Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Conferenza stampa annuale del 27 marzo 2018

Mark Branson, Direttore

Tecnologia e settore finanziario: opportunità e rischi

Gentili Signore, egregi Signori,

nel mio intervento odierno affronterò il tema della tecnologia, passando in rassegna sia le opportunità che i rischi connessi. Le parole chiave sono ormai note: *blockchain*, ICO, *big data*, rischi cibernetici, eccetera. Ma quali sono le implicazioni più profonde di queste parole a effetto?

Alla luce dell'attuale scenario caratterizzato da bassi tassi d'interesse, scarsa redditività e nuovi modelli di comportamento dei clienti, l'innovazione si profila come una questione fondamentale, si potrebbe quasi dire esistenziale per il settore finanziario.

L'innovazione non può essere imposta dallo Stato, è anzi principalmente un compito demandato al settore finanziario. In veste di autorità di vigilanza vogliamo tuttavia garantire che il dispositivo normativo renda possibile questo processo di innovazione. Ciò non deve avvenire attraverso una politica strutturale camuffata; si tratta piuttosto di abbattere le attuali barriere di accesso al mercato e di promuovere una concorrenza «sana».

Apertura nei confronti dell'innovazione non è però sinonimo di ingenuità. La digitalizzazione e l'innovazione finanziaria generano nuovi rischi oppure rischi già noti sotto una nuova veste. Il nostro compito come autorità di vigilanza è quello di individuare questi rischi, monitorarli e, se necessario, contenerli. Penso per esempio ai rischi di riciclaggio di denaro nell'ambito del sistema *blockchain*, ai rischi di perdita a cui sono esposti gli investitori nelle ICO e, in particolare, anche alla minaccia comportata dai rischi cibernetici.

La promessa della tecnofinanza

Ma iniziamo dall'approfondire il tema delle opportunità offerte dalla tecnofinanza. Sul mercato sta sbarcando un ampio ventaglio di prodotti e applicazioni. I progetti sono finanziati attraverso il *crowd*, il denaro viene trasmesso attraverso gli smartphone, nuove fasce di popolazione nei Paesi emergenti ottengono l'accesso ai servizi finanziari e i robot assumono decisioni d'investimento.

Riconosciamo il formidabile potenziale offerto dalla tecnofinanza e dalla tecnologia *blockchain* per la piazza finanziaria. In questo ambito si profila anche un ruolo specifico per noi in veste di autorità di vigilanza: vogliamo rendere possibile l'innovazione, come peraltro abbiamo avuto modo di dimostrare in

Laupenstrasse 27
3003 Berna
Tel. +41 (0)31 327 91 00
Fax +41 (0)31 327 91 01
www.finma.ch

b1004961-0000559

ripetute occasioni. Nella fattispecie, definiamo con coerenza la nostra regolamentazione a valle mediante un orientamento improntato al principio della neutralità tecnologica, senza quindi operare distinzioni tra il canale digitale e quello analogico. Inoltre, la FINMA ha originariamente lanciato l'idea della *sandbox* e quella della licenza *fintech*. Inoltre, nei limiti del possibile, abbiamo fornito ai gestori delle ICO anche un supporto orientativo.

Il nostro obiettivo è fare in modo che gli innovatori diano vita a una concorrenza sana, a fronte di una contestuale tutela dell'integrità della piazza finanziaria. La nostra apertura nei confronti dell'innovazione è infatti pari alla risolutezza con cui procediamo per contrastare la criminalità finanziaria.

Blockchain: euforia collettiva o motore dell'innovazione?

La *blockchain* è una tecnologia elettrizzante. Per esempio, è ipotizzabile che, un giorno, alcuni aspetti dell'attuale struttura dei mercati finanziari diventino obsoleti – a tale proposito si rivela quanto mai attuale la profezia pronunciata da Bill Gates nel 1994, secondo cui *«Banking is essential, banks are not»*.

