SwissBanking

Agosto 2019, 2ª edizione

Linee guida dell'ASB per l'apertura di conti aziendali per imprese DLT

Indice

Prefazione **3**

1. Contesto di base e struttura delle Linee guida **4**

2. Domande in materia di *due diligence* per i clienti aziendali con nesso DLT **6**

3. Aspettative di carattere generale nei confronti degli emittenti di *token* ***8***

4. Aspettative nei confronti degli emittenti di *token* in caso di finanziamento con criptovalute **11**

5. Obblighi di diligenza in caso di finanziamento mediante monete a corso legale (*fiat*) **14**

6. Modelli operativi specifici **15**

Appendice – Glossario **17**

Prefazione

Negli ultimi anni il numero di aziende attive nel segmento della *Distributed Ledger Technology* («imprese DLT») è fortemente aumentato in Svizzera. L'Associazione svizzera dei banchieri (ASB) accoglie con favore questo sviluppo e valuta positivamente l'elevato dinamismo del mercato, in quanto un simile trend accresce l'attrattività della piazza produttiva e finanziaria elvetica. Le banche vedono la tecnologia *blockchain* come opportunità in grado di offrire un ampio ventaglio di possibilità per la piazza finanziaria e tecnologica svizzera.

Con l'aumento del numero di aziende DLT è cresciuta anche la domanda di conti aziendali presso le banche in Svizzera. Mentre lo sviluppo tecnologico in sé non rappresenta un rischio particolare e deve essere giudicato in modo tecnologicamente neutrale, l'apertura di conti comporta per le banche una serie di sfide. Le applicazioni specifiche DLT possono essere infatti correlate anche a rischi, in particolare nell'ambito del riciclaggio di denaro in caso di impiego di criptovalute, oppure anche per finalità di frode. In Svizzera sono in vigore rigorose disposizioni di legge e stringenti obblighi di diligenza che regolamentano le attività finanziarie. Per le banche è quindi previsto lo svolgimento di un'accurata verifica in occasione di un'apertura di conto.

Sotto la guida dell'ASB, un gruppo di lavoro ha sottoposto le «Linee guida per l'apertura di conti aziendali per imprese *blockchain*» del 2018 a un'incisiva rielaborazione sotto il profilo sia contenutistico che terminologico. Le Linee guida si propongono di fungere da supporto alle banche affiliate nei colloqui con le aziende interessate e, al contempo, di contribuire alla gestione del rischio nella conduzione delle relazioni d'affari. La pubblicazione delle presenti Linee guida è accolta con favore dal Dipartimento federale delle finanze (DFF) e dalla FINMA. La Crypto Valley Association (CVA) ha parimenti contribuito all'ulteriore sviluppo del documento sotto il profilo dei contenuti e ne sostiene l'attuazione nella prassi operativa.

1. Contesto di base e struttura delle Linee guida

Le Linee guida trattano i possibili requisiti che, in occasione dell'apertura di un conto aziendale, una banca può porre a un'impresa che presenta una correlazione con la cosiddetta *Distributed Ledger Technology* (DLT). Tali requisiti sono in parte più stringenti rispetto agli obblighi legali minimi attualmente in vigore a carico delle aziende con un nesso DLT, ma non perseguono l'obiettivo di emendare le normative applicabili e le direttive vigenti emanate dalle autorità competenti in materia.

Le Linee guida si basano sul principio secondo cui la regolamentazione per la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo così come ogni altra normativa trasversale sono applicabili per tutti gli intermediari finanziari coinvolti anche nel campo DLT. Gli obblighi antiriciclaggio a cui una banca è generalmente tenuta in occasione dell'apertura di conti aziendali si fondano quindi sulla versione attualmente vigente della Convenzione relativa all'obbligo di diligenza delle banche (CDB), dell'ORD-FINMA sul riciclaggio di denaro, della LRD e del CP svizzero, nonché sulle direttive specifiche interne delle singole banche. Le Linee guida si basano sulla CDB e ne costituiscono un'estensione, coprendo a titolo integrativo le questioni correlate all'ambito DLT. Ai fini della redazione della presente versione, le raccomandazioni del Gruppo di azione finanziaria internazionale (GAFI) pubblicate nel giugno 2019 sono state tenute in considerazione nella massima estensione possibile. Il presente documento verrà aggiornato secondo necessità in funzione degli sviluppi correnti.

Le Linee guida si prefiggono di definire le diverse peculiarità e le dinamiche in atto nelle aziende con nesso DLT. A seconda del grado di maturità dell'impresa e della strategia aziendale specifica, non tutte le raccomandazioni sono rilevanti ai fini dell'apertura di un conto o della tenuta ordinaria dello stesso. Ad esempio, una *start-up* finanziata in modo tradizionale può richiedere nella fase iniziale l'apertura di un conto aziendale e poi organizzare l'emissione di *token* soltanto dopo uno-due anni. Inoltre i clienti aziendali di lunga data possono decidere di offrire servizi mediante tecnologia *blockchain*, accettare criptovalute come mezzo di pagamento o, anche in questo caso, emettere nuovi *token*. In quest'ultimo scenario può trattarsi anche di aziende con un modello operativo senza nesso DLT che intendono finanziarsi attraverso questo canale.

