

Cripto Asset Compliance: regole antiriciclaggio

Sabato 16 ottobre 2021



Indice

Premessa

- 1 Dalle *cryptocurrencies* ai crypto-asset
- 2 AML vs. crypto-asset
- 3 Eventi fraudolenti
- 4 Interventi AML internazionali
- 5 Crypto asset AML compliance in Europa e Italia



Premessa



La blockchain - nata come Blockchain di Bitcoin - è stata, storicamente, la risposta alla crisi bancaria del 2008, ed ha rappresentato e rappresenta tuttora un sistema di pagamento alternativo, in cui ogni indirizzo è assimilabile ad un IBAN, con cui si possono trasferire criptovalute tra i partecipanti del network.

In un momento successivo, oltre alla immediata nascita di altre criptovalute, fondate su modifiche del medesimo protocollo Bitcoin, o su blockchain autonome, si è notata la duttilità di tale sistema decentralizzato che poteva essere usato anche per registrare transazioni che non implicavano necessariamente trasferimenti di criptovalute e valori prettamente di natura monetaria.



Verso i virtual asset

Sul protocollo a registri distribuiti (c.d. DLT) come la Blockchain Technology, si distinguono due tipi di valori:

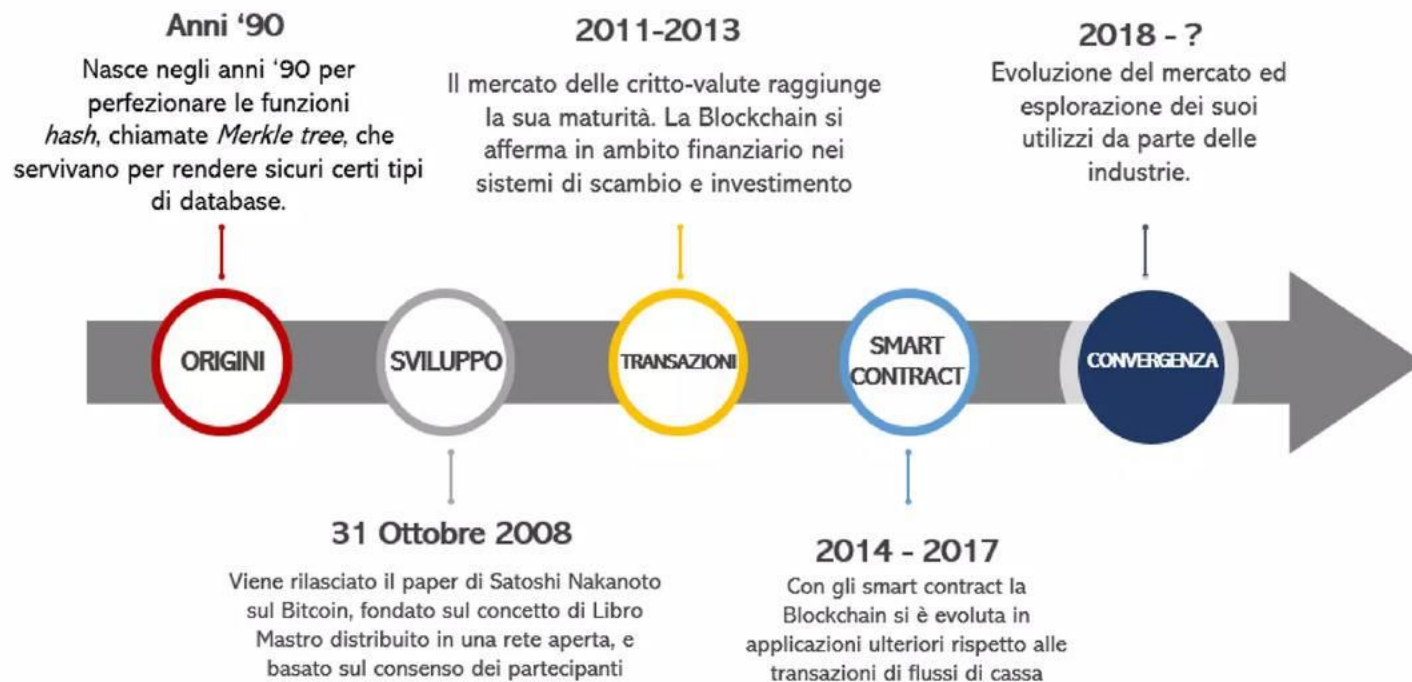
- le criptovalute (payment token), come i Bitcoin o gli Eth, per citare quelle più famose e diffuse, definite anche token nativi in quanto fisiologicamente inseriti in una propria blockchain, che rappresentano la "valuta" di scambio per i partecipanti all'interno della rete di quel registro distribuito;
- i token che rappresentano "gettoni" o asset digitali costruiti sulla blockchain attraverso strumenti quali gli smart contract.





1. Dalle *cryptocurrencies* ai crypto-asset

Evoluzione della Blockchain



Blockchain 2.0 - Internet del valore

Evoluzione

Sperimentata già a partire degli anni '90 – anche grazie a forme monetarie antenate del Bitcoin (i.e. Digi Cash, E-Gold, B-Money), con Satoshi Nakamoto e l'invenzione del Bitcoin nel 2008-2009, la tecnologia Blockchain si avvia a rivoluzionare il settore finanziario, diventando la tecnologia di base di una molteplicità di critto-valute, nate dietro la scia di Bitcoin.



Con l'avvento di Ethereum nel 2013, sorge la possibilità di "stratificare" la Blockchain con il *layer* degli smart contract per dare vita a diverse Dapp e trovare utilizzo in diversi settori.



Attraverso la capacità di combinarsi con altre tecnologie, si avvia la convergenza di Blockchain specie con IOT e AI, ottenendo lo sviluppo di una infrastruttura idonea a soddisfare le esigenze di numerose industrie



Tokenizzazione

Attraverso la possibilità degli smart contract, avutasi a partire dall'avvento di Ethereum (2013-2014), la Blockchain è divenuta programmabile.

Con gli smart contract possono essere collegati ad una blockchain - cioè al protocollo informatico che governa una determinata Catena di Blocchi - una serie potenzialmente infinita di beni, diritti e servizi.

Attraverso la linguistica computazionale, avviene la divisione delle sequenze di caratteri e lessemi descrittivi di una determinata risorsa o oggetto in unità minime di base, dette token, e si ha la possibilità di rappresentarli all'interno di un file blockchain. Durante questo processo, a detto oggetto/risorsa viene assegnato un token rappresentativo contenente uno specifico smart contract e caricato nelle strutture di dati di una blockchain diventandone una parte integrante.

