UNIVERSITA' DEGLI STUDI DI PADOVA
DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI
"MARCO FANNO"

CORSO DI LAUREA IN ECONOMIA INTERNAZIONALE
L-33 Classe delle lauree in SCIENZE ECONOMICHE

Tesi di laurea

LE CRIPTO-VALUTE

THE CRYPTO-CURRENCY

Relatore:
Prof. TUSSET GIANFRANCO

Laureando:
VIGO PAOLO

Anno Accademico 2015-2016

SOMMARIO

INTRODUZIONE

Quello delle monete virtuali è un universo affascinante. Gli strumenti che ne derivano costituiscono l'insieme cangiante e in continua crescita delle cosiddette "cripto-valute", in grado di ridefinire i confini delle transazioni possibili, dalla più semplice alla più complessa, apportando cambiamenti epocali nello scambio di beni e servizi e modificando l'idea stessa del libero mercato. Decidere di trattare determinati argomenti e tralasciarne degli altri è fondamentale quando ci si trova di fronte ad un mare troppo vasto, che coinvolge informazioni provenienti dai più svariati campi, dall'informatica alla psicologia collettiva, e che considera situazioni poste al limite di una vera a propria "zona grigia" delle legislazioni esistenti. Scegliere gli argomenti da trattare muovendosi in questo universo in continua espansione prevede di fare delle scelte, selezionando solo alcuni punti di osservazione e raccontando quanto possibile e importante sia una rivoluzione che passa dal web all'economia reale, dal bit alla moneta fiat. Nel seguente elaborato affronterò i temi che riguardano la nascita e gli sviluppi del Bitcoin, le sue implicazioni monetarie, gli usi più frequenti. Collegherò l'evoluzione della cripto-valuta al fiorire dei mercati illegali all'interno del "dark web": dalla nascita di "The Silk Road" per la compravendita internazionale di sostanze stupefacenti, all'importanza del "dark market" come porto franco in grado di fornire informazioni e documenti estremamente interessanti (basti pensare al caso WikiLeaks), alle implicazioni di un sistema finanziario che non contempla intermediari e abbraccia l'anonimato, cercando infine di fornire un giudizio che tuttavia non potrà ancora essere definitivo ma pronto a considerare e presentare opinioni contrastanti.

CAPITOLO PRIMO –

LA CRIPTO-VALUTA NEL NUOVO SISTEMA ECONOMICO

Che l'economia globale si stia muovendo verso un futuro sempre più digitale è ormai un dato di fatto. La virtualità degli strumenti economici costituisce una pratica altrettanto assodata, soprattutto in relazione al mondo degli scambi economico-finanziari oggi realizzati attraverso modalità che solo alcuni anni fa avremmo considerato inattuabili. Quando utilizziamo bancomat, carte di credito, assegni oppure predisponiamo un bonifico bancario, la transazione non si conclude con il trasferimento del bene "carta moneta" ma con un trasferimento virtuale, che prevede in sostanza un processo di "informatizzazione" dello stesso concetto di moneta. Ciò per certo ha posto i presupposti per la nascita di monete elettroniche e del tutto virtuali come il Bitcoin. Le cosiddette cripto-valute costituiscono l'esempio (ed esperimento) più riuscito in tale ambito, rappresentando un vero e proprio segnale di svolta nel campo delle nuove tecnologie finanziarie. Il concetto di cripto-valuta ha origine nel 1998, a partire da un gruppo di affermati *crittografi* e ideatori del progetto "Cyber-Punks", tra i quali l'ormai noto Julian Assange (co-fondatore della piattaforma WikiLeaks) e una figura ancora non ben identificata che va sotto il nome di Satoshi Nakamoto, di cui parleremo nei capitoli a seguire. Partendo dalle indicazioni fornite dal noto programmatore Wei Dei, tali crittografi cominciarono ad interessarsi alle possibilità di sviluppo delle prime forme di *crypto-currency*, basandosi sull'idea che fosse possibile, una volta stabiliti i caratteri e i criteri di creazione, realizzare una moneta digitale che potesse semplicemente essere generata e distribuita tramite Internet. Dal progetto di questo gruppo di giovani informatici, nasce la prima vera "moneta alternativa" internazionalmente accettata, che va sotto il nome di Bitcoin (più brevemente: BTC), alla quale seguiranno altre forme ed imitazioni che sono state comunque in grado di raggiungere un consenso non indifferente soprattutto nell'ambito della FinTech. I principi guida della realtà BTC sono descritti in un documento pubblicato nel Gennaio 2009 e ora accessibile in rete (http://bitcoin.org/bitcoin.pdf). La pubblicazione di tale testo da parte di una fonte anonima, conosciuta con il nome di Satoshi Nakamoto, sancisce la nascita

del nuovo strumento valutario, evidenziandone gli aspetti innovativi e potenzialmente rivoluzionari e classificandolo come un progetto completamente *open-source.* È possibile individuare una delle principali motivazioni che hanno spinto lo stesso Nakamoto (sempre che possa essere considerato un individuo singolo) alla realizzazione della realtà BTC in questa sua breve citazione: "*Bitcoin is very attractive to the liberitarian viewpoint if we can explain it proprely".* Per certo, la natura liberista di questo nuovo strumento è da subito identificabile nelle sue modalità di gestione e diffusione: esso si basa sulla possibilità di effettuare transazioni da un soggetto all'altro, sfruttando un protocollo di tipo *peer-to-peer* (P2P), ad architettura distribuita, che non necessita di alcuna autorità centrale di gestione, controllo o governo. La mancanza di una gestione centralizzata comporta dunque l'assenza di figure intermediarie, consentendo di ottenere (ed è questo uno dei fattori di successo principali) l'anonimato, oltre che l'evidente abbattimento dei costi di transazione. Le transazioni vengono quindi consentite e certificate attraverso un database pubblico, distribuito e crittografato, che va sotto il nome di BlockChain (nei paragrafi a seguire).

Sulla base di questo modello originario, sono andate sviluppandosi numerose altre interessanti variazioni, che hanno portato alla creazione di altrettante cripto-valute (il sito altcoins.com ne riporta all'incirca 50). Tra queste l'originaria BTC costituisce sicuramente quella di maggiore successo, registrando una capitalizzazione di mercato pari a circa 10 miliardi di Dollari (Fonte: Blockchain.info, dati 20 Ottobre 2016). A seguire:

1. **Bitcoin (BTC)**: Capitalizzazione (USD): 10.085.494.745
2. **Ethereum (ETH):** Capitalizzazione (USD): 1.024.557.809
3. **Ripple (XRP):** Capitalizzazione (USD): 315.702.720
4. **Litecoin (LTC):** Capitalizzazione (USD): 181.668.004

(Fonte: www.coingecko.com , dati 20 Ottobre 2016)

Tra queste principali cripto-valute, la scelta di trattare in particolare il caso del Bitcoin, è stata dettata non solo dal fatto che, ad oggi, risulti essere la moneta virtuale più diffusa,

ma anche da motivazioni "gerarchiche", essendo il sistema su cui il BTC è stato costruito, lo schema originario e fondamentale su cui si baserà la costruzione di tutte le altre monete virtuali.

1.1 La nascita del Bitcoin: Satoshi Nakamoto

"*Ci sono molti modi per fare soldi: puoi guadagnarli, rubarli, falsificarli o, se sei Satoshi Nakamoto, puoi semplicemente inventarli*". Così Joshua Davis (The New Yorker) nel 2011 apriva l'articolo relativo al misterioso fondatore della prima cripto-valuta. In effetti, quello che è successo la sera del 3 Gennaio 2009 poco si allontana dalla definizione di "invenzione". La creazione della nuova valuta in quella stessa sera non prevedeva l'utilizzo di carta, argento o oro; quanto piuttosto un codice originario composto da circa 31000 stringhe e un annuncio su Internet. Nakamoto, che si presentava come un giovane giapponese di 36 anni, affermò di aver impiegato più di un anno a creare il software necessario, mosso in parte dalla rabbia nei confronti della recente crisi finanziaria, in parte dal sogno di creare una valuta che risultasse impermeabile alle imprevedibili politiche monetarie. Le varie pubblicazioni di Nakamoto erano realizzate utilizzando un indirizzo di posta elettronica registrato su un mail hosting anonimo (Vistomail) e un account di webmail gratuito (gmx.com), connesso ad un browser che ne garantisse l'anonimato. Da subito sono sorte numerose teorie relative alla sua identità: da chi lo considera la cima di un perfetto "*Schema Ponzi"* (vedi sotto-capitolo 2.3.1), a chi sostiene che Nakamoto sia solo un nome multiplo sotto il quale agisce programmaticamente "*un nucleo di destabilizzatori del senso comune*" (fonte: Bitcointalk.org). Quello che sappiamo per certo è che a partire dalla fine del 2010 Nakamoto abbia definitivamente abbandonato il progetto Bitcoin, anche questa volta annunciando, tramite una pubblicazione anonima, che fosse arrivato il momento di "pensare a cose più importanti".

