'ammontare totale messo in circolazione, il quale è conosciuto pubblicamente ed è fissato nel lungo periodo.

Dalle varie analisi econometriche emerge che, in generale, le forze di mercato della domanda e dell'offerta hanno chiaramente un'influenza sul prezzo dei bitcoin. Tuttavia, le variabili legate al lato della domanda, come ad esempio il numero di *bitcoin addresses*, appaiono esercitare un impatto più pronunciato sul prezzo rispetto ai driver legati all'offerta, come il numero di bitcoin. Quindi, mentre un aumento dello stock di bitcoin porta ad un loro deprezzamento, un accrescimento delle dimensioni dell'economia o del numero di indirizzi porta ad un incremento del prezzo bitcoin.

1.3.2. DRIVER #2: ATTRATTIVITÁ DEI BITCOIN

Vi sono molteplici fattori specifici che, in aggiunta a quelli che tradizionalmente influenzano il prezzo, determinano la domanda. Ciò è parzialmente collegato sia al fatto che i bitcoin sono stati creati in un periodo relativamente recente, sia alla natura stessa della valuta.

Innanzitutto, il prezzo risente del rischio e dell'incertezza che caratterizza l'intero sistema Bitcoin. Come già esposto, i bitcoin sono privi di un valore intrinseco, né hanno un valore derivante dal consumo o da processi di produzione (come avviene per l'oro); ne consegue che la loro sorte dipenda anche dall'accettazione e dalla valorizzazione come mezzo di scambio in futuro. Le aspettative riguardanti l'accettazione e il valore sono molto rilevanti, poiché attualmente i bitcoin sono nella fase in cui è necessario stabilire una propria quota di mercato e infondere credibilità e fiducia tra i consumatori.

In seconda istanza, essendo una valuta virtuale, rispetto a quelle tradizionali, i bitcoin sono maggiormente vulnerabili ai cyber attacchi, i quali possono destabilizzare l'intero sistema ed, in un'eventualità remota, portarlo al collasso. Nel passato tali attacchi erano abbastanza frequenti; basti pensare che nel 2013 Moore and Christin condussero uno studio in cui analizzarono quaranta piattaforme in cui era possibile scambiare la criptovaluta e, infatti, riscontrarono che diciotto di queste chiusero poco dopo a causa di tali attacchi informatici. Ad oggi, tuttavia, la situazione è notevolmente cambiata e si sono raggiunti alti livelli di protezione e sicurezza.

Infine, il prezzo dei bitcoin risente indubbiamente dell'attrattività come opportunità d'investimento per i soggetti interessati. Le decisioni dei potenziali investitori infatti, sono influenzate sia da un aumento sia da una diminuzione dell'attenzione da parte dei media. Il

ruolo dell'informazione è particolarmente importante in quanto strettamente collegato a costi di ricerca e a molteplici opportunità d'investimento alternative. Poiché la domanda di investimenti dipende dai costi associati alla ricerca di informazioni per potenziali alternative disponibili sul mercato, le opportunità d'investimento a cui è dedicata particolare attenzione da parte dei media, è probabile che siano preferite dagli investitori, in quanto vengono ridotti i costi di ricerca. È però opportuno sottolineare che l'azione dei media può avere un effetto sia positivo sia negativo sul prezzo dei bitcoin, in quanto dipende ovviamente dal tipo di notizia dominante nel determinato periodo.

Il più spiccato e statisticamente significativo impatto sul prezzo della valuta è dato dalle variabili che misurano l'attrattività, quali le visualizzazioni su Wikipedia e nuovi post. Quest'ultima ha un'influenza positiva, in quanto riflette la sempre maggiore accettazione e fiducia nella valuta, e viene misurata in base all'intensità e alla frequenza delle discussioni sull'argomento tra gli utilizzatori. Tuttavia, come sottolineato dagli studi di Kristoufek, sono le visualizzazioni sulla pagina web Wikipedia ad avere l'impatto maggiormente significativo: infatti, in media, gli articoli riguardanti i bitcoin ottengono ventimila letture al mese; si pensi che tra gli oltre cinque milioni di articoli totali in lingua inglese, solo ottantotto hanno un numero di visualizzazioni superiore a quelle dei bitcoin. Tale variabile permette di ipotizzare la misura degli investitori o degli utenti interessati al sistema Bitcoin e quindi, catturare informazioni circa la domanda di valuta; grazie a questo è possibile, infatti, osservare l'evoluzione della conoscenza della valuta tra i soggetti e, di conseguenza, la maggiore accettazione e domanda della stessa come opportunità d'investimento o mezzo di scambio.

1.3.3. DRIVER #3: SVILUPPI GLOBALI MACROECONOMICI E FINANZIARI

Van Wijk (2013) sottolinea il ruolo degli sviluppi globali macroeconomici e finanziari, evidenziando come variabili il tasso di cambio nominale euro/dollaro, gli indici borsistici ed il prezzo del petrolio, possano determinare il prezzo dei bitcoin. L'impatto di tali indicatori sul prezzo può agire attraverso diversi canali: per esempio, se gli indici di Borsa riflettono andamenti positivi dell'economia, è possibile che venga stimolato l'uso dei bitcoin nel commercio e negli scambi, rafforzandone così la domanda e impattando positivamente sul prezzo. Anche l'inflazione e l'indice dei prezzi sono importanti indicatori che possono fornire una migliore visione degli sviluppi macroeconomici e finanziari. Infatti, secondo Krugman and Obstfeld, il prezzo del petrolio è una delle principali fonti delle pressioni sulla domanda e sui costi, e inoltre fornisce una primitiva indicazione dell'inflazione. In tal modo, quando il prezzo dell'oro nero inizia a segnalare potenziali cambiamenti nel livello generale dei prezzi, ciò può provocare un deprezzamento (o apprezzamento) del prezzo dei bitcoin: allo stesso modo anche

i tassi di cambio possono riflettere e prevedere andamenti inflazionisti (o deflazionistici), andando successivamente ad incidere sul prezzo della valuta.

Secondo Dimitrova (2005) invece, è ammessa una relazione negativa tra il prezzo della valuta e gli indicatori macro-finanziari: un declino nel prezzo delle azioni, infatti, quasi sicuramente porterà gli investitori a vendere gli asset che possiedono. Questo conduce ad un deprezzamento della valuta sottostante ma può stimolare il prezzo dei bitcoin, se i soggetti decidono di sostituire gli investimenti in azioni con investimenti in bitcoin. Quindi, in questo caso, gli indici di borsa sono positivamente collegati al prezzo dei bitcoin. Tuttavia, è necessario e curioso notare che indicatori come il Dow Jones index, il tasso di cambio e il prezzo del petrolio non impattano in maniera significativa sul prezzo dei bitcoin nel lungo periodo (si veda Cianian, Rajcaniova e Kancs 2016).

CAPITOLO 2. FUNZIONE ECONOMICA E GIURIDICA DEI BITCOIN

Le valute virtuali, ed in particolare i bitcoin, sono un fenomeno globale, che travalica i singoli confini nazionali, e in quanto tali, richiederebbero la definizione di un quadro regolamentare chiaro, uniforme e condiviso a livello mondiale. Tale prospettiva sembra però lontana dal realizzarsi e al momento una disciplina legale della fattispecie manca sia a livello europeo sia in gran parte degli ordinamenti nazionali. In assenza di una compiuta regolamentazione del fenomeno, in tale sezione si cercherà di individuare la funzione economica e la natura giuridica dei bitcoin.

2.1. I BITCOIN SONO REALMENTE UNA VALUTA?

Tipicamente, la moneta per essere definita tale deve assolvere tre funzioni caratteristiche: a) mezzo di scambio, utilizzato nei commerci per evitare gli inconvenienti del baratto; b) riserva di valore, consentendo di usare in futuro il potere d'acquisto immagazzinato; c) unità di conto, che permette di misurare il valore di beni e servizi. Di seguito, si andrà ad analizzare ciascuno di questi aspetti in relazione alle caratteristiche dei bitcoin, per capire se questa valuta digitale possa essere considerata una nuova moneta.

2.1.1. BITCOIN COME MEZZO DI SCAMBIO

I bitcoin non possiedono un valore intrinseco, il quale dipende in ultima istanza dall'utilità percepita La maggior parte delle classifiche riguardanti i soggetti più importanti che accettano pagamenti in bitcoin evidenziano come questi siano essenzialmente compagnie informatiche – le quali basano il proprio business sulla vendita di prodotti focalizzati e pensati per le applicazioni bitcoin -, piazze di mercato o enti che offrono servizi di investimento di tipo speculativo. Al fine di ottenere una visione il più possibile accurata relativa al numero di transazioni bitcoin che avvengono quotidianamente, è necessario consultare i dati estraibili dal *pubblic ledger* universale di cui si è parlato in precedenza. Secondo i dati disponibili su blockchain.com, la fonte più attendibile per i dati sul blockchain bitcoin, attualmente (agosto 2017) le transazioni hanno raggiunto un volume giornaliero approssimativamente pari a 347'319. Tuttavia, la maggior parte di queste operazioni avvengono tra soggetti speculatori, e solo una minima parte ha come scopo l'acquisto di beni o servizi. Inoltre, come si può osservare dalle successive mappe, in un mondo con più di 7'000'000 di consumatori, la maggioranza dei quali effettua quotidianamente più transazioni; i bitcoin appaiono nel mercato come una

presenza abbastanza trascurabile, questo è dovuto anche al fatto che il numero di soggetti o punti vendita che accettano pagamenti in bitcoin è esiguo.

