Università
Ca'Foscari
Venezia

Corso di Laurea Magistrale

(Ordinamento
ex D.M. 270/2004)

in Economia e Finanza

Tesi di Laurea

TECNOLOGIA BLOCKCHAIN e DISCIPLINA ANTIRICICLAGGIO in MATERIA DI CRIPTOVALUTE

Relatore:
Ch. Prof. Simone Mazzonetto

Correlatore
Ch. Prof. Marco Vedovato

Laureando
Matteo Busetto
Matricola: 848093

Anno Accademico
2017/2018

A Mario, Lorella e Annachiara.

INDICE

Abstract

Con il presente elaborato, si propone una analisi del funzionamento e delle innovazioni apportate dalla tecnologia Blockchain e dalle criptovalute in ambito finanziario (in particolar modo nell'esecuzione delle transazioni e dei pagamenti), soffermandomi sui rischi legati alla criminalità che caratterizzano questi nuovi strumenti e sulle relative implicazioni normative.

L'obiettivo è quello di fornire una descrizione dei presupposti su cui si basa e del funzionamento della Blockchain che sia quanto più comprensibile ed approfondita possibile, ma allo stesso tempo non eccessivamente tecnica, in modo tale da consentire di sviluppare alcune considerazioni riguardo ai rischi di riciclaggio e finanziamento al terrorismo che le criptovalute presentano ed alcune misure sia tecnologiche (differenti implementazioni nel protocollo) che di indagine che potrebbero attenuarli.

A tal proposito si vedranno anche le risposte normative date dai legislatori nazionali e sovranazionali allo sviluppo di questi nuovi strumenti, ai relativi mercati, nonché alle neonate figure che vi operano all'interno. Tale excursus si svilupperà in primis a livello italiano ed europeo (facendo riferimento al Decreto Legislativo italiano 90/2017 e alla recente V Direttiva UE antiriciclaggio) e successivamente a livello internazionale, portando, tra gli altri, gli esempi delle misure introdotte da Giappone, Stati Uniti e Cina e quelle "più innovative" di Venezuela e Dubai.

INTRODUZIONE

La Blockchain, spesso nota come "Tecnologia Ledger Distribuita", sta venendo divulgata da molti esperti come la più importante innovazione tecnologica dell'odierna economia. Anche se è difficile separare la sostanza dall'euforia, è chiaro che, non solo sono state lanciate migliaia di applicazioni basate su questa tecnologia ma anche che le maggiori imprese di molti settori stanno investendo ingenti risorse in attività legate alla Blockchain stessa. Tuttavia, è anche evidente che difficoltà gravi e ricorrenti ritardano, se non uccidono, quelle che per il momento sono ancora applicazioni modeste della stessa[1].
Nel corso della trattazione (così come spesso accade nella realtà) si farà principalmente riferimento alla Blockchain del sistema Bitcoin, in quanto questa nuova tecnologia, introdotta proprio dal protocollo Bitcoin, si mantiene la più diffusa ed importante tra quelle presenti ad oggi sul mercato. Si porteranno però anche esempi di natura differente descritti puntualmente al momento della citazione, in particolare quelli delle piattaforme Ripple ed Ethereum.

All'inizio dell'elaborato, verranno analizzati i presupposti che hanno portato alla nascita dei sistemi definiti come network Peer-to-Peer, all'interno dei quali si è sviluppata la Blockchain. Quest'ultima infatti, seppur resa nota da un Paper esplicativo pubblicato nel 2008 da uno pseudonimo noto come Satoshi Nakamoto, deve le sue origini anche ad altre applicazioni precedenti. Evidenziandone in primis gli aspetti caratteristici, si proseguirà poi fornendo un excursus maggiormente approfondito degli strumenti tecnico-matematici che permettono l'efficace funzionamento di tale tecnologia, quali la crittografia e gli algoritmi di Hash. Con ciò si vuole fornire uno strumento informativo che permetta allo stesso tempo di consentire una comprensione che sia più ampia possibile di un argomento che ad oggi in letteratura economica e nella cronaca giornalistica risulta tanto dibattuto quanto presentato in maniera frammentaria e talvolta poco esaustiva.
L'aspetto più contestato alle criptovalute è sicuramente il loro utilizzo a fini illeciti, che viene favorito dall'elevato livello di anonimato insito in questi strumenti. Per questa ragione, nel corso del secondo capitolo, ci si soffermerà sugli aspetti legati alla criminalità

[1] A tal proposito si consiglia la lettura di: "Economic Working Paper Series, Working Paper No. 1549" Universitat Pompeu Fabra Barcelona, gennaio 2018.

ed ai cosiddetti “mercati neri” che si sono sviluppati negli ultimi anni anche (o soprattutto) grazie all’utilizzo delle criptovalute come mezzo di scambio all’interno del Dark Web, fornendo a supporto di ciò dati numerici che permettano di sviluppare considerazioni consapevoli.

Successivamente, dopo aver delineato i reati di riciclaggio e finanziamento del terrorismo, verrà riportata la normativa a livello italiano ed europeo al fine di evidenziare come si è evoluta tale disciplina con l’obiettivo di contrastare, oltre alle forme più “tradizionali” con cui sono compiuti tali reati, anche questi nuovi fenomeni. A tal proposito si farà riferimento al *Decreto Legislativo n. 90/2017* ed alla recente *V Direttiva UE antiriciclaggio*.

Per concludere poi, nel tentativo di comprendere le problematiche che si presentano nel tentativo di regolamentare uno strumento tanto innovativo quanto atipico come le criptovalute, con l’obiettivo di tutelarne gli utenti e al contempo di non ostacolarne lo sviluppo, sarà eseguito un confronto tra le principali misure adottate dai regolatori in ambito normativo a livello internazionale. Tra i principali tentativi di regolamentazione verranno analizzati quelli adottati da Giappone, Stati Uniti, Russia e Cina, nonché altri in un certo senso maggiormente innovativi che hanno portato addirittura all’adozione di una “criptovaluta di stato” come nei casi di Venezuela e Dubai.

CAPITOLO 1

"LA TECNOLOGIA BLOCKCHAIN"

1.1) BREVE STORIA DELLE CRIPTOVALUTE

Quando ci riferiamo ai nuovi strumenti di pagamento definiti "criptovalute", molto spesso vi è una confusione di fondo nella terminologia utilizzata per delinearle, sia nel parlare comune che all'interno della letteratura economica. Normalmente, si fa riferimento ai termini "valuta virtuale" e valuta digitale" utilizzandoli come sinonimi, in realtà però, almeno all'origine, tra i due vi è differenza. Le valute virtuali sono un tipo di valuta digitale ma non viceversa.[2] Le varie criptovalute[3] (come la più conosciuta tra queste: il Bitcoin[4]) pur ricadendo nell'ampio insieme delle valute digitali, differiscono dalle stesse. Le criptovalute infatti sono propriamente valute memorizzate e scambiate in maniera elettronica (qualsiasi forma di denaro rappresentato in forma binaria soddisfa questa definizione) ma che rispetto alle valute digitali non sono denominate in moneta avente corso legale (fiat money) bensì possiedono una propria unità di conto[5].

[2] Capaccioli S., "Criptovalute e bitcoin: un'analisi giuridica", Giuffrè Editore, 2015.

[3] Una Criptovaluta è definita come una rappresentazione digitale di valore, la cui proprietà è mantenuta da una Blockchain che la utilizza come strumento di pagamento per compensare gli appartenenti al network e mantenere l'integrità del Sistema stesso. "D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps", Apress, 2017.

[4] Nel corso di tutta la trattazione, come già anticipato all'interno dell'introduzione, faremo riferimento al Bitcoin come criptovaluta principale per spiegare il funzionamento della Blockchain e le relative problematiche nell'ambito della normativa per il contrasto al riciclaggio (in alcuni esempi specifici poi saranno esplicitate anche differenti criptovalute come Ripple, Ethereum o altre).

[5] Tra le varie classificazioni date in letteratura e che attribuiscono le criptovalute a differenti insiemi o sottoinsiemi di valute digitali e virtuali (ad esempio quella di Capaccioli S.) nel presente elaborato si è utilizzata principalmente quella fornita dal Fondo Monetario Internazionale in quanto ritenuta la maggiormente autoritaria e globalmente diffusa. Fonte: "IMF staff discussion note: Virtual Currency and Beyond: initial considerations". Gennaio 2016.

Come si può vedere dalla *Figura 1*, potremmo riassumere le differenti classificazioni utilizzando una forma ad "imbuto" in cui ciascun gruppo superiore contiene al suo interno anche tutti quelli a sé inferiori.

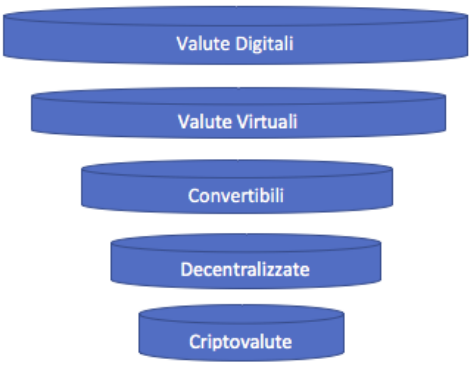


Figura 1: Classificazione valute.

Bisogna inoltre evitare di confondere il concetto di valuta virtuale (e dunque di criptovaluta) con un'altra espressione che spesso è usata in maniera intercambiabile con queste ultime ma che descrive un fenomeno totalmente differente: ci stiamo riferendo alla "moneta elettronica" (e attenzione anche alle monete locali[6]). Con questa espressione si designa il valore monetario definito all'art. 2 n. 2) della *Direttiva 2009/110/CE*, come quel "*valore memorizzato elettronicamente, ivi inclusi la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica*". In questo caso perciò si fa riferimento alla memorizzazione elettronica di valore che però è rappresentato da denaro avente corso legale (per avere un'idea più chiara, si tratta ad esempio, del denaro memorizzato nelle carte di credito o di pagamento) che quindi si riscontra in un mondo antitetico rispetto a quello in cui vorrebbero situarsi le criptovalute (ed in seguito ne vedremo le motivazioni).

[6] Note anche come monete complementari, queste ultime sono utilizzate in ambiti molto ristretti, quali una città o una regione e tra un numero limitato di utenti. Definizione tratta da "V Direttiva europea Antiriciclaggio (2018/843)".

L'innovazione portata dalle criptovalute si evidenzia nel fatto che queste ultime sono costituite da un processo che incorpora i principi della crittografia con una valuta virtuale decentralizzata e quasi sempre limitata nella quantità totale di emissione[7].

Il primo elaborato che introdusse il concetto di criptovaluta venne pubblicato da David Lee Chaum nel 1982[8], lo stesso autore successivamente, nel 1990, fondò la società Digicash, prima impresa che cercò di integrare crittografia e strumenti di pagamento digitali al fine di rendere anonime le transazioni (all'interno però di un sistema centralizzato[9]). La società però entrò successivamente in bancarotta nel 1998.

Per quanto riguarda invece la descrizione di un "Distributed Electronic Cash System", questa venne eseguita per la prima volta nel 1998 da Wei Dai, un ingegnere informatico, e chiamata B-MONEY. Le idee di quest'ultimo, fungeranno da base teorica per il successivo sviluppo delle criptovalute. Tra i principali precursori è importante ricordare anche il lavoro effettuato da Nick Szabo, studente di legge, blogger e crittografo, tramite l'introduzione, nel 2005, del "Bit-gold"[10].

Nel 2008 infine il contributo determinante per portare definitivamente alla ribalta il tema delle criptovalute si concretizzò attraverso la proposta di Satoshi Nakamoto. Questo nome, utilizzato con ogni probabilità come uno pseudonimo (corrispondente ad una persona o gruppo tuttora sconosciuto[11]) fa riferimento al soggetto cui si deve, in primis, la registrazione del dominio "bitcoin.org", in data 18 agosto 2008 e successivamente, il 31 ottobre dello stesso anno, la pubblicazione di un documento[12] in cui veniva descritto un protocollo (un insieme di regole o procedure per la trasmissione di dati tra dispositivi elettronici, come i computer) che permetteva di creare un Peer-to-Peer System, ossia un sistema di cassa elettronico, utilizzando una valuta virtuale, nota come bitcoin[13]. Anche se

[7] La quantità di emissione predefinita non è fattore caratterizzante della totalità di criptovalute esistenti (ad esempio non è così per Ethereum) ma è elemento determinante nella grande maggioranza delle stesse.

[8] D. Chaum, "Blind Signatures for Untraceable Payments", 1982.

[9] La pubblicazione di Chaum inizialmente non riscosse molto successo, ciò fu in parte dovuto al fatto che l'uso della crittografia in quegli anni era associato principalmente al movimento Cypherpunk: movimeto attivo dalla fine degli anni '70 soprattutto negli Stati Uniti, che faceva uso della crittografia informatica per mascherare I messaggi scambiati tra i partecipanti e si opponeva all'establishment di governi e gruppi economici al fine di avviare un cambiamento sociale e politico.

[10] La criptovaluta in oggetto non fu però mai implementata concretamente.

[11] Ad oggi le ipotesi maggiormente accreditate ritengono che dietro questo pseudonimo si celi l'identità di un team di sviluppo che dopo la creazione della tecnologia e della rete Bitcoin abbia preferito mantenere la propria identità come anonima.

[12] Satoshi Nakamoto, "Bitcoin: a peer-to-peer Electronic cash system", 2008.

[13] E' necessario ricordare che, per convenzione, il termine Bitcoin con la "B" maiuscola sta ad indicare la tecnologia e la rete del sistema, mentre bitcoin con la "b" minuscola la valuta utilizzata all'interno del sistema stesso.

alcuni, perlomeno inizialmente, erano scettici riguardo al successo di bitcoin come strumento che potesse rivelarsi al pari della moneta, più il tempo passava e più divenne evidente che a prescindere dal possibile successo o meno in futuro di tale sistema (successo che poi, a livello di rendimenti realizzati e di notorietà mediatica vi è sicuramente stato, almeno fino ad ora) la vera rivoluzione era la tecnologia che stava alla base della stessa valuta virtuale introdotta da Nakamoto: la cosiddetta Blockchain.

Prima di addentrarci però nella comprensione della tecnologia Blockchain e dei meccanismi che la costituiscono è necessario porre dei presupposti teorici di base.

1.2) STRUTTURA DI UN SISTEMA

Quando ci riferiamo alla struttura di un sistema intendiamo la disposizione dell'insieme di elementi singoli che lo compongono, i quali connessi tra loro formano un elemento unico e più complesso.

I tre tipi più comuni di struttura per un sistema (economico, urbanistico o informatico che sia) sono:

- centralizzato

- decentralizzato

- distribuito

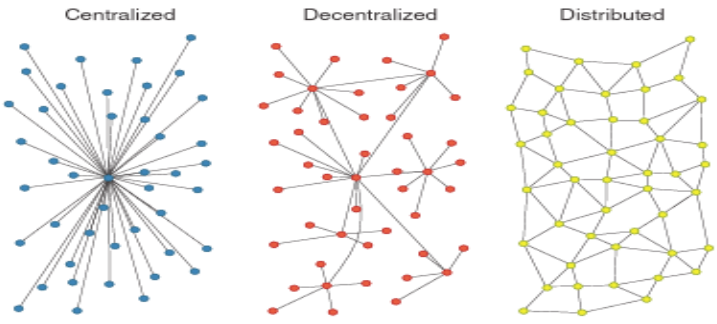


Figura 2: Fonte: "p2pfoundation.net".

- Un sistema centralizzato può essere meglio pensato come una struttura a "mozzo e raggi", dove un componente dominante si trova al centro e coordina gli altri. Questa non solo è la struttura del moderno sistema finanziario ma è anche la struttura utilizzata da linee aeree commerciali ed urbanisti. La città di Boston ad esempio è soprannominata "The Hub" perché si trova al centro di un sistema a raggi che costituisce le periferie. Nell'ora di punta però, se si verifica un incidente al centro, questo può influenzare il trasporto in tutte le zone limitrofe della città. Ciò denota uno dei limiti maggiori di questo tipo di reti, in quanto l'eccessiva dipendenza di tutti i raggi (o partecipanti) nei confronti del centro (inteso come centro cittadino per una rete urbana o di entità centrale per un sistema economico o informatico) si riflette in una debolezza nel momento in cui il coordinamento tra i nodi e l'Hub dovesse, per qualsiasi ragione, fallire. La Grande Depressione avvenuta negli anni '30 del 1900 negli Stati Uniti è un esempio dei pericoli in cui un sistema finanziario centralizzato può incorrere.

- Un sistema decentralizzato cerca di correggere i difetti insiti nei sistemi centralizzati creando più Hub e raggi. In un sistema di questo tipo, ci sono molti nodi (o Hub), ciascuno incaricato di garantire il flusso regolare del traffico, sia che il traffico siano informazioni, piuttosto che messaggi di testo o transazioni finanziarie. Il sistema regionale della Federal Reserve statunitense è un buon esempio di questa decentralizzazione: ciascuna delle banche centrali regionali deve assicurarsi che il sistema finanziario della propria regione sia in buona salute.

  In questo sistema però i vari nodi devono comunque fare riferimento ad una struttura centrale sebbene siano dotati di una certa autonomia.

  Pur rimanendo il rischio che molti Hub falliscano allo stesso tempo, questo sistema è sicuramente un passo avanti, in termini di sicurezza, rispetto al precedente.

- Un'evoluzione del sistema decentralizzato è quello cosiddetto "distribuito" (3° tipo) in cui ogni partecipante agisce come un Hub: ogni individuo, business, computer o governo che sia, possiede uguale responsabilità e assicura il buon funzionamento del network stesso. In un sistema distribuito, se un nodo fallisce, gli altri nodi semplicemente prendono il suo posto e si assicurano che il meccanismo di

trasmissione proceda senza intoppi. È importante notare che nessuno dei componenti è obbligatoriamente collegato in maniera diretta con tutti gli altri, bensì è sufficiente che la connessione tra questi avvenga perlomeno indirettamente.

Questo ultimo tipo di sistemi, oltre ad essere utilizzato (come già abbiamo specificato in precedenza) per organizzare il sistema economico, piuttosto che quello urbanistico, è anche utilizzato nell'architettura dei sistemi informatici presentando una potenza di calcolo maggiore unita a costi di gestione inferiori e ad una maggiore affidabilità oltre alla possibilità di crescita naturale che deriva dall'aggiunta progressiva di nuovi partecipanti al network. In compenso però, a questi vantaggi, si oppongono una maggiore difficoltà di coordinamento e una complessità di programmazione superiore che potrebbero comportare alcuni svantaggi in termini di sicurezza.

Una tipologia di sistemi distribuiti è costituita dai network "Peer-to-Peer". Nella sua forma più semplice, un network Peer to Peer è rappresentato da due computer che scambiano tra di loro informazioni sfruttando una connessione di tipo USB come mezzo di comunicazione. Un sistema di questo tipo si costituisce quando due o più computer si possono inviare le suddette informazioni senza dover passare attraverso un calcolatore centrale (il cosiddetto server) che coordini il tutto; per questo si dice che i componenti di tali reti condividono parte delle loro risorse informatiche: CPU, memoria dell'Hard Disk, RAM, larghezza della banda e così via. Non vi è una gerarchia tra i nodi della rete, come invece ci sarebbe all'interno di una rete centralizzata (dove il server coordina i nodi), ed è appunto per questo motivo che a queste tipologie di rete è attribuito il nome Peer-to-Peer ("capace di condivisione diretta").
A seconda poi del numero di componenti presenti nel sistema, questo sarà più o meno grande e presenterà una potenza di calcolo che aumenta all'aumentare della dimensione del network stesso.

A seconda di come i nodi sono collegati tra loro è possibile suddividere le reti peer-to-peer in strutturate e non strutturate:

- **Reti peer-to-peer strutturate** *(figura 3[14])*: una rete strutturata è caratterizzata da una topologia specifica, che assicura che ogni nodo possa efficientemente cercare e trovare una determinata risorsa o un altro nodo all'interno del sistema in qualsiasi momento. Per facilitare questo compito, ogni rete strutturata organizza al proprio interno le informazioni attribuendo alle stesse un codice. Inoltre, per far sì che il flusso di dati non incontri ostacoli di sorta, è necessario che ogni nodo conservi un elenco dei nodi "vicini" che rispetti criteri molto vincolanti. Questo può costituire un grosso limite in termini di efficienza, nel caso in cui il network sia caratterizzato da nodi che entrano o escono dalla rete molto frequentemente.

- **Reti peer-to-peer non strutturate** *(figura 4)*: come suggerisce anche il nome, una rete non strutturata è caratterizzata da un'apparente disorganizzazione ed è formata da nodi che creano collegamenti casuali con altri nodi appartenenti alla rete. Si tratta, dunque, di reti di facile "formazione", che non richiedono il rispetto di parametri particolarmente stringenti, ma che allo stesso tempo, data la mancanza di una struttura e di un'organizzazione interna, rendono particolarmente complessa (e dispendiosa in termini di tempo) la ricerca di file o risorse all'interno del network stesso: la richiesta di un determinato dato infatti, dovrà essere inviata a tutti i nodi che condividono il file. Ciò, ovviamente, genera un elevato volume di traffico, senza la certezza però di riuscire a individuare la risorse cercata.

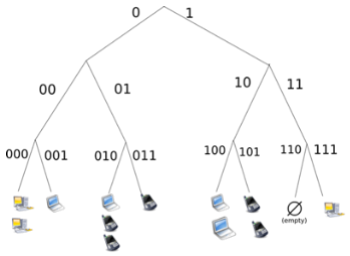


Figura 3.

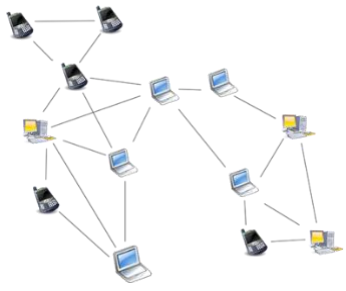
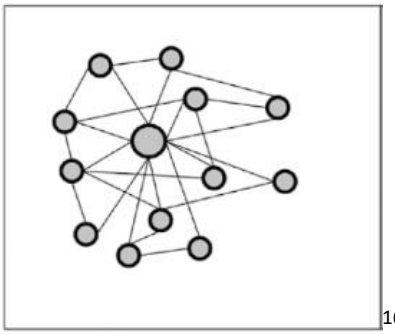


Figura 4.

[14] Immagini tratte da: "www.Fastweb.it"

I sistemi centralizzati e quelli distribuiti (di cui appunto abbiamo visto fanno parte anche i Peer-to-Peer) pur essendo strutturalmente agli antipodi, in realtà possono anche essere combinati tra loro: esistono infatti sistemi distribuiti in cui però tutti i nodi oltre ad interagire reciprocamente, si rifanno ad un nodo centrale (vedasi *Figura 5)* e sistemi centralizzati in cui in realtà il centro è costituito da un insieme di nodi distribuiti (*Figura 6*), collegato a sua volta ai nodi esterni ad esso. (Casi concreti che utilizzano questo tipo di struttura verranno riportati alla fine del capitolo[15]).



[16]

Figura 5.

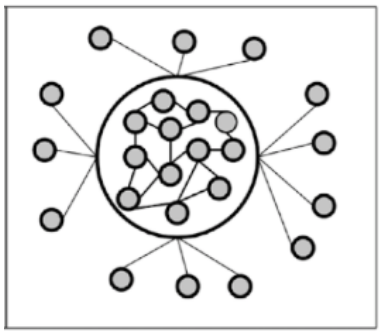


Figura 6.

Uno degli esempi più rilevanti di network distribuiti è stato quello costituito dall'adozione, nel 1972, dei protocolli TCP/IP[17] (trasmission control protocol/internet protocol) i quali posero le basi per lo sviluppo di Internet. Questi protocolli crearono un network pubblico e condiviso, senza nessuna autorità centrale responsabile per il suo mantenimento o miglioramento, sovvertendo il precedente modello di telecomunicazioni basato sul "circuit switching" in cui le connessioni tra 2 parti o macchine dovevano essere prestabilite e sostenute attraverso uno scambio (in linee dedicate).

Il nuovo protocollo trasmetteva informazioni digitalizzandole, spezzettandole in piccolissimi blocchi, i quali, una volta inseriti nel network potevano prendere qualsiasi

[15] Vedasi a tal proposito il caso Ripple.

[16] Immagini esemplificative tratte da: D. Drescher, "Blockchain Basics: A Non-Technical Introduction in 25 Steps", Apress, 2017.

[17] Per Internet Protocol (IP) si intende il protocollo di rete appartenente alla suite di protocolli internet TCP/IP su cui è basato il funzionamento della rete Internet. All'interno di una rete IP, ad ogni interfaccia connessa alla rete fisica viene assegnato un indirizzo che è univoco. "Harvard Business Review- Jen-Feb 2017".

direzione verso il destinatario che a sua volta avrebbe assemblato nuovamente i blocchi ed interpretato i dati.

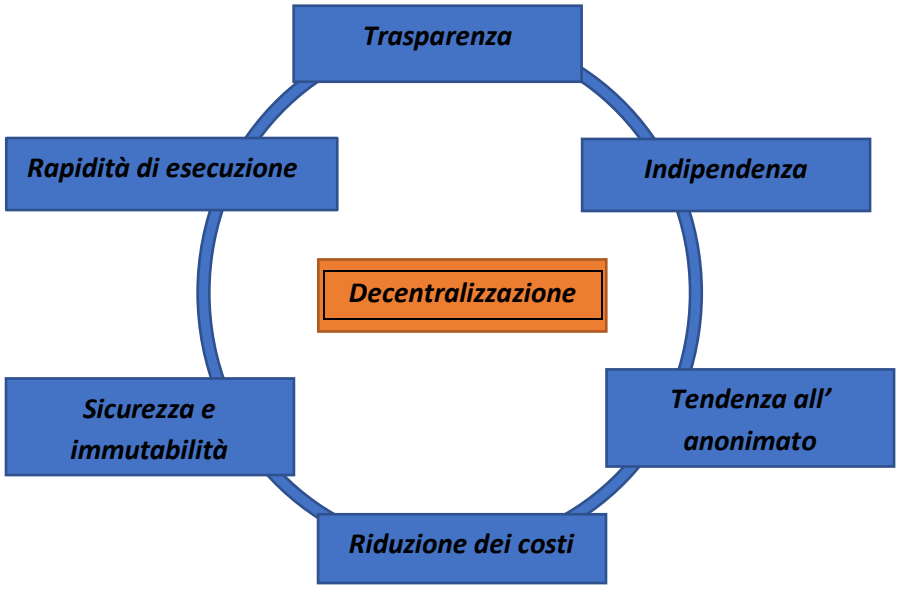
Internet è stato il primo esempio di decentralizzazione sistemica su larga scala. Si pensi ad esempio all'enciclopedia, prima dell'avvento di Internet vi era un'istituzione centrale che creava l'enciclopedia (ad esempio l'Enciclopedia Britannica o la Treccani) e solo chi ne acquistava le copie aveva accesso all'informazione, ora invece dopo l'avvento di internet vi è stata appunto una decentralizzazione, tutti possono accedere all'enciclopedia in maniera rapida e spesso senza costi[18]. Le similitudini tra i protocolli che introdussero internet e la Blockchain sono evidenti: Il processo di sviluppo e manutenzione di una Blockchain è aperto, distribuito e condiviso, proprio come quello per i protocolli TCP/IP e così come i primi hanno posto le basi per l'introduzione di internet i bitcoin hanno introdotto la Blockchain[19].

Per quanto riguarda invece il primo esempio dirompente di programma basato su un sistema Peer to Peer di massa all'interno della rete internet, bisogna fare riferimento alla fine degli anni '90 (più precisamente al 1999) con l'avvento di Napster. Quest'ultimo infatti, configuratosi come un sistema di file-sharing che, sebbene non fosse un Peer to Peer puro, in quanto utilizzava un sistema centrale per mantenere la lista dei partecipanti connessi e dei file condivisi (e quindi si situasse in quella tipologia ibrida tra sistemi distribuiti e centralizzati presentata precedentemente) consentiva di effettuare transazioni direttamente tra i vari partecipanti. Tramite Napster infatti, gli utenti erano in grado di condividere qualsiasi tipo di file Mp3 musicale si trovasse all'interno del proprio computer con gli altri partecipanti alla rete. Il successo dello stesso durò però pochi anni in quanto nel 2001 Napster fu obbligata a chiudere l'attività per violazione di Copyrights.

Se volessimo riassumere all'interno di alcune macro categorie, le caratteristiche e i vantaggi dei sistemi di tipo distribuito (e dunque Peer to Peer), questi ultimi potrebbero essere così schematizzati:

[18] In questa analisi non ci soffermiamo a discutere sul fatto che Wikipedia o altre enciclopedie gratuite/a basso costo online abbiano contenuti di dubbia veridicità o bassa qualità rispetto alle enciclopedie tradizionali ma lo consideriamo solo come un esempio esplicativo per comprendere il concetto di decentralizzazione delle informazioni che è stato portato dall'avvento di internet.

[19] Esempio tratto da TEDx Talks "New kids on the Blockchain" 24/03/2016.



1.3) BLOCKCHAIN: DEFINIZIONE ED INTRODUZIONE

Il termine Blockchain[20], come già anticipato nell'introduzione a questo elaborato, apparso per la prima volta per descrivere il sistema di registrazione introdotto dal protocollo Bitcoin, è ormai generalmente utilizzato per descrivere qualsiasi forma di tecnologia DLT (Distributed Ledger Technology) ispirata al design di quella che sta alla base della più famosa (almeno ad oggi) criptovaluta. La base teorica da cui si sostanzia la Blockchain è la volontà di creare un sistema che non richieda un emittente o un controllore (ente terzo) bensì che si sviluppi in maniera decentralizzata e si caratterizzi per l'essere resistente e sicuro così da permettere lo scambio diretto tra le parti coinvolte.

Il protocollo ideato si caratterizza per il fatto di essere "open-source" ossia a codice libero, permettendo a chiunque di scaricarlo ed eventualmente di utilizzarlo o modificarlo per

[20] Nella sua forma più semplice una Blockchain è un database condiviso dove tutte le transazioni di un determinato asset sono registrate all'interno di blocchi di dati crittografati in modo da risultare immutabili. Per quanto riguarda invece un Distributed Ledger System, con questo termine si intende un network che utilizza una tecnologia ispirata a quella che sta alla base delle criptovalute per verificare o trasferire valore. D. LEE Kuo Chuen, R. H. DENG, "Handbook of blockchain, digital finance and inclusion – volume 2", Elsevier, 2018.

crearne implementazioni differenti[21]. Questo fattore si rivela molto interessante dal momento che consente a chiunque di apportare migliorie al protocollo iniziale proponendone in futuro versioni alternative e migliorando eventuali limiti che dovessero sopraggiungere, in modo da consentire alla tecnologia stessa ampie possibilità di continuità anche in periodi successivi a quello durante il quale stiamo scrivendo. Tale sistema di registrazione presenta un potenziale tanto innovativo quanto dirompente che ha affascinato i tecnici, i leader aziendali e le aziende tecnologiche, soprattutto all'interno del segmento FinTech[22], in quanto affronta due degli aspetti più rischiosi della vita e degli affari svolti tramite l'ausilio di Internet: FIDUCIA ed INTEGRITA'[23]. I problemi riguardanti sicurezza, privacy e fiducia che contraddistinguono Internet sono da tempo riconosciuti e, fin dagli inizi degli anni '80, gli esperti hanno lavorato per trovare una soluzione a questi ultimi. Fino a pochi anni fa, l'utilizzo di intermediari è stato il metodo migliore per completare le operazioni in modo sicuro e garantire un soddisfacente livello di fiducia nella validazione delle stesse. Come sappiamo però, la sicurezza di questi intermediari è spesso un punto debole e le violazioni dei dati lasciano vulnerabili le informazioni personali e finanziarie dei singoli, mettendo spesso a rischio la fiducia negli stessi[24].

Per realizzare i propri obiettivi, la tecnologia Blockchain utilizza un registro (definito come Ledger) che serve da un lato, come mezzo per **dimostrare la proprietà** (la quale prevede 3 steps per essere "certificata": identificazione del proprietario, indicazione dell'oggetto posseduto, registrazione dell'oggetto in capo al proprietario stesso) e dall'altra per **documentarne il trasferimento**. Ciò risulta più semplice per il fatto che questo registro è

[21] A tal proposito si vedrà che partendo dai caratteri basici della tecnologia Blockchain introdotta da Bitcoin sono state successivamente sviluppate ulteriori versioni della stessa, che hanno portato alla creazione di molteplici criptovalute alternative (cosiddette Alt-coin) le quali hanno cercato di apportare alcune migliorie al codice di sviluppo iniziale soprattutto a livello di sicurezza ed efficienza. Oltre a ciò, sono state sviluppate anche versioni di Blockchain che pur partendo dai tratti fondamentali della stessa, ne hanno in un certo senso snaturato gli aspetti fondamentali per far si di creare protocolli differenti e specifici per determinati usi (ad esempio le piattaforme Ethereum e Ripple che vedremo alla fine del capitolo).

[22] FinTech: definito come insieme di soluzioni tecnologiche e start-up che hanno cambiato e/o migliorato il modo in cui società finanziarie, banche e assicurazioni fanno business. Steven R. Kursh, Natalia A. Gold, D 'Amore-McKim School of Business, Northeastern University - Boston, MA, USA 2016.

[23] Integrità intesa come la capacità di un sistema di compiere transazioni veritiere rispetto alla proprietà e di assicurare che solo il vero proprietario possa trasferire i propri diritti a terzi. In aggiunta a ciò il Sistema dovrà essere: sicuro, completo, corretto e libero da errori. D. Dresher, "Blockchain Basis", Apress, 2017.

[24] A tal proposito, il 45% degli intermediari finanziari, come le reti di pagamento, le borse valori ed i servizi di trasferimento di denaro, sono soggetti ogni anno a frodi o crimini. Fonte: Alex Tapscott e Don Tapscott "Harvard business Review", 01/03/2017".

aperto a tutti e che chiunque può dunque consultarlo (semplicemente scaricando sul proprio terminale il software dedicato).
Il fatto di avere un solo registro "fisico", come accade in molte situazioni nell'odierna società, comporta dei rischi in quanto quest'ultimo può essere danneggiato, manipolato o addirittura distrutto; per questo il Ledger Blockchain, essendo condiviso, consultabile da tutti e non posseduto singolarmente da nessuno permette di mantenere le informazioni con una maggiore integrità e come vedremo in seguito, con possibilità di modifica davvero ridotte.

1.3.1) Problemi a cui la Blockchain cerca di porre rimedio

Soffermandosi in primis sull'integrità di una transazione, uno degli ostacoli principali che da sempre si ripropone nell'esecuzione di un pagamento è il cosiddetto problema del "Double Spending". Con questa espressione si fa riferimento al fatto che una parte possa realizzare 2 transazioni nello stesso momento, ma possedere le risorse adeguate solo per realizzare una delle stesse, creando un pericolo nel funzionamento del sistema. Questa debolezza fino ad oggi è stata risolta affidandosi ad un ente terzo (banca o intermediario che sia) che svolgesse la funzione di "validatore" centrale delle operazioni, assicurandosi che solo quelle veritiere venissero registrate ed eliminando eventuali doppioni. Ciò però non può avvenire in un sistema Peer-to-Peer dato che, come abbiamo visto fin dall'inizio, in questo tipo di sistemi non è presente un'autorità centrale validatrice. Il rischio di doppia spesa perciò è ancora più elevato dal momento che, nel contesto dei beni digitali, i dati in un computer possano essere copiati senza troppe limitazioni e quindi risultare facilmente duplicabili sfruttando eventuali "debolezze" del registro condiviso, il quale potrebbe non essere sempre aggiornato nello stesso istante da tutti i partecipanti, permettendo potenzialmente a chi ha l'ultima versione dello stesso di sfruttare il gap con chi non la ha e trasferire la proprietà più di una volta, eliminando quella unicità necessaria per garantire l'affidabilità del sistema stesso.
Spostandoci poi nell'ambito della fiducia, un ulteriore problema è quello, già conosciuto anche in passato, come "Problema dei Generali Bizantini[25]", nel quale, tramite una metafora, si immagina che alcune divisioni dell'esercito bizantino (rappresentati in questo

[25] Problema proposto per la prima volta nel 1982 dagli scienziati informatici L. Lamport, R. Shostak e M. Pease.

caso i vari nodi appartenenti ad un sistema distribuito) siano accampate in una valle agli antipodi delle mura di una città nemica, ognuna delle quali comandata dal proprio generale. I generali possono comunicare l'uno con l'altro solo attraverso l'ausilio di messaggi trasportati personalmente dai propri soldati, date le mura che li separano. Dopo aver osservato il nemico, questi ultimi devono concordare un piano comune di azione. Alcuni generali però potrebbero essere traditori e cercare di impedire ai generali leali di raggiungere un accordo. I generali (ipotizzati come metafora dei computer) devono perciò essere in possesso di uno strumento (un algoritmo[26] nel nostro caso) che garantisca:

1) Che tutti i generali fedeli decidano per lo stesso piano d'azione.
I generali fedeli faranno tutto quello che dice l'algoritmo, ma i traditori possono fare tutto ciò che desiderano. L'algoritmo deve garantire la condizione 1 indipendentemente da ciò che i traditori faranno. I generali fedeli poi non dovrebbero soltanto raggiungere l'accordo, bensì concordare anche su un piano ragionevole.

Ci si vuole perciò assicurare anche che:

2) Un piccolo numero di traditori non possa far sì che i generali fedeli adottino un piano negativo.
Internet è un network di computer non sicuro, è come le mura della valle attraverso le quali i messaggi dei generali devono essere inviati ma in cui non c'è nessuna assicurazione sul fatto che il messaggio inviato sia lo stesso che poi verrà ricevuto, ciò è tanto più pericoloso quanto più è prezioso il messaggio/bene inviato (pensiamo al valore di una criptovaluta).

La soluzione a questo problema richiede un metodo per proteggere i contenuti dal momento in cui questi sono inviati a quello in cui sono ricevuti, una tecnica per ridurre al

[26] Nella sua forma essenziale, quando si parla di algoritmo si fa riferimento ad una procedura step by step, visualizzabile attraverso la forma di un diagramma ad albero e scandita da passaggi molto precisi. L'espressione deriva dalla parola latina "algorithmus", a sua volta derivante da "Al-Khwarizmi": soprannome di un matematico arabo (Muhammad ibn Mūsa) del nono secolo, ritenuto tra i primi ad aver teorizzato il concetto. In origine utilizzato per indicare procedimenti di calcolo basati su cifre arabe, il termine algoritmo è stato poi adottato nella matematica e nella logica moderna, dove indica un procedimento di calcolo descrivibile da un certo numero di formule, nonché in informatica per indicare un insieme di istruzioni da applicare per eseguire un'elaborazione o risolvere un problema.

minimo il numero di messaggi inviati e una per individuare quelli falsi. Vedremo che la Blockchain cerca di superare queste criticità attraverso l'utilizzo della crittografia, con l'ausilio di un sistema criptato di messaggi che impone un costo per decodificare gli stessi fornendo al contempo un modo per verificare che il messaggio sia stato legittimamente decodificato ed un incentivo ai "generali" onesti. Infatti si analizzerà in seguito che, se i generali traditori volessero inviare un messaggio falso (transazione erronea) dovrebbero sostenere il costo di possedere una strumentazione informatica all'avanguardia e quello legato al consumo di energia elettrica richiesta per operare con la stessa. Se qualcuno volesse immettere nella rete un messaggio falso senza sostenere questo costo, gli altri partecipanti, potrebbero, semplicemente guardando la potenza di calcolo utilizzata da questo soggetto, capire che la transazione è falsa.

1.4) BLOCKCHAIN: IL FUNZIONAMENTO

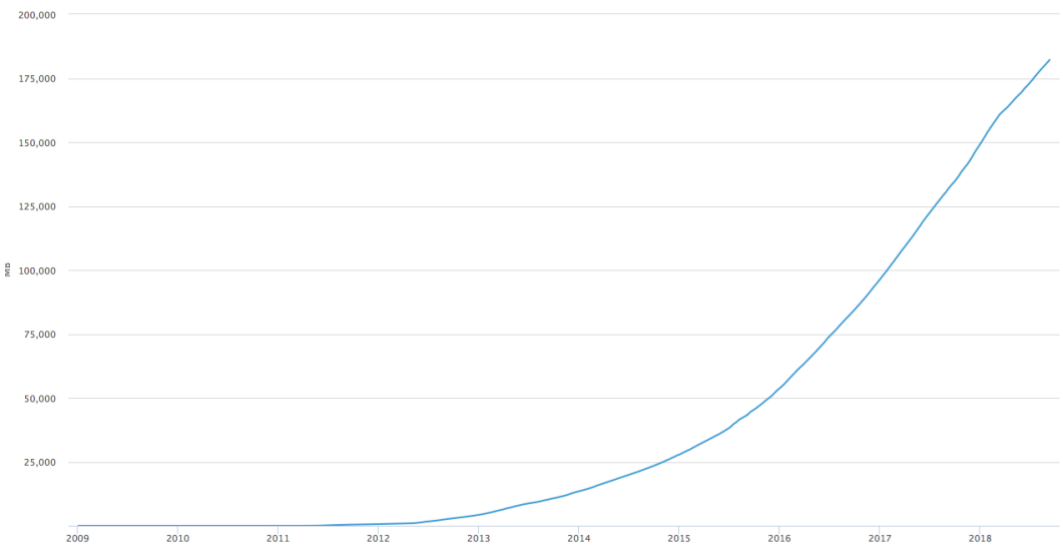
La Blockchain funziona come un'applicazione software che utilizza internet come modalità di connessione tra una rete distribuita di nodi (Peer-to-Peer network). Questo protocollo è progettato specificamente per il trasferimento di valore e proprietà, con il fine di rendere possibili transazioni economiche sicure, trasparenti ed immutabili. La caratteristica distintiva di questa tecnologia sta nel fatto che la stessa concatena le transazioni, crittograficamente verificate, in sequenze di liste (o "blocchi"). I sostenitori della tecnologia Blockchain affermano che il suo sviluppo è equiparabile, a livello di importanza, all'introduzione della contabilità a doppia entrata, il metodo rivoluzionario di contabilizzare attività e passività emerso nell'Italia rinascimentale e che, secondo alcuni storici, pose le basi del capitalismo, permettendo agli investitori e agli imprenditori di collaborare in società e di organizzare spedizioni mercantili oltre l'orizzonte conosciuto alla ricerca di successo commerciale. In questa analogia, la Blockchain è una sorta di contabilità a tre entrate, la terza delle quali è una ricevuta crittografica (verificabile) che quest'ultima fornisce nel momento in cui si realizza una transazione.

Ogni computer facente parte del network è connesso al sistema tramite internet ed identificato da uno specifico ed univoco indirizzo con la possibilità di connettersi e disconnettersi al network stesso in qualsiasi momento. Inoltre ogni computer mantiene

una lista degli altri con i quali comunica attraverso l'uso di messaggi. Tali messaggi sono inviati tramite uno stile definito "gossip" che fa in modo che ogni computer quando riceve un messaggio lo condivida con tutti gli altri con i quali è in contatto fino a quando questo raggiunge tutti i partecipanti (bisogna ricordarsi che i nodi non sono connessi direttamente con tutti gli altri bensì indirettamente). Nel momento in cui un partecipante si disconnette, "esce momentaneamente" dalla rete ma, alla riconnessione riceverà tutti i blocchi contenenti i dati delle transazioni che si sono verificate nel frattempo.
Qualsiasi computer può entrare a fare parte del network semplicemente inviando una richiesta ai nodi dello stesso. Questi ultimi aggiungeranno l'indirizzo del richiedente alla loro lista e invieranno una conferma al nuovo partecipante. Attraverso questo sistema si può sviluppare un'espansione pressoché illimitata della rete in quanto per entrare nella stessa non sono presenti barriere all'entrata.

Ma come viene documentata la proprietà all'interno del sistema?