1.2 La rete BTC

La creazione del Bitcoin risponde esattamente alla filosofia "diffusa" della rete: è privilegiato l'utilizzo di strumenti considerati "fuori sistema", attraverso logiche diffuse, generate dagli utenti stessi e dunque non centralizzate. La crittografia alla base della rete BTC è particolarmente innovativa, e riguarda un tipo di software che cripta ogni movimento: il mittente e il destinatario di ogni transazione sono identificati da una stringa di numeri e ad ogni singolo movimento di moneta corrisponde una registrazione pubblica. Acquirenti e venditori mantengono così l'anonimato, ma tutti i membri della rete possono vedere che la transazione è stata effettuata dall'utente "A" in direzione dell'utente "B". Risulta evidente che il funzionamento di un tale software preveda che la moneta possa essere scambiata direttamente da un individuo all'altro, senza bisogno di intermediari, così che banche centrali e autorità governative non giochino alcun ruolo all'interno del sistema e così che "*tutto si basi su prove criptate, piuttosto che sulla fiducia"*, come chiarisce lo stesso Nakamoto nel documento del 2009. Nello specifico, i Bitcoin sono file crittografati che contengono informazioni sul loro possessore. Ogni importo Bitcoin è infatti legato alle cosiddette *chiavi crittografiche*: una chiave è privata (nota solo al proprietario), ed è quella che permetterà di spendere moneta; l'altra, detta *indirizzo bitcoin*, è invece pubblica, ed è quella che permetterà di riceverla. A differenza di quanto avviene per le altre monete, la creazione del Bitcoin è affidata a complessi algoritmi, generati attraverso un procedimento detto *mining*. I cosiddetti *miners* (una sorta di minatori digitali) eseguono un software gratuito, chiamato Bitcoin Miner, il quale, una volta lanciato sul computer, esegue un algoritmo e avvia il processo di generazione dei calcoli atti alla coniazione di moneta. Lo stesso algoritmo tuttavia, con l'aumentare di BTC immessi nel sistema, aumenta di complessità, necessitando di una sempre maggiore potenza di calcolo. In questo modo con il passare del tempo risulta sempre più difficile e (come vedremo) dispendioso eseguire i calcoli necessari, fino alla fine: una fine infatti esiste, ed è stata imposta dallo stesso creatore dell'algoritmo, che ha definito un limite massimo di Bitcoin generabili pari a ฿ 21.000.000.

La connessione tra tutti gli utenti che hanno attivo il software di creazione della moneta definisce quindi la Rete BTC, la quale asserisce ai due compiti principali di: 1) generazione della moneta; 2) memorizzazione e pubblicazione delle transazioni.

1.2.1 Generazione

La rete Bitcoin crea e distribuisce al suo interno, in maniera completamente casuale, un "*blocco di monete*" che deve essere trovato e calcolato dagli utenti entro un determinato lasso di tempo, pena la sua definitiva eliminazione. La probabilità che un utente, ovvero il singolo *nodo,* possa quindi ricevere quel blocco, dipende dalla potenza di calcolo che egli stesso aggiunge alla rete nella sua interezza. Così i computer di ogni individuo lavorano contemporaneamente cercando di risolvere questi problemi di calcolo e il nodo che riuscirà a trovare la soluzione in tempo riceverà come premio l'intero *blocco*. Ogni blocco contiene una certa quantità di Bitcoin, l'entità del quale è un valore programmato che diminuisce nel tempo fino ad arrivare a zero. In questo modo non verranno generati e immessi nel sistema più dei 21 milioni di Bitcoin stabiliti dall'algoritmo originario e, stando all'attuale ritmo, è previsto il raggiungimento di tale limite entro il 2033. Il *coefficiente di difficoltà computazionale* aumenta dunque col passare del tempo e, conseguentemente, i miners sono costretti ad aumentare in maniera proporzionale la potenza di calcolo dei propri processori. I Bitcoin costituiscono quindi la risorsa principale, sempre più difficile da trovare e meno abbondante man mano che la loro generazione procede; proprio come ai tempi della scoperta di nuove riserve auree e della conseguente estrazione.

1.2.2 Memorizzazione e fenomeno del Double-spending

Oltre che creare moneta la Rete BTC memorizza costantemente tutte le operazioni di trasferimento dei Bitcoin. L'intero sistema monetario viene gestito da un database che risiede tra tutti i nodi e che memorizza tutti gli scambi, anche in questo caso senza bisogno di un'autorità centrale o di un sistema di regolamentazione. La crittografia viene qui utilizzata per evitare il fenomeno definito come *double-spending*, considerato l'elemento di maggiore criticità del concetto di moneta digitale. Infatti, una volta effettuata la riproduzione (ovvero la copia) di un file, è praticamente impossibile distinguere la copia dall'originale, proprio perché il file è costituito di bit. Si parla dunque di double-spending quando si ha la possibilità di spendere un "*gettone digitale*" (Joshua Davis, *The New Yorker*) per due o più volte. Ma in questo caso la stabilità del sistema è garantita dal coinvolgimento di ogni operatore sia nella costruzione che nella verifica delle transazioni,

grazie all'architettura prevista dal sistema P2P: viene elaborato un vero e proprio *registro pubblico,* in grado di memorizzare le singole transazioni, e realizzato anche in questo caso attraverso la tecnica del software di tipo open-source. Tale registro, comune e condiviso tra i nodi della rete, consente di:

- Conoscere quale sia l'ammontare complessivo di Bitcoin presenti nel sistema in un preciso istante.
- Certificare le informazioni relative alle singole transazioni, così da rendere pubblico ogni trasferimento attraverso l'inserimento nel registro ed evitare che si verifichino transazioni doppie (attraverso l'utilizzo dello stesso Bitcoin), in quanto tutti possono verificarne l'autenticità.
- Essendo un registro pubblico, consente l'interazione diretta tra i membri, senza bisogno di intermediari o terze-parti per validare l'avvenuta transazione.

1.3 Block-Chain e Sistema a Blocchi

Come definito sopra, nel sistema BTC ogni qualvolta viene effettuata una transazione, questa viene datata e inserita in un registro pubblico e distribuito. Questo database (totalmente decentralizzato) prende il nome di *BlockChain* o "Catena di Blocchi", e segue un processo di realizzazione tanto semplice quanto efficace: essendo un database distribuito, trova fondamento nell'architettura P2P e chiunque può semplicemente prelevarlo dal web (collegandosi al sito https://bitcoin.org/bin/block-chain/), diventando a tutti gli effetti un "nodo" della rete.

La BlockChain si qualifica quindi come un vero e proprio libro contabile: aperto, modificabile ma soprattutto libero dalle autorizzazioni di governi e banche per effettuare le transazioni. Infatti ogni transazione è resa possibile se approvata dal 50% + 1 dei nodi. Considerando le spiegazioni precedentemente fornite e riducendo all'essenziale la definizione di Bitcoin, possiamo dunque pensare ad esso come ad un'informazione nascosta nel blocco che, in quanto tale, va scovata. Ogni blocco contiene 25 Bitcoin (all'incirca € 15.000 al tasso di cambio attuale) e viene liberato dai miners dotati della suddetta potenza di calcolo utile a risolvere l'algoritmo che li protegge. Chi libera un

blocco incassa dunque 25 Bitcoin, che potrà successivamente rivendere sul mercato ottenendo un guadagno. Tuttavia anche i nodi, supervisionando e autorizzando le transazioni, incassano una piccola percentuale del totale delle transazioni stesse. In questo modo viene garantito il regolare funzionamento della Catena che offrirà in ogni caso un guadagno (benché minimo) a tutti i nodi. Non c'è da stupirsi dunque se nel report rilasciato lo scorso Agosto dal World Economic Forum (http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf), si dichiara che "[…] la finanza del futuro non potrà prescindere dalla tecnologia di certificazione distribuita e criptata, che è alla base del sistema Bitcoin" o ancora "La Blockchain non resterà ai margini dell'industria finanziaria, ne diventerà il cuore pulsante" (*World Economic Forum: An ambitious look at how Blockchain can reshape financial services)*. L'impatto rivoluzionario della BlockChain riguarda dunque in primo luogo l'effetto su elementi quali trasparenza e fiducia, oltre che efficienza e semplificazione operativa e burocratica. Ciò che la BlockChain è stata in grado di mettere in discussione è proprio l'ortodossia tradizionale dei *business model* odierni: attraverso la costruzione di un registro distribuito in maniera trasparente, in grado di generare fiducia (in tempo reale) tra i partecipanti del mercato ed eliminare le asimmetrie informative tra gli individui. Nello stesso report si parla di oltre 90 Banche Centrali che hanno dichiarato i loro interessi nei confronti di progetti legati alla BlockChain e di circa 2,5 miliardi di dollari investiti nella tecnologia di certificazione distribuita. Risulta tuttavia ovvio che per arrivare ad un'effettiva e completa applicazione del protocollo BlockChain, sarà necessario risolvere le questioni legate al quadro legale e regolatorio, compito sicuramente non semplice visti i molteplici interessi in gioco.

