Insights

protiviti®
Global Business Consulting

Regulatory Compliance

Maggio 2024

a cura di:

Francesco Monini
Managing Director

Mattia Santi
Manager

Crypto e Travel Rule: cosa sta succedendo?

I crypto-asset, insieme ai relativi prodotti e servizi, hanno registrato una crescita evidente negli ultimi anni.

Questa rapida adozione solleva interrogativi sul futuro dei mercati finanziari e sull'interconnessione tra i crypto-asset e i sistemi finanziari tradizionali.

I rischi associati ai crypto-asset sono molteplici e diversificati, comprendendo rischi operativi e finanziari, oltre a quelli legati alla gestione delle riserve di asset e al possibile impatto della "cryptoization", ovvero la sostituzione delle valute nazionali con crypto-asset.

L'adozione dei crypto-asset pone anche significative sfide per i regolatori globali, che devono affrontare la complessità di un settore in continua evoluzione, sia dal punto di vista tecnologico che regolamentare, spesso caratterizzato da una deregolamentazione o da una regolamentazione ancora in fase iniziale.

L'identificazione e la gestione di tali rischi costituiscono un'attività estremamente complessa e sensibile al fattore tempo.

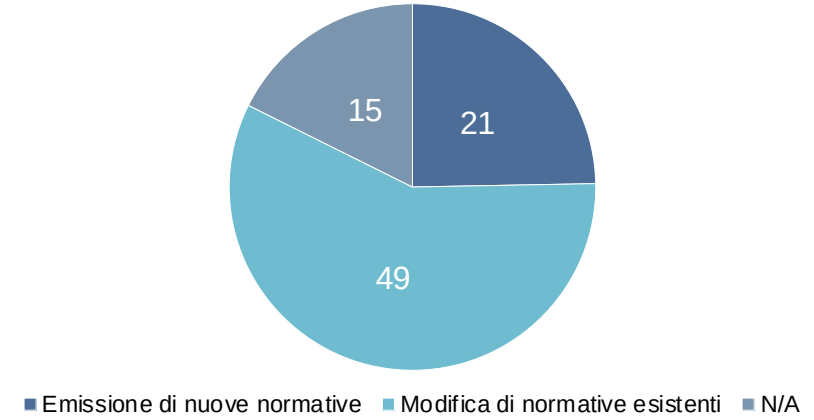
Le principali sfide regolamentari

Questa crescita straordinaria dei crypto-asset negli ultimi anni ha portato con sé sfide significative nel campo della regolamentazione.

Nell'ottobre 2022, il Financial Stability Board (FSB) ha pubblicato il resoconto di un sondaggio in cui sono stati coinvolti 24 soggetti membri del FSB, tra cui 23 autorità nazionali e la Commissione Europea, insieme a 24 giurisdizioni non membri rappresentate nei Gruppi Consultivi Regionali (GCR) del FSB[1].

15 membri del FSB e 10 giurisdizioni GRC hanno dichiarato che stanno attuando o pianificando di rafforzare la regolamentazione nel settore crypto. Delle 70 normative emesse, 49 consistono nella modifica di regolamentazioni esistenti, mentre solo 21 sono rappresentate da nuove normative ad hoc.

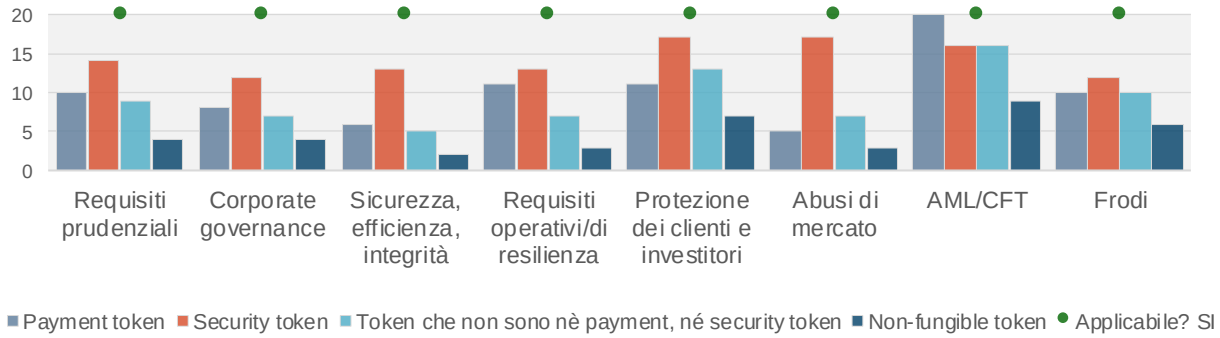
Le normative emesse dai membri FSB e dalle giurisdizioni GRC *(Fonte: FSB)*



Allo stesso modo, circa un terzo dei partecipanti al sondaggio ha introdotto una definizione di "crypto-asset" e 13 giurisdizioni hanno introdotto una definizione per i "security token" e per i "payment token".

Per quanto riguarda i principali ambiti normativi a cui i crypto-asset sono soggetti, il framework AML/CFT risulta essere quello maggiormente coperto, seguito da quello relativo alla trasparenza e tutela dei possessori di crypto-asset.

