

ANTIRICICLAGGIO E CRIPTOATTIVITÀ

Indicatori di rischio, adeguata verifica e criticità applicative

Simone Nepote

21 maggio 2026

Le prestazioni professionali che coinvolgono criptoattività richiedono al commercialista un livello di presidio antiriciclaggio sensibilmente più elevato rispetto a molte operazioni tradizionali.

Gli obblighi di base restano quelli ordinari (salvo la riduzione del limite per le «operazioni occasionali» relative al trasferimento di criptoattività a 1.000 euro):

- autovalutazione del rischio di studio
- adeguata verifica della clientela: identificazione del cliente, dell'esecutore e del titolare effettivo, acquisizione di informazioni su scopo e natura della prestazione
- conservazione documentale (qualora il commercialista agisca quale mandatario nell'operazione: data, importo, causale dell'operazione e mezzi di pagamento utilizzati --> l'*address* del *wallet* mittente/destinatario e l'*hash* della transazione che funge da ricevuta informatica immutabile)
- eventuale segnalazione di operazioni sospette
- astensione quando necessario

ciò che cambia è la profondità dell'istruttoria e la necessità di una documentazione molto più robusta e ragionata.

Le criticità che richiedono un innalzamento del «rischio» e conseguentemente dell'attenzione del professionista:

- **pseudonimato o anonimato:** la tecnologia *blockchain* consente di operare senza un legame diretto e immediato tra l'indirizzo pubblico (*address*) o il dispositivo fisico (*wallet*) e l'identità fisica del titolare, rendendo complessa l'identificazione del titolare effettivo ossia il «reale beneficiario»
- **velocità e transnazionalità delle operazioni:** i flussi possono essere spostati globalmente in pochi secondi, scavalcando i controlli degli intermediari finanziari tradizionali
- **gestione decentralizzata delle operazioni tramite protocolli informatici:** soprattutto nelle reti c.d. *permissionless* (es. Bitcoin), la mancanza di un ente centrale di controllo impedisce al professionista di avere un referente giuridico certo per la verifica delle transazioni

**RISCHIO DI RICICLAGGIO E DI FINANZIAMENTO DEL
TERRORISMO INTRINSECAMENTE ELEVATO**

→ RISCHIO ALTO → ADEGUATA VERIFICA RAFFORZATA

Indicatori di anomalia (Provvedimento UIF del 12 maggio 2023) Specificamente dedicati alle cryptoattività contenuti nella sezione B del Provvedimento (caratteristiche delle operazioni):

n. 26. Operatività in crypto-assets che per ammontare, intensità o modalità di esecuzione delle operazioni ovvero per l'origine o la destinazione dei flussi risulta incoerente con il profilo economico, patrimoniale o finanziario del soggetto, ... ovvero presenta una configurazione inusuale o illogica, specie quando nella movimentazione effettuata manchi la convenienza economica.

n. 27. Operatività in crypto-assets, specie se di importo rilevante, in contropartita di address per i quali, sulla base delle informazioni disponibili, non è possibile risalire con ragionevole certezza all'effettivo titolare o che risultano collegati, anche indirettamente, a contesti a rischio ovvero a paesi o aree geografiche a rischio elevato o non cooperativi o a fiscalità privilegiata ovvero con normativa antiriciclaggio carente o inadeguata in particolare con riguardo alle valute virtuali.

I punti chiave a cui rimandano gli indicatori di anomalia 26 e 27:

1. Incoerenza dell'operazione in criptoattività con il profilo del cliente:

- redditi ufficialmente modesti ma disponibilità in criptoattività molto elevate
- una storia patrimoniale non compatibile con l'entità dei *wallet* detenuti
- flussi digitali sproporzionati rispetto all'attività economica esercitata
- richieste di consulenza o di assistenza relative a operazioni complesse in ambito *crypto* senza adeguato *background* economico o finanziario

2. Operazioni di elevato valore verso *wallet* o *address* non identificabili

- il cliente non è in grado di dimostrare la disponibilità effettiva del *wallet*
- il *wallet* di destinazione o provenienza non è riferibile a soggetti identificabili
- i trasferimenti coinvolgono *address* collegati a contesti rischiosi
- la ricostruzione del flusso è tecnicamente possibile ma soggettivamente opaca