In altre parole con gli smart contract, beni, diritti e servizi vengono ad essere rappresentati digitalmente in asset che circolano e vengono trasferiti lungo la medesima catena dei blocchi beneficiando delle caratteristiche tecnologiche impiegate quali, ad esempio: transnazionalità, riduzione di intermediari, velocità pressoché istantanea di esecuzione, azzeramento dei costi di transazione, ecc.

Le criptovalute o valute virtuali sono necessarie per una blockchain in quanto contribuiscono al suo corretto funzionamento e in un certo senso ne costituiscono il motore.

I *miners*, in definitiva, eseguono i calcoli crittografici per verificare ed approvare un'operazione su blockchain infatti, vengono remunerati attraverso *coin* creati nativamente dalla stessa blockchain.



Un token (o "gettone") è anch'esso, in senso lato, una criptovaluta con le caratteristiche di sicurezza, trasferibilità e non duplicabilità.

Ma a differenza delle criptovalute, non contribuendo al funzionamento della blockchain, può essere utilizzato come rappresentazione di un bene o di un diritto su un bene o servizio.



Cartolarizzazione via token



Il token digitale, gestito da uno smart contract, può rappresentare il possesso di asset reali o digitali, diritti di accesso a beni reali o digitali, oppure a servizi, diritti di voto, possibilità di svolgere azioni o ricoprire ruoli, o avere un incentivo per un determinato comportamento ecc..

E mano a mano che è progredita la tecnologia blockchain una vasta tipologia di diritti e beni off-chain sono stati «incorporati» e rappresentati in token trasferibili sulla catena dei blocchi.

Con tokenizzazione intendiamo quindi la possibilità di rappresentare il valore di un certo bene, o di un certo diritto o servizio o di una certa azione in tanti token e custodirli o scambiarli su blockchain.



Tipi di token



Payment Token o Token Nativi o di pagamento: sono tutte le criptovalute utilizzate per il funzionamento della Blockchain e che, attraverso domanda e offerta, hanno acquistato nel tempo un valore di scambio



Equity e Security Token sono prettamente strumenti finanziari. Gli Equity rappresentano una frazione della proprietà del capitale di una impresa registrato su Blockchain. I Security invece non creano diritti sul capitale dell'impresa, ma attribuiscono il diritto di compartecipazione ad utili, ecc.



Utility Token rappresentano un diritto all'acquisto o al pre-acquisto di beni e/o servizi che una piattaforma offre o si propone di offrire in futuro. Sono titoli di legittimazione finalizzati alla fruizione di un servizio digitale e sono stati utilizzati moltissimo negli ultimi anni per la raccolta di finanziamenti attraverso le ICO

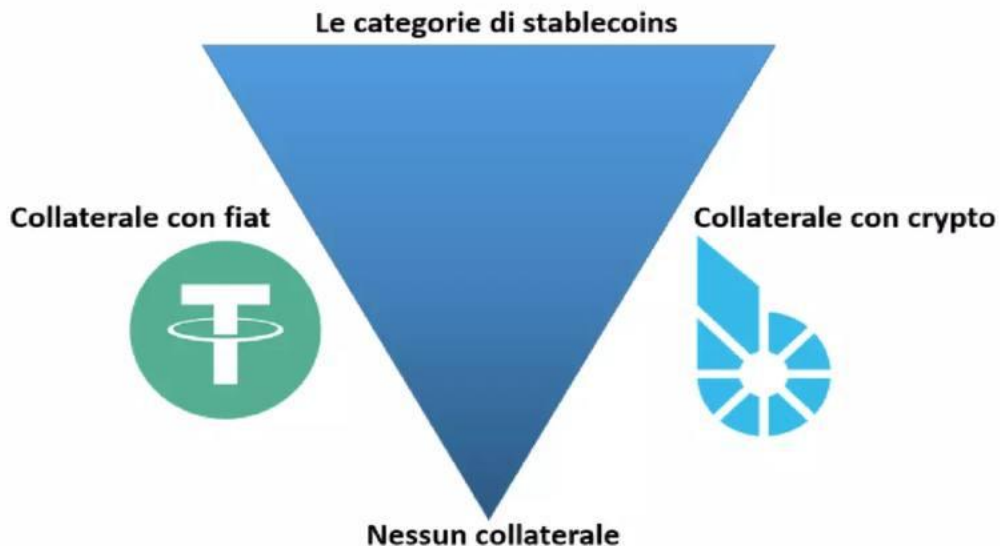


Asset Token sono valori digitali correlati e garantiti da beni off chain e che incorporano un diritto ad essere convertiti in quel determinato bene sottostante

Stablecoin

A completamento dell'excursus sui cripto-asset, occorre indicare le stable-coin.

Queste sono token gestiti da smart-contract o token nativi di pagamento (criptovalute) che sono collateralizzate, con un rapporto di conversione fisso, con valute a corso legale o con altre valute virtuali, oppure controllati da algoritmi che ne stabilizzano il prezzo rispetto ad un paniere di riferimento.