1.4 La rete dei miners e il costo del mining

Uno dei problemi fondamentali affrontati al momento della creazione del sistema BTC, riguardava le modalità di emissione della nuova moneta in un sistema autonomo e non centralizzato, che si distinguesse da tutti i sistemi monetari precedenti (costruiti sulla base di organismi regolatori come le Banche Centrali). Per creare un sistema decentralizzato e

al tempo stesso credibile fu necessario escogitare un metodo di generazione della moneta altrettanto decentralizzato ma soprattutto autonomo. La soluzione fu, come abbiamo visto, l'emissione di Bitcoin a fronte di un lavoro atto alla conservazione del sistema stesso; la garanzia dunque di un premio a tutte le componenti della rete in grado di fornire la capacità di elaborazione necessaria a creare e a fortificare la rete stessa, e in modo proporzionale alla potenza di calcolo fornita. Nel primo periodo di esistenza della rete Bitcoin i partecipanti al sistema erano pochi ma, come abbiamo chiarito, più avanti si va col tempo più l'algoritmo si complica, ed è proprio la difficoltà di creazione una delle chiavi del funzionamento della rete Bitcoin. Ad oggi invece sono molte le persone che si sono aggiunte come partecipanti alla rete, dedicandosi al mining e rendendo in altre parole più difficile (oltre che inferiore) il guadagno medio per ogni partecipante. Forse ciò che ha spinto molte persone ad interessarsi alla pratica del mining è stata proprio la falsa credenza che la generazione di Bitcoin non comporti dei costi. Tuttavia la creazione di moneta virtuale ha comunque un prezzo e, date le difficoltà di calcolo attuali, un prezzo assolutamente non indifferente. La voce di costo principale è ovviamente rappresentata dalla quantità di energia elettrica necessaria al computer per effettuare il calcolo, a cui si aggiunge la manutenzione degli impianti stessi. Sommando le due componenti e tenendo conto del valore attuale del singolo Bitcoin, emerge chiaramente quanto non risulti conveniente, ad oggi, aderire alla rete di miners: la potenza di calcolo richiesta per acquisire un blocco è elevata e i costi necessari per l'ammortamento del computer e l'utilizzo di energia elettrica sono superiori ai guadagni ottenibili. Analizzando nello specifico la prima voce di spesa (l'energia elettrica) notiamo che:

Per calcolare la quantità di Bitcoin generabile con l'utilizzo di un kilowattora (kWh), è necessario prima di tutto tenere conto del tipo di hardware utilizzato e del livello di difficoltà corrente (entrambi valori consultabili dal proprio computer). Determinato quindi il valore del coefficiente di difficoltà ed il tipo di hardware utilizzato, è possibile a questo punto calcolare quanti Bitcoin per kilowattora si possono generare utilizzando la formula:

$$BTC/kWh = MHJ / Difficulty$$

dove: MHJ (MegaHashesJoule) esprime la qualità di un certo tipo di hardware e Difficulty il coefficiente di difficoltà di calcolo.

Tuttavia agli scenari appena presentati occorre aggiungere altri elementi quali ad esempio le *Pool Tax*, ossia le commissioni destinate alle *mining-pools* (gruppi di mining): per partecipare al gruppo infatti è necessario destinare una percentuale all'organizzatore del pool. Altro elemento è che si presume che il computer effettui calcoli per il 100% del tempo e senza presentare inefficienze. Di fatto invece, la formula prima esposta tiene conto solo della corrente consumata, senza considerare gli elementi appena esposti. Da questa prima analisi è chiaro che il mining risulti un'attività in perdita, e la perdita risulterebbe di gran lunga maggiore se si considerassero anche l'usura e l'ammortamento degli elaboratori. Dunque la conclusione è che al momento generare Bitcoin attraverso il mining non risulta conveniente, o almeno non quanto lo sia acquistarli direttamente sul mercato.

CAPITOLO SECONDO –

IL SISTEMA MONETARIO BTC

2.1 Bitcoin e Gold Standard

Dato che la quantità complessiva di Bitcoin in circolazione è fissata da un algoritmo, alcuni hanno colto un'evidente correlazione tra Bitcoin e *Gold Standard*, il sistema monetario aureo nel quale la base monetaria è ancorata ad una quantità d'oro prestabilita. Attraverso il Gold Standard i paesi legavano le rispettive monete all'oro, consentendone l'importazione e l'esportazione attraverso i confini. In questo modo il Gold Standard, come un sistema a valute di riserva, comporta lo stabilirsi di tassi di cambio fissi tra le valute; una volta che le Banche Centrali dei vari paesi abbiano fissato il prezzo dell'oro rispetto alla valuta nazionale, sarà possibile effettuare il cambio non solo tra l'oro e le singole valute aderenti al sistema ma tra le valute stesse. Dopo vari tentativi di applicazione (l'ultimo dei quali nel 1947 attraverso gli accordi di Bretton Woods, rimasti in vigore fino alla crisi petrolifera del 1971), il Gold Standard venne definitivamente abbandonato, facendo spazio all'era tutt'ora in corso del denaro privo di una base aurea, la cosiddetta *fiat money*, in cui sono le Banche Centrali a regolare la quantità di denaro circolante nel paese e il suo costo attraverso il tasso di conto. Il vantaggio del sistema fiat money è la flessibilità, che consente ai policy makers una migliore gestione dei periodi critici (come una guerra o un'improvvisa crisi petrolifera), attenuandone le conseguenze per la popolazione. Attraverso il gold standard invece la gestione sociale risulta difficoltosa ed è impossibile abbattere la disoccupazione attraverso ad esempio politiche fiscali espansive (aumenti della spesa pubblica). Al tempo stesso tuttavia il sistema fiat money favorisce il verificarsi di problemi come quelli che l'economia mondiale sta vivendo in questo momento, ovvero il considerevole aumento della speculazione finanziaria, sostenuta dall'incertezza che si ha nel calcolare gli spostamenti di ricchezza dalle diverse zone del mondo. Da quando l'oro non costituisce più la base dei sistemi monetari, e soprattutto dopo la crisi del 2008, i sostenitori del Gold Standard vedono nella sua riadozione il metodo migliore per stabilizzare il sistema monetario. Tra questi Ron Paul, membro del partito repubblicano ed ex leader del movimento per il restauro del Gold Standard, il quale nel 1982 auspica addirittura l'abolizione della FED: Paul infatti

riconosce nell'assenza del sistema autoregolatore tipico del sistema aureo, la motivazione del *"dirigismo distruttivo"* da parte della Banca Centrale Americana (Ron Paul, *The Case for Gold: a Minority Report of the U.S. Gold Commission*, 1982). Tuttavia, sia concesso di precisare che, ammesso che ci sia una "soluzione", difficilmente questa può risiedere nei sistemi del passato (che hanno già dimostrato i propri limiti) ma debba piuttosto essere ricercata nelle innovazioni e nei cambiamenti che si profilano attualmente.

A questo punto, è doveroso chiedersi quali siano le analogie tra una moneta totalmente virtuale quale il Bitcoin e un metallo prezioso quale l'oro. Per farlo, consideriamo prima di tutto quali siano le proprietà che nel passato hanno reso l'oro la moneta di scambio per eccellenza. Tra le principali:

- Scarsità: in quanto disponibile in quantità limitata
- Durevolezza: è infatti un metallo nobile ed uno degli elementi più stabili in natura
- Divisibilità: per poter essere impiegato come bene di scambio
- Riserva di valore: dotato di un potere d'acquisto stabile nel tempo, garantito anche dalla impossibilità di contraffazione.

Andando a questo punto a confrontare le suddette qualità con quelle del Bitcoin, le somiglianze (dirette o indirette) sembrano numerose. Infatti riassumendone le principali caratteristiche:

1. Scarsità: abbiamo visto infatti che la possibilità di "trovare" monete decresce con il passare del tempo e con il numero di Bitcoin già immessi nel sistema. Il fatto che prima o poi si arriverà al momento in cui non sarà più possibile creare nuova moneta, una volta stabilizzato il sistema, protegge gli utenti dal rischio di inflazione.
2. Impossibilità (o estrema difficoltà) di falsificazione: la crittografia offre la possibilità di evitare fenomeni come quello del double-spending.
3. Gestione peer-to-peer (P2P): è un sistema distribuito tra tutti i nodi della rete, senza fare capo ad un organismo centrale.
4. Facilità di implementazione: il codice è di tipo open source e non esistono costi di licenza.

Inoltre è doveroso notare come l'attuale limitato volume di scambi renda il valore dei Bitcoin particolarmente volatile. Tuttavia, se il suo uso continuasse ad aumentare, il

valore potrebbe stabilizzarsi notevolmente e, come avviene per l'oro, aumentare con il tempo. Il teorico aumento di valore nel tempo andrebbe così a compensare la perdita di potere d'acquisto delle monete tradizionali dovuta all'inflazione.

2.2 La moneta "a prova di censura"

"Una valuta digitale anonima e a prova di censura": così *l'Electronic Frontier Foundation* (Associazione no profit che si occupa di libertà civili all'interno del contesto digitale) definisce il Bitcoin, relativamente al fatto che qualsiasi transazione avvenga tramite questa valuta, risulti non tracciabile né censurabile. Ne deriva uno degli aspetti più discussi sul tema: se da una parte esiste il dubbio circa l'effettiva esistenza dell'anonimato, dall'altro ci si domanda se questo possa essere considerato un bene o meno. Relativamente al primo punto: per quanto a livello puramente teorico sia impossibile ricollegare una transazione all'individuo che l'ha effettuata, nella realtà, occorre tenere presente che vengono sempre lasciati degli "indizi": ad ogni transazione; movimento; inserimento di Bitcoin in un *wallet* corrispondono sempre elementi che possono facilmente essere individuati attraverso sistemi di tracciamento, i quali sono già a disposizione delle agenzie governative. Basti pensare alla semplice raccolta storica di dati che, se analizzati da esperti, possono facilmente condurre all'individuazione di un profilo univoco.

