Dipartimento di Economia e Finanza

Cattedra di Diritto dei Mercati e degli Intermediari Finanziari

La Disciplina Antiriciclaggio e il Nuovo Approccio Legato alle Valute Virtuali

Relatore:
Prof.ssa Mirella Pellegrini

Candidato:
Andrea Ceci
Matr.690911

Correlatore:
Prof.ssa Paola Lucantoni

Anno Accademico 2017/2018

INDICE

CAPITOLO III

LA V DIRETTIVA E GLI STRUMENTI DI CONTRASTO

INTRODUZIONE

Sono sempre stato affascinato dal fenomeno internet con i suoi limiti e con le grandi opportunità che offre.

Nelle navigazioni effettuate sono venuto a conoscenza dell'esistenza del dark web e ho scoperto che offriva la possibilità di effettuare tutta una serie di acquisti relativamente a sostanze proibite, armi e, addirittura, assoldare sicari.

Il pagamento proposto poteva avvenire tramite alcune valute virtuali; la qual cosa ha suscitato in me un interesse.

Mi sono chiesto, cosa sono e come funzionano le criptovalute? E, ancora, sono soggette ad una disciplina come le altre valute? Perché, sulle suddette pagine web si richiede il loro utilizzo?

Quindi, per sviluppare l'argomento mi sono reso conto della necessità di valutare le normative vigenti in funzione, soprattutto, di un potenziale uso illecito delle criptovalute.

Da qui la necessita di ripercorrere i capisaldi delle normative vigenti in particolare le direttive antiriciclaggio, specificatamente a fenomeni di facilitazione del riciclaggio di denaro riveniente da attività illecite o criminali.

Sarà, altresì, necessario, soffermarsi su come sono nate e come operano le stesse, la principale delle quali è il Bitcoin.

Questa parte, ancorché, molto tecnica, è importante per individuare quegli aspetti che rispondono alla mia domanda principale: perché ne viene richiesto il ricorso per regolare queste transazioni illecite che sconfinano anche in supposte operazioni criminali.

Da qui condurrò un'indagine per capire se è effettivamente possibile effettuare operazioni di riciclaggio tramite le valute virtuali.

In effetti, scopriremo che è proprio la loro struttura e le piattaforme che le regolano e che ne determinano, spesso, una difficile tracciabilità e che quindi hanno attratto l'attenzione di soggetti dediti ad attività criminose.

Osserveremo, quindi, qual è stata la risposta dell'Unione Europea, in particolare attraverso la V Direttiva, e se questa è sufficiente a contrastare il fenomeno.

CAPITOLO I

IL FENOMENO DEL RICICLAGGIO E L'EVOLUZIONE NORMATIVA

1.1 PREMESSA: RICICLAGGIO, FINANZIAMENTO DEL TERRORISMO E AUTORICICLAGGIO.

Il riciclaggio è un'attività che consiste nell'utilizzare denaro e beni di provenienza illecita reinvestendo gli stessi in attività legali avendone occultato la provenienza mediante determinate operazioni finanziarie. L'illegalità di queste deriva dal legame con il reato che ha determinato i proventi finanziari. Lo scopo di tali operazioni, infatti, è proprio quello di rendere impossibile ricostruire i movimenti dei capitali in questione fino all'evento delittuoso che li ha generati. Tale *modus operandi* costituisce per le organizzazioni criminali non solo un ulteriore importante strumento di finanziamento, dal momento che le stesse hanno già ingenti profitti dalle attività illegali, ma anche, attraverso il controllo di una vasta rete di attività finanziarie e produttive, la possibilità di diffondersi sul territorio, controllarlo ed inserirsi all'interno del tessuto economico e sociale.

Il reato di riciclaggio viene definito dalla normativa nell'art. 2, d.lgs. n. 231/2007, che prevede espressamente: «*Ai fini di cui al comma 1, s'intende per 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».* Secondo il novellato quinto comma dell'art. 2 del d.lgs. n. 231/2007, inoltre, il riciclaggio è considerato tale *«anche se le*

attività che hanno generato i beni da riciclare si sono svolte fuori dai confini nazionali», confermando l'indicazione interpretativa per *cui «la conoscenza, l'intenzione o la finalità, che debbono costituire un elemento delle azioni di cui al comma 4, possono essere dedotte da circostanze di fatto obiettive»*[1].

Inoltre, in linea con gli ordinamenti internazionali e con le direttive comunitarie viene equiparato al riciclaggio qualsiasi attività finalizzata alla creazione di risorse economiche, il cui obiettivo è quello del compimento di delitti con finalità terroristiche, creando in tal modo nuovi ambiti applicativi per la normativa antiriciclaggio in merito alla lotta al terrorismo sul piano finanziario[2]. Infatti, i tragici attentati del 2001 hanno mostrato il possesso da parte di alcuni network terroristici internazionali di una grande disponibilità finanziaria, mostrando la gravità e l'attualità del pericolo connesso al riciclaggio di capitali e all'inserimento di gruppi eversivi all'interno dei circuiti economici e finanziari globali[3]. Le definizione del reato di finanziamento del terrorismo viene esplicitata per effetto del Decreto Legislativo 25 maggio 2017, n. 90, l'articolo 2, comma 6*,* del d.lgs. n. 231/2007: «*ai fini di cui al comma 1, s'intende per finanziamento del terrorismo 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»*[4]*.* Di conseguenza è rilevante per la disciplina antiriciclaggio, non solo, la creazione, la movimentazione e l'utilizzo di ricchezza di provenienza illecita, ma anche, la creazione, se pur lecita, della stessa se finalizzata a sostenere sul piano finanziario attività di tipo terroristico. Infatti, sebbene il riciclaggio di denaro e il finanziamento del terrorismo siano fenomeni distinti, ciascuno con la propria ratio e le proprie peculiarità, *de facto* essi utilizzano le stesse tecniche di occultamento nel portare a termine i propri fini illeciti.[5] Nel riciclaggio, *money laundering*, gli artifici finanziari vengono utilizzati per nascondere la provenienza del denaro, cercando di "lavarlo" rendendolo lecitamente riutilizzabile. Invece per quanto riguarda il finanziamento del terrorismo, *money dirtying*, gli stessi metodi hanno la finalità di nascondere la fonte dei capitali, che non deve essere necessariamente illegale, per riutilizzarla in seguito. Il nesso tra le due attività, dunque, consiste in quell'insieme di tecniche

[1] Cfr. art. 2, comma 2, d.lgs. n. 231/2007. Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione.

[2] Capriglione Francesco. Manuale di diritto bancario e finanziario. Milano: Wolters Klower, 2016, p. 526.

[3] Baccarini Andrea Piergiorgio. Unione Europea e riciclaggio di denaro del terrorismo internazionale e della criminalità organizzata. Nella rivista Amministrazione in Cammino. 2006.

[4] Cfr. art. 2, comma 6, d.lgs. n. 231/2007. Cit.

[5] Kersten Armand. Financing of Terrorism - A Predicate Offence to Money Laundering? European Journal of Law Reform, n. 4, 2002, p. 306.

finanziarie atte a rendere irrintracciabili i flussi di denaro. Per questo entrambi i reati sono soggetti al medesimo regime, definito AML/CTF, ovvero *Anti Money Laundering and Counter Terrorism Financing*.

Infine, è fondamentale determinare il reato di autoriciclaggio e sottolinearne la differenza da quello di riciclaggio. Dal 1° gennaio 2015 è in vigore la nuova fattispecie dell'autoriciclaggio, novità estremamente importante, in quanto vengono sanzionati per il reato di riciclaggio solamente i soggetti estranei che autonomamente contribuiscono al consolidamento dei patrimoni ottenuti illegalmente[6], mentre coloro che hanno commesso i reati alla base venivano puniti solamente per quelle scelte delittuose e non per la manifestazione di consumo o di autoriciclaggio del ricavato[7]. Come si evince dall' articolo 648-bis c.p., che ne regola le norme sanzionatorie: *"Fuori dei casi di concorso nel 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[8]"*.

Invece, dall'introduzione dell'articolo 448-ter c.p. viene sanzionato: "*Chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa[9]"*. Quindi, in poche parole, il reato di autoriciclaggio punisce non solo la condotta del soggetto che fa rientrare i soldi sporchi nell'economia legale ma che ha anche compiuto o concorso a commettere il reato non colposo che sta a monte, mentre risponde del reato di riciclaggio chi non ha concorso nel reato alla base ma ha ripulito i soldi sporchi nell'interesse di chi ha compiuto il delitto.

Nel nostro paese l'introduzione di una fattispecie *ad hoc* legata al riciclaggio è nata in seguito alla volontà di contrastare reati tipici delle organizzazioni mafiose come le estorsioni e i sequestri di persona a scopo di estorsione, mentre a livello internazionale, come si vedrà in seguito analizzando le prime convenzioni internazionali, è stato il traffico di droga, e la sua crescita esponenziale, ad indurre i legislatori a porre la attenzione sulla necessità di contrastare questa enorme fonte di finanziamento per le organizzazioni criminali.

---

[6] Nanulla Gaetano. La lotta alla mafia. Milano: Giuffrè, 2012, pag. 319.

[7] Brizzi Ferdinando, Capecchi Gianluca, Rinaudo Antonio. La reimmissione della liquidità illecita nel circuito economico ed il delitto di reimpiego tra prevenzione patrimoniale e giustizia penale: prospettive di future armonizzazioni. In archivio penale(web) 2014.

[8] Cfr. art. 648-bis c.p. art.5 della legge 9 agosto 1993. Ratifica ed esecuzione della convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato, fatta a Strasburgo l'8 novembre 1990.

[9] Cfr. art. 648-ter c.p. art.3 della legge Dicembre 2014, n°186. Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio.

Negli ultimi decenni il riciclaggio di proventi illeciti ed il loro conseguente reinvestimento è aumentato in maniera esponenziale sia sul piano nazionale che su quello internazionale. Tra le principali cause di questo preoccupante sviluppo possiamo annoverare:

- i progressi tecnologici, quali internet e altri sistemi online capaci di velocizzare notevolmente i trasferimenti di denaro e gli investimenti di risorse economiche, connettere virtualmente luoghi geografici situati anche in continenti opposti e mantenere l'anonimato;
- la globalizzazione dei mercati, ossia l'abbattimento delle frontiere e l'integrazione con Paesi caratterizzati da economie emergenti;
- la sofisticazione dei servizi d'investimento e dei prodotti finanziari;
- l'adozione della moneta unica con riferimento esclusivo al contesto europeo[10].

Appare chiaro come la globalizzazione e l'internalizzazione dei mercati finanziari hanno consentito alle organizzazioni criminali di espandersi, agevolando l'attività di riciclaggio a cavallo di più ordinamenti nazionali. L'abbattimento delle frontiere interne ed esterne consente di spostare i capitali nei c.d. paradisi fiscali. Questi ultimi sono degli stati non collaborativi alla lotta all'evasione fiscale e al riciclaggio sia dal punto di vista giuridico sia da quello finanziario. Spesso sono caratterizzati da regimi fiscali blandi, dal segreto bancario che garantisce l'anonimato ai titolari di depositi e la possibilità di compiere transazioni finanziarie coperte e da un insieme estremamente agevolato di requisiti contabili e societari per la costituzione di società di servizi finanziari. Queste "zone franche" sono vere e proprie calamite per i proventi da reato, dove è possibile realizzare consistenti evasioni fiscali e accumulare fondi che potrebbero essere destinati al finanziamento del terrorismo[11].
Inoltre, l'evoluzione tecnologica nei sistemi di pagamento e della trasmissione di denaro garantiscono non solo grande velocità e sicurezza nella trasmissione di denaro ma, essendo la finanziarizzazione dell'economia un processo in continua evoluzione, anche nuove tecniche per poter riciclare il denaro sporco garantendosi l'anonimato. Un esempio calzante è quello delle valute virtuali, dei money transfer e dell'economia digitale in generale, tema che tratteremo più avanti nella trattazione.

[10] Razzante Ranieri. La regolamentazione antiriciclaggio in Italia. Aggiornato alla delibera della Banca d'Italia 10 marzo 2011 sui controlli antiriciclaggio. Torino: G. Giappichelli Editore, 2011, p.1.
[11] Grasso Pietro. Prefazione, in Elementi normativi internazionali e nazionali in materia di riciclaggio, Bari: Cacucci, 2010, pag. 14.

1.2 GLI EFFETTI E LE FASI DEL RICICLAGGIO

Gli effetti prodotti dal riciclaggio sono molteplici. In *primis*, il reinvestimento dei profitti generati dalle attività illecite costituisce una vera e propria linfa vitale per le organizzazioni criminali, moltiplicandone la forza economica e la diffusione. Esso è alla base della crescita e del proliferarsi delle imprese criminali, in quanto le stesse, accumulando grandi ricchezze, hanno bisogno del mercato dei capitali per svolgere tre funzioni: riciclare i patrimoni, ossia dare ad essi un crisma di legalità collocandoli in attività fuori della portata degli investigatori e realizzando un numero tale di transazioni finanziarie da recidere i legami con la loro fonte; garantire a quei patrimoni il grado di liquidità richiesta dalla conduzione di attività illegali soggette a elevata incertezza; investire i patrimoni in forma redditizia[12]. Tutto ciò, tra l'altro, genera enormi difficoltà ad imprese ed imprenditori che svolgono la propria professione in modo legale. Infatti, nel mercato imprenditoriale l'impresa criminale può produrre alterazioni profonde della concorrenza, in quanto gli imprenditori che agiscono legalmente, e sostengono una serie di costi in base ai quali fissano i prezzi di acquisto e di vendita, non sono in grado di sostenere la concorrenza di soggetti, che operano con la disponibilità di illeciti mezzi finanziari a costi largamente inferiori e in misura superiore a quella dei concorrenti.
Ad aggravare la situazione si aggiunge l'utilizzo di metodi criminali ed intimidatori che permettono alle imprese criminali di ridurre i costi e i rischi connessi all'attività imprenditoriale. Basti pensare alla collusione e alla corruzione per aggirare i costi burocratici o all'intimidazione per risolvere problematiche con i lavoratori, i sindacati e i fornitori. Tutto ciò porta l'impresa criminale a poter esercitare una posizione di monopolio all'interno del mercato, che non danneggi solamente gli attuali concorrenti, ma anche i possibili concorrenti che desiderassero entrare nel settore. Da notare, inoltre, che i criminali tendono particolarmente ad entrare nel mercato nei periodi di recessione, durante i quali i concorrenti hanno una contrazione delle risorse, mentre essi possono contare sulle risorse di illecita provenienza[13].
Dal punto di vista macroeconomico il riciclaggio destabilizza l'assetto del finanziario del "sistema paese" per la volatilità dei tassi di cambio e dei tassi di interesse, determinati da trasferimenti transfrontalieri non facilmente monitorabili. Tutto ciò ha ripercussioni negative sul gettito fiscale e sulla ripartizione della spesa pubblica a causa di un'errata valutazione della ricchezza.
Il riciclaggio è un fenomeno estremamente complesso. Parte di questa complessità deriva dal comportamento dell'operatore giuridico che, modificando continuamente la norma e rendendola sempre più complessa e completa, spinge il criminale a ricercare nuovi metodi, sempre più affinati,

[12] La Gala Canio Giuseppe. Il riciclaggio di denaro: Strumenti di contrasto e misure patrimoniali. Supplemento al n.4/2000 della rassegna dell'Arma dei Carabinieri. 2000, p.16.
[13] Zanchetti Mario. Il riciclaggio di denaro proveniente da reato. Milano: Giuffrè, 1997.

per sfuggire al campo applicativo[14]. Al passo con le tecniche criminali si è evoluta anche l'analisi criminologica. Inizialmente il fenomeno veniva strutturato in due fasi, *Money Laundering* e *Money Recycling,* successivamente si è passati ad una divisione in tre fasi; ovvero:

- *Placement stage:* ossia la fase di collocamento nel mercato dei proventi illeciti. L'obbiettivo perseguito da questa fase è quello di "sbarazzarsi" del denaro contante e trasformalo in c.d. "moneta scritturale", fisicamente impalpabile e rappresentata da saldi attivi presso le istituzioni finanziarie[15]. Ciò avviene attraverso operazioni di deposito, cambio, acquisto di strumenti finanziari e trasferimento di denaro contante. Il "collocamento" può essere svolto presso istituti finanziari tradizionali, come le banche o le assicurazioni, o presso quelli non tradizionali, come uffici di cambio, venditori di metalli preziosi, mediatori di merci - al fine di cambiare la forma dei profitti, camuffandola in diritti su beni di alto valore - ed infine casinò. Per rendere più difficile il compito a chi volesse ricostruire i flussi di denaro e a causa dei limiti di denaro movimentabile imposti dalle autorità, i versamenti vengono frazionati. Questa tecnica, chiamata *"smurfing",* consiste nell'aprire più conti in una stessa banca o in più banche diverse attraverso dei prestanome.
- *Layering stage:* Questa fase ha la finalità di camuffare qualsivoglia collegamento tra il denaro riciclato e l'attività criminale da cui proviene. Si sostanzia in una stratificazione di trasferimenti e di riconversioni in denaro contante, spezzando in tal modo la traccia documentale dei trasferimenti, la c.d. *paper trail*[16]. Per ridurre i sospetti degli intermediari finanziari coinvolti sono state introdotte delle tecniche di "prelavaggio". Queste tecniche si sostanziano in operazioni di sovrafatturazione attraverso esercizi commerciali. Ad esempio, per banalizzare il meccanismo, un cinema o un teatro che dichiara più spettatori di quelli reali, staccando più biglietti e mettendo in cassa i profitti dei traffici illeciti.

  Le operazioni di "*layering"* sono spesso sofisticate e complesse, in quanto consistono in trasferimenti internazionali di fondi, operazioni societarie in paesi off-shore e transazioni simulate[17].
- *Integration stage:* ovvero la fase di reinserimento del denaro sporco nel sistema legale.

[14] Maiello Vincenzo – Della Ragione Luca. Riciclaggio e reati nella gestione dei flussi di denaro sporco. Milano. Giuffrè Editore, 2018, pag. 58.
[15] Buonadonna Fabrizio – Tramontano Gennaro.Codice Antiriciclaggio. Normativa, Prassi, Giurisprudenza. Aggiornato al D.lgs 21 novembre 2007, N. 231. Macerata: Halley Editrice, 2008, pag. 13.
[16] Buonadonna Fabrizio – Tramontano Gennaro.Codice Antiriciclaggio. Normativa, Prassi, Giurisprudenza. Aggiornato al D.lgs 21 novembre 2007, N. 231. Cit. pag. 14.
[17] Stile Alfonso. Riciclaggio e reimpiego di proventi illeciti, pag.6.

Nella fase finale, dopo essere stati ripuliti vengono reimmessi nel sistema, spesso mescolandoli con i proventi di un'altra attività lecita. Ciò avviene dopo averli fatti transitare attraverso istituti finanziari di cui nessuno sospetterebbe.

1.3 DALLE ORIGINI DELLA DISCIPLINA ALLA II DIRETTIVA ANTIRICICLAGGIO

La necessità di contrastare del riciclaggio ebbe origine negli anni '80 con la comparsa delle prime normative internazionali. La comunità internazionale ritenne che tutti i possibili provvedimenti esclusivamente nazionali non sarebbero stati efficaci contro un fenomeno di carattere sempre più transnazionale, ma che fosse necessaria una linea comune. Infatti, istituire una normativa che arginasse in maniera efficace questo problema divenne ben presto una priorità per i legislatori nazionali e internazionali, i quali erano ben consci dello strettissimo legame tra il fenomeno e la criminalità organizzata e della necessità di evitare che le risorse economico-finanziarie di queste organizzazioni venissero reimpiegate nell'economia legale. Inizialmente la disciplina era proprio finalizzata al soddisfacimento di questa necessità ed era rivolta al contrasto del riciclaggio per ciò che concerneva esclusivamente il sistema finanziario e bancario. Solo successivamente, la normativa antiriciclaggio diventò anche uno strumento volto a indebolire le organizzazioni criminali, al fine di mantenere l'integrità e l'efficienza dell'intero sistema economico, finanziario e bancario[18].
In questo contesto maturò la giusta consapevolezza che fosse necessario "colpire" le organizzazioni criminali dal punto divista economico cercando di impedire che queste usassero il riciclaggio come forma di finanziamento, creando una fitta rete di protezione del sistema economico mediante il controllo sul mercato e la trasparenza dello stesso.
Una corretta normativa antiriciclaggio deve essere estremamente dinamica, in quanto è necessario che essa stia al passo con l'evolversi delle organizzazioni criminali e delle loro tecniche sempre più all'avanguardia.
Inoltre, la dimensione transnazionale del fenomeno ha imposto di adottare contromisure normative di analoga estensione che non esauriscano la propria efficacia al di fuori del livello nazionale. Infatti, come abbiamo visto in precedenza la globalizzazione dell'economia, l'integrazione dei mercati finanziari e strumenti finanziari innovativi sono un forte alleato di questo fenomeno. In proposito si è espresso anche Mario Draghi nella "Commissione Parlamentare d'Inchiesta Sul Fenomeno Della

[18] Razzante Ranieri. La regolamentazione antiriciclaggio in Italia. Aggiornato alla delibera della Banca d'Italia 10 marzo 2011 sui controlli antiriciclaggio. Cit. pag. 26-27.

Mafia e Sulle Altre Associazioni Criminali anche Straniere" affermando: *"Nelle sue forme più significative, il riciclaggio manifesta una marcata attitudine a svolgersi in un contesto internazionale. Articolando la propria azione in molteplici giurisdizioni, i criminali tendono a cogliere le opportunità offerte dalla globalizzazione dell'economia e dall'integrazione dei mercati finanziari. La possibilità di ricorrere a strumenti finanziari innovativi e la disponibilità di sofisticate tecnologie per la trasmissione delle informazioni e degli ordini consentono loro di agire con grande velocità, di stratificare molteplici atti di trasformazione e trasferimento, di operare a distanza in piazze diverse, di dissimulare l'identità degli attori e la titolarità effettiva dei beni*[19]*".*

1.3.1 I PRIMI ACCORDI INTERNAZIONALI

Il primo documento di carattere internazionale fu la raccomandazione "*Misure contro il trasferimento e la custodia di fondi di origine criminale"* emanata dal Comitato dei Ministri del Consiglio d'Europa il 27 giugno del 1980 e rivolta ai Paesi membri. Nella Raccomandazione si invitavano i legislatori ad intervenire sui sistemi bancari al fine di prevenire l'ingresso di capitali illeciti all'interno di istituzioni finanziarie e creditizi legittime.
Infatti, i richiedeva alle banche di:

- identificare i propri clienti nel momento in cui si instaurava un rapporto con gli stessi o nel caso di operazioni in contanti;
- sviluppare delle forme di collaborazione basate sullo scambio d'informazioni a livello nazionale e internazionale;
- istituire meccanismi di controllo casuali o sistematici per verificare la provenienza del denaro.

Successivamente fu di notevole importanza la "*Dichiarazione di principi concernenti la prevenzione dell'uso criminale del sistema bancario a fini di riciclaggio del denaro"*, sottoscritta il 12 dicembre 1988 a Basilea dai rappresentanti delle Banche Centrali e degli Organi di Vigilanza bancaria del Gruppo dei Dieci. Questa viene considerata una vera e propria pietra miliare nella lotta al riciclaggio, sui quali principi verrà basata tutta la futura disciplina in materia.
Le linee direttrici della Dichiarazione di Basilea sono:

[19] Draghi Mario. L'azione di prevenzione e contrasto al riciclaggio. Testimonianza nella Commissione Parlamentare d'Inchiesta Sul Fenomeno Della Mafia e Sulle Altre Associazioni Criminali, Anche Straniere. Roma, 22 luglio 2009.

- l'obbligo d'identificazione della clientela, con la contestuale esortazione a non eseguire operazioni d'importo elevato se l'identità della stessa sia dubbia;
- l'impegno delle banche a non portare a termine le operazioni richieste dai soggetti sospettati di riciclaggio;
- la collaborazione delle banche con le autorità inquirenti, nei limiti del rispetto della normativa interna preposta alla tutela della riservatezza della clientela.

La dichiarazione dei principi non ha propriamente carattere normativo, in quanto essa non impose alcun obbligo giuridico diretto ai singoli istituti di credito, e gli impegni assunti dai singoli paesi non furono coercibili; tuttavia, nonostante il contenuto di tale dichiarazione avesse carattere semplicemente formale, fu adottato da molti Stati[20].

Un punto di svolta nel percorso della disciplina fu la "*Convenzione ONU contro il traffico illecito di stupefacenti e sostanze psicotrope",* stipulata a Vienna nel dicembre 1988, in quanto fu la prima volta che un organismo internazionale adottasse un provvedimento vincolante nella lotta al riciclaggio. La convenzione evidenzia l'importanza della collaborazione tra gli Stati nella lotta contro la criminalità organizzata, focalizzandosi sul narcotraffico e sui proventi da esso derivanti e dando vita alla criminalizzazione del reato di riciclaggio in un elevato numero di paesi. Lo scopo dichiarato era quello di "*privare coloro che praticano il traffico illecito del frutto delle loro attività criminali ed eliminare in tal modo il loro movente principale[21]".* I Paesi Membri furono obbligati a introdurre nelle loro legislazioni delle disposizioni per il contrasto al narcotraffico e reati riguardanti la conversione o il trasferimento di beni illeciti. Queste disposizioni furono delineate dalla Convenzione solamente a grandi linee, a scapito dell'uniformità tra le varie normative; il che avrebbe favorito la cooperazione internazionale[22].

Nel febbraio 1990 il GAFI (*Gruppo d'Azione Finanziari Internazionale*; in inglese FATF: *Financial Action Task Force)* emanò 40 Raccomandazioni antiriciclaggio. Il GAFI è un organismo intergovernativo composto da esperti legali, penali e finanziari, istituito nel G-7 di Parigi nel 1989, con il compito di definire gli standard per la lotta al riciclaggio, il finanziamento del terrorismo e dei programmi di proliferazione delle armi di distruzione di massa promuovendone l'implementazione delle varie normative con riflessi sui regolamenti e sugli aspetti operativi.

Facciamo un piccolo excursus relativo al GAFI e alle Raccomandazioni

Le Raccomandazioni, adottate da 180 paesi considerati "cooperativi", costituiscono degli *standard* a cui i paesi si devono uniformare nel rispetto della struttura legale, amministrativa e operativa di

[20] Razzante Ranieri. La regolamentazione antiriciclaggio in Italia. Aggiornato alla delibera della Banca d'Italia 10 marzo 2011 sui controlli antiriciclaggio. Cit. p. 29.

[21] Cfr. art.1 della Convenzione ONU conto il traffico illecito di stupefacenti e sostanze psicotrope.

[22] Scapellato Filippo. Il fenomeno del riciclaggio e la normativa di contrasto. Torino: Giappichelli Editore, 2013, pag.22.

ciascuno degli stessi. Le prime Raccomandazioni erano dirette contro il riciclaggio dei proventi derivanti dal traffico di droga. Queste vennero aggiornate e modificate più volte e nel 1996 vennero integrate con attenzione ad un *range* più ampio di reati presupposto e prendendo in considerazione nuove tecniche di riciclaggio.

Sempre nel 1990 a Strasburgo intervenne nuovamente il Consiglio d'Europa tramite la *Convenzione sul riciclaggio, l'identificazione, il sequestro e la confisca dei proventi di reato.* La Convenzione impose da un lato l'introduzione di un efficace normativa nazionale per il riciclaggio, e dall'altro fornì la base normativa necessaria al fine di favorire la cooperazione tra gli Stati nel caso in cui il riciclaggio si verificasse come un fenomeno transnazionale.[23] Inoltre, i Paesi si obbligarono ad adottare determinate misure in merito alla confisca dei beni o proventi illeciti, individuazione delle operazioni sospette, abolizione del segreto bancario e cooperazione internazionale. L'importanza di questo documento risiede nell'obbligatorietà delle fattispecie delittuose in tema di riciclaggio che erano determinate dalla Convenzione. La Convenzione fu recepita nell'ordinamento italiano con la legge n.328/1993 ed entrò in vigore il 1º maggio 1994, incidendo notevolmente sul nostro codice penale in merito sia alla definizione di riciclaggio, sia per ciò che concerne la cooperazione internazionale.

In seguito, la Convenzione di Palermo del 2000 ha un'importanza strategica grazie all'identificazione del riciclaggio in un reato transnazionale e che di conseguenza necessita la cooperazione tra vari Stati. Infatti, l'articolo 6 "ribattezza" il riciclaggio come reato internazionale, chiedendo agli Stati di inserirlo come tale nei loro ordinamenti, di catalogarlo come reato grave, e di prevedere tra i reati presupposti quelli commessi non solo all'interno, ma anche all'esterno. Inoltre, vennero istituiti specifici controllo sugli intermediari finanziari. sui movimenti di capitale. Potrebbe sembrare che questa convenzione non abbia apportato nessuna novità in termini di disposizioni, ma il tutto va contestualizzato nella "transnazionalità" delle stesse.[24] La Convenzione fu recepita nel nostro ordinamento con la legge n.146 del 16 marzo 2006.

Nel 2001, in seguito ai noti attentati terroristici, il mandato del GAFI venne ampliato con il compito di proporre strategie di contrasto al finanziamento del terrorismo, al quale seguì l'emanazione di 8 (in seguito 9) speciali raccomandazioni su questa tematica.

Le 9 Raccomandazioni speciali invitavano gli Stati membri a:

- recepire e attuare gli strumenti normativi per la lotta al finanziamento del terrorismo definiti dagli organismi internazionali preposti;

[23] Favaro Sergio. Il coordinamento delle forze di polizia nella lotta al riciclaggio. Rivista della Guardia di Finanza, 2002, pag. 315

[24] Razzante Ranieri. La regolamentazione antiriciclaggio in Italia. Aggiornato alla delibera della Banca d'Italia 10 marzo 2011 sui controlli antiriciclaggio. Cit. p.36.

- introdurre il reato di finanziamento al terrorismo;
- congelare e confiscare i beni e capitali appartenenti ai terroristi;
- cooperare con gli organi investigativi di altri Paesi per ciò che concerne la lotta al terrorismo;
- mettere in atto misure volte al monitoraggio di movimenti *cross-bording* di contante e titoli al portatore;
- disciplinare poteri di fermo e confisca dei capitali provenienti da attività di riciclaggio e/o destinati al finanziamento del terrorismo;[25]

Gli ultimi aggiornamenti sono stati effettuati nel 2003 e nel 2012. Quest'ultimo aveva l'obiettivo di far fronte alle nuove tecniche sviluppate dai riciclatori e dai terroristi, con maggiore attenzione ai soggetti, aree e paesi dove i rischi sono maggiori come stabilito dai principi dell'approccio basato sul rischio che verrà trattato in seguito.
Nell'attuale formulazione le 40 Raccomandazioni vengono ripartite in 8 sezioni:

- politiche e coordinamento antiriciclaggio e contro il finanziamento del terrorismo. Si auspica che gli Stati, dopo aver identificato e valutato i rischi in questione, designino un'autorità per coordinare la loro azione e destinare risorse adeguate allo scopo e richiedano la collaborazione di professionisti nel campo finanziario e non;
- riciclaggio e confisca. Si auspica che Stati introducano il reato di riciclaggio nei loro ordinamenti secondo le convenzioni di Vienna e di Palermo, individuino il ventaglio più ampio possibile di reti presupposto e adottino misure legislative per sequestrare, congelare e confiscare i beni ed i proventi riciclati;
- finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa. Si auspica che gli Stati introducano il reato di finanziamento del terrorismo e che adottino misure sia di congelamento dei beni e fondi appartenenti o diretti al terrorismo sia rivolte ad enti, soprattutto *no profit*, che possano essere utilizzati a scopo di terrorismo;
- misure preventive. Si auspica che le regole di riservatezza degli operatori non compromettano l'adozione delle Raccomandazioni e vengano adottate adeguate misure per la verifica della clientela e segnalazione delle operazioni sospette;
- trasparenza e titolari effettivi di persone giuridiche e simili. Si auspicano misure per l'adeguata verifica dei titolari e i beneficiari degli enti in questione;
- poteri e responsabilità delle autorità competenti. Gli operatori finanziarie gli altri soggetti che hanno l'obbligo di collaborare devono essere sottoposti a determinati controlli. Inoltre, si

[25] Battaglia Sergio Maria e Russo Angelo. Contrasto al riciclaggio e cooperazione internazionale, nella rivista Opinio Juris: Law and Politic Review, 2016.

richiede agli Stati di istituire unità d'informazione finanziaria (FIU: *Financial Intelligence Unit*) come principale centro di raccolta e analisi delle segnalazioni;

- cooperazione internazionale. Si richiede agli Stati di aderire ad una serie di convenzioni internazionali e di collaborare tra di loro;[26].

1.3.2 LA I DIRETTIVA ANTIRICICLAGGIO

La lotta al riciclaggio in ambito europeo ha avuto una svolta fondamentale a partire dagli anni '90, grazie ad una imponente produzione normativa volta alla regolamentazione di una serie di obblighi in materia, inizialmente rivolti alle istituzioni finanziari e bancarie ed in seguito anche ai professionisti. Ci si riferisce alle 4 Direttive antiriciclaggio che sono state emanate rispettivamente nel 1991, 2001, 2005, 2015 e alle quali si aggiunge la recente pubblicazione della quinta, la Direttiva n.2018/843 del 30 maggio 2018. Si sottolinea che le Direttive europee, al di là dei vari auspicii e inviti, contenuti nei vari "considerando" introduttivi, si occupano di regolamentare solamente il lato preventivo della disciplina, mentre quello repressivo/penale è stato regolamentato successivamente tramite l'utilizzo di strumenti della cooperazione intergovernativa e non tramite quelli comunitari. Infatti, lo *ius puniendi* è tradizionalmente considerato appartenente alla sovranità nazionale e gelosamente salvaguardato dagli Stati.[27]
La ragione dell'utilizzo da parte dell'Unione Europea della direttiva invece che del regolamento risiede nella necessità di concedere un'adeguata tempistica ai destinatari per fare in modo che gli stessi riuscissero ad uniformarsi alle disposizioni previste, dato che le varie discipline non erano adeguatamente articolate in tal senso.
Le direttive, infatti, sono atti legislativi che stabiliscono un obiettivo che tutti i Paesi dell'UE devono raggiungere. Tuttavia, a differenza dei regolamenti che sono vincolanti in tutti gli elementi, per quanto concerne le direttive spetta ai singoli paesi definire attraverso disposizioni nazionali come raggiungere tali obiettivi.[28]

La prima Direttiva antiriciclaggio, la n.91/308/CEE, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività illecite, fu emanata dalla Comunità Economica Europea il 10 giugno 1991[29] e venne abrogata completamente dall'articolo 44 della

[26] [27] Scapellato Filippo. Il fenomeno del riciclaggio e la normativa di contrasto. Cit. pag.24-25.
[28] www.europa.eu.
[29] Pubblicata in G.U.C.E. L. 166 del 28 giugno 1991.

Direttiva n.2005/60/CE. Essa è ritenuta uno dei provvedimenti più importanti nella storia europea della lotta al riciclaggio, in quanto diede un fondamentale impulso legislativo ai Paesi membri, di cui le legislazioni erano prive di una base normativa efficace per il contrato del riciclaggio. La finalità della Direttiva era quello di salvaguardare gli enti finanziari e creditizi "dall'inconsapevole" coinvolgimento nel riciclare proventi di attività illecite, senza pregiudicare la libera circolazione dei capitali nel mercato monetario. I soggetti destinatari della Direttiva sono gli istituti finanziari, creditizi e bancari, tuttavia la direttiva stabiliva che la disciplina potesse essere estesa anche ai professionisti. Infatti, la Direttiva esplicita che "*la possibilità di procedere al riciclaggio non soltanto per il tramite di enti creditizi e finanziari, ma anche di altri tipi di attività professionali e categorie di imprese, gli Stati membri devono estendere totalmente o parzialmente le disposizioni della presente direttiva a quelle professioni e imprese che svolgono attività particolarmente suscettibili di utilizzazione a fini di riciclaggio*[30]*"*. Tale aspetto è un punto molto importante che verrà ripreso ed integrato nelle successive Direttive.
In particolare, la Direttiva, avendo recepito le Raccomandazioni del Consiglio d'Europa e del GAFI, la Dichiarazione di Basilea e la Convenzione ONU di Vienna stabilì:

- la definizione del reato di riciclaggio, allargandone la portata rispetto alle precedenti definizioni. Infatti, per riciclaggio si intese: "*la conversione o il trasferimento di beni, effettuati essendo a conoscenza del fatto 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; l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o diritti sugli stessi, effettuati essendo a conoscenza del fatto che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; 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; la partecipazione ad uno degli atti di cui ai punti precedenti, l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno di commetterlo o il fatto di agevolarne l'esecuzione*[31]*"*. Per "attività criminosa" si intende quelle contemplate nella citata Convenzione di Vienna, ovvero i reati in materia di traffico di stupefacenti e ogni altra attività considerata tale dagli Stati membri. Da qui la possibilità di estendere gli effetti della direttiva anche ai proventi di altre attività criminali; (art.1)

[30] [31] Cfr. Direttiva n.91/308/CEE.

- il divieto del riciclaggio; (art.2)
- l'obbligo per gli intermediari d'identificazione e la registrazione della clientela "*mediante documento probante […] per tutte le operazioni con clienti il cui importo sia pari o superiore a 15.000 ECU, a prescindere dal fatto che siano effettuate con un'unica operazione o con più operazioni tra le quali sembri esistere una connessione;"* (art.3)
- l'obbligo di conservare la documentazione per un periodo minimo di 5 anni (art.4) e di esaminare con cura ogni operazione che possa esser connessa al riciclaggio; (art.5)
- l'obbligo di piena collaborazione degli enti creditizi e finanziari con le autorità "*comunicando o segnalando a quest'ultime le operazioni anomale o sospette e fornendo tutte le informazioni necessarie per porre in essere le procedure stabilite dalla seguente normativa*" (art.6), e l'obbligo di astenersi dalle stesse. (art.7);
- l'obbligo per gli intermediari di istituire strutture interne di comunicazione e controllo al fine di prevenire le realizzazioni di operazioni di riciclaggio e di formare su tali aspetti il personale per fare in modo che i dipendenti siano a conoscenza delle disposizioni della Direttiva e siano in grado di riconoscere possibili operazioni di riciclaggio. (art.11)

La direttiva in esame fu recepita in Italia con l'art.15 della legge 6 febbraio 1996, n.52 (c.d. legge comunitaria) e con i decreti legislativi 26 maggio 1997 n.153 e 25 settembre 1999 n.374. In realtà la maggior parte delle disposizioni della Direttiva erano state anticipate dal d.l. n.143/1991, conv. in legge n.197/1991.

