DIPARTIMENTO DI ECONOMIA E FINANZA

Cattedra di Diritto dei mercati e degli intermediari finanziari

Criptovalute: le ragioni del successo ed il progetto di una *stablecoin* internazionale

Relatore:

Prof.ssa Mirella Pellegrini

Correlatore:

Prof.ssa Paola Lucantoni

Candidata:

Federica Andreotti

Matricola 692431

Anno accademico: 2018/2019

INDICE

INTRODUZIONE

‹‹Vince chi, preparato se stesso, aspetta di cogliere il nemico impreparato»[1].

Da queste poche pagine a scopo introduttivo si articola un lavoro di tesi volto ad analizzare le più intricate caratteristiche del criptomercato e le lacune normative all'interno delle quali queste ultime abilmente si districano. È chiaro che stiamo assistendo allo sviluppo di un fenomeno che entrerà a far parte del sistema economico sempre più prepotentemente, come è evidente l'assenza di un quadro normativo capace di gestirne il controllo. Ma per "contrattaccare" un fenomeno è fondamentale conoscerlo a fondo. Lo scopo di questo elaborato è esattamente quello di studiarne tutti gli aspetti per poi comprenderlo, e giungere infine alla risposta ottimale da parte del legislatore ed identificare i caratteri di una criptovaluta ideale.

Nel primo capitolo infatti, per approcciarci gradualmente all'oggetto di studio, ci limiteremo ad illustrare il funzionamento della tecnologia *blockchain* e gli attori chiave della comunità virtuale. In seguito capiremo com'è che le monete virtuali vengono emesse e suggeriremo alcuni indizi che distinguono una *Initial Coin Offering* vantaggiosa da una truffa. Per concludere questa fase preliminare di studio, proveremo ad individuare i vantaggi e le potenzialità che la *blockchain technology* apporterebbe all'intero sistema finanziario, ipotizzando infine 4 possibili scenari sul futuro della stessa, avvalorati e "promossi" dal parere di esperti del settore.

Il secondo capitolo invece, grafici alla mano, si appresta ad un'analisi prettamente finanziaria, utile a comprendere le ragioni del successo delle sei criptovalute più scambiate: tether, bitcoin, ethereum, litecoin, bitcoin cash, ripple. L'andamento del prezzo di ognuna ci aiuterà a capire quali sono i fattori che spingono il valore di una moneta virtuale verso l'alto per poi provocarne una brusca discesa nell'arco di pochi giorni. Identificheremo, di conseguenza, i motivi per cui gli utenti scelgono il mercato *crypto* come campo da gioco a fini speculativi, nonostante i 70 rischi individuati dall'EBA (Autorità Bancaria Europea). Supponendo che i soggetti scelgano di investire in criptovalute proprio perché poco consapevoli dei pericoli che rischiano di correre, dedicheremo l'ultimo paragrafo all'intervento europeo che si concretizza con

[1] Così S. TZU, *L'arte della guerra*, R. FRACASSO e W. MING (a cura di), Roma, Newton & Compton, 1994.

l'approvazione della V Direttiva antiriciclaggio, che per prima fornisce un'esatta definizione di "criptovaluta".

Per introdurre il terzo capitolo infatti, illustreremo le nuove e recenti modifiche della normativa antiriciclaggio partendo da una breve panoramica attraverso il susseguirsi delle cinque direttive, per chiudere con il più recente intervento normativo nelle vesti del Regolamento UE 2019/758, il quale prevede delle misure supplementari che gli enti creditizi e gli istituti finanziari devono adottare per mitigare il rischio di riciclaggio e di finanziamento del terrorismo, qualora operino in Paesi terzi. Nello specifico, capiremo quali vantaggiose e pericolose opportunità il sistema virtuale offre alle organizzazioni criminali che intendono riciclare denaro sporco e/o finanziare il terrorismo servendosi del criptomercato, riconoscendo nell'anonimato delle transazioni la principale problematica da risolvere con maggior urgenza. Infatti, nonostante l'Italia abbia anticipato le previsioni europee con il d. lgs. n. 90/2017, sono ancora tante le lacune che impediscono un'ottimale prevenzione dei rischi. Ipotizzeremo nell'ultimo paragrafo alcune soluzioni che potrebbero sanare le crepe normative.

Una volta completata la fase di studio del fenomeno, possiamo tentare, nell'ultimo capitolo, di sviluppare l'identikit di una criptovaluta ideale, che assorba i vantaggi, ma non presenti gli svantaggi, delle criptovalute tradizionali. Nel progettare ed identificare con precisione i caratteri di questa nuova moneta virtuale, ci accorgiamo di esser stati anticipati da uno degli uomini attualmente più potenti al mondo: Mark Zuckerberg ha annunciato, nel mese di giugno 2018, il lancio di Libra, la criptomoneta di Facebook. Libra presenta molte delle caratteristiche che la criptovaluta ideale deve avere, ma non gode di una solida struttura normativa sulla quale atterrare. Attraverso un'analisi *swot* proveremo ad individuare i punti di forza e le opportunità, e cercheremo di capire come aggirare le debolezze e vanificare le minacce.

1. CRIPTOVALUTE: DEFINIZIONE E RISCHI

1.1 Cos'è una criptovaluta ed il meccanismo P2P

Il settore finanziario, con particolare riferimento alle modalità di scambio di beni, servizi e ogni attività finanziaria, sta subendo un cambiamento radicale che procede, non a caso, di pari passo con i progressi della crittografia, ovvero lo strumento che permette di rendere un messaggio intellegibile solo a persone autorizzate[2]. Tra le applicazioni della digitalizzazione che hanno generato un maggior impatto sul settore finanziario, risalta senza dubbio la nascita della "criptovaluta", o "valuta virtuale". L'espressione "criptovaluta", letteralmente "valuta nascosta", testimonia e conferma la possibilità di utilizzarla solo se a conoscenza di un determinato codice di accesso. A differenza di come siamo, o forse sarebbe meglio dire eravamo, abituati ad identificare e maneggiare la moneta nella nostra quotidianità, la criptovaluta non esiste in forma fisica: si scambia unicamente in via telematica. Tanti concetti tradizionalmente utilizzati per le monete a corso legale vengono adattati al contesto: per la moneta virtuale non si parla più di "portafoglio", bensì di "*e-wallet"*.

Il più lontano antenato della criptovaluta è *eCash*, frutto della mente matematica di David Chaum[3], un sistema di pagamento ideato per inviare e ricevere moneta elettronica in modo anonimo e sicuro. Attraverso il nuovo software, l'utente poteva utilizzare denaro in formato digitale firmato crittograficamente da una banca americana, la Mark Twain di Saint Louis, che ha usufruito di questo sistema per i micropagamenti dal 1995 al 1998, fino a quando la banca venne acquistata da Merkantile Bank, grande emittente di carte di credito, strumento che di fatto fa venir meno l'utilità del software di Chaum. Per l'appunto, in Europa, dove le transazioni in contanti erano di gran lunga preferite alle carte di credito, istituire un sistema digitale di micropagamento avrebbe avuto, a mio parere, molto più senso. È infatti giugno del '98 quando *eCash* è disponibile in Svizzera attraverso il Credit Suisse, presso la Deutsche Bank in Germania, UniCredit Bank Austria AG, Posten AB (servizio postale svedese), e presso la Den Norsken Bank in Norvegia.

[2] Sul punto si veda Consob.it, *Le criptovalute*, www.consob.it/web/investor-education/criptovalute.
[3] Per approfondimenti si rinvia D. Chaum, *Blind signature for untraceable payments*, in R. L. Rivest e A. T. Sherman (eds), *Advances in cryptology: proceedings of crypto 82,* Springer book archive, 1983, pp. 199 – 203.

Nonostante le grandi potenzialità del nuovo strumento, DigiCash, la società avviata da Chaum nel 1990 con *eCash* come marchio di fabbrica, fallisce nel 1998: la carta di credito rimane la "*currency of choise*[4]", la valuta preferita. «*As the Web grew, the average level of sophistication of users dropped. It was hard to explain the importance of privacy to them*»[5]. Il padre di *eCash* colpevolizza, per il suo fallimento, la mancata capacità degli utenti di dare alla privacy l'importanza che merita, sottovalutando un sistema di pagamento che permetteva di fare acquisti senza dover necessariamente aprire un conto con il fornitore o trasmettere numeri di carte di credito.

Sono trascorsi ormai dieci anni quando colui che preferisce essere chiamato Satoshi Nakamoto, ma di cui tutt'ora non si conosce l'identità, pubblica un nuovo protocollo in cui illustra un sistema di pagamento elettronico *peer-to-peer* attraverso una nuova criptovaluta, ad oggi la più famosa al mondo: il bitcoin[6]. Con il termine "*peer-to-peer*", che sta per "rete paritaria", si intende una rete di *personal computer*, detti "nodi", che interagiscono in modo diretto condividendo risorse multimediali in assenza di *server* intermediari. Questa architettura si oppone per la prima volta ai servizi *client-service*, dove le comunicazioni dei vari clienti sono indirizzate ad un'unica entità centrale.

Le funzioni principali di questo nuovo meccanismo decentralizzato sono tre: *discovering*, cioè la scoperta diretta di nuovi *peer*; sharing, condivisione diretta di *file* all'interno di una rete; *querying*, richiesta diretta di contenuti ad altri *peer*.[7] ‹‹La rete *peer to peer* permette potenzialmente a qualsiasi utente di trasferire soldi a velocità quasi istantanea a bassissimo o senza alcun costo (…)[8]». Un esempio pratico di transazione che utilizza la modalità *peer to peer* è stata da poco adottata da Poste Italiane, sintomo che l'assenza di intermediari può senza dubbio attirare l'attenzione degli utenti: da poco più di tre anni è possibile trasferire denaro da una carta *postepay* all'altra semplicemente attraverso l'applicazione da scaricare sul proprio *smartphone*. L'unico dato necessario è il numero di telefono dell'utente a cui si vuole inviare o chiedere l'importo; il trasferimento non richiede commissioni per una somma inferiore o uguale a € 25. Si tratta di una modalità che riduce di gran lunga i tempi, i costi, che

[4] Così J. PITTA, *Requiem for a bright idea*, 1999, www.forbes.com
[5] Cfr. J. PITTA, *Requiem for a bright idea,* 1999, www.forbes.com
[6] Per approfondimenti si veda S. Nakamoto, *Bitcoin: a peer-to-peer electronic cash system*, ottobre 2008, www.cryptovest.co.uk.
[7] Sul punto si veda P. CELLINI, *La rivoluzione digitale*, Luiss University Press, 2018, Roma, pp. 330 – 331.
[8] Cfr. S. CAPACCIOLI, *Criptovalute e bitcoin: un'analisi giuridica*, Giuffrè editore, Milano, 2015, cit a p. 254.

permette di concludere una transazione senza dover necessariamente conoscere dati personali o il numero di carta della controparte: un sistema senz'altro di successo che rappresenta un traguardo dell'innovazione finanziaria.

Il nuovo protocollo di Nakamoto, che risponde a delle regole proprie[9], si avvale di una tecnologia inedita, la *blockchain technology*, che non prevede infatti l'intervento di intermediari (banche o altre istituzioni finanziarie) per far sì che gli utenti possano scambiarsi denaro in modo sicuro e diretto allo stesso tempo.

1.2 Principali caratteristiche

La moneta virtuale è stata definita dalla BCE come «una rappresentazione di valore digitale che non è né emessa da una banca centrale o da un ente pubblico né è necessariamente legata a una valuta legale, ma è accettata da persone fisiche e giuridiche come mezzo di pagamento e può essere trasferita, memorizzata o scambiata elettronicamente»[10]. Al fine di evidenziare i possibili rischi derivanti dall'utilizzo di criptovalute, la Banca d'Italia ne individua le principali caratteristiche[11]:

- vengono create da un emittente privato secondo regole proprie alle quali i membri della comunità scelgono di aderire;
- non sono fisicamente detenute dall'utente, il quale possiede un *e-wallet* (c.d. portafoglio elettronico) al quale si accede tramite *password*. Questi portafogli sono, di fatto, dei *software* sviluppati da soggetti qualificati, quali i *wallet providers*. In un secondo momento è possibile, in alcuni casi, convertire la valuta digitale in moneta legale e viceversa attraverso piattaforme di scambio;

[9] Così D. KNEZEVIC, *Impact of blockchain technology in chanching the financial sector and other industries*, marzo 2018, Montenegrin Journal of Economics.

[10] Cfr. Banca Centrale Europea, *Parere della Banca Centrale Europea su una proposta di direttiva del Parlamento europeo e del Consiglio che modifica la Direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica la Direttiva 2009/10/CE*, ottobre 2016, Gazzetta Ufficiale dell'Unione europea, paragrafo 1.1.3. La definizione sembra basarsi su quella proposta al paragrafo 19 dell'«*Opinion on virtual currencies*» dell'Autorità bancaria europea del 4 luglio 2014 (EBA/Op/2014/08) disponibile sul sito Internet dell'ABE all'indirizzo www.eba.europa.eu

[11] Per approfondimenti si rinvia a A. CAPONERA e C. GOLA, *Aspetti economici e regolamentari delle "cripto-attività"*, in Banca d'Italia (a cura di), *Questioni di Economia e Finanza (occasional papers)*, marzo 2019, www.bancaditalia.it.

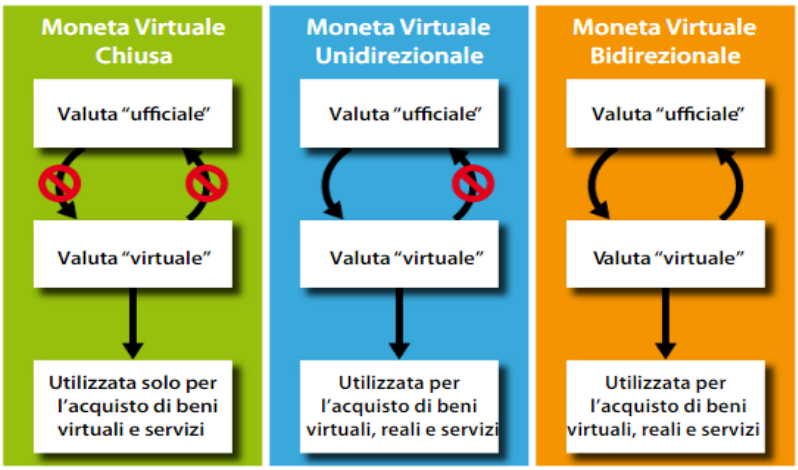
- i titolari dei portafogli elettronici mantengono l'anonimato;
- la transazioni che hanno per oggetto il trasferimento di moneta virtuale sono tecnicamente irreversibili, pertanto non è mai possibile chiederne l'annullamento;
- la criptovaluta non ha corso legale, possono essere utilizzate per l'acquisto di beni e servizi solo se l'*accipiens* è disponibile ad accettarla.

È inevitabile che tali caratteristiche comportino, intrinsecamente, dei rischi. Il fatto che ogni utente, sulla base di regole proprie, possa creare una nuova moneta virtuale lascia spazio ad una concorrenza senza freni, ma soprattutto un gioco senza regole può trarre facilmente in inganno quegli investitori che non padroneggiano il criptomercato. Essendo inoltre un sistema interamente virtuale, è cruciale il rischio di consegnare tutto il nostro *wallet* nelle mani di potenziali *hackers*. Per questo non bisognerebbe mai investire più di quanto ci si possa permettere di perdere[12]. Tuttavia, un aspetto ancora più critico risiede nell'anonimato delle transazioni, caratteristica che senza dubbio attira l'attenzione di organizzazioni criminali[13].

È inoltre possibile suddividere le monete virtuali in tre macro-tipologie, sulla base della loro interazione con la moneta legale[14]:

1. valuta virtuale non acquistabile, "non convertibile" o "chiusa", perché non prevede la possibilità di essere convertita in moneta con corso legale e pertanto utilizzabile solo all'interno dei confini della comunità virtuale;
2. valuta a "convertibilità limitata", può essere acquistata con moneta tradizionale, ma non può essere a sua volta riconvertita nuovamente in moneta avente corso legale;
3. valuta "pienamente convertibile", può essere acquistata e rivenduta in cambio di moneta tradizionale.

[12] Cfr. S. CAVALLI, *Tradying crypto: 5 cose da evitare se si trada con Bitcoin e non solo*, luglio 2019, www.cryptonomist.ch.
[13] Analizzeremo questo aspetto con maggiore attenzione nel terzo capitolo.
[14] Si veda European Central Bank, *Virtual currency schemes*, ottobre 2012, p.16, www.ecb.europa.eu.



Fonte: http://www.telecomitalia.com/tit/it/notiziariotecnico/2014-01/capitolo-06.html

Nello specifico, la differenza tra criptovaluta e moneta tradizionale risiede nell'incapacità della valuta virtuale di adempiere alle tre funzioni proprie di una valuta ufficiale: unità di conto, mezzo di pagamento e riserva di valore. La funzione di unità di conto della criptovaluta viene intuitivamente meno dal momento in cui i prezzi delle stesse sono soggetti a fluttuazioni ampie, anche all'interno di una stessa giornata. Il mancato corso legale non permette inoltre di considerare la moneta virtuale un utile mezzo di pagamento. Infine, per quanto riguarda la funzione di riserva di valore, bisogna tener presente che il numero di unità di criptovaluta che possono essere prodotte è limitato, pertanto più numerose saranno le transazioni regolate in criptovalute, maggiore sarà il loro valore. È di conseguenza improbabile che le monete virtuali vengano utilizzate come riserva di valore.

Dopo aver sottolineato gli aspetti che distinguono la criptovaluta dalla valuta ufficiale, bisogna prestare attenzione nel non confonderla con la moneta elettronica. I requisiti di quest'ultima, sono minuziosamente riportati nell'articolo 1, par. 3, lettera b, della Direttiva 2000/46/CE, ‹‹riguardante l'avvio, l'esercizio, e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica». Essa è definita come ‹‹un valore monetario rappresentato da un credito nei confronti dell'emittente che sia:

1. memorizzato su un dispositivo elettronico;
2. emesso dietro ricezione di fondi il cui valore non sia inferiore al valore monetario emesso;
3. accettato come mezzo di pagamento da imprese diverse dall'emittente».

In conclusione, sembra essere più corretto classificare le valute virtuali come un "bene", di cui all'art. 810 c.c., intendendosi qualunque cosa, sia essa materiale o

immateriale, idonea a soddisfare un'utilità o una necessità dell'uomo, o ancora come possibilità di subire espropriazione e della limitatezza e che, in quanto tale, rappresenti oggetto di diritti[15].

1.3 Attori chiave della comunità virtuale

Una seconda e più approfondita analisi svolta dalla Banca Centrale Europea[16], distingue i diversi servizi resi dai principali attori della comunità virtuale sulla base della natura degli stessi.

- Gli ***inventors***, con identità nota o in alcuni casi sconosciuta, sono coloro che creano la nuova valuta virtuale e sviluppano la parte tecnica della rete, volta al mantenimento e miglioramento delle caratteristiche tecniche della valuta, incluso l'eventuale algoritmo.

- I ***miners*** si occupano, spesso lavorando in gruppo, di convalidare le transazioni affinché il nuovo blocco formatosi venga aggiunto alla *blockchain*, attraverso la risoluzione di complessi calcoli matematici. Il loro contributo risulta fondamentale per mantenere attiva la catena, e per questo ricevono, per ogni blocco generato, una ricompensa in criptomoneta, per un importo che va dimezzandosi ogni quattro anni. Le monete ricevute potranno poi essere vendute sul mercato. In assenza della figura dei minatori, non sarebbero rare operazioni con intento fraudolento, spese doppie o unità false. In virtù del loro prezioso contributo, sono autorizzati a chiedere una commissione di transazione da coloro che scelgono di avviarla.

- Gli **utenti** entrano a far parte della comunità virtuale con lo scopo di ottenere criptovaluta utile all'acquisto di beni e servizi reali o virtuali dai commercianti

[15] Per approfondimenti si rinvia S. GALMARINI, *Antiriciclaggio*, Wolsters Kluwer, 2019, Milano, p. 748.
[16] Cfr. European Central Bank, *Virtual Currency schemes – a further analysis*, febbraio 2015, www.ecb.europa.eu.

disposti ad accettarla, utile per effettuare pagamenti da persona a persona o a fini di investimento. L'utente ottiene unità di valuta virtuale attraverso:

1. l'acquisto;
2. l'impegno in attività premiate con unità di valuta virtuale (es. partecipazione ad attività promozionali);
3. auto-generazione di moneta, o "*mining"* (in questo caso l'utente è un *miner*);
4. vendita di beni e servizi virtuali e reali contro pagamento in valuta virtuale;
5. ricevere criptovaluta a titolo di donazione.

- I ***wallet providers*** avviano e forniscono agli utenti un portafoglio digitale in cui archiviare le chiavi crittografiche[17] di valuta virtuale ed i codici di autenticazione delle transazioni, ordinate cronologicamente.

- Gli ***exchangers*** sono coloro che quotano i tassi di cambio a cui acquistare e vendere valuta virtuale contro le principali valute a corso legale e contro altre valute virtuali. Per di più sono autorizzati a fornire statistiche, *wallet* e servizi di conversione ai commercianti che accettano la criptovaluta come mezzo di pagamento.

- Le **piattaforme di *trading*** rappresentano *l'alter ego* dei mercati ufficiali, mettendo in contatto gli acquirenti ed i venditori di criptovalute senza però fungere da strumento di intermediazione. Le piattaforme, a differenza degli *exchangers*, non acquistano/vendono in proprio ed in alcuni casi offrono solamente la possibilità di individuare potenziali controparti per poi realizzare lo scambio di persona[18].

[17] Ogni utente dispone di una chiave privata ed una chiave pubblica. Ne analizzeremo in seguito le funzioni.

[18] Sul punto si veda S. GALMARINI, *Antiriciclaggio*, Wolsters Kluwer, 2019, Milano, pp. 746-747.

1.4 Initial coin offering

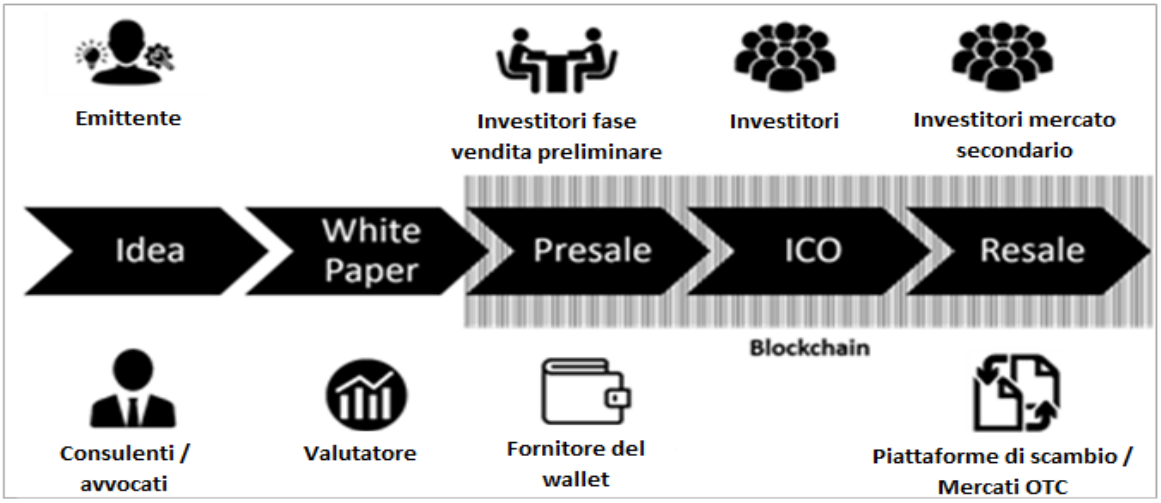
1.4.1 Definizione e struttura

Prima di essere acquistate o vendute su una piattaforma di scambio, le valute virtuali vengono emesse attraverso un meccanismo strutturalmente simile all'*Initial Public Offering* (IPO) e all'*equity corwdfunding*[19] ma che, a differenza di questi ultimi, prevede l'emissione di *coin* o *token*[20] digitali al posto dei tradizionali strumenti finanziari: *l'Initial coin offering* o ICO. Gli investitori acquistano i *token* contro valuta ufficiale (EUR, USD, YEN ecc.) oppure contro criptovalute (generalmente Bitcoin o Ether)[21]. Tale strumento rappresenta di fatto una forma di finanziamento richiesta da soggetti che intendono realizzare un determinato progetto che sarà realizzato tramite *Blockchain*. Strutturalmente il meccanismo riproduce le fasi di un processo di finanziamento utile ad una fase di lancio di una nuova realtà imprenditoriale di piccole dimensioni alla ricerca di finanziatori.

- **FASE 1** - IDEA: elaborazione di un progetto innovativo da sviluppare;
- **FASE 2** – WHITE PAPER: redazione e pubblicazione sul web di un documento informativo non standardizzato che specifichi emittente, progetto e informazioni utili su *token* e criptovaluta in oggetto[22];

- **FASE 3** – OFFERTA: utilizzo della *Blockchain* per il coinvolgimento degli investitori sul mercato primario e, ove previsto, secondario.

[19] L'attività di *equity corwdfunding* è disciplinata dal regolamento Consob ‹‹Regolamento sulla raccolta di capitali di rischio tramite portali online», adottato con delibera n. 18592 del 26 giugno 2013.
[20] Rappresentazione digitale di qualsiasi bene o funzione.
[21] Dati forniti da Consob.it, *Le criptovalute,* www.consob.it/web/investor-education/criptovalute.
[22] Analizzeremo il contenuto del *whitepaper* nel paragrafo successivo.



FONTE: www.consob.it

Nello specifico, lo strumento utilizzato su *blockchain* è lo *smart contract*, introdotto dalla piattaforma Ethereum[23]. Si tratta di un programma informatico concordato dalle controparti dalla duplice funzione: da un lato illustra l'accordo tra le parti, dall'altro attua automaticamente ciò che l'accordo prevede. È, di fatto, un contratto autoeseguibile[24]. Attraverso questo strumento, una volta che l'investitore invia alla società la criptovaluta richiesta, riceve nel suo *e-wallet*, precedentemente fornito nella fase "*pre-sale*", un numero predeterminato di *token*.

1.4.2 Un esempio di ICO: PayPro

La pagina principale del sito web relativo ad una specifica ICO riporta tutte le informazioni necessarie[25]:

- **PERIODO**, più una precisazione sul "sottoperiodo" che prevede il bonus. Nel caso in esame, l'ICO copre un periodo che va dall'8 gennaio al 4 febbraio 2018,

[23] Piattaforma decentralizzata per la creazione e pubblicazione *peer-to-peer* di *smart contracts*.
[24] Sul punto si veda G. SARTOR, *L'informazione giuridica e le tecnologie dell'informazione*, Giappichelli editore, 2010, Torino, p. 203.
[25] Per approfondimenti si rinvia a R. DINALE, *Guida completa alle ICO*, gennaio 2018, www.medium.com.

ma godono del bonus solo gli investitori che scelgono di finanziare PayPro entro il 15 gennaio;

- **INVESTIMENTO MINIMO** per poter prendere parte all'ICO, 15 ETH, cioè Ether, nel caso in esame. Al momento dell'offerta corrispondono a $ 20 000;

- **BONUS**, tendenzialmente decrescente, come incentivo immediato. Nel caso di PayPro è pari al 35% nella prima settimana, per poi scendere progressivamente fino ad annullarsi;

- **TASSO DI CAMBIO** tra valuta richiesta e *token*, nel caso in esame 1,48 nella prima settimana. Ciò vuol dire che 15 ETH, pari all'investimento minimo, equivalgono a 10,125 PYP (*token* del PayPro). Considerando che il valore di 15 ETH equivale a $ 20 000, è facile calcolare il valore di un *token*, pari a $ 1.92;

- **REGISTRAZIONE**: molte imprese richiedono l'iscrizione in una *whitelist*, prima di poter procedere con l'investimento, in modo da conoscere i propri clienti e ridurre il rischio di riciclaggio del denaro (*Know your costumer and anti-money laundering – KYC & AML*).

Periodo e relativo bonus dell'ICO PayPro, FONTE: https://medium.com/cryptoitalia

1.4.3 Come distinguere una buona ICO da una truffa?

Nonostante una maggior regolamentazione internazionale[26] e una più minuziosa educazione del mercato, è sempre bene affidarsi al cosiddetto *Do Your Own Research*, or *DYOR*, per essere in grado autonomamente di percepire segnali e allarmi che potrebbero ricondurre ad una truffa. Il primo elemento da esaminare è il *Whitepaper*: questo documento dovrebbe essere senza dubbio esaustivo, immediatamente disponibile, ma soprattutto, trattandosi di un documento prettamente tecnico, non dovrebbe essere strumento di marketing pubblicizzando attività promozionali. Esso rappresenta e quantifica la professionalità di chi sta lavorando al progetto che si intende finanziare. In secondo luogo, è utile controllare la presenza di una *Whitelist;* se presente, l'impresa intende evitare qualsiasi iniezione di capitale sporco. Osservazione numero tre: occhio al bonus! Se quest'ultimo, al fine di "premiare" gli investitori che scelgono di assumere un maggior rischio, è tendenzialmente alto, potrebbe rappresentare un grande svantaggio per gli ultimi arrivati. Se il bonus della prima settimana è uguale o supera, ad esempio, il 50 % del tasso di cambio, i primi investitori avranno dei margini più che superiori rispetto ai successivi. Questo incentiverà i primi a vendere in massa per ottenere un profitto facile e sicuro, ma senza passare inosservato: la vendita di massa farà sì che l'offerta superi di gran lunga la domanda, generando un'inevitabile riduzione del prezzo, danneggiando gli investitori successivi. Durante la *DYOR*, entra in gioco anche l'*hard cap,* un limite al finanziamento, riportato nel *whitepaper*. Se un progetto è valido, la squadra al lavoro è in grado di valutare l'ammontare dei fondi necessari e, di conseguenza, stabilire un limite massimo. Nel caso di PayPro, tale limite non era stato fissato. Inoltre, è da non sottovalutare l'opportunità di conoscere i membri del *team*. La possibilità di consultare l'identità di ogni singolo membro sulla pagina web dell'impresa è una condizione necessaria, ma non sufficiente, per poter procedere con l'investimento. Fondamentale è inoltre il contributo di una *Roadmap:* un'attenta e chiara pianificazione non può che essere un forte segnale di garanzia, punto di forza dell'ICO di PayPro, la cui veridicità delle informazioni è stata verificata sul web.

[26] La regolamentazione nazionale sarà oggetto del paragrafo successivo.

FONTE: https://medium.com/cryptoitalia

Bisogna poi conferire il giusto peso alla comunicazione e confronto con l'utente finale attraverso i più noti strumenti, tra cui: Facebook, Twitter, Slack, Discord, Telegram, Reddit, BitcoinTalk, Medium[27]. Maggiore è la comunicazione, maggiore la credibilità.

1.4.4 Il quadro regolamentare

Relativamente alle ICO, la mancanza di un quadro regolamentare specifico soffre un confine labile con l'incertezza circa l'applicabilità delle varie discipline vigenti in campo di *securities* e IPO. Il quadro regolamentare poco chiaro ha di fatto favorito la proliferazione delle ICOs a livello mondiale, raccogliendo, solo nel 2017, un importo

[27] Così R. DINALE, *Guida completa alle ICO*, gennaio 2018, www.medium.com.

pari a 5,68 miliardi di dollari, un successo che non a caso procede di pari passo con l'incremento di valore delle principali criptovalute: Bitcoin + 1.318 % vs USD, Ether + 9.162 % vs USD[28]. Nonostante l'alto grado di incertezza, è però possibile tentare di ricostruire la disciplina nazionale attualmente applicabile in base alla tipologia dei diritti che l'acquisto di *token* conferisce all'investitore[29].

1. ***TOKEN* DI CLASSE 1**: in questo caso il *token* non conferisce diritti nei confronti di una controparte, ma ha la mera funzione di assicurare un diritto di proprietà sul *token* stesso. Da qui la possibilità di riferirsi alla modifica recente della disciplina antiriciclaggio che, con il d.lgs. 25/5/2017, n. 90, ha modificato il precedente d.lgs. n. 213/2007 definendo la "valuta virtuale" come ‹‹la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente» alla lettera qq) dell'articolo 1, primo comma. Tale modifica permette di applicare le norme previste dal decreto ai ‹‹prestatori di servizi relativi all'utilizzo di valuta virtuale, limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso». Alle suddette condizioni, nel momento in cui un *exchange* inizia ad operare in Italia ha l'obbligo, ad esempio, di iscriversi nell'elenco di cambia valute (art. 17 bis, comma 8 bis del decreto legislativo 13 agosto 2010, n. 141), ed è chiamato ad applicare la normativa antiriciclaggio sia per quanto concerne l'attività di verifica della clientela, sia per quanto riguarda la segnalazione di operazioni sospette[30]. Il fatto che il contributo di tali soggetti, tanto quello dell'*exchanger* quanto quello del *wallet provider*, sia particolarmente utile, ma non strettamente necessario, evidenzia delle lacune in merito all'attuale normativa.

2. ***TOKEN* DI CLASSE 2**: questa tipologia di *token* conferisce all'investitore diversi diritti nei confronti del soggetto emittente e/o soggetto terzo. Tale caratteristica ci obbliga a definire delle sottoclassi:

[28] Dati forniti da Consob.it, *Le criptovalute, www.consob.it/web/investor-education/criptovalute*.
[29] Per approfondimenti si rinvia a M. NICOTRA, *ICO Initial Coin Offering: una ricostruzione giuridica del fenomeno*, marzo 2019, www.blockchain4innovation.it.
[30] Analizzeremo nel terzo capitolo le criticità di tale normativa.

