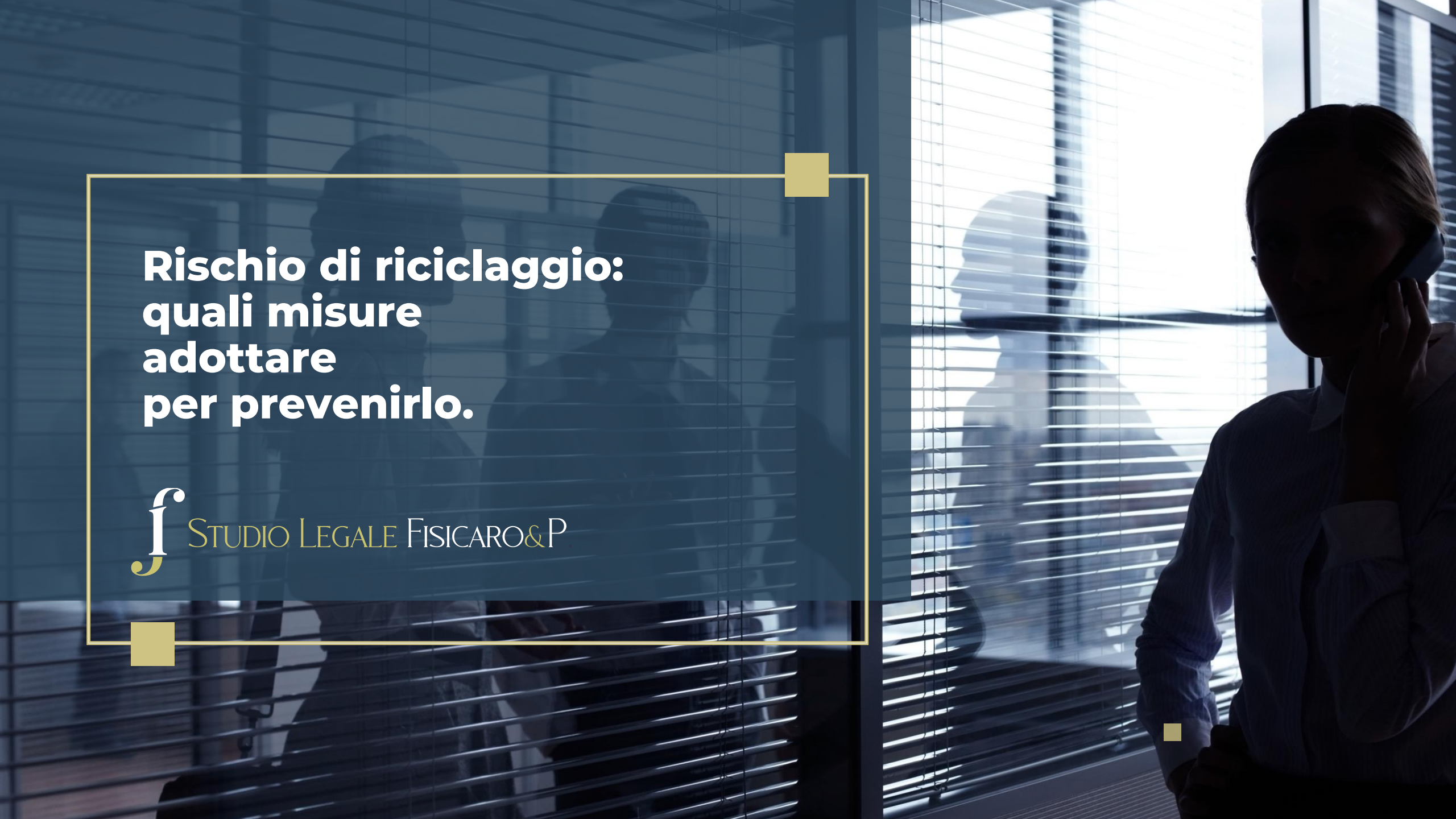
Rischio di riciclaggio: quali misure adottare per prevenirlo.



Studio Legale Fisicaro&P

CRIPTOVALUTE

Le criptovalute hanno raggiunto **una crescita esponenziale nel modo degli affari in poco più di un decennio*.** Esse sono utilizzate come mezzo di pagamento in alternativa alle monete tradizionali anche a scopo di investimento (attesa l'alta redditività che possono assicurare). La circolazione delle criptovalute avviene nel vasto mondo della rete, al di fuori di un preciso quadro normativo suscitando numerosi interrogativi, anche per i possibili impieghi fini di **evasione fiscale e di riciclaggio.**

- Nel corso della primavera del **2022**, è stata registrata una **riduzione** della capitalizzazione complessiva di mercato delle circa 8.000 criptovalute attive, che è scesa da $ 2.9. trilioni di novembre 2021 a $ 1.1. trilioni di agosto 2022 (CoinMarketCap).

- Le ragioni sono riconducibili alle particolari **congiunture economiche**, ma anche alle prime **iniziative di regolamentazione del settore**, che hanno causato la "fuga" di operatori determinati ad approfittare di un settore che, fino a poco tempo fa, registrava l'assenza dell'intervento dei legislatori europeo e nazionali.

