BANCA D'ITALIA
EUROSISTEMA

# La regolamentazione delle nuove tecnologie basate sulla Distributed ledger technology – DLT, tra tutela del mercato e rischi di sistema

Università Luiss Guido Carli di Roma
Guardia di Finanza – Scuola di Polizia Economico-Finanziaria

Intervento di Giuseppe Siani
Capo del Dipartimento Vigilanza bancaria e finanziaria della Banca d'Italia

Roma, 3 maggio 2022

## 1. Introduzione

A oltre dieci anni dalla nascita di Bitcoin si osserva, a livello globale un forte sviluppo delle *crypto*-attività e del relativo ecosistema. L'ampiezza e la velocità dei cambiamenti derivano in particolare dalla profonda novità che caratterizza la tecnologia dei registri distribuiti (la *Distributed ledger technology*, DLT), i nuovi servizi così come i nuovi "oggetti" da essa generati (tra cui le *crypto*-attività), i nuovi attori – diversi dagli intermediari tradizionali – che si affacciano sul mercato.

Non è esagerato affermare che la DLT abbia introdotto, nel mondo finanziario, un nuovo paradigma, basato su tre dimensioni fortemente interconnesse ma distinte. La prima è tecnologica, con l'introduzione di un'infrastruttura di mercato distribuita, che consente di trasferire valore o diritti, senza una autorità fiduciaria centralizzata. La seconda consiste nel modo di rappresentare digitalmente valore, con l'introduzione di *token* che possono essere privi di una attività sottostante (c.d. *unbacked*, come ad esempio Bitcoin) o rappresentare digitalmente strumenti finanziari o altre attività (*backed crypto assets*). La terza novità è l'ingresso sul mercato di nuovi soggetti, che possono operare anche in modo decentralizzato attraverso meccanismi di governo peculiari.

Questi tre piani (tecnologia, *token*, nuovi attori) sono anche alla base della cd. "finanza decentralizzata" (*decentralized finance* o *DeFi*). Essi possono essere singolarmente analizzati in modo coerente ed efficace e quindi favorire il mantenimento di prospettive di analisi tradizionali per tipologia di intermediari e/o di prodotto. Tuttavia, solo una loro valutazione integrata, che sfrutti competenze e risorse specializzate in diversi comparti, può consentire di monitorarne i rischi e scegliere le risposte regolamentari e di supervisione più appropriate.

Il mio intervento riflette il punto di vista del supervisore. Esso deve comprendere gli sviluppi del mercato e cercare di mitigare i rischi per gli intermediari, per la stabilità

finanziaria e per i consumatori, in attesa di un quadro regolamentare europeo più definito e di standard consolidati a livello internazionale. Mi concentrerò in particolare su tre aspetti: l'ecosistema *crypto* e i relativi rischi; l'evoluzione in corso della normativa e le attività della Banca svolte finora. Cercherò infine di fornire una visione integrata delle sfide future per il supervisore prudenziale.

## 2. La DLT, le crypto-attività, l'ingresso di nuovi agenti economici

Per affrontare un problema complesso è spesso utile scomporlo nelle sue parti. Distinguerei quindi tra tecnologia DLT; strumenti monetari e finanziari basati su tale tecnologia; agenti economici coinvolti (regolati e non).

Un registro elettronico DLT è un sistema distribuito il cui "stato" in ogni istante è condiviso e accettato dai soggetti coinvolti. In un sistema tradizionale questo risultato è ottenuto grazie al ruolo di un soggetto fiduciario. Con la DLT la sincronizzazione del registro condiviso è possibile anche tra soggetti che non si coordinano e non beneficiano di fiducia reciproca.

