Giulio Soana

Obblighi di prevenzione del riciclaggio e cripto-attività. Interventi legislativi ed opportunità regolamentari

(doi: 10.4478/106720)

Osservatorio del diritto civile e commerciale (ISSN 2281-2628)
Fascicolo Speciale, settembre 2022

Ente di afferenza:
()

Obblighi di prevenzione del riciclaggio e cripto-attività

Interventi legislativi e opportunità regolamentari

Giulio Soana

Money-Laundering Prevention Obligations and Crypto-Assetes. Legislative Actions and Regulatory Opportunities

The article analyses how the AML regulation reacted to the crisis caused by the introduction and development of crypto assets. In a field rooted in the regulation of intermediaries, the disintermediation of financial flows permitted by blockchain mined the same validity of the underlying policy strategy. The debate resulting from this crisis and the legislative attempts of fitting the previous approach into the new paradigm, provide an interesting case study to understand how the policy maker can react to similar exogenous shocks. Besides the analysis of the past and current regulation, the article aims at proposing new guidelines for this field. Eminently, as underlined by the MiCa Regulation and the recent FATF Guideline, this is an extremely dynamic area both from a technological and a policy standpoint. The AML regulation in the field of crypto-assets still needs further innovation so to implement a strategy that can address the peculiarities of blockchain's governance model.

Keywords: Money-Laundering, Crypto-Assets, FATF, MiCAR, Blockchain, Cyber-Laundering.

1. Valute virtuali e rischio riciclaggio. Un'introduzione

Il primo passo per comprendere l'impatto delle valute virtuali sulla normativa antiriciclaggio è inquadrare in che modo tali strumenti minino la preesistente strategia di controllo dei flussi finanziari.

La normativa antiriciclaggio si sviluppa in un'epoca, la fine degli anni '80[1], che vede la nascita dei primi sistemi di pagamento digitale e, più in generale, la crescente digitalizzazione della struttura finanziaria. La transizione del sistema economico dal contante alla moneta elettronica crea un'occasione unica per il rafforzamento dei meccanismi di sorveglianza: segnatamente il mutamento in parola comporta il passaggio da un sistema di pagamento basato su token ad uno fondato su account[2].

[1] Per una breve storia del sistema antiriciclaggio si veda E. Musco, *Riciclaggio, autoriciclaggio e reimpiego*, Zanichelli, 2022, pp. 5 e ss.

[2] Per una discussione in merito alle differenze intercorrenti tra questi due sistemi si veda C. Kahn, W. Roberds, *Why pay? An introduction to payments economics*, in *Journal of*

Una breve introduzione a tali sistemi aiuterà a comprenderne la rilevanza in termini di politica criminale. Nei mezzi di scambio basati su token lo spostamento del valore si ha con il mero passaggio di un oggetto, il quale costituisce materializzazione del valore stesso: ad esempio, il pagamento in contanti si realizza con lo spostamento della banconota dalla disponibilità del *solvens* a quella dell'*accipiens.* Al contrario, nei mezzi di scambio basati su account, il pagamento si compie mediante la riassegnazione di un credito da *solvens* ad *accipiens*; così, nei sistemi di pagamento elettronico, lo spostamento di valore si ha con la riassegnazione di un credito vantato nei confronti del fornitore del servizio – banca o altra istituzione finanziaria – dal *solvens* all'*accipiens.*

La fondamentale differenza, in termini di sorveglianza, tra questi due sistemi è che, in un modello basato su token, per ricevere un pagamento l'*accipiens* non ha alcuna necessità di identificare la controparte ma dovrà semplicemente verificare l'autenticità del token stesso; al contrario, in un sistema basato su account, l'identificazione è necessaria[3], sia al fine di accertare che il *solvens* abbia effettivamente i fondi che desidera trasferire, sia per comunicare al terzo debitore la transazione e permettergli di modificare la posta contabile. Inoltre, mentre il pagamento mediante token è un sistema c.d. da pari a pari (p2p) – lo spostamento di valore avviene direttamente tra le parti senza alcuna intermediazione – l'utilizzo di un sistema basato su account implica l'inclusione di un soggetto terzo che, per l'appunto, tiene i conti e garantisce l'adempienza del *solvens*; tale soggetto terzo acquisisce una posizione privilegiata, in quanto collettore di una grande quantità di dati in merito allo stato patrimoniale e alle transazioni dei propri clienti[4].

Financial Intermediation, 2009, 18(1), pp. 6 ss., che utilizzano la differente ma sostanzialmente omogenea terminologia di *store of value systems* e *account based systems.*

[3] C. Kahn, *Tokens vs. Accounts: Why the Distinction Still Matters*, Federal Reserve Bank of Saint Louis, https://www.stlouisfed.org/on-the-economy/2020/october/tokens-accounts-why-distinction-matters: «When you pay with an account, the crucial question for the recipient is your identity: "Are you really the account holder?", When you pay with a token, your identity is irrelevant; instead, the crucial question for the recipient is: "Is this object I'm receiving real or counterfeit?"».

[4] Come affermato da David Chaum in D. Chaum, *Security without identification: Transaction systems to make big brother obsolete*, in *Communications of the ACM*, 1985, 28(10), p. 1030, «the foundation is being laid for a dossier society, in which computers could be used to infer individuals' lifestyles, habits, whereabouts, and associations from data collected in ordinary consumer transactions […]. As computerization becomes more pervasive, the potential for these problems will grow dramatically. On the other hand, organizations are vulnerable to abuses by individuals. Everyone pays inidirectly when cash, checks, consumer credit, insurance, and social services are misused. The obvious solution for organizations is to devise more pervasive, efficient, and interlinked computerized record-keeping systems, perhaps in combination with national identity cards or even fingerprints. However, this would exacerbate the problem of individuals' loss of monitorability and control, and would likely be unacceptable to many».

In questo rinnovato sistema, gli intermediari finanziari divengono dei colli di bottiglia informativi per il sistema economico posto che gli scambi digitali di valore passano necessariamente per i loro bilanci e, pertanto, sotto il loro potenziale controllo. Il legislatore antiriciclaggio si inserisce nel mutamento dell'architettura delle transazioni finanziarie adottando una doppia strategia: la progressiva limitazione dell'uso del contante – con l'introduzione di tetti ai pagamenti in contanti e alla possibilità stessa di detenere oltre una certa somma – e la regolamentazione di un numero crescente di intermediari a cui sono imposti doveri di identificazione, monitoraggio e segnalazione dei propri clienti; sfruttando la posizione privilegiata di tali intermediari, quali checkpoint obbligati per la trasmissione digitale di valore, la normativa crea una sistema di allarme decentralizzato spostando parzialmente l'onere, ed il costo, della repressione penale – almeno in termini di prima identificazione della *notitia criminis* – sui privati.

Fulcro della strategia antiriciclaggio è, dunque, la regolamentazione degli intermediari mediante l'imposizione di obblighi di monitoraggio della clientela[5].

Le criptovalute minano questa strategia introducendo la possibilità di effettuare pagamenti digitali senza la necessità di avvalersi di un terzo intermediario[6]: fondamentale innovazione introdotta dalla blockchain – la tecnologia sottostante le criptovalute – è, invero, la possibilità di effettuare trasferimenti digitali di valore da pari a pari[7]. La blockchain, mediante la sostituzione del tradizionale sistema di contabilità centralizzata gestita dall'intermediario con un sistema appunto di contabilità decentralizzata gestita dall'intera comunità degli utenti, permette scambi di valore digitali ad utenti individuali senza la necessità di utilizzare un intermediario, sia nella fase dell'accesso al mercato che in quella dello scambio del valore[8]. L'assenza di un filtro obbligato all'ingresso comporta che le criptovalute aggiungono alla globalità ed immaterialità già caratterizzante le tradizionali transazioni digitali, la componente della pseudonimia[9]: invero, nel mondo cripto, ogni utente può creare un account da sé senza doversi rivolgere ad un terzo che lo possa identificare. Le transazioni in criptovalute sono, pertanto, definite

[5] C. Brening, G. Müller, *Economic Analysis of Cryptocurrency Backed Money Laundering*, in *ECIS 2015 Completed Research Papers*, 2015, 20, pp. 4 ss.