CRIPTOVALUTE:
IL BITCOIN

Al pari di altre “criptovalute”, il bitcoin è una moneta virtuale, che si propone come strumento di pagamento alternativo alla moneta tradizionale, **in modo indipendente da qualsiasi autorità** centrale. Di esso si inizia a parlare nel 2008, con la pubblicazione, sotto lo pseudonimo di Satoshi Nakamoto, ormai celebre contributo Bitcoin: *A Peer-to Peer Electronic Cash System*, ove si osserva che il commercio via internet poggia quasi esclusivamente sulle istituzioni finanziarie, mentre un nuovo sistema pagamento elettronico potrebbe essere più adeguato a facilitare gli scambi.

VALUTE VIRTUALI E RISCHI AML/CFT

Principali caratteristiche delle valute virtuali:

- Sono create da un emittente privato (nel caso delle c.d. **valute centralizzate**) o, in via diffusa, da utenti che utilizzano software altamente sofisticati (nel caso delle c.d. **valute decentralizzate**);

- Non sono fisicamente detenute dall'utente, ma sono movimentate attraverso un conto personalizzato noto come **e-wallet** (portafoglio elettronico), che si può salvare sul proprio computer o su uno smartphone, o che può essere consultato via internet, al quale si accede grazie ad una password. Questi portafogli elettronici sono generalmente software, **sviluppati e forniti da appositi soggetti (c.d. wallet providers).** Esistono poi delle piattaforme di scambio, che offrono il servizio di conversione delle valute virtuali convertibili in moneta legale;

- Possono essere **acquistate** con moneta tradizionale su una piattaforma di scambio ovvero ricevute online direttamente da qualcuno che le possiede, per poi essere **detenute su un e-wallet**; utilizzando questo portafoglio i titolari possono effettuare acquisti presso esercizi commerciali o persone fisiche che **accettano le valute virtuali**, effettuare rimesse in favore di **altri soggetti titolari di portafogli di valute virtuali**, nonché **riconvertirle in moneta legale**;

- I titolari dei portafogli elettronici e i soggetti coinvolti nelle transazioni rimangono **anonimi;**

- Le **transazioni** tramite le quali vengono trasferite sono **tecnicamente irreversibili** (una volta fatta la transazione non è possibile chiederne l'annullamento).

L'esempio più noto di valuta virtuale è rappresentato dal **Bitcoin.**

Le transazioni in valute virtuali avvengono attraverso tecnologie sofisticate, la più diffusa è la **blockchain**. Nella blockchain ogni transazione è validata grazie ad un sistema di doppie chiavi crittografiche.

Quando la transazione viene validata dai partecipanti, essa diventa tecnicamente irreversibile.

Le valute virtuali non devono essere confuse con i tradizionali strumenti di pagamento elettronici (carte di debito, carte di credito, bonifici bancari, carte prepagate e altri strumenti di moneta elettronica, ecc.). Le valute virtuali differiscono dalle piattaforme elettroniche finalizzate esclusivamente a favorire transazioni assimilabili a forme di baratto.

TECNOLOGIA BLOCKCHAIN

In stretta sintesi, il bitcoin poggia sulla tecnologia ***blockchain***, una catena informatica raffigurabile come una sorta di libro mastro distribuito (*distributed ledger),* in continuo accrescimento e formata da anelli digitali (block), all'interno di ciascuno dei quali è **racchiuso un certo numero di operazioni**. Essa consente di **realizzare scambi mediante l'uso della crittografia**. L'accesso al sistema da parte dell'utente avviene con una **chiave privata**, con cui si interfaccia con altri utenti mediante **c.d. "chiave pubblica**", usata per confermare i trasferimenti. Quindi, i trasferimenti non vengono validati singolarmente, ma in gruppi organizzati in blocchi concatenati l'uno all'altro.

La tracciabilità delle transazioni e degli utenti

Il sistema blockchain, a differenza dei mezzi di pagamento elettronici tradizionali, rende difficile l'identificazione dei soggetti che effettuano le transazioni (pseudo-anonymity). Tuttavia, permette la completa tracciabilità (anche a ritroso) di tutte le transazioni.

Le transazioni che avvengono sulla blockchain permettono di identificare i proprietari dei wallet e le loro transazioni se e solo se gli utenti si rivolgono a una società specializzata che gestisce per conto del cliente il wallet e se detta società specializzata è regolata. Ciò non avviene se l'utente "scarica l'app" da internet (infra) e gestisce il wallet in autonomia, ovvero se compra la "valuta virtuale" direttamente da un miner o svolge esso stesso detta attività. In questo caso la tracciabilità dei soggetti sarebbe possibile solo attraverso investigazioni della polizia postale sugli indirizzi IP associati ai wallets.

I soggetti che operano attraverso piattaforme site in giurisdizioni dove dette entità non sono regolate pongono rilevanti problemi di tracciabilità. Esistono inoltre programmi che operano su internet (i cosiddetti "anonymiser", "mixer" o "tumbler") che permettono di oscurare la catena delle transazioni effettuate sulla blockchain.