La Blockchain in primo luogo descrive il trasferimento di proprietà e in secondo mantiene traccia dello stesso in una maniera tale che non sia più modificabile una volta registrato. Le informazioni utilizzate per descrivere una transazione sono: dati identificativi dell'account del trasferente e del ricevente, l'ammontare del bene trasferito, data e ora in cui sono avvenute le transazioni, una piccola tassa da pagare al sistema per l'esecuzione della transazione stessa e una prova che il proprietario della somma o del bene approvi il trasferimento. Dal momento che la transazione contiene tutte le informazioni riguardanti l'account che cede la proprietà, quello che la riceve e l'oggetto in questione, chiunque, tramite il registro, può ricostruire le informazioni dello scambio. La Blockchain infatti mantiene l'intera storia di tutte le transazioni che sono avvenute dalla sua introduzione ad oggi secondo l'ordine temporale in cui si sono verificate; ogni transazione che non fa parte di queste è come se non fosse mai esistita. Come mostra il grafico sottostante (*Figura 7*) le dimensioni dell'intera catena sono aumentate dalla sua introduzione ad oggi, infatti al giorno 30 settembre 2018 la Blockchain del sistema Bitcoin presenta una dimensione di più di 184.000 megabyte (ossia 184 GB).



[27]

Figura 7: Grafico tratto da "Blockchain.com".

Il meccanismo è costituito da blocchi, incatenati insieme tramite un codice a 64 caratteri assegnato ad ognuno di essi, i quali contengono un insieme di molteplici transazioni individuali. Inoltre è utilizzato anche un sistema di chiavi crittografiche pubbliche e private per fornire riservatezza e per stabilire "l'autorità". Tutti i dati sono crittografati sia con una chiave pubblica che con una privata, quindi, per sbloccare i dati o una transazione, devono essere presenti entrambe le chiavi: una cripta, l'altra decripta il messaggio cifrato e viceversa[28].

In altre parole, la brillantezza della tecnologia Blockchain sta nella sua struttura di singolo record di tutte le transazioni che non presenta duplicazioni o discrepanze tra i record. Prima che qualsiasi transazione possa essere registrata nel libro mastro, la rete di nodi deve raggiungere un consenso, da quel momento in poi ogni transazione registrata è visibile a tutti ma non più modificabile.

La proprietà e la verifica delle transazioni vengono realizzate tramite il "Mining" (perlomeno ciò accade nel sistema Blockchain introdotto da Bitcoin e nella maggior parte delle criptovalute, poi vedremo che in alcuni altri network ci possono essere strumenti di validazione differenti). Con questo termine si intende un sistema per l'elaborazione dei dati

[27] La maggior parte dei grafici riportanti dati riferiti alla Blockchain del Sistema Bitcoin vengono estratti dal sito "Blockchain.com" (http://www.blockchain.com) in quanto quest'ultimo è il sito maggiormente preciso e autorevole disponibile ad oggi.

[28] "Business Education Innovation Journal Volume 8 Number 2", December 2016.

crittografici che garantisce l'integrità del sistema. L'attività di estrazione (mining appunto) controlla continuamente le transazioni precedenti, assicurandosi che la sequenza cronologica dei blocchi sia corretta e impedendo la modifica di blocchi che contengono transazioni già validate in passato. Se un blocco viene modificato, tutte le transazioni successive che coinvolgono quel blocco diventano invalide. Questa attività impedisce anche che nuovi blocchi non validi siano aggiunti alla Blockchain, infatti per poter fare ciò sarebbero richieste notevoli risorse di calcolo[29] a ciascun nodo della rete in quanto quest'ultimo dovrebbe essere in grado di modificare la transazione desiderata e tutte quelle successive ad una velocità superiore a quella con cui la rete le valida (che è di circa 10 minuti per blocco) e ciò diventa tanto più difficile quanto più passa il tempo, in quanto vengono aggiunti sempre nuovi blocchi alla catena principale. Inizialmente, per lo meno fino al 2012, i tempi di convalida si attestavano in circa un minuto. In seguito, dato l'aumento del numero delle transazioni e della popolarità del network, questa tempistica è diventata di circa 10 minuti.

Quando si utilizza la tecnologia Blockchain in un'operazione finanziaria, non ci sono terze parti, in quanto il valore "scorre" da colui che inizia l'operazione alla parte ricevente. Il mediatore finanziario è sostituito dal sistema tecnologico Blockchain, con il potenziale per ridurre le frodi e il furto d'identità. Ciò ha implicazioni significative sia per i servizi finanziari che per le compagnie di assicurazione in quanto elimina le operazioni manuali nelle transazioni finanziarie, rendendo la movimentazione del denaro più veloce ed in tempo reale. Il mining effettua controlli continui più volte al giorno, evitando quindi la necessità di verifiche periodiche poiché i dati sono visibili pressoché a tutti (o perlomeno così accade nelle reti pubbliche).
Le Blockchains dipendono da server distribuiti che ospitano una replica di tutti i dati contenuti in una di esse; quindi, la sincronizzazione dei dati è essenziale per assicurare che il set completo di dati venga visualizzato in tutti i server.

[29] Le interfacce di programmazione delle applicazioni Blockchain (API) sono comunemente utilizzate per il mining attraverso una varietà di linguaggi informatici come C ++, Java, .NET (C #), Python, Ruby, PHP, Node, Javascript, Assembly e altri.

La Blockchain utilizza principalmente 2 tecnologie di base per garantire il proprio corretto funzionamento:

- Algoritmi Hash (detti anche funzioni)
- Crittografia Asimmetrica

1.4.1) Hash function (algorithm)

Nei sistemi distribuiti Peer-to-Peer ci si trova di fronte ad un numero molto elevato di transazioni, è dunque necessario riuscire ad identificarle in maniera univoca il più velocemente e precisamente possibile. Un algoritmo hash o hash è una funzione (o struttura di dati) che prende un input di lunghezza arbitraria e lo converte in una stringa di lunghezza predefinita corrispondente[30].

Le principali caratteristiche di queste funzioni sono quelle di fornire un unico valore hash per qualsiasi tipologia di dato, il fatto di essere deterministiche (ossia di generare lo stesso valore hash solo per un medesimo input di dati), casuali (non è possibile prevedere il valore dell'hash basandosi sui dati di input), di possedere unicità direzionale (ossia la funzione non prevede la possibilità di risalire dagli output agli input che l'hanno originata) e resistenza (molto difficilmente si possono trovare stringhe di dati diversi che forniscono lo stesso hash value[31]).

Quando un messaggio viene generato, la funzione utilizza la crittografia per trasformarlo, a prescindere dalla sua dimensione, in un codice di un numero predefinito di caratteri (questo processo è conosciuto come Secure Hash Algorithm) che cambia a seconda del tipo di algoritmo considerato.

Gli algoritmi hash non sono stati introdotti dal sistema Bitcoin bensì hanno una lunga storia di utilizzo nell'ambito delle firme digitali[32] e nell'e-commerce. L'analisi matematica di questi algoritmi era (e spesso è ancora) basata sulla perfetta casualità. Supponiamo che

[30] Wouter Penard, Tim Van Werkhoven, "On the Secure Hash Algorithm family", 2002.

[31] Per fare questo sarebbe necessario creare 2^{80} valori hash. Ipotizzando un computer con una potenza di calcolo di 1 terahash (10^{12} indirizzi hash al secondo), potenza che è decisamente superiore ai calcolatori in commercio oggi, si impiegherebbero $1{,}48*10^{20}$ secondi, ovvero 38.309 anni.

[32] Una "Digital Signature" è uno schema matematico per dimostrare l'autenticità di un messaggio/documento. "D. LEE Kuo Chuen, R. H. DENG, Handbook of blockchain, digital finance and inclusion – volume 2", Elsevier, 2018.

per ogni input z il valore hash h(z) sia uniformemente distribuito su tutti i valori che potrebbe assumere e che ogni h(z) sia indipendente da tutti gli altri h(y) per y ≠ z. Tali funzioni di hash perfette rendono molto più semplice questa analisi, in quanto ogni nuovo valore hash sembra completamente casuale. Queste funzioni crittografiche hanno diverse proprietà aggiuntive che le rendono idonee ad essere utilizzate come strumento di controllo per verificare l'integrità di un messaggio e come parte di uno schema di firma digitale. Tale schema consiste in una chiave segreta Ks, una chiave pubblica Kp e due funzioni Sign(M, Ks) che producono una firma S e verificano se quest'ultima è una firma valida per il messaggio M. Il requisito della funzione è che Sign(M, Sign(M,Ks), Kp) sia vera per un paio di chiavi (Ks e Kp). Per inserire tale firma può essere utilizzato un sistema crittografico come l'RSA[33] in cui la chiave segreta (Ks) viene utilizzata per firmare il messaggio e la chiave pubblica (Kp) per verificare la firma stessa (e decriptare il messaggio). L'Algoritmo Secure Hash (SHA) è stato sviluppato dal NIST (National Institute of Standards and Technology, USA) in associazione con l'NSA (National Security Agency) e pubblicato per la prima volta nel maggio 1993 come "Secure Hash Standard". La prima revisione di questo algoritmo è stata pubblicata nel 1995 a causa di un difetto inedito riscontrato nella precedente, ed indicata con la sigla SHA-1. La prima versione chiamata SHA-0, è stata perciò ritirata dall'NSA stessa. La funzione hash SHA è simile alla funzione hash di MD4[34], ma aggiunge una certa complessità all'algoritmo e ne modifica la dimensione del blocco utilizzata. Il SHA era originariamente inteso come parte del Digital Signature Standard (DSS), un sistema utilizzato per firmare i dati che necessitava di questo tipo di funzione per realizzare il suo compito.

Oltre all'hash SHA-1, il NIST ha anche pubblicato un insieme di funzioni hash più complesse per le quali l'output varia da 224 a 512 bit. Questi algoritmi di hash, denominati SHA-224, SHA-256, SHA-384 e SHA-512 (a volte raggruppati sotto la sigla: SHA-2) sono più complessi a causa delle funzioni non lineari aggiunte alla funzione di compressione. Il SHA-256[35] utilizza un blocco della dimensione di 512 bit e restituisce 64 caratteri, mentre SHA-512 ha una dimensione di 1024 bit e dispone di 80 caratteri.

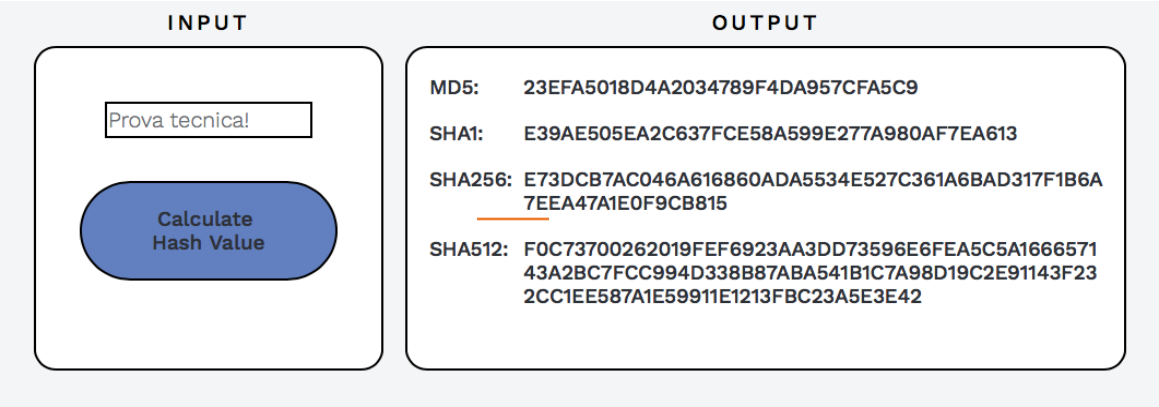
[33] R. L. Rivest, A. Shamir, L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems", 1978.

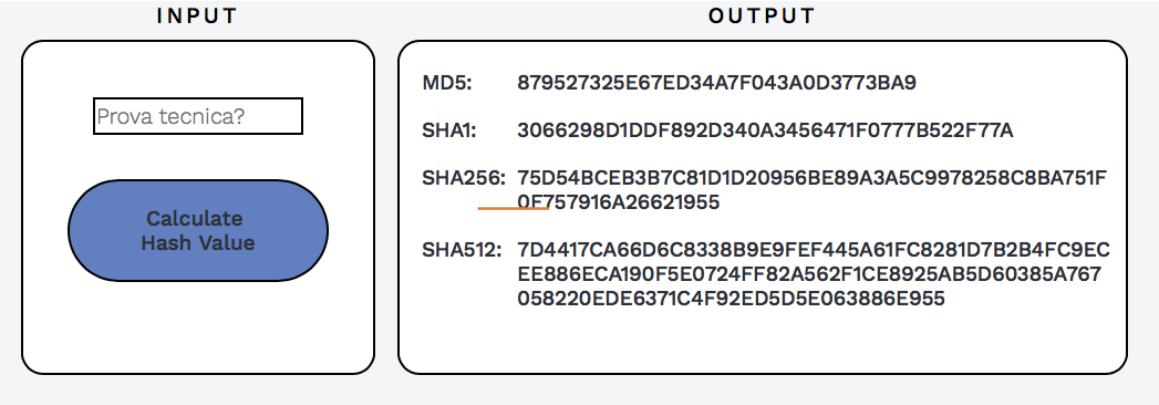
[34] L'MD4 è una funzione crittografica di hashing scritta da Ronald Rivest del MIT nel 1990 (fonte: http://people.csail.mit.edu/rivest/).

[35] Questa versione dell'algoritmo è quella utilizzata dal protocollo Bitcoin.

È inoltre possibile combinare differenti insiemi di dati o di hash per ottenere un hash unico e ottimizzare quindi la memorizzazione e il trasferimento degli stessi tenendo solo il valore di output fornito dall'hash senza dover mantenere i singoli dati; in questo modo invece di comparare i dati confrontandoli esplicitamente in tutto il loro contenuto, si è in grado di confrontare direttamente il loro hash crittografico. Se la stringa differisce allora i dati sottostanti saranno differenti, se invece corrisponde i dati saranno i medesimi. La sensibilità di questi algoritmi nella creazione dell'output, in risposta alla variazione dei dati sottostanti, è molto elevata, infatti come possiamo vedere dal seguente esempio, cambiando anche solo la punteggiatura in una breve frase il valore crittografico della stringa corrispondente alla stessa sarà completamente diverso.

Tramite l'utilizzo del seguente simulatore http://www.blockchain-basics.com/HashFunctions.html è possibile verificare che immettendo un messaggio qualsiasi ad esempio "Prova tecnica", semplicemente cambiando "!" con "?" si ottiene una stringa totalmente differente:

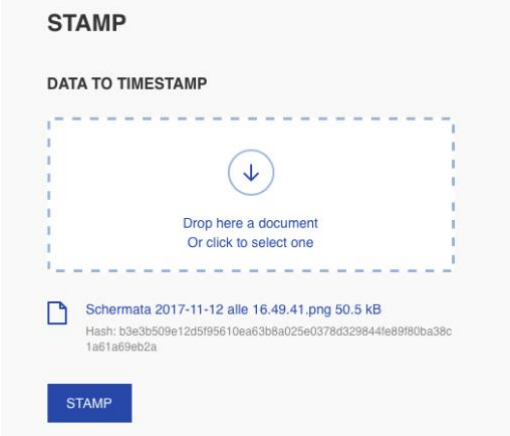




Ritornando per un momento al problema del "Double Spending", come abbiamo visto, c'è bisogno, per il beneficiario, di un modo per sapere che il precedente proprietario non abbia firmato nessun'altra transazione precedente a quella che sta realizzando con la controparte in questione. Per questo la prima transazione realizzatasi è quella che conta e che viene registrata dal sistema grazie ad un strumento chiamato "Peer-to-Peer Distributed Timestamp Server[36]", il quale genera una prova inconfutabile dell'ordine cronologico con il quale sono avvenute le transazioni e le certifica come veritiere. Ogni timestamp include il precedente timestamp nel suo hash, formando una catena, con ogni timestamp addizionale che rinforza quelli precedenti[37].

Il processo di timestamping si sostanzia in 2 fasi: la prima in cui è certificato il momento (data/ora) in cui viene compiuta l'operazione e una seconda che permette di verificare se l'output fornito è corretto.

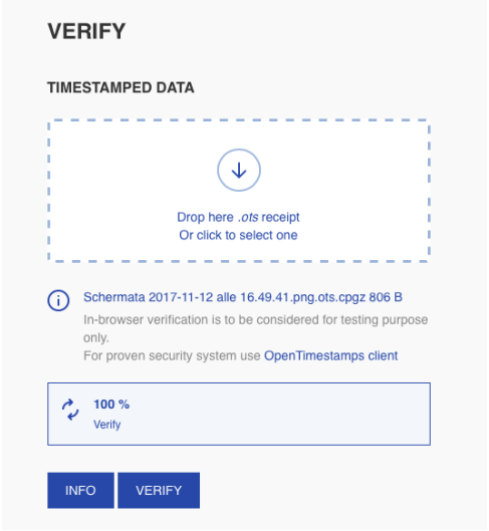
Vediamone un esempio; inseriamo un file all'interno della piattaforma "opentimestamps.com": una volta selezionata la funzione "STAMP" ci verrà restituita come output una ricevuta in formato "zip." Quest'ultima certificherà l'orario di esecuzione dell'operazione.

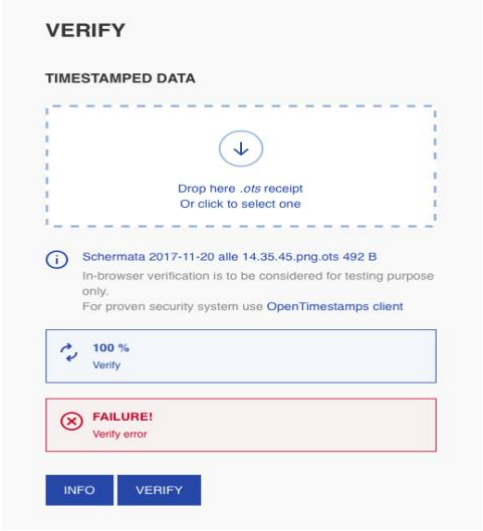


[36] Sequenza di informazioni cifrate che identificano quando un evento è accaduto, solitamente fornendo la data e l'ora del giorno. Il Trusted Timestamping è il processo utilizzato dai network Peer-to-Peer per mantenere traccia della creazione e della modifica di un determinato documento, in modo tale che nemmeno il creatore dello stesso sia abilitato a modificarlo una volta registrato. D. LEE Kuo Chuen, R. H. DENG, "Handbook of blockchain, digital finance and inclusion – volume 2", Elsevier, 2018.

[37] Il sistema Bitcoin utilizza un sistema simile a quello HashCash, introdotto come strumento antispam all'interno dei client e-mail e come contromisura ad attacchi di tipo DOS (Denial of Service). A. Back et Al., "HashCash, 2002".

In un secondo momento vi è la possibilità, anche da parte di terzi, inserendo la "ricevuta" precedentemente ottenuta in un secondo box, di verificare se la stessa è corretta e se dunque la transazione è avvenuta in quel determinato momento. Se si sostituisse la ricevuta con quella ottenuta tramite l'inserimento di un altro file, al momento della verifica si riscontrerebbe un errore e si potrebbe individuare la discordanza tra le operazioni (come si può vedere dalle schermate sottostanti):





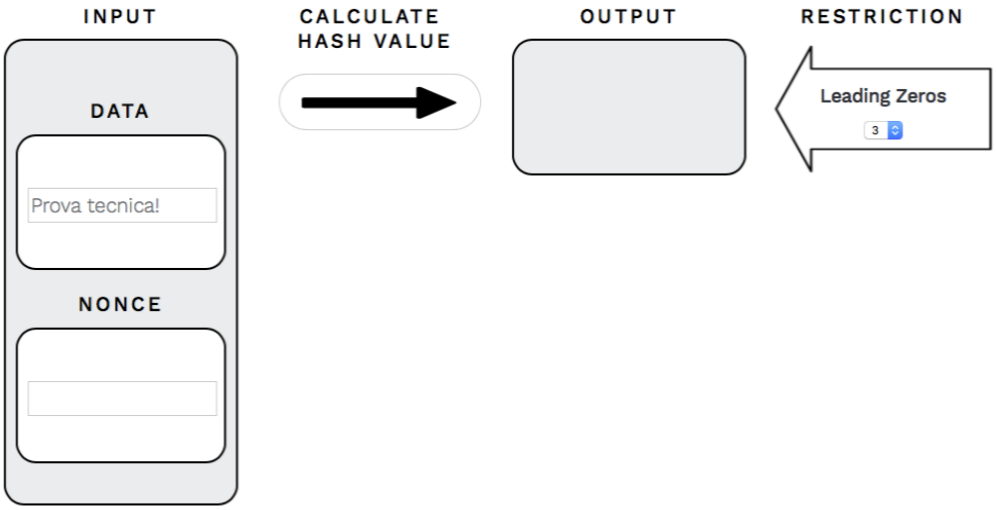
Infine, per certificare le transazioni contenute nei singoli blocchi, i miners dovranno risolvere una sorta di puzzle matematico. Questo puzzle può essere risolto solamente attraverso un metodo iterativo (il cosiddetto metodo "sbaglia e prova") in quanto richiede di individuare un numero (chiamato NONCE[38]) il quale, combinato con i dati considerati, fornisca, una volta calcolatone l'hash, una stringa con determinate caratteristiche. Questo comporta la ricerca di un valore che quando viene individuato faccia iniziare la stringa dell'hash con un certo numero di zeri.

Anche in questo caso cerchiamo di capire al meglio il funzionamento dell'operazione tramite una simulazione, semplificata, della stessa: ricordando il messaggio utilizzato nell'esempio esplicitato in precedenza[39], dobbiamo individuare un numero (il Nonce

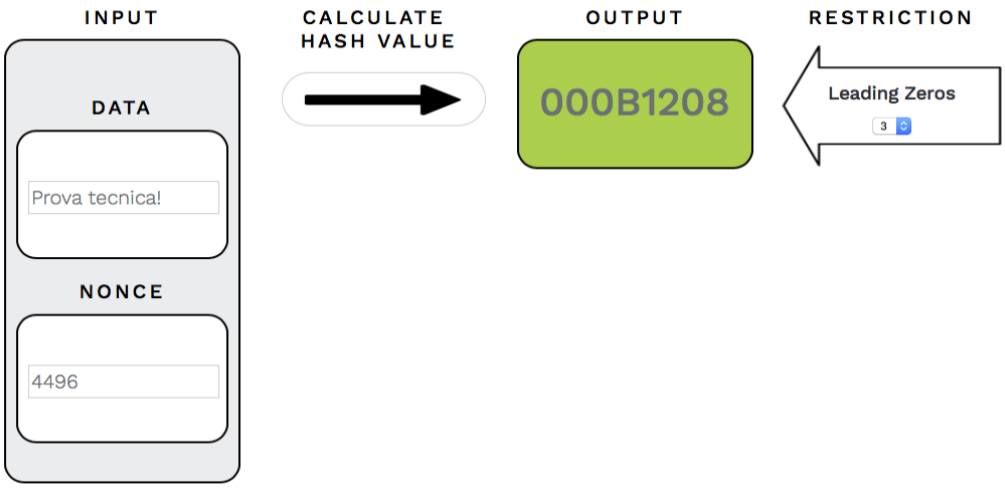
[38] In crittografia il termine Nonce indica un numero, generalmente casuale, il quale possiede un utilizzo unico. Il termine infatti deriva dalla espressione inglese "number used once", che significa appunto numero usato una sola volta.

[39] Per l'esecuzione della simulazione si è utilizzata la medesima piattaforma dell'esempio iniziale: http://www.blockchain-basics.com/HashFunctions.html.

appunto) che combinato con l'hash del messaggio "Prova tecnica!" consenta di ottenere come output una funzione hash che inizi con tre zeri ("Leading zeros").



Dal successivo grafico si può vedere come il Nonce che risolve il puzzle sia il numero 4496. (la funzione output è un hash esemplificativo e a tale scopo non è presentato nella sua interezza di 64 caratteri per il protocollo SHA-256 ma solo nella prima parte al solo fine di mostrare al lettore che quest'ultima debba iniziare con 3 zeri):



Una volta ottenuta la soluzione del puzzle, il blocco non può essere modificato senza ripetere tutto il lavoro computazionale eseguito sullo stesso.

La difficoltà del problema da risolvere è impostata in base al numero di partecipanti alla risoluzione dello stesso e si riflette nel numero iniziale di zeri che la funzione hash deve avere, dunque, in ordine di difficoltà crescente, un puzzle di difficoltà 1 implica che l'output dell'hash che si vuole ottenere debba avere almeno uno zero iniziale e una di 10 che la funzione identificativa abbia 10 zeri iniziali. In sostanza maggiore sarà il numero di zeri iniziali maggiore sarà la difficoltà di risoluzione e maggiore la potenza di calcolo computazionale richiesta dal problema stesso; di conseguenza la maggior difficoltà influenza il numero di tentativi necessari per individuare il Nonce risolutivo.
Se una soluzione è ottenuta in maniera troppo rapida, la difficoltà di risoluzione dei successivi blocchi aumenterà e viceversa. Normalmente questa ultima viene ripristinata ogni 2016 blocchi creati (ciò avviene ogni 14 giorni circa) per un ammontare che assicuri che il tempo di risoluzione del puzzle crittografico si mantenga approssimativamente nell'ordine di 10 minuti.
Una volta che un nodo del sistema riesce a risolvere il puzzle la soluzione sarà immediatamente disponibile anche per gli altri partecipanti, che la potranno verificare. Questo Hash puzzle è definito anche "Proof of Work" in quanto la soluzione dello stesso prova che qualcuno ha compiuto il lavoro (inteso come tempo e potenza di calcolo utilizzata) necessario per risolverlo e per garantire la veridicità delle operazioni all'interno di quel blocco. Ciò assicura che nessuno possa bypassare il costo computazionale riducendo arbitrariamente la difficoltà.

1.4.2) Crittografia asimmetrica

La seconda tecnologia utilizzata dalla Blockchain è quella conosciuta come crittografia asimmetrica che svolge la funzione di identificare gli utilizzatori all'interno del network e proteggere le loro proprietà impedendo a persone non autorizzate di accedervi. L'idea di base è quella di trattare gli account personali dei partecipanti al sistema (i cosiddetti portafogli o "Wallet") come un mailbox[40] in cui tutti possono trasferire proprietà, ma solo il proprietario della stessa può accedervi tramite l'utilizzo di una "chiave". L'account personale, considerando l'esempio del network Bitcoin, si sostanzia in una stringa

[40] Nel caso della criptovaluta Bitcoin un indirizzo Bitcoin è equivalente ad un indirizzo fisico o ad uno e-mail. È la sola informazione da fornire a qualcuno affinché possa pagarti con Bitcoin. "bitcoin.org".

alfanumerica (simile a quelle utilizzate per identificare un conto corrente) formata da un numero di caratteri compreso tra 27 e 34 che inizia con un 1 o un 3, la quale rappresenta una destinazione sulla rete Bitcoin[41].

A differenza delle banconote, i bitcoin non devono essere posseduti in unità intere (ad esempio, 5, 10, 50) e, a meno che una quantità di bitcoin facente riferimento ad un dato indirizzo non sia esattamente spesa in una transazione, la parte decimale restante della stessa (il cosiddetto "resto") viene restituita ad un nuovo indirizzo, che forma un nuovo "pacchetto" di criptovaluta.

Tutti gli indirizzi, rappresentanti ciascuno una certa quantità di bitcoin posseduta da un utente, saranno memorizzati nel suo wallet. Così, come in un portafoglio di denaro convenzionale, il saldo di portafoglio Bitcoin è la somma dei saldi di tutti gli indirizzi all'interno del portafoglio. Sebbene i singoli indirizzi siano progettati per agire in maniera indipendente ed anonima, è possibile collegare indirizzi appartenenti allo stesso portafoglio quando si utilizza più di uno di questi per effettuare una singola transazione. Ogni volta che viene creato un nuovo wallet, abbinate allo stesso vengono generate 100 chiavi pubbliche, le quali fanno riferimento ad un'unica chiave privata. In questo modo ogni utente è in grado di utilizzare 100 indirizzi diversi collegati al medesimo portafoglio e gestibili possedendo una sola chiave privata. Questo meccanismo punta a favorire l'anonimato delle operazioni, in quanto un utente potrebbe utilizzare in maniera intercambiabile i suoi indirizzi rendendo maggiormente complicata l'associazione degli stessi al medesimo wallet e quindi ad un unico proprietario (vedremo però in seguito, nel secondo capitolo, che in realtà ci sono alcuni modi per rendere "meno anonimo" il sistema e ricondurre ad uno stesso utilizzatore più indirizzi o addirittura di conoscere l'identità dello stesso).

Quando si parla di crittografia asimmetrica l'equivalente digitale di "chiudere una porta" è definito criptazione e quello di "aprirla" decriptazione, ciò però può essere compiuto solo se si è in possesso di una chiave digitale univoca per quel determinato oggetto. Il processo inizia con la criptazione del testo o dei dati tramite una chiave crittografica univoca, successivamente questo testo criptato viene inviato ad un altro partecipante al network, il

[41] Un tipico indirizzo assomiglia a questo: "13uRbMgunUpShBVTewXjtQTBv5MndwfXhb".

quale, se in possesso della chiave corrispondente sarà in grado di decriptarlo ottenendo il messaggio originale.
La differenza tra la crittografia simmetrica e quella asimmetrica è che la prima utilizza una sola chiave crittografica mentre quella asimmetrica, utilizza 2 tipi di chiavi: una pubblica ("public key") e una privata ("private key"), delle quali una è utilizzata per criptare e l'altra per compiere il processo inverso: il punto più interessante sta nel fatto che non si potrà mai decriptare un messaggio con la chiave che è stata usata per generarlo e viceversa.

A tal proposito, ci sono 2 maniere distinte di utilizzare tali chiavi:

- Public to private: la chiave pubblica cripta, quella privata decripta. Chiunque può creare un testo criptato ma solo il proprietario della chiave privata potrà decriptarlo.
- Private to public: il processo è inverso rispetto al precedente, solo il proprietario della chiave privata può criptare i messaggi che però possono essere letti da tutti coloro i quali siano in possesso della chiave pubblica.

La Blockchain utilizza il primo dei due approcci per identificare i proprietari degli account e trasferire la proprietà tra gli stessi, mentre utilizza il secondo per autorizzare le transazioni; il proprietario che trasferisce crea del testo cifrato con la sua chiave privata, tutti gli altri nodi possono verificare che lo stesso abbia approvato il trasferimento utilizzando la chiave pubblica di quel soggetto. Questa procedura è detta "Digital Signature[42]" ed è l'equivalente, trasposto digitalmente, della firma tradizionale: il messaggio criptato infatti rappresenta la propria firma digitale.
In un primo momento, chi riceve il messaggio criptato, può calcolare autonomamente il valore dell'hash corrispondente allo stesso, successivamente con la chiave pubblica del soggetto inviante decripta il messaggio; se i due valori hash ottenuti sono uguali, il ricevitore può concludere in primis che il messaggio è stato firmato dal corretto inviante perché ha potuto decriptarlo con la corrispondente chiave pubblica ed inoltre che il messaggio è quello corretto in quanto il testo decriptato è uguale al valore dell'hash che ha ottenuto egli stesso tramite la verifica iniziale.

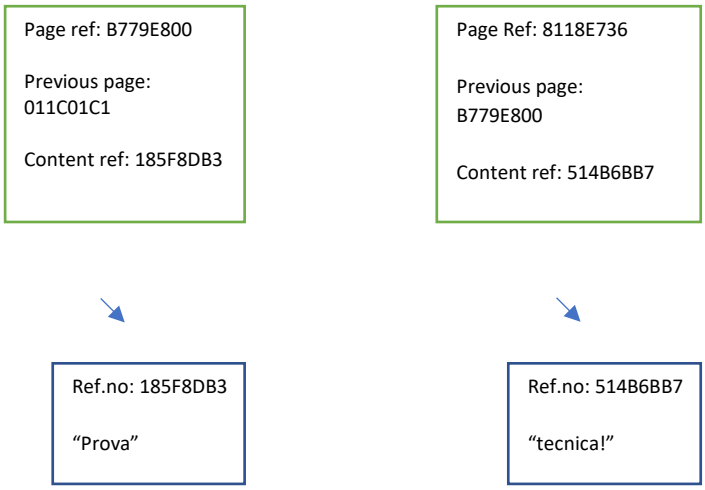
[42] Il sistema Bitcoin utilizza come strumento per la firma digitale l'algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm). Fonte: "nvlpubs.nist.gov".

Ma come vengono conservate tutte le transazioni per mantenerne traccia?

La sfida con cui ha dovuto confrontarsi la tecnologia Blockchain è stata quella di conservare tutte le transazioni in modo tale da mantenerne l'ordine di esecuzione e da poter individuare facilmente eventuali modifiche avvenute a posteriori[43]. A tale scopo la stessa crea una sorta di catalogo (o catena di blocchi) al quale interno sono inserite le varie referenze alle singole transazioni, contenute in pagine numerate; i numeri di queste ultime garantiscono la possibilità di individuare immediatamente eventuali rimozioni di pagine o dati semplicemente verificando che l'ordine delle stesse sia mantenuto correttamente, generando dipendenza tra ogni pagina e la sua precedente. Ognuna infatti contiene al suo interno un numero di riferimento identificativo della precedente, facendo così in modo che nelle pagine non siano contenute tutte le informazioni e i dati esplicitamente, bensì vengano registrati solo i rispettivi codici di riferimento. Per questo il sistema viene detto catalogo perché appunto contiene solo le referenze a dati ed informazioni che sono conservati separatamente, allo scopo di permettere di ritrovare le stesse in maniera agevole e con il minor peso, in termini di byte, possibile (si pensi ad una sorta di elenco di differenti "link" che rinviano, per la consultazione delle informazioni, ad un altro documento).

Vediamone un esempio. Il catalogo in ogni sua pagina contiene tre codici, uno che identifica la stessa, uno di riferimento per la pagina precedente (con la quale è concatenata) ed infine un ultimo che corrispondente al contenuto in termini di dati ed informazioni per la pagina considerata:

[43] Queste ultime sono mantenute indicando data ed ora di esecuzione, importo e controparti coinvolte (anche se la loro vera identità viene mantenuta segreta, infatti sono riportati solo gli indirizzi Bitcoin coinvolti e non le controparti reali). Ciò assomiglia, in un certo senso, a quello che accade nelle borse valori, in cui si maniene traccia del momento in cui è avvenuta e dell'importo della transazione pur senza indicare chi l'ha compiuta.



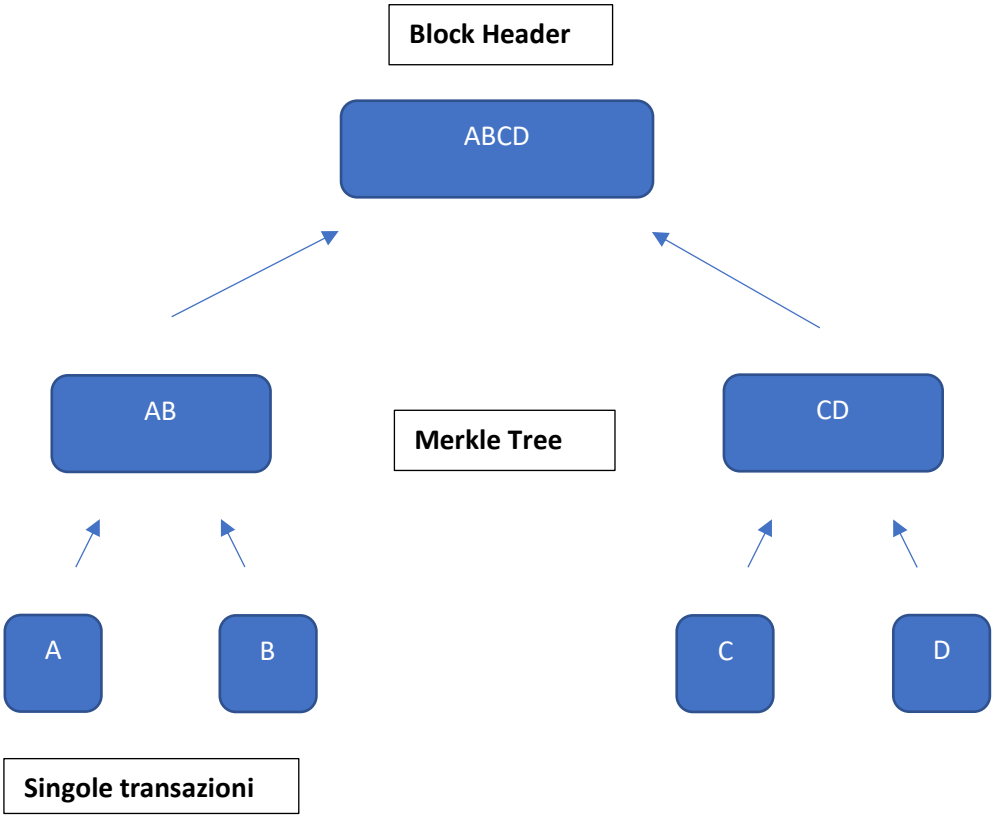
Il valore di riferimento delle pagine (che nell'esempio per la pagina di sinistra è B779E800) è calcolato in base al contenuto delle stesse e deriva dal valore hash della combinazione tra il codice della precedente pagina 011C01C1 e quello del contenuto di riferimento 185F8DB3.

Utilizzando gli hash come numeri di riferimento, chiunque potrebbe verificare la correttezza dei valori rappresentati semplicemente ricalcolando le rispettive funzioni.

Ogni pagina del catalogo si riferisce ad un singolo "Block Header" (ossia il codice di riferimento di un blocco, al contenuto del quale rimanda il famoso "link" nella pagina del catalogo che abbiamo citato in precedenza) della struttura di dati della Blockchain all'interno del quale sono contenute le informazioni e i dati cui il catalogo fa riferimento. Questo Block Header è un codice che fa riferimento ad un cosiddetto Merkle Tree[44], una struttura di dati che al suo interno contiene tutte le informazioni riguardanti le transazioni che sono compattate all'interno del blocco, senza il bisogno di memorizzare singolarmente tutti i singoli hash corrispondenti alle stesse. Per questo, schematizzando, un blocco della Blockchain consiste in un Block Header ed un Merkle Tree che contiene tutti i dati delle transazioni. Ogni header contiene una hash reference al block header e altre informazioni

[44] Questa struttura "ad albero" (Merkle Tree appunto) è utilizzata per permettere un risparmio, a livello di spazio su disco, nel memorizzare la catena totale di transazioni. Quando infatti una transazione risulta "sepolta" sotto un numero di blocchi successivi abbastanza elevato, quest'ultima non verrà riportata direttamente nella Blockchain, bensì verrà riportato solamente il cosiddetto Merkle Root ossia il valore hash finale che fa riferimento a tutti i valori hash sottostanti ad esso. Questo consente di verificare una singola transazione senza Dover scaricare l'intera Blockchain.

quali la versione del software, il timestamp, il livello di difficoltà e il Nonce. In maniera molto semplificata, un procedimento di Merkle Tree può essere così rappresentato:



Per validare le transazioni senza inviarle tutte a tutti i nodi si accorpano le stesse (come per A e B nell'esempio riportato sopra) attraverso un nicknumber (AB), alla fine per tutte le transazioni del blocco si otterrà il cosiddetto Merkle Root (ABCD) che sarà l'unico codice, incluso nel Block Header, che funge da contenitore per tutti i dati delle transazioni memorizzate nel Merkle Tree, il quale verrà trasmesso al blocco successivo contenendo al suo interno tutte le transazioni validate (ma che occuperà meno in termini di spazio).

Come ci si assicura che le transazioni aggiunte siano solo quelle valide?

A tale scopo bisogna che, sia i dati delle stesse, che i blocchi ed i rispettivi Block Header siano validi. Ciò comporta: regole di validazione per i dati e regole di validazione per i Block Header; le prime prescrivono quali informazioni sono necessarie per descrivere una transazione, le seconde impongono che solo i blocchi i quali Header contengono una corretta soluzione al proprio hash puzzle siano processati velocemente.

1.4.3) Processo di selezione dei blocchi

Come affermato in precedenza, le nuove transazioni potrebbero non arrivare tutte nello stesso momento a tutti i nodi, per questo c'è bisogno di un meccanismo che permetta agli stessi di lavorare solo sulla catena corretta e non su altre ambigue o errate. Questo sistema, definito "Distributed Consensus" o "Consensus Protocol[45]" permette a tutti i partecipanti al network di selezionare a maggioranza una versione di catena delle transazioni da proseguire. Questa scelta si basa su 2 criteri principali:

- Criterio della catena più lunga: si fonda sull'idea che la struttura di dati della Blockchain che comprende il maggior numero di blocchi sia quella che rappresenta il maggior sforzo computazionale.

Ma cosa accade se due catene hanno la stessa lunghezza? Alcuni nodi potrebbero continuare l'una ed altri l'altra, per questo si utilizza un secondo criterio:

- Criterio della catena più "pesante": nel momento in cui le due catene di blocchi fossero di uguale lunghezza, ci si baserebbe sull'idea che la catena che è stata costituita utilizzando la maggior difficoltà di calcolo in aggregato rappresenti il maggior sforzo computazionale e quindi sia da ritenersi quella corretta.

Questo secondo criterio in particolare mostra una delle assunzioni fondamentali del sistema, infatti fino a quando i nodi onesti mantengono la maggioranza della potenza computazione di tutto il sistema (51%), la catena mantenuta dagli stessi tenderà a crescere più velocemente rispetto a tutte le altre catene alternativamente proposte. Ogni nodo, considerato singolarmente, ha solo una piccola voce nel processo di selezione di una catena di transizioni ma la maggioranza della popolazione di nodi forma una entità più forte ed in grado di scegliere la propria storia. Tutto ciò ovviamente implica una fondamentale fiducia nell'organizzazione dei minatori (in particolar modo riguardo alla loro onestà) e nei sistemi digitali in quanto, come abbiamo anche visto nella parte iniziale di questo capitolo attraverso il Problema dei generali Bizantini, se un gruppo di miners disonesti riuscisse a

[45] Meccanismo tramite cui gli utenti all'interno di uno di questi network P2P concordano sulla validità dei dati contenuti nel libro mastro. "Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector" Enisa, Dicembre 2016.

prendere possesso del 51% della rete di validatori, non sarebbero più i partecipanti onesti a decidere arbitrariamente la veridicità o meno delle transazioni processate, bensì quelli disonesti.

Prove empiriche dimostrano che i miners si comportano in modo strategico e formano organizzazioni: i cosiddetti "Pool". Questi ultimi agiscono come un'unica entità con un coordinatore centralizzato, seguendo determinati piani.

La forza di un pool è la somma della potenza computazionale dei suoi membri. Tutti i membri di un pool infatti cooperano per creare i blocchi e condividono in maniera proporzionale le rispettive ricompense (quantità di bitcoin prestabilite) quando uno di loro ne crea con successo uno nuovo. Sebbene entrare in un pool non cambi le aspettative di guadagno attese di un minatore, diminuisce la varianza delle operazioni e rende le entrate medie più prevedibili.

Ad oggi i principali pool di miners per dimensioni possono essere così rappresentati:

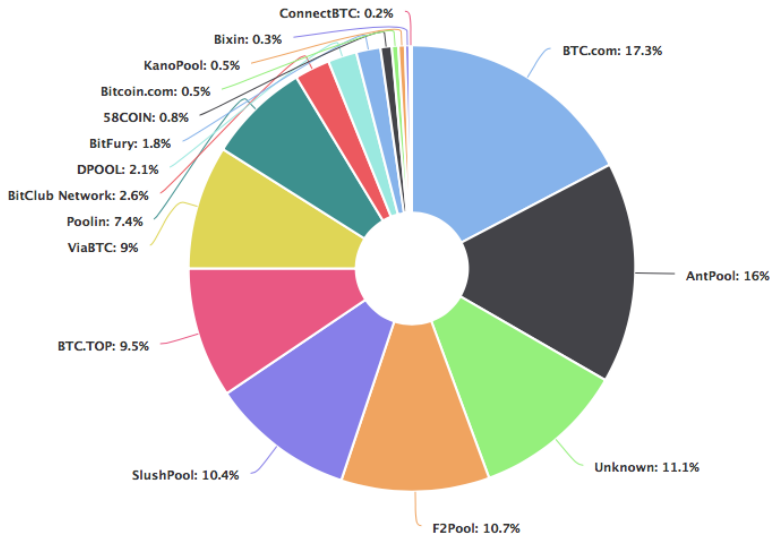


Figura 8: Il grafico qui sopra mostra la percentuale di mercato dei gruppi di minatori più popolari.
Fonte: "Blockchain.com". Dati aggiornati al 1 ottobre 2018.