1.3.3. LA II DIRETTIVA ANTIRICICLAGGIO

Dopo 10 anni dall'emanazione della prima Direttiva, che era stata di fondamentale importanza avendo costituito il principale strumento della lotta al riciclaggio, il legislatore comunitario decise di integrare e aggiornare le normative predisposte dalla stessa con la seconda Direttiva antiriciclaggio, la n.2001/97/CE del 4 dicembre 2001[32]. Infatti, vi erano molteplici aspetti che necessitavano di correzioni o di miglioramenti. In generale era necessario un approccio più deciso nella lotta al riciclaggio in considerazione delle tecniche dei riciclatori, che negli anni si erano notevolmente evolute, in quanto l'intensificazione dei controlli spinse i criminali a sperimentare nuovi metodi alternativi, come espressamente osservato nei "considerando" nella parte introduttiva del testo.

[32] Pubblicata in G.U. dell'Unione Europea, L 344 del 28 dicembre 2001.

Inoltre, dei tremendi attentati terroristici dell'11 settembre che resero evidente come la lotta al terrorismo fosse una questione indispensabile.

Le novità introdotte da questa Direttiva furono molteplici. In *primis* venne ampliato il campo d'applicazione della disciplina, non più limitata ai soli reati legati al traffico di droga ma estendendo il ventaglio dei reati presupposto[33] ad altri reati dell'attività criminale. Questo stabilendo una "*definizione molto più ampia del riciclaggio, fondata su una gamma più vasta di reati "base" o "presupposto" basata sulle 40 raccomandazioni del GAFI."* Ciò avvenne ridefinendo il concetto di "attività criminosa", che in precedenza faceva riferimento solamente ai reati contenuti nell'art.3 della Convenzione di Vienna. Un'attività criminosa fu, dunque, considerata come "*un qualsiasi tipo di coinvolgimento criminale nella perpetrazione di un reato grave"*. In questa categoria, oltre al terrorismo, rientrano: la frode, la corruzione e qualsiasi *"reato che possa fruttare consistenti proventi e sia punibile con una severa pena detentiva in base al diritto penale dello Stato membro[34]".* La seconda novità di maggior rilievo fu l'estensione degli obblighi soggettivi di collaborazione fino a quel momento riguardanti esclusivamente gli enti creditizi e finanziari. Questa scelta fu presa poiché ci si rese conto che i riciclatori utilizzavano anche enti non finanziari per riciclare i loro proventi illeciti ed in particolare enti di soggetti che per loro stesse caratteristiche consentivano accumuli e trasferimenti, anche ingenti, di ricchezze in modo non tracciabile.[35]

In particolare, gli obblighi antiriciclaggio vennero estesi a "*revisori, contabili esterni e consulenti tributari, agenti immobiliari, notai e altri liberi professionisti legali, commercianti di oggetti di valore elevato quali pietre o metalli preziosi o opere d'arte e case d'asta, ogniqualvolta il pagamento sia effettuato in contanti e per un importo pari o superiore a €15.000, case da gioco*".[36]

La Direttiva incluse in questi obblighi anche i notai e i professionisti legali indipendenti, qualora partecipino ad attività di natura finanziaria, societaria e tributaria. Questa tematica era stata già anticipata nella prima Direttiva concedendo ai legislatori nazionali la facoltà di estendere gli obblighi a questa categoria, qualora gli stessi l'avessero ritenuto opportuno. Gli obblighi in questione riguardavano: l'identificazione della clientela; la registrazione delle operazioni e la conseguente conservazione dei dati per un periodo minimo di 5 anni; la segnalazione delle operazioni sospette. Da segnalare l'introduzione dell'obbligo d'identificazione della clientela anche nelle transazioni non *face to face,* ovvero a distanza tramite l'utilizzo di strumenti tecnologici come quelli di pagamento online che garantivano l'anonimato. Nella consapevolezza che questa tipologia di strumenti veniva utilizzata per aggirare i controlli della prima Disciplina. Da queste circostanze si sviluppò il principio *know your costumer*, già presente nelle 40 Raccomandazioni GAFI. Questo principio si sostanzia

[33] Danovi Remo. La nuova normativa antiriciclaggio e le professioni. Milano: Giuffrè,2008, pag. 2.
[34] Cfr. Direttiva n.2001/97/CE. Art.1.
[35] Urbani Alberto. Disciplina Antiriciclaggio e Ordinamento del credito. Padova: CEDAM, 2006, pag. 205-208.
[36] Cfr. Direttiva n.2001/97/CE. Art.2 bis.

nell'approfondire la conoscenza del cliente con la finalità di favorire la nascita di collaborazioni attive con le autorità competenti.[37] Inoltre, si impose alle autorità di vigilanza della borsa, del cambio estero e dei mercati dei derivati finanziari di informare "*le autorità responsabili per la lotta al riciclaggio di proventi di attività illecite qualora vengano a conoscenza di fatti che possano costituire una prova di riciclaggio di tali proventi.*"[38] Infine, la Direttiva stabilì l'obbligo per tutti i soggetti a cui era rivolta di collaborare pienamente con le autorità responsabili per la lotta al riciclaggio.
La Direttiva n.2001/97/CE fu recepita in Italia con il D.lgs. 20 febbraio 2004 n.56.

1.4. IL RINNOVAMENTO DELLA DISCIPLINA TRAMITE LA III DIRETTIVA

La direttiva antiriciclaggio n.2005/60/CE, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, è stata approvata dal Parlamento Europeo e dal Consiglio il 26 ottobre del 2005.[39] Questa Direttiva rinnovò completamente l'intera disciplina, abrogando la storica Direttiva del '91, che era già stata modificata ed integrata nel 2001 dalla seconda Direttiva antiriciclaggio. La Direttiva si basa su determinate assunzioni contenute nei "considerando" iniziali. In *primis* viene ribadito che il riciclaggio ed il finanziamento del terrorismo sono fenomeni di livello internazionale. Si rende necessario, di conseguenza, un'azione normativa a livello internazionale e viene specificato che qualsivoglia intervento di natura esclusivamente nazionale o anche comunitario, senza cooperazione o coordinamento internazionale, avrebbe effetti decisamente limitati. Proprio per questo le misure adottate si basano sulle 40 Raccomandazioni del GAFI, a cui si aggiungono le 9 riguardanti il finanziamento del terrorismo che sono state revisionate nel 2003. Proprio il finanziamento del terrorismo, il quale è ridefinito dalla Direttiva come *"la fornitura o la raccolta di fondi, in qualunque modo, direttamente o indirettamente, con l'intenzione di utilizzarli, in tutto o in parte, per compiere uno dei reati di cui agli articoli da 1 a 4 della decisione quadro 2002/475/GAI del Consiglio, del 13 giugno 2002, sulla lotta contro il terrorismo, o sapendo che saranno utilizzati a tal fine[40]",* viene considerato come capace di scuotere le fondamenta stesse della società. In tale luce l'ambito

[37] Corradino Michele. Strategie normative di contrasto al riciclaggio di denaro di provenienza illecita, in Normativa antiriciclaggio e contrasto della criminalità economica a cura di Di Brina L. e Picchio Forlati M. L. Padova: CEDAM, 2002, pag. 23.
[38] Cfr. Direttiva n.2001/97/CE. Art.10.
[39] Pubblicata in G.U. dell'Unione Europea, L 309/15 in data 25 novembre 2005.
[40] Cfr. Direttiva n.2005/60/CE. Considerando n.4.

dell'applicazione della disciplina antiriciclaggio è stato esteso anche a questo fenomeno; le misure della Direttiva, appunto, sono espressamente rivolte ai "*proventi di attività criminose e di finanziamento del terrorismo".* La Direttiva, inoltre, basandosi sulle considerazioni che i flussi ingenti di denaro e le azioni compiute dai criminali per mascherarne l'origine possano danneggiare la stabilità, la solidità, la reputazione e la fiducia negli enti creditizi e nel sistema finanziario e, infine, minacciare il mercato unico, si propone come uno strumento per contrastare le basi economiche della criminalità e del terrorismo[41]. Essa non solo ha ribadito le disposizioni della disciplina precedente chiarendone alcuni punti, ma ne ha anche ampliato i contenuti.
In *primis* sebbene la Direttiva in questione non ha modificato la definizione di riciclaggio rispetto alle precedenti, ne ha aumentato la portata implementando quelli che sono i reati presupposto ed in tal modo cercando di approcciare il fenomeno con una prospettiva più completa.
Ciò è stato ottenuto ampliando il novero dei reati gravi, ovvero:

- *gli atti definiti agli articoli da 1 a 4 della decisione quadro 2002/475/GAI;*
- *ognuno dei reati definiti nell'articolo 3, paragrafo 1, lettera a) della convenzione delle Nazioni Unite contro il traffico illecito di stupefacenti e sostanze psicotrope del 1988;*
- *le attività delle organizzazioni criminali quali definite nell'articolo 1 dell'azione comune 98/733/GAI del Consiglio, del 21 dicembre 1998, relativa alla punibilità della partecipazione a un'organizzazione criminale negli Stati membri dell'Unione europea;*
- *la frode, perlomeno la frode grave, quale definita nell'articolo 1, paragrafo 1 e nell'articolo 2 della convenzione relativa alla tutela degli interessi finanziari delle Comunità europee;*
- *la corruzione;*
- *i reati punibili con una pena privativa della libertà o con una misura di sicurezza privativa della libertà di durata massima superiore ad un anno ovvero, per gli Stati il cui ordinamento giuridico prevede una soglia minima per i reati, i reati punibili con una pena privativa della libertà o con una misura di sicurezza privativa della libertà di durata minima superiore a sei mesi[42];*

In secondo luogo la Direttiva ha allargato il campo di applicazione della normativa, estendendo gli obblighi antiriciclaggio non solo a quei soggetti che erano stati già interessati dalla Direttiva n.2001/97/CE, ma anche *"ai prestatori di servizi relativi a società o trust, case da gioco e altre persone fisiche o giuridiche che negoziano beni, soltanto quando il pagamento è effettuato in contanti*

[41] Balsamo Antonio. La destinazione delle somme di denaro fa scattare il finanziamento del terrore, in Guida al Diritto, 2006, n. 1, pag. 37 - 38.
[42] Cfr. Direttiva n.2005/60/CE. Art.3 comma 5.

per un importo pari o superiore a 15 000 EUR, indipendentemente dal fatto che la transazione sia effettuata con un'operazione unica o con diverse operazioni che appaiono collegate [43]". Inoltre, i Paesi membri possono decidere di estendere gli obblighi antiriciclaggio anche a attività professionali e categorie d'imprese qualora si ritenga che le loro attività siano particolarmente suscettibili al rischio di essere utilizzati a fini di riciclaggio o di finanziamento del terrorismo. Sempre secondo la prospettiva di una lotta su scala mondiale gli obblighi antiriciclaggio sono stati estesi anche alle succursali e controllate aventi sede in paesi al di fuori dell'Unione Europea[44], qualora la loro legislazione in materia fosse carente.

In seguito, sono stati introdotti importanti obblighi di verifica della clientela, secondo il principio di derivazione internazionale del *know your costumer.* Ciò si sostanzia in degli obblighi più stringenti per ciò che concerne la *due diligence* della clientela; ovvero una serie di attività che vanno oltre la semplice identificazione del cliente, con controlli formali e sostanziali per tutta la durata del rapporto professionale. Ciò comprende anche la verifica del titolare effettivo, ovvero il soggetto che in ultima istanza possiede o controlla il cliente, per conto del quale viene effettuata una determinata operazione. In caso di società ci si riferisce al possesso o al controllo diretto o indiretto di una percentuale sufficiente delle azioni o dei diritti di voto in seno a tale entità giuridica. Il criterio viene soddisfatto per una percentuale di azioni pari al 25% più una.

L'adeguata verifica della clientela, come prescritto dall' art.9, deve sempre essere effettuata prima dell'instaurazione del rapporto professionale. Gli obblighi di verifica, secondo l'art.7, devono essere applicati quando si instaura un rapporto d'affari; nel caso in cui si eseguono transazioni occasionali con importo dai €15.000 in su, indipendentemente dal fatto che vengano effettuate con una o più operazioni; nel momento in cui vi sia il sospetto di riciclaggio o di finanziamento del terrorismo o nel caso di dubbi sulla veridicità e adeguatezza dei dati riguardanti l'identificazione del cliente.

Entrando più nello specifico, verificare in modo adeguato la clientela consiste nel:

- *identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;*
- *se necessario, identificare il titolare effettivo ed adottare misure adeguate e commisurate al rischio per verificarne l'identità, in modo tale che l'ente o la persona soggetti alla presente direttiva siano certi di conoscere chi sia il titolare effettivo, il che implica per le persone giuridiche, i trust ed istituti giuridici simili adottare misure adeguate e commisurate alla situazione di rischio per comprendere la struttura di proprietà e di controllo del cliente;*
- *ottenere informazioni sullo scopo e sulla natura prevista del rapporto d'affari;*

[43] Cfr. Direttiva n.2005/60/CE. Art.2.

[44] Tolla Marco. Elementi normativi internazionali e nazionali in materia di riciclaggio. Bari: Cacucci, 2010, pag. 178

- *svolgere un controllo costante nel rapporto d'affari, in particolare esercitando un controllo sulle transazioni concluse durante tutta la durata di tale rapporto in modo da assicurare che tali transazioni siano compatibili con la conoscenza che l'ente o la persona in questione hanno del proprio cliente, delle sue attività commerciali e del suo profilo di rischio, avendo riguardo, se necessario, all'origine dei fondi e tenendo aggiornati i documenti, i dati o le informazioni detenute*[45].

Un altro punto fondamentale della Direttiva è quello dell'introduzione del *risk based approach* secondo il quale vengono valutati e definititi gli obblighi di adeguata verifica della clientela. Questo approccio determina il rischio di riciclaggio basandosi sul profilo soggettivo, legato alla natura del cliente in questione, e sul profilo oggettivo, derivato dal rapporto d'affari o transazione richiesta dallo stesso. Il *risk based approach* si basa su tre tipologie di obblighi. In *primis* ci sono gli obblighi ordinari di adeguata verifica della clientela, che sono quelli che abbiamo appena trattato. In secondo luogo, ci sono gli obblighi rafforzati che ricorrono quando il rischio di riciclaggio o di finanziamento del terrorismo è più elevato.
Nello specifico si adoperano i suddetti quando:

- il cliente non è fisicamente presente ai fini di identificazione;
- in caso di conti di corrispondenza con enti corrispondenti di paesi terzi;
- quando ci sono operazioni o rapporti d'affari con persone politicamente esposte residenti in un altro stato membro o in un paese terzo.[46]

Le persone politicamente esposte sono quelle persone fisiche che occupano o hanno occupato importanti cariche pubbliche. Nella categoria vengono incluse anche i loro familiari diretti o coloro con i quali tali persone intrattengono notoriamente stretti legami.
Infine, gli obblighi semplificati di adeguata verifica quando il rischio di riciclaggio è scarso.
Gli obblighi semplificati sussisto nel caso in cui il rischio sia chiaramente inferiore, ed in particolare quando "*il cliente è un ente finanziario e creditizio soggetto alla presente Direttiva o situato in un altro paese che imponga obblighi equivalenti."*
Inoltre, gli Stati membri possono autorizzare un regime di obblighi semplificati a:

- *società quotate i cui valori mobiliari sono ammessi alla negoziazione su un mercato regolamentato ai sensi della direttiva 2004/39/CE in uno o più Stati membri e alle società*

[45] Cfr. Direttiva n.2005/60/CE. Art.8.
[46] Cfr. Direttiva n.2005/60/CE. Art.13.

quotate di paesi terzi che sono soggette ad obblighi di comunicazione conformi alla normativa comunitaria;

- *titolari effettivi di conti collettivi gestiti da notai o altri liberi professionisti legali di uno Stato membro o di un paese terzo, purché siano soggetti ad obblighi in materia di lotta al riciclaggio e al finanziamento del terrorismo conformi agli standard internazionali e al controllo del rispetto di tali obblighi e purché le informazioni sull'identità del titolare effettivo siano accessibili, a richiesta, agli enti che operano quali enti di deposito dei conti collettivi;*
- *autorità pubbliche nazionali;*
- *qualunque altro cliente caratterizzato da uno scarso rischio di riciclaggio o di finanziamento del terrorismo che soddisfi i criteri tecnici stabiliti.*[47]

Per ciò che concerne gli obblighi di segnalazione, coloro che sono soggetti alla Direttiva hanno l'obbligo di collaborare con l'UIF (FIU, *Financial Intelligence Unit)*, ovvero l'unità nazionale centrale con il compito di ricevere, analizzare e comunicare alle autorità competenti le informazioni riguardanti un possibile riciclaggio o finanziamento del terrorismo. Inoltre, secondo l'art. 24 gli stessi hanno l'imposizione di astenersi da compiere le operazioni di cui sospettano avere una relazione con il riciclaggio o con il finanziamento del terrorismo. Questi soggetti sono tutelati perché, in *primis* non sono responsabili per qualsiasi segnalazione effettuata in buona fede ai sensi della Direttiva in secondo luogo gli Stati membri si impegnano a proteggerli da qualsiasi atto lesivo o minaccia dal momento in cui questi denuncino un'operazione sospetta.

È importante sottolineare che è stato disposto l'obbligo di non comunicare al cliente di aver effettuato una segnalazione, di conservare i documenti e le informazioni per ciò che concerne i rapporti d'affari, le registrazioni, le scritture e gli obblighi di adeguata verifica della clientela, affinché possano essere riutilizzati per eventuali indagini di riciclaggio o finanziamento del terrorismo.

In aggiunta è stato richiesto agli attori operanti nel settore finanziario di organizzare programmi interni di formazione del personale per aiutarlo a riconoscere attività che potrebbero essere connesse al riciclaggio.

Infine, per ciò che concerne l'ambito sanzionatorio, viene introdotto il principio secondo il quale le sanzioni devono esser effettive, proporzionali e dissuasive.

Gli Stati membri ebbero l'obbligo di recepire la Direttiva n.2005/60/CE entro il 15 dicembre 2007, essa è stata affiancata dalla Direttiva n. 2006/70/CE approvata il 1° agosto 2006[48], intitolata *definizione del concetto di "persone politicamente esposte" di cui alla Direttiva n.2005/60/CE.*

[47] Cfr. Direttiva n.2005/60/CE. Art.11.

[48] Pubblicata in G.U. dell'Unione Europea, L 214 in data 4 agosto 2006.

Quest' ultima ha stabilito le misure d'attuazione della recente disciplina comunitaria, stabilendo i criteri tecnici delle procedure semplificate di adeguata verifica della clientela.

1.5 LA IV DIRETTIVA ANTIRICICLAGGIO

A distanza di dieci anni dalla terza Direttiva antiriciclaggio, il legislatore decise di riformare la materia tramite la Direttiva (UE)2015/849 (c.d. quarta Direttiva antiriciclaggio) del Parlamento Europeo e del Consiglio approvata il 20 maggio 2015.[49] Tale direttiva ha modificato il regolamento (UE) n. 648/2012 e ha abrogato la Direttiva n.2005/60/CE e la Direttiva n.2006/60/CE.
Questa Direttiva pur confermando la base normativa delle direttive del 2005 e del 2006, risponde alla necessità di salvaguardare l'integrità degli enti creditizi e finanziari e la fiducia nell'intero sistema finanziario attraverso misure più stringenti[50]. La Direttiva, nell'implementare e migliorare la disciplina, si basa sul sopracitato aggiornamento delle Raccomandazioni del GAFI del 2012.
La Direttiva ha perseguito i seguenti obiettivi:

- ampliare il campo d'applicazione della disciplina ai prestatori di servizi di gioco d'azzardo;
- imporre l'adozione dell'approccio basato sul rischio nell'individuazione da parte delle autorità nazionali e dei soggetti obbligati di misure di contrasto al ML/FT;
- inasprire gli obblighi di adeguata verifica semplificata, in quanto le disposizioni precedenti avevano determinato l'esclusione di alcune categorie di soggetti;
- perfezionare gli obblighi rafforzati di adeguata verifica della clientela rafforzata, estendere la loro applicazione alle persone politicamente esposte e a coloro che lavorano in organizzazioni internazionali;
- rendere più chiare e accessibili le informazioni sul titolare effettivo di persone giuridiche e trust e migliorare la gestione dei dati personali in conformità con le norme sulla protezione degli stessi;
- implementare la collaborazione tra le FIU;
- Prevedere un ampio spettro di sanzioni amministrative efficaci, proporzionali e dissuasive[51].

[49] Pubblicata in G.U. dell'Unione Europea, in data 5 giugno 2015.
[50] Quattrocchi Danilo, Mongiello Licia. Le FAQ del MEF sulle novità della normativa di attuazione della IV Direttiva Antiriciclaggio. In www.dirittobancario.it, ottobre 2017.
[51] Di Carlo Francesco. Un nuovo regime per l'applicazione di misure semplificate e rafforzate di adeguata verifica: dalle novità regolamentari all'analisi di alcuni casi concreti. Atti del seminario di alto aggiornamento ABI Antiriciclaggio 2018: novità, impatti e prospettive, 11 e 12 Luglio 2018.

Procediamo con ordine nell'approfondire gli aggiornamenti apportati dalla quarta Direttiva.
In *primis* oltre ai soggetti obbligati in precedenza anche ad "*altri soggetti che negoziano beni, quando il pagamento è effettuato o ricevuto in contanti per un importo pari o superiore a €10.000, indipendentemente dal fatto che la transazione si effettuata con un'operazione unica o con diverse operazioni che appaiono collegate ai prestatori di servizi di gioco d'azzardo*[52]". In merito a ciò, gli Sati membri hanno la possibilità di esentare gli operatori di gioco in presenza di un basso rischio, determinato in seguito ad un'opportuna valutazione.

1.5.1 L'APPROCCIO BASATO SUL RISCHIO E I TRE LIVELLI DI RISK ASSESSMENT

L'approccio basato sul rischio è sicuramente il cardine della disciplina[53], in quanto viene utilizzato dagli intermediari per individuare, valutare e gestire i rischi connessi con il riciclaggio e il finanziamento del terrorismo, stabilendo misure di contrasto che siano proporzionali ai rischi effettivamente individuati. Esso era già stato introdotto nella precedente direttiva, ma è stato notevolmente implementato e razionalizzato da quella in questione. In base a tale principio, gli intermediari orientano le modalità e la profondità delle analisi che devono condurre per l'assolvimento degli obblighi di adeguata verifica, in modo coerente e commisurato all'effettiva esposizione ai rischi di riciclaggio e di finanziamento del terrorismo[54]. Essi devono autonomamente valutare il set informativo e conoscitivo acquisito sul cliente, e adottare le misure, di volta in volta adeguate, per neutralizzare il rischio di ML/TF misurato. Tale approccio viene indicato chiaramente nel "considerando" iniziale 22: "*il rischio di riciclaggio e di finanziamento del terrorismo non è sempre lo stesso in ogni caso. Di conseguenza, dovrebbe essere adottato un approccio olistico basato sul rischio. Tale approccio basato sul rischio non costituisce un'opzione indebitamente permissiva per gli Stati membri e per i soggetti obbligati: implica processi decisionali basati sull'evidenza fattuale, al fine di individuare in maniera più efficace i rischi di riciclaggio e di finanziamento del terrorismo che gravano sull'Unione e su coloro che vi operano*[55] ".

[52] Cfr. Direttiva (UE) 2015/849. Art. 2, comma 3.
[53] Galmarini Sabrina, Saba Claudio, La Scala Studio Legale. IV Direttiva Antiriciclaggio e approccio basato sul rischio. In www.dirittobancario.it, gennaio 2018.
[54] Tortora Gianluca. Adeguata Verifica Semplificata. Atti del seminario di alto aggiornamento ABI Antiriciclaggio 2018: novità, impatti e prospettive, 11 e 12 Luglio 2018.
[55] Cfr. Direttiva (UE) 2015/849. Considerando 22.

Mentre, nel "considerando" 23 ne viene espressa l'importanza di: "*sostenere l'approccio basato sul rischio è una necessità per gli Stati membri e per l'Unione per individuare, comprendere e mitigare i rischi di riciclaggio e di finanziamento del terrorismo a cui sono esposti. L'importanza di un approccio sovranazionale nei confronti dell'individuazione del rischio è stata riconosciuta a livello internazionale*[56]*".*

Con l'introduzione della quarta Direttiva l'approccio basato sul rischio viene strutturato su tre livelli distinti ed implica il coinvolgimento di diversi soggetti. I tre livelli di *risk assessment* sono europeo, nazionale e dei soggetti obbligati.

Per ciò che concerne il *risk assessment* a livello europeo, regolato dall'art. 6 della Direttiva, esso è affidato alla Commissione, che ha il compito di elaborare una valutazione sovranazionale dei rischi ML/TF presenti nel mercato comunitario e coordinare la valutazione del rischio delle attività transfrontaliere. A tal fine gli Stati membri hanno l'obbligo di condividere le loro rispettive valutazioni con gli altri Stati e con le istituzioni europee EBA (*European Banking Authority*), ESMA (*European Securities and Market Authority*), EIOPA (*European Insurance and Occupational Pensions Authority*). Le valutazioni individuali degli Stati devono essere inviate alla Commissione ogni due anni con il fine di fornire un costante aggiornamento su cui la Commissione stessa basa le proprie decisioni. Le valutazioni devono contenere informazioni riguardanti i settori maggiormente esposti al rischio, i rischi che caratterizzano i settori d'interesse e le tecniche di riciclaggio utilizzate dai criminali. Inoltre, la Commissione richiede pareri oltre che alle AEV (Autorità Europee di Vigilanza) anche ad esperti di AML/CTF di ciascun Stato e ai rappresentanti delle FIU. Infine, la Commissione invia al Parlamento Europeo e al Consiglio una relazione che identifica, analizza e valuta tali rischi a livello dell'Unione.

Un altro compito della Commissione è quello di guidare gli Sati membri nella scelta delle loro politiche di valutazione, formulando raccomandazioni riguardo le misure idonee da adottare per affrontare i rischi individuati e come indicato dall'art. 6 "*qualora gli Stati membri decidano di non applicare alcuna delle raccomandazioni nei rispettivi sistemi nazionali di AML/CTF lo notificano alla Commissione fornendone una motivazione*[57]*".* Questo meccanismo viene definito *comply or explain.*

Il risk assessment a livello nazionale prevede che gli Stati membri adottino tutte le misure necessarie per *"individuare, valutare, comprendere e mitigare i rischi di riciclaggio e di finanziamento del terrorismo che lo riguardano, nonché le eventuali problematiche connesse in materia di protezione dei dati*[58]*".* Inoltre, gli Stati devono designare un'autorità o stabilire un meccanismo per affrontare i rischi in questione, e renderne al corrente la Commissione e le AEV.

[56] Cfr. Direttiva (UE) 2015/849. Considerando 23.
[57] Cfr. Direttiva (UE) 2015/849. Art.6, comma 4.
[58] Cfr. Direttiva (UE) 2015/849. Art.7, comma 1.

Essi, come tra l'altro indicato dalla prima raccomandazione del GAFI, devono svolgere un'analisi periodica che ha l'obiettivo di identificare, analizzare e valutare le minacce di riciclaggio di denaro e di finanziamento del terrorismo, individuando quelle più rilevanti, i metodi di svolgimento di tali attività criminali, le vulnerabilità del sistema nazionale di prevenzione, di investigazione e di repressione di tali fenomeni, e quindi i settori maggiormente esposti a tali rischi[59]. In Italia, questa analisi per la prima volta è stata condotta nel 2014 dai partecipanti al CFS (Comitato di Sicurezza Finanziaria), da rappresentanti del Consiglio dei Ministri e da altre amministrazioni con competenze specifiche su temi d'interesse. Il CSF è presieduto dal Direttore Generale del Tesoro, è composto da rappresentanti dei ministeri, dell'Unità di Informazione Finanziaria e delle Forze di polizia. Esso si occupa di monitorare il funzionamento del sistema di prevenzione e di sanzioni per ciò che concerne il campo dell'ML/TF, ponendosi come punto di raccordo tra le amministrazioni e gli enti operanti nel settore. Tra i poteri di cui tale organismo è in possesso determinante è quello di poter richiedere informazioni alle amministrazioni in esso rappresentate, anche in deroga al segreto d'ufficio.
L'analisi nazionale è strutturata in due fasi:

- valutazione del "rischio ML/TF inerente" nel sistema;
- valutazione dell'efficacia dei presidi di prevenzione, investigazione e repressione.

Il "rischio inerente" nel sistema è valutato tramite l'analisi delle criticità e delle minacce, le quali sono rappresentate dai reati presupposto del riciclaggio e dal processo di raccolta, trasferimento e utilizzo dei fondi a fini terroristici. Esso è composto dai rischi attuali e potenziali a cui l'ordinamento è esposto.
La prima fase dell'analisi si prefigge di individuare le minacce più rilevanti anche attraverso una quantificazione dei proventi delle attività criminali.
Nella seconda, invece, fase vengono analizzati i presidi di prevenzione, investigazione e repressione focalizzandosi sulle vulnerabilità del sistema, con lo scopo di capire se le misure adottate sono in grado di mitigare i rischi ML/TF. Nello specifico si tratta dei presidi realizzati dai soggetti obbligati, ovvero intermediari finanziari, professionisti e operatori non finanziari, dell'adeguatezza delle misure per i controlli transfrontalieri, della trasparenza delle persone giuridiche e dei trust, dell'adeguatezza delle attività legate all'analisi delle operazioni sospette[60].
Tutto ciò permette di indicare agli Stati dove destinare le risorse e quali priorità stabilire nella lotta al riciclaggio. I risultati della valutazione vengono condivisi con la Commissione, le AEV e gli altri Stati membri.

[59] [56] Comitato di Sicurezza Finanziaria. Analisi nazionale dei rischi di riciclaggio e finanziamento del terrorismo. Ministero dell'Economia e delle Finanze, 2014.

Infine, per quanto riguarda i soggetti obbligati i loro adempimenti antiriciclaggio si suddividono in tre step:

- identificazione e assessment dei rischi ML/TF;
- adeguata verifica della clientela, graduando il livello e la tipologia sulla base del rapporto (continuativo o occasionale) e in base alle informazioni ottenute in sede di assessment;
- controllo costante e aggiornamento periodico delle valutazioni effettuate del rischio;

Il *risk assessment* in questione viene regolamentato dall'art. 8 della Direttiva in questione. In particolare, viene richiesto ai soggetti obbligati di adottare le misure necessarie per identificare e valutare i rischi ML/TF in base a fattori riguardanti i clienti, i paesi o le aree geografiche, i prodotti, i servizi, le operazioni e i canali di distribuzione. Le misure devono essere proporzionali alla natura e alla dimensione dei soggetti obbligati[61]. Tale analisi, denominata autovalutazione, ha lo scopo di identificare i settori di operatività nei quali concentrare gli sforzi di gestione de rischi ML/TF, sia per ciò che concerne l'acquisizione del cliente sia nello svolgimento di un rapporto continuativo. Il risk assessment dei soggetti obbligati è il primo dei tre importanti adempimenti a cui gli stessi dovranno attenersi.
Il processo di autovalutazione risulta, dunque, un crocevia fondamentale da cui dipenderanno le misure adottate dagli intermediari in conformità con quanto richiesto dalla Direttiva.
L'autovalutazione si compone di tre macro-attività. La prima fase concerne l'identificazione dei rischi attuali e potenziali a cui l'intermediario può essere esposto in base alla natura e all'estensione dell'attività svolta. Questa attività è definita come identificazione del "rischio inerente"; essa viene effettuata per ciascuna delle principali linee di business dell'intermediario a cui viene fornita una valutazione su una scala di quattro valori[62].
Ai fini di questa valutazione vengono presi in esame i seguenti elementi:

- la natura, la dimensione, la differenziazione e la complessità dei vari settori di business dell'intermediario;
- l'esposizione ad operazioni anonime o non tracciabili;
- il volume e la quantità delle transazioni ed il numero di quelle che avvengono in contanti;
- il mercato di riferimento dei prodotti e servizi forniti dall'intermediario;
- i canali distributivi, distinguendo tra rapporti diretti con la clientela e rapporti attraverso terzi;

[61] Cfr. Direttiva (UE) 2015/849. Art.8, comma 1.
[62] Tortora Gianluca. Adeguata Verifica Semplificata. Cit.

- il numero di clienti che appartengono alle fasce di rischio più elevate o clienti residenti in aree a rischio elevato;
- la presenza di succursali e filiazioni in paesi terzi, dove il rischio di riciclaggio è maggiore;
- il livello di movimenti transfrontalieri dei fondi.

In seguito dopo aver valutato il "rischio inerente" occorre effettuare l'analisi delle vulnerabilità: Il che consiste nel valutare l'adeguatezza del sistema dei presidi rispetto ai rischi precedentemente individuati.
Infine, l'ultimo *step* del processo di autovalutazione consiste nella determinazione del "rischio residuo" a cui è esposto l'intermediario e la conseguente mitigazione dello stesso. Il "rischio residuo" è il rischio che permane a seguito dell'applicazione delle tecniche di mitigazione del rischio[63].
Lo strumento dell'autovalutazione è estremamente importante, poiché, oltre alla funzione di *compliance* e di antiriciclaggio, può essere utilizzato per indirizzare diverse attività relative all'organizzazione complessiva dell'intermediario, al fine di rendere più efficienti le risorse aziendali dando la precedenza agli interventi e alle attività a maggior rischio o meno presidiate dai controlli vigenti.
I risultati dell'autovalutazione verranno inseriti nella Relazione annuale prodotta dalla funzione antiriciclaggio e trasmessi alla Banca d'Italia.

1.5.2. L'ADEGUATA VERIFICA DELLA CLIENTELA

Il secondo *step* degli adempimenti antiriciclaggio riguarda l'adeguata verifica della clientela, che come accennato in precedenza è stata una delle principali modifiche della quarta direttiva antiriciclaggio. La *Costumer Due Diligence,* è stata modificata basandosi sul principio del *risk based approach*, che consente di rispondere in maniera più tempestiva ed efficace alle minacce che si presentano. Lo stesso GAFI con l'aggiornamento nel 2012 delle sue Raccomandazioni invitò i Paesi ad utilizzare questo approccio in quanto da la possibilità di adottare misure più flessibili, per distribuire le loro risorse in modo più efficiente e applicare misure preventive commisurate alla natura dei rischi, al fine di concentrare i propri sforzi nel modo più efficace possibile[64]. Infatti, in base a tale approccio, l'analisi condotta dagli intermediari per l'assolvimento degli obblighi di adeguata verifica

[63] Tortora Gianluca. Adeguata Verifica Semplificata. Cit.
[64] FATF. The FATF Recommendations. International Standards on Combating Money Laundering and The Financing of Terrorism and Proliferation. Parigi, 2012.

viene sviluppata in modo coerente e commisurato all'effettiva esposizione ai rischi di riciclaggio e di finanziamento del terrorismo.
Rispetto alla precedente direttiva viene mantenuta la tripartizione tra obblighi ordinari, semplificati e rafforzati, però sono state sia integrate le circostanze in cui questi entrano in vigore sia modificati i rispettivi obblighi.
Per quanto riguarda gli obblighi ordinari, si aggiungono alle circostanze già presenti nella precedente disciplina i casi in cui:

- *un'operazione occasionale rappresenti un trasferimento di fondi quale definito all'articolo 3, punto 9), del regolamento (UE) 2015/847 del Parlamento europeo e del Consiglio (1), superiore a 1 000 EUR;*
- *nel caso di persone che negoziano in beni, quando eseguono operazioni occasionali in contanti d'importo pari o superiore a 10 000 EUR, indipendentemente dal fatto che l'operazione sia eseguita con un'unica operazione o con diverse operazioni che appaiono collegate;*
- *per i prestatori di servizi di gioco d'azzardo, all'incasso delle vincite, all'atto della puntata, o in entrambe le occasioni, quando eseguono operazioni d'importo pari o superiore a 2 000 EUR, indipendentemente dal fatto che la transazione sia eseguita con un'unica operazione o con diverse operazioni che appaiono collegate*[65].

Gli obblighi di adeguata verifica della clientela consistono nell'identificare il cliente, l'esecutore e il titolare effettivo e verificarne l'identità, acquisire e valutare le informazioni relative allo scopo del rapporto continuativo o della prestazione ed infine eseguire un controllo costante nel corso del rapporto con il cliente. Al fine di verificare l'identità del cliente si rende necessaria l'acquisizione dei dati e dei documenti identificativi mentre, in relazione all'esecutore, deve essere verificata l'esistenza e l'ampiezza dei poteri di rappresentanza. Invece, rispetto alle precedenti disposizioni, è richiesta l'analisi dell'operazione ed in particolare di rapportare i volumi della stessa con le risorse economiche a disposizione del cliente.
L'identificazione del titolare effettivo è uno degli argomenti più rilevanti della nuova direttiva. In quanto la necessità di ottenere informazioni accurate e aggiornate sullo stesso è di rilevanza fondamentale per identificare coloro che cercano di occultare la loro identità con schemi che rendono difficile rintracciarli. Infatti, nel caso in cui il soggetto obbligato sia una società di capitali, si è sempre rivelato difficoltoso capire chi fosse la persona fisica titolare in ultima istanza del possesso o del potere di controllo dell'entità oggetto di identificazione.

[65] Cfr. Direttiva (UE) 2015/849. Art.11.

La direttiva oltre a riprendere la definizione di titolare effettivo della terza direttiva, che abbiamo già osservato in precedenza, ne aggiunge anche delle importanti modifiche. La prima riguarda il criterio che attribuisce il possesso o il controllo con una soglia di azioni del 25% più una. Questa infatti non viene più considerata un criterio automatico che individua la titolarità effettiva, bensì una prova la quale deve essere corroborata da altri elementi al fine di essere dimostrata. La seconda modifica riguarda l'utilizzo dell'approccio progressivo, definito dalle Raccomandazioni del GAFI, nell'individuare il titolare effettivo. La modulazione segue un preciso ordine; in *primis* si identifica colui che è titolare di un numero sufficiente di azioni o diritti di voto, in concordanza con il criterio della soglia del 25% più una, in seguito chi esercita il controllo attraverso altri mezzi ed, infine avendo esperito tutti i mezzi possibili ed in assenza di motivi di sospetto, qualora non venisse individuato nessuno in base ai precedenti criteri, si procede ad indentificare il titolare effettivo nelle persone che occupano una posizione dirigenziale di alto livello.