Non essendo possibile ricondurre le singole transazioni ai possessori dei wallet, risulta difficile l'assolvimento degli obblighi previsti dalla normativa antiriciclaggio in materia di "titolare effettivo".

COMUNICAZIONE DELLA BANCA D'ITALIA DEL 15 GIUGNO 2022
in materia di tecnologie decentralizzate nella finanza e cripto-attività

Lo sviluppo di tecnologie decentralizzate nel campo dei servizi finanziari poggia sul ruolo centrale della **crittografia** e della **tecnologia dei registri distribuiti** (Distributed Ledger Technology – DLT/blockchain).

I due paradigmi tecnologici sono **fortemente complementari.**

Il **primo** consente di proteggere le informazioni relative alle transazioni e la loro non ripudiabilità; esso garantisce l'integrità e, se previsto, la confidenzialità delle medesime informazioni ed è alla base del meccanismo di autorizzazione delle transazioni.

Il **secondo** (DLT/blockchain) consiste in un registro elettronico condiviso i cui dati sono protetti sia tramite tecniche crittografiche sia attraverso la "ridondanza" (copie delle stesse informazioni possono essere validate e archiviate presso tutti i partecipanti attivi al registro).

La blockchain rappresenta un particolare tipo di DLT. Nello specifico, si parla di blockchain perché le transazioni memorizzate sono raggruppate in una sequenza di "blocchi" collegati tra loro per via crittografica, creando così una registrazione in ordine cronologico e non modificabile di tutte le transazioni effettuate fino a quel momento. Esistono inoltre soluzioni tecnologiche di tipo decentralizzato ma alternative alla DLT/blockchain, quali ad esempio l'online peer-to-peer (P2P), o user-matching che consente a due controparti in qualità di utilizzatori (ad esempio creditori e debitori) di interagire direttamente senza dover ricorrere alla presenza di un intermediario.

Caratteristiche delle DLT:

In linea di principio, le DLT possono recare **benefici** per gli utilizzatori, connessi con miglioramenti dell'efficienza nell'offerta di servizi finanziari, ampliamento degli orari di operatività dei sistemi, riduzione dei costi e dei tempi per le transazioni transfrontaliere, accrescimento della velocità nei trasferimenti di attività finanziarie e avanzamento della frontiera tecnologica, anche grazie a un rafforzamento della concorrenza.

Le **soluzioni DLT** realizzano ecosistemi complessi all'interno dei quali ciascuna parte – intermediari vigilati, fornitori di tecnologia, altri operatori e utenti – si pone in relazione con le altre con modalità anche molto diverse rispetto a quanto accade nel sistema finanziario tradizionale.

Il ruolo degli sviluppatori e dei fornitori delle soluzioni IT, nonché dei soggetti deputati allo sviluppo e alla gestione degli smart contracts, è centrale per assicurare il corretto funzionamento dell'ecosistema e garantire la stabilità finanziaria e la tutela della clientela.

Affinché le DLT possano effettivamente apportare benefici agli utilizzatori, esse devono avere le caratteristiche delle tecnologie più mature, ovvero essere affidabili nella continuità del servizio e, in generale, resilienti agli attacchi informatici, scalabili (quindi in grado di adeguare la capacità di registrare un numero crescente di operazioni senza un deterioramento significativo dei tempi e della qualità del servizio), efficienti dal punto di vista economico e ambientale (in particolare, capaci di supportare a costi modesti e sostenibili sotto il profilo ambientale un volume elevato di operazioni), avere una governance robusta e identificabile.

Gli attori della blockchain:

- **fornitori di infrastrutture**: progettano e sviluppano blockchain, o piattaforme sulle quali avvengono le transazioni;
- **validatori:** rendono sicura una blockchain mediante la validazione delle operazioni, che avvengono secondo un determinato meccanismo di consenso;
- **fornitori di hardware**: producono gli elementi fisici in grado di far funzionare l'ecosistema crittografico (es. computer idonei per la convalida delle transazioni, dispositivi specializzati per l'archiviazione sicura dei beni);
- **fornitori di servizi finanziari**: offrono ai privati e alle altre organizzazioni servizi quali la custodia di criptovalute, scambio tra criptovalute e moneta fiat o altre criptovalute, prestiti, investimenti in criptovalute, pagamenti in cryptoassets e una serie di altre operazioni finanziarie;
- **fornitori di servizi on-chain per la gestione dei diritti di proprietà intellettuale**: sfruttano le blockchain per autenticare diritti di proprietà intellettuale e disintermediarne lo sfruttamento, consentendo direttamente ai loro titolari di impostare le regole di utilizzo e di acquisire le entrate. L'esempio più noto è quello degli NFT, che hanno avuto un boom nelle arti digitali alla fine del 2021;
- **fornitori di servizi di gioco**;
- **fornitori di altri servizi on-chain**: sfruttano la sicurezza della blockchain (in paticolare, la capacità di autenticazione) per offrire una varietà di altri servizi, dalla verifica delle credenziali alla gestione dell'identità;
- **fornitori di servizi commerciali**: fungono da intermediari tra un cliente e imprenditore per abilitare il pagamento in criptovaluta.