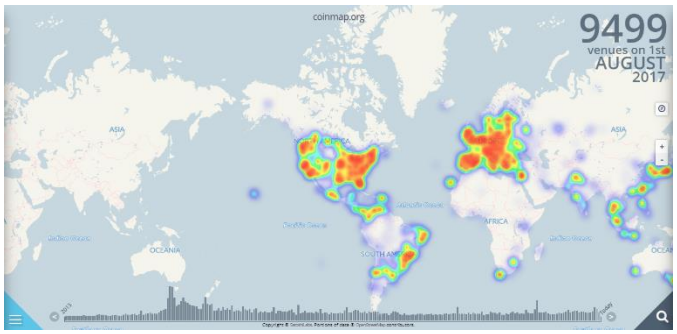

Figura 2.1: Mappa mondiale degli esercenti che accettano pagamenti in bitcoin.

Le seguenti mappe sono state tratte da coinmap.org, la piattaforma di riferimento di tutti gli esercenti per evidenziare all'utenza la propria adesione al circuito bitcoin e l'accettazione della valuta. Come si può notare, l'utilizzo dei bitcoin in sedi fisiche quali hotel, negozi, ristoranti interessa soprattutto gli Stati Uniti d'America e l'Europa, mentre il resto del pianeta sembra esserne ancora escluso. In particolare, in Italia i liberi professionisti e i punti vendita che accettano già questa forma di pagamento sono circa 180.

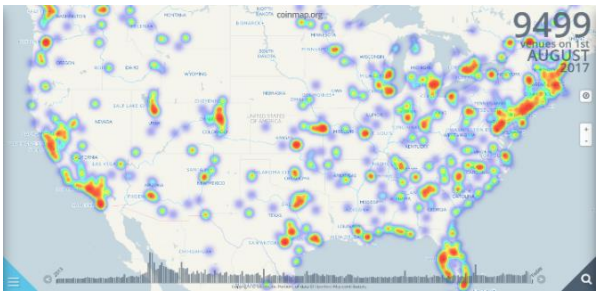

Figura 2.2: Situazione negli Stati Uniti

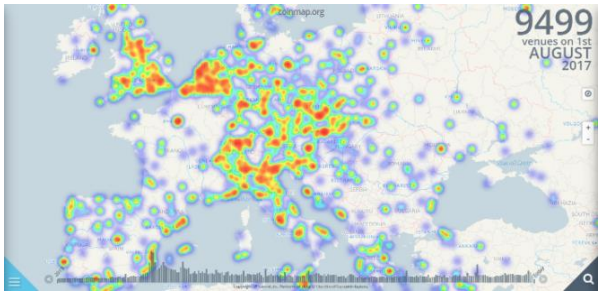

Figura 2.3: Situazione in Europa

Un altro grande ostacolo all'ampio utilizzo della criptovaluta come mezzo di scambio nasce dalla difficoltà insita all'ottenimento di nuovi bitcoin. Infatti, a meno che un consumatore non sia un *miner* - il che richiede un dispendio imponente di capitale per effettuare l'attività di estrazione di BTC-, questi è costretto ad acquistare la valuta in un mercato di cambio online e successivamente deve trovare un meccanismo per poterli custodirli in totale sicurezza, operazioni, queste, che implicano comunque dei costi (si veda Yermack 2013).

Tuttavia, a partire dal marzo 2016, le cose si sono notevolmente semplificate e probabilmente si è aperta una nuova prospettiva di sviluppo; infatti Wirex Limited, piattaforma bancaria cloud-based con sede a Londra, ha introdotto una carta di debito che permette di pagare transazioni in Bitcoin sfruttando i circuiti internazionali di Mastercard e Visa in circa 130 Paesi. Per attivare il servizio è necessario anzitutto possedere un account PayPal, a cui si devono aggiungere un account Wirex e una carta virtuale E-Coin (creata dalla medesima Wirex Limited) con una disponibilità di almeno tre dollari. Una volta effettuato l'accesso all'interno del profilo PayPal si selezionerà l'opzione "*Add a Card*", si compileranno tutti i campi con le informazioni

anagrafiche richieste e i dati relativi alla carta virtuale, e si effettueranno poi tutti i passaggi necessari all'attivazione. A parere di chi scrive, benché si tratti di un'operazione molto innovativa, la carta, una volta in funzione, presenta ancora grossi limiti all'utilizzo dei bitcoin come mezzo di scambio, in quanto l'operazione minima deve essere di almeno 10$, per ogni transazione Paypal trattiene 5$ di tariffa e per convertire del denaro con valuta legale in bitcoin sono necessari, ogni volta, dai cinque ai sette giorni lavorativi per il trasferimento sulla carta.

2.1.2. BITCOIN COME UNITÁ DI CONTO

Affinché una valuta possieda la funzione di unità di conto è necessario che i consumatori la considerino e la trattino come numerario, cioè come unità base per valutare il valore, nel confrontare i prezzi di beni alternativi. Per esempio, si intuisce immediatamente che un caffè che abbia il prezzo di 2 euro in un bar, costi il doppio rispetto al caffè venduto ad 1 euro in un altro bar della medesima categoria.

I bitcoin, invece, si trovano di fronte a numerosi ostacoli prima di diventare un'unità di conto utile e stimata. Innanzitutto, uno dei maggiori problemi deriva dalla sua estrema volatilità, in quanto il valore dei bitcoin cambia significativamente di giorno in giorno, rispetto alle valute tradizionali decisamente più stabili. Di conseguenza, un esercente che decide di accettare pagamenti in bitcoin sarà costretto a ricalcolare i prezzi di frequente, e tale pratica è dispendiosa per chi la deve eseguire nonché confusionale per chi intende acquistare un determinato bene. Questo problema si risolverebbe solo in un mondo per ora ipotetico, in cui il bitcoin si affermasse come valuta principale. Un'ulteriore difficoltà sorge in relazione ai differenti prezzi per i bitcoin che in qualsiasi momento è possibile osservare sul mercato. Per esempio, consultando uno dei maggiori siti che monitora i prezzi dei bitcoin nei mercati del mondo, al momento della stesura di questo elaborato, i cinque valori di quotazione più elevata rispetto al dollaro sono i seguenti: 1 bitcoin nelle rispettive exchanges (Borse) è pari a $4508 su OKCoin, $4350,5 su ANX, $4299,8 su Bitfinex, $4297,2 su Kraken e $4273 su BitStamp (https://it.investing.com). La disparità dei differenti dati di mercato appena riportati registra un'oscillazione percentuale del 5,49 tra il valore più elevato e quello minimo, fenomeno, questo, in palese violazione della legge del prezzo unico, e che creerebbe continue opportunità di arbitraggio. Infatti, la legge del prezzo unico afferma che se opportunità d'investimento equivalenti vengono scambiate simultaneamente in mercati concorrenziali diversi, devono essere scambiate allo stesso prezzo in entrambi i mercati; invece, si intende come arbitraggio la pratica di acquistare beni equivalenti in mercati differenti per sfruttare la differenza di prezzo .Quindi, l'incertezza del valore di mercato dei bitcoin rappresenta un vero dilemma per ogni terza parte –venditore o consumatore che sia- la quale cerchi di avere un valido punto di

riferimento per poter fissare i prezzi o effettuare confronti tra questi. Al fine di ovviare a tale problema, molti siti web hanno iniziato a fare affidamento su complesse aggregazioni di prezzo, basate sulla media dei differenti prezzi dei bitcoin scambiati nelle ultime 24 ore, ma tale valore aggregato, non rappresenta comunque, nel momento effettivo in cui avviene la transazione, il vero costo della merce prodotta o venduta né per il consumatore, né per il venditore.

Tuttavia, l'ostacolo maggiore - spesso non considerato o banalizzato dai fedeli sostenitori - all'ampio utilizzo dei bitcoin come unità di conto, è rappresentato dal costo relativamente alto di un bitcoin se comparato alla maggior parte di prodotti e servizi ordinari, ad esempio in un possibile scenario futuro in cui divenga possibile, magari anche in punti di vendita fisici, acquistare qualsiasi bene tramite la criptovaluta. Questo costringe i venditori a dover esporre i prezzi in bitcoin di qualsiasi bene con quattro o più cifre decimali, e nonostante vengano rispettate esattamente tutte le regole del calcolo matematico, e quindi come tali siano inequivocabili, ciò crea nel consumatore un profondo disorientamento. Per esempio, in uno scenario ipotetico, un caffè potrebbe costare 0,0003 BTC, una spremuta d'arancia 0,0009 BTC e una pizza al ristornante 0,0024 BTC; in maniera alternativa, questi prezzi potrebbero essere rappresentati tramite la notazione scientifica, rispettivamente come segue: $3x10^{-4}$ BTC, $9x10^{-4}$ BTC e $2{,}4x10^{-3}$ BTC. È comunque estremamente difficoltoso, se non addirittura impossibile, trovare nel mondo un'altra valuta che esprima i propri prezzi in tale modo; oltre a ciò, la maggior parte dei software utilizzati per registrare il prezzo della merce venduta, come ad esempio le casse al supermercato, ammettono solo due cifre decimali dopo la virgola. Inoltre, come già detto in precedenza, appare problematico per i consumatori comparare il prezzo dei vari beni: nell'esempio sopra riportato, la pizza è nove volte più costosa rispetto al caffè, ma persino acquirenti con un livello di istruzione medio-alto, in molti casi pratici, in cui è necessaria una certa celerità, farebbero fatica ad effettuare il calcolo a causa della lunghezza del numero e della presenza di numerosi zero (si veda Yermack 2013). Generalmente, i sostenitori dei bitcoin tendono a rigettare questo aspetto fallimentare del non allineamento dei prezzi espressi in BTC con gli ordinari punti di riferimento del consumatore; ma a loro favore, numerose fonti sono d'accordo nell'affermare che è possibile la divisione dei bitcoin in otto cifre decimali; infatti fino al momento in cui il valore di un'unità di BTC assume un valore troppo elevato per poter essere utilizzabile per le piccole transazioni quotidiane, le persone possono comunque iniziare a utilizzarla come unità di misura, se espressa in termini di milli-bitcoin (mBTC) o micro-bitcoin (μBTC).