Senza qui entrare nel merito di aspetti complessi, mi limito a sottolineare che questa architettura non è priva di implicazioni per il regolatore e il supervisore prudenziale. Ad esempio, così come accade per i sistemi tradizionali anche quelli basati su DLT devono garantire alcune condizioni fondamentali: essere resilienti agli attacchi informatici; supportare a costi modesti – e io aggiungerei anche in modo sostenibile dal punto di vista ambientale – un volume elevato di transazioni; avere una *governance* robusta e identificabile: quest'ultimo è un aspetto che può rivelarsi particolarmente critico quando alla decentralizzazione tecnica della struttura della DLT (che lavora su più nodi) non si accompagna un protocollo controllato da una singola entità per la gestione delle regole di scrittura sul registro.

In ogni caso, proprio la natura decentralizzata della DLT può rendere non semplice la manutenzione e l'aggiornamento del protocollo che la governa, per migliorarne ad esempio la sicurezza o l'efficienza. In particolare, non tutti i protocolli DLT garantiscono le condizioni desiderate di efficienza, scalabilità, sostenibilità e buona *governance*. L'approccio comunemente adottato dai vari regolatori e organismi internazionali è quello della neutralità tecnologica, ma questo criterio, potrebbe dover essere valutato in maniera non necessariamente acritica[1].

Per quanto riguarda le *crypto*-attività, è utile in primo luogo distinguere quelle prive di attività sottostanti (*unbacked)* da quelle che rappresentano strumenti monetari o finanziari (*backed crytptoassets*). Tra queste ultime possiamo individuare due macro classi: strumenti simili alla moneta elettronica, che avrebbero come sottostante depositi e attività liquide; strumenti finanziari "tokenizzati", alcuni dei quali simili a fondi d'investimento[2].

---

1 Si veda, al riguardo: Bains, P. "Blockchain Consensus Mechanisms: A Primer for Supervisors. IMF, Fintech notes, n. 3, 2022.

2 Vi sono inoltre altri strumenti, come gli *utility tokens*, che permettono di accedere a reti o community con varie finalità, oppure i *non-fungible tokens* (NFT) che permettono di trasferire il possesso di opere d'arte o altri beni non omogenei.

*L'industria sta già sviluppando prodotti più complessi e rischiosi in cui si combinano crypto-attività e finanza strutturata, proponendo contratti derivati su crypto-attività (anche prive, a loro volta, di un sottostante), prestiti collateralizzati da crypto-attività o la possibilità di accrescere l'esposizione al rischio attraverso un uso massiccio della leva finanziaria, in taluni casi configurando veri e propri schemi piramidali* [3].

Vi sono infine gli agenti economici che creano e consentono di trasferire *crypto*-attività e forniscono i relativi servizi. Coesistono nel nuovo scenario soggetti a noi ben noti – banche, intermediari finanziari, istituti di moneta elettronica, istituti di pagamento, operatori centralizzati che organizzano l'infrastruttura di mercato, fornitori esterni di funzioni critiche non solo di natura informatica – con altri del tutto nuovi.

Vi sono tra questi, per esempio, i fornitori di borsellini elettronici (*wallet providers*) e i gestori delle piattaforme per la compravendita di *crypto*-attività e lo scambio delle stesse con valute tradizionali. È importante pertanto assicurare a questi soggetti e agli intermediari ora vigilati le stesse regole secondo il consueto approccio *same activity, same risk, same rules*. In questa direzione vanno gli sforzi del legislatore europeo.

Altri attori dell'ecosistema crypto – caratterizzati da meccanismi di *governance* "decentralizzata" – sembrano di più difficile classificazione rispetto alle categorie tradizionali della vigilanza per soggetti e imporranno ragionamenti ulteriori. Tornerò su questo aspetto nel seguito.

## 3. I rischi per gli intermediari

Rispetto al significativo sviluppo del mercato osservati in altri paesi, in Italia gli intermediari si sono mossi con maggiore cautela. Dati raccolti attraverso l'Indagine Fintech svolta nel 2021 dalla Banca d'Italia mostrano che solo pochi intermediari hanno sinora avviato collaborazioni con partner specializzati, per consentire ai clienti di acquistare e custodire *crypto*-attività come Bitcoin ed Ether. Iniziative di carattere sperimentale si registrano nell'ambito dei pagamenti e della 'tokenizzazione' di *assets* finanziari.