Ciascun sistema può essere più o meno decentralizzato. Il panorama, sotto questo profilo, è largamente variegato.

CRIPTOVALUTE TRA RISCHI E BENEFICI

I **vantaggi** derivanti dal loro utilizzo, in termini di velocità, sicurezza, tracciabilità degli scambi e inclusione finanziaria, si accompagnano a **rischi** connessi, tra l'altro, con l'assenza di una completa regolamentazione del fenomeno e con la difficoltà di associare le transazioni ai relativi disponenti e beneficiari; ne deriva la possibilità di **utilizzo distorto a fini criminali** (frodi, es. rug pull, furti ed estorsioni, attacchi di phishing, hackeraggio) e **l'esigenza** – manifestata da Autorità sovranazionali e nazionali – **di includere questi strumenti nel perimetro di applicazione della normativa di prevenzione del riciclaggio e del finanziamento del terrorismo**.

CRIPTOVALUTE
LE SFIDE*

Le principali sfide che il settore delle criptovalute deve affrontare sono legate, in particolare, alla **sfiducia** nei confronti di tale prodotto tecnologico, da un lato, e, dall'altro, al **c.d. blockchain trilemma**, cioè il raggiungimento di sicurezza, decentralizzazione e scalabilità allo stesso tempo.

Esistono diversi **fattori che minano alla base la fiducia nei confronti delle criptovalute**. Sono state individuate principalmente quattro macro categorie: **attività criminale, cattiva gestione del rischio, bassi livelli di governance e codici poco controllati**.

*Studio No. 711 "What's next for crypto?" di Claudia Biancotti, in "Questioni di Economia e Finanza (Occasional Papers)" della Banca d'Italia (settembre 2022).

Financial Action Task Force (FATF-GAFI)

Fatf report on virtual currencies – key definitions and potential AML/CTF risks (june 2014)
Il FATF, in tale rapporto, ha introdotto la prima definizione di criptovaluta, indicata come una rappresentazione digitale di valore che può essere ceduta/scambiata digitalmente e funzionare come mezzo di scambio, unità di conto e riserva di valore, senza corso legale all'interno delle giuridizioni.

Il medesimo individuava altresì le principali aree di rischio:

- **Anonimato,** che caratterizza le criptovalute rispetto ai tradizionali metodi di pagamento diversi dal contante (i sistemi di criptovaluta decentralizzati sono particolarmente vulnerabili ai rischi di anonimato);
- Assenza di un organo entrale incaricato di gestire determinati rischi o l'identificazione della clientela;
- Pluralità di infrastrutture informatiche, localizzate anche in paesi esteri;
- Pluralità di soggetti, spesso localizzati in paesi diversi, che rende molto più difficile per le autorità di regolazione e di polizia l'accesso a alle informazioni.

European Banking Authority (EBA)

EBA Opinion on 'virtual currencies' (EBA/Op/2014/08), 4 July 2014

Anche l'EBA ha sollevato preoccupazioni in merito alle caratteristiche intrinseche del sistema delle criptovalute, in particolare individuando la principale vulnerabilità nella stessa molteplicità delle criptovalute in circolazione, rispetto alle quali non è possibile sviluppare una compiuta analisi, in quanto molte di esse sfuggono al controllo e all'osservazione.

L'EBA forniva così una definizione di cripovaluta, mutuando in qualche misura quella dettata anche dal GAFI-FATF. La criptovaluta è stata definita come una rappresentazione digitale di valore, che non viene emessa da una banca centrale o altra pubblica autorità, non necessariamente collegata ad una valuta avente corso legale, ma che viene accettata come mezzo di pagamento sia da parte di persone fisiche che giuridiche, e può essere trasferita, conservata o scambiata elettronicamente. Tale definizione verrà poi ripresa dal legislatore dell'Unione europea.

UNIONE EUROPEA (UE)

- **Direttiva UE 2015/849** (c.d. quarta direttiva antiriciclaggio)

- **Direttiva UE 2018/843** (c.d. quinta direttiva antiriciclaggio)

I **principali rischi** per l'integrità del sistema finanziario ed economico comprendono quelli connessi al verificarsi di fattispecie di **riciclaggio e finanziamento del terrorismo**, oltre ai **crimini finanziari** che possono perpetrarsi per mezzo delle criptovalute.

Tali rischi sono generalmente collegati all'**anonimato** nell'uso delle criptovalute e alla loro natura di strumenti di pagamento che non tengono conto di confini nazionali.

Direttiva (UE) 2015/849
Considerando n. 9

L'**anonimato** delle valute virtuali ne consente il potenziale uso improprio per scopi criminali. 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. Per contrastare i rischi legati all'anonimato, le unità nazionali di informazione finanziaria (FIU) dovrebbero poter ottenere informazioni che consentano loro di **associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta.** Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, **un'autodichiarazione** alle autorità designate.