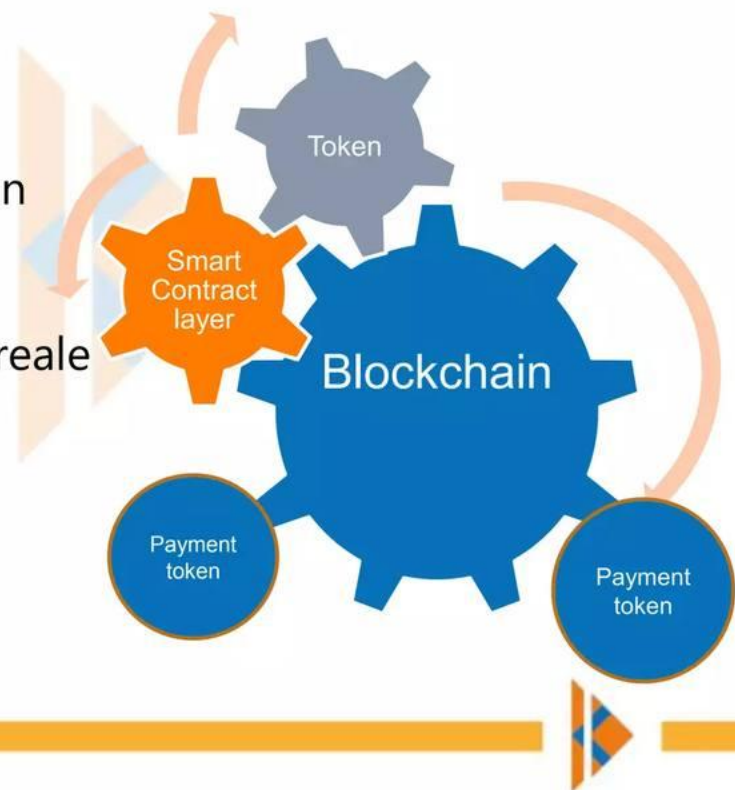


2. AML vs. cripto-asset

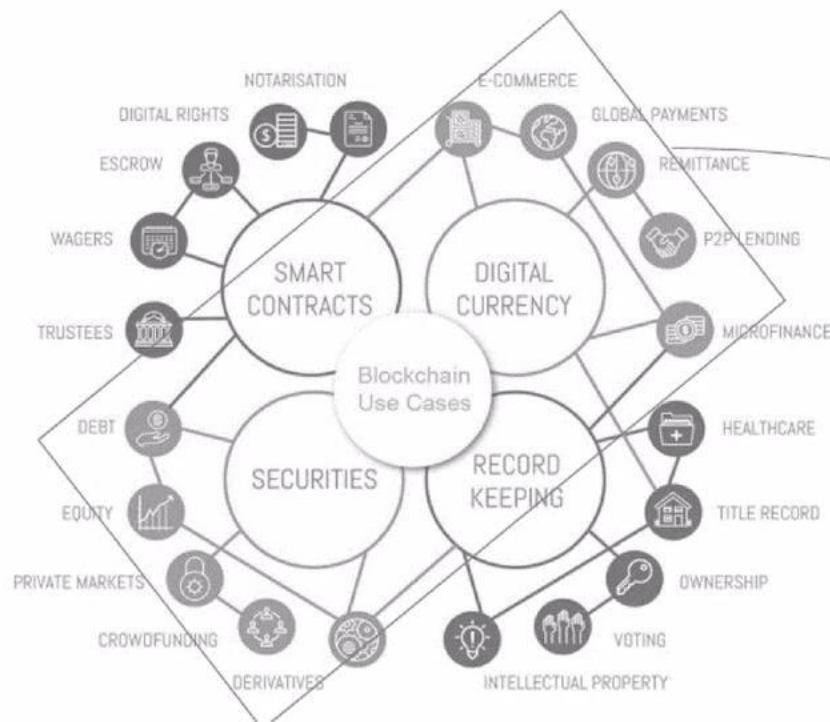


Impatto immediato con il settore finanziario

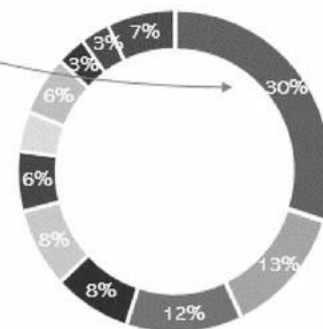
- Le criptovalute sono la prima forma di impiego della Blockchain
- Le criptovalute sin dal loro primo sviluppo sono state un sistema alternativo di pagamento
- La prima intersezione della Blockchain con l'economia reale si ha nel settore finanziario e bancario
- Con l'avvento degli smart contract e la tokenizzazione aumenta la trasversalità delle forme di impiego della Blockchain rispetto a svariate *sub-industries* del settore bancario e finanziario.



Overview



BC Use Cases



- Banking & Finance
- Insurance
- Media & Entertainment-Game
- Professional Services
- Gov. & Public Goods
- Healthcare
- Technology Services
- Supply Chain



Reazione dei regolatori

- Risposta trasversale degli ordinamenti attraverso l'utilizzo del *layer* normativo comune ai vari comparti di attività finanziaria costituito dalla disciplina e dagli obblighi antiriciclaggio
- **Base globale e uniforme del governo della disciplina AML**
- Primi interventi normativi positivi e definitivi della tecnologia BC e delle cripto valute
- **All'impatto globale, *disruptive* e trasversale della BC in ambito finanziario e bancario ha risposto (e corrisposto) quel settore normativo – la disciplina antiriciclaggio - comune ai diversi ordinamenti (globale) e comune a tutte le aree di attività finanziaria**
- La BC comincia ad entrare negli ordinamenti giuridici degli Stati
- Molte autorità finanziarie di controllo degli Stati cominciano tra il 2015 e il 2018 a rilasciare avvisi sui rischi di partecipazione alle vendite al pubblico di token digitali (ICOs) sottolineando la necessità di protezione degli investitori
- Sulla base della distinzione della tipologia dei token, i processi di vendita dei token di natura prettamente finanziaria vengono attratte dalle discipline nazionali sugli strumenti finanziari
- Cominciano a svilupparsi esempi di regolamentazione autonoma e ad hoc sui cripto-asset

Disclaimer

Le criptovalute sono il traguardo raggiunto dalla democratizzazione finanziaria, caratterizzata dall'assenza di intermediari e di controllo statale, che mira alla creazione di un mercato libero, la cui regolamentazione sia lasciata ai singoli utenti partecipanti del sistema. Da ciò la ragione per cui i fautori della moneta virtuale hanno fortemente osteggiato, sin dall'inizio l'intervento di *regulation*, in un settore la cui forza risiede esattamente nella parità di condizioni tra tutti gli individui in mancanza di un organismo *super partes* che ne controlli l'operato e nell'inesistenza di regole che rallentino l'operatività. Ma l'**assenza di supervisione regolamentare** e la facilità con cui gli attori criminali possono creare nuovi account per l'esecuzione di attività manipolatoria hanno reso i mercati delle criptovalute particolarmente vulnerabili all'infiltrazione criminale.

Molti di questi rischi si materializzano **non** sulla Blockchain in sé stessa, **ma nell'ecosistema circostante**.

La Blockchain non è criminale, ma possono essere criminali talune attività esercitate con il suo utilizzo. E i fenomeni criminosi **possono riguardare** gli enti emittenti, i portafogli virtuali ed altre **attività che supportano l'accesso dei consumatori/utenti** alla DLT. E' interesse degli Stati proteggere gli utenti, ma è soprattutto interesse degli operatori e degli utilizzatori mantenere pulito e legale l'impiego delle criptovalute.

Vulnerabilità al riciclaggio

Il potenziale che le criptovalute hanno di **favorire il riciclaggio di proventi illeciti** a livello globale e di **finanziare con immediatezza gruppi terroristici** nasce dalle loro caratteristiche intrinseche (i.e. l'anonimato, liquidità o facile convertibilità, e la natura senza confini) e dall'**operatività in mercati non sorvegliati**.

Ciò, unitamente ad alcune caratteristiche intrinseche, aumenta il potenziale di vulnerabilità delle valute virtuali.