Le normative applicabili alle differenti tipologie di crypto-asset *(Fonte: FSB)*



Emergono chiarezza e coerenza come temi centrali. In questo senso, sempre il FSB nel luglio 2023 ha finalizzato il suo framework regolamentare per le attività legate ai crypto-asset che include raccomandazioni di alto livello per la regolamentazione e supervisione delle stablecoin e dei crypto-asset più in generale.

[1] *FSB, Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets, 2022.*

All'interno di tale documento il FSB ha inoltre codificato il principio della "stessa attività, stesso rischio, stessa regolamentazione" che l'organismo applicherà per la definizione di ulteriori standard in materia[2].

In questo contesto, l'Unione Europea si distingue per la recente emanazione del nuovo regolamento sul trasferimento di fondi (TFR)[3] e di MiCAR[4], che rappresentano i primi framework regolamentari cross-border armonizzati nel mondo dei crypto-asset.

Questi passi significativi non solo riflettono la volontà di affrontare le sfide, ma anche di creare un ambiente regolatorio favorevole, supportando l'innovazione e la sicurezza nell'ecosistema crypto. In sintesi: il panorama normativo sta evolvendo, aprendo nuove opportunità per il settore e offrendo un quadro più chiaro e affidabile per gli operatori.

Le origini del framework AML/CFT Crypto

In ambito Anti-Financial Crime, il principale obbligo in capo ai Virtual Asset Service Provider (VASP) consiste nell'implementazione della Travel Rule.

Per meglio comprendere come si configuri il tema al giorno d'oggi è utile provare a fare un salto indietro nel passato, precisamente al 1990, anno in cui il Financial Action Task Force (FATF), pubblicò per la prima volta le 40 Raccomandazioni per contrastare il riciclaggio di denaro e il finanziamento del terrorismo. Le raccomandazioni furono riviste per la prima volta nel 1996 e vennero successivamente avvallate da 130 Paesi divenendo uno standard internazionale. Fra queste, la Raccomandazione 16 proponeva standard globali per i trasferimenti di fondi, noti anche come Travel Rule (d'ora in avanti anche TR), che richiedevano alle istituzioni finanziarie di identificare sia l'ordinante che il beneficiario di ciascun trasferimento, nonché di accompagnare i trasferimenti con dati necessari alla loro identificazione.

Successivamente, nel 2006 e poi nel 2015, l'Unione Europea ha emanato le previgenti versioni del regolamento sul trasferimento di fondi[5], ossia la versione europea dei Travel Rule, concepiti per armonizzare l'approccio europeo e allineare la legislazione con la Raccomandazione 16. Nel 2019 e nel 2021, il FATF ha ampliato l'ambito di applicazione della Raccomandazione 16 estendendo la definizione di istituzione finanziaria per includere i VASP, anche tramite l'emanazione di una specifica Guidance[6].

Questo aggiornamento ha spinto l'Unione Europea ad emanare un nuovo regolamento sui trasferimenti di fondi a maggio 2023, impegnando tutti gli operatori crypto europei (Crypto Asset Service Provider – CASP, secondo la definizione del TFR e di MiCAR) a conformarsi ai requisiti della Travel Rule entro la fine del 2024.

Con il nuovo TFR è stato inoltre dato mandato all'European Banking Authority (EBA) di emanare specifiche linee guida a supporto dei CASP nell'implementazione di questi nuovi standard, soprattutto in situazioni in cui manchino o siano incomplete le informazioni sull'ordinante o sul beneficiario; ad esempio, in caso di operatività con la finanza decentralizzata (DeFi), ossia gli indirizzi auto-ospitati su blockchain. Nel novembre 2023, l'EBA ha emanato le prime consultazioni sulle Linee Guida della Travel Rule[7], evidenziando l'impegno europeo per un'implementazione efficace e armonizzata della nuova regolamentazione.

La Travel Rule

La Travel Rule delineata dal FATF pone l'attenzione sulla raccolta di informazioni cruciali quali il nome e l'indirizzo fisico (o un altro identificatore unico, come il numero di identità nazionale o un numero di identificazione del cliente, o la data di nascita) dell'ordinante, nonché il nome del beneficiario della transazione, oltre ai numeri di conto (ossia l'indirizzo nella blockchain in un trasferimento di crypto-asset) di entrambe le parti.