Direttiva (UE) 2018/843

- Assoggettamento agli adempimenti previsti dalla disciplina antiriciclaggio per i soggetti che erogano servizi di piattaforme di scambio di valute virtuali (**exchangers**) e per i prestatori di servizi di portafoglio digitale (**wallet service providers**);

- Definizioni di valuta virtuale, di exchanger e di wallet service provider.

In Italia una prima disciplina della materia è stata introdotta nel luglio 2017, in occasione della riforma del D.lgs. 231/2007, che ha incluso tra i destinatari degli obblighi antiriciclaggio i prestatori di servizi relativi all'utilizzo di valuta virtuale.

La definizione di valuta virtuale nell'ordinamento giuridico italiano

Art. 1, comma 2, lett. qq), del D.Lgs. n. 231/2007, come modificato dai D.Lgs. nn. 90/2017 e 125/2019.

La valuta virtuale è definita come *«La rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente».*

Il D.Lgs. n. 231/2007, modificato dai D.Lgs. nn. 90/2017 e 125/2019, ha recepito la definizione di valuta virtuale contenuta nella Direttiva UE 2018/843 del 30 maggio 2018, art. 1 (d).

Il **D.Lgs. 125/2019, di recepimento della c.d. quinta direttiva antiriciclaggio**:

- **amplia la definizione di valuta virtuale**, includendo anche la finalità di finanziamento, oltre che di scambio;

- inserisce nell'attività di cambiavalute i **servizi di conversione** "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" (art. 1, comma 2, lett. ff);

- include nella disciplina i prestatori di servizi di portafoglio digitale, i **c.d. wallet provider** definiti come "ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche on line, servizi di salvaguardia di chiavi crittografiche private per contro dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali" (art. 1, comma 2, lett. ff bis).

SEGNALAZIONI DI OPERAZIONI SOSPETTE

Ricevute: ripartizione per tipologia di segnalante
(valori assoluti)

TIPOLOGIA DI SEGNALANTE	2021			2022		
	1° sem.	2° sem.	Totale	1° sem.	2° sem.	Totale
Totale	**70.123**	**69.401**	**139.524**	**74.233**		**74.233**
Soggetti obbligati non finanziari	**7.336**	**8.346**	**15.682**	**9.329**		**9.329**
Professionisti	2.708	2.413	5.121	2.556		2.556
Notai e CNN	2.476	2.212	4.688	2.347		2.347
Dottori commercialisti, esperti contabili, consulenti del lavoro	136	106	242	102		102
Studi associati, interprofessionali e tra avvocati	20	21	41	23		23
Avvocati	16	17	33	13		13
Società di revisione e revisori legali	33	44	77	44		44
Altri soggetti esercenti attività professionale	27	13	40	27		27
Operatori non finanziari	1.326	1.576	2.902	1.889		1.889
Soggetti in attività di custodia e trasporto valori	829	801	1.630	987		987
Operatori in commercio o fabbricazione di oro o preziosi	310	427	737	570		570
Operatori in valuta virtuale	116	210	326	235		235
Altri operatori non finanziari	71	138	209	97		97
Prestatori di servizi di gioco	3.302	4.357	7.659	4.884		4.884

La criminalità ricicla i proventi illeciti depositando e trasferendo criptovaluta in maniera anonima.
Ciò e reso possibile anche in quanto sono possibili trasferimenti di criptovaluta senza passare per alcun tipo di intermediario, il quale ha invece l'obbligo di segnalare eventuali operazioni «sospette».

I depositi in criptovaluta possono essere facilmente e rapidamente trasferiti in tutto il mondo;

Attraverso l'uso delle criptovalute è possibile commerciare prodotti illegali con maggiore facilità, soprattutto per mezzo del c.d. dark web.

I rischi di riciclaggio

Comunicazione UIF del 30 gennaio 2015

Sin dal gennaio **2015** la UIF ha richiamato l'attenzione dei destinatari degli obblighi di segnalazione sui rischi di riciclaggio e finanziamento del terrorismo connessi con l'utilizzo delle valute virtuali.

La UIF raccomandava, in particolare, agli operatori di gioco di cui all'articolo 14, lettere d), e) ed e-bis) del decreto antiriciclaggio, e agli intermediari finanziari di prestare particolare attenzione alle operatività poste in essere attraverso valute virtuali.

Invitava gli agli intermediari finanziari, specie quando prestano servizi di pagamento, di valutare con specifica attenzione le operazioni di prelevamento e/o versamento di contante e le movimentazioni di carte di pagamento, connesse con operazioni di acquisto e/o vendita di valute virtuali, realizzate in un arco temporale circoscritto, per importi complessivi rilevanti.

CRIPTOVALUTE

La UIF (Unità di Informazione Finanziaria per l'Italia) ha individuato i profili comportamentali a rischio, tratti dall'esperienza dell'analisi delle segnalazioni di operazioni sospette ricevute dall'Unità.