- ***Token* di classe 2a**, rappresentativo di *assets*, e che conferisce pertanto il diritto ad un pagamento specifico o a pagamenti futuri. Potremmo classificare tali *assets* nella categoria di valori mobiliari, strumenti finanziari o come strumento partecipativo al capitale di rischio. In questo caso risulterà necessario applicare le norme del diritto societario, la normativa prevista dal TUF e le norme inerenti all'appello pubblico del risparmio, con particolare riferimento alla direttiva Mifid e regolamento Consob n 11971/1999, aggiornato con le modifiche apportate con delibera n. 21016 del 24 luglio 2019, in vigore dal 6 agosto 2019. Gode di particolare attenzione però, il *token* che rappresenta uno strumento partecipativo al capitale di rischio. In questo specifico caso, una ICO attraverso *exchange* potrebbe non risultare conforme alla legge italiana prevista per l'*equity crowdfunding* basata sul decreto legge n 179/2012 e sul regolamento Consob n. 19520/2013. Entrambe le normative stabiliscono che si può ricorrere a tale forma di raccolta solamente in favore di *startup* o imprese innovative a patto che i portali *online* siano gestiti da soggetti iscritti in un apposito albo detenuto dalla Consob. Qualora invece il *token* rappresenti un *asset* non classificabile come strumento finanziario è necessario verificare che non si ricada nella disciplina del pubblico risparmio[31], attività riservata esclusivamente alle banche;

- ***Token* di classe 2b**, rappresentativo di *assets* diversi dagli strumenti finanziari o che conferisce diritti sulla prestazione di un servizio o su un bene, anche immateriale. Di fatto, durante la *Initial coin offering*, vengono proposte varie formule vantaggiose per gli acquirenti, solitamente si tratta di una riduzione dell'importo dovuto per la prestazione di un servizio o l'utilizzo di un bene. Parliamo di una vera e propria offerta al pubblico, ex art.1336 c.c., che rende difficile inquadrare il contratto in una tipica fattispecie, ed assume per lo più il carattere di negozio misto, regolato autonomamente dalle parti. Sarà inoltre applicabile la disciplina prevista

[31] Acquisizione di fondi tra il pubblico con obbligo di rimborso.

dal Codice del Consumo (d.lgs. 6 settembre 2005, n. 206) oltre alle singole normative identificate sulla base della specifica prestazione oggetto del contratto;

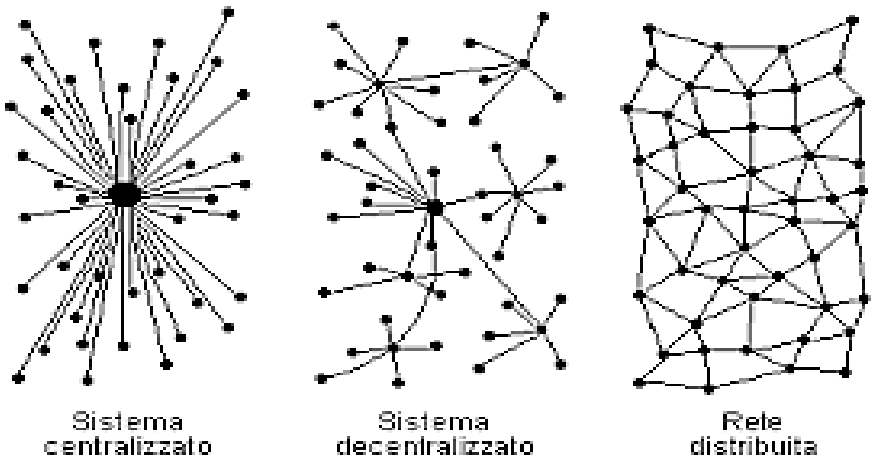
3. ***TOKEN* DI CLASSE 3**: questa tipologia conferisce all'investitore un diritto di comproprietà, nel senso che gode di diritti di proprietà su una piattaforma di *smart contracts* e che non sono rivolti verso l'emittente, bensì gestiti dalla piattaforma stessa. All'investitore, ad esempio, può essere riconosciuto un compenso economico in virtù dell'utilizzo della piattaforma da parte di terzi. Dato che questa fattispecie ha come oggetto un bene indiviso, quale la piattaforma, su cui il titolare esercita i propri diritti congiuntamente ad altri, non può che essere riconducibile alla fattispecie della comunione. Tale disciplina stabilisce infatti, nel diritto privato, che ogni comunista ha il diritto di usufruire del servizio o di utilizzare il bene nella sua interezza e in qualsiasi momento, a patto che non ne modifichi la destinazione e che non impedisca agli altri comproprietari di farne lo stesso utilizzo[32].

1.5 Distributed ledger e *blockchain*

Ognuno di noi possiede dei beni, siano essi materiali, come denaro o proprietà, o immateriali, come diritti o dati personali (raccolti in una cartella clinica, ad esempio). Attualmente ci affidiamo ad enti terzi per memorizzare e trasmettere i nostri beni: banche, agenzie o *social media companies.* Depositiamo il nostro denaro nelle banche, incaricandole di effettuare e ricevere pagamenti per nostro conto. Ciò è possibile perché il sistema finanziario fornisce gli strumenti tecnici per trasferire denaro limitando, quanto più possibile, la possibilità di frode. Usufruire di questi servizi però, non è gratuito, tantomeno immediato: molte operazioni richiedono giorni per essere completate. Per di più, i dati memorizzati in modo centralizzato rappresentano una calamita per i pirati informatici. I nostri dati personali, forniti a terzi autorizzati ad

[32] Così A. CONCAS, *La comunione, in che cosa consiste e che cosa comporta*, marzo 2018, www.diritto.it.

effettuare le transazioni di cui abbiamo bisogno, potrebbero essere utilizzati a nostro danno[33]. Una "sorveglianza invasiva" è il prezzo da pagare per poter usufruire di determinati servizi. C'è un'alternativa? Un sistema digitale noto come *distributed ledger technology* o *DLT* potrebbe avere la soluzione. È progettato per consentire agli utenti di archiviare i propri dati in modo sicuro ed inviarli direttamente al destinatario, rendendo vano l'intervento di intermediari, ma soprattutto tenendo traccia in ogni momento di chi detiene cosa. Tutto ciò è possibile grazie al principio di decentramento, che non prevede la necessità di raccogliere dati presso un *database* centrale, ma diffonde copie a tutti gli utenti della comunità virtuale, in modo che ognuno abbia un quadro completo di cosa accade. Gli utenti, detti "nodi", sono connessi tra loro in una rete distribuita.



www.consob.it/web/investor-education/criptovalute

Una modifica, prima di essere convalidata, deve essere verificata ed accettata da tutti gli utenti. Il più noto sistema *DLT* è la *blockchain*[34], progettata per prevenire la manomissione dei dati. I blocchi di dati convalidati, sono collegati in ordine cronologico attraverso una catena crittografata. Ogni blocco, identificato da un codice, contiene le informazioni relative ad un insieme di transazioni più il codice del blocco

[33] Il trattamento dei dati personali e della privacy è disciplinato dal regolamento (UE) n. 2016/679, meglio noto con la sigla GDPR (*General Data Protection Regulation*).
[34] Così G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, Giappichelli editore, 2010, Torino, a p. 200.

precedente, in modo da poter ripercorrere la catena retroattivamente. Qualora uno degli utenti cerchi di modificare un blocco di dati, tutti possono vedere quello che sta accadendo. Nella pratica, i dati non possono essere retroattivamente alterati senza la conseguente modifica di tutti i blocchi successivi, a meno che non si abbia, se il protocollo lo prevede, la maggioranza della rete. Le componenti basilari di questo inedito modello tecnologico risultano quindi essere:

- i **nodi**, fisicamente i *server* di ciascun partecipante alla catena;
- le **transazioni**, i valori di "scambio" da verificare, approvare e archiviare nel registro;
- i **blocchi**, "baule" di un insieme di transazioni;
- il ***ledger,*** il registro pubblico nel quale vengono annotate irreversibilmente tutte le transazioni oggetto della *blockchain*, tra loro incatenate tramite la crittografia;
- l'***hash***, operazione non invertibile che permette di ‹‹mappare un codice alfanumerico di lunghezza variabile in una stringa unica ed univoca di lunghezza determinata»[35]. Tale operazione identifica ogni blocco in modo univoco e sicuro senza dover necessariamente risalire al testo che lo ha generato. Di fatto genera un'impronta digitale per ogni blocco.

1.5.1 Funzionamento della *blockchain* e regole da seguire

Il trasferimento si svolge come segue[36]: se il soggetto X intende inviare 2 bitcoin al soggetto Y, X predisporrà un messaggio, nel linguaggio del software Bitcoin, che illustra con esattezza l'oggetto della transazione (2 bitcoin), il destinatario (Y), il mittente (X), e il precedente proprietario dell'oggetto della transazione. (Es. X trasferisce a Y 2 bitcoin, ottenuti da X con una precedente transazione da parte di Z). Una volta che X sottoscrive il trasferimento attraverso la sua chiave privata[37], che rappresenta la firma digitale, diffonde la transazione a tutti i nodi della rete che

[35] Così S. GALMARINI, *Antiriciclaggio*, Wolsters Kluwer, 2019, Milano, cit. a p. 743.
[36] Sul punto si veda G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, Giappichelli editore, 2010, Torino, p. 200 e s.
[37] L'utente può scegliere di mantenere segreta la propria identità e/o avere più indirizzi.

potranno procedere con l'eventuale validazione. In questa fase, gli utenti verificheranno che la firma digitale del mittente sia corretta, e che quest'ultimo disponga dei fondi sufficienti per il trasferimento. Questa verifica è possibile dal momento in cui esiste un *database* pubblico che registra i saldi di ogni utente aggiornati in tempo reale. L'autenticità della transazione è dunque più che garantita, nonostante l'assenza di intermediari, in quanto ogni trasferimento porta la firma digitale del mittente (chiave privata), riporta chiaramente il precedente trasferimento ricevuto dal mittente e restituisce la chiave pubblica del destinatario. In questo modo solo il soggetto X può trasferire le somme precedentemente ricevute da Z, e solo Y potrà nuovamente trasferirle in un secondo momento. A questo punto, un utente che abbia validato un numero significativo di transazioni, può riunirle per tentare di formare un nuovo blocco. Affinché questo sia possibile, quest'ultimo deve avere le caratteristiche richieste dal sistema, ma soprattutto è necessario verificare che nessun altro utente stia cercando, allo stesso tempo, di creare blocchi con le stesse transazioni. Questo rischio viene eliminato grazie alla funzione di *hash*. Ogni nuovo blocco deve contenere:

1. l'impronta del blocco precedente, che corrisponde all'attuale ultimo blocco della catena;
2. le transazioni;
3. un *nonce*, sigla di "*number used once*", è un numero utilizzabile una sola volta al fine di evitare che i dati relativi alle vecchie transazioni possano essere riutilizzati successivamente.

L'impronta del blocco, generata dalla funzione *hash* sottoforma di *nonce,* deve contenere un certo numero di 0 inziali, stabilito per tutta la rete *blockchain*, che aumenta progressivamente. In questo modo la creazione di blocchi diventerà sempre più complicata. Supponiamo che ad oggi, il numero iniziale di 0 fissati sia pari a 99, sarà necessario un grande numero di tentativi per creare il nuovo blocco, ognuno con un *nonce* diverso, mantenendo sempre invariato l'*hash* del blocco precedente e le transazioni da raccogliere. Questo processo è noto come "*mining*", letteralmente "scavare", proprio perché equiparabile alla fatica del lavoro in miniera. Una volta terminata questa operazione, il blocco viene diffuso in rete in attesa che gli utenti verifichino ed, eventualmente, ne convalidino l'aggiunta. Il nodo che vanta la

creazione del nuovo blocco, viene ricompensato in bitcoin e riceve una *fee* da parte di chi trae vantaggio dalla registrazione.

Così strutturata, la tecnologia *blockchain* si presenterebbe come valida alternativa alla disciplina giuridica: è un primissimo esempio di come sia possibile ottenere certezza negli scambi senza ricorrere alla sanzione giuridica, grazie all'ampiezza della rete ed alla numerosità degli utenti. Non è da sottovalutare la capacità che la criptovaluta vanta nel sapersi imporre come moneta seppur priva di corso legale.

Tuttavia, nonostante il modello cooperativo renda più sicuro e rapido il processo di validazione, la grande potenza di calcolo necessaria per il funzionamento delle *blockchain* ha sollevato delle preoccupazioni ambientali. Basti pensare che i bitcoin necessitano, da soli, di talmente tanta energia che potrebbero contribuire al riscaldamento globale[38]. La base della problematica risiede nell'enorme potenza di calcolo necessaria per approvare una transazione e generare un blocco. Di conseguenza, più è lunga la catena, più difficile saranno risolvere i calcoli, più energia sarà necessaria. Un rapporto pubblicato nel 2018 da Morgan Stanley ci informa che la potenza computazionale necessaria per generare una unità di criptovaluta richiede la stessa "dose" di energia che una famiglia nordamericana utilizza in due anni[39]. I ricercatori dell'Università delle Hawaii stimano che solo nel 2017 l'uso di bitcoin ha emesso 69 milioni di tonnellate di anidride carbonica[40]. Questi dati permettono di prevedere che entro il 2033 la temperatura potrebbe aumentare di due gradi a causa della produzione della principale criptovaluta. In seguito ai risultati di questo studio l'IPCC (gruppo intergovernativo sul cambiamento climatico) avvisa che 2 gradi centigradi rappresentano la soglia che la temperatura media globale non deve assolutamente superare per evitare cambiamenti irreversibili del pianeta[41]. Di conseguenza la normativa dovrebbe fissare un limite massimo di energia spendibile per la formazione di un blocco, che obbligherebbe gli sviluppatori a lavorare ad un nuovo algoritmo più efficiente di quello attuale, Proof of Work, al fine di ridurre il consumo energetico necessario per risolvere il calcolo ed aggiungere un nuovo blocco.

---

[38] Sul punto si veda M. MUSSO, *I bitcoin potrebbero far aumentare la temperatura di 2 gradi entro il 2033*, ottobre 2018, www.wired.it.

[39] Per approfondimenti si rinvia a Morgan Stanley Investment Management, *Blockchain*, 2018, www.morganstanley.com.

[40] Sul punto si veda C. MORA, R. L. ROLLINS, K. TALADAY, M. B. KANTAR, M. K. CHOCK, M. SHIMADA, E. C. FRANKLIN*, Bitcoin emissions alone could push global warming above 2°C,* ottobre 2018, www.nature.com.

[41] Cfr. Special report dell'IPCC, *Global warming of 1.5°*, ottobre 2018, www.ipcc.ch.

Infatti, se da un lato la complessità di questo algoritmo garantisce una maggior sicurezza, dall'altro richiede l'intervento di macchine molto potenti che richiedono un'ingente quantità di energia elettrica.

Questo elemento però non ha dissuaso molte grandi aziende dallo sperimentare questa nuova tecnologia, per poter fare a meno di intermediari risparmiando tempo e denaro[42].

1.5.2 L'impatto della *blockchain technology* sul settore finanziario: vantaggi e potenzialità

Gran parte della dottrina sostiene che la tecnologia *blockchain* rivoluzionerà il *modus operandi* del commercio, dell'industria e dell'istruzione, favorendo il rapido sviluppo dell'economia basata sulla conoscenza su scala globale. Le potenziali applicazioni della tecnologia *blockchain* sono garantite dalla sua immutabilità, trasparenza ed attendibilità di tutte le transazioni[43]. Alla *blockchain technology* va il merito di aver trasformato "*the internet of information sharing*" in "*the internet of value exchange*", diventando un *hot topic* per molte più aziende, istituzioni, paesi.

Tra i quattro potenziali vantaggi conferiti dalla nuova tecnologia[44], spicca la possibilità di semplificare i processi del settore bancario. Innanzitutto facilità e automatizza i processi di "*matching*" tra clienti con esigenze opposte. In secondo luogo, questi processi, poiché più trasparenti, permettono di soddisfare in modo più rapido ed efficiente i requisiti regolamentari richiesti e di risalire facilmente alla cronologia di tutte le transazioni effettuate. Inoltre, la tecnologia *blockchain* rafforza l'efficienza del mercato: coinvolgere intermediari in un processo di trasferimento comporta tempi più o meno lunghi esponendosi ad errori, ritardi, ulteriori costi e assunzione di rischi evitabili. Grazie alla *blockchain technology* disponiamo di un inedito e quanto più utile strumento quale lo *smart contract* che trasferisce beni automaticamente, reagendo al trascorrere del tempo e agli *input* forniti.

[42] Affronteremo nello specifico questo aspetto nel quarto capitolo.
[43] Cfr. S. UNDERWOOD, *Blockchain beyond bitcoin*, novembre 2016, Vol. 59 n. 11, www.cacm.acm.org.
[44] Per approfondimenti si rimanda a D. KNEZEVIC, *Impact of blockchain technology in changing the financial sector and other industries*, marzo 2018, Montenegrin Journal of Economics.

Nello specifico, la *blockchain technology* è in grado di trasformare, più o meno radicalmente, i più comuni servizi finanziari.

SERVIZIO FINANZIARO	**IMPATTO DELLA BLOCKCHAIN**	**STAKEHOLDERS**
Autenticazione	Identità verificabili crittograficamente[45]	Agenzie di *rating*, regolatori, *retail banking* ecc.
Trasferimento di valore – effettuare un pagamento, trasferire moneta, acquistare beni e servizi	Riduzione di tempi e costi grazie all'assenza di intermediari	Servizi di trasferimento di moneta, *retail banking*, *wholesale banking*, telecomunicazioni ecc.
Riserva di valore – la moneta, la merce e gli *assets* finanziari, il conto corrente sono riserve di valore	Un meccanismo di pagamento con una riserva di valore sicura e affidabile riduce la necessità strumenti finanziari diversi.	*Retail banking*, *investment banking*, telecomunicazioni, regolatori ecc.
Servizi di credito – carte di credito e debito, *corporate bonds*, *government bonds*, ABS ecc.	Il debito può essere emesso o saldato sulla *blockchain* in tempi minori, costi minori, riducendo il rischio sistemico e le frizioni. Essendo la *blockchain* un registro pubblico di dati disponibile per tutti gli utenti, anche la reputazione può essere un elemento importante per chiedere un	*Wholesales, commercial and retail banking*, finanza pubblica, *credit rating agencies* ecc.

[45] Analizzeremo il problema dello pseudonimato nel terzo capitolo.

	finanziamento, strumento utile per gli imprenditori.	
Scambio di valore	Forte aumento della rapidità dell'operazione	Tutte le industrie
Finanziamento e investimento	Nuove modalità e ulteriori opportunità	Banche di investimento e società di *venture capital*
Management risk	Notevole riduzione	*Risk management, insurance, regolatori, wholesale banking* ecc.

Source: D. Tappsocott and A. Tapscott, 2017, p. 63, modificato.

Come illustrato dalla tabella, la tecnologia *blockchain* rappresenta una reale, nuova opportunità nella creazione e gestione del valore. I benefici, costi significativamente più bassi, maggior rapidità nei movimenti, riduzione dei rischi, innovazione, hanno il potenziale per modificare non solo il sistema dei pagamenti, ma anche il *modus operandi* delle banche di investimento, di revisione e contabilità, delle società di *venture capital*, banche *retail* e la totalità delle industrie.

1.5.3 Il futuro della *blockchain technology*: 4 potenziali scenari

Attraverso lo studio e l'analisi di *paper* e dati in circolazione, è intuitivo ipotizzare quattro possibili scenari sul futuro della tecnologia *blockchain*.

1. **I SCENARIO**: **fallimento**. Lo stesso Mike Hearn, esponente di rilievo della Bitcoin Community, ritiene che sono diverse le ragioni che porteranno il bitcoin al fallimento[46]. Una delle cause è innanzitutto il limite della piattaforma di poter eseguire non più di tre transazioni al secondo, aspetto che rende il sistema poco competitivo rispetto ad altri come PayPal o Visa. In fase di progettazione si parlava di almeno sette transazioni al secondo, ignorando

[46] Per approfondimenti si rinvia a A. BAI, *Bitcoin al capolinea secondo Mike Hearn*, 2016, www.hwupgrade.it.

che l'incremento della complessità delle operazioni avrebbe potuto compromettere questa possibilità. In più, il punto di forza di Bitcoin si fondava sul fatto che la sicurezza dipendeva strettamente dall'alta partecipazione al sistema, dato che per prendere possesso della rete bisognava avere il controllo della maggioranza. È intuitivo pensare che sia altamente improbabile che milioni di persone commettano una frode nello stesso momento. Tuttavia, proprio nel 2016, Hear afferma che pochi *miners* cinesi controllano più del 50 % della rete Bitcoin.

Un particolare fallimento si è dimostrata la possibilità di poter considerare il bitcoin come un "bene rifugio", proprio nei mesi estivi del 2019. Alcuni analisti avevano preso in considerazione tale ipotesi in virtù del fatto che il prezzo del bitcoin sia rimasto sempre superiore ai 9 mila dollari, anche in presenza di mercati azionari in difficoltà[47]. Questo aspetto sembrava infatti suggerire che l'andamento del prezzo del bitcoin fosse inversamente proporzionale rispetto ai mercati finanziari tradizionali. Tuttavia, come si legge anche su *twitter*, ‹‹(…) mentre le crescenti tensioni commerciali hanno fatto precipitare i mercati azionari globali, gli investitori hanno cercato rifugio in paradisi monetari sicuri. Lo yen giapponese, il franco svizzero e soprattutto l'oro sono aumentati. Tuttavia Bitcoin è precipitato più delle azioni!»[48].

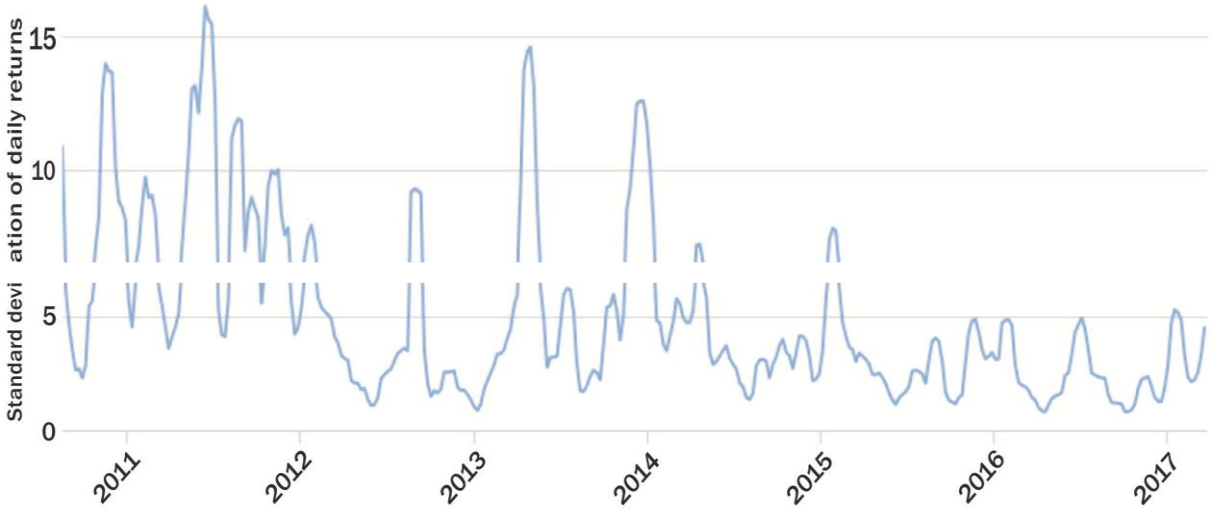
2. **II SCENARIO: impatto profondo sul settore finanziario, impatto limitato sulle industrie.** Avvaliamoci di alcuni dati[49]: a febbraio 2018 il valore di 1 BTC corrisponde a 8667,50 euro, mentre nel 2009 era pari a 0,0001 USD. L'indice di volatilità sta progressivamente acquisendo un trend meno "movimentato".

[47] Sul punto si veda M. CAVICCHIOLI*, Peter Schiff: "bitcoin ha di nuovo fallito come bene rifugio*, agosto 2019, www.cryptonomist.ch.
[48] Post su *twitter* di Peter Schiff, agente di borsa e commentatore finanziario, il 28 agosto 2019.
[49] Dati forniti da D. KNEZEVIC, *Impact of blockchain techonoly in changing the financial sector and other industries*, marzo 2018, Montenegrin Journal of Economics.

PREZZO DI MERCATO DEL BITCOIN

FONTE: www.blockchain.info.

INDICE DI VOLATILITA' DEL BITCOIN



FONTE: www.blockchain.info

Bitcoin ha raggiunto *users* in 130 paesi differenti, registrato più di 200 000 000 transazioni, creato più di 12 000 000 *e-wallet*, raccolto attraverso le ICOs più di $ 270 000 000 dal 2013 al 2018. Ma nonostante il forte e significativo progresso nel settore finanziario, alcuni sostengono che per diverse applicazioni questo tipo di tecnologia non sia un'idea promettente. Certo è, a mio parere, che prima di sfruttare e approfittare delle potenzialità della nuova

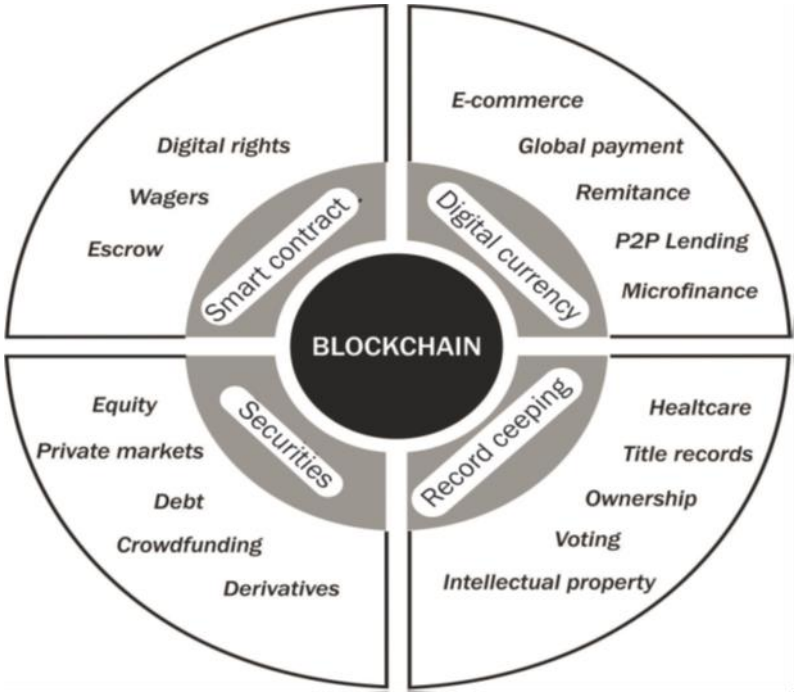
tecnologia nel campo industriale, della sanità o dell'istruzione è necessario curare la normativa, nazionale e comunitaria, che attualmente presenta diverse lacune in merito.

3. **III SCENARIO: rapida trasformazione del settore finanziario, lenta trasformazione nel campo dell'industria, istruzione e salute**. A confermare la prima ipotesi di questo scenario, riportiamo le prime 10 monete virtuali in ordine di capitalizzazione, per meglio comprendere l'entità del fenomeno in esame.

#	Name	Market Cap	Price	Circulating Supply
1	Bitcoin	€168.246.553.556	€9.387,11	17.923.150 BTC
2	Ethereum	€17.651.898.113	€163,96	107.658.017 ETH
3	XRP	€10.190.181.581	€0,237066	42.984.656.144 XRP *
4	Bitcoin Cash	€4.959.326.463	€275,64	17.992.038 BCH
5	Litecoin	€4.023.983.742	€63,66	63.209.724 LTC
6	Tether	€3.681.078.223	€0,904177	4.071.193.568 USDT *
7	Binance Coin	€3.159.108.386	€20,31	155.536.713 BNB *
8	EOS	€3.132.363.377	€3,36	930.867.255 EOS *
9	Bitcoin SV	€2.185.007.019	€122,38	17.854.986 BSV
10	Monero	€1.194.950.912	€69,48	17.197.791 XMR

Fonte: coinmarketcap.com, 8 settembre 2019

Fino al 2015, le principali istituzioni finanziarie scartavano la possibilità di investire e speculare attraverso il Bitcoin. Successivamente, Generale, Commonwealth Banke of Australia, Bank of Montreal, CIBC, RBC, State Street, TD Bank, BNY Mellon, Wells Fargo, Nordea, Mizuho Bank, UniCredit, Commerzbank e altri hanno cambiato opinione a riguardo, iniziando ad investire in tecnologia. Le più note università come Princeton, Stanford, New York University, e la Duke tengono corso su *blockchain*, bitcoin, e criptovalute. Ricerche recenti dimostrano che sono tante le industrie già "sconvolte" e coinvolte nell'impatto della tecnologia *blockchain*, e altrettante ne risentiranno, evolvendosi nel corso dei prossimi 5 anni[50]. Entrambe le categorie vengono illustrate nella figura seguente:



FONTE: Impact of blockchain technology in changing the financial sector and other indistries, di D. KNEZEVIC, Montenegrin Journal of Economics.

I risultati della ricerca dell'Osservatorio Blockchain & Distributed Ledger della School of Management del Politecnico di Milano confermano che nel 2018, mentre il 48 % dei progetti realizzati attraverso la *blockchain technology* sono stati promossi da banche ed altri intermediari finanziari, gli operatori logistici e la pubblica amministrazione sono promotori rispettivamente dell'8% e del 10 % della totalità dei

[50] Così D. KNEZEVIC, *Impact of blockchain tecnhology in changing the financial sector and other industries*, marzo 2018, Montenegrin Journal of Economics.

progetti.[51] Nonostante sia evidente l'interesse, da parte delle industrie, di sperimentare la logica della decentralizzazione, a rallentare lo sviluppo sono probabilmente diversi fattori come la mancanza di competenze e la difficoltà nel valutare con esattezza benefici e costi. Non è da ignorare il grande ostacolo rappresentato dai non modesti costi dell'energia elettrica in Italia.

4. **IV SCENARIO**: **forte e rapido impatto sul settore finanziario e sulla maggior parte delle industrie (entro 5 anni)**. Tre sono le ragioni che fanno di quest'ultimo uno scenario poco realistico. In *primis*, per i motivi dapprima elencati sulla base della pessimistica previsione di Mark Hearn, la piattaforma bitcoin non gode di carattere competitivo nei confronti degli altri sistemi P2P. In *secundis*, è vero che la trasparenza della procedura rappresenta un vantaggio agli occhi dei regolatori, ma è anche vero che si tratta di una tecnologia non ancora standardizzata. Infine, maggiore sarà l'ammontare di criptovalute in gioco, maggiore sarà l'attenzione degli *hacker* sulla piattaforma. Il tutto viene sintetizzato così da gran parte della dottrina: ‹‹Il potenziale di questa tecnologia è immenso, ma per poter essere applicata completamente bisogna attendere qualche anno. Questo per due ragioni. In primo luogo, al momento questa tecnologia è incapace, da sola, di gestire un volume di transazioni necessario per supportare la mole di lavoro delle maggiori imprese. In più, un'applicazione di questa tecnologia nel settore industriale richiede la definizione di norme governative, intervento che richiederà non poco tempo»[52].

   Lo stesso Parlamento Europeo ha tuttavia riconosciuto, lo scorso 3 ottobre 2018, le potenziali opportunità che questa tecnologia potrebbe garantire all'Unione in un prossimo futuro: dal voto elettronico ai servizi pubblici, dalla gestione dei brevetti ai pagamenti digitali[53].

[51] Cfr. Osservatori Digital Innovation della School of Management del Politecnico di Milano, *La distribuzione dei casi blockchain & distributed ledger per processo e per settore, 2016-2018,* maggio 2019, pubblicazione acquistabile su www.osservatori.net.

[52] Cfr. D. KNEZEVIC, *Impact of blockchain technology in chanching the financial sector and other industries*, marzo 2018, Montenegrin Journal of Economics.

[53] Per approfondimenti si rinvia a European Parlament, *Distributed ledger technologies and blockchains: building trust with disintermediation,* ottobre 2018, www.iusinitimere.it.

2. LE PRINCIPALI CRYPTOCURRENCIES: LE RAGIONI DEL SUCCESSO E LA RISPOSTA EUROPEA

2.1 Premessa e concetti fondamentali

Al fine di evidenziare le caratteristiche che accomunano e distinguono le principali criptovalute, in questo capitolo procederemo con un'analisi che sfrutta i dati riportati sul sito coinmarketcap.com, il quale fornisce informazioni su capitalizzazione di mercato, prezzo, circolante e volume degli scambi delle ultime 24 ore di tutte le 2494 monete virtuali attualmente oggetto di compravendita in 20397 mercati[54].

Nello specifico, la **capitalizzazione di mercato** è il risultato del prodotto tra numero di unità di moneta virtuale in circolazione e prezzo medio di mercato, il quale, su coinmarketcap.com, corrisponde alla media ponderata dei prezzi proposti sulla totalità delle piattaforme di scambio che detengono la valuta in esame:

$$CdM = N \times \bar{P}$$

Di fatto, la capitalizzazione di mercato degli strumenti finanziari viene calcolata in modo analogo. Tuttavia, come abbiamo già accennato e come vedremo nello specifico nel capitolo successivo, i rischi relativi al "criptomercato" son ben più complessi e ben più difficili da arginare.

[54] Dati forniti da coinmarketcap.com al 28 agosto 2019.

Di seguito, riportiamo le prime dieci criptovalute che vantano una maggior capitalizzazione:

#	Nome	Cap. del mercato
1	Bitcoin	€165.829.584.213
2	Ethereum	€18.183.745.914
3	XRP	€10.310.794.256
4	Bitcoin Cash	€4.987.036.310
5	Litecoin	€4.109.745.153
6	Tether	€3.663.926.505
7	Binance Coin	€3.555.485.931
8	EOS	€2.943.054.614
9	Bitcoin SV	€2.132.182.922
10	Stellar	€1.213.567.905

Fonte: coinmarketcap.com, 28 agosto 2019.

L'indiscusso primato di bitcoin viene confermato da una capitalizzazione di mercato che crea un distacco con il secondo posto di ethereum che ammonta a circa € 148 miliardi.

Per meglio comprendere la metodologia con cui coinmarketcap.com calcola il **prezzo** della singola valuta virtuale, ci avvaliamo di un esempio riportato sullo stesso sito con cui calcoleremo un prezzo fittizio per litecoin.