Come si può notare dal diagramma (*Figura 8*), tre pool di miners (ad esempio BTC.com, Antpool, Slushpool) potrebbero, agendo congiuntamente, controllare il 43,7% della rete e se a questi ultimi se ne aggiungesse un altro, che controllasse poco più del 6% (come ad esempio Poolin), la somma degli stessi sarebbe in grado di controllare la maggioranza della

potenza computazionale di tutto il network. Questo fattore, considerato uno dei più grandi pericoli del sistema Blockchain di Bitcoin presenta vari aspetti da considerare. In primis bisogna capire se effettivamente ad un gruppo di miners converrebbe comportarsi in maniera disonesta in quanto ciò causerebbe un crollo della fiducia nei confronti della rete stessa mettendo in fuga la parte onesta dei partecipanti e di conseguenza apportando danni anche agli stessi partecipanti disonesti.

Il funzionamento del procedimento di esecuzione delle operazioni del network fin qui esplicitato può perciò essere così schematizzato:

1) Un utente esegue una transazione ad un altro partecipante al network.
2) Le singole transazioni di nuova esecuzione vengono trasmesse a tutti i partecipanti del sistema.
3) Ogni Miner (o Pool che sia) accorpa le transazioni in un blocco e lavora alla ricerca di una soluzione del puzzle per il proprio blocco.
4) Quando un nodo trova la soluzione del puzzle la trasmette a tutti gli altri nodi (i quali accetteranno la soluzione solo se tutte le transazioni contenute nel blocco stesso sono valide e non ci sono esempi di Double Spending).
5) I nodi esprimono la loro accettazione per il blocco considerato lavorando alla creazione del blocco successivo della catena il quale utilizzerà l'hash del blocco accettato come "previous hash".
6) I blocchi così creati andranno a formare la catena (Blockchain) e saranno di pubblico dominio per tutti i partecipanti.

1.4.4) Sistema di ricompensa/punizione

Creare blocchi validi consuma energia, tempo e denaro per la risoluzione del puzzle computazionale che risulta fondamentale per il corretto svolgimento delle operazioni, per questo è necessario convincere i partecipanti a farsi carico della risoluzione dello stesso motivandoli adeguatamente con delle ricompense e al contrario c'è bisogno di una maniera per punire i nodi che cercano di compromettere l'integrità dell'intero sistema contraffacendo transazioni.

Di per sé sarebbe già un'adeguata punizione il mancato riconoscimento della ricompensa dopo che il nodo ha sostenuto il costo computazionale (o l'eventuale revoca della stessa se fosse stata conferita ma in un secondo momento si venisse a scoprire che il blocco era errato, duplicato o troppo vecchio) però "le armi" più importanti su cui viene fatto affidamento contro i nodi disonesti sono la maggioranza dei nodi onesti e gli effetti delle ricompense.

Il miglior modo, in termini di efficienza ed efficacia per risolvere la competizione è quello di stabilire criteri di ricompensa ben definiti, per questo l'algoritmo alla base della tecnologia Blockchain mantiene una competizione continua che si fonda su 2 differenti "sfide": una basata sulla velocità e una sulla qualità, solo i nodi che vincono entrambe le competizioni ricevono la ricompensa. Chi perde la gara sulla velocità diventa riferimento in quella per la qualità e valida il blocco che il vincitore della competizione sulla velocità ha inviato (ciò consente una attenta verifica dei blocchi validati). Per vincere la gara sulla velocità bisogna risolvere per primi il puzzle, ma non c'è un modo per risolvere lo stesso in anticipo rispetto agli altri perché ciò dipende dal contenuto del blocco stesso. La competizione basata sulla qualità invece si focalizza sulla correttezza del blocco: una volta che un nodo invia un blocco del quale presume di aver risolto il puzzle, questo è trasmesso a tutti gli altri partecipanti i quali agiscono da arbitri verificando se lo stesso rispetta le regole di validazione delle transazioni e del Block Header. Quando i nodi ricevono il blocco da verificare capiscono di aver perso la competizione sulla velocità; al contempo però hanno la possibilità, verificando l'operazione eseguita dal vincitore nel minor tempo possibile, di partecipare alla successiva competizione per la certificazione del nuovo blocco. Tutto ciò porta il processo ad elevati livelli di velocità e competitività, con un ritmo che viene imposto dalla rapidità con cui vengono completate le due competizioni.

Il nodo che ha vinto la competizione riceve, oltre ad una ricompensa in bitcoin, una piccola ricompensa sotto forma di tassa (fee[46]) in proporzione alle transazioni che sono all'interno del blocco che ha validato.

Inizialmente, la ricompensa per il mining all'interno del sistema Bitcoin era stabilita in 50 bitcoin (a cui andavano aggiunte le piccole "fee" per ogni transazione), questo ammontare

[46] L'importo di questa piccola "commissione" è libero e viene deciso dall'autore della stessa. Considerando però che secondo il protocollo con un'unica operazione di convalida si possono registrare fino ad un massimo di circa 4.200 transazioni, questa commissione fornisce in sostanza un incentivo ai miners per accelerare la registrazione delle operazioni che prevedono una ricompensa maggiore. Essi infatti possono selezionare quali operazioni registrare prima di altre e naturalmente opteranno per quelle aventi una fee maggiore.

però è stato programmato per essere dimezzato nel tempo seguendo una progressione geometrica che prevede un dimezzamento del premio ogni 4 anni circa, il che corrisponde alla creazione di 210.000 blocchi (ogni 10 minuti è prodotto un certo numero di bitcoin secondo un algoritmo). La ricompensa è passata a 25 BTC per ogni blocco a partire dal 28 novembre 2012 e a 12,5 BTC per blocco dal 9 luglio 2016 (e sarà tale per i prossimi 2 anni, ossia fino al 2020).

Quando l'ammontare prestabilito sarà raggiunto, l'incentivo per i partecipanti alla validazione nel network sarà rappresentato solo dalle commissioni di transazione. Queste commissioni sono utilizzate come strumento di protezione per evitare che alcuni utenti inviino transazioni al solo scopo di sovraffollare delle stesse la rete, la modalità precisa con cui funzionano queste fee è ancora in fase di sviluppo e probabilmente cambierà nel tempo; per ora possiamo dire che la commissione non è legata alla quantità di criptovaluta inviata, ma dipende da fattori quali la mole di dati contenuti nella transazione o il numero di indirizzi in cui è suddiviso l'importo che deve essere trasferito.

Uno strumento di ricompensa però, per soddisfare il proprio scopo, deve essere percepito come strumento di valore e risultare affidabile affinché i nodi che mantengono la Blockchain continuino a svolgere il proprio compito, per questo lo strumento di pagamento usato per compensare i supporters del sistema impatta direttamente anche sull'attendibilità dello stesso.

Uno degli argomenti più dibattuti è il fatto che il prezzo delle criptovalute con cui si ricompensano i partecipanti al mantenimento dell'integrità del network, non sia collegato al valore di nessun asset reale e che quindi sia soggetto ad una elevatissima e non prevedibile volatilità. Ciò è immediatamente visibile anche semplicemente osservando le fluttuazioni del bitcoin nell'ultimo anno (come ripetuto già varie volte dall'inizio dell'elaborato, utilizziamo i dati relativi al Bitcoin in quanto rappresentativi in maniera abbastanza esaustiva dell'intero mercato delle criptovalute):

Figura 9: Dati che si riferiscono al periodo ottobre 2017-settembre 2018 e che presentano il prezzo di bitcoin in dollari statunitensi. Tratti da "Blockchain.com"

Come si può vedere dal grafico (*Figura 9*) il prezzo di bitcoin è passato dai circa 4.000 $ di valore di ottobre 2017 ai quasi 20.000 di dicembre dello stesso anno (in poco più di 2 mesi ha quintuplicato il suo valore) per poi riscendere attorno a quota 6300 $ durante l'estate 2018.

Ma allora perché vi sono così tanti partecipanti che fanno a gara per validare i blocchi?

Questo aspetto può essere in parte spiegato dal fatto che il valore di uno strumento deriva anche dalla percezione che hanno dello stesso gli utilizzatori/acquirenti (dopotutto non è lo stesso anche per i beni reali in cui il prezzo si basa su domanda/offerta e quindi sulla percezione che hanno venditori ed acquirenti del valore dello stesso?). Bouoiyour e Selmi[47] suggerivano 3 differenti driver per determinare lo sviluppo del prezzo dei bitcoin (e così come per questi ultimi anche per altre famiglie di criptovalute):

[47] Bouoiyour J., Selmi R., "What does Bitcoin look like? Ann Econ Finance 16", (Forthcoming), 2015.

1) Forze di mercato di domanda ed offerta: L'offerta è determinata dallo stock totale di Bitcoin in circolazione, mentre la domanda dall'ampiezza di questa economia negli scambi e dalla velocità di esecuzione di questi ultimi.

Le criptovalute sono caratterizzate da una scarsa disponibilità (la grande maggioranza); prendiamo come esempio quello di Bitcoin, la cui disponibilità cresce (come anticipato precedentemente) secondo una serie geometrica ogni 4 anni, con un numero totale che tende asintoticamente a 21 milioni come limite ultimo, in cui si prevede la creazione dell'80% delle stesse nei primi 10 anni e dove si raggiungerà l'ammontare prestabilito nell'estate 2041[48].

Non bisogna però dimenticarsi che i bitcoin sono divisibili in sotto unità più piccole, come ad esempio i bit[49], fino all'ottava cifra decimale (dunque il numero massimo totale può essere di 21*10^14 unità) e se necessario, in futuro, anche in unità più piccole[50]. Inoltre, anche la capitalizzazione nei confronti del mercato è importante per stabilire il valore ed il ruolo di dominanza o meno di una criptovaluta nei confronti delle sue concorrenti[51]. A tal proposito il Bitcoin, che, come si è detto fin dall'inizio, rappresenta la prima e la più conosciuta criptovaluta, deve il suo elevato prezzo anche al fatto che ricopre il ruolo di criptovaluta dominante nel mercato delle stesse: la sua quota infatti ricopre poco più 52% del totale[52] delle circa 2.000 in circolazione. Dal grafico sottostante (*Figura 10)* si può notare come le 3 principali criptovalute per capitalizzazione (nell'ordine Bitcoin, Ethereum e Ripple) detengano più del 70% della quota dell'intero mercato.

[48] Nel 2013 è stata generata la metà delle possibili monete e nel 2017 si è arrivati ai tre/quarti (precisamente dal gennaio 2009 a novembre 2018 sono stati generati poco più di 17 mln di Bitcoin[48]). Dati tratti da: "Blockchain Luxembourg S.A.".

[49] Il bit è un'unità comune utilizzata per indicare una sotto unità del bitcoin: 1.000.000 di bit equivalgono a 1 bitcoin (BTC). Tratto da "bitcoin.org".

[50] La più piccola unità possibile ad oggi viene chiamata Satoshi (1 BTC corrisponde a 100.000.000 satoshi). Tratto da "bitcoin.org".

[51] A ciò si uniscono altri fattori, tra cui uno dei più importanti è l'anonimato intrinseco della criptovaluta stessa e la sua adattabilità o meno al commercio di beni illeciti (fattori che però vedremo nel secondo capitolo).

[52] Questi dati cambiano continuamente e potrebbero variare di giorno in giorno data l'elevata volatilità di questo mercato. Dati tratti da: "Coinmarketcap.com" aggiornati al giorno 01/10/2018.

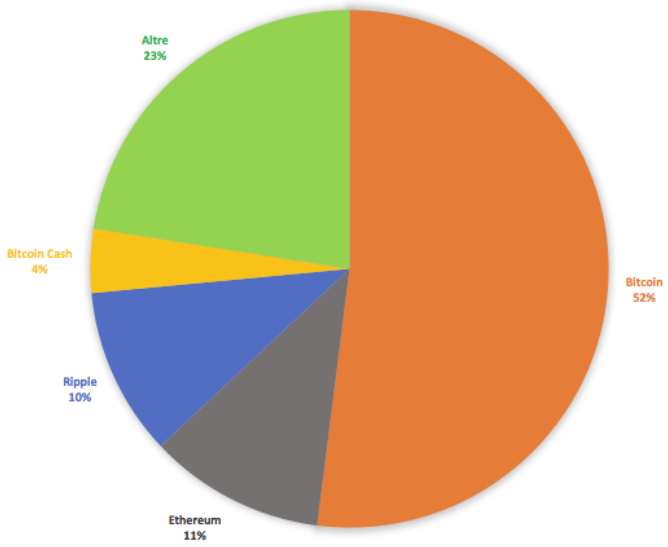


Figura 10: Dati tratti da "Coinmarketcap.com" al 1 ottobre 2018.

2) Attrattività della criptovaluta (valore futuro): alcuni investitori considerano questo nuovo strumento un'interessante opportunità in quanto vedono un potenziale rialzista nel prezzo.

3) Influenza degli scenari macroeconomici e finanziari: l'impatto degli indicatori macroeconomici e finanziari sui bitcoin (o su una qualsiasi altra criptovaluta) potrebbe agire attraverso vari canali; ad esempio scenari economici positivi potrebbero stimolare l'uso delle criptovalute negli scambi rafforzandone la domanda e conseguentemente aumentandone il prezzo. Allo stesso tempo però non è detto che scenari negativi genererebbero una caduta di prezzo, in quanto le stesse criptovalute potrebbero essere usate come investimento alternativo, di diversificazione/copertura.

A tal proposito, quasi quarant'anni fa, Robert Metcalfe[53] propose una relazione tra il valore di una rete e le dimensioni della rete stessa. Egli affermava che il valore di un network è proporzionale al quadrato del numero dei nodi che vi partecipano proponendo la seguente legge:

[53] Informatico statunitense inventore della tecnologia Ethernet.

$$U = n(n-1)$$

Dove "U" sta a rappresentare l'utilità (il valore) del network ed "n" il numero di partecipanti.

È possibile che la relazione tra il valore di una rete e la dimensione dei suoi nodi possa dipendere dal tipo di rete, e reti che possono crescere liberamente e organicamente con poche barriere all'ingresso o bassi costi potrebbero seguire la relazione di Metcalfe, mentre altri tipi di reti no[54].

Non bisogna però dimenticare che all'interno del sistema introdotto dalla Blockchain, ci sono diverse "sotto-reti". La prima tra queste è quella degli utenti finali connessi alla Blockchain e in possesso di beni che possono essere scambiati tra loro sulla rete stessa. La seconda è la rete di miners che con il loro lavoro mantengono il meccanismo di trasferimento efficiente e sicuro. Infine vi è la rete di distributori collegati al network che scambiano il bene digitale sottostante (criptovaluta) con attività e beni reali (ad esempio gli Exchange). È probabile che il valore della rete abbia una relazione matematica positiva anche con ciascuna di queste sotto-reti.

Tornando, per un momento a parlare dell'attività di mining compiuta all'interno della Blockchain del sistema Bitcoin, possiamo notare come l'hardware utilizzato per tale attività si sia evoluto molto rapidamente dal 2009 ad oggi; infatti se in un primo momento i minatori utilizzavano l'unità centrale di elaborazione (CPU) del loro computer per svolgere il proprio lavoro, presto questa si è rivelata non abbastanza veloce portando conseguentemente all'utilizzo dell'unità di elaborazione grafica (GPU) la quale era in grado di gestire i calcoli tra le 50 e le 100 volte più velocemente rispetto alla precedente, consumando una minore quantità di energia per unità di lavoro. Durante l'inverno del 2011 poi, è sorta una nuova industria con attrezzature appositamente dedicate al mining (i cosiddetti ASIC: Application Specific Integrated Circuitchips) che hanno spinto gli standard prestazionali su livelli ancora più elevati; le attrezzature in questione erano utilizzabili

[54] Alcuni (Andrew Odluzko e Benjamin Tilly, 2005) sostengono però che questa legge sia troppo ottimistica in quanto conferisce la medesima importanza a tutti i nodi del network mentre in realtà questo fattore non si dimostra sempre veritiero.

semplicemente collegandole via USB al proprio terminale e permettendo di creare per la prima volta veri e proprio centri aggregati per il mining.[55]

Negli ultimi anni però, dato l'elevato incremento nel prezzo delle criptovalute, l'attività di mining è stata intrapresa da un numero sempre maggiore di partecipanti, rendendo di conseguenza quasi tutte le precedenti strumentazioni utilizzate dai singoli inutili se confrontate a quelle possedute da gruppi sempre più grandi di miners.

Come si può vedere nel grafico riportato di seguito (*Figura 11*) la difficoltà di risoluzione del puzzle crittografico è aumentata a dismisura a partire dall'introduzione del sistema Bitcoin nel 2009 soprattutto nel periodo a cavallo tra fine 2017 e inizio 2018 in cui il prezzo della criptovaluta è passato dai 3.100 $ di valore al 14 settembre 2017 al picco massimo di quasi 20.000 $ toccato nella seconda metà del mese di dicembre 2017.

Ad oggi, il livello di difficoltà per la creazione di un nuovo blocco si attesta attorno a 7.000 miliardi, il che significa che servono all'incirca 7.000 miliardi di tentativi per ottenere la soluzione dell'hash puzzle[56].

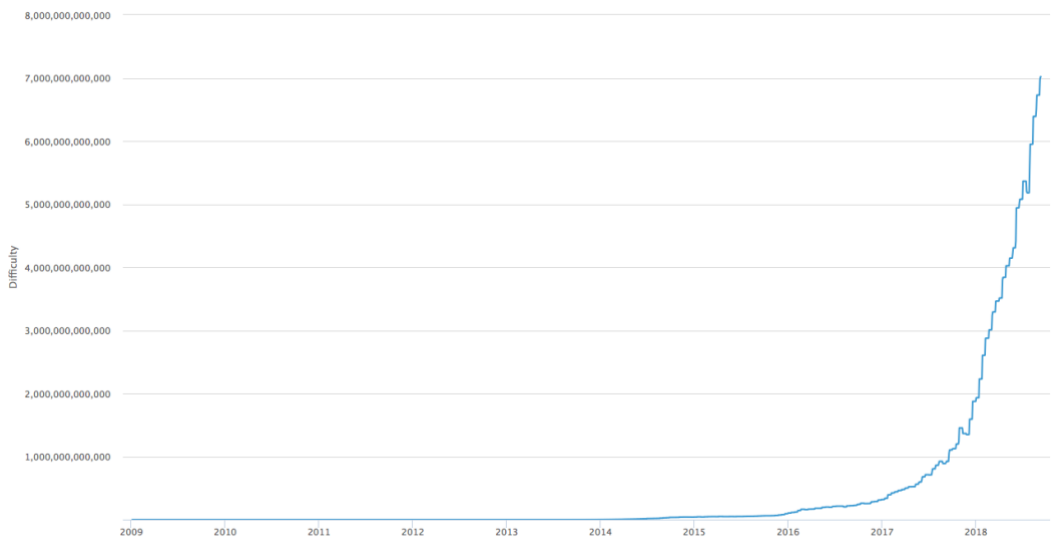


Figura 11: Tratto da "Blockchain.com" al 12 settembre 2018.

[55] Fonte: "Bitcoinmining.com".

[56] Dato al 12 settembre 2018 tratto da "Blockchain.com".

Tipologie di blockchain

Dopo averne spiegato il funzionamento, precisiamo che possono esistere due tipi di Blockchain: pubbliche o private. Le prime consentono a chiunque di registrare e leggere i dati senza l'autorizzazione di un'autorità, (come esempio più importante, appunto il Bitcoin). Chiunque con un computer o un dispositivo Smart può scaricare il software Bitcoin e creare un portafoglio digitale personale. Le Blockchain private invece hanno partecipanti prestabiliti che controllano l'accesso in lettura e scrittura, operando come una rete chiusa. Una Blockchain privata potrebbe essere costituita da un gruppo di società collegate o da un dipartimento all'interno di un'azienda. (Vedasi *Figura 12*).

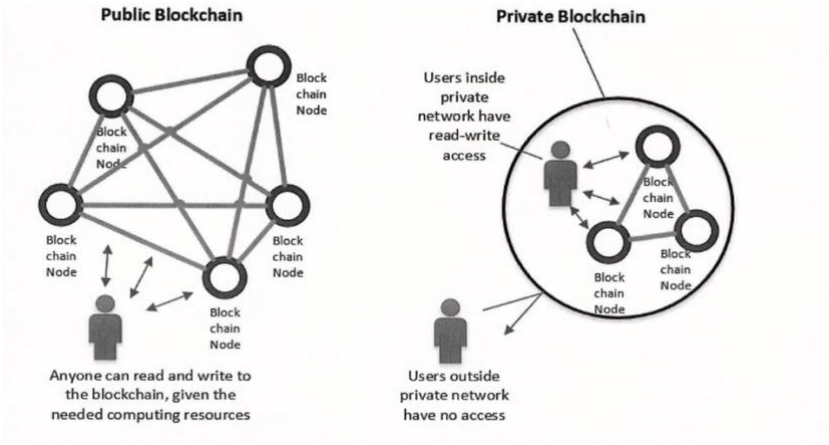


Figura 12: Immagine tratta da: "Business Education Innovation Journal" Volume 8 Number 2", dicembre 2016.

1.5) COME VENGONO CUSTODITE LE CRIPTOVALUTE: WALLET E SERVIZI DI EXCHANGE

Come abbiamo visto, solo chi possiede la chiave privata può dimostrare la proprietà di una determinata quantità di criptovaluta. A tal proposito i Wallet contenenti queste chiavi crittografiche (e quindi le corrispondenti proprietà in valuta virtuale) possono essere custoditi "autonomamente" tramite supporti hardware, oppure rivolgendosi a terze parti tramite piattaforme di Cloud System (attraverso I cosiddetti "wallet online"). Nello specifico poi, se ci riferiamo alla custodia autonoma, si può distinguere tra portafogli custoditi all'interno del proprio computer: I cosiddetti "desktop wallet", portafogli mobili ("mobile wallet") che possono invece essere installati tramite applicazione dedicata, nei

dispositivi mobili Smart, oppure "hardware wallet"[57]. Quest'ultima categoria di custodia autonoma viene solitamente riconosciuta come la più sicura; infatti gli indirizzi sono memorizzati all'interno di un apposito dispositivo hardware dedicato che può essere collegato ad un computer tramite connessione USB e permette allo stesso di essere immune da eventuali attacchi hacker che potrebbero invece colpire i dispositivi elettronici (PC, tablet o smartphone).

Il problema della memorizzazione però si riscontra nel fatto che, se queste chiavi crittografiche per errore venissero smarrite oppure sottratte, non ci sarebbe un sistema od una autorità che possa ristabilire la sicurezza del singolo account verificando a chi corrisponde la proprietà dell'account violato (come accade invece ad esempio nell'ambito delle operazioni bancarie), fattore che comporterebbe la conseguente perdita della propria ricchezza. Inoltre le criptovalute eventualmente smarrite non saranno mai più recuperabili e diminuirà quindi la disponibilità totale delle stesse all'interno del network.

Al contrario, se invece di utilizzare il sistema di memorizzazione su hardware, che appunto può comportare lo smarrimento delle proprie criptovalute o il malfunzionamento dello stesso hardware (con conseguente perdita dei dati salvati), si ricorresse al salvataggio su Cloud o piattaforme gestite da società, il problema diventerebbe un altro, ossia quello dell'integrità dei servizi offerti da questi enti terzi; questi ultimi infatti spesso sono risultati vulnerabili a furti ed attacchi informatici che hanno compromesso irrimediabilmente, parte o la totalità delle disponibilità dei clienti degli stessi[58].

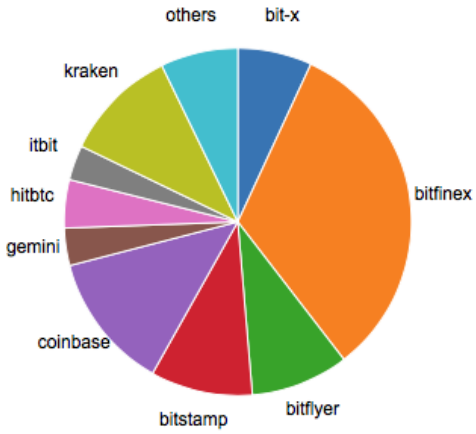
Lo stesso discorso riguarda i cosiddetti "Exchange", ossia intermediari che permettono di scambiare le criptovalute con le principali valute mondiali aventi corso legale, rendendo il denaro espresso in valuta virtuale immediatamente spendibile, liquido e pronto per le transazioni in qualsiasi mercato reale. I siti di Exchange offrono infatti un servizio di cambio, un po' come fanno gli sportelli di Forexchange negli aeroporti e hanno il "potere" di gestire i prezzi di scambio tra valuta virtuale e moneta fiat oltre che di garantire la liquidità di questo mercato[59].

[57] Secondo il lavoro svolto nel settembre 2017 da G. Hilleman e M. Rauchs (Cambridge University), il mobile wallet è utilizzato dal 65% circa degli utenti, mentre l'hardware wallet dal 23% degli stessi.

[58] Il furto di crittografia è istantaneo, irreversibile e tipicamente anonimo.

[59] Secondo le stime di Sanford C. Bernstein & Co, pubblicate nel rapporto "Crypto trading - The next big thing is here" il giro di affari degli Exchange potrebbe raggiungere quest'anno i 4 miliardi.

Nella seguente figura sono presentati i principali Exchange, per market share, operanti in bitcoin:



bitfinex	32,6%
coinbase	12,8%
kraken	10,6%
bitstamp	9,5%
bitflyer	9,1%
bit-x	6,9%
altri	18,5%

Figura 13: Dati tratti da: "data.bitcoinity.org" al 17 settembre 2018.

Questi intermediari convenzionalmente si suddividono in 2 categorie: quelli che operano principalmente in bitcoin[60] e quelli che permettono uno scambio diretto tra svariate criptovalute e moneta fiat. I primi permettono ad un soggetto in possesso di bitcoin il cambio con qualsiasi altra famiglia di criptovalute (nel caso si volesse operare con questi Exchange senza essere in possesso di bitcoin, sarebbe necessario in primis convertire le valute virtuali di cui si è in possesso in bitcoin, sostenendo quindi un maggiore costo in termini di commissioni), mentre i secondi forniscono un servizio che non prevede steps precedenti dove dover ottenere bitcoin, bensì un meccanismo di conversione diretta.

I servizi offerti dagli Exchange solitamente sono di 3 tipi:

- "Gestione ordini di acquisto/vendita": la piattaforma permette di associare gli ordini di acquisto e vendita dei differenti clienti (talvolta favorendo anche lo scambio in presenza fisica tra gli stessi). In questo caso l'Exchange svolge solo la funzione di intermediario tra chi compra e chi vende, non acquista mai in proprio. (Il guadagno portato da questo servizio si sostanzia nelle commissioni).

[60] Gli exchange di questo tipo più conosciuti sono Bitfinex, Bitflyer e Kraken.

- "Brokeraggio": possibilità offerta agli utilizzatori di acquistare o vendere una determinata quantità di criptovaluta ad un prezzo prefissato. A differenza del precedente servizio, nel caso del brokerage, l'Exchange si occupa in maniera diretta di acquistare/vendere per conto del proprio cliente e non solo di unire domanda ed offerta.

- "Trading": tramite questo servizio si permettono acquisti, anche tramite l'utilizzo di leva finanziaria, di criptovalute o ETF sulle stesse. L'utente opera solo con la piattaforma stessa, senza la possibilità che vi siano interazioni con altri utilizzatori (la piattaforma infatti è uno dei soggetti che effettuano l'operazione e partecipa al rischio insito nella stessa). Questo servizio, data la volatilità del mercato, è quello che solitamente richiede le commissioni più elevate e che applica un prezzo di cambio più sfavorevole per il cliente rispetto ai precedenti[61]

Spesso però, specialmente in passato, quando si faceva riferimento agli Exchange si trattava di aziende non regolamentate e con strutture societarie poco affidabili (con sedi in isole del Pacifico e alcune volte senza indirizzi o bilanci pubblici). In momenti di caos mediatico o di boom del settore è facile (come è già successo) che alcuni Exchange possano fallire. L'esempio più eclatante fu la dichiarazione di bancarotta dell'allora famoso Exchange Mt.Gox[62] datata 28 febbraio 2014. Il "cambiavalute virtuali" giapponese aveva iniziato ad operare nel luglio 2010 nell'ambito del cambio tra valute fiat e bitcoin arrivando a gestire tra il 2013 e l'inizio del 2014 il 70% di tutti questi scambi a livello mondiale. Già nel giugno 2013 la piattaforma sospese le contrattazioni per 2 settimane a causa di attacchi informatici, ma in quel caso la sua attività poté proseguire senza troppi intoppi (pur subendo un danno d'immagine e la diffusione tra gli utenti dei primi dubbi circa la solvibilità della stessa). Non fu così però nel febbraio dell'anno successivo quando, dopo essere "sparita" dalla rete per due giorni, la società si vide costretta ad effettuare domanda di

[61] Ad esempio per un exchange di questo come Coinbase, le commissioni si aggirano attorno al 3,5%.
[62] Il sito, sorto inizialmente nel 2009 ad opera di Jed McCaleb come piattaforma per lo scambio e il trading sulle carte da gioco del famoso game "Magic" deve il suo nome proprio a quest'ultimo; infatti Mt.Gox sta per "Magic: The Gathering Online Exchange". Successivamente, nel 2011, la piattaforma fu venduta a Mark Karpeles e alla sua compagnia Tibanne. The Wall Street Journal, 25/02/2014.

bancarotta protetta al Tribunale di Tokyo in seguito ad un presunto attacco hacker subito[63]. La piattaforma subì una perdita di circa 750.000 bitcoin di proprietà degli utenti e di 100.000 di proprietà della stessa società, per un totale di 850.000 (che dato il valore all'epoca della criptovaluta corrispondevano a circa 473 milioni di dollari[64]) e si vide costretta ad ammettere, ad opera del proprio CEO (M. Karpeles) in diretta Tv di aver riscontrato una falla relativa alle misure di sicurezza strutturale del sito che aveva permesso l'attacco. Sebbene quello nei confronti di Mt.Gox risulta essere l'attacco hacker più ricordato ad un Exchange, nel gennaio di quest'anno (2018) un'altra piattaforma giapponese, Coincheck, ha subito un importante attacco che ha causato il furto del corrispettivo di 533 milioni di dollari[65] nella criptovaluta Nem. Quest'attacco, seppur di dimensioni maggiori rispetto a quello nei confronti di Mt. Gox, ha avuto un impatto mediatico inferiore di quello citato precedentemente (anche se ha causato da gennaio in poi una profonda correzione dei prezzi in tutto il cripto-mercato), ciò è probabilmente dovuto al fatto che all'epoca della bancarotta, la società creata da Jed McCaleb gestiva circa l'80% del cambio di criptovaluta in Giappone e operava principalmente in bitcoin (mentre nel caso di Coincheck i Nem erano meno conosciuti al pubblico, pur situandosi in quel momento tra le prime 10 criptovalute per capitalizzazione).

1.6) LIMITAZIONI TECNICHE

Uno strumento digitale e decentralizzato come le criptovalute, senza nessun tipo di valore sottostante a garanzia e con una regolamentazione ancora molto frammentaria e parziale, pone sicuramente l'utilizzatore in una posizione di rischio molto elevata. Infatti, oltre ad alcune limitazioni tecniche, (insite nel protocollo che ne caratterizza l'origine) le quali possono diminuire i benefici di questi nuovi sistemi, vi sono anche alcuni aspetti che potrebbero minare il funzionamento dello strumento stesso comportando grandi perdite per l'utilizzatore.

[63] Non fu però totalmente chiaro se fu proprio un attacco hacker a causare le perdite o se questo sia anche dovuto a una mala gestione (o all'unione delle due componenti).
[64] Dato tratto da: "Il Sole 24 Ore" del 28/02/2014.
[65] Dato fornito da: "Rapporto Clusit" 2018

Infatti, seppur per molti aspetti la Blockchain si dimostri una tecnologia rivoluzionaria che potrebbe permettere di superare alcune problematiche odierne, essa non è totalmente perfetta o esente da limitazioni e forse tale (per ora) da essere applicata su larga scala nel mercato.

Riepiloghiamo di seguito alcune delle principali problematiche e dei rischi che si possono riscontrare:

1) Rischio di privacy: per mantenere l'elevato grado di trasparenza la Blockchain tiene traccia dell'insieme di tutte le transazioni avvenute dall'introduzione della stessa. Senza questo livello di trasparenza la stessa non potrebbe conseguire i propri obiettivi; questo fattore però, nonostante l'anonimato (parziale) dei partecipanti al network, risulta essere limitante in casi di applicazione che richiedono maggiore privacy e potrebbe rivelarsi maggiormente problematico man mano che la catena aumenta, in quanto con il passare del tempo vengono affinate tecniche per l'analisi dei profili degli utenti sempre più efficaci.

2) Sicurezza per gli utenti e integrità degli enti terzi operanti nel sistema: come si è già visto nel paragrafo precedente uno dei principali problemi dello strumento di pagamento basato sul sistema Blockchain è quello relativo alla dimostrabilità della proprietà (che può avvenire solo se in possesso della chiave privata crittografica) e della sicurezza degli intermediari che custodiscono o gestiscono le valute virtuali degli individui.

3) Limitata scalabilità[66]: l'utilizzo dell'hash puzzle come misura per garantire l'immutabilità della catena di blocchi e per imporre un costo a chi cercasse di violare la stessa finisce per creare un rallentamento nella velocità del processo. Questa caratteristica è considerata un serio problema che potrebbe, se non implementato nella maniera migliore, limitare le applicazioni della Blockchain in ambiti/settori in cui serva una elevata velocità. In ogni caso non bisogna dimenticare che molte Blockchain (e le rispettive criptovalute) hanno già migliorato questi aspetti, altre

[66] Con scalabilità si intende la possibilità di gestire un determinato numero di transazioni al secondo. Perciò se in ipotesi in futuro si realizzassero operazioni al secondo in misura maggiore rispetto a questo numero, tendenzialmente potrebbe accadere che le operazioni "in eccesso" non vengano mai registrate in quanto la rete si ritorverebbe in una situazione in cui sarebbe satura di operazioni da validare.

sono in evoluzione e quindi questa limitazione potrebbe ridursi e le stesse tecnologie, con il tempo, essere implementate in maniera sempre migliore al fine di ottenere maggior velocità e sicurezza.

4) Elevati costi: questo problema è legato al precedente ossia all'hash puzzle che per fornire la Proof of Work deve necessariamente comportare un dispendio in termini di energia e tempo. Basti pensare che secondo i dati forniti da Digiconomist, il consumo annuale di energia per il mining di Bitcoin si aggira (giugno 2018) attorno a 73 TW/h (ossia 262,8*10^15 Joule[67]), dato che supera il consumo di intere nazioni come la Colombia, la Svizzera o la Repubblica Ceca. Per rendersi conto più concretamente in prospettiva dell'energia consumata dalla rete Bitcoin possiamo confrontarla con un altro sistema di pagamento: VISA. Secondo la società stessa, nell'ultimo anno, i propri consumi hanno raggiunto un totale di 674,922 Gigajoule (674,9*10^9 Joule) di energia derivante da varie fonti energetiche a livello globale per tutte le sue operazioni (ciò significa che VISA ha un fabbisogno energetico pari a circa 17.000 famiglie statunitensi). Sappiamo anche che VISA ha elaborato 111,2 miliardi di transazioni nel 2017[68]. Con l'aiuto di questi numeri, è possibile confrontare entrambe le reti e mostrare che Bitcoin è estremamente più energivora nelle transazioni rispetto a VISA (si noti che la *Figura 14* confronta una singola transazione in Bitcoin a 100.000 transazioni VISA).

   Inoltre l'energia utilizzata per il mining[69] di Bitcoin (e di altre criptovalute basate sul meccanismo di Proof-of-Work) deriva soprattutto da combustibili fossili a basso costo in quanto i principali pools di miners si situano nel continente asiatico; portando così con sé anche un problema ambientale non irrilevante, il quale potrebbe/dovrebbe scongiurare l'interesse di parte degli investitori che si focalizzano sempre più su prodotti di investimento che siano equi e sostenibili.

[67] Derivante dalla conversione: 73 TW/h = 73*3,6*10^15 Joule.
[68] Dati ricavati da: "Corporate Responsibility Report VISA", 2016.
[69] Interessante notare che nei mesi di giugno e luglio 2018, prima Apple e poi Google hanno bandito dai propri store digitali (rispettivamente AppleStore e Play Store) le applicazioni che eseguono mining sui computer MAC, sui dispositivi con sistema operativo IOS e su quelli Android. Fonte: "Il Sole 24 Ore" del 29/07/18.

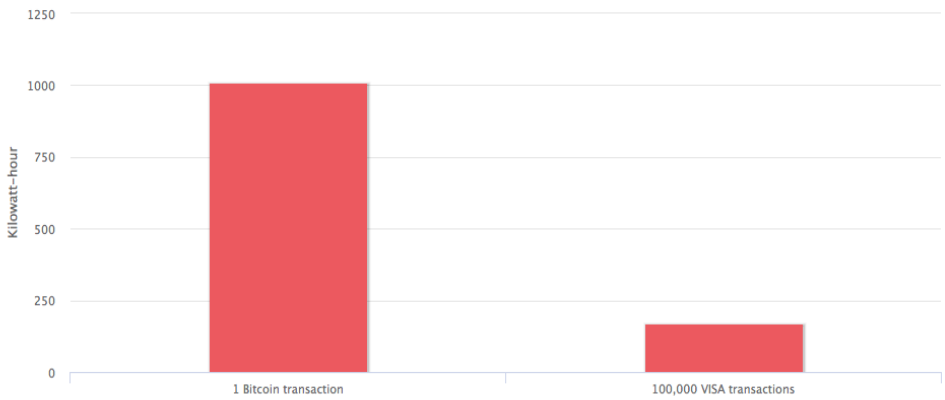


Figura 14: Dati tratti da "BitcoinEnergyConsumption.com"

5) Centralità occulta: Sebbene, perlomeno in origine, le criptovalute siano nate come realtà decentralizzata ed autonoma, c'è il rischio che soggetti con elevate disponibilità economiche investano in hardware specifico che permetta loro di risolvere in anticipo rispetto agli altri i puzzle crittografici (perlomeno nei casi di Blockchain con meccanismo di consenso basato sul Proof of Work) rendendo l'attività non profittevole per gli altri nodi che non hanno accesso alle medesime. Ciò costringerebbe molti ad abbandonare il network, creando una sorta di oligopolio all'interno del sistema solo per coloro i quali abbiano determinati standard di potenza computazionale che potrebbero formare dei pool aggregati tali da poter controllare il sistema (in questo caso in cosa divergerebbe questo sistema dall'attuale sistema economico centralizzato formato dalle banche?)[70].

6) Poca flessibilità data l'immutabilità del registro Blockchain e il mantenimento di tutte le transazioni per un periodo pressoché illimitato, quest'ultima risulta difficilmente migliorabile a livello di sviluppo software o di bug-fixing nel suo protocollo (come appunto per quanto riguarda il problema di aumento della velocità enunciato in precedenza). Una delle maggiori sfide nel superare queste limitazioni sta nella distinzione tra migliorare la tecnologia Blockchain oppure cambiarne totalmente alcune parti del protocollo. Per questo infatti sebbene la versione del protocollo che caratterizza il sistema Bitcoin sia l'esempio più puro di

[70] Basti pensare che ad oggi (giugno 2018) più di 5 milioni di Bitcoin sul totale di circa 17 milioni sono posseduti da 1.600 wallet. (dato tratto da Il sole 24 ore 25/06/18).

network decentralizzato Peer-to-Peer, probabilmente questa non è l'implementazione più efficiente ed adeguata della tecnologia Blockchain alla società odierna.

7) Termine della produzione: nel momento in cui terminerà la produzione dei bitcoin (o di qualsivoglia altra criptovaluta), all'interno di un sistema Proof of Work, si potrebbe riscontrare un problema nell'ambito degli incentivi per i miners. Questi ultimi infatti, una volta finita la ricompensa in bitcoin, si ritroverebbero ad essere ripagati per il proprio lavoro attraverso le fee contenute in ogni transazione. Tale compenso però potrebbe rivelarsi poco attrattivo dati i sempre più elevati costi dell'attività di mining, portando all'uscita dal network di buona parte dei suoi "validatori" e alla riduzione della sicurezza del sistema stesso (in conseguenza si ridurrebbe anche la difficoltà del puzzle crittografico, ma non è detto che questa riduzione sia adeguatamente elevata da attrarre nuovi minatori). Per contro invece, se dovessero aumentare le commissioni sulle singole transazioni il sistema perderebbe una delle proprie caratteristiche fondamentali ossia quella di comportare bassi costi per l'esecuzione delle transazioni degli utenti.

1.7) DIFFERENTI MECCANISMI PER IL "CONSENSUS"

Come abbiamo visto fin dall'inizio di questa trattazione, l'obiettivo con cui è nata la tecnologia Blockchain è stato quello di favorire il trasferimento di valore tra soggetti senza dover passare attraverso il sistema bancario o un equivalente sistema centralizzato. La stessa tecnologia però, in alcuni casi, è stata anche implementata per svolgere ulteriori funzioni rispetto a quella principale o per essere utilizzata proprio dagli intermediari che pareva si volessero per così dire "accantonare": banche ed istituzioni finanziarie.
Le Blockchain cosiddette alternative (Alt-Chains) si caratterizzano per una struttura differente del protocollo che le governa e che in alcuni casi ne porta a modificare i meccanismi attraverso cui le stesse ottengono l'integrità necessaria. A questo scopo

presentiamo le due più importanti[71] Blockchain alternative a quella Bitcoin che portano innovazione all'interno del meccanismo di Consensus con nuove soluzioni tecnologiche (già implementate o in corso di implementazione).

1.7.1) Ripple (Distributed Agreement Protocol)

Il primo esempio di integrazione della tecnologia Blockchain all'interno del sistema bancario/finanziario è quello portato dalla Startup californiana Ripple. Quest'ultima, è stata fondata nel settembre 2012 da Chris Larsen e Jed McCaleb (lo stesso fondatore di Mt.Gox) inizialmente sotto il nome di "Opencoin" successivamente cambiato prima in Ripple Labs, Inc. (2013) e poi definitivamente in Ripple nel 2015.

La società, cresciuta grazie al finanziamento di Business Angels e fondi di Venture Capital, si caratterizza per l'innovazione portata dalla creazione di un protocollo (RTXP) open source basato sulla tecnologia Peer-to-Peer all'interno di un network (RippleNet) che permette ai propri clienti (banche, fornitori di servizi di pagamento, società finanziarie) di eseguire pagamenti in qualsiasi parte del mondo in modo istantaneo, affidabile ed economico. Attraverso un software chiamato xCurrent[72] funzionante all'interno del network è possibile regolare istantaneamente pagamenti transfrontalieri. La soluzione è specificatamente progettata per soddisfare le esigenze di banche ed istituzioni finanziarie adeguandosi alle loro strutture di gestione dei rischi, di informativa, di compliance o trattamento della privacy[73]; Il software specifico infatti viene installato all'interno dell'infrastruttura informatica preesistente ed è costruito per interfacciarsi con la stessa tramite un'interfaccia API. Per quanto concerne ciò che più ci interessa in questo trattato, questa soluzione, permettendo al software Ripple di interagire, senza modificare le procedure

[71] I sistemi analizzati sono considerati i più importanti sia a livello di capitalizzazione nel mercato delle alternative a Bitcoin, sia a livello di innovazione/modifica apportate all'idea originale di Blockchain introdotta dal sistema di Nakamoto.

[72] Successivamente ne verrà esplicato il funzionamento. Per ulteriori informazioni si faccia riferimento al sito: "Ripple.com"

[73] xCurrent crea una connessione diretta e sicura tra le controparti finanziarie comunicanti. Tutti i dati riguardanti un pagamento vengono inviati direttamente tra le istituzioni che partecipano alla transazione; né Ripple (la società) né terze parti hanno accesso a questi dati. Questo design garantisce che i fornitori di servizi finanziari abbiano il controllo sull'accesso ai dati dei propri clienti e sul modo in cui vengono archiviati.

interne del membro della rete, in ambito ad esempio di individuazione di frodi o di misure antiriciclaggio, riduce al minimo i costi di integrazione e le interruzioni dell'operatività.