Le caratteristiche che - dal punto di vista dei legislatori – facilitano il riciclaggio sono:

- anonimato delle transazioni grazie al quale, ad ogni titolare di un account è garantita totale riservatezza circa la sua identità, tanto con riferimento alla privacy relativa alla propria persona, quanto a quella inerente l'oggetto delle proprie transazioni;
- facilità e assenza di costi per l'apertura di una molteplicità di account;
- facilità di conversione (estrema liquidità);
- basso rischio nella trasferibilità
- istantaneità delle transazioni.



Le criptovalute **sono a metà strada tra il contante e la moneta elettronica**

presentando i vantaggi di entrambi (moneta fisica: anonimato, convertibilità/liquidità, basso rischio di trasferimento; moneta elettronica: rapidità e minori costi di transazione)

The background of the slide features a close-up, low-angle shot of two brown leather boxing gloves resting on a dark, reflective surface, likely a boxing ring. The gloves are positioned symmetrically, with their fingers curled. A bright light source from above creates a strong highlight on the top of each glove and a shimmering reflection on the surface below. The overall atmosphere is dramatic and focused. On the left side, there is a large red curved shape that serves as a design element, containing a dashed purple line and a solid purple circle.

Il vero punto dolente delle valute virtuali è rappresentato dall'anonimato/pseudo-anonimato delle transazioni e dalla globalità del loro utilizzo.

Il contrasto al riciclaggio di denaro si fonda sulla identificabilità ed identificazione delle persone. Tanto che la stessa disciplina giuridica è conosciuta con l'acronimo KYC, conosci il tuo cliente....



3. Eventi fraudolenti

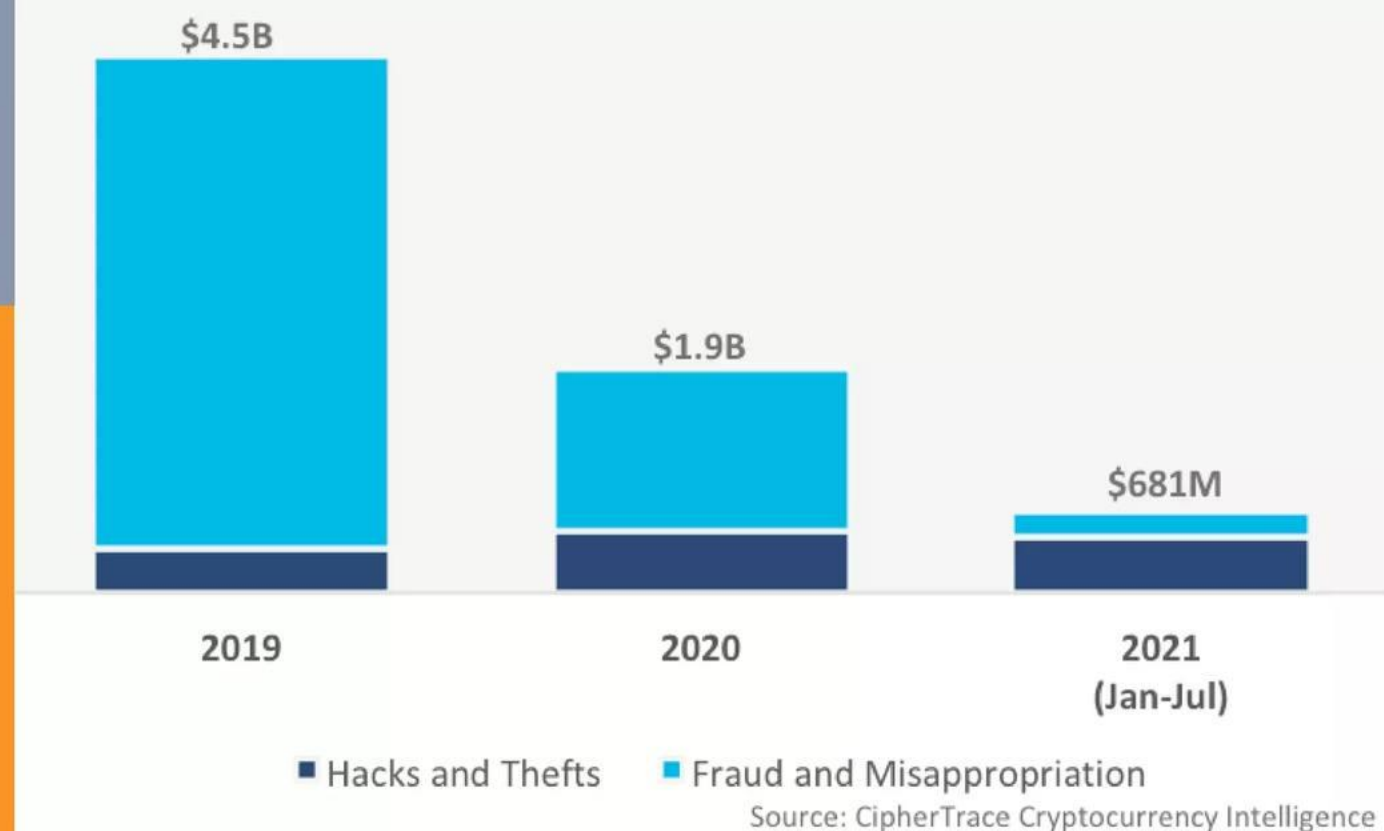


Attività criminale compiuta frodi, hacking e appropriazioni indebite

Alla fine di luglio 2021, i principali furti, hack e frodi di criptovalute hanno totalizzato \$ 681 milioni.

Tale dimensione registra una tendenza che continua a diminuire rispetto massimi degli anni precedenti.

Ad una ripartizione dei tipi di furti e frodi conferma però una tendenza osservata all'inizio dello scorso trimestre: i criminali legati alla De Fi continuano a crescere.