Sia A il prezzo di 1 litecoin espresso in bitcoin fornito direttamente dall'*exchange* e sia B il prezzo di 1 bitcoin espresso in dollari. Il prezzo di 1 litecoin espresso in dollari (X) sarà pari a:

$$X = A \times B$$

Pertanto, se il valore di 1 LTC equivale a 0.01 BTC e 1 BTC equivale, al momento del calcolo, a 10,000 USD, il prezzo sarà pari a:

$$1\ LTC\ = 0.01\ \times 10{,}000\ = 100\ USD$$

Le conversioni in altre valute (ad esempio l'euro), partono in ogni caso dal prezzo espresso in dollari che verrà poi convertito sulla base del tasso di cambio disponibile su openexchangerates.org.

Di seguito riportiamo le dieci criptovalute più "costose":

#	Nome	Prezzo
1	Bitcoin	€9.263,27
2	Maker	€474,63
3	Bitcoin Cash	€277,49
4	Ethereum	€169,14
5	Bitcoin SV	€119,42
6	Dash	€81,31
7	Monero	€69,73
8	Litecoin	€65,10
9	Zcash	€44,90
10	Binance Coin	€22,86

Fonte: coinmarketcap.com, 28 agosto 2019.

Anche in questo caso il primo posto di bitcoin mantiene le distanze dalle altre posizioni. Un aspetto da non ignorare si evince dal fatto che un'unità della decima valuta virtuale in ordine di prezzo può "comprare" solo € 22,86. Questo dato lascia

intuire che della totalità delle 2494 criptovalute in circolazione, sono veramente poche quelle che hanno un valore sostanziale[55].

Sulla falsa riga del calcolo del prezzo, è facile risalire al processo con cui coinmarketcap.com calcola il **volume degli scambi** delle ultime 24h. Il sito fornisce un esempio simile al precedente: sia C il numero di unità di litecoin scambiati in termini di bitcoin nelle ultime 24 ore fornito dall'*exchange* e sia D il prezzo di 1 bitcoin espresso in dollari. Allora il volume di litecoin scambiati espresso in dollari sarà pari a:

$$Y = C \times D$$

Pertanto, se i litecoin scambiati nelle ultime 24 ore equivalgono a 100 BTC, ed il prezzo di 1 BTC equivale a 10,000 USD, il volume di LTC scambiati nelle ultime 24 ore equivale a:

$$100 \times 10{,}000 = 1{,}000{,}000\ USD$$

Anche in questo caso, laddove avessimo bisogno di esprimere il risultato in una valuta diversa, partendo dai dati espressi in dollari si procederà con la conversione per mezzo del tasso di cambio disponibile su openexchangerates.org.

Le prime dieci criptovalute in ordine di volume sono le seguenti:

#	Nome	Volume (24h)
1	Tether	€13.599.796.750
2	Bitcoin	€12.285.723.338
3	Ethereum	€4.926.511.882
4	Litecoin	€2.148.351.860
5	Bitcoin Cash	€1.130.483.517
6	XRP	€1.036.767.251
7	EOS	€994.723.694

[55] Al 28 agosto 2019, sono solo 38 le monete virtuali che vantano un tasso di cambio con l'euro superiore ad uno.

#	Nome	Volume (24h)
8	Ethereum Classic	€697.270.094
9	TRON	€415.127.436
10	TrueUSD	€328.363.382

Fonte: coinmarketcap.com, 28 agosto 2019.

Come si evince dal *ranking*, bitcoin in termini di volume degli scambi si lascia scavalcare da tether, l'unica criptovaluta, come affermato da Il Sole 24 Ore, ‹‹in grado di far tremare il Bitcoin». Tether spicca tra le altre monete virtuali in quanto "*stablecoin*". È stata progettata per non soffrire di alta volatilità, e per questo ancorata ad un tasso di cambio con il dollaro che si aggira sempre intorno ad 1. L'andamento grafico lo conferma:

1 USDT (sigla di tether, appunto perché ancorata al valore del dollaro) ha raggiunto il suo valore più alto a dicembre 2017, pari a $ 1.05, il valore più basso ad aprile 2017, pari a circa $0.91. Ciò è possibile perché ogni singola unità di tether viene emessa solo

se è coperta da un dollaro nelle riserve della Tether Limited, società delle Isole Vergini britanniche[56]. Il punto di forza di questa criptovaluta risiede, a mio parere, nella possibilità per chi le acquista di sfruttare tutte le opportunità operative proprie delle monete virtuali, senza però subire il rischio di un'elevata volatilità[57]. Una delle potenzialità è quella di conferire all'investitore la possibilità di sfuggire ai momenti di tensione: nel momento in cui il valore del bitcoin, per fare un esempio, dovesse subire una brusca discesa, l'investitore potrebbe convertire i bitcoin in tether senza dover necessariamente passare per la moneta reale, senza subire particolari perdite. Questa importante funzionalità fa del tether la valuta, ad oggi, più scambiata. Misurare il volume degli scambi è forse ancor più utile, ai fini di un'analisi, del calcolo di prezzo e capitalizzazione, perché si può intuitivamente tradurre in una misura dell'interesse che gli investitori hanno nei confronti di uno specifico prodotto, in questo caso una moneta virtuale. Da lì si può procedere, come nel caso di tether, ad analizzarne i motivi.

Quando si parla di criptovalute, avere dei dati relativi al **circolante** è fondamentale: una delle caratteristiche principali delle monete virtuali è proprio la possibilità di poter emettere un numero limitato di unità. Gli aspetti da analizzare in questo caso sono principalmente due: l'ammontare del circolante in valore assoluto, capire se si tratta di una cifra alta oppure no sulla base del confronto con le altre criptovalute, e l'ammontare attuale del circolante rispetto al massimo limite raggiungibile. In primo luogo, è intuitivo supporre che minore è il numero massimo di unità che è possibile emettere, maggiore sarà il valore della criptovaluta: un modesto limite massimo si traduce in "scarsità", che a sua volta si traduce in valore. Per conferma, osserviamo infatti che il numero massimo di unità di bitcoin che verranno emesse è pari a 21 milioni, a differenza del numero massimo di unità di litecoin (che infatti vale molto meno[58]) pari a 84 milioni. Attraverso la stessa intuizione, possiamo concludere che quanto più l'ammontare di circolante già emesso si avvicina al limite massimo, tanto più aumenterà il valore della moneta: più ci si avvicina al limite, più il prodotto scarseggia, più il valore aumenta. Nel caso di bitcoin sono già state emesse quasi 18 milioni di unità, pari all'86% circa del totale.

[56] Sul punto si veda P. SOLDAVINI, *Cos'è Tether, la criptovaluta legata al dollaro che fa tremare il Bitcoin*, febbraio 2018, ilsole24ore.com.

[57] Proprio sulla base di queste considerazioni, il quarto capitolo sarà dedicato ad un'analisi *swot* relativa alla possibilità di progettare una *stablecoin* internazionale.

[58] Analizzeremo questo aspetto più nello specifico al paragrafo 2.2.2.

2.2 Differenze e analogie: cosa si intende per Altcoin

La singolare caratteristica del sistema Bitcoin di essere *open-source*, da un lato prevede che nessun ente controlli e gestisca la piattaforma, dall'altro che chiunque partecipi al *network* possa apportare modifiche al sistema al fine di migliorarne il meccanismo alla base. Questa possibilità ha inevitabilmente favorito l'opportunità di generare nuove criptovalute, con l'intento di garantire un miglioramento più o meno innovativo alla piattaforma Bitcoin.

Sulla base di questo aspetto possiamo definire "Altcoin", abbreviazione di "*alternative coin*", tutte le monete virtuali, alternative al bitcoin, nate per sostituire o migliorare almeno una componente del sistema[59]. Nei paragrafi successivi analizzeremo con maggior attenzione le principali Altcoin, nello specifico bitcoin cash, litecoin, ripple, ed ethereum. Solo per fare un esempio, uno degli aspetti più "scomodi" del sistema Bitcoin è rappresentato dai tempi necessari per un trasferimento che risultano essere relativamente lunghi, e molte delle Altcoin sono nate per ovviare a questa problematica.

In virtù di quanto detto nella premessa, analizzerei le principali Altcoin non sulla base della capitalizzazione di mercato, che dipende a sua volta da altri fattori quali prezzo, circolante emesso, limite massimo al circolante ecc., bensì sulla base del volume degli scambi, che si traduce in interesse da parte degli investitori.

[59] Sul punto si rinvia a Anonymous, *Che cosa sono le Altcoin e perché sono importanti*, maggio 2018, www.bitcoin.it

2.2.1 Ethereum

Al terzo posto in ordine di volume degli scambi, subito dopo bitcoin, spicca ethereum, le cui innovazioni rispetto alla piattaforma originale meritano particolare attenzione. Di fatto Ethereum è una *blockchain platform* che però permette agli utenti di sfruttare diverse applicazioni decentralizzate non necessariamente ancorate al mero scambio di *cryptocurrencies*. È una rete che consente a tutti i partecipanti di beneficiare di un archivio inalterabile e condiviso di operazioni regolate attraverso *smart contracts*[60]: dal *crowfunding* alla tutela della proprietà intellettuale o alla registrazione di un dominio. Sono contratti intelligenti, per l'appunto, perché reagiscono ad input rispondendo con output consequenziali. Un esempio applicativo è rappresentato da Etherisc, un'assicurazione sui viaggi aerei decentralizzata che si avvale della piattaforma Ethereum. Il contratto incorpora le informazioni sugli orari di partenza e in caso di ritardo del volo fa scattare automaticamente il rimborso. La sicurezza e la trasparenza del meccanismo ha spinto anche Axa, prima grande compagnia assicurativa, a scegliere gli *smart contracts* di Ethereum, per consentire rimborsi assicurativi su carta di credito in caso di ritardo sui voli[61]. Recenti studi del Norton Rose Fulbright, il secondo più grande studio legale degli Stati Uniti, sono volti a sviluppare dei prototipi di *smart contract* per la liquidazione degli indennizzi nelle operazioni di M&A.

Per poter usufruire di questo strumento sulla piattaforma è necessario pagare in valuta ether (ETH). La *ratio* di questa *blockchain platform*, nata nel 2013 dalla mente di Vitalik Buterin, risiede nella volontà di voler offrire agli utenti delle possibilità inedite ovunque e per sempre. Non è infatti stata concepita per essere bloccata o censurata, e non esiste un limite massimo di ether da poter emettere, a differenza delle altre

[60] Rimandiamo al primo capitolo per la definizione di "*smart contract*".
[61] Sul punto si veda D. AQUARO, *Smart contract: cosa sono (e come funzionano) le clausole su blockchain,* Il Sole 24 Ore, giugno 2019, www.ilsole24ore.com.

criptovalute[62]. Lo *smart contract* lamenta però dei limiti applicativi tecnico-giuridici: l'irreversibilità della *blockchain* non permette di modificare un errore, ed è uno strumento utile solo le condizioni contrattuali sono facili da tradurre in un linguaggio informatico (es. se c'è una scadenza, effettua il pagamento).

Confrontare il prezzo di ethereum con quello delle altre criptovalute non è, a mio parere, utile all'ottenimento di risultati particolarmente significativi. Questo perché l'utilizzo di Ethereum è incentivato dalle molteplici funzioni che la piattaforma offre, come finora descritto, di cui invece non godono gli utenti che scambiano bitcoin ed altre valute virtuali. Non sarebbe di conseguenza un confronto basato su una parità di condizioni. Analizziamone in ogni caso l'andamento.

Il motivo che si cela dietro l'ascesa del prezzo di ethereum dal mese di dicembre 2017 è particolarmente curioso. Pare che questo aumento sia dovuto al successo dell'applicazione ludica nata sulla piattaforma nota come CryptoKitties, che chiede ai giocatori di scambiare ethereum per svolgere le attività previste. Lo *smart contract* di CryptoKitties ha rappresentato circa il 14 % del volume delle transazioni dell'intera rete[63], che ha generato di conseguenza un aumento del prezzo della criptovaluta. Il

[62] Per approfondimenti si rinvia a M. BELLINI, *Che cos'è e quali sono gli ambiti applicativi di Ethereum*, agosto 2019, www.blockchain4innovation.it.
[63] Cfr. C. CITTON, *Prezzo Ethereum e volume di scambi: CryptoKitties nuovo strumento finanziario?*, dicembre 2017, www.blastingnews.com.

gioco prevedeva la possibilità di acquistare, vendere e allevare gatti virtuali al fine di permettere loro di accoppiarsi per generare altri cryptogatti. Ogni gatto presentava caratteristiche diverse dagli altri, alcune più rare di altre, e per questo più costose. È un'idea basata sulla rarità e sul collezionismo digitale che ha dimostrato che applicare la tecnologia *blockchain*, per la prima volta, in un contesto non finanziario, può tradursi in un grande successo. Questo esperimento conferma, come lo stesso Fred Wilson, uomo d'affari e *blogger* finanziario americano, sostiene, che la *blockchain technology* si rivela particolarmente utile e apprezzata come strumento per acquistare, vendere, detenere e scambiare risorse digitali contro altre risorse digitali (unità di ethereum in questo caso) in un mercato dalle dimensioni globali[64].

Percorrendo la classifica delle criptomonete più scambiate ci imbattiamo in una valuta che sembra in parte "rubare" il nome a quella in esame: ethereum classic. In realtà sono due versioni della stessa piattaforma, nate da una scissione che risale a luglio del 2017. Poco più di un anno prima, nasce il DAO, Decentralized Autonomous Organization, uno dei primi esempi di *smart contract:* gli utenti potevano scegliere di inviare fondi all'organizzazione in ethereum, ricevendo per contro dei *token*, che conferivano agli investitori il diritto di poter votare i progetti ai quali destinare i fondi raccolti. A giungo 2016 però, un mese dopo della nascita di DAO, il sistema venne hackerato con il conseguente furto di 12 milioni (ETH), prima ancora che si finanziasse uno solo dei progetti[65]. In questo esatto momento ci fu la scissione: un gruppo riteneva che fosse necessario manomettere la *blockchain* a ritroso, modificando il codice in modo da poter rimborsare gli investitori, il secondo invece riteneva che il codice fosse legge (*cod is law*), e per questo non andasse modificato in nessun caso, probabilmente per non perdere credibilità e non creare dei precedenti. Questa seconda corrente di pensiero diede vita ad Ethereum Classic e la sua relativa criptovaluta: ETC. Pur classificandosi tra le più scambiate, quest'ultima è molto più in basso rispetto ad ETH. Il motivo, a mio parere, è da individuare nel fatto che la stragrande maggioranza di ICOs accettano ether, e solo una piccola minoranza accetta ETC. Prevediamo inoltre che questa divergenza in ordine di volume degli scambi andrà con il tempo aumentando. Questo perché sono diversi i progetti a cui il team di Ether sta lavorando:

[64] Cfr. C. CITTON*, Prezzo Ethereum e volume di scambi: CryptoKitties nuovo strumento finanziario?,* dicembre 2017, www.blastingnews.com.

[65] Per approfondimenti si rinvia a V. LOMANNO, *Ethereum VS Ethereum Classic: tutte le differenze, 2018*, www.coiners.it.

hanno in programma di sostituire il sistema di generazione dei blocchi Proof of Work con un sistema Proof of Stake, più economico e rispettoso dell'ambiente[66]; progettano inoltre di inserire aggiornamenti per solidificare l'anonimato ed aumentare la velocità delle transazioni[67].

2.2.2 Litecoin

Litecoin nasce il 7 ottobre 2011 per opera di Charlees Lee, ex dipendente Google. La moneta virtuale alternativa al bitcoin viene sviluppata per due ordini di ragioni: supportare un maggior numero di transazioni in un minor tempo ed aumentare il numero massimo di unità da poter emettere[68], pari a 84 milioni (rispetto al limite massimo di 21 milioni fissato per Bitcoin). Di conseguenza il litecoin vale decisamente meno: al 29 agosto 2019, 1 BTC equivale a € 8 628, 63, mentre 1 LTC corrisponde a "solo" € 58,73[69]. Era questo in realtà l'intento dell'ideatore Charles Lee, che definiva le due criptovalute come l'oro e l'argento: due "beni" con la stessa funzione, ma con diverso valore, perché l'uno più "raro" dell'altro.

Per capire perché il volume degli scambi di litecoin si classifica tra i più alti, analizziamone la volatilità.

[66] Per approfondimenti si rinvia a F. PROVENZANI, *Cos'è il Proof Of Work (PoW) e Proof Of Stake (PoS)?,* aprile 2019, www.money.it.
[67] Cfr. V. LOMANNO, *Ethereum VS Ethereum Classic: tutte le differenze*, 2018, www.coiners.it
[68] Dati forniti dal sito ufficiale litecoin.org.
[69] Dati disponibili su www.coinmarketcap.com al 29 agosto 2019.

Il prezzo del litecoin si è mosso in un *range* che sfiora il suo picco minimo a gennaio 2015 con € 1,02, per raggiungere il picco massimo a dicembre 2017 pari a € 339,48. Le ragioni per cui il litecoin rimane una delle monete più scambiate potrebbero essere diverse, sulla base di mie considerazioni personali. *In primis*, il fatto che il 75 % della totalità di unità sia già stato emesso potrebbe suonare come un campanello d'allarme per gli investitori, i quali sanno e prevedono che il valore andrà man mano aumentando. Questo suggerimento potrebbe stimolare gli investitori a comprare adesso, per poi rivendere ad un prezzo più alto. In secondo luogo, gli anni precedenti al 2017, anno in cui il prezzo del litecoin è salito notevolmente, potrebbero essere risultati necessari agli investitori per conoscere il mondo delle criptovalute, imparare a padroneggiare, per quanto possibile, la rete Bitcoin, per poi rendersi conto delle lacune che la piattaforma presentava, tra cui i tempi necessari a completare una transazione, o dell'altissimo tasso di volatilità. Tali problematiche potrebbero rappresentare uno dei motivi per cui gli investitori hanno iniziato a scegliere una moneta alternativa, soprattutto in virtù di un'oscillazione di prezzo molto più contenuta. Di conseguenza, se gli investitori comprano litecoin è normale che il prezzo salga.

Peraltro, il litecoin e il bitcoin sembrano essere correlati:

La differenza sta nel *range* di oscillazione: nelle ultime 52 settimane il valore più alto sfiorato dal bitcoin è pari € 12 529,97, il più basso pari a € 2 898,94, con un distacco di circa diecimila euro. Il litecoin invece, avendo registrato nello stesso arco temporale un valore massimo pari a € 132,99 e minimo pari € 20,73, rappresenta un'alternativa ideale per quegli investitori più avversi al rischio che pur volendo speculare nel "criptomercato", non sono disposti a gestire le altissime cifre del bitcoin.

2.2.3 Bitcoin Cash

Bitcoin Cash è tra le più giovani criptovalute presenti sul mercato. Nasce nel 2017 per ovviare ad un importante problema operativo del Bitcoin: la scalabilità, cioè la capacità di sostenere più transazioni possibili al secondo, in base alla dimensione del blocco. Mentre Litecoin riduce il tempo di elaborazione, con Bitcoin Cash ciò che cambia è la dimensione del blocco stesso, otto volte superiore ad un singolo blocco di Litecoin e Bitcoin[70]. Nonostante il numero di unità massimo da poter emettere sia lo stesso del bitcoin, pari a 21 milioni, bitcoin cash vale molto meno, pur classificandosi al terzo posto in ordine di prezzo, subito dopo maker: 1 BTC equivale a € 251,60[71]. Nonostante il suo più che modesto valore, il bitcoin cash è meno scambiato rispetto al litecoin, probabilmente a causa di una volatilità meno contenuta:

[70] Per approfondimenti si rinvia al sito ufficiale www.bitcoincash.org.
[71] Dati forniti da coinmarketcap.com al 31 agosto 2019.

Nelle ultime 52 settimane, il massimo valore raggiunto da bitcoin cash è pari € 593,68, contro un valore minimo di € 68,18. È chiaro che, tra le due, litecoin è adatto ad investitori più avversi al rischio.

Procedendo con un'analisi a tutto campo, è però evidente che tanto il prezzo di bitcoin cash, tanto quello di bitcoin e litecoin, subiscono una grave discesa a gennaio 2018, per poi incorrere in una più lieve intorno ad aprile dello stesso anno. La causa principale è da riconoscere, personalmente, nell'intervento del primo ministro della Corea del Sud, Lee Nak-yeon, che il 21 dicembre 2017 annunciò una serie di restrizioni sul *criptotrading*: divieto alle transazioni anonime, facoltà per le autorità finanziarie di chiudere alcune piattaforme di scambio laddove lo ritenessero necessario e maggior potere agli investigatori nelle attività di controllo a fini antiriciclaggio[72]. Considerando che la Corea del Sud era, al momento dell'annuncio, uno dei *leader* mondiali per volume di *cryptotrading*, le conseguenze sui prezzi devono esser state rilevanti. Una concreta minaccia di regolamentazione in Corea del Sud, ed un potenziale "adattamento" della normativa vigente in Russia, Italia, Francia e Germania volto a controllare l'abuso di criptovalute hanno spaventato gli investitori che hanno iniziato a vendere il contenuto dei loro *wallets* determinando la discesa dei prezzi, risultato che a sua volta ha incrementato le vendite, rendendo la discesa ancora più ripida.

La risalita di cui invece stanno godendo litecoin e bitcoin, potrebbe dipendere, a mio parere, dalla data di *halving*, giorno in cui dimezza il valore della ricompensa che spetta ai *miners* che generano un nuovo blocco, e che di conseguenza potranno vendere un volume di monete inferiore del 50 %. Una riduzione dell'offerta, se la domanda rimane costante, genera un aumento dei prezzi. Dato che la data di *halving* è nota a tutti gli investitori, il mercato prevede con certezza una riduzione dell'offerta, anticipando gli "acquisti", e anticipando di conseguenza anche l'ascesa dei prezzi. Da considerare è inoltre il fatto che minore sarà la ricompensa, minore sarà il numero di *miners* disposti a sfruttare le proprie risorse per generare un nuovo blocco, mantenendo attivo il meccanismo. Questo aspetto, meno quantitativo, potrebbe allo stesso modo ridurre notevolmente l'offerta. Per Bitcoin, il prossimo *halving* è previsto per maggio 2020, in seguito al quale la ricompensa scenderà da 12.5 BTC a 6.25 BTC. La

[72] Per approfondimenti si veda L. ZORLONI, *Stretta in Corea sull'uso dei bitcoin. Chi altro vuole regolare la criptovaluta?*, dicembre 2017, www.wired.it

ricompensa che spetta invece ai *miners* che generano blocchi sulla piattaforma Litecoin è già scesa da 25 LTC a 12.5 LTC lo scorso 5 agosto.

Questo approccio suggerirebbe, anche agli investitori più inesperti, di acquistare bitcoin nei primi mesi del prossimo anno, per poi rivenderli in prossimità del mese maggio, periodo in cui una serie di condizioni certe determineranno un'ascesa del prezzo. Nello specifico, avendo osservato che il prezzo del bitcoin sembra essere correlato con quello del litecoin, possiamo basarci sull'andamento di quest'ultimo per progettare un investimento in bitcoin. L'ascesa del prezzo del litecoin antecedente alla data di *halving* del 5 agosto 2019, ha avuto inizio il 28 aprile dello stesso anno partendo da un valore di 68,89 USD, per toccare l'apice il 21 giugno con un valore pari a 137,40 USD. Il prezzo è aumentato del 99,45 % in vista della data in cui la ricompensa spettante ai *miners*, e di conseguenza l'offerta di moneta, dimezza. Questo risultato pare suggerci di optare per una strategia *long*, acquistando bitcoin, poco più di tre mesi prima della data di *halving*, per poi chiudere con una strategia *short*, vendendo bitcoin, un mese e mezzo prima della stessa data. Nel caso del bitcoin, la data di *halving* è prevista per il 20 maggio del prossimo anno. Converrebbe di conseguenza acquistare bitcoin nella prima metà di febbraio, per poi vendere nella prima settimana di aprile. Se, come accaduto proprio qualche mese fa con litecoin, il valore del bitcoin aumentasse del 99 %, investire € 1000 a febbraio, restituirebbe un profitto di € 990 ad aprile. Si tratta di una previsione, a mio parere, in ogni caso pessimistica. Bisogna tener presente che il prezzo del litecoin si muove in un *range* molto meno ampio, e quindi un'ipotesi di un aumento del 99 % potrebbe non rendere onore al reale aumento in cui il prezzo del bitcoin incorrerà l'anno prossimo, dato che quest'ultimo soffre di uno dei più alti tassi di volatilità del criptomercato. Proprio per questo non siamo in grado ad oggi di calcolare con certezza l'ammontare di bitcoin che corrisponderebbe ad un investimento iniziale di € 1000 nel mese di febbraio 2020.

Confinando il grafico del prezzo del litecoin alle date corrispondenti rispettivamente a due mesi prima e due mesi dopo dell'*halving* del 25 agosto 2015, è evidente una ripida ascesa del prezzo nella seconda metà del mese di luglio con un picco massimo pari a 8,36 dollari, per poi scendere e rimanere costante nei mesi di settembre ed ottobre intorno ai 3 dollari.

2.2.4 Ripple

La criptovaluta di Ripple, XRP, è l'ultima a vantare un volume degli scambi superiore al miliardo. Il suo aspetto innovativo merita particolare attenzione in quanto la rete Ripple è stata sviluppata al fine di fornire un sistema utile al diretto trasferimento dei beni in tempo reale, offrendo un'alternativa più rapida ed

economica rispetto agli attuali sistemi di trasferimento di denaro come SWIFT[73], utile in particolar modo alle banche ed agli intermediari finanziari. Questo perché, a differenza della piattaforma Bitcoin, sulla rete Ripple è possibile scambiare e trasferire denaro in valute diverse, senza pagare alcuna commissione. Ciò che gli utenti scambiano sono dei crediti IOU (*I Owe you*), la cui unità di misura è appunto la criptovaluta XRP. I cosiddetti *gateaway* della rete Ripple convertiranno poi la moneta virtuale nella valuta in cui l'utente deve inviare denaro o riceverlo[74]. La *ratio* di questa piattaforma non ha quindi un fine speculativo, come per Bitcoin, bensì è volta ad agevolare gli scambi tra più agenti riducendo tempi e costi. Anche per questo non esiste un numero massimo di unità di XRP da poter emettere: alla nascita della piattaforma sono state emesse 100 miliardi di unità a disposizione degli utenti che volessero usufruirne come strumento di trasferimento.

Proprio in virtù della funzione di XRP, quale quella di essere una moneta di compensazione universale, e non creata a fini esclusivamente speculativi, il suo valore è rimasto pressoché costante, per lo meno fino alla prima metà del 2017.

[73]Acronimo di Society for Worldwide Interbank Financial Telecommunications: sistema che permette trasferimenti di denaro attraverso un *network* internazionale.

[74] Per approfondimenti si rinvia a C. GAGLIARDUCCI, *Ripple: cos'è, come funziona e quali differenze con il Bitcoin?,* maggio 2017, www.money.it.

Una significativa ascesa, superando ampiamente i 3 dollari, si ha nei primi mesi del 2018, e potrebbe essere direttamente collegata con l'annuncio di circa 100 istituti finanziari interessati ad una *partnership* con Ripple[75]. La successiva discesa è probabilmente da collegare invece, come nel caso delle altre criptovalute, all'annuncio del primo ministro della Corea del Sud che ha senz'altro disincentivato gli utenti ad investire nel criptomercato.

2.3 Le ragioni del successo: costi e benefici del mercato *crypto*

L'espansione, al momento incontrollata, del *cryptotrading* è stata, ed è tutt'ora, un campanello di allarme per autorità internazionali, governi, banche centrali e autorità di vigilanza. Nello specifico, l'EBA (Autorità Bancaria Europea) ha approfondito e descritto il fenomeno evidenziando i benefici, economici ed individuali, che incentivano gli individui ad addentrarsi nel mondo, quasi del tutto ombroso, delle criptovalute[76].

Tra i benefici economici, risalta senz'altro la triade "economicità – velocità – sicurezza". I costi di transazione previsti sono senza dubbio più bassi in virtù dell'assenza di intermediari, in media pari all'1% dell'ammontare[77]. Un ulteriore aspetto da non ignorare è sicuramente la velocità delle transazioni. Abbiamo riscontrato già nei paragrafi precedenti l'essenzialità di questa caratteristica: alcune delle principali altcoin sono nate proprio con lo scopo di accelerare ulteriormente i tempi previsti dalla piattaforma Bitcoin (Litecoin, Bitcoin Cash). Abbiamo a che fare inoltre con delle piattaforme *no-stop*, un servizio disponibile 24/7, a differenza dei tradizionali intermediari a cui siamo abituati. Inoltre, la sicurezza e l'irreversibilità delle transazioni, le quali vengono tutte trascritte in un registro comune, garantiscono una trasparenza di cui non sempre godiamo nei mercati tradizionali. Non è raro infatti che i commercianti si trovino a dover pagare addebiti avviati dal consumatore sulla

[75] Sul punto si veda Anonymous, *Ripple: la criptovaluta che piace alle banche,* gennaio 2018, www.01.net.it.

[76] Per approfondimenti si rinvia a European Banking Authority, *Opinion on virtual currencies*, luglio 2014, pp. 16 – 21, www.eba.europa.eu.

[77] Cfr. J. BRITO, *Beyond silk road: potential risks, threats, and promises of virtual currencies*, *Testimony before the Senate Committee on homeland security and governmental affair*, 18 novembre 2013, p. 11.

base di false dichiarazioni di mancata consegna del prodotto[78]. Questa potenzialità però, può rappresentare di fatto un'arma a doppio taglio: l'irreversibilità delle transazioni non protegge gli utenti da eventuali errori o frodi da cui, letteralmente, non si può tornare indietro.

A livello individuale invece, non è da sottovalutare l'opportunità di poter trasferire denaro mantenendo l'anonimato, conservando i propri dati personali. In questo senso, pagare con moneta virtuale è come pagare in contanti, eliminando il rischio di consegnare i propri dati nelle mani di chi potrebbe abusarne[79]. Non dimentichiamo, in ultimo, che la tecnologia *blockchain* nasce con lo scopo di dare inizio ad un sistema decentralizzato, che non soffrisse il controllo di autorità centrali con la facoltà di influenzare l'offerta di moneta. Uno dei benefici del mercato *crypto* è quello appunto di gestire, potremmo dire, "democraticamente" le transazioni, e la relativa possibilità di trasferire denaro oltre i confini comunitari, approfittando talvolta di regolamentazioni estere meno sviluppate e meno affidabili. Infatti, se da un lato questa opportunità garantisce un'integrazione finanziaria, oserei dire, mondiale, dall'altro permette alle organizzazioni criminali, collaborando con altre organizzazioni all'estero, di approfittare di una normativa meno stringente e meno severa[80] vigente in altri Paesi. Purtroppo è necessario ammettere, a mio parere, che proprio il binomio "anonimato – assenza di controllo" suscita l'interesse delle organizzazioni criminali nei confronti delle criptovalute, e rappresenta quindi una delle motivazioni per cui questo mercato ha riscosso, e sta riscuotendo, un importante successo. I dati lo confermano: a febbraio 2018 Rob Wainwright, direttore dell'Europol, stima un ammontare di contanti di provenienza illecita pari a 113 miliardi di euro, di cui il 4 % è stato convertito in criptovalute, per un totale di 4,5 miliardi di euro circa[81]. Lo stesso Parlamento Europeo conferma che una percentuale della totalità delle transazioni *crypto*, compresa tra il 25 ed il 50 %, potrebbe essere destinata a scopi illeciti[82].

[78] Cfr. J. BRITO, *Beyond silk road: potential risks, threats, and promises of virtual currencies, Testimony before the Senate Committee on homeland security and governmental affair*, 18 novembre 2013, p. 10.
[79] Cfr. R. WU, *Why we accept Bitcoin*, Forbes, febbraio 2014, www.forbes.com.
[80] Approfondiremo la questione della transnazionalità delle operazioni *crypto* nel terzo capitolo.
[81] Così K. CORCORAN, *Europol: i criminali ricorrono alle criptovalute per riciclare 5,5 miliardi di dollari in contanti di provenienza illecita in Europa,* febbraio 2018, www.businessinsider.com.
[82] Per approfondimenti si rinvia a M. DABROWSKI (CASE) e L. JANIKOWSKI (CASE), *Virtual currencies and central banks monetary policy: challenges ahead,* luglio 2018, www.europarl.europa.eu.

Per riassumere, le ragioni che hanno portato allo sviluppo e alla rapida crescita di questo mercato oscuro sono: economicità, rapidità e sicurezza delle transazioni, e la possibilità per le organizzazioni criminali di poter operare in un contesto non ancora regolamentato. In aggiunta, le tre autorità di vigilanza europea, EBA (Autorità Bancaria Europea), ESMA (Autorità Europea degli Strumenti finanziari e dei Mercati) ed EIOPA (Autorità Europea delle Assicurazioni e delle Pensioni Aziendali e Professionali), individuano un'altra ragione nella non consapevolezza dei rischi che si corrono facendo uso di criptovalute. L'EBA in particolare, rintraccia 70 rischi che tutti coloro che si servono delle piattaforme del criptomercato corrono, dagli utenti ai fornitori di servizi, all'intero sistema finanziario[83]. Tra i rischi che l'autorità europea riconosce come "*high risks"* risalta la possibilità di significative ed inaspettate variazioni del tasso di cambio: l'assenza di un'autorità centrale che stabilizza i tassi rende l'operazione della formazione del prezzo poco trasparente, nonché facilmente manipolabile da un poco numeroso gruppo di soggetti che possiedono un importante ammontare di criptovaluta. A questo aspetto si sommano le caratteristiche intrinseche del sistema che rendono il prezzo altamente volatile. Abbiamo visto nei paragrafi precedenti come la stessa data di *halving*, oppure la nascita di un'applicazione che permette agli utenti di giocare sulla piattaforma scambiandosi moneta virtuale, possano in poco tempo generare una ripida ascesa del prezzo. Dall'altro lato però, l'annuncio di un possibile intervento regolamentare, come di fatto è accaduto nel 2018, potrebbe spingere il prezzo verso il basso. L'EBA inserisce questo rischio tra i *medium risks*: l'eventualità di un intervento regolamentare costringerebbe gli utenti o a rispettare le norme che renderanno di certo il sistema, prima decentralizzato, meno vantaggioso, oppure a vendere, indipendentemente dalle condizioni di mercato che potrebbero essere non favorevoli. Lo stesso vale per l'eventualità che le autorità decidano di tassare le transazioni che hanno per oggetto valuta virtuale (*medium risk*): anche in questo caso l'utente sarà costretto a rispettare le norme oppure a vendere, registrando eventualmente una significativa perdita. Tra gli *high risk*s invece, insieme ad una totale assenza di garanzia dei depositi, di vigilanza e di tutela legale e contrattuale, il rischio più sottovalutato, a mio parere, è il mancato corso legale delle monete virtuali. Questo perché chi le acquista potrebbe rischiare di non riuscire a venderle, scambiarle con le valute virtuali oppure fare acquisti, essendo l'accettazione

[83] Per approfondimenti si rinvia a European Banking Authority, *Opinion on virtual currencies*, luglio 2014, pp. 21 – 38, www.eba.europa.eu.

di pagamento in criptovaluta su base volontaria. Di fatto si rischia di non avere un'opzione di uscita e di subire perdite nel frattempo[84].

