BANCA D'ITALIA
EUROSISTEMA

Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività

Roma, giugno 2022

Introduzione

Il settore finanziario, al pari di altri, sta utilizzando in maniera sempre più estesa e significativa le potenzialità offerte dalla digitalizzazione. Tra le nuove soluzioni, ha assunto rilievo l'applicazione di tecnologie decentralizzate, le cosiddette *distributed ledger technologies* (DLT)[1]. Si tratta di tecnologie di applicazione potenzialmente molto vasta, anche in ambiti non connessi con la finanza. La presente comunicazione si concentra sugli utilizzi riconducibili alla detenzione e al trasferimento di valori e diritti, che sono rappresentati digitalmente mediante le cosiddette cripto-attività[2], anche in mancanza di un soggetto o gestore centrale.

Le cripto-attività possono generare rischi di vario genere. Una rapida e ampia diffusione di questi strumenti potrebbe compromettere la stabilità del sistema finanziario a causa dell'interdipendenza dei soggetti che vi partecipano, regolamentati e non, nonché della mancanza di controlli e strumenti che possono limitare gli effetti di eventi sfavorevoli. Il mondo delle cripto-attività è infatti ancora largamente deregolamentato. Sono in corso a livello internazionale ed europeo i lavori per disegnare un nuovo insieme di regole e di controlli per questi prodotti e per i relativi "ecosistemi" (vedi *infra* paragrafo 2) ma la loro entrata a regime richiederà ancora tempo.

---

1 Nell'ambito dell'ordinamento giuridico nazionale, ex art. 8-ter, comma 1, d.l. 14 dicembre 2018 n. 135, convertito con modificazioni dalla legge n. 12 del 2019. "Si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili".

2 Si intende una rappresentazione digitale di valore o di diritti che possono essere emessi, trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga.

Al tempo stesso, gli sviluppi registrati dal settore – l'elevata crescita del numero e del valore delle cripto-attività[3]; l'estrema volatilità delle quotazioni; i ricorrenti episodi di crisi di operatori e schemi della specie, dovuti a truffe, a incidenti informatici o a difetti di fondo, che hanno comportato anche di recente ingenti perdite per i soggetti coinvolti; la forte opacità degli scambi e degli assetti proprietari di gran parte di questi schemi; in molti casi, l'elevatissima volatilità del loro prezzo – sollevano preoccupazioni per tematiche che rientrano nel mandato delle autorità. La Banca d'Italia è interessata alle cripto-attività nell'esercizio di sue molteplici funzioni: di controllo prudenziale sugli intermediari vigilati; di sorveglianza sul regolare funzionamento del sistema dei pagamenti; di salvaguardia della stabilità monetaria e finanziaria; di contrasto al riciclaggio e al finanziamento del terrorismo; di tutela della clientela.

Con questa comunicazione si intendono conseguire due obiettivi: in primo luogo, richiamare l'attenzione degli intermediari vigilati, dei soggetti sorvegliati e di quelli che operano a vario titolo negli ecosistemi decentralizzati, anche come utenti, tanto sulle opportunità quanto sui rischi connessi con l'uso di tali tecnologie nella finanza e con le attività e i servizi relativi alle cripto-attività (emissione, custodia, scambio, prestiti, servizi di pagamento, cfr. *infra*); in secondo luogo, evidenziare alcuni profili rilevanti per la definizione, da parte dei predetti soggetti, di presidi volti ad attenuare i rischi connessi con l'impiego delle tecnologie decentralizzate e/o con l'operatività in cripto-attività.

Il documento vuole pertanto costituire un riferimento per gli utenti, gli intermediari, i fornitori tecnologici, i gestori di schemi, infrastrutture e portafogli digitali che operano nell'ambito di ecosistemi di cripto-attività, sia prima della definizione compiuta del quadro di regolamentazione europea in divenire sia dopo la sua definizione; tale quadro regolamentare, infatti, non ricomprenderà nel proprio ambito applicativo l'intera filiera dei soggetti sopra menzionati, né interamente la complessità delle soluzioni tecnologiche a supporto degli ecosistemi di cripto-attività (*infra*, paragrafo 2).

---

[3] Il valore aggregato a livello globale delle cripto-attività rapportato a quello delle attività finanziarie è pari a circa l'1% (Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets*, febbraio 2022) ma va comunque ricordato che la dimensione del fenomeno non sempre rispecchia i rischi potenziali per la stabilità finanziaria. Ad esempio, il mercato dei mutui *sub-prime* prima dello scoppio della crisi finanziaria del 2007 ammontava a circa 1.300 miliardi di dollari, cioè la metà del valore delle cripto-attività registrato a novembre 2021.

Con riguardo a quest'ultimo profilo, occorre aver presente che l'utilizzo di modelli decentralizzati nella finanza trova nel fattore tecnologico il suo elemento qualificante, in grado di connettere i diversi attori del sistema anche in mancanza di relazioni dirette. L'impronta della tecnologia e il ruolo dei soggetti che concretamente concorrono ad imprimerla – quali gli sviluppatori degli algoritmi – costituiscono parte integrante degli schemi e degli accordi attraverso i quali vengono realizzati, nell'ambito delle soluzioni decentralizzate, i "trasferimenti di valore": la forte connessione esistente tra tali fenomeni e le istanze di mantenimento della stabilità finanziaria e monetaria costituisce la ragione per cui le banche centrali osservano e monitorano con grande attenzione anche l'operatività di tali soggetti.

La comunicazione è articolata come segue: nel paragrafo 1. si riportano le principali caratteristiche dell'applicazione di tecnologie decentralizzate ai servizi finanziari; nel paragrafo 2. si descrive lo stato della cooperazione internazionale e del contesto regolamentare in materia; nel paragrafo 3. si propongono principi e punti di riferimento per gli intermediari vigilati e i soggetti attratti nell'ambito della sorveglianza sul sistema dei pagamenti; nel paragrafo 4. vengono richiamati i possibili rischi per gli utilizzatori di cripto-attività; infine, nel paragrafo 5. vengono indicati i prossimi passi che la Banca d'Italia è intenzionata a compiere per contribuire allo sviluppo ordinato e sicuro delle nuove soluzioni digitali a cui si è fatto cenno.

1. Le principali caratteristiche dell'applicazione di tecnologie decentralizzate ai servizi finanziari

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*[4]). 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

---

[4] 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.

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)[5].

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.

Affinché ciò avvenga le DLT 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.

Le soluzioni DLT realizzano ecosistemi complessi all'interno dei quali ciascuna parte – intermediari vigilati, fornitori di tecnologia, altri operatori (cfr. *infra*) 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*[6], è centrale per assicurare il corretto funzionamento dell'ecosistema e garantire la stabilità finanziaria e la tutela della clientela.

---

5 Questo registro ha una duplice funzione. Da un lato, esso consente di memorizzare in modo inalterabile le informazioni relative alle transazioni in modo da prevenirne la manipolazione. Dall'altro lato, fornisce il meccanismo che consente l'aggiunta di nuove informazioni anche in assenza di un ente centrale di garanzia: le informazioni non possono essere aggiunte al registro distribuito fino a quando non viene raggiunto, tra i partecipanti al registro stesso, il consenso sulla loro validità; ciò incrementa la resilienza di tali registri rispetto ad eventuali tentativi di contraffazione. Numerosi sono i casi d'uso potenziali della DLT/*blockchain*, ad esempio nell'ambito dei servizi resi dalla pubblica amministrazione (registri immobiliari, voto, identità digitale ecc.), nel campo della sanità, dei media, dell'energia e altri; al suo utilizzo sono associati rischi di natura sia finanziaria sia non finanziaria.