La novità più importante introdotta nell'ambito dell'adeguata verifica della clientela riguarda la raccolta e la condivisione delle informazioni, tramite la creazione di un registro centralizzato. Le informazioni riguardano la proprietà effettiva delle società e dei trust. Gli Stati membri devono imporre alle società e alle altre entità giuridiche nel loro territorio di ottenere e conservare informazioni adeguate, accurate e attuali che riguardano la titolarità effettiva e informazioni base come il nome della società, l'indirizzo e la prova dell'atto costitutivo e della ragione sociale. Queste informazioni al fine di promuovere la trasparenza dovranno essere conservate nel sopracitato registro centrale che deve essere situato all'esterno della società in conformità con il diritto dell'Unione[66].

Le informazioni in questione sono accessibili, in conformità con la tutela della privacy, alle autorità competenti e alle FIU senza alcuna restrizione, ai soggetti obbligati, alle persone e alle organizzazioni legittimamente interessate, le quali possono accedere al nome, data di nascita, cittadinanza e paese di residenza del titolare effettivo.

In caso di trust per titolare effettivo si intende:

- *il costituente;*
- *il trustee;*
- *il guardiano, se previsto;*
- *i beneficiari;*
- *qualunque altra persona fisica che esercita il controllo sul trust tramite una proprietà diretta o indiretta o con altri mezzi*[67].

[66] Maiello Vincenzo, Della Ragione Luca. Riciclaggio e reati nella gestione dei flussi di denaro sporco. Cit. pag. 31.
[67] Cfr. Direttiva (UE) 2015/849. Art. 3, comma 6.

Anche i fiduciari dei trust sono tenuti a ottenere le adeguate informazioni sull'identità dei soggetti sopracitati, al fine di consentire l'individuazione del titolare effettivo. Le informazioni, però, devono essere conservate nel registro fiscale solamente nel caso in cui il trust generi obblighi fiscali.
Questa limitazione, che non è presente nelle disposizioni relative alle società e agli altri enti, ha generato notevoli discussioni e critiche da parte degli Stati membri i quali hanno considerato la norma non precisa e facilmente eludibile[68]. Anche in questo caso il registro centrale assicura un accesso tempestivo ai soggetti obbligati e senza limitazioni alle autorità e alle FIU.
Come già preannunciato nel corso della trattazione il *risk based approach* permette di graduare le misure di CDD in funzione del rischio e ciò si concretizza nelle misure di adeguata verifica semplificate ed in quelle rafforzate. Le misure semplificate, già presenti nella disciplina previgente, subiscono un'importate modifica. In precedenza, gli intermediari erano obbligati ad applicarle in presenza di determinate fattispecie considerate a basso rischio in quanto quali erano espressamente previste delle esenzioni dagli obblighi di ordinaria verifica. Le esenzioni erano stabilite in base a criteri sia riguardanti la tipologia del cliente e del prodotto venduto sia geografici.
L'importante modifica apportata dalla direttiva è quella di aver eliminato questi casi di esenzione e di aver previsto delle misure semplificate, che sono tali sotto il profilo della frequenza, dell'estensione e della profondità ma che prevedono, comunque, di eseguire tutte le fasi del processo di verifica.
In primo luogo, le misure semplificate consentono di modulare i tempi di esecuzione delle attività d'identificazione. Ad esempio, tramite l'immediata raccolta dei dati identificativi ed un rinvio fino ad un massimo di 30 giorni per l'acquisizione della copia del documento.
In secondo luogo, i soggetti obbligati, al verificarsi di determinate circostanze, possono ridurre non solo la quantità di dati da raccogliere ma anche la frequenza dell'aggiornamento degli stessi e la profondità e la frequenza del monitoraggio del rapporto.
Invece, per ciò che concerne gli strumenti di moneta elettronica, sono stati stabiliti specifici parametri entro i quali i soggetti obbligati possono decidere di applicare misure semplificate.
Le misure, in questo caso, consistono nell'identificare il cliente/esecutore prima dell'apertura del rapporto continuativo, rinviando l'acquisizione della copia del documento fino al momento dell'attivazione dello strumento o fino alla prima operazione di avvaloramento dello stesso.
Ciò è possibile solamente:

- nel caso in cui lo strumento non sia ricaricabile o che abbia un limite di spesa mensile di massimo €250;
- sia possibile utilizzarlo solamente per l'acquisto di bene o servizi;

[68] Longhi Massimo. IV Direttiva antiriciclaggio e trasparenza dei trust: cominciamo bene. IPSOA Quotidiano del 10 febbraio 2015.

- non sia alimentato con moneta elettronica anonima;
- l'emittente controlli le operazioni effettuate in modo idoneo a consentire le rilevazioni di operazioni anomale o sospette[69].

Spetta ai soggetti obbligati, valutando caso per caso in base a determinati fattori predeterminati, decidere di applicare le misure semplificate o meno sia nei confronti di rapporti continuativi sia nelle transazioni occasionali che vengano considerate a basso rischio. I fattori che guidano la scelta riprendono quelli che determinavano l'esenzione nella terza direttiva.
Vengono considerati fattori a basso rischio relativi al cliente, esecutore e titolare effettivo i soggetti quali:

- società ammesse alla quotazione su un mercato regolamentato con obblighi di comunicazione sulla titolarità effettiva;
- pubbliche amministrazioni;
- clienti che sono residenti o che hanno sede in aree geografiche a basso rischio;
- intermediari bancari e finanziari comunitari o con sede in un paese terzo con efficace regime di contrasto al riciclaggio (con determinate eccezioni), considerando eventuali sanzioni o misure d'intervento per inosservanza degli obblighi antiriciclaggio.

I fattori relativi a prodotti, servizi, operazioni o canali di distribuzione sono:

- contratti di assicurazione vita rientranti nei rami di cui all'art.2, co.1, del D.lgs. n. 209/2005, nel caso in cui il premio annuale non ecceda i €1.000 o il cui premio unico non sia superiore a €2.500;
- determinate tipologie di forme pensionistiche complementari;
- regimi di previdenza che versano prestazioni ai dipendenti, i cui i contributi versati sono detratti dalla retribuzione e che non permettono il trasferimento dei diritti ai beneficiari;
- prodotti in cui i rischi di riciclaggio o finanziamento del terrorismo sono mitigati da fattori come limiti di spesa o trasparenza della titolarità e che non consentono l'anonimato o l'occultamento dell'identità del cliente o del titolare effettivo.

Infine, i fattori geografici a basso rischio sono:

[69] Cfr. Direttiva (UE) 2015/849. Art. 12.

- paesi comunitari;
- paesi terzi con efficienti sistemi di prevenzione al riciclaggio o che, fonti autorevoli ed indipendenti valutano essere caratterizzati da un basso livello di corruzione o di permeabilità ad attività criminose.[70]

Le misure semplificate di adeguata verifica della clientela non vengono applicate, oltre a quando non sussistono le condizioni in base agli indici di rischio, anche quando le attività di monitoraggio e le informazioni sul cliente lo escludono da una fattispecie a basso rischio e quando ci sia il rischio di ML/TF.
Per ciò che concerne le misure rafforzate di adeguata verifica della clientela, invece, vengono effettuate delle integrazioni e alcune modifiche. Rispetto alla normativa previgente vengono mantenuti alcuni casi specifici in cui c'è l'obbligo di adottare misure rafforzate. Tale obbligo persiste, per persone fisiche o entità giuridiche residenti in paesi terzi ad alto rischio, nel caso di rapporti di corrispondenza transfrontalieri con enti rispondenti di un paese terzo e per i rapporti con le persone politicamente esposte; aspetto che tratteremo in seguito. Oltre a questi casi subentra l'obbligo di adottare misure rafforzate in presenza di un rischio elevato, non legato con una casistica predeterminata, valutato tale in base ad una serie di fattori stabiliti. I fattori anche in questo caso sono relativi ai clienti, ai prodotti ed in base a criteri geografici.
I fattori di rischio elevato relativi al cliente, esecutore e titolare effettivo sono:

- rapporti continuativi instaurati in circostanze anomale;
- clienti e/o titolari effettivi aventi sede in are geografiche a rischio elevato, con indici reputazioni negativi o che ricoprono cariche pubbliche in ambiti non rientranti nella nozione di PEP (persone politicamente esposte) ma con una rilevante esposizione al rischio di corruzione;
- strutture qualificabili come veicoli di interposizione patrimoniale;
- società che hanno emesso azioni al portatore o siano partecipate da fiduciari;
- attività economiche con elevato utilizzo di contante o riconducibile a settori particolarmente esposti al rischio di corruzione o con assetto proprietario anomalo o eccessivamente complesso.

I fattori riguardanti i prodotti, i servizi, le operazioni e i canali di distribuzione sono:

[70] Cfr. Banca d'Italia. Allegato I delle Disposizioni in Materia di Adeguata Verifica della Clientela. Documento per la consultazione, Aprile 2018.

- servizi con un elevato grado di personalizzazione offerti a clienti con un patrimonio rilevante;
- prodotti o operazioni he potrebbero favorire l'anonimato o che includono meccanismi di distribuzione di nuova generazione o tecnologie innovative;
- operazioni in contanti frequenti e ingiustificate con banconote di grosso taglio o con biglietti danneggiati o contraffatti;
- versamenti di contante dall'estero d'importo complessivo o superiore a €10.000;
- rapporti continuativi od operazioni occasionali mancanti delle adeguate procedure di riconoscimento;
- pagamenti ricevuti da terzi che non presentano un evidente collegamento con il cliente o con la sua attività.

Infine, i fattori geografici sono:

- paesi terzi ritenuti, da fonti autorevoli e indipendenti, carenti di efficaci presidi di prevenzione antiriciclaggio o ad elevato livello di corruzione o di permeabilità ad attività criminose o carenti sotto il profilo della conformità agli *standard* internazionali sulla trasparenza e sullo scambio di informazioni a fini fiscali;
- paesi soggetti a sanzioni, embargo o misure analoghe da parte di competenti organismi nazionali o internazionali;
- paesi che sostengono o finanziano organizzazioni terroristiche o nei quali le stesse operano[71].

Inoltre, a differenza della previgente disciplina, per ciò che concerne l'identificazione a distanza, la mancata presenza fisica del cliente non determina più l'obbligo di adottare misure rafforzate. Anche per le succursali o filiazioni controllate a maggioranza da soggetti obbligati con sede nell'Unione Europea, che hanno sede in paesi terzi, non è più necessario applicare automaticamente le misure rafforzate, qualora queste si conformino alle politiche e alle procedure a livello di gruppo a norma dell'art. 45[72].

Le misure rafforzate di adeguata verifica si caratterizzano per un'acquisizione d'informazioni maggiore e di migliore qualità, le quali vengono aggiornate con maggior frequenza. La richiesta di maggiori informazioni si sviluppa da un lato in merito all' identità del cliente, del titolare effettivo e sull'assetto proprietario e di controllo dello stesso. Con questo si intende l'acquisizione d'informazioni sulla reputazione, sugli atti pregiudizievoli, sui familiari e su coloro con cui il cliente

[71] Cfr. Banca d'Italia. Allegato II delle Disposizioni in Materia di Adeguata Verifica della Clientela Cit.
[72] Cfr. Direttiva (UE) 2015/849. Art. 18, comma 1.

intrattiene frequentemente rapporti d'affari. Dall'altro lato si acquisiscono maggiori informazioni sul rapporto continuativo per comprenderne appieno la natura e lo scopo.
Per una verifica delle informazioni di migliore qualità si intende un'indagine sull'origine del patrimonio e dei fondi del cliente e la richiesta che, all'inizio del rapporto continuativo, il cliente effettui un bonifico a valere su un conto di una banca UE o extracomunitaria, ma con validi presidi antiriciclaggio. Una maggior frequenza negli aggiornamenti, invece, è necessaria per rilevare eventuali variazioni del profilo del cliente e possibili elementi di riciclaggio.
Se i soggetti obbligati non riescono a completare gli adempimenti di adeguata verifica rafforzata, non devono dare corso all'operazione e, inoltre, sono tenuti a non avviare un rapporto continuativo con quel determinato cliente o a porre fine a quello già in essere.
Per quanto riguarda le persone politicamente esposte, aspetto accennato in precedenza, la quarta direttiva ne da una definizione molto più ampia ed esaustiva, specificando le categorie di soggetti che rientrano nelle PEP. Tra questi vengono inclusi anche i soggetti che occupano le cariche principali nelle organizzazioni internazionali e quelli che detengono cariche secondarie a livello nazionale, aspetto che la direttiva previgente escludeva. Alle persone politicamente esposte la direttiva applica indiscriminatamente misure di verifica rafforzate. Questo tema, infatti, è considerato fondamentale dal legislatore in quanto è strettamente legato alla lotta alla corruzione.
Inoltre, i soggetti obbligati, nel caso in cui una persona non ricopra più la carica per la quale è stato designato come PEP, sono tenuti a considerare che il rischio correlato con il soggetto sia ancora presente. Per tale ragione devono continuare ad applicare misure rafforzate, per un minimo di un anno, fino a che non ritengono che il rischio in questione sia cessato.
È importante precisare che le regole che vengono applicate nei confronti delle PEP hanno una valenza preventiva, non penale, e non devono essere interpretate come volte a stigmatizzare tali persone in quanto soggetti coinvolti in attività criminose. Rifiutare un rapporto d'affari con una persona perché politicamente esposta è contrario allo spirito della direttiva stessa e alle Raccomandazioni del GAFI.[73]

1.5.3 LE ALTRE NOVITA' DELLA DIRETTIVA: COOPERAZIONE TRA LE FIU E SISTEMA SANZIONATORIO

La cooperazione tra FIU dei diversi Stati membri è un aspetto estremamente importante della nuova direttiva, in quanto si lega strettamente al concetto di un'azione unitaria a livello europeo nel contrasto del riciclaggio di denaro e del finanziamento del terrorismo. Questa tematica è regolamentata dal

[73]Cfr. Direttiva (UE) 2015/849. Considerando 33.

capo IV della direttiva che disciplina sia le disposizioni generali delle FIU e i rispettivi meccanismi di cooperazione internazionale, ma anche l'accesso e l'utilizzo delle informazioni da parte delle stesse e la vigilanza di determinati servizi e persone. Regolamentare la cooperazione internazionale tra le FIU era diventata una necessità, in quanto, l'autonomia di ciascuno Stato membro nella scelta del modello delle FIU aveva creato molteplici differenze tra le stesse che non favorivano la cooperazione. La cooperazione, fino a quel momento, era stata agevolata dal Gruppo Edgemont. Quest'ultimo è un organismo internazionale che unisce 159 FIU e che fornisce una piattaforma di scambio in sicurezza e riservatezza di *expertise* ed informazioni con il fine di supportare e coordinare gli sforzi nazionali ed internazionali per la lotta al riciclaggio e al finanziamento del terrorismo. A tal proposito, nell'art. 52, la direttiva richiede alle FIU la massima collaborazione a prescindere dallo *status* organizzativo. La Commissione gioca un ruolo fondamentale, poiché è titolata a prestare l'assistenza necessaria ad agevolare il coordinamento e lo scambio d'informazioni, a tal fine può convocare periodicamente riunioni con i rappresentati delle FIU e prestare consulenza sull'interpretazione della direttiva, sull'individuazione delle operazioni sospette e sull'identificazione dei fattori e delle tendenze rilevanti per l'analisi dei rischi ML/TF.

Come abbiamo osservato il sistema sanzionatorio è sempre stato quasi esclusivamente di competenza nazionale, solo a partire dalla terza direttiva si è cercato di creare dei principi cardine a cui uniformarsi. In particolare, ci si riferisce all'indicazione che le sanzioni fossero, in conformità con la *Reccomandation* 35 del GAFI, efficaci, proporzionali e dissuasive. Inoltre, era stato disposto che ogni Stato riconoscesse la responsabilità delle persone fisiche e giuridiche per le violazioni delle norme attuanti la direttiva.
Nonostante le linee guida impartite, gli Stati crearono dei sistemi sanzionatori che erano completamente autonomi e divergenti.
La quarta direttiva antiriciclaggio, infine, si occupa di regolamentare le sanzioni in modo tale da migliorare il contrasto al riciclaggio e al finanziamento del terrorismo. Essa, nel Capo VI, riprende le disposizioni sanzionatorie della terza direttiva e ne amplia alcuni punti. Nello specifico, viene stabilito che le sanzioni amministrative pecuniarie massime debbano essere pari almeno al doppio dell'importo dei profitti ricavati grazie alla violazione, nel caso in cui tale importo possa essere determinato, o pari almeno a € 1.000.000, nel caso in cui non lo sia. Invece, per le entità giuridiche le sanzioni amministrative pecuniarie massime ammontano a € 5.000.000 o al 10% del fatturato complessivo annuo dell'entità stessa. Se il soggetto è tenuto a preparare un bilancio consolidato, la percentuale in questione si riferisce a tale bilancio[74].

[74] Cfr. Direttiva (UE) 2015/849. Art.59, comma 2 e 3.

Le autorità competenti possono imporre direttamente sanzioni e misure amministrative sia in collaborazione con altre autorità. Un aspetto interessante da sottolineare è il fatto che la direttiva introduce la possibilità di applicare sanzioni anche a membri dell'organo di gestione di entità giuridiche o ad altre persone fisiche responsabili di violazioni in relazione al mancato esercizio da parte loro delle funzioni di vigilanza e controllo.

CAPITOLO II

IL RICICLAGGIO E LE VALUTE VIRTUALI

Traiamo spunto dall'*excursus* sulla disciplina antiriciclaggio, che ci ha permesso di capire l'evoluzione del contesto in materia per evidenziare come il legislatore ha sviluppare una normativa sempre più evoluta che comprendesse via via tutte le fattispecie del caso. Quindi la presente trattazione si propone di osservare quali sono le nuove tecniche di riciclaggio e quali potrebbero essere i passi necessari per contrastare questo fenomeno. Infatti, appare chiaro come la criminalità, supportata da determinate situazioni favorevoli come, ad esempio, i paradisi fiscali, sia riuscita negli anni a trovare *escamotage* sempre più ingegnosi ed articolati per riciclare il denaro sporco ed aggirare le norme ed i controlli delle autorità. Come già detto in precedenza l'evoluzione tecnologica è stata utilizzata dai riciclatori come utile veicolo per effettuare movimenti transfrontalieri di denaro con velocità e sicurezza. Ciò è solamente la punta dell'iceberg di una questione estremamente più complessa. Infatti, l'ultima frontiera dei pagamenti digitali, legata in particolare al mondo delle valute virtuali, comporta, come ogni evoluzione tecnologia in questo campo, potenziali benefici legati all'utilizzo di nuovi strumenti finanziari che devono essere disciplinati e correttamente monitorati al fin di evitare utilizzi impropri e illegali.
Per poter valutare come le organizzazioni criminali riescono ad utilizzare al meglio, a fini illegali, le valute virtuali bisogna capire il loro funzionamento.

2.1 INTRODUZIONE A BITCOIN E ALLE VALUTE VIRTUALI

Le valute virtuali vengono definite come "*la rappresentazione digitale di valore non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata ad una valuta avente corso legale e che viene utilizzata come mezzo di scambio per l'acquisto di beni e sevizi, trasferita, archiviata e negoziata elettronicamente*[75]*"*.

[75] Cfr. Art 1, lett. qq) del d.lgs. 25 maggio 2017, n.90. Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006.

Per analizzare il funzionamento delle valute virtuali o criptovalute è opportuno andiamo ad approfondire quella più conosciuta: il bitcoin.

In *primis*, dobbiamo sottolineare la fondamentale distinzione tra Bitcoin e bitcoin, concetto che, per chi conosce la materia, è scontato ma che è alla base della comprensione per chi si approccia per la prima volta al mondo delle valute virtuali.

Per Bitcoin si intende il primo sistema di pagamento a registrazione crittografica *peer to peer* (nodo a nodo) ovvero, una rete di scambi senza la presenza di un'autorità incaricata di validare e registrare le transazioni. Il sistema è basato sul concetto di *distributed ledger techology* o *blockchain,* una sorta di registro o libro mastro pubblico e condiviso che annota le transazioni effettuate sulla rete e che vengono validate da alcuni utenti chiamati *miner*.

Questa tecnologia permette di garantire l'affidabilità di transazioni monetarie online senza l'utilizzo di un server centrale, che solitamente ha il compito di autentificare le transazioni. Il bitcoin (BTC), invece, è la valuta virtuale che è stata creata appositamente per la rete. Il Bitcoin è apparso per la prima volta nel 2009 tramite la pubblicazione online del documento "*Bitcoin A peer-to-peer electronic cash system"* sottoscritto da Satoshi Nakamoto, pseudonimo di uno o più hacker. Il sistema è stato reso operativo il 3 gennaio del 2009 tramite il software Bitcoin Core, disponibile in modalità *open source* ovvero, non protetto da *copyright*[76]. Questo comporta che chiunque può potenzialmente apportare delle modifiche, che devono essere approvate a maggioranza da tutti i nodi della rete. È possibile diventare un nodo della rete istallando il *software* che ci permetterà anche di scambiare bitcoin.

Il Bitcoin venne creato con la finalità di permettere trasferimenti di denaro digitale senza doversi basare sulla fiducia nei confronti di una terza parte. Per terza parte ci si riferisce o ad un'istituzione finanziaria, nel caso di una transazione bancaria come ad esempio un semplice bonifico, o ad un server centralizzato, utilizzato anche nelle transazioni online come PayPal o ad agenzie di trasferimento di denaro come Western Union. Infatti, in questi casi è il server centralizzato che tiene conto dei bilanci degli utenti ed autentifica le transazioni, assicurandosi che il denaro non venga né distrutto né generato. Ciò viene espressamente scritto dallo sviluppatore di Bitcoin nel suo *whitepaper*: *"una versione interamente peer to peer del denaro elettronico permetterebbe di effettuare pagamenti online direttamente da un utente all'altro senza passare per un'istituzione finanziaria*[77]*".* In tal modo Bitcoin punta anche ad eliminare i costi della mediazione fornita dagli intermediari per transazioni che non sono irreversibili. Il concetto di irreversibilità è fondamentale in quanto, al contrario la reversibilità delle transazioni pone le parti in causa a rischio di frode, aumentando contemporaneamente il costo delle transazioni stesse. Un esempio di ciò potrebbe essere

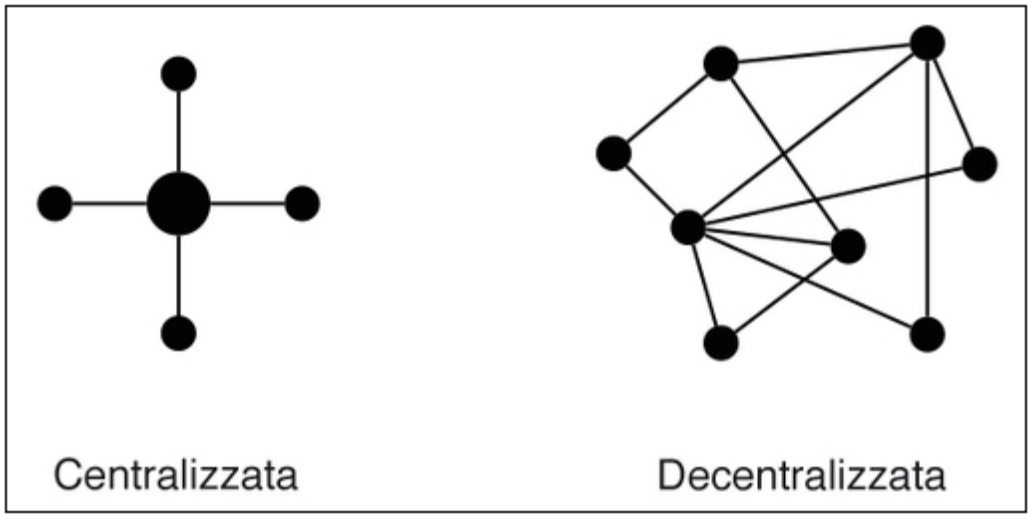
[76] Calzone Ottavio. Bitcoin e distributed ledger technology. In www.sicurezzanazionale.gov.it, febbraio 2017, pag. 9.
[77] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, in bitcoin.org. Novembre 2008, pag.1.

quello di un acquirente che comprando un articolo tramite carta di credito contestasse in seguito il pagamento o sostenesse che lo stesso non sia stato autorizzato. Per questo le transazioni tramite Bitcoin sono assolutamente irreversibili.

In poche parole, Bitcoin si propone di creare un sistema decentralizzato completamente indipendente da intermediari bancari o organismi governativi, sottraendo al settore bancario la funzione di gestione del sistema di pagamento e della relativa contabilità[78]. Non essendoci un'autorità centrale che controlla le transazioni si potrebbe presentare il problema noto come *double spending,* che consiste nello spendere più volte lo stesso *token* (la moneta digitale effettiva)[79].

Proprio per risolvere questa questione il Bitcoin utilizza sistema *peer to peer* crittografato basato sulla *blockchain*. Un sistema *peer to peer* è un sistema decentralizzato dove i nodi (utenti) si scambiano tra loro un costante flusso d'informazioni[80] e hanno uguale accesso alle risorse pubbliche, la qualcosa consente trasferimenti di denaro direttamente da un nodo all'altro in modo efficace e rapido. Ogni utente, connettendosi alla rete, può interagire con gli altri utenti, validare ed autorizzare transazioni, controllare il registro pubblico e segnalare errori al resto della rete. Una rete decentralizzata è molto resistente, in quanto in caso di malfunzionamento di uno o più nodi, quelli restanti continuerebbero a funzionare reindirizzando la connessione attraverso la rete.

Figura 1: rete centralizzata e decentralizzata.



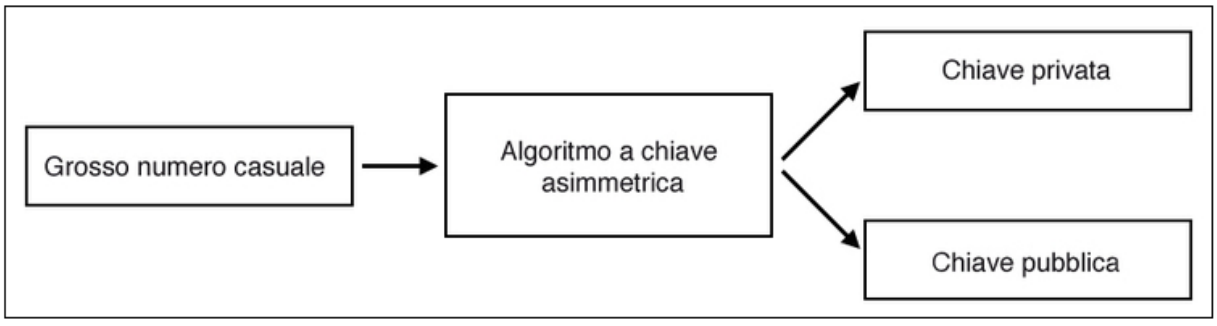
Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

[78] Amato Massimo, Fantacci Luca. Per un pugno di Bitcoin. Milano: Egea, Università Bocconi Editore, 2016.
[79] Dupont Quinn. Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance. Londra: Routledge, 2018, pag. 140.
[80] Studio Legale Giovanni Paolo Accinni e Associati. Profili di complessità e di rischio delle "criptovalute". In Archivio Penale, 2017, pag.4.

2.1.1. COME FUNZIONA IL SISTEMA BITCOIN: CRITTOGRAFIA E BLOCKCHAIN

Essendo un sistema di verifica aperto il problema principale potrebbe risultare quello della sicurezza delle transazioni: questa questione viene definita "il problema dei generali bizantini" (trattasi di una metafora finalizzata a capire come in un determinato contesto si possa raggiungere un consenso in una situazione in cui è possibile la presenza di errori di comunicazione). Dal punto di vista informatico il problema consiste nel raggiungere un consenso su una rete distribuita dove alcuni nodi possono essere difettosi o corrotti. Da qui la necessità di portare a termine in sicurezza un'operazione di scambio di criptovaluta su una rete che non è sicura di per sé. Per rendere sicure le transazioni Bitcoin utilizza la crittografia asimmetrica, ovvero, un tipo di crittografia che si serve di due chiavi una privata e una pubblica e che permette sia di verificare che il messaggio spedito sia rimasto inalterato sia di autenticare il mittente. Le due chiavi sono create allo stesso momento partendo da un grosso numero casuale tramite un algoritmo crittografico asimmetrico a curva ellittica, chiamato ECDSA *(Elliptic Curve Signature Algorithms)*[81]. Esse non possono essere confuse, ma sono strettamente connesse da un legame matematico che fa in modo che la chiave pubblica funzioni solamente con la corrispettiva chiave privata[82] ed inoltre, dalla chiave pubblica non si può risalire a quella privata.

Figura 2: Gli algoritmi a chiave asimmetrica generano una chiave pubblica e una chiave privata basandosi su un grosso numero casuale.

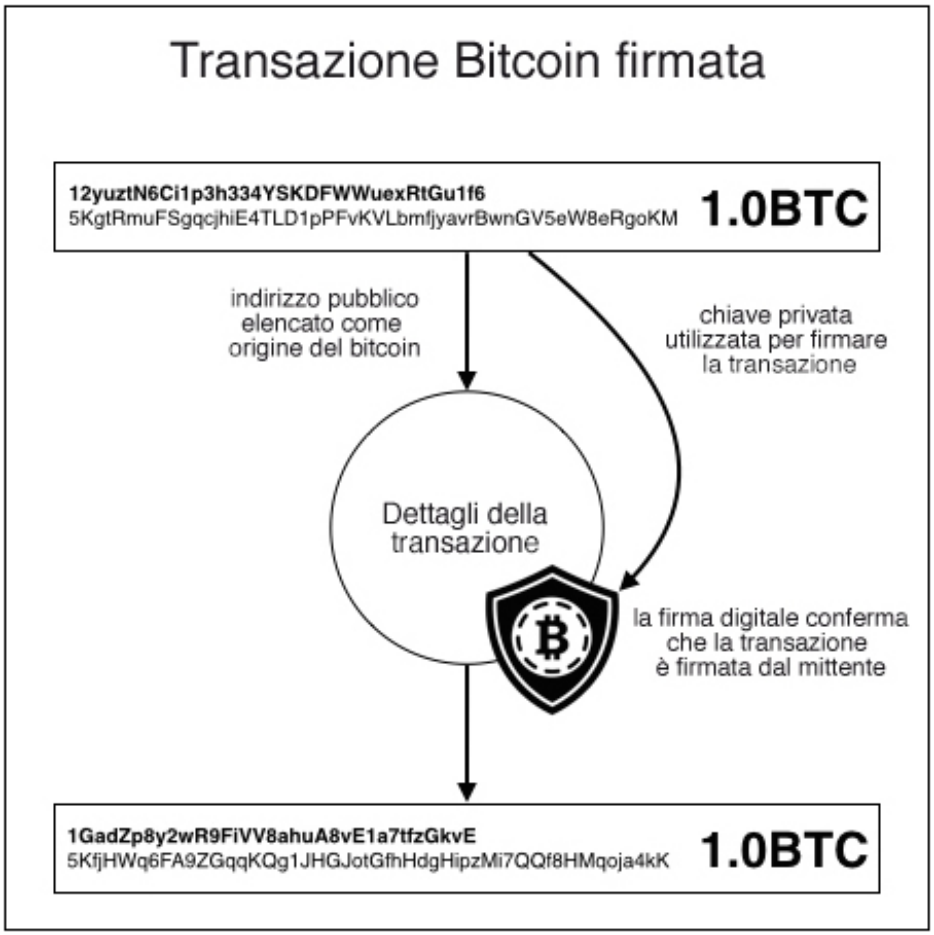


Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

[81] Calzone Ottavio. Bitcoin e distributed ledger technology. Cit. pag. 8.
[82] Passarelli Nina. Bitcoin e antiriciclaggio. In www.sicurezzanazionale.gov.it, 15 novembre 2016, pag.5.

La chiave privata viene utilizzata per crittografare un documento, in questo caso il denaro digitale, ponendo una firma digitale. La chiave pubblica viene utilizzata per decrittografare il documento, verificandone la firma. Chi effettua una transazione genera una coppia di chiavi ed invia al destinatario quella pubblica[83]. Il mittente firma il documento con la chiave privata e lo invia al destinatario, che con la chiave pubblica è in grado di verificare la firma e assicurarsi dell'identità del mittente[84]. Prima di inviare la transazione alla blockchain essa deve essere autenticata dalle firme di tutti gli indirizzi imput da cui provengono i fondi utilizzati.

Figura 3: una transazione con firma digitale.



Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

Le transazioni, raggruppate in blocchi, vengono aggiunte alla blockchain e sono convalidate da una rete di nodi indipendenti, in quanto è il consenso della rete a determinare quali blocchi validare o

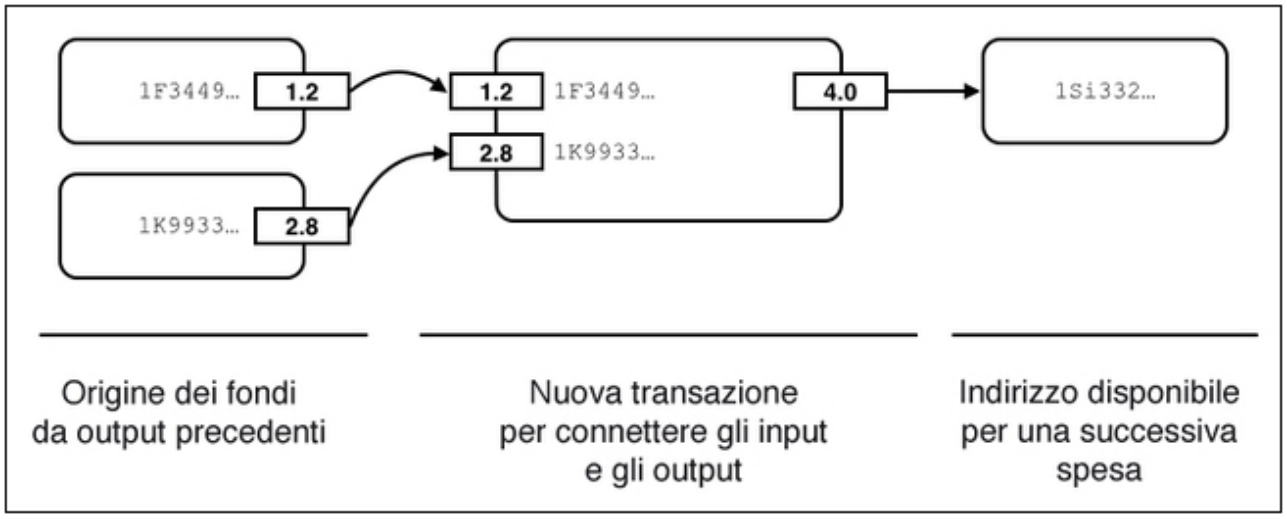
[83] Tampanella Biagio. La crittografia tra arte e scienza. In sicurezzanazionale.gov.it, settembre 2015, pag. 7.
[84] Demarchi Roberto. Gli algoritmi crittografici del bitcoin. In Sicurezza e Giustizia, 2017, pag.45.

meno. La blockchain, che è sicuramente l'innovazione più importante di Bitcoin, è simile ad un libro contabile elettronico, pubblico, in continua espansione e su cui vengono registrate cronologicamente ed in modo permanente tutte le transazioni. Le principali caratteristiche della blockchain sono l'immutabilità del registro, la tracciabilità delle transazioni e la sicurezza basata su tecniche crittografiche[85]. Essa, grazie a complessi algoritmi di crittografia, che analizzeremo in seguito dettagliatamente, non è manomissibile ed è sempre verificabile nel tempo.

Quindi la gestione dei conti e delle transazioni non è più centralizzata ma affidata alla rete e quindi, "decentralizzata". Da questo deriva il termine utilizzato precedentemente *distributed ledger*, che tradotto letteralmente significa "libro mastro distribuito".

I blocchi di transazioni, di cui è articolata la blockchain, sono costituiti da un *blocknumber* identificativo e da informazioni sulla transazione riguardanti l'importo della stessa e lo pseudonimo di chi la compie, aspetto che approfondiremo in seguito. I blocchi sono concatenati l'uno all'altro rendendo possibile risalire a tutte le transazioni bitcoin effettuate fino al *genesis block* ovvero, il blocco iniziale della prima transazione effettuata nel 2009. Le transazioni sono convalidate se gli output corrispondono agli input delle transazioni precedenti. Infatti, non ci sono singoli bitcoin o frazioni degli stessi che vengono trasferiti, come spesso si pensa in modo errato. In questo modo viene risolto il problema della *double spending* ovvero, quando vengono effettuate due transazioni superando il saldo disponibile, questa risulta la prima tecnologia in grado di superare questa problematica senza affidarsi ad un server centrale.

Figura 4: una transazione Bitcoin che impiega due input e un output.

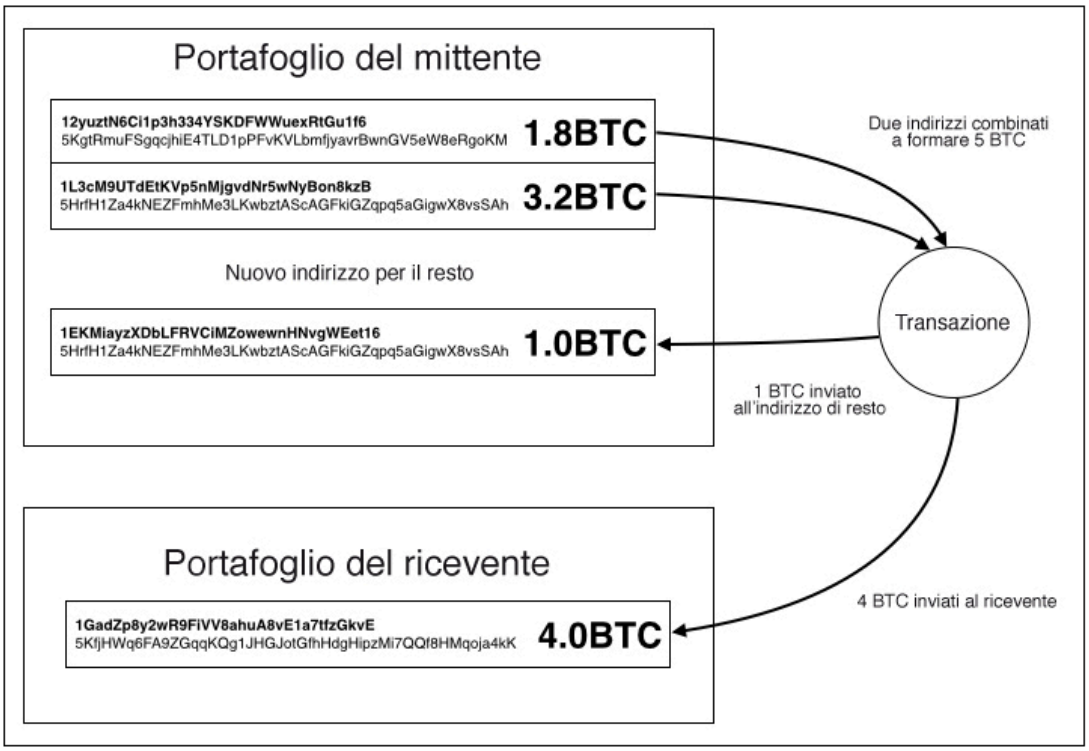


Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

[85] Bellini Mauro. Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia. In blockchain4innovation.it, gennaio 2019.