Infine, è vero che un sistema decentralizzato garantisce una serie di vantaggi agli utenti, ma è anche vero che un intero sistema basato su un algoritmo e codici informatici non necessariamente corrisponde all'alternativa ideale. Sono infatti due gli *high risks* che derivano direttamente da questo aspetto. *In primis* l'eventualità che malfunzionamenti e blocchi operativi potrebbero mandare in *tilt* il sistema, impedendo di fatto all'utente di vendere e/o acquistare quando vuole, cioè quando le condizioni di mercato lo suggeriscono. In ultimo, non sono rari gli episodi di hackeraggio e attacchi informatici di vario genere. Nei primi mesi del 2014, l'attacco informatico che ha colpito la piattaforma di scambio giapponese Mt. Gox ha comportato la perdita di circa 750 mila bitcoins di proprietà di migliaia di utenti[85]. Le modalità con cui un *hacker* può attaccare un sistema informatico sono talmente vaste e complesse che è altamente improbabile che l'utente che si avvicina per la prima volta al criptomercato le conosca tutte e sappia difendersi[86]. Questo è esattamente ciò che intendono le tre autorità di vigilanza europea quando affermano che i soggetti scelgono di investire in criptomonete anche e soprattutto perché non sono pienamente consapevoli dei rischi che ne derivano.

2.4 Necessità di un intervento normativo: l'Unione Europea risponde

Mentre fino allo scorso anno, tanto le autorità nazionali quanto quelle europee, si limitavano a scoraggiare le banche e gli altri intermediari vigilati dall'acquistare, detenere o vendere valute virtuali[87], l'approvazione della Direttiva Ue 2018/843 (V Direttiva antiriciclaggio) in vigore da luglio 2018 sembra voler cambiare le carte in tavola. L'Europa finalmente riconosce che si trova di fronte ad un fenomeno destinato

[84] Cfr. European Insurance and Occupational Pensions Authority, *Avviso, L'ESMA, l'ABE e l'EIOPA informano i consumatori sui rischi delle valute virtuali,* 2014, www.eiopa.europa.eu.
[85] Cfr. Banca d'Italia, *Avvertenze sull'utilizzo delle cosiddette "valute virtuali"*, 30 gennaio 2015, Roma, www.bancaditalia.it.
[86] Elencheremo nel terzo capitolo tutte le tipologie di hackeraggio con cui è possibile attaccare un *personal computer*.
[87] Per approfondimenti si rinvia a Banca d'Italia, *Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee,* 19 marzo 2018, Roma, www.bancaditalia.it.

a durare nel tempo e che ha dimostrato di essere un valido strumento nelle mani di organizzazioni criminali, e che pertanto necessita di essere regolamentato. Con la V Direttiva antiriciclaggio, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che gli Stati membri dovranno recepire entro il 10 gennaio 2020, la comunità europea per la prima volta riconosce e dà una definizione esatta di criptovaluta: ‹‹una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo *status* giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente». Ne definisce inoltre i casi d'uso sottolineando che ‹‹(…). Sebbene le valute virtuali possano essere spesso utilizzate come mezzo di pagamento, potrebbero essere usate anche per altri scopi e avere impiego più ampio, ad esempio come mezzo di scambio, di investimento, come prodotti di riserva di valore o essere utilizzate in casinò *online*. L'obiettivo della presente direttiva è coprire tutti i possibili usi delle valute virtuali». Il Provvedimento europeo in questione però, a mio parere, non ha particolarmente arricchito il contesto normativo, se non per l'aver ampliato la sfera dei soggetti tenuti all'adempimento degli obblighi antiriciclaggio. Rispetto alla IV Direttiva infatti, la V Direttiva coinvolge anche la figura dei *wallet providers*, anch'essi soggetti agli obblighi di verifica della clientela e all'attuazione di controlli sistematici, come imposto in capo agli *exchangers* con la precedente Direttiva 2015/849[88]. Attraverso i soggetti obbligati, le autorità competenti dovrebbero essere in grado di monitorare le operazioni che hanno per oggetto criptomonete. Questo intervento legislativo tuttavia non colma tutte le lacune e non riesce totalmente a frenare le attività illecite: il ruolo del *wallet provider*, così come quello dell'*exchanger*, risulta essere meramente eventuale, dal momento in cui l'utente può scegliere di detenere le criptovalute in un proprio *portfolio* personale senza depositarle in un *wallet*. Il problema da risolvere resta quello dell'anonimato, caratteristica che non consente alle Unità nazionali di Informazione Finanziaria di associare l'indirizzo elettronico alfanumerico all'identità della persona fisica o giuridica che c'è dietro. Sarebbe utile considerare la possibilità di chiedere agli utenti di scegliere, su base volontaria, se consegnare un'autodichiarazione alle autorità competenti.

[88] Analizzeremo nello specifico nel terzo capitolo gli obblighi che gli *exchangers* ed i *wallet providers* sono tenuti a rispettare.

Pochi mesi dopo l'approvazione della quinta direttiva, a luglio del 2018, anche il *report* del Parlamento Europeo conferma la necessità di non vietare, e tantomeno ignorare, le criptomonete[89]. L'intervento regolamentare rappresenta una sfida per i legislatori, che in via prioritaria devono intervenire sulla questione ambientale e capire in che modo ostacolare le attività illecite che sfruttano l'anonimato e la transnazionalità delle operazioni.

A gennaio 2019, l'ESMA ha però individuato ulteriori lacune nell'attuale quadro normativo finanziario comunitario[90], delineando principalmente due problemi relativi alle attività crittografiche. Quelle attività che sono qualificate come finanziarie secondo la direttiva MiFID (*Markets in financial instruments directive*, 2004/39/EC) creano difficoltà interpretative alle autorità nel momento in cui si trovano ad applicare la normativa e ad adeguarla alle caratteristiche delle criptomonete. Quelle attività che invece non rientrano nell'attuale quadro normativo finanziario generano notevoli rischi per gli investitori, propri delle attività non regolamentate. Un priorità infatti del presidente dell'ESMA Steven Maijoor viene da lui stesso dichiarata come segue: "Al fine di garantire parità di condizioni e garantire un'adeguata protezione degli investitori in tutta l'UE, riteniamo che le lacune e le questioni identificate siano affrontate al meglio a livello europeo"[91]. Questo intervento suggerirebbe senza dubbio e cela l'intenzione di una modifica all'attuale regolamento MiFIR (*Markets in financial instruments regulation*), curandone i limiti interpretativi.

Per concludere, è chiaro che l'attuale quadro normativo, per quanto "innovativo", non sia adeguato ad un fenomeno in continua evoluzione a livello globale, e la direttiva appena entrata in vigore non è sufficiente alla prevenzione dei rischi. La vera sfida del legislatore sarà regolamentare una tecnologia nata proprio con lo scopo di non sottostare ad una *governance* centralizzata.

[89] Per approfondimenti si rinvia a M. DABROWSKI e L. JANIKOWSKI, *Virtual currencies and central banks monetary policy: challenges ahead,* luglio 2018, www.europarl.europa.eu.
[90] Cfr. European Securities and Markets Authority, *Crypto-assets need common eu-wide approach to ensure investor protection,* 9 gennaio 2019, www.esma.europa.eu.
[91] Cfr. European Securities and Markets Authority, *Crypto-assets need common eu-wide approach to ensure investor protection,* 9 gennaio 2019, www.esma.europa.eu.

3. BITCOIN E "RICICLAGGIO DIGITALE"

3.1 Normativa antiriciclaggio: nuove e recenti modifiche

La normativa antiriciclaggio attuale si basa su un articolato sistema di fonti di carattere internazionale, comunitario e nazionale. Nello specifico le regole comunitarie hanno tentato di inglobare, negli anni, l'evoluzione dei principi internazionali con lo scopo di conciliare ed uniformare il contesto normativo dei diversi Stati membri. Si tratta di un impegno europeo decennale che inizia negli anni '90 con la Direttiva 91/308/CE, I direttiva antiriciclaggio, e che registra il più recente intervento con l'approvazione della V Direttiva n. 2018/243. Le cinque direttive in materia di antiriciclaggio e contrasto al finanziamento del terrorismo (dagli acronimi inglesi AML/CFT) si sono susseguite in linea con lo sviluppo dei fenomeni che hanno lo scopo di ostacolare, attenendosi alle "Raccomandazioni" che, sebbene non siano giuridicamente vincolanti, perseguono importanti *standard* di riferimento a livello mondiale.

La prima direttiva obbligava gli enti creditizi e finanziari all'identificazione, registrazione e alla segnalazione di operazioni sospette. Dieci anni dopo, la seconda direttiva 2001/97/CE ampliò la sfera dei soggetti obbligati, coinvolgendo anche i professionisti. Nel 2005 la terza direttiva 2005/60/CE estese gli obblighi e le strategie di contrasto già sperimentate in materia di riciclaggio di denaro sporco anche al contrasto del terrorismo internazionale. In seguito poi alle Raccomandazioni del GAFI (Gruppo di Azione Finanziaria Internazionale) del 2012, che inglobavano le violazioni fiscali nell'ambito dei reati - presupposto del riciclaggio e rafforzavano gli obblighi di adeguata verifica della clientela, nel 2015 viene approvata la quarta direttiva 2015/849/UE. Quest'ultima per l'appunto ha introdotto l'obbligo di criminalizzare i reati fiscali oltre a controlli molto più stringenti per le attività e le operazioni svolte da persone politicamente esposte. Tutti i Paesi membri, in seguito all'approvazione della direttiva, hanno dovuto recepire le norme previste nella legislazione nazionale entro due anni. A testimoniare invece l'urgenza con cui il quadro normativo deve adeguarsi ai repentini cambiamenti e sviluppi tecnologici del sistema finanziario, c'è stata una riduzione del termine entro il quale recepire la quinta direttiva: tutti i Paesi membri devono adeguare entro 18 mesi la normativa nazionale ad un provvedimento europeo che modifica il precedente dopo soli tre anni. Quest'urgenza è stata probabilmente sintomo di un campanello di allarme acceso dagli attacchi terroristici che dal 2015

hanno attaccato il cuore dell'Europa principalmente in Francia, per poi colpire il Belgio, la Danimarca, la Germania. Lo sviluppo tecnologico del sistema finanziario non può che procedere di pari passo con l'emergere di nuove e più complesse modalità con cui le organizzazioni terroristiche possono reperire fondi. Lo scopo della più recente direttiva è infatti quello di rendere ancor più trasparente il contesto economico e finanziario dell'Unione.

Il provvedimento europeo[92] ha modificato la IV Direttiva intervenendo *in primis* in merito alle carte prepagate anonime, utile strumento nelle mani di potenziali membri di gruppi terroristici: è stato ridotto il limite massimo al di sotto del quale i soggetti obbligati possono non applicare le misure di adeguata modifica della clientela, da 250 a 150 euro. La V Direttiva ha inoltre ampliato i soggetti obbligati a rispettare quanto previsto dalla normativa antiriciclaggio, che ad oggi sono: i prestatoti di servizi di portafoglio digitale (*wallet providers*), ma anche i galleristi, i gestori di case d'asta e gli antiquari, nel caso in cui il valore dell'operazione o di una serie di operazioni legate tra loro sia pari o superiore a 10.000 euro. Come già accennato nel capitolo precedente e come vedremo meglio in seguito, aver coinvolto nella normativa anche i *wallet providers* non ostacolerà del tutto coloro che intendono ripulire proventi illeciti all'interno dei confini virtuali.

Ancor più recente è la pubblicazione sulla Gazzetta UE del Regolamento 2019/758[93] che integra la IV Direttiva, del 14 maggio 2019. Tale provvedimento, applicabile in tutti gli Stati membri dal 3 settembre 2019, stabilisce alcune misure specifiche supplementari che gli enti creditizi e gli istituti finanziari devono adottare in merito ai controlli antiriciclaggio, qualora operino in Paesi terzi attraverso succursali o filiazioni controllate a maggioranza. L'intervento normativo si è reso necessario dal momento in cui un ente si trova ad operare in un territorio estero la cui legislazione impedisce la piena circolazione delle informazioni in virtù, ad esempio, di una legge sul segreto bancario. Il regolamento interviene per illustrare il comportamento che l'istituto

[92] Cfr. Gazzetta Ufficiale dell'Unione europea, DIRETTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 30 maggio 2018 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE, www.eur-lex.europa.eu.

[93] Cfr. Gazzetta Ufficiale dell'Unione europea, REGOLAMENTO DELEGATO (UE) 2019/758 DELLA COMMISSIONE del 31 gennaio 2019 che integra la direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'azione minima e il tipo di misure supplementari che gli enti creditizi e gli istituti finanziari devono intraprendere per mitigare il rischio di riciclaggio e di finanziamento del terrorismo in taluni paesi terzi, www.eur-lex.europa.eu.

finanziario deve tenere nel caso in cui operi in un Paese terzo che non consente l'attuazione delle procedure previste dalla normativa comunitaria, pregiudicando in tal modo il contrasto al riciclaggio e finanziamento del terrorismo. In particolare ciò accade quando le norme del Paese in cui ha sede la succursale:

- non consentono un adeguato presidio del rischio;
- vietano o limitano la condivisione e il trattamento dei dati dei clienti a fini antiriciclaggio;
- non consentono o limitano la comunicazione di informazioni relative a operazioni sospette;
- vietano o limitano il trasferimento dei dati dei clienti agli Stati membri a fini antiriciclaggio;
- vietano o limitano la conservazione dei documenti nelle modalità prescritte dalla normativa europea.

Nei sopradescritti casi, l'istituto finanziario entro 28 giorni deve:

- comunicare alle autorità competenti il nome del Paese terzo;
- illustrare all'autorità competente in che modo la legge vigente nel Paese terzo ostacola le procedure volte al contrasto al riciclaggio e al finanziamento del terrorismo;
- provvedere affinché le succursali possano superare le restrizioni e i divieti che ostacolano le misure antiriciclaggio per mezzo del consenso informato dei clienti e dei titolari effettivi o misure supplementari.

Nel caso in cui, una volta applicate le misure specifiche previste dal Regolamento, l'istituto o l'ente non riesca a garantire la corretta prevenzione dei rischi di riciclaggio e finanziamento del terrorismo, la filiale sarà obbligata a non concludere l'operazione occasionale ovvero a porre fine al rapporto continuativo. Qualora le difficoltà applicative siano più estese, è probabile che la filiale dovrà cessare, eventualmente in modo parziale, l'attività.

La *ratio* di tale provvedimento normativo è di fondamentale importanza per un'Europa che solo da pochi mesi ha iniziato ad approcciarsi al mercato delle criptovalute con l'intenzione di adeguarvi il quadro normativo. Come già accennato, e come specificheremo in seguito in questo capitolo, la transnazionalità delle operazioni *crypto* agevola le organizzazioni criminali che approfittano di normative meno

stringenti dei Paesi terzi per poter ripulire proventi illeciti senza ostacoli. È di certo più difficile delineare un quadro normativo con questo approccio ad un contesto virtuale, che di fatto non ha confini oltre i quali operare. Pertanto è fondamentale armonizzare quanto più possibile le norme dapprima nei confini comunitari, poi a livello internazionale, in modo da poter godere solo degli enormi vantaggi che le monete virtuali garantiscono, senza offrire scorciatoie alle organizzazioni criminali.

3.2 Criptovalute come valido strumento di attività illecite

È recente anche la presa di coscienza nazionale circa la pericolosità dell'anonimato[94] che caratterizza le transazioni finanziarie effettuate mediante criptovaluta, concretizzatasi con l'emanazione del d.lgs. n. 90/2017. L'interesse che la moneta virtuale suscita agli occhi di investitori, legislatori, autorità giudiziarie e associazioni criminali cresce e decresce di pari passo con l'andamento altalenante del suo valore. La sussistenza di specifiche peculiarità del contesto, quali intertemporalità, assenza di frontiere, bassi costi e complessità dei meccanismi, richiede un intervento legislativo altrettanto minuzioso e complesso. La difficoltà nell'adeguare la normativa al fenomeno risiede nella continua evoluzione dello stesso e delle relative tecniche di riciclaggio utilizzate dalle organizzazioni criminali con lo scopo di reimmettere nei circuiti legali flussi illeciti[95]. I fattori che hanno favorito, e favoriscono, la progressiva sofisticazione delle tecniche di riciclaggio si manifestano attraverso l'innovazione finanziaria, la globalizzazione dei mercati e il sempre più rapido sviluppo tecnologico. Con internet, ciò che di certo aumenta è la "distanza" tra il riciclatore ed il capitale illecito, rendendo più difficile l'attività di indagine. Il progresso informatico-tecnologico ha peraltro permesso alla "rete", nell'attività di riciclaggio, di configurarsi sia come strumento/veicolo, sostituendo il corriere fisico con un *computer* per la fase di *placement* (c.d. riciclaggio digitale strumentale), oppure coinvolgendo anche le fasi di *layering* ed *integration*, con la creazione di nuove tecniche di riciclaggio con cui

[94] Sarebbe più corretto parlare di pseudonimato: dal registro pubblico è possibile risalire all'*account* che ha generato una specifica operazione, ma non all'identità della persona fisica o giuridica. Analizzeremo con maggior attenzione questo aspetto nei paragrafi successivi.

[95] V. McNIVEN, consulente del governo americano per il *cybercrime*, ha dichiarato che ‹‹Il *cybercrime* si evolve ad una velocità talmente elevata, che la legge non riesce a tenere il passo» in occasione di un convegno sulla sicurezza informatica nel settore bancario tenutosi nel 2005 in Arabia Saudita.

conquistare la disponibilità "fisica" di denaro, immettere capitali illeciti in circuiti leciti e rimpiegare i proventi tutto direttamente *online* (c.d. riciclaggio digitale integrale). Questa seconda tipologia è senza dubbio particolarmente pericolosa e lascia spazio all'ideazione di strategie di riciclaggio sempre più articolate, che richiede un'attività di prevenzione e contrasto altrettanto, se non di più, articolata. La difficoltà nell'adeguare la normativa al contesto risiede anche e soprattutto nell'incertezza esistente intorno alla natura giuridica della "rete". Sono principalmente tre le dottrine interpretative che si pronunciano a riguardo[96]. La prima, più pratica e poco sottile, identifica la rete come un territorio (seppur virtuale) in cui i confini tra gli Stati sono logici e non fisici. Sulla base di questo primo postulato, si sviluppa una seconda dottrina la quale specifica che è necessario tener presente la natura giuridica di internet sulla base dell'inquadramento giuridico dei singoli gestori (Paesi) sparsi per il mondo. La terza ed ultima[97], al contrario, conferisce alla rete un carattere prettamente anarchico: internet è uno spazio logico in cui gli utenti navigano in autonomia ed in assenza di controllo statale. Ed è forse proprio quest'ultima corrente di pensiero, a mio parere, a meglio descrivere un contesto come quello in esame, utenti che collaborano in assenza di regole.

La criptovaluta più gettonata, tra le 2543[98] in circolazione, nel commercio illegale, le truffe e l'acquisto di materiale pedopornografico è il bitcoin[99]. Nell'ambito del *malware*[100], e non solo, la principale valuta virtuale è strumento di:

- ***ransomware***, un *malware* che infetta il dispositivo limitandone l'accesso, richiedendo un riscatto (*ransom*) all'utente per poter recuperare la possibilità di accedere;
- ***trojan horse***, virus noto come "cavallo di Troia" perché si nasconde all'interno di un programma apparentemente innocuo, ma che una volta insediatosi nel *pc* è in grado di rubare le chiavi private degli utenti;

[96] Sul punto si veda Guardia di Finanza, Scuola di Polizia Tributaria, *Profili economici, finanziari e criminali nel contesto internazionale: analisi di alcuni paesi nell'area del centro e sud America,* 2007-2008, Quaderni 18, p. 50.

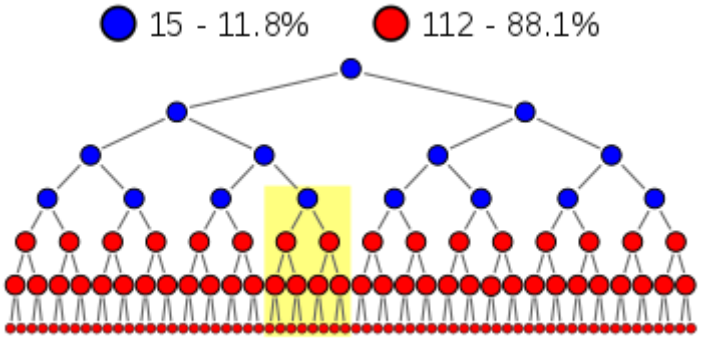
[97] Questa terza dottrina si fonda sulla *Dichiarazione di indipendenza del Cyberspazio* di John Perry Barlow a Davos (Svizzera), febbraio 1996.

[98] Dati forniti da coinmarketcap.com al 31 agosto 2019.

[99] Così S. GALMARINI, *Antiriciclaggio*, Wolsters Kluwer, 2019, Milano, a p. 751.

[100] Abbreviazione di *malicious software*, letteralmente "software malintenzionato", ideato per arrecare danni tangibili al computer o rubare di nascosto dati di vario tipo.

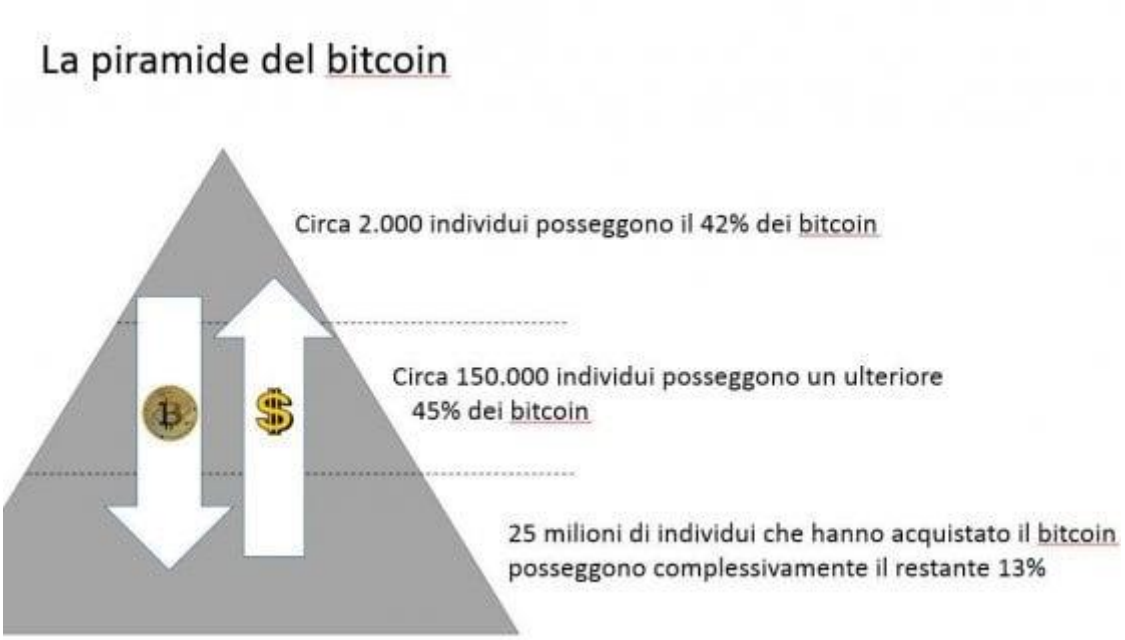
- ***clipboard malware***, virus che controlla la memoria del pc sostituendo l'indirizzo copiato dall'utente nella *clipboard*[101] di *windows* con quello dell'*hacker*;
- ***mining botnet***, software che installa segretamente un *miner*, che crea moneta virtuale che viene trasferita nei *wallet* dei criminali;
- **schemi estorsivi non cyber**: sequestri di persona, ricatti sessuali o qualunque minaccia che preveda un riscatto in bitcoin;
- **attacchi diretti a piattaforme di *exchange* e *mixing,*** che operano attraverso monete virtuali**;**
- **acquisto di materiale illecito sulla *darknet*[102]**;
- ***double spending,*** strategia che consiste in pagamenti rapidi in differenti punti vendita con la stessa provvista;
- **attività di riciclaggio *tout court***, attraverso servizi che lamentano una inadeguata *policy* antiriciclaggio;
- ***schemi Ponzi***. Lo schema Ponzi è un modello economico che promette forti guadagni ai partecipanti a patto che questi ultimi reclutino nuovi investitori. Il reclutato poi, a fondo perduto, acquista di fatto la possibilità di coinvolgere altri soggetti in cambio di un aumento delle commissioni[103].



Fonte: Wikipedia

[101] Componente del sistema operativo che gestisce lo scambio di dati tra le varie applicazioni in uso sul dispositivo.
[102] Rete virtuale privata alla quale è concesso accedere solo agli utenti autorizzati.
[103] Sul punto si veda V. BARELA, *Riflessioni in tema di network marketing per un'analisi di diritto comparato*, ottobre 2017, www.comparazionedirittocivile.it. Questo modello prende il nome da Charles Ponzi, un italiano immigrato negli USA che per primo attuò questa truffa coinvolgendo 40 immigrati.

Gli utenti blu incassano la maggior parte degli utili, la quota di profitto scende mano a mano che si percorre la piramide verso il basso. Il funzionamento del sistema Bitcoin è molto simile ad uno schema piramidale di questo tipo, come illustrato nella figura seguente.



Fonte: https://www.repubblica.it/economia/diritti-e-consumi/banche-e-assicurazioni/2019/07/06/news/lo_schema_ponzi_dei_bitcoin-230492580

Come si evince dallo schema, secondo il sito bitinfocharts.com[104], la grande maggioranza delle criptovalute appartiene a pochi investitori, presumibilmente ai primi ideatori dello schema. I dati[105] suggeriscono infatti, che solo 2 000 individui sono proprietari del 42 % dei bitcoin, per un valore di mercato pari a 75 miliardi di dollari; un ulteriore 45 % è nelle mani di circa 150 000 utenti, per un valore di mercato di 500 mila dollari, mentre 25 milioni di individui posseggono solo il restante 13 %, corrispondente a qualche migliaio di dollari. Questi utenti sono coloro che investono in Bitcoin da poco più di 2 anni, attirati dalle pubblicità che assicurano facili guadagni, e che generano i profitti degli investitori appartenenti alle fasce superiori. Le loro opportunità di guadagno dipendono dalla possibilità

[104] Sito che analizza gli indirizzi dei portafogli possessori di bitcoin.
[105] Sul punto si veda A. GUZZINI, *Lo Schema Ponzi dei bitcoin*, la Repubblica, luglio 2019, www.repubblica.it.

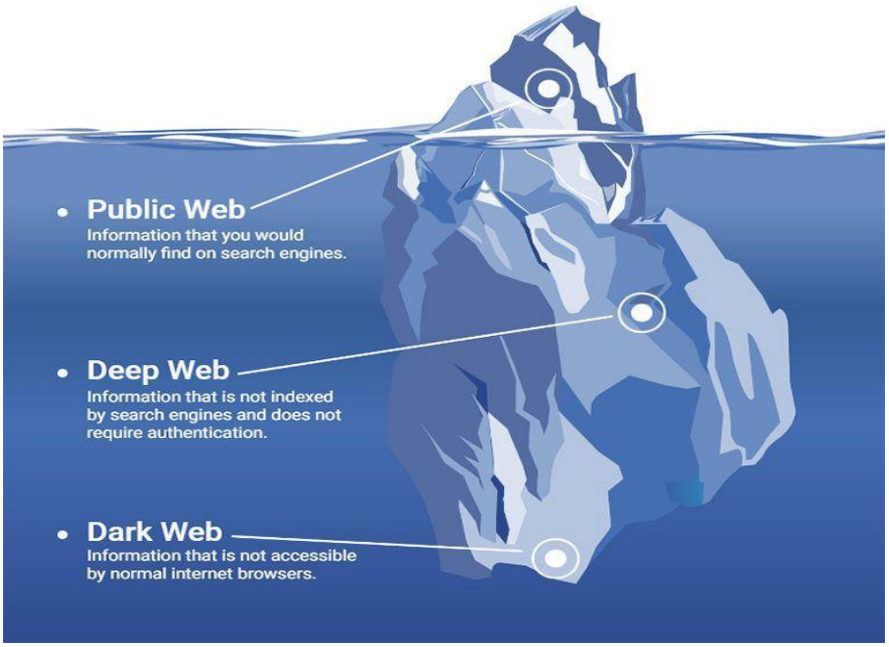
che altri entrino a far parte dello schema. Infatti, è proprio il numero di nuovi utenti a determinare il giusto funzionamento del processo piramidale. Continuando ad avvalerci dei dati di digiconomist.com, sappiamo che i *miners* consumano oltre 3 miliardi di energia elettrica ogni anno, costo che deve essere necessariamente finanziato con la vendita di bitcoin a nuovi utenti. Laddove il valore della criptovaluta, e quindi l'interesse nei confronti della stessa, dovesse scemare a causa della difficoltà nel reclutare nuovi utenti, è probabile che a subire danni saranno proprio coloro che sono alla base della piramide. In dottrina c'è chi definisce la piramide Bitcoin uno schema Ponzi 4.0: si tratta di ‹‹un asset che si per sé non sta creando nulla. Quando si comprano asset non produttivi, tutto quello su cui si conta è che ci sia qualcuno che paghi più di te perché è ancora più entusiasta.»[106]

Il contesto ideale per lo sviluppo sempre più rapido di tecniche di riciclaggio per mezzo delle criptovalute è senz'altro il <u>*deep web*</u> ("*web* sommerso"). Questo "strato" del *web* non consente un accesso immediato attraverso i comuni motori di ricerca, per questo rappresenta una sede ideale per i reati informatici. Il *deep web*, sebbene presenti tutte le caratteristiche che lo rendono idoneo ad attività di tipo criminale, non è illegale e presenta numerosi siti *web* di natura lecita, oltre a pagine ad accesso riservato o contenuti non testuali il cui accesso richiede la conoscenza di una specifica *password* o *link*. Un sotto strato del *deep web* è il <u>*dark web*,</u> sede di contenuti volontariamente nascosti ai normali navigatori. Le piattaforme appartenenti a questo più profondo strato del web nascono al servizio di attività illegali o immorali e sono principalmente finanziate da criptovalute. I mercati operanti in questo settore commerciano materiale pedo-pornografico, droghe, prodotti farmaceutici illegali, prodotti contraffatti, merce oggetto di furto, armi e sono senz'altro complici di attività legate al terrorismo, traffico di organi, estorsione e *cybercrime*, volto al furto di identità e/o dati personali[107]. La soluzione ideale sarebbe inserire nella normativa delle specifiche sanzioni per chiunque tenti di accedere ad un sito del *dark web*. Il legislatore potrebbe stabilire l'obbligo per tutte le aziende produttrici di *personal computer*, *smartphone*, *tablet* e tutti gli

[106] Così Warren Buffet, imprenditore ed economista statunitense soprannominato "oracolo di Omaha". Cfr. M. SIDERI, *Schema Bitcoin, siamo di fronte ad un Ponzi 4.0: ecco come funziona,* Corriere della Sera, dicembre 2018, www.corriere.it.

[107] Cfr. M. CHERTOFF e T. SIMON, *The Impact of the Dark Web on Internet Governance and Cyber Security,* paper series n. 6, febbraio 2015, Centre for International Governcance Innovation.

strumenti che consentono di accedere al *web*, a partire dal 2020, di programmarli in modo che, nel momento in cui l'utente proverà ad accedere ad un sito di *dark web*, la polizia postale ne riceverà immediata segnalazione. Una sanzione significativa potrebbe ridurre senza dubbio il tasso di successo di questo sotto strato del *web* inaccessibile ai più.



Fonte: https://www.aggiornamentisociali.it/articoli/dark-web-che-cos-e-e-come-funziona

Ontologicamente, le caratteristiche stesse del sistema Bitcoin, per sua natura, favoriscono la capacità della criptovaluta di "dissimulare" il valore oggetto del trasferimento nei confini della realtà virtuale, ed è qui che si riscontra una delle principali fonti di pericolo.