Ad oggi (ottobre 2018) la società collabora con più di 100 istituzioni finanziarie implementando sperimentazioni del proprio sistema di pagamenti cross-border all'interno delle stesse. Tra i partner di Ripple ritroviamo importanti colossi della finanza mondiale tra cui:

Figura 15: Informazioni disponibili direttamente sul sito della società: "ripple.com".

Tutti i membri di RippleNet sono connessi tra loro tramite questa tecnologia standardizzata. XCurrent è un sistema globale di regolamento in tempo reale (RTGS) che consente agli utilizzatori di predisporre, inviare e regolare le proprie transazioni con elevata velocità, trasparenza[74] ed efficienza. Tale soluzione è basata su ILP, un protocollo aperto e neutrale, che consente l'interoperabilità tra diversi registri e reti di pagamento, meccanismo che permette la realizzazione di un pagamento end-to-end crittograficamente sicuro con immutabilità della transazione e chiarezza delle informazioni. Il sistema RippleNet è una rete decentralizzata basata su un accordo tra Ripple e i partecipanti alla stessa, nella quale però tutti i partecipanti utilizzano la medesima tecnologia e aderiscono ad un insieme coerente di regole e standard di pagamento. La tecnologia distribuita di

[74] xCurrent consente agli utilizzatori di avere completa chiarezza delle commissioni e del costo fisso del pagamento prima di iniziare la transazione. Questa trasparenza ad esempio consente alla banca di comunicare accuratamente ai propri clienti il costo totale di invio del pagamento prima di spostare i fondi.

Ripple punta a sopperire alle carenze del sistema bancario/finanziario odierno nell'esecuzione dei pagamenti, riducendo i costi, aumentando la velocità di elaborazione e offrendo visibilità end-to-end sulle commissioni di pagamento, sui tempi e sulla consegna. L'ecosistema dei partecipanti a RippleNet è suddiviso in due gruppi principali: i membri della rete (banche, fornitori di servizi di pagamento ed istituzioni finanziarie che collaborano con la stessa Ripple) e gli utenti della stessa (aziende, consumatori). La principale funzione per cui è stata pensata Ripple è quella di essere utilizzata tra diversi intermediari finanziari allo scopo di favorire il raggiungimento di una maggiore efficienza nel sistema dei pagamenti e il miglioramento (se non la concorrenza) di tecnologie considerate un po' antiquate come quella SWIFT[75] (Society For Worldwide Interbank Financial Telecommunication) ossia quella utilizzata principalmente oggigiorno per eseguire pagamenti transfrontalieri.

Quando si parla di Ripple comunemente, tramite la stessa parola, si fa riferimento sia alla piattaforma creata dall'omonima società che alla criptovaluta che opera attraverso la stessa (e si identifica con la sigla "XRP"). In realtà però, a livello di sviluppo le due cose sono indipendenti: la società infatti è stata creata con l'obiettivo di implementare un nuovo sistema di pagamento in tempo reale all'interno del sistema finanziario tradizionale, la criptovaluta invece come strumento per operare all'interno dello stesso, strumento però che non vuole sostanziarsi in una nuova valuta che svolga la funzione di riserva di valore o di investimento, bensì come mezzo che viaggiando rapidamente all'interno del network ne possa velocizzare le transazioni (cosa che non sarebbe possibile se le stesse fossero realizzate in moneta fiat[76]). Gli XRP infatti non vengono considerati da molti come una vera

[75] SWIFT: Consorzio di banche di più paesi fondato a Bruxelles il 3 marzo 1973, con lo scopo di razionalizzare i rapporti bancari internazionali attraverso lo scambio di informazioni di carattere finanziario. Le banche aderenti alla SWIFT possono scambiarsi messaggi attraverso un sistema di telecomunicazioni. Il collegamento fra le banche aderenti e la SWIFT è assicurato da un organo di coordinamento presente nei vari paesi. I collegamenti interbancari avvengono utilizzando tecniche operative e attrezzature sofisticate che consentono lo scambio di messaggi di ogni tipo (ordini di pagamento, accreditamenti ecc.) in tempo reale e senza bisogno di codifica. Creata e gestita da banche, la rete è ora accessibile anche alle seguenti categorie di operatori non bancari: agenti di cambio (*brokers*) e operatori di borsa (*dealers*), istituzioni di compensazione e di deposito e istituti autorizzati allo scambio di titoli. Definizione tratta da: "bankpedia.org".

[76] L'importo di XRP esistenti (100 miliardi) è ampio proprio perchè l'obiettivo insito negli stessi è quello di essere utilizzati dalle istituzioni finanziarie per compiere pagamenti (anche di elevato importo) e questo unito al fatto che siano pensati, come già anticipato, al fine di agevolare i pagamenti e non a fini di riserva di valore giustifica il fatto che il prezzo di conversione dei Ripple (al 1 ottobre 2018) si aggiri attorno a 0,57 $. La stessa criptovaluta inoltre è divisibile fino alla sesta cifra decimale (0,000001 XRP).

e propria criptovaluta dal momento che ne snaturano in un certo senso quella decentralizzazione che caratterizza l'essenza del fenomeno stesso, dato che è la società (Ripple) che controlla il network e non i partecipanti (anche se poi vedremo che la stessa sta apportando alcune modifiche al protocollo per renderlo più decentralizzato).

Vediamo ora le principali differenze tra il protocollo utilizzato da Ripple e quello implementato nel sistema Bitcoin:

- Ripple Consensus vs Proof of Work: In precedenza abbiamo visto che il protocollo Bitcoin utilizza come strumento di validazione delle transazioni il cosiddetto sistema di "Proof of Work" nel quale il consenso sulla veridicità di una delle stesse è dato dalla potenza di calcolo computazionale utilizzata per risolvere una sorta di puzzle crittografico, in Ripple invece, per la validazione ci si basa su un "Distributed Agreement Protocol[77]", ossia una sorta di consenso distribuito nel quale i partecipanti affermano di aver ricevuto per prima quella determinata transazione validandola ed evitando il problema del Double Spending. Non tutti i partecipanti però possono partecipare a questo meccanismo, infatti solo alcuni nodi della rete sono classificati come "Trusted Validator[78]" ossia verificatori affidabili e questi ultimi sono quasi interamente controllati da Ripple stessa. Per questo non si può dire che il sistema elaborato dalla stessa società sia un peer-to-peer puro, in quanto la decentralizzazione non è totale. A tal proposito però in dichiarazioni recenti, Ripple ha affermato di lavorare ad una cessione di questo ruolo di Trusted Validator anche a terze parti per allargare la base del Consensus rendendola più simile a quella di un network Peer-to-Peer puro sebbene mantenendo determinati standard di sicurezza e scalabilità[79].

- Creazione delle criptovalute: Come abbiamo visto nei paragrafi iniziali, la creazione di nuovi bitcoin avviene grazie al lavoro dei miners e culminerà con una quantità totale pari a 21 milioni, per quanto riguarda gli XRP, questi ultimi sono già stati tutti

[77] David Schwartz, "The Ripple Protocol Consensus Algorithm", Ripple Labs Inc., 2014.
[78] Questi ultimi vengono inseriti in una "recommended UNL list".
[79] Rome reginelli, "Decentralization Strategy Update", 17 ottobre 2017. Ripple.com.

"creati" nel loro numero massimo ossia quello di 100 miliardi. Ripple possiede 6 miliardi di criptovalute del sistema, mentre il 55% del totale si trova bloccato all'interno di alcuni portafogli (sempre detenuti dalla società stessa) tramite i quali, con cadenza mensile, viene immessa nel mercato una quantità pari a un miliardo degli stessi fino al momento in cui il totale non sarà completamente distribuito all'interno del network.

Questo sistema, seppur criticato dai sostenitori della decentralizzazione pura (come il precedente) permette una maggior velocità nella validazione delle transazioni, elimina i rischi legati alla presenza di pool di miners e garantisce un minor dispendio di denaro ed energia pur assomigliando maggiormente al sistema di pagamenti tradizionale che a quello Bitcoin (infatti ritorna il problema dell'entità centrale, la stessa Ripple, che di fatto controlla e vigila sul sistema).

- Caratteristiche criptovaluta di sistema: Tramite Ripple si possono effettuare transazioni in valute differenti attraverso l'uso della valuta virtuale ideata da Ripple stessa. Quest'ultima permette transazioni istantanee e molto più veloci rispetto a quelle ottenute con altri cripto-sistemi come Bitcoin o Ethereum. Gli scambi infatti si possono definire in maniera praticamente istantanea, fattore che permette di processare quasi 1.500 transazioni al secondo fino a poter arrivare, se implementato adeguatamente, ad un massimo di 50.000, al pari di quelle processabili attualmente dal sistema di pagamento Visa[80] (Bitcoin è in grado di processare circa 5/6 transazioni al secondo ed Ethereum 15/20). In pratica, all'interno del network Ripple, quando una parte invia un pagamento in valuta locale questo verrà convertito in XRP per "viaggiare" all'interno del sistema e poi essere riconvertito nella valuta desiderata[81] al momento della ricezione del pagamento da parte della controparte (allo stesso modo però gli utilizzatori possono anche svolgere direttamente i pagamenti utilizzando gli XRP).

[80] Dato fornito da Visa stessa al 15 luglio 2017.

[81] Questa operazione di conversione tra la valuta XRP e la valuta fiat avviene ad opera dei cosiddetti "Ripple Gateway" una sorta di Exchange interni al sistema (la funzione può essere svolta anche dalle istituzioni finanziarie che collaborano con Ripple stessa).

Figura 16: A sinistra: Rapidità di esecuzione delle transazioni a confronto tra i sistemi Ripple, Ethereum e Bitcoin. A destra: numero di transazioni gestite al secondo. Fonte: Ripple.com

Per operare, il network Ripple, si basa sull'utilizzo principale di xCurrent a cui si affiancano altri 2 strumenti: xRapid e xVia.

xCurrent

Componenti software del sistema xCurrent**:**

Vediamo ora maggiormente nel dettaglio come si sviluppa una transazione attraverso il software xCurrent. Quest'ultimo è costituito da 4 componenti principali:

1) Messenger: applicazione API-based che abilita comunicazioni bidirezionali tra gli intermediari operanti all'interno del network Ripple in modo che questi ultimi possano coordinare e verificare le informazioni attinenti alla transazione prima che questa venga processata, in modo tale da evitare errori o costi aggiuntivi. Se necessario l'istituzione beneficiaria può chiedere informazioni supplementari.
   Successivamente vi è una fase di validazione che comprende verifiche di compliance e dei rispettivi portafogli. Una volta che le istituzioni hanno tutte le informazioni necessarie possono pre-validare il pagamento, prima che l'ILP ledger processi effettivamente lo stesso. Nel momento in cui l'operazione si è conclusa, il Messenger invia una notifica alle parti. (Sebbene il procedimento possa sembrare complesso il tutto avviene in maniera autonoma, è crittografato e standardizzato permettendo che la transazione si realizzi in pochi secondi).

Figura 17: Nel dettaglio si può vedere un esempio di scambio di informazioni tra il Messenger delle controparti di una transazione. Fonte: "Ripple.com".

2) ILP[82] Ledger: "sottoregistro" del registro generale che ogni istituzione finanziaria partecipante al network possiede per tenere traccia delle proprie transazioni all'interno del sistema Ripple. Quest'ultimo abilita le controparti a stanziare i fondi automaticamente il che significa che l'operazione o verrà realizzata immediatamente (se tutto è corretto: dati, analisi, disponibilità sui conti ecc.) o non si realizzerà affatto.

3) Validator: dispositivo che conferma crittograficamente il successo o il fallimento dell'operazione di pagamento. Quest'ultimo, coordinando i movimenti di fondi tra i registri (ledger) delle controparti, è l'unica fonte considerata veritiera nella verifica dell'esecuzione dell'operazione. Le controparti possono fare affidamento sul Validator dell'entità inviante o anche implementarne uno proprio.

4) FX Ticker: componente che facilita lo scambio tra ILP ledgers, fornisce il tasso di cambio dell'operazione (se necessario) e tiene traccia dei dettagli della transazione. Durante la transazione, coordina i trasferimenti sui registri ILP per il regolamento, garantisce la validità del tasso di cambio applicato nella fase di validazione iniziale

[82] ILP: "Interledger Protocol": protocollo aperto che permette l'esecuzione delle transazioni in tempo reale.

e trasferisce l'importo del pagamento al registro ILP della banca beneficiaria. *(Figura 18)*

Figura 18: Tratto da: "Ripple: product Overview, A technical overview of xCurrent", 2017.

Nella seguente tabella viene proposto un confronto tra le principali caratteristiche dei sistemi Bitcoin e Ripple:

CARATTERISTICHE	BITCOIN	RIPPLE
METODO DI CONSENSUS	Proof of Work (eseguito dai Miners)	Ripple Protocol Consensus Algorithm (eseguito da Trusted Validators)
NUMERO DI UNITA' PRODOTTE	21 MILIONI. Terminerà nel 2041.	100 MILIARDI. Importo già totalmente generato.
DISTRIBUZIONE CRIPTOVALUTA	Distribuita a coloro che validano le transazioni risolvendo il puzzle	6 mld posseduti da Ripple, il 55% del totale invece in

	crittografico (Miners). Al momento la ricompensa è di 12,5 bitcoin per blocco minato.	Escrow (1 mld distribuito mensilmente).
VELOCITA' TRANSAZIONI	Ogni 10 MINUTI circa viene creato un blocco. La singola transazione ha tempi variabili anche in base alle "fee" incluse.	Non essendo presente il mining le transazioni sono pressoché ISTANTANEE (1.500 processabili al secondo).
PARTICOLARITA'	La criptovaluta più conosciuta e con la maggior capitalizzazione.	Costituisce uno degli strumenti di pagamento più veloci sul mercato (sebbene ancora in fase di testing).
NOTE	Definibile come vera e propria criptovaluta decentralizzata.	Ritenuta una "criptovaluta centralizzata". Pensata per utilizzo in collaborazione con il settore bancario/finanziario.

Il secondo esempio che verrà illustrato è invece quello della piattaforma Ethereum, la quale viene definita una "Blockchain 2.0" poiché oltre ad aver introdotto un nuovo meccanismo di consensus (come vedremo non ancora totalmente implementato) permette che la propria Blockchain venga utilizzata anche per scopi diversi dai soli pagamenti, ossia come sistema per registrare, confermare e trasferire tutti i tipi di contratti o proprietà. Questo concetto è generalmente conosciuto come "Smart Property": ogni asset può essere registrato in una Blockchain e la sua proprietà controllata da chiunque sia in possesso della chiave privata di accesso. Inoltre tramite dei contratti prestabiliti detti "Smart Contracts" si può stabilire un trasferimento automatico di proprietà al presentarsi di determinate condizioni (ad esempio la conclusione del pagamento delle rate prestabilite per l'acquisto

di un bene). Questi contratti presuppongono lo stesso tipo di accordo di fare o non fare qualcosa in cambio di un'altra, che costituisce i contratti tradizionali, ma rimuovono il bisogno di fiducia tra le parti, ciò perché un contratto Smart è sia definito che eseguito da un codice automatico che non include discrezionalità. I 3 elementi che contraddistinguono questi contratti sono:

- Autonomia: una volta attivato il contratto non vi è necessità che le controparti si mantengano in contatto.
- Autosufficienza: questi contratti sono in grado di agire per raccogliere fondi, fornendo servizi o emettendo capitale e di spendere poi questi ultimi per acquistare risorse.
- Decentralizzazione: sono contratti distribuiti e ad auto-esecuzione attraverso i nodi del network.

Gli Smart Contracts non rendono possibile nulla che prima non fosse possibile, semplicemente permettono a problemi comuni di essere risolti in una maniera tale che si minimizzi il bisogno di fiducia. Esempi di ciò possono essere una somma di denaro resa disponibile per un ragazzo al compimento della maggiore età oppure un'eredità resa subito disponibile per i parenti alla morte di una persona (il software scansiona i registri sulle morti e quando accerta la stessa sblocca i fondi).

1.7.2) Ethereum (proof-of-Stake e Smart Contracts)

Prima di passare alla descrizione dettagliata della piattaforma in oggetto è importante fare una precisazione. Quando parliamo di criptovalute sostanzialmente indichiamo con questo nome qualsiasi valuta virtuale, in realtà però vi è una distinzione tra le criptovalute definite come "Coin" e quelle definite "Token". Le prime sono indipendenti, nel senso che il loro funzionamento lo è, che queste non dipendono da nessun'altra criptovaluta o piattaforma bensì possiedono la propria Blockchain e operano all'interno di un network proprio. Per

quanto riguarda invece i Token[83], queste ultime non possiedono una propria piattaforma ma operano all'interno della Blockchain di un'altra criptovaluta indipendente (ossia di una Coin).

Ethereum è una piattaforma decentralizzata e un linguaggio di programmazione informatica sviluppata a partire dal 2013[84] dal canadese Vitalik Buterin[85]. Fondamentalmente è un'infrastruttura che permette di utilizzare qualsiasi tipo di Blockchain o protocollo come una piattaforma universale di sviluppo per creare proprie Bockchain e relative criptovalute.

Attraverso Ethereum il fondatore Buterin ha creato oltre ad una valuta virtuale (l'Ethereum appunto, identificata come Ether o ETH[86]) una piattaforma all'interno della quale si possono sviluppare applicazioni, software e Smart Contracts[87]. Il progetto Ethereum è infatti adatto all'utilizzo in molteplici ambiti e non limita le sue potenzialità di utilizzo per gli utenti alla realizzazione di determinate operazioni, bensì si configura come un protocollo che permette all'utente stesso di creare le proprie operazioni.

Per effettuare le transazioni all'interno del network si utilizza l'omonima valuta virtuale e tutti gli utenti che volessero sviluppare le proprie applicazioni o software all'interno dello

[83] Esempi di questo tipo sono le piattaforme Ethereum (che a breve si inizierà a trattare) e Neo sulle quali si basano vari "Token" come EOS, TRON, Ontology o VeChaiN. Ethereum e NEO sono esempi di criptovalute cosiddette "2.0" in quanto svolgono sia il ruolo di piattaforma che permette ad altre criptovalute di funzionare (i Token), sia hanno creato una valuta virtuale propria. A detta degli stessi sviluppatori l'Ether non è creato per competere con bitcoin, in quanto senza lo stesso non potrebbe esistere (le due criptovalute vengono definite complementari), inoltre ETH è definito come una "crypto-fuel", il cui scopo è quello di ripagare i partecipanti al network per il lavoro svolto, e non è pensato per essere utilizzato o considerato come una moneta, una risorsa, una quota partecipativa o qualsiasi altra cosa. (Fonte: "ethereum.org").

[84] Anche se la prima versione disponibile della stessa è datata febbraio 2014, successivamente aggiornata con nuovi linguaggi di programmazione basati sui codici Python, Go e Lisp. Per finanziare la creazione della piattaforma (in quanto si ricorda che all'epoca l'ideatore era solo un ragazzo ventenne) è stato utilizzato un sistema di pre-vendita (conosciuto come ICO, basandosi sulle somiglianze con l'Initial Public Offering, IPO) che permise la raccolta dell'equivalente a quasi 20 milioni di dollari in bitcoin.

[85] Programmatore di origini russe che tramite la piattaforma ha voluto espandere le potenzialità della Blockchain a 360° non limitandola alle sole criptovalute. Ad oggi la piattaforma è gestita da un gruppo di sviluppatori appartenenti alla Ethereum Foundation, una non-profit svizzera.

[86] A differenza delle altre criptovalute, quella sviluppata dall'omonima piattaforma non ha limiti di emissione e continuerà ad aumentare secondo uno schema prestabilito (non bisogna però escludere la possibilità che gli sviluppatori possano applicare qualche modifica in questo ambito al protocollo iniziale, come dichiarato di recente dallo stesso fondatore).

[87] Questi contengono funzioni di codice che gli permettono di interagire con altri contratti, "prendere decisioni", archiviare dati e inviare Ether (ETH) ad altri. Gli Smart Contracts sono definiti dai loro creatori, ma la loro esecuzione e, per estensione, i servizi che offrono, sono forniti dalla rete Ethereum stessa. Esisteranno e saranno eseguibili finché esiste l'intera rete, e scompariranno solo se fossero programmati per autodistruggersi. Informazioni tratte da: "ethereum.org".

stesso dovranno pagare agli sviluppatori una commissione per il servizio.
L'offerta totale di Ether non è limitata, come invece accade per Bitcoin; inizialmente (durante il cosiddetto "pre-selling") vennero creati 60 milioni di ETH per i contributori e 12 per il fondo di sviluppo (parte dei quali ora sono in possesso della Ethereum Foundation), in seguito, a partire dal 2015, la quantità di criptovaluta prodotta è stata limitata a 18 milioni all'anno (il 25% dell'offerta iniziale) sostanziandosi oggi in circa 100 milioni totali.

Sebbene anche Bitcoin supporti lo sviluppo degli Smart Contracts (notizia che potrà sorprendere molti), a differenza del sistema ideato da S. Nakamoto, Ethereum, pur utilizzando un meccanismo di Consensus basato sul Proof of Work (mining[88]), ne utilizza una variante, seppur molto simile, cosiddetta "memory-intensive[89]" invece che "processor-intensive", la quale non è basata sull'algoritmo SHA-256 bensì su EtHash (una versione modificata dell'algoritmo di Dagger-Hashimoto). La stessa piattaforma però si prefigge di implementare una nuova modalità di funzionamento per il protocollo definita "Proof of Stake" che prenderà il posto del Proof of Work. Il nuovo protocollo in oggetto, non del tutto integrato ad oggi[90] nel sistema, dipende da forze di mercato piuttosto che dalla potenza computazionale posseduta per mantenere la sicurezza del network, aumentando per un partecipante le chances di ottenere una ricompensa nel processo di mining in proporzione alle criptovalute già possedute dallo stesso. La logica sta nel fatto che più criptovalute possiederà un soggetto e più ampio sarà l'interesse dello stesso per il buon funzionamento e la sicurezza del sistema del quale queste sono proprie. Se infatti ci fosse un attacco (oltre ad essere molto costoso in termini economici, poiché comporterebbe l'acquisto di un determinato numero di valute virtuali, nello specifico il 50 + 1%) il risultato sarebbe un calo

[88] Ad oggi (luglio 2018) i minatori di Ethereum ricevono 3 ETH per ogni blocco minato e tra 0,625-2,265 ETH per blocco minato ma non aggiunto alla catena principale (prima della modifica apportata attraverso il "Bitzantine Update queste ricompense erano rispettivamente di 5 e 2-3 ETH). Un blocco in media è creato ogni 15 secondi.
[89] Questa "versione" basata sul Proof-of-Work viene definita memory intensive in quanto progettata per avere un tempo di verificabilità molto ridotto (15 secondi a blocco) all'interno di un ambiente a CPU lenta, che limita le performance dei partecipanti in termini di velocità, in quanto ogni 30.000 blocchi (circa 5 giorni) la struttura di dati della Blockchain Ethereum viene rigenerata tramite un codice (DAG) che limita quindi la "memory-brandwidth" (ossia la velocità di lettura dei dati) dei computer dei partecipanti al network, riducendo il possibile hash-rate di calcolo massimo raggiungibile dagli stessi. Ciò permette di ridurre i benefici per eventuali pool di miners in quanto il possesso di unità super veloci risulterebbe inutile.
[90] Il sistema presenta ancora alcuni svantaggi come la possibilità di subire attacchi a lungo raggio in cui la catena più lunga può essere sostituita dal blocco "genesi" e per questo è ancora in sviluppo. "D. LEE Kuo Chuen, R. H. DENG, Handbook of Blockchain, digital finance and inclusion – volume 2", Elsevier, 2018.

del valore della criptovaluta che comporterebbe una grave perdita per la stessa persona che l'avesse lanciato.

Il Proof of Stake ha il vantaggio di rendere sicuro il network senza bisogno di utilizzare la potenza computazionale (con il conseguente dispendio di risorse in termini di energia) come deterrente per eventuali attacchi e di abbassare le barriere all'entrata del sistema rimuovendo i benefici derivanti dall'uso di hardware specializzato (e costoso).

Nella seguente tabella si propone, come fatto precedentemente con Ripple, un confronto schematico tra i principali tratti caratteristici di Ethereum e quelli di Bitcoin, al fine di evidenziarne somiglianze e differenze strutturali:

CARATTERISTICHE	BITCOIN	ETHEREUM
METODO DI CONSENSUS	Proof of Work (eseguito dai Miners)	Proof of Work Nel breve periodo previsto switch in Proof of Stake
NUMERO DI UNITA' PRODOTTE	21 MILIONI. Termina nel 2041.	SENZA LIMITE (18 MILIONI l'anno più 72 MILIONI prodotti in pre-selling). Ad oggi in circolazione circa 103 MILIONI.
DISTRIBUZIONE CRIPTOVALUTA	Distribuita a coloro che validano le transazioni risolvendo il puzzle crittografico (Miners). Al momento la ricompensa è di 12,5 bitcoin per blocco minato.	Distribuita a coloro che validano le transazioni risolvendo il puzzle crittografico (Miners). Al momento la ricompensa è di 3 ETH per blocco aggiunto e tra 0,625-2,625 per blocco minato ma non aggiunto.

VELOCITA' TRANSAZIONI	Ogni 10 MINUTI circa viene creato un blocco. La singola transazione ha tempi variabili anche in base alle "fee" incluse.	Ogni 15 SECONDI viene generato un blocco.
PARTICOLARITA'	La criptovaluta più conosciuta e con la maggior capitalizzazione.	Possibilità di implementare Smart Contracts e di creare proprie Blockchain e Token.
NOTE	Definibile come vera e propria criptovaluta decentralizzata.	ETH creato come "Crypto-fuel", non allo scopo di sostituire la moneta.

CAPITOLO 2

“CRIMINALITA’ e DISCIPLINA ANTIRICICLAGGIO”

2.1) CRIMINALITA’ ED AMPIEZZA DEL MERCATO NERO

Le criptovalute sono uno dei più grandi mercati scarsamente regolamentati al mondo (probabilmente il più grande in assoluto). Sebbene queste ultime abbiano vari potenziali benefici, tra cui una maggior velocità ed efficienza rispetto a molti sistemi tradizionali di pagamento, al giorno d’oggi a farla da padrone sono le preoccupazioni che riguardano il loro uso nel commercio illegale (droghe, hacking e furti, pornografia illegale, armi), il potenziale per finanziare il terrorismo, riciclare denaro ed evitare il controllo sui capitali. Non c'è alcun dubbio riguardo al fatto che, fornendo un meccanismo di pagamento digitale e quasi completamente anonimo, le criptovalute abbiano facilitato la crescita dei mercati online "darknet" in cui vengono scambiati beni e servizi illegali.

Prima però di passare nel dettaglio all’analisi dei possibili scenari applicativi delle criptovalute come strumento che favorisce la criminalità e il riciclaggio di denaro, soffermiamoci un momento sulla capitalizzazione di mercato delle stesse, in modo da renderci conto dell’ampiezza del fenomeno. Ciò si rivelerà utile anche in seguito, quando ci addentreremo a parlare di regolamentazione all’interno di tale settore.
Ad oggi (1 ottobre 2018) la capitalizzazione del mercato delle criptovalute si attesta su un valore vicino ai 220 miliardi di dollari[91]. Queste cifre cambiano di giorno in giorno (basti pensare che nel gennaio dell’anno in corso la capitalizzazione di suddetto mercato aveva ampiamente superato quota 800 miliardi di dollari) dunque può risultare difficile comunicare in maniera esaustiva le dimensioni del fenomeno e anche i dati riportati di volta in volta devono considerarsi solo esemplificativi perché potrebbero essere stravolti

[91] Dato in tempo reale tratto da: “coinmarketcap.com”.

in brevissimo tempo. Tanto per fare un paragone, la capitalizzazione del mercato azionario italiano a giugno 2018 si attestava a 634 miliardi di euro[92] (ossia, dato il tasso di cambio del periodo di riferimento, circa 736 miliardi di $). A gennaio poi, quest'ultima era di 678 miliardi di euro (843 mld di dollari), valore che mostra come in quel momento il mercato delle criptovalute avesse una capitalizzazione paragonabile a quella di tutto l'azionariato quotato nel mercato italiano.

Di seguito viene riportata una tabella con le 13 principali criptovalute per capitalizzazione, che rappresentano circa l'85% dell'intero mercato, (che ricordiamo è formato da più di 2000 differenti criptovalute), alcune delle quali saranno trattate più nel dettaglio in seguito quando ci addentreremo a parlare del fenomeno del riciclaggio di denaro.

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	$111.443.338.823	$6.454,75	$3.882.502.001	17.265.312 BTC
2	Ethereum	$19.462.987.442	$190,95	$1.774.347.343	101.928.995 ETH
3	XRP	$10.817.724.365	$0,272399	$282.726.415	39.712.852.387 XRP *
4	Bitcoin Cash	$7.633.714.803	$440,09	$303.484.948	17.345.850 BCH
5	EOS	$4.543.073.552	$5,01	$563.011.072	906.245.118 EOS *
6	Stellar	$3.886.448.510	$0,206904	$75.892.469	18.783.810.227 XLM *
7	Litecoin	$3.107.495.473	$53,33	$294.861.746	58.270.456 LTC
8	Tether	$2.756.544.291	$1,00	$2.508.022.865	2.756.421.736 USDT *
9	Monero	$1.825.477.473	$111,29	$43.966.959	16.402.295 XMR
10	Cardano	$1.745.929.185	$0,067340	$89.012.300	25.927.070.538 ADA *
11	Dash	$1.594.122.266	$191,65	$208.861.662	8.317.763 DASH
12	IOTA	$1.577.128.582	$0,567408	$29.851.246	2.779.530.283 MIOTA *
13	TRON	$1.270.078.503	$0,019317	$110.066.069	65.748.111.645 TRX *

Figura 19: Capitalizzazione delle prime 13 criptovalute al giorno 1 ottobre 2018. Dati tratti da: "coinmarketcap.com".

[92] Dato ottenuto da "report ufficiale giugno 2018" di Borsaitaliana.

La capitalizzazione di mercato è data dal calcolo del numero di criptovalute in circolazione moltiplicato per il relativo prezzo (come si evince dalla relazione sottostante):

MC = N° x P

Con "MC" ad indicare appunto la capitalizzazione di mercato (Market Capitalization), "N°" il numero di criptovalute in circolazione e "P" il prezzo delle stesse.

Ora che si è sottolineata l'ampiezza del fenomeno, vediamo di soffermarci su alcuni dati riguardanti le attività criminali che vengono compiute tramite l'ausilio di questi nuovi strumenti.

Già da sola, la criptovaluta Bitcoin è coinvolta, a livello mondiale, in attività illegali per un valore di circa 72 miliardi di dollari all'anno[93], una cifra che si avvicina, per grandezza, al valore totale dei mercati statunitensi ed europei per le droghe. Tanto per avere un'idea della scala del fenomeno, un report dell'ufficio nazionale di controllo sulle droghe della Casa Bianca statunitense stima che gli utilizzatori di droga negli Stati Uniti nel 2010 abbiano speso una cifra complessiva che si aggira attorno ai 100 miliardi di dollari[94], mentre, seppur utilizzando metodi differenti, il centro Europeo per il Monitoraggio delle droghe e della tossicodipendenza (EMCDDA) ha stimato che in Europa, nel 2013, la spesa sia stata di circa 24 miliardi di euro (cifra che negli ultimi anni si stima in crescita fino a raggiungere il possibile valore di 31 miliardi di euro)[95]. Sebbene la comparazione dei dati non possa essere adeguatamente precisa in quanto il dato relativo alle spese illecite in bitcoin comprende oltre alle droghe (che restano comunque il fattore di impiego principale) altre attività criminali, mentre i dati sui mercati per così dire "reali" facciano solo riferimento al mercato

[93] Dato per l'anno 2017, riportato dalla ricerca di Foley S., Karlsen J., Putnins T., intitolata: "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", University of Sidney, Gennaio, 2018. Il gruppo di ricercatori però sottolinea anche il fatto che questo dato non dimostri (per ora) che le criptovalute stiano contribuendo ad alimentare mercati neri, ma sicuramente che forniscano un metodo di pagamento atto a favorire giri d'affari che prima erano svolti principalmente in contanti (al fine di dimostrare se questa innovazione tecnologica, facilitando l'accesso a beni illegali, ne possa favorire la crescita, serviranno ulteriori studi).

[94] Report preparato da RAND Corporation in: "How big is the U.S. market for illegal drugs?", 2014 (www.rand.org/t/RR534).

[95] La stima è stata fatta dall'European Monitoring Centre for Drugs and Drug Addiction/Europol all'interno del: "EU Drug Markets Report" per l'anno 2017 (http://www.emcdda.europa.eu/attachements.cfm/att_194336_EN_TD3112366ENC.pdf).

degli stupefacenti (ed a singoli paesi) e non siano stati aggiornati di recente, ciò permette comunque di capire quanto il mercato illegale online (e-market) si avvicini, per ampiezza in termini monetari, a quello più "tradizionale".

È importante poi considerare le differenze tra criptovalute e denaro: dopotutto, anche il denaro contante è in gran parte anonimo (rintracciabile eventualmente solo attraverso i numeri seriali) e pertanto ha tradizionalmente svolto un ruolo rilevante nell'agevolare la criminalità e il commercio illegale. La differenza fondamentale però sta nel fatto che le criptovalute consentono transazioni che oltre a presentare un elevato livello di anonimità, come potrebbe accadere per quelle effettuate tramite denaro contante, ne permettono l'esecuzione attraverso l'utilizzo di internet; queste ultime hanno perciò il potenziale per causare un'importante rivoluzione in come opera il mercato nero, spostando l'anonimato tipico delle operazioni effettuate via cash in un nuovo e-commerce illegale di ampiezza mondiale effettuato online.

2.2) IL DARKNET E LA SUA MICROSTRUTTURA

Il "Darknet" o "Dark Web" è una rete virtuale come internet, ma a cui è possibile accedere solo tramite particolari protocolli di comunicazione che garantiscono un maggiore anonimato rispetto alla rete "abituale". Il Darknet[96] contiene marketplace online, che assomigliano ad ebay o Amazon ma che si basano su comunicazioni anonime, le quali rendono questi mercati meno accessibili rispetto ai negozi online tradizionali. I mercati darknet sono perciò particolarmente popolari per lo scambio di beni e servizi illegali proprio perché le identità di acquirenti e venditori restano nascoste. Per accedere a un mercato darknet, un utente è generalmente tenuto a creare un account sullo stesso, in modo tale da poter poi accedere alla consultazione dei prodotti presenti e pubblicati dai rispettivi venditori.
Simile al modo in cui PayPal ha spinto lo sviluppo di ebay, la natura sicura, decentralizzata e tendente all'anonimato delle criptovalute ha avuto un ruolo importante nel successo dei mercati del dark web.

[96] Si stima che, il giro d'affari di questo mercato sommerso ammonti ad una cifra compresa tra 300 e 500 mila dollari al giorno, cifra che si mantiene di anno in anno in crescita. (Rapporto Clusit 2016).

Un utente che desidera acquistare beni o servizi su un mercato darknet, dopo essersi registrato nello stesso, dovrà acquisire una delle criptovalute accettate per il pagamento (in genere da un Exchange terzo) e quindi depositarla presso un indirizzo appartenente al mercato (definito "hot wallet") il quale gestirà i fondi come una sorta di deposito di garanzia. Questo sistema assiste anche gli amministratori del mercato nella mediazione delle controversie tra acquirenti e venditori e punta a ridurre al minimo le truffe in cui vengono raccolte somme di denaro senza che poi siano però spedite le merci.
In alcuni mercati i fondi vengono rilasciati quando il venditore indica che le merci sono state inviate, in altri addirittura fino a quando l'acquirente non comunica che i beni sono stati ricevuti.

L'evoluzione dei mercati neri consente ai venditori di beni e servizi illegali di raggiungere un pubblico globale portando ad una sorta di internazionalizzazione di questo tipo di commercio che richiede metodi sempre più complessi di comunicazione e logistica per evitare il rilevamento delle operazioni. A tal fine, gli acquirenti che effettuano un ordine ad un venditore online, comunicano utilizzando la crittografia PGP (Pretty Good Privacy), che codifica e decodifica i messaggi utilizzando una coppia di chiavi pubbliche e private. Su alcuni mercati (solitamente in quelli di più recente creazione), questa funzionalità è integrata nel sito web stesso. Logisticamente poi, gli articoli vengono in genere recapitati per posta tramite l'utilizzo di svariati metodi per ridurre al minimo la probabilità che tali consegne vengano intercettate dalle forze dell'ordine, includendo a tale scopo: loghi professionali, buste sottovuoto, invio di piccole quantità di prodotto volta per volta o tramite l'applicazione di indirizzi di ritorno falsi. Ai clienti viene inoltre consigliato, dagli stessi marketplace, di evitare di usare il proprio nome o indirizzo reali per minimizzare il rischio di essere rintracciabili.
Dopo aver ricevuto le merci, i compratori sono incoraggiati a rilasciare un feedback sul venditore, sulla qualità del prodotto ed in generale sul servizio complessivo. Questi feedback sono fondamentali per il venditore il quale necessita di crearsi una reputazione in suddetto mercato, elemento fondamentale in questo tipo di commercio basato principalmente sulla fiducia tra i partecipanti.

Al fine di consentire una connessione anonima e non tracciabile, per permettere l'accesso (che ovviamente può avvenire solo da remoto) a questi mercati, viene utilizzato il cosiddetto sistema di comunicazione TOR. Quest'ultimo, sviluppato inizialmente dalla Marina Militare statunitense, permette di offuscare le comunicazioni tra le controparti e gli indirizzi IP di connessione, facendo transitare i messaggi attraverso vari nodi nel network TOR in modo tale da far perdere le tracce degli stessi.

Situandosi per così dire al di sotto della rete ordinaria, la rete Tor è costituita da computer connessi ad internet su cui gli utenti hanno installato un particolare software applicativo; se un utente Tor vuole, per esempio, visualizzare in modo anonimo la prima pagina di un quotidiano online, il suo computer elabora una richiesta, strutturata su diversi livelli di crittografia e la trasmette ad un altro computer all'interno del network Tor, che viene selezionato casualmente. Questo computer, noto come "guardia", rimuoverà il primo livello di crittografia e inoltrerà la richiesta ad un altro computer, selezionato anche questa volta in modo casuale nella rete, il quale continuerà le operazioni facendo rimbalzare la richiesta tra differenti nodi del sistema.

L'ultimo computer della catena, definito "uscita", rimuove lo strato finale di crittografia, esponendo la vera destinazione della richiesta: il sito in oggetto. La guardia conosce l'indirizzo Internet del mittente e l'uscita conosce l'indirizzo Internet del sito di destinazione, ma nessun computer della catena conosce entrambi. Questo schema di routing, formato da un involucro di successivi livelli di crittografia, è ciò che dà nome alla rete che è appunto nota come " The Onion Router" (TOR).

2.2.1) Il caso Silk Road

La combinazione tra l'uso dei TOR per coprire le comunicazioni e delle criptovalute per i pagamenti, ha portato alla sempre maggiore proliferazione di questo tipo di mercati illegali, il più conosciuto dei quali era il cosiddetto "Silk Road", operativo a partire dal 2011. Il primo messaggio postato sul dark web che menzionava l'esistenza di questo sito risale al 27 gennaio 2011, quando, all'interno di un forum dedicato all'uso di droghe chiamato "Shroomery" un utente comunicò di essersi imbattuto in un sito il cui nome era appunto Silk Road; due giorni più tardi un altro affermò che quel sito poteva definirsi come un

Amazon.com anonimo[97]. Il fondatore di Silk Road, Ross William Ulbricht, per mascherare la propria identità utilizzava il nickname di "Dread Pirate Roberts" e nascondeva la propria posizione connettendosi alla rete da un Internet Café di San Francisco attraverso l'uso di un VPN (Virtual Private Network) per creare un falso indirizzo IP.

Ulbricht non era un hacker particolarmente abile, le sue prime versioni del sito infatti presentavano seri problemi di progettazione e sicurezza. Alla prima iterazione del sito poi, vendeva egli stesso le droghe, attività che gli permise di svilupparsi una reputazione nell'ambito, se così si può definire, del "servizio clienti". Inizialmente Ulbricht elaborava tutte le transazioni manualmente, senza addebitare commissioni e utilizzando la messaggistica per comunicare con acquirenti e venditori riuscendo in questo modo a crearsi un'ampia rete relazionale che gli permise di sviluppare successivamente un mercato completo.

Man mano che il sito si ingrandiva però, la sua struttura diventava inevitabilmente più burocratica. Appena gli fu possibile, lo stesso fondatore introdusse un sistema di classificazione automatizzato che consentiva ai venditori affidabili di acquisire una reputazione positiva all'interno del mercato tramite un sistema di feedback di valutazione sui venditori stessi e sulla merce acquistata. Ulbricht creò inoltre un forum di discussione in cui gli utilizzatori potevano condividere le proprie esperienze con clienti o venditori e i visitatori farsi un'idea della controparte con cui avrebbero potuto interagire. Questo meccanismo permetteva inoltre di poter espellere i venditori che si rendessero partecipi di frodi o che ingannassero i rispettivi clienti.

Per connettersi al sito di Silk Road, come abbiamo visto anche in precedenza nel paragrafo dedicato al darknet, era sufficiente utilizzare un software Tor ed essere in possesso dello strumento di pagamento designato: i bitcoin. Una volta all'interno della pagina Web ci si trovava di fronte ad un vero e proprio mercato online[98], che però basava la propria esistenza sulla vendita di prodotti illegali a partire da qualsiasi tipo di droga fino a materiale pornografico, documenti top secret, armi, identità digitali o carte di credito.

I pagamenti venivano gestiti da un sistema di deposito a garanzia automatico, in base al quale gli acquirenti potevano depositare fondi all'interno di un portafoglio gestito direttamente dal sito e rifiutarsi di pagare il venditore fino al momento dell'arrivo della

[97] L'FBI in seguito alle indagini ritiene che questi messaggi siano stati postati dallo stesso creatore e gestore del sito: il texano Ross William Ulbricht.

[98] Si stima che le visite giornaliere al sito fossero circa 60.000.

merce. Tuttavia, i venditori con una reputazione consolidata erano spesso in grado di ottenere un pagamento immediato da parte dei propri clienti (questo tipo di pagamenti veniva definito a finalizzazione anticipata).

Silk Road nella prima metà del 2012 generava un giro d'affari stimato in 1.2 miliardi di dollari, che in seguito all'ampliamento dell'offerta di prodotti, permetteva alla piattaforma ricavi annuali compresi tra 30 e 45 milioni di dollari[99].

Inizialmente vi era un numero limitato di nuovi account disponibili per i venditori i quali dovevano essere acquistati tramite un'asta; successivamente però venne addebitato un importo fisso per ogni nuovo account da venditore creato. Il sito inoltre tratteneva una commissione del 10% sulle transazioni, la quale diminuiva in base all'aumento della quantità acquistata.

Nonostante si fosse venuta a creare una competizione di mercato all'interno del sito tra i diversi venditori, quest'ultima non era garanzia di onestà: a volte infatti i commercianti approfittavano dei feedback positivi ricevuti per frodare i clienti, affermandosi come spacciatori di droga apparentemente affidabili, effettuando un gran numero di vendite quasi simultanee, ma chiedendo poi ai clienti di finalizzare il pagamento prima di ottenere la merce e scomparendo al momento dell'ottenimento dei pagamenti senza mai inviare la merce stessa. Dal momento che i truffatori utilizzavano pseudonimi e la rete Tor, proprio come chiunque altro all'interno del mercato, i clienti truffati potevano fare ben poco, se non sfogare la propria rabbia nei forum di discussione.

Inoltre i clienti risultavano vulnerabili anche perché dovevano fornire indirizzi postali ai venditori se volevano ricevere le consegne. Secondo le regole di Silk Road, i venditori avrebbero dovuto cancellare queste informazioni non appena la transazione fosse avvenuta, tuttavia, era impossibile per Ulbricht essere certo del rispetto di questa regola. Alcuni rivenditori hanno sistematicamente infranto questi principi[100].