---

[2] *FSB, FSB Global Regulatory Framework for Crypto-Asset Activities - Umbrella public note to accompany final framework, 2023.*
[3] *EU, Regolamento (UE) 2023/1113 del Parlamento Europeo e del Consiglio del 31 maggio 2023 riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività.*
[4] *EU, Regolamento (UE) 2023/1114 del Parlamento Europeo e del Consiglio del 31 maggio 2023 relativo ai mercati delle cripto-attività.*
[5] *Il riferimento è al Regolamento (CE) n. 1781/2006 del Parlamento europeo e del Consiglio, del 15 novembre 2006, riguardante i dati informativi relativi all'ordinante che accompagnano i trasferimenti di fondi e al Regolamento (UE) 2015/847 del Parlamento Europeo e del Consiglio del 20 maggio 2015 riguardante i dati informativi che accompagnano i trasferimenti di fondi.*
[6] *FATF, Updated Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers, 2021.*
[7] *EBA, EBA/CP/2023/35 – Consultation Paper – Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113 ('The Travel Rule Guidelines'), 2023.*

I requisiti della Travel Rule delineati dal FATF per i VASP dell'ordinante e del beneficiario

	VASP ordinante	VASP beneficiario
Dati ordinante	• Obbligatori, i.e. trasmissione dei dati/informazioni al VASP del beneficiario • Accurati, i.e. il VASP dell'ordinante è tenuto a verificare l'accuratezza di tali dati/informazioni all'interno dei propri processi di customer due diligence (CDD)	• Obbligatori, i.e. il VASP del beneficiario deve ottenere tali dati/informazioni dal VASP dell'ordinante • L'accuratezza dei dati non è richiesta. Il VASP del beneficiario può assumere che i dati/informazioni sono già stati verificati dal VASP dell'ordinante
Dati beneficiario	• Obbligatori, i.e. trasmissione dei dati/informazioni al VASP del beneficiario • L'accuratezza dei dati non è richiesta, tuttavia il VASP dell'ordinante è tenuto a monitorare la transazione per verificare l'assenza di sospetto di riciclaggio	• Obbligatori, i.e. il VASP del beneficiario deve ottenere tali dati/informazioni dal VASP dell'ordinante • Accurati, i.e. il VASP del beneficiario è tenuto a verificare i dati/informazioni e confermare la consistenza dei dati/informazioni ricevuti
Azioni richieste	• Raccolta dei dati/informazioni dall'ordinante e conservazione degli stessi • Screening del nominativo del beneficiario rispetto alle liste sanctions • Monitoraggio delle transazioni e, ove necessario, invio di una segnalazione di operazione sospetta (SOS)	• Raccolta dei dati/informazioni dal VASP dell'ordinante e conservazione degli stessi • Screening del nominativo dell'ordinante rispetto alle liste sanctions • Monitoraggio delle transazioni e, ove necessario, invio di una segnalazione di operazione sospetta (SOS)

Per le istituzioni bancarie e finanziarie tradizionali[8], la Travel Rule si rivela di vitale importanza quando si intrattengono rapporti con servizi legati alle crypto-attività, come la custodia o la gestione dei trasferimenti di crypto-asset tra o da altri VASP. Come accennato in precedenza, la Travel Rule si propone di armonizzare gli standard AML/CFT relativi ai crypto-asset con quelli già consolidati per le transazioni fiat.

Affrontare la Travel Rule comporta sfide che possono essere suddivise in tre categorie principali:

1. **Differenze temporali nell'implementazione ("sunrise issue"):** la variabilità nei tempi di adozione della normativa tra diverse giurisdizioni, nota come "sunrise issue", rappresenta una delle principali sfide per i regolatori. Questa discrepanza temporale può generare arbitraggi, complessità e incertezza nell'adeguamento alle regole oltre ad elevati costi di compliance in caso di operatività cross-border.
2. **Approcci ibridi tra le giurisdizioni**: un secondo ostacolo emerge dagli approcci divergenti – e non sempre coerenti fra loro – adottati dalle diverse giurisdizioni nell'implementazione della Travel Rule. Questi possono includere considerazioni sulla definizione di soglie *de minimis*, questioni relative alla tutela della privacy e gestione delle transazioni legate alla DeFi.
3. **Definizione della soluzione tecnologica**: la terza sfida è rappresentata dalla selezione di soluzioni tecnologiche adeguate, o anche da una combinazione di più soluzioni, in grado di garantire la conformità ai requisiti del FATF e delle normative locali. La scelta di un approccio tecnologico efficace è cruciale per affrontare con successo le complessità della Travel Rule.

Ciò che emerge è che in questo panorama dinamico, navigare attraverso le sfide della Travel Rule richiede non solo una comprensione profonda delle normative, ma anche una flessibilità e un'innovazione tecnologica che permettano di adattarsi ai rapidi cambiamenti del complessivo ecosistema crypto.

[8] *Si ricorda che nei confronti di tali operatori la Travel Rule non risulta essere una novità, essendo gli stessi già soggetti ai previgenti Regolamenti (CE) n. 1781/2006 e (UE) 2015/847.*