La situazione sta rapidamente cambiando, grazie soprattutto agli accordi con terze parti. Progetti fortemente innovativi potrebbero prendere avvio anche prima dell'aggiornamento delle norme. Come supervisori, è necessario farsi trovare pronti per gestire con attenzione questa fase transitoria. Occorre infatti conciliare l'esigenza di evitare rischi eccessivi, non opportunamente mitigati, con la possibilità per il sistema di cogliere i benefici dell'innovazione.

I rischi da presidiare in prospettiva dipenderanno da come ciascun intermediario si collocherà nella catena del valore e dallo specifico modello di business adottato.

---

[3] Si tratta di schemi d'investimento che promettono rendimenti molto elevati rispetto ai tassi di mercato utilizzando i fondi versati da altri investitori; come noto l'intera architettura crolla non appena gli investitori richiedono i fondi versati. L'uso di *smart contracts* associati a *crypto*-attività ha favorito questo tipo di truffe. Si veda Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P. Zhou, Y. (2018), "Detecting Ponzi Scheme on Ethereum: Towards Healthier Blockchain Technology", in, Web Economics, Monetization, and Online Markets, aprile 2018. Si veda inoltre SEC, "Ponzi Schemes using virtual currencies", Investor Alert.

Quando l'iniziativa legislativa della Commissione UE sulle *crypto*-attività (cfr. par. 4) sarà ultimata i soggetti vigilati potrebbero svolgere nuove attività. La prestazione di servizi per la custodia delle *crypto*-attività, anche a clientela *retail* è certamente uno degli ambiti che potrebbe assumere maggior rilievo. Inoltre, alcuni intermediari potrebbero voler offrire servizi per la negoziazione di *crypto*-attività, o per l'effettuazione di pagamenti attraverso *stablecoins*. Potrebbero poi essere direttamente coinvolti nell'emissione di *stablecoins* o nella gestione delle relative riserve. I prestatori di servizi di investimento potrebbero proporre infine nuovi prodotti per permettere ai clienti di investire in panieri di *crypto*-attività, come già avviene in altre giurisdizioni.

Nel monitorare i diversi profili di rischio è importante considerare attentamente gli elementi di novità introdotti dalla DLT e dalle *crypto*-attività.

Un rilievo particolare va assegnato ai rischi operativi, che possono essere assai complessi da comprendere in relazione a tecnologie del tutto nuove e assumere una dimensione sistemica. Il loro presidio impone in primo luogo una attenta gestione dell'infrastruttura informatica e la tutela della *cyber-security*.

La custodia sicura di chiavi crittografiche – proprie o per conto della clientela – che rappresentano a tutti gli effetti il possesso di una *crypto*-attività e consentono di effettuare le transazioni – richiede investimenti e competenze tecnologiche di rilievo; la collaborazione con operatori specializzati può sicuramente rappresentare un'opzione ragionevole, ma impone a sua volta un attento presidio sulle funzioni esternalizzate e una corretta gestione del rapporto con "terze parti". Com'è noto, l'Unione Europea è al lavoro per introdurre – attraverso il regolamento sulla *Digital Operational Resilience* (DORA) – un regime di sorveglianza sui fornitori critici di servizi ICT per il settore finanziario e certamente tra questi potrebbero rientrare anche servizi funzionali alla gestione di *crypto*-attività.

*Le disposizioni di DORA sulla governance e gestione del rischio ICT ribadiscono il ruolo fondamentale e le responsabilità degli organi aziendali nella definizione delle strategie e politiche di* risk appetite *e per la gestione dei rischi ICT. Ai membri di questi organi sono richieste conoscenze per essere in grado di comprendere a pieno i sistemi adottati dagli intermediari e i rischi cui questi sono esposti. Parimenti, i sistemi di controllo interni sono destinatari di compiti specifici volti ad assicurare il corretto funzionamento dell'intermediario e l'efficace presidio di tutti i rischi ICT, inclusi quelli derivanti dal ricorso a parti terze, anche al di fuori del perimetro dell'esternalizzazione (ad esempio nel caso di catene di fornitori).*