Ciò creò un'ovvia vulnerabilità, anzi, una minaccia esistenziale agli affari di Ulbricht: se infatti fossero trapelati in massa i dati degli utenti, questi ultimi, perdendo la principale caratteristica garantita da quel tipo di mercato, ossia l'anonimato, sarebbero fuggiti in

[99] Dati forniti da "Forbes" 02/09/2013.

[100] A tal proposito uno di questi, Michael Duch, testimoniò durante il processo a Ulbricht, di aver mantenuto i nomi e gli indirizzi di tutti i suoi clienti in un unico foglio di calcolo.

massa dallo stesso. E così, quando un utente di Silk Road con lo pseudonimo di "Friendly Chemist" minacciò di fare proprio ciò, ossia di rivelare i dati di un gran numero di utenti, Ulbricht pagò 150.000 dollari ad un utente, che si pensava fosse un sicario, per organizzare l'omicidio del suo ricattatore, aggiungendo poi altri 500.000 $ per uccidere anche i soci di quest'ultimo.

Non è chiaro ad oggi, se qualcuno, sia realmente stato ucciso da qualcun altro, infatti sembra molto probabile che il tutto fosse una truffa in cui lo stesso Friendly Chemist e il suo presunto assassino erano associati (o addirittura la stessa persona). Tuttavia ciò segnò la fase finale di una straordinaria trasformazione: Ulbricht cominciò come un idealista, che si proponeva di costruire un mercato libero da ciò che descriveva come il "ladro omicida" dello stato e finì con il suo tentativo di proteggere con la forza ciò che aveva creato.

Il 2 ottobre 2013 le autorità statunitensi chiusero Silk Road ed arrestarono lo stesso fondatore con le accuse di associazione a delinquere per il traffico di stupefacenti, reati informatici e riciclaggio di denaro, punendolo poi con l'ergastolo.

Nelle figure successive sono raffigurati alcuni esempi dell'interfaccia web del sito in questione al fine di evidenziare le somiglianze e la semplicità d'uso dello stesso, che sembrano, come già abbiamo detto, accomunarlo ad un tradizionale negozio online.

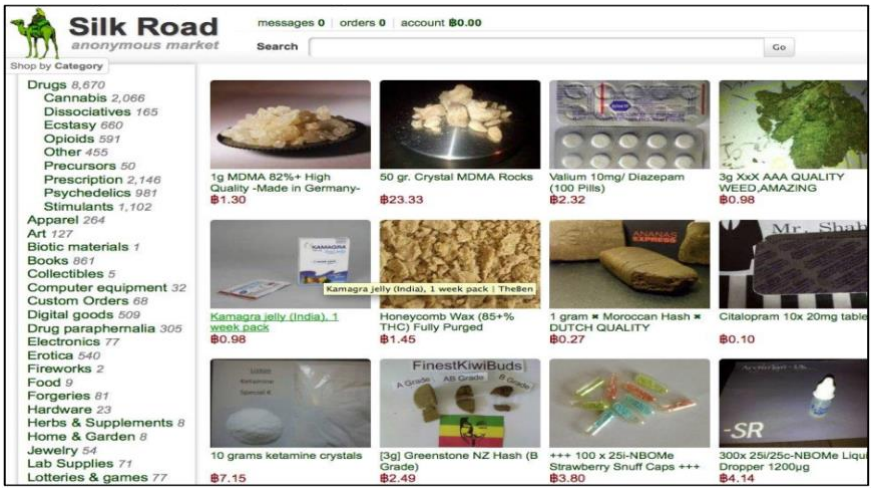


Figura 20: Esempio dell'Homepage di Silk Road dove acquistare un'enorme varietà di droghe. Immagini tratte da "Silkroaddrugs.org".

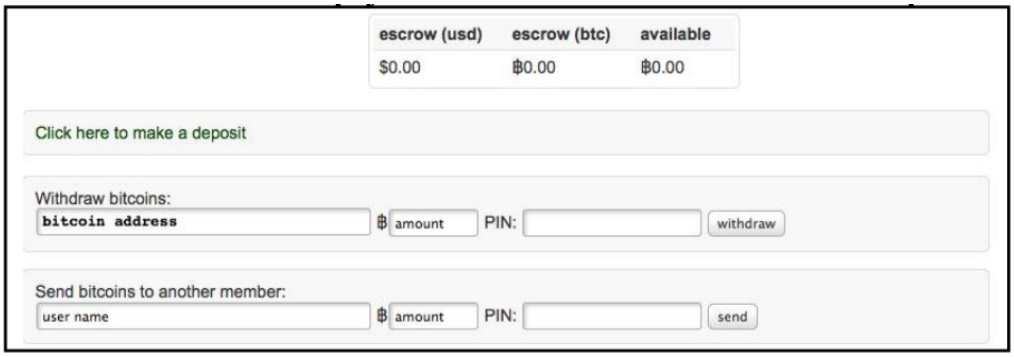


Figura 21: interfaccia del sistema pagamento del sito che raffigura il portafoglio di garanzia (hot wallet) e i dati richiesti per eseguire un pagamento in Bitcoin.

Figura 22: Esempio di informazioni riguardo ad una specifica merce (droga LSD) e al relativo venditore all'interno del mercato di Silk Road.

Nonostante la chiusura del sito Silk Road (ottobre 2013) ed un'azione congiunta di numerose agenzie governative internazionali, che prese il nome di "Operazione Onymous"[101] (novembre 2014), negli ultimi anni le transazioni nel dark web sono triplicate ed i rispettivi ricavi più che raddoppiati[102] attestandosi a fine 2016 tra i 10 e i 18 milioni di euro al mese.

Si sono succeduti a Silk Road una cinquantina di altri siti simili, tra i più famosi dei quali si riscontravano (o si riscontrano tutt'ora): Atlantis (chiuso a fine 2013), AlphaBay e Hansa Market (sequestrati dalle autorità governative nel luglio 2017), Dream Market (pare tuttora operativo) in aggiunta a nuove versioni di Silk Road (2.0, 3.0 e Silk Road Reloaded) gestite da alcuni utenti vicini a Ulbricht.

[101] L'operazione, eseguita il 6 novembre 2014 tramite la cooperazione delle agenzie governative degli Stati Uniti e di altri 16 paesi europei, ha portato a 17 arresti tra venditori ed amministratori che gestivano questi mercati online e alla rimozione di oltre 410 servizi nascosti. Inoltre, sono stati sequestrati bitcoin per un valore (all'epoca) di circa 1 milione di dollari, 180.000 euro in contanti, farmaci, oro e argento. Tra i più importanti mercati posti offline vi era Silk Road 2.0, il cui gestore è stato arrestato. Fonte: "Europol.Europa.eu" 07/11/14.

[102] Dati del Centro di Analisi Rand Corporation: "https://www.rand.org".

Dalle indagini è emerso poi che, al momento della chiusura di un mercato, gli utenti dello stesso si spostano in massa su un altro; ciò si va ad unire al fatto che all'aumentare dei mercati neri online disponibili aumentano le transazioni illecite ed anche il numero di utenti coinvolti in questo tipo di attività.

MERCATO	DATA INIZIO OPERATIVITA'	DATA CHIUSURA (o stato attuale)
Silk Road 1	**31/01/11**	**02/10/13**
Sheep	**28/04/13**	**29/11/13**
Black Market Reloaded	**30/06/11**	**02/12/13**
Agora	**03/12/13**	**03/12/13**
BuyItNow	**30/04/13**	**17/02/14**
Pirate Market	**29/11/13**	**15/08/14**
Pandora	**21/10/13**	**19/08/14**
Silk Road 2.0	**06/11/13**	**05/11/14**
Blue Sky Market	**03/12/14**	**05/11/14**
TorBazaar	**26/01/14**	**05/11/14**
Cloud-Nine	**11/02/14**	**05/11/14**
Topix 2	**25/03/14**	**05/11/14**
The Marketplace	**28/11/13**	**09/11/14**
Andromeda	**05/04/14**	**18/11/14**
Evolution	**14/01/14**	**14/03/15**
BlackBank	**05/02/14**	**18/05/15**
Mr Nice Guy 2	**21/02/15**	**14/10/15**
Middle Earth	**22/06/14**	**04/11/15**
Abraxas	**13/12/14**	**05/11/15**
East India Company	**28/04/15**	**01/01/16**
Silk Road Reloaded	**13/01/15**	**27/02/16**
Nucleus	**24/10/14**	**13/04/16**
Anarchia	**07/05/15**	**09/05/16**
Real Deal	**09/04/15**	**01/11/16**
AlphaBay	**22/12/14**	**13/07/17**
Dream Market	**15/11/13**	**Operativo**
Outlaw	**29/12/13**	**Operativo**
Tochka	**30/01/15**	**Operativo**
Valhalla (Silkkittie)	**01/10/13**	**Operativo**

Italian Black Market	**01/12/17**	**Operativo**
Zion	**N.D.**	**Operativo**
Olympus	**N.D.**	**Operativo**
Wall street market	**N.D.**	**Operativo**
The Majestic Garden	**N.D.**	**Operativo**
Crypto Market / Diabolus	**14/02/15**	**Pare non più operativo**
Darknet Heroes	**27/05/15**	**Pare non più operativo**

Figura 23: Report dei principali mercati neri del Web con le rispettive date di inizio operatività e di eventuale chiusura (se non ancora operativi) aggiornata al 15 settembre 2018 ed ordinata a livello cronologico.

Altri casi di utilizzo illecito delle criptovalute

Oltre al più conosciuto Silk Road, un altro caso eclatante di utilizzo delle criptovalute a fini illeciti fu quello di Liberty Reserve (ad oggi ancora il maggior caso di riciclaggio online mai realizzato). Nel maggio dello stesso anno in cui fu chiuso il sito di Ulbricht (2013) il Dipartimento di giustizia USA ha accusato tale società di aver concorso al riciclaggio di una cifra vicina a 6 miliardi di dollari di denaro proveniente da attività illecita. La società Liberty Reserve era stata costituita per "occuparsi di intermediazione mobiliare", in realtà però, dalla sua sede in Costa Rica, la stessa forniva supporto ad associazioni criminali al fine di riciclare denaro prodotto illecitamente da queste ultime. La società in oggetto vantava quasi un milione di clienti in tutto il mondo e risulta che abbia gestito all'incirca 55 milioni di transazioni a sfondo illegale attraverso l'emissione di una propria valuta virtuale chiamata "Liberty Dollar". Inoltre, ai clienti della stessa veniva richiesto di effettuare prelievi e depositi servendosi di Exchange terzi e fidati, situati in paesi sprovvisti di qualsiasi presidio antiriciclaggio. Una volta creato il proprio account, al cliente era permesso effettuare qualsiasi tipo di transazione in svariati paesi utilizzando i propri Liberty Dollar. (La chiusura del sistema ha richiesto la cooperazione di ben 18 giurisdizioni).

Degno di nota è anche il caso più recente del cittadino russo Alexander Vinnik, arrestato nel luglio 2017 con l'accusa di aver utilizzato la piattaforma BTC-e[103] per riciclare 4 miliardi di dollari derivanti da evasione fiscale, narcotraffico e furti informatici.

[103] Intermediario mobiliare estero che si occupava (ad oggi ridulta chiusa) del cambio tra criptovalute e valute tradizionali. "https://btc-e.com/index.html".

Infine è bene ricordare che negli ultimi anni si è registrato un utilizzo sempre maggiore delle criptovalute anche nell'ambito dei cosiddetti "attacchi Ransomware" ossia attacchi informatici che consistono nella diffusione di un virus che permette di criptare i dati dei dispositivi terzi colpiti e tramite i quali i criminali chiedono alle vittime un riscatto da pagare in bitcoin o simili in cambio dei codici di decriptazione. Il caso che ha fatto più scalpore in questo ambito è stato sicuramente quello denominato "WannaCry" che ha colpito su scala mondiale centinaia di migliaia di computer con sistema operativo Windows nel maggio 2017[104].

2.3) ANONIMATO INSITO NELLE CRIPTOVALUTE

I bitcoin, cosi come le altre criptovalute esistono in uno stato di tensione tra l'anonimato[105] (nel senso che le identità reali non sono necessarie per l'utilizzo del sistema) e la tracciabilità (in quanto tutte le transazioni sono registrate sulla Blockchain). Tuttavia, proprio poiché tutte le transazioni sono memorizzate pubblicamente all'interno di un registro, questo anonimato (o come spesso viene definito: "pseudo-anonimato") di un utente si basa sul fatto che lo pseudonimo che lo stesso utilizza all'interno del network non venga collegato alla sua vera identità. L'anonimato intrinseco nelle criptovalute, non si sostanzia solo in una riservatezza a livello personale, ma anche a livello di impresa (senza quest'ultimo la Blockchain potrebbe rivelare facilmente flussi di cassa e altri dettagli finanziari delle stesse imprese eventualmente operanti nel network).

Negli ultimi anni poi, per mascherare la propria identità, oltre ad utilizzare reti di connessione TOR, gli utenti fanno ricorso ai cosiddetti "mixing services" (o "tumbler") e ad operazioni di "wash trades" in modo tale da alterare l'indirizzo dei bitcoin posseduti incrementando la difficoltà per eventuali terzi nel tracciare le loro attività. Il tumbling, nella sua forma più semplice, coinvolge un utente che invia una determinata quantità di bitcoin (o altra criptovaluta) ad un tumbler provider, il quale in cambio di una piccola tassa, restituisce la somma ad un indirizzo differente da quello con cui l'utente li ha inviati. Le

[104] Tra i sistemi infettati ci sono stati anche quelli di importanti società come Portugal Telecom, FedEx, L'università di Milano-Bicocca, Telefonica, la casa automobilistica Renault e altri.

[105] Si parla di anonimato quando un'entità, all'interno di un gruppo/ambiente formato da diversi partecipanti, si mantiene non tracciabile. "Anonymity of Bitcoin Transaction: An Analysis of Mixing Services" University of Munster 2013.

Wash Trades invece vengono compiute direttamente dall'utente che invia criptovalute da un indirizzo ad un altro che però egli stesso controlla.
Questi servizi possono essere percepiti come strumenti di riciclaggio di denaro anche semplicemente leggendo i nomi, per così dire suggestivi, di alcuni di questi come ad esempio "BitLaundry" o "Bitcoin Fog". La motivazione principale che spinge a fornire questi servizi sta nel fatto che gli utilizzatori pagheranno una commissione ai provider (che verrà decurtata dalla somma iniziale al momento della restituzione della stessa). Queste fee dipendono dal tipo di mixing e possono essere fisse oppure variabili.
Di seguito le principali caratteristiche di alcuni dei più importanti tra questi servizi:

• **Helix:** il maggiormente conosciuto ed utilizzato, creato nel giugno 2014 dal motore di ricerca per il darkweb "Grams", offre la funzionalità di effettuare transazioni in modo anonimo, per le quali richiede una commissione del 2,5%, stabilendo che queste ultime abbiano una dimensione minima di 0,2 BTC e una massima di 21 BTC e originando un flusso di ritorno per il cliente in meno di 30 minuti.

• **Bitcoin Fog** è un servizio di mixing accessibile solo tramite Tor. Permette di generare fino a 5 indirizzi per il deposito di bitcoin e richiede una commissione (casuale) tra l'1 e il 3% del valore della transazione. I bitcoin possono essere prelevati da un massimo di 20 indirizzi differenti e rinviati in un intervallo di 6-96 ore, con un importo minimo che deve essere di almeno 0,2 BTC.

• **BitLaundry** è un semplice servizio di mixaggio, che, a differenza ad esempio di Bitcoin Fog, non consente di depositare bitcoin in un portafoglio virtuale. Gli indirizzi di destinazione, il numero di transazioni in uscita ed un intervallo di tempo devono invece essere specificati. Per ogni transazione viene generato un indirizzo monouso a cui l'utente deve inviare almeno 0,25 BTC. La commissione di mixaggio per BitLaundry è costituita da due parti. La prima consiste nel 2,49% del totale, la seconda in 0,00249 BTC per transazione in uscita.

Tutti questi servizi però presentano il rischio che l'operatore stesso sia un hacker o collabori con uno, portando il cliente ad affrontare la possibilità di subire il furto delle proprie

criptovalute[106]. Per ridurre questo rischio, sarebbe possibile combinare l'uso di una serie di questi servizi in una sorta di effetto cascata inviando a ciascuno degli stessi una piccola quantità di ricchezza. Tuttavia, ciò comporta un ulteriore dispendio di tempo oltre che il pagamento di commissioni più elevate.

Se per quanto riguarda alcune criptovalute questi servizi di tumbler vengono forniti da operatori terzi, per altre gli stessi sono direttamente incorporati nel protocollo di funzionamento: è il caso ad esempio di Monero, DASH, ZCash, Verge e NAV. Vediamone rapidamente i tratti caratteristici che rendono queste ultime le "criptovalute più anonime":

- **Monero (XRM)**: creata il 18 aprile 2014 da Fransisco Cabañas e Riccardo Spagni, Monero, basa la propria fortuna sullo slogan di offerta di sicurezza, privacy e non tracciabilità. La criptovaluta infatti è appositamente progettata per risolvere il problema della tracciabilità tipico dei sistemi Peer-to-Peer pubblici. Nel network Monero la Blockchain è si pubblica ma non permette di identificare i dettagli relativi agli indirizzi di invio e ricezione delle transazioni, offuscandoli, così come gli importi delle stesse. Per il resto la struttura è molto simile a quella del protocollo Bitcoin, con una produzione di criptovaluta limitata (18,4 milioni) e un meccanismo di consensus basato sul Proof of Work. Gli stessi principi vengono utilizzati anche da **ZCash** per garantire la privacy tramite il suo algoritmo "Zero-Knowledge SNARK".

- **DASH**: introdotta nel gennaio 2014 da Ryan Taylor, DASH si caratterizza per il fatto di presentare due differenti figure che regolano il network: da un lato infatti riscontriamo i Miners (meccanismo di consenso basato sul PoW), come avviene nella rete Bitcoin, dall'altro però si presenta una nuova figura ossia quella dei cosiddetti "Masternodes". Questi ultimi hanno il compito di svolgere le operazioni opzionali offerte agli utenti dalla piattaforma: tra queste vi è la possibilità di effettuare transazioni in totale anonimato (definite "Private Send") che funzionano tramite un meccanismo simile a quello messo in atto dai servizi di mixaggio, ossia

[106] Ciò ad esempio accadde nel 2017 quando una versione fake del tumbler Helix riuscì a sotrarre le criptovalute degli utilizzatori.

facendo inviare al cliente una certa somma ad un indirizzo scelto casualmente tra quelli dei partecipanti a questo servizio e successivamente inviandola alla controparte tramite un differente indirizzo in modo tale da occultarne la tracciabilità. Le unità di criptovaluta prodotte dal sistema Dash saranno 18,9 milioni (la remunerazione per la creazione di un blocco viene distribuita per il 90% in misura eguale a Miners e Masternodes mentre il restante 10% rimane depositato in un fondo di proprietà della piattaforma). A differenza di Monero, la Blockchain di DASH è pubblica, elemento che avvicina la piattaforma maggiormente al concept di quella Bitcoin.

- **Verge (XVG):** fondata tramite Initial Coin Offering[107] nel 2014, la piattaforma Verge permette agli utenti di occultare i propri indirizzi IP integrando direttamente nel proprio protocollo un sistema di navigazione Tor che si unisce ad uno I2P[108] tramite il cosiddetto "Wraith Potocol". La Blockchain di Verge è pubblica ma grazie all'ausilio dei sistemi citati precedentemente, permette di mantenere l'anonimato dei propri utenti così come di nascondere la location dalla quale operano. La quantità totale di XVG prodotti sarà di 16.5 miliardi.

- **NAV**: L'ultima piattaforma che trattiamo, NAV (fondata nel 2014), si differenzia dalle precedenti per il fatto che il protocollo che la costituisce è basato sul meccanismo di Proof of Stake. Al fine di garantire l'anonimato il sistema abilita

[107] Le ICO sono una forma di finanziamento, utilizzata da startup o da soggetti che intendono realizzare un determinato progetto, resa possibile tramite la tecnologia. In estrema sintesi, per reperire dei finanziamenti si propone al pubblico (normalmente tramite il *cd. "whitepaper"*) un progetto che sarà realizzato tramite Blockchain con creazione di "Token" da cedere, a fronte di un corrispettivo, ai soggetti finanziatori. "Blockchain4innovation.it".

[108] I2P: "Invisible Internet Protocol" che permette, con un meccanismo simile a quello implementato nel Tor, di godere di una connessione anonima.

l'utilizzo di una seconda Blockchain, definita "Subchain" che permette di far perdere le tracce del collegamento tra le parti coinvolte in una transazione.

Nella tabella sottostante si riporta un riepilogo schematico in merito alle caratteristiche delle 5 criptovalute descritte:

CRIPTOVALUTA	Monero	ZCash	DASH	Verge	NAV
Consensus Method	PoW	PoW	PoW	PoW	PoS
N° totale cripto. da emettere	18,4 MILIONI	21 MILIONI	18,9 MILIONI	16,5 MILIARDI	/
Metodo Occultamento	Dati controparti e importi offuscati	Dati controparti e importi offuscati	Masternodes	TOR e I2P	Subchain
Transazioni su Blockchain	Private-Pubbliche (a scelta dell'utente)	Private-Pubbliche (a scelta dell'utente)	Pubbliche	Pubbliche	Pubbliche
Offuscamento IP	No	Si	Si	Si	Si

A quanto detto si aggiunge il fatto che molto spesso le disponibilità in criptovalute vengano scambiate tra gli attori coinvolti in una transazione (soprattutto se questa è di origine illecita) tramite lo scambio diretto in presenza fisica. Come si è visto infatti, data la possibilità di memorizzare gli indirizzi corrispondenti ad una certa quantità di criptovaluta in un supporto mobile (quale smartphone, tablet o strumenti appositamente creati simili a

speciali chiavette USB), questi ultimi risultano scambiabili in maniera diretta e senza lasciare nessun tipo di traccia sulla Blockchain. Sicuramente tra tutte le forme viste fino ad ora, questa risulta la più anonima e difficile da rintracciare. Allo scopo di favorire tale pratica, negli ultimi anni si è assistito alla diffusione di siti internet e piattaforme specializzati (tra gli altri servizi) nell'organizzare incontri personali per concludere transazioni in criptovaluta tramite lo scambio di supporti elettronici portatili. Tra questi il più rilevante a livello di utenti risulta essere "localbitcoins.com", attivo in quasi 250 nazioni tra cui l'Italia e che offre oltre alla possibilità di organizzare incontri diretti in più di 15.000 città, anche quella di acquistare/vendere direttamente online la quantità di criptovaluta desiderata tramite quasi 60 diversi metodi di pagamento (tra cui bonifici bancari, acquisti tramite PostePay e altri). La piattaforma inoltre fornisce addirittura un metodo di sicurezza antifrode per i pagamenti online mantenendo le disponibilità in criptovaluta in un apposito wallet custodito nella rete.

2.3.1) Tecniche di "mitigazione" dell'anonimato

Sebbene le criptovalute si siano rivelate uno strumento utile a favorire il commercio illegale, secondo alcuni (Koshy, McDaniel, 2014) la natura pubblica delle transazioni salvate nella Blockchain renderebbe possibile il tracciamento degli indirizzi IP degli utilizzatori illegali. Una transazione infatti coinvolge solitamente più indirizzi di un unico utilizzatore, per esempio colui che paga in bitcoin potrebbe inviare gli stessi attraverso l'utilizzo di indirizzi multipli e ricevere il resto dell'operazione in un nuovo indirizzo. Poiché un utente deve essere in possesso della chiave privata di ogni indirizzo da cui le criptovalute sono inviate in una data transazione, tutti gli indirizzi che inviano valuta in quella determinata transazione possono essere associati ad un solo utilizzatore; a questo si può giungere tramite l'ausilio di un algoritmo chiamato "Union Find Algorithm" che consiste in una struttura di dati che è in grado di tracciare un insieme di elementi frazionati in molteplici transazioni apparentemente disgiunte per risalire ad un eventuale collegamento tra loro. Supponiamo che si osservino due transazioni separate, una nella quale il pagamento in bitcoin viene inviato dagli indirizzi A e B ed un'altra in cui quest'ultimo è inviato dagli indirizzi B e C. Se l'algoritmo identifica gli indirizzi A e B della prima transazione come appartenenti ad un solo utente, e quelli della seconda (B e C) come appartenenti allo stesso

utente si potrà stabilire, per transitività, che tutti e tre gli indirizzi (A, B e C) appartengono a quel determinato utilizzatore.

Anche se si riuscisse però, come anticipato nel precedente paragrafo, a risalire agli esecutori di determinate operazioni nella rete, come si potrebbe individuare quali delle stesse hanno natura illecita, e quindi di conseguenza, quali indirizzi bitcoin sono posseduti da utilizzatori coinvolti in tali attività?

Secondo un interessante metodo utilizzato dall'Università di Sidney[109], si possono utilizzare 3 differenti approcci per stabilire, perlomeno inizialmente, un campione di utenti illeciti da utilizzare poi per trarre conclusioni più ampie ed approfondite:

A. Bitcoin sequestrati da agenzie governative: attraverso gli indirizzi bitcoin[110] sequestrati o le transazioni illegali (data, ora ed importi) scoperte nell'ambito di operazioni delle forze governative è possibile risalire agli utilizzatori illeciti associando gli indirizzi o gli identificativi delle transazioni ai dati contenuti nella Blockchain. (Ad esempio si possono ottenere i dati riguardanti gli indirizzi bitcoin nel momento in cui le entità governative mettono gli stessi all'asta dopo averli sequestrati).

B. "Hot wallet[111]" dei mercati illegali darknet: tramite i wallet centrali posseduti dai marketplace illegali in cui gli utenti depositano o prelevano i fondi nell'ambito di operazioni di compravendita, si possono identificare gli utenti che operano all'interno di un determinato mercato darknet. Questa operazione si può realizzare registrandosi nel rispettivo mercato e ottenendo di conseguenza l'indirizzo su cui depositare i propri fondi per operare; così facendo, dopo aver ottenuto l'indirizzo

[109] Foley S., Karlsen J., Putnins T., "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" University of Sidney, gennaio 2018.
[110] Si possono ottenere gli indirizzi Bitcoin ad esempio nel momento in cui le entità governative mettono gli stessi all'asta dopo averli sequestrati
[111] Un hot wallet è un portafoglio contenente criptovalute – nel caso di quelli a disposizione degli exchanges, condiviso tra più utenti – che è connesso ad internet e permette il deposito, il prelievo ed il trading delle monete digitali a cui è destinato. Gli exchanges affiancano solitamente ad esso un cold wallet, sconnesso dalla rete e protetto da maggiori misure di sicurezza, destinato a custodire i fondi in deposito a lungo termine. (Rapporto_Clusit_2018_MI).

del wallet centrale, si può risalire agli utenti che hanno operato su quel portafoglio ed identificarli come illeciti, sempre tramite l'ausilio delle informazioni registrate all'interno del ledger pubblico.

C. Utenti identificati in forum del darknet: come ultima possibilità elencata nella ricerca vi è quella di utilizzare le informazioni contenute nel dark web. Infatti, soprattutto attraverso l'utilizzo dei forum presenti nello stesso, si possono identificare utenti che non erano stati individuati con i due precedenti approcci. Ciò diventa possibile poiché nei suddetti forum, gli utenti sono soliti pubblicare gli indirizzi Bitcoin dai quali hanno subito frodi, o in riferimento ai quali lasciano un feedback (positivo o negativo che sia) riguardo ad una transazione avvenuta con la controparte che li possiede.

I dati riepilogativi ottenuti dagli studiosi sono presentati nella successiva tabella (*Figura 24*):

Group / Subgroup	Users	Transaction Count (Mil)	Holding Value ($Mil)	Number Of Addresses (Mil)	Volume ($Bil)
1. All Users	106,244,432	605.69	2,964.66	221.71	1,862.51
	(100.00%)	(100.00%)	(100.00%)	(100.00%)	(100.00%)
2. Observed Illegal Users	6,223,337	196.11	1,342.43	58.38	241.46
	(5.86%)	(32.38%)	(45.28%)	(26.33%)	(12.96%)
2A. Seized Users	1,016	23.83	9.39	8.30	17.51
	(0.00%)	(3.93%)	(0.32%)	(3.74%)	(0.94%)
2B. Black Market Users (not in 2A)	6,221,873	157.30	1,324.32	49.71	220.91
	(5.86%)	(25.97%)	(44.67%)	(22.42%)	(11.86%)
2C. Forum Users (not in 2A or 2B)	448	14.98	8.72	0.38	3.03
	(0.00%)	(2.47%)	(0.29%)	(0.17%)	(0.16%)
3. Other Users	100,021,095	409.58	1,622.23	163.33	1,621.05
	(94.14%)	(67.62%)	(54.72%)	(73.67%)	(87.04%)

Figura 24: Tabella riassuntiva degli utenti illeciti classificati secondo I 3 metodi precedentemente citati. Tratto da: Foley S., Karlsen J., Putnins T., "Sex, drugs, and bitcoin: "How much illegal activity is financed through cryptocurrencies?" University of Sidney, gennaio 2018.

Sempre facendo riferimento allo studio dell'università di Sidney, si può vedere che gli utilizzatori illegali sono sempre stati presenti nel network fin dalla sua creazione nel 2009,

con dei picchi nel periodo 2012 – 2015, anni che coincidono con la crescita molto rapida di svariati mercati neri.

Se attraverso i 3 metodi precedentemente esposti era risultato che il campione di utenti illeciti riscontrato era del 5,86%[112] sul totale (vedasi *Figura 24*) è sorprendente vedere che, utilizzando questo campione all'interno di metodi matematici più complessi, gli studiosi dell'Università di Sidney hanno ottenuto una percentuale di utenti coinvolti in attività illecite che è pari al 25.24 % sul totale[113] e corrisponde a circa 27 milioni di utenti. Questo risultato, deriva dall'utilizzo di due differenti metodi di analisi: in primis una variante dell'algoritmo Smart Local Moving (SLM)[114], strumento matematico che funziona analizzando la modularità della struttura dei nodi di un network intercambiandoli tra loro al fine di rilevare "gruppi" di utenti dalle caratteristiche, dall'operatività simile o che interagiscono tra loro. In particolar modo, assegnando all'algoritmo come "illeciti" il campione di utenti rilevati, quest'ultimo è in grado di riscontrare ulteriori utenti che in precedenza non era stato possibile individuare grazie alle eventuali interazioni di questi ultimi con i precedenti. Il secondo metodo utilizzato è invece il modello Detection Controlled Estimation (DCE)[115] che sfrutta le differenze comportamentali tra utilizzatori legali ed illegali per identificare in maniera probabilistica la popolazione di utenti illeciti all'interno del network.

Per di più lo studio compiuto mostra che 269 milioni di transazioni ossia il 44.33% del totale sono di natura illecita. Questi numeri vengono però attenuati dal fatto che negli ultimi anni c'è stato l'ingresso nel mondo delle criptovalute (e soprattutto in questa analisi, nel network Bitcoin) di molti utenti "onesti", in quanto nei primi anni la percentuale di utenti dediti ad attività illecita era compreso tra il 60 e l'80% del totale.
Normalmente gli utenti illegali tendono a compiere più transazioni (in media il doppio o il triplo) degli utenti leciti, di importo minore (circa la metà rispetto all'importo medio delle

[112] I dati in analisi considerano il periodo che va dalla prima transazione avvenuta in Bitcoin il 3 gennaio 2009 ad aprile 2017. Questi ultimi sono stati estratti dalla Blockchain pubblica di Bitcoin (ex Blockchain.info ora con nuovo dominio Blockchain.com).
[113] il campione totale di utenti Bitcoin analizzato è di 106.244.432, numero che è stato ottenuto eliminando dal totale 83 exchanges (per non considerare nel calcolo delle transazioni quelle di conversione tra Bitcoin e moneta avente corso legale e 28 miners (i principali, in quanto il loro ruolo è quello di fornire conferma delle transazioni). Il totale degli utenti analizzati movimenta all'incirca 606 milioni di transazioni per un controvalore di 1,9 miliardi.
[114] Sviluppato da Waltman e Van Eck (2013).
[115] Metodologia sviluppata ad inizio anni '90 da Feinstein.

transazioni che si attesta sui 5.000 dollari), spesso ricorrenti con le stesse controparti e possedendo di volta in volta piccole quantità di bitcoin, in modo tale da ridurre al minimo le perdite in caso di confisca, a differenza degli utenti legali che tendono a detenerne maggiori quantità per ragioni di investimento o speculazione.
Gli utenti illeciti poi, soprattutto i venditori, tendono, seppur interagendo spesso con le stesse controparti (maggior concentrazione), ad operare con un maggior numero di queste ultime in totale, fattore che evidenzia il loro elevato numero di transazioni. Inoltre questi ultimi si caratterizzano spesso per un "Existance Time" prolungato all'interno del network, ossia un tempo di permanenza tra la prima e l'ultima transazione superiore rispetto agli altri utenti, il che indica il loro coinvolgimento per così dire "senior" nel sistema Bitcoin.

In generale, come si è già detto, durante tutto l'elaborato, si è fatto (e si farà) riferimento al Bitcoin come principale strumento per effettuare i pagamenti nell'ambito delle Blockchain e in relazione al compimento di attività illecite, bisogna però porre in evidenza che nella scelta dello strumento con cui concludere commerci illegali solitamente vi è un incremento nell'utilizzo di Bitcoin quando nel mercato vi è un numero ridotto di altre criptovalute che presentano maggiore opacità e quando vi è un minore hype attorno a Bitcoin stesso[116]. Perciò pur essendo tuttora tale criptovaluta la più diffusa in generale (rappresentando da sola, tra le più di 2.000 criptovalute esistenti, più del 52% del mercato) negli ultimi tempi si è avuta una crescita nell'utilizzo di altre tipologie di valute virtuali, sia grazie alla loro crescente popolarità (Ethereum) che per la loro maggiore riservatezza e opacità (come abbiamo visto ad esempio per Monero, Dash o Zcash tra le altre).
Il fatto che le criptovalute siano utilizzate maggiormente come strumento di pagamento in operazioni di compravendita di beni dagli utenti illeciti e come strumento di investimento o speculazione dagli utenti leciti, dovrebbe far riflettere sulle vere funzionalità che queste intendono assolvere e sul fatto che, senza dubbi, possano favorire il riciclaggio di denaro derivante da attività non legali per poi rimetterlo in circolo nel sistema reale una volta convertito in moneta fiat[117].

[116] Misurato in base all'intensità nella ricerca della parola Bitcoin nel motore di ricerca Google.
[117] Per moneta fiat si intende la moneta su cui sono basate le tipiche economie moderne, la quale non è garantita o scambiabile in alcuna merce, viene messa in circolazione da un governo (con un valore di scambio che dipende direttamente dall'economia nazionale e dalle politiche economiche dell'istituzione che la ha emessa) e non ha alcuna limitazione di emissione. Nello specifico la moneta a corso legale è una forma di moneta fiat ed è a corso legale in quanto risulta fungibile, trasferibile, divisibile e riconoscibile. S. Capaccioli: "Criptovalute e Bitcoin: un'analisi giuridica". Giuffrè Editore, 2015.

Seppur alcuni sostengano che ad esempio la vendita di droghe tramite il dark web possa in qualche modo essere un vantaggio in quanto in ogni caso quest'ultima sarebbe venduta per le strade aumentando la violenza e il degrado (Barratt et al. 2016) o che basandosi sui feedback la qualità delle sostanze sarebbe migliore "danneggiando un po' meno" i consumatori (Soska et al. 2015) è altrettanto vero che il fenomeno criptovalute potrebbe finire solo per incrementare il compimento di attività illegali, rendendo tali prodotti più accessibili e convenienti, riducendo il rischio nel rispettivo commercio (grazie al maggiore anonimato per compratori e venditori). In aggiunta, se una delle funzionalità intrinseche delle criptovalute, che è quella di strumento di pagamento, è sostenuta dal fatto che queste ultime siano utilizzate per scambi illegali, di conseguenza una componente che conferisce valore alle stesse pare proprio derivare dal loro uso in questo tipo di commercio. Ciò dovrebbe portare a scoraggiare tutti quegli investitori socialmente responsabili (così come già abbiamo visto per il caso del Bitcoin nei consumi eccessivi di energia dovuti al mining) ad investire nelle stesse.
Non bisogna poi dimenticare che, una eventuale maggiore attenzione delle autorità su Bitcoin, o una proliferazione di un gran numero di valute più opache potrebbe portare a diminuirne il valore, dal momento che gli scambi illeciti si svolgerebbero con altre famiglie di cryptocurrencies.

Dalle considerazioni fatte fino ad ora emerge che l'anonimato insito nelle criptovalute si può dunque considerare inferiore a quello garantito dal contante (anche se superiore a quello pressoché nullo di carte di credito o bancomat) in quanto nonostante l'utilizzo di pseudonimi e il crescente sviluppo di servizi che garantiscono maggiore anonimato, vi è la possibilità, seppur ridotta, di riuscire ad individuare indirizzi appartenenti a persone che svolgono attività illecite.

2.4) NATURA GIURIDICA DELLE CRIPTOVALUTE

L'introduzione del concetto di criptovaluta pone problemi d'inquadramento da un punto di vista giuridico per il fenomeno, dovuti al fatto che le stesse abbiano natura virtuale,

polimorfa[118], ibrida (poiché rispondono a varie esigenze), anonima (presumibile o meno) e ubiqua. Sapendo che in letteratura economica non vi è una corrente di pensiero unanime che considera o meno le criptovalute come equiparabili a moneta avente corso legale, proviamo a vedere all'interno di quale "categoria giuridica" si potrebbero inserire Bitcoin e le sue implementazioni alternative.

Il concetto economico di "Moneta"

All'inizio della trattazione è stata presentata la differenza tra valuta digitale e virtuale, proviamo ora però a chiederci cosa rende una valuta (ossia una unità di scambio) uno strumento uniformemente accettato come "moneta".

Gli economisti solitamente sostengono che la moneta per essere tale, debba possedere le tre seguenti caratteristiche: unità di conto, mezzo di scambio e riserva del valore.

Mezzo di scambio

Una delle principali funzioni di ogni moneta è quella di strumento di intermediazione negli scambi di beni e/o servizi.

Si possono identificare varie caratteristiche delle criptovalute come mezzo di scambio che differiscono sostanzialmente dalle valute tradizionali: in primis i costi di transazione nelle operazioni effettuate attraverso queste ultime, i quali risultano minori rispetto a quelli degli attuali sistemi di pagamento e che fungono solo da copertura per il mantenimento del sistema (ad esempio nel caso del Bitcoin per ricompensare i Miners); non ci sono costi legati a terze parti o intermediari. Per le valute tradizionali invece oltre ai costi di produzione, si aggiungono quelli di autenticazione, trasporto, sorveglianza (anche se nel caso dei Bitcoin dovremmo considerare come costo anche quello legato al consumo di energia). Le possibilità di crescita come mezzi di scambio per le criptovalute si riscontrano anche nella loro maggiore anonimità e trasparenza che permettono a chiunque di seguire la catena di transazioni ma non sempre di sapere la vera identità di chi le ha compiute (questo però come abbiamo già visto è anche il principale problema a fini antiriciclaggio e di lotta alla criminalità).

[118] Con polimorfa si intende la capacità adattiva delle criptovalute a varie esigenze (come emerge anche dalla stessa natura open source del protocollo su cui sono basate).

Dopo aver elencato le principali caratteristiche che potrebbero favorire l'adozione delle criptovalute come mezzi di scambio soffermiamoci anche sulle limitazioni di queste ultime che potrebbero ostacolarla. Uno dei principali problemi in questo ambito si riscontra nel fatto che a differenza delle monete aventi corso legale, il bitcoin e i le altre criptovalute non sono universalmente accettati come strumento di pagamento e non vi è alcun obbligo ad esempio per un venditore di accettare bitcoin come contropartita per le proprie merci o servizi (come per esempio accade nell'area europea dove chiunque è obbligato ad accettare, come strumento di pagamento, gli Euro). Inoltre l'uso di criptovalute in scambi di mercato comporta alti rischi per gli utilizzatori coinvolti, dal momento che non vi è alcuna autorità demandata a risolvere le dispute tra le parti e nessun meccanismo disponibile per annullare o modificare una eventuale transazione erronea.

Unità di conto

Per soddisfare la funzione di unità di conto, come qualsiasi altra moneta, una valuta dovrebbe essere in grado di misurare il valore relativo di beni, servizi e delle altre transazioni nell'economia. Identifichiamo due caratteristiche chiave delle criptovalute come unità di conto, che differiscono sostanzialmente dalle valute tradizionali: divisibilità e volatilità dei prezzi.

Un'importante caratteristica distintiva del Bitcoin è la sua divisibilità quasi infinita, il che implica che i prezzi possono essere quotati in più posizioni decimali (ad oggi queste ultime sono 8 ma potrebbero aumentare in futuro). In effetti, la divisibilità è una caratteristica necessaria per una valuta al fine di accogliere una equa valutazione per transazioni di tutti i tipi e dimensioni. Per contro però, le differenze di prezzo dell'entità di più cifre decimali (ad esempio quattro o più) possono confondere gli utilizzatori e causare loro problemi nella comprensione e nel confronto tra i prezzi relativi di beni e servizi. Per tale ragione, la maggior parte delle valute del mondo usa non più di due decimali per le quotazioni (Yermack 2014)[119].

Un secondo aspetto da tenere in considerazione per quanto riguarda la capacità di uno strumento di fungere da unità di conto sta nel fatto di considerare la volatilità del prezzo dello stesso. I prezzi delle varie criptovalute mostrano una volatilità di breve periodo

[119] Yermack D. "Is bitcoin a real currency? An economic appraisal". NBER working paper no. 19747.

estremamente elevata, che diminuisce la loro capacità di rappresentare un'unità di conto affidabile. Le frequenti variazioni dei prezzi causano costi diretti e indiretti ad imprese e consumatori: le aziende che ad esempio utilizzano bitcoin, devono adeguare i prezzi frequentemente, altrimenti potrebbero subire una diminuzione dei ricavi (a causa di beni e servizi sottoprezzati) o una perdita di competitività (a causa di beni e servizi troppo cari). Questo diventa particolarmente problematico per le imprese che pagano in moneta tradizionale per l'acquisizione dei propri fattori di produzione ma che poi accettano anche pagamenti in criptovaluta al momento della vendita, poiché genera discrepanze nei prezzi relativi tra output ed input in presenza di elevata volatilità. I frequenti cambiamenti dei prezzi a loro volta diventano un fattore di disturbo per i consumatori, poiché diventa più difficile per questi ultimi individuare il valore reale di un bene o servizio.

Riserva di valore

Il valore del denaro deve rimanere stabile nel tempo per consentirne l'uso negli scambi in diversi momenti.

Le valute tradizionali sono solitamente inflazionistiche, il che significa che il loro valore si riduce nel tempo e quindi diminuisce la capacità della moneta stessa di funzionare come riserva di valore (anche se negli ultimi anni per quanto riguarda l'inflazione si necessiterebbe di una discussione a parte). Al contrario, un importante vantaggio delle criptovalute è la loro protezione contro l'inflazione come rifugio dall'interferenza dei governi. Dato che, con i meccanismi attuali, per molte criptovalute il numero futuro di Coin o Token è limitato ad un massimo (vedasi i 21 milioni di unità totali previsti per Bitcoin) senza alcuna espansione oltre tale importo (se non data dalla divisione delle stesse in unità più piccole, fattore che però comunque non ne cambierebbe, nella sostanza, il numero totale), queste ultime saranno esposte a pressioni deflazionistiche se il loro uso come alternativa di investimento o come mezzo di scambio aumenta. Possiamo concludere che, in assenza di pressioni inflazionistiche, la popolarità di Bitcoin e delle altre criptovalute dovrebbe aumentare rispetto alle valute tradizionali, sebbene la pressione deflazionistica possa agire come una forza compensativa.