Altri indicatori rilevanti nelle operazioni *crypto* che sono contenuti nella sezione A (comportamento e caratteristiche qualificanti del soggetto):

- reticenza informativa
- strutture complesse e opache
- PEP e soggetti a rilevanza pubblica
- operazioni incoerenti, insolite o economicamente irrazionali
- operatività frequente e di grande valore con soggetti privi di collegamento apparente / prive di un rapporto economico sottostante noto
- operazioni ripetute, frazionate o di importo rilevante attraverso criptoattività per allontanare la percezione / l'attenzione dell'operazione unitaria
- passaggi continui tra conti bancari, *money transfer*, *exchange* e *wallet* che rendono difficile ricostruire il percorso economico complessivo
- operazioni nei mercati *over the counter* (fuori dei canali o mercati regolamentati ufficiali), in cui le controparti non sono pienamente identificabili e/o mancano contratti, quietanze o prove chiare del rapporto economico sottostante
- residenza del cliente, della controparte o la destinazione dei flussi verso aree geografiche a rischio
- utilizzo anomalo di soggetti interposti e ricorso a strutture societarie prive di reale sostanza economica

Le principali differenze operative che Interessano l'ADEGUATA VERIFICA RAFFORZATA:

- identificazione documentale del cliente potenziata:
 - acquisizione di almeno due documenti di riconoscimento del cliente in corso di validità
 - riscontro del rilascio di un dispositivo di firma digitale da parte di un ente certificatore
 - richiesta di una certificazione di conferma rilasciata da un ente creditizio o finanziario
- svolgimento di riscontri documentali più approfonditi per verificare l'identità del titolare effettivo
- verificare la provenienza dei fondi in modo rigoroso; assicurarsi che il primo pagamento relativo all'operazione avvenga tramite un conto intestato al cliente presso un ente creditizio che non abbia sede in Paesi terzi ad alto rischio
- intensificare la frequenza delle procedure di controllo costante
- In caso di trasferimenti da o verso un portafoglio non custodito, è necessario identificare anche il cedente/cessionario e acquisire informazioni dettagliate sulla destinazione delle cryptoattività

Alcuni suggerimenti pratici:

- ✓ formalizzare sempre l'incarico con descrizione precisa dell'oggetto
- ✓ formare adeguatamente i dipendenti e i collaboratori, presidiare correttamente eventuali deleghe ed esternalizzazioni e prevedere un passaggio finale obbligatorio di validazione del professionista
- ✓ non limitarsi alle dichiarazioni del cliente:
 - individuare chi controlla realmente i *wallet*, chi impartisce le istruzioni, chi beneficia economicamente delle operazioni e chi ha la disponibilità sostanziale delle chiavi o dei rapporti con *exchange* e piattaforme
 - acquisire elementi probatori della provenienza delle cryptoattività o dei fondi impiegati e la documentazione relativa a *wallet*, *exchange*, conti di appoggio, estratti o report
- ✓ aggiornare il fascicolo ogni volta che intervengono: nuovi *wallet*; nuove piattaforme; nuovi soggetti coinvolti; forti incrementi patrimoniali; trasferimenti esteri
- ✓ approfondire le criticità emerse e motivare per iscritto perché si è ritenuto di proseguire invece di astenersi o perché non si è ritenuto necessario inoltrare una SOS, ove il dubbio sia stato valutato ma superato
- ✓ ricorrere all'astensione quando il quadro documentale non è affidabile. Per le operazioni in cryptoattività, l'astensione costituisce uno strumento di tutela molto importante quando: il cliente non produce evidenza attendibile dell'origine degli asset; le spiegazioni sono vaghe o contraddittorie; non è possibile individuare il titolare effettivo sostanziale; l'operazione appare priva di una logica economica comprensibile; la documentazione fornita è parziale, incompleta o manipolabile



www.odcec.torino.it
www.linkedin.com/company/odcec-torino/
www.youtube.com/channel/UCBUHnLEOEHA6YY-MLr8vG8A/videos