[6] G. Soana, *Regulating cryptocurrency checkpoints. Fighting a trench war with cavalry?*, in *Economic Notes*, 2021, 2.

[7] Committee on Homeland Security and Governmental Affairs, *Beyond Silk Road: potential risks, threats, and promises of virtual currencies*, cit., p. 34.

[8] D. Brown, *Cryptocurrency and Criminality: The Bitcoin Opportunity* in *The Police Journal: Theory, Practice and Principles*, 2016, p. 328.

[9] D. Carlisle, *Virtual Currencies and Financial Crime: Challenges and Opportunities* in *Royal United Services Institute for Defence and Security Studies*, 2017, p. vi.

pseudonime[10] in quanto, seppur il singolo account è identificato univocamente mediante una c.d. chiave pubblica, tale chiave pubblica non fornisce alcuna indicazione in merito all'identità dell'utente che la utilizza. Inoltre, le criptovalute permettono la creazione senza alcun costo di un numero indefinito di account, con la conseguente possibilità per l'utente di utilizzare una differente chiave pubblica per ogni transazione effettuata[11].

D'altra parte, la blockchain, se garantisce una certa opacità in termini di individuazione degli utenti, è piuttosto trasparente quanto alla catena delle transazioni. Invero, le criptovalute non reintroducono il sistema di transazioni mediante token tipico dei contanti, ma mantengono un sistema basato su account[12]: spostano semplicemente la gestione del registro contabile dal terzo intermediario all'intero network di utenti, i quali, mediante un sistema cooperativo/competitivo, si occupano del mantenimento ed aggiornamento di quest'ultimo. Tale gestione corale comporta che il registro blockchain sia pubblico, in quanto chiunque può entrare a farne parte e partecipare al suo mantenimento senza alcun filtro all'ingresso. Ciò implica che, a differenza dei registri privati tenuti dagli intermediari, l'intero registro blockchain è pubblicamente accessibile e chiunque può monitorare l'attività e verificare la ricchezza associata ad una determinata chiave pubblica.

Le criptovalute, pertanto, nel bypassare la necessità per gli utenti di avvalersi di intermediari negli scambi di valore digitale, intaccano la premessa fattuale su cui è basata la normativa antiriciclaggio - per scambiare valore online è necessario avvalersi di un intermediario – diminuendone fortemente la cogenza concreta.

È interessante sottolineare come tale effetto sul sistema di sorveglianza approntato dalla normativa antiriciclaggio non sia casuale ma voluto; invero scopo, quantomeno iniziale, delle criptovalute è proprio quello di fornire agli individui uno strumento di pagamento digitale che sfugga alla necessità di avvalersi di un terzo intermediario e, pertanto, di sottoporsi alla sorveglianza

[10] G. Soana, *Cripto-valute e riciclaggio. Modus operandi e tentativi regolatori*, in *Diritto di Internet*, 2019, p. 674; seppure sull'efficacia di detta pseudonimia si veda S. MeikleJohn *et al.*, *A Fistful of Bitcoins: Characterizing Payments among Men with No Names*, in *Proceedings of the 2013 Conference on Internet Measurement Conference*, 2016.

[11] Per approfondire il funzionamento della blockchain si veda l'approfondita analisi di A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, 2017.

[12] Le criptovalute sono, da alcuni, erroneamente identificate come sistemi di pagamento mediante token sulla base dell'assenza di un intermediario nella struttura dei pagamenti da queste permessi; questa qualificazione è errata in quanto le criptovalute si basano integralmente su un sistema di contabilizzazione basato su account – le c.d. chiavi pubbliche – a cui sono abbinati entrate ed uscite contabili sulla cui base il soggetto si può dire proprietario delle relative cripto.

pubblica e privata[13]. In quest'ottica, le criptovalute costituiscono uno degli esempi di maggior successo di utilizzo normativo del codice informatico da parte di privati, ovvero di sviluppo di un'architettura tecnologica quale mezzo per l'ottenimento di un fine normativo[14].

2. Lo spettro definitorio. Dalle valute virtuali alle cripto-attività

Il rischio esistenziale che le valute virtuali pongono al sistema di sorveglianza dei flussi finanziari non è certamente passato inosservato. Se, da una parte, le valute virtuali sono divenute il mezzo di scambio privilegiato per la remunerazione dei reati online - dai *ransomware* ai *dark market*[15] – d'altra parte, la regolamentazione antiriciclaggio è stata la prima normativa ad incidere su questo mercato, con la Raccomandazione del Gruppo di Azione Finanziaria Internazionale (GAFI) risalente al «lontano» 2015.

In un mondo in continua e frenetica evoluzione il primo ostacolo con cui si è dovuto confrontare il legislatore è stato cristallizzare in una definizione il fenomeno delle valute virtuali. La complessità di tale sforzo è resa evidente dalla ampia variazione nella terminologia e nel contenuto delle definizioni dettate nel corso del tempo, nonché dai differenti approcci presi

[13] Le radici di tale azione di tecnologia normativa vanno ricercate nel movimento cypherpunk e, più in generale, in quella linea di ricerca ed attivismo preoccupato dalle crescenti potenzialità di sorveglianza dalla digitalizzazione. Già nel lontano 1975, l'allora direttore del Centro di Studi Avanzati in Scienze Comportamentali dell'Università di Stanford Paul Armer, aveva identificato nella digitalizzazione degli strumenti di pagamento lo strumento con il potenziale di creare il miglior sistema non intrusivo di sorveglianza, si veda P. Armer, *Computer Technology and Surveillance,* Center for Advanced Study in the Behavioral Sciences University of Stanford California, 1975; a tali preoccupazioni diedero seguito altri studiosi, in particolare David Chaum e, a partire dai primi anni Novanta il c.d. movimento cypherpunk. In particolare, il movimento cypherpunk si proponeva quale scopo ultimo lo sviluppo di soluzioni crittografiche accessibili e democratiche volte al miglioramento della privacy individuale; una delle linee di ricerca principale di tale gruppo era proprio lo sviluppo di un mezzo di pagamento che permettesse di preservare la privacy individuale, per un approfondimento su storia ed obbiettivi di tale movimento si veda by P. Anderson, *Cypherpunk ethics. Radical ethics for the digital age*, 2022 e C. Jarvis, *cypherpunk ideology: objectives, profiles, and influences (1992-1998),* in *Internet Histories*, 2021, 7, quest'ultimo identifica quattro obiettivi fondamentali caratterizzanti questo movimento «1) Unregulated citizen encryption access; 2) Anonymous communications; 3) Freedom to conduct anonymous economic transactions (crypto currencies); 4) Development of leaking platforms to constrain government power».

[14] Si veda quanto affermato da F. Brunton, *Digital Cash. The unknown history of the anarchist, utopians, and technologists who created cryptocurrencies*, Princeton University Press, 2019.

[15] Committee on Homeland Security and Governmental Affairs, *Beyond Silk Road: potential risks, threats, and promises of virtual currencies*, cit., p. 34.

dai regolatori a livello globale. Dato l'ambito del presente articolo, la presente analisi si concentrerà sulla dimensione europea analizzando, pertanto, le fonti GAFI e UE.

Partendo dalla prima delle definizioni fornite a livello GAFI, questa può essere rintracciata nel report pubblicato dal medesimo GAFI nel 2014[16], poi ripresa dalla Raccomandazione del 2015[17]. Entrambi questi documenti etichettavano l'oggetto della regolamentazione con il termine valuta virtuale, distaccandosi parzialmente dalla definizione, al tempo prevalente, di criptovaluta. La valuta virtuale veniva definita come: «una rappresentazione digitale di valore che può essere scambiata digitalmente e può essere utilizzata quale (1) mezzo di scambio (2) unità di conto e (3) riserva di valore ma non ha corso legale in alcuna giurisdizione[18]». Fulcro della definizione in parola, per come evidenziato dall'utilizzo del termine valuta e dal richiamo espresso alle tre funzioni classiche della moneta, era la natura di mezzo di scambio di origine privata delle valute virtuali[19].