Una delle principali minacce alla capacità delle criptovalute di preservare il loro valore per i titolari è il problema della sicurezza informatica. In passato, molti proprietari di queste ultime hanno perso i loro risparmi a causa di furti o attacchi informatici. Le valute

tradizionali danno la possibilità di proteggersi dal furto tramite il deposito delle stesse presso un intermediario bancario che ne garantisce la custodia, le criptovalute invece, dovendo essere conservate in supporti informatici propri o di terze parti (non sempre affidabili come garanti) risultano maggiormente esposte a rischi.

Riassumendo perciò, una moneta, a livello giuridico/economico, sarà accettata come tale se si ritiene che: una certa quantità di quest'ultima rappresenti il valore di un bene acquistato/ceduto, verrà accettata ovunque nel momento in cui si vorrà utilizzarla per acquistare/vendere un altro bene e che la stessa non perderà il suo valore nel tempo che intercorre tra la cessione di un bene e l'acquisto di un altro. Tutte le 3 caratteristiche identificano la moneta in quanto tale e la mancanza di una di queste porterebbe alla non accettazione di uno strumento come moneta in una transazione.
Se ci basassimo però solamente su questa definizione per così dire di "letteratura economica", allora nessuna delle attuali valute potrebbe considerarsi moneta, in primis poiché nessuna delle stesse ha mantenuto o può mantenere valore per un periodo illimitato di tempo (inflazione, crisi). Sembra dunque che il concetto di mantenimento del valore sia più un qualcosa di soggettivamente diffuso, ossia che il valore di uno strumento definito come moneta debba essere mantenuto pressoché tale per un periodo sufficientemente lungo in base a quando il soggetto che lo detiene pensa di spenderla. Inoltre nessuna moneta cosiddetta tradizionale (pensiamo a Dollaro, Euro o Yen) è accettata ovunque, infatti non è possibile ad esempio pagare in tutto il mondo utilizzando dollari (sebbene sia la moneta più diffusa) bensì spesso vi è la necessità di convertire la stessa in moneta locale del luogo in cui si vuole effettuare una transazione. Da ciò si evince che la definizione di moneta può essere applicata in senso lato oppure tramite un'accezione più ristretta poiché nella realtà la definizione data dalla letteratura economica è difficilmente riscontrabile contemporaneamente in tutte le sue sfaccettature.

Andando poi oltre la definizione letteraria del termine, è possibile ricostruire la storia dell'utilizzo della moneta, dall'antichità ad oggi. Risulta complicato stabilire con precisione le origini delle società monetarie, sembra infatti che i primi pagamenti effettuati con una qualche forma di denaro risalgano addirittura al 2.200 a.C.

La natura della moneta è mutata nel corso dei secoli, in origine la stessa assumeva la connotazione di moneta merce: vale a dire di uno strumento di pagamento rappresentato da un bene avente valore intrinseco come oro o argento, con una quantità limitata per natura. Successivamente la stessa si è per così dire evoluta in rappresentativa, ossia in banconote che potevano essere scambiate per una determinata quantità di oro o argento ed infine nelle economie moderne, ha assunto il ruolo di moneta fiduciaria (cosiddetta fiat) dichiarata a corso legale ed emessa da una banca centrale senza però alcun valore intrinseco. La stessa infatti basa il proprio valore sulla fiducia riposta dagli utilizzatori nei confronti della banca centrale che dovrà mantenerlo. Al giorno d'oggi poi la moneta può esistere anche indipendentemente da una rappresentazione fisica, ad esempio su un conto corrente come registrazione informatica, oppure come deposito su un conto di risparmio.
Pur integrando alcune funzioni della moneta, le criptovalute non ricadono in nessuna delle precedenti categorie, non essendo moneta merce in quanto non possiedono un valore intrinseco, moneta rappresentativa poiché rappresentano solo se stesse e non hanno un valore sottostante e moneta fiat dal momento che non sono emesse da una banca centrale.

Riflettendo su quanto detto fino ad ora, da un lato si potrebbe essere portati ad affermare che le criptovalute, essendo comparabili alle valute tradizionali (fiat) in molteplici aspetti per quanto riguarda l'uso, potrebbero essere definite moneta. Ricordandoci poi quanto diceva Adam Smith ossia che: "All money is a matter of belief" (tutto il denaro è una questione di fede) questa tesi parrebbe ulteriormente confermata. Non dobbiamo però dimenticarci che, data l'evoluzione del concetto di moneta negli anni e ritrovandoci ora in un'epoca in cui la moneta ha funzione fiduciaria in quanto emessa da banche centrali, quest'ultima è accettata come tale ed identificata dal rispettivo termine ("moneta appunto") nel momento in cui è riconosciuta dagli stati nei quali ha corso legale. Perciò, non essendo le criptovalute considerate come moneta avente corso legale nella maggior parte dei paesi, sembra più opportuno concludere (almeno ad oggi) che la stessa non ricade nell'accezione di moneta, perlomeno per quella che noi consideriamo moneta "tradizionale".

Dopo essere arrivati a questa possibile conclusione, potremmo allora chiederci se, a livello giuridico (e dunque al fine del relativo inquadramento normativo) il concetto di criptovaluta non possa situarsi all'interno di qualche altra macrocategoria:

- Potremmo definire le stesse come dei beni (assets)? In economia, a livello teorico, un bene è definito come qualsiasi mezzo (materiale o immateriale) suscettibile di essere utilizzato da parte di un individuo, per soddisfare un proprio bisogno, oppure al fine di produrre attraverso questo, un altro bene. Le principali caratteristiche che quest'ultimo deve possedere sono: utilità, ossia capacità di soddisfare un bisogno, disponibilità limitata ed accessibilità, intesa come possibilità di essere ottenuto in maniera abbastanza agevole utilizzando i normali mezzi a disposizione. Anche in questo caso a prima vista pare che le criptovalute posseggano tutte le caratteristiche sopra elencate; come però è possibile intuire, ogni ordinamento giuridico (nazionale o sovranazionale che sia), dà una propria definizione di proprietà e di bene che quindi potrebbe differire di caso in caso portando all'impossibilità di definire in maniera abbastanza uniforme il fenomeno.

- Potrebbero quindi essere commodities, ossia materie prime? Con questo termine (che deriva dal latino "commoditas") ci si riferisce a un insieme di prodotti indifferenziati (ossia che non presentano una differenziazione qualitativa) per i quali esiste una domanda nel mercato. In questo caso però è evidente che l'essenza della criptovaluta non possa rientrare all'interno di questa categoria, in quanto mancherebbe fin da subito dell'aspetto fondamentale che la costituisce, ossia la materialità.

- Potrebbero essere security/strumenti finanziari? Il sistema delle criptovalute è un sistema in un certo senso autoregolato, pensato per agire in maniera autosufficiente all'interno di un insieme di regole che sono quelle che delineano il protocollo stesso che le costituisce. L'utilizzo di queste ultime perciò presuppone l'accettazione di queste regole auto-costituite dal sistema stesso che ne regolano il funzionamento e che non sono modificabili. Come nel caso della definizione di bene anche qui ci troviamo di fronte a possibili differenze nella qualificazione di uno

strumento come strumento finanziario in base all'ordinamento giuridico considerato. Se prendessimo ad esempio l'ordinamento italiano le criptovalute non potrebbero essere ritenute uno strumento finanziario in quanto non presenti nell'elenco di strumenti definiti come tali *all'art. 1, comma 2* del Testo Unico della Finanza (TUF).

Queste riflessioni sono solo un'introduzione che permetterà poi di capire (nel corso del terzo capitolo) il perché, non essendoci nel mondo una definizione uniformemente condivisa del concetto di criptovaluta, i vari stati (o confederazioni degli stessi che siano) presentino ognuno definizioni e regolamentazioni talvolta differenti per il fenomeno. Inoltre le considerazioni precedenti portano a riflettere sul fatto che, rinchiudere le criptovalute all'interno di un unico concetto giuridico probabilmente sia riduttivo e allo stesso tempo pericoloso e che forse sarebbe più adatto lasciare in un certo senso aperta la definizione, concentrandosi piuttosto su disposizioni specifiche per quanto riguarda determinate categorie di utilizzatori, ambiti in cui avviene questo utilizzo od operazioni (come vedremo ad esempio per la conversione da criptovaluta a denaro avente corso legale e viceversa). Infatti, mentre il sistema su cui si basano le criptovalute è autosufficiente, le stesse, si configurano in differenti concetti giuridici a seconda del contesto o dello schema giuridico di riferimento.

2.5) IL FENOMENO DEL RICICLAGGIO DI DENARO

Il mondo dei reati economico/finanziari nel corso del tempo si è sempre più caratterizzato per una elevata professionalizzazione nella commissione degli stessi. Infatti, come affermava il sociologo americano E. H. Sutherland (1949), molto spesso le persone coinvolte in questi crimini sono di "*alto stato socio-economico e violano leggi designate a regolare le loro stesse attività occupazionali*[120]".

Tale distinzione tra questi nuovi fenomeni delittuosi e quelli per così dire più tradizionali, solitamente caratterizzati dalla violenza, ha fatto emergere non tanto l'abbandono del precedente sistema criminale, quanto un affiancamento e una diversificazione dello stesso.

[120] Fenomeno che viene definito come "White Collar" alla fine degli anni '30 negli Usa.

Questa evoluzione ha favorito la creazione di nuovi legami di interesse della criminalità organizzata con varie figure professionali, soprattutto operanti nell'ambito bancario e finanziario, nonché in nuovi settori dell'economia moderna[121].

A tutto ciò si deve la proliferazione di una nuova tipologia di reati definiti come "crimini economici[122]" ossia un insieme di atti illegali che solitamente vengono commessi in assenza di violenza fisica, attraverso frode, al fine di ottenere denaro o proprietà, di evitare il pagamento o la perdita di denaro o per ottenere vantaggi economici personali (o per la propria attività).

Il collegamento tra questi ed altri reati e l'economia reale, viene dato dal fenomeno definito come "riciclaggio". Con questa espressione si vuol fare riferimento a quanto stabilito nel nostro ordinamento dal *D.lgs. n. 90 del 25 maggio 2017* (che ribadisce quanto già stabilito nell'*art. 2 comma 1 del D.lgs. 231/2007*[123]) che all'*art. 2 comma 4* definisce come fenomeni riferibili al riciclaggio:

a) *la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni*.

b) *L'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività*.

c) *L'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività*.

d) *La partecipazione ad uno degli atti di cui alle lettere a), b) e c), l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione*.

[121] Fonte: "http://www.carabinieri.it/docs/default-source/default-document-library/supplemento-al-n-4.pdf?sfvrsn=2".

[122] H. Edelhertz (1970).

[123] Questa definizione deriva dal recepimento *dell'art. 1 comma 2 della direttiva europea 2005/60/Ce* e risulta più ampia di quella che era stata inizialmente delineata dagli articoli *648 bis e ter* del *Codice Penale italiano*.

Sebbene questa sia la definizione più recente (e quella attualmente utilizzata), l'ipotesi criminosa che definiva il delitto di riciclaggio è stata introdotta per la prima volta a livello normativo nel Codice Penale italiano nel 1978 attraverso l'*art. 648 bis,* che definiva così l'autore di tale reato: *"… chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa …*" integrato nell'ambito dell'*art. 648* assieme all'art. *648-ter.*

È importante precisare che, il riciclaggio, assume la connotazione di attività economica criminale che si caratterizza per il fatto di essere "autonoma" rispetto alla specifica azione criminosa o illegale da cui ha origine il flusso di proventi illeciti. Anche a livello di normativa penalistica infatti, ad essere punite come riciclaggio di denaro non sono le condotte realizzate dai soggetti che hanno compiuto i reati originari (le quali hanno prodotto la ricchezza illecita), bensì quelle poste in essere da soggetti talvolta diversi ed estranei allo stesso delitto[124].

La rilevanza economica del riciclaggio si sostanzia non solo nella sua funzione di attività che favorisce la crescita del mercato illegale, ma anche nelle profonde alterazioni che il fenomeno provoca all'interno dei meccanismi economici, incidendo oltre che negativamente sul sistema produttivo e commerciale anche sul regime di libera concorrenza.

Secondo il G.A.F.I.[125], dal punto di vista economico/finanziario, il riciclaggio si articola principalmente in 3 fasi:

[124] Per le situazioni in cui chi ricicla il denaro è anche l'autore del delitto primario che ha portato alla generazione dei proventi illeciti, la *legge n. 186 del 15/12/2014*, ha introdotto il delitto di "Autoriciclaggio". A differenza del riciclaggio, in questo caso, viene meno la figura cosiddetta "terza" che si occupa delle azioni di sostituzione/impiego dei proventi illeciti generati.

[125] G.A.F.I.: "Gruppo di Azione Finanziaria Internazionale" o "Financial Task Action Force (F.A.T.F.)" è un organismo intergovernativo creato nel 1989 nel corso del G7 di Parigi che ha per scopo l'elaborazione e lo sviluppo di strategie di lotta al riciclaggio dei capitali di origine illecita e, dal 2001, anche di prevenzione del finanziamento al terrorismo. Il G.A.F.I. elabora standard riconosciuti a livello internazionale per il contrasto delle attività finanziarie illecite, analizza le tecniche e l'evoluzione di questi fenomeni, valuta e monitora i sistemi nazionali.
Del Gruppo fanno parte 35 membri in rappresentanza di stati e organizzazioni regionali che corrispondono ai principali centri finanziari internazionali, nonché, come osservatori, i più rilevanti organismi finanziari internazionali e del settore (tra i quali FMI, Banca Mondiale, ECB, Nazioni Unite, Europol, Egmont).
Definizione tratta da: "Mef: Ministero del Tesoro" (http://www.dt.tesoro.it/it/attivita_istituzionali/rapporti_finanziari_internazionali/fatf_gafi.html).

- Introduzione nel mercato: in questa fase i proventi derivanti dall'attività delittuosa sono collocati materialmente all'interno dell'economia reale tramite una varietà di operazioni: depositi, acquisti di beni, ecc.
- "Laundering": in un secondo momento, tramite operazioni aventi natura finanziaria, i criminali cercano di separare i proventi illeciti dalla fonte che li ha generati (il cosiddetto "lavaggio") in modo tale da rendere quanto più difficile possibile un'eventuale ricostruzione futura dei flussi che hanno generato gli stessi.
- Integrazione: la fase finale di questo procedimento si sostanzia nel tentativo di integrare le ricchezze provenienti da reato con quelle che invece provengono da attività lecita per poi poter essere immesse nei circuiti finanziari tradizionali.

Questo utilizzo indebito si può realizzare attraverso la conversione, dei proventi illeciti ottenuti in moneta fiat, in valuta virtuale e dando in seguito avvio alla fase di "laundering" oppure nella maniera opposta, ossia quando vi è la vendita di merce di natura illecita a fronte del pagamento in valuta virtuale, convertendo poi tale valuta in moneta avente corso legale e realizzando le stesse operazioni finanziarie che si realizzavano nel caso precedente per mascherare l'origine delittuosa del denaro.

Come si può vedere dunque, il sistema è complesso e si sostanzia in una serie di operazioni connesse.

A livello accademico si fa risalire il fenomeno del riciclaggio agli anni 20 del novecento, quando, negli Stati Uniti, alcune figure e gruppi criminali iniziarono la creazione di business volti a conferire un'origine legittima al denaro generato da operazioni e traffici illeciti. Tra questi sicuramente il più ricordato è il famoso gangster della mafia di Chicago, Al Capone, che acquistando autolavaggi e lavanderie (in cui i pagamenti per i servizi avvenivano in contante) mescolava denaro di provenienza lecita ed illecita dichiarandolo come guadagno derivante dalle attività dei propri negozi (da ciò nacque l'espressione "Money Laundering" ossia appunto lavaggio del denaro).
La normativa italiana attraverso il D*ecreto Legislativo n. 591 del 1978*, poi modificato dalla *Legge n. 55/1990* (nota come "Legislazione Antimafia"), introdusse gran parte dei principi e degli adempimenti che verranno poi delineati durante la Convenzione di Strasburgo (conclusasi l'8 novembre 1990). Tramite questa convenzione, gli stati membri del Consiglio

D'Europa[126] si impegnarono nell'adozione di una serie di nuovi provvedimenti di carattere legislativo che delineavano il reato di riciclaggio in maniera più similare a quella cui siamo abituati oggi. Questi principi verranno recepiti nel nostro sistema normativo attraverso la *Legge n. 328/1993,* rendendo grazie a questa modifica il reato di riciclaggio applicabile a qualsivoglia tipologia di reato non colposo e non solo ad una serie di reati cosiddetti "presupposti" come avveniva una volta.
Sempre nello stesso anno (1990) un importante contributo all'evoluzione del contorno normativo della disciplina venne dato dal G.A.F.I. che nel mese di febbraio, elaborò una lista di *40 raccomandazioni* tra le quali spiccavano l'abolizione dell'anonimato nelle transazioni finanziarie, la necessità di identificazione dell'autore di una operazione e quella di cooperazione tra i vari stati. Il nostro paese recepì tali raccomandazioni tramite la *Legge n. 197 del 5 luglio 1991.*

Successivamente, man mano che le modalità utilizzate dalla criminalità per riciclare il denaro si rendevano più sofisticate, è stata ampliata la platea dei soggetti a cui era richiesta una collaborazione in merito al contrasto del fenomeno, nello specifico nel *D.lgs. n. 374 del 25 settembre 1999* venivano aggiunti agli intermediari finanziari, tra gli altri, anche i soggetti operanti nel recupero crediti, nel commercio di cose antiche e più in generale dediti ad attività finanziarie ritenute particolarmente suscettibili di utilizzazione a fini di riciclaggio.
La partecipazione richiesta inizialmente a questi e ad altri soggetti era maggiormente di natura passiva, di semplice verifica, ma con il passare del tempo, soprattutto a partire dall'introduzione della terza direttiva UE dedicata al tema (*2005/60/CE*) è diventata sempre più attiva, trasformandosi quasi in una sorta di "vigilanza aggiuntiva".
Ad oggi, i soggetti che vengono definiti come obbligati al rispetto della disciplina antiriciclaggio sono quelli elencati nell'*art. 3 del D.lgs. n. 90/2017* che va ad integrare quelli già presente nel *D.lgs. n. 231/2007*, raggruppati in 5 macro-categorie[127]:

[126] Consiglio D'Europa: organizzazione internazionale che si occupa di promuovere la democrazia, i diritti umani e la ricerca di soluzioni a problemi sociali. Vede tra i membri fondatori (1949): Italia, Francia e Regno Unito e ad oggi conta 47 stati membri.
[127] Per ritrovare il testo completo, fare riferimento alla Gazzetta Ufficiale della Repubblica Italiana: "http://www.gazzettaufficiale.it/eli/id/2017/06/19/17G00104/sg".

- **Intermediari bancari e finanziari**: banche, Poste Italiane, istituti di moneta elettronica (IMEL), istituti di pagamento, società di intermediazione mobiliare (Sim), società di gestione del risparmio (SGR) e d'investimento (Sicav e Sicaf), agenti di cambio, Cassa Depositi e Prestiti, imprese di assicurazione e consulenti finanziari.
- **Altri operatori finanziari**: società fiduciarie, mediatori creditizi e soggetti che esercitano professionalmente l'attività di cambio valuta.
- **Professionisti:** (nello svolgimento della professione in forma individuale, societaria o associata): dottori commercialisti, notai ed avvocati (quando compiono, in nome o per conto dei propri clienti, operazioni di natura finanziaria o immobiliare), revisori legali e le società di revisione legale.
- **Operatori non finanziari**: prestatori di servizi relativi a società e trust, soggetti che esercitano attività di commercio di cose antiche, opere d'arte od oro, i prestatori di servizi relativi all'utilizzo di valuta virtuale (di cui si farà una trattazione più approfondita nel seguito del lavoro).
- **Prestatori di servizi di gioco** (sia online che su rete fisica).

Alla definizione di riciclaggio riportata precedentemente, si va ad aggiungere anche quella del fenomeno di "finanziamento del terrorismo" (fenomeno che è divenuto di forte interesse a livello internazionale soprattutto in seguito all'attacco terroristico alle Torri Gemelle avvenuto l'11 settembre 2001[128]) il quale viene delineato, al *comma 6 dello stesso art. 2* che definiva il riciclaggio, come: "*… qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette.*"

Nella seguente tabella si presenta un riassunto dell'evoluzione storica delle diverse forme con cui si era (e si è) soliti riciclare denaro dal '900 fino ad oggi:

[128] Al quale si sono susseguite una serie di raccomandazioni speciali del G.A.F.I.

PERIODO	**FINO AGLI ANNI '70**	**ANNI '80**	**ANNI '90**	**ANNI 2000**	**OGGI**
TIPOLOGIA	**Materiale**	**Bancario**	**Finanziario**	**Professionale**	**Informatico**
CARATTERISTICHE	Movimentazione di denaro contante.	Riciclaggio facilitato dall'utilizzo dei servizi forniti dagli intermediari creditizi (banche).	A causa dell'aumento dei controlli bancari il fenomeno si "muove" verso nuovi intermediari finanziari (Sim, Sgr, ecc.).	Crescente ricorso a esperti di professioni giuridiche ed economiche.	Le nuove metodologie si caratterizzano per la movimentazione tramite i nuovi strumenti informatici (queste si affiancano alle tipologie precedenti).

2.6) OBBLIGHI ANTIRICICLAGGIO (Normativa italiana)

Per quanto riguarda invece la normativa nazionale, la cornice legislativa che contrasta il fenomeno del riciclaggio è rappresentata, ad oggi, dal *Decreto Legislativo n. 231 del 21 novembre 2007*[129], che è stato da ultimo modificato dal *D.lgs. n. 90 del 25 maggio 2017*, il quale prevede una architettura normativa che si sostanzia in 3 diversi gruppi di obblighi:

1. **Adeguata verifica della clientela**. *L'art.17 del D.lgs. 231/2007* stabilisce che i soggetti obbligati devono eseguire una adeguata verifica della propria clientela in occasione dell'instaurazione di un rapporto continuativo, del conferimento dell'incarico per l'esecuzione di una prestazione professionale o nel momento

[129] Quest'ultimo è entrato in vigore il 29 dicembre dello stesso anno. Link del documento completo: http://www.gazzettaufficiale.it/eli/id/2007/12/14/007X0246/sg.

dell'esecuzione di una operazione occasionale che comporti la movimentazione di importi uguali o superiori a 15.000 euro, indipendentemente dal fatto che questa sia effettuata tramite un'operazione unica oppure frazionata. Inoltre, questa adeguata verifica andrà compiuta ogni qualvolta il soggetto obbligato abbia sospetti in merito ad una operazione oppure dubiti sulla veridicità o adeguatezza dei dati precedentemente forniti dal cliente.

Il contenuto di questi obblighi (esplicitato *all'art. 18 dello stesso decreto 231/2007* e dalle relative modificazioni già citate in precedenza), si sostanzia nell'identificazione del cliente con la relativa verifica dell'identità (eseguita in presenza dello stesso) e dell'eventuale titolare effettivo, la raccolta di informazioni in merito all'instaurazione del rapporto o allo scopo della prestazione e il monitoraggio costante nel corso di tutta la durata della relazione con lo stesso cliente.

Tutti i precedenti elementi previsti dalla normativa e richiesti ai soggetti obbligati[130] si basano su un approccio "Risk-Based" ossia basato sul rischio, infatti ogni verifica viene effettuata in base al livello di rischio dell'operazione e del cliente (o al cambiamento dello stesso livello di rischio nel corso di un rapporto continuativo) e dovrà essere proporzionale ai rischi effettivamente individuati. Per quanto riguarda le operazioni o il rapporto continuativo è richiesto di analizzarne: tipologia, modalità di esecuzione, frequenza, ragionevolezza, ammontare, scopo, area geografica di destinazione, controparte (con attenzione alla cosiddetta "black list[131]" delle entità in ambito di riciclaggio). Per la clientela invece la verifica riguarda, tra le altre, la natura giuridica della stessa, la residenza, l'attività svolta e il comportamento operativo. Normalmente il profilo di rischio (definito come "Autovalutazione") stilato dai soggetti obbligati per la propria clientela, è supportato da una procedura informatica, che in base a tutte le informazioni raccolte riguardo al cliente, ne determina un profilo di rischio riciclaggio che sarà suddiviso in quattro categorie: irrilevante, basso, medio o alto[132].

[130] Per "soggetti obbligati" si intendono i destinatari della disciplina antiriciclaggio, ossia tutti coloro previsti *all'art. 3 del D.lgs. n. 231/2007 (*e del corrispondente aggiornamento portato *dall'art. 3 del D.lgs. n. 90/2017)*.

[131] Lista di paesi che non collaborano in relazione al contrasto al riciclaggio e al finanziamento del terrorismo. *L'art. 36 del D.L. n. 78/2010* prevede che il Ministero dell'Economia, tramite decreto, predisponga una lista di questi ultimi.

[132] Questa procedura è basata su un documento del G.A.F.I.: "Guidance for a risk-based approach in the banking sector" dell'ottobre 2014.

La metodologia di autovalutazione che si compie (secondo le indicazioni fornite da Banca D'Italia) si articola in: una fase istruttoria, di raccolta dei dati e delle informazioni necessarie, seguita poi da una fase di elaborazione e da una di preparazione degli esiti che si concludono con la fase di discussione collegiale e di approvazione di eventuali misure di adeguamento (gli esiti della quale saranno inseriti nella Relazione Annuale che viene prodotta ad opera della funzione antiriciclaggio).
Agli obblighi fin qui descritti si aggiungono anche quelli previsti per i clienti. Questi ultimi, esplicitati all'interno dell'*art. 22*, stabiliscono che gli stessi debbano fornire alla controparte che deve adempiere agli obblighi di adeguata verifica, tutte le informazioni necessarie e aggiornate per consentire l'adeguato svolgimento della procedura stessa.

Infine, la normativa prevede agli *articoli 23 e 24,* situazioni nelle quali le misure di adeguata verifica della clientela possano essere svolte in maniera semplificata ovvero rafforzata. Il primo caso può essere applicato quando il cliente presenta un basso rischio di riciclaggio e di finanziamento al terrorismo, mentre il secondo quando questo rischio risulta elevato (in base ai relativi fattori di rischio rilevati). Le misure semplificate si traducono in una diminuzione, in termini di estensione e frequenza, degli obblighi previsti all'*art. 18*. Nel caso invece della verifica rafforzata, il soggetto obbligato dovrà acquisire dalla clientela informazioni aggiuntive riguardo ai soggetti stessi (o ad eventuali titolari effettivi), alla natura dell'operazione o del rapporto e intensificare la frequenza di applicazione delle procedure di controllo. A queste si aggiungerà una maggiore raccolta di informazioni se il rapporto di corrispondenza transfrontaliera è instaurato con un istituto finanziario o ente creditizio di un paese terzo che comporterà anche una valutazione sulle qualità delle misure messe in atto da quest'ultimo nel contrasto al riciclaggio (e al finanziamento del terrorismo).

2. **Conservazione e registrazione**. Ai soggetti obbligati allo svolgimento dell'adeguata verifica della clientela viene anche chiesto di conservare tutte le informazioni e i dati che possano rivelarsi utili a prevenire, individuare o accertare eventuali attività

di riciclaggio o finanziamento al terrorismo e a permettere lo svolgimento di analisi da parte dell'UIF[133] o di altre autorità competenti (*articoli 31-34*). I documenti acquisiti nell'ambito dell'adeguata verifica della clientela dovranno essere conservati per un periodo di 10 anni dal momento dell'esecuzione dell'operazione occasionale o della cessazione del rapporto continuativo e devono consentire di ricostruire: la data di instaurazione del rapporto, la causale, la data e l'importo dell'operazione, i dati identificativi del cliente (e/o titolare effettivo) e i mezzi di pagamento utilizzati. I sistemi di conservazione inoltre devono essere idonei a garantire oltre alla tutela da qualsiasi perdita di dati (integrità) e alla massima tempestività di utilizzo, anche il rispetto delle norme in merito alla protezione dei dati personali.

Su indicazione dell'UIF poi, gli intermediari bancari e finanziari trasmettono alla stessa i dati aggregati (secondo le istruzioni in merito alle varie tipologie che l'Unità di Informazione Finanziaria stessa stabilisce) riguardanti la propria attività, in modo tale da permettere all'autorità di effettuare analisi mirate e di individuare eventuali fenomeni di riciclaggio e finanziamento al terrorismo.

3. **Segnalazione delle operazioni sospette**. L'*art. 35* stabilisce che i soggetti obbligati prima di compiere una operazione debbano inviare all'UIF, senza ritardo, una segnalazione di operazione sospetta nel momento in cui *"sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso tentativi (o che gli stessi siano già stati compiuti) di riciclaggio/finanziamento del terrorismo o che i fondi provengono da attività criminosa*". Il sospetto deriva dalle caratteristiche, dall'entità, dalla natura delle operazioni, dal loro collegamento/frazionamento o da qualsiasi altra circostanza conosciuta. Inoltre, con cadenza periodica, l'UIF provvede

[133] Con la sigla "UIF" si indica l'Unità di informazione finanziaria per l'Italia. Istituita dal d.lgs. n.231/2007 presso la Banca d'Italia in conformità alle regole internazionali che prevedono la presenza in ogni stato di una unità di indagine finanziaria, è dotata di piena autonomia operativa e gestionale con l'obiettivo di contrastare i fenomeni del riciclaggio e del finanziamento al terrorismo. La UIF è l'autorità a cui è attribuito l'incarico di acquisire i flussi finanziari e tutte le informazioni riguardanti ipotesi dei delitti precedentemente citati utilizzando come tramite principalmente le segnalazioni di operazioni sospette trasmette da intermediari finanziari, professionisti ed altri operatori. A tal proposito l'Unità di Informazione Finanziaria valuta la rilevanza dei fatti e degli atti ai fini della trasmissione degli stessi agli organi investigativi e della collaborazione con l'autorità giudiziaria per lo sviluppo di un eventuale azione di repressione. Definizione tratta da: "uif.bancaditalia.it".

ad aggiornare l'elenco degli indicatori di anomalia per agevolare, l'individuazione di eventuali operazioni sospette.

Nel caso sia rilevata la presenza degli elementi di sospetto precedentemente citati, l'operazione in oggetto non deve essere compiuta dai soggetti obbligati prima di aver inviato la segnalazione di operazione sospetta all'autorità[134].

In aggiunta a ciò, secondo quanto stabilito dall'*art. 47*, i soggetti obbligati trasmettono con cadenza periodica all'UIF (secondo le modalità e le tempistiche stabilite dalla stessa) informazioni e dati riguardanti operazioni a rischio riciclaggio/finanziamento del terrorismo che saranno utilizzati per approfondire operazioni sospette o effettuare analisi.

Alla normativa attuale si è arrivati dopo un percorso, intrapreso dall'Unione Europea, che a partire dal 1990 e per tutti gli anni successivi, ha portato a recepire, di volta in volta, l'evoluzione dei principi internazionali, in modo tale da favorire la realizzazione di un ambiente normativo armonizzato tra tutti gli stati membri. Quest'ultimo si è sostanziato nell'emissione di 5 direttive e altri diversi provvedimenti in ambito di contrasto al riciclaggio e al finanziamento del terrorismo (a tal proposito si veda la *Figura 24*).

La quarta di queste (*Direttiva 2015/849*), recepita recentemente anche in Italia tramite il precedentemente citato *D.lgs. n. 90 del 25 maggio 2017*, si pone in linea con le "nuove raccomandazioni" promulgate dal G.A.F.I. nel febbraio 2012 (quando le precedenti 40 raccomandazioni erano state profondamente riviste) a cui si aggiungono le nove raccomandazioni speciali introdotte nel 2001, nell'ambito del contrasto al finanziamento del terrorismo.

Di seguito viene proposta una linea del tempo con le differenti Direttive UE in materia di antiriciclaggio:

[134] I soggetti obbligati non sono sottoposti a tale obbligo nei casi in cui l'esecuzione dell'operazione non possa rinviarsi tenuto conto della normale operatività o nei casi in cui il differimento dell'operazione possa portare ad ostacolare le indagini. In tali casi, dopo aver eseguito l'operazione bisognerà immediatamente informare l'UIF. *Art. 35* D.lgs*. n. 231/2007*.

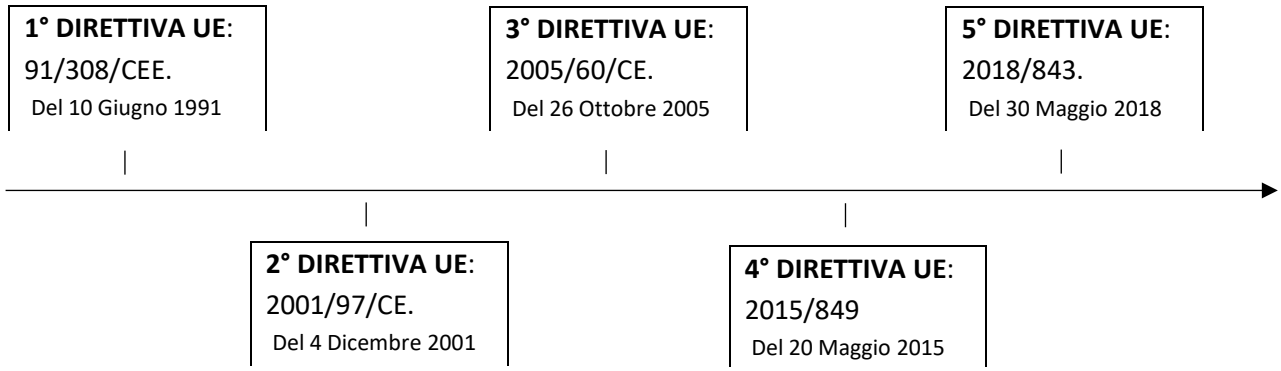


Figura 245: Cronologia Direttive europee antiriciclaggio.

2.7) DISCIPLINA ANTIRICICLAGGIO E CRIPTOVALUTE (Italia-Europa)

Fino ad oggi, a livello europeo (non italiano), non vi era nessun accenno all'interno della normativa antiriciclaggio ai crimini compiuti in questo ambito grazie all'utilizzo delle criptovalute, a partire però dall'ultima Direttiva europea le cose si preparano, seppur in parte, a cambiare. L'intervento normativo del legislatore certamente non sorprende, dato che, nonostante il carattere altamente rivoluzionario e il ruolo in parte residuale ricoperto dalle criptovalute in Europa, queste ultime nel corso del 2017 hanno attirato su di sé i riflettori della stampa e degli addetti ai lavori, oltre che per i favolosi rendimenti, anche per i problemi di trasparenza che le circondano.

La quarta Direttiva europea sull'antiriciclaggio e sul finanziamento del terrorismo, la numero *84/2015*, pur riformando integralmente la materia, non arrivava ad affrontare concretamente la regolamentazione del mercato delle criptovalute[135]; probabilmente ciò è dovuto anche al periodo a cui risale (il 2015) nel quale tale fenomeno non aveva ancora assunto le proporzioni odierne e si delineava come abbastanza marginale rispetto ai volumi dei tradizionali sistemi di pagamento o mercati reali[136].

[135] In precedenza vi erano stati solo alcuni "avvertimenti" dati dalle Banche Centrali nazionali per gli utilizzatori di tali strumenti come nel caso della Banca D'Italia (30 gennaio 2015): "https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf".

[136] Basti pensare che solo un anno dopo la pubblicazione della IV direttiva europea antiriciclaggio, l'Unione aveva già preparato una nuova Proposta di Direttiva, la n. 0208/2016, che fu trasmessa dalla Commissione al Consiglio Europeo in data 6 luglio 2016.

L'Italia però, introducendo nel proprio sistema normativo questa Direttiva europea attraverso il *D.lgs n. 90 del 25 maggio 2017*, ha anticipato (come primo stato a livello europeo) all'interno della nuova disciplina antiriciclaggio anche alcuni contenuti che si apprestavano ad essere inclusi nella V Direttiva UE (pubblicata nella Gazzetta Ufficiale dell'Unione il 19 giugno 2018).

2.6.1) D.lgs. n. 90 del 25 maggio 2017

Con questo decreto legislativo, introdotto il 25 maggio dello scorso anno, che recepisce la IV direttiva UE nel nostro paese, si va principalmente a riformare parte del *D.lgs. n. 231/2007*.

Tra le principali innovazioni che come abbiamo detto vanno a creare una prima regolamentazione per il mercato delle criptovalute e che permettono di introdurre alcuni dei principi che verranno poi esplicitati dalla V direttiva UE sul tema, vi è sicuramente l'inclusione, tra i soggetti obbligati (nella categoria di operatori non finanziari, *art.3, comma 5, lettera i*)) dei cosiddetti "prestatori di servizi relativi all'utilizzo di valuta virtuale". Questi ultimi, anche se solo nello svolgimento dell'attività di conversione tra valute virtuali e valute aventi corso legale, sono stati così inclusi negli obblighi previsti dalla normativa a fini antiriciclaggio che fino a quel momento non annoverava alcun partecipante a questo nuovo criptomercato. Questa novità, fornisce anche per la prima volta una definizione degli stessi prestatori di servizi relativi all'utilizzo di valuta virtuale (*art. 1, comma 2, definizioni, lettera ff*)), delineandoli come: "*qualsiasi persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da, ovvero in, valute aventi corso legale*". Inoltre, per la prima volta viene anche data una definizione giuridica alle criptovalute ritenute appunto valuta virtuale e descritte come: "*la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente*".

Ciò si rivela molto importante in quanto, oltre ad inquadrare all'interno di una precisa categoria quegli intermediari che nel mondo crypto vengono solitamente identificati con il nome di Exchange e dando una definizione giuridica, valida ai fini della legge, alle

criptovalute, rende l'attività degli stessi Exchange soggetta a tutti gli obblighi in tema di disciplina antiriciclaggio e di contrasto al finanziamento del terrorismo a cui devono adempiere gli altri intermediari finanziari, operatori e professionisti che già sottostavano alla normativa, facendone dunque rientrare l'esercizio sotto la vigilanza delle Autorità competenti di settore.

Con l'introduzione del *D.lgs. n. 90*, i prestatori di servizi relativi all'utilizzo di valuta virtuale sono stati anche aggiunti *all'art. 17-bis del D.lgs. n. 141 del 13 agosto 2010*, (che a sua volta era stato modificato dai Decreti Legislativi *n. 218 del 14 dicembre 2010, e n. 169 del 19 settembre 2012*), tra gli intermediari obbligati (*art. 17-bis comma 8-ter*) a comunicare, secondo i tempi e le modalità stabilite dal Ministro dell'economia e delle finanze, al Ministero dell'economia la propria operatività sul territorio nazionale. Tale comunicazione costituisce condizione essenziale per l'esercizio legale dell'attività degli stessi e ne introduce il relativo obbligo di iscrizione in una sezione speciale del registro dei cambiavalute per così dire "tradizionali" previsto dall'art. *128-undecies* del TUB[137] e custodito dall'Organismo degli Agenti e dei Mediatori.

Inoltre, secondo il *D.L. n. 167 del 28 giugno 1990* (integrato con la *legge n. 227 del 4 agosto 1990* e successive modificazioni) si prevede che i prestatori di servizi di valuta virtuale, tra gli altri, debbano trasmettere all'Agenzia delle Entrate i dati relativi al secondo comma dell'*art. 31* di tale decreto, ossia quelli relativi alle operazioni effettuate (anche in valuta virtuale) aventi un importo uguale o superiore a 15.000 a prescindere dal fatto che l'operazione in questione sia unica ovvero formata da più operazioni frazionate che appaiano collegate. Da quanto detto, si evince che l'Exchange, come da soggetto obbligato, nel momento in cui instaura un rapporto continuativo o effettua un'operazione casuale (per gli stessi importi precedentemente citati) con un cliente, sarà tenuto ad identificare lo stesso tramite le procedure delineate dagli *art. 17* e seguenti all'interno dell'adeguata verifica della clientela. In più se il cliente fosse una persona giuridica, un trust o un soggetto giuridico affine, sarà richiesta all'Exchange la verifica dell'identità del suo titolare effettivo[138].

<u>Sanzioni amministrative e penali previste dal D.lgs. n. 90/2017</u>

[137] TUB: Testo Unico delle Leggi in materia bancaria e creditizia.

[138] In ogni caso comunque, l'estensione delle verifiche sarà sempre commisurata al livello di rischio rilevato per quel determinato cliente.

Il *D.lgs. n. 90/2017* ha apportato profonde modifiche al regime sanzionatorio previsto dal *D.lgs. n. 231/2007,* limitando le possibilità di sanzioni penali solo nei casi di eccezionale gravità nella violazione degli obblighi di adeguata verifica della clientela e di conservazione della documentazione prescritta, portando le sanzioni penali a non eccedere, nel massimo, 3 anni di reclusione e una sanzione pecuniaria che può arrivare a 30.000 euro.

Al nuovo *articolo 55 del D.lgs. n. 231/2007*, nei primi 3 commi, sono state introdotte tre fattispecie delittuose volte a sanzionare gravi violazioni della triplice struttura degli obblighi antiriciclaggio.

Nel primo comma è così previsto che "*Chiunque, essendo tenuto all'osservanza degli obblighi di adeguata verifica […], falsifica i dati e le informazioni relative al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro*". La stessa fattispecie si applica a chi viola gli obblighi di conservazione previsti dagli *art. 31 e ss*. dello stesso decreto.

Al terzo comma si introduce poi anche una fattispecie delittuosa a carico del cliente nel momento in cui quest'ultimo "*essendo obbligato, [...], a fornire i dati e le informazioni necessarie ai fini dell'adeguata verifica della clientela, fornisce dati falsi o informazioni non veritiere*".

Per quanto riguarda invece le sanzioni di carattere amministrativo, queste ultime sono disciplinate dagli *articoli 56 e ss.,* dove per le ipotesi di violazioni gravi, ripetute o plurime degli obblighi previsti è applicata una sanzione pecuniaria che va da 2.500 a 50.000 euro (sanzione che nel caso di violazioni degli obblighi di segnalazione di operazioni sospette può arrivare a 300.000 euro). Inoltre, se le precedenti violazioni dovessero portare al soggetto che le compie un qualsiasi vantaggio economico, l'importo della sanzione sarà elevato fino al doppio di tale beneficio illecito, se quest'ultimo è determinato o determinabile (e non inferiore a 450.000 euro) e fino ad un milione di euro se non determinabile[139]. Tali sanzioni vengono poi inasprite all'*art. 62*, se le violazioni sono compiute da intermediari bancari e finanziari vigilati oppure da soggetti con funzioni amministrative, direttive o di controllo che operano all'interno di questi ultimi. Per gli intermediari infatti la sanzione amministrativa applicata può arrivare al 10% del fatturato

[139] Disposizioni previste all'*art. 58 del D.lgs. n. 90/2017*.

annuo[140], mentre per amministratori, direttori o addetti al controllo va da 10.000 a 5.000.000 di euro (in più, nel caso in cui il vantaggio economico ottenuto da questi ultimi sia superiore a tale importo la sanzione può essere innalzata fino al doppio di tale beneficio).

Infine, *l'art. 72* del Decreto Legislativo ha previsto l'inserimento dell'art. *648-quarter* nel Codice Penale, il quale prevede la confisca dei beni che risultano il prodotto o il profitto di attività derivanti da riciclaggio, ricettazione o impiego di denaro avente provenienza illecita (delitti previsti agli *art. 648, 648-bis e ter C.P.*[141]).

2.6.2) V Direttiva europea antiriciclaggio: 2018/843

Come già si è visto, la nuova normativa antiriciclaggio italiana, nell'incorporazione della IV Direttiva Europea tramite il *D.lgs. n. 90/2017,* ha anticipato alcune delle novità nell'ambito delle criptovalute, che si apprestavano ad essere introdotte dalla Direttiva successiva ovvero la V. Queste anticipazioni però, ad oggi, sono già in vigore solo nell'ordinamento italiano, per questo è di grande importanza quanto inserito nella regolamentazione europea, poiché oltre ad ampliare quanto già visto nelle modifiche alla disciplina antiriciclaggio italiana, permette che la disciplina, che dovrà essere recepita entro il 10 gennaio 2020 (ossia entro 18 mesi dalla data di emissione della Direttiva) in tutti gli stati membri, uniformando in questo modo l'intera materia a livello europeo.