Attacco a Colonial Pipeline

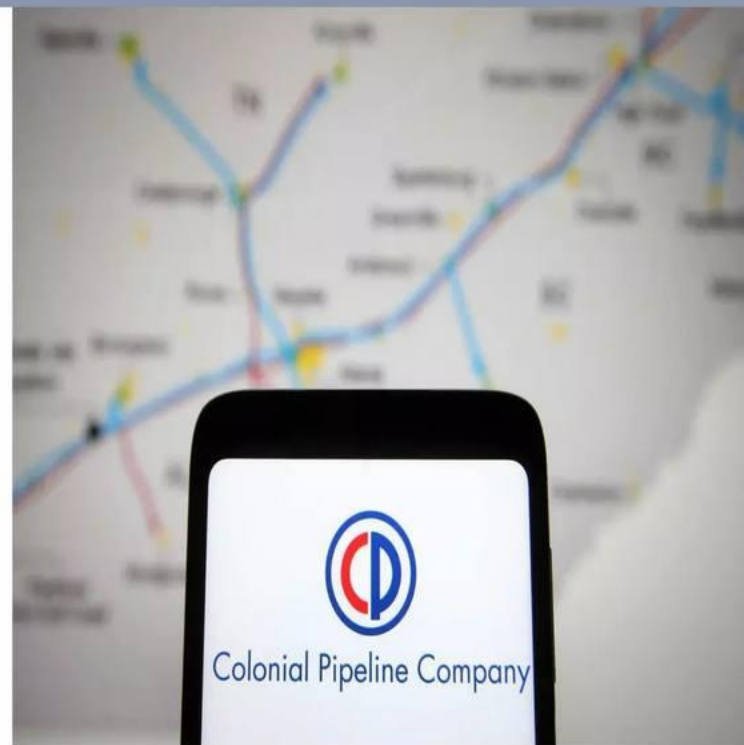
Il 7 maggio 2021, il gruppo di criminali informatici con sede in Russia, DarkSide ha attaccato la Colonial Pipeline, che gestisce la maggior parte delle infrastrutture critiche degli Stati Uniti di gasdotti ed oleodotti.

Come parte dell'attacco, gli attori di DarkSide hanno crittografato i dispositivi sulla rete e rubato file non crittografati, minacciando di rilasciarli al pubblico se l'azienda non avesse pagato un riscatto in Bitcoin.

Secondo l'analisi blockchain, il giorno successivo Colonial Pipeline ha pagato il riscatto di 75 BTC, per un valore di oltre 4,2 milioni di dollari all'epoca.

La Cyber Crimes Squad della San Francisco Field Division dell'FBI ha utilizzato l'analisi blockchain per determinare il flusso di fondi per il pagamento del riscatto della Colonial Pipeline. In questo mandato, l'FBI ha anche annunciato di essere in possesso della chiave privata per l'indirizzo di criptovaluta collegato a 63,7 BTCA seguito dell'attacco.

La Casa Bianca ha emesso un ordine esecutivo per migliorare la sicurezza informatica degli Stati Uniti contro "campagne informatiche malevole persistenti e sempre più sofisticate che minacciano il settore pubblico, il settore privato e, in definitiva, la sicurezza e la privacy del popolo americano".



Campagne di crowdfunding di gruppi terroristici

Il 1° luglio, l'Ufficio nazionale israeliano per il finanziamento del terrorismo (NBCTF) ha emesso un ordine di sequestro che elenca diversi indirizzi di criptovalute su diverse blockchain associate a campagne di donazioni condotte dall'organizzazione terroristica designata Hamas.

Oltre a bitcoin ed Ethereum, l'ordine di sequestro dimostra che Hamas ha raccolto anche donazioni in Tether, TRON, Cardano, XRP e DOGE, indicando i loro tentativi di uscire dalla dipendenza da bitcoin dopo che il Dipartimento di Giustizia degli Stati Uniti ha annunciato il sequestro di \$ 2 milioni in criptovaluta da importanti gruppi terroristici, tra cui al-Qaeda, ISIS e Hamas nell'agosto 2020 (come riportato nel nostro Rapporto sui crimini di criptovaluta di fine anno 2020 e il riciclaggio di denaro).

THE HAMAS BITCOIN FUNDRAISING CAMPAIGN

\$108,000

total donations

\$73,000

since 10th May



ELLIPTIC

FEB 2021

MAR 2021

APR 2021

MAY 2021

\$73,300



4. Interventi AML internazionali

Gli USA sono stati i primi ad essere, prematuramente aggressivi nei confronti delle crypto valute, applicando, sin dal 2013, le normative antiriciclaggio in molti casi giudiziari.

Una delle prime misure regolamentari adottate dagli USA è costituita dal provvedimento del Marzo del 2013 della *Financial Crimes Enforcement Network* (FinCEN) che annuncia l'applicazione delle leggi esistenti all'uso delle crypto valute (cfr. *Application of FinCEN's Regulation to Person Administering, Exchanging or Using Virtual Currencies*, March 18, 2013).

Il Dipartimento di Giustizia americano (DoJ - *Department of Justice*) ha invocato il Money Laundering Control Act del 1986 nel perseguire il CEO di Bitinstant, Charlie Shrem, dichiarato poi colpevole, e condannato a due anni di carcere, per aver agevolato e favorito la trasmissione di denaro senza licenza nel 2014.

Nel 2015, la FinCEN ha invocato il Bank Secrecy Act del 1970 nella sua prima azione esecutiva civile contro Ripple Labs, poi condannata a pagare \$ 700.000 per non aver implementato programmi AML efficaci nei due anni seguenti al provvedimento emesso da FinCEN nel 2013.

Giappone e Singapore

In Giappone, dove è avvenuta nel Febbraio del 2014 la bancarotta di MtGox, il governo è stato costretto ad attuare, sin da allora, misure di protezione per i consumatori che utilizzano valute digitali, includendovi anche delle disposizioni in tema di antiriciclaggio.

Successivamente, nel 2015, il Giappone ha emesso una proposta di riforma della legge sui servizi di pagamento e ad aprile 2017 è entrata in vigore la nuova legge sui servizi di pagamento che comprendono anche quelli relativi all'uso di valute virtuali.

Dal 2014 Singapore ha imposto agli Exchange di valuta virtuale con sede nella città-stato di verificare le identità dei clienti e segnalare transazioni sospette.

Organizzazioni internazionali

Diverse organizzazioni internazionali, tra il 2014 ed i 2015, hanno cercato di fornire un coordinamento degli standard legali e regolamenti nazionali in materia di AML pertinenti alle valute virtuali.

L'Ufficio delle Nazioni Unite contro la droga e il crimine (UNODC) ha pubblicato nel 2014 un manuale dettagliato per l'individuazione e il sequestro delle *cryptocurrencies* implicate nel riciclaggio di denaro.

L'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE), ha addestrato funzionari per indagare sul riciclaggio di denaro attraverso le valute virtuali.

Nel 2015 l'International Organization of Securities Commissions (IOSCO) ha istituito una «task force blockchain», mentre il Commonwealth ha convocato un gruppo di lavoro di dieci membri sulle valute virtuali per coordinare gli approcci AML.

Allo stesso modo, Interpol ed Europol hanno istituito un partenariato congiunto per coordinare le attività di polizia "contro l'abuso di valute virtuali per transazioni criminali e riciclaggio di denaro.

Il riciclaggio di denaro e il finanziamento del terrorismo sono fenomeni trans-nazionali, che non possono essere combattuti con successo solo su base nazionale. La reazione ai fenomeni richiede perciò uniformità di comportamenti da parte delle autorità governative nell'adozione delle misure da introdurre.