Tale approccio viene parzialmente rivisto nel 2018, quando, mediante una modifica al proprio glossario, il GAFI ritorna sulla definizione alterandone la forma ed il contenuto; nella nuova definizione il termine utilizzato cambia da valuta virtuale ad asset virtuale, definito come una «rappresentazione digitale di valore che può essere scambiata o trasferita digitalmente ed utilizzata a fini di pagamento o investimento[20]». Con la definizione del 2018, pertanto, il GAFI si allontana dalla funzione monetaria per abbracciare una concezione più ampia della funzione e della natura di questi asset.

Il cambio di approccio è ascrivibile a due principali ragioni.

Dal punto di vista politico, l'utilizzo del termine valuta, e il conseguente accostamento di questi strumenti alle valute *fiat*[21], è stato indicato come fuorviante per il mercato – in quanto fa presumere, erroneamente, un profilo di

[16] Financial Action Task Force, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, Paris, 2014.

[17] Financial Action Task Force, *Guidance for a risk-based approach Virtual Currencies*, Paris, 2015.

[18] *Ibidem*, p. 26: «Virtual currency is a digital representation of value that can be digitally traded and functions as a (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment)6 in any jurisdiction».

[19] Per un'analisi di questa definizione si veda Soana, *Cripto-valute e riciclaggio. Modus operandi e tentativi regolatori,* cit., p. 677.

[20] «A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes», per il glossario del GAFI, https://www.fatf-gafi.org/glossary/.

[21] Con il termine valuta *fiat* si identificano tradizionalmente le valute emesse da una Banca Centrale ed avente corso legale in una determinata giurisdizione.

rischio simile alla moneta a corso legale – e pericoloso per il mantenimento del monopolio statuale della moneta, virtualmente insidiato da tali strumenti.

Dal punto di vista della conformazione del mercato, se la prima delle valute virtuali, il Bitcoin, era nata con lo scopo di fornire un mezzo di scambio libero dal giogo dell'intermediazione e della sorveglianza pubblica e privata, la funzione monetaria di tali strumenti è risultata limitata con un utilizzo concreto principalmente legato alla funzione di investimento/speculazione. Inoltre, la creazione di Ethereum[22] nel 2014 ha comportato una diversificazione nel mercato di riferimento, con il progressivo inquadramento dei token blockchain quali strumenti flessibili per l'incorporazione e la trasmissione di valore digitale, ed il conseguente sviluppo di funzionalità più complesse – dai c.d. Token non-fungibili (NFT) alla finanza decentralizzata (DeFi). In quest'ottica, la definizione del 2018 amplia la prospettiva, sia dal punto di vista terminologico utilizzando il termine più neutro di asset, sia contenutistico abbandonando la tripartizione tipica della moneta per una generica funzione di pagamento o investimento.

Nonostante la differenza in termini di approccio, entrambe le definizioni GAFI sono ispirate allo stesso principio di base: la neutralità tecnologica[23]. Il principio in parola statuisce che il legislatore debba regolamentare i fenomeni tecnologici – in questo caso l'emissione privata di token digitali di valore – in maniera unitaria, senza esprimere una preferenza per una piuttosto che per altra tecnologia[24]; in tal senso, le definizioni fornite dal GAFI non danno alcuna rilevanza all'utilizzo, da parte della specifica valuta, di tecnologia blockchain ovvero di altra tecnologia.

L'approccio normativo appare fallace se analizzato alla luce del rischio concretamente posto dalle valute virtuali al sistema antiriciclaggio: invero, come evidenziato nel precedente paragrafo, la natura decentralizzata e disintermediata della tecnologia blockchain crea una vulnerabilità essenzialmente nuova e diversa rispetto alla mera emissione centralizzata di valore da parte di un soggetto privato.

La domanda pertanto sorge spontanea: se è la tecnologia stessa a creare una nuova necessità regolamentare è corretto prescinderne nel definire la portata di una normativa?

[22] Su Ethereum si veda, https://ethereum.org/en/what-is-ethereum/.

[23] Come espressamente affermato dallo stesso GAFI, sul punto si veda Financial Action Task Force, *Updated guidance for a risk-based approach. Virtual assets and virtual asset service providers*, Paris, 2021, p. 22, «these definitions aim for technology neutrality. That is, they should be applied based on the basic characteristics of the asset or the service, not the technology it employs».

[24] Su questo concetto e i suoi aspetti critici si veda C. Reed, *Taking sides on technology neutrality*, in *SCRIPTed*, 2007, p. 4; B. Greenberg, *Rethinking technology neutrality*, in *Minn. L. Rev.*, 2015, p. 100.

Il pericolo è fornire una risposta regolamentare che, attraverso un approccio del «tutti dentro», non si adatti alle caratteristiche e agli specifici rischi del fenomeno analizzato. In quest'ottica, è chiaro come sia qualitativamente differente una valuta virtuale basata su blockchain – che permette transazioni da pari a pari, in assenza di filtri all'ingresso e di un centro di governance centralizzato – da una centralmente emessa da un ente privato – che ha la possibilità di gestire la rete e ne trae un guadagno. Se, nel primo caso, data la natura decentralizzata della governance blockchain, il rischio è quello dell'assenza di intermediari che possano formare oggetto di regolamentazione, nel secondo caso, vi è un soggetto, il gestore della rete, che può essere sottoposto alla normativa antiriciclaggio ed ai correlativi obblighi di identificazione e monitoraggio. Ciononostante, sulla base delle definizioni fornite dal GAFI, entrambi questi strumenti sarebbero oggetto della stessa regolamentazione.

Questo approccio sembra essere stato superato, almeno a livello definitorio, dal legislatore europeo. Invero, se la V Direttiva Antiriciclaggio[25] ricalca la definizione fornita dal GAFI nel 2018, seppur adottando la precedente terminologia di valuta virtuale, la nuova proposta di Regolamento sul mercato in cripto-attività (MiCaR) presentata dalla Commissione Europea nel 2020 ed attualmente in fase di approvazione, propone un deciso cambio di rotta[26].

A differenza della precedente Direttiva, la proposta di Regolamento adotta una definizione che si incentra sulla tecnologia sottostante: segnatamente, l'articolo 3, co. 1.2, definisce cripto-attività «una rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga». Questa definizione, rispetto a quella dettata dalla V Direttiva, da una parte, amplia l'oggetto della regolamentazione estendendo l'ambito dalla rappresentazione di valore a quella di diritti ed eliminando il vincolo del fine di pagamento o investimento, dall'altra, restringe l'applicabilità della regolazione alle sole attività che utilizzino tecnologie a registro distribuito.

Nonostante il Regolamento MiCa non costituisca normativa di settore, la definizione da questo dettata è destinata ad assumere, almeno sulla base dei testi attualmente proposti, una valenza sistematica. Invero, il futuro pacchetto antiriciclaggio – composto da Regolamento Antiriciclaggio[27], VI Direttiva[28] e Regolamento sulla *travel rule*[29] – proposto dalla Commissione nel 2020, la cui approvazione è attesa nel corso del prossimo anno, adotta la

[25] Direttiva dell'Unione Europea, 30 maggio, 2018, n. 843.
[26] Proposta di Regolamento dell'Unione Europea, 24 settembre, 2020, n. 0265.
[27] Proposta di Regolamento dell'Unione Europea, 20 luglio 2021, n. 0239.
[28] Proposta di Direttiva dell'Unione Europea, 20 luglio 2021, n. 0250.
[29] Proposta di Regolamento dell'Unione Europea, 20 luglio 2021, n. 0241.

terminologia di cripto-attività e rinvia, quanto al contenuto della definizione, al Regolamento MiCA.

Se la customizzazione della strategia antiriciclaggio, mediante il restringimento dell'ambito di applicazione alle sole tecnologie a registro distribuito, è certamente un passo avanti per la creazione di un approccio *ad hoc*, la definizione in parola non inquadra quegli elementi che sono di maggior rilevanza per il controllo dei flussi finanziari: la disintermediazione e l'assenza di un organo di governance. Segnatamente, a norma dell'articolo 3 MiCAR per tecnologia a registro distribuito si intende: «Un tipo di tecnologia che supporta la registrazione distribuita di dati cifrati»; questa definizione ricomprende tutta una serie di tecnologie estremamente differenti tra loro per caratteristiche e modalità di funzionamento, vanificando, parzialmente, i benefici della customizzazione normativa.