Oltre a dare una definizione di "valuta virtuale" simile a quella vista nell'ordinamento italiano, ossia di: "*una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente*" (*art 3, punto 18*)), la V Direttiva UE fornisce anche una definizione di "prestatori di servizi di portafoglio digitale". Questi ultimi infatti, che nel *D.lgs. n. 90/2017* italiano venivano inclusi nella definizione delle attività che vengono definite come proprie dei prestatori di servizi di valuta virtuale ("… conservazione di valuta virtuale …") vengono invece definiti in maniera autonoma (all'*art. 3 punto 19)*) ossia come:

[140] Tale possibilità si ha quando tale importo percentuale è superiore a 5 milioni di euro ed il fatturato è disponibile e determinabile. *"Art.62 D.lgs. n. 90/2017".*

[141] Codice Penale, fonte: "http://www.ipsoa.it/codici/cp".

"*soggetti che forniscono servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*".
Non vi è invece, nel testo normativo, una specifica definizione di "prestatori di servizi di valuta virtuale" come avviene nel nostro ordinamento, la stessa però può essere desunta dalla lettura incrociata dello stesso *articolo 3* da cui risulta che chiunque scambi monete aventi corso legale con valute virtuali (o viceversa) sarà ricompreso tra le obbligazioni previste a fini antiriciclaggio. Gli stessi prestatori di servizi di cambio tra valuta avente corso legale e valuta virtuale vengono poi menzionati, assieme ai prestatori di servizi di portafoglio digitale, *all'art. 47, paragrafo 1,* in cui viene previsto che gli Stati membri assicurino la registrazione degli stessi.

Inoltre, la stessa Direttiva introduce anche alcune limitazione all'utilizzo di carte prepagate anonime (spesso utilizzate per l'acquisto di criptovalute) presso enti creditizi e istituti finanziari degli Stati membri. L'importo massimo memorizzato in maniera elettronica in queste è infatti stabilito in 150 euro.

In seguito si presenta una schematizzazione delle differenze presenti tra IV, V *Direttiva UE e D.lgs. n. 90/2017* italiano:

Direttiva/decreto legislativo	*IV DIRETTIVA UE*	*D.lgs. n. 90/2017 (Italia)*	*V DIRETTIVA UE*
Tematica			
"Prestatori di servizi relativi all'utilizzo di valuta virtuale"	Non inclusi.	Inclusi nelle disposizioni antiriciclaggio quali "soggetti obbligati".	Inclusi.

"Prestatori servizi di portafoglio digitale"	Non inclusi.	Non definiti esplicitamente (però inclusi nella precedente definizione).	Definiti in maniera autonoma.
Definizione "Valuta Virtuale"	Non presente.	Presente.	Presente.
Obblighi di registrazione per gli "Exchange"	Non presenti.	Presenti.	Presenti.
Limiti alle carte prepagate anonime	Limite previsto, di importo massimo: 250 euro.	Limite previsto, di importo massimo: 250 euro.	Presente, limite per somme massime di 150 euro.

CAPITOLO 3

“NORMATIVA INTERNAZIONALE: UN’ANALISI GLOBALE”

Il potenziale per un rapido cambiamento nel settore finanziario generato dall’introduzione della tecnologia Blockchain e delle criptovalute è una sfida per i regolatori finanziari e le autorità di vigilanza a livello mondiale. Questi fenomeni, relativamente recenti, sono emersi in assenza di una regolamentazione efficace e sebbene questo abbia da un lato contribuito al loro successo, ha dall’altro evidenziato i problemi ed i rischi che questa tecnologia presenta se confrontata con i sistemi utilizzati nel sistema economico “tradizionale”.

3.1) LE SFIDE CHE I REGOLATORI DEVONO AFFRONTARE

Come ormai dovrebbe essere chiaro a questo punto dell’elaborato, creare un inquadramento normativo per questo nuovo fenomeno delle criptovalute risulta molto complesso e se da un lato vi è la necessità di regolamentarne il mercato, al fine di tutelarne gli utilizzatori, è altrettanto chiaro che essendo una novità tecnologica avente ampia applicabilità, se implementata adeguatamente potrebbe apportare molteplici benefici all’attuale sistema economico/finanziario. Anche se abbiamo già analizzato nel secondo capitolo la normativa Italiana ed Europea di contrasto al riciclaggio e al finanziamento del terrorismo effettuato tramite criptovalute, facciamo un passo indietro e ricapitoliamo le principali sfide con cui si sono dovute (e/o si dovranno) confrontare le differenti autorità a livello globale al momento di regolamentare, in maniera più o meno restrittiva, queste ultime:

- Definizione del fenomeno: le valute virtuali combinano assieme le proprietà di moneta, merci, strumenti finanziari e mezzi di pagamento, per tale ragione la classificazione di queste ultime come uno piuttosto che un altro strumento ha

implicazioni nel loro trattamento legale, in particolar modo nel determinare quale autorità debba regolarle e vigilare sulle stesse. Infatti anche all'interno della stessa giurisdizione talvolta risulta complicato classificarle, in quanto ciascuna autorità tende ad inquadrarle secondo le proprie politiche e priorità. Per tale ragione, in alcuni casi le criptovalute non vengono inserite all'interno di una specifica classe bensì ci si preoccupa piuttosto di regolarne la differente natura in base agli ambiti di applicazione, ai tipi di transazione o alle controparti dalle quali vengono utilizzate.

- Natura decentralizzata del fenomeno: il fatto che il fenomeno considerato si sostanzi in un sistema decentralizzato non permette di poterne regolamentare una eventuale entità centrale la quale si occupi della vigilanza. Appurato ciò, si può capire perchè risulti così difficile stabilire se regolamentare i partecipanti o le istituzioni finanziarie che interagiscono con gli stessi e perchè molto spesso le varie autorità si siano maggiormente concentrate sulla possibilità di "controllare" le criptovalute nel momento in cui queste ultime "impattano" sull'economia reale (quindi ad esempio, come vedremo, nel momento in cui queste sono convertite in moneta avente corso legale). Anche se questa ipotesi è di difficile realizzazione (sebbene non impossibile nel futuro prossimo), quanto precedentemente descritto potrebbe venire meno nel momento in cui il cripto-mercato diventasse così ampio da rendere non più necessaria la conversione tra valute virtuali e moneta fiat.
- Natura transnazionale delle criptovalute: il fatto che spesso i pagamenti e le operazioni effettuate utilizzando le criptovalute avvengano al di fuori dei territori nazionali o coinvolgano controparti appartenenti a differenti stati, pone il problema della cooperazione tra differenti stati e giurisdizioni.
- Difficoltà nella tracciabilità: nonostante si sia visto come in alcuni casi sia possibile risalire alla vera identità degli utilizzatori, ciò risulta comunque complicato soprattutto perché spesso ciascuna famiglia di criptovalute adotta un funzionamento proprio specifico che rende difficile la creazione di una regolamentazione universale in merito.

Dato quanto si è visto, è chiaro che ogni ordinamento giuridico avrà dato una sua risposta, più o meno approfondita e più o meno simile a quella data da altri, per inquadrare il fenomeno delle criptovalute all'interno di un ambiente regolamentato. Per questo in

seguito verrà svolta un'analisi regolamentare attraverso svariati paesi che permetterà di evidenziare le peculiarità normative adottate da ciascuno di questi.

3.1) GIAPPONE

Il Giappone è stato uno dei primi paesi, a livello globale, ad introdurre alcune misure nel tentativo di regolamentare il mercato delle criptovalute. Questo sicuramente è dovuto al fatto che, nello stato nipponico, siano stati svariati i casi di truffe o furti di criptovalute come quello precedentemente citato della piattaforma di Exchange Mt. Gox, che, con il suo collasso nel febbraio 2014 comportò perdite per i clienti pari a 850 mila bitcoin. A ciò appunto si deve la necessità riconosciuta nel paese prima che in qualsiasi altro di salvaguardare gli utilizzatori.

A tal proposito, già nel 2014 furono istituiti presso la Financial Services Agency[142] un gruppo di studio ed uno di lavoro per approfondire le tematiche legate ai sistemi di pagamento e regolamento introdotti dalle criptovalute. La relazione finale prodotta da questi gruppi di lavoro raccomandava l'introduzione di un sistema di registrazione per le attività che avevano ad oggetto lo scambio di criptovalute in modo tale da rendere le transazioni avvenute tramite questi strumenti soggette alle normative sul riciclaggio di denaro e al tempo stesso favorire l'introduzione di un sistema di tutela per gli utenti. A tal proposito la relazione venne presentata al consiglio finanziario dell'FSA che si adoperò affinché il governo presentasse una proposta di legge per modificare la legge sui servizi di pagamento. Tale legge, ossia il Payment Services Act, venne modificata nel 2016 ed entrò in vigore a partire dal 1° aprile 2017, sancendo così l'accettazione ufficiale delle valute virtuali come sistema di pagamento.

All'interno dello stesso PSA inizialmente si ribadisce la definizione di moneta (valuta avente corso legale) ossia di strumento avente liquidità obbligatoria ed accettazione universale e successivamente viene data quella di valuta virtuale, la quale però ricomprende due aggregati. Un 1° tipo di valuta virtuale viene definito come: "valore finanziario registrato elettronicamente all'interno di dispositivi elettronici (escludendo qualsiasi moneta fiat) che può essere utilizzata per pagare un prezzo in cambio di beni acquistati, noleggiati o come

[142] Agenzia governativa giapponese e regolatore finanziario responsabile della supervisione del settore bancario, finanziario ed assicurativo, con la finalità di garantire la stabilità del sistema finanziario e la protezione di depositanti ed investitori. Fonte: "Investopedia".

contropartita per un servizio ricevuto o effettuato da parte/a favore di una o più persone non specificate". Per quanto riguarda invece il 2° tipo quest'ultimo si riscontra come un: "valore finanziario registrato elettronicamente all'interno di dispositivi elettronici (escludendo qualsiasi moneta fiat) che può essere scambiato con qualsiasi altro valore finanziario del 1° tipo con una persona non specificata e trasferito tramite un sistema elettronico di elaborazione dei dati".
In base a questa definizione quindi Bitcoin, Litecoin o differenti Alt-Coins sarebbero classificati all'interno del primo gruppo in quanto utilizzate come sistema di pagamento, mentre le "Counterparty Coin" (le cosiddette XCP) nel secondo, tra le quali ad esempio l'Ether, in quanto non possono (ad oggi) essere utilizzate come strumento di pagamento ma si possono intercambiare con altre criptovalute appartenenti al primo tipo.

La suddetta normativa poi prevede che gli intermediari definiti come "Virtual Currency Exchange Services" debbano essere registrati presso la Financial Services Agency (FSA). Rientrano all'interno di questa categoria quei soggetti che svolgono:

1) Acquisto/vendita di valute virtuali (cioè scambio tra valute virtuali e fiat o viceversa) o conversione tra differenti famiglie di queste ultime.
2) Attività di intermediazione, brokeraggio o agenzia per le attività previste al punto 1).
3) Gestione o custodia di monete fiat o valute virtuali in nome dei clienti in relazione alle attività previste ai punti 1) e 2)[143].

I requisiti di base richiesti a questi ultimi per la registrazione sono:

- Possesso dello status di società per azioni o di Exchange straniero (che possieda però un ufficio fisico e un rappresentante avente cittadinanza giapponese nello stato stesso, come previsto dal comma 5 dell'*art.63* del PSA).
- Capitale sociale di almeno 10 milioni di Yen e un patrimonio netto positivo.
- Un sistema interno che garantisca conformità alle regole stabilite nel Payment Services Act (con la relativa presenza di figure incaricate della compliance e dell'internal audit) ed una appropriata e sicura esecuzione dei servizi.

[143] A tal proposito la registrazione non è richiesta ai meri "wallet provider" o prestatori di servizi di portafoglio digitale in quanto gli stessi eseguono tale funzione in maniera indipendente rispetto alle attività previste ai punti 1) e 2).

- Obbligo di presentare una relazione eseguita da un revisore esterno.
- Il richiedente dovrà presentare un nome commerciale, un indirizzo, un elenco degli azionisti certificati, nonché una lista delle valute virtuali accettate e un esempio di format contrattuale attraverso il quale interagisce con i propri clienti.
- Inoltre la società richiedente non dovrà mai aver violato il PSA e aver subito sanzioni negli ultimi 5 anni.

Il sistema di registrazione si sostanzia in una prima fase di consultazione con l'FSA, i cui tempi possono variare in base ai singoli casi ma che solitamente richiede 3 o 4 mesi per completarsi, in cui il richiedente fornisce all'agenzia tutta la documentazione necessaria (descrizione dell'ente, metodi di business adottati, struttura interna ed altri) a cui è seguita un'application per la registrazione[144].

In aggiunta a ciò, il focus dell'autorità si indirizza sulla struttura organizzativa della società richiedente, la quale dovrà fornire adeguate informazioni ai clienti riguardo alle valute virtuali che utilizza, alla relativa natura ed ai rischi delle stesse, nonché assicurarsi che il cliente sia a conoscenza di come vengono conservate e amministrate le proprie disponibilità in criptovaluta (ciò deve essere incorporato nel contratto stipulato tra Exchange e cliente). Per quanto riguarda poi le disponibilità dei clienti, queste dovranno essere conservate in maniera separata rispetto a quelle proprie del fornitore di servizi e risultare sempre individuabili in maniera chiara (per evitare altri casi simili a quello "Mt. Gox"). La parte più interessante di quest'ultimo obbligo previsto dalla normativa sta nel fatto che le disponibilità in moneta fiat dei clienti dovranno essere depositate all'interno di un conto bancario a nome del cliente a cui appartengono (e che dovrà differire da quello in cui sono depositati i fondi propri dell'Exchange). Al fine di poter aprire un conto bancario a nome del cliente, l'Exchange sarà tenuto a verificare l'identità dello stesso e a sviluppare un robusto sistema di prevenzione e controllo interno per scongiurare attività di riciclaggio. I casi in cui l'Exchange sarà obbligato ad effettuare l'identificazione del cliente sono quelli in cui si presenta:

[144] La quale prevede anche il pagamento di una tassa di registrazione di 150.000 Yen. A febbraio 2018 gli Exchange registrati in Giappone erano 16, a cui se ne aggiungevano altri 100 in attesa di registrazione.

- Un rapporto continuativo (fornitura di servizi) che implica la gestione o lo scambio di criptovalute.
- Acquisti o vendita di valute virtuali per un importo uguale o superiore a 200.000 Yen.
- Trasferimenti di valuta virtuale di importo maggiore o uguale a 100.000 Yen.

In ogni caso, nel corso dell'operatività di un Exchange, la regolamentazione giapponese prevede che lo stesso debba seguire una procedura di tipo "Know Your Costumer" al fine di prevenire attività di riciclaggio di denaro e finanziamento del terrorismo.
La struttura normativa giapponese è inoltre arrivata anche a regolamentare la tassazione di questi nuovi strumenti del mercato criptovalutario. Infatti nel settembre 2017 è stato stabilito, ad opera dell'Agenzia Fiscale Nazionale, che i proventi derivanti dalla negoziazione di valute virtuali, i cosiddetti "capital gains" siano soggetti alle imposte sul reddito (ed inseriti all'interno della categoria "entrate varie"). Questi profitti, aggregati agli altri redditi, come salari o reddito d'impresa, saranno dunque soggetti alla tassazione aggregata (che va dal 5 al 45% nell'ambito del sistema fiscale progressivo[145]). Da ciò si può anche vedere come Bitcoin e le altre criptovalute in Giappone non siano considerati moneta avente corso legale bensì (per ora) siano maggiormente assimilabili agli asset, perlomeno a livello fiscale.

ICO Giappone

Le aziende e gli individui considerano sempre di più le offerte iniziali di criptovalute (ICO) come un modo per raccogliere capitali o partecipare ad opportunità di investimento. Sebbene queste risorse digitali e la tecnologia alla base di esse possano presentare un nuovo ed efficiente strumento per effettuare transazioni finanziarie, le stesse portano anche un maggiore rischio di frode e manipolazione perché i mercati di queste attività sono meno regolamentati rispetto a quelli dei mercati di capitali tradizionali. Per questo attraverso uno statement, nell'ottobre 2017, l'FSA ha cercato di regolare anche le Initial Coin Offering[146]. Queste ultime infatti ad oggi devono essere registrate, in quanto tale

[145] Fino al 27 marzo 2017 le criptovalute erano anche soggette ad una tassazione sul valore aggiunto (VAT) dell'8%, ora non più.
[146] Nuovo metodo per raccogliere capitale attraverso l'utilizzo della tecnologia Blockchain e la creazione di una specifica criptovaluta (token).

raccolta, che presuppone la vendita di criptovalute (token) ad investitori, si delinea come una attività soggetta alla regolamentazione del PSA.

PAESE	STATUS LEGALE CRIPTOVALUTE	DEFINIZIONI DATE	EXCHANGE	MINING	ICO
GIAPPONE	Virtual Currencies, accettate come sistema di pagamento	2 tipologie di valute virtuali, Virtual Currency Exchange Services	REGISTRATI presso FSA (disponibilità Exchange e clientela separate)	/	CONSENTITE (prevista registrazione)

3.3) STATI UNITI

Prima di addentrarsi in qualsiasi descrizione, bisogna ricordare che, essendo gli Stati Uniti una federazione, la normativa emanata dalle autorità centrali (a livello federale) è talvolta ampliata da quella dei singoli stati.
Nel corso della trattazione, si farà principalmente riferimento alle leggi ed ai provvedimenti emessi a livello federale (pur riportando però anche un esempio a livello statale) che ricadono al di sotto della giurisdizione di svariate autorità quali: Federal Reserve (FED), SEC (Security and Exchange Commission) ossia l'autorità che regola la borsa, CFCT (Commodity Future Trading Commission), FinCEN (Financial Crimes Enforcement Network) e IRS (Internal Revenue Service) ossia l'Agenzia delle Entrate statunitense[147].

Nel 1970, il Congresso degli Stati Uniti approvò il Foreign Transaction Reporting Act, più comunemente noto come "Bank Secrecy Act" (BSA). Lo scopo della legge, che fu il primo significativo passo nel contrasto al riciclaggio di denaro intrapreso dagli USA, fu di rendere

[147] Gli Stati Uniti vengono riconosciuti dal G.A.F.I. (FATF) come un paese avente elevati standard normativi di contrasto al riciclaggio e al finanziamento del terrorismo. Nel 2016 infatti nel report stilato dallo stesso gruppo, gli USA sono risultati essere conformi a 9 e ampiamente conformi a 21 delle 40 raccomandazioni G.A.F.I.

più difficile l'esecuzione del fenomeno in oggetto e di impedire che le banche statunitensi diventassero, a loro insaputa, mediatrici in questa attività illegale. Ciò avvenne anche attraverso l'introduzione di una nuova autorità, la "FinCEN", istituita come ufficio operante al di sotto del Dipartimento del Tesoro degli Stati Uniti ed avente responsabilità normative nella gestione del BSA[148]. Tale provvedimento, stabilisce il quadro di base per gli obblighi AML imposti agli istituti finanziari. Tra gli altri, autorizza il Segretario del Tesoro ad emanare norme che richiedano agli istituti finanziari (compresi i broker) di tenere registri ed archiviare rapporti riguardanti le transazioni finanziarie che possono rivelarsi utili ad indagare riguardo ad attività di riciclaggio di denaro e/o altri reati finanziari.

Nonostante l'introduzione di questo atto però, il reato di riciclaggio venne definito come crimine federale solo nel 1986 grazie all'introduzione del Money Laundering Control Act.

Oltre al Bank Secrecy Act, altre importanti novità furono apportate grazie al Patriot Act[149]: tale legge, promulgata dal Congresso nell'ottobre 2001 in risposta agli attacchi terroristici dell'11 settembre, ha modificato e rafforzato, tra gli altri, il BSA stesso, imponendo un numero di obblighi AML direttamente ai broker-dealer, tra cui: programmi di compliance, di identificazione del cliente, rilevamento e archiviazione di segnalazioni di attività sospette, due diligence su conti corrispondenti esteri e il rispetto delle "misure speciali" imposte dal Segretario del Tesoro per affrontare particolari problemi di AML. La sezione 352 del Patriot Act prevede che tali programmi di contrasto al riciclaggio (e al finanziamento del terrorismo) debbano avere forma scritta e includere, perlomeno: politiche, procedure e controlli interni ragionevolmente progettati per raggiungere la conformità con la BSA e le sue norme di attuazione, le politiche e le procedure che possono essere ragionevolmente prevedibili per rilevare e trasmettere le segnalazione di operazioni sospette (attività definita come SAR: Suspect Activity Reprting)[150], la designazione di un addetto alla conformità AML e la formazione continua dei dipendenti.

[148] La mission della FinCEN è quella di salvaguardare il sistema finanziario dagli utilizzi illeciti e di combattere il riciclaggio di denaro sporco promuovendo allo stesso tempo la sicurezza nazionale attraverso la raccolta, l'analisi e la diffusione dell'intelligence finanziaria e dell'uso strategico delle autorità finanziarie. "Fincen.gov".

[149] La sigla Usa Patriot Act sta per: "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act".

[150] E' richiesto di presentare una segnalazione di attività sospetta se: (i) una transazione è condotta o tentata da, presso, o attraverso un broker-dealer; (ii) la transazione comporta o aggrega fondi o altre attività di almeno $ 5000; e (iii) il broker-dealer sa, sospetta o ha motivo di sospettare che la transazione: (a) coinvolga fondi o sia intesa a camuffare fondi derivati da attività illegali, (b) è progettata per eludere i requisiti della

La sezione 326 poi, ha modificato il BSA per richiedere alle istituzioni finanziarie, compresi i broker-dealer, di stabilire programmi di identificazione dei clienti (anche questi ultimi redatti per iscritto) denominati "CIP: Customer Identification Programs" al fine di ottenere le informazioni relative all'identità, alla residenza e al codice di identificazione ai fini d'imposta prima di instaurare un rapporto con gli stessi e di mantenere un registro delle relative informazioni ottenute.

Avanzando poi a livello cronologico e riferendosi al contrasto del riciclaggio effettuato tramite l'utilizzo delle criptovalute è importante fare riferimento all'anno 2013, quando la FinCEN emanò alcune linee guida (FIN-2013-G001) nelle quali definiva la valuta virtuale come una "rappresentazione di valore che sostituisce la moneta" e classificava le persone che amministrano, scambiano o utilizzano valute virtuali come "Money Services Business (MSB)[151]" secondo quanto previsto dal Bank Secrecy Act. Facendo ciò l'autorità ha distinto gli utenti che fanno uso delle valute virtuali al solo scopo di acquisto/vendita di beni e servizi da coloro che accettano, convertono o trasmettono valuta virtuale: gli Exchanger (i quali appunto ricadono sotto la definizione di MSB).

A seconda della particolare classe di intermediari finanziari coinvolti, secondo il BSA, possono essere applicati programmi di prevenzione contro il rischio di riciclaggio e requisiti di registrazione/conservazione di dati differenti. In ogni caso, sia che si tratti di un MSB o di un intermediario che si occupa di acquisto/vendita di titoli o materie prime, la normativa richiede allo stesso soggetto di mantenere un programma di conformità AML basato sul rischio, di segnalare eventuali attività sospette od altre transazioni e di conservare determinati dati. Gli MSB sono poi tenuti a registrarsi presso la FinCEN (a differenza di broker e dealer in titoli o merci, che invece si registrano presso i rispettivi regolatori). In

BSA, (c) non ha scopi commerciali o apparentemente leciti, e il broker-dealer non è a conoscenza di alcuna spiegazione ragionevole sulla motivazione della transazione dopo aver esaminato i fatti disponibili, o (d) comporta l'uso del broker-dealer per facilitare l'attività criminale.
Gli intermediari finanziari devono segnalare l'attività sospetta utilizzando un modulo che il Tesoro ha emesso per il settore dei valori mobiliari e dei futures: il SAR-SF.

[151] Il termine "Money Services Business" comprende qualsiasi persona oppure azienda organizzata, che svolge attività (regolare o meno) in una o più delle seguenti classi: (1) commercio o scambio di valuta; (2) conversione di assegni; (3) emissione di assegni turistici, vaglia postali o valori memorizzati; (4) vendita o rimborso di assegni turistici, vaglia o valori memorizzati; (5) trasmissione di denaro; o (6) servizio postale all'interno degli Stati Uniti. Sono esclusi da questa nozione: banche, banche estere, alcune persone registrate presso SEC e CFTC ei loro equivalenti non statunitensi e le persone che svolgono attività non a scopo di lucro. D. Holman, B. Stettner: "Anti-money laundering regulation of cryptocurrency" ICLG, 2018.

aggiunta, sempre ai Money Services Business è richiesto di ottenere l'identificazione delle controparti e la conservazione dei dati nel momento in cui gestiscano trasferimenti per importi uguali o superiori a 3.000 dollari[152]. Analogamente, mentre i requisiti di Transaction Reporting ("CTR") non si applicano agli scambi diretti tra differenti criptovalute, le transazioni che coinvolgono contanti o equivalenti in cambio di valuta virtuale, dovranno essere segnalate, in base alle regole precedentemente citate, tra cui appunto l'ottenimento dell'identificazione dell'individuo che presenta la transazione e di qualsiasi persona per conto della quale eventualmente la transazione venga effettuata.

A quanto fino ad ora detto, vanno aggiunte altre tre "correnti di pensiero" a livello regolamentario, che invece di inserire le valute virtuali nella categoria, per così dire similare a quella occupata dalla moneta tradizionale, definiscono le stesse come:

- Security

La SEC, che si occupa di regolare le transazioni di titoli, prevede una definizione di "Security" (titolo appunto), data all'interno del Security Act, molto ampia[153], che parrebbe includere, se non tutte, perlomeno varie famiglie di criptovalute.

- Commodity (Materie prime)

La CFTC osservò (nel 2014) che le criptovalute potevano essere equiparate alle "materie prime" ai sensi del Commodity Exchange Act ("CEA"), ritenendo in tal modo di poter avere un'ampia giurisdizione sui derivati che fanno riferimento a queste ultime (futures, opzioni e swap) e sui partecipanti al mercato che negoziano tali contratti. A tal proposito, a partire dal 18 dicembre 2017, la stessa commissione ha permesso lo scambio regolamentato di

[152] Senza dimenticare l'obbligo previsto per tutti gli scambi ed i tipi di business che prevede di riportare tutte le transazioni (uniche o frammentate) di importo maggiore od uguale a 10.000 $ avvenute in contanti.

[153] Il termine "Security" indica qualsiasi nota, azione, azione propria, titolo futuro, swap basato su titoli, obbligazione, prova di indebitamento, certificato di interesse o partecipazione a qualsiasi accordo di partecipazione agli utili, certificato di garanzia collaterale, abbonamento, quota trasferibile, contratto di investimento, certificato di fiducia di voto, certificato di deposizione per un titolo, interessi indeterminati frazionari in petrolio, gas o altri diritti minerari, qualsiasi put, call, straddle, option o privilegio su qualsiasi titolo , certificato di deposito, o gruppo o indice di titoli (compresi gli eventuali interessi ivi contenuti o in base al valore degli stessi), o qualsiasi put, call, straddle, option o privilegio stipulati su una borsa valori nazionale relativa a valuta estera, o, in generale, qualsiasi interesse o strumento comunemente noto come "Security", o qualsiasi certificato di interesse o partecipazione, certificato temporaneo o provvisorio, ricevuta, garanzia, warrant o diritto di sottoscrivere o acquistare, qualsiasi dei suddetti. Definizione tratta da "Security Act 1933", Sec.2 punto 1).

derivati (futures) aventi ad oggetto bitcoin. Inoltre, sotto la propria autorità esecutiva, la CFTC ritiene di poter perseguire sospetti di frode o manipolazione nei confronti della criptovaluta stessa.

- Property (Proprietà)

Infine, l'Internal Revenue Service, tramite l'articolo "Notice 2014-21" (25 marzo 2014), ha emanato una serie di disposizioni in merito al trattamento impositivo nei confronti di bitcoin e delle altre valute virtuali. In primis viene sottolineato il fatto che le valute virtuali siano trattate come proprietà (e non come moneta) e quindi soggette ai principi applicabili previsti dalla Legge Federale degli Stati Uniti. Tra le altre cose, ciò significa che:

- Gli stipendi corrisposti ai dipendenti attraverso l'uso di valuta virtuale devono essere segnalati dal datore di lavoro (tramite un modulo W-2) e sono soggetti alle imposte sul reddito e a quelle sui salari federali.
- I pagamenti effettuati tramite valuta virtuale ad appaltatori indipendenti o ad altri fornitori di servizi sono soggetti a tassazione e generalmente, agli stessi, si applicano le norme fiscali relative all'impiego.
- Il guadagno o la perdita (i cosiddetti Capital Gains) derivanti dalla vendita o dallo scambio di valuta virtuale saranno tassati. Inoltre un pagamento effettuato utilizzando la valuta virtuale è soggetto alla segnalazione di informazioni nella stessa misura di qualsiasi altro pagamento effettuato[154].
- Anche per i Miners di criptovalute la normativa prevede l'inclusione all'interno del reddito lordo (e dunque tassabile) del valore di mercato delle criptovalute minate nel momento in cui queste vengano convertite in moneta fiat. Questo valore sarà calcolato in base al valore di cambio tra la valuta virtuale considerata ed il dollaro nel giorno di creazione della stessa.

Quanto visto riguardo all'inquadramento dato da SEC, CFTC e IRS alle valute virtuali va sicuramente a creare un conflitto rispetto a quanto affermato dalla FinCEN che poneva il fenomeno all'interno della regolamentazione degli intermediari noti come MSB richiedendo agli Exchange una registrazione.

[154] A tal proposito l'Agenzia delle Entrate statunitense richiese all'Exchange Coinbase (il più grande presente negli Stati Uniti all'epoca) dati e transazioni dei clienti che avevano acquistato criptovalute tra 2013 e 2015 (con sentenza della Corte Californiana: caso n° 17 –cv-01431-JSC).

Come anticipato precedentemente anche a livello dei singoli stati spesso ci possono essere ulteriori integrazioni normative per quanto riguarda le criptovalute: è questo il caso ad esempio dello stato di New York.

3.3.1) Bit-license New York[155]

Pubblicata il 24 giugno 2015 nel Registro di Stato di New York, tale normativa fornisce (come molte delle altre che abbiamo visto precedentemente per altri stati a livello globale) in primis alcune importanti definizioni al fine di inquadrare il fenomeno delle criptovalute e le relative attività collegate:

- "Virtual Currency": ogni tipo di unità digitale utilizzata come mezzo di scambio o forma di conservazione digitale di valore. Il concetto di valuta virtuale include: unità digitali aventi una entità centrale di deposito o amministrazione, unità digitali decentralizzate o che possano essere create od ottenute attraverso il calcolo computazionale. Al contrario però in tale categoria non vanno considerate le unità digitali che vengono utilizzate esclusivamente all'interno di piattaforme di gaming o all'interno di programmi fedeltà/a premi, le quali non abbiano mercato al di fuori delle piattaforme stesse o che non possano essere convertite da o in moneta fiat, così come unità digitali utilizzate come parte di carte prepagate.

- "Exchange Service": conversione o cambio di moneta fiat o altri valori con valute virtuali e viceversa o conversione di un tipo di valuta virtuale in un'altra.

- "Virtual Currency Business Activity": la pratica di una delle seguenti attività che coinvolga New York ovvero un suo residente: ricezione, trasmissione, conservazione o mantenimento in custodia di valute virtuali, servizi di brokeraggio o di exchange (come precedentemente definito) per la clientela nella

[155] Normativa completa disponibile al link:
"https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm".

vendita/acquisto di valute virtuali, il controllo, l'amministrazione e l'emissione di tali strumenti.

La Bit-license, similmente ai provvedimenti presi a livello federale dalla FinCEN, prevede che nessuna persona, sprovvista di apposita autorizzazione possa intraprendere alcuna attività concernente valute virtuali (ad eccezione di persone autorizzate dalla NY Banking Law o commercianti e consumatori che utilizzino le stesse solo per acquisto/vendita di beni e servizi o a scopo di investimento).

Al fine di ottenere la licenza, i richiedenti dovranno fornire, in forma scritta, tutti i dati previsti dal sovrintendente tra cui quelli anagrafici, l'organizzazione sociale, il business svolto (con una dettagliata descrizione dell'attività caratteristica e dei servizi forniti oltre ad una spiegazione riguardo a come vengono stabiliti i prezzi di conversione delle valute virtuali in moneta fiat), la lista dettagliata (anche a livello biografico e di esperienza/qualificazione) dei principali attori coinvolti nello svolgimento dell'attività, il report di un'agenzia indipendente ed addirittura un set di impronte digitali e due fototessere per le figure societarie che abbiano accesso ai fondi dei clienti al fine di prevenire frodi (come prestabilito dal Federal Bureau of Investigation e dalla State Division Criminal Justice Services)[156].

Per quanto riguarda gli obblighi di conservazione, tutti i dati relativi alle transazioni ed i documenti in copia originale dei contratti devono essere mantenuti dai soggetti autorizzati per un periodo minimo di 7 anni. Inoltre, ogni applicante dovrà corrispondere una tassa di iscrizione di 5.000 $ a copertura delle spese burocratiche; la licenza in oggetto sarà concessa o meno dal supervisore entro un periodo di 90 giorni e potrà essere revocata dallo stesso a causa di violazioni di tale normativa o per giusta causa.

A partire da gennaio 2017 il Dipartimento dei servizi finanziari (DFS) di New York ha anche previsto la necessità di una certificazione annuale di conformità (compliance) alla normativa per i soggetti obbligati, la quale sarà predisposta ad opera del Consiglio di Amministrazione o dell'alta dirigenza.

In sintesi, come si può notare, il potenziale inquadramento in più definizioni giuridiche e l'assenza di una linea comune di azione rendono già di per sé difficile accertare lo stato

[156] Per maggiori dettagli fare riferimento alla Sezione 200.4: Application del "Regulations of the Superintendent of the Financial services".

normativo del fenomeno criptovalute negli Stati Uniti e al tempo stesso si prevedono differenti applicazioni regolamentari a seconda della tipologia di operazioni compiute dai differenti clienti e dal tipo di intermediario coinvolto. Per questo, sebbene sicuramente la regolamentazione statunitense si possa ritenere abbastanza avanzata, in quanto perlomeno si dedica alla definizione di alcuni aspetti del fenomeno (come la definizione di valuta virtuale e di Exchange Service) rimane il fatto che la linea di azione non sia definita in maniera unanime a livello federale da tutte le autorità coinvolte, fattore già evidente dal momento che ciascuna delle stesse spesso si esprime in maniera differente a riguardo.

ICO USA

Dopo aver "messo in guardia", tramite differenti comunicazioni, i consumatori sui rischi e le possibili frodi relativi alle Initial Coin Offering, la SEC ha stabilito che queste ultime sono equiparabili ad offerte di titoli (securities offerings) e ricadono dunque sotto la giurisdizione della stessa. Per tale ragione, sebbene la regolamentazione di questo fenomeno sia ancora agli albori (ancora di più di quella relativa alle criprovalute), negli Stati Uniti le ICO devono essere registrate presso la SEC stessa.

PAESE	**STATUS LEGALE CRIPTOVALUTE**	**DEFINIZIONI DATE**	**EXCHANGE**	**MINING**	**ICO**
STATI UNITI	Non uniformemente definito (Security, Commodity, Property)	Virtual Currency	REGISTRATI ed equiparati a Money Services Business (MSB)	Valore "minato" tassato	CONSENTITE: equiparate a Securities offerings (sotto giurisdizione SEC)

3.4) CINA

Le prime regole AML in Cina sono state introdotte nel 1997, attraverso una legge penale ("Criminal Law Act") che includeva il divieto di riciclaggio di denaro. Successivamente, nel

2003 sono state introdotte norme amministrative per la presentazione di relazioni riguardo alle attività sospette in concomitanza con la creazione, avvenuta l'anno successivo, di un'unità di intelligence finanziaria, denominata "Chinese Anti-Money Laundering Monitoring Analysis Centre". Nel 2007 il paese è anche entrato a far parte del G.A.F.I.
La Cina, pur avendo portato solo parzialmente a compimento la maggior parte delle raccomandazioni del G.A.F.I. (e per questa ragione esser stata posta dallo stesso gruppo all'interno di un processo di "follow-up" fino al 2012), ha recentemente avuto un rapido sviluppo nella propria normativa antiriciclaggio, soprattutto grazie alla pubblicazione, avvenuta il 28 dicembre 2016, ad opera della Banca Popolare Cinese del cosiddetto, "Decree No. 3". Tra i punti salienti di tale decreto vi è un insieme di requisiti relativi alla segnalazione di transazioni sospette: il Decreto ha abrogato i precedenti parametri e le relative soglie di monitoraggio previste, che venivano applicate universalmente a tutte le istituzioni finanziarie, richiedendo ad ogni istituto di implementare proprie regole di monitoraggio delle transazioni (con applicazione avvenuta a partire dal 1 luglio 2017). A tal proposito poi, tutte le istituzioni finanziarie risultano obbligate a:

- Eseguire una valutazione in corso d'opera dell'efficacia dei propri meccanismi di monitoraggio delle transazioni.
- Programmare adeguati presidi di avviso di eventuali anomalie.
- Mantenere una documentazione dettagliata dei processi decisionali avvenuti durante la revisione di situazioni di "allerta" (come ad esempio le motivazioni alla base della mancata considerazione di alcuni indici di anomalia o del perché, al contrario, in determinate situazioni siano state avviate ulteriori indagini).

Tra gli obblighi previsti vi è anche quello di mantenere traccia (archiviare) dei rapporti riguardanti transazioni sospette (STR: Suspicious Transaction Report). Si parla di transazione sospetta quando l'istituto finanziario, sa o ha motivo di sospettare che il proprio cliente, i fondi o le attività, oppure le transazioni condotte/tentate dallo stesso possano comportare potenziali attività di riciclaggio o finanziamento del terrorismo, indipendentemente dall'importo in questione.

Gli obblighi antiriciclaggio si applicano a:

- Istituti bancari.

- Società finanziarie e società di gestione di fondi.
- Compagnie assicurative, società di gestione patrimoniale e società di brokeraggio assicurativo.
- Società fiduciarie, società di leasing finanziario e società di intermediazione valutaria
- Altre istituzioni impegnate in attività finanziarie.

La Cina ha poi promulgato ulteriori misure antiriciclaggio[157] , in vigore dal 1 luglio 2017, con l'obiettivo di migliorare ulteriormente il monitoraggio di transazioni finanziarie sospette e relative a riciclaggio, finanziamenti terroristici, corruzione e frode fiscale.
In aggiunta al requisito per cui le istituzioni finanziarie sono tenute a riportare eventuali transazioni sospette alla Banca Popolare Cinese seguendo il criterio del "ragionevole dubbio", (a prescindere dell'ammontare delle transazioni stesse) grazie a questi provvedimenti, sono state riviste le soglie per cui le istituzioni finanziarie sono tenute a riportare anche le transazioni di elevato ammontare presso l'ente "China Anti-Money Laundering Monitoring and Analysis Center". Pertanto andranno segnalate:

- Singole transazioni (o insieme di più transazioni frammentate) in contanti superiori a 50,000 RMB**.**
- Singole transazioni (o insieme di più transazioni frammentate) in valuta estera superiori a 10,000 USD.

Per quanto riguarda nello specifico le criptovalute, nel 2013[158] la Cina ha definito il Bitcoin e le altre valute virtuali come delle "Virtual Commodity" ossia beni virtuali, in quanto ritiene che le stesse non siano in possesso delle caratteristiche che delineano la moneta e che non ne acquisteranno in futuro lo stesso stato legale. Sebbene il pubblico sia libero di usare le valute virtuali come mezzo di scambio, le istituzioni finanziarie non sono autorizzate a fare altrettanto. La regolamentazione proibisce infatti a queste ultime di prezzare i propri prodotti e servizi in bitcoin o simili, di scambiare, fornire assicurazione e servizi correlati, negoziare o gestire valuta virtuale in qualsiasi forma.

[157] "*Administrative Measures for Financial Institutions' Reports of Large-value and Suspicious Transactions*".
[158] Fonte: "Notice on Precautions against the risk of Bitcoins", 6 dicembre 2013.

La Repubblica Popolare Cinese sembra essere il più severo regolatore tra le principali economie in materia di criptovalute. Questo fatto è particolarmente curioso dal momento che, nel 2017, nel paese si riscontrava la presenza del 50% di miners bitcoin a livello globale e che l'adozione di criptovalute in Cina è aumentata a un tasso più elevato di qualsiasi altro paese.

ICO Cina

Il 4 settembre 2017 la Cina ha posto al bando le ICO definendole come "una minaccia seria per l'ordine economico e finanziario" che si sostanzia in una raccolta di fondi pubblici (fundraising) non registrati e illegali, i quali potrebbero risultare reati penali ai sensi di legge equiparabili alla emissione illegale di titoli, alla raccolta fondi illegale o a frodi finanziarie (Ponzi Schemes). Inoltre è stata istituita una commissione guidata dalla Banca Centrale Cinese (la Banca Popolare) che ha il compito di effettuare ispezioni approfondite presso oltre 60 piattaforme che si occupano di finanziamento tramite ICO, al fine di tutelare gli interessi degli investitori e di gestire le ripercussioni di questo tipo di raccolta fondi in termini di rischio finanziario.

PAESE	**STATUS LEGALE CRIPTOVALUTE**	**DEFINIZIONI DATE**	**EXCHANGE**	**MINING**	**ICO**
CINA	Virtual Commodity (utilizzo consentito solo ai singoli)	Virtual Currency	SCAMBI PROIBITI	/	NON CONSENTITE (definite una minaccia per l'ordine economico e finanziario)

3.5) RUSSIA

Così come fatto precedentemente per le altre nazioni, iniziamo dicendo che la Russia risulta essere (secondo il "Mutual Evaluation Report[159]") conforme a 10 ed ampiamente conforme a 13 delle 40 (a cui si aggiungono le 9 speciali) raccomandazioni del G.A.F.I. pur essendo parzialmente inadempiente in 2 delle 6 raccomandazioni chiave.
La principale legge che disciplina l'AML in Russia è quella *No. 115-FZ* "On Combating Legalisation (Laundering) of Proceeds from Crime and Financing of Terrorism (conosciuta come AML Law)" del 7 agosto 2001[160].
Tale legge, dopo aver definito il riciclaggio come "l'atto di conferire un legittimo aspetto al possesso, uso o alla cessione di fondi monetari o altri beni ottenuti attraverso la commissione di un reato" delinea i soggetti inclusi negli obblighi antiriciclaggio suddividendoli in due categorie generali. La prima di queste comprende le entità soggette all'elenco completo dei requisiti, le cosiddette "targeted institutions" (*articolo 5*) che includono istituzioni finanziarie, assicurazioni, fondi di investimento e pensione ed altri fornitori di servizi connessi al settore finanziario ed i "professional advisers" ossia avvocati, notai ed altri consulenti che a differenza del primo gruppo sono soggetti ad obblighi AML attenuati.

I principali adempimenti richiesti dalla normativa sono:

- Nomina di uno speciale funzionario interno per imprese e società che si occupi di compliance e la costituzione di procedure appropriate per consentire allo stesso di agire.
- Identificazione dei clienti e valutazione del relativo rischio.
- Monitoraggio e identificazione di transazioni problematiche a cui si uniscono gli obblighi di segnalazione di eventuali operazioni sospette (*articolo 7(2) AML Law*).

[159] Report redatto dal G.A.F.I. Fonte: http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate).
[160] Il riciclaggio di denaro è stato però criminalizzato come reato in un secondo momento, da due articoli del Codice Criminale (CC): il 174 e il 174.1, introdotti nel 2003 specificamente a tale scopo, al fine di attuare i principi della Convenzione di Strasburgo del 1990.

- Conservazione di registri contenenti le transazioni monitorate e i dati dei clienti.
- Misure speciali di sospensione e di "congelamento" per eventuali operazioni sospette.
- Programmi di formazione e sensibilizzazione del personale.

Nel 2017 poi, la Russia ha apportato importanti miglioramenti al proprio quadro giuridico ed applicativo in ambito AML/CFT, aggiornando e modificando varie leggi per migliorarne l'efficacia. Tra questi emendamenti risulta importante proprio quello applicato alla legge *No. 115-FZ del 2001* (che si unisce ai 16 avvenuti l'anno precedente) il quale riduce la soglia per rendere le società definite come "targeted" soggette ai requisiti AML. Se infatti in precedenza tale soglia di attività si sostanziava nell'ammontare di 850.000 dollari ora la stessa è stata ridotta a 170.000.