L'emissione e circolazione di *crypto*-attività avviene su un gran numero di *blockchain* con caratteristiche differenti, in termini di *governance*, di sicurezza, di prestazioni, in alcuni casi completamente decentralizzate e non soggette ad alcune forma di regolamentazione e vigilanza. È quindi fondamentale che gli operatori finanziari abbiano la capacità di comprendere e discriminare i rischi assunti relativi al funzionamento di infrastrutture non sorvegliate e non facilmente sorvegliabili.

L'ampliamento della gamma di servizi offerti potrà introdurre ulteriori dimensioni di rischio di mercato e di liquidità, che gli intermediari ben conoscono e sono abituati a gestire ma che potrebbero assumere anche forme nuove. Ad esempio, per agevolare

le negoziazioni della clientela (es. scambio o acquisto di *crypto*-attività in denaro) gli intermediari potrebbero avere necessità di detenere direttamente *crypto*-attività, esponendosi ai rischi di mercato derivanti dalla loro elevata volatilità[4].

Complessità ulteriori si presenterebbero per gli intermediari direttamente coinvolti nell'emissione degli *stablecoins* con funzione monetaria. La funzionalità di tali schemi li rende simili a fondi di mercato monetario a valore patrimoniale netto (*Net asset value*, NAV) costante, con le ben note criticità derivanti da possibili *cliff-effect* non appena si manifesta un disallineamento tra valore del sottostante e valore nominale del *token* usato come mezzo di pagamento, anche per effetto di una gestione inappropriata del rischio di liquidità. L'eventuale perdita di fiducia del pubblico potrebbe avere conseguenze sistemiche, con un effetto di contagio anche per gli emittenti "sani", come accaduto durante la crisi del 2008 per i fondi di mercato monetario. Rischi analoghi riguardano la qualità e la natura delle riserve che sostengono le *stablecoin*[5].

Mi preme ribadire inoltre l'importanza di un corretto presidio dei rischi di riciclaggio e finanziamento del terrorismo, connessi con la natura anonima o "pseudo-anonima" che le transazioni in *crypto*-attività possono avere, specie se avvengono tramite borsellini elettronici gestiti in autonomia dagli utenti, senza il coinvolgimento alcun intermediario (*unhosted wallets*); il tema ha acquistato ulteriore rilievo negli ultimi mesi, anche in relazione alla paventata possibilità di utilizzare *crypto*-attività per eludere le sanzioni internazionali imposte alla Russia.

*Come evidenziato anche dal Gruppo di Azione Finanziaria Internazionale (GAFI)*[6]*, l'implementazione di questi presidi porrà sfide connesse, ad esempio, con l'individuazione e il tracciamento degli effettivi beneficiari dei trasferimenti, specie nei casi in cui i beneficiari non detengano crypto-wallet presso altri soggetti obbligati al rispetto della normativa AML oppure li detengano presso soggetti che abbiano sede in paesi la cui disciplina antiriciclaggio non sia pienamente conforme agli standard del GAFI.*

## 4. L'evoluzione della normativa

Le riflessioni dei supervisori si sviluppano in un quadro normativo e giurisprudenziale nazionale ancora incerto. Manca una definizione di *crypto*-attività nella normativa civilistica o in quella sui servizi finanziari applicabile per fini prudenziali o di tutela degli utilizzatori.

---

4 A titolo di esempio, il 3 maggio 2021 il prezzo di BTC era pari a 57.209 dollari; il 20 luglio aveva perso oltre il 47 per cento, per apprezzarsi del 121 per cento da lì al 20 ottobre.