L'uniformità di approccio è garantita dal Gruppo d'Azione Finanziaria (GAFI) - Financial Action Task Force (FATF) - GAFI-FATF.

Costituito nel 1989 in occasione del vertice dei Capi di Stato e di Governo del G7 tenutosi a Parigi, il GAFI-FATF è un organismo intergovernativo con lo scopo di ideare e promuovere strategie di contrasto al riciclaggio dei capitali di origine illecita. Ospitato all'interno dell'OCSE, il GAFI-GAFI è l'organo intergovernativo il cui compito principale è **ideare e promuovere strategie per combattere il riciclaggio di denaro e prevenire il finanziamento del terrorismo**.

Il GAFI-GAFI elabora raccomandazioni riconosciute a livello internazionale per combattere le attività finanziarie illecite, analizza le tecniche e l'evoluzione di questi fenomeni, valuta e monitora i sistemi nazionali.

Il compito principale di GAFI-GAFI è aggiornare, integrare e interpretare le Quaranta raccomandazioni su ML ("R") sviluppate dal 1990 e le Nove raccomandazioni speciali (SR) su TF. Le **raccomandazioni sono considerate globalmente come lo standard mondiale** anche per la lotta contro l'ML / TF. Molti paesi si sono impegnati a metterle in atto, sebbene non abbiano effetti giuridici direttamente vincolanti (c.d. soft law).

Virtual Currencies: Key Definitions and Potential AML/CFT Risks

Assessment preliminare sui rischi derivanti dall'impiego di valute virtuali. Contiene la prima definizione ufficiale di valuta virtuale con valenza giuridica ai fini dell'AML.

Emerging Terrorist Financing Risks

In tale documento il GAFI/FATF sottolinea l'allarmante vicenda di Ali Shukri Amin- contestuale agli attentati terroristici di Parigi del gennaio del 2015 -, che aveva fornito istruzioni su Twitter per utilizzare Bitcoin per coprire la fornitura di fondi a Daesh, portata come modello straordinario dei rischi legati all'anonimato delle valute virtuali

Nota interpretativa della Raccomandazione n. 15

Aggiornamento dello standard AML n. 15 per renderlo applicabile, esplicitamente, ai fornitori di servizi di utilizzazione di Valuta Virtuale



GAFI/FATF: Guidance for
a Risk-Based Approach to
Virtual Currencies – aprile
2015



GAFI/FATF: Integrazione
glossario delle
Raccomandazioni con la
definizione di Valuta
Virtuale – ottobre 2018



GAFI/FATF: *Guidance for
a Risk-Based Approach to
Virtual Assets and Virtual
Asset Service Providers* –
giugno 2019



GAFI FATF: Nota
interpretativa della
Raccomandazione n. 15
pertinente ai provider di
servizi di valuta virtuale –
febbraio 2019



Il GAFI/FAFT estende la definizione e ricomprende i Virtual Asset

Con il progredire degli use cases Blockchain anche al di fuori delle valute virtuali, anche il GAFI/FATF si adegua. Nell'ottobre del 2018 vengono inserite, nel Glossario Generale delle Raccomandazioni la definizione di Virtual Asset (VA) e di Virtual Asset Service Provider (VASP).

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. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

Virtual asset service provider means any natural or 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; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.



Interpretazione della Raccomandazione GAFI/FATF n. 15

La [nota interpretativa del 19 febbraio del 2019](#) del GAFI/FATF che integra la Raccomandazione n. 15 per renderla applicabile, da giugno del 2019, quale standard internazionale contro i Rischi ML/FT a cui sono esposti i c.d. VASP, o *Virtual Asset Service Provider*.

I VASP sono le persone fisiche o giuridiche, come definite nel Glossario Generale delle Raccomandazioni emendato ad ottobre del 2018, che esercitano professionalmente, in nome o per conto di altre persone fisiche o giuridiche, una o più delle seguenti attività:

1. scambio tra Asset Virtuali e monete aventi corso legale;
2. scambio di una o più forme di Asset Virtuali tra loro;
3. trasferimento di Asset Virtuali;
4. custodia e/o gestione di Asset Virtuali, ovvero di strumenti che ne abilitano il controllo; o
5. partecipazione o fornitura di servizi finanziari correlati all'offerta di un emittente, ovvero alla vendita di Asset Virtuali.



I VASP devono:

- a) essere soggetti ad adeguati livelli di disciplina e monitoraggio ai fini della prevenzione, mitigazione e contrasto dei Rischi ML/FT;
- b) osservare le Raccomandazioni dalla n. 10 alla 21 **nel caso svolgano transazioni al di sopra della soglia dei 1.000 USD e qualora effettuino un trasferimento elettronico di fondi cross-border o a livello domestico**;
- c) essere soggetti a processi di autorizzazione/licenza o di registrazione in un albo specifico;
- d) essere sottoposti alla supervisione di una autorità nazionale con poteri di imporre sanzioni anche di tipo disciplinare, incluse misure di ritiro, limitazione o sospensione della licenza o della registrazione;
- e) essere soggetti, relativamente ai Rischi ML/FT, al **controllo di un'autorità nazionale** competente alla conduzione di una vigilanza basata sul rischio che sia **munita di poteri di ispezione, coercitivi e sanzionatori (di tipo operativo e pecuniario)** per obbligare alla produzione di documenti e informazioni.

L'autorità nazionale di controllo per gli obblighi AML/CFT sui VASP non può essere una c.d. *Self-Regulating Body* o SBR, nemmeno se il VASP è estraneo alla categoria dei soggetti finanziari, cioè se sia una qualsiasi entità DNFBP, o *Designated non-financial businesses and professions*, che ingaggia qualche attività concernente VA (aperta polemica con il modello della Svizzera)

L'applicazione delle disposizioni sui wire - transfer (R16) a tutti i trasferimenti di fondi concernenti VA al di sopra dei 1.000 USD (c.d. Travel Rule), sia cross-border che domestici costituisce un serio problema.

Occorre infatti che il VASP richieda, registri e conservi le informazioni attinenti all'identità dell'originator di un pagamento e del suo provider, in un sistema nel quale i pagamenti sono soprattutto P2P e gli end point non sono sempre identificabili.



Aggiornamento Travel Rule

Il 5 luglio 2021, la Financial Action Task Force (GAFI) ha completato la sua seconda revisione di 12 mesi dell'attuazione dei suoi standard rivisti sui virtual asset e fornitori dei relativi servizi. Questa revisione esamina come le giurisdizioni e il settore privato hanno implementato gli Standard rivisti dalla prima revisione.

La Travel Rule è stata la più focalizzata sulla questione in termini di conformità dei VASP agli standard GAFI rivisti. Tuttavia, solo 10 giurisdizioni hanno riferito di applicare attivamente i requisiti delle regole di viaggio per i VASP.