3.3 La capacità "dissimulatoria" del Bitcoin

Il sistema di trasferimento di moneta di cui è oggetto bitcoin ed ogni *cryptocurrency* è il primo risultato di un meccanismo che potremmo definire di "finanza democratica" che, in virtù dell'assenza di intermediari e di controllo statale, si basa su una regolamentazione preposta esclusivamente dai singoli utenti. Parte della dottrina

sostiene che la tecnologia sia il modo migliore per ottenere una reale democrazia: in seguito alle crisi che hanno sgretolato la fiducia nei confronti delle istituzioni, i codici informatici ed i *software* presentano una chiarezza ed una trasparenza di cui gli esseri umani non godono.[108] Due delle priorità, garantite infatti dall'assenza di norme ed intermediari, sono la rapidità delle transazioni e la totale libertà degli utenti, a cui gli investitori non intendono rinunciare. Collocandosi dunque nello spazio che intercorre tra la moneta elettronica e moneta fisica, la moneta virtuale ne trae i rispettivi vantaggi, ma diventando oggetto di una specifica definizione legislativa: ‹‹rappresentazione di valore digitale che non è né emessa da una banca centrale o da un ente pubblico, né è legata a una valuta legalmente istituita, non possiede uno *status* giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio, ed eventualmente per altri fini, e può essere trasferita, memorizzata o scambiata elettronicamente.»[109]

Tuttavia, il vero punto dolente del legislatore nel tentativo di individuare e prevenire rischi, è intrinseco nell'anonimato delle transazioni: al fine di garantire all'utente la *privacy* relativa ai propri dati personali e all'oggetto della compravendita rispetto al controllo statale, la sua identità rimane totalmente riservata. In realtà, non è appropriato parlare di "anonimato", bensì sarebbe più corretto avvalersi della definizione di "pseudonimato". Ogni transazione, infatti, viene registrata nel libro contabile digitale (cd. *distrubuted ledger*), dal quale è possibile risalire agli *accounts* che hanno preso parte alla relativa operazione trascritta. Sebbene il meccanismo *blockchain* sia un valido strumento utile alla tracciabilità delle transazioni in rete, ripercorrere la catena a ritroso conduce ad un algoritmo di pura matrice matematica di elaborata risoluzione, che difficilmente riconduce all'identità di una persona fisica o giuridica. Le problematiche che intralciano di fatto questo meccanismo sono principalmente due: *in primis*, le transazioni, essendo transnazionali[110], possono

[108] Intervista a Nathaniel Popper, giornalista finanziario del New York Times. Cfr. F. CHIUSI, *Cosa insegna Bitcoin alla politica 2.0,* L'Espresso, luglio 2015, www.espresso.repubblica.it.

[109] Art. 1 lett. qq) d.lgs. 25 maggio 2007, n. 231, così come modificato dal 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. Punto 2 c dell'art. 1 Directive EU 2015/849.

[110] In merito occorre distinguere l'internazionalità dalla transnazionalità. Mentre nel primo caso parliamo di un gruppo criminale che opera anche all'estero grazie ad elaborate ramificazioni, un'operazione è transnazionale quando gruppi criminali di diversa nazionalità cooperano sinergicamente per sfruttare al meglio tutte le opportunità che ogni Paese garantisce. Per approfondimenti si rinvia a Guardia di Finanza, Scuola di Polizia Tributaria, *Profili economici, finanziari*

coinvolgere controparti che operano in due Sati diversi, uno dei quali potrebbe non godere di un'adeguata normativa antiriciclaggio; *in secundis*, una transazione può essere riconducibile ad *accounts* diversi, che però di fatto appartengono allo stesso utente, data l'opportunità di poter essere titolari di più indirizzi contemporaneamente. È facile a questo punto intuire quanto un sistema che garantisce l'anonimato/pseudonimato e l'assenza di un controllore susciti un grande interesse da parte di chi cerca l'opportunità di poter ripulire proventi delittuosi o di finanziare gruppi terroristici senza "ostacoli".

Oltre alle possibilità che la natura stessa del sistema offre agli investitori che non godono delle migliori e lecite intenzioni, esistono diversi *escamotages*, individuati dal Gruppo di Azione Finanziaria Internazionale[111], utili a garantire una più solida dissimulazione:

- ***anonymizers***, *software* che consente di eseguire operazioni senza essere identificati. I più utilizzati sono quei programmi che permettono di inviare *email* senza consentire al destinatario di risalire al mittente. La strategia più recente e più gettonata dagli *hacker* è quella di far sì che l'indirizzo del mittente corrisponda con quella del destinatario. Un esempio di "*mail* truffa" che sta cercando di farsi largo tra chiunque disponga di un indirizzo di posta elettronica è il seguente:

  "Ciao!
  Come avrai notato, ti ho inviato una mail dal tuo account.
  Ciò significa che ho accesso al tuo account.
  Ti sto guardando da alcuni mesi.
  Il fatto è che sei stato infettato da malware attraverso un sito per adulti che hai visitato.
  Se non hai familiarità con questo, ti spiegherò.
  Virus Trojan mi dà pieno accesso e controllo su un computer o altro dispositivo.

e criminali nel contesto internazionale: analisi di alcuni paesi nell'area del centro e sud America, 2007-2008, Quaderni 18, p. 49.

[111] Rapporto GAFI–FATF, Report, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, 2014 in www.faft-gafi.org; TYRA, "*Bitcoin launders your dirty money but it doesn't come out very clean*.", Bitcoin Magazine, 14 dicembre 2013.

Ciò significa che posso vedere tutto sullo schermo, accendere la videocamera o il microfono, ma non ne sai nulla.
Ho anche accesso a tutti i tuoi contatti e alla tua corrispondenza.
Perché il tuo antivirus non ha rilevato il malware?
Risposta: il mio malware utilizza il driver, aggiorno le tue firme ogni 4 ore in modo che il tuo antivirus era silenzioso.
Ho fatto un video che mostra come ti accontenti nella metà sinistra dello schermo, e nella metà destra vedi il video che hai guardato. Con un clic del mouse, posso inviare questo video a tutte le tue e-mail e contatti sui social network.
Posso anche postare l'accesso a tutta la corrispondenza e ai messaggi di posta elettronica che usi.
Se vuoi impedirlo, trasferisci l'importo di 237€ sul mio indirizzo bitcoin (se non sai come fare, scrivi a Google "Compra Bitcoin").
Il mio indirizzo Bitcoin (BTC Wallet) è: 17YKd1iJBxu616JEVo15PsXvk1mnQyEFVt
Dopo aver ricevuto il pagamento, eliminerò il video e non mi sentirai mai più.
Ti do 48 ore per pagare.
Non appena apri questa lettera, il timer funzionerà e riceverò una notifica.
Auguri!";

- ***tumbler***, meccanismo che permette di collegare una transazione ad un indirizzo diverso da quello effettivo. Si tratta della strategia utilizzata nel famoso caso americano *Silk Road*[112], in cui le transazioni riconducevano ad una serie di *accounts* inesistenti;

- ***tor***, acronimo di "*The Onion Router*", *browser* che permette di accedere agli indirizzi *web* attivi sul *dark web*.

In seguito a queste analisi, non c'è dubbio sul fatto che la criptovaluta sia perfettamente idonea ad ‹‹ostacolare concretamente l'identificazione della provenienza delittuosa del

[112] Sito *web* definito come "l'Amazon delle droghe", perché nato per vendere prodotti di contrabbando. Il sito venne chiuso definitivamente dall'FBI nel 2014.

profitto illecito», clausola a cui si subordina incondizionatamente la configurazione dell'art. 648 *bis* c.p.

3.4 Il "criptoriciclaggio" nelle fattispecie codicistiche

Per individuare una fattispecie codicistica nella quale inserire il "criptoreato", bisogna innanzitutto chiarire se risulti opportuno identificare la moneta virtuale come un "bene" o "altra utilità" a cui fanno riferimento gli artt. 64 *bis* e *ter*.1. c.p. Considerando che la categoria di "beni" comprende tanto i beni materiali quanto i beni immateriali, le criptovalute possono costituire oggetto del reato in quanto la dottrina sostiene che ‹‹nella nostra interpretazione, sono beni, come definiti dal codice civile, e anche se non lo fossero rientrerebbero certamente nel concetto di altre utilità.»[113]

In un secondo momento è necessario verificare se il fatto integri il reato di riciclaggio o autoriciclaggio, cioè se l'utente "riciclatore" sia l'autore del reato oppure un soggetto terzo, nelle vesti di cambiavalute (*exchanger*), depositario online di valute (*wallet provider*), *host provider* (colui che suggerisce la piattaforma di scambio), o un *miners*. In questo secondo caso infatti, i soggetti accettano il rischio di commettere il reato ai sensi dell'articolo 648 *bis* c.p., non richiedendo né l'identità dell'utente, né la provenienza dei valori, pur essendo pienamente a conoscenza del rischio del reato di riciclaggio insito nell'anonimato[114].

In ultimo, bisogna affrontare un ulteriore *step*: capire se l'*iter criminis* si sia verificato interamente *online*, tanto il reato presupposto quanto il delitto di riciclaggio, oppure se sia stato caratterizzato da una fase *offline* (il reato presupposto), subito prima del vero e proprio riciclaggio avvenuto *online*. Il primo è esattamente il caso in cui, attraverso l'istallazione di un *malware*, la vittima è chiamata a versare una somma di denaro in bitcoin: il reato presupposto risulta già costituito da criptovaluta. A questo punto per l'estorsore, a cui il sistema garantisce già l'anonimato, sarà estremamente semplice dissimulare il profitto del reato con ulteriori operazioni, divenendo così punibile ai sensi dell'art. 648 *ter*. c.p. Come evidenziato da recenti studi frutto di una

[113] Così S. CAPACCIOLI*, Criptovalute e bitcoin: un'analisi giuridica*, Giuffrè editore, 2015, Milano, a p. 252.

[114] Capiremo nel paragrafo successivo come il d.lgs. n.90/2017 è intervenuto a riguardo.

collaborazione di Paesano[115], Interpol e Europol, la fase successiva al riciclaggio viene spesso effettuata in una criptovaluta diversa dalla precedente. Le più gettonate sono Monero o Zcash, caratterizzate da un maggior grado di anonimato rispetto a Bitcoin.

Ciò detto, è lecito considerare il reato di "criptoriciclaggio" come riconducibile alla fattispecie punibile dall'art. 648 *bis* del codice penale, il quale testualmente prevede: ‹‹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 delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000.» Ciò che rimane da verificare è la compatibilità del reato con quanto previsto dall'art. 648 *ter*. del codice penale: ‹‹Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648 *bis*, impiega in attività economiche o finanziarie, denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da cinquemila euro a venticinquemila euro.» Dovendo escludere a priori che la circolazione di bitcoin nei confini virtuali o il suo cambio in valuta virtuale possa considerarsi ‹‹attività economica o finanziaria», è necessario avvalersi delle interpretazioni riguardo la definizione di "attività finanziaria" fornite da giurisprudenza[116] e dottrina. Quest'ultima stabilisce che «è da ritenersi finanziaria l'attività così qualificata dalle disposizioni del Testo Unico in materia (nella specie il riferimento è all'art. 106 del TUF) ovverosia "l'assunzione di partecipazioni (acquisizione e gestione di titoli su capitale di imprese), la concessione di finanziamenti sotto qualsiasi forma, la prestazione di servizi di pagamento (incasso e trasferimento di fondi, esecuzione di ordini di pagamento, emissione di carte di credito o debito), l'attività di cambiovalute"»[117]. Di conseguenza, qualora l'attività si svolga interamente *online*, senza quindi l'intervento di un *exchanger*, l'operazione non può essere punibile penalmente ai sensi dell'art. 648 *ter*. Tuttavia, la condotta senza dubbio dissimulatoria del soggetto, volta ad impedire l'identificazione della provenienza delittuosa del profitto illecito, integra pienamente il delitto di riciclaggio ai sensi dell'art. 648 *bis*.

[115] Investigatore finanziario presso il *Basel Institute of governance.*

[116] Cass., sez. II, 28 luglio 2016, n. 33074, con nota di CARRELLI PALOMBI, *Autoriciclaggio*. *Prime precisazioni della Cassazione sull''elemento materiale e su quello psicologico*, settembre 2016, fascicolo n. 9, www.IlPenalista.it.

[117] Così A. GULLO, *Il delitto di autoriciclaggio al banco di prova della prassi: i primi (rassicuranti) chiarimenti della Cassazione,* in Dir. pen. proc., n 4/2017, a p. 482.

3.5 L'attività dei cambia valute e il concorso nel reato di riciclaggio: problematiche del d.lgs. n.90/2017

Nel caso alternativo, in cui l'attività si svolga in parte *online* ed in parte *offline*, risulta necessario l'intervento della figura del cambia valuta per il passaggio dall'una all'altra "zona", che inevitabilmente collabora ad ostacolare ulteriormente l'identificazione della provenienza delittuosa. È a questo punto che è inevitabile un intervento legislativo, concretizzatosi con il d.lgs. n.90/2017, con cui il legislatore nazionale fissa le prime forme di regolamentazione in materia.

Come prima prerogativa, anticipando le previsioni europee dettate dalla V Direttiva antiriciclaggio di cui abbiamo discusso nel primo paragrafo, il legislatore ha voluto definire con precisione la qualifica di cambia valute virtuali. All'art. 1, lettera ff), i cambia valute operano nelle vesti di ‹‹prestatori di servizi relativi all'utilizzo di valuta virtuale: ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale», e sono da inserire tra i soggetti destinatari degli obblighi di antiriciclaggio, in forza del d.lgs. n. 231/2007, che li definisce ‹‹operatori non finanziari» proprio con questo scopo. In virtù di quanto stabilito, coloro che svolgono l'attività di cambia valute virtuali devono:

- **essere iscritti** in un apposito registro detenuto dall'OAM[118], pena la sanzione amministrativa prevista dal comma quinto dell'art. 17 *bis*, d.lgs. n.141/2010: ‹‹l'esercizio abusivo dell'attività di cui al comma 1 è punita con una sanzione amministrativa da 2.065 euro a 10.329 euro emanata dal Ministero dell'economia e delle finanze». Il potenziale *exchanger* deve, ai sensi dell'art. 17 bis, comma 2, d. lgs. n. 141/2010, presentare specifici requisiti:

  ‹‹a) per le persone fisiche: cittadinanza italiana o di uno Stato dell'Unione europea, ovvero di Stato diverso secondo le disposizioni dell'articolo 2 del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sul decreto dello straniero, di cui

[118] Organismo degli Agenti in attività finanziaria e dei Mediatori creditizi.

al decreto legislativo 25 luglio '98, n. 286[119], e domicilio nel luogo della Repubblica;

b) per i soggetti diversi dalle persone fisiche: sede legale o amministrativa o, per i soggetti comunitari, stabile organizzazione nel territorio della Repubblica»;

- **segnalare** al Ministero dell'Economia e delle Finanze l'inizio dell'operatività su territorio nazionale;

- **aderire** al sistema pubblico antifrode.

Alle condizioni attuali inoltre, coloro che svolgono attività di cambia valute possono essere accusati di abusivismo bancario o finanziario, ai sensi della normativa appena illustrata. L'articolo 166 del TUF infatti, punisce con la reclusione da uno a otto anni e una multa da quattromila a diecimila euro chi ‹‹svolge servizi o attività di investimento o gestione collettiva del risparmio» senza esserne autorizzato.

Nello specifico, la normativa italiana pone a carico dei cambia valute i seguenti adempimenti:

- **obbligo di identificare il cliente**. La rilevanza di questa figura non è trascurabile anche e soprattutto in quanto il cambia valute è l'unico che ha la possibilità di individuare l'identità dell'utente prima che sparisca e si celi dietro una chiave alfanumerica. Questo perché il soggetto interessato ad acquistare o vendere bitcoin è obbligato a scegliere tra due alternative: recarsi di persona presso l'*exchanger*, oppure utilizzare il proprio conto corrente o altro servizio di pagamento, che in ogni caso è sottoposto ad una specifica normativa. In questo senso, l'*exchanger* è di fatto un "custode" della normativa antiriciclaggio da parte di tutti gli utenti Bitcoin**;**

- **obbligo di adeguata verifica del cliente**. Ai sensi degli artt. 17, 18 e 19 del d.lgs. n. 231/2007, l'*exchanger* deve:

[119] "Diritti e doveri dello straniero".

- verificare l'identità sulla base dei documenti e dati forniti da una fonte attendibile ed indipendente;
- identificare e verificare l'identità del c.d. titolare effettivo, il quale corrisponde alla ‹‹persona fisica, diversa dal cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è instaurato, la prestazione professionale è resa o l'operazione è eseguita»[120];
- ottenere informazioni sullo scopo e la natura del rapporto o della prestazione;
- non rinunciare ad un controllo costante durante tutto il rapporto.

L'obbligo di adeguata verifica sorge in capo ai prestatori di servizi relativi all'utilizzo di criptovaluta:

- in occasione dell'instaurazione di un rapporto continuativo[121];
- in occasione di un'operazione occasionale che preveda il trasferimento di una somma pari o superiore a € 15 000, attraverso un'operazione unica o più operazioni potenzialmente collegate;
- in occasione di un'operazione che implichi un trasferimento di fondi superiore a € 1 000;
- in ogni caso nelle ipotesi in cui:
  1) sussista il sospetto di riciclaggio o finanziamento del terrorismo, indipendentemente da deroghe, soglie ed esenzioni;
  2) sussistano dubbi sulla veridicità e/o adeguatezza dei dati utili alla verifica dell'identità;

- **obbligo di conservare i dati** relativi al cliente e alle operazioni;

- **obbligo di astensione** dall'effettuare operazioni in caso di impossibilità di procedere con una adeguata verifica del cliente e/o del titolare effettivo;

[120] Art. 1, comma 2, lett. *pp*, d. lgs. n. 231/2007.
[121] ‹‹Rapporto di durata, rientrante nell'esercizio dell'attività di istituto svolta dai soggetti obbligati, che non si esaurisce in un'unica operazione», ai sensi dell'art. 1, comma 2, lettera *ll*, d. lgs. n. 231/2007.

- **obbligo di segnalare** le potenziali operazione criminose alla UIF, presso la Banca d'Italia, nel caso in cui siano a conoscenza o sospettino ‹‹che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa», sulla base dei presupposti oggettivi previsti dall'art. 35 del d. lgs. n. 231/2007. Quest'ultimo stabilisce che ‹‹il sospetto è desunto dalle caratteristiche, dall'entità, dalla natura delle operazioni, dal loro collegamento o frazionamento o da qualsivoglia altra circostanza conosciuta, in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita»;

- **obbligo di segnalare** al Ministero dell'Economia e delle Finanze, i trasferimenti di denaro e contante effettuati per un importo pari o superiore a € 3000. In merito a questo specifico obbligo, non sono poche le criticità emerse e segnalate dal CNN (Consiglio Nazionale del Notariato). La finalità delle norme sul limite all'uso del contante è garantire la tracciabilità delle transazioni oltre una determinata soglia. È ovvio che nell'applicare questa normativa al sistema Bitcoin viene meno la *ratio* di tali norme. Per di più, la normativa antiriciclaggio distingue minuziosamente il "denaro contante", dai "fondi" e dai "mezzi di pagamento". In virtù del fatto che le valute virtuali rientrano nella definizione di "fondi" e "mezzi di pagamento", le limitazioni in capo al "denaro contante" non possono ritenersi valide per le criptovalute. È il caso dell'art. 49 del d. lgs. n. 231/2007, che fissa limitazioni all'uso di contante e alla circolazione di assegni bancari e circolari. Pertanto risulta necessario modificare tale obbligo specificando il divieto di trasferire denaro, contante e moneta virtuale, nonostante il venir meno della *ratio*;

- **obbligo di attuare procedure interne** volte a gestire il rischio di riciclaggio e di finanziamento del terrorismo (c.d. *risk based approach*). Tale approccio impone di rispettare specifici obblighi amministrativi, tra cui l'obbligo di attuare programmi di formazione permanente e aggiornamento del personale in materia di antiriciclaggio piuttosto che istituire un responsabile aziendale delle segnalazioni UIF.

La maggior parte degli obblighi sopraelencati possono essere lecitamente oggetto di *outsourcing*, delegando ad un soggetto terzo il ricorso alle prestazioni.

Di fatto, gli *exchangers* potrebbero essere chiamati a rispondere a titolo di riciclaggio o di concorso all'autoriciclaggio qualora contribuiscano a mutare dolosamente la natura del profitto pur sospettando la provenienza illecita. Questo perché ‹‹il soggetto che non ha adempiuto all'obbligo di comunicare ex d.lgs. n. 231 del 2007, art. 41 le operazioni sospette (...) non può essere visto se non come espressione dell'intento di P. di favorire S.» [122] Pertanto, l'omissione dell'adempimento dell'obbligo di operazioni sospette (c.d. SOS), concorre inevitabilmente nella condotta di riciclaggio. Coinvolgere nella normativa coloro che professionalmente hanno la facoltà di immettere nel circuito economico lecito il bitcoin "sporco", risulta necessario dal momento in cui l'autore del reato non avrebbe in nessun modo potuto, senza l'intervento dell'*exchanger*, "ripulire" quanto ottenuto attraverso la precedente operazione illecita. È più che giusto, dunque, che la normativa nelle vesti del d.lgs. n.90/2017 coinvolga la figura del cambia valute.

Le lacune del decreto risultano però evidenti in quei casi in cui le attività illecite oggetto del delitto presupposto del reato di riciclaggio sono generate e commesse unicamente *online*, e la valuta virtuale non viene trasformata in reale. I dati dimostrano che la maggior percentuale di reati di riciclaggio i bitcoin si presentano già come proventi di attività illecite, e non necessariamente fuoriescono dai confini virtuali. Di conseguenza il decreto legislativo in esame cerca di ostacolare una via d'uscita che tuttavia non è obbligatoria. Per porre rimedio a tale lacuna, la Commissione Europea ha avanzato una nuova proposta: la *Fifth Directive Anti Money Laundering*, come già accennato nel secondo capitolo, estende la normativa antiriciclaggio anche ai *wallet providers*, definiti dall'art. 3, punto 19 della suddetta direttiva come quel ‹‹soggetto che fornisce la salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali». In seguito all'approvazione[123] del quinto emendamento della Direttiva Antiriciclaggio, anche i *wallet providers* sono chiamati ad attuare controlli sistematici, nonché obbligati alla

[122] Cass., sez. II, sent. 14 luglio 2017, N. 42561.

[123] Approvato in data 19/4/2018 dal Parlamento europeo con 574 voti in favore, 13 voti contrari e 60 astensioni. Si tratta del testo frutto dell'accordo raggiunto a dicembre 2017 con il Consiglio.

verifica della clientela. Purtroppo la problematica persiste: anche la figura del *wallet provider* risulta non strettamente necessaria, essendo niente più di un "deposito informatizzato", e dal momento in cui l'utente potrebbe conservare le proprie monete virtuali in un portafoglio personale[124].

Per queste ragioni, le modifiche che il d.lgs. n. 90/2017 ha apportato al d.lgs. n. 231/2007 sembrano non procedere di pari passo con la rapidità e la complessità proprie del fenomeno finanziario in esame. Probabilmente, secondo una pura considerazione personale, l'ideale non è mettere in guardia, ed eventualmente punire, i potenziali complici del reato, bensì lavorare ed intervenire su quella che è la caratteristica più attraente del sistema: la scarsa tracciabilità delle transazioni. È irrilevante la distinzione tra "anonimato" e "pseudonimato", dal momento in cui anche se le forze dell'ordine riuscissero senza problemi a risalire all'*account* che ha generato la transazione, il codice alfanumerico non permetterà comunque di risalire all'identità fisica o giuridica dell'utente. Da non dimenticare inoltre, è la complicazione derivante dalla possibilità di un soggetto di possedere più *accounts* contemporaneamente.

3.6 Principali tecniche informatiche di riciclaggio

Dalla più remota esperienza investigativa[125], è evidente come le organizzazioni criminali siano sempre alla ricerca di nuovi strumenti. La sopradescritta natura del sistema virtuale lascia intuire che sono diverse le modalità che consentono senza sforzi alle organizzazioni criminali di convertire il bitcoin "sporco" in moneta fisica e pulita[126].

Generalmente le **transazioni** avvengono su piattaforme **peer-to-peer (exchanger non registrati)**: i due soggetti scelgono di incontrarsi in un luogo pubblico, necessariamente coperto da una rete *wi-fi*, per trasferire bitcoin al prezzo di mercato corrente in cambio di valuta legale. Il venditore riceve gli estremi del *wallet* dell'acquirente e, dopo aver ottenuto l'iscrizione nella *blockchain*, riceve il pagamento

[124] Sul punto si veda E. MESSINA, *Bitcoin e riciclaggio*, in B. QUATTROCIOCCHI (a cura di), *Norme, regole e prassi nell'economia dell'antiriciclaggio internazionale,* Giappichelli editore, Torino, 2017, p.381 e s.
[125] Cfr. U. RAPETTO, *Cyberlaundering - Il riciclaggio del terzo millennio*, Atti del Congresso internazionale tenutosi in data 11.06.1999, all'Università di Trento.
[126] Sul punto si veda S. GALMARINI, *Antiriciclaggio*, Wolters Kluwer, 2019, Milano, p. 752 e s.

in valuta legale che corrisponde all'importo versato in bitcoin soggetto al tasso di cambio corrente, più una commissione che varia tra il 10 e il 15 %, molto più alta rispetto alla commissione pari all'1 o 2 % richiesta dalle piattaforme autorizzate. Questa differenza risulterebbe essere il prezzo da pagare per non attirare l'interesse dell'autorità antiriciclaggio.

Non è da sottovalutare inoltre, la possibilità di **trasferimenti internazionali**. I proventi illeciti possono essere ancor più facilmente convertiti i bitcoin in quei Paesi noti come "paradisi fiscali" che vantano limitati controlli e una poco adeguata normativa antiriciclaggio. Questo *escamotage* va tenuto in forte considerazione nel momento in cui si lavora sulla normativa vigente, in quanto favorisce senza ostacoli il finanziamento di fondi ad organizzazioni terroristiche[127].

Le problematiche derivanti da una diversa normativa tra l'uno e l'altro Stato si riscontrano anche in un secondo caso. Nel 2014 è stato installato il primo **ATM Bitcoin** (*Automated Teller Machine*), distributori che consentono di convertire contante in bitcoin, che viene accreditato direttamente sul proprio *wallet* e viceversa. Dopo due anni, già 640 ATM erano stati installati in tutto il mondo. La postazione italiana si trova a Roma, presso il *Luiss Einlab* alla Stazione Termini. Le criticità riscontrate sono principalmente due: *in primis,* in virtù di una diversa e più lacunosa normativa antiriciclaggio, alcuni Stati non applicano le procedure di adeguata verifica della clientela e raccolta dati; *in secundis*, anche laddove la normativa preveda il rispetto di tali obblighi, gli sportelli ATM raramente hanno la capacità di distinguere un documento reale da uno ottenuto sul *dark web* o attraverso altre procedure illecite.

Altrettanto dissimulatorie risultano le **pratiche di *tumbling***, le quali consentono di spacchettare un rilevante ammontare relativo ad un'unica transazione in una moltitudine di operazioni ognuna di modeste dimensioni. Questo perché dato che le transazioni sono sempre visibili sulla *blockchain*, seppur difficilmente si riesce a risalire all'identità dell'utente, il soggetto criminale desidera evitare che un importo rilevante attiri l'attenzione delle Autorità di controllo. In questo modo, anche qualora una micro-transazione venisse intercettata e dovesse essere oggetto di sequestro, non

[127] Come osservano C. DI GREGORIO e G. MAINOLFI, *Le transazioni finanziarie sospette: controlli e adempimenti*, Bancaria Editrice, 2004, Roma, cit. a p. 65, "proprio lo strumento telematico può rendere meno efficace il sistema di segnalazione predisposto dall'autorità di vigilanza monetaria, per la possibilità offerta alla clientela di rivolgersi con una certa facilità a soggetti esteri per i quali non vigono analoghi obblighi di trasparenza ed identificazione".

inciderebbe sulla totalità dell'ammontare. Così come per le piattaforme *peer-to-peer*, le commissioni previste per i servizi di *tumbling* variano tra il 5 ed il 15 %, in base al volume dell'importo e il grado di frammentazione.

Il lavoro delle forze dell'ordine e delle Autorità preposte al controllo si fa più difficile nel momento in cui entra in gioco il mercato dell'***online gambling***[128]. Le piattaforme di questo tipo sono lo strumento ideale per chi ha bisogno di far circolare profitti di attività illecite, a fini di corruzione e riciclaggio. Innanzitutto perché l'estesa ramificazione di queste piattaforme rende difficile l'attività di monitoraggio del denaro, soprattutto perché spesso i *server* che si occupano della raccolta delle giocate e della gestione sono dislocati in Stati esteri rispetto alla sede legale ed operativa dell'impresa. In più, è altrettanto difficile individuare la posizione esatta del giocatore, il quale può senza difficoltà bluffare dichiarando un'ubicazione diversa rispetto a quella in cui realmente si trova. Le possibilità che il gioco di azzardo *online* offre alle organizzazioni criminali sono molteplici. Basti pensare che un giocatore potrebbe utilizzare una somma di denaro per perderlo volontariamente a favore di complici. Questi ultimi, dichiarando la provenienza della somma come vincita da gioco d'azzardo, di fatto avranno in tasca denaro pulito.

Queste molteplici opportunità di trasferimento di denaro hanno reso la criptovaluta un valido strumento di diversificazione nelle fonti di finanziamento delle organizzazioni terroristiche che fino a non molto tempo fa erano limitate ai confini del mercato illecito di stupefacenti, di armi e sequestro di persona. Di fatto, come affermato in dottrina, è chiaro che i confini all'interno dei quali ci si muove è una sorta di ‹‹(…) porto franco del web, in cui è possibile riservare spazi estesi alla convergenza tra affari ed applicazioni digitali, finanza senza frontiere ed imprese invisibili.»[129]

3.7 Bitcoin e finanziamento del terrorismo

La rapidità tipica delle transazioni bitconiane, nonché l'intrinseco carattere di pseudonimato, agevolano, senza dubbio, trasferimenti di ingenti somme di denaro dai

[128] Gioco d'azzardo *online*.
[129] Così P. VALENTE, *Il continente digitale*, Il Sole 24 Ore, aprile 2002, Milano, cit. a pp. 198-199.

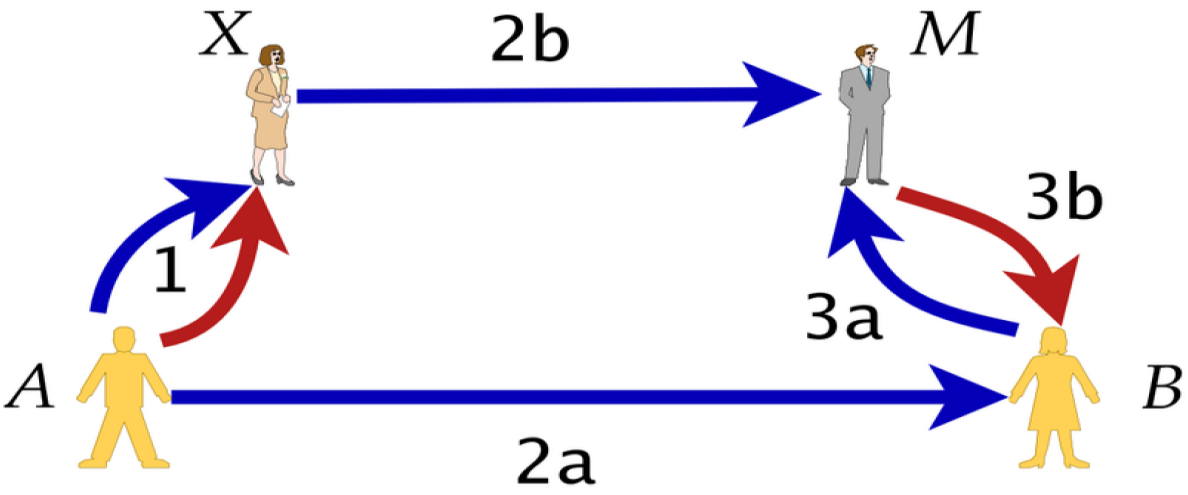
Paesi occidentali verso Paesi ad alto tasso terroristico e viceversa, ovvero da questi ultimi a favore dei cosiddetti "lupi solitari", singoli componenti del gruppo terroristico, ma "cittadini" occidentali. Bisogna in tal caso verificare che la condotta antigiuridica in esame sia sanzionabile ai sensi dell'art. 270 *quinques*.1 c.p.

Quest'ultimo disciplina il ‹‹finanziamento di condotte con finalità di terrorismo», e punisce con la reclusione da sette a quindici anni ‹‹chiunque, al di fuori dei casi di cui agli articoli 270-*bis* e 270-*quater*.1, raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo di cui all'articolo 270-*sexies* (…) indipendentemente dall'effettivo utilizzo dei fondi per la commissione delle citate condotte.» Innanzitutto, come già verificato nel primo capitolo, la moneta virtuale rientra nella categoria di "bene" o "altra utilità", a cui l'articolo in esame fa chiaro riferimento (‹‹beni (…) in qualunque modo realizzati (…)»). Rimane da analizzare il punto di vista soggettivo. Resta fuori dalla categoria dei soggetti sanzionabili ai sensi dell'art. 270 *quinques*.1 c.p. chiunque «promuove, organizza, dirige o finanzia associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico» e chi ‹‹partecipa a tali associazioni», perché punibile ai sensi dell'art. 270 *bis* c.p., e «chi organizza, finanzia o propaganda viaggi in territorio estero finalizzati al compimento delle condotte con finalità di terrorismo di cui all'articolo 270 *sexies* c.p.» perché sanzionato dall'art. 270 *quater*.1. L'articolo in esame quindi, sembra punire coloro che, estranei al gruppo terroristico, nelle vesti di soggetti terzi, agevolino e forniscano supporto economico alla realizzazione dell'operazione, a favore di un gruppo di cui non è membro. In questa categoria non sembra rientrare il "lupo solitario" di cui sopra, che subirebbe invece la sanzione prevista dall'art. 270 *bis* c.p.: reclusione da sette a quindici anni.