Relativamente al secondo aspetto: naturalmente è intuibile, una volta assunto l'anonimato come condizione verificata nella maggior parte dei casi, quanti aspetti positivi e allo stesso tempo negativi esso possa apportare: l'anonimato facilita ovviamente tutte quelle operazioni illegali che necessitano di tale condizione per la loro realizzazione; vedremo più approfonditamente nel terzo capitolo quanto fondamentale risulti l'anonimato nel commercio di stupefacenti realizzato attraverso il *Dark Web*. Esistono tuttavia aspetti positivi di portata non indifferente: chiunque, nel rispetto delle leggi, può sfruttare la condizione di anonimato nello svolgere le proprie attività sottraendosi al controllo perenne delle autorità. Occorre inoltre tenere presente come in molti paesi, caratterizzati ad esempio da una tassazione particolarmente alta o dal prelievo (di denaro contante) limitato e ristretto, l'alternativa proposta da una moneta anonima e autonoma potrebbe

risultare particolarmente interessante, soprattutto in un'ottica di attrazione per nuove forme di investimento.

2.3 Prime critiche al sistema Bitcoin

2.3.1 Lo schema Ponzi

Per quanto riguarda le principali critiche rivolte alla realtà BTC, la prima fra tutte è quella che guarda al nuovo sistema monetario come ad un semplice (e presto fallimentare) *Sistema Ponzi.* Uno schema di questo tipo richiede che più individui investano soldi per pagare altre persone le quali abbiano già investito, e sono in attesa del loro guadagno: è uno schema "piramidale", che dal vertice si diffonde coinvolgendo la base, e risulta comunque una struttura non sostenibile, ormai riconosciuta solo come truffa. Tuttavia nel caso Bitcoin non esiste un elemento centrale che abbia dato avvio alla truffa; non è individuabile dunque quale sia il "vertice" della piramide e anzi, diverse entità singole (come i *miners*) hanno investito soldi per offrire un servizio e ricavarne un guadagno. In questo caso il servizio fornito è proprio quello che mantiene il network e permette alle transazioni di essere registrate.

2.3.2 Realtà digitale

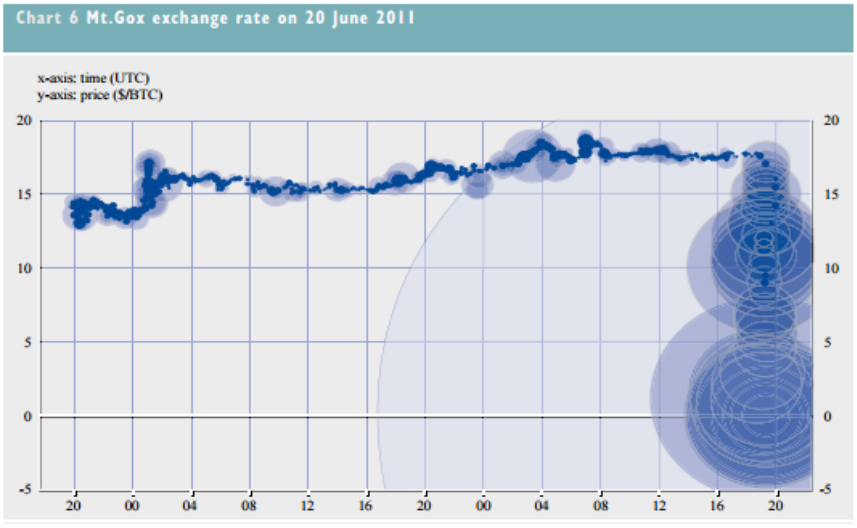
Altra frequente critica è quella che guarda al Bitcoin come ad una pura realtà virtuale, non considerabile moneta a causa del suo valore fluttuante e per la mancanza di una Banca Centrale. Definendo la moneta in base alle tre funzioni cui assolve (mezzo di scambio, riserva di valore e unità di conto) sarà possibile identificarla come un buon mezzo di scambio se ad esempio divisibile, facilmente trasportabile e definita. Il Bitcoin è uno strumento di pagamento che presenta tutto ciò, ed in modo assai efficiente.

2.3.4 L'insicurezza

Il Bitcoin non è sicuro poiché la sua scarsità, e il relativo limite ai 21 milioni non è realmente garantito. Una delle vulnerabilità può essere ricercata nelle mining pools e nei mercati di scambio: Nel 2011 è stato attaccato MtGox, il più grande sito di trading di Bitcoin, costretto a chiudere per una settimana per risolvere i problemi di sicurezza. Secondo un comunicato stampa della società di Mark Karpeles, un hacker avrebbe

sottratto Bitcoin per un controvalore di circa $500.000 dai conti di MtGox, vendendoli tutti. L'eccesso di offerta di Bitcoin avrebbe fatto istantaneamente precipitare il loro prezzo: da $17,50 a 1 centesimo in meno di un'ora. Il mercato si è poi ristabilizzato ma l'incidente ha comunque messo sotto i riflettori la falla, dimostrando che, di fatto, attaccare il sistema Bitcoin è possibile. La Banca Centrale Europea, in un documento di cui parleremo nei paragrafi a seguire, riporta il grafico contenente il valore dei Bitcoin nella piattaforma di MtGox durante le ore dell'attacco (vedi fig. 2.1). L'espressione di quel grafico riguarda proprio l'instabilità connessa ad una moneta definita come troppo "volatile e immatura", in grado di scatenare il panico in pochi minuti e tra milioni di utenti. Tale problematica risiede comunque nella natura stessa dei Bitcoin, in quanto essi possono essere conservati in un *wallet*, un portafoglio virtuale, che può risultare facilmente hackerabile. Tutto ciò, in prospettiva, diventa sempre più problematico: "*Se da una parte la sicurezza informatica potrà solo che aumentare, dall'altra potrà permanere l'insicurezza legata all'assenza di una regolamentazione in materia che possa dunque tutelare gli acquirenti, specie se i Bitcoin dovessero rafforzare il loro ruolo di strumenti di investimento."* Dichiara Dianora Poletti, ex preside della Facoltà di Economia dell'Università di Pisa.

***Fig.2.1**: Tasso di cambio BTC/USD durante le ore dell'attacco a MtGox. Fonte:BCE*



2.4 Paul Krugman sui Bitcoin

In un post dall'eloquente titolo "*Adam Smith hates Bitcoin"* (http://krugman.blogs.nytimes.com/2013/04/12/adam-smith-hates-bitcoin/) il premio Nobel Paul Krugman espone manifestatamente il proprio scetticismo nei confronti della realtà BTC, sostenendo che lo stesso Smith avrebbe disprezzato i Bitcoin proprio per la natura dispendiosa della loro "estrazione". Infatti, ciò che Smith criticava riguardo l'estrazione di oro e argento nel XVIII secolo, sostenendo che venivano impiegate preziose risorse per creare qualcosa di assolutamente simbolico, potrebbe benissimo essere rapportato alla realtà dei Bitcoin: "*Ci troviamo in un mondo di tecnologia ad alta informazione, e le persone credono che sia intelligente, o all'avanguardia, creare una sorta di moneta virtuale la cui generazione richiede un dispendio di risorse reali che Adam Smith avrebbe considerato stupido e fuori moda nel 1776"*. Ma questo non costituisce l'unico commento di Krugman al fenomeno della moneta virtuale; in un secondo post dello stesso blog, l'economista sostiene che "*quello che vogliamo da un sistema monetario non è di rendere ricche le persone che detengono denaro, ma che esso faciliti le transazioni e renda l'economia ricca nel suo insieme. E non è affatto quello che sta accadendo con il Bitcoin*." Krugman infatti, ai tempi della bolla del 2008 ha sostenuto che il crescente valore in dollari del Bitcoin aveva fatto cadere il valore dei beni così prezzati e l'economia Bitcoin ha subito, in effetti, una massiccia deflazione. La moneta virtuale, volendo proseguire con le analogie, anche in questo caso si comporta esattamente come l'oro: è deflazionistica, costosa, ed esiste in quantità limitata. Il Bitcoin è costruito per rivalutarsi di continuo (il che spiega la deflazione). Se da una parte l'offerta di moneta cartacea aumenta costantemente, dall'altra l'offerta di Bitcoin risulta limitata, ne deriva che il suo valore, in linea teorica, è destinato a salire nel tempo. Proprio questo tuttavia sta portando gli utenti della rete Bit, a fare incetta di Bitcoin, depositandoli anziché spendendoli (Bitcoin detti *silenti*), con la speranza che aumentino di valore, ma facendo diventare il Bitcoin, di fatto, oggetto della speculazione e intralciandone il ruolo principale: facilitare gli scambi e il commercio, come osservato dallo stesso Krugman.