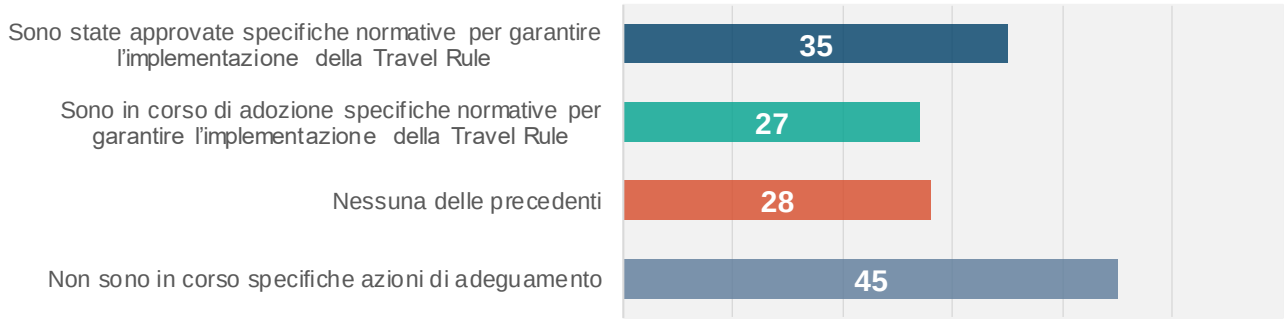
La sunrise issue

Come menzionato in precedenza, una delle sfide predominanti nell'ecosistema crypto è di natura regolamentare. Tale sfida si riflette anche nell'implementazione della Travel Rule, dove si osserva una varietà di tempistiche tra i diversi Paesi, spesso con l'implementazione di periodi transitori in alcuni casi.

Sul punto, il FATF, nel suo update annuale del 2023 relativo all'implementazione della Travel Rule[9], ha rilevato progressi limitati. Il 54% dei partecipanti (73 su 135 giurisdizioni) fino ad allora non aveva intrapreso alcuna azione per l'attuazione della Travel Rule.

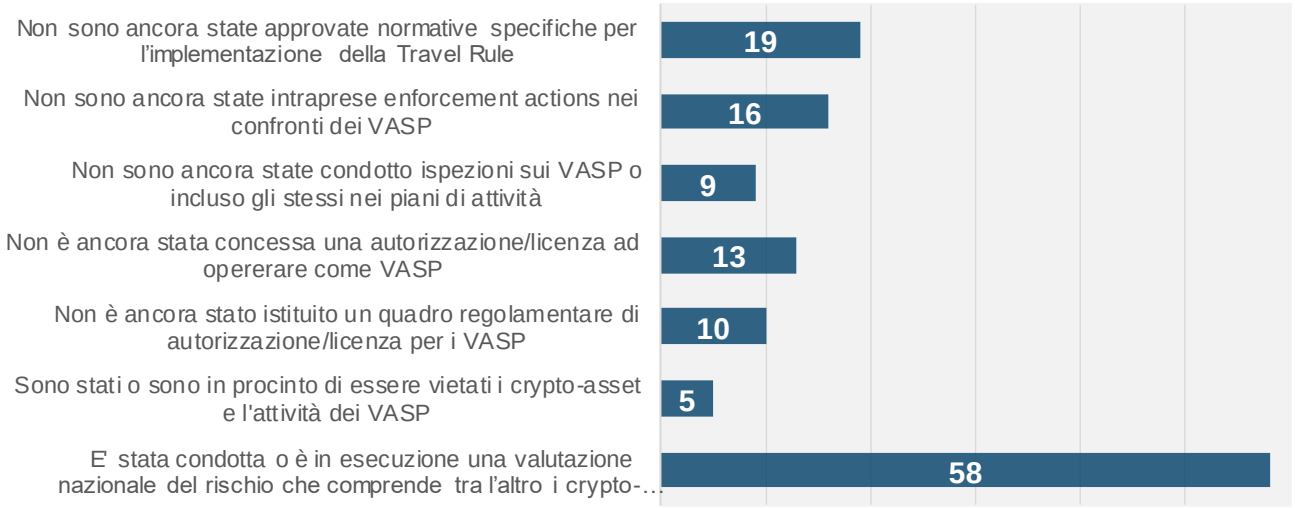
35 giurisdizioni hanno approvato specifiche normative per garantirne l'implementazione, mentre altre in altre 27 giurisdizioni sono in fase di adozione. Il FATF ha comunque evidenziato alcune evoluzioni, principalmente legate all'emanazione del TFR a livello europeo, portando il numero di giurisdizioni che hanno specifiche normative in ambito a 58. In coerenza con il report del 2022, anche nel 2023 il FATF ha evidenziato come solo il 21% delle giurisdizioni (13 su 62 rispondenti) ha indicato di aver emesso raccomandazioni o finding o intrapreso misure nei confronti dei VASP per il mancato allineamento con i requisiti della Travel Rule.

Lo stato di implementazione della Travel Rule (Fonte: FATF)



In ultimo, il 28 marzo 2024, il FATF ha diffuso un rapporto che illustra lo stato di attuazione degli standard FATF riguardanti i crypto-asset e i VASP in 58 giurisdizioni ritenute di particolare rilevanza per queste attività. Tale elenco comprende 38 Paesi membri del FATF e ulteriori 20 giurisdizioni considerate significative in base ai relativi volumi di scambio[10].

Il dettaglio del report FATF (Fonte: FATF)



[9] *FATF, Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers, 2023.*
[10] *FATF, Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity, 2024.*

Oltre alle suddette conclusioni, il rapporto fornisce una valutazione della conformità di ciascuna giurisdizione alla Raccomandazione 15, evidenziando il giudizio e l'anno di valutazione. In questo senso, le Bahamas sono l'unico Paese nell'elenco considerato pienamente conforme alla stessa sulla base di una valutazione condotta nel 2022.