Le Linee guida da un lato trattano quindi elementi specifici DLT nell'ambito del processo KYC, dall'altro definiscono una serie di aspettative concrete nei confronti degli emittenti di *token*. Di conseguenza, il documento opera una distinzione tra aziende con punti di contatto di carattere generale con la DLT e aziende con punti di contatto specifici con tematiche antiriciclaggio, in particolare per quanto concerne i c.d. *criptoasset* e l'emissione di *token*.

Ai fini dell'emissione di *token*, le Linee guida operano inoltre una differenziazione tra finanziamento attraverso criptovalute (di norma Bitcoin o Ethereum) e finanziamento mediante monete a corso legale (c.d. moneta *fiat*).

Le Linee guida coprono soltanto la fattispecie dell'emissione di *token* condotta da una società operativa con sede in Svizzera e si basano sulla Guida pratica della FINMA per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle *initial coin offering* (ICO) del 16 febbraio 2018. In caso di connessioni con Paesi esteri (ad es. partecipanti a un'emissione di *token* e ulteriori parti coinvolte con domicilio all'estero), i rischi risultanti dall'applicazione delle prescrizioni legali estere (diritto fiscale, penale, in materia di riciclaggio di denaro, sul mercato dei capitali, ecc.) devono essere adeguatamente rilevati, valutati e controllati.

La presente versione delle Linee guida non comprende la tenuta di conti denominati in *criptoasset* a favore dei clienti.

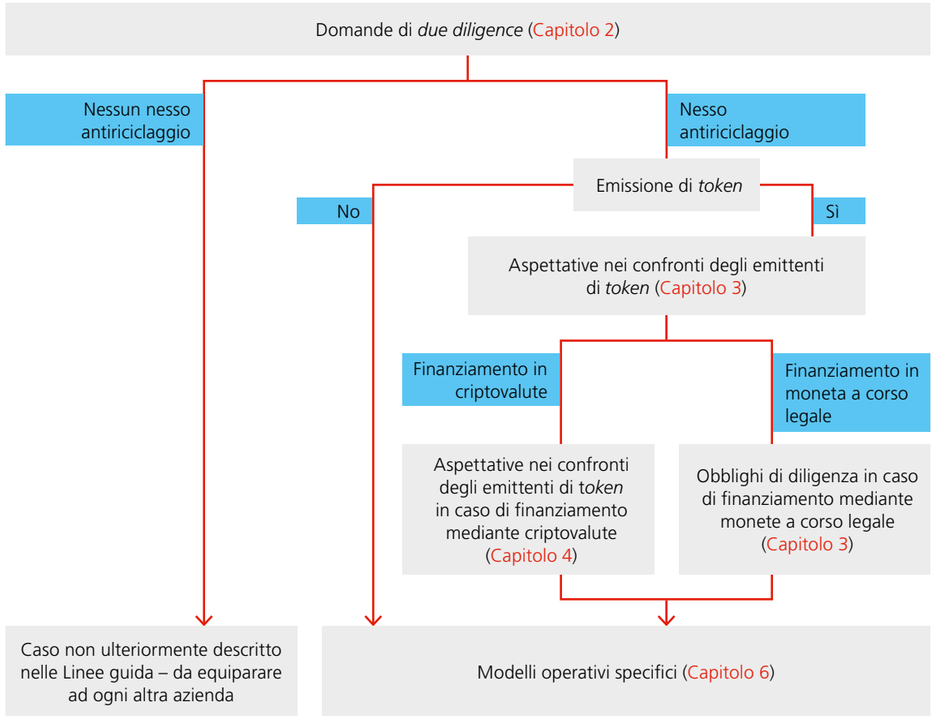
Le Linee guida si rivolgono esclusivamente ai membri dell'ASB. Le direttive interne di questi ultimi sono in ogni caso prevalenti. Il presente documento non definisce standard minimi validi per l'intero settore. L'interpretazione e/o l'applicazione concreta delle presenti Linee guida sono comunque subordinate al margine di discrezionalità di ogni singolo istituto in funzione della propria specifica propensione al rischio.

Non sussiste alcun diritto legale all'apertura di un conto nei confronti dei membri dell'ASB.

Le Linee guida vengono aggiornate ed estese con cadenza periodica.

Fig. 1

Struttura delle Linee guida



Fonte: ASB

2. Domande in materia di *due diligence* per i clienti aziendali con nesso DLT

Questo capitolo definisce le aspettative specifiche nell'ambito del processo KYC che derivano dalle connessioni di carattere generale dell'attività del cliente con la tecnologia DLT (con o senza emissione di *token*).

Si raccomanda di richiedere la presentazione dei documenti e dei giustificativi di seguito indicati prima dell'apertura di conti intestati a clienti commerciali. I punti elencati possono essere presi in considerazione anche nel momento in cui un conto per una società in costituzione viene convertito in un conto societario operativo.

Provvedimento / verifica	Raccomandazione
2.1 Nesso DLT	Descrizione esatta dei punti di contatto
2.2 Descrizione del modello operativo	• Descrizione esaustiva e comprensibile, basata su documentazione effettiva e affidabile come ad es. *White Paper* • Descrizione dei flussi di pagamento attesi • Descrizione degli iter procedurali previsti • In lingua nazionale/lingua commerciale • Indicazione della forma giuridica • Descrizione di eventuali *smart contract*, incl. *audit review* indipendente nel caso di *token* già esistenti, ai fini di un'ulteriore mitigazione dei rischi
2.3 Esclusione delle società di sede	• L'azienda attesta in modo dimostrabile di essere operativa (CDB 16) e di disporre di sostanza a livello locale. • In caso di nuova costituzione: l'azienda illustra il proprio progetto e scopo nonché le proprie aspettative in merito a entrate ed uscite correnti.
2.4 Competenze normative	L'azienda dispone di un interlocutore dedicato per tutte le questioni di *compliance* e assoggettamento e in particolare di: • conoscenze delle regolamentazioni/disposizioni rilevanti • una descrizione di come l'azienda recepisce le disposizioni normative rilevanti (direttive interne).
2.5 Validazione del modello operativo dopo l'apertura del conto	I titolari del conto sono tenuti a informare la banca in caso di cambiamento rilevante in merito all'impiego della tecnologia *blockchain* o a un'imminente emissione di *token*.
2.6 Suddivisione (*triage*)	• Se l'azienda non presenta elementi specifici in ambito di antiriciclaggio per le attività DLT (emissione di *token*, *criptoasset*): apertura del conto in conformità alle direttive interne, analogamente alle altre società operative. • Se l'azienda prevede l'emissione di *token* nel corso dei successivi dodici mesi: Procedere al Capitolo 3 (Emissione di *token*). • Se l'azienda non emette *token*, ma presenta comunque punti di attinenza in materia di antiriciclaggio specifici per le attività DLT: Procedere al Capitolo 6 (Modelli operativi specifici).

Le aziende che hanno già emesso *token* in precedenza, o comunque prima dell'apertura della relazione di conto, sono tenute a presentare su richiesta una documentazione completa del processo KYC/antiriciclaggio ai sensi del Capitolo 3 e del Capitolo 4 e ad attestare la conformità con il quadro normativo vigente in Svizzera.

3. Aspettative di carattere generale nei confronti degli emittenti di *token*

Questa sezione riguarda l'emissione di *token* (spesso detta anche *Token Generating Event* – TGE), indipendentemente dalla tipologia di finanziamento. In particolare viene trattata soltanto l'emissione di *token* da parte di una società operativa con sede in Svizzera.

La salvaguardia della reputazione e dell'integrità della piazza finanziaria e lavorativa svizzera riveste la priorità assoluta. Le raccomandazioni espresse nel Capitolo 3 e nel Capitolo 4 si fondano su questo obiettivo prioritario e al contempo sono funzionali anche a tutelare l'emittente di *token*.

Un'apertura di conto ai sensi del Capitolo 2 può essere effettuata già prima delle misure e delle verifiche descritte nel Capitolo 3 in relazione all'emissione di *token*. Un conto aziendale tradizionale può essere in seguito rimodulato in un «conto DLT» (utilizzato ad esempio per la raccolta di fondi nell'ambito di un'emissione di *token* e/o destinato a modelli operativi specifici ai sensi del Capitolo 6) a condizione che vengano rispettati gli obblighi di diligenza descritti nei seguenti capitoli. In tale ambito, se un conto aziendale utilizzato già in precedenza viene in seguito impiegato anche per il finanziamento o l'emissione di *token*, la banca deve adottare una serie di accorgimenti operativi tali da rendere possibile il flusso di fondi derivante dall'emissione di *token* soltanto dopo la conclusione con esito positivo delle necessarie verifiche.

La banca non effettua alcuna analisi di tipo giuridico circa la natura e il grado di maturità dei *token* e parte dal presupposto di un assoggettamento dell'emittente alla LRD. Laddove non sia presente un assoggettamento alla LRD, l'emittente dei *token* deve indicarlo alla banca e motivarlo adeguatamente. In caso di dubbio, l'emittente è tenuto a presentare un'attestazione specifica mediante una richiesta di assoggettamento a cui la FINMA ha dato riscontro. Dalla LRD derivano diversi obblighi di diligenza, nonché il dovere di affiliarsi a un organismo di autodisciplina (OAD) oppure di delegare la raccolta di valori patrimoniali a un intermediario finanziario assoggettato alla LRD in Svizzera.

Le direttive specifiche interne agli istituti possono prevedere ulteriori requisiti aggiuntivi. Tali direttive interne sono sempre prevalenti rispetto alle Linee guida.

Provvedimento / verifica	Raccomandazione
3.1 Descrizione (*token*)	• Descrizione dettagliata sia dei *token* di nuova emissione in conformità all'allegato della Guida pratica della FINMA per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle *initial coin offering* (ICO) del 16 febbraio 2018, sia del relativo stato di sviluppo (grado di maturità prima della distribuzione sul mercato, data di emissione). • Prima dell'emissione dei *token*, l'emittente dimostra che il progetto da finanziare esiste effettivamente e che i fondi in entrata sul conto provengono dall'emissione di *token* e saranno in seguito utilizzati per lo scopo espressamente indicato. • La documentazione dei *token*, perlopiù sotto forma di un *White Paper*, costituisce una componente fondamentale della *due diligence* della banca. Tale documento deve essere quindi consegnato entro il minor tempo possibile alla banca che gestisce il conto. • Contestualmente all'emissione dei *token*, l'emittente dà visibilità sul relativo funzionamento e sui dati correlati all'applicazione DLT. • *Audit review* tecnica da parte di un soggetto indipendente per un eventuale *smart contract* come ulteriore misura di mitigazione dei rischi.
3.2 Pianificazione della gestione della liquidità	Prima dell'emissione dei *token*, l'emittente informa la banca che gestisce il conto in merito ai seguenti punti: • Ripartizione attesa tra monete a corso legale e singole criptovalute nell'ambito della raccolta di capitale (scenario: ad es. 50% monete a corso legale, 25% Bitcoin, 25% Ethereum). • Importi e frequenza previsti con cui i fondi convertiti in moneta a corso legale vengono trasferiti presso la banca che gestisce il conto. • Procedura di rimborso se l'importo target non viene raggiunto (facendo riferimento alla relativa clausola contrattuale). • Presso quali *exchange* vengono convertite le criptovalute (cfr. punto 4.7).
3.3 Gestione dei rischi derivanti dalle giurisdizioni estere	Un emittente di *token* dispone di opportune linee guida e di misure adeguate al fine di escludere gli investitori domiciliati in determinati Paesi sulla base della normativa interna alla banca. In caso di emissione di *token* nell'ambito di una *Security Token Offering* (STO), l'emittente consegna alla banca che gestisce il conto un elenco dei Paesi target e attesta il costante e puntuale rispetto delle relative disposizioni normative locali. Su richiesta, l'emittente dei *token* mette queste informazioni a disposizione della banca.

3.4 Assoggettamento alla LRD	La banca parte dall'assunto di un assoggettamento alla LRD per l'emittente di *token*. Tale assoggettamento si fonda esclusivamente sulla Guida pratica FINMA in materia di ICO del 16 febbraio 2018. Laddove non sia presente un assoggettamento alla LRD, l'emittente dei *token* deve indicarlo alla banca e motivarlo adeguatamente. In caso di dubbio, egli è tenuto a presentare segnatamente una richiesta di assoggettamento a cui la FINMA ha dato riscontro. In caso di assoggettamento alla LRD, l'emittente di *token* deve fornire le seguenti evidenze: • Nome dell'OAD e conferma dell'affiliazione all'OAD stessa, oppure • In caso di delega: nome dell'intermediario finanziario, conferma della sua affiliazione all'OAD e conferma della delega. • Documentazione completa in conformità al regolamento interno di *compliance* della banca che gestisce il conto.
3.5 Obblighi dopo l'emissione	• Gli obblighi di natura giuridica derivano dalla LRD. • Su richiesta della banca, l'emittente attesta che l'impiego corrente dei fondi è conforme alla finalità preannunciata. • Su richiesta della banca, l'emittente attesta la conformità alle limitazioni di cui al punto 3.3 per quanto concerne i partecipanti esteri. • In linea di principio, ogni provvedimento volto alla creazione di trasparenza relativamente ai passaggi di possesso (dei *token*) dopo la conclusione dell'emissione dei *token* stessi è funzionale alla mitigazione dei rischi ed è accolto con favore dalla banca che gestisce il conto. Questo aspetto comprende la fornitura, su richiesta della banca, delle informazioni relative alle modalità di trasferimento dei *token*, laddove le stesse risultino disponibili. • Per i modelli operativi con elementi di collegamento alla LRD, l'affiliazione ad un OAD è obbligatoria.
3.6 Suddivisione (*triage*) in base alla tipologia di finanziamento	• Se l'emittente dei *token* organizza il finanziamento del tutto o in parte via *blockchain* / mediante criptovalute: Procedere al Capitolo 4 (Emissione di *token* in caso di finanziamento con criptovalute) • Se il finanziamento avviene esclusivamente mediante monete a corso legale: Procedere al Capitolo 5 (Obblighi di diligenza).

4. Aspettative nei confronti degli emittenti di *token* in caso di finanziamento con criptovalute

Questo capitolo descrive il processo di finanziamento d'impresa che avviene in parte o del tutto mediante criptovalute. Le presenti Linee guida partono dall'assunto che la banca che gestisce il conto non accetti criptovalute in maniera diretta.

L'emittente dei *token* dispone la conversione delle criptovalute in moneta a corso legale attraverso un *exchange* di diritto svizzero o regolamentato in modo equivalente oppure presso una banca di diritto svizzero o regolamentata in modo equivalente, e trasferisce poi i relativi fondi presso la banca che gestisce il conto.

Indipendentemente dall'assoggettamento alla LRD, in caso di accettazione di criptovalute le Linee guida raccomandano di richiedere all'emittente di *token* l'applicazione degli standard KYC, antiriciclaggio e in materia di sanzioni rilevanti in Svizzera per la raccolta di fondi.

Inoltre, l'accettazione di *token* di pagamento nell'ambito di un'emissione di *token* può essere sostanzialmente equiparata a un'operazione per cassa. A tale riguardo è tuttavia necessario considerare che ogni operazione viene registrata sulla *blockchain* e che quindi attraverso le transazioni in criptovalute sussiste un rischio di violazione di sanzioni a prescindere dal relativo importo. Ulteriori obblighi derivano dalla struttura del *token* e/o da un assoggettamento alla LRD.

Le direttive specifiche degli istituti possono prevedere requisiti supplementari o definire valori di soglia divergenti da quelli fissati nelle Linee guida. Le direttive interne sono sempre prevalenti rispetto alle Linee guida.

Provvedimento / verifica	Raccomandazione
4.1 Criptovalute accettate	La criptovaluta deve essere idonea in linea di principio a un'analisi di *wallet*. Eventuali deroghe devono essere debitamente motivate.
4.2 Emittente di *token* (in generale)	I dati di ogni sottoscrittore che gli emittenti di *token* sono tenuti a raccogliere sono desumibili in via generale dai requisiti fissati nelle normative applicabili (ad es. LRD, ORD-FINMA, regolamenti OAD e Circolare Video identificazione e identificazione online della FINMA). Sulla base di tali disposizioni, l'emittente deve quindi raccogliere le seguenti informazioni: nominativo, indirizzo (incl. Paese), data di nascita, nazionalità e luogo di nascita. Le informazioni raccolte dovrebbero comprendere anche i relativi indirizzi del *wallet* (chiave pubblica) dal quale gli investitori inviano i fondi. A prescindere dall'obbligo di assoggettamento LRD dell'emittente, ci si attende che almeno a partire da un importo di sottoscrizione di CHF 15 000 venga effettuata un'identificazione e un accertamento degli aventi diritto economico ai sensi di LRD / ORD-FINMA / CDB. Ogni ulteriore misura volta all'incremento della trasparenza è funzionale alla mitigazione del rischio, soprattutto alla luce di possibili violazioni di sanzioni. I dati rilevati in sede di identificazione comprendono inoltre i relativi indirizzi di *wallet* che l'investitore utilizza per il versamento dei fondi. In linea di principio è opportuno documentare l'identificazione e la titolarità del diritto economico in maniera analoga ai processi in essere all'interno del rispettivo istituto. Se la banca intende richiedere all'emittente la documentazione relativa agli investitori, tale fattispecie deve essere regolamentata nel contratto tra la banca stessa e l'emittente di *token*. A tale riguardo, la banca è tenuta a salvaguardare adeguatamente i dati personali degli investitori (sottoscrittori / partecipanti / percettori di *token*). L'identificazione dell'avente diritto economico dovrebbe avvenire in modo conforme ai processi vigenti del rispettivo istituto. Il controllo della titolarità del diritto economico sui valori patrimoniali può essere confermato mediante la richiesta di una transazione digitalmente firmata o di una microtransazione utilizzando la chiave pubblica dell'emittente. L'emittente può far registrare il processo o l'esecuzione di una microtransazione sulla *blockchain*.

4.3 Emittenti di *token* di pagamento (caso specifico)	Gli emittenti di *token* di pagamento sono assoggettati alla LRD. Essi devono pertanto ottemperare alla procedura per l'accettazione di valori patrimoniali da parte degli investitori ai sensi delle disposizioni del diritto in materia di lotta al riciclaggio di denaro, sancite tra l'altro nella LRD e nella Circolare FINMA 2016/7 Video identificazione e identificazione online, nonché nei regolamenti degli organismi di autodisciplina. Per gli emittenti di *token* di pagamento, nel caso di transazioni di importo inferiore a CHF 3000 trovano applicazione gli obblighi di diligenza semplificati ai sensi dell'art. 12 cpv. 2 lett. d ORD-FINMA; nella fattispecie, non è necessario richiedere un'autenticazione per le copie dei documenti d'identificazione degli investitori.
4.4 Verifica delle banche	Raffronto dei nominativi dei sottoscrittori con le consuete banche dati (in particolare elenchi relativi a PEP, attività antiterrorismo e sanzioni) da parte dell'emittente di *token*. Su richiesta, tali risultati vengono messi a disposizione della banca unitamente alle direttive interne in materia di monitoraggio dei PEP e dei nominativi oggetto di sanzioni.
4.5 Verifica del *background* (provenienza dei fondi) e stima del rischio degli indirizzi di *wallet* utilizzati dagli investitori (antiriciclaggio)	In generale, per l'emittente è raccomandabile adottare un approccio basato sul rischio per quanto concerne la verifica del *background*. Una tracciabilità generale della provenienza dei fondi sulla *blockchain* non è al momento richiesta. In linea di principio, ogni ulteriore elemento di trasparenza apportato dall'emittente è funzionale alla mitigazione del rischio. Soprattutto in casi particolari o in presenza concreta di elementi di sospetto è opportuno effettuare una verifica approfondita attraverso un'analisi del *wallet* o la raccolta di ulteriore documentazione (ad es. *due diligence* approfondita in luogo di una semplice consultazione della banca dati a fronte di importi d'investimento elevati o di domicilio in un Paese a rischio elevato). Una verifica approfondita da parte dell'emittente è raccomandata in ogni caso per le sottoscrizioni di importo superiore a CHF 100 000 (in un'unica soluzione o cumulativamente). Questa verifica approfondita comprende il legame univoco documentato tra indirizzo del *wallet* e investitore. Prima dell'entrata dei fondi, la banca che gestisce il conto può riservarsi la facoltà di richiedere le suddette indicazioni relative agli investitori e, in presenza di elementi di sospetto concreti, può parimenti disporre ulteriori accertamenti da parte dell'emittente (ad es. ottenimento di analisi specifiche del *wallet*).

4.6	Certificato di qualità della verifica KYC / antiriciclaggio	A prescindere dall'assoggettamento alla LRD si raccomanda di effettuare le verifiche KYC / antiriciclaggio in conformità agli standard vigenti. Un emittente non assoggettato alla LRD deve pertanto rivolgersi a tale scopo a un intermediario finanziario o a un'azienda specializzata in *compliance* LRD. Su richiesta della banca che gestisce il conto, tali evidenze vengono messe a disposizione; l'emittente deve parimenti documentare il rispetto delle direttive in materia di PEP interne all'azienda.
4.7	*Exchange* per la conversione di criptovalute in monete a corso legale	I *crypto exchange* e la conversione delle criptovalute in monete a corso legale rappresentano un rischio particolare per le banche, in quanto da una prospettiva LRD le criticità si concentrano proprio in questo ambito. Di conseguenza, le banche devono imporre a un *exchange* una serie di requisiti di mitigazione dei rischi: ad esempio, deve trattarsi di un *exchange* di diritto svizzero o regolamentato in modo equivalente oppure di una banca terza di diritto svizzero o regolamentata in modo equivalente. La definizione di «regolamentazione equivalente» deve fondarsi sulle direttive interne della rispettiva banca.
4.8	Sospetto di riciclaggio di denaro	In caso di sospetto di riciclaggio di denaro, l'investitore non viene ammesso (salvo laddove ciò sia giuridicamente obbligatorio a seguito del divieto di *tipping-off* dopo avvenuta comunicazione al MROS, art. 9a LRD). La responsabilità per l'esclusione compete all'emittente di *token*. Ai fini dei necessari accertamenti nell'ambito delle procedure KYC o di *due diligence* a carico di un emittente di *token*, la banca che gestisce il conto può derogare al segreto bancario sulla base di un apposito consenso rilasciato dal cliente bancario nel contratto o mediante *waiver* separato. La banca è tenuta a indicare esplicitamente questa fattispecie ai clienti commerciali; di conseguenza, si raccomanda agli emittenti di dichiarare la stessa in modo trasparente ai propri sottoscrittori nei *Terms & Conditions*.
4.9	Disposizioni in materia di sanzioni	L'emittente si attiene scrupolosamente alle disposizioni in materia di sanzioni (ad es. Legge sugli embarghi).

5. Obblighi di diligenza in caso di finanziamento mediante monete a corso legale (*fiat*)

In caso di finanziamento mediante monete a corso legale trovano applicazione i valori di soglia definiti nel Capitolo 4 nonché gli obblighi di identificazione e accertamento degli aventi diritto economico ai sensi di LRD / ORD-FINMA / CDB.

6. Modelli operativi specifici

Nel suo rapporto «Basi giuridiche per le tecnologie di registro distribuito e *blockchain* in Svizzera» del 14 dicembre 2018, il Consiglio federale ha stabilito che le seguenti attività DLT (in aggiunta all'emissione di *token* già trattata nel Capitolo 3 e nel Capitolo 4) sono assoggettate alla LRD laddove l'attività in questione venga esercitata a titolo professionale (art. 7 LRD):

- I fornitori di *wallet* che detengono in custodia le chiavi private dei clienti e consentono ai clienti stessi di inviare e ricevere criptovalute hanno il potere di disporre su valori patrimoniali di terzi e devono essere quindi classificati come intermediari finanziari assoggettati alle disposizioni antiriciclaggio. Attualmente non è prevista una regolamentazione specifica per i fornitori di *wallet* che non gestiscono la custodia e che non hanno possibilità d'intervento ai fini della trasmissione dei *token*.
- I gestori di piattaforme di negoziazione che hanno accesso alle chiavi private dei clienti e quindi hanno anche potere di disporre sui valori patrimoniali di terzi, oppure lavorano sulla base di *smart contract* che possono disporre di valori patrimoniali attraverso la conferma, l'approvazione o il blocco di ordini, fungono da intermediari fra i clienti nell'ambito di un rapporto trilaterale. Di conseguenza, le disposizioni antiriciclaggio trovano applicazione anche per tali piattaforme di negoziazione centralizzate. Le piattaforme di negoziazione che non presentano le caratteristiche suindicate e sono quindi strutturate in maniera del tutto decentralizzata (ovvero non prevedono alcuna possibilità di influenza da parte dello sviluppatore della piattaforma) non sono assoggettate alle disposizioni antiriciclaggio.

La valutazione del rischio specifico dei clienti commerciali che erogano servizi in relazione a criptovalute o *token* attraverso uffici di cambio o piattaforme di negoziazione centralizzate può essere agevolata dalla considerazione di alcuni dei seguenti elementi:

Provvedimento / verifica	Raccomandazione
6.1 Conversione di criptovalute in moneta a corso legale (*fiat*)	Operazioni svolte attraverso un *exchange* di diritto svizzero o regolamentato in modo equivalente, oppure di una banca terza di diritto svizzero o regolamentata in modo equivalente. La definizione di «regolamentazione equivalente» deve fondarsi sulle direttive interne della rispettiva banca.
6.2 Antiriciclaggio / Conformità alle sanzioni	Programma antiriciclaggio / di monitoraggio sanzioni conforme alle disposizioni svizzere per l'*onboarding* e il monitoraggio corrente delle transazioni.
6.3 Programma antiriciclaggio	Interlocutore dedicato e qualificato per le questioni di *compliance*.
6.4 Negoziazione	Su richiesta della banca che gestisce il conto, la piattaforma di negoziazione indica che i valori patrimoniali negoziati sono conformi ai requisiti di registrazione del rispettivo Paese di riferimento (ad es. valori patrimoniali di diritto statunitense).
6.5 Vigilanza	Il fornitore di servizi è assoggettato alla regolamentazione antiriciclaggio nella versione attualmente in vigore.
6.6 Autorizzazione	Si fonda sui modelli di licenza esistenti (ad es. licenza *fintech*).
6.7 Segmento di clientela	Su richiesta, la piattaforma di negoziazione DLT mette a disposizione ulteriori informazioni sulla struttura della propria clientela, come ad es. ripartizione in base al volume delle transazioni / provenienza geografica.

- Uffici di cambio: l'attività svolta a titolo professionale di compravendita di criptovalute o *token* come controprestazione per moneta a corso legale o altri *criptoasset* costituisce un'attività di scambio bilaterale assoggettata alla regolamentazione antiriciclaggio.
- I criptofondi, intesi come investimenti collettivi di capitale che allocano il loro patrimonio prevalentemente o esclusivamente in *criptoasset*, sono equiparati agli altri investimenti collettivi di capitale ai sensi delle disposizioni in materia di lotta al riciclaggio di denaro.

Nel caso di aziende che offrono la possibilità di usufruire dei loro servizi o prodotti dietro pagamento in criptovalute si raccomanda di basarsi sulle verifiche del *background* di cui al punto 4.5 e/o sui valori di soglia raccomandati al punto 4.2.

Appendice – Glossario

Token

In parole semplici, i *token* sono unità di informazioni digitali protette mediante crittografia che vengono iscritte in un registro basato su DLT. La FINMA classifica i *token* in base alla loro funzione economica, operando una distinzione fra *token* di pagamento, d'investimento e di utilizzo. Cfr. anche Guida pratica della FINMA per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle *initial coin offering* (ICO) del 16 febbraio 2018.

Distinzione fra ICO, ITO, TGE, STO, IEO

Non esiste ancora un consenso universale per la terminologia specifica: *Initial Coin Offering* (ICO), *Initial Token Offering* (ITO), *Token Generating Event* (TGE), *Security Token Offering* (STO), *Initial Exchange Offering* (IEO). L'accento è posto sull'emissione di unità di informazioni e/o di funzioni digitali, trasferibili e uniche (*coin* o *token*) che possono rappresentare una vasta gamma di diritti: fungibili come diritti di credito e societari verso un'azienda, su cose, oppure altri diritti assoluti o relativi.

Un *token* può anche fungere solo da mezzo di pagamento (*Coin Payment Token*) senza che ai detentori vengano riconosciuti altri diritti specifici. Laddove i *token* incorporino esplicitamente diritti nei confronti dell'emittente, viene utilizzato piuttosto il concetto di STO («*Security Token Offering*»). Come metodo di raccolta di capitale presso un'organizzazione che emette per la prima volta dei *token* per finalità di finanziamento si presuppone spesso l'attuazione di un'ICO («*Initial Coin Offering*») ovvero, in termini tecnici più puntuali, di un'ITO («*Initial Token Offering*»). A seconda della configurazione, i *token* possono costituire anche un diritto valore DLT e/o essere classificati come valori mobiliari ai sensi della legislazione finanziaria vigente.

Una IEO è una tipologia di raccolta di capitale che viene attuata solo attraverso un *exchange* e per la quale l'*exchange* stesso si fa carico della raccolta dei fondi e della contestuale emissione dei *token* per conto dell'emittente.

Nelle presenti Linee guida i termini di TGE e di emissione di *token* vengono usati come sinonimi e in modo interscambiabile.