6 Un riferimento allo *smart contract* è contenuto nell'art. 8-ter, comma 2, d.l. 14 dicembre 2018 n. 135 (convertito con modificazioni dalla legge n. 12 del 2019), ai sensi del quale esso è definito come "un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse".

Questa caratteristica rende problematico inquadrare tali fenomeni nella regolamentazione esistente. Ad esempio, quest'ultima prevede il meccanismo di esternalizzazione che consente agli intermediari di avvalersi dei servizi di fornitori di tecnologia ma, nel caso delle DLT, tale interazione si può instaurare anche in assenza di legami diretti (contrattuali). In questo senso la tecnologia "lega" le componenti oggettive (strumenti, infrastrutture tecniche e organizzative) e soggettive (le diverse tipologie di operatori coinvolti) degli ecosistemi in nuovi prodotti e servizi, espressione "sintetica" di ciascun contributo. Tale rilevanza della componente tecnologica e degli stessi fornitori di tecnologia realizza una sorta di "governance algoritmica" che scardina gli schemi di governo tradizionali e della quale è necessario tenere conto.

Proprio con riferimento alla governance, una distinzione rilevante va fatta tra DLT *permissioned* o *permissionless.* Le prime richiedono che un utente, per accedere e apportare modifiche al registro (*ledger*), debba ottenere il permesso da parte di un soggetto o entità centrale, che *de facto* assume responsabilità di governance. Nelle DLT *permissionless* invece è difficile o impossibile individuare tale responsabile[7]; le operazioni possono essere effettuate senza l'intervento di soggetti esterni (ad esempio intermediari) tramite l'utilizzo di *smart contracts*, ossia, come già accennato, programmi informatici che vengono eseguiti automaticamente al verificarsi di specifiche condizioni, garantendo in tal modo per via algoritmica il rispetto degli aspetti contrattuali sottesi all'erogazione del servizio. Anche questa caratteristica, alla base della cosiddetta "finanza decentralizzata"[8] (*decentralized finance* – DeFi), rende problematico inquadrare le cripto-attività nella regolamentazione esistente, e contribuisce a spiegare le difficoltà e i ritardi registrati in questo settore dal legislatore e dalle autorità di regolamentazione a livello mondiale.

In tale contesto, il peculiare ruolo svolto dagli *smart contracts* nell'ambito delle tecnologie decentralizzate in finanza ha profonde implicazioni sulla

---

7 Nello specifico, le reti *permissionless* permettono l'accesso a ogni utente che decida di connettersi e partecipare, generando nuove transazioni, effettuando il compito di *miner* (processo di validazione e finalizzazione delle transazioni) o semplicemente leggendo il registro delle transazioni memorizzate. Le reti *permissioned*, invece, operano per conto di una comunità che condivide un interesse comune, dove l'accesso al ruolo di *miner* è limitato a un numero esiguo di individui considerati fidati (il livello di lettura del registro e di partecipazione nella generazione di nuove transazioni può essere soggetto a limitazioni o meno a seconda dell'organizzazione che controlla la rete).

8 Financial Stability Board*, Decentralised financial technologies: Report on financial stability, regulatory and governance implications*, 2019.

governance di un ecosistema: regole, diritti e doveri sono iscritti all'interno di protocolli e programmi – predisposti e resi liberamente disponibili sull'infrastruttura da utilizzatori della stessa, anche residenti in diverse giurisdizioni – rendendo difficile identificare un soggetto o entità centrale cui riferire le responsabilità di governance, e quindi il foro competente e la legge applicabile, in particolare nelle DLT *permissionless*.

Con specifico riferimento al fenomeno delle cripto-attività, è utile evidenziare che esso non esaurisce le potenzialità applicative delle nuove tecnologie decentralizzate nel settore finanziario; inoltre, richiede la capacità di distinguere tra diverse categorie di prodotti e di utilizzi sulla base dei vari livelli di rischio che le caratterizzano anche in funzione della esistenza o meno di un valore intrinseco.

Fermo restando quanto sopra richiamato relativamente alle DLT *permissioned* o *permissionless*, una prima distinzione attiene alla possibilità che le cripto-attività possano essere scambiate: 1) direttamente da "utente" a "utente" (cd. "DeFi pura"[9]); 2) tramite gli operatori che svolgono specifiche attività di "*exchange*"[10] e di *trading* di cripto-attività (anche mediante ricorso a fasi gestite "*off chain*", cioè fuori dalla DLT, come in ipotesi il regolamento delle operazioni).

Sulla base di un ulteriore importante criterio di classificazione, le cripto-attività possono essere distinte in due categorie: 1) *unbacked crypto-assets*, cripto-attività prive di un meccanismo di stabilizzazione che ne ancori il valore a un'attività di riferimento (es. Bitcoin, ma potrebbero essere ricomprese anche le cosiddette "*stablecoins* algoritmiche", il cui meccanismo di stabilizzazione è basato appunto su un algoritmo che ne condiziona la domanda e l'offerta sul mercato); 2) *asset linked stablecoins*, cripto-attività garantite da attività sottostanti (es. valute ufficiali, crediti, merci, etc.) che mirano a mantenere un valore stabile rispetto a una valuta *fiat* (es. euro o dollari), un bene specifico o un *pool* o paniere di attività.

Da quest'ultima classificazione deriva la possibilità di distinguere meglio anche le diverse caratteristiche e funzioni di una varietà eterogenea di attività

---

9 Nella sua versione più "pura", la DeFi non contempla l'intervento di intermediari e intende replicare in forma interamente decentralizzata diverse attività svolte nell'ambito del sistema finanziario tradizionale per il tramite di intermediari autorizzati.

10 Gli *exchangers* prestano: 1) servizi di scambio di "*crypto*" con "*crypto*" o di questi strumenti con valute *fiat*; 2) altri servizi connessi con quelli di custodia di cripto-attività (cd. "portafogli digitali").

digitali che presentano rischi assai differenti ad esse associati: alcune di tali attività digitali possono trovare pieno titolo tra gli strumenti di pagamento, in quanto emesse da banche centrali[11]; altre, rappresentate da cripto-attività definibili in via generale come "token privati", possono essere più o meno stabili in valore.

Tra queste ultime, figurano alcune cripto-attività garantite da una riserva che possono essere ancorate ad una singola valuta *fiat* e associate a un "debito" di rimborso integrale a carico di un soggetto (normalmente l'emittente) nonché essere utilizzate come strumento di pagamento. Una funzione di scambio o di riserva di valore potrebbe, entro certi limiti, essere associata a cripto-attività (sempre garantite da una riserva) il cui valore sia ancorato ad attività a bassa volatilità e connesso con un diritto di credito dell'utilizzatore alla restituzione del valore di mercato dell'attività sottostante. Altre cripto-attività, ancorate a strumenti potenzialmente volatili come strumenti finanziari, benché anch'esse assistite da un diritto di rimborso per l'utilizzatore, potrebbero avere una funzione di investimento in quanto prevalentemente speculative e pertanto contraddistinte da più elevati profili di rischio.