Altre 14 giurisdizioni hanno riferito di aver introdotto i regolamenti sulle regole di viaggio ma non sono stati ancora applicati i requisiti. Nessuna giurisdizione ha riferito di essere a conoscenza di alcun VASP che rispettasse pienamente tutti gli elementi della regola di viaggio.

Esistono varie tecnologie e strumenti disponibili che consentono ai VASP di conformarsi alla Travel Rule, tuttavia la conformità alla Travel Rule continua a essere segnalata come difficile a causa della "mancanza di una tecnologia unificata per supportarla", secondo il rapporto GAFI.

Dalla prima revisione di 12 mesi del GAFI, ci sono stati progressi significativi nello sviluppo della tecnologia delle regole di viaggio. Diversi standard e protocolli, come la Travel Rule Information Sharing Architecture (TRISA), possono ora aiutare a consentire l'interoperabilità tra le soluzioni e, se potenziati da strumenti di analisi blockchain come in CipherTrace Traveler, possono anche aiutare ad identificare l'indirizzo ospitato e i VASP per scambiare i dati necessari per la conformità alla Travel Rule.





5. Cripto asset *AML compliance* in Europa e Italia

Percorso verso la V° Direttiva AML

Il percorso verso l'adozione della Direttiva (UE) 2018/843 del 30 maggio del 2018 (V° Direttiva AML) è così composto:

- **Luglio 2014:** EBA - *Opinion on Virtual Currencies* (successiva di un mese al provvedimento del GAFI/FATF), con l'individuazione di 70 schemi di rischio derivanti dall'uso di valute virtuali e con la raccomandazione di adottare un regime AML specifico, o di estendere quello esistente alle criptovalute.
- **Maggio 2015:** Parlamento Europeo, Consiglio – Direttiva (UE) 2015/849 del 25 maggio 2015 (IV° Direttiva AML), con l'adozione del principio di c.d. RBA del GAFI/FATF ma senza alcun riferimento all'uso di criptovalute.
- **Giugno 2016:** Commissione - *Impact Assessment* di accompagnamento della proposta di riforma del testo della IV Direttiva con l'inclusione delle valute virtuali nell'ambito del perimetro della disciplina AML
- **Giugno 2017:** Commissione – *Supranational Risk Assessment* **con la raccomandazione agli Stati membri di estendere comunque la IV° Direttiva per includervi, quali nuovi soggetti obbligati gli exchange ed i wallet provider.**



Estensione dei soggetti obbligati

IV DIRETTIVA

A chi si applica

- Intermediari bancari e finanziari;
- Altri operatori finanziari;
- Professionisti;
- Altri operatori non finanziari;
- Prestatori di servizi di gioco;

V DIRETTIVA

Amplia la platea degli obbligati includendovi:

- **prestatori di servizi di cambio tra valute virtuali e valute legali** (che il D.Lgs. n.90/2017, per quanto riguarda il nostro ordinamento, già includeva tra i soggetti obbligati agli adempimenti in materia di antiriciclaggio (art. 3 D.Lgs. n. 231-2007);
- **prestatori di servizi di portafoglio digitale** (i c.d. Wallet).
- **agenti immobiliari** anche quando agiscono in qualità di intermediari nella locazione di un bene immobile, ma solo in ordine alle operazioni per le quali il canone mensile è pari o superiore a 10.000€;
- **commercianti di opere d'arte**, laddove il valore dell'operazione sia pari o superiore a 10.000€
- **qualunque altra persona** (oltre i professionisti e altri soggetti già individuati come obbligati) **che presti, in via principale, assistenza o consulenza fiscale;**



L'UE adotta la Travel Rule

Il 20 luglio 2021, la Commissione Europea ha pubblicato un nuovo pacchetto di misure AML/CFT incentrate sulle cryptocurrencies:

- Regolamento istitutivo della nuova Autorità AML/CFT dell'UE (ABE)
- Un nuovo regolamento AML/CFT con ulteriori norme in materia di ADV della clientela
- Una proposta per l'aggiornamento della 5° Direttiva antiriciclaggio (AMLD6)
- La Revisione Reg 2015/247 sui trasferimenti di fondi per tracciare i trasferimenti di cripto-asset.

Il pacchetto legislativo includeva la revisione del regolamento 2015 sui trasferimenti di fondi per tracciare i trasferimenti di criptovalute (regolamento 2015/847/UE), ed essendo, lo strumento normativo prescelto un regolamento, esso sarà immediatamente applicabile in tutti gli Stati senza necessità di attuazione interna

In base alla proposta, tutti i trasferimenti di criptovalute superiori a 1000 EUR sono trattati come bonifici transfrontalieri e soggetti ai regolamenti sulla Travel Rule.

I provider dei servizi del disponente dovrebbero garantire che i trasferimenti siano accompagnati da:

- il nome dell'autore,
- il numero di conto del cedente, se tale conto esiste e viene utilizzato per elaborare la transazione,
- l'indirizzo dell'originatore, il numero del documento personale ufficiale, il numero di identificazione del cliente o la data e il luogo di nascita.
- nome del beneficiario
- il numero di conto del beneficiario, se tale conto esiste e viene utilizzato per elaborare la transazione

Regolamento Mi.Ca.

Il 24 settembre 2020, la Commissione europea (CE) ha adottato un nuovo pacchetto di **finanza digitale** che si ripropone di trasformare l'economia europea nei prossimi decenni. Tale pacchetto - volto a migliorare la competitività del settore **Fintech** del continente mitigando il rischio e garantendo la stabilità finanziaria - include anche una proposta legislativa sulle criptovalute e crypto asset, denominata [Markets in Crypto-assets \(MiCA\)](#) ed ideata per sviluppare la tecnologia Blockchain e la regolamentazione degli asset virtuali nell'Unione europea (UE).

Il Mi.Ca si concentra fortemente sulla regolamentazione dei crypto-asset che attualmente si trovano al di fuori del diritto europeo (i c.d. *unregulated tokens*) come le **stablecoin**, le **criptovalute** e i **fornitori di servizi di criptovaluta** -, indicati come **CASP** (un termine usato anche nei quadri normativi di altri paesi, come il Giappone e il Sud Africa, mentre, con riferimento al GAFI/FATF, i fornitori di servizi di criptovaluta vengono definiti come **VASP**, o **Virtual Asset Service Providers**).