Chain analysis
La *chain analysis* persegue lo scopo di verificare da quale fonte provengono i valori patrimoniali in criptovalute. Può essere preso in considerazione un ampio ventaglio di criteri, ad es. pagamenti in uscita o in entrata su determinati *wallet*, attinenze con il Darknet, con c.d. *mixer* e *tumbler* e con pagine web specializzate in frodi (*scam*) o in gioco d'azzardo (*gambling*), nonché transazioni da Paesi ad alto rischio. Può essere parimenti presa in considerazione una classificazione del rischio delle piazze di negoziazione dalle quali vengono alimentati i *wallet* in questione.

Distributed Ledger Technology (DLT) / Blockchain
La *Distributed Ledger Technology* (DLT) consente una gestione dei dati congiunta e sicura in una rete (decentralizzata) di computer. In parole semplici, un *Distributed Ledger* è una banca dati (libro mastro) gestita su una molteplicità di calcolatori interconnessi, in grado di sincronizzare e validare in modo sostanzialmente autonomo e continuativo le transazioni / i dati immessi dai partecipanti. Questi ultimi hanno a disposizione in qualsiasi momento una cronologia immutabile, a prova di manipolazioni e con tutte le informazioni verificabili e archiviate in un determinato record di dati. Il concetto di DLT ha una portata più ampia rispetto a quello di *blockchain* e comprende ulteriori modalità di configurazione.

Blockchain (applicazione DLT)
Le *blockchain* sono una possibile forma di *Distributed Ledger Technology* (DLT) e rappresentano registri digitali o banche dati costantemente ampliabili e non modificabili. Una rete di calcolatori interconnessi (nodi di rete, «*nodes*») esegue il protocollo del *software*: le transazioni o anche altri dati vengono raccolti in blocchi in modo sostanzialmente autonomo e continuativo e poi verificati e aggiunti alla catena esistente di blocchi già validati. La *blockchain* viene utilizzata ad es. per le transazioni in Bitcoin, Ethereum e altre criptovalute. Per rendere possibile la concatenazione dei blocchi, la *blockchain* impiega una chiave crittografica denominata «*hash*». Per tale chiave vengono utilizzate procedure di cifratura (asimmetriche) che per ogni utente sono costituite da una chiave pubblica e una chiave privata («*public key*» e «*private key*»). Gli utenti amministrano la coppia di chiavi pubblica-privata mediante cosiddetti *wallet* (portafogli), i quali possono essere basati su diversi supporti (*wallet* online, per *desktop* o *smartphone*, in formato cartaceo o *hardware*). Una *blockchain* pubblica (*public*) è strutturata in modo decentralizzato, è accessibile a tutti e viene gestita senza intermediari da una molteplicità di partecipanti anonimi (esempi a riguardo: Bitcoin ed Ethereum). Per contro, una *blockchain* privata è gestita da uno o più amministratori di rete ed è accessibile soltanto a partecipanti debitamente identificati e autorizzati. Esistono inoltre forme miste come le *blockchain* consortili, per le quali solo determinate istanze possono validare le transazioni, mentre il protocollo può essere anche pubblico.

Exchange
Presso gli *exchange* (uffici di cambio) le criptovalute possono essere convertite in monete a corso legale convenzionali (come il CHF), oppure in altre criptovalute.

Criptoasset / «digital asset»
I *criptoasset* sono valori digitali (valori patrimoniali criptobasati) archiviati nell'ambito di un'applicazione DLT e protetti mediante crittografia, il cui contenuto risulta documentato in maniera univoca (ad es. criptovalute o diritti valori digitali). Un *token* rappresenta l'informazione registrata nel *ledger* della quale il proprietario può disporre mediante un codice di accesso. A differenza delle monete a corso legale emesse da una banca centrale (come il dollaro statunitense o il franco svizzero), una criptovaluta esiste come mezzo di pagamento soltanto in forma digitale. Le criptovalute più note e diffuse sono attualmente il Bitcoin e l'Ethereum, ognuna dotata di un proprio sistema di pagamento. A seconda della struttura intrinseca, un *token* può essere collegato ad altri valori (ad es. valute, *commodity*, titoli mobiliari) e rappresentare gli stessi come *digital asset* (ad es. «*asset backed token*»).

Smart contract
Protocolli informatici autoeseguenti basati su *blockchain* che contengono condizioni contrattuali predefinite nel codice di programma. Una transazione gestita attraverso *smart contract* viene eseguita automaticamente laddove tutte le parti coinvolte adempiano alle condizioni precedentemente definite. Attraverso uno *smart contract* è possibile replicare, verificare o supportare sotto il profilo tecnico l'esecuzione del contenuto di contratti con valenza giuridica. Il protocollo informatico supervisiona automaticamente le condizioni registrate e, in presenza di un determinato evento («*trigger event*»), esegue autonomamente le azioni concordate tra le controparti. A seconda della loro configurazione, gli *smart contract* possono costituire essi stessi contratti con valenza giuridica.

SwissBanking

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Casella postale 4182
CH-4002 Basilea

office@sba.ch
www.swissbanking.org