Cripto-attività, prive di qualsiasi valore intrinseco, non riferite ad alcuna attività dell'economia reale o finanziaria, non assistite da alcun diritto in capo all'utilizzatore a ricevere indietro alcunché non possono, come tali, essere idonee a svolgere una funzione né di pagamento né di investimento (si tratta quindi di *unbacked crypto-assets*, come sopra richiamato): per tale ragione, e per i rischi che le caratterizzano, il loro utilizzo non dovrebbe essere in alcun modo incentivato. In relazione a ciò, si evidenzia che quanto riportato più avanti al paragrafo 3 non può essere inteso come linea di orientamenti atti a contrastare in modo di per sé esclusivo ed esaustivo i rischi derivanti dall'operatività in quest'ultima categoria di cripto-attività, il ricorso alle quali, come detto, resta sempre altamente rischioso, privo di tutele e per ciò stesso fortemente scoraggiato (cfr. *infra*)[12].

---

11 Ci si riferisce, ad esempio, ai lavori in corso nell'ambito dell'Eurosistema dedicati al progetto di euro digitale (https://www.ecb.europa.eu/paym/digital_euro/html/index.it.html#:~:text=L'euro%20digitale%20sarebbe%20come,affiancherebbe%20il%20contante%20senza%20sostituirlo).

12 Si evidenzia, al riguardo, che il Bitcoin in data 12 maggio 2022 ha raggiunto un valore di circa 26.350 dollari USA, con una pronunciata diminuzione rispetto al massimo storico di quasi 69.000 dollari toccato il 10 novembre 2021. Il valore di Ethereum, la cui quotazione si aggirava tra i 4.500 e i 4.800 dollari tra il 6 e il 13 novembre 2021, nella data del 12 maggio 2022 è sceso sotto i 1.800 dollari.

° ° °

Gli aspetti richiamati possono essere, almeno in parte, intercettati e indirizzati facendo leva sui compiti, propri dell'Istituto, di vigilanza su banche e intermediari finanziari, di tutela della clientela e di sorveglianza sul regolare funzionamento del sistema dei pagamenti. A complemento di questo impianto, si ravvisa peraltro l'esigenza di rafforzare la cooperazione con le altre autorità di controllo coinvolte a vario titolo in questo campo, in particolare la Consob, l'AGCM, l'Ivass.

È inoltre importante iniziare a delineare un sistema di principi e buone prassi (cfr. *infra*, paragrafo 3) che, ancorché non vincolanti, mitighino i rischi connessi con l'operatività in questo settore[13]. In particolare – specie nelle aree più distanti dal perimetro regolamentare, dove più avvertita è la dominanza del fattore tecnologico e dei soggetti che lo generano e lo condizionano – esiste lo spazio per lavorare alla definizione di *standard* a cui fare riferimento quali "parametri di qualità" degli aspetti costitutivi delle tecnologie decentralizzate (come gli *smart contracts*): il ricorso a forme di partenariato pubblico-privato può rappresentare, in questa prospettiva, un'opzione di cui tenere conto (cfr. paragrafo 3.2).

2. La cooperazione internazionale e il contesto regolamentare

Sebbene la diffusione dell'utilizzo delle tecnologie decentralizzate nella finanza risulti al momento come detto contenuta, essa può generare rischi di vario genere. Il rapido sviluppo di tali tecnologie, come detto, può infatti incidere sulla stabilità del sistema finanziario anche in virtù della connessione e interdipendenza tra i soggetti coinvolti, che operano in un contesto privo di un sistema organico di regole e controlli. In particolare, l'interazione sempre più stretta tra i soggetti coinvolti rende più complesso il presidio dei rischi.

---

13 L'utilizzo di tecnologie decentralizzate nella finanza presenta le stesse tipologie dei rischi della finanza tradizionale (credito, mercato, operativo, cibernetico, liquidità, etc.) accrescendone però la rilevanza sulla stabilità finanziaria, derivante ad esempio: i) dal rischio operativo all'interno di un ecosistema decentralizzato; ii) dai rischi sugli elementi di vulnerabilità non del tutto esplorati della DLT circa la continuità del servizio; iii) dal rischio cibernetico e di frodi legato alla presenza di più soggetti non regolati ed autonomi; iv) dalla presenza di strumenti e paradigmi tecnologici non puntualmente disciplinati; v) dall'assenza, per i nuovi sistemi, di standard di settore di riferimento e vi) dalla dimensione transazionale del fenomeno, che rende difficile regolarne l'influenza a livello di singole giurisdizioni.

Al riguardo, il tema è stato oggetto di documenti di ricerca e focus da parte di diverse banche centrali[14].

Le cripto-attività sono all'attenzione di numerose autorità internazionali, governi, banche centrali e autorità di vigilanza, interessati a comprendere se, e in che modo, regolamentarle, tenendo conto in particolare della varietà di casistiche esistenti con riferimento, come evidenziato in precedenza, sia alla possibile funzione economica, sia ai diversi profili di rischio. Per tale ragione in vari *fora* internazionali (tra cui FSB, BCBS, IOSCO, CPMI)[15] è stata avviata una serie di iniziative volte a integrare questi strumenti in quadri normativi di supervisione sugli intermediari, di funzionamento dei mercati finanziari e di sorveglianza sul sistema dei pagamenti[16].

In Europa, nell'ambito della strategia sulla finanza digitale definita dalla Commissione nel settembre 2020, sono state pubblicate, tra le altre, le seguenti due proposte legislative: il *Markets in Crypto Assets Regulation* (MiCAR) e il *Digital Operational Resilience Act* (DORA). Il primo introduce una disciplina armonizzata per l'emissione e l'offerta al pubblico di cripto-attività, nonché per i relativi servizi (es. di negoziazione e portafoglio digitale); il secondo ha come obiettivo il rafforzamento della resilienza operativa digitale dell'intero settore finanziario, anche attraverso l'introduzione di un regime di sorveglianza sui fornitori critici di servizi ICT, tra i quali potrebbero rientrare coloro che prestano servizi funzionali alla gestione delle cripto-attività.

In particolare, MiCAR non ricomprende nel proprio ambito di applicazione le cripto-attività che rientrano nella definizione di strumenti finanziari di cui alla direttiva MiFID (cd. strumenti finanziari tokenizzati);

---

14 Cfr. Federal Reserve: https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf; Bank of England: https://www.bankofengland.co.uk/financial-stability-in-focus/2022/march-2022); Deutsche Bundesbank: https://www.bundesbank.de/resource/blob/707710/3f3bd66e8c8a0fbeb745886b3f072b15/mL/2017-09-distributed-data.pdf.

15 Consiglio per la Stabilità Finanziaria (Financial Stability Board - FSB), Comitato di Basilea per la Vigilanza Bancaria (Basel Committee on Banking Supervision - BCBS), Comitato dei pagamenti delle infrastrutture di mercato (Committee on Payments and Market Infrastructures - CPMI). Il tema è rilevante anche per autorità di altri settori, in particolare quello fiscale: Organizzazione per la Cooperazione e lo Sviluppo Economico (Organization for Economic Co-operation and Development - OECD).

16 FSB: https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/
BCBS: https://www.bis.org/bcbs/publ/d519.htm
CPMI-IOSCO: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD685.pdf
IOSCO: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf.

rispetto a queste ultime si segnala che, sempre nel contesto della strategia sulla finanza digitale, nella Gazzetta Ufficiale dell'Unione Europea del 2 giugno 2022 è stato pubblicato il regolamento relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito (cd. DLT *pilot regime*) il quale, diversamente da MiCAR, si riferisce a strumenti finanziari tokenizzati[17].