Tuttavia, recenti studi[130] dimostrano come in realtà la minaccia di agevolare l'attività di gruppi terroristici attraverso la rete non sia poi così reale. Il finanziamento digitale non è tra gli *escamotages* più gettonati principalmente per due motivi: il fatto che la criptovaluta non abbia corso legale, costringe i finanziatori ad affidarsi all'intervento dell'*exchanger*, che tuttavia è chiamato a rispettare la normativa illustrata nei paragrafi

[130] Per approfondimenti si rinvia a Z. K. GOLDMAN, E. MARUYAMA, E. ROSENBERG, E. SARAVALLE, J. SOLOMON-STRAUSS, *Terrorist use of virtual currencies. Containing the potential threat,* Center of New American Security, maggio 2017, www.cnas.org.

precedenti; in secondo luogo, il tradizionale sistema di trasferimento *hawala*[131]registra un tasso di successo elevato oggi tanto quanto in passato. Si tratta di un sistema di trasferimento informale basato sulla fiducia e che coinvolge, oltre al mittente e al destinatario della somma, due "banchieri *hawala*". Nato secoli fa in India e in Cina, questo sistema permetteva agli immigrati all'estero di trasferire somme di denaro alle proprie famiglie evitando onerose commissioni. Il processo è molto semplice: il mittente consegna in contanti la somma di denaro al banchiere *hawala* (passaggio 1 da A ad X nella figura sottostante) sommata alle commissioni; quest'ultimo versa sul conto corrente del suo corrispondente, un banchiere *hawala* residente nel Paese del destinatario, la somma di denaro al netto delle commissioni (passaggio 2b da X a M); in ultimo, il secondo banchiere consegna in contanti il denaro al beneficiario, trattenendo anch'egli le commissioni (passaggio 3 tra M e B). La mancanza di traccia documentale di tali flussi di denaro, rende questo processo un utilissimo strumento per riciclare denaro che però, in quanto privo di documentazione, potrebbe indurre i banchieri a trattenere le somme scegliendo di non terminare l'operazione. Proprio per questo è da sempre noto come un meccanismo basato sull'onore e sulla fiducia.



Fonte: compliancejournal.it

[131] Sul punto si veda Anonimo, *I metodi di riciclaggio: il sistema hawala,* ottobre 2017, www.compliancejournal.it

A conferma di quanto analizzato, la stessa Commissione europea considera il rischio che gruppi terroristici si affidino a canali di finanziamento che fanno uso di bitcoin mediamente basso[132]. Nello specifico, la minaccia relativa all'utilizzo di moneta virtuale a fini terroristici è quantificata con un valore pari a 2 su una scala da 1 a 4.

3.8 Possibili soluzioni volte a colmare le lacune dell'attuale normativa: alcune considerazioni a carattere personale

Sulla base delle analisi svolte in questo capitolo, abbiamo individuato le due strade che il riciclatore si trova di fronte, e percorrendo le quali avrebbe la possibilità di ripulire proventi di origine delittuosa. Da un lato, può scegliere di rivolgersi ad un *exchanger* per convertire la criptovaluta in moneta avente corso legale, ma in questo caso la normativa ha già chiaramente delineato gli obblighi che la figura del cambia valute è chiamato a rispettare a fini antiriciclaggio. Dall'altro lato, il riciclatore potrebbe decidere di trattenere i proventi all'interno dei confini virtuali. In questo secondo caso, immaginiamo che il soggetto avrà intenzione di spendere le somme ottenute attraverso attività illecite su quei siti *web* che accettano la moneta virtuale come mezzo di pagamento. Individuiamo proprio in questo passaggio una lacuna del d. lgs. n. 90/2017, il quale stabilisce che i prestatori di servizi relativi all'utilizzo di valuta virtuale sono tenuti al rispetto degli obblighi antiriciclaggio ‹‹limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute avente corso forzoso»[133]. Sembrano quindi rimanere fuori dal novero dei soggetti obbligati i prestatori di servizi relativi all'utilizzo di criptovaluta che non svolgono attività di conversione, quali ad esempio, i gestori dei siti di *e – commerce* che accettano la moneta virtuale come mezzo di pagamento. In questo modo, il riciclatore può tranquillamente ripulire il denaro sporco prenotando un viaggio su Expedia, una delle più grandi agenzie di viaggio *online*, oppure acquistando un televisore su

[132]Cfr. Commissione Europea, *Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to crossborder situations, in Eur-Lex, Brussels*, 26.6.2017 SWD(2017) 241 final.
[133] Art. 3, comma 5. lett. *i,* d. lgs. n. 231/2007.

Overstock.com[134]. O ancora, come già segnalato nei paragrafi precedenti, sarebbe ancora più facile per il soggetto reimmettere i proventi illeciti nei circuiti leciti attraverso il gioco d'azzardo *online*.

Di conseguenza è necessario stilare una serie di obblighi che tutte le attività di *e - commerce* che dichiarano di accettare pagamenti in criptovaluta dovrebbero essere chiamati a rispettare.

Sulla falsa riga di quanto previsto dal d. lgs. n. 90/2017 in capo agli *exchanger*, è necessario che:

- il *sito web* che accetta pagamenti in criptovalute e intende svolgere la propria attività nei confini italiani sia iscritto in un apposito registro tenuto dalla Polizia Postale. In allegato sarà necessario consegnare un elenco che riporta i nomi ed i dati personali dei dipendenti del gruppo commerciale[135];
- il *Compliance Manager* del sito *web* di cui sopra sia obbligato a:
  - identificare il cliente che intende pagare in criptovaluta;
  - verificarne l'identità sulla base di documenti, dati e informazioni ottenuti da fonte affidabile;
  - conservare i dati relativi al cliente e all'operazione e comunicarli immediatamente alla Polizia Postale. Quest'ultima conserverà tutti i dati relativi ai pagamenti effettuati in criptovaluta sui siti di *e – commerce* all'interno dei confini nazionali in un apposito registro;
  - segnalare l'impossibilità di concludere la vendita laddove non fosse possibile procedere con l'adeguata verifica del cliente;
  - segnalare al MEF la vendita di uno o più prodotti ad un cliente a fronte di un pagamento uguale o superiore a 3 000 euro, oppure più pagamenti la cui somma è superiore o uguale a 3 000 effettuati in meno di 30 giorni;
  - segnalare la potenziale operazione, prima di concludere la vendita, alla UIF presso la Banca d'Italia, nell'ipotesi in cui abbia motivi ragionevoli per sospettare sia in corso un'attività di riciclaggio sulla base dei presupposti

[134] I sopracitati sono solamente due dei tanti siti di *e – commerce* che si stanno adeguando ed attrezzando alla rivoluzione digitale accettando pagamenti in criptovaluta. Per approfondimenti si rinvia a I. CAIELLI, *Fare shopping con bitcoin e criptovalute: ecco chi li accetta,* giugno 2018, www.wired.it.

[135] Questo passaggio risulta fondamentale dal momento in cui un dipendente del gruppo commerciale potrebbe rivelarsi complice del criminale che intende riciclare le proprie somme con un acquisto sul sito. Avere a disposizione i dati personali dei dipendenti potrebbe in questo caso agevolare le indagini.

oggettivi previsti dall'art. 35 del d. lgs. n. 231/2007. Nello specifico, come già segnalato nei paragrafi precedenti, ‹‹il sospetto è desunto (…) tenuto conto anche della capacità economica e dell'attività svolta dal soggetto a cui è riferita».

È necessario inoltre che gli obblighi previsti ai sensi dell'art. 16 del d. lgs. n. 231/2007 siano rivolti anche ai *Compliance Managers* del gruppo di *e – commerce*, quali:

- adozione di specifici presidi interni, controlli o procedure;
- adottare programmi di formazione permanente ed aggiornamento del personale in tema di antiriciclaggio.

Ricorriamo ad un esempio pratico (e, purtroppo, estremamente semplificativo) per capire in che modo modifiche di questo tipo potrebbero da un lato rendere più difficile al riciclatore ripulire i suoi proventi, e dall'altro facilitare l'attività di indagine delle autorità. Supponiamo che il soggetto leso, Mario Rossi, abbia scoperto che il suo *pc* è stato infettato da un *roansomware*, un *virus* che impedisce l'accesso al proprio *software* se non attraverso il pagamento di un riscatto in criptovaluta. Il signor Rossi paga la somma richiesta, e si reca presso la Polizia Postale per sporgere denuncia. Il soggetto leso che paga il prezzo non incorre in alcun profilo penale[136]. A questo punto la Polizia Postale, per mezzo dell'apposito registro in cui sono riportati tutti i pagamenti effettuati in criptovalute su tutti i siti di *e – commerce* che accettano moneta virtuale come mezzo di pagamento, sarà in grado di identificare un gruppo di utenti che hanno speso l'esatta somma che il signor Rossi ha pagato, con un solo acquisto o più acquisti. È vero che il soggetto che ha ricevuto la somma di denaro dal signor Rossi potrebbe aver consegnato i proventi nelle mani di diversi complici che hanno poi speso le somme in diversi siti di *e – commerce* in giorni diversi, e di conseguenza il registro di cui sopra potrebbe non essere particolarmente utile, ma potrà senz'altro agevolare l'attività di indagine. Le autorità competenti potranno risalire facilmente alle identità di potenziali criminali, e non basarsi semplicemente su dei codici alfanumerici che celano i dati della persona fisica che effettua i pagamenti in criptovaluta.

[136] Così Alessandra Bisi, avvocato dello studio Bisi – Stella, intervistata da C. PANERAI, *Pagare il riscatto per CryptoLocker è lecito o si commette reato?,* febbraio 2016, www.achab.it.

È inoltre necessario "educare" gli utenti: chiunque sia proprietario di un *personal computer, smartphone* o *tablet* deve sapere quali sono gli organi competenti a cui rivolgersi in caso di hackeraggio. Questo perché, ad esempio, l'art. 615 c.p. che punisce chiunque acceda abusivamente ad un sistema informatico o telematico protetto da misure di sicurezza, è volto a sanzionare un reato che è punito a querela di parte. Ciò vuol dire che il soggetto leso deve necessariamente sporgere una querela presso la polizia postale chiedendo, di fatto, che la persona che ha commesso il reato venga punito, altrimenti la norma non è applicabile[137].

Per quanto concerne i siti di gioco d'azzardo ed i casinò *online*, è di fondamentale importanza obbligare il giocatore a dichiarare la propria identità certificata attraverso un documento in corso di validità. Questo non rappresenterà un grande problema per quel giocatore che non ha nulla da nascondere, ma di certo indurrà il riciclatore a scegliere un'altra strada per ripulire proventi illeciti.

Altrettanto giusta era l'intenzione del primo ministro della Corea del Sud, Lee Nak-yeon, che nel dicembre del 2017 annunciò di voler vietare le transazioni anonime[138]. A mio parere, è lo pseudonimato delle transazioni che, più di tutte le altre caratteristiche proprie del contesto, suscita l'interesse e facilita i piani dei potenziali criminali. È pertanto necessario intervenire quanto prima a riguardo, seguendo l'esempio del primo ministro Nak-yeon.

In ultimo, merita particolare attenzione la questione della transnazionalità, cioè l'opportunità di collaborare con organizzazioni criminali residenti all'estero. Per quanto utopica, la soluzione ideale sarebbe costruire una normativa che non solo superi i confini nazionali, ma anche quelli della comunità europea, in modo da impedire alle organizzazioni criminali di godere delle opportunità che i Paesi che non prevedono una severa normativa antiriciclaggio garantiscono. Sarebbe opportuno quindi lavorare ad un trattato internazionale che coinvolga e richieda soprattutto la collaborazione dell'UNODC, l'Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine, tra gli obiettivi del quale spicca appunto il contrasto al crimine organizzato transnazionale. Solo in presenza di una normativa a carattere

[137] Così Alessandra Bisi, avvocato dello studio Bisi – Stella, intervistata da C. PANERAI, *Pagare il riscatto per CryptoLocker è lecito o si commette reato?,* febbraio 2016, www.achab.it.
[138] Per approfondimenti si veda L. ZORLONI, *Stretta in Corea sull'uso dei bitcoin. Chi altro vuole regolare la criptovaluta?*, dicembre 2017, www.wired.it.

internazionale sarebbe possibile considerare la criptovaluta come una vera valuta a tutti gli effetti.

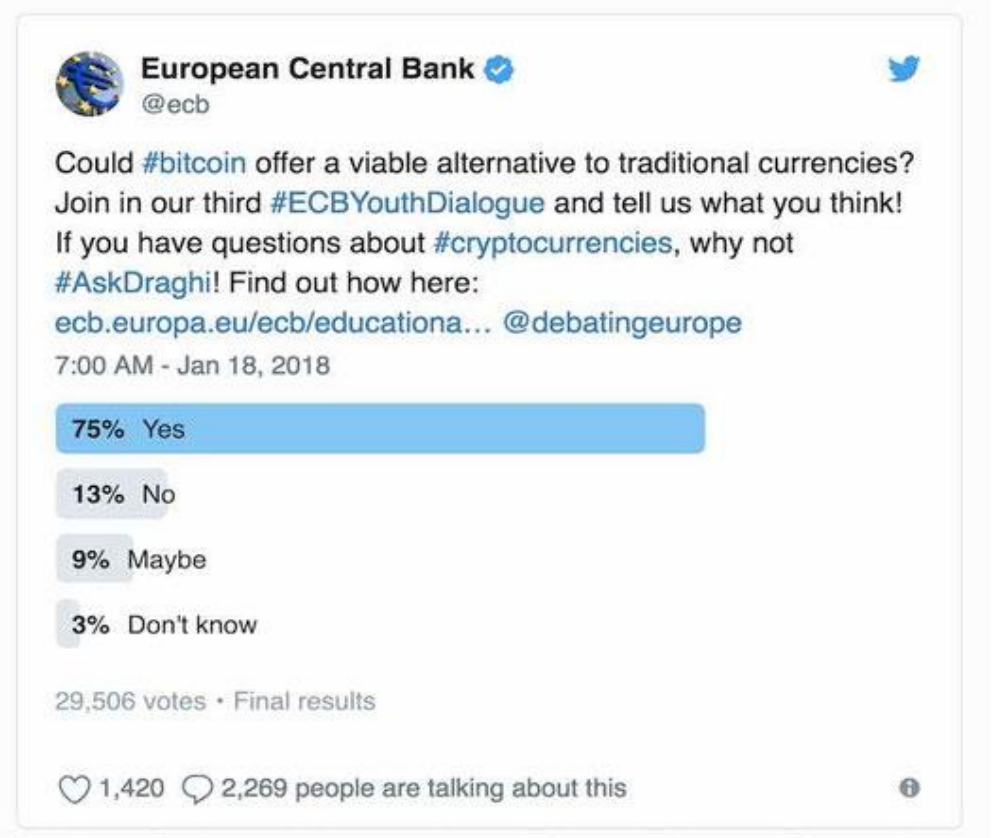
4. IN ARRIVO LA CRIPTOVALUTA DI FACEBOOK: ANALISI SWOT DI UNA POTENZIALE *GLOBALCOIN*

4.1 L'identikit della criptovaluta ideale

Nonostante i numerosi rischi che il criptomercato comporta e le lacune normative che non garantiscono una solida prevenzione degli stessi, i cittadini italiani ed europei sembrano pronti alla digitalizzazione finanziaria ed entusiasti delle nuove opportunità che quest'ultima offre. Analizzando dapprima i confini nazionali, osserviamo che sono oltre 600 i punti vendita che accettano bitcoin come mezzo di pagamento, soprattutto al nord, circa 100 in più rispetto allo scorso anno.

Fonte: Quibitcoin.it

Sintomo di un sempre più forte desiderio di spezzare i confini nazionali e comunitari e di essere parte di un sistema finanziario globale, anche i cittadini europei, già a gennaio del 2018, considerano il bitcoin una valida alternativa alle valute tradizionali.



Fonte: www.twitter.com

Sono ben oltre 22 mila i cittadini europei che, come illustrato nel secondo capitolo, non sono disposti a rinunciare a tutti i vantaggi offerti dal criptomercato (economicità, rapidità, sicurezza, anonimato, assenza di controllo) e che probabilmente non sono coscienti degli innumerevoli rischi che il *cryptotrading* comporta.

Proviamo ad ipotizzare i caratteri di una criptovaluta ideale, creata *ex novo*, e che possa evitare *ex ante* quei rischi finora elencati. Le autorità nazionali ed europee hanno sempre tentato di disincentivare l'utilizzo di criptovalute soprattutto in virtù di una tutt'altro che contenuta volatilità. Lo stesso prezzo del bitcoin negli ultimi 30 giorni ha raggiunto al ribasso il valore di € 8 549,80 per poi risalire fino a raggiungere il valore di € 9 890,25, per un delta che supera ampiamente i mille euro[139]. Per ovviare a questa problematica, la nostra valuta virtuale ideale dovrebbe essere una ***stablecoin***,

[139] Dati forniti da www.coinmarketcap.com al 21 settembre 2019.

una valuta coperta da riserve che garantiscano un tasso di cambio con le principali valute tradizionali pressoché costante.

Tra i rischi più allarmanti, spicca inoltre la mancanza di autorità centrali, sostituite nel caso del Bitcoin dagli stessi utenti, i quali hanno il compito di verificare e convalidare le transazioni. Per quanto la grande numerosità degli utenti possa in qualche modo garantire la sicurezza delle transazioni, perché è improbabile che milioni di persone scelgano di commettere una frode nello stesso momento, è un rischio che non possiamo permetterci di correre. Come già accennato, nel 2016 pochi *miners* cinesi controllavano più del 50 % della rete Bitcoin[140]. Di conseguenza è necessario creare una **nuova *blockchain*** che sia però **controllata da soggetti "*trusted*", che per primi hanno investito nel progetto**, e che per questo non daranno ragione di dubitare del corretto funzionamento della piattaforma volto esclusivamente allo scopo per cui è stata ideata: facilitare i pagamenti.

L'ultimo ostacolo da arginare risiede nell'anonimato delle transazioni, forse la caratteristica più pericolosa del criptomercato. È di fondamentale importanza, a mio parere, eliminare totalmente questo aspetto tra le caratteristiche di una criptovaluta ideale, magari chiedendo agli utenti di scaricare sul proprio *smartphone* o *tablet* un'app che, nelle vesti di un *wallet provider*, offra un portafoglio digitale agli utenti solo in seguito ad **una registrazione che richiede dati personali**. Da quel momento l'utente potrà operare sulla piattaforma *blockchain* per mezzo di un codice alfanumerico attraverso il quale però si possa facilmente risalire all'identità della persona fisica o giuridica: una sorta di codice fiscale.

Per riassumere, la criptovaluta ideale deve essere **stabile**, operare in una **nuova *blockchain* gestita da soggetti *trusted***, la quale permette agli utenti di effettuare una transazione solo attraverso un **codice alfanumerico che suggerisce i dati personali**. Nel delineare però l'identikit di questa valuta virtuale, ci accorgiamo facilmente che questa potenziale moneta ottimale è già stata progettata e si chiama Libra. Si tratta della *cryptocurrency* di Facebook, annunciata dallo stesso Mark Zuckerberg lo scorso giugno e il cui lancio è previsto per il 2020. Cerchiamo a questo punto di capire, attraverso un'analisi SWOT, se questa moneta rispecchia il nostro identikit e quali

[140] Per approfondimenti si rinvia a A. BAI, *Bitcoin al capolinea secondo Mike Hearn*, 2016, www.hwupgrade.it.

sono gli aspetti da curare e le lacune dal colmare prima del lancio, per fare di Libra la criptomoneta ideale.

4.2 Punti di forza

Come già accennato, la rete Libra si baserà su una *blockchain* **centralizzata**, ‹‹evolutiva ed affidabile» che ‹‹permetterà la creazione di un nuovo ecosistema finanziario con nuovi utilizzi a favore dell'innovazione e dell'inclusione finanziaria»[141]. Questa struttura permette infatti di sfruttare tutte le potenzialità operative di una *blockchain*, ma che gode per di più di un "controllo dall'alto". Infatti a gestire la criptomoneta sarà un consorzio composto attualmente da 28 membri, la Libra Association. Nello specifico, oltre a Facebook, hanno scelto di aderire a questo progetto anche Mastercard, PayPal, PayU, Stripe e Visa appartenenti al settore pagamenti, ma anche operatori *e-commerce* come Ebay, Spotify e Uber, oltre a Vodafone e Illiad per il mondo delle telecomunicazioni[142]. Il consorzio di Libra Association, con sede a Ginevra, avrà il compito di gestire la *blockchain* e autorizzare le transazioni, nelle vesti di un intermediario "*trusted*". Sul *whitepaper* si legge: ‹‹L'associazione è pensata per facilitare le operazioni di Libra, per gestire la riserva che mantiene stabile il valore della valuta e per coordinare gli accordi tra i suoi *stakeholder*. Ciascuno dei membri dell'associazione mantiene un nodo della rete di Libra ed elegge un rappresentante nel consiglio dell'associazione, che prende le decisioni per votazione. Ciascun membro fondatore non può detenere più di un voto o dell'1% del totale dei voti, per impedire che nessun membro assuma un controllo eccessivo sulla rete». Il loro diritto di voto è stato di fatto acquistato con un investimento iniziale pari ad almeno 10 milioni di dollari, da parte di ciascun membro[143].

Un altro compito del consorzio che "governa" la Libra Blockchain è quello di gestire le riserve utili a mantenere **stabile** il valore della criptomoneta. Dal *whitepaper*

[141] Così si legge sul *whitepaper* riportato sul sito ufficiale www.libra.org.
[142] I nomi dei 28 *partners* sono disponibili nella sezione dedicata sul sito ufficiale www.libra.org.
[143] Così Ido Sahe Man, presidente di Saga Foundation, intervistato da R. BROWNE, *Bitcoin vs Libra: Here are the key differences between the two cryptocurrencies,* luglio 2019, www.cnbc.com.

sappiamo che tali riserve corrispondono ad un paniere di ‹‹asset a bassa volatilità, come depositi bancari e titoli di Stato a breve termine denominati in valute di Banche centrali stabili e ad alta reputazione». A differenza di tether, la *stablecoin* analizzata nel secondo capitolo e le cui riserve erano di fatto dollari, nel caso di libra le criptomonete emesse sono coperte da *asset* reali che matureranno degli interessi. Questi ultimi andranno a coprire i costi del sistema, garantiranno basse commissioni e pagheranno dividendi agli investitori, cioè i membri della Libra Association[144]. Nella pratica, nel momento in cui compriamo € 5 di libra, l'associazione li investirà in attività a bassa volatilità da banche centrali stabili ed il compratore avrà in tasca una quota di tale investimento. Nel caso in cui lo stesso compratore avrà di nuovo bisogno di quei € 5, una parte delle attività sarà venduta e la stabilità degli *asset* garantirà al soggetto di riottenere proprio € 5 (o poco più o poco meno). È un aspetto che trasforma la valuta digitale in una moneta quasi più "concreta", perché dal valore certo, senza rinunciare alla rapidità, facilità ed economicità delle operazioni virtuali. Immaginiamo inoltre che gli ideatori stiano lavorando all'elaborazione di un tasso di cambio fisso rispetto ad ogni valuta tradizionale, per evitare che gli scambi aventi ad oggetto valute diverse consentano speculazioni.

Un'altra problematica che libra potrebbe aiutarci a risolvere è quella dell'anonimato, anche se il *whitepaper* di Libra Association non ci suggerisce molto a riguardo, limitandosi ad affermare che ‹‹Libra continuerà a valutare nuove tecniche che migliorino la *privacy* nella *blockchain*» e che ‹‹l'utilizzo della tecnologia *blockchain* consente agli utenti di mantenere uno o più indirizzi che non sono collegati alla loro identità del mondo reale». Questa considerazione potrebbe rivelarsi preoccupante perché, proprio come Facebook, pare di capire che gli utenti possano creare uno o più profili *fake* con cui effettuare pagamenti. Ciò che però distingue questa piattaforma dalla originale Bitcoin, non dimentichiamo, è la presenza di un intermediario centralizzato. I membri del consorzio infatti, da Facebook a PayPal, o a Mastercard, sono noti per negare i loro servizi a coloro che non rispettano le regole previsti nei propri regolamenti. Si tratterebbe quindi di stabilire regole più ferree e non consentire a chiunque, come di fatto succede con Bitcoin, di operare all'interno della piattaforma. Si chiama Calibra la società sussidiaria di Facebook che, nelle vesti di *wallet provider*, fornirà portafogli digitali e permetterà agli utenti di accedere e partecipare al *network*

[144] Per approfondimenti si rinvia a S. COSIMI, *Libra, ecco come funziona la moneta di Facebook,* La Repubblica, giugno 2019, www.larepubblica.it.

di Libra e potrebbe essere proprio questa la chiave che potrebbe non permettere a tutti di accedere ai servizi finanziari. Di fatto si tratterà di un'applicazione con cui salvare, inviare o spendere libra direttamente dal proprio *smartphone*, perchè collegata a Whatsapp e Messenger. Lo stesso Mark Zuckerberg ha dichiarato: ‹‹Calibra sfoggerà un team dedicato di esperti che combatterà gli usi fraudolenti della valuta, doteremo Libra di una protezione antifrode, così che se i fondi vengono persi noi li rimborseremo»[145]. Questa affermazione ci lascia intuire che usufruire dei servizi offerti dalla società non sarà così facile come per Bitcoin e soprattutto che **non saranno pochi i controlli e le verifiche a cui gli utenti che intendono far uso di libra saranno sottoposti**. Ciò che in realtà potrebbe spaventarci è l'altro lato della medaglia: sappiamo che Facebook in merito a *privacy* non presenta una fedina penale totalmente pulita, e sembrerebbe sorgere il problema inverso. Chi ci garantisce che in questo modo la Libra Association, e di conseguenza i relativi membri, non entrino in possesso di informazioni, che non si limitano ai nostri dati personali, attraverso Facebook? Personalmente credo che se questo è il prezzo da pagare per rinunciare all'anonimato delle transazioni, ben venga. È pur vero che chi decide di iscriversi su un *social network* è cosciente del fatto che nel momento in cui rende pubbliche informazioni, *hobbies*, passioni ed abitudini ne perde, di fatto, la proprietà.

In ultimo, non dobbiamo ignorare la problematica ambientale. È da imputare all'attività di *mining* del bitcoin circa l'1% del consumo mondiale, più di quanto non consumi lo Stato di New York[146]. La produzione e la conservazione di Libra però, in virtù del funzionamento della piattaforma che non prevede il *mining*, non richiederà la stessa potenza di calcolo e lo stesso Facebook, inoltre, sta lavorando per rendere i propri ***data center* maggiormente ecosostenibili**[147]. Di conseguenza, se la Libra Blockchain riuscirà a "rubare" qualche utente alle tradizionali criptovalute, anche se riconosciamo che lo scopo degli utenti è ben diverso, l'eccessivo consumo di energia elettrica sarà notevolmente ridotto.

Sono rari i commenti negativi e poco fiduciosi nei confronti di questa nuova *stablecoin*, se non in merito alle lacune normative in cui il progetto andrà

[145] Cfr. S. COSIMI, *Libra, ecco come funziona la moneta di Facebook,* La Repubblica, giugno 2019, www.larepubblica.it.
[146] Stima formulata dall'Università di Princeton. Per approfondimenti si rinvia a la Repubblica, *Bitcoin, produrli ormai consuma più energia di uno Stato*, agosto 2018, www.larepubblica.it.
[147] Per approfondimenti si rinvia a QuiFinanza, *Facebook Libra: perché la nuova moneta di Zuckerberg non farà bene all'ambiente,* giugno 2019, www.quifinanza.it.

incastrandosi. Basti pensare che questo strumento permetterà a oltre 1,7 miliardi di utenti *unbanked*, che non dispongono cioè di un conto corrente bancario, di accedere a servizi finanziari volti a facilitare la stessa quotidianità di ognuno, offrendo la possibilità di pagare una fattura direttamente dal proprio *smartphone*, senza doversi recare di persona presso un intermediario autorizzato[148]. Certo è che integrare diverse categorie di servizi, e cioè permettere di effettuare pagamenti per mezzo di un'applicazione di messaggistica istantanea come Whatsapp o Messenger, crea ulteriori dimensioni di rischi in tema di sicurezza e privacy[149]. Quello che è ovvio è che le istituzioni, dal governo, alle banche centrali, alla commissione europea non può aspettare che accada restando a guardare[150], come di fatto è già accaduto per le criptovalute. È necessario individuare i *gap* normativi e colmarli prima che anche libra diventi uno strumento nelle mani delle organizzazioni criminali, gettando via una grande opportunità che Zuckerberg sta offrendo al sistema finanziario globale.

4.3 Debolezze

Siamo senza dubbio di fronte ad un nuovo e potentissimo strumento digitale, considerando il raggio d'azione globale del *social network* che c'è dietro, il più famoso al mondo e che conta oltre 2 miliardi di utenti. Il problema è che tale strumento andrà ad incastrarsi in un vuoto normativo, così come affermato dal presidente dell'EBA Jose Manuel Campa[151]. Da un lato le attività finanziarie sono regolamentate dalle leggi comunitarie in materia di investimenti, dall'altro i pagamenti elettronici devono rispettare quanto previsto dalla normativa dei pagamenti. Le criptovalute, ed in particolare libra, vanno a posizionarsi proprio lungo il confine che intercorre tra le due zone. Dato che attualmente non esiste un'agenzia indipendente a livello europeo che possa contrastare il riciclaggio di denaro ed il finanziamento del terrorismo, tale ruolo

[148] Così Valeria Portale, Direttore degli Osservatori Innnovative Payments e Blockchain & Distribuited Ledger del Politecnico di Milano. Cfr. F. META, *Facebook svela Libra, Zuckerberg: "Facile come inviare foto"*, giugno 2019, www.corrierecomunicazioni.it.

[149] Così Raffaele Mauro, manager director di Endeavor Italy. Cfr. F. META, *Facebook svela Libra, Zuckerberg: "Facile come inviare foto"*, giugno 2019, www.corrierecomunicazioni.it.

[150] Così Francesco Boccia, deputato del Partito Democratico. Cfr. F. META, *Facebook svela Libra, Zuckerberg: "Facile come inviare foto"*, giugno 2019, www.corrierecomunicazioni.it.

[151] Cfr. A.DINI, *Libra, l'Eba: "C'è un vuoto normativo, Facebook potrebbe avere gioco facile",* settembre 2019, www.corrierecomunicazioni.it.

viene delegato alle autorità nazionali, le quali fanno dell'EBA una "tigre di carta"[152], con l'unica facoltà di dettare le linee guida.

La prima problematica sorge in capo all'idoneità delle monete alternative alle valute tradizionali di saldare un debito. L'art. 1277 del codice civile limita espressamente questa facoltà alle monete aventi corso legale, escludendo di fatto le criptovalute e di conseguenza anche libra, a meno che il creditore non acconsenta (art. 1197 c.c.). In virtù di quanto espresso, nessuna attività commerciale sarà pertanto costretta ad accettare un pagamento in critpovaluta, il che potrebbe creare un certo tipo di disagio a quel turista che sceglie l'Italia come meta e non ha intenzione di convertire le proprie monete in euro. Si tratta per lo più di un rischio "pratico".

Come già accennato, una parentesi particolare merita la questione della *privacy*. Il rischio è che tramite questa intersezione tra servizi che permette di inviare denaro attraverso un *social* con le stesse modalità con cui siamo soliti inviare foto, Zuckerberg, ed i relativi *partners*, potrebbero essere in grado di acquisire più informazioni personali di quanto già non facciano. Pertanto, nell'interesse della comunità europea, è necessario che questo progetto si attenga a quanto previsto dal GDPR Regolamento UE 2016/679, il quale disciplina il trattamento dei dati personali dei cittadini europei da parte di persone, società o organizzazioni.

In ultimo, se Calibra nasce come uno strumento che potenzialmente potrà offrire agli utenti i tradizionali servizi bancari, quale anche quello del mero "deposito", è bene che la società acquisisca la licenza bancaria, cioè un'autorizzazione legale per poterlo fare. È un passaggio di fondamentale importanza dal momento in cui l'ottenimento della licenza prevede il soddisfacimento di una serie di requisiti relativi a capitale minimo, applicazione delle normative, sicurezza e protezione dei dati. Se Calibra sarà legalmente autorizzata ad offrire servizi bancari, non dovremmo aver motivo di dubitare delle buone intenzioni di chi gestisce le nostre criptomonete in libra. A conferma di ciò, lo stesso Mark Zuckerberg ha affermato, in seguito ad un incontro nello studio ovale con l'attuale presidente Donald Trump e dopo esser stato ricevuto a

[152] Così A.DINI, *Libra, l'Eba: "C'è un vuoto normativo, Facebook potrebbe avere gioco facile",* settembre 2019, www.corrierecomunicazioni.it.

Capitol Hill da parlamentari democratici e repubblicani, che Libra non sarà lanciata senza il via libera da parte dei regolatori[153].

Pertanto, per quanto rilevante, l'attuale assenza di regole sembra essere l'unica debolezza. Probabilmente la mancanza di un preciso quadro legislativo riguardo il criptomercato rispecchiava la consapevolezza che un intervento normativo più o meno rigido avrebbe determinato la morte del *cryptotrading*[154], che nasce, come ricordato più volte, con l'intento di operare in un contesto decentralizzato, sfuggendo a quello tradizionale. L'entità però del progetto in esame e la sistematicità di un fenomeno che entra direttamente nelle case di 2 miliardi di utenti non permette di giocare di strategia e bisogna correre ai ripari quanto prima. Se il rischio più pericoloso si nasconde dietro l'anonimato delle transazioni, è necessario che Libra Association garantisca di essere più che rigido nella verifica dei dati di chi sceglie di servirsi di Calibra. Avere a che fare con una *blockchain* nata *ex novo* che ci permette di stabilire le regole del gioco, non è una possibilità da sottovalutare. Questo strumento potrebbe suscitare l'interesse di una parte degli utenti Bitcoin, lasciando sulla piattaforma originale gli speculatori ed i criminali.

C'è da dire che non basta ovviamente farsi trovare pronti all'interno dei confini europei, trattandosi di un fenomeno globale è fondamentale fare squadra a livello internazionale, necessità che desta non poche preoccupazioni[155].

4.4 Opportunità

Anche se non sono poche le preoccupazioni che l'arrivo di Libra sta destando, non si può negare che si tratta di uno strumento che di certo conferirà all'intero sistema economico una serie di vantaggiose opportunità di crescita. In questi ultimi ormai

[153] Per approfondimenti si rinvia a V. ROBECCO, *Zuckerberg a Washington: Libra con l'ok delle autorità e i social non si vendono,* il Giornale, settembre 2019, www.ilgiornale.it.