I portafogli di bitcoin sono formati da un insieme di indirizzi e chiavi private, come è possibile osservare dalla figura, ciascuno di essi viene utilizzato per lo scambio dei bitcoin. Questi vengono convenzionalmente chiamati *wallet*, ma il termine tecnico da utilizzare è *keychain* ovvero portachiavi[86]. Infatti, i portachiavi servono per utilizzare e salvaguardate le chiavi. È estremamente importante proteggere le proprie chiavi private, in quanto la conoscenza di esse consente libero accesso all'utilizzo dei fondi. Una delle precauzioni più note è quella del *cold storage*, che consiste nel conservare fisicamente le chiavi, stampandole su un foglio sotto forma di codice QR o conservandole su una chiavetta USD[87]. Inoltre, solitamente vengo adoperati indirizzi *multi-signature,* i quali necessitano di due o più chiavi per autenticare la compravendita di bitcoin[88]. Il saldo totale del portafoglio è costituito dal saldo di tutti gli indirizzi, che è possibile combinare in un'unica operazione. Essi vengono creati in modo gratuito da Bitcoin ed è possibile averne un numero illimitato. Ogni indirizzo utilizzato per la transazione viene registrato, tenendo in considerazione l'intero saldo del portafoglio. I bitcoin non spesi vengono reindirizzati ad un indirizzo di resto, che può essere sia un nuovo indirizzo sia quello utilizzato per il trasferimento. La maggior parte degli utenti però, utilizza un nuovo indirizzo in modo tale da aumentare la privacy della transazione.

Figura 5: transazione bitcoin con indirizzo di resto.

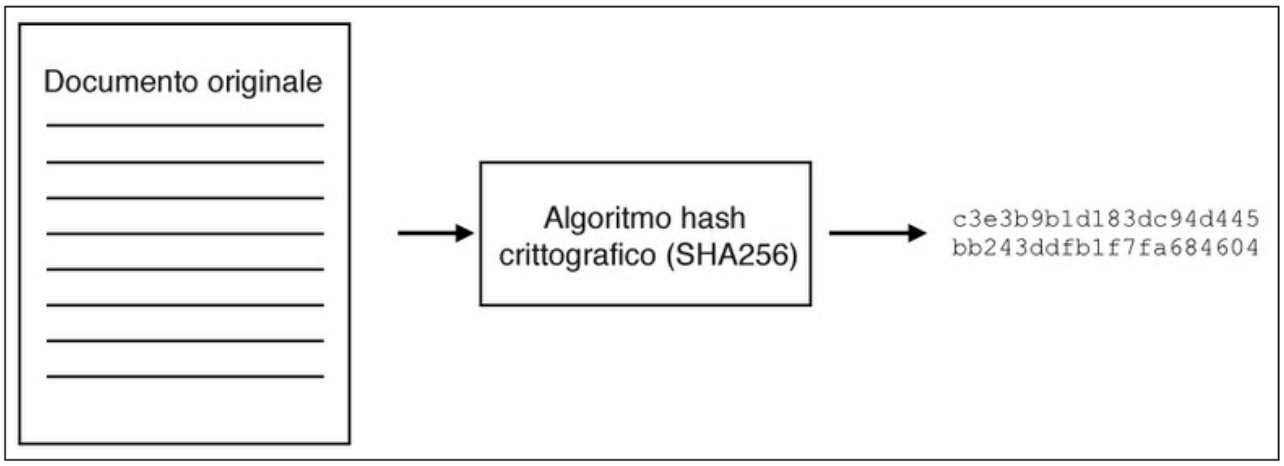


Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

[86] Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute. Milano: Apogeo, 2016.
[87] Investopedia. What is cold storage for Bitcoin? In www.investopedia.com, novembre 2018.
[88] Carlisle David. Virtual Currencies and Financial Crime: Challenges and Opportunities. Royal United Services Institute for Defence and Security Studies, marzo 2017, pag. 21.

Gli indirizzi bitcoin sono creati dalla chiave pubblica. Per comprendere il procedimento con cui vengono creati è necessario introdurre il concetto di algoritmi hash crittografici. Gli algoritmi hash crittografici sono delle funzioni che creano dei digest, ovvero, un'impronta digitale che contiene un certo numero di informazioni. Il digest è in pratica una breve stringa di caratteri che corrisponde alla sintesi di un certo quantitativo di dati[89]. L'algoritmo hash più conosciuto è lo SHA256 (Secure Hash Algoritm), il quale è stato sviluppato dal NSA (National Security Agency). Lo SHA256 genera un digest di 40 caratteri da un qualsiasi documento, indipendentemente dalla grandezza di questo. Una qualsiasi modifica del documento, anche se minima, produrrà un codice completamente diverso. Inoltre, nonostante il digest abbia una forte relazione matematica con il documento da cui è stato generato, una volta criptate le informazioni, esse non possono essere decriptate per tornare al documento originale[90]. I codici hash vengono utilizzati per verificare che il documento iniziale non sia stato modificato, ciò avviene semplicemente tramite il confronto tra il codice hash del documento originale e con quello ricavato dalla copia del documento. Bitcoin oltre a ciò che concerne la creazione degli indirizzi utilizza delle codificazioni Hash per diverse funzionalità. Ad esempio, tutte le transazioni sono codificate con questa modalità ed il codice viene firmato per garantire la sicurezza dell'operazione. I blocchi stessi della blockchain sono sottoposti a codifica hash per assicurare che la cronologia delle transazioni non venga alterata.

Figura 6: Gli hash crittografici generano un digest a partire da un documento.



Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

[89] Calzone Ottavio. Bitcoin e distributed ledger technology. Cit. pag. 9.
[90] Tampanella Biagio. La crittografia tra arte e scienza. Cit. pag. 6.

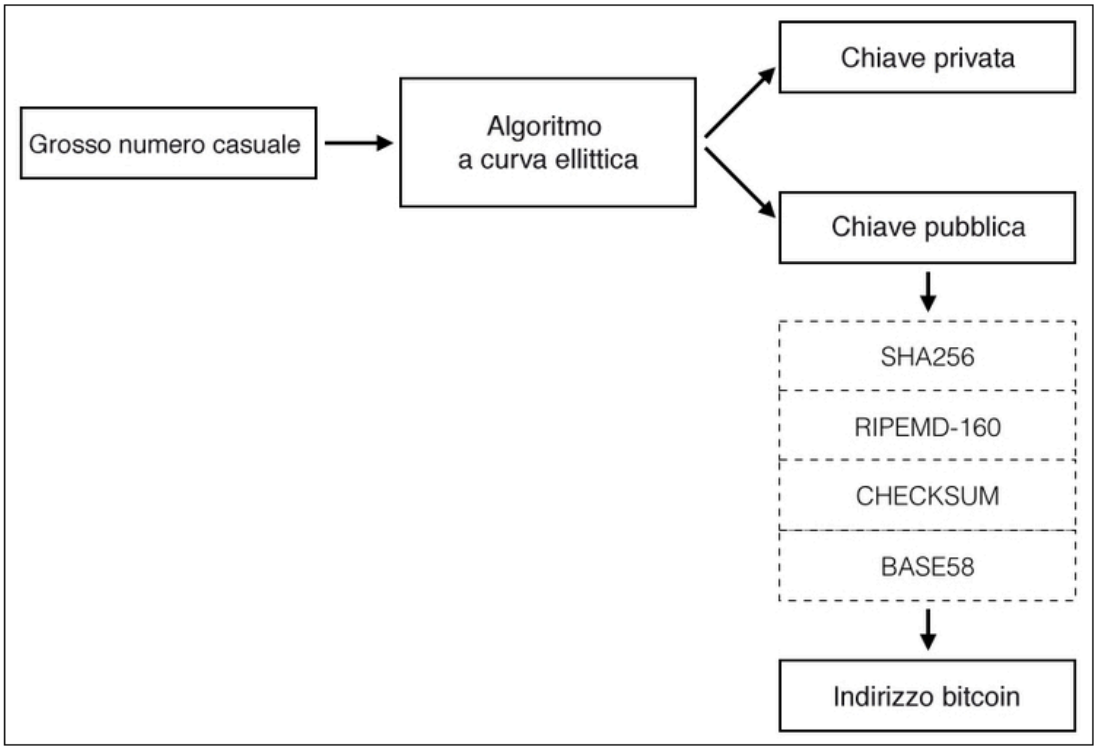
Ritornando al processo di generazione degli indirizzi, essi sono creati applicando alla chiave pubblica gli algoritmi hash SHA256 e RIPEMD-160[91]. In seguito, viene inserito all'inizio del codice un identificativo numerico, che caratterizza la rete di appartenenza. Infatti, oltre alla rete principale esiste un'altra rete utilizzata dagli sviluppatori per effettuare dei test, chiamata *Testnet3*. L'identificativo della rete principale è 00.

Successivamente, viene calcolato un codice *checksum*, la cui funzionalità è quella di garantire che i caratteri contenuti dall'indirizzo siano corretti[92]; se il *checksum* è errato, lo è anche l'indirizzo inserito. Il *checksum* viene aggiunto alla fine della sequenza alfanumerica ottenuta fino ad adesso.

L'ultimo passaggio nella creazione dell'indirizzo consiste nell'applicare una funzione BASE 58 alla sequenza, con il fine di codificare una grossa sequenza in una più piccola leggibile da chiunque.

Chiaramente questo processo è automatizzato e il suo risultato è un indirizzo pubblico che viene utilizzato per ricevere ed inviare bitcoin.

Figura 7: il processo di generazione di un indirizzo Bitcoin a partire da una chiave pubblica.



Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

[91] Ferraresso Andrea. Bitcoin: come funziona il sistema. Le coppie di chiavi, il funzionamento della blockchain, la proof-of.work. In mediunm.com, maggio 2016.

[92] Passarelli Nina. Bitcoin e antiriciclaggio. Cit. pag.5.

2.1.2. IL MINING

In precedenza, abbiamo parlato di verifica delle transazioni. Infatti, le nuove transazioni inviate alla rete sono definite inizialmente come non confermate in quando la rete non ha ancora stabilito se queste siano valide o meno. Il compito di verificarle è svolto dai miner, nodi che risolvendo un difficile problema di calcolo matematico processano e confermano le transazioni raggruppandole in blocchi e costruendo in tal modo la blockchain[93]. L'attività svolta dai miner è essenziale per il funzionamento del sistema, in quanto senza di loro non si potrebbero effettuare transazioni in bitcoin[94]. Essi sono pagati dallo stesso sistema per cui risolvono il problema, per cui più problemi crittografici riescono a risolvere più essi guadagnano bitcoin.

Il mining prevede l'uso di un nuovo blocco di transazioni come base di un problema di difficile soluzione. Per ricevere la ricompensa, che si sostanzia in nuovi bitcoin emessi dal sistema, più il costo delle commissioni per aver validato la transazione, essi devono trasmettere la prova (*proof of work)* che il problema matematico sia stato risolto[95]. Le commissioni guadagnate dai miner sono un incentivo che viene dato loro da chi compie le transazioni al fine di processare e convalidare più velocemente le stesse.

Analizziamo in modo più specifico l'attività di mining.

In *primis* ogni nodo possiede una copia dell'intera blockchain, contenente ogni transazione dall'inizio alla fine della catena. Grazie a ciò i miner sono in grado di verificare il saldo della spesa di ogni transazione ed evitare il sopracitato fenomeno della *double spending*.

In secondo luogo, essi verificano l'integrità della firma digitale utilizzando algoritmi crittografici. Il miner è sempre in grado di accertarsi dell'originalità della transazione, in quanto ogni alterazione produrrebbe una firma non valida.

Cosi facendo il miner ha a disposizione una lista di transazioni valide con le quali può creare un nuovo blocco che sarà utilizzato come base per risolvere il difficile problema di calcolo. Questo consiste nel generare un codice hash di difficoltà inferiore rispetto al target stabilito. Precedentemente abbiamo visto che gli algoritmi crittografici hash vengono utilizzati per creare una sintesi alfanumerica di un certo quantitativo di dati. In questo caso i dati in questione sono rappresentati dal nuovo blocco di transazioni che si sta sottoponendo a validazione. I miner utilizzano la funzione hash per generare un risultato. Se questo risultato è inferiore al target stabilito, esso viene considerato come

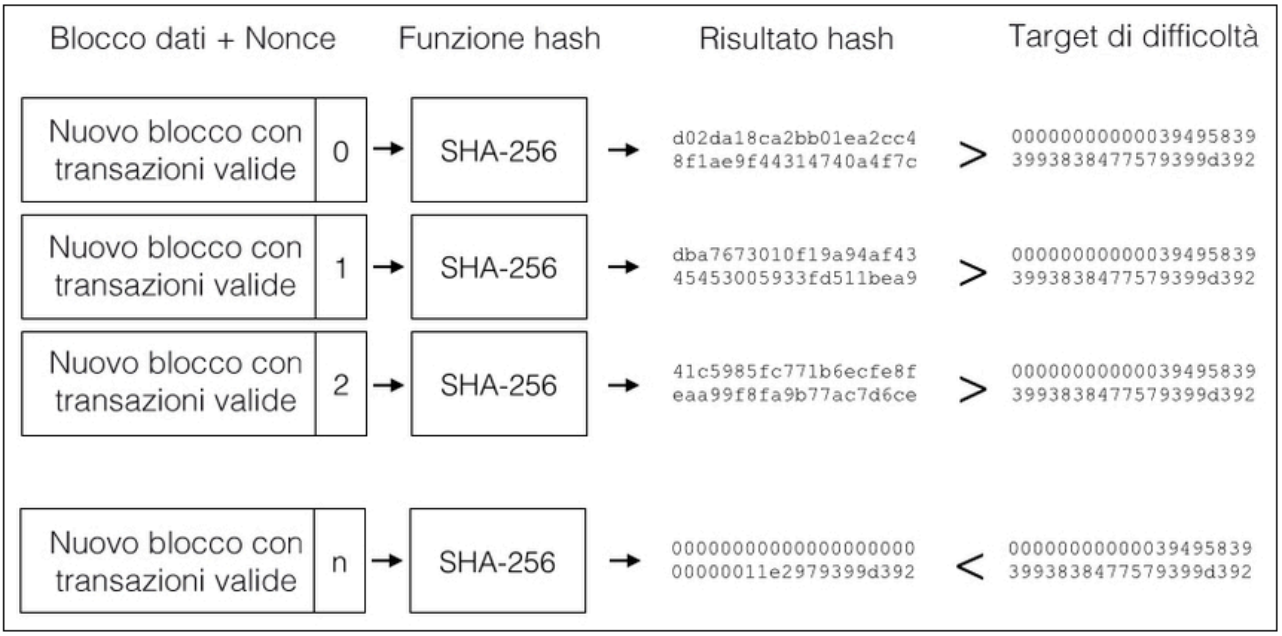
[93] Bellini Mauro. Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia. Cit.

[94] Mancini Marco. Valute virtuali e Bitcoin. In Analisi Giuridica dell'Economia. Bologna: Il Mulino, giungo 2015, pag. 120.

[95] Bernaschi Massimo e Mastrstefano Enrico. Una descrizione (quasi) informatica del funzionamento di bitcoin. In Etica Economica, novembre 2014, pag. 2.

soluzione. Se il risultato non dovesse corrispondere, verrebbe aggiunto un numero ai dati, chiamato *nonce*, per dare al miner un altro tentativo[96].

Figura 8: L'attività di mining prevede l'incremento di un codice nonce, per generare un nuovo codice hash, fino a trovare una soluzione.



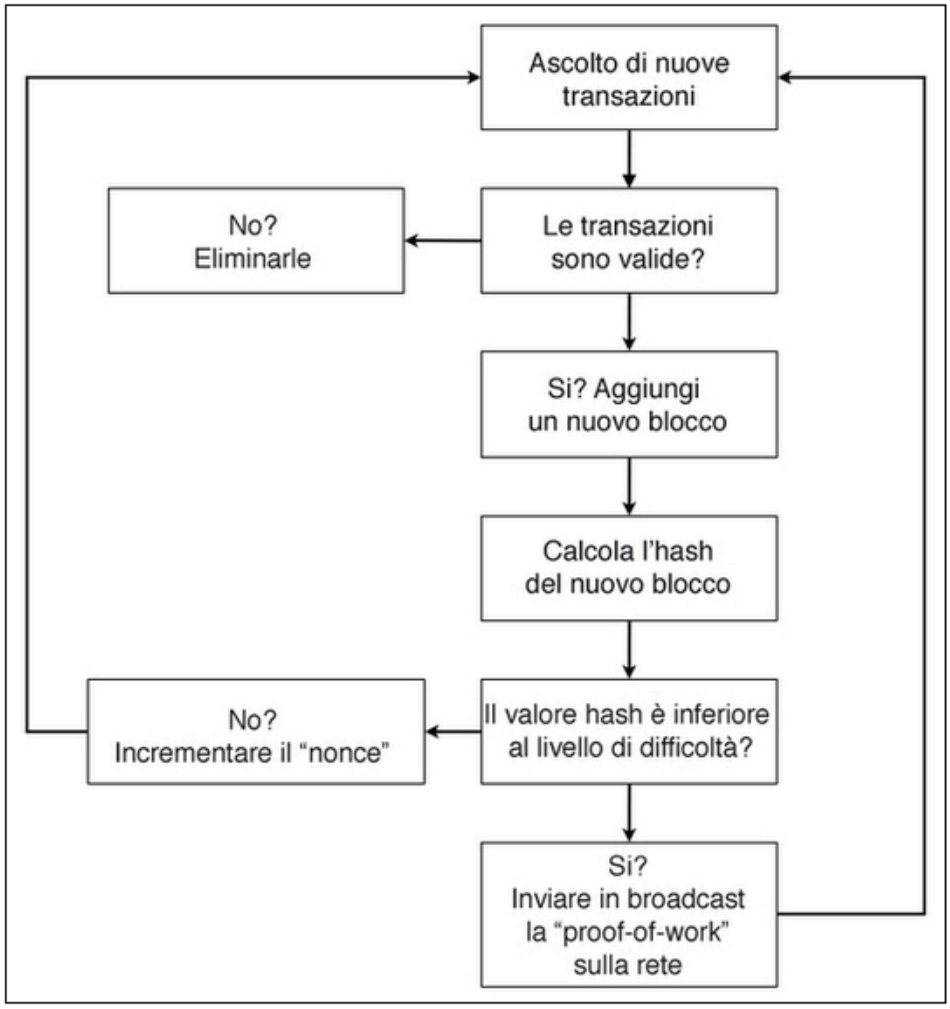
Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

Abbiamo detto più volte che aggiungendo anche una singola variazione ai dati, il codice hash risultante sarebbe stato completamente diverso da quello precedente. Quindi, anche il nuovo codice hash, che il miner dovrà ricercare, seguirà questa logica. L'operazione viene ripetuta finche non verrà trovata una soluzione. Una volta trovata viene trasmessa alla rete come nuovo blocco contenente anche l'obbiettivo di difficoltà e il nonce vincente. Questa viene chiamata *proof of work*[97]. Nella figura si può osservare come il blocco di dati viene utilizzato diverse volte come base di calcolo al fine di trovare un codice hash minore del livello di difficoltà. Il livello di difficoltà viene regolato in modo da mantenere la frequenza delle ricompense all'incirca ogni 10 minuti. Se la frequenza dei blocchi che sono stati accettati è inferiore a 10 minuti, la difficoltà viene aumentata e viceversa. Esso viene aggiornato ogni 2016 blocchi[98].

[96] Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute. Cit.
[97] Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute. Cit.
[98] Ferraresso Andrea. Bitcoin: come funziona il sistema. Le coppie di chiavi, il funzionamento della blockchain, la proof-of.work. Cit.

Questa operazione viene definita soluzione ad un difficile problema di calcolo, in quanto è un'operazione estremamente costosa a livello computazionale. Per ottenere la *proof of work* il codice hash viene eseguito milioni di volte al secondo.

Figura 9: un riepilogo delle attività di mining di bitcoin.



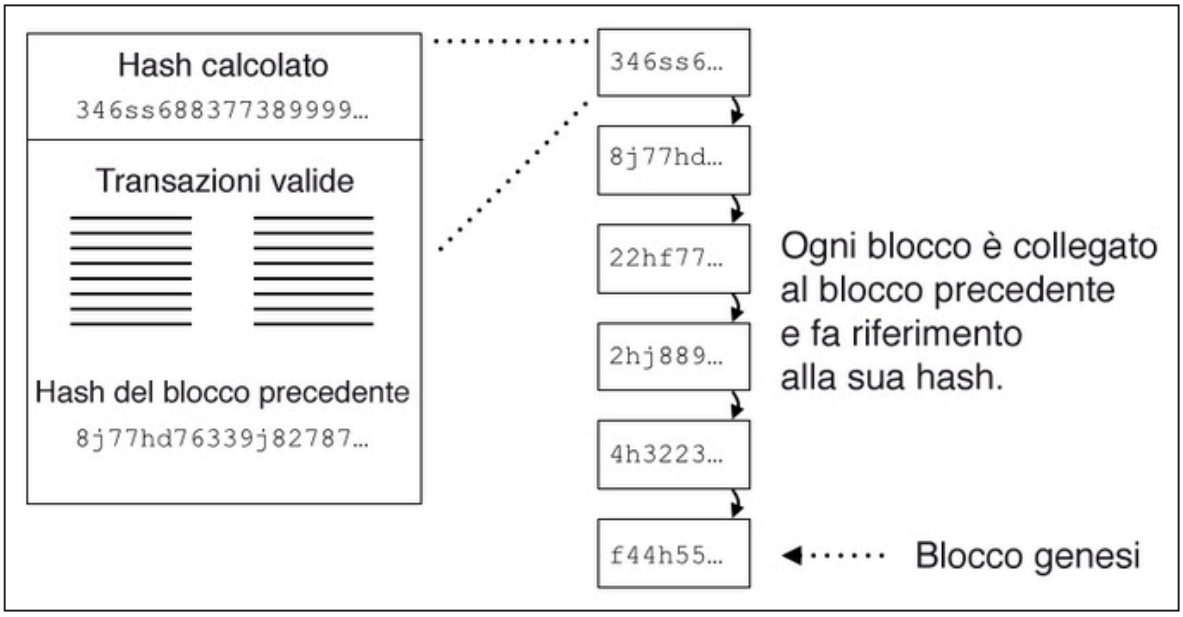
Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

Come abbiamo visto, la blockchain è una concatenazione di blocchi ed ogni nodo della rete gestisce una copia completa della blockchain. I miner ascoltano le transazioni sulla rete e minano i nuovi blocchi. La conferma del blocco viene definita tramite un codice hash, questo viene calcolato sul blocco stesso, sulle precedenti transazioni e sul codice hash del blocco precedente[99]. Quindi, ogni

[99] Capogena Alessandro, Peraino Leandro, Perugi Silvia, Cecili marco, Zbrorowski Giovanni, Ruffo Andrea. Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione. In Diritto Mercato Tecnologia, n°3, 2015, pag. 38.

blocco contiene il codice hash del blocco precedente ed ogni minima variazione modificherà il codice hash e l'intera catena, che perderebbe in questo modo la sua validità[100].

Figura 10: la blockchain è costituita da più blocchi concatenati.



Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

In linea teorica chiunque può diventare un miner. Chiaramente la situazione non è cosi nella realtà, in quanto per minare i bitcoin non basta il computer di casa. Vista la complessità dei problemi matematici da risolvere, per fare mining è necessario l'utilizzo computer che sono stati progettati appositamente con questo scopo, con hardware dotati di un'elevata potenza di calcolo[101]. È vero che i miner vengono ricompensati, ma tutto ha un prezzo, ed in questo caso è anche ingente, infatti, le società che si occupano di mining e che sono situate principalmente negli Stati Uniti, in Corea ed in Cina hanno effettuato enormi investimenti in attrezzature al fine di poter svolgere questa attività. John McAfee che possiede la più grande società di mining negli Stati Uniti disse che per effettuare il mining di un bitcoin, il costo tra l'investimento in attrezzature e di elettricità è di circa 100€ a bitcoin.

[100] European Central Bank. Virtual currencies Schemes. Ottobre 2012, pag.24.
[101] Mancini Novella. Bitcoin: rischi e difficoltà normative. Bologna: Il Mulino, in Banca impresa società, 2016, pag.126.

2.1.3 IL BITCOIN COME VALUTA VIRTUALE

Dopo aver analizzato il funzionamento di Bitcoin, focalizziamoci sulla moneta virtuale che è stata creata appositamente per la rete in questione: il bitcoin.

Il bitcoin viene definito contante digitale, in quanto il sistema Bitcoin è stato in grado di unire le caratteristiche delle due monete preesistenti, quella fisica e quella elettronica, condensandone i rispettivi vantaggi. Il contante ha le peculiarità di essere accessibile a chiunque e anonimo, infatti in una transazione in contanti non viene ovviamente tracciato né il mittente né il destinatario e non viene indicata la casuale del pagamento. La moneta elettronica, invece, si caratterizza per la tracciabilità, la facilità di utilizzo e la possibilità di effettuare pagamenti a distanza e di non dover essere cambiata alla frontiera. Il bitcoin si posiziona tra le due tipologie di moneta in quanto, come un bonifico permette pagamenti a distanza e, come il contante, permette pagamenti istantanei e senza costi né per il pagante né per il ricevente[102].

Inoltre, esso è anonimo come una banconota in quanto le identità delle controparti che la scambiano non sono note, in più è possibile dividerlo fino ad 8 cifre decimali e moltiplicarlo a piacere in quanto è un puro numero digitale. Ciò da la possibilità di effettuare sia transazioni di grande importo sia micro-pagamenti. Infine, al pari di una carta di pagamento è possibile effettuare pagamenti in tempo reale, in sicurezza ed in tutto il mondo ma in questo caso senza la presenza di nessun intermediario finanziario che ne certifichi la disponibilità dei fondi o che autorizzi la transazione. I costi delle transazioni utilizzando il sistema Bitcoin sono inferiori a quelli del sistema di pagamento elettronico. Si tratta di circa l'1% della transazione avvenuta in bitcoin contro il 2-4% dei sistemi elettronici tradizionali[103]. Bitcoin non si propone solo come una tecnologia all'avanguardia, ma anche come una moneta alternativa e con ciò intendiamo non solo la trasmissione di potere d'acquisto da un soggetto ad un altro ma anche l'essere nel contempo un'unità di conto, un mezzo di scambio e una riserva di valore. Infatti, recentemente parecchi negozi fisici cominciano ad accettare in pagamento il bitcoin esponendone addirittura il logo per una pronta visibilità per coloro che intendono utilizzare questa forma di pagamento.

Un altro fattore che caratterizza i bitcoin e, che lo differenzia da ogni altro tipo di moneta utilizzata, è quello di essere un attivo per chi lo possiede senza essere un passivo per qualcun altro. Infatti, i soldi tenuti su un conto corrente rappresentano un credito del cliente ed un debito della banca, anche la moneta scritturale che abbiamo nei portafogli e, che è stata emessa da una determinata banca centrale, non rappresenta solamente un attivo per chi la possiede, bensì è anche un passivo per la

[102] Passarelli Nina. Bitcoin e antiriciclaggio. Cit. pag. 2.

[103] [82]Amato Massimo, Fantacci Luca. Per un pugno di Bitcoin. Cit. pag. 10.

banca centrale stessa. Il bitcoin, invece, è una moneta elettronica che non costituisce un credito o un debito per nessuno, essa è un numero contabilizzato su un registro digitale che non da alcun diritto ad una conversione in contanti. Per questo si considerano i bitcoin concettualmente simili all'oro. Infatti, anche l'oro è un bene che costituisce un attivo per il possessore ma non rappresenta un passivo per chi non lo detiene. Si può quindi dire che il possessore di bitcoin come quello dell'oro è un "creditore senza debitore[104]". I bitcoin e l'oro hanno altre importanti affinità, tra queste il fatto che il potere d'acquisto di entrambi dipende dalla presenza di qualcuno che è disposto ad accettarli come mezzo di scambio. Inoltre, a differenza delle altre monete il cui valore può essere determinato anche dall'emissione della banca centrale di competenza, il valore dei bitcoin, come quello dell'oro, dipende dalla sua scarsità e dalla domanda nei mercati. La scarsità dell'oro è determinata dalla natura e dalla sua difficoltà di estrazione, mentre quella del bitcoin ha origine nel protocollo informatico che ne regola la quantità e che rende costosa e difficile la sua creazione; per il bitcoin, infatti, si parla di scarsità artificiale. In precedenza, abbiamo trattato la questione del mining osservando che i miner ricevono una ricompensa in nuovi bitcoin per il loro lavoro di validazione dei blocchi di transazioni. È proprio questa la modalità con cui vengono creati nuovi bitcoin, tramite l'emissione ai miner stessi. Tutto ciò viene stabilito da un protocollo informatico che regola la quantità di bitcoin da emettere come ricompensa. Il protocollo regola l'emissione in modo tale da far crescere la quantità di bitcoin creati all'inizio molto velocemente e successivamente sempre più lentamente, fino a stabilizzarsi asintoticamente sotto la soglia dei 21 milioni verso il 2030. I blocchi vengono validati mediamente ogni 10 minuti e la quantità di bitcoin emessa si dimezza ogni 210.000 blocchi, ovvero ogni 4 anni circa[105]. Nel 2008 la ricompensa per la validazione di ogni blocco era di 50 bitcoin, nel novembre del 2012 questa è stata diminuita a 25 bitcoin e successivamente nel luglio 2016 la ricompensa è scesa a 12,5[106].

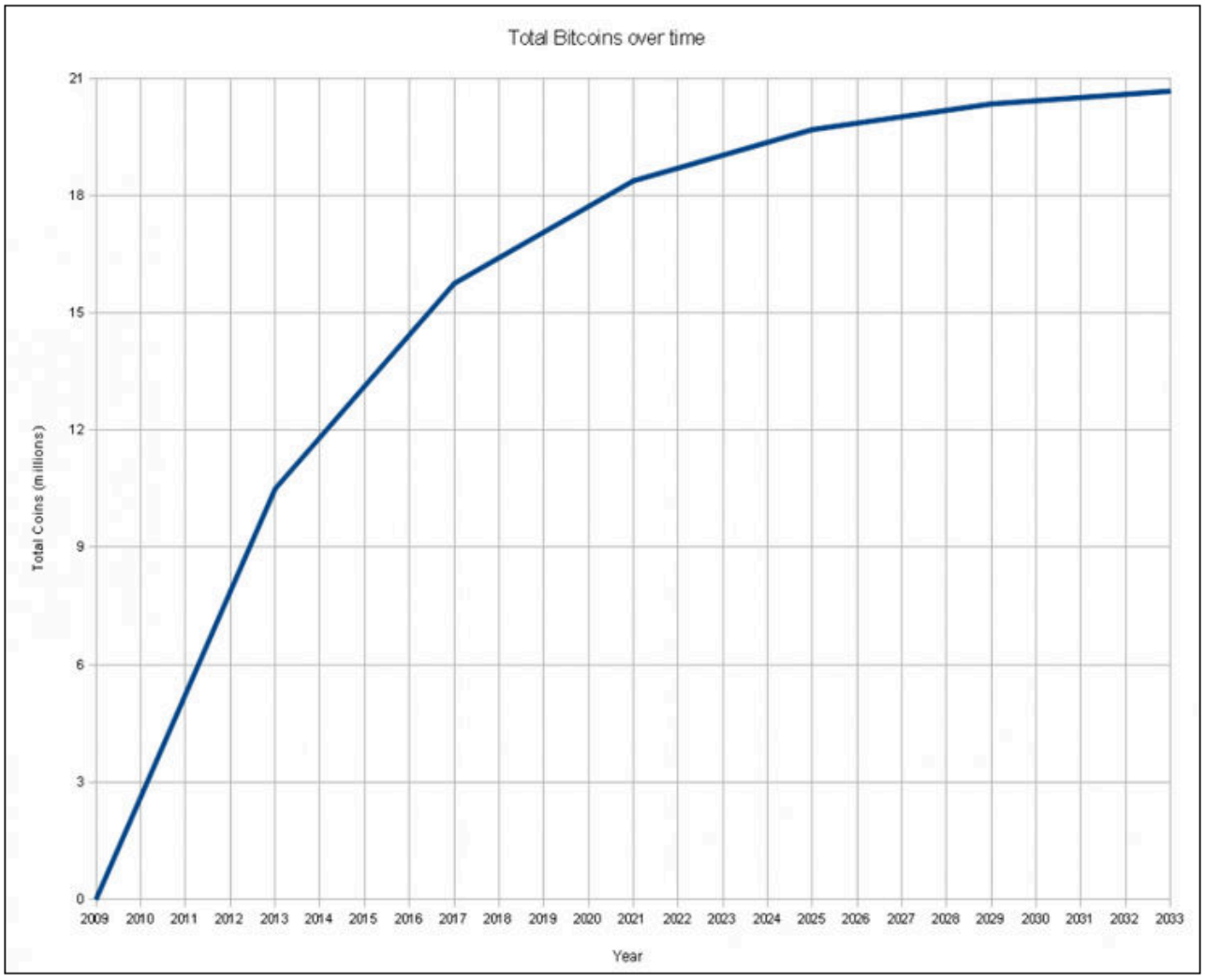
La figura mostra la curva di distribuzione di bitcoin nel tempo; essa è stata ideata per compensare la legge di Moore, che prevede che la potenza di calcolo raddoppi ogni due anni. La quantità di bitcoin cresce con un andamento decrescente, considerando che i bitcoin sono divisibili fino ad 8 cifre decimali, di cui il sottomultiplo minore è chiamato satoshi in omaggio allo pseudonimo del suo inventore, è stimato che l'ultima frazione di bitcoin verrà scoperta all'incirca nell'anno 2140[107].

Il fatto che la sua quantità venga determinata da un protocollo matematico e non da una banca centrale, che ne può determinare il valore grazie alle proprie decisioni, costituisce nell'opinione dei programmatori di Bitcoin e dei suoi sostenitori un punto di forza ragguardevole. Ciò a cui punta

[105] Calzone Ottavio. Bitcoin e distributed ledger technology. Cit. pag. 11
[106] Team Tokens24. Redditività del Mining di Bitcoin nel 2018. In www.tokens24.com, marzo 2018.
[107] Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute. Cit.

Bitcoin è la completa eliminazione del fattore umano nella creazione della moneta, non fidandosi dei banchieri centrali in quanto suscettibili di errore o di perseguire interessi di parte.

Figura 11: emissione di bitcoin nel corso del tempo.



Fonte: Caetano Richard. Bitcoin: guida all'utilizzo delle criptovalute.

Investire nei bitcoin può risultare piuttosto imprevedibile e rischioso in quanto il loro valore è stato soggetto nell'ultimo periodo a grande volatilità[108]. Questo può portare gli investitori meno consapevoli ad ottenere grandi guadagni ma anche a soffrire perdite notevoli. Procedendo con ordine riepiloghiamo la storia del valore dei bitcoin per comprendere quanto questo asset sia estremamente volatile e soggetto a grandi speculazioni fino a diventare una bolla finanziaria tra la fine del 2017 ed il 2018.

[108] Studio Legale Giovanni Paolo Accinni e Associati. Profili di complessità e di rischio delle "criptovalute". Cit. pag. 9.

Il prezzo dei bitcoin è rappresentato dal tasso di cambio dollaro/bitcoin e come quello di qualsiasi altra valuta risponde alle leggi della domanda e dell'offerta. Quindi, in assenza di qualcuno disposto a pagare una somma per ottenere bitcoin il cambio è rimasto a 0 fino all'agosto del 2010, quando un bitcoin è stato scambiato per $0,074. La parità con il dollaro è stata raggiunta all'inizio dell'anno seguente. Da quel momento i bitcoin hanno riscosso sempre più risonanza mediatica, ed il loro prezzo è stato soggetto a diverse impennate fino a culminare con la bolla menzionata in precedenza. La prima bolla è avvenuta nel 2013, in quell'anno il prezzo salì in modo considerevole fino a novembre, quando ebbe un'impennata fino a raggiungere il valore di $1.205. Ci furono diverse motivazioni che determinarono questa notevole crescita del prezzo. Determinanti furono i fatti accaduti a Cipro durante la crisi finanziaria che il paese ha vissuto in quegli anni. Cipro fu colpita da un'ingente crisi finanziaria che culminò nel 2013 quando venne imposto il *bail-in* fino al 9,9% sui depositi bancari[109]. Il *bail-in* è il prelievo forzoso di una percentuale arbitraria dei depositi bancari[110]. Chiaramente questa misura scatenò il panico sia tra la popolazione cipriota che tra gli investitori stranieri, soprattutto russi, che detenevano i propri capitali presso le banche dell'isola. Il risultato fu lo scatenarsi di una corsa agli sportelli e molti dei capitali ritirati venne convertito proprio in bitcoin. Tutto ciò diede ai bitcoin un'inaspettata risonanza mediatica a livello globale. Un altro avvenimento che ha determinato l'impennata dei prezzi del 2013 è stata l'apertura del mercato cinese verso i bitcoin. Il responsabile della sorveglianza dei flussi finanziari delle Cina dichiarò che da quel momento in poi per i cinesi sarebbe stato possibile investire nella criptovaluta ed aggiunse che la Cina stessa avrebbe aperto una posizione lunga sul bitcoin. Questo fece schizzare il prezzo della criptovaluta fino alla quota sopracitata salvo poi diminuire velocemente nei mesi successivi assestandosi sui $300 anche a causa del dietrofront della Cina in merito alla sopracitata politica d'acquisto della criptovaluta.

Questa bolla, che all'epoca è stata significativa, appare quasi irrilevante in confronto a quella che ci fu a cavallo tra il 2017 ed il 2018. Negli ultimi mesi dl 2017 il prezzo dei bitcoin è iniziato ad aumentare in modo sempre più consistente fino al mese di novembre quando ha avuto un balzo vertiginoso. Il 10 dicembre 2017 è stato toccato il picco record di $19.345,49. Da quel momento in poi il valore del bitcoin ha iniziato una brusca diminuzione segnando perdite record. Il drastico calo successivo al picco è stato *demand driven*, ovvero determinato principalmente dalla fuga degli investitori speculativi dell'ultima ora.[111] Al momento in cui si scrive (dicembre '18) il prezzo continua una discesa, che sembra inesorabile, causata dallo scoppio della bolla di cui la criptovaluta è stata protagonista.