UIF COMUNICAZIONE 28 MAGGIO 2019
Utilizzo anomalo delle valute virtuali in materia di tecnologie decentralizzate nella finanza e cripto-attività

Dal punto di vista <u>oggettivo</u> meritano attenzione le ipotesi di costituzione anomala della provvista impiegata in acquisti di Virtual asset e, in particolare, le figure di collettori che operano una raccolta di fondi da una pluralità di soggetti, mediante:

- ricariche, anche frazionate, di carte prepagate eseguite in contanti od online, anche da diverse zone del territorio nazionale;

- accrediti di bonifici, anche esteri;

- ripetuti versamenti di contanti, singolarmente di importo non significativo, ma complessivamente di ammontare rilevante.

Particolare attenzione va rivolta alla **possibile connessione con fenomeni criminali** caratterizzati dall'utilizzo di tecnologie informatiche quali *phishing* o *ransomware*, con truffe realizzate attraverso siti Internet o clonazione di carte di credito, ovvero al sospetto di **reimpiego di fondi** derivanti da attività commerciali non dichiarate, spesso svolte online. Rilevano, altresì, gli acquisti di Virtual asset **con fondi che potrebbero derivare da frodi**, distrazioni di fondi o schemi piramidali.
Occorre prestare attenzione ai casi in cui l'utilizzo di Virtual asset in operazioni speculative, immobiliari o societarie appaia finalizzato ad accrescerne l'opacità e, in generale, ai casi in cui l'operatività appaia illogica o incoerente rispetto al profilo del cliente o alla natura e allo scopo del rapporto.

È inoltre da considerare l'utilizzo di Virtual asset connesso con sospetti di abusivismo e con violazioni della disciplina in materia di: i) offerta al pubblico di prodotti finanziari, qualora siano promessi rendimenti periodici collegati all'operatività in Virtual asset; ii) prestazione di servizi di investimento, laddove agli investitori sia offerta la possibilità di effettuare "operazioni regolate per differenza aventi come sottostante (anche) valute virtuali".

Per il corretto apprezzamento delle situazioni è necessario **valutare attentamente le caratteristiche dei soggetti**, anche specializzati, a vario titolo coinvolti nell'operatività in Virtual asset, nonché la presenza di:

- collegamenti, diretti o indiretti, con soggetti sottoposti a procedimenti penali o a misure di prevenzione ovvero con persone politicamente esposte o con soggetti censiti nelle liste pubbliche delle persone o degli enti coinvolti nel finanziamento del terrorismo;

- soggetti con residenza, cittadinanza o sede in Paesi terzi ad alto rischio ovvero in una zona o in un territorio notoriamente considerati a rischio, in ragione anche dell'elevato grado di infiltrazione criminale;

- soggetti operanti in aree di conflitto o in Paesi che notoriamente finanziano o sostengono attività terroristiche o nei quali operano organizzazioni terroristiche, ovvero in zone limitrofe o di transito rispetto alle predette aree;

- strutture proprietarie artificiosamente complesse od opache volte a rendere difficoltosa l'individuazione del titolare effettivo;

- soci e/o esponenti apparentemente privi delle competenze tecniche che tipicamente il settore richiede.

Cass. pen., Sez. II, 07.07.2022, n. 27023

Integra il delitto di **autoriciclaggio** la condotta di chi impiega e sostituisce il denaro preveniente dalla commissione di reati di truffa **mediante l'acquisto di criptovalute** in modo da ostacolarne concretamente l'identificazione della provenienza delittuosa.

Il fatto

All’indagato veniva contestata la commissione di **truffe** di cui all’art. 640 cod. pen. in ragione delle articolate condotte di frode realizzate, che avevano indotto plurime persone offese ad effettuare versamenti in suo favore nella prospettiva - del tutto inesistente ma artificiosamente delineata - di partecipare ad aste giudiziarie o a procedure esecutive rispetto alle quali il <omissis> si presentava come preposto dall'autorità giudiziaria in qualità di legale.

L’autore del reato presupposto aveva duqnue curato il trasferimento delle somme provento dei reati di truffa attraverso disposizioni online in favore di un conto tedesco intestato alla piattaforma di scambio di bitcoin per il successivo acquisto di valuta virtuale.

La pronuncia della Corte di cassazione

L’acquisto di criptovalute, <<condotta di impiego e sostituzione in attività speculative>> con denaro preveniente dalla commissione di reati presupposto <<reato di truffa aggravata>>, costituisce un modo per ostacolare concretamente l'identificazione della provenienza delittuosa del denaro.

La Corte ha sottolineato che la condotta dell’indagato rileva sul piano penale poiché quest’ultimo provvedeva a **curare immediatamente il trasferimento di somme non appena accreditate <<attraverso disposizioni on line in favore di altro conto tedesco** intestato alla piattaforma di scambio di bitcoin, per il successivo acquisto di valuta virtuale il cui impiego finale risulta ancora imprecisato, **ponendo così in essere un investimento dei profitti illeciti in operazioni di natura finanziaria, idonee a ostacolare la tracciabilità e la ricostruzione della origine delittuosa del denaro>>.**

La pronuncia della Corte di cassazione

- L'indicazione normativa ex art. 648 ter. 1 cod. pen. delle attività (economiche, finanziarie, imprenditoriali e speculative) in cui il denaro, profitto del reato presupposto, può essere impiegato o trasferito, lungi dal rappresentare un elenco formale delle attività suddette appare diretta ad individuare delle macro aree, tutte accomunate dalla caratteristica dell'impiego finalizzato al conseguimento di un utile, con conseguente inquinamento del circuito economico, nel quale, vengono immessi denaro o altre utilità provenienti da delitto e delle quali il reo vuole rendere non più riconoscibile la loro provenienza delittuosa;

- possono essere ricondotte nell'ambito della dizione di "attività speculativa" molteplici attività e, in particolare, tutte quelle in cui il soggetto ricerca il raggiungimento di un utile, anche assumendosi il rischio di considerevoli perdite.