Anticipazione sul Regolamento Mi.Ca. (2)

La proposta del regolamento Mi. CA mira ad *"armonizzare il quadro europeo per l'emissione e il commercio di vari tipi di token crittografici come parte della strategia di finanza digitale europea"*, e si pone come quadro normativo completo atto a regolamentare le criptovalute e i loro fornitori di servizi nell'UE e a delineare un **unico regime di licenza in tutti gli stati membri presumibilmente entro il 2024**.

Il Mi.CA propone un quadro giuridico per attività, mercati e fornitori di servizi che attualmente non sono regolamentati a livello dell'UE e **consentirà la fornitura dei servizi di criptovaluta attraverso una licenza valida in tutto il territorio dell'UE**. In quanto regolamento, il Mi.CA sarà applicabile in tutta l'Unione Europea (UE) e, direttamente, a tutti gli Stati membri senza attuazione nel diritto nazionale.

Glossario- Fonti italiane

Decreto AML: è il D.lgs. 21 novembre 2007 n. 231 «Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione».

Decreto di Riforma: è il D.lgs. 25 maggio 2017, n. 90 di «Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006».

2° Decreto di Riforma: è il D.lgs. 4 ottobre 2019, n. 125, recante «Modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva (UE) 2015/849, nonché attuazione della direttiva (UE) 2018/843 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE».

Sintesi normativa

SIMPLE CONCEPTS

Con il Decreto di Riforma, entrato in vigore il **4 luglio 2017**, il legislatore ha anticipato, **relativamente all'utilizzo di Valuta Virtuale**, parte dei contenuti della V° Direttiva AML (poi entrata in vigore a maggio del 2018 e attuata ora con il 2° Decreto di Riforma)

Tra le novità più rilevanti, il Decreto di Riforma ha introdotto essenzialmente tre aspetti:

- la definizione di Valute Virtuali;
- La definizione della categoria dei prestatori di servizi relativi all'utilizzo di Valuta Virtuale;
- l'applicazione della disciplina dei "cambiavalute" a questi ultimi.



Prestatore di servizi di cripto asset

Il Prestatore di Servizi di Utilizzo di Valuta Virtuale è ora definito normativamente 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"*** (art. 1, comma 2, lettera fa., Decreto AML).



Wallet Provider

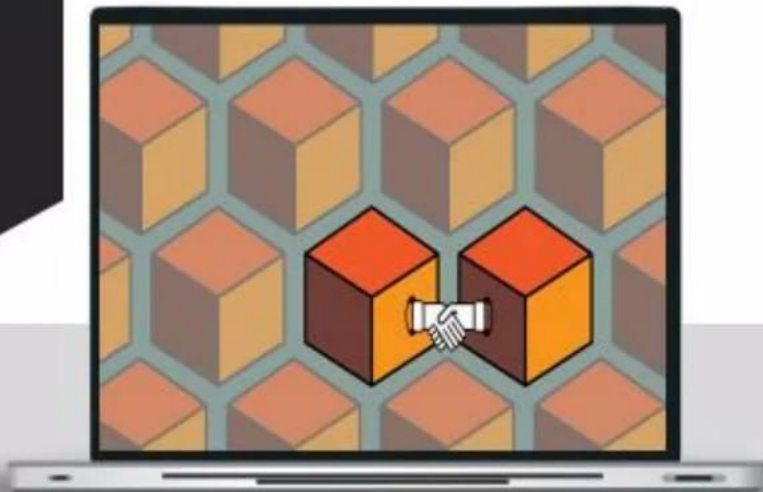
Con l'attuazione delle V° Direttiva, attraverso il 2° Decreto di Riforma, sono stati inseriti tra i soggetti obbligati all'osservanza del Decreto AML, anche i Prestatori di Servizi di Portafoglio Digitale.

Questi sono ora 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*** (art. 1, comma 2, lettera ff-bis Decreto AML).



Quando sono obbligatori gli adempimenti AML

~~Se c'è
conversione~~



Il Prestatore di Servizi di Utilizzo di Valuta Virtuale - ~~«limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso»~~ (nuovo art. 3, comma 5, lett. i), Decreto AML) – rientra tra i soggetti obbligati all'osservanza di obblighi specifici in tema di antiriciclaggio.

Per effetto del 2° Decreto di Riforma, il predetto inciso è stato soppresso e sono stati inclusi, tra i soggetti obbligati anche i Prestatori di Servizi di Portafoglio Digitale.

Adempimenti AML



Art. 35 Decreto AML

Segnalazione

Segnalare a UIF le operazioni in caso di sospetto o di sussistenza di motivi ragionevoli per sospettare il compimento di operazioni di riciclaggio

Art. 16 Decreto AML

Mitigare il rischio

Adottare presidi e attuare controlli e procedure interne necessari a mitigare e gestire i rischi

Art. 15 Decreto AML

Analisi e autovalutazione del rischio

Elaborare un documento di valutazione sulla base dell'analisi nazionale e dei fattori associati alla clientela, all'area geografica, ai canali distributivi e servizi offerti

Art. 17 Decreto AML

Adeguate verifica della clientela

Identificare il cliente e verificarne l'identità sulla base di documenti dati o informazioni, ottenere informazioni sullo scopo e sulla natura del rapporto, svolgere un controllo costante

Art. 42 Decreto AML

Astensione

Non instaurare il rapporto continuativo, né eseguire operazioni o prestazioni professionali, ponendo fine al rapporto continuativo in caso di impossibilità di esecuzione dell'adeguata verifica

Art. 16, 3 Decreto AML

Formazione

Garantire lo svolgimento di programmi permanenti di formazione, finalizzati alla corretta applicazione delle disposizioni e il riconoscimento di operazioni sospette

Art. 31 Decreto AML

Conservazione

Conservare le informazioni, indicando (i) la data del rapporto; (ii) i dati identificativi del cliente, e le informazioni sullo scopo e la natura del rapporto; (iii) la data, l'importo e la causale dell'operazione; (iv) i mezzi di pagamento,

Art. 46 Decreto AML

Comunicazioni oggettive

Comunicare a UIF a cadenze regolari operazioni a rischio riciclaggio

A PRESTO!

Giulia Arangüena

Blockchain e Fintech Partner **GIM Legal STA S.r.l.**, Comitato Scientifico Blockchain Roundtable di **San Marino Innovation S.p.A.**, Research Fellow **Digital Euro Association**, Membro Comitato Tecnico Scientifico **Think Europe Institute**, Membro Consiglio Direttivo **Italia 4 Blockchain** Responsabile Funzione Anti riciclaggio e Compliance **Mistral Pay Ltd**, Docente in E finance per Internet and Ecosystem Master **Università di Pisa**, Scholarship in Blockchain and local financial instrument **Università di Torino**, Lecturer in Diritto dell'Informatica Giuridica di Università di Pisa e in Diritto Bancario di **Università Roma 3**.