[109] Da Rold Vittorio. Cipro, salvataggio choc: prelievo forzoso fino al 9,9% sui depositi bancari. Corsa dei correntisti ai bancomat. Oggi si riunisce il Parlamento. Sole 24 Ore, 16 marzo 2016.
[110] Calzone Ottavio. Bitcoin e distributed ledger technology. Cit. pag. 3.
[111] Minenna Marcello. L'esplosione della bolla Bitcoin: un'autopsia. Il Sole 24 Ore, 31 dicembre 2018.

Appare evidente come il bitcoin, soprattutto in questo periodo, sia stato soggetto a grandi speculazioni, prima rialziste ed in questo periodo ribassasse. Le vittime di questa situazione sono gli investitori occasionali che si sono lasciati prendere dalla frenesia del momento e hanno investito nella valuta quando la crescita del prezzo sembrava non fermarsi mai. A fonte di ciò, c'è anche chi ha ottenuto guadagni interessanti. Discorso diverso per gli investitori professionali che si muovono prima della massa e che hanno ottenuto grandi guadagni investendo prima della bolla e che hanno disinvestito, o preso posizioni corte ben prima che la stessa scoppiasse.
Per concludere, il bitcoin è un asset estremamente volatile e ciò non è mai un aspetto positivo quando ci si riferisce ad una valuta. Basti pensare che nella prima transazione in bitcoin, avvenuta nel 2010, furono comprate due pizze dal valore di $25 per 10.000 bitcoin. Ad adesso un bitcoin, nonostante le recenti grandi perdite, vale $3.818 e i bitcoin utilizzati per comprare le pizze valgono più di 38 milioni di dollari[112]. È senza dubbio un'evoluzione allarmante e, al momento, difficilmente controllabile per una valuta che ha meno di dieci anni di vita.

2.2. IL RICICLAGGIO ATTRAVERSO I BITCOIN

Abbiamo osservato come le virtual currencies, con particolare riferimento ai bitcoin, presentano dei vantaggi per coloro che le utilizzano.
Tra questi ricordiamo:

- la velocità del sistema utilizzato, che consente transazioni in pochissimi secondi;
- la natura globale del sistema di pagamento per la quale è possibile effettuare e ricevere pagamenti a livello internazionale;
- la facilità di utilizzo, anche da parte di chi non ha una solida preparazione informatica;
- la possibilità di effettuare micro-pagamenti;
- il bassissimo costo delle transazioni.

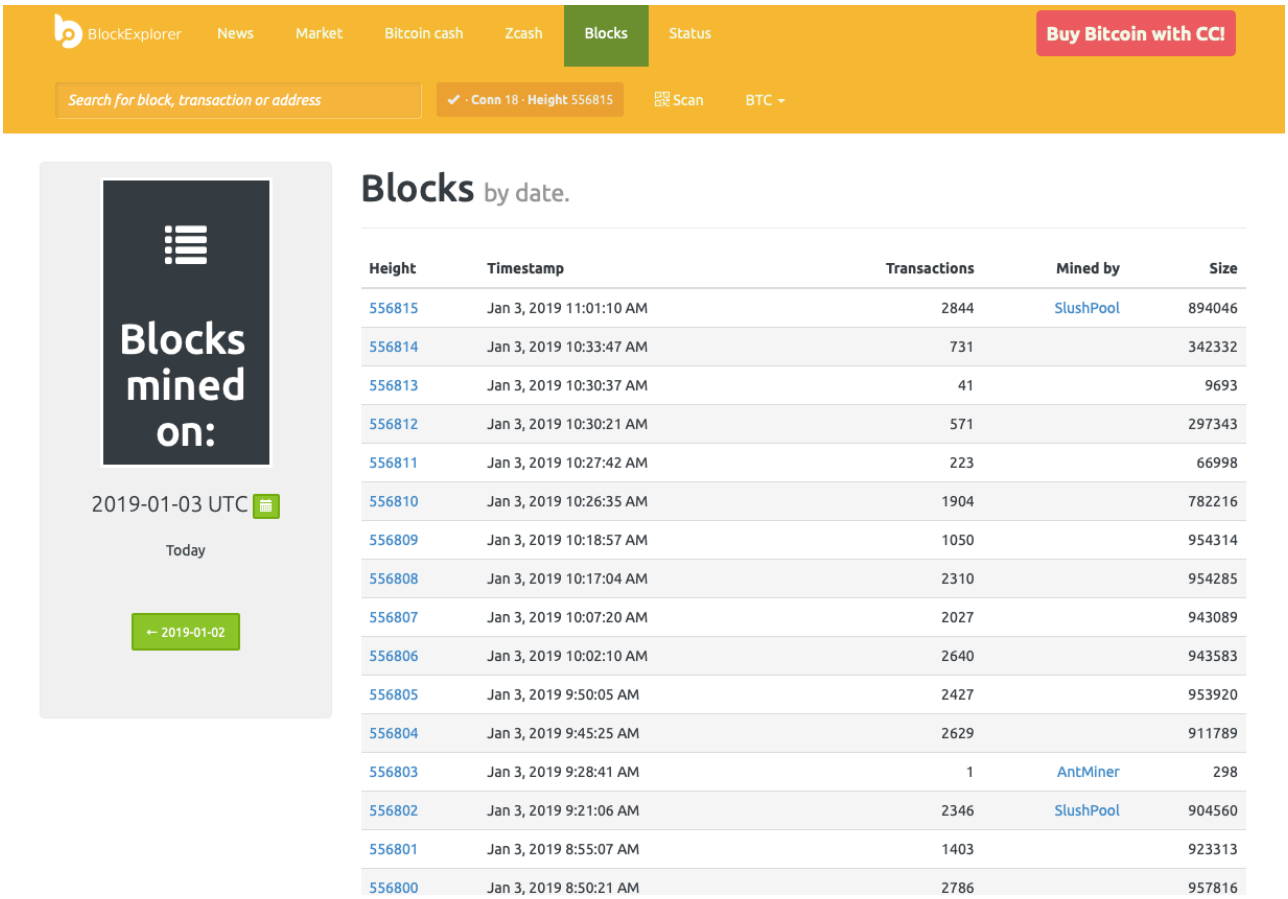
Oltre alle qualità trattate ci sono delle caratteristiche intrinseche nel sistema delle criptovalute che le rendono terreno fertile per il proliferarsi di attività criminali. Inoltre, le valute virtuali, come evidenziato in precedenza, sono state protagoniste di una diffusione esponenziale in un breve lasso di tempo. Questa crescita non è stata accompagnata da una regolamentazione internazionale adeguata

[112] Dati consultabili su finance.yahoo.com.

che cerchi di limitare gli usi illeciti delle criptovalute. Nonostante ciò, i principali organismi internazionali sono ben consapevoli che le criptovalute convertibili in moneta legale presentano profili di rischio estremamente elevati per ciò che concerne il riciclaggio ed il finanziamento del terrorismo. Tant'è che L'EBA (European Banking Autority) nella catalogazione dei rischi connessi alle valute virtuali, contenuta nell'analisi "EBA Opinion on Virtual Currencies", assegna il livello più alto possibile di pericolosità al rischio di riciclaggio, di finanziamento del terrorismo, della compravendita di sostanze e materiale illegale e all'utilizzo di queste nel perseguire ricatti o truffe.[113]
Perché le valute virtuali risultano cosi appetibili all'utilizzo per fini criminali?
La componente che gioca un ruolo fondamentale nella questione è quella dell'anonimato. Infatti, come abbiamo visto, tramite le valute virtuali è possibile effettuare con velocità operazioni in tutto il mondo celando la propria identità. Seppure è vero che la Blockchain permette di risalire cronologicamente a tutte le transazioni effettuate e che quindi è possibile osservare tutti i flussi di denaro in entrata ed in uscita di un determinato indirizzo. É quanto mai determinante il fatto che gli indirizzi Bitcoin sono contraddistinti dall'anonimato, in quanto non permettono di conoscere l'identità del suo possessore.
L'anonimato delle transazioni bitconiane deriva dalla natura degli indirizzi utilizzati per effettuare le transazioni. Questi, infatti, sono formati da dei codici alfanumerici che non svelano l'identità del possessore[114]. Per di più durante la creazione di un indirizzo Bitcoin non viene richiesto un identificativo che consenta di confermare che il nominativo inserito sia reale. Quindi, è possibile creare un indirizzo Bitcoin inserendo uno pseudonimo che permette di celare la propria reale identità. Questo rende estremamente difficile per le autorità rintracciare coloro che utilizzano i bitcoin con fini illeciti. Appare chiaro come i criminali traggano giovamento da qualsiasi sistema che possa agevolarli a nascondere la propria identità. Sotto questo punto di vista la blockchain ha dei lati positivi e dei lati negativi.
Da un lato, come già detto, il carattere pubblico della blockchain da la possibilità ad ogni utente di osservare in tempo reale tutte le transazioni effettuate. Quindi in linea teorica questo permetterebbe un controllo su larga scala delle transazioni che sono già autentificate e accertate dal sistema stesso. Per di più accedendo nelle specifiche di un singolo indirizzo si possono osservare tutte le sue transazioni creando una sorta di filo d'Arianna del denaro.

[113] European Banking Authority. EBA Opinion on "virtual currencies". Luglio 2014, pag. 22.
[114] Mancini Marco. Valute virtuali e Bitcoin. Cit. pag.120.

Figura 12: i blocchi di transazioni minati in ordine cronologico.



Height	Timestamp	Transactions	Mined by	Size
556815	Jan 3, 2019 11:01:10 AM	2844	SlushPool	894046
556814	Jan 3, 2019 10:33:47 AM	731		342332
556813	Jan 3, 2019 10:30:37 AM	41		9693
556812	Jan 3, 2019 10:30:21 AM	571		297343
556811	Jan 3, 2019 10:27:42 AM	223		66998
556810	Jan 3, 2019 10:26:35 AM	1904		782216
556809	Jan 3, 2019 10:18:57 AM	1050		954314
556808	Jan 3, 2019 10:17:04 AM	2310		954285
556807	Jan 3, 2019 10:07:20 AM	2027		943089
556806	Jan 3, 2019 10:02:10 AM	2640		943583
556805	Jan 3, 2019 9:50:05 AM	2427		953920
556804	Jan 3, 2019 9:45:25 AM	2629		911789
556803	Jan 3, 2019 9:28:41 AM	1	AntMiner	298
556802	Jan 3, 2019 9:21:06 AM	2346	SlushPool	904560
556801	Jan 3, 2019 8:55:07 AM	1403		923313
556800	Jan 3, 2019 8:50:21 AM	2786		957816

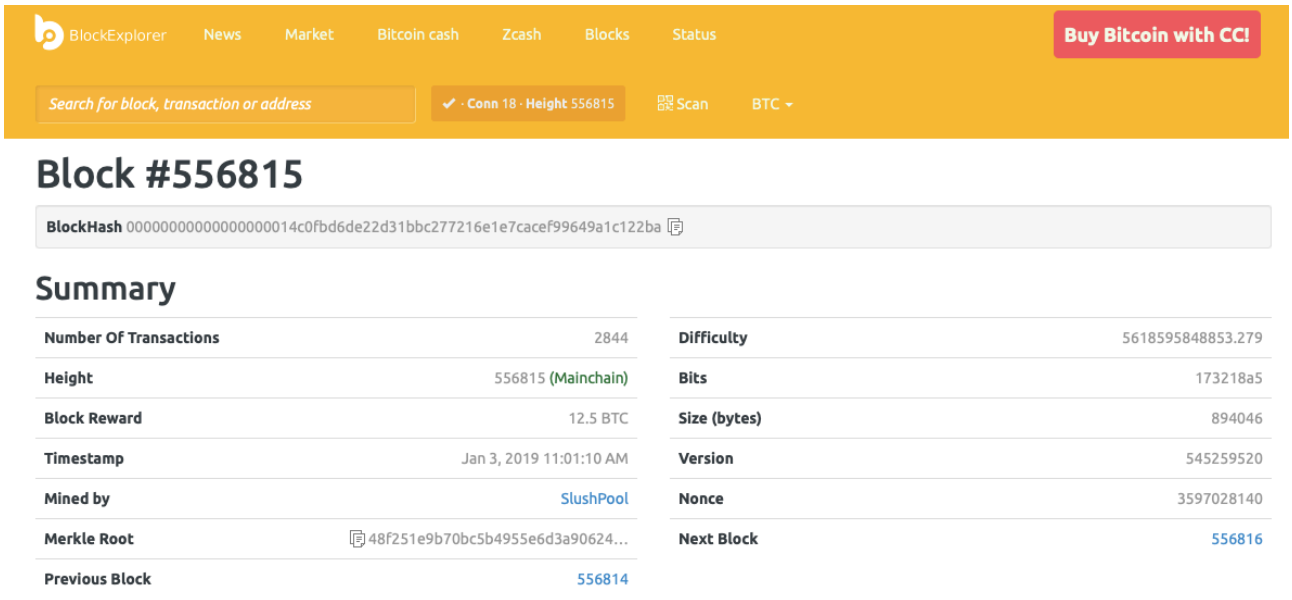
Fonte: blockexplorer.com

Tutto ciò si può fare in modo estremamente semplice anche da computer di casa accedendo al sito www.blockexplorer.com. Una volta effettuato l'accesso si possono osservare, come mostrato nell'immagine soprastante, i vari blocchi che sono stati confermati dai miner nel tempo.

Accedendo ad un singolo blocco, come mostrato nell'immagine seguente, troviamo le specifiche dello stesso con tutte le transazioni effettuate, con dettagli sulle quantità di bitcoin scambiati ed i vari indirizzi coinvolti[115].

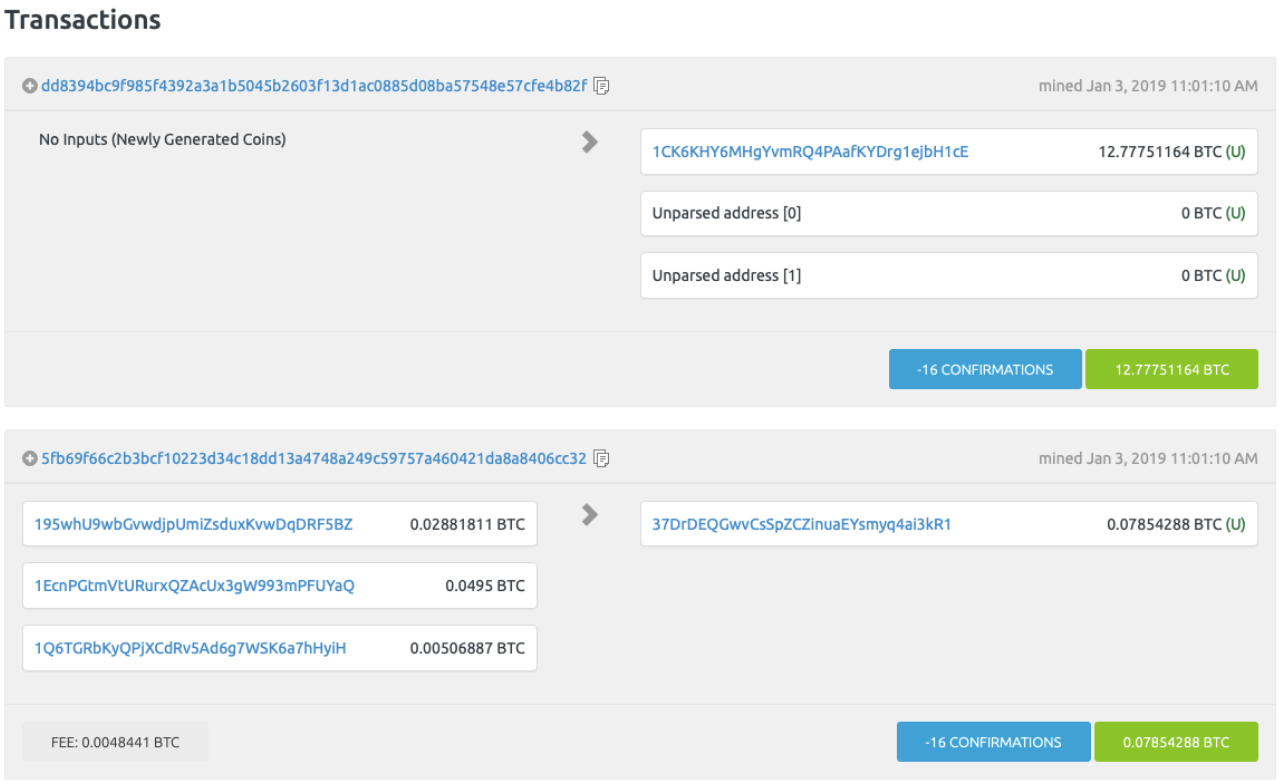
[115] Blocchi di transazioni sulla rete Bitcoin del 3gennaio 2019. Osservabili su blockexplorer.com

Figura 13: le specifiche di un blocco presente sulla blockchain



Fonte: blockexplorer.com

Figura 14: due tipologie di transazioni del blocco.



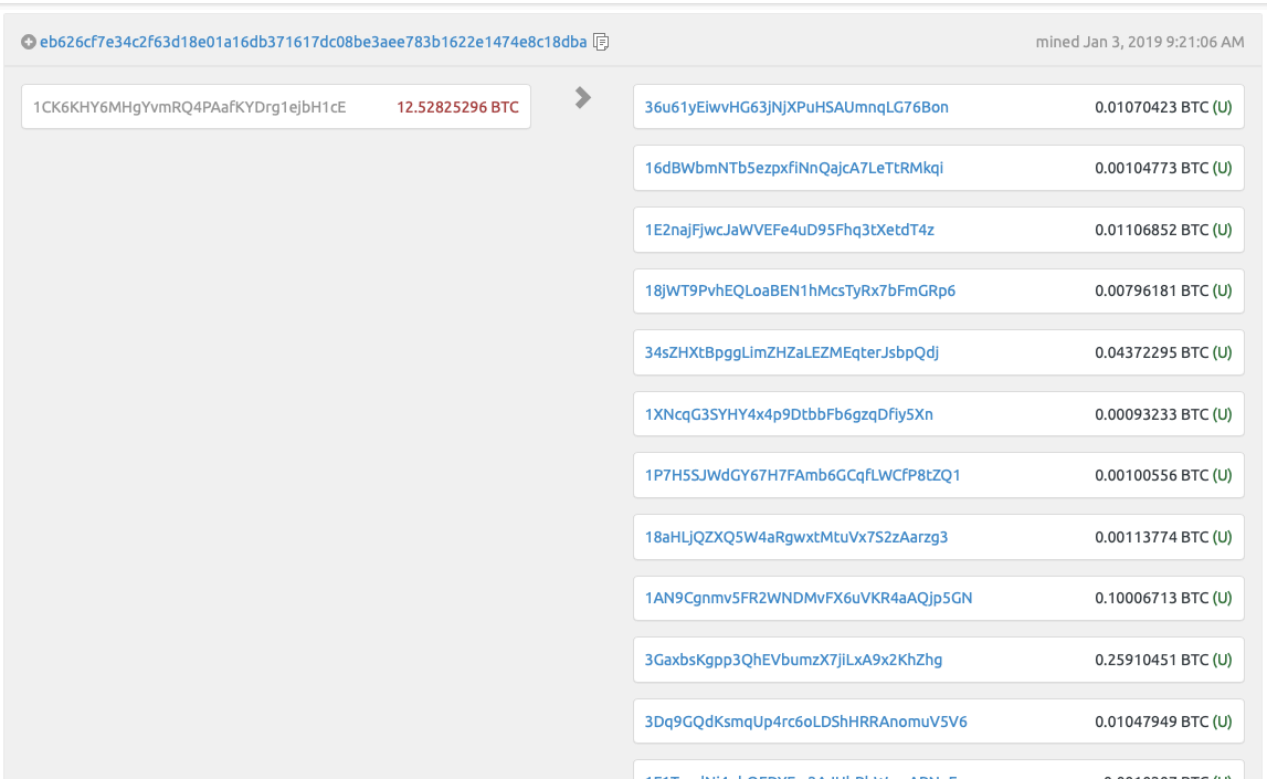
Fonte: blockexplorer.com.

Nell'esempio precedente possiamo osservare due tipologie di transazioni. La prima viene effettuata con dei bitcoin che sono stati minati e sono contraddistinti dalla dicitura "*No Imputs (Newely Generated Coins)".* Nella seconda, invece, il mittente utilizza dei bitcoin che gli sono stati inviati in precedenza. In questo caso le specifiche mostrano gli indirizzi che hanno inviato precedentemente i bitcoin per la transazione.

La blockchain è molto trasparente in termine di cronologia delle transazioni, ma non lo è sull'identità di chi è coinvolto nelle transazioni e qui veniamo ai lati negativi del sistema.

Infatti, dietro questi indirizzi, identificabili solamente tramite questi codici, si potrebbe celare qualunque persona, la quale potrebbe operare da qualsiasi parte del mondo inviando moneta virtuale con estrema facilità ed in modo pressoché istantaneo. Per di più accedendo casualmente all'indirizzo della prima transazione e osservando la sua cronologia possiamo constatare come la somma ricevuta è stata frazionata in piccole parti e viene, in seguito, girata a più di 260 indirizzi. Il tutto in una sola transazione. Nell'immagine sottostante sono presenti solo alcuni degli indirizzi coinvolti nella transazione, ma si può osservare come questi ricevano piccole frazioni di bitcoin[116].

Figura 15: alcuni dei 260 indirizzi coinvolti in una singola transazione.



Fonte: https://blockexplorer.com.

[116] Transazioni sulla rete Bitcoin del 3 gennaio 2019. Osservabili su blockexplorer.com

Se pensiamo che ciascuno di questi indirizzi può eseguire in pochi secondi transazioni simili coinvolgendo altrettanti account di ogni parte del globo possiamo avere una idea dell'incredibile ramificazione di transazioni che si può facilmente creare qualora qualcuno volesse nascondere una somma di denaro virtuale.

Inoltre, è possibile creare potenzialmente infiniti indirizzi Bitcoin senza dover dare nessun identificativo ed in modo totalmente gratuito. Quindi, non si può sapere quanti indirizzi fanno capo ad una singola persona. In questo modo, invece di inviare i soldi con una singola cospicua transazione o con più transazioni ma da un singolo indirizzo, il riciclatore potrebbe creare numerosi indirizzi con diversi identificativi a cui inviare piccole somme di denaro. Cosi facendo le transazioni non salterebbero all'occhio e non desterebbero sospetti nelle autorità[117].

In riferimento a ciò, c'è da approfondire anche un'altra tematica. Abbiamo detto in precedenza che il sistema Bitcoin è decentralizzato e che è stato creato proprio in ottica di sottrarlo alla gestione e al controllo di un'istituzione finanziaria; in quanto è il sistema stesso, attraverso i suoi protocolli, gestisce e autentica tutte le transazioni. Chiaramente questo aspetto è un intralcio per le autorità che hanno il compito di controllare l'eventuale presenza di transazioni a copertura di operazioni illecite. Infatti, come è noto, gli interventi di contrasto alle movimentazioni illegali dei flussi di denaro si sviluppano solitamente tramite indagini della polizia giudiziaria che approfondisce principalmente le segnalazioni di operazioni sospette effettuate tramite le banche o tramite altri intermediari finanziari. L'assenza di un gestore centralizzato nel mondo delle valute virtuali, che seguendo i principi del *Know Your Costumer* e del *Risk Based Approach* segnali le operazioni sospette, priva le autorità di un interlocutore affidabile[118].

Inoltre, i servizi di valute virtuali, come gli exchange che si occupano di cambiare valuta virtuale con valute legali ed i wallet provider, ovvero quegli ambienti criptati dove è possibile inserire, spedire e ritirare le criptovalute, si basano su complesse infrastrutture che coinvolgono diverse entità, spesso locate in molteplici parti del mondo. Questa molteplicità dei servizi comporta che possa non essere chiaro a chi competono le responsabilità di contrasto al riciclaggio e lotta al finanziamento del terrorismo[119]. Ovvero, i record dei clienti e delle transazioni potrebbero essere detenuti da diverse entità appartenenti a diverse giurisdizioni rendendo difficile per le autorità potervi accedere.

Le caratteristiche intrinseche del sistema Bitcoin, che abbiamo analizzato, seppur agevolando il mantenimento dell'anonimato non sono sufficienti a nascondere completamente le tracce degli utenti, in quanto bisogna ricordare che il sistema è stato architettato con finalità diverse da quelle che poi hanno portato a favorire le attività criminali.

---

[117] Accinni Giovanni Paolo. Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017). In Archivio Penale, 2018, pag. 6.

[118] Accinni Giovanni Paolo. Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017). Cit. pag. 13.

[119] FATF Report. Virtual Currencies: Key Definitions and Potential AML/CFT Risk. June 2014, pag. 9.

Infatti, nonostante le informazioni presenti sulla blockchain non rappresentino affatto una "minaccia" diretta all'anonimato degli utenti, queste però potrebbero essere associate con informazioni addizionali per creare un collegamento con le identità reali degli stessi.[120]
Le informazioni che vengono ricercate ed utilizzate dalle autorità per rintracciare i soggetti sono divise in quattro tipologie e sono le seguenti:

- dati personali: quelle informazioni che collegano un account on-line con un'identità reale. Questi dati sono solitamente estrapolati dai vari account utilizzati sul web ed includono informazioni come il nome, l'indirizzo e-mail, codice fiscale e luogo e data di nascita;
- dati comportamentali: queste informazioni riguardano schemi comportamentali che vengono osservati durante la navigazione online e confrontati con quelli degli altri utenti al fine di individuare comportamenti anomali;
- dati finanziari: ovvero le informazioni estrapolabili da transazioni eseguite online come numeri di conti, ammontare e tempistica delle transazioni ed indirizzi bitcoin.
- dati di rete: queste informazioni includono indirizzi IP, configurazioni del browser e cookies[121].

I malintenzionati per evitare di diffondere queste informazioni e quindi risultare completamente irrintracciabili debbono prendere delle precauzioni ed adottare determinati schemi di comportamento.
Oltre alla modalità ed il metodo di pagamento con cui si acquistano i bitcoin, argomento che tratteremo in modo specifico nel capitolo successivo, risulta fondamentale utilizzare dei servizi di mixing per aumentare l'anonimato delle transazioni.
Il mixing è un servizio che consente agli utenti di oscurare la cronologia delle transazioni aggregando un certo numero di trasferimenti e nascondendo l'origine e la destinazione di ogni singolo pagamento, in modo tale da non consentire il collegamento tra il vecchio indirizzo del cliente, che ha spedito la valuta virtuale da mixare, e quello nuovo che la riceve mixata.
In poche parole, il mixing permette di escludere l'associazione tra valuta virtuale in entrata e quella in uscita, di fatto "ripulendola"[122].
I Servizi di mixing applicano fondamentalmente due tecniche per ottenere i risultati desiderati.
La prima tecnica è quella di inviare i soldi depositati a più conti, che a loro volta li invieranno ad altri conti. Questa metodologia ha lo scopo di rendere la rete di scambi di valuta virtuale più grande e

[120] [121] Novetta. Survey of Bitcoin Mixing Services: Tracing Anonymous Bitcoins. Reperibile su novetta.com, 2015, pag. 2.
[122] Bignazzi Sarah. Caratteristiche dell'operatività in criptovalute e connessi profili penali. Atti del seminario di alto aggiornamento ABI Antiriciclaggio 2018: novità, impatti e prospettive, 11 e 12 Luglio 2018.

confusa. Gli indirizzi utilizzati in questa pratica sono denominati "conti di rimbalzo" o "conti *bounce*".

La seconda tecnica consiste nel raggruppare il denaro virtuale di più utenti che si sono rivolti al servizio di mixing in un unico indirizzo, chiamato "conto *pool*", ed in seguito inviare i fondi a più indirizzi.

Tipicamente i servizi di mixing si servono di numerosi conti, ciascuno con una diversa finalità.

Oltre ai conti *bounce* e *pool* ci sono anche:

- i conti d'ingresso, chiamati *gateaway*, dove gli utenti inviano i fondi che intendono mixare;
- i conti di uscita, chiamati *withdrawing*, da cui gli utenti ricevono il denaro una volta mixato[123].

Affinché l'anonimato venga garantito, il mixer non deve registrare né rivelare la connessione tra gli indirizzi di input e di output[124].

La tabella seguente illustra i più comuni servizi di mixing reperibili on line e le loro rispettive caratteristiche.

Tabella 1: i principali siti di mixing e le loro caratteristiche.

Servizio di mixing	***Trasferimento minimo***	***Trasferimento massimo***	***Costo***	***Tempistica***	***Account richiesto?***
Bestmixer	0.001 BTC	Nessun limite	1-5% + 0,001 per indirizzo	Da 0 a 72 ore	No
Bit Launder	Nessun limite	Nessun limite	2% -3% (per un servizio più sicuro)	Fino a 24 ore	user name, password ed e-mail
Shared Coin	0.01 BTC	50 BTC	0.0005 BTC	Da 30 sec a 5 min	user name, password ed e-mail
Bitcoin Blender	0.01BTC	Nessun limite	1-3%	Da 0 a 99 ore	user name e password

Fonte: Novetta. Survey of Bitcoin Mixing Services: Tracing Anonymous Bitcoins.

[123] Calzone Ottavio. Servizi di mixing e Monero. In www.sicurezzanazionale.gov.it, luglio 2017, pag. 5.
[124] Familiari Sabrina. Criptovalute: i sistemi di mixaggio per il riciclaggio di denaro. Centro Ricerca sulla Sicurezza ed il Terrorismo (C.R.S.T), marzo 2018. In crstitaly.org. pag. 2.

È opportuno specificare che l'attività di mixing delle valute virtuali è legale, mentre potrebbe essere illegale la provenienza dei fondi.

Nonostante la loro apparente legalità questo tipo di siti hanno un'alta frequenza di chiusura. L'esempio più lampante è quello di Bitmixer, che era il servizio di mixing più conosciuto ed utilizzato e veniva ritenuto dagli utenti come il più affidabile[125].

Il servizio chiuse improvvisamente nel 2017 quando il gestore del sito scrisse un post sul forum bitcointalk.org[126] dove spiegava le motivazioni della chiusura. Bitcointalk.org, per inciso, è il principale forum a livello globale di bitcoin e valute virtuali, che venne fondato proprio da Satoshi Nakamoto, lo pseudonimo che creò Bitcoin. Nel post in questione il gestore di Bitmixer spiegava di essersi pentito della sua attività di mixing di valute virtuali che probabilmente coinvolgeva a sua insaputa anche proventi di attività illecite. Inoltre, lo stesso gestore rispondendo ad un commento al suo post ha scritto: "*Per quanto riguarda il motto "Non sono un criminale, perché dovrei ripulire i miei bitcoin?", ci credevo davvero alcuni anni fa. Ma guardate, nel 2016 abbiamo ripulito circa un milione di bitcoin: quanti di questi pensiate possano essere proventi di attività non criminale? Non lo so, abbiamo semplicemente fornito uno strumento senza chiedere da dove venissero i bitcoin. Ma non penso che tutti i bitcoin fossero puliti[127]".* Chiaramente non si può sapere se, come è probabile, dietro questa scelta ci siano motivazioni diverse rispetto a quelle fornite.

Per concludere, al fine di risultare irrintracciabili oltre all'utilizzo dei servizi di mixing, che non sono infallibili, ed evitare che i propri dati personali, finanziari, comportamentali e di rete vengano raccolti ed associati è necessario:

- considerare che tutte le operazioni effettuate da uno stesso portafoglio sono collegabili e di conseguenza non comprare mai articoli anonimi e articoli personali dallo stesso portafoglio;
- utilizzare sempre una tipologia di browser particolare che permette di rendere ignoto al venditore il proprio indirizzo IP[128]. In particolare, il più utilizzato è TOR (The Onion Router) di cui parleremo in modo specifico nel capitolo successivo. In questo modo sarà possibile nascondere tutti i dati di rete menzionati in precedenza;
- utilizzare almeno due servizi di mixing di seguito per rendere anonimi i propri bitcoin.
  Lo schema da utilizzare è: procurarsi i bitcoin tramite uno dei vari siti disponibili, per esempio LocalBitcoins.com; utilizzare prima il servizio di mixing A ed in seguito il servizio di mixing B; solo dopo aver svolto questi passaggi inviare i bitcoin al portafoglio anonimo.

[125] Del Checco Paolo. Birmixer, il più grande mixer di Bitcoin, si pente e chiude in battenti. In bitcoinforensics.it, luglio 2017.
[126] bitcointalk.org
[127] Cfr. bitcointalk.org
[128] L'indirizzo IP è un codice numerico che identifica e localizza ogni computer connesso ad una rete.

In questo caso le transazioni rimarranno private anche nel caso in cui uno dei servizi di mixing sia stato compromesso;

- utilizzare conti differenti per ogni operazione di mixing, nel caso in cui il servizio di mixing richieda la registrazione dell'utente. In questo modo non sarà possibile per il servizio enumerare i portafogli del cliente;
- utilizzare esclusivamente canali di comunicazione crittografati sia per contattare il servizio di mixing sia per qualsiasi altra comunicazione. Nello specifico le e-mail non criptate sono facilmente intercettabili.
  Ad esempio, un canale di comunicazione sicuro è Bitmessage in quanto è criptato, anonimo, decentralizzato e non censurabile[129].

Questa enunciazione aiuta a capire come effettivamente coloro che seguono i passi sopracitati vanno ad assumere la consapevolezza di potersi rendere irrintracciabili e di fatto questa è la prassi che viene più frequentemente utilizzata.
Va sottolineato che l'utilizzo di alcune piattaforme che forniscono servizi di valute virtuali possono essere esse stesse fonte di azioni criminali sotto forma di truffe o attacchi informatici nei quali i clienti hanno perso il loro capitale[130]. Ciò accade quando o i wallet dei clienti vengono hackerati o gli exchange chiudono la propria piattaforma improvvisamente facendo perdere ai clienti i fondi versati. Ricordiamo che i wallet sono i portafogli virtuali formati da un insieme di indirizzi e chiavi private che permettono di inviare e ricevere le criptovalute[131]. Questo tipo di truffe sono possibili perché esiste una tipologia di wallet, chiamati custodial, che vengono solitamente offerti dagli exchange stessi, i quali detengono sui propri server le chiavi private degli utenti. Nel mondo delle valute virtuali chi ha possesso delle chiavi private ha il sostanziale controllo dei fondi contenuti nel wallet.
Il principio, su cui si basano i custodial wallet, è simile a quello di una banca che detiene i soldi di un cliente. Il cliente non ha un controllo totale sui soldi che ha depositato, nonostante questi siano suoi. Esistono altre tipologie di wallet, non custodial, che forniscono all'utente il pieno controllo sulle sue chiavi private, e quindi sui suoi fondi.
I non custodial wallet si basano su:

- un software scaricabili direttamente sul pc o sullo smartphone. In questo caso è il dispositivo che detiene le chiavi private;

[129] Come utilizzare bitcoin in modo anonimo. In coinmixer.es.
[130] Banca d'Italia. Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee. Marzo 2018, pag.1.
[131] European Central Bank. Virtual currencies Schemes. Ottobre 2012, pag. 8.

- un hardware come un chip crittografato che memorizza le chiavi private. In questo caso è comunque necessario un software per scambiare le criptovalute.
- un foglio di carta che contiene sia la chiave privata che quella pubblica. Anche i questo caso è necessario l'utilizzo di un software[132].

È importante sottolineare che i non custodial wallet non effettuano procedure *Know Your Costumer* e che quindi sono quelli più adatti per chi desidera mantenere il proprio anonimato.

2.3 COME PROCURARSI LE VALUTE VIRTUALI IN MODO ANONIMO

Precedentemente abbiamo anticipato come il processo e la modalità di pagamento con cui si entra in possesso delle valute virtuali è una componente fondamentale se si desidera essere irrintracciabili.
Ad esempio, se un utente acquista dei bitcoin con una carta di credito personale tramite un exchange di criptovalute che segue le procedure identificative Know Your Costumer, egli sarà con grandi probabilità facilmente rintracciabile. In questo caso a nulla varrà l'anonimato che caratterizza la blockchain e di cui abbiamo parlato in precedenza. Infatti, le autorità potranno ripercorrere le transazioni dell'indirizzo in questione fino a quella effettuata con l'exchange (eseguita con carta di credito) grazie alla blockchain stessa. A questo punto le autorità potranno richiedere all'exchange i dati di pagamento utilizzati dall'utente e risalire fino alla sua reale identità.
In poche parole, il modo in cui si entra in possesso della valuta virtuale è il primo di una lunga fila di espedienti che bisogna seguire "correttamente" se si vuole preservare il proprio anonimato.
Esistono diversi modi per procurarsi delle criptovalute, che qui di seguito riepiloghiamo.
Il primo di questi è il mining, che come abbaiamo già trattato, consiste nell'attività di verifica e d'inserimento delle transazioni nella blockchain e prevede una ricompensa in criptovaluta per il miner.
Il secondo modo per procurarsi delle valute virtuali è tramite gli exchange. Questi sono delle piattaforme che operano come intermediari e che consentono la conversione di valuta fiat in criptovaluta e viceversa[133].
Inoltre, gli exchange rappresentano anche un tema di estrema attualità per ciò che concerne l'ambito legislativo internazionale. Infatti, negli ultimi anni la carenza di una disciplina adeguata che ne regolasse l'attività ha permesso una proliferazione di queste piattaforme spesso incontrollata.

[132] Bignazzi Sarah. Caratteristiche dell'operatività in criptovalute e connessi profili penali. Cit.
[133] Bignazzi Sarah. Caratteristiche dell'operatività in criptovalute e connessi profili penali. Cit.

Molte di queste piattaforme di scambio non eseguono degli adeguati controlli di identificazione della clientela. Infatti, in molti casi i clienti di queste piattaforme non sono tenuti a fornire delle credenziali identificative, mentre, nel caso queste siano richieste spesso non vengono verificate tramite la controprova di documenti identificativi.

Da quanto risulta da uno studio condotto recentemente dalla società di analisi P.A.ID Strategies sui 25 principali exchanger e wallet provider ubicati in Europa ed in Nord America, il 68% delle piattaforme analizzate non seguirebbero le procedure *Know Your Costumer,* permettendo agli utenti di operare semplicemente fornendo un indirizzo e-mail e un numero di telefono[134]. L'email ed il numero di telefono sono delle misure di verifica molto deboli. Infatti, chiunque desiderasse rimanere anonimo potrebbe rivolgersi ad uno di questi exchanger o wallet provider utilizzando una mail criptata e un telefono "usa e getta".