In aggiunta a quanto sopra, nell'ambito dell'*AML* (*anti-money laundering*) *package*, la proposta di riforma del quadro normativo e istituzionale in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo (CFT), presentata dalla Commissione a luglio 2021, include tra i soggetti obbligati tutti i prestatori di servizi in cripto-attività e, in linea con gli standard del FATF-GAFI (*Financial Action Task Force*-Gruppo di Azione Finanziaria Internazionale), estende ai trasferimenti in cripto-attività l'obbligo (già in vigore per quelli in valuta legale) di trasmettere i dati informativi relativi all'ordinante e al beneficiario, al fine di garantirne la tracciabilità e l'individuazione di eventuali transazioni sospette.

La Banca d'Italia partecipa da tempo ai lavori in materia di cripto-attività in sede internazionale ed europea e segue gli sviluppi nel mercato. Dal 2015 sono state pubblicate – anche d'intesa con la Consob e l'Unità di Informazione Finanziaria per l'Italia (UIF), che opera in forma autonoma all'interno dell'Istituto di emissione – avvertenze per gli intermediari vigilati e per gli utenti, evidenziando i rischi collegati all'acquisto e alla detenzione di cripto-attività, la complessità delle tecnologie sottostanti, la carenza di tutele legali e contrattuali, la possibilità – in ultima istanza – di perdere integralmente le somme investite (sul punto, si veda, più avanti, il paragrafo 4).

Mentre procedono le discussioni in corso a livello internazionale e i lavori per il completamento del quadro normativo atteso nell'Unione europea, le connessioni tra la finanza tradizionale e quella che si avvale di tecnologie decentralizzate crescono: si creano nuove opportunità di *business*, ma anche maggiori occasioni di contagio tra i due ecosistemi. È dunque necessario conciliare l'esigenza di evitare rischi eccessivi con la

---

17 Il Regolamento (UE) 2022/858 del 30 maggio 2022 relativo al DLT *pilot regime* riguarda l'introduzione di un regime pilota per consentire alle infrastrutture di mercato (che offrono servizi di negoziazione e regolamento titoli) di sperimentare l'applicazione della DLT all'offerta di tali servizi su alcune tipologie di strumenti finanziari. Il Regolamento si applicherà a partire dal 23 marzo 2023, salvo alcune eccezioni che entrano in vigore in anticipo rispetto a tale data.

possibilità per il sistema di cogliere i benefici dell'innovazione collegati a uno sviluppo virtuoso delle tecnologie decentralizzate applicate al settore finanziario.

Con specifico riguardo all'ordinamento nazionale giova ribadire che, nelle more della definizione di MiCAR, attualmente non esiste in Italia un quadro normativo specifico per le cripto-attività.

Anche per i profili AML/CFT, in attesa dell'approvazione delle proposte normative contenute nel *AML package* europeo, il settore è solo parzialmente regolato. La normativa antiriciclaggio italiana, di cui al d.lgs. 231/2007, da ultimo modificato dal d.lgs. 125/2019 in recepimento della direttiva AML V[18], fa propria una nozione molto ampia sia di valuta virtuale (in cui rientrano le cripto-attività con finalità sia di pagamento che di investimento) sia di prestatore di servizi in tale comparto (VASP – *Virtual Asset Service Provider*), comprendente qualsiasi persona fisica o giuridica che offra servizi collegati alle valute virtuali in via professionale[19]. I VASP sono tenuti ad adempiere agli obblighi di adeguata verifica, conservazione dei dati e delle informazioni e di segnalazioni delle operazioni sospette.

Il d.lgs. 90/2017 ha inoltre previsto che l'Organismo degli Agenti e dei Mediatori (OAM) iscriva in una sezione speciale (istituita *ex novo* e attiva dal 16 maggio 2022) del registro dei cambiavalute i VASP in possesso di requisiti minimali, secondo le modalità stabilite dal decreto del Ministero dell'Economia e delle Finanze del 13 gennaio 2022. In particolare, il decreto stabilisce che l'attività di VASP è riservata ai soggetti con sede legale in Italia o ai soggetti UE con stabile organizzazione in Italia, non essendo ammessa l'operatività nella forma della libera prestazione di servizi.

Anche sotto altri profili, come quello fiscale, è avvertita la necessità di definire discipline ad hoc, che conferiscano certezza agli operatori e agli investitori. L'Italia non è ad oggi dotata di una disciplina tributaria per questo comparto, i cui profili fiscali sono per ora basati sull'applicazione, in via interpretativa, di norme dettate per altre tipologie di operazioni e attività. Il disegno di un'apposita normativa potrà avvalersi sia della

---

18 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 (cd. direttiva AML V).

19 Nello specifico, il decreto antiriciclaggio fa riferimento ai "prestatori di servizi relativi all'utilizzo di valuta virtuale" (in cui sono ricompresi, tra l'altro, anche emittenti e offerenti di valuta virtuale) e ai "prestatori di servizi di portafoglio digitale" (collettivamente indicabili come VASP).

regolamentazione in via di introduzione a livello sovranazionale, sia dei lavori attualmente in corso presso l'OCSE e la Commissione europea in materia di scambio di informazioni tra prestatori dei servizi per cripto-attività e amministrazioni finanziarie[20]. In prospettiva, appare opportuno favorire un bilanciamento tra la considerazione delle peculiarità del settore e le esigenze di coerenza fra la disciplina fiscale delle cripto-attività e quella di altri cespiti, nonché con l'ordinamento giuridico in generale, anche per motivi di equità di trattamento.

L'approvazione del regolamento MiCAR contribuirà a ridurre l'incertezza normativa e favorirà uno sviluppo ordinato del mercato delle cripto-attività. Peraltro, pur rappresentando un primo e importante passo in avanti, MiCAR non affronta tutte le diverse componenti degli ecosistemi di cripto-attività e della loro applicazione nella finanza decentralizzata. Ad esempio, con riferimento all'ambito oggettivo sono escluse da MiCAR, allo stato del negoziato in corso presso le istituzioni UE, le cripto-attività uniche e non fungibili, c.d. *Non fungible tokens* o NFT, come le opere della *digital art*; dal punto di vista soggettivo, il regolamento introduce norme applicabili a entità chiaramente identificabili (i.e. emittenti, offerenti, fornitori di servizi), che non esauriscono il novero dei soggetti coinvolti nei sistemi di finanza decentralizzata. Non saranno pertanto disciplinati i programmatori (di *smart contracts*) e i titolari di token di governance delle cosiddette "*Decentralised Autonomous Organization*" (DAO); resteranno fuori dall'ambito applicativo anche i cosiddetti *unhosted wallets*, *software* che abilitano allo scambio *peer-to-peer* tra indirizzi su DLT.

In aggiunta, già si profilano iniziative in questo settore – anche grazie agli accordi tra intermediari vigilati e terze parti – e altre verranno presumibilmente avviate anche prima dell'iter di completamento delle norme europee e della loro piena entrata a regime; ciò motiva l'esigenza che le Autorità assumano un atteggiamento proattivo, volto a far sì che gli sviluppi di mercato siano improntati fin da subito a caratteristiche di sicurezza.

---

[20] Cfr. consultazione pubblica su *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*: https://www.oecd.org/tax/exchange-of-tax-information/public-consultation-document-crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf

3. Riferimenti per gli intermediari, gli operatori (gestori di schemi, *wallet providers*, gestori di infrastrutture di pagamento) e i fornitori di soluzioni tecnologiche in materia di cripto-attività

L'uso di cripto-attività comporta una pluralità di rischi in grado di minare la stabilità del sistema finanziario. Tra i rischi finanziari rilevano quelli di liquidità, mercato, credito e controparte; tra quelli non finanziari vengono in evidenza rischi operativi e di tipo *cyber*, legali, reputazionali, di riciclaggio e finanziamento del terrorismo e di terze parti.