5 È noto il caso, ad esempio, della quota elevata di *commercial paper* detenuta da Tether a sostegno della sua *stablecoin* USDT; qui il rischio è duplice: problemi di Tether potrebbero riverberarsi sul mercato delle carte commerciali; la fragilità di parte di queste ultime potrebbe comportare, in alcuni scenari, la caduta dello stesso schema. Per tali ragioni la società è stata indotta a ridurre drasticamente questa tipologia di riserve e da febbraio scorso, ai sensi di un accordo raggiunto con l'ufficio del procuratore generale di New York, è stata sottoposta a vincoli operativi e di trasparenza (che includono la pubblicazione periodica dei dettagli delle sue riserve).

6 FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (ottobre 2021).

È importante inoltre aver presente che attualmente l'emissione di *crypto*-attività non trova nelle norme esistenti compiuta e specifica disciplina e che le bozze dei Regolamenti europei, attualmente, in discussione potrebbero mantenere vuoti normativi che dovranno essere attentamente valutati e colmati.

L'unico riferimento è contenuto attualmente nella disciplina settoriale antiriciclaggio, nonché nelle misure a carico dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale[7]. In particolare, la normativa italiana[8] ha introdotto una nozione ampia di valuta virtuale e di *virtual asset service provider* (VASP), con definizioni coerenti con quelle proposte dal GAFI.

*I prestatori di servizi in crypto-attività sono tenuti ad adempiere agli obblighi di adeguata verifica, conservazione dei dati e delle informazioni e segnalazione delle operazioni sospette* [9].

La proposta di riforma del quadro normativo e istituzionale AML a livello europeo, presentata dalla Commissione a luglio 2021, adotta un approccio simile a quello del legislatore italiano, includendo tra i soggetti obbligati tutti i prestatori di servizi in *crypto*-attività; inoltre, la proposta, in linea con gli standard del GAFI, estende ai trasferimenti in valuta virtuale l'obbligo (già in vigore per i trasferimenti in valuta *fiat*) di trasmettere i dati informativi relativi all'ordinante e al beneficiario, al fine di garantirne la tracciabilità.

Alcuni Stati europei hanno inoltre recentemente adottato approcci normativi specifici alle *crypto*-attività diversi tra loro, che – sebbene ispirati da principi condivisibili – rischiano di favorire arbitraggi regolamentari. È quindi condivisa l'esigenza di definire un quadro normativo europeo strutturato, armonizzato, e neutrale dal punto di vista tecnologico che sia in grado di accompagnare la diffusione di tecnologie preservando la stabilità del sistema.

È quello che la Commissione europea ha inteso fare adottando la *Digital Finance Strategy*, nell'ambito della quale la *Markets in Crypto-Assets Regulation* (MiCAR) intende disciplinare l'emissione, l'offerta al pubblico o l'ammissione alle negoziazioni di *crypto*-attività non classificabili come strumenti finanziari e la connessa prestazione di servizi[10].

---

7 D.lgs. 231/2007 - misure concernenti la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e successive modificazioni (rif. d.lgs. 4 ottobre 2019, n. 125).

8 Con il d.lgs. 125/2019 che recepisce la V Direttiva AML.

9 I controlli in materia AML sui VASP spettano alla GdF (e all'UIF limitatamente alla verifica degli obblighi di segnalazione). La competenza a sanzionare le violazioni in materia antiriciclaggio è invece del MEF (con avvio della procedura sanzionatoria da parte di GdF o UIF).

10 Il Regolamento MiCA non si applica alle *crypto*-attività che rientrano nella definizione di strumenti finanziari (i.e. ai sensi della MiFID): per questi strumenti è in via di adozione il Regolamento EU per l'introduzione di un regime Pilota (*Pilot regime*) per le infrastrutture del mercato finanziario basate su tecnologia DLT, anch'esso parte delle misure regolamentari della *Digital Finance Strategy*.

Più in dettaglio, MiCAR introduce una disciplina specifica basata su obblighi di pubblicità e regole prudenziali per gli emittenti di *stablecoins*, che sono distinti in *asset-referenced token* (ART) ed *e-money token* (EMT)[11]. Non è allo stato previsto – soprattutto per via della complessità tecnica – un regime di autorizzazione all'emissione e di supervisione per *crypto*-attività diverse dagli *stablecoins,* che sono in molti casi immesse nel sistema in maniera totalmente decentralizzata mediante protocolli informatici, in assenza di specifiche attività di controllo.