I wallet provider forniscono il software (wallet) che contiene le chiavi private e gli indirizzi e permette di inviare e ricevere le valute virtuali. Solitamente gli exchange, oltre a effettuare servizi di cambio, operano anche come wallet provider.

Come è possibile osservare dall'immagine seguente, solamente 8 piattaforme delle 25 analizzate conducono delle adeguate verifiche sull'identità dei loro clienti richiedendo dei documentid'identita; 6 di queste richiedono delle informazioni personali senza verificarne l'autenticità; ben 11 non richiedono neanche informazioni non verificate[135].

[134] P.A.ID Strategies. The Cryptocurrency Identity Crisis: An Industry Scorecard for Digital Id Verification for KYC and AML. In paidstrategies.com, giugno 2018.

[135] P.A.ID Strategies. The Cryptocurrency Identity Crisis: An Industry Scorecard for Digital Id Verification for KYC and AML. Cit.

Figura 16: Procedure identificative delle principali 25 piattaforme di servizi di valute virtuali dell'Europa e del Nord America.

Wallet/Exchange	Wallet/ Exchange	Requires Unverified Personal Information	Requires official ID docs to begin trading	ID Verification Score
Coinbase	E	✓	✓	9
Gemini	E	✓	✓	9
Poloniex	E		✓	9
itBit	E	✓	✓	9
Luno	W	✓	✓	8
Bonpay	W	✓	✓	8
Mercatox	W	✓		7
Kraken	E	✓	✓	7
Bitstamp	E	✓	✓	7
CoinCorner	W	✓		7
QuadrigaCX	E	✓		6
Cex.IO	E	✓		6
Blockchain Wallet	W			6
Wirex	W			6
Lykke Wallet	W	✓		6
Coinexchange	E			5
Exmo	E			5
Coinjar	W			5
Liqui	E			4
Local Bitcoins	E			4
YoBit.net	E			4
BitPanda	W			4
Bitwala	W			3
SpectroCoin	W			2
Indacoin	E	✓		2

Fonte: P.A.ID Strategies. The Cryptocurrency Identity Crisis: An Industry Scorecard for Digital Id Verification for KYC and AML.

Inoltre, va considerato che questo studio è stato condotto tenendo in considerazione piattaforme del Nord America e dell'Europa le cui giurisdizioni sono molto attive nel campo AML/TF.

Molti paesi, al di fuori di quelli presi in esame nell'analisi, hanno presidi antiriciclaggio estremamente deboli che agevolano il riciclaggio di denaro tramite criptovalute con lo stesso meccanismo che caratterizza i paradisi fiscali. Questi stati avendo delle legislazioni in materia poco stringenti e non essendo collaborativi con le autorità straniere favoriscono la nascita di exchange che non effettuano procedure identificative KYC. In questo modo riescono ad attirare i capitali dei riciclatori, la cui

necessità è chiaramente quella di poter cambiare criptovalute in valuta fiat e viceversa lasciando meno tracce possibili. Queste operazioni sono agevolate dalla grande facilità e rapidità con cui è possibile effettuare trasferimenti transfrontalieri tramite le valute virtuali.
Il riciclatore, una volta entrato in possesso di valuta virtuale in modo anonimo, potrebbe trasferirla liberamente e anonimamente in paesi privi di regolamentazioni antiriciclaggio, creando una fitta rete di trasferimenti e convertirla in valuta fiat da reimmettere nel sistema[136]. In alterativa i criminali potrebbero vendere beni e servizi illegali, come droghe e armi, in cambio di valuta virtuale per convertirla successivamente in valuta fiat da utilizzare per finanziare le proprie attività illecite[137].
Visti i grandi interessi economici sottostanti a dette operazioni, si sta verificando che alcuni stati europei, come la Svizzera e Malta, avendo intuito il grande potenziale economico delle valute virtuali stanno già creando dei regimi fiscali agevolati per chi effettua investimenti in questo tipo di moneta.
Il terzo metodo per procurarsi delle valute virtuali è scambiandola direttamente con altri soggetti senza l'utilizzo di piattaforme di intermediazione. Infatti, è possibile accordarsi privatamente con altre persone, incontrarsi ed effettuare lo scambio tramite delle applicazioni che permettono di inviare direttamente le valute virtuali al wallet dell'altro soggetto. Addirittura, lo scambio può essere effettuato anche in contanti garantendo l'anonimato delle controparti. Infatti, scambiando la moneta fisicamente si interrompe il filo d'Arianna che possono seguire gli investigatori e le forze dell'ordine. Questo tipo di accordi è possibile raggiungerli sia personalmente sia attraverso delle piattaforme d'incontro tra acquirenti e venditori che mettono d'accordo chi vuole scambiare valute virtuali con contanti.

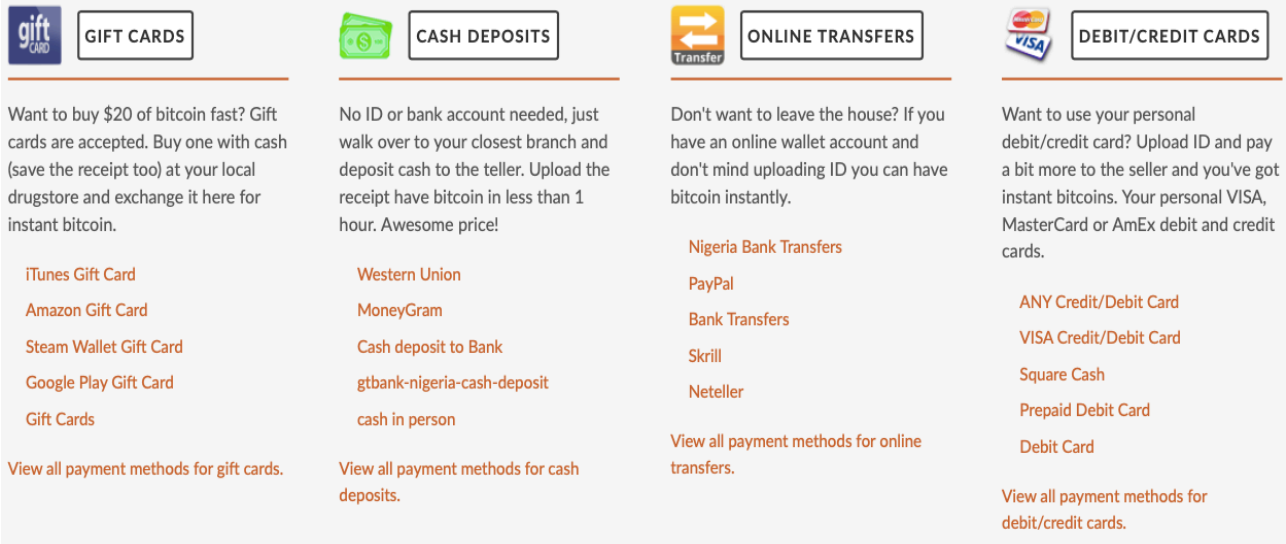
Esistono due tipologie di piattaforme:

- i *marketplace,* siti internet accessibili da chiunque;
- Siti web segreti che costituiscono il dark web e che sono accessibili solamente da determinati browser.

I *marketplace* più noti reperibili da un comune motore di ricerca come Google sono Localbitcoins e Paxful[138]. Accedendo al sito di Paxful possiamo constatare la grandissima molteplicità dei metodi di pagamento con cui è possibile acquistare bitcoin.

[136] Accinni Giovanni Paolo. Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017*)*. Cit. pag. 13.
[137] Carlisle David. Virtual Currencies and Financial Crime: Challenges and Opportunities. Cit. pag 15.
[138] localbitcoins.net e paxful.com.

Figura 17: Metodi di pagamento sulla piattaforma paxful



Fonte: paxful.com

Come si evince dall'immagine su questo tipo di piattaforme è possibile acquistare bitcoin con i metodi di pagamento più disparati. Ai fini della nostra analisi ci concentriamo sui metodi di pagamento in contanti, che sono quelli che permettono di mantenere di più l'anonimato.

Nella descrizione della colonna dedicata al metodo di pagamento in contanti si può specificatamente leggere come non venga richiesto nessun ID ne conto corrente. Infatti, per creare un account su questi siti è necessario fornire solamente un'e-mail e alcune volte un numero di telefono.

Una volta inseriti questi dati è possibile acquistare o vendere valute virtuali tramite un semplice annuncio[139].

Ad esempio, accedendo alla sezione *"cash in person"* è possibile consultare tutte le offerte per scambiare bitcoin con contanti. Selezionando una delle offerte ci si può in contatto con il venditore e accordarsi per un incontro durante il quale effettuare lo scambio.

[139] Familiari Sabrina. Criptovalute: i sistemi di mixaggio per il riciclaggio di denaro. Cit. pag. 2.

Figura 18: Offerte per comprare bitcoin con cash sulla piattaforma localbitcoins.

Buy bitcoins with cash near Rome, Italy

Seller	Distance	Location	Price/BTC	Limits
cryptobro (3000+; 99%)	1.1 km	Rome, Metropolitan City of Rome, Italy	3,303.31 EUR	At least 10000 EUR
Micio (70+; 100%)	1.1 km	Rome, Metropolitan City of Rome, Italy	3,477.10 EUR	At least 1000 EUR
superorrea2 (500+; 99%)	176.9 km	81031 Aversa, Province of Caserta, Italy	3,462.13 EUR	300 - 3,000 EUR
superorrea2 (500+; 99%)	188.8 km	80133 Naples, Metropolitan City of Naples, Italy	3,462.13 EUR	300 - 3,000 EUR
pino89 (3000+; 100%)	189.1 km	Naples, Italy	3,493.89 EUR	At least 100 EUR

Fonte: localbitcoins.net

Per di più accedendo ad una delle offerte presenti su Paxful possiamo notare come il potenziale venditore fornisca a chiunque desideri un modo di contattarlo al di fuori della piattaforma. Nello specifico il soggetto indica un sito personale, dove trovare la sua e-mail e i suoi contatti telefonici[140].

Offer terms by gavrilobtc Community tips

Questa offerta è valida solo e strettamente per la quantità in euro qui descritta (500-2999 euro) e per pagamenti di persona in Udine città o nel raggio max di 20 km. Non invio bitcoin senza aver prima verificato se avete il denaro in contanti e se le banconote sono autentiche. Per accordi di differenti quantità in bitcoin o appuntamenti fuori dalla zona descritta, contattatemi utilizzando i riferimenti del mio blog www.gavrilobtc.it. Per quantità inferiori ai 500€ potete utilizzare il BTM (Bitcoin Teller Machine - bancomat) di viale Palmanova 420 a Udine.

Gli esempi presentati fanno riferimento a dei siti molto noti che sono accessibili tramite qualsiasi motore di ricerca e che quindi sono consultabili da chiunque.

Esiste, tuttavia, un mondo segreto di siti a cui è possibile accedere solamente tramite dei motori di ricerca particolari che non permettono il tracciamento dell'indirizzo IP. Stiamo parlando dei siti che

[140] Offerta dell'utente gavrilobtc sulla piattaforma Paxful.com

costituiscono il dark web, ovvero la parte nascosa del web, che in seguito tratteremo in maniera molto approfondita.
Tra questi siti nel dark web, tra le altre cose, è possibile trovare molti annunci per la compravendita di valute virtuali. Chiaramente questo tipo di compravendite, che potremo definire "nell'ombra", essendo accessibili a pochi e basandosi su sistemi che evitano il tracciamento, sono le migliori per mantenere l'anonimato. Sono questi i processi che, spesso, vengono utilizzate dai criminali specializzati per procurarsi valute virtuali in maniera anonima.
Questo mondo sommerso di scambi illegali è estremamente vasto, difficile da monitorare quindi fonte di copertura per le azioni criminali.
Un servizio televisivo di Striscia la Notizia del novembre 2018 ci mostra come sia possibile, per chi è esperto della materia, connettersi al dark web ed instaurare una compravendita di bitcoin al di fuori dei canali ufficiali[141]. L'inviato, dopo aver mostrato una molteplicità di siti dove poter acquistare beni illegali come armi, droghe o dove è addirittura possibile assoldare dei sicari, si connette ad un sito di scambio di valute virtuali. In seguito, instaura una compravendita con un soggetto accordandosi per effettuare lo scambio incontrandosi in un parco di Londra. L'accordo prevedeva una transazione bitcoin, effettuata tramite wallet "non custodial" gestibili da uno smartphone, a fronte di un pagamento in contanti. Dopo aver fatto fallire la transazione all'ultimo secondo grazie ad una scusa, l'inviato ci spiega come questo tipo di transazioni sia all'ordine del giorno.
Per concludere, l'ultimo modo per procurarsi le valute virtuali è tramite degli ATM dedicati[142].
Questi funzionano come dei veri e propri ATM tramite i quali è possibile comprare valute virtuali.
Fornendo l'indirizzo del proprio wallet è possibile sia comprare delle valute virtuali sia ritirare il denaro. Entrambe le operazioni vengono svolte esclusivamente in contanti.
Il tipo di identificazione necessaria per svolgere le operazioni varia a seconda dell'exchange a cui l'ATM appartiene e allo stato in cui si trova. Alcuni di questi richiedono di scannerizzare il passaporto o di prendere l'impronta digitale, altri, invece, richiedono semplicemente l'indirizzo del wallet con il quale si vuole effettuare la transazione[143]. Come si può osservare accedendo al link inserito nelle note, questo tipo di ATM sono diffusi in tutto il mondo, compresi paesi dove le legislazioni AML/CTF sono carenti. Si può facilmente immaginare che gli Atm in questi stati abbiano procedure identificative altrettanto deboli.

[141] Il servizio è consultabile presso: www.mediasetplay.mediaset.it.
[142] La mappa degli Atm è consultabile presso: coinatmradar.com/bitcoin-atm-map
[143] Come acquistare agli ATM Bitcoin in Italia? Ecco la guida completa. In coinlist.me.

2.4 METODI DI RICICLAGGIO CON VALUTE VIRTUALI ALTERNATIVE

Fin ora abbiamo trattato in modo dettagliato solamente i bitcoin, in quanto è la moneta virtuale più conosciuta, diffusa e con una capitalizzazione maggiore. Esistono, però, moltissime altre criptovalute alcune con caratteristiche simili ai bitcoin altre, invece, si differenziano dal punto di vista delle procedure tecniche o contemplano finalità differenti rispetto al puro trasferimento di denaro.
Come possiamo osservare dalla tabella riassuntiva le principali valute alternative ai bitcoin sono Ethereum, Ripple, IOTA, Litecoin, Bitcoin Cash e Monero.

Tabella 2: Le principali valute alternative al bitcoin.

Criptovaluta	Market cap	Anno di creazione	Algoritmo	Numero max di monete	Mining – Decentrato	Particolarità
Ripple (XRP)	$13,6 MLD	2012	RPCA	100 MLD	No Si	Rete di transazioni per il settore bancario
Ethereum (ETH)	$12,9 MLD	2013	Ethash	100 MLN	Si Si	Blockchain utilizzabile con altri scopi[144]
Bitcoin Cash (BCH)	$2,3 MLD	2017	SHA-256	2,78 MLN	Si Si	Velocita di transazione più alta
IOTA (MIOTA)	$856 MLN	2016	Tangle	100 MLD	No No	Ottimizzato per l'Internet of Things[145]

[144] Nello specifico: smart contracts e crowfunding. Gli smart contract sono la trasposizione in codice di un contratto che si autoesegue automaticamente nel momento in cui vengono soddisfatte determinate condizioni
[145] Utilizzo della rete per il funzionamento di smart objects.

Litecoin (LCT)	$1,9 MLD	2011	Scrypt	84 MLN	Si Si	Migliore distribuzione per il mining
Monero (XMR)	$757 MLN	2014	Cryptonight		Si Si	Alto grado di anonimato

Fonte: www.ionos.it

Bisogna specificare che nonostante la varietà delle monete virtuali in circolazione il bitcoin resta di gran lunga la criptomoneta più importante. Un dato significativo in tal senso è la capitalizzazione di mercato; quella di bitcoin è di ben $64 MLD[146].

Ai fini della nostra analisi ci soffermeremo solamente su una di queste; Monero, una moneta virtuale lanciata nel 2014 per garantire maggiore privacy[147].

Infatti, Monero ha delle caratteristiche particolari che la rendono estremamente rilevante dal punto di vista del riciclaggio di denaro e del potenziale utilizzo che i criminali ne possono fare sul dark web.

La caratteristica principale in tal senso è il fatto che la blockchain di Monero non è trasparente, in quanto le transazioni sono visibili solamente a chi ha accesso alla chiave privata, e dunque solamente a chi compie la transazione stessa[148].

Nello specifico, Monero si basa su un protocollo di funzionamento, chiamato CryptoNote, che prevede la creazione automatica di una nuova coppia di chiavi "usa e getta" per ogni operazione. Ricordiamo, invece, che Bitcoin prevede un'unica chiave privata associata alla rispettiva chiave pubblica, da cui si genera l'indirizzo. Cosi facendo Monero si assicura che nessuna unità monetaria possa essere collegata ad un'altra transazione, poiché è come se gli indirizzi, con cui si inviano e si ricevono i monero, cambiassero ad ogni transazione.

Inoltre, le informazioni relative alle transazioni, come ad esempio gli importi scambiati, sono visibili solamente alle parti coinvolte.

Per di più Monero prevede un sistema di mixing automatico per ogni transazione[149].

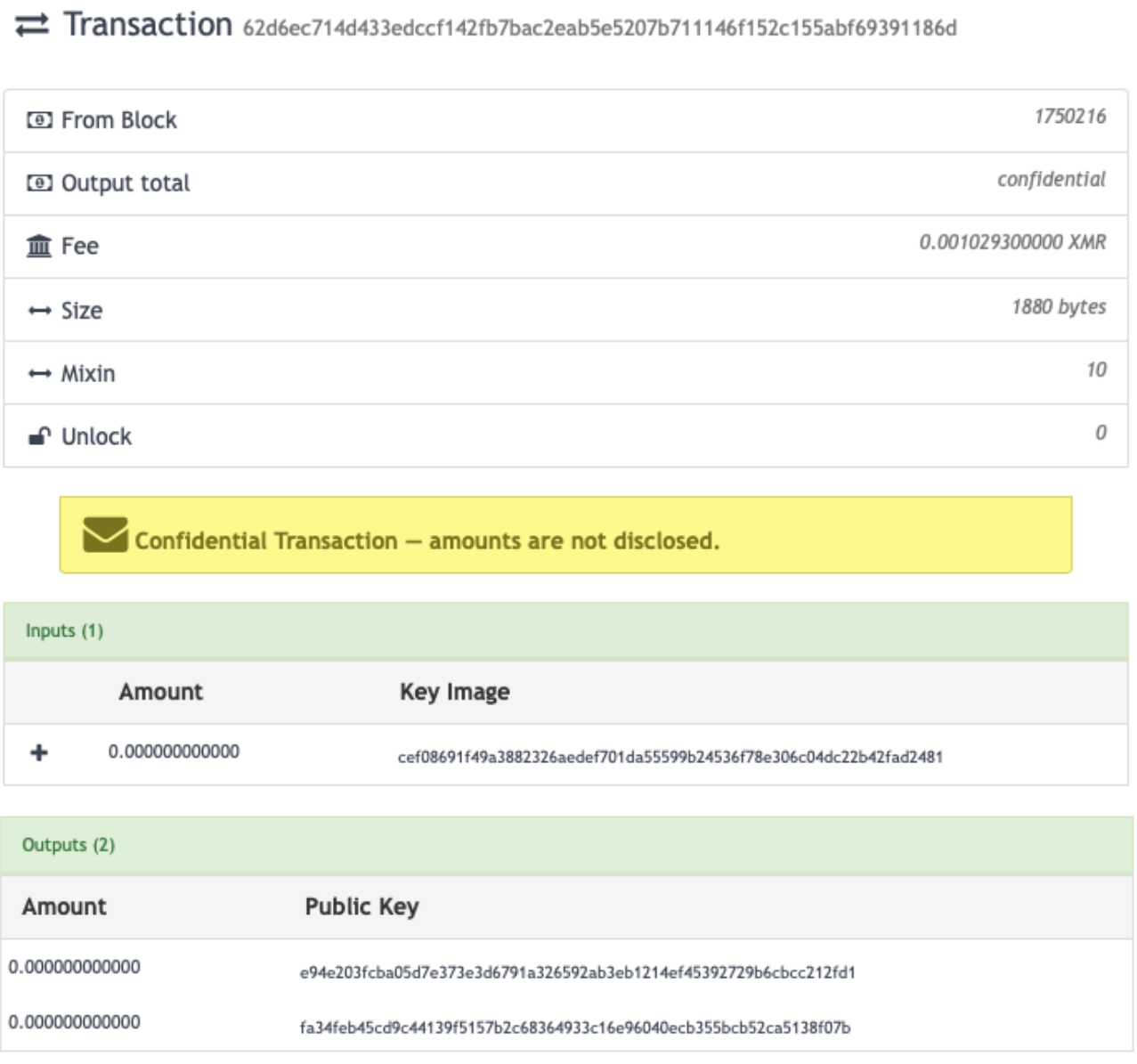
Questo è basato sul meccanismo delle *"Ring Signatures"*, il quale prevede che le transazioni siano firmate non solo dal relativo mittente, ma da un gruppo intero di soggetti. Ricordiamo che la firma

[146] Dati di coinmarketcap.com a gennaio 2019.
[147] Familiari Sabrina. Criptovalute: i sistemi di mixaggio per il riciclaggio di denaro. Cit. pag. 4.
[148] Pearson Jordan. Meet Monero, the Currency Dark Net Dealers Hope is More Anonymous than Bitcoin. In www.motherboard.vice.com. 23 agosto 2016.
[149] Accinni Giovanni Paolo. Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017). Cit. pag. 8.

ha lo scopo di autenticare la transazione. In questo modo non sarà possibile capire chi del gruppo di firmatari è l'effettivo mittente del denaro.

Accedendo alla blockchain di Monero, consultabile tramite il sito moneroblocks.info, possiamo notare, come a differenza delle transazioni Bitcoin mostrate in precedenza, non è possibile né quantificare l'importo delle transazioni effettuate né identificare gli indirizzi coinvolti, in quanto quelli indicati sono "usa e getta"[150].

Figura 19: Transazione anonima su Monero.



Fonte: moneroblocks.info

[150] Transazioni sul sistema Monero. Osservabile su moneroblock.info

Inoltre, da quando Alphabay, uno dei principali siti illegali del dark web, oggi chiuso dalle autorità, nel settembre 2016 annunciò che da quel momento avrebbe accettato pagamenti in Monero, essa può essere utilizzata sul web per scambi illegali di qualsiasi tipo[151].

Per concludere Monero risulta una moneta virtuale effettivamente anonima, quindi si presta ancora di più a potenziali usi criminali.

Infatti, la strategia di un riciclatore potrebbe essere quella di convertire i proventi rivenienti da attività illecite in monero, con quest'ultimi effettuare dei trasferimenti anonime ed infine riconvertire i monero in valuta fiat avendo di fatto ripulito i capitali[152].

[151] Carlisle David. Virtual Currencies and Financial Crime: Challenges and Opportunities. Cit., Pag. 16.

[152] Accinni Giovanni Paolo. Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017). Cit. pag. 13.

CAPITOLO III

LA V DIRETTIVA ANTIRICICLAGGIO E GLI STRUMENTI DI CONTRASTO

3.1 PRINCIPALI NOVITA' RIGUARDANTI LE VALUTE VIRTUALI

Il 30 maggio 2018 è stata adottata la Quinta Direttiva antiriciclaggio UE 2018/843 del Parlamento Europeo e del Consiglio[153], che modifica la precedente Quarta Direttiva.

Analizziamo quali sono state le novità introdotte dalla nuova disciplina, focalizzandoci in *primis* sull'argomento trattato in questa tesi.

Come si evince dalle considerazioni iniziali del testo della Direttiva il legislatore europeo è ben conscio della problematica inerente alle valute virtuali. Tant'è che reputa possibile che, in assenza dell'obbligo per i servizi di valute virtuali di individuare le attività sospette, "*i gruppi terroristici possano essere in grado di trasferire denaro verso il sistema finanziario dell'Unione o all'interno delle reti delle valute virtuali dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su queste piattaforme".* Inoltre, valuta che sia "*di fondamentale importanza ampliare l'ambito di applicazione della direttiva (UE) 2015/849 in modo da includere i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute legali e i prestatori di servizi di portafoglio digitale".* Infine, aggiunge che *"ai fini dell'antiriciclaggio e del contrasto del finanziamento del terrorismo (AML/CFT), le autorità competenti dovrebbero essere in grado di monitorare, attraverso i soggetti obbligati, l'uso delle valute virtuali[154]".*

Basandosi sulle precedenti considerazioni la portata della Direttiva antiriciclaggio viene estesa includendo:

- i prestatori di servizi di cambio valute virtuali e valute aventi corso forzoso, ovvero gli exchange;
- i prestatori di servizi di portafoglio digitale;

Cosi facendo gli exchange e i wallet provider dovranno applicare, come già succede per le banche, i controlli di *due diligence* e i requisiti di adeguata verifica sulla propria clientela.

[153] Pubblicata in G.U.C.E. L. il 19 giugno 2018.
[154] Cfr. Direttiva (UE9 2018/843. Considerando N°8.

Inoltre, questi prestatori di servizi dovranno essere registrati, cosi come avviene già per i cambiavalute, gli uffici di incasso degli assegni e i fornitori di servizi per aziende e società fiduciarie. In questo modo si cerca di porre fine al regime di anonimato associato alle valute virtuali[155].
Ci si interroga se queste misure siano sufficienti o meno; lasceremo alle conclusioni della trattazione le valutazioni del caso.
Inoltre, viene abbassata la soglia di utilizzo delle carte prepagate anonime, oltre la quale i soggetti obbligati sono autorizzati a non applicare le misure di adeguata verifica della clientela. L'importo massimo che è possibile memorizzare passa da €250 a €150.
Questa misura è estremamente importante, in quanto le carte prepagate anonime sono considerate uno dei principali strumenti utilizzati nell'ambito del finanziamento del terrorismo[156].
Queste, infatti, possono essere caricate con denaro contante e trasportate agevolmente oltre confine, senza la necessità di dichiarare tale spostamento o che, ad esse, sia associato un determinato nominativo. In seguito, il denaro può essere ritirato dagli ATM del paese di destinazione, bypassando, di fatto, i controlli relativi all'uscita/entrata del denaro.
A dimostrazione di ciò dalle indagini in seguito agli attentati di Parigi del 13 novembre 2015 è emerso che i terroristi hanno utilizzato carte prepagate, acquistate in Belgio, per noleggiare la stanza d'albergo e l'auto utilizzata per gli spostamenti[157].
Per di più le carte prepagate sono uno strumento molto utilizzato anche negli scambi di criptovalute con valute fiat. Come abbiamo visto in precedenza, sono uno degli strumenti accettati dagli exchange e nei siti in cui ci si può interfacciare con soggetti con i quali scambiare valute virtuali.

3.2 IMPLEMENTAZIONI ALLA PRECEDENTE NORMATIVA

In aggiunta a quanto detto precedentemente vengono aggiunti al novero dei soggetti obbligati anche:

- persone che commerciano opere d'arte o che agiscono in qualità di intermediari, anche quando tale attività è effettuata da gallerie d'arte o casa d'aste, qualora il valore dell'operazione o di una serie di operazioni interconnesse sia pari o superiore a €10.000[158].

[155] Pesci Daniela. Le implicazioni su rischi di antiriciclaggio. Atti del seminario di alto aggiornamento ABI Antiriciclaggio 2018: novità, impatti e prospettive, 11 e 12 Luglio 2018.
[156] Cfr. Direttiva (UE) 2018/843. Considerando N°14.
[157] Razzante Ranieri e Mugavero Roberto. Terrorismo e nuove tecnologie. Pisa: Pacini Editore, 2016, pag. 68.
[158] Cfr. Direttiva (UE9 2018/843. Art 2, comma d.

In ottica della lotta al finanziamento del terrorismo e con il fine di ampliare le fonti informative disponibili alle autorità competenti, la Direttiva ha rafforzato i poteri delle *Financial Intelligence Unit* (FIU) per ciò che concerne l'analisi domestica e la collaborazione internazionale[159]. Il legislatore ha disposto che le FIU possano essere in grado di richiedere, ottenere ed utilizzare informazioni da qualsiasi soggetto obbligato, anche nel caso in cui non sia stata trasmessa una segnalazione di operazione sospetta[160], senza limitazioni derivanti da norme o procedure nazionali.

Inoltre, con il fine di migliorare la collaborazione tra le FIU e le autorità di vigilanza antiriciclaggio, viene rafforzata la capacità di collaborazione internazionale limitando, nel contempo, la capacità di rifiuto di collaborare.

La collaborazione, infatti, non potrà essere negata adducendo come motivazione il collegamento con vicende fiscali, indagini o procedimenti penali[161].

Una delle modifiche di maggior rilievo riguarda le informazioni sulla titolarità effettiva delle società e di altri soggetti giuridici, nonché di trust ed istituti giuridici affini. Con il fine di migliorarne la trasparenza la Direttiva ha stabilito che le informazioni siano accessibili anche al pubblico e non solo, come in precedenza, alle autorità competenti e ai soggetti obbligati.

Il pubblico potrà avere accesso al nome, alla data di nascita, al paese di residenza, alla cittadinanza del titolare effettivo e alla natura e all'entità dell'interesse beneficiario detenuto[162].

La Direttiva, inoltre, prevede una maggiore correlazione tra i registri centrali degli stati membri per facilitarne l'accesso ai dati, disponendo la creazione di un sistema di interconnessione europeo tra tutti i registri nazionali dei titolari effettivi, delle società e dei trust[163].

Gli Stati, dunque, dovranno assicurarsi che le informazioni corrette ed aggiornate siano disponibili attraverso i rispettivi registri nazionali e tramite il sistema di interconnessione[164].

Vengono, inoltre, implementate le misure di adeguata verifica rafforzata per rapporti d'affari o operazioni che coinvolgono paesi terzi ad alto rischio.

In tal caso le misure che i soggetti obbligati devono applicare sono:

- *ottenere informazioni supplementari sul cliente e sul titolare effettivo;*
- *ottenere informazioni supplementari sullo scopo e sulla natura prevista del rapporto d'affari;*
- *ottenere informazioni sull'origine dei fondi e del patrimonio del cliente e del titolare effettivo;*

[159] De Vivo Annalisa e Trinchese Gabriella. Le Novità della V Direttiva Antiriciclaggio. Fondazione nazionale dei Commercialisti. Consultabile in www.fondazionenazionalecommercialisti.it, settembre 2018, pag. 5.
[160] Cfr. Direttiva (UE9 2018/843. Art. 1, comma 18.
[161] UIF. Quaderni dell'antiriciclaggio dell'Unità di Informazione Finanziaria. Settembre 2018, pag. 60.
[162] Cfr. Direttiva (UE9 2018/843. Art. 1, comma 15 c.
[163] Di Carlo Francesco. Un nuovo regime per l'applicazione di misure semplificate e rafforzate di adeguata verifica: dalle novità regolamentari all'analisi di alcuni casi concreti. CIt.
[164] De Vivo Annalisa e Trinchese Gabriella. Le Novità della V Direttiva Antiriciclaggio. Cit. pag. 12.

- *ottenere informazioni sulle motivazioni delle operazioni previste o eseguite;*
- *ottenere l'approvazione dell'alta dirigenza per l'instaurazione o la prosecuzione del rapporto d'affari;*
- *svolgere un controllo rafforzato del rapporto d'affari, aumentando il numero e la frequenza dei controlli effettuati e selezionando gli schemi di operazione che richiedono un ulteriore esame*[165].

Per di più, viene disposta la creazione di un elenco nazionale delle funzioni considerate importanti cariche pubbliche con il fine di facilitare l'individuazione delle Persone Politicamente Esposte.
Altresì, è stato introdotto un divieto esplicito di tenere cassette di sicurezza in forma anonima.
Infine, è importante segnalare l'aggiunta dei seguenti fattori di rischio e tipologie indicative di situazioni potenzialmente ad alto rischio ai casi già indicati nell'Allegato III della IV Direttiva Antiriciclaggio:

- *clienti che sono cittadini di paesi terzi i quali presentano domanda di residenza o di cittadinanza nello Stato membro in cambio di trasferimenti in conto capitale, acquisti di immobili o titoli di Stato o investimenti in società nello Stato membro in questione*;
- *operazioni relative a petrolio, armi, metalli preziosi, prodotti del tabacco, artefatti culturali e altri oggetti di importanza archeologica, storica, culturale e religiosa o di raro valore scientifico, nonché avorio e specie protette*[166].

Gli Stati membri sono tenuti ad uniformarsi alle disposizioni della direttiva entro il 10 gennaio 2020.

3.3 ITALIA: PROCESSI NORMATIVI IN ATTO

Sotto il profilo regolatorio l'Italia risulta all'avanguardia rispetto agli altri paesi in quanto ha anticipato, con il D.lgs. 25 maggio 2017 n. 90 di recepimento della IV Direttiva antiriciclaggio, le disposizioni della V Direttiva in ambito delle valute virtuali. Nello specifico, il legislatore nazionale ha chiarito che la valuta virtuale seppur *"utilizzata come mezzo di scambio per l'acquisto di beni e*

[165] Cfr. Direttiva (UE9 2018/843. Art. 1, comma 11.
[166] Cfr. Direttiva (UE) 2018/843. Art. 1, comma 44 g e f.

servizi non è emessa da una banca centrale o da un'autorità pubblica, non è necessariamente collegata ad una valuta avente corso legale[167]*"*

Inoltre, ha introdotto nel nostro ordinamento gli obblighi di *due diligence* e di adeguata verifica della clientela a carico dei prestatori di servizi inerenti alle criptovalute, limitatamente a ciò che concerne la conversione di valute virtuali con valute aventi corso forzoso. Nello specifico gli exchange dovranno applicare gli obblighi di adeguata verifica della clientela in occasione dell'istaurazione di un rapporto continuativo o anche nel caso dell'esecuzione di un'operazione occasionale, che comporti la trasmissione di un importo pari o superiore a €15.000[168].

Per altro, come ricordato dal comunicato n°22 del MEF del febbraio 2018, sussiste la necessità di comunicare al predetto MEF l'operatività dei prestatori di servizi relativi all'utilizzo di valute virtuali. Per di più sono inclusi nell'obbligo di comunicazione anche gli operatori commerciali che accettano le valute virtuali come corrispettivo di qualsivoglia prestazione avente ad oggetto beni, servizi o altre utilità. L'iniziativa mira ad utilizzare una prima rilevazione sistematica del fenomeno a partire dalla consistenza numerica degli operatori del settore che, a regime, dovranno iscriversi in uno speciale registro tenuto dall'OAM, l'organismo degli agenti e dei mediatori, per poter esercitare la loro attività sul territorio nazionale[169].

Una puntualizzazione a parte, a mio avviso, merita il discorso della moneta elettronica, perché la stessa ben si presta a facilitare scambi tra denaro contabilizzato sul conto carta e la moneta virtuale. Relativamente alla moneta elettronica ci soffermiamo su strumenti di natura prepagata, ricaricabile e anonima.

Infatti, il legislatore ha inteso ingabbiare le modalità di emissione e di gestione di dette carte.

L'Italia, con il decreto legislativo di cui sopra, nel recepire la IV Direttiva ha limitato l'avvaloramento della carta a €250 e probabilmente nei tempi previsti dalla V Direttiva lo ridurrà a €150.

Questo aspetto assume una grande rilevanza in quanto abbiamo modo di verificare come lo strumento in questione avrebbe potuto prestarsi ad una situazione di lavaggio del denaro.

Questo potrebbe avvenire sia tramite la possibilità di ricaricare la carta in cambio della valuta virtuale, sia per scambi *brevi manu* delle due monete, soprattutto per ciò che concerne le caratteristiche delle carte anonime.

---

[167] Cfr. D.lgs. 25 maggio 2017 n° 90, Art.1 comma 2 lett. qq.

[168] Gravaglia Roberto. Valute virtuali e moneta elettronica: cosa cambia con il recepimento in Italia della IV direttiva antiriciclaggio. In pagamentidigitali.it, giugno 2017.

[169] Ministero dell'Economia e delle Finanze. Valute virtuali: in consultazione pubblica lo schema di decreto per censire il fenomeno. Comunicato n°22. Febbraio 2018.

3.4 GLI STRUMENTI DI CONTRASTO

Come correttamente evidenziato da Ranieri Razzante nel libro Finanziamento del Terrorismo e Nuove Tecnologie di fronte ad una varietà di processi tecnici estremamente evoluti, che se non governati lasciano spazio allo sfruttamento degli stessi da parte dei criminali, si rende necessario predisporre tutta una serie di monitoraggi e di accessi ai dati che riguardano la pluralità dei prodotti bancari o finanziari, soprattutto di fund transfert. A tal proposito nel predetto testo si sottolinea che devono poi essere normati il più possibile quegli strumenti di pagamento, come le carte prepagate, che sono entrati oggi nella disponibilità di tutti, che hanno il pregio di realizzare la c.d. inclusione finanziaria di soggetti che non sono bancarizzabili, ma con le controindicazioni che abbiamo descritto in precedenza[170].

Per quanto riguarda le carte prepagate, nonché tutte le altre carte di pagamento, sussiste una normativa stringente che riguarda gli IMEL (Istituti di Moneta Elettronica), che impone un monitoraggio puntuale e dettagliato delle transazioni e dei rapporti.

"*L'identificazione dei titolari e delegati deve diventare dappertutto, come per altro da tempo predicato dal FATF un must dell'attività di monitoraggio costante prevista dalle regole della Know Your Costumer che in Europa, ad esempio, mediante numerosi provvedimenti vincolanti delle Istituzioni e dei regulator, costituiscono l'armatura del sistema dei controlli preventivi su operazioni anomale e sospette di riciclaggio e finanziamento del terrorismo[171]".*

È intuibile che la cooperazione è fondamentale al fine del contrasto. In tal proposito si va concretizzando una banca dati europea dove si monitorano i *beneficial owner* di società, trust e fiduciarie in virtù della IV Direttiva antiriciclaggio.

Altresì, è fondamentale la collaborazione internazionale anche relativamente al fenomeno delle valute virtuali. Tant'è che la V Direttiva prevede: *"...il conferimento dei poteri di istituire e mantenere una banca dati centrale in cui siano registrate le identità degli utenti e gli indirizzi dei portafogli e a cui possano accedere le FIU[172]".*

Purtroppo, queste misure difficilmente potranno avere l'efficacia desiderata finché permarrà il fenomeno dei paesi che fanno dello *shadow banking* un elemento per attrarre capitali.

Per contrastare un fenomeno cosi globale come quello delle valute virtuali è necessario che almeno la maggior parte stati adottino presidi legislativi adeguati.