2.5 Rapporto BCE: "The Virtual Currency Schemes"

Nell'Ottobre del 2012 la Banca Centrale Europea ha redatto un documento (www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.) dal titolo "The Virtual Currency Schemes", che analizza la nascita e la diffusione delle cosiddette cripto-valute, presentando come case studies il LindenDollar e il Bitcoin e definendo quest'ultimo come "la moneta più controversa e allo stesso tempo di maggior successo, con elementi di innovazione tali da renderla molto più simile ad una moneta convenzionale piuttosto che ad una virtuale." Uno degli aspetti più interessanti del documento è la considerazione che la BCE attribuisce alla nascita del sistema Bit, facendone risalire le radici "teoriche" alla *Scuola Austriaca*. In particolare il documento cita "[…] *le critiche della Scuola Austriaca sia al sistema monetario attuale, sia agli interventi istituzionali da parte dei governi, che non fanno che produrre inasprimenti del ciclo economico e inflazione sempre più elevata*." In effetti alcuni esponenti della Scuola Austriaca (tra cui F. Hayek), hanno esplicitamente auspicato una denazionalizzazione della moneta; tuttavia, uno dei capisaldi del pensiero austriaco, Ludwig Von Mises, ci ricorda come sia necessario porsi nella direzione opposta: ogni moneta secondo Mises viene accettata non perché imposta dal governo, né per mera convinzione sociale, ma solo perché essa è in qualche modo rappresentata da un bene che ne determina il valore. Il Bitcoin invece nasce e si propone unicamente come mezzo di scambio e, non avendo alcun valore intrinseco, non può essere utilizzato come merce. Il Bitcoin, per quel che ne possiamo dedurre, ha valore soltanto nel momento in cui le persone sono disposte ad utilizzarlo. Nel suddetto documento, la BCE sembra apprezzare la creatività e l'innovazione dei sistemi di pagamento generati dai Bitcoin: tuttavia, considerata l'instabilità intrinseca del prezzo di queste valute ma soprattutto la mancanza di una specifica regolamentazione al riguardo ed il rischio di un loro uso illegale da parte di utenti anonimi, la Banca Centrale Europea spinge affinché si instauri un procedimento di analisi e di verifica necessario per contenere i rischi connessi alla proliferazione di questa cripto-valuta. Più precisamente, nella parte finale del documento, all'interno del paragrafo denominato "*Conclusions on the lack of Regulations"* si specifica che l'introduzione di una regolamentazione specifica sul fenomeno Bitcoin da parte delle autorità, costituisce "una sfida certamente avvincente e che risulta necessario cogliere".

In virtù di ciò e a conclusione di questa parte, si ritiene opportuno considerare come l'estrema ed evidente instabilità della cripto-valuta passata in un solo anno da $14 (Dati gennaio 2013) a circa $1.200 (Dati dicembre 2013) per poi crollare nuovamente, spiegabile proprio per l'assenza di un mercato di controllo, rappresenti uno dei principali ostacoli al suo utilizzo e alla sua accettazione. Anche se il Bitcoin superasse "l'incertezza della sicurezza", fino a quando manterrà un andamento così altalenante potrà solamente aspirare alla penetrazione avuta fino ad ora**.** È innegabile che nel micro-commercio si stiano aprendo posizioni di fiducia sui Bitcoin, ma l'eccessiva instabilità resta comunque l'elemento preclusivo alla sua diffusione. Tuttavia la regolamentazione auspicata nel documento BCE, se da un lato sicuramente rafforzerebbe la fiducia in questa moneta, dall'altro potrebbe snaturare la ragione stessa della sua nascita, generando una contraddizione sul piano ideologico oltre che puramente economico.

CAPITOLO TERZO –

LA REALTA' BTC NEI MERCATI DEL DARK WEB

3.1 Deep Web

Il *Deep Web*, o "web sommerso", è quella parte della rete in cui è possibile trovare le informazioni non segnalate (dunque non catalogate) dai tradizionali motori di ricerca. Questi ultimi solitamente utilizzano un software, chiamato *crawler* (una specie di sonda), che segue i link presenti nelle pagine web, raccogliendoli, analizzandoli e restituendone un indice dei contenuti disponibili. I motori di ricerca classificano poi i risultati in base ad algoritmi che indicano il grado di rilevanza rispetto ad una determinata *chiave di ricerca*. Per raccogliere e analizzare dati, quindi per indicizzarli, i crawler possono accedere solo ai database relativi a pagine "statiche". Per questo, all'interno del deep web è possibile individuare tutte quelle pagine "dinamiche" che possono essere richiamate solamente eseguendo una specifica ricerca all'interno di un sito. All'interno del deep web è possibile individuare una "porzione" più complessa da esplorare, definita *Dark Web*, per accedere alla quale è necessario utilizzare speciali software che permettono di raggiungere siti web anonimi e non rintracciabili; tra questi, il software più utilizzato è TOR, di cui tratteremo nei paragrafi a seguire. Il dark web è dunque un'ulteriore "dimensione" della rete, uno strato posto ancora più in profondità, che non solo non viene indicizzato dai comuni motori di ricerca (come avviene anche per il deep web), ma che neppure segue le regole del "web di superficie", essendo accessibile proprio solamente tramite specifiche applicazioni, il cui obiettivo principale è quello di rendere anonima ogni attività svolta, a partire dalla singola ricerca. Per raggiungere le pagine del dark web è necessario dunque conoscerne l'indirizzo esatto, una specie di chiave, in quanto gli indirizzi (url) presentano spesso nomi incomprensibili, in gran parte costituiti da complesse sequenze numeriche. Infine è necessario tenere presente che questi siti hanno solitamente vita molto variabile e breve. Trattandosi di un territorio in cui ci si muove in completo anonimato, uno degli usi principali riguarda il commercio illegale: da siti che

offrono droga o armi a pagine che presentano e vendono contenuti pedopornografici. Tuttavia è doveroso ricordare come oltre a questi utilizzi, fenomeni quali ad esempio WikiLeaks, la nascita di gruppi segreti come Anonymous o l'associarsi dei giovani protagonisti della Primavera Araba, e la stessa creazione di una moneta virtuale e sovranazionale non sarebbero stati possibili senza un territorio libero quale il dark web. All'interno di esso tuttavia è possibile trovare, oltre ai contenuti già presenti nel web tradizionale, numerosi siti scientifici, blog personali, siti-biblioteca, documenti contenenti informazioni riservate e molti altri servizi inaccessibili agli utenti del web di superficie. Il dark web dunque non necessariamente costituisce un pericolo di per sé e non occorre demonizzarlo; non prima, almeno, di averlo conosciuto.

3.2 Case Study: Il traffico di stupefacenti nel Deep Web

In questa sede si è ritenuto più opportuno mettere in luce una delle tre principali tipologie di commercio illegale del dark web, realizzato tramite l'utilizzo di Bitcoin: quello degli stupefacenti; soprattutto dopo recenti episodi che hanno portato alla chiusura di piattaforme online per la compravendita di droga quali *The Black Market Reloaded* o il più conosciuto *TheSilkRoad*. Quest'ultimo (probabilmente il sito più citato dalle testate giornalistiche relativamente al fenomeno del dark web) si presenta come un *e-commerce* all'interno del quale sono disponibili prodotti che non potrebbero essere commerciati legalmente, tra cui: droga; armi; carte di credito clonate; passaporti contraffatti; vari tipi di medicinali e molto altro. Accedere a TheSilkRoad (chiuso per tre volte consecutive su iniziativa di agenzie governative americane e successivamente riaperto attraverso domini differenti) risulta fin troppo semplice, ed è possibile reperire consigli e modalità d'iscrizione a partire dalle informazioni presenti nel web di superficie; proprio per questo si è ritenuto più interessante rivolgersi ad altre realtà, poste più in profondità e con modalità di accesso differenti e più complesse. Molti di questi siti sono, di fatto, ospitati sul computer del loro creatore e possono essere trovati e raggiunti solo attraverso l'utilizzo del software TOR, di cui parleremo approfonditamente più avanti.

Il traffico di stupefacenti costituisce la fonte di guadagno principale tra le tipologie di commercio presentate nel dark web e sopra citate, garantendo un introito netto di circa $1.200.000.00 mensili per i cosiddetti *sellers* delle principali piattaforme (Fonte: *SilkRoadForum.onion).* Il punto di partenza per l'analisi qui presentata è costituito da un'interessante ricerca condotta nel Febbraio 2014 dalla Dott.ssa Monica J. Barrat (membro della "Global Drug Survey International Advisory") per la rivista Australiana "*Addiction*" (http://onlinelibrary.wiley.com/doi/10.1111/add.12470/abstract9). Qui vengono elencate e commentate le percentuali relative alla compravendita on-line di sostanze stupefacenti da parte di consumatori con un'età media compresa tra i 24 e i 25 anni. Su un campione di 9470 individui distinti tra cittadini Inglesi, Americani e Australiani: il 18% dei 2394 cittadini Americani intervistati, ha confermato di aver effettuato almeno un acquisto di sostanze stupefacenti attraverso le piattaforme del dark web; a seguire, il 10% dei 4315 cittadini Inglesi e il 7% dei rimanenti 2761 cittadini Australiani. Quanto segue è ancora più interessante, poiché tra le motivazioni fornite riguardo la preferenza per un acquisto di sostanze stupefacenti online, la qualità della merce costituisce il 77% delle risposte totali, successivamente: la maggiore sicurezza nell'acquisto (62%) e i sistemi di *rating* nei confronti dei venditori (60%). La Dott. Barratt a commento dei risultati ottenuti attraverso la ricerca afferma che "[…] Ovviamente comprare droghe nel mondo reale comporta un rischio in ogni caso, e per alcuni l'equivalente online potrebbe essere più conveniente e sicuro che organizzare un acquisto standard". In effetti, navigando tra le principali piattaforme dedicate a questo tipo di commercio, ciò che più colpisce (oltre alle modalità di presentazione dei prodotti) sono le continue rassicurazioni circa la sicurezza nella spedizione della merce, come vedremo più avanti.