*Queste crypto-attività sarebbero tuttavia oggetto di norme in materia di offerta al pubblico, ammissione alle negoziazioni (con obblighi di disclosure e di condotta) e rientrerebbero nella disciplina dei servizi (es. servizi di cambio, custodia) alla clientela. MiCAR introduce inoltre un regime di autorizzazione e supervisione sui prestatori di servizi in crypto-attività (crypto-asset service providers, CASP), cui saranno applicati requisiti prudenziali e organizzativi simili a quelli previsti per gli intermediari tradizionali, nonché obblighi comportamentali nei confronti della clientela.*

MiCAR riconosce inoltre l'importante ruolo che gli intermediari vigilati potranno assumere in qualità di emittenti e di prestatori di servizi in *crypto*-attività. L'attuale proposta prevede infatti che l'emissione di *stablecoins* ancorati a un'unica valuta avente corso legale (gli EMT) sarebbe consentito solo alle banche e agli IMEL. Alle banche sarebbe anche consentita l'emissione di ART, previo il rispetto di limitati obblighi di notifica e approvazione da parte dell'autorità competente.

Analogamente, i servizi in *crypto*-attività potranno essere offerti in tutto o in parte da intermediari vigilati (tra gli altri, banche, SIM, IMEL, SGR) nell'ambito delle autorizzazioni di cui già godono, previa notifica all'autorità nazionale di un programma di attività aggiornato e di indicazioni sull'adeguamento degli assetti di governo e controllo. Per gli intermediari già soggetti a regole prudenziali (come banche e IMEL) sono previste clausole di raccordo per evitare la sovrapposizione di requisiti e sono fatte salve le prerogative delle autorità prudenziali[12].

*Vi sono spazi per perfezionare il testo nel corso del negoziato, pur auspicando una rapida conclusione dello stesso. Crediamo vada ribadita l'esigenza di salvaguardare la tutela della stabilità finanziaria e dei diritti dei consumatori. Rileva in particolare l'esigenza di una chiara distinzione tra le due categorie di stablecoin disciplinate da MiCAR e dell'obbligo di rimborso al valore nominale per i soli e-money token, per i quali appare ragionevole immaginare una funzione come mezzo di scambio. Di converso, l'uso diffuso come mezzo di scambio di stablecoins ancorate a panieri di attività, non legati a singole valute, porrebbe a nostro avviso rischi significativi per la stabilità finanziaria.*

---

11 EMT e ART sono *crypto*-attività che intendono mantenere un valore stabile riferendosi rispettivamente a una sola valuta avente corso legale (EMT), ovvero a altri valori o diritti, incluse valute aventi corso legale (ART). Gli EMT sono considerati moneta elettronica da cui mutuano la disciplina, salvo alcune deroghe e integrazioni per tenere conto anche delle peculiarità tecnologiche. Essi sono rimborsati al valore nominale ed è sempre previsto un diritto di rimborso diretto nei confronti dell'emittente; gli ART prevedono in genere un diritto di rimborso diretto nei confronti dell'emittente al valore di mercato, necessariamente fluttuante, per evitare che diventino strumenti simili ai depositi.

12 La proposta non disciplina invece i requisiti prudenziali applicabili alle esposizioni bancarie in *crypto*-attività; questo aspetto è in discussione presso il Comitato di Basilea (BCBS) e dovrebbe essere incorporato in una futura revisione del Regolamento CRR da avviare dopo il 2025.

## 5. L'attività della Banca d'Italia

Dal 2015 sono state pubblicate – anche congiuntamente con la Consob e d'intesa con la UIF – avvertenze per gli intermediari vigilati e per gli utenti per evidenziare i rischi collegati all'acquisto e alla detenzione di *crypto*-attività, la complessità delle tecnologie sottostanti, la carenza di tutele legali e contrattuali, la possibilità – in ultima istanza – di perdere integralmente le somme investite.