2.1.3. BITCOIN COME RISERVA DI VALORE

La valuta che assume la funzione di riserva di valore consente al proprietario di possederla in un certo momento e poterla scambiare per beni o servizi in un tempo futuro a sua scelta; quando viene spesa il soggetto si aspetta di ricevere in cambio qualcosa che abbia il medesimo valore economico della moneta nel momento in cui ne è entrato in possesso. Nel corso della storia il considerare una valuta come riserva di valore essenzialmente significava proteggerla da eventuali furti, nascondendola fisicamente o depositandola in banca. Chiaramente, la classica soluzione del "nascondere sotto il materasso" o in altri luoghi, i bitcoin non può funzionare, in quanto non possiedono una manifestazione fisica e tangibile. Questi, infatti, devono essere conservati in account informatici chiamati *digital wallets*, la cui sicurezza e difesa della privacy è diventata l'attività di maggior impegno nell'ecosistema dei Bitcoin. Alcune compagnie di "portafogli digitali" hanno iniziato, infatti, a stipulare accordi contrattuali con società di assicurazioni al fine di fornire almeno le garanzie assicurative base sul deposito. In linea teorica, questa soluzione è efficace e può funzionare, ma il consumatore è costretto a farsi carico del costo della valutazione della sicurezza, della società assicuratrice e della compagnia che fornisce il servizio di conservazione dei bitcoin.

Nel caso in cui il consumatore riesca a risolvere queste problematiche e a trovare un modo per custodire in sicurezza i propri bitcoin, è successivamente costretto a confrontarsi con un ulteriore problema: la gestione del rischio derivante dalla volatilità propria della valuta (si veda Yermack 2013).

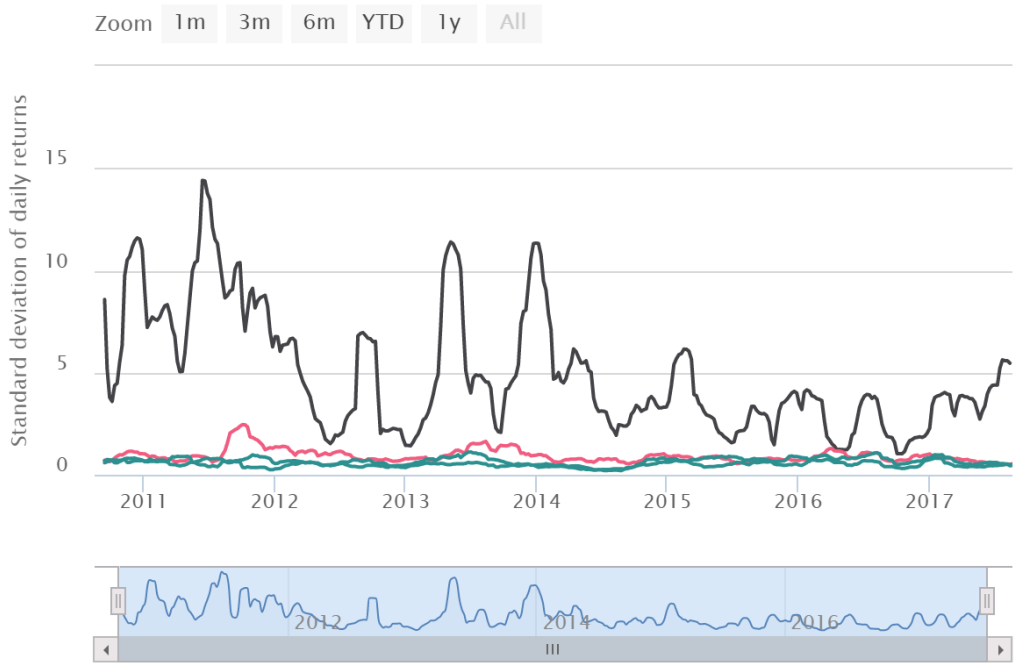

Grafico 2.1: Serie temporale della volatilità dei bitcoin.

Nel grafico è illustrata la volatilità del tasso di cambio bitcoin-dollaro (colore nero), calcolata utilizzando i dati disponibili a partire dal 2011. Al fine di un miglior confronto, sono state riportate anche le deviazioni standard[4] dei tassi di cambio di Euro, Yen e oro, sempre rispetto al dollaro americano. I tassi di cambio sono rappresentati rispettivamente dai colori verde scuro (Euro), verde (Yen) e rosa (oro). Come si evince, ha sia un andamento molto irregolare, caratterizzato da brusche e improvvise fluttuazioni, sia un tasso di volatilità nettamente superiore rispetto alle altre valute. Queste ultime infatti, solitamente oscillano tra lo 0,5% e l'1,0%, l'oro invece in media ha una volatilità intorno all'1,2%, mentre i bitcoin si sono attestati attorno al 5% a partire dal 2016, ma raggiungendo in passato (2014) anche picchi del 14,4%. Quindi, si può concludere che possedere bitcoin, anche se per un breve periodo, è abbastanza rischioso e ciò in sostanza è contradittorio con la funzione di riserva di valore che una moneta possiede (disponibile su https://www.buybitcoinworldwide.com).

2.2. NATURA GIURIDCA DEL FENOMENO

L'inquadramento dei bitcoin all'interno di una categoria giuridica ben definita non è ancora chiaro. A riguardo sono state sviluppate numerose teorie, ognuna delle quali ha sottolineato aspetti diversi da non sottovalutare. La strada più tradizionale è quella che tenta di ricondurre la valuta alla categoria giuridica del denaro.

Tuttavia, dal punto di vista giuridico, il termine moneta negli stati moderni identifica esclusivamente la moneta a corso legale, espressione della sovranità statale, cioè le banconote e le monete denominate nella valuta adottata in ciascun ordinamento, la cui emissione è di solito riservata alle banche centrali[5]. Secondo l'art. 128 del Trattato di funzionamento dell'Unione europea (TFUE), solo tale tipologia di moneta è garantita dalla legge, la quale ne regola l'emissione e le conferisce valore legale, imponendo al creditore l'obbligo di accettarla in pagamento al suo valore nominale e sancendone l'efficacia liberatoria nell'adempimento delle obbligazioni pecuniarie. Nessuna delle caratteristiche della moneta a corso legale è ravvisabile nelle valute virtuali, quali i bitcoin. Essi infatti, non sono espressione della sovranità di alcuno Stato, non sono autorizzati, emessi o garantiti da alcuna banca centrale o autorità pubblica, non hanno un valore predeterminato e/o ufficiale né hanno efficacia liberatoria *erga omnes.* Al contrario, sono generati da soggetti privati e non traggono il proprio valore dalla legge, ma esclusivamente dal grado di spontanea accettazione che incontrano sul mercato. Ne consegue,

[4] In finanza, la deviazione standard di un rendimento è detta anche volatilità.

[5] Gli Stati che hanno aderito all'Unione monetaria europea hanno operato una cessione di sovranità in favore delle Istituzioni europee, devolvendo loro le proprie competenze in materia monetaria e sostituendo alle proprie monete l'euro. Quindi, l'euro, moneta legale degli Stati dell'Eurozona, è più precisamente, espressione di una sovranità sovranazionale.

quindi, che l'utilizzo dei bitcoin come mezzo solutorio presuppone il previo accordo delle parti del rapporto obbligatorio. Quanto esposto, porta ad escludere senza dubbi che il sistema Bitcoin sia assimilabile alla moneta legale, e allo stesso tempo, che possa essere confuso con la moneta scritturale o con la moneta elettronica, poiché, pur avendo in comune la matrice privata e, soprattutto con la seconda, l'utilizzo della tecnologia informatica, rappresenta in forma digitale un valore non espresso in moneta a corso legale.

I bitcoin non possono neppure essere ricondotti alla categoria dei prodotti finanziari, definiti all'art.1, comma 1, lettera u) del Testo Unico della Finanza (TUF) come "gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria". Gli strumenti finanziari sono a loro volta, specificati in un'elencazione contenuta nel comma 2 della medesima norma, ma, da un lato, nessuna delle fattispecie ivi indicate sembra adattarsi ai bitcoin, dall'altro il successivo comma 4 del citato articolo, afferma espressamente che "i mezzi di pagamento non sono strumenti finanziari". Infatti, nonostante i bitcoin abbiano anche una finalità d'investimento, non si può negare che sia predominate la funzione di mezzo di pagamento. D'altra parte, gli strumenti finanziari in senso stretto vengono sottoposti dallo stesso TUF ad una rigida e stingente disciplina, la quale verrebbe violata quotidianamente da coloro che estraggono o scambiano bitcoin, se quest'ultimi venissero appunto considerati strumenti finanziari. Tuttavia, nessuna azione è stata adottata dalle autorità italiane per sanzionare queste violazioni, il che consente di escludere tale categorizzazione dei bitcoin, quanto meno allo stato attuale e per quanto concerne l'ordinamento italiano. La versatilità funzionale di tale valuta sembra, quindi ostare, quanto meno alla stregua della disciplina positiva italiana, anche a una loro qualificazione giuridica in termini di prodotto finanziario (si veda Mancini 2015).