Nell'introdurre una disciplina del mercato delle cripto-attività, che sottoporrà a vigilanza anche nuove categorie di soggetti, MiCAR riconoscerà un ruolo importante alle banche e agli altri intermediari finanziari vigilati; questi ultimi possono svolgere una varietà di possibili funzioni all'interno degli ecosistemi di cripto-attività, contribuendo al loro funzionamento, supportando e facilitando il trasferimento dei token, la custodia, le interazioni con i titolari e i movimenti in entrata e in uscita dall'ecosistema.

Parimenti, l'operatività in cripto-attività non può non tenere conto degli obiettivi sottesi all'esercizio, da parte delle banche centrali, della sorveglianza sul regolare funzionamento del sistema dei pagamenti, richiamato nella stessa regolamentazione MiCAR in corso di definizione come fattore chiave da valutare in fase autorizzativa e durante lo svolgimento dell'attività dei soggetti coinvolti. Anche oltre e prima di MiCAR, il nuovo quadro di sorveglianza dell'Eurosistema (cfr. *infra* paragrafo 3.2) si rivolge ai gestori di schemi (anche quando attengono a cripto-attività con funzione di pagamento) e alle funzionalità che ne supportano l'offerta e l'utilizzo (es. *wallets* digitali), oltre che alle piattaforme che svolgono le funzioni di trasferimento/regolamento nell'ambito dei cosiddetti *stablecoins arrangements* e ai fornitori di tecnologia.

Premesso quanto sopra, nei sotto-paragrafi che seguono verranno richiamati alcuni profili di attenzione per le banche, gli intermediari finanziari e gli operatori attratti nell'ambito della sorveglianza sul sistema dei pagamenti, nonché per i fornitori tecnologici; ciò fermo restando il presupposto, indicato nel paragrafo 1, che esistono alcune categorie di cripto-attività – a valenza speculativa e altamente rischiose – la cui diffusione resta fortemente scoraggiata.

3.1 Banche e intermediari finanziari[21]

In attesa che si definiscano le indicazioni in corso di elaborazione a livello internazionale ed europeo, indipendentemente dalla specifica tipologia di operatività nel settore delle cripto-attività, gli attuali regimi prudenziali[22] contengono principi ai quali le banche e gli altri intermediari vigilati possono fin da subito fare riferimento per valutare e presidiare i rischi connessi con l'eventuale avvio dell'operatività in cripto-attività.

Tale operatività, oltre alla detenzione di esposizioni in cripto-attività, potrebbe consistere, da parte delle banche e degli intermediari finanziari, in una o più delle seguenti attività:

– emissione e/o rimborso di cripto-attività (ove previsto);

– custodia e gestione della riserva nel caso di *asset-linked stablecoins*;

– gestione di infrastrutture e validazione di transazioni[23];

– prestazione di servizi relativi alle cripto-attività quali: portafoglio digitale (*wallet*), *exchanger*, piattaforma di *trading*, esecuzione di ordini, collocamento, ricezione e trasmissione di ordini per conto di terzi, consulenza.

In relazione alle suddette attività – e tenendo conto delle specificità di ciascuna e delle relative tipologie di rischio – si richiama l'attenzione degli intermediari, sulla base delle regole e delle buone prassi già oggi applicabili, sull'importanza di assicurare:

– il coinvolgimento tempestivo degli organi di governo aziendale e delle funzioni di controllo di secondo e di terzo livello, sin dalla fase iniziale di studio delle iniziative, per valutarne la conformità alla regolamentazione vigente, la coerenza con gli indirizzi strategici, gli obiettivi e le politiche di governo dei rischi, nonché la relativa sostenibilità economica e finanziaria;

---

21 Trattasi delle seguenti categorie di intermediari bancari e finanziari, rispetto ai quali la Banca d'Italia svolge la propria attività di vigilanza: banche e gruppi bancari; SIM e gruppi di SIM; SGR, SICAV e SICAF; Istituti di moneta elettronica – IMEL; Istituti di pagamento; intermediari finanziari ex art. 106 TUB.

22 Tra cui quelli definiti nell'ambito del Comitato di Basilea nonché dalle norme comunitarie (es. CRR/CRD5).

23 Con riferimento alle attività di gestione di infrastrutture e validazione di transazioni, si veda il paragrafo 3.2.

– adeguati flussi informativi verso gli organi aziendali e le funzioni di controllo interno in merito al livello e all'andamento della loro esposizione, diretta o indiretta, a tutte le tipologie di rischio collegate all'operatività nel settore delle cripto-attività, agli eventuali scostamenti rispetto alle politiche approvate dall'organo con funzione di supervisione strategica, alla tipologia di operazioni e servizi prestati e ai rispettivi rischi; particolare attenzione dovrà essere dedicata all'adeguato presidio dei rischi di riciclaggio e finanziamento del terrorismo connessi all'operatività in cripto-attività – incluso il rischio di elusione di sanzioni internazionali – nonché dei rischi reputazionali e legali, tenuto conto anche del quadro normativo in evoluzione;

– che gli organi aziendali e le funzioni di controllo interno siano in possesso di idonee competenze per comprendere appieno opportunità e rischi che caratterizzano l'operatività in cripto-attività e l'utilizzo di tecnologie decentralizzate, in rapporto al contesto competitivo e al modello di *business* dell'intermediario, alla sua strategia e al complessivo profilo di rischio;

– che gli assetti organizzativi siano, tempo per tempo, coerenti ed adeguati alle iniziative intraprese, per assicurare l'efficace presidio dei rischi da essi derivanti, la tutela della clientela, la prevenzione e gestione dei conflitti di interesse con altre attività svolte. Particolare attenzione è prestata all'adeguatezza dei processi e delle procedure volte ad assicurare l'identificazione, valutazione e mitigazione dei rischi (reputazionali o di altro genere) derivanti dall'esternalizzazione o dal ricorso a servizi prestati da terze parti, anche ove non qualificabili come esternalizzazioni (es. operatori specializzati nella custodia di *assets* digitali, *wallets*, piattaforme di *trading*).

In caso di esternalizzazione o affidamento a terze parti di funzioni operative relative all'operatività in cripto-attività o all'impiego di tecnologie decentralizzate, dato il carattere innovativo delle stesse assumono importanza centrale: (i) la valutazione delle condizioni previste dalla normativa per la qualificazione come funzioni "essenziali" o "importanti" delle stesse; (ii) la capacità degli intermediari di selezionare e monitorare nel continuo il fornitore dei servizi, in modo da assicurare che quest'ultimo disponga non solo delle competenze tecniche/tecnologiche idonee al corretto svolgimento del servizio affidato ma anche della capacità di assicurare nel continuo il rispetto delle regole di vigilanza (in termini, ad esempio, di livello di servizio

concordato; adeguatezza dei flussi informativi; sicurezza delle informazioni relative all'attività dell'intermediario; sicurezza dei propri sistemi).