La Banca d'Italia – in linea con la posizione delle autorità di supervisione europee (EBA, ESMA, EIOPA) e con gli orientamenti nel tempo espressi dagli organismi internazionali (FSB, FATF) – ha raccomandato agli intermediari particolare prudenza e ha ricordato in particolare l'importanza del presidio dei rischi operativi – inclusi quelli di natura legale e reputazionale – che derivano dalla distribuzione di servizi (es. *wallet*) di terzi.

Nell'esperienza concreta, abbiamo inoltre sollecitato gli intermediari che hanno sviluppato *partnerships* con terzi a introdurre precisi limiti operativi per restringere e monitorare l'attività della clientela che opera in *crypto*[13]. Gli intermediari che valuteranno di offrire servizi collegati alle *crypto*-attività dovranno quindi individuare specifici presidi antiriciclaggio che consentano, ad esempio, di identificare e profilare correttamente la clientela, di monitorare in tempo reale le operazioni effettuate e di individuare transazioni anomale; particolare attenzione dovrà essere posta all'attività di *due diligence* eseguita nei confronti di soggetti terzi (regolati e non) coinvolti a vario titolo nell'offerta dei servizi.

Pur in assenza di specifiche norme di trasparenza, è stata richiamata l'attenzione degli intermediari sull'esigenza di comunicare correttamente alla clientela che le *crypto*-attività non sono oggetto di regolamentazione. È stata ribadita l'importanza di assicurare il pieno coinvolgimento delle funzioni di controllo e dei massimi organi decisionali prima di intraprendere nuove attività.

La Banca d'Italia ha inoltre cercato di promuovere lo sviluppo di una sana innovazione in questo campo con una filiera completa e integrata di *innovation facilitator*, che comprende il Canale Fintech, una finestra *web* disponibile a chiunque voglia dialogare con la Banca in materia di innovazione; Milano Hub, il nostro centro a sostegno dello sviluppo digitale del mercato; il "*regulatory sandbox*", sviluppato sotto la guida del Comitato Fintech del MEF, e basato su uno stretto coordinamento tra il supervisore bancario, finanziario e quello responsabile delle infrastrutture dei mercati.

Quest'ultimo, in coerenza con le evidenze registrate sugli altri due canali, ha registrato un grande interesse di intermediari e operatori Fintech per sperimentare in un ambiente controllato prodotti e servizi innovativi basati su DLT e crypto-asset; questa iniziativa costituirà anche per il nostro Istituto un punto di osservazione privilegiato, dalla

---

13 Tra i presidi adottati dagli intermediari vi sono, ad esempio, limiti operativi rapportati alla situazione reddituale e patrimoniale del cliente, l'utilizzo del solo conto corrente aperto presso la banca per acquistare *crypto*-attività o ricevere il corrispettivo in caso di vendita, l'impossibilità di trasferire sul *wallet* aperto presso il *partner crypto*-attività provenienti da *wallet* esterni.

cui esperienza trarre indicazioni utili per promuovere interventi sulle regole, sia a livello nazionale che europeo.

Al fine di rafforzare il set informativo disponibile, stiamo ora valutando di avviare una rilevazione dedicata, al fine di disporre di un quadro aggiornato e completo dello sviluppo di questo comparto di operatività.

## 6. Considerazioni conclusive

L'ecosistema costruito intorno alle *crypto*-attività è ancora in una fase di sviluppo complessa, fluida, ed estremamente incerta nei suoi esiti finali.

Sebbene MiCAR possa rappresentare un progresso significativo, si tratta di un primo passo di un percorso che dovrà proseguire in futuro; da un lato, in particolare, coerentemente con l'attuale disciplina dei servizi finanziari, si introducono norme applicabili a entità chiaramente individuate, persone fisiche e giuridiche, alle loro attività e servizi. Tuttavia, lo sviluppo continuo della finanza decentralizzata introduce nuove sfide e richiede iniziative ulteriori, ad esempio con riferimento alle regole applicabili a nuove forme organizzative, apparentemente prive di un'autorità centrale e collettivamente controllate dagli utenti, come le cd. *Decentralized Autonomous Organizations* (DAO).