3.2.1 TOR – The Onion Router

Come detto, per accedere ai servizi forniti nel dark web sono necessari alcuni software e browser specifici. Tra questi, il più importante e conosciuto è sicuramente TOR, seguito da altre realtà tra le quali è opportuno ricordare:

- OSIRIS (http://osiris.kodeware.net): un progetto per lo più italiano italiano, che si presenta come un programma gratuito destinato alla creazione di portali web realizzati tramite architetture P2P.

- PSIPHON: un software canadese "anti-censura" che permette di aggirare i blocchi (detti *firewall*) dell'accesso alla rete, favorendo la circolazione dei documenti. È molto utilizzato in paesi in cui la censura è riconosciuta e costituisce una barriera quasi insormontabile alla libera circolazione delle notizie.

Per quanto riguarda TOR invece, è possibile introdurre questa realtà presentandolo come un semplice sistema di comunicazione anonima per Internet, il quale permette di navigare sia nel dark web che nella rete tradizionale. TOR appartiene alla categoria PET (Privacy Enhanced Technolgy) ed è basato sulla seconda generazione del protocollo di *onion routing*. TOR, nato grazie ai finanziamenti dello *US Naval Research Laboratory*, con finalità essenzialmente militari nell'ambito di ricerca delle comunicazioni protette, è stato un progetto della Electronic Frontier Foundation ed è attualmente gestito da The Tor Project, un'associazione senza scopo di lucro. Il funzionamento di questo software è relativamente semplice: esso fa viaggiare dati criptati attraverso diversi nodi, in modo da dissimulare l'identità della connessione sui siti visitati. Quando si naviga o si invia un messaggio, dal computer parte un pacchetto di informazioni a partire dal proprio indirizzo IP. TOR cripta questo pacchetto di dati, che invece di raggiungere direttamente il server relativo al sito visitato passa per stazioni intermedie (costituite da altri utenti che hanno deciso di fare parte della rete TOR in qualità di *relay)* fino alla destinazione. In pratica il software protegge gli utenti dall'analisi del traffico attraverso una rete di onion router (relay), che consentono il traffico anonimo in uscita. I vari nodi si comportano dunque

come router, reindirizzando casualmente i pacchetti di dati all'interno di un circuito crittografato. È quindi un sistema costruito a "strati" (da questo il termine "onion", cipolla).

I siti web creati per TOR non hanno le classiche estensioni di dominio che già conosciamo, ad esempio "*.com*" o "*.it*", ma possiedono un'estensione propria, chiamata appunto "*.onion*" . Un sito protetto da TOR può essere molto difficile da trovare e non è possibile visitarlo se non si è a conoscenza dell'indirizzo esatto, peraltro consultabile solamente tramite l'installazione del browser (è sufficiente collegarsi al sito www.thetorproject.com ed effettuare il download). Il tipico indirizzo di questi siti è una successione di numeri e lettere e molti di essi prevedono come abbiamo detto la compravendita di materiale illegale. Tuttavia ciò che di più "spaventa" riguardo TOR, ma riguardo anche il dark web in generale, è proprio il fatto che è uno strumento che fa dell'assenza del controllo la sua forza; e ciò non può che non incutere timore. Ma è necessario ricordare che piattaforme di questo tipo hanno consentito a 36 milioni di persone di avere libertà di accesso e di espressione sul web. Per questo TOR ha già dimostrato di poter giocare un ruolo chiave per le rivoluzioni politiche e sociali nei regimi autoritari, permettendo la trasmissione, la condivisione e l'interconnessione degli individui, come già dimostrato in Iran e in Egitto.

3.2.2 La compravendita attraverso TOR

Dunque, una volta scaricato il browser e inserito l'indirizzo preciso riferito al sito che si intende visitare (in questa sede è stato possibile affidarsi ad una lista completa delle piattaforme dedicate alla compravendita di stupefacenti collegandosi al sito www.hiddenwiki.onion), è possibile cominciare a muoversi all'interno dei cosiddetti *dark net markets*. A questo punto si ritiene opportuno ricordare come la maggior parte delle piattaforme presenti siano costruite e gestite dai reparti addetti alla sicurezza informatica (in Italia: Polizia Postale e C.N.A.I.P.I.C.) con l'obiettivo di prevenire e combattere l'utilizzo illecito delle realtà presenti nel dark web. È altrettanto opportuno far presente quanto non sia particolarmente difficile intuire quali tra i tanti siano i siti "controllati": sono gli unici che al momento della registrazione (che come vedremo risulta obbligatoria per quasi tutti i mercati) richiedono un indirizzo e-mail valido e, nella fase di un eventuale acquisto, l'indirizzo di residenza corrente, violando quello che abbiamo visto essere uno dei principi-cardine della realtà dark-web: l'anonimato. Altri siti invece, in fase di registrazione, richiedono semplicemente la scelta di un *username*, una *password* e l'eventuale inserimento di un *codice CAPTCHA.*

Una volta inserito l'indirizzo esatto, dopo alcuni minuti di caricamento (l'attesa è principalmente dovuta ai continui trasferimenti di informazioni relative all'IP descritti sopra) la pagina che si apre è solitamente sempre la stessa, e presenta le varie opzioni di registrazione disponibili, attraverso la scelta di un username, una password e/o un codice PIN, da inserire ogni volta che si effettua il log-in. Nei tre siti che sono stati in esame per lo svolgimento di questo capitolo, le caratteristiche principali sono pressoché le stesse, e una volta effettuato il log-in, si viene reindirizzati in una pagina contenente le varie categorie di prodotto disponibili. Nei paragrafi a seguire verranno descritte nel dettaglio le caratteristiche della compravendita relative ai due aspetti di: modalità di pagamento tramite Bitcoin; modalità di spedizione. Si è ritenuto opportuno tuttavia, porre prima l'accento sulle caratteristiche distintive dei mercati presi da esempio, secondo la centralizzazione e decentralizzazione degli stessi.

3.2.3 Mercati centralizzati e decentralizzati

Prima distinzione fondamentale relativa ai mercati della Dark Net è quella che riguarda la gestione dei Bitcoin all'interno della piattaforma. I mercati vengono distinti in centralizzati e decentralizzati. I primi sono quei mercati che tengono in deposito, e dunque hanno in completa gestione, i fondi di Bitcoin affidatigli dagli utenti. Essi infatti depositano all'interno di un *online wallet* i Bitcoin destinati all'acquisto esclusivo della merce proposta nella piattaforma, e sarà compito del gestore della stessa assicurare la loro conservazione ma soprattutto garantire il rilascio dei fondi dal compratore al venditore una volta che entrambi abbiano raggiunto l'accordo ed abbiano confermato la transazione. In questo tipo di mercato la fiducia nei confronti della gestione centralizzata gioca un ruolo fondamentale: sono due i casi (il primo risalente al 2013, il secondo all'anno passato) che hanno visto lo smantellamento totale di due piattaforme per il traffico di stupefacenti successivamente alla "fuga" dei rispettivi gestori insieme al portafoglio complessivo di Bitcoin depositati (nel caso del luglio 2013 il corrispettivo era di circa $24.000.000 totali).

Nel secondo caso invece, il mercato decentralizzato limita il suo stesso potere e non prevede il deposito di Bitcoin in un unico portafoglio quanto piuttosto un sistema basato su "chiavi" di accesso ai singoli fondi creati dagli utenti. Il mercato di tipo decentralizzato più conosciuto è *The Dark Market Project*; esso prevede che lo sblocco del fondo Bitcoin necessario ad un versamento avvenga tramite l'uso di due chiavi, l'una a disposizione del venditore, l'altra del compratore e la transazione può realizzarsi solo una volta che entrambi abbiano utilizzato le proprie chiavi di accesso. In questo modo la responsabilità viene limitata ad entrambi i soggetti, e i gestori della piattaforma hanno il compito esclusivo di controllo e registrazione dei versamenti effettuati. È una tipologia di mercato certamente più sicura, ma allo stesso tempo più complessa dal punto di vista tecnico; ciò comporta naturalmente un minore afflusso di clienti rispetto ad un mercato a gestione centralizzata.