Una terzia via, al fine di delineare la natura giuridica di questa nuova valuta, discende dal corretto inquadramento storico-giuridico del denaro tradizionale. Originariamente, infatti, il denaro nasce come merce: un particolare tipo di merce, con caratteristiche particolari che lo rendono adatto ad essere impiegato per le funzioni fondamentali esposte in precedenza. È solo con l'avvento delle monete fiat, cioè a corso legale, prive di qualunque valore di mercato se non fosse per l'*imprimatur* delle autorità monetarie, che il denaro cessa di essere percepito come una merce; ma, in verità, esso storicamente nasce come tale, e come tale era originariamente inquadrato. I bitcoin recuperano solo in parte questa funzione originaria, ovviamente presentando delle differenze rispetto al denaro-merce tradizionale. Tuttavia, pur essendo intangibili e rappresentati da codici informatici, sono certamente più vicini al denaro-merce in senso proprio di quanto non lo sia al denaro fiduciario delle banche centrali: infatti, a differenza

di questo, ma proprio come oro e argento, hanno valore non perché il loro uso sia imposto, ma perché, e fino al momento in cui, le persone e le aziende sul mercato decidono liberamente di attribuirgli valore. Pertanto, l'inquadramento giuridico più corretto per un bitcoin è alla fine anche il più semplice: esso è innanzitutto un bene, nel senso fatto proprio e definito dal Codice Civile all'art.810: "sono beni le cose che possono fare oggetto di diritti". Naturalmente si tratterà di un bene mobile e, poiché privo di qualsiasi supporto materiale, immateriale. Quella appena citata è una nozione ampia e variegata che ricomprende al suo interno beni molto diversi tra di loro, dalla proprietà individuale ai segni distintivi dell'impresa, dai diritti della personalità all'avviamento commerciale. Ebbene, si ritiene che finché non verrà creata una nuova e apposita figura giuridica ad opera del legislatore, nel diritto italiano attuale, la valuta bitcoin può correttamente essere inquadrata come una nuova categoria di bene immateriale, a sé stante, ma con dei punti di contatto con la proprietà intellettuale. In effetti, pur essendo vero che un'unità non può essere interamente assimilata ad un prodotto dell'ingegno in senso tradizionale, non avendo il carattere della creatività, è altresì vero che anche l'acquisto della proprietà a titolo originario di uno o più bitcoin avviene tramite l'impiego di risorse sia economiche, sia intellettuali, le quali si estrinsecano nella soluzione di un problema e nella creazione di un bene nuovo, prima non esistente, univoco, e avente la caratteristica di essere privo di una materialità intrinseca. Inoltre, un'unità di bitcoin è a tutti gli effetti un bene rivale che non può essere utilizzato contemporaneamente da più di un soggetto. Questa ricostruzione quindi, appare coerente con l'impostazione che in maniera corretta mette in evidenza la natura originaria di merce del denaro: i bitcoin hanno certamente delle differenze evidenti rispetto a tutti gli altri beni che storicamente sono stati impiegati come denaro, a partire dai metalli preziosi, i quali mantengono una propria utilità anche a prescindere dall'utilizzo come denaro, tuttavia mettere in luce la natura originaria di bene, utilizzato poi come moneta, consente di recuperare la reale natura del denaro.

Se fornire una classificazione giuridica delle criptovalute, e in particolare dei bitcoin, solleva questioni di una certa complessità, ancora più problematico può risultare l'analizzare il fenomeno da un punto di vista prettamente fiscale. Con riferimento al trattamento fiscale da applicare a tali operazioni, non si può prescindere da quanto affermato dalla Corte di Giustizia dell'Unione europea nella sentenza del 22 ottobre 2015, causa C-264/14. In tale occasione, la Corte europea ha riconosciuto che le operazioni che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale bitcoin e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra il prezzo di acquisto delle valute e quello di vendita praticato da un operatore ai propri clienti, costituiscono

prestazioni di servizio a titolo oneroso. Più precisamente, secondo i giudici europei, tali operazioni rientrano tra le operazioni "relative a divise, banconote e monete con valore liberatorio" di cui all'art.135, paragrafo 1, lettera e) della direttiva 2006/112/CE. Quindi, in assenza di una specifica normativa applicabile al sistema delle monete virtuali, tale sentenza costituisce necessariamente un punto di riferimento sul piano della disciplina fiscale applicabile ai bitcoin. In particolare, in Italia, l'Agenzia delle Entrate ha deciso di pubblicare un parere accolto molto positivamente sia dagli utenti in possesso di BTC sia dalle società di intermediazione. Tale parere chiama direttamente la sentenza appena citata, la quale stabilisce legittimità e legalità dei bitcoin ed esonera utenti ed aziende al pagamento dell'imposta sul valore aggiunto (IVA). Quindi, non dovranno pagare l'IVA né i privati che posseggono un certo quantitativo di BTC, né le società di intermediazione che offrono la possibilità di convertire bitcoin in altri tipi di valuta e viceversa. Invece, dovranno pagare le imposte dirette (IRES[6] e IRAP[7]) i soggetti che offrono la suddetta intermediazione, con la tassazione proporzionata ai ricavi derivanti dall'acquisto e dalla vendita di bitcoin effettuata dai clienti finali. Infine, l'Agenzia delle Entrate ha stabilito che le persone fisiche che detengono bitcoin al di fuori dell'attività d'impresa, effettuando operazioni a pronti di valuta, non generano redditi imponibili poiché manca la finalità speculativa.

In sede conclusiva, è utile affermare che il sistema Bitcoin integra una fattispecie innovativa e complessa, le cui funzioni potenziali non sono forse compiutamente definite nemmeno dall'attuale utilizzo come mezzo di scambio e di investimento. Infatti, i bitcoin, consistendo in un protocollo di comunicazione crittografato, integrano un sistema multifunzionale di scambio estremamente versatile, suscettibile di molteplici ed ulteriori impieghi. Ad esempio, la tecnologia della blockchain potrebbe essere utilizzata in un modo multilivello, per registrare non solo le transazioni in criptovaluta, ma anche gli stessi contratti che rappresentano la causa giuridica dell'attribuzione patrimoniale che ne consegue. L'estrema versatilità della valuta va necessariamente tenuta in considerazione negli interventi legislativi futuri, al fine di adottare un modello giuridico il più coerente possibile al loro concreto utilizzo e alle attività economiche svolte attraverso questa (Mancini 2015).
Concludendo, affinché i bitcoin diventino una valuta riconosciuta legalmente dalla BCE e dalle altre banche centrali come moneta a tutti gli effetti, è anzitutto necessario che il loro valore

[6] IRES (Imposta sul reddito delle Società): imposta entrata in vigore nell'ordinamento italiano dal 1° gennaio 2014.
[7] IRAP (Imposta Regionale sulle Attività Produttive): introdotta dal d. legisl. 446/1997 al fine di conferire alle Regioni un tributo dal gettito rilevante, sostituendo numerose entrate poco sistematiche e fonti di distorsioni. Presupposto dell'imposta è l'esercizio abituale di un'attività autonomamente organizzata, diretta alla produzione o allo scambio di beni o alla prestazione di servizi

giornaliero si stabilizzi in modo da poter diventare affidabile nei traffici commerciali, sia come riserva di valore sia come unità di conto. Infatti, l'eccessiva volatilità che si evince dal grafico 2.1 è tipica di un investimento speculativo, più che di una valuta. Inoltre, come già spiegato, il sistema Bitcoin deve fronteggiare una serie di difficoltà dovute ai suoi prezzi con decimali non convenzionali rispetto ai beni comuni, alla carenza di acquirenti che accettino la valuta, alla difficoltà nel procurarsi i bitcoin da un venditore, oltre ad altri problemi minori. Infine, un'ulteriore barriera all'ampio utilizzo dei bitcoin, è rappresentata dalle conoscenze informatiche necessarie, le quali devono essere relativamente alte. Dal punto di vista legale, le transazioni in bitcoin sono rischiose a causa della mancanza di una disciplina a tutela del consumatore in questo ambito, come ad esempio previsioni di risarcimento in caso di contenzioso tra acquirente e venditore. Mentre la legge vigente fornisce regole basilari per risolvere tali dispute, nel caso dei bitcoin non vi è nessun presupposto per la sua applicazione, poiché, in ogni caso, i governi o le istituzioni non hanno alcuna via legale per pignorare o sequestrare i bitcoin. Problemi simili sorgono nella tutela dei crediti dei consumatori e nell'impegno dei bitcoin come garanzia per un prestito. A causa della mancanza di affiliazione con qualsiasi Stato sovrano, il Bitcoin si dimostra inadatto all'uso nei mercati creditizi, poiché nessuna istituzione può intervenire realmente o appropriarsene in caso di default. La valuta sembra soffrire dall'essere disconnessa e isolata dai sistemi bancari e di pagamento degli Stati Uniti e di altri Paesi. La maggior parte delle monete infatti, sono custodite e trasferite tramite conti correnti bancari personali, i quali a loro volta sono protetti da regolamentazioni, assicurazioni sul deposito e trattati internazionali. Senza l'accesso a queste infrastrutture il Bitcoin si è dimostrato essere vulnerabile a frodi e furti da parte di abili hacker. Ciò nonostante, molti sostenitori hanno argomentato che il sistema Bitcoin ha sorpassato tutti i difetti dei sistemi di sicurezza finanziaria standard.