Tenuto conto delle specifiche caratteristiche delle cripto-attività, del tipo di operatività e delle tecnologie decentralizzate, si evidenzia inoltre agli intermediari l'esigenza di garantire:

– l'adeguata definizione delle fasce di clientela a cui si intende offrire/distribuire prodotti o servizi in cripto-attività, in relazione alla complessità degli stessi e a eventuali previsioni normative applicabili, valutando l'introduzione di limiti operativi quali-quantitativi, anche rapportati alla situazione reddituale e patrimoniale del cliente; ciò, in particolare, con riguardo a servizi di *wallet*, di *exchange*, piattaforme di *trading*, esecuzione di ordini, collocamento, ricezione e trasmissione di ordini per conto di terzi, consulenza, ovvero a tutte le attività connesse al rimborso di cripto-attività;

– la correttezza del rapporto con la clientela, con particolare riferimento ai servizi e alle attività menzionate al punto precedente, sia attraverso un'adeguata informativa sui rischi e sulle caratteristiche connesse con l'operatività in cripto-attività, anche ad opera di terze parti, sia mediante un rafforzamento delle procedure per la rilevazione delle frodi e per la gestione dei reclami. Fermi restando i presidi posti dall'Ordinamento sia a tutela della correttezza delle pratiche commerciali intrattenute con la clientela sia nell'ambito di altre discipline di settore, e in mancanza di una normativa ad hoc, particolare attenzione dovrà essere posta ai rischi legali e reputazionali derivanti da transazioni eseguite dalla stessa clientela tramite portali o piattaforme di *trading* verso cui venga consentito o facilitato l'accesso: nello specifico, è fortemente sconsigliato rendere disponibile o agevolare tale accesso ove manchi la possibilità per l'intermediario di verificare che i predetti portali o piattaforme siano in grado di evitare l'operatività su cripto-attività connotate da elevati profili di rischio (come nel caso degli *unbacked crypto-assets*);

– l'adozione di tutti i presidi necessari al contenimento dei rischi operativi – con particolare attenzione al rischio informatico – e la tutela della *cybersecurity*; in questo contesto è necessario che gli intermediari identifichino e gestiscano opportunamente i rischi connessi al funzionamento di infrastrutture tecnologiche attualmente non regolate né sorvegliate. Si sottolinea, nello specifico, la rilevanza di tale tipologia

di rischio nei servizi che riguardano la custodia delle cripto-attività e delle chiavi private che abilitano all'accesso e allo scambio delle stesse[24];

– la mitigazione anche delle nuove dimensioni che potrebbero assumere i rischi finanziari collegati alla prestazione di servizi in cripto-attività o all'emissione delle stesse, entro i limiti previsti dal quadro normativo vigente. Particolare rilevanza assumono i rischi finanziari – segnatamente, di credito, di mercato e di liquidità – laddove l'operatività in cripto-attività sia associata all'obbligo di rimborso: i) delle somme impiegate da parte della clientela (laddove sia previsto un rimborso alla pari rispetto al valore nominale della cripto-attività); oppure ii) del valore di mercato degli *asset* sottostanti (qualora si preveda un rimborso, di livello variabile, collegato al valore delle attività cui la cripto-attività sia eventualmente riferita). Inoltre, si evidenzia che i medesimi rischi possono richiedere specifica attenzione con riferimento alla gestione e all'investimento delle attività della riserva, ove esistente, sottostante a una cripto-attività;

– una accurata valutazione del trattamento prudenziale applicabile alle eventuali esposizioni in cripto-attività che, in attesa della definizione del quadro legislativo in materia, andrà valutato caso per caso, nel contesto di una preventiva interlocuzione con l'Autorità di Vigilanza[25];

– nel comparto del risparmio gestito, la coerenza e l'allineamento tra la strategia di investimento dei fondi, il relativo profilo di liquidità, la politica di rimborso e la forma degli stessi, nonché tutti i profili attinenti alla tutela dei sottoscrittori.

Si richiama l'attenzione degli intermediari sul fatto che l'operatività connessa con le cripto-attività deve essere attentamente presidiata in una prospettiva di sana e prudente gestione. In assenza di un pieno presidio dei rischi suindicati, è necessario che le banche e gli intermediari finanziari si astengano dallo svolgimento di questa tipologia di attività ovvero la dismettano. Quanto precede è da declinare secondo il principio di proporzionalità, in relazione alla complessità operativa, dimensionale

---

24 Tali rischi possono ricomprendere lo smarrimento e il furto delle chiavi crittografiche e, conseguentemente, delle stesse cripto-attività.

25 Il Comitato di Basilea sta finalizzando un secondo documento di consultazione sul trattamento prudenziale delle cripto-attività con l'obiettivo di pubblicare entro la fine dell'anno il documento finale. Cfr. www.bis.org/press/p220531.htm.

e organizzativa degli intermediari nonché, come sopra delineato, alla concreta operatività svolta in cripto-attività o mediante utilizzo di tecnologie decentralizzate. La Banca d'Italia si riserva comunque di effettuare in ogni momento ulteriori approfondimenti e analisi, anche caso per caso, con riguardo a specifiche iniziative o attività.

3.2 Operatori[26] (gestori di schemi, wallet providers*, gestori di infrastrutture di pagamento) e fornitori tecnologici*

Per le attività di sorveglianza l'Istituto utilizzerà innanzitutto alcune indicazioni tratte dal Rapporto che il CPMI e l'IOSCO[27] hanno indirizzato al mercato e alle autorità competenti per analizzare le modalità di applicazione degli attuali principi internazionali agli *stablecoin arrangements*.

Nella stessa direzione di attrarre nell'ambito della sorveglianza soggetti operanti in ecosistemi cripto è orientato il nuovo quadro di sorveglianza dell'Eurosistema, il c.d. "PISA *framework*" (*Payment Instruments, Schemes and Arrangements*), pubblicato a novembre 2021 e che entrerà in vigore a novembre dell'anno in corso. Quest'ultimo – con l'obiettivo di tenere in considerazione i cambiamenti (tecnologici e normativi) che caratterizzano il mercato dei pagamenti – ha esteso il perimetro di controllo anche a nuove soluzioni di pagamento, quali ad esempio le *stablecoins* (che vengono ricomprese in virtù di un riferimento al "*transfer of value*" invece che al tradizionale concetto di "*transfer of funds*"). Il *framework* consentirà pertanto di includere nel perimetro di controllo della sorveglianza anche cripto-attività con funzione di pagamento e le funzionalità che ne supportano l'offerta e l'utilizzo (es. i *wallets*).

---

26 Gli operatori sorvegliati che siano intermediari finanziari vigilati faranno riferimento anche a quanto indicato nel par. 3.1.

27 Il 1° dicembre 2021 si è conclusa la consultazione pubblica su tale Rapporto, Cfr. https://www.bis.org/cpmi/publ/d198.pdf. Il CPMI e l'IOSCO – valorizzando l'uso sinora prevalente dei nuovi *assets* e in particolare la cosiddetta "*transfer function*" delle cripto-attività ancorate a un'unica valuta *fiat*, ovvero il trasferimento di valore tra utenti che tipicamente è associato al funzionamento di un sistema di pagamento - prendono a riferimento per la componente infrastrutturale di progetti di *stablecoins* sistemici i *Principles for financial market infrastructures* – PFMI applicabili ai sistemi di pagamento (nonché ad altre infrastrutture di mercato, quali i CSD, che svolgono una *transfer function*). Se ne può evincere una "forza attrattiva" delle funzionalità di pagamento di questi *asset*, anche in connessione con gli impatti che possono avere sull'efficienza e sull'affidabilità del sistema dei pagamenti nel suo complesso, e per questa via un ruolo di primo piano delle Banche centrali che hanno tra i propri compiti la salvaguardia di tali obiettivi.