L'Italia, invece, è tra le 13 giurisdizioni per cui non è ancora disponibile una valutazione di conformità rispetto alla Raccomandazione in questione. Aspetto questo che fa ipotizzare un possibile enforcement su questo tema per il nostro Paese nel prossimo futuro.

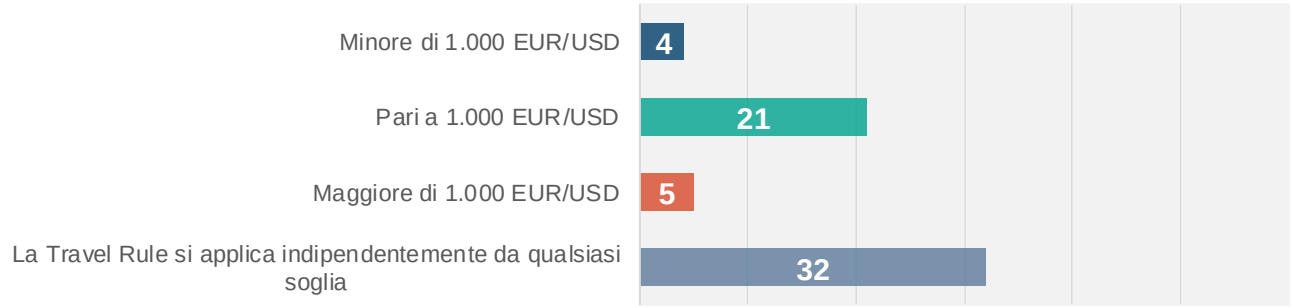
Gli approcci ibridi

Nel contesto degli approcci alla Travel Rule, una delle principali divergenze riscontrate riguarda l'applicazione di diverse soglie de minimis. È importante ricordare che le Raccomandazioni del FATF hanno fissato una soglia di USD/EUR 1.000 per l'applicazione della Travel Rule.

Sempre secondo il report del FATF di luglio 2023, delle 62 giurisdizioni che hanno dichiarato la propria posizione sulla soglia de minimis, il 32% ha affermato di aver già implementato o di avere l'intenzione di introdurre una soglia de minimis fissata a USD/EUR 1.000, il 58% di introdurre una soglia più bassa o soglia EUR 0, infine l'8% di implementare una soglia più alta rispetto a quella proposta dal FATF.

A titolo di esempio, negli Stati Uniti la soglia è fissata a USD 3.000, mentre il TFR stabilisce una soglia a livello europeo di EUR 0.

Le soglie della Travel Rule *(Fonte: FATF)*



Queste differenze nelle soglie de minimis evidenziano la diversità di approcci adottati a livello globale, con alcune giurisdizioni che seguono le raccomandazioni del FATF, mentre altre preferiscono adattare tali soglie in base alle proprie esigenze e contesti normativi. La definizione e l'implementazione di queste soglie rappresentano un aspetto cruciale nell'armonizzazione delle pratiche internazionali nell'ambito della Travel Rule.

Esplorando ulteriormente le divergenze tra la Travel Rule disciplinata dal FATF e dal TFR, sebbene le due normative siano in gran parte allineate, emergono alcune differenze chiave.

Il TFR, in primis, prevede una distinzione tra trasferimenti di crypto-asset che coinvolgono o meno la blockchain (o DLT – distributed ledger technology). Nel primo caso, risulta necessario raccogliere l'indirizzo nella DLT (ossia il codice alfa-numerico su blockchain da/verso cui i crypto-asset sono trasmessi), nel secondo caso il conto di crypto-attività detenuto dal VASP.

In particolare, il TFR prevede la trasmissione di un insieme più ampio di informazioni sull'ordinante, richiedendo l'indirizzo (compreso il nome del paese), il numero del documento di identificazione personale e il numero di identificazione del cliente. Il FATF non richiede l'inclusione di tutte queste informazioni, ma stabilisce almeno la presenza di un indirizzo fisico, un numero di identità nazionale, un numero di identificazione del cliente o la data e il luogo di nascita.

FATF e TFR a confronto

FATF		CORRELAZIONE	TFR	
Nome	● ●	Y	Nome	● ●
Numero di conto (wallet su blockchain)	● ●	Non chiara	Indirizzo su DLT OR	● ●
			Conto di crypto-attività (se il trasferimento non è avvenuto su blockchain)	● ●
Indirizzo OR	●	Y	Indirizzo (incluso il Paese)	●
Numero documento identità OR	●	Y	Numero documento identità	●
Data e luogo nascita	●	Y	Data e luogo nascita*	●
LEI**	●	Y	LEI o equivalente**	●

● Ordinante ● Beneficiario * Eventuale ** Ove disponibili

Il TFR specifica, inoltre che nel caso (raro) in cui il nome, l'indirizzo su blockchain o il numero del conto, l'indirizzo fisico e il numero del documento di identificazione non siano sufficienti per identificare l'ordinante, il VASP dovrebbe raccogliere e trasferire anche informazioni sulla data e il luogo di nascita.

