Verso un approccio attivo alle privacy stablecoins: il quadro per un'adozione scalabile e conforme ai requisiti KYC/AML

SINTESI NON TECNICA DELLO STUDIO

"ENGAGING WITH PRIVACY STABLECOINS: A FRAMEWORK FOR SCALABLE AND KYC/AML-COMPLIANT ADOPTION"

Michele Manna [†]

L'uso delle *stablecoin* è cresciuto rapidamente ma resta lontano dall'aver raggiunto un elevato livello di diffusione come strumento di pagamento al dettaglio. Affinché ciò avvenga, è necessario che lo strumento sia utilizzato nei pagamenti quotidiani, svolga la funzione di unità di conto e sia integrato nei bilanci delle famiglie e delle società.

Il primo contributo del lavoro è mostrare che il divario tra l'utilizzo corrente di questi strumenti e una loro ampia diffusione dipende da limiti strutturali, che non possono essere risolti con interventi marginali. In sintesi, ciò riflette il fatto che le *stablecoin* attualmente operanti al livello base delle blockchain (Layer-1, L1) non soddisfano le condizioni necessarie affinché il principio di *no-questions-asked* (NQA) possa operare su larga scala. In base a questo principio, uno strumento può diffondersi ampiamente se può essere accettato senza bisogno di effettuare verifiche approfondite, ossia "senza porsi domande".

Nel lavoro, il principio NQA è tradotto in termini operativi su larga scala se tre condizioni sono soddisfatte congiuntamente: la "scalabilità dimensionale", la "scalabilità normativa" e la "privacy delimitata" (*constrained privacy*). Attualmente, le *stablecoin* operanti al livello L1 delle blockchain non soddisfano alcuno di questi criteri.

La scalabilità dimensionale indica la capacità del sistema su cui si scambia lo strumento di mantenere livelli di efficienza adeguati anche in presenza di forti aumenti del numero di utenti e del volume delle transazioni. I dati mostrano che le blockchain a livello L1 sono in grado di elaborare un numero di transazioni per unità di tempo molto inferiore rispetto ai maggiori circuiti delle carte di credito, mentre i tempi di latenza sono più elevati.

Significato analogo ha il concetto di scalabilità normativa: la verifica dei requisiti normativi rilevanti, in primo luogo l'identificazione del cliente (*know-your-customer*, KYC), deve essere agevole, anche su ampi volumi. In realtà, nelle *stablecoin* utilizzate a livello L1 questi controlli richiedono laboriose attività di ricostruzione e analisi svolte ex post, con costi e tempi non accettabili se replicati su larga scala.

Infine, le *stablecoin* a livello L1 producono un equilibrio insoddisfacente sotto il profilo della privacy. Da un lato, il registro delle transazioni è pubblico e, seppur con tecniche non semplici, è possibile risalire all'identità degli utilizzatori. Allo stesso tempo, esistono forme di occultamento (*obfuscation*) incompatibili con la normativa applicabile agli intermediari vigilati. In questo ambito, la soluzione non può ricercarsi in meri miglioramenti tecnici degli attuali meccanismi di identificazione del cliente, bensì nello sviluppo di sistemi nei quali l'identificazione del cliente è integrata fin dall'origine.

[†] Unità di Informazione Finanziaria per l'Italia.

Il secondo contributo del lavoro consiste nel sostenere che le *stablecoin* operanti al livello 2 (Layer-2, L2) dell'architettura blockchain, se dotate di adeguati elementi di protezione della privacy fino a divenire "*privacy stablecoin*", appaiono in grado di offrire un'alternativa credibile. Con queste caratteristiche diventa infatti possibile soddisfare, almeno in linea di principio, le tre condizioni operative alla base del principio NQA. Il paper discute in dettaglio la possibilità che tale obiettivo possa essere effettivamente raggiunto, evidenziando anche alcuni limiti e rischi dell'attuale stato di sviluppo delle tecnologie in materia.

Nel condurre questo esame, pur mantenendo un linguaggio accessibile, il lavoro introduce alcuni elementi tecnici – tra cui le tecnologie di *zero-knowledge proof* (ZKP) – con l'obiettivo di offrire una base concettuale comune per policymaker, operatori dei mercati finanziari e soggetti attivi nello sviluppo di queste tecnologie.

Si sottolinea inoltre l'importanza, ai fini di un pieno rispetto del principio NQA, di superare il rischio di cambio, dato che le due *stablecoin* che attualmente coprono in misura preponderante il mercato sono entrambe ancorate al dollaro americano. Quindi, ulteriore condizione per un ampio sviluppo delle *stablecoin* nei pagamenti al dettaglio è la disponibilità di strumenti di questa categoria denominati anche nelle altre valute principali.

L'effettiva attuazione del principio NQA – e quindi delle condizioni operative di scalabilità dimensionale, scalabilità normativa e privacy delimitata – dipenderà in modo critico dalle prossime evoluzioni della tecnologia. L'innovazione in questo ambito sta avanzando rapidamente, ma il percorso tecnologico resta aperto a esiti differenti. Alla luce dell'ampio spettro di soluzioni tecniche possibili e della complessità nel combinare elementi spesso molto sofisticati, è possibile, ma tutt'altro che certo, che le *privacy stablecoin* realizzino il loro potenziale nel senso sopra indicato. Inoltre, non va sottovalutato il rischio di errori nello sviluppo di sistemi complessi, in particolare nelle tecnologie ZKP, che potrebbero compromettere il raggiungimento dei risultati attesi.

In effetti, non vi è garanzia che le forze di mercato, lasciate operare in totale autonomia, convergeranno spontaneamente verso soluzioni che concilino elevati livelli di innovazione tecnologica con un pieno rispetto della normativa. È plausibile che prevalga la ricerca di un equilibrio tra rispetto degli obblighi normativi e preferenze degli utenti, senza che tale equilibrio coincida necessariamente con il pieno perseguimento di tutti gli obiettivi regolamentari.

Si pone quindi un classico problema di coordinamento: non vi è garanzia che le forze di mercato da sole convergano verso architetture pienamente in linea con i requisiti posti dalle autorità. Se queste ultime adottassero un approccio del tutto passivo, nel tempo potrebbero consolidarsi equilibri subottimali, che amplierebbero lo spazio per attività di riciclaggio.

Il lavoro conclude sottolineando l'importanza di un ruolo attivo di coordinamento da parte delle autorità, che potrebbero promuovere il dialogo con sviluppatori, intermediari e partecipanti al mercato, al fine di favorire uno sviluppo delle innovazioni coerente sia con le esigenze del settore privato sia con quelle del settore pubblico.