I soggetti che forniscono la tecnologia a supporto dei servizi bancari, finanziari e di pagamento[28] sono già oggetto, a certe condizioni, di disposizioni prudenziali per l'*outsourcing* e di controlli di sorveglianza[29].

Con specifico riguardo all'operatività in cripto-attività e all'uso nella finanza di tecnologie decentralizzate, in relazione anche al presidio del rischio sistemico e del corretto funzionamento del sistema dei pagamenti, si invitano gli operatori e i fornitori tecnologici, a seconda dei casi, a tenere conto che:

- è essenziale che la gestione della tecnologia si fondi il più possibile su una governance chiara e definita nonché su requisiti di gestione dei diversi rischi (ad esempio operativi, *cyber*, riguardanti la protezione delle informazioni e dei dati) a cui dovrebbero fare riferimento – nelle circostanze in cui ciò risulti applicabile (in particolare nel caso delle DLT *permissioned*, in cui è possibile identificare soggetti responsabili) – gli sviluppatori dei programmi che determinano il funzionamento della DLT o i soggetti su cui sono concentrati poteri di gestione del funzionamento della DLT (e.g. validazione delle transazioni oppure governance in senso più ampio);

- i fornitori di servizi tecnologici, ove chiaramente individuabili, possono rientrare nell'ambito delle norme di vigilanza in qualità di *outsourcee* degli intermediari vigilati e/o essere sottoposti a controlli di sorveglianza in virtù dell'applicazione, a certe condizioni, dei principi di sorveglianza sul sistema dei pagamenti. I controlli su questi soggetti potrebbero estendersi al monitoraggio delle transazioni *peer-to-peer,* abilitate da *software* (cosiddetti *unhosted wallets*); in tal senso i fornitori delle tecnologie utilizzate e delle funzionalità a supporto (es. soggetti che gestiscono la DLT fornendo l'impianto tecnologico di supporto e programmazione) dovrebbero garantire la disponibilità di adeguata

---

28 Es. servizi di elaborazione e registrazione di dati, di fornitura di reti informatiche e di comunicazione, di fornitura e manutenzione di terminali e dispositivi utilizzati per i servizi di pagamento.

29 In particolare, la Banca d'Italia assoggetta a sorveglianza, ai sensi del proprio Provvedimento del 9 novembre 2021, i fornitori di infrastrutture o servizi tecnici considerati critici per l'ordinato funzionamento del sistema dei pagamenti italiano; tra i servizi che tali fornitori erogano rientrano, a titolo esemplificativo, i servizi di messaggistica e di rete, i servizi e/o applicazioni di *business* strumentali alla compensazione e/o al regolamento di operazioni di pagamento e i servizi tecnologici di interfaccia multi operatore per l'accesso di terze parti ai sensi del Regolamento delegato (UE) n. 2018/389.

rendicontazione informativa[30], anche considerando il ruolo e i vincoli che fanno capo agli intermediari vigilati e alle infrastrutture di pagamento sottoposte alla sorveglianza;

- le infrastrutture che abilitano alla funzione di trasferimento delle cripto-attività, con particolare riguardo a quelle ancorate a un'unica valuta *fiat* e che costituiscono una componente delle piattaforme di *trading* su cui le stesse vengono scambiate, dovrebbero conformarsi ai principi di sorveglianza applicabili alle infrastrutture finanziarie, con particolare riferimento a quelli attinenti alla governance e alla gestione integrata dei rischi;

- le cripto-attività con funzione di pagamento e le funzionalità che ne supportano l'offerta e l'utilizzo (es. i *wallets*) dovrebbero conformarsi ai principi di sorveglianza su strumenti, schemi, *arrangements*, con particolare riferimento a quelli in materia di solidità della base legale, governance, nonché rischio di credito e di liquidità. In particolare, per assicurare la rimborsabilità ed essere "più sicure" per utilizzatori ed emittente, le riserve delle *stablecoins* ancorate ad attività dovrebbero rispecchiare il più possibile la composizione ed il valore del paniere o della singola attività alla quale sono riferite.

Fermo restando quanto precede, ove l'attività risulti rilevante ai fini del regolare funzionamento del sistema dei pagamenti o di singole componenti dello stesso, avuto anche riguardo all'eventuale "trasferimento di valore"[31] nell'ambito di sistemi digitali complessi, la Banca d'Italia si riserva altresì di valutare la possibilità di fare ricorso alle prerogative ad essa riconosciute dall'art. 146 del Testo Unico Bancario (Sorveglianza sul sistema dei pagamenti).

Considerata anche la difficoltà in alcuni casi – si pensi ad esempio al caso della DeFi nella sua accezione "pura" – di individuare soggetti specifici

---

30 Ad esempio, la lista di tutte le transazioni effettuate nei confronti di *unhosted wallets* (ove ciò sia possibile per differenza rispetto ad una lista di *hosted wallets*, come ad esempio quella ricavabile dal censimento dei soggetti che effettuano attività di portafoglio digitale detenuto dall'OAM), in modo da consentire, qualora necessario, l'esecuzione di attività di monitoraggio specifico (cd. "*blockchain analysis*") e/o di ricostruzione a posteriori da parte dell'Autorità Giudiziaria (cd. *blockchain forensics*).

31 Dal punto di vista dell'Eurosistema, nel contesto del PISA *framework*, i recenti sviluppi tecnologici giustificano l'estensione del campo di applicazione dell'attuale sorveglianza sugli strumenti di pagamento a tutti gli strumenti di pagamento elettronici che consentono "trasferimenti di valore" tra utenti finali.

cui applicare determinati requisiti, è suscettibile di approfondimento, nell'ottica di un rafforzamento dei necessari presidi di mitigazione dei rischi, la possibilità di intervenire sui processi di definizione e di sviluppo degli standard tecnologici utilizzati.

Tali standard potrebbero costituire punti riferimento "di qualità" per lo sviluppo e l'implementazione degli *smart contracts* ed altri aspetti costitutivi delle tecnologie decentralizzate; essi dovrebbero altresì essere definiti e gestiti mediante un modello di governance che sappia sfruttare le sinergie derivanti dall'interazione del settore pubblico con il settore privato, in una prospettiva di co-regolazione in virtù della quale l'Autorità dialoga costantemente con gli operatori tecnologici per lo sviluppo di *benchmarks* condivisi, affinché la tecnologia possa evolversi in modo coerente e compatibile con i diritti e le tutele che meritano di essere garantite.

4. Tutela della clientela – richiamo alle avvertenze sui rischi delle cripto-attività

Con specifico riferimento alla tutela della clientela che intende acquistare o negoziare cripto-attività, la Banca d'Italia torna a richiamare l'attenzione sui contenuti delle avvertenze da essa pubblicate (anche congiuntamente con la Consob) a partire dal 2015, dei comunicati adottati dalle Autorità di vigilanza europee (EBA, ESMA ed EIOPA), in linea con gli orientamenti espressi dagli organismi internazionali (FSB, FATF)[32]. In particolare, le predette Autorità, facendo seguito ad analoghe iniziative intraprese in passato, hanno da ultimo ribadito che le cripto-attività sono strumenti altamente rischiosi e speculativi e non sono adatte per la maggior parte dei consumatori come investimento o mezzo di pagamento o scambio.