Questa tecnologia viene già ampiamente utilizzata nel contesto delle criptovalute e delle ICO. Le *initial coin offering* si sono evolute in un brevissimo arco di tempo da un metodo di finanziamento pressoché sconosciuto a un vero e proprio magnete di capitali, che solo nel 2017 ha consentito di raccogliere in tutto il mondo oltre sei miliardi di dollari. Quattro delle sei maggiori ICO sono state effettuate in Svizzera, la quale si è affermata come un importante *hub* per questo tipo di operazioni. Non sorprende quindi che la FINMA sia chiamata a gestire un gran numero di richieste afferenti a tale ambito. Abbiamo tratto spunto da questo fenomeno per fissare in un'apposita guida pratica le modalità con cui le domande vengono trattate sulla base delle leggi attualmente vigenti in materia di mercati finanziari.
I primi riscontri su questo approccio sono stati positivi, e ciò è stato accolto positivamente dagli offerenti che operano con serietà. Essi sanno che un *playground* di stampo anarchico su vasta scala resterà sempre un'utopia.

Nonostante il clima di grande fermento a tratti imperante, non va però dimenticato che le criptovalute sono rischiose. Ai nostri occhi, un approccio totalmente libertario appare fuori luogo. Le oscillazioni di valore di questi strumenti sono estreme; inoltre, spesso i rischi non vengono spiegati a dovere ai clienti delle ICO. In molti casi sono disponibili soltanto informazioni perlopiù approssimative su progetti sovente ancora molto acerbi. Al pari degli altri investimenti nelle *start-up*, il rischio di perdita è considerevole. Sussiste inoltre un certo potenziale per il riciclaggio di denaro. Molti offerenti di criptovalute fanno infatti leva proprio sulla loro scarsa trasparenza e anonimità. E, non da ultimo, le sedi di negoziazione delle criptovalute sono state prese di mira da ripetuti attacchi di hacker, con danni dell'ordine delle centinaia di milioni di dollari. Alla luce di queste argomentazioni, siamo fautori di un approccio semplice: le ICO relative a *token* di pagamento o a criptovalute sottostanno alla Legge sul riciclaggio di denaro, mentre le ICO che offrono possibilità d'investimento devono essere trattate alla stregua dei valori mobiliari.

Cyber-rischi: aspettative della FINMA

Partendo dalla parola chiave «attacco di *hacker*» vorrei ora passare al tema che concerne i rischi cibernetici e gli istituti finanziari. Proprio questi ultimi costituiscono infatti uno degli obiettivi prediletti dai

pirati informatici, che ben si presta anche ad altri attacchi cibernetici. Non a caso, le più recenti statistiche della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI indicano che due terzi degli attacchi a infrastrutture di rilevanza critica colpiscono il settore finanziario.

Il rischio di tali aggressioni aumenta di pari passo con la crescente digitalizzazione. Gli attacchi cibernetici sono nel frattempo diventati il maggiore rischio operativo per il settore finanziario. Noi – e intendo sia il settore privato che le autorità – siamo quindi chiamati ad affrontare questo tema con serietà. In linea di principio abbiamo constatato che la sensibilità degli assoggettati nei confronti di questo argomento è elevata e che, in media, essi sembrano essere ben preparati. Ogni giorno vengono parati molteplici attacchi. Per esempio, attualmente ogni giorno in Svizzera vengono individuati fino a cento attacchi a operazioni di e-banking sferrati dal malware Retefe.

Tuttavia, anche il miglior sistema di difesa è efficace quanto il suo anello più debole. Per esempio, dopo essersi infiltrati nella banca centrale del Bangladesh, gli *hacker* sono riusciti a ottenere l'accesso al sistema dei pagamenti internazionali Swift. In Svizzera è stato recentemente sottratto un elevato volume di dati dei clienti presso una cassa malati.

Che cosa si attende la FINMA alla luce di questi rischi? A livello centrale, che gli istituti finanziari siano consapevoli della propria vulnerabilità. Un efficace strumento a tale riguardo è costituito dal cosiddetto *penetration testing*. Altrettanto importante è la capacità di reazione in caso di attacco cibernetico. In caso di attacco, occorre ripristinare l'operatività nel più breve tempo possibile. Ogni istituto è quindi chiamato a mettere a punto un proprio efficace dispositivo da attuare in caso di crisi e a garantirne il buon funzionamento.