Infine, i bitcoin affrontano un problema economico-strutturale di lungo termine relazionato al limite massimo di 21 milioni di unità che possono essere emesse, a cui si aggiunge la mancanza di possibilità di espansione dell'offerta dopo l'anno 2140. Se i bitcoin otterranno un enorme successo e subentreranno alle valute correnti, verrà esercitata nell'economia una forza deflazionistica fino al punto in cui l'offerta non aumenterà insieme alla crescita economica. Tale situazione implicherà un numero sempre maggiore ogni anno, di lavoratori che accettino pagamenti in bitcoin, probabilmente facendo nascere proteste politiche contro la valuta simili a quelle già avvenute negli USA durante il movimento populista alla fine del XIX secolo[8].

[8] Una delle figure più significative di questo movimento, fu il politico William Jennings Bryan, il quale con il suo celebre discorso "Cross of Golds" si candidò alla Casa Bianca, sostenedo la teoria e la creazione di una futura moneta caratterizzata da un'offerta inflessibile.

CAPITOLO 3. TRA RISCHI ED OPPORTUNITÁ: IL BITCOIN OGGI

Nonostante siano trascorsi appena nove anni dalla pubblicazione di Nakamoto e dalla creazione dei primi bitcoin, il fenomeno è stato accolto a livello universale con un entusiasmo crescente, tanto da essere stato collocato, dal Time nel 2014, al primo posto tra i dieci eventi più rilevanti dell'anno. Ad oggi, i risvolti pratici e le opportunità legate alla prima valuta veramente globale e mondiale sono molteplici e, forse, ancora più numerose sono le proposte innovative a cui è sottoposta. Tuttavia, nella seppur breve storia, i bitcoin hanno vissuto degli avvenimenti che ne hanno segnato profondamente l'andamento; certamente alcuni ne hanno accresciuto la popolarità, mentre altri ne hanno compromesso, almeno temporaneamente, la reputazione. Di seguito, si esporranno quattro casi reali di una certa rilevanza: i primi due, abbastanza drammatici, vogliono fungere da esempio per sottolineare i rischi e le conseguenze di un uso non appropriato e scorretto dei bitcoin; gli ultimi due, invece, sono applicazioni pratiche del fenomeno, che espongono solo alcune delle innumerevoli opportunità, il cui intento mira al miglioramento del benessere della collettività.

3.1. IL CASO MTGOX

Il metodo più immediato per entrare in possesso di bitcoin è quello di ricorrere ad una Borsa, la quale, tra gli appartenenti alla comunità Bitcoin, viene comunemente denominata Bitcoin *exchange*. Attualmente esistono numerose *exchange* sia per i bitcoin, sia per altre cripto-valute, le quali permettono agli utenti di vendere e acquistare cripto-monete in cambio di valuta reale, solitamente il dollaro statunitense. Tali Borse online funzionano come dei veri e propri mercati: si raccolgono tutti gli ordini di vendita e di acquisto dei clienti e successivamente si trovano le controparti; tuttavia non è l*'exchange* che si pone come intermediario della transazione di un soggetto, ma semplicemente si limita ad abbinare con un meccanismo automatico gli ordini già presenti. Gestire un'attività con queste peculiarità richiede una particolare attenzione relativamente alla sicurezza degli account e delle password degli utenti, poiché una violazione perpetrata da terze parti può compromettere l'intero sistema. La Borsa, inoltre, deve tassativamente assicurare una manutenzione adeguata dei *wallet* della criptovaluta, aggiornandoli e correggendo eventuali bug.

Quello descritto era il contesto in cui operava MtGox, una delle prime e principali borse per bitcoin, attiva fino al 2014. Di seguito verrà esposto l'emblematico caso che ha portato alla sua chiusura, necessario per comprendere i rischi nel sistema Bitcoin se non vengono prese opportune misure di sicurezza. MtGox nasce nel 2009, a Tokyo, come piattaforma di trading

online per le carte da gioco di *"Magic: The Gathering Online eXchange*", da cui appunto prende il nome. Nel 2010 il suo fondatore, l'ingegnere informatico Jed McCaleb, decise di trasformare MtGox in una Borsa di bitcoin, diventando in breve tempo la più importante per i volumi scambiati. Nel marzo 2011, McCaleb vendette la piattaforma a Mark Kerplès, sviluppatore di software francese, che a quel tempo lavorava a Tokyo. Appena tre mesi dopo, l'*exchang*e si trovò ad affrontare i primi problemi: il sito fu vittima di un attacco hacker che compromise moltissimi username e password. In tale occasione, i responsabili dell'attacco furono in grado di accedere alla piattaforma tramite l'account di un auditor (revisore contabile), inviando un ordine di vendita enorme, per un ammontare inesistente di bitcoin. Ciò portò inevitabilmente ad un crollo del tasso di cambio BTC/USD da $17,51 a $0,01 in pochi minuti, seguito da forti disagi e lamentele da parte degli utenti. Come prima contromisura, la direzione di MtGox decise di annullare tutte le operazioni avvenute in giornata e di sospendere il sito per controlli e manutenzione. Tuttavia, i ritardi nei prelievi e nei depositi da e sulla piattaforma non furono un caso isolato in seguito all'attacco, ma continuarono per i mesi successivi, sollevando così numerosi dubbi sulla solvibilità di MtGox. Nonostante ciò, la Borsa continuò ad operare quotidianamente senza rilevanti problemi fino all'aprile 2013, momento che segnò l'inizio del declino definitivo della piattaforma. MtGox infatti, fu vittima di un *Distribuited Denial of Service* (DDoS), cioè di un tipo di attacco informatico, proveniente da più fonti, che mira a rendere - temporaneamente o indefinitamente – non disponibili i servizi di una rete, e che quindi, in questo caso, comportò numerosi ritardi e problemi negli scambi.
A ciò si aggiunse il fatto che nell'ultimo periodo, durante le ore più affollate, tali problemi iniziavano ad essere sempre più frequenti. Inoltre, nel maggio 2013 il Dipartimento di Sicurezza Nazionale degli Stati Uniti sequestrò il conto che la Borsa aveva presso Dwolla, il suo principale *payment provider*, poiché quest'ultimo non si era registrato presso il FinCEN (Financial Crimes Enforcement Network). Nel mese successivo vennero sospesi temporaneamente tutti i prelievi di dollari e per la Borsa diventò impossibile operare. Si giunse così al fallimento nel febbraio 2014.

Alla base del crollo del sistema vi è il software utilizzato da MtGox per la gestione delle transazioni, ed in particolare il modo in cui questo poneva rimedio al *transaction malleability bug*, un'imperfezione che risiede all'interno dello stesso protocollo Bitcoin. Come già visto, durante una transazione bitcoin, il mittente firma digitalmente l'informazione o il messaggio che vuole trasmettere, generando così un ID che li identifica univocamente. Tuttavia tale ID proviene anche da una parte di transazione che non viene firmata digitalmente, e per questo può essere facilmente modificata senza il permesso del mittente, creando così una situazione non

protetta dal punto di vista della sicurezza. Tale bug è comunque noto alla comunità dal 2011 e viene agevolmente aggirato tramite software che registrano accuratamente tutti i movimenti e le transazioni degli utenti. La stessa Bitcoin Foundation, l'ente che promuove lo sviluppo e la diffusione della criptovaluta, ha affermato che ogni società operante con transazioni in bitcoin deve trovare un software per gestire tale falla; generalmente la soluzione maggiormente adottata è stata quella di impedire l'accettazione di transazioni con ID inizianti con la cifra zero. Tuttavia, il software di MtGox riconosceva e accettava anche le operazioni *zero-padded*, lasciando la piattaforma completamente scoperta al problema della *transaction malleability*. La vulnerabilità a questo bug rese la piattaforma vittima di numerosi furti e frodi, che prosciugarono completamente l'*exchange wallet*. A rendere la situazione ancora più critica vi era, sul sito della Borsa, una pagina elencante tutte le transazioni fallite. Nel dettaglio, il processo che portò al crollo dell'*exchange* si svolgeva nel seguente modo:

1. Quando un utente di MtGox trasmetteva un'operazione tramite la piattaforma, vi era la possibilità che la transazione conseguente risultasse con un ID *zero-padded*;
2. In tale ipotesi, la transazione era rifiutata dagli altri software di gestione delle transazioni (i quali avevano adottato opportune precauzioni) e quindi questa veniva ritardata;
3. Gli utenti prendevano visione della pagina elencante tutte le transazioni fallite, fornita dalla medesima Borsa, e successivamente le ritrasmettevano eliminando gli zero iniziali;
4. A questo punto, la transazione con l'ID modificato veniva accettata dal network Bitcoin e registrata nella blockchain. Tuttavia, per MtGox, inconsapevole della modifica, la transazione continuava a risultare fallita, poiché il software attendeva il riconoscimento dell'operazione con l'ID originario *zero-padded.* Di conseguenza, i bitcoin associati a questa transazione figuravano disponibili per operazioni future, quando in realtà erano già stati spesi.

Questo meccanismo si trasformò in un vero e proprio circolo vizioso che durò per diversi mesi, fino al momento in cui la Borsa si ritrovò costretta a sospendere tutte le transazioni in bitcoin, poiché era diventato impossibile sapere realmente quanti Bitcoin fossero effettivamente in suo possesso e quante transazioni, invece, erano state alterate (si veda Mancini Ianiro 2014).

A tutte queste problematiche va aggiunta, inoltre, la presenza di un approccio lasso verso la contabilità; secondo Ryan Selkis, imprenditore del sistema Bitcoin, la Borsa MtGox non ha mai eseguito alcuna procedura di auditing nei confronti dei propri clienti.

Tutto ciò ha condotto MtGox a dichiarare bancarotta il 28 febbraio 2014 in Giappone e solo un mese dopo anche negli Stati Uniti, per evitare che gli utenti si impadronissero di tutti i suoi *asset*, tramite una *class action* già avviata da una parte dei suoi clienti. Secondo quanto riportato

da “bitcoinquotidiano”, si stima che oltre 800.000 bitcoin, un quindicesimo dei dodici milioni in circolazione, al tasso di cambio del giorno dell’annuncio con un valore di più di 450 milioni di dollari, sono stati oggetto di furti, truffe o perdite. Gli utenti coinvolti sono stati poco più di un milione di utenti.

3.2. IL PORTALE SILK ROAD

Uno degli episodi più gravi legati al mondo dei Bitcoin è indubbiamente quello del caso Silk Road, giunto alla cronaca mondiale nell’ottobre 2013, con l’arresto del suo fondatore Ross William Ulbricht, meglio conosciuto con lo pseudonimo “Dread Pirate Roberts”. Silk Road, operativa dal gennaio 2011, come intermediario - in maniera similare ad eBay - forniva agli acquirenti ed ai venditori una piattaforma online in cui poter scambiare i propri beni o servizi. A differenza però degli altri siti di vendita online, Silk Road forniva ai suoi utenti un alto livello di anonimato e le merci offerte appartenevano al “mercato nero” e principalmente consistevano in narcotici, materiale pornografico, armi, servizi di falsificazione di documenti e ingaggio di sicari. Innanzitutto, Ulbricht basò il funzionamento della piattaforma tramite TOR (*The Onion Router*), uno speciale network di computer localizzati in tutto il mondo e connessi tramite internet, pensato per nascondere il vero indirizzo IP del computer e, di conseguenza, l’identità dell’utente. In secondo luogo, Ulbricht progettò Silk Road includendo un sistema di pagamento basato unicamente sull’utilizzo di bitcoin, in modo da facilitare il commercio illegale che si svolgeva nel sito, nascondendo l’identità e la localizzazione degli utenti.

Quindi, successivamente all’acquisto di una somma di bitcoin presso un *exchange*, un qualsiasi soggetto poteva creare il proprio account sulla piattaforma illegale ed iniziare ad acquistare droghe da individui provenienti da tutto il mondo e vedersele recapitate a casa nel giro di pochi giorni, tramite il servizio postale degli Stati Uniti d’America.

Il portale Silk Road utilizzava i bitcoin perché possono essere spesi e accumulati come il denaro, senza la necessità di una terza parte che registri la transazione, la quale, a differenza di PayPal o altri sistemi di pagamento online, non è tracciabile. Inoltre, la piattaforma si avvaleva di un sistema denominato “tumbler” (lett. acrobata), il quale trasformava tutti i pagamenti attraverso una serie semi-random di transazioni dummy, rendendo praticamente impossibile il collegamento tra l’operazione effettuata e i soldi circolati nel sito.

In seguito alle indagini effettuate, il 25 ottobre 2013, l’FBI e la procura degli Stati Uniti del distretto del New York hanno comunicato che i bitcoin circolanti in Silk Road erano approssimativamente 173.991, per un valore pari a 33,6 milioni di dollari. È curioso notare che, appena qualche settimana dopo, il valore di questi 173.991 bitcoin era duplicato arrivando a toccare un picco di 70 milioni di dollari, probabilmente dovuto all’improvvisa popolarità della

valuta e alle visioni e aspettative dei possibili utilizzi in futuro Il 16 gennaio dell'anno successivo, vennero confiscati circa 29.655 bitcoin (per un valore di 28 milioni di dollari) e sequestrata l'intera piattaforma online. Solamente dieci giorni dopo, venne rilasciato un fermo nei confronti delle persone Robert Faiella e Charlie Shrem, Chief Executive Officer di una Borsa di bitcoin, accusati di aver venduto oltre un milione di dollari in bitcoin agli utenti di Silk Road. Dalle denunce penali emerse che, dal dicembre 2011 all'ottobre 2013, Faiella gestì un business di scambio illecito della criptovaluta sul sito illegale, operando sotto il falso nome di "BTCKing" e vendendo bitcoin - l'unica forma di pagamento accettata - ai soggetti interessati ad acquistare sostanze stupefacenti. Non appena riceveva gli ordini dagli acquirenti di Silk Road, questi li trasmetteva alla compagnia "New York" con sede a New York. La società, a cui capo vi era Shrem, era stata costituita con l'obiettivo di permettere ai suoi clienti di cambiare denaro in bitcoin in maniera totalmente anonima, senza fornire o rilasciare alcuna informazione personale circa l'identità, e ovviamente, a questo servizio veniva applicata una tariffa che procurava ulteriori guadagni. Faiella, quindi, otteneva i bitcoin con il consenso e l'assistenza della compagnia e successivamente li rivendeva con un *markup* agli utenti della piattaforma. Shrem, il quale in passato aveva acquistato personalmente stupefacenti su Silk Road, era pienamente consapevole dell'attività criminale svolta dal sito web, ed inoltre, grazie al rapporto di confidenza con Faiella, era a conoscenza del servizio di intermediazione che quest'ultimo svolgeva. Nonostante ciò, il CEO non denunciò mai nulla, anzi curava personalmente le transazioni del BTCKing, in quanto erano una fetta di guadagno notevole negli utili della New York. Sul finire del 2012, quando la compagnia pose fine alla possibilità di effettuare pagamenti in contanti, Faiella cessò temporaneamente la sua attività illecita sulla piattaforma. Nell'aprile 2013 tuttavia, riprese le normali operazioni anche senza l'assistenza della compagnia e continuò a cambiare in bitcoin decine di migliaia di dollari a settimana, fino al momento in cui, nell'ottobre dello stesso anno, Silk Road fu definitivamente chiusa dalle autorità giudiziarie.

Secondo l'FBI, non è comunque possibile stabilire una cifra esatta dei guadagni del Dread Pirate Roberts (DPR), poiché il volume totale delle operazioni effettuate sulla piattaforma cresceva ad un tasso solo approssimativamente costante e soprattutto non si ha alcuna informazione riguardante gli acquisiti avvenuti nei mesi di maggio, giugno e settembre 2013, in quanto DPR ha comunque continuato a ricevere commissioni per le quali sono stati utilizzati sempre computer differenti che l'FBI non è mai riuscito a ritrovare o a penetrare; inoltre, durante le indagini è emerso che un terzo dei bitcoin di tali account furono spostati prima dell'arresto. Comunque si suppone che il mercato di Silk Road generasse ricavi di vendita per più di 9.5 milioni di bitcoin, ai quali va aggiunto un tasso medio di commissioni del 6,67%, pari a circa 633.000 bitcoin. Tuttavia, il problema maggiore risiede nella natura stessa della valuta,

in quanto, anche nel caso in cui tutti i bitcoin venissero localizzati, non sarebbe comunque possibile per l'FBI entrarne in possesso, essendo crittografati (si veda Trautman, 2014).

3.3. SALVARE L'EUROZONA: LA SOLUZIONE DI VAROUFAKIS

Yanis Varoufakis, Ministro delle Finanze durante il primo Governo Tsipras e professore di teoria economica all'Università di Atene, è uno studioso e acceso sostenitore del sistema Bitcoin e delle cripotvalute in generale. In numerosi articoli sul suo blog yanisvaroufakis.eu, ne ha analizzato le origini e la teoria, arrivando ad ipotizzare applicazioni pratiche per diminuire il peso dell'austerity imposta dall'Europa a molti paesi dell'eurozona.

Era il 13 marzo del 2014 quando l'allora ministro nel suo blog personale già definiva i bitcoin come "un meraviglioso algoritmo, l'idea più geniale del XXI secolo, di cui gli economisti non hanno ancora capito il potenziale". E proprio in quel periodo di scarsa liquidità in Grecia, caratterizzato da chiusura delle banche, limiti ai prelievi bancomat, difficoltà ad operare acquisti online a causa dei controlli sui conti collegati agli account, le operazioni in bitcoin cominciarono a lievitare esponenzialmente. Per dare un'idea, tra maggio e giungo dello stesso anno, periodo serratissimo di trattative tra Atene e i creditori per la negoziazione del debito, il valore dei bitcoin in Grecia aumentò di quattrocento volte e i depositi quadruplicarono, arrivando ad un valore medio di 700 euro. L'utilizzo dei bitcoin, infatti, consentì ai cittadini di aggirare i controlli sui capitali e mantenere al sicuro i propri risparmi: il meccanismo consisteva nell'utilizzare gli euro per acquistare i bitcoin, i quali non erano soggetti a nessun controllo, in modo da aggirare i controlli e le restrizioni imposte dallo Stato; nel momento in cui la situazione sarebbe ritornata stabile, i bitcoin sarebbero stati riconvertiti in euro, così da poter rientrare in pieno possesso di tutto il denaro e disporne in assoluta libertà, senza vincoli troppo stringenti.

Secondo la visione di Varoufakis, il sistema Bitcoin è una versione più intransigente e accurata del *Gold Standard,* in quanto l'offerta di moneta è fissata algoritmicamente e con un tasso di crescita predeterminato. Per l'euro invece, vale il moltiplicatore monetario: la banca centrale controlla la base monetaria e poi, attraverso il sistema dei depositi nella banche private, si crea moneta aggiuntiva, come ad esempio M2. Da qui, la principale differenza dell'euro rispetto alla criptovaluta, in quanto non è fissato un limite massimo alla quantità di moneta emettibile. Le banche private dell'Eurozona sono influenzate e sollecitate dagli stati membri: in altre parole, a seconda dello "spirito animale"[9] delle banche e dei cittadini, il sistema bancario dell'Eurozona

[9] Varoufakis usa letteralmente l'espressione animal spirits per indicare l'ottimismo delle banche e dei consumatori.

conia effettivamente moneta; le banche private, infatti, sono responsabili di oltre il 90% dell'offerta di euro.