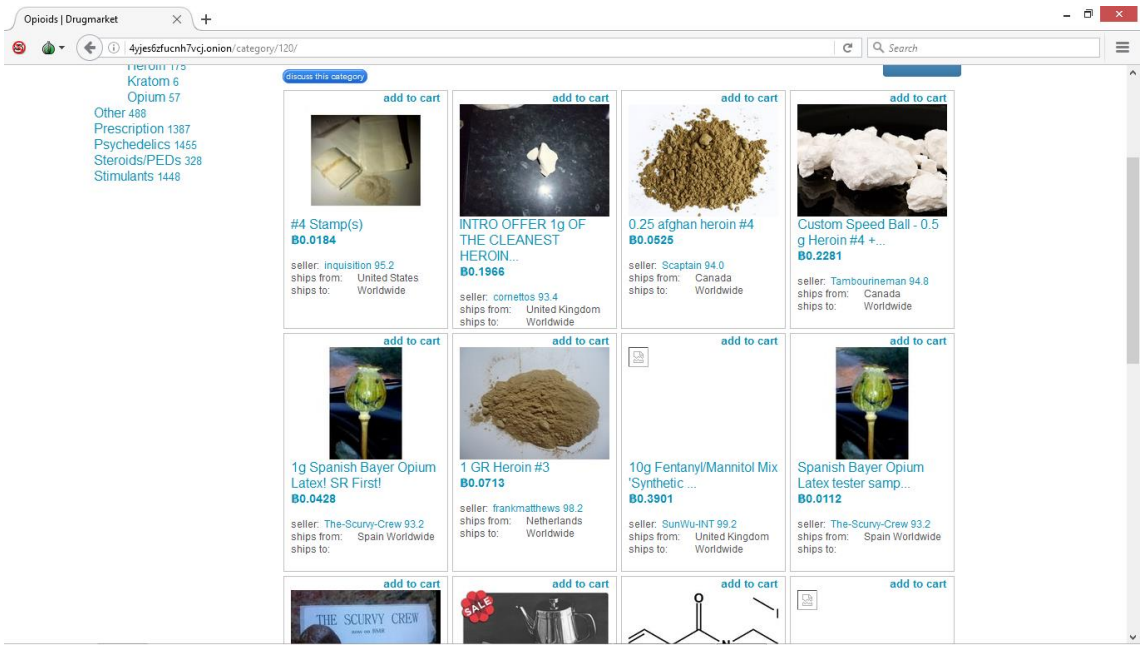
3.3 Prima fase: L'acquisto e le modalità di pagamento

Una volta selezionata la categoria, la pagina che si apre presenta tutte le finestre contenenti il prodotto e le relative informazioni. Potremo dunque verificare ad esempio la quantità di eroina proposta dal venditore, il paese d'origine ed infine, riportato in grassetto, il prezzo in Bitcoin, con a fianco il corrispettivo corrente in Dollari o in Euro. Ciascuno di questi mercati prevede l'acquisto quasi esclusivo tramite moneta virtuale, proprio in relazione alle caratteristiche più volte descritte (prime fra tutte l'anonimato e la non-rintracciabilità). È naturale infatti che nessuno inserirebbe i dati della propria carta di credito su un sito del dark web. Esistono tuttavia altri metodi di pagamento egualmente accettati, tra i quali quello che prevede l'utilizzo di una *PaySafeCard* (PSC), ossia uno strumento di pagamento prepagato spendibile online. Si tratta di una carta con un valore compreso tra i €10 e i €100, ed è possibile acquistarne al massimo dieci in una sola volta (per un valore totale di €1000). Poiché è acquistabile in diversi punti vendita attraverso contante, è un ottimo modo per effettuare pagamenti online mantenendo l'anonimato, ed è ovviamente possibile utilizzarla per acquistare sul mercato i Bitcoin, i quali saranno a loro volta spendibili nelle varie piattaforme.

Il prezzo della merce dunque, riportato in Bitcoin, presenta a lato il corrispettivo nella valuta selezionata, consentendo all'acquirente di effettuare un confronto con i prezzi correnti del mercato tradizionale. Considerando i dati forniti dal DCSA (Dipartimento Centrale Servizi Antidroga), il prezzo medio di una sostanza psicotropa può variare sulla base di diversi fattori quali purezza o paese di provenienza e sulla base che il prezzo sia quello del commercio o quello dello spaccio. Se consideriamo ad esempio l'eroina, distinta nelle due categorie principali di: H-4 (la più raffinata e costosa, detta anche "eroina bianca") ed H-3 (meno pura e chiamata, anche all'interno dei dark net markets "brown sugar"; è solitamente di provenienza afghana), sarà possibile notare che: il prezzo medio nello spaccio della tipologia H-4 è di circa €140 al grammo, quello della Eroina H-3 può invece variare dai €30 ai €35. Confrontando con i prezzi presenti in uno dei mercati del dark-web (vedi fig 3.1) è possibile notare come il prezzo di un grammo H-3

sia corrispondente a ฿ 0,0713. Se effettuiamo il cambio (dati del tasso aggiornati al 4 Novembre 2016) notiamo come il prezzo in euro corrisponda a circa €45, un prezzo lievemente superiore rispetto alla media del mercato tradizionale. Per quanto riguarda le offerte di H-4 invece, è possibile notare la presenza di una "*intro offer*", da parte dunque di un seller nuovo al mercato, pari a ฿ 0,1966: circa €125. Il prezzo in questo caso lievemente inferiore potrebbe essere giustificato proprio dalla natura stessa dell'offerta: come nel commercio tradizionale, un nuovo venditore che si approcci al mercato necessita di visibilità, dalla quale deriveranno i feedback sulla base degli acquisti. In questo tipo di compravendita infatti, il feedback positivo o negativo costituisce uno dei fattori-chiave di successo: nei tre mercati analizzati è dedicato ampio spazio ai "commenti" riportati, dal migliore al peggiore, nella parte inferiore a ciascun annuncio e nella pagina dedicata al singolo venditore.

***Fig.3.1**: Home page della piattaforma DrugMarket.onion*



3.4 Seconda fase: Versamento dei Bitcoin e spedizione

Ciò che più colpisce è proprio l'impressione che si ha durante la navigazione: sembrerebbe una normale compravendita realizzata su un qualsiasi sito di e-commerce, con la presentazione dei prodotti nel dettaglio, l'affidabilità del venditore, il paese di provenienza e le modalità di spedizione disponibili. Per quanto riguarda queste ultime, non è stato particolarmente semplice reperire alcune informazioni al riguardo: la maggior parte dei mercati consentono di ottenere informazioni sulla spedizione solo successivamente ad un eventuale acquisto. Tuttavia è stata colta l'occasione di sfruttare il servizio di messaggistica offerto da *Alphabay* (URL della piattaforma: http://pwoah7foa6au2pul.onion/register.php?aff=41211) volto a mettere in contatto l'eventuale acquirente con il venditore, per capire se fosse possibile ottenere qualche informazione in più. Si tratta di un servizio di messaggistica di tipo PGP (le sue modalità di funzionamento sono esposte in un documento reperibile sul sito http://www.pgpi.org/doc/pgpintro/), che si basa su messaggi crittografati e decriptabili solo attraverso l'utilizzo di particolari "chiavi"; gli stessi messaggi vengono poi eliminati entro un determinato arco di tempo definito dal venditore. Alla prima domanda, circa le modalità di iscrizione al sito in qualità di seller, è stato risposto che è necessario semplicemente seguire le procedure indicate nella sezione "*become a seller*", presente in ciascuno dei tre siti e contenente domande circa la motivazione del proprio interesse; è successivamente necessario creare un nuovo profilo utente attraverso un server da utilizzare a parte. In seguito sono state poste domande circa le modalità di svolgimento vero e proprio del lavoro (ad esempio se il venditore si affidasse ad alcuni dipendenti), alle quali tuttavia non è seguita una risposta. Circa le modalità di spedizione: una volta accordato il prezzo (è stato infatti possibile scoprire una certa flessibilità rispetto al prezzo indicato, soprattutto in relazione alle tipologie di eroina meno pure), il compratore versa i Bitcoin all'interno di un "blocco in sospeso"; il venditore spedisce la merce in un luogo segreto (il seller ha utilizzato il termine "hidden place") e al compratore, attraverso uno dei servizi di messaggistica anonima, verrà inoltrato un link contenente le coordinate di *Google Maps* per raggiungere il luogo (potrebbe trattarsi dell'abitazione di un affiliato al seller). A questo punto, una volta verificata la merce, il compratore inoltrerà al

venditore un *codice di sblocco*, da utilizzare appunto per incassare i Bitcoin accordati e mantenuti in sospeso. Nell'ipotesi in cui il venditore non riceva il codice, l'acquirente non potrà comunque ritirare i Bitcoin che erano stati inseriti nel blocco: questi infatti risultano "amovibili" e se non viene inviato il codice vengono semplicemente persi. In questo modo risulta evidente una tutela per entrambi i soggetti della compravendita: il compratore circa la disponibilità della merce, il venditore circa il pagamento.

3.5 La variabilità dei Bitcoin nel traffico di stupefacenti

Risulta ovvio quanto il valore dei Bitcoin possa influire nel guadagno potenziale dei rivenditori delle varie piattaforme. Una moneta che abbiamo visto essere sì anonima, non rintracciabile e facilmente fruibile, ma caratterizzata anche da un'estrema instabilità. Considerando le tempistiche che intercorrono tra il momento della spedizione della merce e l'invio del codice di sblocco (il rivenditore intervistato ha assicurato un margine massimo di 14 giorni per tutte le tipologie di spedizione nazionali), il valore dei Bitcoin può naturalmente subire variazioni improvvise e consistenti. Come non abbiamo mancato di sottolineare più volte infatti, la moneta in questione può mantenere il proprio valore stabile per settimane e subire un calo imprevisto e profondo nel giro di pochi giorni, se non poche ore (come dimostrato dal caso MtGox affrontato nel precedente capitolo). Naturalmente questo influisce sui guadagni dei rivenditori, rappresentando un rischio che solo coloro che sono già inseriti nel mercato da tempo preferiscono affrontare. In ogni caso l'instabilità del Bitcoin non rappresenta solamente un disincentivo al traffico realizzato nelle piattaforme del dark-web ma costituisce da sempre uno dei temi più ripresi dalla critica allo schema generale delle cripto-valute.