Un esempio renderà evidente questa differenza. Una delle distinzioni più marcate nel mercato blockchain è tra reti *permissionless* e *permissioned*: le prime, utilizzate ad esempio da Bitcoin ed Ethereum, non prevedono alcun centro di governance, chiunque può entrare a farne parte e partecipare all'aggiornamento ed al mantenimento del network; le seconde, caratteristiche delle versioni aziendali e statuali della blockchain, prevedono, al contrario, un centro di governance che può decidere sull'accesso alla rete ed assegnare i relativi diritti di scrittura/lettura[30]. A norma della definizione fornita dal regolamento MiCa, entrambe queste blockchain ricadono nell'ambito delle tecnologie a registro distribuito e sono pertanto sottoposte alla stessa regolamentazione. Nonostante tale scelta normativa, è chiaro come, nel caso delle reti *permissioned*, la strategia da adottare sia sostanzialmente differente da quella delle reti *permissionless*: segnatamente, mentre le seconde si caratterizzano per l'assenza di un ente centralizzato su cui sia possibile imporre una regolamentazione e, pertanto, per il profilo di rischio tipico delle valute virtuali, le prime, al contrario, presentano un centro di governance che controlla l'accesso al network e che può essere oggetto di regolamentazione e porsi quale filtro necessario per l'ingresso al mercato cripto.

In quest'ottica, il Regolamento MiCa, nel customizzare la definizione alle tecnologie a registro distribuito, non incorpora quelle caratteristiche del mercato blockchain rilevanti per la strategia normativa di settore.

Per concludere, *de iure condito*, la definizione di valute virtuali (a livello europeo) e di asset virtuali (a livello GAFI) esprime una nozione molto ampia che prescinde dalla tecnologia a queste sottostante; al contrario, *de iure condendo*, la definizione di cripto-attività (dettata dal Regolamento MiCa)

[30] P. Jayachandran, *The difference between public and private blockchain, in Blockchain Pulse: IBM Blockchain Blog*, https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/.

restringe il campo ad un categoria specifica di tecnologie – le tecnologie a registro distribuito – senza, d'altro canto, distinguere a seconda del livello di governance e centralizzazione da queste permesso. La definizione proposta dal legislatore è, pertanto, eccessivamente ampia e non sufficientemente specifica in termini di identificazione delle categorie rilevanti per il controllo dei flussi finanziari.

3. La regolamentazione antiriciclaggio

Identificata l'ampiezza del campo di gioco tracciato dal legislatore, è ora il momento di analizzare quale sia stata la strategia da questi attuata al fine di riportare il mercato delle valute virtuali all'interno del perimetro di controllo tratteggiato dalla normativa antiriciclaggio.

A tal fine, è possibile suddividere l'azione legislativa di settore in tre fasi scandite rispettivamente dalle raccomandazioni GAFI del 2015, 2019 e 2021.

3.1. Recintare il mercato cripto. La Raccomandazione GAFI 2015 e la V Direttiva

La prima risposta normativa all'avvento delle valute virtuali è stata di tipo prettamente reattivo, legata ad un fatto di cronaca che ha catapultato i Bitcoin da un oscuro fenomeno di cui si discuteva su blog specializzati alle aule del Senato degli Stati Uniti[31]: il *dark market* Silk Road[32]. Creato da un giovane ingegnere texano nel 2011, Silk Road era la prima versione di quella che sarebbe divenuta una fiorente industria: i mercati neri online. Questo sito, sfruttando il software TOR, permetteva ai propri utenti di comprare e vendere online, in pieno anonimato, creando una specie di ebay del commercio illegale[33]. I Bitcoin costituivano un tassello fondamentale di questo mercato essendo l'unica valuta accettata: segnatamente, le valute virtuali chiudevano il cerchio di

[31] Si veda Committee on Homeland Security and Governmental Affairs, *Beyond Silk Road: potential risks, threats, and promises of virtual currencies*, Washington, 2013.

[32] Per una breve storia si veda D. Adler, *Silk Road: The Dark Side of Cryptocurrency*, in *Fordham Journal of Corporate and Financial Law Blog*, 21 February 2018, https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/.

[33] È interessante sottolineare come la creazione di un simile mercato fosse stata già prevista dai primi creatori del movimento cypherpunk, i padri spirituali delle criptovalute, si veda quanto affermato da T. May, *The cryptoanarchist manifesto*, 1988, «crypto anarchy will allow national secrets to be traded freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion».

anonimato di Silk Road permettendo agli utenti di commerciare online senza l'intermediazione di un istituto finanziario e, pertanto, sfuggendo agli obblighi di identificazione e monitoraggio imposti dalla normativa antiriciclaggio.

Le dimensioni di questo mercato e la, almeno iniziale, impotenza delle autorità generarono l'urgenza politica di fornire una risposta rapida e forte; lo strumento scelto fu quello della legislazione antiriciclaggio.

Segnatamente, a giugno 2014, a distanza di appena un anno dall'oscuramento di Silk Road, il GAFI pubblicò il suo primo report sulle valute virtuali seguito, l'anno successivo, dalla prima raccomandazione in questo ambito.

La strategia del GAFI, con la Raccomandazione del 2015[34], era quella di provare a recintare il mercato cripto attraverso la regolamentazione dei suoi punti di intersezione con il mercato finanziario tradizionale[35]. In tal senso, il GAFI raccomandava di «applicare gli obblighi AML/CFT per come specificati dagli standard internazionali ai servizi di cambiavalute ed ogni altra istituzione che agisca quale nodo laddove le attività in valute virtuali si intersecano con il mercato finanziario regolamentato in valuta fiat[36]».

Fulcro di questo primo approccio strategico erano i servizi di cambiavalute tra *fiat* e cripto, ovvero tutti quei soggetti centralizzati che avevano iniziato, a fronte del crescente valore delle valute virtuali, a fornire stabilmente servizi di cambio tra cripto e valute a corso legale.

La raccomandazione fu recepita per prima dal legislatore italiano con il d.lgs. 90/2017 che inserì, tra i soggetti obbligati a norma del d.lgs. 231/2007, «i 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» e, successivamente, dalla Direttiva UE 843/2018 (c.d. V Direttiva AML) che, rispetto all'intervento nazionale, aggiunse tra i soggetti obbligati anche i prestatori di servizi di portafoglio digitale, definiti come «un soggetto che fornisce servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali».

Questo primo approccio, segnato con tutta probabilità più dalla volontà di rammendare rapidamente la falla aperta dai Bitcoin nel sistema di con-

[34] Financial Action Task Force, *Guidance for a risk-based approach Virtual Currencies*, cit.

[35] Come chiaramente statuito da Financial Action Task Force, *Guidance for a risk-based approach Virtual Currencies*, cit., 6, «the focus of this Guidance is on convertible virtual currency exchangers which are points of intersection that provide gateways to the regulated financial system».

[36] Financial Action Task Force, *Guidance for a risk-based approach Virtual Currencies*, cit., 6, «countries should consider applying the relevant AML/CFT requirements specified by the international standards to convertible VC exchangers, and any other types of institution that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system».

trollo dei flussi finanziari e di limitare i correlativi danni, che di fornire una risposta duratura al problema affrontato, si basa su un'incompleta comprensione in merito al funzionamento del mercato delle valute virtuali. Invero, come precedentemente menzionato, le valute virtuali non prevedono alcun nodo necessario – inteso quale intermediario da cui si debba inevitabilmente passare per entrare e/o uscire dal mercato – poiché non esiste un checkpoint obbligato che possa, pertanto, essere disciplinato con effetti equivalenti a quelli ottenuti con la regolamentazione degli intermediari nel mercato tradizionale. Se è vero che gli utenti possono rivolgersi a servizi di cambiavalute centralizzati, tale scelta è, nell'architettura cripto, una mera possibilità e non una necessità: gli individui potranno sempre accedere al mercato acquistando direttamente da altri utenti privati o mediante l'utilizzo di cambiavalute decentralizzati evitando, così, i controlli apprestati dalla normativa in esame.

La parzialità dell'approccio è, d'altro canto, espressamente riconosciuta dallo stesso legislatore Europeo che, al considerando nove della V Direttiva antiriciclaggio, afferma «l'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato».