---

[32] La Banca d'Italia, in linea con gli orientamenti espressi dagli organismi internazionali (FSB, FATF) e le tre autorità di supervisione europee (EBA, ESMA, EIOPA, le c.d. ESAs), ha pubblicato, a partire dal 2015, diverse avvertenze agli utilizzatori e agli intermediari vigilati relativi alle cripto-attività: Banca d'Italia - Avvertenza sull'utilizzo delle cosiddette "valute virtuali" (gennaio 2015) https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/index.html?dotcache=refresh; Banca d'Italia - Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee (marzo 2018) -https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali-2018/index.html?dotcache=refresh; Consob e Banca d'Italia mettono in guardia contro i rischi insiti nelle cripto-attività (aprile 2021) - https://www.bancaditalia.it/media/comunicati/documenti/2021-01/CS_Congiunto_BI_CONSOB_cryptoasset.pdf
Le ESAs hanno di recente pubblicato "*EU financial regulators warn consumers on the risks of crypto-assets*" (marzo 2022).

Le cripto-attività, infatti, non sono attualmente soggette alle norme in materia di trasparenza dei prodotti bancari, dei servizi di pagamento e dei servizi di investimento e sono sprovviste di specifiche protezioni (segnatamente, i servizi aventi a oggetto cripto-attività non sono soggetti a nessuna forma di supervisione o di controllo da parte delle Autorità di vigilanza, fatto salvo quanto sopra riportato).

È necessario pertanto che i clienti siano consapevoli del rischio di perdita anche totale del capitale investito, di frodi ed errori e della mancanza di forme di tutela a loro disposizione. È importante, in particolare, comprendere che, tra tutte, vi sono alcune cripto-attività completamente prive di valore intrinseco, che non sono assistite da alcun diritto di rimborso e che, in via generale, come più volte ricordato in precedenza, non possono essere considerate idonee a svolgere una funzione di pagamento o di investimento in virtù della loro natura altamente rischiosa[33]: l'informativa alla clientela dovrebbe evidenziare che l'operatività riguardante tali cripto-attività è scoraggiata da parte della Banca d'Italia.

Specifica attenzione, in tale ottica, deve essere rivolta dai clienti ai rischi di pubblicità ingannevole, effettuata anche tramite i *social media* e gli *influencers*, e alle proposte di investimento che garantiscono elevati rendimenti[34].

La Banca d'Italia invita comunque gli intermediari vigilati e gli altri operatori a curare nel modo più scrupoloso possibile, anche in assenza di prescrizioni normative, l'informativa da rendere alla clientela che intenda acquistare e detenere cripto-attività utilizzando eventuali canali messi a disposizione dagli intermediari e operatori medesimi; ciò al fine di facilitare la massima consapevolezza in ordine ai rilevanti rischi sopra richiamati, nonché allo scopo di mitigare i gravi rischi legali e reputazionali che siffatte attività possono generare.

---

33 Attenzione va prestata ad esempio anche alle *asset linked stablecoins* che sono in realtà ancorate ad *unbacked crypto-assets* e che pertanto potrebbero, a dispetto delle apparenze, avere le stesse caratteristiche di volatilità/rischiosità di queste ultime, il cui utilizzo va, come detto, scoraggiato.

34 Dall'indagine svolta dall'OAM nel 2021 in collaborazione con l'Università di Tor Vergata sull'orientamento degli italiani sulle cripto-valute, risulta che l'89% del campione analizzato ne ha solo sentito parlare e l'11% non ha conoscenze sul tema; dal sondaggio emerge che, all'aumentare del livello di conoscenza sulle cripto-valute, aumenta la propensione all'investimento.

5. Prossimi passi

La Banca d'Italia – in raccordo con la BCE e con le altre autorità di controllo nazionali – continuerà a monitorare l'andamento del mercato delle cripto-attività e l'evoluzione dell'uso delle tecnologie decentralizzate nella finanza al fine di valutarne i rischi e gli impatti sulla stabilità finanziaria, sugli intermediari bancari e finanziari, sul corretto funzionamento del sistema di pagamenti e sulla tutela della clientela.

L'Istituto continuerà a collaborare nelle varie sedi internazionali (FSB, CPMI e BCBS) ed europee per definire standard di elevata qualità e a rafforzare il dialogo con gli operatori di mercato con l'obiettivo di: i) favorire lo sviluppo di modelli operativi solidi e sostenibili, anche con riferimento all'"impatto ambientale"[35]; ii) garantire un adeguato livello di interoperabilità (e "standard di colloquio") tra diverse soluzioni tecnologiche a supporto della finanza decentralizzata e dell'operatività in cripto-attività; iii) assicurare il rispetto della normativa vigente, in particolare di quella AML; iv) favorire la parità competitiva con le altre giurisdizioni alla luce dello sviluppo tecnologico.

La Banca d'Italia potrà inoltre promuovere e offrire supporto a iniziative volte a definire *standard* e buone prassi che possano costituire un punto di riferimento condiviso[36] specie nell'ambito di settori di attività e di sviluppo non inclusi nelle regole vigenti e in quelle di prossima emanazione, accrescendo l'attrattività della piazza finanziaria nazionale.

L'Istituto è aperto al dialogo con i vari *stakeholders*, anche attraverso i facilitatori di innovazione che esso gestisce[37], per promuovere la definizione e lo sviluppo di standard tecnologici abilitanti, a cui tali soggetti potranno fare riferimento qualora intendano sviluppare servizi connessi alle tecnologie

---

35 Una specifica attenzione va infatti posta ai meccanismi di consenso utilizzati per la validazione delle transazioni che, con specifico riferimento a determinate soluzioni (in particolare, la *proof-of-work* utilizzata dal Bitcoin), possono avere un impatto sostanziale sotto il profilo ambientale e climatico a causa del consumo intensivo di energia. Una più recente tipologia di meccanismi di consenso è la cosiddetta *proof-of-stake* (PoS), normalmente considerata a minor consumo energetico. Sul tema, si veda ad esempio FSB *"Assessment of Risks to Financial Stability from Crypto-assets*", febbraio 2022, pp. 9-10.

36 Come ad esempio standard tecnologici legati alla definizione e all'implementazione degli *smart contracts* e degli algoritmi di consenso, oppure buone prassi di governance decentralizzata.

37 Si fa riferimento all'offerta integrata di facilitatori di innovazione gestita dalla Banca d'Italia al fine di favorire il dialogo con il mercato (Canale Fintech), sostenere lo sviluppo di progetti *fintech* (Milano Hub), consentire forme controllate di sperimentazione (Sandbox regolamentare).

DLT; ciò con l'obiettivo di individuare e sostenere nell'ambito del sistema finanziario e dei pagamenti un'innovazione virtuosa e adeguatamente presidiata, al fine di mitigare i rischi che essa può comportare e massimizzare i benefici che ne possono derivare a vantaggio del sistema economico e degli attori che lo compongono: consumatori, famiglie, imprese, enti della pubblica amministrazione.

Nell'ambito dei compiti ad essa attribuiti, la Banca d'Italia, anche in stretto raccordo con la Banca Centrale Europea e con le altre autorità di controllo, monitorerà in ogni caso la funzionalità degli assetti di governo e controllo e l'efficacia degli eventuali limiti e presidi operativi interni, anche antiriciclaggio, introdotti dagli intermediari.

A completamento dell'iter di definizione del richiamato quadro normativo europeo in materia di cripto-attività l'Istituto, d'intesa con le altre autorità competenti, potrà intervenire con indicazioni aventi anche natura prescrittiva per contribuire a garantire uno sviluppo dei servizi basati su tecnologie decentralizzate sicuro, efficiente, inclusivo, sostenibile.

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia