

Descrizione dei Wallet Omnibus, dei relativi rischi e dei presidi adottati dalla Società

1. Descrizione dei Wallet Omnibus

Il servizio di custodia è prestato mediante un modello fondato sull'utilizzo di Wallet Omnibus, ossia portafogli digitali sui quali sono detenute Cripto-attività riferibili a una pluralità degli Utenti, con registrazione nominativa delle posizioni individuali all'interno del Registro delle Posizioni.

Tale registro, tenuto dalla Società e aggiornato in tempo reale, consente di individuare il saldo e i diritti di ciascun Utente sulle Cripto-attività custodite, pur in assenza di una segregazione *on-chain* per singolo Utente mediante indirizzi *blockchain* individuali.

Le Cripto-attività degli Utenti sono quindi detenute all'interno di *wallet* condivisi, ma le relative posizioni sono segregate e attribuite nominativamente nei sistemi interni della Società. In questo senso, il modello distingue tra la dimensione tecnica della custodia, nella quale le Cripto-attività sono aggregate all'interno di uno o più Wallet Omnibus, e la dimensione contabile e giuridica della titolarità, nella quale le disponibilità riferibili a ciascun Utente sono registrate separatamente nel Registro delle Posizioni.

Sotto il profilo operativo e di sicurezza, l'infrastruttura di custodia combina l'utilizzo di *cold wallet*, non connessi alla rete Internet e destinati alla conservazione prevalente delle Cripto-attività, e *hot wallet*, connessi all'infrastruttura operativa della Società e funzionali alla gestione dell'operatività ordinaria. Tutti i *wallet* impiegati dalla Società sono di tipo *omnibus*; le disponibilità individuali sono tracciate attraverso il Registro delle Posizioni aggiornato in tempo reale e la generazione e gestione delle chiavi private è soggetta a controlli di sicurezza rafforzati.

Il modello non comporta il trasferimento della proprietà delle Cripto-attività alla Società. Cryptosmart agisce infatti su istruzioni impartite dall'Utente, non diviene proprietaria delle Cripto-attività custodite e non le utilizza per conto proprio. Le Cripto-attività e i fondi degli utenti sono segregati rispetto al patrimonio della Società, sia sul piano operativo, mediante l'utilizzo di *wallet* e conti dedicati agli utenti distinti da quelli della Società, sia sul piano legale e contabile, mediante registrazioni nominative e contabilità separata attestante i diritti degli Utenti.

2. Profili di rischio e presidi adottati dalla Società

Rischio di concentrazione

Un eventuale incidente operativo o di sicurezza che interessi un *wallet omnibus* potrebbe avere impatto su una pluralità degli Utenti.

Presidi adottati – la Società mantiene la parte prevalente delle cripto-attività in *cold wallet* caratterizzati da sistemi di firma multipla (*multisig*) sui Cold Wallet. La Società, inoltre, applica soglie massime di giacenza sugli Hot Wallet; trasferendo automaticamente verso i Cold Wallet le eccedenze non necessarie per l'operatività ordinaria. In tal modo viene limitata la quantità di Cripto-attività esposta *online* e ridotto l'impatto potenziale di eventi che dovessero interessare i *wallet* operativi.

Rischio legato ai sistemi interni di registrazione

Nel modello basato su Wallet Omnibus, la corretta attribuzione delle disponibilità al singolo Utente dipende dal corretto funzionamento dei sistemi interni con cui la Società registra le operazioni e aggiorna il Registro delle Posizioni. Un malfunzionamento di tali sistemi potrebbe comportare errori nell'attribuzione delle posizioni.

Presidi adottati – la Società mantiene un Registro delle Posizioni per singolo Utente; effettua riconciliazioni periodiche, almeno giornaliere, tra le risultanze dei propri sistemi e le consistenze effettivamente detenute; conserva la tracciabilità delle operazioni tramite *audit trail*; mantiene dei *backup* del registro delle Posizioni; applica controlli operativi e di secondo livello; adotta procedure per la gestione di anomalie, rettifiche e verifiche. Ne deriva che sia la Società, che l'Utente, possono verificare, in ogni momento, le relative giacenze.

Rischio di non immediata evidenza on-chain individuale

La posizione dell'Utente non coincide necessariamente con una giacenza immediatamente verificabile su un singolo indirizzo *blockchain* personale.

Presidi adottati – la Società assicura la tracciatura nominativa della posizione dell'Utente nei propri sistemi; effettua la riconciliazione tra le disponibilità registrate a favore dell'Utente e quelle complessivamente detenute; garantisce all'Utente la possibilità di consultare le proprie disponibilità tramite la Piattaforma e la relativa rendicontazione.

Rischio di ritardi o limitazioni operative

Alcune operazioni, in particolare depositi e prelievi, possono essere soggette a tempi tecnici, a controlli di sicurezza, a verifiche interne, al numero di conferme richieste sulla *blockchain* o a trasferimenti tra Hot Wallet e Cold Wallet.

Presidi adottati – la Società adotta procedure operative formalizzate; effettua controlli preventivi sui prelievi; utilizza sistemi di monitoraggio continuo; prevede processi di *escalation* e gestione degli eventi operativi.

Rischio cyber residuo sugli hot wallet

Gli Hot Wallet, essendo collegati all'infrastruttura operativa, presentano un rischio *cyber* residuo più elevato rispetto a quello ascrivibile ai Cold Wallet. Tale rischio può riguardare, ad esempio, accessi abusivi, compromissioni tecniche o altri eventi di sicurezza informatica che potrebbero comportare la perdita delle Cripto-attività custodite.

Presidi adottati – come diffusamente rappresentato, la Società limita le disponibilità mantenute sugli Hot Wallet; applica misure di autenticazione forte; adotta controlli sugli accessi e sui prelievi; utilizza meccanismi di *whitelisting* degli indirizzi autorizzati; monitora continuamente l'operatività; mantiene sistemi di *logging*, gestione incidenti e risposta agli eventi di sicurezza.

Rischio di errata segregazione rispetto al patrimonio della Società

Sebbene il modello di Wallet Omnibus non implichi, di per sé, una commistione giuridica tra le Cripto-attività della clientela e il patrimonio della Società, sussiste il rischio che eventuali errori di configurazione dei *wallet*, delle registrazioni interne o dei processi contabili possano incidere sulla corretta separazione tra *asset* della clientela e *asset* propri della Società. Tale rischio assume particolare rilievo in scenari patologici, quali insolvenza, procedure concorsuali, accertamenti da parte di terzi o contestazioni sulla titolarità delle Cripto-attività.

Presidi adottati – La Società prevede che le Cripto-attività e i fondi degli utenti siano segregati rispetto al patrimonio della Società, mediante *wallet* e conti dedicati agli Utenti, registrazioni nominative e contabilità separata attestante i diritti degli Utenti. In caso di insolvenza, le cripto-attività e i fondi degli utenti restano nella disponibilità dei legittimi titolari e sono restituiti agli aventi diritto sulla base del Registro delle Posizioni e dei registri rilevanti.

Rischio di errore nell'esecuzione di trasferimenti da Wallet Omnibus

L'utilizzo di Wallet Omnibus comporta che le operazioni in uscita siano eseguite tecnicamente a partire da *wallet* condivisi. In tale contesto, un errore nella selezione dell'*asset*, dell'importo, della *blockchain*, dell'indirizzo di destinazione o della posizione interna dell'Utente potrebbe determinare l'esecuzione di un trasferimento DLT non coerente con l'istruzione ricevuta. Considerata l'irreversibilità delle transazioni su DLT, l'errore potrebbe non essere recuperabile una volta che la transazione sia stata validata sulla *blockchain*.

Presidi adottati – La Società adotta controlli preliminari sulle istruzioni di trasferimento, volti a verificare la completezza dei dati, la disponibilità delle Cripto-attività, la coerenza dell'istruzione con le procedure interne e l'eventuale sussistenza di cause di rifiuto o sospensione. La *policy* di trasferimento prevede che l'Utente debba fornire i dati necessari per l'operazione, quali *wallet address*, importo e tipo di cripto-attività, e che la Società possa rifiutare l'istruzione in caso di dati mancanti, non validi, disponibilità insufficienti, motivi di sicurezza o casi previsti dalla normativa antiriciclaggio. La Società adotta apposite misure operative per evitare errori nell'esecuzione di trasferimenti da Wallet Omnibus.

Rischio di dipendenza dalla corretta gestione delle chiavi private

Nel modello di Wallet Omnibus, la perdita, compromissione, indisponibilità o errata gestione delle chiavi private può avere impatto non solo su una singola posizione individuale, ma su tutte le cripto-attività detenute nel *wallet* interessato. Il rischio è rilevante perché la chiave privata costituisce il mezzo tecnico essenziale per disporre delle Cripto-attività custodite.

Presidi adottati – La Società utilizza soluzioni di custodia fondate su meccanismi di firma distribuita e sistemi multi-firma/MPC, in modo che nessun soggetto disponga autonomamente dell'intera chiave privata o del *quorum* necessario per movimentare unilateralmente le Cripto-attività. L'architettura è basata su *key share* allocate in parte presso l'infrastruttura sicura del *provider* tecnologico e in parte presso l'infrastruttura di Cryptosmart; è disponibile un pacchetto di *backup* e recupero delle chiavi crittografiche per scenari di necessità.