È probabilmente a causa di tale consapevolezza che il legislatore Europeo arricchisce la strategia di mero recintamento adottata dal GAFI – che raccomandava la regolamentazione dei soli cambiavalute *fiat*/cripto – con l'inclusione dei prestatori di portafoglio digitale, probabilmente per la somiglianza dell'attività da questi svolta con quella di deposito bancario. Per i gestori di portafoglio vale stessa la critica già stessa sollevata per i cambiavalute: non vi è alcuna necessità per gli utenti di utilizzare un prestatore di servizi di portafoglio, potendo questi custodire le proprie valute virtuali privatamente senza doversi rivolgere ad alcun intermediario[37].

Se la strategia regolamentare unicamente incentrata sugli intermediari equipara in maniera errata il funzionamento del mercato cripto a quello tradizionale, al contempo, la regolamentazione dei soli punti di intersezione tra i due mercati sottovaluta la capacità di nascondimento delle valute virtuali e la potenzialità espansiva del mercato stesso.

Dal primo punto di vista, al momento del cambio, l'intermediario che effettua i controlli antiriciclaggio vede solo l'ultimo tratto della catena di transazioni associata ad un determinato account, permettendo al soggetto

[37] D. Carlisle, *Virtual Currencies and Financial Crime: Challenges and Opportunities*, cit., 24.

attivo di occultare l'origine illecita dei proventi cambiati attraverso una serie di operazioni non sottoposte a monitoraggio: quali il cambio dei proventi attraverso diverse criptovalute[38], l'utilizzo di servizi di offuscamento della catena delle transazioni[39], ecc. Il rischio è che, anche laddove il criminale utilizzasse un cambiavalute e l'intermediario svolgesse correttamente i controlli antiriciclaggio, questi sarebbero inutili data l'impossibilità per il soggetto obbligato di identificare la transazione come sospetta.

Dal secondo punto di vista, regolare i meri punti di contatto comporta che quanto avviene all'interno del mercato rimane escluso da ogni forma di monitoraggio; tale esclusione sottovaluta l'attitudine di attività economiche cripto-native ad essere utilizzate quali innovative forme di riciclaggio.

Un esempio di come questo secondo rischio possa concretizzarsi è offerto dalle c.d. Offerte Iniziali di Criptovalute (ICO)[40]. Le ICO sono una forma innovativa di finanziamento per startup effettuata attraverso l'emissione di valute virtuali. Essenzialmente, una startup, al fine di finanziarsi, effettua un'emissione di criptovalute native – una valuta creata *ad hoc* per il progetto – che è legata in vari modi al successo dell'impresa stessa (aumento del valore della criptovaluta, diritto di voto, diritto ai dividendi etc.); solitamente, chiunque può acquistare questa criptovaluta pagando con altra criptovaluta e finanziare, pertanto, l'impresa.

A norma della strategia legislativa fin ora analizzata, sia l'emissione di criptovalute sia l'acquisto mediante altra criptovaluta non è attività regolamentata e, pertanto, non richiede la sottoposizione ad alcun controllo antiriciclaggio. Si pensi allora ad un soggetto che si trovi a detenere Bitcoin di origine illecita -derivanti, ad esempio, dalla vendita di stupefacenti su un *dark market* – questi potrebbe creare una startup fittizia, effettuare una ICO ed autofinanziarsi mediante versamenti anonimi da lui stesso effettuati; se questi procedesse a rivolgersi ad un cambiavalute, quest'ultimo non avrebbe ragione di dubitare dell'origine lecita delle valute virtuali cambiate essendo

[38] Questa condotta è conosciuta in gergo come *chain hopping*, ed è particolarmente efficace in quanto interrompe la catena di transazioni spezzettandola tra varie blockchain, si veda A. Moiseienko, O. Kraft, *From money mules to chain hopping. Targeting the finances of cybercrime*, *Rusi*, 2018, pp. 40-41.

[39] Data la relativa trasparenza del registro blockchain, sono stati creati una serie di servizi che permettono di offuscare la catena delle transazioni garantendo maggiore privacy; questi servizi, utilizzati anche a fini legali, giocano un ruolo cruciale nell'utilizzo criminoso delle valute virtuali, per un esempio si veda il recente caso del mixer Tornadocash che è stato sanzionato dal Dipartimento del Tesoro Americano per il ruolo svolto nel riciclaggio dei proventi del Lazarus Group, un collettivo di hacker collegato con la Corea del Nord, si veda, https://home.treasury.gov/news/press-releases/jy0916.

[40] Per il rapporto esistente tra ICO e riciclaggio si veda G. Forgang, *Money Laundering through Cryptocurrencies* in *Economic Crime Forensics Capstones*, 2019, 4, p. 17.

queste derivate da una ICO lecita e destinate a finanziare la startup del nostro tecnologico criminale.

Se le ICO sono state il primo esempio di attività lucrativa tutta interna al mercato cripto, non sono certo l'unica: si pensi agli NFT[41], le soluzioni di finanza decentralizzata (DeFi)[42] etc.

Per concludere, il legislatore nel 2014/2015 si trova ad affrontare, in un clima emergenziale, la falla aperta dalle valute virtuali nell'infrastruttura antiriciclaggio; la risposta fornita è incentrata su un approccio tradizionale focalizzato sugli intermediari – i cambiavalute e, nel caso europeo, i fornitori di servizi di portafoglio – e sul tentativo di recintare il mercato cripto al fine di evitare traboccamenti di denaro illecito nel mercato tradizionale.

3.2. Entrare nel mercato cripto. La Raccomandazione GAFI 2019

La parzialità dell'approccio adottato nel 2015, unitamente al vertiginoso aumento nel valore e nella rilevanza delle valute virtuali, portò ad un progressivo ripensamento della strategia impiegata con la prima Raccomandazione, che si concretizzò nella revisione del glossario GAFI - di cui al precedente paragrafo - e nell'emissione della Raccomandazione 2019[43].

Tale Raccomandazione modifica solo parzialmente la rotta presa nel 2015: se, da una parte, il GAFI abbandona l'idea di provare a recintare il mercato delle valute virtuali mediante la creazione di un sistema di sorveglianza di confine, d'altra parte, la seconda Raccomandazione continua a concentrare il fuoco regolamentare sugli intermediari, semplicemente ampliandone il novero.

Invero, la principale innovazione introdotta nel 2019 consiste nell'ampliamento della definizione di fornitore di servizi di valuta virtuale (VASP) mediante l'inclusione, in aggiunta ai, già precedentemente regolati, servizi di cambiavalute da cripto a *fiat*, anche di quegli enti che svolgono professionalmente: 1) attività di cambio tra valute virtuali (cripto-to-cripto), 2) attività di trasferimento di valute virtuali per conto di terzi, 3) custodia o amministrazione di valute virtuali, 4) partecipazione o fornitura di servizi finanziari relazionati all'emissione o vendita di valute virtuali[44].

[41] Per un approfondimento in merito all'impatto degli NFT sulla normativa antiriciclaggio si veda A. Mosna, G. Soana, *When art goes virtual: what status for collectible NFTs under the current EU Anti Money-Laundering regime?*, in *EU Law Analysis*, 13 August 2022.

[42] Per un'analisi del concetto di DeFi si veda OCSE, *Why Decentralized Finance matters and the policy implications*, Paris, 2022.

[43] Financial Action Task Force, *Guidance for a Risk-based approach. Virtual assets and virtual asset service providers*, Paris, 2019.

[44] Si veda Financial Action Task Force, *Guidance for a Risk-based approach. Virtual assets and virtual asset service providers*, cit., p. 57: «Virtual asset service provider as any natural or

All'ampliamento operato dalla seconda Raccomandazione si è adeguato il legislatore Nazionale con il D.lgs. 125/2019, il quale ha esteso gli obblighi antiriciclaggio a tutti i Prestatori di Servizi relativi all'utilizzo di valuta virtuale definiti come «ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute» e ai prestatori di servizi di portafoglio digitale definiti come «ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali».