Il FATF, d'altro canto, non dettaglia specifici casi d'uso per gli indirizzi geografici a differenza delle Linee Guida EBA in consultazione, le quali chiariscono se l'ordinante è[11]:

- una persona fisica, dovrebbe essere condiviso il luogo di residenza abituale;
- una persona vulnerabile, dovrebbe essere condiviso l'indirizzo finisco ricavato anche da altra documentazione disponibile;
- una persona giuridica, dovrebbe essere condiviso l'indirizzo della sede legale.

Allo stesso modo, le Linee Guida EBA in consultazione stabiliscono che in caso di trasferimenti raggruppati di crypto-asset, sia obbligatorio trasmettere le informazioni su tutti gli ordinanti, a meno che non vi siano limitazioni tecniche che impediscano la trasmissione di tali dati. Al contrario, il FATF non fornisce una guida corrispondente in merito a tale fattispecie.

Per quanto riguarda, infine, i trasferimenti da/verso DeFi, ossia indirizzi auto-ospitati, il FATF sottolinea l'importanza di ottenere e trasmettere informazioni accurate sul beneficiario, evidenziando tuttavia che le modalità specifiche per ottenere queste informazioni potrebbero variare tra le giurisdizioni.

Anche su questo punto, il TFR le Linee Guida EBA in consultazione, prevedono ulteriori accorgimenti quali:

- l'utilizzo di blockchain analytics tool, third party data provider, etc. per identificare le transazioni che coinvolgono la DeFi, real time prima di eseguire il trasferimento da parte del VASP dell'ordinante e prima di accreditare i fondi da parte del VASP del beneficiario, nonché verificare tramite tali strumenti le informazioni ricevute dall'ordinante;
- in caso di trasferimenti di crypto-asset maggiori a EUR 1.000, dovrebbe essere verificata la proprietà dell'indirizzo auto-ospitato (es. tramite l'utilizzo degli strumenti di cui sopra, la firma della transazione con la coppia di chiavi private sia nell'account che nel wallet, etc.).

Concretamente, ciò significa che se un soggetto (che ha un conto presso un VASP) desidera trasferire EUR 1.000 ad un altro soggetto (ad esempio suo fratello che possiede un indirizzo auto-ospitato), il VASP del soggetto

[11] *Le Linee Guida EBA in consultazione precisano inoltre che l'indirizzo dovrebbe essere fornito, seguendo un ordine di priorità, nel modo seguente: i) nome completo del Paese; ii) codice postale; iii) città; iv) stato; v) provincia; vi) comune; vii) nome della strada; viii) numero civico; ix) nome del palazzo. Infine è importante notare che una casella postale o un indirizzo virtuale non è considerato un tipo di indirizzo valido e non sarà conforme ai requisiti del TFR.*

trasferente è tenuto a verificare l'identità del soggetto ricevente e a dimostrare che possiede e controlla (cioè ha il potere di disporre) del suo indirizzo DeFi.

Come anticipato, le modalità tecniche per effettuare tali analisi non sono definite in modo esaustivo ed EBA fornisce solo alcune indicazioni[12]. È importante tenere presente che un metodo non esclude gli altri. Un VASP può offrire ai propri utenti uno, più di uno o tutti i metodi disponibili.

Le modalità tecniche attualmente maggiormente utilizzate

	Visual Proof	Satoshi Test	Manual signing	AOPP
OVERVIEW	• Al cliente viene chiesto di effettuare uno screenshot del proprio wallet/ indirizzo DeFi che mostra l'indirizzo di prelievo • Una volta caricato sulla piattaforma del VASP, l'indirizzo DeFi viene confrontato con quello inserito per cui il cliente ha chiesto l'approvazione • Se l'indirizzo mostrato nello screenshot corrisponde all'indirizzo di prelievo, il VASP può autorizzare il prelievo	• Il cliente esegue una transazione concordata tra l'indirizzo DeFi e il VASP prima del trasferimento desiderato • Il VASP definisce un importo minimo, un lasso di tempo e un indirizzo di destinazione • Il cliente invia l'importo all'indirizzo entro il limite di tempo specificato • Una volta verificata la transazione, il cliente dimostra di controllare l'indirizzo DeFi	• Il VASP chiede al cliente di firmare un messaggio specifico con la propria chiave privata • Una volta copiato il messaggio nel proprio wallet DeFi e firmato con la propria chiave privata, il VASP può verificare che la firma corrisponda al messaggio e alla chiave pubblica, dimostrando che il cliente controlla l'indirizzo DeFi	• L'Address Ownership Proof Protocol (AOPP) è una variante automatizzata del Manual Signing per VASP e utente
PROS	• Facile esecuzione per tutti i clienti • Supportato per tutti i wallet DeFi	• Sicurezza maggiore rispetto alla Visual Proof	• Fornisce una prova sicura del controllo tramite crittografia	• Fornisce una prova sicura del controllo tramite crittografia • Automatizzato sia lato cliente che VASP, fornendo una buona user experience
CONS	• Poco affidabile e suscettibile di contraffazione • In base a come è implementata la soluzione, verifiche time consuming e manuali da parte del VASP	• Più lento e costoso per l'utente in termini di commissioni di transazione sulla blockchain	• Non supportato da tutti i wallet DeFi • Attività più complesse da eseguire per un utente medio	• Non supportato da tutti i wallet DeFi

[12] *Sul punto, si evidenzia che EBA nelle Linee Guida in consultazione non richiede un utilizzo combinato di tali modalità, nemmeno nelle casistiche a maggior rischio.*

Le soluzioni tecnologiche

La scelta dello strumento o di soluzioni integrate per il monitoraggio delle transazioni di crypto-asset è una scelta che richiede adeguata ponderazione.