I rischi sono tuttavia di portata di gran lunga superiore ai semplici furti di denaro o di dati. Attacchi mirati, magari sferrati perfino da organizzazioni terroristiche oppure da enti statali o parastatali, potrebbero assumere una dimensione sistemica. Sebbene, nel confronto internazionale, gli istituti finanziari svizzeri godano di un buon posizionamento, constatiamo che, nella protezione del sistema nel suo complesso, l'azione della Svizzera è meno incisiva rispetto a quella di altri Paesi. I Paesi che ospitano importanti piazze finanziarie si adoperano in tal senso con maggiore efficacia, per esempio istituendo centri di competenza in ambito cibernetico o svolgendo *penetration test* capillari. Anche la Svizzera dovrebbe mettere a punto un monitoraggio sistematico e definire i processi corrispondenti; in questo frangente la FINMA è disposta ad assumere un ruolo di rilievo. Abbiamo infatti arricchito in modo mirato il nostro organico con specialisti in questo settore e non siamo restii a operare ulteriori investimenti in tal senso.

Il Consiglio consultivo per il futuro della piazza finanziaria, sotto la guida del Prof. Brunetti, ha formulato tre importanti raccomandazioni concernenti la sicurezza cibernetica della piazza finanziaria svizzera, alle quali l'opinione pubblica ha dato, a torto, scarso riscontro.

Innanzitutto, è necessario ampliare l'accesso a MELANI, anche per i piccoli istituti finanziari in Svizzera. Secondo, deve essere istituzionalizzata e migliorata la collaborazione in materia di cyber-sicurezza tra gli specialisti dell'industria finanziaria e le autorità. Non esiste praticamente nessun altro ambito in cui gli interessi del settore privato e delle istanze di vigilanza siano tanto allineati come nella lotta contro i rischi cibernetici. Terzo, occorre mettere a punto e sottoporre a test un dispositivo per la sicurezza cibernetica specifico al settore finanziario da attuare in caso di crisi.

La FINMA sostiene espressamente le raccomandazioni del Consiglio consultivo per il futuro della piazza finanziaria e collabora in maniera attiva. Unendo le forze possiamo ottenere molto di più che agendo da soli. In questa circostanza la Svizzera non sta certo con le mani in mano, ma altri Paesi fanno nettamente di più.

Una forte concentrazione come conseguenza dell'*outsourcing*

Le cyberminacce sono in parte intensificate dal fenomeno di crescente esternalizzazione dei processi operativi e delle infrastrutture informatiche.

Gran parte delle banche svizzere ha esternalizzato campi di attività essenziali. Talvolta gli istituti bancari cedono in *outsourcing* la totalità dei loro processi di *back-office*, sviluppo che pone anche la vigilanza di fronte a numerose sfide.

In Svizzera constatiamo in particolare una forte concentrazione presso alcuni operatori, ai quali molte banche hanno ceduto in *outsourcing* i propri servizi. Anche per questi soggetti applichiamo quindi gli stessi parametri impiegati per gli istituti finanziari. Dal 2016 disponiamo delle basi giuridiche che ci consentono di intervenire in loco e di sottoporre a verifica i partner degli istituti finanziari in materia di esternalizzazione. Presso tali fornitori di servizi abbiamo infatti già effettuato vari controlli in loco e continueremo in modo sistematico su questa linea.

Cogliere le opportunità, individuare i rischi

La tecnologia finanziaria offre un potenziale formidabile. In veste di autorità di vigilanza, faremo tutto quanto in nostro potere per consentire un'innovazione nel settore finanziario fondata sul principio della serietà. Saranno poi il mercato e i clienti, e non le condizioni quadro a livello normativo, a decidere se le varie applicazioni sono in grado di mantenere le proprie promesse. È questo il filo conduttore del nostro operato.

Il criptomondo è un coacervo di innovatori, ma anche di impostori, arbitraggisti in ambito regolamentare e truffatori. In collaborazione con le autorità partner, il nostro compito è quello di dare agli innovatori che operano con serietà la possibilità di portare a termine con successo i propri progetti, di contrastare le attività di arbitraggio e di infliggere ai truffatori la punizione che meritano. Sia le opportunità che i rischi connessi alle nostre tecnologie richiedono tutta la nostra attenzione e il nostro impegno.

Vi ringrazio per la vostra attenzione.