La pronuncia della Corte di cassazione

A sostegno della dorsale illecita, la Corte di legittimità richiama il **parere della BCE**: le valute virtuali possono essere utilizzate per scopi diversi dal pagamento e comprendere prodotti di riserva di valore a fini di risparmio ed investimento, aspetto recepito **nella V direttiva UE antiriciclaggio 2018/843**.

Inoltre, come sottolineato in dottrina, la configurazione del sistema di acquisto di bitcoin si presta ad agevolare condotte illecite, in quanto è possibile garantire un alto grado di anonimato (**sistema cd. permissionless**), senza previsione di alcun controllo sull'ingresso di nuovi "nodi" e sulla provenienza del denaro convertito.

Sebbene sul piano della prevenzione corre l'obbligo per i destinatari delle misure di prevenzione di inoltrare le segnalazioni di operazioni sospette, «nella fattispecie in esame tale nuovo meccanismo di controllo non abbia consentito di evitare la commissione del reato di autoriciclaggio. Difatti, accertata la reimmissione del profitto delle truffe nel circuito dell'economia legale, sono risultate, da quanto si legge nell'ordinanza, estremamente difficili le attività di ricostruzione dell'identità del soggetto al quale riferire le singole transazioni in criptovaluta, anche perché <<l'account impiegato dal (omissis) faceva riferimento a false generalità dell'intestatario del conto corrente bancario di provenienza».

Cass. pen., Sez. II, 07/07/2022, n. 27024

Poiché il reato di autoriciclaggio ha natura istantanea e si consuma nel momento in cui vengono poste in essere le condotte di impiego, sostituzione o trasformazione di beni costituenti l'oggetto materiale del delitto presupposto, esso si concretizza laddove il denaro proveniente dalla commissione delle truffe sia stato utilizzato per **l'acquisto di criptovalute** tramite l'effettuazione di una serie di bonifici, partiti da un conto corrente acceso presso una banca on line con sede nel circondario di Milano, ed indirizzati ad una banca tedesca. Tale condotta finalizzata all'occultamento della provenienza delittuosa si è realizzata, quindi, nella prospettiva accusatoria, rilevante per la determinazione della competenza, con gli atti dispositivi (bonifici) con i quali le somme di provenienza illecita sono state impiegate per comprare moneta virtuale.

Il problema dell'anonimato degli utenti è difficile, ma si possono trovare soluzioni parziali. Ad esempio, le transazioni peer-to-peer tra normali utenti di criptovalute possono essere autorizzate a rimanere anonime se sotto a certa quantità. A un livello più complesso, le autorità di regolamentazione potrebbero attingere al corpo molto ampio della ricerca sull'identità digitale e incoraggiare l'uso di tecnologie di identificazione che riducano la fuga di informazioni al minimo.
Tali tecnologie consentirebbero almeno l'anonimato delle parti interessate nei confronti chiunque tranne le autorità: non è necessario fornire informazioni personali agli scambi o altro azienda75. È possibile implementare algoritmi ancora più sofisticati ed è probabile che ne siano disponibili altri, dato il ritmo veloce della ricerca nel campo76. Questi possono essere fusi con i suggerimenti del settore, come la recente proposta di token soulbound77, o NFT non trasferibili che incorporano informazioni su un singolo individuo e potrebbe essere utilizzato nella verifica dell'identità e delle credenziali.
L'anonimato del validatore e la resistenza alla censura sono i problemi più difficili da risolvere, in particolare quando si tratta di blockchain ad alta decentralizzazione e alta automazione. Per nominare solo un'opzione soft, le autorità di regolamentazione potrebbero caricare i propri contratti intelligenti su tali blockchain, per monitorare le transazioni e alzare bandiere rosse per operazioni sospette. Ciò, tuttavia, non equivale a poter bloccare a transazione – è una scelta che preserva l'integrità dell'ecosistema, a costo di lentezza, ex post arranca attraverso i laboratori forensi blockchain e i tribunali.
Un'opzione alternativa è richiedere che gli sviluppatori incorporino determinati controlli nei protocolli, quando la catena è in una fase nascente ancora centralizzata, così come alcuni indirizzi sono già inseriti nella lista nera di a su base volontaria da molti fondatori del protocollo. Quando e se la catena diventa completamente decentralizzata, l'aggiornamento dei controlli dovrebbe essere effettuato direttamente dalle autorità, ma il tipo di azioni loro consentite potrebbe essere vincolato fin dall'inizio in modo trasparente per prevenire abusi.78 Si tratta di un soluzione che sacrifica in parte i valori crittografici, ma consente un'applicazione più rapida delle normative.