In questo senso, il FATF ha riconosciuto passi significativi compiuti nel precedente biennio riguardo alla creazione e all'adozione di soluzioni tecnologiche in quest'ambito. Tuttavia, è imperativo perseguire ulteriori miglioramenti per rendere queste soluzioni globali, interoperabili e in grado di adattarsi alle sfumature dei requisiti nazionali.

Sul punto, le soluzioni a supporto attualmente presenti sul mercato possono essere suddivise in due principali macro-categorie:

- **Blockchain analytics tool**: questa categoria comprende strumenti che analizzano e monitorano i dati della blockchain, i wallet, gli indirizzi DeFi e le relative transazioni. L'obiettivo principale è mitigare i rischi associati al riciclaggio, al finanziamento del terrorismo e alla violazione/elusione delle sanzioni internazionali.
- **Protocolli della Travel Rule**: questa categoria comprende gli strumenti e protocolli disegnati per garantire la trasmissione dei dati sull'originatore e sul beneficiario in coerenza con la Travel Rule.

L'integrazione sinergica di entrambe queste categorie di strumenti consente un approccio olistico al monitoraggio delle transazioni di crypto-asset, affrontando sia le sfide legate alla gestione dei rischi anti-financial crime che quelle specifiche della Travel Rule.

Blockchain analytics tool

La blockchain, lungi dall'essere anonima, opera su un principio di pseudonimia.

Sebbene il possessore dei crypto-asset dietro a una specifica transazione o wallet o indirizzo DeFi possa rimanere sconosciuto, ogni movimento sulla blockchain viene accuratamente registrato. Il flusso di crypto-asset, insieme ad altri dati relativi alla transazione (importo, tempo, valuta, wallet/indirizzo DeFi di invio e ricezione, etc.) e gli elementi wallet/indirizzo DeFi coinvolto (saldo attuale, entrate, uscite, etc.) su una blockchain pubblica sono tracciabili e visibili a chiunque.

Gli strumenti di analisi della blockchain capitalizzano questa vasta quantità di dati disponibili per tracciare le transazioni, clusterizzare i wallet/indirizzi DeFi (ossia associare al medesimo cluster wallet/indirizzi DeFi che appaino essere controllati dal medesimo individuo), associare i cluster alle entità del mondo reale dietro di essi, categorizzare i servizi offerti da ciascun cluster tramite l'attribuzione di uno specifico livello di rischio, identificare l'esposizione diretta e indiretta tra due o più cluster[13].

Molti strumenti sono attualmente a disposizione, da opzioni gratuite come Etherscan e Blockchain.com a soluzioni soggette a licenza come Chainalysis, TRM Labs, Elliptic, solo per citarne alcune[14].

[13] *L'esposizione diretta si riferisce ai fondi inviati da una entità all'altra senza intermediari. L'esposizione indiretta invece si riferisce al caso in cui due cluster interagiscono tramite un terzo. Un'esposizione diretta implica una forte connessione tra cluster. D'altra parte, in presenza di un'esposizione indiretta, occorre analizzare nel dettaglio come sono collegati i cluster per poter giudicare l'associazione tra di loro.*