Varoufakis, quindi, individua una potenziale applicazione del sistema Bitcoin nelle periferie dell'Eurozona, le quali sono asfissiate dalla politica monetaria attuale e colpite da un'ondata di recessione e deflazione. Le economie di questi Stati hanno un bisogno disperato di liquidità e di un alleggerimento dell'*austerity*, tuttavia, secondo l'ex ministro, il fulcro del problema risiede nel fatto che i leader europei si rifiutano addirittura di iniziare un dibattito logico e razionale sulle riforme istituzionali che potrebbero rendere l'Eurozona nuovamente sostenibile. La soluzione viene individuata nella creazione, da parte dei Paesi periferici, di un proprio sistema di pagamento, garantito dalle tasse future e nominativamente legato all'euro. Inoltre, essi potrebbero usare un algoritmo simile a quello dei Bitcoin per rendere il sistema trasparente, efficiente e senza costi di transazione. Il sistema pensato da Varoufakis, alla cui base ci sarebbe una moneta fiscale, prenderebbe il nome di FT-coin, dove FT sta per *Future Taxes* (Tasse Future) e funzionerebbe come segue:

il cittadino paga, ad esempio, 1000 euro per acquistare 1 FT-coin da una piattaforma web di Tesoreria Nazionale la quale ha un contratto che la impegna a: (a) cambiare 1 FT-coin con 1000 euro in qualsiasi momento o (b) accettare il FT-coin due anni dopo la sua emissione come strumento di pagamento che estingue 1.500 euro dovuti in imposte. Chiaramente, ciascun Paese (Italia, Spagna, Irlanda) avrebbe un proprio mercato di questa valuta complementare. Ogni anno, successivamente all'entrata in vigore del sistema da almeno due anni, la Tesoreria emette un nuovo lotto di FT-coin al fine di sostituire quelli che sono stati estinti con il pagamento delle tasse. Tale sistema si baserebbe sulla previsione che il numero totale di FT-coin in circolazione non eccederebbe mai una certa percentuale del PIL, ad esempio il 10%.

Una volta in possesso dei FT-coin, il cittadino potrà liberamente decidere se conservarli in un *e-wallet* o utilizzarli nelle transazioni comuni. Per avere la certezza che il sistema sia completamente trasparente e che le transazioni siano gratis, FT-coin dovrebbe avere alla base lo stesso algoritmo utilizzato dai Bitcoin ed essere supervisionato da un'autorità nazionale indipendente non governativa. Come nel caso specifico della criptovaluta, l'ammontare totale di FT-coin potrebbe essere fissato in relazione ad una variabile che non sia controllata dal governo, ad esempio il PIL nominale, mentre ogni singola transazione potrebbe essere monitorata e controllata dalla comunità, con gli stessi funzionamenti ipotizzati da Nakamoto.

Tale sistema porterebbe grandi vantaggi, in quanto creerebbe:

- Una fonte di liquidità per i governi esterna al mercato dei titoli di Stato, che non coinvolgerebbe le banche

- Un’offerta nazionale di euro perfettamente legale nel contesto dei trattati europei, la quale potrebbe essere utilizzata per aumentare il benessere degli elementi più deboli della società o per pagare alcune opere nazionali assolutamente necessarie;
- Un metodo di pagamento trasparente e completamente gratuito, scollegato dalle banche e monitorato dai cittadini.

Concludendo, Varoufakis sottolinea che, mentre i bitcoin, per loro natura, sono caratterizzati da una prevedibile deflazione e quindi risultano inadatti ad essere una valuta alternativa all’euro o al dollaro, il sistema dei FT-coin potrebbe essere utilizzato profittevolmente al fine di aiutare gli Stati dell’Eurozona a creare un sistema di pagamento elettronico, comunque legato all’euro, il quale consentisse, almeno nel medio termine, di superare l’asfissiante pressione deflazionistica imposta dalla politiche di *austerity*.

3.4. IL CROWDFUNDING

Secondo una definizione comunemente accettata, il *crowdfunding* (lett. crowd folla e funding finanziamento) è la raccolta di capitale tramite portali online che ha l’obiettivo di finanziare gli sforzi di persone e organizzazioni, mediante un processo collaborativo di molteplici soggetti che utilizzano il proprio denaro in comune. Tale fenomeno si caratterizza, innanzitutto, per l’orizzontalità del finanziamento, cioè per la sua attitudine a provenire dal basso, da una folla di investitori atomistici e puntiformi che investono generalmente piccole somme di denaro, ma che nel complesso raggiungono cifre importanti; in secondo luogo, si caratterizza per la dipendenza dalla rete Internet. L’attività di *crowdfunding*, infatti, è inscindibile dallo sviluppo di piattaforme online che permettono il collegamento tra i finanziatori e i beneficiari delle donazioni; tale circostanza rende il *crowdfunding* un fenomeno della rete.

Le piattaforme di *crowdfunding* basate su sistemi di pagamento Bitcoin sono un fenomeno presente già da alcuni anni, ma che hanno avuto una diffusione significativa solo negli ultimi tempi. Da alcuni studi, infatti, emerge che nell’ecosistema della criptovaluta esistono molteplici attività basate su uno scambio continuo di piccole quantità di bitcoin, frazioni che solitamente variano dal milionesimo al millesimo di bitcoin. Tale “sottobosco” di operazioni ha un ruolo fondamentale nella diffusione capillare della valuta virtuale e tuttora funge da ostacolo alla concentrazione della moneta nelle mani di pochi eletti. L’interesse verso questa realtà è ancora limitato, ma potrebbe crescere in misura significativa qualora questi organismi, - per il momento in uno stato di concorrenza perfetta - dovessero crescere economicamente a fronte della prevedibile crescita di interesse per il mercato del Bitcoin nel prossimo futuro. Inoltre, è opportuno sottolineare che, almeno in Italia, non vi sono particolari ostacoli legislativi alla diffusione di piattaforme di *crowdfunding* basate sul sistema di scambio di bitcoin, purché

queste operazioni non comportino circolazione di moneta avente corso legale e non finanzino progetti al di fuori della legalità (si veda Caroli e Chiari 2013).

Data la velocità delle transazioni e l'assenza di costi di commissione, si può affermare che il sistema Bitcoin si adatta perfettamente alla funzione richiesta per questo tipo di attività, inoltre, trattandosi comunque in sostanza di donazioni, viene fatto particolare affidamento all'acquisto d'impulso e alla leva emotiva, permettendo di donare immediatamente criptovaluta tramite un'applicazione dal cellulare, ad esempio BitPay, la quale nel passato ha permesso agli utenti di inviare donazioni in BTC alla Croce Rossa in Nepal. Molte organizzazioni, tra le quali Save the Children, hanno iniziato ad attivare sul proprio sito una raccolta di bitcoin da convertire successivamente in moneta avente corso legale; attualmente se ne contano più di cento, differenziate in base al tipo di attività a cui le donazioni saranno devolute; è possibile spaziare infatti dall'arte all'open source, passando per intrattenimento, attivismo e religione. In tale panorama non si può non citare la Bitcoin Foundation (bitcoinfoundation.org), entità chiave dell'intero ecosistema, riconosciuta come imparziale e terza dalle altre organizzazioni del settore, ha come obiettivo principale standardizzare, tutelare e promuovere l'uso della criptovaluta al fine di procurare benefici a tutti gli utilizzatori del mondo, inclusi coloro che se ne vogliono avvalere per attività di crowdfunding.

Probabilmente, i maggiori beneficiari di questo innovativo metodo di finanziamento saranno le organizzazioni no-profit, in quanto, a differenza delle donazioni tradizionali, la criptovaluta permette ai cittadini di donare qualsiasi ammontare di denaro in qualsiasi momento e istantaneamente; inoltre, attraverso l'uso dei bitcoin, le tariffe e le commissioni legate alle transazioni, anche quelle con scopo benefico, si ridurrebbero notevolmente, consentendo quindi di far giungere l'intero importo alla reale causa e non disperso tra vari intermediari.

In tale scenario si colloca la particolare iniziativa intrapresa dall'associazione ambientalista Legambiente, prima organizzazione no-profit del nostro territorio, che ha avviato, lo scorso dicembre, una nuova collaborazione con la startup Helperbit al fine di adottare la tecnologia Bitcoin e blockchain, aggiungendo così un ulteriore canale per le raccolte fondi e offrendo, allo stesso tempo, ai propri donatori trasparenza e tracciabilità dei flussi economici. Nella fase introduttiva, questo progetto verrà riservato alla campagna di raccolta fondi "La rinascita ha il cuore giovane", lanciata con il fine di aiutare giovani imprenditori delle aree colpite dal sisma, accelerare la ricostruzione del tessuto produttivo e rafforzare il sostegno a tali comunità. È un'iniziativa particolarmente innovativa in questo ambito, che offre molteplici vantaggi in termini di sicurezza, tempi e costi e permette inoltre di aprirsi a panorami internazionali, ricevendo donazioni di bitcoin provenienti da tutto il mondo. Per intraprendere questo percorso, Legambiente ha deciso di affidarsi a Helperbit, startup italiana che utilizza la tecnologia

Blockchain nel settore della beneficenza e delle emergenze umanitarie, vincitrice di diverse competizioni internazionali e selezionata dalle Nazioni Unite per il World Humanitarian Summit. Guido Baroncini Turricchia, amministratore delegato e co-fondatore della startup, ha affermato e in un certo senso auspicato che "La sicurezza dimostrata sui temi della trasparenza legata alla blockchain e la propensione all'innovazione rendono Legambiente una delle no-profit italiane più all'avanguardia. Spero che questa realtà sia da esempio, e stimoli anche altre no-profit ad intraprendere un percorso volto alla trasparenza". Al momento della contribuzione infatti, sarà possibile prendere visione di tutte le donazioni e successivamente, tramite la piattaforma di Helpberit, si potrà verificare come i fondi vengono spesi, avere la garanzia che abbiano raggiunto la destinazione finale e monitorare l'impatto derivante dagli aiuti economici.