Questo aspetto viene evidenziato in particolare da un report, presentato dal FATF al G20 dei Ministri della Finanza e dei Governatori delle Banche Centrali nel luglio del 2018, che analizzava i presidi

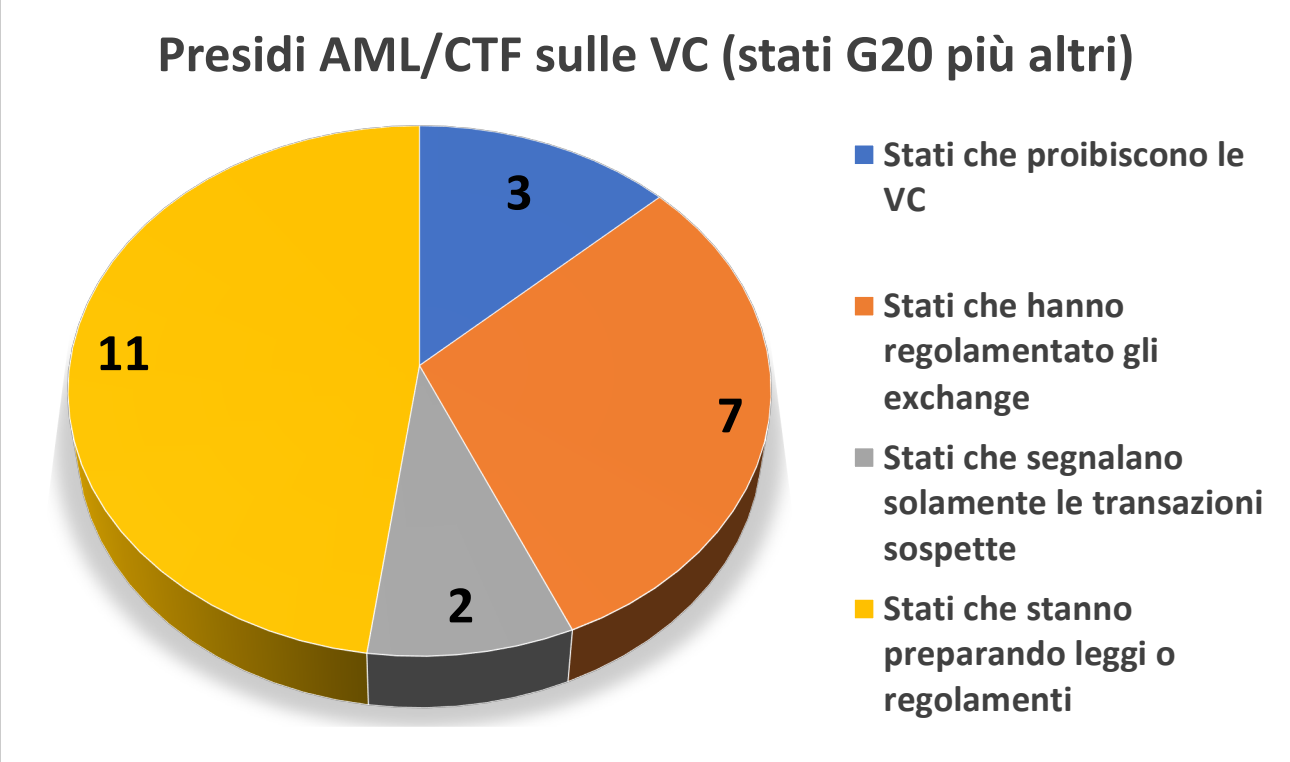
[170] Razzante Ranieri e Mugavero Roberto. *Terrorismo e nuove tecnologie*. Cit. pag. 73.

[172] Cfr. Direttiva (UE9 2018/843. Art. 1, comma 41 lett.g.

AML/TF con focus sulle valute virtuali. Nello specifico il report prendeva in esame la situazione normativa antiriciclaggio interessandosi non solo delle legislazioni degli Stati del G20 ma anche di quelle di altri Stati rilevanti al fine dell'analisi.
Lo studio ha evidenziato che:

- alcuni stati proibiscono l'utilizzo delle valute virtuali e/o proibiscono alle istituzioni finanziarie di trattarle. Questi stati sono la Cina, l'India e l'Indonesia.
- alcuni stati estendono la regolamentazione AML/CTF già esistente al campo delle valute virtuali. Ad esempio, specificando che le norme rivolte ai money transfer, alle banche o ad altre istituzioni finanziarie vengano destinate anche agli exchange di valute virtuali.
  I paesi in questione sono l'Australia, la Francia, la Germania, l'Italia, il Giappone, la Svizzera e gli U.S.A.
- la maggior parte degli stati sta ancora lavorando ad una regolamentazione in materia.
  Questi stati sono il Brasile, il Canada, il Messico, l'Olanda, la Russia, l'Arabia Saudita, la Corea del Sud, la Spagna, la Turchia e l'UK[173].

Per pronta visione si riepiloga nel grafico seguente la situazione dei presidi AML/CTF.



Fonte: FATF Report to the G20 Finance Ministers and Central Bank Governors. July 2018.

[173] FATF Report to the G20 Finance Ministers and Central Bank Governors. July 2018, pag 2.

Come si evince dall'analisi la maggior parte degli stati sono in ritardo, dal punto di vista legislativo, per contrastare un fenomeno che travalica con facilità i confini fisici delle nazioni.
Inoltre, è opportuno ricordare che quest'analisi si focalizza solamente sugli stati principali del panorama internazionale. Si può supporre come la situazione dei presidi AML/CTF negli altri stati sia decisamente più debole, se non addirittura inesistente.

CONCLUSIONI

Lo scopo del presente elaborato, come evidenziato nell'introduzione, era quello di verificare se le normative vigenti fossero in grado di contemplare i vari fenomeni che girano attorno al crimine (per crimine si intende anche tutto quello che riguarda il terrorismo) e all'illegalità.

Di fatto le prime quattro Direttive, di fronte ad una pluralità di fattispecie illegali criminose, hanno attuato tutta una serie di provvedimenti ed hanno fornito indicazioni circa la collaborazione da attuare tra gli stati membri, entrambi finalizzati a circoscrivere e limitare gli effetti di detti fenomeni.

Mentre, le valute virtuali sono un fenomeno relativamente giovane che, vista la complessità dell'architettura informatica e la non facile identificabilità dei soggetti che intervengono nel sistema, forse deve essere ancora compreso nella sua interezza in modo da poterlo normare in ottica delle fattispecie di cui sopra.

Infatti, come abbiamo illustrato precedentemente, il legislatore con la V Direttiva ha potuto disciplinare soltanto taluni aspetti, che come evidenziato più avanti, risultano insufficienti a contrastare in modo adeguato il fenomeno del riciclaggio tramite le valute virtuali.

Peraltro, ci troviamo in un contesto dove l'evoluzione tecnologica si caratterizza per un doppio aspetto.

Da una parte, consente alle autorità competenti di affinare gli strumenti e le tecniche di monitoraggio, ma dall'altra alimenta i presupposti per nuove e più articolate tecniche che consentono, a coloro che ne sanno trarre benefici, di individuare canali per nuove e più sofisticate operazioni di riciclaggio.

Questo è il caso della nascita e del rapido sviluppo delle valute virtuali che, come abbiamo evidenziato, si caratterizzano per un impianto strutturale e una complessità dei processi che ne consentono una difficile tracciabilità.

Oltre alla complessità tecnica ci sono anche altri fattori che non hanno permesso al legislatore, almeno fino ad ora, di accompagnare questa diffusione con dei presidi legislativi adeguati che regolamentino l'utilizzo di criptovalute o che forniscano gli strumenti necessari alle autorità per contrastare l'utilizzo di queste con fini illegali.

Tra questi fattori in *primis*, va sottolineato che il mondo virtuale, e le criptovalute che in esso hanno ragione di sviluppo, cambia e si evolve molto più velocemente di quanto siano in grado di fare gli stati con normative puntuali e pressanti. Tutto ciò avviene in un contesto mondiale dove sussistono stati che non sono collaborativi per propri interessi finanziari ed economici.

In secondo luogo, come abbiamo visto le valute virtuali non vengono controllate da istituzioni finanziarie. Esse non sono emesse né garantite da nessuna banca centrale né da un'autorità pubblica e non godono, quindi, dello stato giuridico di valuta o moneta[174].

Infine, bisogna ricordare che l'assenza di intermediari finanziari priva l'autorità di interlocutori disciplinabili dal punto di vista degli obblighi di segnalazione delle operazioni finanziarie. Infatti, è compito degli intermediari segnalare le operazioni sospette su cui le autorità indagano. Nel caso delle criptovalute, invece, le autorità competenti non sempre hanno la possibilità di vigilare ed individuare transazioni che si sviluppano su una molteplicità di piattaforme, spesso non soggette ad obblighi normativi.

Questo insieme di fattori rendono il mondo delle valute virtuali un'opportunità per i criminali, sempre abili a sfruttare a loro vantaggio i buchi normativi e contesti finanziari non trasparenti.

Mentre per coloro che intendono operare correttamente con le valute virtuali, queste possono costituire rischi concreti in termine di perdite finanziarie.

A conferma di ciò, le Autorità Europee di Vigilanza (AEV) hanno pubblicato nel Marzo del 2018 un'avvertenza nella quale allertano i "consumatori" circa la natura estremamente rischiosa e altamente speculativa delle valute virtuali.

Secondo le AEV l'acquisto di valute virtuali comporta i seguenti rischi:

- rischio di volatilità estrema e di bolla speculativa. Le valute virtuali sono soggette ad una grande volatilità dei prezzi. Chi decide di acquistare deve essere consapevole che può perdere una parte significativa, o persino l'intero ammontare, dell'investimento;
- assenza di protezione. Nonostante i requisiti dell'UE in materia di contrasto al riciclaggio della V Direttiva che regolamenteranno i servizi di valute virtuali, queste ultime rimangono non regolamentate ai sensi del diritto dell'unione. Neanche le piattaforme e i portafogli digitali sono regolamentate ai sensi del diritto dell'UE. Quindi chi effettua attività di compravendita di valute virtuali non beneficia delle garanzie e delle salvaguardie associate ai servizi finanziari regolamentati. Ad esempio, se una di queste piattaforme dovese fallire, subire un attacco informatico o la confisca dei beni in seguito ad azioni di contrasto, il consumatore non godrebbe di nessuna specifica tutela giuridica o garanzia di riavere le valute virtuali che possedeva;
- assenza di opzioni d'uscita. I detentori di valute virtuali potrebbero avere difficoltà a venderle o scambiarle con valute fiat per un lungo periodo di tempo, e subire perdite nel frattempo;
- mancanza di trasparenza sui prezzi ed informazioni fuorvianti;

[174] ESMA, EBA, EIOPA. L'ESMA, l'EBA e l'EIOPA informano i consumatori sui rischi delle valute virtuali. Marzo 2018, pag. 1.

- interruzioni delle operazioni. Queste son dovute a problemi operativi di alcune piattaforme di negoziazione che hanno comportato la sospensione delle contrattazioni. Cosi facendo i clienti non possono acquistare o vendere valute virtuali nel momento desiderato subendo delle perdite;
- inidoneità delle valute virtuali per la pianificazione d'investimenti o per scopi previdenziali dovuta all'elevata volatilità, incertezza sul futuro o inaffidabilità delle piattaforme[175].

La rischiosità delle criptovalute viene confermata anche dalla Banca d'Italia, che nella comunicazione del 30 gennaio 2015 scoraggia le banche e gli altri intermediari vigilati dall'acquistare, detenere o vendere le valute virtuali[176].
Tramite le sopracitate avvertenze le autorità, facendo ricorso all'utilizzo della *moral suasion,* esortano i consumatori ad un uso attento e consapevole delle valute virtuali che, nonostante la legalità delle transazioni, non hanno un'identità legale ben definita e non garantiscono un'adeguata protezione né ai consumatori né al sistema finanziario nel suo complesso[177].
Per quanto riguarda la problematica che stiamo trattando, cioè, quella della lotta al riciclaggio, la risposta del legislatore europeo si è concettizzata con la Quinta Direttiva antiriciclaggio, che ha volutamente inserito i prestatori di servizi virtuali tra i soggetti obbligati alla *due diligence* e all'adeguata verifica della clientela.
Tuttavia, nonostante la recente disciplina cerchi di "ingabbiare" i nuovi ambiti in cui si sta sviluppando il riciclaggio di denaro, questa presenta due importanti criticità.
In primis, l'operatività transnazionale tipica di questo mercato non può essere disciplinata tramite l'applicazione di norme nazionali/europee o internazionali che sono limitate dai confini territoriali[178], che invece il mondo virtuale non ha.
Infatti, come abbiamo analizzato nel corso della trattazione, le criptovalute si prestano con grandissima facilità a movimentazioni transnazionali di denaro. Per di più, i servizi di valute virtuali vengono forniti da *players* che risiedono nei punti più disparati del mondo.
Appare chiaro, dunque, che in assenza di una forte cooperazione internazionale, qualsiasi normativa, seppur emanata dall'Unione Europea, può risultare insufficiente nei confronti di un fenomeno cosi internazionale.

[175] ESMA, EBA, EIOPA. L'ESMA, l'EBA e l'EIOPA informano i consumatori sui rischi delle valute virtuali. Cit. pag. 2.
[176] Banca d'Italia. Comunicazione del 30 gennaio 2015 – valute virtuali. Provvedimenti di carattere generale delle autorità creditizie, sezione II – Banca d'Italia. In Open Review of management, Banking and Finance.
[177] Pellegrini Mirella, Di Perna Francesco. Cryptocurrency (and Bitcoin), a new challenge for the regulator. Londra: Fondazione Geraldo Capriglione Onlus in association with Regent's Univerisity London, marzo 2018.
[178] Pesci Daniela. Le implicazioni su rischi di antiriciclaggio. Cit

Si rende quanto mai necessario, quindi, un lavoro di cooperazione internazionale e dialogo tra i vari stati o presidi internazionali per creare una disciplina di contrasto efficace che sia uniforme e condivisa.

Finché ci saranno stati non cooperativi come i paradisi fiscali o i c.d. stati canaglia sarà impossibile arginare in maniera effettivamente determinante il fenomeno del riciclaggio tramite le valute virtuali.

Questo aspetto viene corroborato anche dalla Direttiva stessa nel considerando n°16, in cui il legislatore dichiara che: "*Gli Stati membri dovrebbero adoperarsi per garantire un approccio più efficiente e coordinato in relazione alle indagini finanziarie in materia di terrorismo, incluse quelle relative all'uso improprio delle valute virtuali*[179]".

Questa criticità viene confermata dal report the FATF presentato al G20, che abbiamo analizzato nel capitolo precedente.

La seconda criticità, riscontrabile nella disciplina AML, nei confronti delle valute virtuali, riguarda il fatto che l'inclusione dei prestatori dei servizi di valute virtuali tra i soggetti obbligati non risolve completamente il problema dell'anonimato.

Questa problematica viene sollevata dalla Direttiva stessa che nel considerando n° 9 analizza che "*poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato*[180]*"*.

Infatti, come abbiamo analizzato nel corso della trattazione, esistono diverse modalità per procurarsi valute virtuali in modo anonimo e, di conseguenza, sfruttare tali *escamotage* per poter utilizzare le criptovalute con fini illeciti.

Quindi, per ammissione del legislatore stesso, la Direttiva non è in grado di contrastare in modo determinante questo fenomeno.

Ciò trova conferma in uno sviluppo esponenziale di un mercato nascosto dove i criminali possono effettuare i propri traffici illeciti in maniera del tutto anonima grazie all'utilizzo delle valute virtuali.

Il mercato virtuale di cui stiamo parlando è quello del dark web. Il dark web è una parte segreta del web che è accessibile solamente tramite determinati browser, che nascondono l'indirizzo IP dell'utente permettendogli di non essere localizzabile[181].

In questo modo è possibile accedere a degli indirizzi web segreti dove si effettuano compravendite di qualsiasi tipo. In questi siti è possibile acquistare armi, droghe, documenti d'identità e, come abbiamo visto, in uno dei capitoli precedenti, acquistare valute virtuali in modo anonimo.

La maggior parte di questi scambi viene effettuata o in bitcoin o in Monero rendendo queste transazioni completamente segrete, attraverso i meccanismi sopra delineati.

---

[179] Cfr. Direttiva (UE) 2018/843. Considerando n°16.

[180] Cfr. Direttiva (UE) 2018/843. Considerando n°9.

[181] Spagnulo Eugenio. Cinque cose da sapere sul deep web. In focus.it, febbraio 2014.

È importante sottolineare come questi traffici illegali effettuati sul dark web in assenza delle criptovalute, probabilmente, non avrebbero la stessa diffusione.

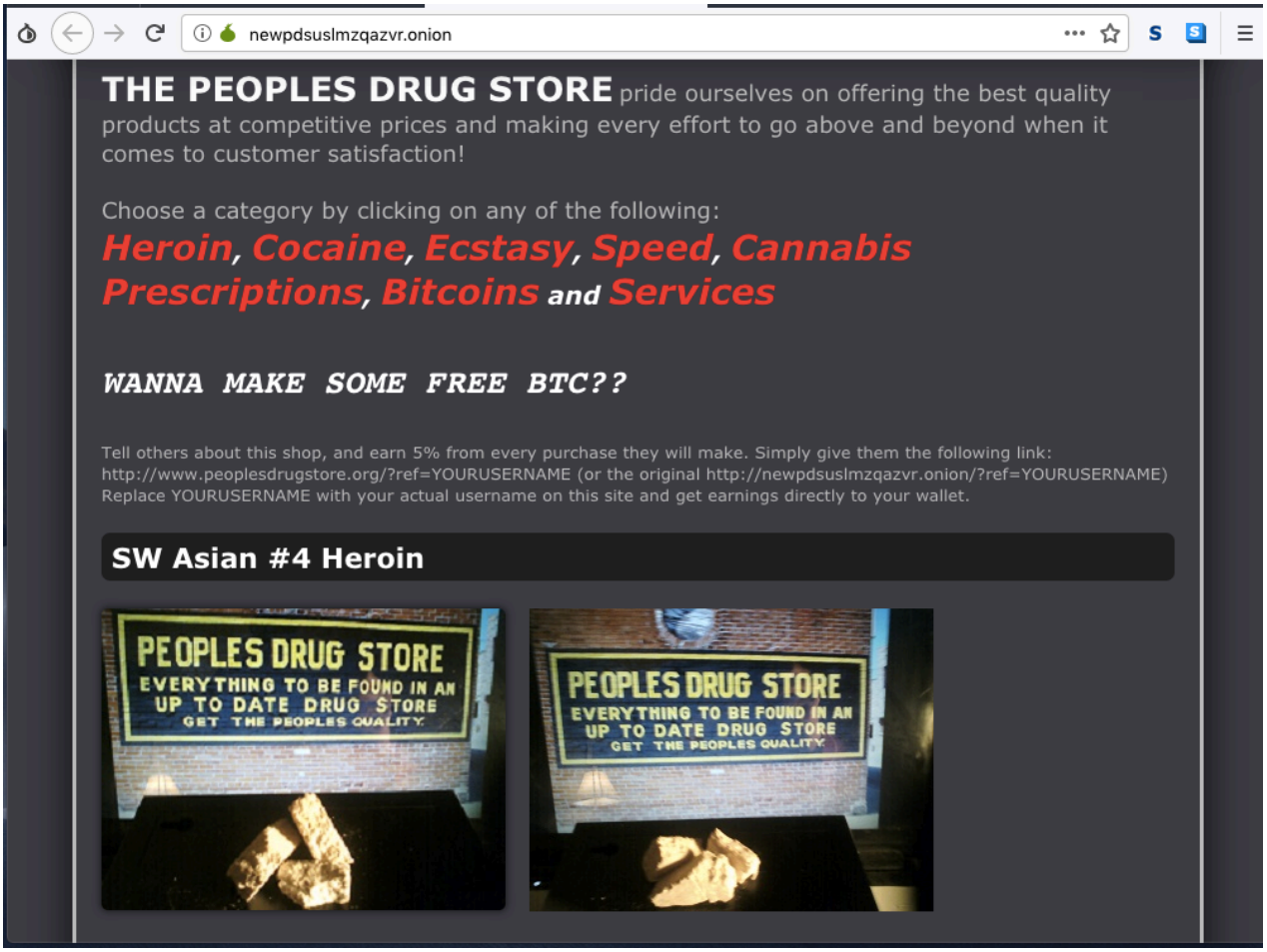
Io stesso, nel corso delle mie ricerche per questa trattazione, sono riuscito ad entrare nel dark web e, accedendo a determinati siti, ho potuto constatare la consistenza de fenomeno.

Figura 20: Armi in vendita nel dark web.

Fonte: Dark web

Come è possibile osservare dalle immagini sul dark web è possibile acquistare prodotti di svariato genere; da telefonini Apple e documenti d'identità fino a droghe e armi.
Inoltre, gli scambi vengono effettuati in bitcoin nella stragrande maggioranza dei casi.

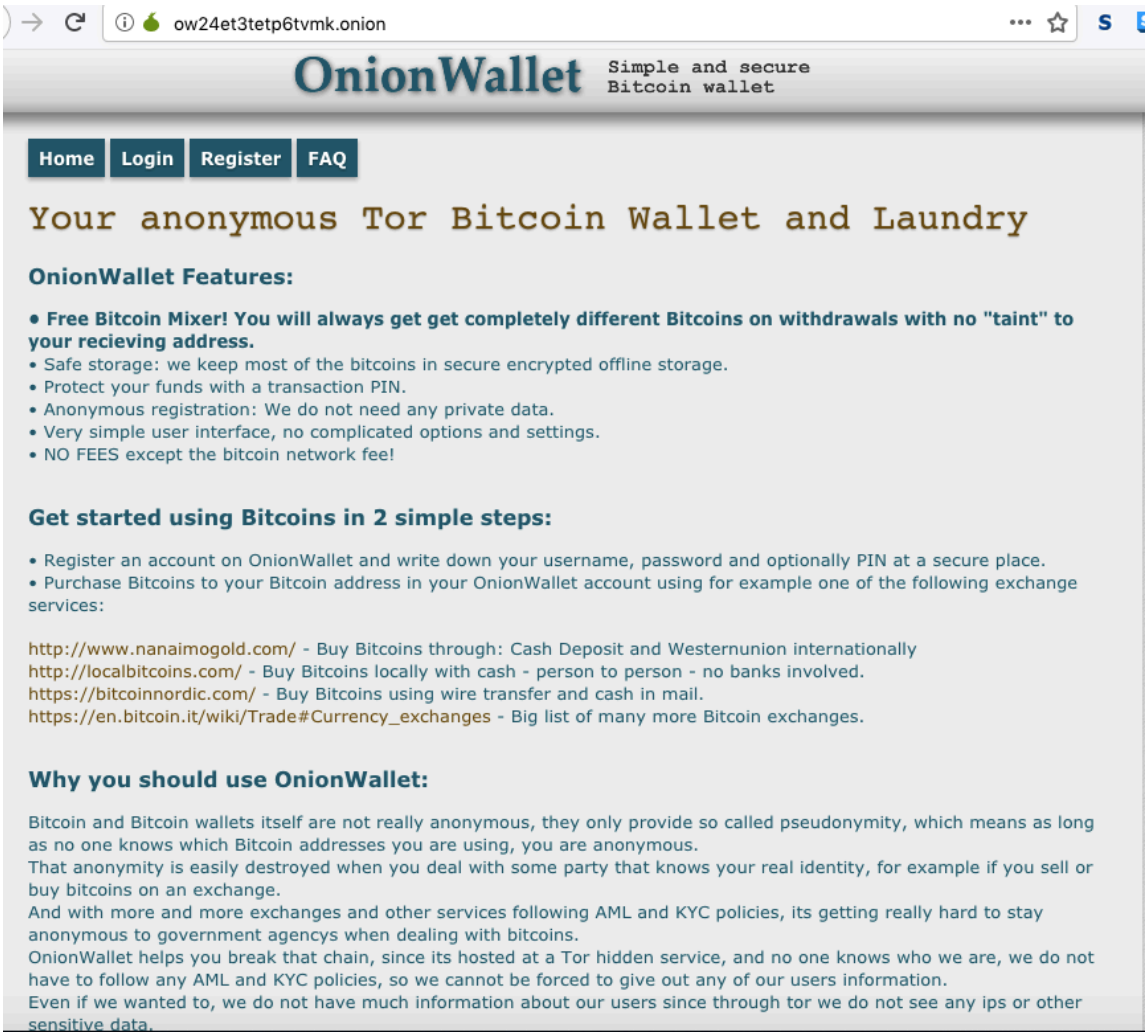
Figura 21: droghe in vendita nel dark web.



Fonte: Dark web

Peraltro, sempre nel dark web è possibile ottenere precise istruzioni su come "lavare" le valute virtuali possedute.

Figura 22: istruzioni finalizzate al riciclaggio



Fonte: dark web.

Si può, pertanto, concludere facendo un'amara constatazione: si stanno sviluppando delle situazioni, nel campo delle valute virtuali, che per le loro caratteristiche di complessità e globalizzazione, ben si prestano ad essere oggetto di attenzione da parte di coloro che hanno intenti criminali e/o illeciti.
L'augurio è che si pervenga ad una più stretta collaborazione tra le nazioni più importanti che porti a emettere normative puntuali e, soprattutto, condivise che forniscano alle autorità preposte gli strumenti necessari a contrastare il riciclaggio dei proventi ottenuti dalle attività criminali attraverso, soprattutto, l'utilizzo delle valute virtuali.

Forse la considerazione che fece Giovanni Falcone, circa la possibilità di individuare i mafiosi seguendo i flussi di denaro, oggi andrebbe riconsiderata alla luce di quanto abbiamo fin qui esposto.

BIBLIOGRAFIA

Accinni Giovanni Paolo. *Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017)*. In Archivio Penale, 2018**.**

Amato Massimo, Fantacci Luca. *Per un pugno di Bitcoin*. Milano: Egea, Università Bocconi Editore.
Baccarini Andrea Piergiorgio. *Unione Europea e riciclaggio di denaro del terrorismo internazionale e della criminalità organizzata.* Nella rivista Amministrazione in Cammino. 2006.

Balsamo Antonio. *La destinazione delle somme di denaro fa scattare il finanziamento del terrore*, in Guida al Diritto, 2006, n. 1.

Banca d'Italia. *Allegato I delle Disposizioni in Materia di Adeguata Verifica della Clientela.* Documento per la consultazione, Aprile 2018.

Banca d'Italia. *Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità Europee*. Marzo 2018.

Banca d'Italia. *Comunicazione del 30 gennaio 2015 – valute virtuali*. Provvedimenti di carattere generale delle autorità creditizie, sezione II – Banca d'Italia.

Battaglia Sergio Maria, Russo Angelo. *Contrasto al riciclaggio e cooperazione internazionale*. In Opinio Juris: Law and Politic Review, 2016.

Bellini Mauro. *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia.* In blockchain4innovation.it, gennaio 2019.

Bernaschi Massimo, Mastrostefano Enrico. *Una descrizione (quasi) informatica del funzionamento di bitcoin*. In Etica Economica, novembre 2014.

Bignazzi Sarah. *Caratteristiche dell'operatività in criptovalute e connessi profili penali*. Slide del seminario di alto aggiornamento ABI Antiriciclaggio 2018: novità, impatti e prospettive, 11 e 12 Luglio 2018.

Brizzi Ferdinando, Capecchi Gianluca, Rinaudo Antonio. *La reimmissione della liquidità illecita nel circuito economico ed il delitto di reimpiego tra prevenzione patrimoniale e giustizia penale: prospettive di future armonizzazioni*. In archivio penale(web) 2014.

Buonadonna Fabrizio, Tramontano Gennaro. *Codice Antiriciclaggio. Normativa, Prassi, Giurisprudenza. Aggiornato Al D.lgs. 21 novembre 2007, N. 231*. Macerata: Halley Editrice, 2008.

Caetano Richard. *Bitcoin: guida all'utilizzo delle criptovalute.* Milano: Apogeo, 2016.

Calzone Ottavio. *Bitcoin e distributed ledger technology.* In www.sicurezzanazionale.gov.it, febbraio

Calzone Ottavio. *Servizi di mixing e Monero*. In www.sicurezzanazionale.gov.it, luglio 2017.

Capogena Alessandro, Peraino Leandro, Perugi Silvia, Cecili marco, Zbrorowski Giovanni, Ruffo Andrea. *Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione.* In Diritto Mercato Tecnologia, n°3, 2015.

Capriglione Francesco. *Manuale di diritto bancario e finanziario.* Milano: Wolters Klower, 2016.

Carlisle David. *Virtual Currencies and Financial Crime: Challenges and Opportunities.* Royal United Services Institute for Defence and Security Studies, marzo 2017.

Come acquistare agli ATM Bitcoin in Italia? Ecco la guida completa. In coinlist.me.

Comitato di Sicurezza Finanziaria. *Analisi nazionale dei rischi di riciclaggio e finanziamento del terrorismo.* Ministero dell'Economia e delle Finanze, 2014.

Corradino Michele. *Strategie normative di contrasto al riciclaggio di denaro di provenienza illecita*. In Normativa antiriciclaggio e contrasto della criminalità economica. Padova: CEDAM, 2002.

Da Rold Vittorio. *Cipro, salvataggio choc: prelievo forzoso fino al 9,9% sui depositi bancari. Corsa dei correntisti ai bancomat. Oggi si riunisce il Parlamento.* Sole 24 Ore, 16 marzo 2016.

Danovi Remo. *La nuova normativa antiriciclaggio e le professioni*. Milano: Giuffrè, 2008.

De Vivo Annalisa e Trinchese Gabriella. *Le Novità della V Direttiva Antiriciclaggio.* Fondazione nazionale dei Commercialisti. In www.fondazionenazionalecommercialisti.it, settembre 2018.

Del Checco Paolo. *Birmixer, il più grande mixer di Bitcoin, si pente e chiude in battenti.* In bitcoinforensics.it, luglio 2017.

Demarchi Roberto. *Gli algoritmi crittografici del bitcoin.* In Sicurezza e Giustizia, 2017.

Demarchi Roberto. *Gli algoritmi crittografici del bitcoin.* In Sicurezza e Giustizia, 2017.

Di Carlo Francesco. *Un nuovo regime per l'applicazione di misure semplificate e rafforzate di adeguata verifica: dalle novità regolamentari all'analisi di alcuni casi concreti.* Atti del seminario di alto aggiornamento ABI Antiriciclaggio 2018: novità, impatti e prospettive, 11 e 12 Luglio 2018.

Draghi Mario. *L'azione di prevenzione e contrasto al riciclaggio.* Testimonianza nella Commissione Parlamentare d'Inchiesta Sul Fenomeno Della Mafia e Sulle Altre Associazioni Criminali, Anche Straniere. Roma, 22 luglio 2009.

Dupont Quinn. *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*. Londra: Routledge, 2018.

ESMA, EBA, EIOPA. *L'ESMA, l'EBA e l'EIOPA informano i consumatori sui rischi delle valute virtuali.* Marzo 2018.

European Banking Authority. *EBA Opinion on "virtual currencies"*. Luglio 2014.

European Central Bank. *Virtual currencies Schemes*. Ottobre 2012.

Familiari Sabrina. *Criptovalute: i sistemi di mixaggio per il riciclaggio di denaro.* Centro Ricerca sulla Sicurezza ed il Terrorismo (C.R.S.T), marzo 2018. In crstitaly.org.

FATF. *FATF Report to the G20 Finance Ministers and Central Bank Governors.* July 2018.

FATF. *The FATF Recommendations. International Standards on Combating Money Laundering and The Financing of Terrorism and Proliferation*. Parigi, 2012.

FATF. *Virtual Currencies: guidance for a risk based approach.* Giugno 2015.

FATF. *Virtual Currencies: Key Definitions and Potential AML/CFT Risk*. Giugno 2014.
Favaro Sergio. *Il coordinamento delle forze di polizia nella lotta al riciclaggio*. Rivista della Guardia di Finanza, 2002.

Ferraresso Andrea. *Bitcoin: come funziona il sistema. Le coppie di chiavi, il funzionamento della blockchain, la proof-of-work.* In mediunm.com, maggio 2016.

Galmarini Sabrina, Saba Claudio, La Scala Studio Legale. *IV Direttiva Antiriciclaggio e approccio basato sul rischio.* In www.dirittobancario.it, gennaio 2018.

Grasso Pietro. *Prefazione, in Elementi normativi internazionali e nazionali in materia di riciclaggio*. Bari: Cacucci, 2010.

Gravaglia Roberto. *Valute virtuali e moneta elettronica: cosa cambia con il recepimento in Italia della IV direttiva antiriciclaggio.* In pagamentidigitali.it, giugno 2017.

Investopedia. *What is cold storage for Bitcoin?* In www.investopedia.com, novembre 2018.

Kersten Armand. *Financing of Terrorism - A Predicate Offence to Money Laundering?* European Journal of Law Reform, n. 4, 2002.

La Gala Canio Giuseppe. *Il riciclaggio di denaro: Strumenti di contrasto e misure patrimoniali*. Supplemento al n.4/2000 della rassegna dell'Arma dei Carabinieri. 2000.

Longhi Massimo. *IV Direttiva antiriciclaggio e trasparenza dei trust: cominciamo bene.* IPSOA Quotidiano del 10 febbrai 2015.

Maiello Vincenzo, Della Ragione Luca. *Riciclaggio e reati nella gestione dei flussi di denaro sporco.* Milano: Giuffrè Editore, 2018.

Mancini Marco. *Valute virtuali e Bitcoin. In Analisi Giuridica dell'Economia*. Bologna: Il Mulino, giungo 2015.

Mancini Novella. *Bitcoin: rischi e difficoltà normative.* Bologna: Il Mulino, in Banca impresa società, 2016.

Minenna Marcello. *L'esplosione della bolla Bitcoin: un'autopsia.* Il Sole 24 Ore, 31 dicembre 2018.

Ministero dell'Economia e delle Finanze. *Valute virtuali: in consultazione pubblica lo schema di decreto per censire il fenomeno.* Comunicato n°22. Febbraio 2018.

Nanulla Gaetano. *La lotta alla mafia.* Milano: Giuffrè, 2012.

Novetta. *Survey of Bitcoin Mixing Services: Tracing Anonymous Bitcoins*. Reperibile su novetta.com, 2015.

ONU. *Convenzione delle Nazioni Unite contro il traffico illecito di stupefacenti e sostanze psicotrope*. Vienna: dicembre 1988.

P.A.ID Strategies. *The Cryptocurrency Identity Crisis: An Industry Scorecard for Digital Id Verification for KYC and AML.* Giugno 2018.

Passarelli Nina. *Bitcoin e antiriciclaggio*. In www.sicurezzanazionale.gov.it, 15 novembre 2016.

Pearson Jordan. *Meet Monero, the Currency Dark Net Dealers Hope is More Anonymous than Bitcoin*. In www.motherboard.vice.com. 23 agosto 2016.

Pellegrini Mirella, Di Perna Francesco. *Cryptocurrency (and Bitcoin), a new challenge for the regulator*. Londra: Fondazione Geraldo Capriglione Onlus in association with Regent's Univerisity London, marzo 2018.

Pesci Daniela. *Le implicazioni su rischi di antiriciclaggio*. Slide del seminario di alto aggiornamento ABI Antiriciclaggio 2018: novità, impatti e prospettive, 11 e 12 Luglio 2018.

Quattrocchi Danilo, Mongiello Licia. *Le FAQ del MEF sulle novità della normativa di attuazione della IV Direttiva Antiriciclaggio.* In www.dirittobancario.it, ottobre 2017.

Razzante Ranieri e Mugavero Roberto. *Terrorismo e nuove tecnologie*. Pisa: Pacini Editore,2016.

Razzante Ranieri. *La regolamentazione antiriciclaggio in Italia. Aggiornato alla delibera della Banca d'Italia 10 marzo 2011 sui controlli antiriciclaggio.* Torino: G. Giappichelli Editore, 2011.

Satoshi Nakamoto. Bitcoin: *A Peer-to-Peer Electronic Cash System*. In www.bitcoin.org. Novembre 2008.

Scapellato Filippo. *Il fenomeno del riciclaggio e la normativa di contrasto*. Torino: Giappichelli Editore, 2013.

Spagnulo Eugenio. *Cinque cose da sapere sul deep web.* In focus.it, febbraio 2014.

Stile Alfonso. *Riciclaggio e reimpiego di proventi illeciti*.

Studio Legale Giovanni Paolo Accinni e Associati. *Profili di complessità e di rischio delle "criptovalute".* In Archivio Penale, 2017.

Tampanella Biagio. *La crittografia tra arte e scienza.* In sicurezzanazionale.gov.it, settembre 2015.

Team Tokens24. *Redditività del Mining di Bitcoin nel 2018.* In www.tokens24.com, marzo 2018.

Tolla Marco. *Elementi normativi internazionali e nazionali in materia di riciclaggio.* Bari: Cacucci, 2010.

Tortora Gianluca. *Adeguata Verifica Semplificata.* Atti del seminario di alto aggiornamento ABI Antiriciclaggio 2018: novità, impatti e prospettive, 11 e 12 Luglio 2018.

UIF. *Quaderni dell'antiriciclaggio dell'Unità di Informazione Finanziaria*. Settembre 2018.

Urbani Alberto. *Disciplina Antiriciclaggio e Ordinamento del credito*. Padova: CEDAM, 2006.

Zanchetti Mario. *Il riciclaggio di denaro proveniente da reato*. Milano: Giuffrè, 1997.

SITOGRAFIA

bbc.com

bitcoin.org

bitcointalk.org

bitcoinforensics.it

blockchain4innovation.it

blockexplorer.com

coinlist.me

coinmixer.es

coinatmradar.com/

deepwebitalia.com

eba.europa.eu

ec.europa.eu

eur-lex.europa.eu

europarl.europa.eu

focus.it

finance.yahoo.com

localbitcoins.net

moneroblocks.info

paxful.com

rusi.org

uif.bancaditalia.it

www.abiformazione.it

www.archiviopenale.it

www.bancaditalia.it

www.blockchain.com

www.blockchain4innovation.it

www.dirittobancario.it

www.ecb.europa.eu

www.eticaeconomia.it

www.fatf-gafi.org

www.fondazionenazionalecommercialisti.it

www.gdf.gov.it

www.ilsole24ore.com

www.investopedia.com

www.ionos.it

www.mediasetplay.mediaset.it

www.mef.gov.it

www.motherboard.vice.com

www.novetta.com

www.pagamentidigitali.it

www.paidstrategies.com

www.sicurezzanazionale.gov.it

www.tokens24.com

RIASSUNTO

Per sviluppare la tesi in argomento si rende necessario valutare le normative vigenti in relazione, soprattutto, al recente sviluppo delle criptovalute e del loro potenziale utilizzo illecito.
Vengono ripercorsi, quindi, i capisaldi delle normative vigenti, in particolare le direttive antiriciclaggio specificatamente a fenomeni di facilitazione del riciclaggio di denaro riveniente da attività illecite o criminali. Da qui, la necessità di ripercorrere la storia, relativamente recente, delle valute virtuali, come sono nate (nel caso in questione il Bitcoin) e come operano. L'indagine sarà tesa a capire se è effettivamente possibile effettuare operazioni di riciclaggio tramite le criptovalute.
In effetti, scopriremo che è proprio la loro struttura e la sofisticazione dei processi di ingegneria informatica, che è alla base delle piattaforme che le regolano e che ne determinano, spesso, una difficile tracciabilità, a richiamare l'attenzione di soggetti dediti ad attività criminose.
Osserveremo, quindi, qual è stata la risposta dell'Unione Europea, in particolare attraverso la V Direttiva, e se questa è sufficiente a contrastare il fenomeno.