L'attribuzione di precise responsabilità agli sviluppatori di protocolli informatici (a esempio *smart contracts*)[14] e l'introduzione di presidi in materia di *governance* o *risk management* per le organizzazioni decentrate è una possibilità meritevole di considerazione. Restano inoltre fuori dell'ambito applicativo di MiCAR anche altri soggetti, quali a esempio gli *unhosted wallets*, *software* che abilitano allo scambio *peer to peer* tra utenti su DLT, che sollevano rischi *cyber* e di riciclaggio la cui diffusione può rendere più difficile il monitoraggio del fenomeno da parte delle Autorità.

Il nostro ruolo istituzionale rimane comunque quello di "monitorare" questo significativo cambiamento del sistema, individuando possibili casi di fallimento del mercato, mitigandone i rischi, senza pregiudicare l'innovazione. Sarà pertanto necessario continuare gli sforzi innanzitutto per comprendere i vantaggi per il sistema finanziario ed economico nel suo complesso che lo sviluppo di servizi finanziari su DLT può offrire, riconoscendo che al ricorre di alcune condizioni, il mercato può "internalizzare" o mitigare taluni rischi, grazie alle nuove tecnologie. Dobbiamo essere comunque pronti a intercettare in modo tempestivo eventuali nuove forme di rischio;

A tal fine, occorre rafforzare il "dialogo" esistente tra mercato e autorità anche nell'ambito degli *innovation facilitators,* cercando di preservare la necessaria apertura all'innovazione e il rispetto dei tempi assai stringenti che sono imposti dalla concorrenza internazionale.

---

[14] Questi ultimi normalmente negano l'assoggettamento a forme di responsabilità, sostenendo che la stessa sarebbe piuttosto da riferirsi all'intera base di utenti (pseudonimia).

Infine, è necessario monitorare l'interazione tra il modello di intermediazione tradizionale e quello decentralizzato, favorendo soluzioni tecnologiche robuste e sostenibili. A questo proposito, le sfide principali risiedono nell'identificazione del confine del perimetro regolamentare e nel come preservare la necessaria chiarezza sui profili di *governance* (chi è responsabile di che cosa, e come) in un mondo potenzialmente "atomistico".

L'innovazione mette infatti in discussione paradigmi di business, di supervisione e regolamentari, consolidati da decenni, come quello della vigilanza per soggetti. È richiesta pertanto un'intensa collaborazione tra le autorità coinvolte volti a monitorare i rischi in modo integrato e sfruttare sinergie informative e di competenze, per assicurare la necessaria coerenza di trattamento.

In conclusione, in questo contesto di rapido sviluppo della tecnologia si prospetta uno scenario inedito, in cui si integrano componenti finanziarie e tecnologiche, cosi come responsabilità di vigilanza prudenziale, su prodotti bancari e di investimento, sorveglianza sul sistema dei pagamenti (infrastrutture, prodotti, servizi), stabilità finanziaria, tutela del consumatore.

La Banca d'Italia continuerà a monitorare il mercato, in raccordo con le altre Autorità, e sarà pronta a intervenire, anche in anticipo rispetto alla definizione del quadro regolatorio europeo, attraverso la pubblicazione di specifiche indicazioni per gli utilizzatori, gli intermediari e i fornitori delle soluzioni tecnologiche in materia di *crypto*-attività.

Presterà inoltre particolare attenzione alla crescente integrazione dei profili di vigilanza prudenziale sugli intermediari finanziari, sui fornitori di funzioni critiche e di sorveglianza sul regolare funzionamento del sistema dei pagamenti connessi con le *crypto*-attività. Interverrà inoltre con tutti gli altri strumenti a sua disposizione per intercettare e prevenire potenziali minacce per la tutela degli utilizzatori e per la stabilità del sistema.

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