[14] *L'efficacia di questi strumenti è stata peraltro corroborata da una Corte Distrettuale del Distretto di Columbia, negli Stati Uniti, la quale ha emesso un'ordinanza riguardante l'ammissibilità dei risultati delle investigazioni sulla blockchain attraverso tool di blockchain analytics in sede giudiziale. La decisione in oggetto, datata 29 febbraio 2024, potrebbe avere implicazioni significative per i futuri casi riguardanti transazioni crypto e crimini correlati alle valute digitali stabilendo un precedente riguardante l'ammissibilità potenziale delle prove derivanti da tali software. In particolare, la Corte si è concentrata sulla soluzione di Chainalysis, Reactor, la quale opera utilizzando tre livelli di euristica (un'euristica si riferisce a una funzione o tecnica computazionale utilizzata per risolvere problemi o prendere decisioni basate sulle informazioni disponibili). Tali tecniche vengono utilizzate per clusterizzare gli indirizzi su blockchain identificando modelli o caratteristiche nei dati che suggeriscono che siano controllati dallo stesso soggetto. La prima euristica si basa sulla caratteristica del co-spending, dove vengono utilizzati più indirizzi di input su blockchain in una singola transazione. Questa euristica assume che più indirizzi su blockchain che finanziano una singola transazione siano controllati da un unico soggetto, perché la condivisione di chiavi private tra soggetti diversi è altamente improbabile. La seconda euristica osserva e traccia comportamenti e modelli specifici unici ai singoli soggetti sulla blockchain, consentendo il raggruppamento degli indirizzi in base a questi modelli. La terza euristica utilizza informazioni off-chain ottenute da fonti come documenti giudiziari, social media, etc. e più in generale grazie alle attività di open source (OSINT) intelligence. La Corte ha anche osservato l'ampio utilizzo di Reactor dal 2016 in varie indagini, testimoniando la sua elevata affidabilità basata sull'applicazione nel mondo reale e su come le tecniche di clustering di Reactor fossero già ampiamente convalidate in sede giudiziale (il riferimento è alle subpoena indirizzate ai VASP). I teste hanno inoltre descritto un processo sistematico in cui il processo di clustering da parte di Chainalysis viene completato con i dati/informazioni forniti dai VASP a seguito delle subpoena, convalidando così l'accuratezza di Reactor. Il governo* americano – in una specifica sessione tenutasi a porte chiuse – *ha inoltre chiarito che ha svolto una approfondimenti su un elevato numero di indirizzi su blockchain clusterizzati da Chainalysis, confermando un livello di affidabilità di Reactor pari al 99,9146%. La Corte ha infine sottolineato l'ampia adozione di soluzioni di blockchain analytics, come Reactor, sia nel pubblico che nel privato, citando Chainalysis come uno standard di mercato. Per maggiori dettagli si rimanda a UNITED STATES v. STERLINGOV (2024), Criminal Action No. 21-399 (RDM), Decided: February 29, 2024.*

Protocolli della Travel Rule

Dall'introduzione della Travel Rule sono emersi diversi protocolli volti a facilitare lo scambio conforme e sicuro delle informazioni tra VASP. Tra le soluzioni commerciali più rilevanti – per citarne alcune – vi sono Sygna Protocol, VerifyVASP, TRISA, Shyft, TRUST, mentre va menzionato anche il Travel Rule Protocol (TRP), un protocollo open-source sviluppato nel 2020 da un consorzio privato che include ING, Standard Chartered e BitGO e che ha rapidamente guadagnato consensi.

Nonostante la varietà di protocolli disponibili, la principale sfida evidenziata dal FATF e dalla normativa europea è rappresentata dalla mancanza di interoperabilità tra gli essi. A differenza delle transazioni fiat che utilizzano lo SWIFT come rete dominante per lo scambio di informazioni finanziarie, per le transazioni di crypto-asset non è ancora emerso uno standard globale equivalente per lo scambio di informazioni tra VASP. La mancanza di interoperabilità tra i vari protocolli del Travel Rule costituisce un ostacolo all'adozione più ampia dei requisiti della Travel Rule, nonché ad un efficiente uso dei dati.

In questo senso, gli attuali protocolli della Travel Rule possono essere paragonati alle piattaforme social di messaggistica oggi presenti: è possibile scambiarsi messaggi, audio, media all'interno della piattaforma, ma non è possibile inviare un messaggio ad utenti che utilizzano altre piattaforme.

Per far fronte a tali limitazioni, sia il FATF, che il TFR e le Linee Guida EBA in consultazione riconoscono le attuali limitazioni di queste soluzioni, inclusa la possibilità di limitazioni tecniche che potrebbero ostacolare la trasmissione delle informazioni sull'ordinante e sul beneficiario. In tali circostanze, la normativa europea prevede un regime transitorio fino al 2025, garantendo la possibilità di utilizzare infrastrutture o servizi che potrebbero non essere completamente in grado di trasmettere tutte le informazioni richieste.

Conclusioni

L'evoluzione della legislazione non sempre riesce a tenere il ritmo dell'evoluzione del mercato, soprattutto con la rapidità dell'avanzamento tecnologico. In tale contesto la necessità di una visione globale condivisa emerge prepotentemente quando si tratta di definire framework normativi atti a regolamentare temi di portata globale come nel caso dei crypto-asset.

La Travel Rule è un esempio emblematico delle sfide poste dalla regolamentazione sui crypto-asset.

La mancanza di regolamentazione in alcuni paesi, da un lato, e l'incremento delle normative specifiche per i crypto-asset, dall'altro, generano incertezza giuridica e standard divergenti, costringendo gli operatori del settore a ulteriori sforzi di compliance per rispettare tutti i requisiti applicabili.

Allo stesso modo, nonostante le soluzioni tecnologiche attuali siano in grado di affrontare le sfide relative monitoraggio delle transazioni su blockchain, risulta essenziale un maggiore allineamento e interoperabilità per razionalizzare le stesse e superare le attuali limitazioni.

Cosa puo' fare Protiviti

In qualità di market leader nel settore finanziario sia a livello italiano sia globale, grazie all'esperienza acquisita tramite progetti con i più importanti attori del mercato finanziario e le competenze dei suoi professionisti, Protiviti ha definito un framework metodologico di governance e controlli mirato a supportare i propri clienti nella transizione digitale e integrazione verso i servizi crypto.

CONTATTI

Francesco Monini
Managing Director
francesco.monini@protiviti.it

Mattia Santi
Manager
mattia.santi@protiviti.it