[154] Così Fabio Di Vizio, pm della Procura di Firenze e uno dei massimi esperti in Italia nella lotta all'evasione fiscale e al riciclaggio. Cfr. R. GALULLO e A. MINGUZZI, *Facebook, con Libra alto rischio di evasione e riciclaggio*, Il sole 24 ore, giugno 2019, www.ilsole24ore.it.

[155] «Quando sedevo io in consessi europei e internazionali erano altri tempi. Quando si fece l'euro, ad esempio, il clima era diverso e c'era la volontà di cooperazione e collaborazione tra Paesi europei che si fidavano l'uno dell'altro», così Vincenzo Visco, già ministro delle Finanze e del Tesoro tra il 1996 e il 2008. Cfr. R. GALULLO e A. MINGUZZI, *Facebook, con Libra alto rischio di evasione e riciclaggio*, Il sole 24 ore, giugno 2019, www.ilsole24ore.it.

quasi vent'anni abbiamo tutti avuto modo di verificare in prima persona i benefici che la moneta unica garantisce, seppur limitatamente ai confini comunitari. In questo caso però, abbiamo a che fare con una moneta che non solo sarà unica a livello globale, il che non farà che amplificare i vantaggi di cui parlavamo, ma assorbirà anche tutti i benefici propri di uno strumento virtuale.

Il primo settore a trarne beneficio sarà sicuramente il turismo. Avere nel proprio portafoglio una moneta che permette di pranzare, salire sui mezzi pubblici e visitare i musei di uno Stato estero senza dover convertire la propria valuta non può che incentivare tutti i cittadini del mondo a viaggiare di più. Alle condizioni attuali, solo per fare un esempio, il turista italiano a Londra decide di convertire, generalmente all'arrivo, un determinato ammontare di euro in sterline. Se poco prima della partenza però, il turista ha terminato tutte le sterline che aveva nel portafoglio, rinuncerà ad acquistare un *souvenir* al negozio dell'aeroporto al prezzo di 5 sterline, essendo una cifra troppo bassa per spingere il turista a convertire altri euro. L'attività commerciale in questione però, subendo gli esiti di questo episodio con tutti i turisti passanti per l'aeroporto, perderà non pochi incassi. È vero che se fosse possibile pagare in criptovalute, ad esempio in bitcoin, il problema sarebbe risolto, ma non dimentichiamoci che libra è una criptovaluta stabile, mentre il prezzo del bitcoin è altamente volatile. Sarebbe poco pratico per il turista seguire in tempo reale l'andamento del prezzo del bitcoin per capire qual è il momento giusto per prendere il caffè al bar.

Nel paragrafo precedente, abbiamo evidenziato la preoccupazione delle autorità riguardo la *privacy* degli utenti ed il trattamento dei dati personali. Dall'altro lato però, pagare con una moneta che è, potremmo dire, autografata da chi ne fa uso, potrebbe tradursi in un grande vantaggio per le attività commerciali. In che modo? Se Calibra, al momento del pagamento in libra, fornisse al venditore alcuni dati, garantirebbe la tracciabilità degli acquisti. Ovviamente l'applicazione non dovrà dichiarare niente che non sia già scritto, ad esempio, sulla carta d'identità. Ma se una piccola attività in centro storico avrà la possibilità di conoscere anche solo l'età, il sesso e la professione del compratore, sarà in grado di capire meglio cosa vendere, quando vendere e quando scontare. Prendiamo il caso di un piccolo ristorante in centro storico. Se il proprietario conosce l'età e l'occupazione dei suoi clienti, potrà perfezionare la propria offerta di conseguenza. Se ad esempio, secondo una precisa analisi statistica, nota che il

mercoledì a pranzo i suoi clienti sono soprattutto studenti, mentre il venerdì sera il suo ristorante è preferito da una clientela più adulta e benestante, potrà lavorare ad un menù a basso costo stile *fast food* il mercoledì, ed organizzare serate pianobar con un'offerta più "costosa" di venerdì.

In virtù dei vantaggi sopradescritti, tanto il rivenditore di *souvenir* quanto il proprietario del ristorante in centro si troveranno d'accordo sulla possibilità di offrire degli incentivi a quei clienti che sceglieranno di pagare in libra, in virtù di un rapporto *do ut des*. In questo caso, a mio parere, potrebbero anche trovare man forte da parte dello Stato che proprio di questi tempi sta lavorando alla possibilità di tassare il contante per incentivare all'utilizzo di moneta elettronica, essendo il contante il primo complice dell'evasione fiscale e delle organizzazioni criminali[156]. Di conseguenza lo Stato potrebbe fornire esso stesso degli incentivi a quelle attività che accettano pagamenti effettuati con moneta elettronica, tra cui anche libra, che di fatto si interpone tra le funzionalità di una moneta elettronica e quelle di una criptovaluta.

Proprio in virtù di questo aspetto, oltre ai vantaggi garantiti dalla "virtualità" di questa moneta, non dimentichiamo che stiamo parlando di uno strumento oggetto di una piattaforma *blockchain*, che a sua volta assicura ulteriori vantaggiose opportunità. Come già sperimentato dal Ministero del Lavoro del Regno Unito, la tecnologia *blockchain* potrebbe rivelarsi utile per i pagamenti assistenziali[157]. I cittadini, attraverso il loro *smartphone* o *tablet*, potranno ricevere e spendere le prestazioni sociali erogate, una volta convalidate con il loro consenso le transazioni su un libro mastro distribuito, al fine di garantire una maggior trasparenza e quindi maggior fiducia tra il governo ed i richiedenti. Facendo un ulteriore passo in avanti poi, se i cittadini pagassero le imposte attraverso una transazione sulla piattaforma, sarebbero poi in grado di monitorare e verificare l'allocazione dei loro risparmi da parte del governo. O ancora, anche le organizzazioni umanitarie potrebbero chiaramente mostrare e dimostrare come le somme dei donatori vengono distribuite e a cosa sono destinate.

[156] Sul punto si veda C. SARRA, *Altre tasse e lotta al contante: Conte svela la sua manovra,* il Giornale, settembre 2019, www.ilgiornale.it.

[157] Per approfondimenti si rinvia a P. BOUCHER (Servizio ricerca del Parlamento europeo), *Come la tecnologia blockchain può cambiarci la vita (ANALISI APPROFONDITA),* febbraio 2017, www.europarl.europa.eu.

In questo senso, il fatto che libra sia un moneta elettronica, ma anche una criptovaluta, ci permette di beneficiare della totalità dei vantaggi che le due tipologie di monete offrono: da un lato la sicurezza, l'economicità, la rapidità e la trasparenza della tecnologia *blockchain*, e dall'altro la "stabilità" di una moneta elettronica. A tutto ciò bisogna sommare, per di più, la possibilità di far crollare tutti i confini, attraverso la prima moneta globale unica.

4.5 Minacce

In virtù di quanto descritto, è doveroso ammettere che libra si presenta con prepotenza come valida alternativa alle valute sovrane e Libra Association come valoroso sostituto degli intermediari finanziari tradizionali, ma procediamo per gradi.

Per fare un esempio, fino ad una decina di anni fa pensare di organizzare autonomamente un viaggio senza rivolgersi ad un'agenzia sembrava impossibile. Ad oggi, non c'è niente di più facile che prenotare alberghi, ristoranti e perfino una macchina *in loco* direttamente da casa. Di conseguenza molte agenzie di viaggio hanno chiuso. Se Calibra permetterà, non solo agli 1,7 miliardi di soggetti *unbanked*, ma a tutti gli utenti di Zuckerberg di usufruire dei più comuni servizi finanziari direttamente dal proprio *smartphone*, non è improbabile che le banche perderanno un bel po' di clienti. C'è da dire inoltre, che alle condizioni attuali il sistema bancario non goda di grande fama, il che spiana inevitabilmente la strada a qualsiasi alternativa valida, in questo caso libra. Questo per due ordini di ragioni[158]: *in primis* i tempi necessari per concludere una transazione che riducono, anche per un fattore psicologico, la domanda di servizi finanziari; in più non sveliamo nulla di nuovo affermando che le banche hanno seminato una considerevole sfiducia da parte dell'opinione pubblica, ed i clienti, ormai sempre più *smart*, scelgono nuove soluzioni.

Altrettanto preoccupante è la possibilità che la libra sostituisca le valute tradizionali che siamo abituati a toccare con mano. Come già illustrato nei paragrafi precedenti, Libra Association si occuperà di gestire le riserve che garantiranno la stabilità della

[158] Sul punto si veda V. IMPERATORE, *Libra, la moneta di Zuckerberg renderà superflue le banche. Ma loro non se ne sono accorte*, Il Fatto Quotidiano, giugno 2019, www.ilfattoquotidiano.it.

moneta, impegnando le valute tradizionali incassate in *asset* reali. In che modo questo schema utile a contrastare la volatilità, da sempre considerato come fattore di rischio, può rappresentare una minaccia per il sistema economico? Il problema nasce dal fatto che più libra avrà successo, maggiore sarà l'ammontare di valute sovrane "assorbite", minore sarà il circolante alla portata delle scelte di politica monetaria delle autorità centrali.

Per non dar modo a queste minacce di rivelarsi più che fondate, anche in questo caso è necessario intervenire e prevenire attraverso l'unico strumento a disposizione: le regole. Un intervento normativo ben cucito sul caso Libra è necessario affinché il servizio di pagamenti, da sempre pubblico, non diventi oggetto di *business* dei "*big"* del settore privato, ad oggi primi membri e finanziatori della Libra Association. Tra questi ultimi, ad esempio, spicca PostePay, che tramite un'app permette già da diversi anni di trasferire denaro *peer-to-peer*, in un istante, solamente conoscendo il numero di cellulare della persona a cui si desidera inviare o chiedere denaro. Se l'ammontare da trasferire supera i € 25, è prevista una commissione, probabilmente per confinare l'utilizzo del servizio ai micropagamenti, evitando il rischio di sostituire gli intermediari finanziari a cui ci rivolgiamo per trasferire somme più ingenti. Allo stesso modo, si potrebbe pensare di fissare dei limiti per Calibra. Se questo strumento nasce per facilitare e velocizzare i pagamenti, per favorire la crescita economica attraverso l'utilizzo di una moneta unica, e non per sostituire gli attori del sistema bancario che di fatto vive grazie ai depositi dei propri clienti, bisogna sfruttare al meglio lo strumento "commissione". Personalmente, credo che non molti utenti sceglieranno di utilizzare il *wallet* di Calibra come deposito: per quanto le banche possano aver perso la fiducia dell'opinione pubblica, affidare i propri risparmi ad uno *smartphone* senza la possibilità di potersi rivolgere ad un consulente in carne ed ossa spaventerebbe i più, posto anche il rischio di hackeraggio ed attacchi informatici di cui abbiamo ampiamente discusso nel capitolo precedente. Ciononostante, per evitare questo rischio, possiamo seguire l'esempio di PostePay di cui parlavamo sopra, la cui carta prepagata stabilisce tre limiti: limite di importo trasferibile in una sola operazione o più operazioni giornaliere, limite di ricarica annuale e importo massimo depositato[159]. Superati questi limiti, stabiliti e fissati dalle stesse autorità, l'utente dovrà sostenere una commissione più o meno salata sulla base della misura in cui si superano tali limiti.

[159] Per approfondimento si rinvia a al sito ufficiale www.carteprepagate.org.

Questo approccio dovrebbe preservare il ruolo del sistema bancario e delle valute tradizionali, facendo di libra “solo” un validissimo strumento utile a rendere più agevole e rapido il sistema economico nella sua interezza e che non lamenta problematiche, ma abilmente colma le attuali.

CONCLUSIONI

A conclusione dell'elaborato non possiamo affermare di aver fatto luce sulla totalità degli aspetti ombrosi del *cryptotrading*, ma abbiamo di certo identificato le problematiche sulle quali intervenire con più urgenza. Se le autorità fino ad oggi hanno scelto di rinviare un eventuale intervento normativo perché non credevano che il fenomeno avrebbe raggiunto una tale portata e un così vasto bacino di utenza, alle condizioni attuali, in cui stiamo per assistere al lancio della criptomoneta legata al *social network* più famoso al mondo, prorogare non può essere più considerata una possibilità. La soluzione ideale prevede la regolamentazione di questi strumenti per sfruttarne quelle che, senza dubbio, sono delle vantaggiose opportunità ed eliminare *ex ante* i rischi.

L'occasione offerta da Mark Zuckerberg si districa perfettamente tra queste necessità. Per "curare" un qualcosa che è già "malato" e che non siamo completamente in grado di controllare è necessario ripartire da zero offrendo un'alternativa. Mettendo a disposizione dei cittadini una moneta che garantisce molti dei vantaggi delle criptovalute tradizionali, ma che ne supera i limiti, la Libra Blockchain attirerà l'attenzione di molti utenti Bitcoin, riducendo il valore della criptovaluta più "preziosa" al mondo, oggetto di molte transazioni criminali volte a favorire riciclaggio e finanziamento del terrorismo e che contribuisce non poco a peggiorare la già grave problematica ambientale. Per questo è di fondamentale importanza collaborare a livello internazionale per garantire a Libra di nascere in un contesto normativo pronto a valorizzarne tutti i punti di forza.

Ciò non fa venir meno la necessità di fissare delle regole del gioco ben precise per le criptovalute tradizionali, che gli speculatori e le attività criminali continueranno per ovvie ragioni a preferire. La V Direttiva antiriciclaggio ci conferma la presa di coscienza dell'Unione europea dell'entità e delle dimensioni raggiunte del mercato in esame, ma sono necessari interventi ben precisi che dimostrano che le autorità sono pronte a rispondere a quelle che saranno le conseguenze ineludibili del progresso.

Bibliografia e sitografia

AQUARO D., *Smart contract: cosa sono (e come funzionano) le clausole su blockchain,* Il Sole 24 Ore, giugno 2019, www.ilsole24ore.com.

BAI A., *Bitcoin al capolinea secondo Mike Hearn*, 2016, www.hwupgrade.it.

BANCA D'ITALIA, *Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee*, 19 marzo 2018, Roma, www.bancaditalia.it.

BANCA D'ITALIA, *Avvertenze sull'utilizzo delle cosiddette "valute virtuali"*, 30 gennaio 2015, Roma, www.bancaditalia.it.

BARELA V., *Riflessioni in tema di network marketing per un'analisi di diritto comparato*, ottobre 2017, www.comparazionedirittocivile.it.

BELLINI M., *Che cos'è e quali sono gli ambiti applicativi di Ethereum*, agosto 2019, www.blockchain4innovation.it.

BOUCHER P. (Servizio ricerca del Parlamento europeo), *Come la tecnologia blockchain può cambiarci la vita (ANALISI APPROFONDITA),* febbraio 2017, www.europarl.europa.eu.

BRITO J., *Beyond silk road: potential risks, threats, and promises of virtual currencies, Testimony before the Senate Committee on homeland security and governmental affair,* 18 novembre 2013, www.govinfo.gov.

BROWNE R., *Bitcoin vs Libra: Here are the key differences between the two cryptocurrencies,* luglio 2019, www.cnbc.com.

CAIELLI I., *Fare shopping con bitcoin e criptovalute: ecco chi li accetta,* giugno 2018, www.wired.it.

CAPACCIOLI S., *Criptovalute e bitcoin: un'analisi giuridica*, Giuffrè editore, Milano, 2015.

CAPONERA A. e **GOLA C**., *Aspetti economici e regolamentari delle "cripto-attività"*, in Banca d'Italia (a cura di), *Questioni di Economia e Finanza (occasional papers)*, marzo 2019, www.bancaditalia.it.

CASS., *sez. II, 28 luglio 2016, n. 33074, con nota di CARRELLI PALOMBI, Autoriciclaggio. Prime precisazioni della Cassazione sull''elemento materiale e su quello psicologico, settembre 2016, fascicolo n. 9, www.IlPenalista.it.*

CAVALLI S., *Tradying crypto: 5 cose da evitare se si trada con Bitcoin e non solo*, luglio 2019, www.cryptonomist.ch.

CAVICCHIOLI M., *Peter Schiff: "bitcoin ha di nuovo fallito come bene rifugio*, agosto 2019, www.cryptonomist.ch.

CELLINI P., *La rivoluzione digitale*, Luiss University Press, Roma, 2018.

CHAUM D., *Blind signature for untraceable payments*, in R. L. Rivest e A. T. Sherman (a cura di), *Advances in cryptology: proceedings of crypto 82*, Springer book archive, 1983.

CHERTOFF M. e SIMON T., *The Impact of the Dark Web on Internet Governance and Cyber Security*, paper series n. 6, Centre for International Governance Innovation, febbraio 2015.

CHIUSI F., *Cosa insegna Bitcoin alla politica 2.0,* L'Espresso, luglio 2015, www.espresso.repubblica.it.

CITTON C., *Prezzo Ethereum e volume di scambi: CryptoKitties nuovo strumento finanziario?*, dicembre 2017, www.blastingnews.com.

COMPLIANCE JOURNAL, *I metodi di riciclaggio: il sistema hawala,* ottobre 2017, www.compliancejournal.it

CONCAS A., *La comunione, in che cosa consiste e che cosa comporta*, marzo 2018, www.diritto.it.

CONSOB, *Le criptovalute*, www.consob.it.

CORCORAN K., *Europol: i criminali ricorrono alle criptovalute per riciclare 5,5 miliardi di dollari in contanti di provenienza illecita in Europa,* febbraio 2018, www.businessinsider.com.

COSIMI S., *Libra, ecco come funziona la moneta di Facebook,* La Repubblica, giugno 2019, www.larepubblica.it.

DABROWSKI M. e JANIKOWSKI L., *Virtual currencies and central banks monetary policy: challenges ahead*, luglio 2018, www.europarl.europa.eu.

DI GREGORIO A. e MAINOLFI G., *Le transazioni finanziarie sospette: controlli e adempimenti,* Bancaria Editrice, Roma, 2004.

DI PERNA F. e PELLEGRINI M., *Cryptocurrency (and Bitcoin), a new challenge for the regulator,* Open Review on Management, Banking and Finance, marzo 2018, www.openreviewmbf.org.

DINALE R., *Guida completa alle ICO*, gennaio 2018, www.medium.com.

DINI A*., Libra, l'Eba: "C'è un vuoto normativo, Facebook potrebbe avere gioco facile",* settembre 2019, www.corrierecomunicazioni.it.

EUROPEAN BANKING AUTHORITY, *Opinion on virtual currencies*, luglio 2014, www.eba.europa.eu.

EUROPEAN CENTRAL BANK, *Parere della Banca Centrale Europea su una proposta di direttiva del Parlamento europeo e del Consiglio che modifica la Direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica la Direttiva 2009/10/CE*, Gazzetta Ufficiale dell'Unione europea, ottobre 2016.

EUROPEAN CENTRAL BANK, *Virtual currency schemes,* ottobre 2012, www.ecb.europa.eu.

EUROPEAN CENTRAL BANK, *Virtual Currency schemes – a further analysis*, febbraio 2015, www.ecb.europa.eu.

EUROPEAN COMMISION, *Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to crossborder situations,* in Eur-Lex, Brussels, 26.6.2017 SWD(2017) 241 final.

EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY, *Avviso, L'ESMA, l'ABE e l'EIOPA informano i consumatori sui rischi delle valute virtuali*, 2014, www.eiopa.europa.eu.

EUROPEAN PARLAMENT, *Distributed ledger technologies and blockchains: building trust with disintermediation,* ottobre 2018, www.iusinitimere.it.

EUROPEAN SECURITIES AND MARKETS AUTHORITY, *Crypto-assets need common eu-wide approach to ensure investor protection,* 9 gennaio 2019, www.esma.europa.eu.

IMPERATORE V., *Libra, la moneta di Zuckerberg renderà superflue le banche. Ma loro non se ne sono accorte,* Il Fatto Quotidiano, giugno 2019, www.ilfattoquotidiano.it.

IPCC (special report), *Global warming of 1.5°*, ottobre 2018, www.ipcc.ch.

GAFI–FATF, *Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 2014 in www.faft-gafi.org; TYRA, "Bitcoin launders your dirty money but it doesn't come out very clean.",* Bitcoin Magazine, 14 dicembre 2013.

GAGLIARDUCCI C., *Ripple: cos'è, come funziona e quali differenze con il Bitcoin?,* maggio 2017, www.money.it.

GALMARINI S., *Antiriciclaggio,* Wolsters Kluwer, Milano, 2019.

GALULLO R. e MINGUZZI A., *Facebook, con Libra alto rischio di evasione e riciclaggio,* Il Sole 24 Ore, giugno 2019, www.ilsole24ore.it.

GOLDMAN Z. K., MARUYAMA E., ROSENBERG E., SARAVALLE E., SOLOMON-STRAUSS J., *Terrorist use of virtual currencies. Containing the potential threat,* Center of New American Security, maggio 2017, www.cnas.org.

GUARDIA DI FINANZA, Scuola di Polizia Tributaria, *Profili economici, finanziari e criminali nel contesto internazionale: analisi di alcuni paesi nell'area del centro e sud America,* Quaderni 18, 2007-2008.

GULLO A., *Il delitto di autoriciclaggio al banco di prova della prassi: i primi (rassicuranti) chiarimenti della Cassazione,* in Dir. pen. proc., n 4/2017.

GUZZINI A., *Lo Schema Ponzi dei bitcoin*, la Repubblica, luglio 2019, www.repubblica.it.

KNEZEVIC D., *Impact of blockchain technology in chanching the financial sector and other industries,* Montenegrin Journal of Economics, 2018.

LA REPUBBLICA, *Bitcoin, produrli ormai consuma più energia di uno Stato,* agosto 2018, www.larepubblica.it.

LOMANNO V., *Ethereum VS Ethereum Classic: tutte le differenze*, 2018, www.coiners.it.

MESSINA E., *Bitcoin e riciclaggio*, in B. QUATTROCIOCCHI (a cura di), *Norme, regole e prassi nell'economia dell'antiriciclaggio internazionale,* Giappichelli editore, Torino, 2017.

META F., *Facebook svela Libra, Zuckerberg: "Facile come inviare foto",* giugno 2019, www.corrierecomunicazioni.it.

MORA C., ROLLINS R. L., TALADAY K., KANTAR M. B., CHOCK M.K., SHIMADA M., FRANKLIN E.C., *Bitcoin emissions alone could push global warming above 2°C,* ottobre 2018, www.nature.com.

MORGAN STANLEY INVESTMENT MANAGEMENT, *Blockchain*, 2018, www.morganstanley.com.

MUSSO M., *I bitcoin potrebbero far aumentare la temperatura di 2 gradi entro il 2033*, ottobre 2018, www.wired.it.

NAKAMOTO S., *Bitcoin: a peer-to-peer electronic cash system*, ottobre 2008, www.cryptovest.co.uk.

NICOTRA M., *ICO Initial Coin Offering: una ricostruzione giuridica del fenomeno*, marzo 2019, www.blockchain4innovation.it.

PANERAI P., *Pagare il riscatto per CryptoLocker è lecito o si commette reato?*, febbraio 2016, www.achab.it.

PITTA J., *Requiem for a bright idea*, 1999, www.forbes.com.

PROVENZANI F., *Cos'è il Proof Of Work (PoW) e Proof Of Stake (PoS)?,* aprile 2019, www.money.it.

QUI FINANZA, *Facebook Libra: perché la nuova moneta di Zuckerberg non farà bene all'ambiente,* giugno 2019, www.quifinanza.it.

RAPETTO U., *Cyberlaundering - Il riciclaggio del terzo millennio*, Atti del Congresso internazionale tenutosi in data 11.06.1999, all'Università di Trento.

ROBECCO V., *Zuckerberg a Washington: Libra con l'ok delle autorità e i social non si vendono*, il Giornale, settembre 2019, www.ilgiornale.it.

SARRA C., *Altre tasse e lotta al contante: Conte svela la sua manovra,* il Giornale, settembre 2019, www.ilgiornale.it.

SARTOR G., *L'informazione giuridica e le tecnologie dell'informazione,* Giappichelli editore, Torino, 2010.

SCHOOL OF MANAGEMENT DEL POLITECNICO DI MILANO (osservatori della Digital Innovation), *La distribuzione dei casi blockchain & distributed ledger per processo e per settore, 2016-2018,* maggio 2019, www.osservatori.net.

SIDERI M., *Schema Bitcoin, siamo di fronte ad un Ponzi 4.0: ecco come funziona,* Corriere della Sera, dicembre 2018, www.corriere.it.

SOLDAVINI P., *Cos'è Tether, la criptovaluta legata al dollaro che fa tremare il Bitcoin,* Il Sole 24 Ore, febbraio 2018, ilsole24ore.com.

TZU S., *L'arte della guerra*, R. FRACASSO e W. MING (a cura di), Roma, Newton & Compton, 1994.

UNDERWOOD S., *Blockchain beyond bitcoin*, Vol. 59 n. 11, novembre 2016, www.cacm.acm.org.

VALENTE P, *Il continente digitale,* Il Sole 24 Ore, Milano, aprile 2002.

WU R., *Why we accept Bitcoin*, Forbes, febbraio 2014, www.forbes.com.

ZORLONI L., *Stretta in Corea sull'uso dei bitcoin. Chi altro vuole regolare la criptovaluta?*, dicembre 2017, www.wired.it

1. CRIPTOVALUTE: DEFINZIONE E RISCHI

1.1 Cos'è una criptovaluta: principali caratteristiche

La nascita ed il conseguente successo della "criptovaluta" sono tangibili testimoni dei progressi raggiunti dalla crittografia (strumento che permette di rendere un messaggio intellegibile solo a persone autorizzate) che hanno determinato, e stanno determinando, un cambiamento radicale nel settore finanziario, in particolar modo relativamente allo scambio di beni, servizi ed ogni attività finanziaria. Infatti il prefisso "cripto", letteralmente "nascosto", suggerisce che la possibilità di utilizzarla è subordinata alla conoscenza di un determinato codice di accesso. Si tratta di una moneta che, a differenza di come siamo, o eravamo, abituati, non esiste in forma fisica e viene scambiata per via telematica sulla base di una tecnologia inedita presentataci per la prima volta da Satoshi Nakamoto nel 2009. La *blockchain technology* non prevede infatti l'intervento di intermediari e permette agli utenti di trasferire denaro in modo diretto, rapido e sicuro sulla base di un meccanismo *peer-to-peer*, opponendosi per la prima volta ai servizi *client-service*, in cui le comunicazioni tra gli utenti vengono sempre prima indirizzate ad un'entità centrale.

È la stessa Banca d'Italia a delineare le principali caratteristiche delle criptovalute, al fine di identificare i relativi rischi che il *cryptotrading* comporta:

- vengono create da un emittente privato secondo regole proprie alle quali gli utenti scelgono di aderire;
- non sono fisicamente detenute dall'utente ma riempiono un *e – wallet* (c.d. portafoglio elettronico), cioè un *software* sviluppato da soggetti qualificati, ai quali si accede tramite *password*;
- tutti gli utenti, nello svolgere le loro attività sulla piattaforma, mantengono l'anonimato ed hanno la possibilità di registrarsi sulla stessa con uno o più *accounts* diversi;
- le operazioni di trasferimento di denaro sulla piattaforma sono irreversibili, pertanto non è mai possibile chiederne l'annullamento, neanche in caso di errore;
- non hanno corso legale, è possibile effettuare un pagamento in criptovaluta solo se il creditore è disposto ad accettarla.

È inevitabile che tali caratteristiche comportino, intrinsecamente, dei rischi. Il fatto che ogni utente, sulla base di regole proprie, possa creare una nuova moneta virtuale lascia spazio ad una concorrenza senza freni, ma soprattutto un gioco senza regole può trarre facilmente in inganno quegli investitori che non padroneggiano il criptomercato. Essendo inoltre un sistema interamente virtuale, è cruciale il rischio di consegnare tutto il nostro *wallet* nelle mani di potenziali *hackers*. Per questo non bisognerebbe mai investire più di quanto ci si possa

permettere di perdere. Tuttavia, un aspetto ancora più critico risiede nell'anonimato delle transazioni, caratteristica che senza dubbio attira l'attenzione di organizzazioni criminali.

1.2 Attori chiave

In *Virtual Currency schemes – a further analysis,* analisi svolta dalla Banca Centrale Europea, identifichiamo invece quali sono i principali attori della comunità virtuale e quali servizi offrono nello specifico agli utenti.

- Gli ***inventors***, la cui identità non necessariamente è nota, sono coloro che creano la nuova valuta virtuale e sviluppano la parte tecnica della rete, volta al mantenimento e miglioramento delle caratteristiche tecniche della valuta.
- I ***miners*** si occupano, spesso lavorando in gruppo, di convalidare le transazioni affinché il nuovo blocco di transazioni formatosi venga aggiunto alla *blockchain*, attraverso la risoluzione di complessi calcoli matematici. Il loro contributo risulta fondamentale per mantenere attiva la catena, e per questo ricevono, per ogni blocco generato, una ricompensa in criptomoneta, pari ad un importo che va dimezzandosi ogni quattro anni. Le monete ricevute potranno poi essere vendute sul mercato.
- Gli **utenti** entrano a far parte della comunità virtuale con lo scopo di ottenere criptovaluta utile all'acquisto di beni e servizi reali o virtuali dai commercianti disposti ad accettarla, utile per effettuare pagamenti da persona a persona o a fini di investimento.
- I ***wallet providers*** avviano e forniscono agli utenti un portafoglio digitale in cui archiviare le chiavi crittografiche di valuta virtuale ed i codici di autenticazione necessari per effettuare qualsiasi tipo di operazione sulla piattaforma.
- Gli ***exchangers*** sono coloro che quotano i tassi di cambio a cui acquistare e vendere valuta virtuale contro le principali valute a corso legale e contro altre valute virtuali. Per di più sono autorizzati a fornire statistiche, *wallets* e servizi di conversione ai commercianti che accettano la criptovaluta come mezzo di pagamento.
- Le **piattaforme di *trading*** rappresentano l'*alter ego* dei mercati ufficiali, mettendo in contatto gli acquirenti ed i venditori di criptovalute senza però fungere da strumento di intermediazione. Le piattaforme, a differenza degli *exchangers*, non acquistano/vendono in proprio ed in alcuni casi offrono solamente la possibilità di individuare potenziali controparti per poi realizzare lo scambio di persona.

1.3 Lo scambio: funzionamento della *blockchain* e regole da seguire

La tecnologia *blockchain* è un sistema DLT (*distributed ledger technology*) progettata per prevenire la manomissione dei dati. Una modifica, prima di essere convalidata, deve essere verificata ed accettata da tutti gli utenti, ed i blocchi di dati convalidati sono collegati in ordine cronologico attraverso una catena crittografata. Ogni blocco, identificato da un codice, contiene le informazioni relative ad un insieme di transazioni più il codice del blocco precedente, in modo da poter ripercorrere la catena retroattivamente. Qualora uno degli utenti cerchi di modificare un blocco di dati, tutti possono vedere quello che sta accadendo. Nella pratica, i dati non possono essere retroattivamente alterati senza la conseguente modifica di tutti i blocchi successivi, a meno che non si abbia, se il protocollo lo prevede, la maggioranza della rete. Il trasferimento si svolge come segue: se il soggetto X intende inviare 2 bitcoin al soggetto Y, X predisporrà un messaggio, nel linguaggio del software Bitcoin, che illustra con esattezza l'oggetto della transazione (2 bitcoin), il destinatario (Y), il mittente (X), e il precedente proprietario dell'oggetto della transazione. (Es. X trasferisce a Y 2 bitcoin, ottenuti da X con una precedente transazione da parte di Z). Una volta che X sottoscrive il trasferimento attraverso la sua chiave privata, che rappresenta la firma digitale, diffonde la transazione a tutti i nodi della rete, che potranno procedere con l'eventuale validazione. In questa fase, gli utenti verificheranno che la firma digitale del mittente sia corretta, e che quest'ultimo disponga dei fondi sufficienti per il trasferimento. Questa verifica è possibile dal momento in cui esiste un *database* pubblico che registra i saldi di ogni utente aggiornati in tempo reale. L'autenticità della transazione è dunque più che garantita, nonostante l'assenza di intermediari, in quanto ogni trasferimento porta la firma digitale del mittente (chiave privata), riporta chiaramente il precedente trasferimento ricevuto dal mittente e restituisce la chiave pubblica del destinatario. In questo modo solo il soggetto X può trasferire le somme precedentemente ricevute da Z, e solo Y potrà nuovamente trasferirle in un secondo momento. A questo punto, un utente che abbia validato un numero significativo di transazioni, può riunirle per tentare di formare un nuovo blocco.

Si tratta sicuramente di un primissimo esempio che garantisce certezza degli scambi senza ricorrere ad intermediari e relative sanzioni giuridiche. Ma qual è l'entità delle conseguenze che l'assenza di un quadro regolamentare comporta?

2. PRINCIPALI CRYPTOCURRENCIES: LE RAGIONI DEL SUCCESSO E LA RISPOSTA EUROPEA

Al fine di analizzare le principali criptovalute ed evidenziarne differenze e analogie, è utile procedere con un'analisi che si basi su capitalizzazione, prezzo, circolante emesso, ma soprattutto volume degli scambi, valore che si traduce direttamente in una misura dell'interesse che la singola moneta virtuale suscita negli investitori. Infatti, se bitcoin mantiene il primato in termini di capitalizzazione e prezzo, si lascia superare da

tether in merito al volume degli scambi. Questo dato risulta particolarmente utile dal momento in cui evidenzia una specifica caratteristica di questa moneta virtuale di cui nessuna delle principali altcoin ("*alternative coin*") gode: è una moneta stabile ancorata al valore del dollaro con un relativo tasso di cambio pressoché costante pari a uno. È un dato che senza dubbio ci suggerisce le potenzialità di una *stablecoin* in un contesto di altissima volatilità come quello del criptomercato: nel momento in cui il valore del bitcoin, per fare un esempio, dovesse subire una brusca discesa, l'investitore potrebbe convertire i bitcoin in tether senza dover necessariamente passare per la moneta reale, senza subire particolari perdite.

Analizzeremo di seguito le quattro valute virtuali più scambiate subito dopo tether e bitcoin.

