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

Comunicazione FINMA sulla vigilanza 08/2023

Staking

20 dicembre 2023

Laupenstrasse 27, 3003 Berna, tel. +41 (0)31 327 91 00, www.finma.ch

Indice

1 Introduzione

L'entrata in vigore del progetto della legge TRD ha creato in particolare anche una base legale per la custodia di beni crittografici, che protegge i clienti in caso di insolvenza del depositario. A fronte della crescente rilevanza dei cosiddetti servizi di *staking*, la FINMA ha dovuto rispondere a sempre più domande sull'utilizzo di queste disposizioni sulla custodia per le offerte di *staking*. A seconda dell'assetto del servizio di *staking* è possibile che i requisiti del progetto TRD non siano soddisfatti e che i valori patrimoniali non godano della protezione dall'insolvenza in caso di insolvenza del depositario.

L'attualità delle questioni tematizzate è aumentata soprattutto attraverso il passaggio dalla *blockchain* Ethereum a un meccanismo di consenso *proof of stake*, il cambiamento della situazione macroeconomica e l'adeguamento dei tassi d'interesse, accentuando così la necessità di intervento. Al fine di sensibilizzare i partecipanti al mercato sul tema dello *staking*, la FINMA ha discusso l'argomento con i rappresentanti del settore nel quadro di tavole rotonde. Inoltre, presso vari istituti assoggettati ha effettuato un sondaggio sui loro servizi di *staking*.

Con la presente Comunicazione sulla vigilanza la FINMA informa in merito all'esito della discussione relativa all'inquadramento secondo la regolamentazione in materia di mercati finanziari dei servizi di *staking* per i clienti. Al riguardo l'enfasi è posta sulla precisazione dell'interpretazione della legge per quanto riguarda la distinzione tra valori depositati protetti in caso di fallimento e depositi esposti al rischio d'insolvenza, i relativi obblighi di autorizzazione ai sensi del diritto bancario e gli effetti sulle esigenze di capitalizzazione per gli istituti autorizzati.

2 *Staking*

2.1 Descrizione

Finora non sussiste alcuna comprensione unitaria del termine *staking*. La FINMA definisce lo *staking* come la procedura di blocco di beni crittografici nativi sull'indirizzo di *staking* di un nodo validatore per partecipare al processo di convalida di una *blockchain* basata su un meccanismo di consenso *proof of stake*. Quale ricompensa per lo *staking* di beni crittografici, gli operatori partecipano attraverso cosiddette ricompense di *staking (staking-rewards)*.

Le *blockchain* basate sul meccanismo di *proof of stake* si differenziano tra di loro in quanto il processo inverso di sblocco *(unstaking)* include a volte un periodo di *lock-up/exit* (variabile) che comporta un ritardo nel riscatto dei

beni crittografici bloccati. Inoltre, le *blockchain* creano a volte anche incentivi negativi ai fini di un'attività di convalida conforme alle regole, dato che i beni crittografici bloccati a favore dello *staking* possono essere di norma soggetti a cancellazione parziale o completa *(slashing)* in caso di comportamento illecito da parte di un nodo validatore.

2.2 Varianti

Nella pratica si sono attestate diverse varianti di *staking*. Agli scopi della presente Comunicazione sulla vigilanza si opera una distinzione tra le seguenti configurazioni:

- ***Custodial staking***: nel caso del *custodial staking* il cliente trasferisce i beni crittografici a terzi. Il *custodial staking* comprende entrambe le varianti di *direct staking* e della catena di *staking:*
  - ***Direct staking***: nel *direct staking* il fornitore di servizi gestisce direttamente il nodo validatore oppure esternalizza la gestione affidandola a un fornitore di servizi tecnici, ma conserva però almeno le chiavi di prelievo (*withdrawal keys*) per il riscatto dei beni crittografici del cliente detenuti in *staking*.
  - **Catena di *staking***: in una catena di *staking* i beni crittografici da mettere in *staking* vengono inoltrati dall'istituto con la relazione d'affari a uno o più terzi, i quali gestiscono il nodo validatore e detengono le chiavi di prelievo (*withdrawal keys*).
- ***Non-custodial staking*:** nel *non-custodial staking*, i clienti mantengono il controllo esclusivo sulle chiavi di prelievo (*withdrawal keys*), motivo per cui non ha luogo alcuna custodia o accettazione di valori patrimoniali da parte di terzi.

2.3 Rischi

L'utilizzo di servizi di *staking* comporta diversi rischi:

- Rischio tecnico di un malfunzionamento della procedura di *staking*; inoltre sussiste il rischio di *slashing* di beni crittografici in seguito a un comportamento illecito del nodo validatore; le sanzioni possono anche sorgere automaticamente nel caso in cui il nodo validatore per esempio si disconnette a causa di problemi tecnici o della mancanza di sufficienti misure di Business Continuity Management.
- Rischio di controparte a fronte della situazione giuridica poco chiara in caso di fallimento; in Svizzera vige attualmente un'incertezza giuridica per quanto riguarda il trattamento secondo il diritto in materia di fallimento di beni crittografici detenuti in *staking* in determinate situazioni (vedi capitolo 3.2). Questa incertezza giuridica sussiste ancor più se la custodia o lo *staking* vengono delegati a istituti esteri, dato che all'estero

spesso il trattamento secondo il diritto fallimentare dei beni crittografici non è disciplinato in modo specifico.

- Rischio di mercato, considerato che in una fase di volatilità potrebbe non essere possibile vendere al momento giusto i beni crittografici detenuti in *staking*, se il processo di sblocco *(unstaking)* include un periodo di *lock-up*/*exit* che comporta un ritardo nel riscatto dei beni crittografici bloccati. Per determinate *blockchain* come Ethereum il periodo di *lock-up* è più lungo se il numero di ordini di sblocco *(unstaking)* aumenta, motivo per cui in caso di crisi possono verificarsi periodi di *lock-up* molto lunghi e un'impossibilità tecnica temporanea di vendere i beni crittografici. La durata del periodo di *lock-up* è a volte poco trasparente e imprevedibile per i clienti a causa della costante variazione della coda di prelievo (*withdrawal-queue*) e del numero di validatori.

3 Trattamento prudenziale

3.1 Base per la custodia di beni crittografici

Dal 1° agosto 2021 è entrato integralmente in vigore il progetto della legge TRD. Il nuovo art. 242*a* LEF ha creato una base legale per la custodia sicura in caso di fallimento di beni crittografici. Il grafico seguente illustra le condizioni che devono essere soddisfatte per una rivendicazione in caso di fallimento del depositario (*Aussonderung*).

Trattamento secondo il diritto in materia di fallimento (art. 242*a* cpv. 2 LEF):

In linea con questa regolamentazione sancita dal diritto in materia di fallimento, nell'ambito del progetto della legge TRD è stata aggiunta nell'art. 16 n. 1bis LBCR anche una disposizione congruente per gli istituti ai sensi del diritto bancario. L'art. 16 LBCR descrive i cosiddetti "valori depositati", i quali ai sensi dell'art. 37*d* LBCR vengono separati dalla massa fallimentare a favore dei clienti deponenti (*Absonderung*). La separazione mira a un trattamento preferenziale dei valori che figurano nell'estratto conto dei clienti deponenti e che non vengono tenuti nei libri contabili della banca.

Queste disposizioni sono rilevanti anche ai fini della valutazione di eventuali obblighi di autorizzazione secondo il diritto bancario. Dall'entrata in vigore del progetto della legge TRD, oltre all'accettazione a titolo professionale di depositi del pubblico, è soggetta ad autorizzazione anche l'accettazione esplicita a titolo professionale di mezzi di pagamento crittografici (token di pagamento) detenuti in custodia collettiva ai sensi dell'art. 5*a* OBCR.

Trattamento ai sensi del diritto bancario (artt. 1*a* e 1*b* LBCR in combinato disposto con gli artt. 5 e 5*a* OBCR):

La custodia di token di pagamento su un conto collettivo con quote dei clienti chiaramente indicate richiede un'autorizzazione ai sensi del diritto bancario. Per questo tipo di custodia basta un'autorizzazione fintech conformemente all'art. 1*b* LBCR, a condizione che i token di pagamento siano messi a disposizione in ogni momento. Nessuna autorizzazione ai sensi del diritto bancario comporta, invece, la custodia individuale di token di pagamento che sono messi a disposizione in ogni momento. Tuttavia, tali depositari si qualificano come intermediari finanziari ai sensi della LRD che devono affiliarsi a un organismo di autodisciplina per la vigilanza in materia di lotta contro il riciclaggio di denaro.

Per le banche si pone inoltre la questione concernente quali beni crittografici custoditi debbano essere iscritti a bilancio come depositi del pubblico e quali possano essere tenuti fuori bilancio come valori depositati. Questa domanda è importante perché i valori patrimoniali iscritti a bilancio devono soddisfare requisiti prudenziali.

Registrazione contabile e requisiti prudenziali:

La qualifica come valori depositati fuori bilancio presuppone tassativamente che i beni crittografici vengano *messi in ogni momento a disposizione del cliente*. Se i beni crittografici non vengono messi a disposizione del cliente in ogni momento, nel caso dei token di pagamento si configurano depositi del pubblico da iscrivere a bilancio, i quali comportano ulteriori esigenze di capitalizzazione. Per la custodia collettiva di beni crittografici è inoltre necessario, ai fini della qualifica di valori depositati, che le quote dei clienti deponenti del patrimonio comune siano chiaramente determinate (per esempio tramite un registro interno che assegni chiaramente i beni crittografici ai rispettivi clienti e ne consenta la rivendicazione in caso di fallimento).

3.2 Applicabilità allo *staking*

In relazione ai servizi di *staking* si pongono diverse questioni d'interpretazione in merito alle disposizioni di custodia esposte. La maggior parte ruota attorno all'elemento costitutivo della fattispecie centrale per la protezione in caso di fallimento, in base al quale i beni crittografici devono essere tenuti a disposizione del cliente in ogni momento.

Questo elemento costitutivo della fattispecie non è soddisfatto se il depositario gestisce lo *staking* per proprio conto. Per situazioni di questo genere occorre presupporre un'operazione per proprio conto ai sensi dell'art. 1*a* lett. *b* LBCR. Di conseguenza, tali beni crittografici del depositario detenuti in *staking* per proprio conto non possono essere rivendicabili o separabili in caso di fallimento e sono soggetti a esigenze di capitalizzazione.

La situazione giuridica è incerta quando lo *staking* viene gestito a nome e per conto del cliente. In tali configurazioni la valutazione dello specifico meccanismo di *staking* della *blockchain* interessata deve essere effettuata caso per caso.

In linea di principio, da una prospettiva della protezione in caso di fallimento non presentano problemi le *blockchain* che non prevedono né un periodo di *lock-up,* né un meccanismo di sanzione *(slashing)* per lo *staking*. Senza periodi di *lock-up*, uno *slashing* o analoghe restrizioni del potere di disporre, i

beni crittografici sono a disposizione del cliente in ogni momento e sono quindi in genere rivendicabili o separabili.

Il messaggio sul nuovo art. 242*a* LEF afferma: «Concretamente ciò significa che, dal momento in cui il terzo gli ha trasmesso il potere di disporre dei beni o dal momento in cui ha acquisito il potere di disporre dei beni per conto del terzo, il fallito è tenuto ad avere ininterrottamente il potere di disporre (ai sensi del cpv. 1) dei beni; per adempiere tale obbligo è tuttavia sufficiente che il fallito possieda ininterrottamente il numero di unità custodite per conto del terzo. In altre parole, il fallito può sostituire singoli token, a condizione che il loro numero totale non sia inferiore a quello necessario per soddisfare in qualsiasi momento l'avente diritto».[1]

Se i beni crittografici custoditi nel quadro del servizio di *staking* sono soggetti a un rischio di *slashing* e/o a un ritardo nello sblocco o *unstaking* (periodo di *lock-up/exit*), l'offerente conserva il potere di disporre delle chiavi di prelievo (*withdrawal keys*), ma è tuttavia controverso se secondo il messaggio del Consiglio federale è possibile sostenere che la restituzione dei beni crittografici custoditi possa essere garantita all'avente diritto in qualsiasi momento. È pertanto discutibile se sia ottemperata la condizione della disponibilità in ogni momento ai sensi dell'art. 242*a* cpv. 2 LEF e dell'art. 16 n. 1bis LBCR. Al riguardo sussiste *de lege lata* un'incertezza giuridica.

Il requisito della disponibilità in ogni momento è il risultato della norma speciale specifica per la tecnologia dell'art. 242*a* cpv. 2 LEF e dell'art. 16 n. 1bis LBCR, che a causa delle circostanze al momento del progetto di legge è definito in base alla fattispecie della custodia e non dello *staking*. Finora non sussiste né una giurisprudenza pertinente, né una prassi rilevante dei tribunali fallimentari per stabilire se i beni crittografici detenuti in *staking* su *blockchain* con periodi di *lock-up* e/o *slashing* soddisfino ancora l'elemento costitutivo della fattispecie della disponibilità in ogni momento. Non esistono nemmeno raccomandazioni internazionali concernenti il trattamento dello *staking.*

4 Conseguenze giuridiche

4.1 *Staking* da parte di istituti autorizzati

4.1.1 Catena di *staking*

Se un istituto delega a terzi (altre banche o operatori di *staking* pool) la gestione del nodo validatore nel quadro della catena di *staking*, dal punto di

[1] Messaggio del 27 novembre 2019 concernente la legge federale sull'adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito, FF **2020** 221 p. 279, consultabile all'indirizzo: https://www.fedlex.admin.ch/eli/fga/2020/16/it.

vista contabile l'istituto ha un credito nei confronti di questa controparte dell'istituto autorizzato (di seguito denominato «offerente terzo»). Tale credito può essere iscritto a bilancio come credito nei confronti dell'offerente terzo oppure, se sono soddisfatte determinate condizioni, come credito fiduciario custodito ai sensi dell'art. 16 n. 2 LBCR e dunque trattato come valore depositato.

La qualifica di credito detenuto a titolo fiduciario presuppone un'applicazione analoga delle direttive di Swissbanking sugli investimenti fiduciari, adeguate ai rischi dei beni crittografici, al fine di escludere una negligenza grave da parte dei depositari nei confronti dei loro clienti. Questa precisazione è necessaria per tenere conto dei rischi specifici dello *staking*.

L'accettazione di un tale rapporto fiduciario in relazione allo *staking* presupporrebbe pertanto almeno un accordo fiduciario con uno specifico mandato fiduciario da parte del cliente nonché la relativa scelta dei beni crittografici e dell'importo, che comprende un'informativa approfondita sui rischi del cliente in relazione all'incarico di *staking* (in particolare *slashing* e periodo di *lock-up*) e che sia conforme agli altri obblighi delle direttive.

L'istituto deve nello specifico:

- limitare i rischi di controparte selezionando un istituto assoggettato a vigilanza prudenziale con una buona solvibilità oppure un'affiliata di un gruppo finanziario consolidato e assoggettato a vigilanza prudenziale con una buona solvibilità; nonché
- tramite una specifica *due diligence* accertarsi che:
  - l'offerente terzo non operi senza autorizzazione;
  - l'offerente terzo detenga direttamente le chiavi di prelievo (*withdrawal keys*), escludendo così catene di *staking* più lunghe. Se l'offerente terzo intende coinvolgere un altro fornitore di servizi, nel singolo caso occorre verificare se le misure di mitigazione adottate (come per esempio la firma in via preliminare *[pre-signing]* della transazione di riscatto) hanno un effetto equiparabile;
  - l'offerente terzo deve designare gli indirizzi dei validatori (per esempio mediante un registro interno) in cui detiene i beni crittografici dei depositari e li comunica al depositario;
  - l'offerente terzo adotti tutte le misure necessarie al fine di limitare i rischi operativi in relazione alla gestione del nodo validatore (errori di convalida o stato offline), per escludere ulteriori sanzioni nei confronti del validatore e garantire la continuità operativa; e
  - se sono coinvolti offerenti terzi all'estero, oltre ai requisiti precedentemente menzionati, tali offerenti devono essere assoggettati a vigilanza prudenziale in una giurisdizione regolamentata in modo equivalente, in cui sussista la stessa certezza del diritto come in Sviz-

zera relativamente al trattamento secondo il diritto in materia di fallimento dei beni crittografici custoditi, nonché essere soggetti a una *due diligence* specifica, che includa i punti sovraesposti per gli offerenti nazionali.

- sia allestito un *Digital Asset Resolution Package* (DARP) ai fini di una gestione dei rischi adeguata, che venga regolarmente aggiornato e:
  - contenga le informazioni più importanti necessarie per l'identificazione e la garanzia immediata dei beni crittografici (p.es. descrizione del tipo di custodia, informazioni sulle persone di contatto con accesso alle private keys, informazioni su depositari terzi, ecc.);
  - garantisca che, in caso di fallimento, il liquidatore possa versare rapidamente i beni crittografici ai clienti, in modo da ridurre al minimo il dispendio e i costi per una restituzione ordinata.

4.1.2 *Direct staking*

Nel *direct staking* un istituto gestisce di norma direttamente lo *staking* e ha anche il potere di disporre delle chiavi di prelievo (*withdrawal keys*) per il riscatto dei beni crittografici bloccati. È dunque esclusa una separazione di cui all'art. 16 n. 2 LBCR.

Come menzionato nel capitolo 3.2, sussiste un'incertezza giuridica relativa al fatto se sia ottemperata la condizione della disponibilità in ogni momento ai sensi dell'art. 242*a* cpv. 2 LEF e dell'art. 16 n. 1bis LBCR.

A causa della situazione giuridica poco chiara, la FINMA rinuncia per il momento a richiedere alle banche di soddisfare le esigenze di capitalizzazione relativamente ai beni crittografici detenuti in *staking*; a condizione che (cumulativamente):

- sia disponibile un'istruzione specifica del cliente in merito al tipo e al numero di beni crittografici da mettere in *staking*;
- sia garantito attraverso misure idonee che i beni crittografici collocati su un determinato indirizzo del validatore e dopo lo sblocco *(unstaking)* su uno specifico indirizzo di prelievo (*withdrawal-address*) possano essere assegnati in maniera univoca ai clienti aventi diritto;
- i clienti siano informati in modo trasparente e univoco in merito a tutti i rischi (compresi lo *slashing*, il periodo di *lock-up* e i rischi legati alle incertezze del diritto esistenti in caso di fallimento);
- siano adottate misure appropriate per ridurre i rischi operativi derivanti dalla gestione di un nodo validatore (compreso il Business Continuity Management), in particolare per evitare *slashing* e altre sanzioni; e
- sia allestito un *Digital Assets Resolution Package* (DARP) ai fini di una gestione dei rischi adeguata, che venga regolarmente aggiornato (per il contenuto vedi capitolo 4.1.1).

Se questi requisiti sono soddisfatti, in caso di fallimento di un istituto assoggettato alla vigilanza della FINMA i beni crittografici detenuti in *staking* secondo l'attuale valutazione della FINMA devono essere separati dalla massa fallimentare a favore dei clienti deponenti ai sensi dell'art. 37*d* LBCR in combinato disposto con l'art. 16 n. 1bis LBCR.

Questa prassi è valida solo provvisoriamente, fino a quando non sarà stato effettuato un chiarimento normativo, oppure sarà disponibile una sentenza del tribunale o si verificheranno sviluppi internazionali, comportando così una nuova valutazione dell'interpretazione.

4.2 *Direct staking* da parte di partecipanti al mercato non autorizzati

Per i partecipanti al mercato non autorizzati, fatte salve le stesse riserve relative a chiarimenti legislativi, sentenze dei tribunali o sviluppi internazionali, in linea di principio la FINMA non si assume alcun obbligo di autorizzazione ai sensi del diritto bancario nel caso del *custodial direct staking* a nome e per conto dei clienti. Ciò si configura se i token di pagamento detenuti in *staking* vengono tuttora custoditi individualmente presso il *direct staking*, ossia sussiste un indirizzo *blockchain* separato e chiaramente assegnabile per ogni cliente (a livello di indirizzo di custodia iniziale, dell'indirizzo di *staking* e dell'indirizzo di prelievo [*withdrawal address*]) e l'offerente dispone direttamente delle chiavi di prelievo (*withdrawal keys*). Il depositario deve tuttavia affiliarsi a un organismo di autodisciplina per la vigilanza in materia di lotta contro il riciclaggio di denaro.

Occorre tenere presente che lo *staking* a volte presuppone un importo minimo di beni crittografici (per esempio 32 ETH per Ethereum). Questo ammontare è regolarmente fissato a un livello elevato per incentivare i validatori a comportarsi secondo le regole. Di conseguenza, i beni crittografici di diversi clienti sono spesso riuniti su un unico indirizzo di *staking* in modo tale da raggiungere tale importo, in particolare per le offerte destinate ai piccoli investitori. In questo senso, l'offerta di servizi di *staking* implica di frequente la custodia collettiva di token di pagamento e dunque un'autorizzazione ai sensi del diritto bancario.

5 Glossario

Digital Assets Resolution Package **(DARP)**	Istruzioni operative interne per informare un liquidatore in merito alle responsabilità e alle possibilità di accesso in caso di fallimento di una banca che custodisce beni crittografici
Direct staking	L'istituto gestisce direttamente lo *staking* e pertanto ha il potere di disporre delle chiavi di prelievo *(withdrawal keys)*.
Custodia individuale	Custodia segregata di beni crittografici su indirizzi *blockchain* individuali per ogni cliente
Beni crittografici	Valori patrimoniali digitali gestiti su una *blockchain* e di cui si può disporre solo con l'ausilio di una procedura di accesso crittografica composta da una chiave pubblica *(public key)* e una chiave privata *(private key)*
Periodo di *lock-up/exit*	Durata minima dello *staking* prima che i beni crittografici possano essere sbloccati e/o durata tra la deposizione dell'ordine di sblocco *(unstaking)* e l'effettivo riscatto dei beni crittografici detenuti in *staking*
Custodia collettiva	Custodia segregata di beni crittografici su un indirizzo *blockchain* comune
Slashing	Procedura in cui i beni crittografici detenuti in *staking* vengono di norma eliminati totalmente o parzialmente a causa di un comportamento illecito del validatore
Gestore di *staking (pool)*	Le convalide in blocco vengono effettuate con beni crittografici economicamente di terzi per conto di terzi. Se il validatore utilizza congiuntamente i beni crittografici di diversi clienti, si parla di *staking pool.*
Catena di *staking*	L'istituto delega la responsabilità dello *staking* nel quadro di una catena di *staking* a un offerente terzo che assume il potere di disporre delle chiavi di prelievo (*withdrawal keys*) (altre banche o operatori di *staking pool*).
Fornitore di servizi tecnici	Responsabile delle impostazioni tecniche (componenti hardware e software) per la produzione in blocco. Il fornitore di servizi ha un rapporto solo con il validatore, ma non con i clienti dello *staking.*
Gestore del nodo validatore	Gestore diretto di un nodo validatore della *blockchain* – come gestore di *staking (pool)* o fornitore di servizi tecnici

Chiavi di prelievo (*withdrawal keys*)	Chiavi crittografiche per controllare il riscatto dei beni crittografici detenuti in *staking*; la perdita di queste chiavi comporta anche la perdita dei beni crittografici detenuti in *staking*
Token di pagamento / criptovalute	Beni crittografici che sono impiegati a tutti gli effetti o nelle intenzioni dell'organizzatore o dell'emittente come mezzo di pagamento per l'acquisto di beni o servizi oppure per il trasferimento di denaro o valori (vedi in merito anche l'art. 5*a* cpv. 1 OBCR e la Guida pratica ICO del 16 febbraio 2018)