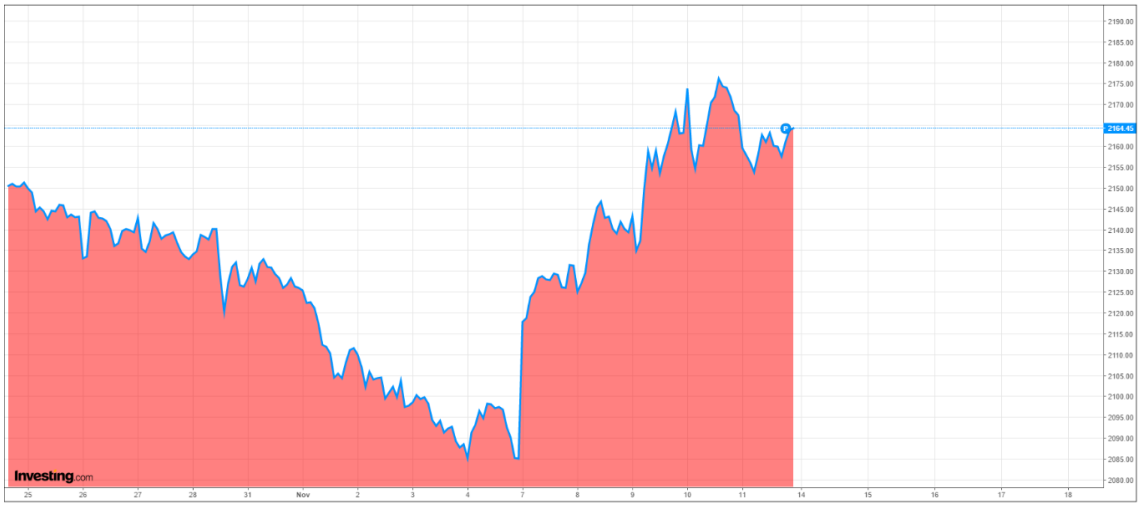
3.6 L'insicurezza dei mercati

L'ossatura decentralizzata, la mancanza di una vera e propria regolamentazione interna o di garanzia da parte di un'autorità centrale (ovvero tutti quei fattori innovativi e rivoluzionari del fenomeno) unitamente all'instabilità dimostrata, costituiscono forse il limite intrinseco alla stessa realtà BTC. L'economia virtuale del caso Bitcoin dimostra in ogni caso una continua e costante maturazione, influenzata sempre di più, paradossalmente, da economia e cambiamenti reali. Nel grafico presentato in Fig. 3.2 sono riportati i valori del prezzo di mercato (in USD) durante la settimana del referendum sulla "Brexit": è possibile notare, successivamente ad una fase più movimentata, un momentaneo assestamento della quotazione sui $600. Una seconda e più significativa variazione è invece quella precedente alle elezioni americane dell'8 Novembre scorso. In contemporanea alla generale penalizzazione dei mercati dovuta alla (per alcuni) inaspettata vittoria del neo-presidente Donald Trump, il valore dei Bitcoin ha dimostrato una costante ascesa (fig. 3.3): da una parte l'S&P500 con i suoi continui ribassi (vedi fig. 3.4), e il VIX (indice della volatilità) che procede parallelamente al rialzo, dall'altra la cripto-valuta con un incremento del 4% e un assestamento finale a $714 (più del doppio rispetto al valore del Novembre 2015). Un comportamento del tutto simile a quello di un bene rifugio (anche in questo potremmo proseguire con le analogie rispetto all'oro già discusse nel secondo capitolo). Proprio l'incertezza relativa alla prossima gestione economica della prima potenza mondiale, nonché un atteso scontro con i vertici della FED, sembra rendere particolarmente attraente una realtà che, nonostante l'intrinseca incertezza già discussa, ha dimostrato di poter "galleggiare" sopra le fluttuazioni di tipo economico e sociale.

***Fig.3.2**: Prezzo di mercato (USD) - 21-26/06/2016* *Fonte: Blockchain.info*

***Fig.3.3**: Prezzo di mercato (USD) - 05-12/11/2016* *Fonte:Blockchain.info*

***Fig.3.4**: Variazioni S&P500 durante la settimana elettorale americana* *Fonte: Investing.com*



3.7 Conclusioni

È forse ancora troppo presto per dare un giudizio definitivo sulla realtà Bitcoin, considerando il limite intrinseco dei 21 milioni. Secondo le ultime stime questo potrebbe essere raggiunto entro il 2033 e forse fino ad allora, a sistema ancora "incompleto", sarà sempre troppo presto. Quello che sappiamo per certo è che la realtà BTC ha rappresentato, e tutt'ora rappresenta, un vero e proprio attacco al controllo autoritario dello stato sulle riserve monetarie: rende possibile un libero mercato, nonostante l'ostilità delle legislazioni. Infatti non ci troviamo semplicemente di fronte alla prima moneta elettronica totalmente indipendente e libera, soggetta a convertibilità con altre unità attraverso il cambio di valuta; quanto piuttosto ad un sistema che sembra in grado di capovolgere e rendere inutili le attuali teorie monetariste così come la tecnica bancaria tradizionale. Lo schema che si è cercato di delineare all'interno di questa trattazione ci pone dunque di fronte alla realtà delle cripto-valute come ad un rischio e, come qualsiasi rischio economico, un'opportunità. Per coglierla in modo profittevole occorre che l'esperienza e la piena consapevolezza dei cambiamenti che sono in atto (sotto tutti i punti di vista del caso: dalla costante informatizzazione dei processi economici ai progressi della cosiddetta "fintech") prevalgano su quel tipo di euforia generica ma soprattutto confusa che solitamente circonda queste tematiche. Occorre sì riconoscerne gli aspetti positivi e rivoluzionari, ma allo stesso tempo individuare e ponderare anche i punti deboli e le meno o più evidenti falle. D'altra parte, si tratta in ogni caso di un sistema informatico, e in quanto tale comprende sempre un potenziale bug, un malfunzionamento, a prescindere dalla profondità in cui giace l'errore.

BIBLIOGRAFIA

BARRATT, M.J., (Febbraio 2014). "*Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States"* in "Addiction". Disponibile su http://onlinelibrary.wiley.com/doi/10.1111/add.12470/abstract .

CHAPMAN, S., (2011). *"Bitcoin: a guide to the Future Currency",* ZDNet.

CHIRIATTI, M., (Ottobre 2016). *"L'ecosistema del Bitcoin si rimette in discussione"* in "Il sole 24 ore". Disponibile su http://nova.ilsole24ore.com/progetti/lecosistema-italiano-del-bitcoin-al-centro/ .

DAVIS, J., (Ottobre 2011). *"The crypto-currency"* in "The New Yorker". Disponibile su http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency/ .

DE BIASE, L., (Maggio 2016). *"Bitcoin: il valore del salto tecnico"* in "Il sole 24 ore". Disponibile su http://lucadebiase.nova100.ilsole24ore.com/2016/05/18/bitcoin-il-valore-del-salto-tecnico/ .

EUROPEAN CENTRAL BANK (BCE), (Ottobre 2012). *"Virtual currency schemes".* Disponibile su http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf .

HARRISON, R., (2007). *"SecondLife: Revolutionary Virtual Market or Ponzi scheme?".* Capitalism 2.0 .

IRRERA, A., (Luglio 2013). *"Are Litecoins the next big thing?"* in "The Wall Street Journal". Disponibile su http://blogs.wsj.com/moneybeat/2013/07/08/forget-bitcoins-litecoins-are-the-next-big-thing/ .

KRUGMAN, P., (Aprile 2012). *"Adam Smith hates Bitcoin"* in "The New York Times". Disponibile su http://krugman.blogs.nytimes.com/2013/04/12/adam-smith-hates-bitcoin/?_r=0 .

MEGGIATO, R., (2014). *"Il lato oscuro della rete: alla scoperta del Deep Web e dei Bitcoin",* Apogeo.

NAKAMOTO, S., (2009). *"Bitcoin; a peer-to-peer Electronic Cash System".* Disponibile su http://bitcoin.org/bitcoin.pdf .

NARULA, N., (Maggio 2016). "*Il futuro del denaro",* Paper presentato alla conferenza internazionale *TEDx* di Parigi. Disponibile su https://www.ted.com/talks/neha_narula_the_future_of_money?language=it .

O' BRIEN, M., (Agosto 2012). *"Why the Gold Standard is the world's worst economic idea"* in "The Atlantic". Disponibile su http://www.theatlantic.com/business/archive/2012/08/why-the-gold-standard-is-the-worlds-worst-economic-idea-in-2-charts/261552/ .

SCHIROLI, I.W., (2012). "*Dark web & Bitcoin"*, Lantana Editore, Cerbara.

SOLDAVINI, P., (Settembre 2016). *"Il futuro della finanza in una BlockChain"* in "Il sole 24 ore". Disponibile su http://nova.ilsole24ore.com/frontiere/il-futuro-della-finanza-in-una-blockchain/ .