2.1 Altcoin maggiormente innovative

2.1.1 Ethereum

Al terzo posto in ordine di volume degli scambi, subito dopo bitcoin, spicca ethereum, le cui innovazioni rispetto alla piattaforma originale meritano particolare attenzione. Di fatto Ethereum è una *blockchain platform* che però permette agli utenti di sfruttare diverse applicazioni decentralizzate non necessariamente ancorate al mero scambio di *cryptocurrencies*. È una rete che consente a tutti i partecipanti di beneficiare di un archivio inalterabile e condiviso di operazioni regolate attraverso *smart contracts*: dal *crowfunding* alla tutela della proprietà intellettuale o alla registrazione di un dominio. Sono contratti intelligenti, per l'appunto, perché reagiscono ad input rispondendo con output consequenziali. Un esempio applicativo è rappresentato da Etherisc, un'assicurazione sui viaggi aerei decentralizzata che si avvale della piattaforma Ethereum. Il contratto incorpora le informazioni sugli orari di partenza e in caso di ritardo del volo fa scattare automaticamente il rimborso. Lo *smart contract* lamenta però dei limiti applicativi tecnico-giuridici: l'irreversibilità della *blockchain* non permette di modificare un errore, ed è uno strumento utile solo le condizioni contrattuali sono facili da tradurre in un linguaggio informatico (es. se c'è una scadenza, effettua il pagamento). Confrontare il prezzo di ethereum con quello delle altre criptovalute non è, a mio parere, utile all'ottenimento di risultati particolarmente significativi. Questo perché l'utilizzo di Ethereum è incentivato dalle molteplici funzioni che la piattaforma offre, come finora descritto, di cui invece non godono gli utenti che scambiano bitcoin ed altre valute virtuali. Non sarebbe di conseguenza un confronto basato su una parità di condizioni.

2.1.2 Ripple

L'aspetto innovativo di Ripple merita particolare attenzione in quanto la relativa rete è stata sviluppata al fine di fornire un sistema utile al diretto trasferimento dei beni in tempo reale, offrendo un'alternativa più rapida ed economica rispetto agli attuali sistemi di trasferimento di denaro come SWIFT, utile in particolar modo alle banche ed agli intermediari finanziari. Questo perché, a differenza della piattaforma Bitcoin, sulla rete Ripple è possibile scambiare e trasferire denaro in valute diverse, senza pagare alcuna commissione. Ciò che gli utenti scambiano sono dei crediti IOU (*I Owe you*), la cui unità di misura è appunto la criptovaluta XRP. I cosiddetti *gateaway* della rete Ripple convertiranno poi la moneta virtuale nella valuta in cui l'utente deve inviare denaro o riceverlo. La *ratio* di questa piattaforma non ha quindi un fine speculativo, come per Bitcoin, bensì è volta ad agevolare gli scambi tra più agenti riducendo tempi e costi. Anche per questo non esiste un numero massimo di unità di XRP da poter emettere, come invece accade generalmente per le criptovalute: alla nascita della piattaforma sono state emesse 100 miliardi di unità a disposizione degli utenti che volessero usufruirne. Proprio in virtù della funzione di XRP, quale quella di essere una moneta di compensazione universale, e non creata a fini esclusivamente speculativi, il suo valore è rimasto pressoché costante, per lo meno fino alla prima metà del 2017.

2.1.3 Litecoin e Bitcoin Cash

Le due valute virtuali in esame nascono come alternative al bitcoin per due ordini di ragioni: supportare un maggior numero di transazioni in un minor tempo ed aumentare il numero massimo di unità da poter emettere. Quello che è curioso notare però è che i prezzi di queste ultime e quelle del bitcoin sembrano essere correlati, con una brusca discesa a gennaio 2018 per poi incorrere in una più lieve ad aprile dello stesso anno.

La causa principale è da riconoscere, a mio parere, nell'intervento del primo ministro della Corea del Sud, Lee Nak-yeon, che il 21 dicembre 2017 annunciò una serie di restrizioni sul *cryptotrading*: divieto alle transazioni anonime, facoltà per le autorità finanziarie di chiudere alcune piattaforme di scambio laddove lo ritenessero necessario e maggior potere agli investigatori nelle attività di controllo a fini antiriciclaggio. Considerando che la Corea del Sud era, al momento dell'annuncio, una dei *leader* mondiali per volume di *cryptotrading*, le conseguenze sui prezzi devono esser state rilevanti. Una concreta minaccia di regolamentazione in Corea del Sud, ed un potenziale "adattamento" della normativa vigente in Russia, Italia, Francia e Germania volto a controllare l'abuso di criptovalute, hanno spaventato gli investitori che hanno iniziato a vendere il contenuto

dei loro *wallets* determinando la discesa dei prezzi, risultato che a sua volta ha incrementato le vendite, rendendo la discesa ancora più ripida.

La risalita di cui invece stanno godendo litecoin e bitcoin, potrebbe dipendere, a mio parere, dalla data di *halving*, giorno in cui dimezza il valore della ricompensa che spetta ai *miners* che generano un nuovo blocco, e che di conseguenza potranno vendere sul mercato un volume di monete inferiore del 50 %. Una riduzione dell'offerta, se la domanda rimane costante, genera un aumento dei prezzi. Dato che la data di *halving* è nota a tutti gli investitori, il mercato prevede con certezza una riduzione dell'offerta, anticipando gli "acquisti", e anticipando di conseguenza anche l'ascesa dei prezzi. Da considerare è inoltre il fatto che minore sarà la ricompensa, minore sarà il numero di *miners* disposti a sfruttare le proprie risorse per generare un nuovo blocco, mantenendo attivo il meccanismo. Questo aspetto, meno quantitativo, potrebbe allo stesso modo ridurre notevolmente l'offerta. Per Bitcoin, il prossimo *halving* è previsto per maggio 2020, in seguito al quale la ricompensa scenderà da 12.5 BTC a 6.25 BTC. La ricompensa che spetta invece ai *miners* che generano blocchi sulla piattaforma Litecoin è già scesa da 25 LTC a 12.5 LTC lo scorso 5 agosto.

Questo approccio suggerirebbe, anche agli investitori più inesperti, di acquistare bitcoin nei primi mesi del prossimo anno, per poi rivenderli in prossimità del mese maggio, periodo in cui con una serie di condizioni certe determineranno un'ascesa del prezzo.

2.2 Le ragioni del successo

L'espansione, al momento incontrollata, del *cryptotrading* è stata, ed è tutt'ora, un campanello d'allarme per autorità internazionali, governi, banche centrali e autorità di vigilanza. Nello specifico, l'EBA (Autorità Bancaria Europea) ha approfondito e descritto il fenomeno evidenziando i benefici, economici ed individuali, che incentivano gli individui ad addentrarsi nel mondo, quasi del tutto ombroso, delle criptovalute. Tra i benefici economici, risalta senz'altro la triade "economicità – velocità – sicurezza". I costi di transazione previsti sono senza dubbio più bassi in virtù dell'assenza di intermediari, in media pari all'1% dell'ammontare. Un ulteriore aspetto da non ignorare è sicuramente la velocità delle transazioni. Abbiamo riscontrato già nei paragrafi precedenti l'essenzialità di questa caratteristica: alcune delle principali altcoin sono nate proprio con lo scopo di accelerare ulteriormente i tempi previsti dalla piattaforma Bitcoin (Litecoin, Bitcoin Cash). Abbiamo a che fare inoltre con delle piattaforme *no-stop*, un servizio disponibile 24/7, a differenza dei tradizionali intermediari a cui siamo abituati. Inoltre, la sicurezza e l'irreversibilità delle transazioni, le quali vengono tutte trascritte in un registro comune, garantiscono una trasparenza di cui non sempre godiamo nei mercati tradizionali. A livello individuale invece, non è da sottovalutare l'opportunità di poter trasferire denaro mantenendo l'anonimato, conservando i propri dati personali. In questo senso, pagare con moneta virtuale è come pagare in contanti, eliminando il rischio di consegnare i propri dati nelle mani di chi potrebbe abusarne. Non dimentichiamo, in ultimo, che la tecnologia *blockchain* nasce con lo scopo di dare inizio ad un sistema

decentralizzato, che non soffrisse il controllo di autorità centrali con la facoltà di influenzare l'offerta di moneta. Uno dei benefici del mercato *crypto* è quello appunto di gestire, potremmo dire, "democraticamente" le transazioni, e la relativa possibilità di trasferire denaro oltre i confini comunitari, approfittando talvolta di regolamentazioni estere meno sviluppate e meno affidabili. Infatti, se da un lato questa opportunità garantisce un'integrazione finanziaria, oserei dire, mondiale, dall'altro permette alle organizzazioni criminali, collaborando con altre organizzazioni all'estero, di approfittare di una normativa meno stringente e meno severa vigente in altri Paesi. Purtroppo è necessario ammettere, a mio parere, che proprio il binomio "anonimato – assenza di controllo" susciti l'interesse delle organizzazioni criminali nei confronti delle criptovalute, e rappresenta quindi una delle motivazioni per cui questo mercato ha riscosso, e sta riscuotendo, un notevole successo.

In aggiunta, le tre autorità di vigilanza europea, EBA, ESMA ed EIOPA, individuano un'altra ragione nella non consapevolezza dei rischi che si corrono facendo uso di criptovalute. L'EBA in particolare, rintraccia 70 rischi che tutti coloro che si servono delle piattaforme del criptomercato corrono, dagli utenti ai fornitori di servizi, all'intero sistema finanziario, tra cui: volatilità, formazione del prezzo poco trasparente e facilmente manipolabile, attacchi informatici, totale assenza di garanzia dei depositi, di vigilanza e di tutela legale e contrattuale ed il mancato corso legale delle monete virtuali, che potrebbe tradursi nel rischio di non avere "opzioni di uscita" e subire perdite nel frattempo.

2.3 Necessità di un intervento normativo: l'Unione europea risponde

Mentre fino allo scorso anno, tanto le autorità nazionali quanto quelle europee, si limitavano a scoraggiare le banche e gli altri intermediari vigilati dall'acquistare, detenere o vendere valute virtuali, l'approvazione della Direttiva Ue 2018/843 (V Direttiva antiriciclaggio) in vigore da luglio 2018 sembra voler cambiare le carte in tavola. L'Europa finalmente riconosce che si trova di fronte ad un fenomeno destinato a durare nel tempo e che ha dimostrato di essere un valido strumento nelle mani di organizzazioni criminali, e che pertanto necessita di essere regolamentato. Con la V Direttiva antiriciclaggio, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che gli Stati membri dovranno recepire entro il 10 gennaio 2020, la comunità europea per la prima volta riconosce e dà una definizione esatta di criptovaluta: ‹‹una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo *status* giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente». Il Provvedimento europeo in questione però, a mio parere, non ha particolarmente arricchito il contesto normativo, se non per l'aver ampliato la sfera dei soggetti tenuti all'adempimento degli obblighi antiriciclaggio. Rispetto alla IV Direttiva infatti, la V Direttiva coinvolge anche la figura dei *wallet providers*, anch'essi soggetti agli obblighi di verifica della clientela e all'attuazione

di controlli sistematici, come imposto in capo agli *exchangers* con la precedente Direttiva 2015/849. Attraverso i soggetti obbligati, le autorità competenti dovrebbero essere in grado di monitorare le operazioni che hanno per oggetto criptomonete. Questo intervento legislativo tuttavia non colma tutte le lacune e non riesce totalmente a frenare le attività illecite: il ruolo del *wallet provider*, così come quello dell'*exchanger*, risulta essere meramente eventuale, dal momento in cui l'utente può scegliere di detenere le criptovalute in un proprio *portfolio* personale senza depositarle in un *wallet*. Il problema da risolvere resta quello dell'anonimato, caratteristica che non consente alle Unità nazionali di Informazione Finanziaria di associare l'indirizzo elettronico alfanumerico all'identità della persona fisica o giuridica che c'è dietro. Sarebbe utile considerare la possibilità di chiedere agli utenti di scegliere, su base volontaria, se consegnare un'autodichiarazione alle autorità competenti.

3. BITCOIN E "RICICLAGGIO DIGITALE"

3.1 Criptovalute come valido strumento di attività illecite: la capacità dissimulatoria del bitcoin

È recente anche la presa di coscienza nazionale circa la pericolosità dell'anonimato che caratterizza le transazioni finanziarie effettuate mediante criptovaluta, concretizzatasi con l'emanazione del d.lgs. n. 90/2017. La sussistenza di specifiche peculiarità del contesto, quali intertemporalità, assenza di frontiere, bassi costi e complessità dei meccanismi, richiede un intervento legislativo altrettanto minuzioso e complesso.

La difficoltà nell'adeguare la normativa al fenomeno risiede nella continua evoluzione dello stesso e delle relative tecniche di riciclaggio utilizzate dalle organizzazioni criminali con lo scopo di reimmettere nei circuiti legali flussi illeciti. Il contesto ideale per lo sviluppo sempre più rapido di tecniche di riciclaggio per mezzo delle criptovalute è senz'altro il *deep web* ("*web* sommerso"). Questo "strato" del *web* non consente un accesso immediato attraverso i comuni motori di ricerca, e per questo rappresenta una sede ideale per i reati informatici. Un sotto strato del *deep web* è il *dark web,* sede di contenuti volontariamente nascosti ai normali navigatori. Le piattaforme appartenenti a questo più profondo strato del *web* nascono al servizio di attività illegali o immorali e sono principalmente finanziate da criptovalute. La soluzione ideale sarebbe inserire nella normativa delle specifiche sanzioni per chiunque tenti di accedere ad un sito del *dark web*. Il legislatore potrebbe stabilire l'obbligo per tutte le aziende produttrici di *personal computer, smartphone, tablet* e tutti gli strumenti che consentono di accedere al *web*, a partire dal 2020, di programmarli in modo che, nel momento in cui l'utente proverà ad accedere ad un sito di *dark web,* la polizia postale ne riceverà immediata segnalazione. Una sanzione significativa potrebbe ridurre senza dubbio il tasso di successo di questo sotto strato del *web* inaccessibile ai più.

Il vero punto dolente del legislatore, tuttavia, nel tentativo di individuare e prevenire rischi, è intrinseco nell'anonimato delle transazioni: sebbene il meccanismo *blockchain* sia un valido strumento utile alla tracciabilità delle transazioni in rete, ripercorrere la catena a ritroso conduce ad un algoritmo di pura matrice matematica di elaborata risoluzione, che difficilmente riconduce all'identità di una persona fisica o giuridica. Le problematiche che intralciano di fatto questo meccanismo sono principalmente due: *in primis*, le transazioni, essendo transnazionali, possono coinvolgere controparti che operano in due Sati diversi, uno dei quali potrebbe non godere di un'adeguata normativa antiriciclaggio; *in secundis*, una transazione può essere riconducibile ad *accounts* diversi, che però di fatto appartengono allo stesso utente, data l'opportunità di poter essere titolari di più indirizzi contemporaneamente.

Oltre alle possibilità che la natura stessa del sistema offre agli investitori che non godono delle migliori e lecite intenzioni, esistono diversi *escamotages*, individuati dal Gruppo di Azione Finanziaria Internazionale, utili a garantire una più solida dissimulazione:

- ***anonymizers***, *software* che consente di eseguire operazioni senza essere identificati. I più utilizzati sono quei programmi che permettono di inviare *email* senza consentire al destinatario di risalire al mittente;
- ***tumbler***, meccanismo che permette di collegare una transazione ad un indirizzo diverso da quello effettivo;
- ***tor***, acronimo di "*The Onion Router*", *browser* che permette di accedere agli indirizzi *web* attivi sul *dark web*.

In seguito a queste analisi, non c'è dubbio sul fatto che la criptovaluta sia perfettamente idonea ad ‹‹ostacolare concretamente l'identificazione della provenienza delittuosa del profitto illecito», clausola a cui si subordina incondizionatamente la configurazione dell'art. 648 *bis* c.p.

3.2 L'attività dei cambia valute e il concorso nel reato di riciclaggio: problematiche del d.lgs. n.90/2017

Nel caso in cui l'attività si svolga in parte *online* ed in parte *offline*, risulta necessario l'intervento della figura del cambia valuta per il passaggio dall'una all'altra "zona", che inevitabilmente collabora ad ostacolare ulteriormente l'identificazione della provenienza delittuosa. È a questo punto che è inevitabile un intervento legislativo, concretizzatosi con il d.lgs. n.90/2017, con cui il legislatore nazionale fissa le prime forme di regolamentazione in materia, fissando degli obblighi ben precisi che proprio l'*exchanger* è chiamato a rispettare. Coinvolgere nella normativa coloro che professionalmente hanno la facoltà di immettere nel circuito economico lecito il bitcoin "sporco", risulta necessario dal momento in cui l'autore del reato non potrebbe in nessun modo, senza l'intervento dell'*exchanger*, "ripulire" quanto ottenuto attraverso la precedente operazione

illecita. È più che giusto, dunque, che la normativa nelle vesti del d.lgs. n.90/2017 coinvolga la figura del cambia valute, con questo decreto obbligato a rispettare obblighi di adeguata verifica del cliente e di segnalazione di operazioni sospette.

Le lacune del decreto risultano però evidenti in quei casi in cui le attività illecite oggetto del delitto presupposto del reato di riciclaggio sono generate e commesse unicamente *online*, e la valuta virtuale non viene trasformata in reale. Per porre rimedio a tale lacuna, la Commissione Europea ha avanzato una nuova proposta: la *Fifth Directive Anti Money Laundering*, come già accennato nel secondo capitolo, estende la normativa antiriciclaggio anche ai *wallet providers*, i quali sono chiamati ad attuare controlli sistematici, nonché obbligati alla verifica della clientela. Purtroppo la problematica persiste: anche la figura del *wallet provider* risulta non strettamente necessaria, essendo niente più di un "deposito informatizzato", e dal momento in cui l'utente potrebbe conservare le proprie monete virtuali in un portafoglio personale. Probabilmente, secondo una pura considerazione personale, l'ideale non è mettere in guardia, ed eventualmente punire, i potenziali complici del reato, bensì lavorare ed intervenire su quella che è la caratteristica più attraente del sistema: la scarsa tracciabilità delle transazioni.

3.3 Possibili soluzioni volte a colmare le lacune dell'attuale normativa: alcune considerazioni a carattere personale

Sulla base delle analisi svolte in questi ultimi paragrafi, abbiamo individuato le due strade che il riciclatore si trova di fronte, e percorrendo le quali avrebbe la possibilità di ripulire proventi di origine delittuosa. Da un lato, può scegliere di rivolgersi ad un *exchanger* per convertire la criptovaluta in moneta avente corso legale, dall'altro il riciclatore potrebbe decidere di trattenere i proventi all'interno dei confini virtuali. In questo secondo caso, immaginiamo che il soggetto avrà intenzione di spendere le somme ottenute attraverso attività illecite su quei siti *web* che accettano la moneta virtuale come mezzo di pagamento. Individuiamo proprio in questo passaggio una lacuna del d. lgs. n. 90/2017, il quale stabilisce che i prestatori di servizi relativi all'utilizzo di valuta virtuale sono tenuti al rispetto degli obblighi antiriciclaggio ‹‹limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute avente corso forzoso». Sembrano quindi rimanere fuori dal novero dei soggetti obbligati i prestatori di servizi relativi all'utilizzo di criptovaluta che non svolgono attività di conversione, quali ad esempio, i gestori dei siti di *e – commerce* che accettano la moneta virtuale come mezzo di pagamento. In questo modo, il riciclatore può tranquillamente ripulire il denaro sporco prenotando un viaggio su Expedia, una delle più grandi agenzie di viaggio *online*, oppure acquistando un televisore su Overstock.com. Di conseguenza è necessario stilare una serie di obblighi che tutte le attività di *e - commerce* che dichiarano di accettare pagamenti in criptovaluta dovrebbero essere chiamate a rispettare, sulla falsa riga di quanto previsto per gli *exchangers* ed i *wallet providers*, con obblighi di registrazione, di adeguata verifica della clientela e segnalazione di operazioni sospette.

Altrettanto giusta era l'intenzione del primo ministro della Corea del Sud, Lee Nak-yeon, che nel dicembre del 2017 annunciò di voler vietare le transazioni anonime. A mio parere, è lo pseudonimato delle transazioni che, più di tutte le altre caratteristiche proprie del contesto, suscita l'interesse e facilita i piani dei potenziali criminali. È pertanto necessario intervenire quanto prima a riguardo, seguendo l'esempio del primo ministro Nak-yeon.

In ultimo, merita particolare attenzione la questione della transnazionalità, cioè l'opportunità di collaborare con organizzazioni criminali residenti all'estero. Per quanto utopica, la soluzione ideale sarebbe costruire una normativa che non solo superi i confini nazionali, ma anche quelli della comunità europea, in modo da impedire alle organizzazioni criminali di godere delle opportunità che i Paesi che non prevedono una severa normativa antiriciclaggio garantiscono. Sarebbe opportuno quindi lavorare ad un trattato internazionale che coinvolga e richieda soprattutto la collaborazione dell'UNODC, l'Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine, tra gli obiettivi del quale spicca appunto il contrasto al crimine organizzato transnazionale. Solo in presenza di una normativa a carattere internazionale sarebbe possibile considerare la criptovaluta una vera valuta a tutti gli effetti.

4. IN ARRIVO LA CRIPTOVALUTA DI FACEBOOK: ANALISI SWOT DI UNA POTENZIALE *GLOBALCOIN*

4.1 L'identikit della criptovaluta ideale

Per concludere, proviamo ad ipotizzare i caratteri di una criptovaluta ideale, creata *ex novo*, e che possa evitare *ex ante* quei rischi finora elencati. Le autorità nazionali ed europee hanno sempre tentato di disincentivare l'utilizzo di criptovalute soprattutto in virtù di una tutt'altro che contenuta volatilità. Per ovviare a questa problematica, la nostra valuta virtuale ideale dovrebbe essere una ***stablecoin***, una valuta coperta da riserve che garantiscano un tasso di cambio con le principali valute tradizionali pressoché costante.

Tra i rischi più allarmanti, spicca inoltre la mancanza di autorità centrali, sostituite nel caso del Bitcoin dagli stessi utenti, i quali hanno il compito di verificare e convalidare le transazioni. Per quanto la grande numerosità degli utenti possa in qualche modo garantire la sicurezza delle transazioni, perché è improbabile che milioni di persone scelgano di commettere una frode nello stesso momento, è un rischio che non possiamo permetterci di correre. Di conseguenza è necessario creare una **nuova *blockchain*** che sia però **controllata da soggetti "*trusted*", che per primi hanno investito nel progetto**, e che per questo non daranno ragione di dubitare del corretto funzionamento della piattaforma volto esclusivamente allo scopo per cui è stata ideata: facilitare i pagamenti.

L'ultimo ostacolo da arginare risiede nell'anonimato delle transazioni, forse la caratteristica più pericolosa del criptomercato. È di fondamentale importanza, a mio parere, eliminare totalmente questo aspetto tra le caratteristiche di una criptovaluta ideale, magari chiedendo agli utenti di scaricare sul proprio *smartphone* o *tablet* un'app che, nelle vesti di un *wallet provider*, offra un portafoglio digitale agli utenti solo in seguito ad **una registrazione che richiede dati personali**.

Nel delineare però l'identikit di questa valuta virtuale, ci accorgiamo facilmente che questa potenziale moneta ottimale è già stata progettata e si chiama Libra. Si tratta della *cryptocurrency* di Facebook, annunciata dallo stesso Mark Zuckerberg lo scorso giugno e il cui lancio è previsto per il 2020. Cerchiamo a questo punto di capire, attraverso un'analisi SWOT, se questa moneta rispecchia il nostro identikit e quali sono gli aspetti da curare e le lacune dal colmare prima del lancio, per fare di Libra la criptomoneta ideale.

4.2 STRENGHTS: punti di forza

Come già accennato, la rete Libra si baserà su una *blockchain* **centralizzata**. Infatti a gestire la criptomoneta sarà un consorzio composto attualmente da 28 membri: il consorzio di Libra Association, con sede a Ginevra, avrà il compito di gestire la *blockchain* autorizzando le transazioni, nelle vesti di un intermediario "*trusted*", e gestendo le riserve utili a mantenere **stabile** il valore della criptomoneta. A differenza di tether, la *stablecoin* analizzata nel secondo capitolo e le cui riserve erano di fatto dollari, nel caso di libra le criptomonete emesse sono coperte da *asset* reali a bassa volatilità come depositi bancari e titoli di Stato a breve termine denominati in valute di Banche centrali stabili e ad alta reputazione. Gli interessi maturati andranno a coprire i costi del sistema, garantiranno basse commissioni e pagheranno dividendi agli investitori, cioè i membri della Libra Association. Un'altra problematica che libra potrebbe aiutarci a risolvere è quella dell'anonimato. I membri del consorzio infatti, da Facebook a PayPal, o a Mastercard, sono noti per negare i loro servizi a coloro che non rispettano quanto previsto nei propri regolamenti. Si tratterebbe quindi di stabilire regole più ferree e non consentire a chiunque, come di fatto succede con Bitcoin, di operare all'interno della piattaforma. Si chiama Calibra la società sussidiaria di Facebook che, nelle vesti di *wallet provider*, fornirà portafogli digitali e permetterà agli utenti di accedere e partecipare al *network* di Libra e potrebbe essere proprio questa la chiave che potrebbe non permettere a tutti di accedere ai servizi finanziari. Di fatto si tratterà di un'applicazione con cui salvare, inviare o spendere libra direttamente dal proprio *smartphone*, perché collegata a Whatsapp e Messenger. Lo stesso Mark Zuckerberg ha dichiarato: ‹‹Calibra sfoggerà un team dedicato di esperti che combatterà gli usi fraudolenti della valuta, doteremo Libra di una protezione antifrode, così che se i fondi vengono persi noi li rimborseremo». Questa affermazione ci lascia intuire che usufruire dei servizi offerti dalla società non sarà così facile come per Bitcoin, e soprattutto che **non saranno pochi i controlli e le verifiche a cui gli utenti che intendono far uso di libra saranno sottoposti**. In ultimo, non dobbiamo ignorare la problematica ambientale. È da imputare all'attività di *mining* del bitcoin circa l'1% del consumo mondiale,

più di quanto non consumi lo Stato di New York. La produzione e la conservazione di Libra però, in virtù del funzionamento della piattaforma che non prevede il *mining*, non richiederà la stessa potenza di calcolo e lo stesso Facebook, inoltre, sta lavorando per rendere i propri ***data center* maggiormente ecosostenibili**. Di conseguenza, se la Libra Blockchain riuscirà a "rubare" qualche utente alle tradizionali criptovalute, anche se riconosciamo che lo scopo degli utenti è ben diverso, l'eccessivo consumo di energia elettrica sarà notevolmente ridotto.

4.3 WEAKNESSES: debolezze

Siamo senza dubbio di fronte ad un nuovo e potentissimo strumento digitale, che andrà però ad incastrarsi in un vuoto normativo. Da un lato le attività finanziarie sono regolamentate dalle leggi comunitarie in materia di investimenti, dall'altro i pagamenti elettronici devono rispettare quanto previsto dalla normativa dei pagamenti. Le criptovalute, ed in particolare libra, vanno a posizionarsi proprio lungo il confine che intercorre tra le due zone.

La prima problematica sorge in capo all'idoneità delle monete alternative alle valute tradizionali di saldare un debito. L'art. 1277 del codice civile limita espressamente questa facoltà alle monete aventi corso legale, escludendo di fatto le criptovalute e di conseguenza anche libra, a meno che il creditore non acconsenta (art. 1197 c.c.).

Una parentesi particolare merita la questione della *privacy*. Il rischio è che tramite questa intersezione tra servizi che permette di inviare denaro attraverso un *social* con le stesse modalità con cui siamo soliti inviare foto, Zuckerberg, ed i relativi *partners*, potrebbero essere in grado di acquisire più informazioni personali di quanto già non facciano. Pertanto, nell'interesse della comunità europea, è necessario che questo progetto si attenga a quanto previsto dal GDPR (Regolamento UE 2016/679), il quale disciplina il trattamento dei dati personali dei cittadini europei da parte di persone, società o organizzazioni.

In ultimo, se Calibra nasce come uno strumento che potenzialmente potrà offrire agli utenti i tradizionali servizi bancari, quale anche quello del mero "deposito", è bene che la società acquisisca la licenza bancaria, cioè un'autorizzazione legale per poterlo fare. È un passaggio di fondamentale importanza dal momento in cui l'ottenimento della licenza prevede il soddisfacimento di una serie di requisiti relativi a capitale minimo, applicazione delle normative, sicurezza e protezione dei dati.

4.4 OPPORTUNITIES: opportunità

In questi ultimi ormai quasi vent'anni abbiamo tutti avuto modo di verificare in prima persona i benefici che la moneta unica garantisce, seppur limitatamente ai confini comunitari. In questo caso però, abbiamo a che

fare con una moneta che non solo sarà unica a livello globale, il che non farà che amplificare i vantaggi di cui parlavamo, ma assorbirà anche tutti i benefici propri di uno strumento virtuale.

Il primo settore a trarne beneficio sarà sicuramente il turismo. Avere nel proprio portafoglio una moneta che permette di pranzare, salire sui mezzi pubblici e visitare i musei di uno Stato estero senza dover convertire la propria valuta non può che incentivare tutti i cittadini del mondo a viaggiare di più.

Inoltre pagare con una moneta che è, potremmo dire, autografata da chi ne fa uso, potrebbe tradursi in un grande vantaggio per le attività commerciali. Se Calibra, al momento del pagamento in libra, fornisse al venditore alcuni dati, garantirebbe la tracciabilità degli acquisti. Ovviamente l'applicazione non dovrà dichiarare niente che non sia già scritto, ad esempio, sulla carta d'identità. Ma se una piccola attività in centro storico avrà la possibilità di conoscere anche solo l'età, il sesso e la professione del compratore, sarà in grado di capire meglio cosa vendere, quando vendere e quando scontare, perfezionando l'offerta in base alle caratteristiche di chi domanda.

Oltre ai vantaggi garantiti dalla "virtualità" di questa moneta, non dimentichiamo che stiamo parlando di uno strumento oggetto di una piattaforma *blockchain*, che a sua volta assicura ulteriori vantaggiose opportunità: se i cittadini pagassero le imposte attraverso una transazione sulla piattaforma, sarebbero poi in grado di monitorare e verificare l'allocazione dei loro risparmi da parte del governo. O ancora, anche le organizzazioni umanitarie potrebbero chiaramente mostrare e dimostrare come le somme dei donatori vengono distribuite e a cosa sono destinate.

4.6 THREATS: le minacce

In virtù di quanto descritto, è doveroso ammettere che libra si presenta con prepotenza come valida alternativa alle valute sovrane e Libra Association come valoroso sostituto degli intermediari finanziari tradizionali. Se Calibra permetterà, non solo agli 1,7 miliardi di soggetti *unbanked*, ma a tutti gli utenti di Zuckerberg di usufruire dei più comuni servizi finanziari direttamente dal proprio *smartphone*, non è improbabile che le banche perderanno un bel po' di clienti, considerando per di più che il sistema bancario attuale non goda di grande fama da parte dell'opinione pubblica. Inoltre, più libra avrà successo, maggiore sarà l'ammontare di valute sovrane "assorbite", minore sarà il circolante alla portata delle scelte di politica monetaria delle autorità centrali.

Per non dar modo a queste minacce di rivelarsi più che fondate, anche in questo caso è necessario intervenire e prevenire attraverso l'unico strumento a disposizione: le regole. Personalmente, credo che non molti utenti sceglieranno di utilizzare il *wallet* di Calibra come deposito: per quanto le banche possano aver perso la fiducia dell'opinione pubblica, affidare i propri risparmi ad uno *smartphone* senza la possibilità di potersi rivolgere ad un consulente in carne ed ossa spaventerebbe i più, posto anche il rischio di hackeraggio ed attacchi

informatici. Ciononostante, per evitare questo rischio, possiamo seguire l'esempio di PostePay, uno dei 28 membri di Libra Association, la cui carta prepagata prevede tre limiti: limite di importo trasferibile in una sola operazione o più operazioni giornaliere, limite di ricarica annuale e importo massimo depositato. Superati questi limiti, stabiliti e fissati dalle stesse autorità, l'utente dovrà sostenere una commissione più o meno salata sulla base della misura in cui si superano tali limiti.

CONCLUSIONI

Dopo aver analizzato le più intricate caratteristiche del criptomercato e le lacune normative all'interno delle quali queste ultime abilmente si districano, è chiaro che stiamo assistendo allo sviluppo di un fenomeno che entrerà a far parte del sistema economico sempre più prepotentemente, come è evidente l'assenza di un quadro normativo capace di gestirne il controllo. Ma per "contrattaccare" un fenomeno è fondamentale conoscerlo a fondo. Lo scopo di questo elaborato è esattamente quello di studiarne tutti gli aspetti per poi comprenderlo, e giungere infine alla risposta ottimale da parte del legislatore ed identificare i caratteri di una criptovaluta ideale.

A conclusione dell'elaborato non possiamo affermare di aver fatto luce sulla quasi totalità degli aspetti ombrosi del *cryptotrading*, ma abbiamo di certo identificato le problematiche sulle quali intervenire con più urgenza. La soluzione ideale prevede la regolamentazione di questi strumenti per sfruttarne quelle che, senza dubbio, sono delle vantaggiose opportunità ed eliminare *ex ante* i rischi: l'occasione offerta da Mark Zuckerberg si districa perfettamente tra queste necessità. Per questo è di fondamentale importanza collaborare a livello internazionale per garantire a Libra di nascere in un contesto normativo pronto a valorizzarne tutti i punti di forza.

Ciò non fa venir meno la necessità di fissare delle regole del gioco ben precise per le criptovalute tradizionali, che gli speculatori e le attività criminali continueranno per ovvie ragioni a preferire. La V Direttiva antiriciclaggio ci conferma la presa di coscienza dell'Unione europea dell'entità e delle dimensioni raggiunte del mercato in esame, ma sono necessari interventi ben precisi che dimostrano che le autorità sono pronte a rispondere a quelle che saranno le conseguenze ineludibili del progresso.