In breve, con la Raccomandazione 2019, il GAFI modifica parzialmente la strategia ma non l'approccio di base. Il novero dei soggetti ricompresi nell'ambito della normativa è esteso al di là dei meri punti di contatto tra mercato cripto e *fiat* con l'inclusione, sostanzialmente, di ogni entità che svolga in forma centralizzata e professionale un servizio relazionato al mercato cripto. D'altra parte, la legislazione del 2019 continua a non affrontare l'innovazione chiave delle valute virtuali: la disintermediazione delle transazioni online e la correlativa modifica nell'architettura degli scambi di valore digitali. La seconda Raccomandazione non propone alcun approccio customizzato volto a rispondere a questa nuova architettura, né in termini di soggetti regolati, né di obblighi su questi imposti; continuando a concentrare la strategia legislativa sugli intermediari, il legislatore dimostra una certa rigidità e, soprattutto, incapacità a comprendere l'impatto dell'evoluzione tecnologica sull'efficacia concreta delle proprie scelte normative, quasi a voler spezzare quel legame reciproco che necessariamente lega realtà e normazione.

legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: *i.* Exchange between virtual assets and fiat currencies; *ii.* Exchange between one or more forms of virtual assets; *iii.* Transfer of virtual assets; and iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset».

4. Modellare l'architettura. La Raccomandazione 2021 e il Regolamento Europeo sulla «travel rule»

La Raccomandazione del giugno 2021[45] costituisce l'ultimo passo nel percorso normativo intrapreso dal GAFI nel 2014. Rispetto al 2014 e al 2019, la Raccomandazione 2021 si confronta con un mondo sempre più ampio e vario: accanto alle criptovalute «tradizionali», i token basati su blockchain sono attualmente pensati e creati per un numero crescente di funzioni che vanno ben oltre quella di mezzo di scambio: quali il collezionismo e l'espressione artistica, con gli NFT, o la fornitura di servizi finanziari, con le implementazioni di finanza decentralizzata (DeFi). Inoltre, le monete stabili (le cosiddette *stablecoins*[46]) minacciano di eliminare uno dei principali fattori di mitigazione del rischio cripto, ovvero la limitata utilizzabilità delle valute virtuali quali strumenti di pagamento. Come sottolineato nella 12-month review alla Raccomandazione del 2019 pubblicata dal GAFI nel 2020, «l'adozione di massa (delle stable coins) rischia di causare un incremento sostanziale nel numero di transazioni in asset virtuali anonime da pari a pari [...] non esplicitamente incluse nella Raccomandazione GAFI[47]» e, pertanto, ridurre drammaticamente la percentuale di transazioni effettivamente intercettate dall'attuale sistema di monitoraggio intermediario-centrico.

A fronte di questo panorama in forte evoluzione, la Raccomandazione 2021 adotta per la prima volta un approccio teso a complementare la tradizionale strategia incentrata sulla regolamentazione degli intermediari con una visione più ampia delle opportunità offerte dal mercato delle valute virtuali.

In quest'ottica, la nuova strategia del legislatore antiriciclaggio sembra muoversi lungo tre traiettorie principali: primo, rendere la blockchain più regolabile; secondo, normare il codice sottostante le applicazioni di valuta virtuale per promuovere la *compliance-by-design*; terzo, spingere l'utilizzo di soluzioni che sfruttino in maniera strutturale e non meramente investigativa

[45] Financial Action Task Force, *Updated guidance for a risk-based approach. Virtual assets and virtual asset service providers*, cit.

[46] Sul punto si veda anche Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, Paris, 2020.

[47] Financial Action Task Force, *12-month review of the revised FATF standards on virtual assets and virtual asset service providers*, Paris, 2020, p. 7: «Looking more broadly at the virtual asset market since June 2019, global government attention has largely focused on proposed so-called "stablecoins" with potential for mass-adoption. So-called stablecoins are a type of asset that purport to maintain a stable price relative to reference assets. The proposed launch of these arrangements has brought significant attention to whether their mass-adoption would lead to a substantial increase in the number of anonymous peer-to-peer virtual asset transactions occurring via unhosted wallets. Peer-to-peer transactions, without the use of a VASP or other AML/CFT-regulated entity, are not explicitly covered by the revised FATF Standards».

la trasparenza del registro blockchain – c.d. *blockchain analytics*. Queste tre linee regolamentari sono, nella Raccomandazione 2021, più dei suggerimenti tra le righe che delle vere e proprie misure normative, in quanto al momento non sono ancora ricomprese tra gli elementi cogenti.

4.1. Rendere la blockchain più regolabile

La prima linea strategica che emergono dalla Raccomandazione 2021 è rendere la blockchain più regolabile: il legislatore con questo approccio normativa è come se cercasse di gentrificare il lato cypherpunk della blockchain. Vi è un aspetto in particolare delle transazioni blockchain che costituisce l'obiettivo principale di questo sforzo: le transazioni da pari a pari.

Segnatamente, nella Raccomandazione 2021, il GAFI riconosce, per la prima volta in maniera ampia, l'esistenza del problema posto dalle transazioni da pari a pari nel sistema di monitoraggio dei flussi finanziari, dedicandogli un'apposita sezione e identificandolo come uno dei rischi chiave per l'infrastruttura antiriciclaggio[48]. Il GAFI chiarisce come il sistema attuale, in quanto incentrato sugli intermediari, rimane cieco rispetto a tutta quella massa di transazioni che per tali intermediari non passa e si sviluppa su canali meramente individuali, nonché come la crescente regolamentazione degli intermediari possa spingere le transazioni illecite verso questo cono d'ombra creando una sorta di zona franca.

D'altra parte, la Raccomandazione, pur riconoscendo la primarietà del problema, preferisce non rivolgere, per il momento, un'indicazione cogente agli stati, bensì, il GAFI dirige un mero invito a monitorare ed analizzare il settore e, laddove sia accertato un livello di rischio particolarmente elevato, applicare misure di mitigazione. Tra le misure elencate dal GAFI ve ne sono due che rivestono particolare rilevanza per la strategia in oggetto: vietare a tutti gli intermediari di effettuare transazioni con account privati – c.d. *unhosted wallet* – o prescrivere obblighi di compliance maggiori in caso di transazioni con account privati[49].

[48] Financial Action Task Force, *Updated guidance for a risk-based approach. Virtual assets and virtual asset service providers*, cit., pp. 18, 36.

[49] Financial Action Task Force, *Updated guidance for a risk-based approach. Virtual assets and virtual asset service providers*, cit., p. 40: «Depending on the assessed risks associated with P2P transactions, or certain types of P2P transactions, countries may consider and implement as appropriate options to mitigate these risks at a national level. These measures may include […] obliging VASPs to facilitate transactions only to/from VASPs and other obliged entities; e. placing additional AML/CFT requirements on VASPs that allow transactions to/from non-obliged entities (e.g., enhanced recordkeeping requirements, EDD requirements)».

Fra gli obblighi di compliance aggravati che possono essere imposti, di particolare importanza è certamente la *travel rule*.

Una piccola introduzione alla c.d. *travel rule* è d'obbligo al fine di comprendere la rilevanza della misura proposta. La *travel rule* costituisce uno degli obblighi direttamente previsti dalla raccomandazione n. 16 degli Standard[50] GAFI – che pertanto si applica a tutte le transazioni anche al di là del mondo cripto – e richiede che il soggetto obbligato includa, come parte di un trasferimento di valore da parte di un suo cliente, informazioni accurate in merito all'ordinante ed al beneficiario dei fondi e che tali informazioni siano conservate lungo la catena dei pagamenti[51]. Applicata al mondo cripto, la *travel rule* impone che i VASP, e gli eventuali intermediari tradizionali coinvolti, raccolgano le necessarie informazioni in merito al proprio cliente ed al proprietario dell'account a cui stanno inviando le valute virtuali e le includano nella transazione.

Il principale problema posto dalla *travel rule* in ambito di valute virtuali è legato al caso in cui la transazione si svolga tra un intermediario ed un account privato; invero, la travel rule – ideata per i bonifici bancari – si basa sul presupposto che ordinante e beneficiario siano entrambi serviti da un intermediario e che, pertanto, ogni intermediario effettuerà l'identificazione del proprio cliente – nell'ambito delle attività di KYC – e sarà pertanto in grado di comunicarlo alla controparte.

Ora il problema che si pone è, in caso di assenza di una controparte regolata a cui rivolgersi, in che modo può l'intermediario ottemperare all'obbligo di identificazione della controparte?

Le possibili risposte sono due.