Passando ora a considerare la normativa riguardante le criptovalute, bisogna da subito dire che, ad oggi, lo stato legale delle stesse in Russia non viene ufficialmente definito. A riguardo è stato pubblicato a marzo di quest'anno il progetto di legge n. 419059-7 sui "Digital Financial Asset" che seppur ancora provvisorio (è stato approvato a luglio 2018 solo nella prima delle tre letture previste dall'iter legislativo), presenta alcuni spunti interessanti. Quest'ultimo infatti definisce "criptovaluta" e "token" come attività finanziarie digitali, cioè come proprietà (e non come sistema legale di pagamento) create in forma elettronica utilizzando dispositivi crittografici le cui informazioni sono memorizzate in portafogli digitali con l'ausilio di dispositivi hardware e software.
In particolare, data la definizione delle criptovalute quali asset, il mining è considerato al pari della produzione di beni e definito come: "attività volta a creare una criptovaluta". Dal momento che solo le aziende o i singoli imprenditori possono essere impegnati nella produzione di beni in Russia, i minatori dovranno registrarsi come imprenditori individuali o creare un'azienda privata per le proprie attività. Rimane possibile il mining effettuato singolarmente da utenti ed in limitate quantità, si prevede infatti che i costi energetici per "l'estrazione mineraria" non possano superare (nell'arco di tre mesi consecutivi) i limiti di consumo energetico stabiliti dal governo[161].

[161] A Mosca, ad esempio, per gli appartamenti dotati di una stufa a gas, il limite è di 45 kWh a persona al mese. Considerando che il consumo energetico della maggior parte dei moderni strumenti di mining va da

ICO Russia

Sempre all'interno del progetto di legge citato precedentemente, vengono introdotte possibili misure per la regolamentazione delle Initial Coin Offerings. L'emittente di token all'interno di una ICO dovrà pubblicare "un memorandum d'investimento" (definito White Paper) unito ad un'offerta pubblica che fornisca dettagliate informazioni sull'emittente e il suo beneficiario effettivo, sul prezzo di acquisto del token, nonché sulla persona che svolge l'attività di depositario. I token potranno essere scambiati per rubli o valuta estera, ma solo attraverso gli operatori Exchange registrati. Si sta inoltre pianificando l'introduzione di un registro per coloro che investono in questo ambito, il quale ha lo scopo di eliminare l'anonimato tipico delle ICO e di renderne più trasparente il processo. Per partecipare alle ICO o ad altri futuri progetti crittografici, gli investitori dovranno, proprio come accade per gli investitori tradizionali, collegare i wallet crittografici alla propria identità (attraverso passaporti, codici fiscali o ID biometrici). Inoltre, gli investitori non autorizzati non potranno investire più di 50.000 rubli, ossia circa 900 Dollari in una singola ICO.

PAESE	**STATUS LEGALE CRIPTOVALUTE**	**DEFINIZIONI DATE**	**EXCHANGE**	**MINING**	**ICO**
RUSSIA (progetto di legge)	Digital Financial Asset (provvisorio)	Criptovaluta, Token	REGISTRATI (unici autorizzati alla conversione di criptovalute)	Miners imprenditori individuali (o singoli con forti limitazioni)	CONSENTITE (obbligo di pubblicazione di un "White Paper" e di una offerta pubblica dettagliata)

0,6 a 2 kW all'ora, è facile calcolare che un dispositivo esaurirà il limite mensile in 22,5-75 ore (massimo di 3 giorni). Questa risulta interessante in quanto permetterebbe di individuare gli eventuali miners non registrati. Non bisogna però dimenticare che tale progetto di legge potrebbe essere ulteriormente modificato prima della seconda lettura (la cui data non è ancora stata stabilita). Fonte: "Maxim Rubchenko, Decenter.com".

Sebbene fino ad ora sembra essersi delineata una certa diffidenza degli stati nei confronti delle criptovalute, ora vediamo due casi in cui lo stato ha abbracciato le innovazioni apportate dalle stesse (ciò non significa che questo sia un fatto positivo) arrivando, nei casi di Venezuela e Dubai ad introdurre addirittura una criptovaluta di stato.

3.6) VENEZUELA

Secondo il report G.A.F.I., il Venezuela è considerato come conforme a 6 e ampiamente conforme a 12 delle 40 (+ 9) raccomandazioni AML/CFT, sebbene il paese risulti parzialmente conforme o non conforme a 5 delle 6 raccomandazioni principali. Il Venezuela fu incluso nell'elenco dei paesi con carenze strategiche in tali ambiti nel 2010 ed è stato oggetto di un'intensa attività di monitoraggio da parte di detta organizzazione. La rimozione da tale elenco è avvenuta nel febbraio 2013, dopo che il governo statale aveva dimostrato di rispettare i requisiti del piano d'azione preparato a tale scopo.
Nonostante ciò, secondo il Dipartimento di Stato degli Stati Uniti, il Venezuela, data anche la vicinanza ai principali paesi produttori di droga (come ad esempio la Colombia), le debolezze del regime AML, la cooperazione bilaterale limitata e la corruzione presente all'interno delle forze dell'ordine e di altri settori pertinenti, rimane un paese vulnerabile al riciclaggio del denaro.

Senza scendere eccessivamente nel dettaglio di una legislazione AML deficitaria, è facile capire che ciò rispecchia anche le condizioni che negli ultimi anni (a partire dal 2013) hanno caratterizzato il paese, il quale si vede coinvolto in una crisi politica con importanti riflessi sulla sfera economica che hanno portato a fenomeni di elevatissima inflazione monetaria[162].

[162] Lo studio "Diáspora en Números", elaborato dalla società Consultores 21 durante il quarto trimestre del 2017, rivela che il 50% dei venezuelani ha dichiarato di voler emigrare, e che la situazione economica è la ragione principale per lasciare il paese. Inoltre, secondo il Fondo Monetario Internazionale l'inflazione nel paese a fine 2018 potrebbe raggiungere il milione percento. Fonte: "https://www.imf.org/external/index.htm".

Per contrastare tale fenomeno il governo venezuelano del Presidente Nicolàs Maduro ha introdotto, il 20 agosto 2018, una nuova moneta avente corso legale, che sostituirà il Bolívar Venezuelano Forte, il cosiddetto Bolívar Venezuelano Sovrano[163], il quale sarà ancorato al "Petro (PTR)" una criptovaluta ideata dal governo venezuelano nel febbraio 2018 anche al fine di aggirare le dure sanzioni finanziarie imposte al Venezuela dalla comunità internazionale[164] e che, nelle intenzioni del governo, vuole consentire al paese di creare un sistema finanziario che non dipenda dagli aiuti e dai diktat internazionali. Al lancio di questa criptovaluta che potremmo definire "di stato[165]", si è accompagnato il "Cryptoasset Constitutional Decree[166]" e la creazione di un Osservatorio sulla Blockchain (SUPCACVEN), con sede a Caracas, che si occuperà di vigilare sullo sviluppo delle varie criptovalute all'interno del paese. Con tale Decreto (CCD) viene delineato il quadro giuridico generale che consente formalmente, l'utilizzo, la circolazione, e lo scambio di criptovalute (tra cui appunto il Petro) tra persone fisiche e giuridiche del settore pubblico o privato, residenti o meno in Venezuela. Inoltre vengono rimesse all'Esecutivo Nazionale:

1) La regolazione della creazione, il rilascio, l'organizzazione, il funzionamento e l'uso di criptoassets.
2) La creazione vera e propria e l'emissione di criptoassets statali.
3) La concessione dell'autorizzazione allo svolgimento di operazioni di scambio nel mercato delle criptovalute e la regolamentazione dello stesso.
4) Il governo promuoverà (non viene specificato come), proteggerà e garantirà l'utilizzo di criptovalute come mezzo di pagamento presso istituzioni statali ed entità private, miste o a proprietà congiunta, sia in Venezuela che al di fuori dello stato.

Inoltre, il Decreto Costitutivo dei Criptoassets introduce la creazione di un apposito registro per gli Exchanges, i miners di valuta virtuale e le altre entità che si dedicano ad operare all'interno di tale neonato mercato.

[163] Un Bolivar venezuelano sovrano equivale a 100.000 Bolivar venezuelani forti.
[164] 1 Petro vale 3.600 Bolivar sovrani secondo un rapporto di fixed exchange rate. Fonte: "http://www.bcv.org.ve/billetes-y-monedas/unidad-de-cuenta".
[165] Il Petro sarà una criptovaluta "sovrana" in quanto emesso dalla Repubblica Bolivariana del Venezuela su una piattaforma Blockchain federale.
[166] Introdotto nella Gazzetta Ufficiale n. 6.370 in data 9 aprile 2018.

In particolare, alle entità che vogliono configurarsi come Exchange, per potersi registrare sarà richiesto di:

- Costituirsi come società per azioni.
- Possedere un capitale minimo che sia circa l'8% del valore medio stimato delle operazioni mensili effettuate dall'entità. Il 20% di detto capitale sarà depositato presso la Banca Centrale Venezuelana e a 6 mesi dalla data del deposito, quest'ultimo verrà considerato come riserva legale della società neocostituita.
- Permettere l'individuazione dei titolari delle partecipazioni azionarie, persone fisiche o giuridiche che siano.
- Possesso da parte della società di un organigramma che contenga almeno un rappresentante legale, un tesoriere, un agente di controllo (compliance), un risk manager, un revisore dei conti e un contabile.
- L'Exchange si dovrà dotare di uno spazio fisico specifico che sia unicamente destinato allo svolgimento delle attività di scambio tra criptovalute e/o moneta fiat e non ad altre.
- È inoltre richiesto il possesso di un manuale interno con norme specifiche in ambito AML e di gestione del rischio[167] (che preveda limitazioni specifiche a seconda delle operazioni svolte) nonché un sistema che garantisca la sicurezza dei dati della clientela.

"El Petro"

Secondo quanto pubblicato dal governo venezuelano all'interno del "White Paper[168]", il Petro si sostanzia in un criptoattivo non convenzionale che sfrutta la tecnologia Blockchain perseguendo l'obiettivo di garantire trasparenza, verificabilità ed integrità delle informazioni per offrire la stabilità che il mercato volatile delle criptovalute ancora non presenta.

Il prezzo del Petro è associato a quello del paniere del petrolio greggio venezuelano (che al

[167] Per tale manuale è prevista una struttura precisa esplicitata in un Paper redatto ad opera del governo (http://www.elpetro.gob.ve/index-en.html#docs).

[168] Documento disponibile all'indirizzo: "http://www.elpetro.gob.ve/pdf/en/Whitepaper_Petro_en.pdf", 30 gennaio 2018.

momento del lancio, si attestava attorno ai 60 dollari statunitensi) e lo stato accetterà il pagamento di imposte, contributi e servizi pubblici nazionali effettuati tramite tale criptovaluta[169].

I presupposti su cui si basa l'introduzione del Petro sono:

- Creazione di uno strumento per ridurre la volatilità all'interno del mercato crypto.

La configurazione del Petro punta ad offrire una criptovaluta che abbia un valore intrinseco, sicuro e stabile, legato ad un settore ben noto come quello petrolifero e quindi adatta ad essere utilizzata anche per l'esecuzione di grandi transazioni, operazioni di credito o addirittura come riserva di valore.

- Uso della tecnologia per accrescere la fiducia e stimolare la crescita dell'economia venezuelana (contrastando l'iperinflazione).

Questo fattore risulta ad oggi abbastanza dibattuto in quanto, dato lo stato dell'economia venezuelana, la connessione del prezzo del Petro all'economia reale del paese sebbene potrebbe essere da un lato una cosa positiva, dall'altra potrebbe rivelarsi una lama a doppio taglio.

Tale criptovaluta si prefigge di avere 3 funzioni fondamentali:

- Mezzo di scambio: potrà essere utilizzata per acquistare beni e servizi (che ad oggi a causa dell'inflazione risultano difficili da acquistare dati i prezzi proibitivi) e convertito in valuta tradizionale grazie ad appositi Exchange, ai quali in futuro si vorrebbero aggiungere anche altri Exchange internazionali.
- Piattaforma digitale: la piattaforma NEM su cui si basa il Petro potrà fungere da base per la creazione di altri strumenti digitali orientati al commercio.
- Strumento di risparmio e di investimento: nella speranza che il valore di tale strumento si riveli stabile (o perlomeno più stabile rispetto a quello della maggior

[169] Dopo l'ICO (in teoria), il prezzo del Petro sarà determinato principalmente da due fattori: il prezzo ufficiale del petrolio venezuelano e le sue performances nelle borse di tutto il mondo secondo il binomio domanda/offerta.

parte delle criptovalute) il governo venezuelano punta ad offrire il Petro come strumento che favorisca il risparmio e che possa fungere da investimento duraturo[170].

Il totale di Petro emessi sarà di 100 milioni, di cui 82.400.000 offerti sul mercato: di questi il 38,4% tramite una fase di prevendita (iniziata il 20 febbraio 2018 e conclusasi un mese dopo) a cui è seguita una ICO (a partire dal 20 marzo che continuerà fino all'esaurimento dei token[171]) che renderà disponibile il 44% della somma, mentre il restante 17,6% verrà mantenuto dallo stato.
Un Petro sarà divisibile fino a 1.000.000 di unità (0,000001), la più piccola delle quali prenderà il nome di "Mene" (parola che significa petrolio nella lingua Wayùu, la seconda più parlata in Venezuela).

Di seguito sono forniti i tassi di cambio di Petro e Bolivar Sovrano al 25 settembre 2018:

Figura 25: Fonte: "Banco Central de Venezuela".

Agli occhi della comunità internazionale questa emissione, realizzata dal governo venezuelano, viene vista come un ultimo disperato tentativo di coprire il debito (i quali rifinanziamenti sono bloccati) ed evitare il default statale, raccogliendo moneta forte in

[170] Secondo quanto dichiarato all'interno del "White Paper" il governo venezuelano si impegnerà a richiedere elevati standard in termini di lotta al riciclaggio e di verifica della clientela agli Exchange che saranno autorizzati a scambiare tale criptovaluta.
[171] Secondo le dichiarazioni di Maduro, il Petro entrerà in funzione a partire dal 1° ottobre 2018 come valuta commerciale internazionale. Fonte: "http://www.bcv.org.ve/".

cambio di token. A tal proposito il Dipartimento del Tesoro degli Stati Uniti ha ammonito i cittadini statunitensi sul fatto che la partecipazione all'offerta iniziale proposta dal Venezuela per la criptovaluta Petro potrebbe rivelarsi una violazione delle sanzioni statunitensi applicate contro il Venezuela, perché si configurerebbe come un'estensione del credito internazionale offerto. Il presidente Donald J. Trump, il 19 marzo, ha firmato un ordine esecutivo con cui vieta a qualsiasi persona statunitense di effettuare transazioni in qualsiasi criptovaluta emessa dal governo venezuelano.

In ogni caso il Venezuela, in questo momento, si delinea sicuramente come il miglior esempio concreto (forse ancora l'unico) in cui il fallimento della politica economica dello stato favorisce l'adozione di forme alternative di pagamento che risultino, in parte o del tutto, slegate nel loro valore dalla situazione politico/economica del paese. A tal proposito i cittadini venezuelani hanno iniziato in massa ad utilizzare le criptovalute come strumento per effettuare pagamenti durante la propria vita quotidiana e sfuggire a quella inflazione che giorno dopo giorno erodeva il loro potere d'acquisto. Il fenomeno è evidente anche guardando al numero di esercizi commerciali che hanno adottato le criptovalute come sistema di pagamento (tra cui spiccano anche marchi come Subway e Calvin Klein) e che sono passati dai 400 di inizio luglio agli oltre 800 di fine agosto[172]. Al contrario di quello che si potrebbe pensare però, la crypto più utilizzata non è Bitcoin, bensì Dash. Questa scelta nasce dal fatto che tale strumento permette costi di transazione inferiori rispetto a quelli che caratterizzano i bitcoin, uniti ad una velocità di esecuzione delle transazioni che richiede solo pochi secondi per il completamento. Inoltre il fattore più originale di Dash si riscontra nel fatto che la stessa viene gestita da una comunità di stakeholder che gestiscono il 10% degli introiti che ricevono i miners (che appunto vengono conservati in una sorta di "cassa comune" di sistema) utilizzandoli per finanziare progetti sul territorio. Fino ad ora queste somme in Venezuela (precisamente 1 milione di dollari) sono stati utilizzati per diffondere presso gli esercizi commerciali tale sistema di pagamento.

[172] Dati tratti da "Il Sole 24 Ore" del 26 agosto 2018.

PAESE	STATUS LEGALE CRIPTOVALUTE	DEFINIZIONI DATE	EXCHANGE	MINING	ICO
VENEZUELA	Petro criptovaluta di stato	/	REGISTRATI (unici autorizzati alla conversione di criptovalute)	Miners come gli Exchange dovranno registrarsi in un apposito Registro.	Il Petro lanciato attraverso ICO (non specificata però la legittimità delle stesse al di fuori del caso statale).

3.7) DUBAI

Tramite il "Regulatory Framework For Stored Values and Electronic Payment Systems", pubblicato il 1 gennaio 2017, la Banca Centrale degli Emirati Arabi Uniti[173] ha fornito per la prima volta una definizione di valuta virtuale indicandola come "qualsiasi tipo di unità digitale utilizzata come mezzo di scambio, unità di conto o forma per la memorizzazione di valore". Le valute virtuali sono però riconosciute tali secondo il regolamento solo se si delineano come:

a) Strumenti che permettono di essere riscattati in cambio di beni, servizi o sconti promozionali nell'ambito di un programma di fidelizzazione o a premi per gli utenti di un determinato emittente.
b) Non possono essere convertite in valuta fiat o in un'altra valuta virtuale.

Da questa definizione si direbbe che le criptovalute (Bitcoin, Ethereum, Ripple ecc.) siano

[173] Gli Emirati Arabi Uniti sono una federazione che comprende Abu Dhabi (la capitale), Dubai, Fujaira, Ajman, Ras al-Khaima, Sharja e Umm al-Qaywayn.

proibite all'interno del paese così come negli altri stati appartenenti alla federazione degli Emirati Arabi Uniti. In realtà però, Il 1° febbraio 2017, il Governatore della Banca Centrale degli Emirati Arabi Uniti, Mubarak Rashed Khamis Al Mansouri, ha rilasciato una dichiarazione a Gulf News affermando che il regolamento in oggetto non copre le criptovalute assimilabili al Bitcoin e alcuna tecnologia sottostante alle stesse come la Blockchain. Lo stesso ha inoltre aggiunto che le valute virtuali stanno venendo esaminate dalla Banca Centrale e che verranno a breve emessi nuovi regolamenti appropriati in tale ambito. Perciò ad oggi, il framework regolamentario che circonda le criptovalute è abbastanza contraddittorio per non dire inesistente.

A discapito di ciò però, lo stato di Dubai, a fine settembre dello scorso anno (2017) ha introdotto una criptovaluta denominata "EmCash". Quest'ultima, sviluppata dal Dipartimento Economico di Stato in partnership con le società Emcredit[174] e ObjectTech è caratterizzata dal fatto di non essere emessa in una quantità predeterminata, bensì verrà creata, in base alla domanda e alle decisioni congiunte di Dipartimento economico di Stato Ed Emcredit. Tramite tale criptovaluta, che verrà conservata all'interno di portafogli virtuali (emPay), si potranno effettuare pagamenti che consentiranno agli utilizzatori di scegliere tra:

- Pagamento in moneta fiat (il Dirham degli Emirati Arabi Uniti: AED) secondo le procedure di regolamento utilizzate tradizionalmente.
- Pagamento in EmCash regolato direttamente tra le parti della transazione.

I due metodi potranno essere utilizzati in maniera intercambiabile.

PAESE	**STATUS LEGALE CRIPTOVALUTE**	**DEFINIZIONI DATE**	**EXCHANGE**	**MINING**	**ICO**
DUBAI (EMIRATI ARABI	EmCash criptovaluta di stato (le altre	Valuta Virtuale	/	/	/

[174] Emirates Credit Information Company Limited (Emcredit Ltd. Or Emcredit) è la società di servizi di informazione degli Emirati Arabi Uniti fondata nel gennaio 2006 in conformità con la direttiva di Sheikh Mohammed bin Rashid Al Maktoum, Vice Presidente e Primo Ministro degli Emirati Arabi Uniti. Fonte: (https://www.emcredit.com/?page_id=37).

UNITI)	parrebbero proibite)				

Di seguito infine viene fornita una tabella riepilogativa di confronto tra le singole normative adottate e lo status delle criptovalute nei differenti stati presentati nel corso della trattazione.

PAESE	***STATUS LEGALE CRIPTOVALUTE***	***DEFINIZIONI DATE***	***EXCHANGE***	***MINING***	***ICO***
EUROPA (e Italia)	Valute Virtuali	Valuta Virtuale, Wallet Provider e Prestatore di Servizi connessi a V.V.	REGISTRATI presso ed equiparati a tutti gli altri soggetti obbligati alla disciplina	/	/
GIAPPONE	Virtual Currencies, accettate come sistema di pagamento	2 tipologie di valute virtuali, Virtual Currency Exchange Services	REGISTRATI presso FSA (disponibilità exchange e clientela separate)	/	CONSENTITE (prevista registrazione)
STATI UNITI	Non uniformemente definito (Security, Commodity, Property)	Virtual Currency	REGISTRATI ed equiparati a Money Services Business (MSB)	Valore "minato" tassato	CONSENTITE: equiparate a Securities offerings (sotto giurisdizione SEC)
CINA	Virtual Commodity (utilizzo consentito solo ai singoli)	Virtual Currency	SCAMBI PROIBITI	/	NON CONSENTITE (definite una minaccia per l'ordine economico e finanziario)
RUSSIA (progetto di legge)	Digital Financial Asset (provvisorio)	Criptovaluta, Token	REGISTRATI (unici autorizzati alla	Miners come imprenditori individuali	CONSENTITE (obbligo di pubblicazione di un

			conversione di criptovalute)	(o singoli con forti limitazioni)	"White Paper" e di una offerta pubblica dettagliata)
VENEZUELA	Petro criptovaluta di stato	/	REGISTRATI (unici autorizzati alla conversione di criptovalute)	I Miners, come gli Exchange, dovranno registrarsi in un apposito Registro.	Il Petro lanciato attraverso ICO (non specificata però la legittimità dello stesso al di fuori del caso statale).
DUBAI (Emirati Arabi Uniti)	EmCash criptovaluta di stato (le altre parrebbero proibite)	Valuta Virtuale	/	/	/

3.8) EXCHANGES: MECCANISMI DI VERIFICA DELLA CLIENTELA

Dopo aver visto che molte delle normative di contrasto al riciclaggio e al finanziamento del terrorismo richiedono ai fornitori di servizi di exchange di verificare l'identità dei propri clienti, cerchiamo di fornire qualche indicazione di come questa venga effettuata dalle piattaforme in oggetto. Per quattro dei cinque principali Exchange che descriveremo, i meccanismi di verifica sono abbastanza simili (cambia solo il grado di intensità degli stessi in base all'operatività offerta). Il primo passo è la verifica dell'identità elettronica, che richiede al cliente di fornire i dati anagrafici di base. All'aumento delle potenzialità operative questa verifica sarà via via intensificata e richiederà maggiore documentazione. L'unico esempio differente è Binance, il quale opera solo nello scambio tra differenti famiglie di criptovalute.

Coinbase

I tipi di verifiche includono il numero di telefono, i dettagli personali, la foto del documento d'identità ed il collegamento di un conto corrente bancario. Negli Stati Uniti, un ulteriore passo è l'aggiunta del proprio SSN[175].

Bitfinex

La piattaforma, per ritirare o aggiungere valute legali ad un account, prevede un meccanismo di verifica che può richiedere fino a più di 5 settimane in termini di tempo. Infatti, sebbene sia possibile depositare, scambiare e ritirare criptovalute immediatamente fin dalla creazione di un account, per verificare un singolo account, e ottenere i permessi per la conversione delle criptovalute in moneta fiat (e viceversa) l'utente deve fornire il proprio numero di telefono, l'indirizzo e-mail, l'indirizzo di residenza (con una prova a supporto dello stesso, come ad esempio una bolletta di una utenza risalente a non oltre 3 mesi prima della richiesta), due "forme di identificazione" emesse dal governo (ad esempio carta d'identità o patente) e un estratto conto bancario sotto la stesso nome.

OKEx

L'exchange operante ad Hong Kong[176], pone limiti alle singole transazioni avvalendosi dell'utilizzo di tre livelli di verifica.

- Livello 1: presenta un limite di 10.000 $ per singola transazione (che diventa di 2.000 $ se la stessa implica moneta fiat), richiedendo in cambio i dati del cliente relativi a: nazionalità, nome reale e un numero identificativo reale (ad esempio l'ID).
- Livello 2: specificamente pensato per il trading, richiede, per le singole transazioni di importo superiore a 10.000 $ la verifica dei documenti di identità. Gli utenti dovranno fornire tre immagini alla piattaforma internet: le parti anteriore e posteriore della propria carta d'identità, e una dichiarazione, in cui si afferma che sono in possesso del documento d'identità rilasciato dal governo.

[175] "Social Security Number": codice a 9 cifre utilizzato negli USA per identificare univocamente le persone fisiche.

[176] Sebbene OKEx non accetti account di residenti ad Hong Kong per quanto precedentemente detto relativamente alla normativa cinese in ambito criptovalute.

- Livello 3: consente transazioni superiori a 200.000 $ fino ad un massimo di 500.000 $ che però richiedono una forma di "verifica video[177]". L'utente dovrà scaricare l'applicazione OKEx oltre a completare le verifiche previste dai livelli 1 e 2.

Kraken

Kraken nel proprio meccanismo di verifica prevede 5 livelli di requisiti, a seconda di come viene utilizzato un determinato account.

- Livello 0: l'unico requisito richiesto è un indirizzo email. Questo livello non consente però depositi, scambi o prelievi.
- Livello 1: Per iniziare il trading è necessario inserire i propri dati anagrafici (nome completo, data di nascita, paese di residenza e numero di telefono). Tuttavia, sebbene siano permesse le negoziazioni sia in valute digitali che fiat, i depositi e prelievi possono essere effettuati solo in valute virtuali.
- Livello 2: oltre ai requisiti previsti dal livello precedente (1), è necessario fornire un indirizzo di residenza. A seconda del Paese di residenza, l'appartenenza a questo livello consente l'accesso a disponibilità di finanziamenti in valuta fiat, nonché depositi e prelievi.
- Livello 3: per il livello 3, oltre ai livelli 1 e 2 è necessario caricare un documento di identità valido e una recente prova di residenza. In alcune situazioni, è necessaria un'ulteriore conferma dell'ID (presentando una propria foto personale che dimostri la proprietà dell'ID e una dichiarazione scritta). Questo livello consente limiti di finanziamento più elevati rispetto al livello 2 e il deposito di moneta fiat negli Stati Uniti, in Canada, Germania, Giappone ed altri paesi.
- Livello 4: quest'ultimo livello rappresenta gli account di maggior valore ed è disponibile sia a livello individuale che aziendale. I requisiti sono gli stessi del livello

[177] Tale procedura all'interno dell'ordinamento italiano è descritta dettagliatamente nell'Allegato 3 delle "Disposizioni in materia di adeguata verifica della clientela" emesse da Banca D'Italia nel mese di aprile 2018. La verifica video deve essere svolta in maniera tale da consentire una chiara visualizzazione del soggetto della stessa, senza presentare disturbi a livello di nitidezza/luminosità e con un audio chiaramente udibile. Inoltre, l'operatore preposto a tale attività acquisisce in anticipo i dati identificativi forniti dal cliente, richiede allo stesso l'esibizione di un documento di identità valido e ne verifica il codice fiscale. La sessione audio/video deve essere svolta seguendo una procedura scritta avente dei contenuti minimi previsti dalla normativa ed è interamente registrata e conservata.

3 con l'aggiunta di un modulo applicativo firmato dal richiedente e di documenti in ambito KYC.

Ad oggi tale piattaforma Exchange accetta come moneta fiat: USD, EUR, GBP, JPY e CAD.

Binance

La piattaforma in oggetto è, a detta di Yahoo Finance, il più grande exchange del mondo di scambio fra criptovalute (per volume di scambi). Binance infatti non supporta lo scambio tra criptovalute e moneta fiat. Per prelievi fino a due BTC al giorno, non è richiesta alcuna verifica dell'identità, cosa che invece viene richiesta per prelievi fino a 100 BTC al giorno tramite il caricamento di un documento di identità con foto.

CONCLUSIONI

Quando si affrontano argomenti sviluppatisi recentemente, ad alto impatto innovativo e non ancora del tutto approfonditi in tutte le relative sfaccettature, risulta complicato e soprattutto risulterebbe sbagliato dare dei giudizi netti o arrivare a delle conclusioni certe. Sicuramente perciò sarebbe difficile poter affermare che la tecnologia Blockchain sarà il futuro di tutti i sistemi di pagamento o che le criptovalute abbiano portato ad un aumento del riciclaggio di denaro o del finanziamento del terrorismo. In ogni caso però, in seguito all'analisi svolta, si possono certamente fare alcune interessanti riflessioni. A tal fine, per rendere il processo il meno ambiguo possibile cercherò di renderlo ordinato e chiaro suddividendolo in due parti: una relativa ad alcune considerazioni sulla prima metà dell'elaborato, ossia sulla tecnologia Blockchain e l'altra riguardante lo stato attuale della regolamentazione delle criptovalute a livello europeo ed internazionale considerandone anche gli eventuali possibili sviluppi.

Per quanto visto nel primo capitolo, risulta innegabile che la Blockchain sia una delle più importanti innovazioni del ventunesimo secolo, probabilmente la più importante in ambito finanziario. Questa tecnologia, che permette di fornire un "certificato crittografico" univoco ed immodificabile a garanzia dell'esecuzione di una transazione, senza l'esigenza di un soggetto o di un intermediario che funga da "validatore", è sicuramente un elemento rivoluzionario che potrà portare benefici in futuro in termini di costi e di rapidità dei processi. Dall'altro lato però, le soluzioni offerte ad oggi dalla Blockchain, perlomeno nelle configurazioni prevalenti ossia ispirate a quella del sistema Bitcoin (quindi basate su un meccanismo di Consensus di tipo "Proof of Work") sono difficilmente sostenibili su larga scala. Ciò è dovuto in primis al fatto che, mentre anno dopo anno le autorità ed i regolatori cercano di tutelare sempre di più i partecipanti al sistema finanziario (soprattutto le parti più "deboli") fornendo garanzie sul risparmio e sugli investimenti degli stessi (vedasi ad esempio la garanzia sui depositi) e regolamentandone le possibilità di investimento e pagamento (come ad esempio fanno le Direttive europee MIFID o PSD[178]) imponendo

[178] Rispettivamente per quanto riguarda le direttive Mifid si fa riferimento alle direttive europee 2004/39/CE e 2014/65/EU, mentre per le Payment Services directives alle 2007/64/Ce e 2015/2366.

limitazioni in tali ambiti in base alle caratteristiche e alle conoscenze dei singoli individui o alle tipologie di società, al contrario le criptovalute e la tecnologia Blockchain su cui si basano, lasciano in un certo senso l'utilizzatore in "balia di se stesso", a farsi carico dei rischi (elevatissimi) che caratterizzano questi strumenti e che vanno dall'imprevedibile volatilità fino alla possibilità di attacchi informatici o di compromissioni delle chiavi crittografiche che risultano fondamentali per stabilire la proprietà delle proprie valute virtuali.
Un ulteriore problema non trascurabile, è quello relativo ai consumi ed ai problemi a livello ambientale che vengono causati dal mining al fine di mantenere l'integrità del sistema: in un momento storico nel quale i principali settori dell'economia si impegnano a ridurre il proprio impatto ambientale e gli investitori acquisiscono sempre maggiore consapevolezza in termini di eticità e sostenibilità riguardo alle attività nelle quali fanno confluire il proprio capitale, è impensabile che una innovazione che si candidi a cambiare il modo in cui si eseguono le transazioni finanziarie e si registrano i relativi dati, presenti costi così elevati a livello ambientale. Ciò dunque, pur riconoscendo che i sistemi Peer-to-Peer su cui si basano le criptovalute potrebbero consentire una maggiore inclusione finanziaria a livello mondiale[179], pone un importante punto interrogativo riguardo alla sostenibilità di tale tecnologia. A tal proposito però, secondo l'opinione di chi scrive, soluzioni per così dire "intermedie" come quelle presentate in particolare dal protocollo Ripple, potrebbero delinearsi come un buon connubio tra l'attuale sistema dei pagamenti (con le relative regolamentazioni e tutele) e "l'anarchia controllata" che caratterizza le criptovalute nella loro forma più pura. La soluzione proposta dalla Startup californiana infatti, come si è visto, permette di adattarsi ai sistemi interni già precostituiti di banche ed intermediari finanziari non andando a stravolgerne la conformazione interna in termini di presidi di gestione del rischio, contrasto al riciclaggio e di conformità alle normative (compliance), unendo a ciò minori costi a livello ambientale.

Come si è visto anche tramite il lavoro svolto dall'Università di Sidney[180], è probabilmente ancora prematuro stabilire se le criptovalute abbiano spinto l'aumento del fenomeno del riciclaggio nel mondo o meno, quello che però è certo, è che questi nuovi strumenti

[179] Secondo i dati forniti dalla World Bank, nel 2017, l'esclusione finanziaria a livello mondiale si attestava al 31% della popolazione. Fonte: "http://ufa.worldbank.org".
[180] Foley S., Karlsen J., Putnins T., "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", University of Sidney, Gennaio, 2018.

favoriscono il compimento di tali attività illecite fornendo maggiore anonimato alle operazioni e permettendo di rendere in alcuni casi impossibile risalire all'identità dell'utilizzatore se quest'ultimo utilizza servizi di tumbling, accede alla rete con software Tor, si serve di criptovalute meno trasparenti di altre o esegue scambi in presenza trasferendo le criptovalute in maniera diretta attraverso la cessione di dispositivi hardware mobili (la forma più anonima di tutte).

Date queste premesse, è evidente il bisogno di un maggiore sforzo da parte delle autorità per regolamentare il fenomeno in modo tale da ridurre le possibilità che capitali illegali entrino all'interno del sistema tradizionale grazie all'utilizzo delle criptovalute. Certamente un buon passo in avanti, a livello nazionale ed europeo, è stato compiuto con il *D.lgs. n. 90/2017 e la V Direttiva UE antiriciclaggio*, attraverso i quali si è cercato, oltre a fornire una definizione giuridica al fenomeno, di regolamentare il punto di contatto tra l'economia reale e il criptomercato (ossia il momento in cui avviene la conversione da moneta fiat a criptovaluta o viceversa) e di includere all'interno dei "soggetti obbligati" le entità come gli Exchange che operano in questo ambito.

A livello internazionale poi, come abbiamo visto analizzando le normative dei vari stati, si può notare che, se già si riscontrano differenze nell'inquadramento giuridico del fenomeno (con paesi che definiscono le valute virtuali come commodities, altri come strumenti di pagamento o rappresentazioni digitali di valore) queste vengono ulteriormente acuite nel momento in cui ci si addentra maggiormente nelle prescrizioni più tecniche e specifiche, per le quali ogni ordinamento prevede le proprie disposizioni più o meno restrittive. Ciò, se confrontato con lo sviluppo storico della normativa antiriciclaggio riguardante "l'economia tradizionale", che, anche grazie alle raccomandazioni del G.A.F.I., è arrivata ad un buon grado di uniformità a livello mondiale, riuscendo negli anni anche a ridurre la presenza di paradisi offshore e di intermediari per così dire "opachi", evidenzia ancora di più il fatto che, con l'avvento delle criptovalute il problema sembra ritornato alla sua fase embrionale, con il rischio che si sviluppi un mercato parallelo a quello tradizionale e meno regolamentato, che canalizzi al suo interno un gran numero di operazioni illecite che si era tentato faticosamente di arginare. Al contempo però, al fine di non ostacolare lo sviluppo (che ricordiamo si trova comunque in una fase che sebbene non sia totalmente embrionale è comunque lontana dal configurarsi come matura), di un fenomeno tanto innovativo quanto delicato a livello di impatto sociale come le criptovalute, è bene non imbrigliare

eccessivamente queste ultime con regolamentazioni, fattore che potrebbe renderle meno attrattive, facendone scemare l'interesse negli utilizzatori. Ciò infatti potrebbe rivelarsi come un fattore controproducente dal momento che finirebbe per impedire che si possano sviluppare implementazioni più efficaci della tecnologia che consentano il superamento di alcuni dei limiti che ad oggi la affliggono. Inoltre, come si è visto nel caso della Cina, una regolamentazione eccessivamente ostruzionistica non favorisce né gli utilizzatori né il mercato in quanto porta il fenomeno a svolgersi ancora più al di fuori delle frontiere controllate, distruggendo i benefici che si potrebbero ottenere con un'adeguata implementazione dello stesso all'interno del sistema economico[181].

Tutto ciò ci porta ad affermare che sicuramente ci sia bisogno di una regolamentazione, ma che questa, più che eccessivamente stringente, debba essere ben condivisa a livello internazionale stabilendo alcune norme di base che permettano di inquadrare il fenomeno e disciplinarne le pratiche esecutive senza però soffocarne i possibili benefici. Perciò, risulta di fondamentale importanza non arrivare obbligatoriamente ad una definizione giuridica uniformemente condivisa da tutti i regolatori per il concetto di "valuta virtuale" quanto piuttosto focalizzare l'attenzione su determinate attività svolte attraverso l'utilizzo delle criptovalute (come ad esempio è stato fatto per la conversione da o in moneta fiat) e figure (piattaforme di Exchange, miners, siti di informazione finanziaria ecc.) che operano all'interno di questo mercato.
Una procedura che senza dubbio dovrebbe essere più chiara e condivisa è quella della verifica della clientela nell'ambito delle piattaforme di Exchange, infatti anche se le norme in molte giurisdizioni prevedono che queste ultime svolgano l'identificazione dei propri clienti, questo meccanismo non viene descritto in termini concreti ed operativi che tengano conto della relativa unicità dello stesso e possano eventualmente prevedere processi aggiuntivi rispetto alla adeguata verifica della clientela "tradizionale". Considerato l'elevato anonimato presente nelle criptovalute, soprattutto in quelle di più recente creazione (Monero, DASH, ecc.) non risultano sufficienti eventuali tecniche simili a quelle

[181] In Cina infatti, come menzionato all'interno del paragrafo dedicato, l'utilizzo delle criptovalute risulta essere tra i più elevati a livello mondiale (sebbene sia proibito dallo stato per gli intermediari finanziari e consentito solo ai singoli) e nel paese si riscontra il maggior numero di pool di miners Bitcoin (circa il 50% del totale).

implementate nella ricerca effettuata dall'università di Sidney[182] per riuscire ad identificare le reali controparti che si celano dietro i differenti account e soprattutto analizzare le eventuali attività a fini illeciti da queste svolte. A tal proposito sembrano invece interessanti alcune tecniche di verifica proposte da alcune piattaforme Exchange[183] che prevedono una verifica via via più dettagliata della controparte con cui interagiscono a seconda dei servizi con i quali sarà permesso di operare a quest'ultima, arrivando anche a forme di verifica video per i livelli di operatività maggiore.
Qualche tentativo di regolamentazione internazionale in materia di criptovalute a dire il vero c'è stato, infatti durante il G-20 dello scorso marzo (2018) le principali autorità mondiali si erano riproposte di analizzare e trattare tali temi, purtroppo però il summit si è concluso rimandando la designazione di principi comuni e prefiggendosi solamente di continuare l'osservazione di un mercato sempre in rapida evoluzione.

Per tutte le riflessioni effettuate, ritengo che il fenomeno delle criptovalute e la tecnologia Blockchain su cui queste ultime si basano, non debbano essere visti come una sostituzione delle attuali istituzioni finanziarie o una contrapposizione all'odierno sistema economico, bensì come nuovi strumenti, basati su innovazioni a livello tecnologico, che possano essere utilizzati dai partecipanti al mercato finanziario e non, per favorire il progresso e la modernizzazione dell'attuale sistema economico in una vastità di ambiti che non si sostanziano solo all'interno del sistema dei pagamenti e che per tale ragione si debbano muovere in maniera non parallela ma integrata all'economia e alla struttura del mercato "reale".

[182] La già citata ed analizzata: Foley S., Karlsen J., Putnins T., "Sex, drugs, and bitcoin: "How much illegal activity is financed through cryptocurrencies?" University of Sidney, gennaio 2018.
[183] Vedasi ad esempio il caso di Okex presentato nell'ultimo paragrafo del terzo capitolo.

BIBLIOGRAFIA

- Drescher D., “Blockchain Basics: A Non-Technical Introduction in 25 Steps”, Apress, 2017.
- Swan M., “Blockchain: Blueprint for a new economy”, 2015.
- Halaburda H., Sarvary M., “Beyond Bitcoin: The economics of digital currencies”, Palgrave Macmillan, 2016.
- Kelly Brian, “The Bitcoin Big Bang: How alternative Currencies are about to change the world”, Wiley, 2014.
- S. Capaccioli, “Criptovalute e Bitcoin: un’analisi giuridica”, Giuffrè Editore, 2015
- D. LEE Kuo Chuen, R. H. DENG: “Handbook of blockchain, digital finance and inclusion – volume 2”, Elsevier, 2018.
- Rapporto Clusit sulla sicurezza ICT in Italia, 2018.
- Enisa, “Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector”, Dicembre 2016.
- Gobierno Bolivariano de Venezuela: “El Petro”, 15 marzo 2018.
- IMF Staff Discussion Note, “Virtual Currencies and Beyond: Initial Considerations”, gennaio 2016.
- Allen & Overy, LLP, “Anti-Money Laudering Regulation of Cryptocurrency: U.S. and Global Approaches”, 2018.
- Baltic Journal of Economic Studies, VOL. 4, No. 1, gennaio 2018.
- D. Holman, B. Stettner, “Anti-money Laundering Regulation of Cryptocurrency” ICLG, 2018.
- D.Schwartz, N. Youngs, “The Ripple Consensus Protocol”, Ripple lab. 2014.
- Decreto legislativo 25 maggio 2017, n. 90 (Italia).
- Direttiva (UE) 2015/849, 20 maggio 2015
- Direttiva (UE) 2018/843, 30 maggio 2018.
- School of Business and Economics, “The Cryptocurrency Tumblers: Risks, Legality and Oversight”, 30 novembre 2017.
- Testo Unico Bancario, Decreto legislativo 1 settembre 1993, n. 385.

SITOGRAFIA

- Blockchain: https://www.blockchain.com
- Ripple: https://ripple.com/
- Ethereum: https://ethereum.org
- Banca Centrale Europea: https://www.ecb.europa.eu/ecb/html/index.it.html
- Coinmarketcap: https://coinmarketcap.com
- Monero: https://getmonero.org
- DASH: https://www.dash.org
- ZCash: https://z.cash
- Verge: https://vergecurrency.com
- NAV: https://navcoin.org
- Enciclopedia Treccani: http://www.treccani.it/
- Il Sole 24 Ore: http://www.ilsole24ore.com
- Visa: https://www.visaitalia.com
- Paypal: https://www.paypal.com/it/home
- Gobierno de Venezuela: http://www.presidencia.gob.ve/Site/Web
- Bank of Japan: https://www.boj.or.jp/en/index.htm/
- Financial Crimes Enforcement Network: https://www.fincen.gov/
- U.S. Security and Exchange Commission: https://www.sec.gov/
- Bitlicense: https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm
- Bitcoin Magazine: https://bitcoinmagazine.com
- People's Bank of China: http://www.pbc.gov.cn/english/130437/index.html
- Central Bank of United Arab Emirates: https://www.centralbank.ae/en/
- Central Bank of the Russian Federation: https://www.cbr.ru/eng/
- Borsa Italiana: https://www.borsaitaliana.it/
- Fastweb: https://www.fastweb.it
- National Institute of Standars and Technology: https://www.nist.gov
- NEM: https://nem.io
- Investopedia: https://www.investopedia.com