Misure per prevenire il rischio di riciclaggio nel mondo delle criptovalute

Il problema dell'anonimato degli utenti è difficile, ma si possono trovare soluzioni parziali. Ad esempio, le transazioni peer-to-peer tra normali utenti di criptovalute possono essere autorizzate a rimanere anonime se sotto a certa quantità. A un livello più complesso, le autorità di regolamentazione potrebbero attingere al corpo molto ampio della ricerca sull'identità digitale e incoraggiare l'uso di tecnologie di identificazione che riducano la fuga di informazioni al minimo.
Tali tecnologie consentirebbero almeno l'anonimato delle parti interessate nei confronti chiunque tranne le autorità: non è necessario fornire informazioni personali agli scambi o altro azienda75. È possibile implementare algoritmi ancora più sofisticati ed è probabile che ne siano disponibili altri, dato il ritmo veloce della ricerca nel campo76. Questi possono essere fusi con i suggerimenti del settore, come la recente proposta di token soulbound77, o NFT non trasferibili che incorporano informazioni su un singolo individuo e potrebbe essere utilizzato nella verifica dell'identità e delle credenziali.
L'anonimato del validatore e la resistenza alla censura sono i problemi più difficili da risolvere, in particolare quando si tratta di blockchain ad alta decentralizzazione e alta automazione. Per nominare solo un'opzione soft, le autorità di regolamentazione potrebbero caricare i propri contratti intelligenti su tali blockchain, per monitorare le transazioni e alzare bandiere rosse per operazioni sospette. Ciò, tuttavia, non equivale a poter bloccare a transazione – è una scelta che preserva l'integrità dell'ecosistema, a costo di lentezza, ex post arranca attraverso i laboratori forensi blockchain e i tribunali.
Un'opzione alternativa è richiedere che gli sviluppatori incorporino determinati controlli nei protocolli, quando la catena è in una fase nascente ancora centralizzata, così come alcuni indirizzi sono già inseriti nella lista nera di a su base volontaria da molti fondatori del protocollo. Quando e se la catena diventa completamente decentralizzata, l'aggiornamento dei controlli dovrebbe essere effettuato direttamente dalle autorità, ma il tipo di azioni loro consentite potrebbe essere vincolato fin dall'inizio in modo trasparente per prevenire abusi.78 Si tratta di un soluzione che sacrifica in parte i valori crittografici, ma consente un'applicazione più rapida delle normative.

Misure per prevenire il rischio di riciclaggio nel mondo delle criptovalute

- Regolamentazione a livello europeo e nazionale;
- Collaborazione tra autorità competenti e attori del mondo delle criptovalute;
- Trovare soluzioni al problema dell'anonimato.

Misure per prevenire il rischio di riciclaggio nel mondo delle criptovalute

Inoltre, potrebbe essere molto utile accogliere le proposte formulate dalla dottrina:

- Le transazioni peer-to-peer tra utenti di criptovalute possono essere autorizzate a rimanere anonime se sotto a certa quantità;

- Le autorità di regolamentazione potrebbero fare riferimento agli strumenti di ricerca sull'identità digitale e incoraggiare l'uso di tecnologie di identificazione che riducano la fuga di informazioni;

- Adozione di tecnologie che consentano almeno l'anonimato delle parti interessate nei confronti degli altri utenti, ma non nei confronti delle autorità;

Nonché dallo stesso settore delle criptovalute:

- Utilizzo dei c.d. Soulbound Token (SBT): token d'identità digitale che rappresentano i tratti, le caratteristiche e i risultati legati a una persona o un'entità. Gli SBT sono emessi dai "Souls", che rappresentano conti o wallet blockchain, e non possono essere trasferiti;

- NFT non trasferibili: incorporano informazioni su un singolo individuo e non possono essere venduti o separati dai loro proprietari. Potrebbero essere utilizzati nella verifica dell'identità e delle credenziali (In particolare, v. proposta di Vitalik Buterin).

Misure per prevenire il rischio di riciclaggio nel mondo delle criptovalute

L'anonimato del validatore in particolare quando si tratta di blockchain ad alta decentralizzazione e automazione rappresenta un problema di difficile soluzione.

Sono stati tuttavia individuate alcune possibili soluzioni:

- Le autorità di regolamentazione potrebbero caricare i propri smart contracts sulla blockchain, per monitorare le transazioni e far scattare notifiche (red flags) in caso di operazioni sospette. Ciò, però, non porta a bloccare la transazione;

- Gli sviluppatori potrebbero prevedere dei sistemi di controllo all'interno dei protocolli, oppure inserire alcuni indirizzi in una c.d. lista nera formata su base volontaria da vari sviluppatori di protocollo. Quando e se la catena diventa decentralizzata, l'aggiornamento dei controlli dovrebbe essere effettuato direttamente dalle autorità.

Thank You

STUDIO LEGALE FISICARO&P.

www.studiolegalefisicaro.it