La prima è quella fornita dal GAFI: in caso di transazione con un account privato, l'intermediario non avrà alcun obbligo di verificare l'identità della controparte, ma dovrà meramente chiedere la relativa informazione al proprio cliente[52].

[50] Financial Action Task Force, *International standards on combating money laundering and the financing of terrorism & proliferation*, Paris, 2012.

[51] *Ibidem*, p. 17: «Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain».

[52] Financial Action Task Force, *Updated guidance for a risk-based approach. Virtual assets and virtual asset service providers*, cit.: «The FATF does not expect that VASPs and FIs, when originating a VA transfer, to submit the required information to individuals who are not obliged entities. VASPs sending or receiving a VA transfer to/from an entity that is not a VASP or other obliged entity (e.g., from an individual VA user to an unhosted wallet), should obtain the required originator and beneficiary information from their customer. Countries should require their VASPs or other obliged entities to implement mechanisms to ensure effective

La seconda è imporre all'intermediario obblighi di compliance maggiori in caso questi abbia ad interagire con un account privato, ovvero di svolgere in proprio la verifica dell'identità della controparte. Questa ipotesi, anche ventilata in sede europea nell'ambito dell'aggiornamento del Regolamento sulla *travel rule*[53], comporterebbe un aggravio rilevantissimo per l'intermediario che vedrebbe estesi i propri obblighi di identificazione antiriciclaggio al di là della propria clientela. Una siffatta soluzione comporterebbe che, per l'intermediario, effettuare una transazione con un account privato avrebbe un costo molto elevato in termini di compliance: ciò potrebbe portare, almeno per le transazioni di minor valore, ad un fenomeno simile al *derisking* con intermediari che rifiutano transazioni con account privati.

Tutte queste soluzioni – divieto per gli intermediari di transare, obblighi di compliance aggravati, verifica della controparte privata in ambito *travel rule* – per ora solo accennate dal regolatore, condividono un approccio comune: la volontà di influenzare lo sviluppo del mercato, e della tecnologia, in una direzione congeniale agli obiettivi legislativi; il legislatore, con tali misure, cambia parzialmente approccio e rivolge la propria attenzione verso la modifica stessa del mercato al fine di escludere o, quantomeno, ridurre fortemente un'attività considerata rischiosa.

Il problema principale legato a queste soluzioni normative è l'allontanare il mercato dalla principale innovazione della blockchain: la disintermediazione. Invero, se l'utilizzo dei VASP è diventato prevalente negli ultimi anni a causa dell'ingresso di sempre più investitori attratti più dalle vertiginose oscillazioni del prezzo che da un interesse, e forse persino, comprensione della blockchain, una valuta virtuale totalmente intermediata non è altro che un modo estremamente inquinante ed inefficiente di scambiare valore. L'innovazione chiave della blockchain è precisamente la possibilità di scambiare valore senza doversi rivolgere, e quindi fidare, di un intermediario: se l'utilizzo degli intermediari diviene *de facto* obbligatorio, qual è lo scopo di questa tecnologia?

scrutiny of such transfers, in particular to meet their STR and sanctions implementation obligations (see the discussion of Recommendation 20 below) and, as discussed above, may choose to impose additional limitations or controls on such transfers with unhosted wallets».

[53] Si veda quanto statuiva il co. 29a della Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) (COM(2021)0422 – C90341/2021 – 2021/0241(COD)) «in cases of a transfer of crypto-assets made from or to an unhosted wallet, the provider of crypto-asset transfers should collect information from its customer both on the originator and the beneficiary. The provider of crypto-asset transfers should verify the accuracy of information with respect to the originator or beneficiary behind the unhosted wallet, and ensure that the transfer of crypto-assets can be individually identified».

In tal senso, se la strategia normativa ha dei meriti in quanto approccia in maniera innovativa ad un problema tuttora aperto, il rischio è che, nel tentativo di gentrificare la blockchain, si perda la ragione stessa che la rende una tecnologia innovativa.

4.2. Dall'intermediario al creatore del network

La seconda linea strategica su cui si muove il legislatore antiriciclaggio con la Raccomandazione 2021 è quella della crescente responsabilizzazione, in termini antiriciclaggio, dello sviluppatore del software, ovvero di colui che materialmente progetta, scrivendone il codice, la rete blockchain o una sua implementazione.

Per comprendere le coordinate di questa strategia normativa è necessario descrivere brevemente il concetto di regolamentazione architetturale. Introdotto dalla dottrina statunitense alla fine del secolo scorso e, in particolare, dai proff. Lessig[54] e Reidenberg[55], questa linea di studio sottolinea come l'azione dell'uomo è guidata e regolata non solo dal diritto – e dalle classiche forze della morale ed economia – ma anche da una forza occulta: l'architettura[56]. Per architettura si intende quel set di regole di tipo ambientale o fisiologico (si pensi alla legge di gravità) che circoscrive esternamente l'uomo dettando ciò che questi può fare; siffatta forza normativa è rimasta piuttosto in disparte nel dibattito accademico tradizionale, in quanto l'architettura analogica preesiste l'uomo ed è per questi una costante più che una variabile su cui questi può agire[57] (si pensi ancora alla forza di gravità, nulla può il legislatore per modificarla o aggirarla). A differenza del mondo analogico, l'architettura del mondo digitale – ovvero, il codice informatico che detta le regole di funzionamento dell'ambiente di volta in volta creato – è di creazione umana e, pertanto, modellabile a fini normativi[58]; in tal senso, è, ad esempio, possibile per il legislatore modificare il codice di un motore di ricerca al fine di impedire che determinate parole o determinati risultati siano trovabili dall'utente. Il legislatore può, pertanto, in ambito digitale agire direttamente

[54] L. Lessig, *Code and other Laws of the Cyberspace*, Basic Books, 2002.

[55] J. Reidenberg, *Lex informatica: The formulation of information policy rules through technology*, in *Tex. L. Rev*, 76, 1997.

[56] L. Lessig, *The law of the horse: What cyber law might teach*, in *Harv. L. Rev.*, 1999, 113, p. 507.

[57] Nondimeno anche nel mondo analogico esistono esempi di utilizzi dell'architettura a fini normativi, si veda Lessig.

[58] J. Reidenberg, *Lex informatica*, cit., p. 568: «Technological architectures may prohibit certain actions on the network, such as access without security clearances, or may impose certain flows, such as mandatory address routing data for electronic messages».

sull'architettura delle tecnologie di volta in volta create, scrivendo il proprio comando direttamente nel codice informatico e garantendo un'applicazione *ex ante* ed automatica del comando normativo[59].

Questo tipo di regolamentazione assume una rilevanza primaria in ambito blockchain[60]; invero, una delle più interessanti innovazioni introdotte dalla blockchain è la possibilità di creare programmi informatici – i c.d. *smart contracts* – i quali, una volta lanciati, si eseguono automaticamente ed inesorabilmente[61]. Uno dei problemi principali posti dagli *smart contracts* è che, data la loro esecuzione automatica ed ineluttabile, sono difficilmente regolabili in quanto manca una controparte umana che nel gestirne l'implementazione possa essere oggetto regolazione.

Emblematico è, in questo senso, il caso di *TornadoCash*[62]: un servizio di mixer completamente autonomo lanciato su Ethereum, che è stato oggetto di sanzioni da parte del Dipartimento del Tesoro Americano in quanto avrebbe permesso al Lazarus Group, un collettivo hacker collegato al governo Nord Coreano, di lavare 455 milioni di dollari; al fine di eseguire tali sanzioni, in assenza di un umano da colpire, il Tesoro Americano ha sanzionato direttamente il codice, ed inoltre, in assenza di un gestore, lo sviluppatore del codice è stato arrestato nei Paesi Bassi ed è attualmente in attesa di giudizio.

Ai nostri fini, ciò che è rilevante sottolineare sono due elementi della vicenda *TornadoCash*: primo, in assenza di un intermediario umano, il regolatore rivolgerà la sua attenzione direttamente sul codice; secondo, colui che ha sviluppato il codice di un'organizzazione autonoma, pur in mancanza di un diretto intento criminoso o di partecipazione all'attività concreta del software autonomo, potrebbe essere responsabile degli usi criminali di tale organizzazione autonoma.