CONCLUSIONI

In questo elaborato si è voluto fornire un quadro sulla situazione attuale di uno dei fenomeni che probabilmente influenzeranno in misura maggiore il futuro sistema dei pagamenti: i Bitcoin. In particolare, nella prima parte, si è analizzato il fenomeno da un punto di vista tecnico, spiegando le basi del funzionamento di una normale transazione in criptovaluta. L'aspetto più rilevante è l'assoluta autonomia da qualsiasi istituzione o ente centrale: il sistema Bitcoin, nelle intenzioni di chi l'ha progettato e per questa sua caratteristica, sembra rendere possibile un libero mercato, indipendente dal controllo dello Stato sulle riserve monetarie. Tuttavia, è necessario considerare il fatto che il volume scambiato delle transazioni bitcoin è di modeste dimensioni e, pertanto, non rappresenta minimamente una minaccia né per le Banche Centrali, né per la permanenza sul mercato degli intermediari che gestiscono i sistemi di pagamento tradizionali.

Ad un'attenta analisi dal punto di vista economico, inoltre, emerge, in tutte le sue sfaccettature, l'inadeguatezza del bitcoin circa il suo utilizzo come moneta, in quanto, come si è visto, non assolve le tre funzioni caratteristiche.

Infatti, l'unica funzione che attualmente soddisfa pienamente è quella di mezzo di scambio, ma il numero di punti vendita disposti ad accettarli è ancora troppo esiguo per permetterne una facilità di utilizzo. Inoltre, la sua eccessiva volatilità non le permette di possedere le caratteristiche né di unità di conto né di riserva di valore. Ma è soprattutto la mancanza di una disciplina che ne regoli gli aspetti di circolazione e funzionamento che costituisce la maggiore criticità di utilizzo, tanto da rendere le sorti del bitcoin nella realtà effettiva, e non virtuale, incerte, e che, di conseguenza, dipenderanno dalle future scelte dei vari legislatori.

L'obbiettivo che si è cercato di perseguire in questa trattazione non era di stabilire – in seguito alle dovute premesse di definizione, funzionamento, caratteri generali - un giudizio assoluto e definitivo della criptovaluta, come rischio od opportunità *tout court*, bensì di fornire, in un'ottica che è e che non può non essere comunque critica, le conoscenze di base necessarie per poter formulare un autonomo giudizio su questo fenomeno nuovo, in evoluzione ed, in parte, ancora in via di sviluppo. Proprio per questo, sarà necessario comunque tenersi sempre aggiornati, non lasciandosi condizionare dall'entusiasmo e dalle speculazioni che sempre accompagnano questi fenomeni innovativi, al fine di cogliere appieno tutte le opportunità e i benefici che i bitcoin possono dare alla società, e, allo stesso tempo, facendo particolare attenzione ai rischi e ai punti deboli che questo sistema comporta.

BIBLIOGRAFIA

AGENZIA DELLE ENTRATE, 2016. *Risoluzione n.72/E*. Italia. Disponibile su: <http://www.agenziaentrate.gov.it/wps/content/nsilib/nsi/documentazione/normativa+e+prassi/risoluzioni/archivio+risoluzioni> [Data di accesso: 01/08/17]

ALI R., BARREDEAR J., CLEWS R., SOUTHGATE J., 2014. *Innovations in Payment Technologies and the Emergence of Digital Currencies*. Bank of England Quarterly Bulletin. Disponibile su: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2499397> [Data di accesso: 20/07/17]

BADEV A., CHEN M., 2014. *Bitcoin: Technical Background and Data Analysis*. Washington: Finance and Economics Discussion Series, Division of Research & Statistics and Monetary Affairs, Federal Reserve Board. Disponibile su: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544331> [Data di accesso: 26/07/17]

BANCA D'ITALIA, 2015. *Avvertenza sull'utilizzo delle cosìdette "valute virtuali".* Roma. Disponibile su: <https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/index.html> [Data di accesso: 19/07/17]

BURLONE P., CARIA R., 2014. *Bitcoin e le altre criptomonete*. Disponibile su: <https://iris.unito.it/retrieve/handle/2318/1551305/112620/IBL_Focus_234-De_Caria_Burlone.pdf> [Data di accesso: 22/07/17]

CAROLI S., CHIARI F., 2013. *Studio preliminare sul crowdfunding in Italia e sulla possibilità di piattaforme basate sul Bitcoin*. Disponibile su: <https://s3.amazonaws.com/academia.edu.documents/31671864/Team_Legal_Report.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1504196882&Signature=fwXOfGgU6KE4UvtenzupmI5aLpg%3D&response-content-disposition=inline%3B%20filename%3DProgetto_Bitcoin_Crowdfunding_Studio_pre.pdf> [Data di accesso: 05/08/17]

CIANIAN P., RAJCANIOVA M., KANCS A., 2016. The economics of Bitcoin price formation. Disponibile su:

<http://www.tandfonline.com/doi/abs/10.1080/00036846.2015.1109038> [Data di accesso: 26/07/17]

Corte di Giustizia dell'Unione europea, 22 ottobre 2015, causa C-264/14. Disponibile su: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128it.pdf> [Data di accesso: 28/07/17]

Direttiva del Consiglio Europeo 2016/112/CE del 28 novembre relativa al sistema comune d'imposta sul valore aggiunto. Disponibile su: <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32006L0112> [Data di accesso: 01/08/17]

EUROPEAN BANKING AUTHORITY (EBA), 2014. *EBA Opinion on "virtual currencies".* Disponibile su: <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> [Data di accesso: 19/07/17]

EUROPEAN CENTRAL BANK (BCE), 2012. *Virtual Currency Schemes*. Disponibile su: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> [Data di accesso: 19/07/17]

EUROPEAN CENTRAL BANK (BCE), 2015. *Virtual Currency Schemes – A Further Analysis.* Disponibile su: < https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> [Data di accesso: 19/07/17]

HABERMEIER K., LECKOW R., OURA H., e SESTENKO N., 2016. *Virtual Currencies and Beyond: Initial Considerations.* Disponibile su: <https://www.bitcoinnews.ch/wp-content/uploads/2013/12/sdn1603.pdf> [Data di accesso: 20/07/17]

IANIRO, MANCINI, 2014. *Bitcoin guida all'uso*. Padova: Exeo srl, pagine 74-79.

KOTKOWSKI R., LIGHTFOOT G., PIOTROWSKA A., POLASIK M., WISNIEWSKI T., 2015. *Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry*. Disponibile su: <http://www.tandfonline.com/doi/abs/10.1080/10864415.2016.1061413> [Data di accesso: 26/07/17]

MANCINI M., 2015. *Valute virtuali e Bitcoin, Analisi Giuridica dell'Economia*. Bologna, Il Molino. Disponibile su: <https://www.rivisteweb.it/doi/10.1433/80273> [Data di accesso: 29/07/17]

NAKAMOTO S., 2008. Bitcoin: *A Peer-to-Peer Electronic Cash System*, unpublished manuscript. Disponibile su: <https://bitcoin.org/bitcoin.pdf> [Data di accesso: 20/07/17]

TRAUTMAN L., 2014. *Bitcoin & What now after liberty reserve, Silk Road and MtGox?. Richmond Journal of Law and Technology*. Disponibile su: <http://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1400&context=jolt> [Data di accesso: 04/08/17]

VAROUFAKIS Y., 2014. *Bitcoin: A Flawed Currency Blueprint with a potentially useful application for the Eurozone*. Disponibile su: <http://www.bridgingeurope.net/uploads/8/1/7/1/8171506/_bref_commentary_y.varoufakis_bitcoin.pdf>
[Data di accesso: 04/08/17]

YERMACK D., 2013. *Is Bitcoin a Real Currency? An Economic Appraisal*. Cambridge: National Bureau of Economic Research. Disponibile su: <http://www.nber.org/papers/w19747.pdf> [Data di accesso: 26/07/17]

SITOGRAFIA

http://coinmap.org/#/world/47.18971246/14.72167969/5 [Data di accesso: 01/08/17]

https://it.investing.com/currencies/btc-usd [Data di accesso: 01/08/17]

https://bitcoin.org/it/ [Data di accesso: 01/08/17]

https://blockchain.info/it/charts [Data di accesso: 02/08/17]

https://support.coinbase.com/ [Data di accesso: 02/08/17]

https://www.bitcoin.com/ [Data di accesso: 01/08/17]

https://bitcoinmagazine.com/articles/the-silk-road-report/ [Data di accesso: 05/08/17]

http://www.bitcoinquotidiano.com/la-bancarotta-protetta-di-mtgox/ [Data di accesso: 05/08/17]

https://bitcoinfoundation.org/ [Data di accesso: 02/08/17]

https://en.bitcoin.it/wiki/Donation-accepting_organizations_and_projects [Data di accesso: 05/08/17]

http://rinascitacuoregiovane.it/oggi-le-donazioni-bitcoin-grazie-alla-startup-italiana-helperbit/ [Data di accesso: 05/08/17]

Parole totali: 14.020