RICICLAGGIO, FINANZIAMENTO DEL TERRORISMO E AUTORICICLAGGIO.

Il riciclaggio è un'attività che consiste nell'utilizzare denaro e beni di provenienza illecita reinvestendo gli stessi in attività legali avendone occultato la provenienza mediante determinate operazioni finanziarie. L'illegalità di queste deriva dal legame con il reato che ha determinato i proventi finanziari. Lo scopo di tali operazioni, infatti, è proprio quello di rendere impossibile ricostruire i movimenti dei capitali in questione fino all'evento delittuoso che li ha generati. Tale *modus operandi* costituisce per le organizzazioni criminali forme di autofinanziamento ma anche la possibilità di acquisire attività produttive sul territorio controllando, di fatto, il tessuto economico e sociale.
Il reato di riciclaggio viene definito dalla normativa nell'art. 2, d.lgs. n. 231/2007. Inoltre, in linea con gli ordinamenti internazionali e con le direttive comunitarie viene equiparato al riciclaggio qualsiasi attività finalizzata alla creazione di risorse economiche, il cui obiettivo è quello del compimento di delitti con finalità terroristiche. La definizione del reato di finanziamento del terrorismo viene esplicitata per effetto del Decreto Legislativo 25 maggio 2017, n. 90, l'articolo 2, comma 6, del d.lgs. n. 231/2007. Di conseguenza è rilevante per la disciplina antiriciclaggio, non

solo, la creazione, la movimentazione e l'utilizzo di ricchezza di provenienza illecita, ma anche, la creazione, se pur lecita, della stessa se finalizzata a sostenere sul piano finanziario attività di tipo terroristico. Infatti, sebbene il riciclaggio di denaro e il finanziamento del terrorismo siano fenomeni distinti, ciascuno con la propria ratio e le proprie peculiarità, *de facto* essi utilizzano le stesse tecniche di occultamento di denaro per portare a termine i propri fini illeciti. Nel riciclaggio, *money laundering*, gli artifici finanziari vengono utilizzati per nascondere la provenienza del denaro, cercando di "lavarlo" rendendolo lecitamente riutilizzabile. Invece per quanto riguarda il finanziamento del terrorismo, *money dirtying*, gli stessi metodi hanno la finalità di nascondere la fonte dei capitali, che non deve essere necessariamente illegale, per riutilizzarla in seguito. Il nesso tra le due attività, dunque, consiste in quell'insieme di tecniche finanziarie atte a rendere irrintracciabili i flussi di denaro. Per questo entrambi i reati sono soggetti al medesimo regime, definito AML/CTF, ovvero *Anti Money Laundering and Counter Terrorism Financing*.

Infine, è fondamentale determinare il reato di autoriciclaggio e sottolinearne la differenza da quello di riciclaggio. Dal 1° gennaio 2015 è in vigore la nuova fattispecie dell'autoriciclaggio. Il reato in questione punisce non solo la condotta del soggetto che fa rientrare i soldi sporchi nell'economia legale ma che ha anche compiuto o concorso a commettere il reato non colposo che sta a monte, mentre risponde del reato di riciclaggio chi non ha concorso nel reato alla base ma ha ripulito i soldi sporchi nell'interesse di chi ha compiuto il delitto.

Nel nostro paese l'introduzione di una fattispecie *ad hoc* legata al riciclaggio è nata in seguito alla volontà di contrastare reati tipici delle organizzazioni mafiose come le estorsioni e i sequestri di persona a scopo di estorsione, mentre a livello internazionale, come si vedrà in seguito analizzando le prime convenzioni internazionali, è stato il traffico di droga, e la sua crescita esponenziale, ad indurre i legislatori a porre la attenzione sulla necessità di contrastare questa enorme fonte di finanziamento per le organizzazioni criminali.

Il riciclaggio è un fenomeno estremamente complesso, e si può suddividere in tre fasi: *placement stage* (collocamento nel mercato dei proventi illeciti); *layering stage* (camuffamento di qualsivoglia collegamento tra denaro riciclato e l'attività criminale); *integration stage* (reinserimento del denaro sporco nel sistema legale).

ANTIRICICLAGGIO: LE ORIGINI DELLA DISCIPLINA

La necessità di contrastare il fenomeno del riciclaggio ebbe origine negli anni '80 con la comparsa delle prime normative internazionali. In questo contesto maturò la giusta consapevolezza che fosse necessario "colpire" le organizzazioni criminali dal punto divista economico cercando di impedire

che queste usassero il riciclaggio come forma di finanziamento, creando una fitta rete di protezione del sistema economico mediante il controllo sul mercato e la trasparenza dello stesso. Una corretta normativa antiriciclaggio deve essere estremamente dinamica, in quanto è necessario che essa stia al passo con l'evolversi delle organizzazioni criminali e delle loro tecniche sempre più all'avanguardia. Inoltre, la dimensione transnazionale del fenomeno ha imposto di adottare contromisure normative di analoga estensione che non esauriscano la propria efficacia al di fuori del livello nazionale. Infatti, concorre a determinare il fenomeno del riciclaggio la globalizzazione dell'economia, l'integrazione dei mercati finanziari e strumenti finanziari innovativi.

Il primo documento di carattere internazionale fu la raccomandazione "*Misure contro il trasferimento e la custodia di fondi di origine criminale"* emanata dal Comitato dei Ministri del Consiglio d'Europa il 27 giugno del 1980 e rivolta ai Paesi membri.

Successivamente fu di notevole importanza la "*Dichiarazione di principi concernenti la prevenzione dell'uso criminale del sistema bancario a fini di riciclaggio del denaro"*, sottoscritta il 12 dicembre 1988 a Basilea dai rappresentanti delle Banche Centrali e degli Organi di Vigilanza bancaria del Gruppo dei Dieci. Questa viene considerata una vera e propria pietra miliare nella lotta al riciclaggio, sui quali principi verrà basata tutta la futura disciplina in materia.

Un punto di svolta nel percorso della disciplina fu la "*Convenzione ONU contro il traffico illecito di stupefacenti e sostanze psicotrope",* stipulata a Vienna nel dicembre 1988, in quanto fu la prima volta che un organismo internazionale adottasse un provvedimento vincolante nella lotta al riciclaggio.

Nel febbraio 1990 il GAFI (*Gruppo d'Azione Finanziari Internazionale*; in inglese FATF: *Financial Action Task Force)* emanò 40 Raccomandazioni antiriciclaggio, che costituiscono il caposaldo della lotta al riciclaggio e al finanziamento del terrorismo.

Sempre nel 1990 a Strasburgo intervenne nuovamente il Consiglio d'Europa tramite la *Convenzione sul riciclaggio, l'identificazione, il sequestro e la confisca dei proventi di reato.*

Nel 2000 venne stipulata la Convenzione di Palermo che ha un'importanza strategica grazie all'identificazione del riciclaggio in un reato transnazionale e che di conseguenza necessita la cooperazione tra vari Stati.

ANTIRICICLAGGIO: LE PRIME 4 DIRETTIVE

Fondamentali nella lotta al riciclaggio e al finanziamento del terrorismo sono le quattro Direttive antiriciclaggio. Di queste la prima e la seconda Direttiva, rispettivamente la n.91/308/CEE e la n. 2001/97/CE, contribuirono a creare la base legislativa della lotta al riciclaggio. In particolare, la prima, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di

attività illecite, definì il reato di riciclaggio e impose agli intermediari i primi obblighi di identificazione e registrazione della clientela, di comunicazione e conservazione dei dati e di collaborazione delle autorità. La seconda, invece, ampliò il campo d'applicazione della disciplina estendendo il novero dei reati presupposto oltre i reati connessi al traffico di droga. Inoltre, gli obblighi vennero estesi anche a soggetti e enti non finanziari.

La disciplina venne rinnovata tramite la terza Direttiva, n. 2005/60/CE, che abrogò le precedenti direttive. Quest'ultima, recependo le raccomandazioni del GAFI e alla luce degli attacchi terroristici dell'11 settembre, estese l'ambito d'applicazione della disciplina anche al fenomeno del finanziamento del terrorismo.

Inoltre, ampliò il campo d'applicazione della disciplina implementando i reati presupposto alla base della definizione di riciclaggio, estese gli obblighi a soggetti non inclusi nella direttiva precedente ed introdusse i due attuali cardini della lotta al ML/TF il principio del *know your costumere* quello del *risk based approach.*

Il primo si sostanzia nell'attività di *due diligence* atta all'approfondire la conoscenza del cliente e stabilisce tre categorie di obblighi di adeguata verifica della clientela: obblighi ordinari, semplificati e rafforzati.

Gli obblighi di adeguata verifica della clientela consistono nell'identificare il cliente, l'esecutore e il titolare effettivo e verificarne l'identità, acquisire e valutare le informazioni relative allo scopo del rapporto continuativo o della prestazione ed infine eseguire un controllo costante nel corso del rapporto con il cliente.

Il secondo viene utilizzato dagli intermediari per individuare, valutare e gestire i rischi connessi con il riciclaggio e il finanziamento del terrorismo, stabilendo misure di contrasto che siano proporzionali ai rischi effettivamente individuati. In base a tale principio intermediari orientano le modalità e la profondità delle analisi che devono condurre per l'assolvimento degli obblighi di adeguata verifica, in modo coerente e commisurato all'effettiva esposizione ai rischi di riciclaggio e di finanziamento del terrorismo.

A distanza di dieci anni dalla terza Direttiva antiriciclaggio, il legislatore decise di riformare la materia tramite la quarta Direttiva (UE) 2015/849.

La nuova disciplina ha razionalizzato e ampliato notevolmente l'approccio basato sul rischio strutturando il *risk assesment su tre livelli*: europeo, nazionale e dei soggetti obbligati.

Il *risk assesment* europeo è affidato alla Commissione che, basandosi sulle valutazioni nazionali degli Stati membri, ha il compito di elaborare una valutazione sovranazionale dei rischi ML/TF presenti nel mercato comunitario e coordinare la valutazione del rischio delle attività transfrontaliere.

A livello nazionale, invece, gli stati devono svolgere un'analisi periodica che ha l'obiettivo di identificare, analizzare e valutare le minacce di riciclaggio di denaro e di finanziamento del terrorismo, individuando quelle più rilevanti, i metodi di svolgimento di tali attività criminali, le

vulnerabilità del sistema nazionale di prevenzione, di investigazione e di repressione di tali fenomeni, e quindi i settori maggiormente esposti a tali rischi.
L'analisi nazionale è strutturata in due fasi:

- valutazione del "rischio ML/TF inerente" (analisi delle criticità e delle minacce) nel sistema;
- valutazione dell'efficacia dei presidi di prevenzione, investigazione e repressione.

Per quanto riguarda i soggetti obbligati i loro adempimenti antiriciclaggio si suddividono in tre *step*:

- identificazione e assessment dei rischi ML/TF (autovalutazione): identificazione del rischio inerente, delle vulnerabilità e del rischio residuo (rischio che permane a seguito dell'applicazione delle tecniche di mitigazione del rischio);
- adeguata verifica della clientela, graduando il livello e la tipologia sulla base del rapporto (continuativo o occasionale) e in base alle informazioni ottenute in sede di assessment;
- controllo costante e aggiornamento periodico delle valutazioni effettuate del rischio;

Inoltre, la direttiva ha inasprito gli obblighi di adeguata verifica semplificata, ha perfezionato gli obblighi rafforzati estendendone, tra l'altro, l'applicazione alle persone politicamente esposte e ha reso più chiare e accessibili le informazioni sul titolare effettivo di persone giuridiche e trust.
La quarta Direttiva formula anche altre indicazioni circa la cooperazione tra FIU dei diversi Stati membri ed è un aspetto estremamente importante, in quanto si lega strettamente al concetto di un'azione unitaria a livello europeo nel contrasto del riciclaggio di denaro e del finanziamento del terrorismo.

IL RICICLAGGIO E LE VALUTE VIRTUALI

L'evoluzione tecnologica è stata utilizzata dai riciclatori come utile veicolo per effettuare movimenti transfrontalieri di denaro con velocità e sicurezza. Infatti, l'ultima frontiera dei pagamenti digitali, legata in particolare al mondo delle valute virtuali, comporta, come ogni evoluzione tecnologia in questo campo, potenziali benefici legati all'utilizzo di nuovi strumenti finanziari che devono essere disciplinati e correttamente monitorati al fine di evitare utilizzi impropri e illegali.
Per poter valutare come le organizzazioni criminali riescono ad utilizzare al meglio, a fini illegali, le valute virtuali bisogna capire il loro funzionamento.

Le valute virtuali vengono definite come la rappresentazione digitale di valore non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata ad una valuta avente corso legale e che viene utilizzata come mezzo di scambio per l'acquisto di beni e sevizi, trasferita, archiviata e negoziata elettronicamente.

Analizziamo le valute virtuali o criptovalute riferendoci a quella più conosciuta: il bitcoin.

Il Bitcoin è apparso per la prima volta nel 2009 tramite la pubblicazione online del documento "*Bitcoin A peer-to-peer electronic cash system"* sottoscritto da Satoshi Nakamoto, pseudonimo di uno o più hacker. Bitcoin è un sistema *peer to peer*, ovvero una rete decentralizzata (senza la presenza di un'autorità incaricata di validare e registrare le transazioni) dove i nodi (utenti) si scambiano tra loro un costante flusso d'informazioni e hanno uguale accesso alle risorse pubbliche. Ogni utente, connettendosi alla rete, può interagire con gli altri utenti, validare ed autorizzare transazioni, controllare il registro pubblico e segnalare errori al resto della rete.

Il Bitcoin venne creato con la finalità di permettere trasferimenti di denaro digitale senza doversi basare sulla fiducia nei confronti di una terza parte.

In poche parole, Bitcoin si propone di creare un sistema decentralizzato completamente indipendente da intermediari bancari o organismi governativi, sottraendo al settore bancario la funzione di gestione del sistema di pagamento e della relativa contabilità.

La blockchain, che è sicuramente l'innovazione più importante di Bitcoin, è simile ad un libro contabile elettronico, pubblico, in continua espansione e su cui vengono registrate cronologicamente ed in modo permanente tutte le transazioni.

I blocchi di transazioni, di cui è articolata la blockchain, sono costituiti da un *blocknumber* identificativo e da informazioni sulla transazione riguardanti l'importo della stessa e lo pseudonimo di chi la compie. I blocchi sono concatenati l'uno all'altro rendendo possibile risalire a tutte le transazioni bitcoin effettuate fino al blocco iniziale.

La sicurezza e l'autenticità delle transazioni viene garantita dalla crittografia asimmetrica, che si basa sull'utilizzo di due chiavi, una privata e una pubblica. La chiave privata viene utilizzata per crittografare un documento, in questo caso il denaro digitale, ponendo una firma digitale. La chiave pubblica viene utilizzata per decrittografare il documento, verificandone la firma. Chi effettua una transazione genera una coppia di chiavi ed invia al destinatario quella pubblica. Il mittente firma il documento con la chiave privata e lo invia al destinatario, che con la chiave pubblica è in grado di verificare la firma e assicurarsi dell'identità del mittente.

I portafogli di bitcoin, chiamati wallet, sono formati da un insieme di indirizzi e chiavi private, che sono utilizzati rispettivamente per ricevere ed inviare bitcoin. Gli indirizzi vengono creati utilizzando degli pseudonimi, in quanto non viene verificata la reale identità degli utenti.

Inoltre, non ci sono limiti al numero di indirizzi che è possibile creare. Tutto ciò garantisce l'anonimato degli utenti.

Altro elemento fondamentale per lo sviluppo del sistema sono i miner, nodi che risolvendo un difficile problema di calcolo matematico processano e confermano le transazioni raggruppandole in blocchi e costruendo in tal modo la blockchain.
Vista la complessità dei problemi matematici da risolvere, per fare il mining è necessario l'utilizzo di potentissimi computer che sono stati progettati appositamente con questo scopo, sia dal punto di vista dell'hardware sia da quello del software.
Le principali società che si occupano di mining sono situate principalmente negli Stati Uniti, in Corea ed in Cina.
Il bitcoin viene definito contante digitale in quanto è stato in grado di unire le caratteristiche delle due monete preesistenti, quella fisica e quella elettronica, condensandone i rispettivi vantaggi.
In particolare, come un bonifico permette pagamenti a distanza e, come il contante, permette pagamenti istantanei e praticamente senza costi per il pagante per il ricevente.
Il Bitcoin, così come altre virtual currencies, presenta dei vantaggi, tra i quali:

- la velocità del sistema utilizzato, che consente transazioni in pochissimi secondi;
- la natura globale del sistema di pagamento per la quale è possibile effettuare e ricevere pagamenti a livello internazionale;
- la facilità di utilizzo, anche da parte di chi non ha una solida preparazione informatica;
- la possibilità di effettuare micro-pagamenti;
- il bassissimo costo delle transazioni.

Questi elementi rendono il Bitcoin e le altre criptovalute terreno fertile per il proliferarsi di attività criminali, anche alla luce di una regolamentazione internazionale non adeguata. Gli organismi internazionali sono ben consapevoli di ciò, tant'è che L'EBA (European Banking Autority) nella catalogazione dei rischi connessi alle valute virtuali assegna, a quest'ultime, il livello più alto possibile di pericolosità al rischio di riciclaggio, di finanziamento del terrorismo, e di tutta una serie di altre attività illegali nonché criminose.
Infatti, tramite le valute virtuali è possibile effettuare con velocità operazioni in tutto il mondo celando, di fatto, la propria identità, in quanto, come abbiamo visto, gli indirizzi Bitcoin sono contraddistinti dall'anonimato.
Chiaramente questo aspetto è un intralcio per le autorità che hanno il compito di controllare l'eventuale presenza di transazioni a copertura di operazioni illecite.
Anche i servizi di valute virtuali, come gli exchange che si occupano di cambiare valuta virtuale con valute legali ed i wallet provider, ovvero quegli ambienti criptati dove è possibile inserire, spedire e ritirare le criptovalute, si basano su complesse infrastrutture che coinvolgono diverse entità, spesso

locate in molteplici parti del mondo. Questa molteplicità dei servizi comporta che possa non essere chiaro a chi competono le responsabilità di contrasto al riciclaggio e lotta al finanziamento del terrorismo.
Le caratteristiche intrinseche del sistema Bitcoin, che abbiamo analizzato, seppur agevolando il mantenimento dell'anonimato non sono sufficienti a nascondere completamente le tracce degli utenti, in quanto bisogna ricordare che il sistema è stato architettato con finalità diverse da quelle che poi hanno portato a favorire le attività criminali.
Infatti, nonostante le informazioni presenti sulla blockchain non rappresentino affatto una "minaccia" diretta all'anonimato degli utenti, queste però potrebbero essere associate con informazioni addizionali per creare un collegamento con le identità reali degli stessi.
Le informazioni che vengono ricercate ed utilizzate dalle autorità per rintracciare i soggetti sono divise in quattro tipologie e sono le seguenti dati: personali, comportamentali, finanziari, di rete.
I malintenzionati per evitare di diffondere queste informazioni e quindi risultare completamente irrintracciabili debbono prendere delle precauzioni ed adottare determinati schemi di comportamento.
Oltre alla modalità ed il metodo di pagamento con cui si acquistano i bitcoin risulta fondamentale utilizzare dei servizi di mixing per aumentare l'anonimato delle transazioni.
Il mixing è un servizio che consente agli utenti di oscurare la cronologia delle transazioni aggregando un certo numero di trasferimenti e nascondendo l'origine e la destinazione di ogni singolo pagamento.
Per concludere, al fine di risultare irrintracciabili oltre all'utilizzo dei servizi di mixing, che non sono infallibili, ed evitare che i propri dati vengano raccolti ed associati è necessario:

- considerare che tutte le operazioni effettuate da uno stesso portafoglio sono collegabili e di conseguenza non comprare mai articoli anonimi e articoli personali dallo stesso portafoglio;
- utilizzare sempre una tipologia di browser particolare che permette di rendere ignoto al venditore il proprio indirizzo IP;
- utilizzare almeno due servizi di mixing di seguito per rendere anonimi i propri bitcoin.
- utilizzare conti differenti per ogni operazione di mixing, nel caso in cui il servizio di mixing richieda la registrazione dell'utente;
- utilizzare esclusivamente canali di comunicazione crittografati sia per contattare il servizio di mixing sia per qualsiasi altra comunicazione. Nello specifico le e-mail non criptate sono facilmente intercettabili. Ad esempio, un canale di comunicazione sicuro è Bitmessage in quanto è criptato, anonimo, decentralizzato e non censurabile.

Questa enunciazione aiuta a capire come effettivamente coloro che seguono i passi sopracitati vanno ad assumere la consapevolezza di potersi rendere irrintracciabili e di fatto questa è la prassi che viene più frequentemente utilizzata.
Per sintetizzare si riepilogano i diversi modi per procurarsi delle criptovalute.
Il primo di questi è il mining che ottiene una ricompensa in criptovaluta per l'attività svolta.
Il secondo modo per procurarsi delle valute virtuali è tramite gli Exchange che convertono la valuta fiat in criptovaluta e viceversa.
Quest'ultimi sono particolarmente attenzionati dal contesto legislativo internazionale perché stanno proliferando in presenza di una disciplina non adeguata.
Particolarmente, molte di queste piattaforme di scambio non eseguono degli adeguati controlli di identificazione della clientela.
Quindi il riciclatore, una volta entrato in possesso di valuta virtuale in modo anonimo, potrebbe trasferirla liberamente e anonimamente in paesi privi di regolamentazioni antiriciclaggio, creando una fitta rete di trasferimenti e convertirla in valuta fiat da reimmettere nel sistema. In alterativa i criminali potrebbero vendere beni e servizi illegali, come droghe e armi, in cambio di valuta virtuale per convertirla successivamente in valuta fiat da utilizzare per finanziare le proprie attività illecite.
Il terzo metodo per procurarsi delle valute virtuali è scambiandola direttamente con altri soggetti senza l'utilizzo di piattaforme di intermediazione. Infatti, è possibile accordarsi privatamente con altre persone, incontrarsi ed effettuare lo scambio tramite delle applicazioni che permettono di inviare direttamente le valute virtuali, anche in cambio di denaro contante, al wallet dell'altro soggetto. Esistono anche delle piattaforme d'incontro tra acquirenti e venditori, tra le quali:

- i *marketplace,* siti internet accessibili da chiunque;
- Siti web segreti che costituiscono il dark web e che sono accessibili solamente da determinati browser.

Su questo tipo di piattaforme è possibile acquistare bitcoin con i metodi di pagamento più disparati.
Ci soffermiamo su un fenomeno particolare che è quello del Dark Web, un mondo di siti nascosti, a cui è possibile accedere solamente tramite dei motori di ricerca particolari che non permettono il tracciamento dell'indirizzo IP.
Nei siti del dark web, tra le altre cose, è possibile trovare molti annunci per la compravendita di valute virtuali. Chiaramente questo tipo di compravendite, che potremo definire "nell'ombra", essendo accessibili a pochi e basandosi su sistemi che evitano il tracciamento, sono le migliori per mantenere l'anonimato. Sono questi i processi che, spesso, vengono utilizzate dai criminali specializzati per procurarsi valute virtuali in maniera anonima.

Sussiste anche una molteplicità di siti dove poter acquistare beni illegali come armi, droghe o dove è addirittura possibile assoldare dei sicari.
Infine, l'ultimo modo per procurarsi le valute virtuali è tramite degli ATM dedicati.
Questi funzionano come dei veri e propri ATM tramite i quali è possibile comprare valute virtuali fornendo l'indirizzo del proprio wallet. Il tipo di identificazione necessaria, alcune volte estremamente semplificata, varia a seconda dell'exchange a cui l'ATM appartiene e allo stato in cui si trova.
Per sola informazione, si segnalano altre valute virtuali quali: Ethereum, Ripple, IOTA, Litecoin, Bitcoin Cash e Monero. Tra queste risalta Monero che, per le sue caratteristiche di totale anonimato, risulta una moneta virtuale molto utilizzata per fini criminali.

LA V DIRETTIVA E LE PRINCIPALI NOVITA' RIGUARDANTI LE VALUTE VIRTUALI

Il 30 maggio 2018 è stata adottata la Quinta Direttiva antiriciclaggio UE 2018/843 del Parlamento Europeo e del Consiglio, che modifica la precedente Quarta Direttiva.
Analizziamo quali sono state le novità introdotte dalla nuova disciplina, focalizzandoci in *primis* sull'argomento trattato in questa tesi.
Come si evince dalle considerazioni iniziali del testo della Direttiva il legislatore europeo è ben conscio della problematica inerente alle valute virtuali. Tant'è che reputa possibile che, in assenza dell'obbligo per i servizi di valute virtuali di individuare le attività sospette, i gruppi terroristici possano utilizzarle per trasferire denaro. Basandosi sulle precedenti considerazioni la portata della Direttiva antiriciclaggio vengono inclusi tra i soggetti obbligati:

- i prestatori di servizi di cambio valute virtuali e valute aventi corso forzoso, ovvero gli exchange;
- i prestatori di servizi di portafoglio digitale;

Cosi facendo gli exchange e i wallet provider dovranno applicare, come già succede per le banche, i controlli di *due diligence* e i requisiti di adeguata verifica sulla propria clientela.
Inoltre, questi prestatori di servizi dovranno essere registrati, cosi come avviene già per i cambiavalute, ed altri soggetti.
In questo modo si cerca di porre fine al regime di anonimato associato alle valute virtuali.

Inoltre, viene abbassata la soglia di utilizzo delle carte prepagate anonime, oltre la quale i soggetti obbligati sono autorizzati a non applicare le misure di adeguata verifica della clientela. L'importo massimo che è possibile memorizzare passa da €250 a €150.
Questa misura è estremamente importante, in quanto le carte prepagate anonime sono considerate uno dei principali strumenti utilizzati nell'ambito del finanziamento del terrorismo.
Queste, infatti, possono essere caricate con denaro contante e trasportate agevolmente oltre confine, senza la necessità di dichiarare tale spostamento o che, ad esse, sia associato un determinato nominativo. In seguito, il denaro può essere ritirato dagli ATM del paese di destinazione, bypassando, di fatto, i controlli relativi all'uscita/entrata del denaro.
Per di più le carte prepagate sono uno strumento molto utilizzato anche negli scambi di criptovalute con valute fiat.
In ottica della lotta al finanziamento del terrorismo e con il fine di ampliare le fonti informative disponibili alle autorità competenti, la Direttiva ha rafforzato i poteri delle *Financial Intelligence Unit* (FIU) per ciò che concerne l'analisi domestica e la collaborazione internazionale. Il legislatore ha disposto che le FIU possano essere in grado di richiedere, ottenere ed utilizzare informazioni da qualsiasi soggetto obbligato, anche nel caso in cui non sia stata trasmessa una segnalazione di operazione sospetta, senza limitazioni derivanti da norme o procedure nazionali.
Inoltre, con il fine di migliorare la collaborazione tra le FIU e le autorità di vigilanza antiriciclaggio, viene rafforzata la capacità di collaborazione internazionale limitando, nel contempo, la capacità di rifiuto di collaborare. La collaborazione, infatti, non potrà essere negata adducendo come motivazione il collegamento con vicende fiscali, indagini o procedimenti penali.
Gli Stati membri sono tenuti ad uniformarsi alle disposizioni della direttiva entro il 10 gennaio 2020.

ITALIA: PROCESSI NORMATIVI IN ATTO

Sotto questo aspetto l'Italia risulta all'avanguardia rispetto agli altri paesi in quanto ha anticipato, con il D.lgs. 25 maggio 2017 n. 90 di recepimento della Quarta Direttiva antiriciclaggio, le disposizioni della Quinta Direttiva in ambito delle valute virtuali. Nello specifico, il legislatore nazionale ha chiarito che la valuta virtuale seppur utilizzata come mezzo di scambio per l'acquisto di beni e servizi non è emessa da una banca centrale o da un'autorità pubblica, non è necessariamente collegata ad una valuta avente corso legale.
Inoltre, ha introdotto nel nostro ordinamento gli obblighi di *due diligence* e di adeguata verifica della clientela a carico dei prestatori di servizi inerenti alle criptovalute, limitatamente a ciò che concerne la conversione di valute virtuali con valute aventi corso forzoso. Nello specifico gli exchange

dovranno applicare gli obblighi di adeguata verifica della clientela in occasione dell'istaurazione di un rapporto continuativo o anche nel caso dell'esecuzione di un'operazione occasionale, che comporti la trasmissione di un importo pari o superiore a €15.000.
Per altro, come ricordato dal comunicato n°22 del MEF del febbraio 2018, sussiste la necessità di comunicare, al predetto MEF, l'operatività dei prestatori di servizi relativi all'utilizzo di valute virtuali.
Per di più sono inclusi nell'obbligo di comunicazione anche gli operatori commerciali che accettano le valute virtuali come corrispettivo di qualsivoglia prestazione avente ad oggetto beni, servizi o altre utilità. L'iniziativa mira ad utilizzare una prima rilevazione sistematica del fenomeno a partire dalla consistenza numerica degli operatori del settore che, a regime, dovranno iscriversi in uno speciale registro tenuto dall'OAM, l'organismo degli agenti e dei mediatori, per poter esercitare la loro attività sul territorio nazionale.
Una puntualizzazione a parte, a mio avviso, merita il discorso della moneta elettronica, perché la stessa ben si presta a facilitare scambi tra denaro contabilizzato sul conto carta e la moneta virtuale.
Questo strumento, infatti, si presta a situazioni di lavaggio di denaro, ad esempio, sia ricaricando la carta in cambio della valuta virtuale, sia scambiando *brevi manu* le due monete.
Il legislatore, con l'intenzione di ingabbiare le modalità di emissione e di gestione delle carte, nel recepire la IV Direttiva ha già limitato l'avvaloramento della carta a €250 e probabilmente nei tempi previsti dalla V Direttiva lo ridurrà a €150.

GLI STRUMENTI DI CONTRASTO

In presenza di una varietà di processi tecnici estremamente evoluti, che se non governati lasciano spazio allo sfruttamento degli stessi da parte dei criminali, si rende necessario predisporre tutta una serie di monitoraggi e di accessi ai dati che riguardano la pluralità dei prodotti bancari o finanziari, soprattutto di fund transfert. A tal proposito nel predetto testo si sottolinea che devono poi essere normati il più possibile quegli strumenti di pagamento, come le carte prepagate, che sono entrati oggi nella disponibilità di tutti, che hanno il pregio di realizzare la c.d. inclusione finanziaria di soggetti che non sono "bancarizzabili", ma con le controindicazioni che abbiamo descritto in precedenza.
Per quanto riguarda le carte prepagate, nonché tutte le altre carte di pagamento, sussiste una normativa stringente che riguarda gli IMEL (Istituti di Moneta Elettronica), che impone un monitoraggio puntuale e dettagliato delle transazioni e dei rapporti, nel quale l'identificazione dei titolari e delegati deve diventare un *must.* A tal proposito risulta fondamentale la cooperazione internazionale.

Altresì, è fondamentale la collaborazione internazionale anche relativamente al fenomeno delle valute virtuali. Tant'è che la Quinta Direttiva prevede come strumento di contrasto la creazione di una banca dati centrale a disposizione delle FIU in cui vengano registrate le identità degli utenti e gli indirizzi dei portafogli.

Purtroppo, queste misure difficilmente potranno avere l'efficacia desiderata finché permarrà il fenomeno dei paesi che fanno dello *shadow banking* un elemento per attrarre capitali.

Questa criticità viene confermata da un report, presentato dal FAFT al G20 dei Ministri della Finanza e dei Governatori delle Banche Centrali nel luglio del 2018, che analizzava i presidi AML/TF con focus sulle valute virtuali. Il report prendeva in esame la situazione normativa antiriciclaggio interessandosi non solo delle legislazioni degli Stati del G20 ma anche di quelle di altri Stati rilevanti al fine dell'analisi.

Lo studio ha evidenziato che la maggior parte degli stati presi in analisi è in ritardo, dal punto di vista legislativo, per contrastare un fenomeno che travalica con facilità i confini fisici delle nazioni.

Nello specifico: ben 11 stati stanno ancora lavorando ad una regolamentazione in materia; 3 stati proibiscono l'uso delle valute virtuali, 2 segnalano solamente le transazioni sospette; solo 7 stati hanno regolamentato i prestatori di servizi di valute virtuali.

Inoltre, è opportuno ricordare che quest'analisi si focalizza solamente sugli stati principali del panorama internazionale. Si può supporre come la situazione dei presidi AML/CTF negli altri stati sia decisamente più debole, se non addirittura inesistente.

CONCLUSIONI

Lo scopo del presente elaborato, come evidenziato nell'introduzione, era quello di verificare se le normative vigenti fossero in grado di contemplare i vari fenomeni che girano attorno al crimine (per crimine si intende anche tutto quello che riguarda il terrorismo) e all'illegalità. Di fatto le prime 4 Direttive, di fronte ad una pluralità di fattispecie illegali e criminose, hanno attuato tutta una serie di provvedimenti ed hanno fornito indicazioni circa la collaborazione da attuare tra gli Stati membri, entrambi finalizzati a circoscrivere e limitare gli effetti di detti fenomeni. Le valute virtuali sono un fenomeno relativamente giovane che, vista la complessità dell'architettura informatica e la non facile identificabilità dei soggetti che intervengono nel sistema, forse deve essere ancora compreso nella sua interezza in modo da poterlo normare in ottica delle fattispecie di cui sopra.

Peraltro, va sottolineato come il mondo virtuale, e le criptovalute che in esso hanno ragione di sviluppo, cambia e si evolve molto più velocemente di quanto siano in grado di fare gli stati con normative puntuali e pressanti

Inoltre, bisogna ricordare che l'assenza di intermediari finanziari, cui potrebbero far capo le criptovalute, priva l'autorità di interlocutori disciplinabili dal punto di vista degli obblighi di segnalazione delle operazioni finanziarie. Anche le piattaforme che gestiscono le valute virtuali, spesso, non sono soggette ad obblighi normativi.
Questo insieme di fattori rendono il mondo delle valute virtuali un'opportunità per i criminali, sempre abili a sfruttare a loro vantaggio i buchi normativi e contesti finanziari non trasparenti.
Al momento, il legislatore europeo si limita, per quanto riguarda la lotta al riciclaggio, ad inserire i prestatori di servizi virtuali tra i soggetti obbligati alla *due diligence* e all'adeguata verifica della clientela.
Tuttavia, il fenomeno è talmente globale che lascia spazio a due importanti criticità.
In *primis*, l'operatività transnazionale tipica di questo mercato non può essere disciplinata tramite l'applicazione di norme nazionali/europee o internazionali (riguardante gli stati collaborativi) che sono limitate a confini territoriali ben delimitati, che invece il mondo virtuale non ha.
Infatti, come abbiamo analizzato nel corso della trattazione, le criptovalute si prestano con grandissima facilità a movimentazioni transnazionali di denaro. Per di più, i servizi di valute virtuali vengono forniti da *players* che risiedono nei punti più disparati del mondo.
Si rende quanto mai necessario, quindi, un lavoro di cooperazione internazionale e dialogo tra i vari stati o presidi internazionali per creare una disciplina di contrasto efficace che sia uniforme e condivisa.
Finché ci saranno stati non cooperativi come i paradisi fiscali o i c.d. stati canaglia sarà impossibile arginare in maniera effettivamente determinante il fenomeno del riciclaggio tramite le valute virtuali.
La seconda criticità, riscontrabile nella disciplina AML, nei confronti delle valute virtuali, riguarda il fatto che l'inclusione dei prestatori dei servizi di valute virtuali tra i soggetti obbligati non risolve completamente il problema dell'anonimato.
Questa problematica viene sollevata dalla Direttiva stessa che nel considerando n° 9 analizza che
"*poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato"*.
Ciò trova conferma in uno sviluppo esponenziale di un mercato nascosto dove i criminali possono effettuare i propri traffici illeciti in maniera del tutto anonima grazie all'utilizzo delle valute virtuali.
Il mercato virtuale di cui stiamo parlando è quello del dark web. Il dark web è una parte segreta del web che è accessibile solamente tramite determinati browser, che nascondono l'indirizzo IP dell'utente permettendogli di non essere localizzabile.
In questo modo è possibile accedere a degli indirizzi web segreti dove si effettuano compravendite di qualsiasi tipo. In questi siti è possibile acquistare armi, droghe, documenti d'identità e, come abbiamo visto, in uno dei capitoli precedenti, acquistare valute virtuali in modo anonimo.

La maggior parte di questi scambi viene effettuata o in bitcoin o in Monero rendendo queste transazioni completamente segrete, attraverso i meccanismi sopra delineati.
È importante sottolineare come questi traffici illegali effettuati sul dark web in assenza delle criptovalute, probabilmente, non avrebbero la stessa diffusione.
Peraltro, sempre nel dark web è possibile ottenere precise istruzioni su come "lavare" le valute virtuali possedute.
Si può, pertanto, concludere facendo un'amara constatazione: si stanno sviluppando delle situazioni, nel campo delle valute virtuali, che per le loro caratteristiche di complessità e globalizzazione, ben si prestano ad essere oggetto di attenzione da parte di coloro che hanno intenti criminali e/o illeciti.
L'augurio è che si pervenga ad una più stretta collaborazione tra le nazioni più importanti che porti a emettere normative puntuali e, soprattutto, condivise che forniscano alle autorità preposte gli strumenti necessari a contrastare il riciclaggio dei proventi ottenuti dalle attività criminali attraverso, soprattutto, l'utilizzo delle valute virtuali.
Forse la considerazione che fece Giovanni Falcone, circa la possibilità di individuare i mafiosi seguendo i flussi di denaro, oggi andrebbe riconsiderata alla luce di quanto abbiamo fin qui esposto.