In quest'ottica, sono numerose le normative che, negli ultimi anni, stanno spostando il fuoco dall'implementazione al design[63] così da garantire che gli standard normativi siano direttamente incisi nel codice del programma; siffatta prospettiva accresce il ruolo dello sviluppatore quale soggetto passivo

[59] L. Lessig, *The law of the horse*, cit., p. 506.

[60] P. De Filippi, A. Wright, *Blockchain and law. The rule of code*, Harvard, Harvard University Press, 2018.

[61] M. Finck, *Blockchain regulation and governance in Europe*, Cambridge, Cambridge University Press, 2018, pp. 67-68.

[62] Si veda il comunicato stampa del Dipartimento del Tesoro: https://home.treasury.gov/news/press-releases/jy0916.

[63] Si veda, ad esempio, l'approccio preso dalla Proposta di Regolamento (2021/0106 COD) in materia di intelligenza artificiale presentata dalla Commissione Europea nel 2021 che si focalizza fortemente sulla fase dello sviluppo con un approccio differenziato a seconda dell'utilizzo concreto della singola tecnologia.

di obblighi normativi, cogliendo la valenza legislativa del codice informatico e, pertanto, la natura regolamentare dell'attività di scrittura di quest'ultimo.

Il GAFI sembra prendere questa direzione seppur con cautela; invero, se da un lato, la Raccomandazione esclude che il mero sviluppo di software comporti la designazione quale VASP, d'altro lato, la stessa raccomandazione afferma che «una parte che diriga la creazione e lo sviluppo di un software o una piattaforma, in modo tale che questi possano fornire professionalmente servizi di VASP per o in vece di altra persona, è da qualificare come VASP, in particolare se mantiene il controllo o sufficiente influenza sui beni, sul software, sul protocollo [...] in quanto tale, dovrebbero effettuare una valutazione del rischio ML/TF prima del lancio o utilizzo del software o della piattaforma e prendere le precauzioni necessarie a mitigare i rischi i una maniera continuativa e con un approccio preventivo[64]». In maniera similare, la Raccomandazione nel parlare delle applicazioni di finanza decentralizzata specifica che «i creatori (di tali applicazioni) (...) potrebbero ricadere nell'ambito della definizione di VASP[65]».

Con questa Raccomandazione il GAFI sembra, quindi, voler dare un segnale a regolatori e partecipanti al mercato in merito alla responsabilità degli sviluppatori, soprattutto laddove questi progettino software decentralizzati: la scrittura di codice informatico è un'attività normativa e, pertanto, è necessario che, laddove la compliance *ex post* non sia possibile, siano creati, già a livello dell'architettura, meccanismi che garantiscano la compliance *ex ante*.

4.3. L'analisi del registro blockchain

L'ultima delle linee regolamentari che emergono dall'analisi della Raccomandazione 2021 è l'invito ad un utilizzo maggiormente strutturale delle

[64] Financial Action Task Force, *Updated guidance for a risk-based approach. Virtual assets and virtual asset service providers*, cit., p. 32, «a party directing the creation and development of the software or platform, so that they can provide VASP services as a business for or on behalf of another person, likely also qualifies as a VASP, in particular if they retain control or sufficient influence over the assets, software, protocol, or platform or any ongoing business relationship with users of the software even if this is exercised through a smart contract. Such a VASP is therefore responsible for complying with the relevant AML/CFT obligations. As such, they should undertake ML/TF risk assessments prior to the launch or use of the software or platform and take appropriate measures to mitigate the risks in an ongoing and forward-looking manner».

[65] Ivi: «However, creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralized, may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services».

tecnologie di analisi del registro blockchain. Segnatamente, se la blockchain, almeno nella sua versione completamente disintermediata, è una tecnologia che pone problemi quanto all'identificazione degli utenti, è al contempo estremamente trasparente quanto ad archiviazione delle transazioni: chiunque può scaricare l'intera catena dei blocchi e così accedere ad ogni transazione mai effettuata con una determinata valuta virtuale.

Nonostante tale chiara opportunità in termini di monitoraggio, ad oggi l'utilizzo dei software di analisi della blockchain[66] è stato sostanzialmente limitato alla fase investigativa. Con la Raccomandazione in analisi, il GAFI sottolinea la necessità di servirsi di questa caratteristica dei sistemi di archiviazione basati su *blockchain* in maniera strutturale, integrando gli strumenti di analisi nei processi di compliance.

Tale esortazione è rivolta sia ai regolatori che ai regolati. In primo luogo, quale strumento di analisi del rischio Paese, del rischio del singolo VASP e del rischio della singola transazione e/o cliente; in secondo luogo, quale strumento per l'identificazione di infrazioni da parte dei VASP e della presenza di VASP non registrati/autorizzati[67].

Il GAFI non fornisce però una struttura completa per l'inquadramento degli strumenti di analisi blockchain in termini regolatori e non investigativi; in tal senso, sarebbe opportuno, data l'evidente potenzialità di questi software a fini di miglioramento dell'attività di vigilanza, dettare linee guida chiare in merito alle *best practices* da adottare nello sviluppo ed utilizzo di tali software, nonché quali siano gli effetti giuridici che dai risultati ottenuti tramite analisi della blockchain sia opportuno e possibile trarre. Segnatamente, un aumento nell'utilizzo di tali software apre nuove opportunità per garantire un maggiore e più diretto coinvolgimento dell'ente statuale nel monitoraggio e nell'accesso al registro delle transazioni. Nel sistema tradizionale, la vigilanza si incentrava sugli intermediari, in quanto questi erano gli unici detentori delle informazioni rilevanti – essendo proprietari dei registri delle transazioni effettuate dai loro clienti – con la *blockchain* il rapporto tra regolatore e intermediario può evolversi, dato che entrambi hanno accesso, quantomeno in termini di transazioni, alle medesime informazioni con la possibilità, quindi, per il primo di giocare un ruolo più attivo. Ovviamente, tale attivismo deve essere accompagnato da chiare linee guida e vincoli normativi che starà al GAFI e al regolatore Europeo sviluppare negli anni a venire.

[66] L'analisi del registro blockchain ha spinto lo sviluppo di una fiorente industria con imprese ormai leader nel settore che collaborano regolarmente con le forze di polizia di tutto il mondo si veda ad esempio Chainanalysis https://www.chainalysis.com/crypto-investigations-and-special-programs/.

[67] Financial Action Task Force, *Updated guidance for a risk-based approach. Virtual assets and virtual asset service providers*, cit., p. 57.

5. Riflessioni conclusive

Le valute virtuali presentano nuove opportunità per la crescita e la democratizzazione del sistema finanziario globale e, più in generale, dell'intero sistema di scambio di valore online. Al contempo, la disintermediazione permessa dalla tecnologia blockchain, chiave della sua carica innovativa e della sua portata dirompente, ha messo in crisi quell'infrastruttura di monitoraggio che, a partire dagli anni Ottanta del secolo scorso, è stata messa in piedi al fine di arginare l'utilizzo di fondi illeciti in un mondo sempre più digitale e globale.

A fronte di questa sfida architetturale al proprio approccio normativo, il GAFI e l'UE hanno approntato una serie di strategie volte a riportare questo nuovo mercato nell'alveo della regolamentazione; tale sforzo ha avuto fino ad ora effetti limitati dato il suo focus sulla tradizionale categoria degli intermediari.

L'ultima Raccomandazione GAFI sembra segnare un cambio di passo con l'affiancamento al classico approccio intermediario-centrico di una nuova tattica tripartita basata su una crescente influenza sullo sviluppo del mercato, sulla regolamentazione architetturale e sull'intervento diretto della vigilanza nel registro blockchain. Questo nuovo corso, seppur al momento solo accennato, costituisce un corretto tentativo di provare a dare risposte innovative a fronte di una tecnologia che pone questioni nuove; d'altra parte, è cruciale che tali risposte, data la loro incisività sulla conformazione stessa della tecnologia regolata, tengano conto della totalità degli interessi coinvolti e non strangolino bensì guidino l'evoluzione della blockchain.

Giulio Soana
Università LUISS Guido Carli e Università Cattolica di Lovanio (Belgio)
via Parenzo 11
00198 Roma
gsoana@luiss.it
Orcid: 0000-0001-7449-5729